Université Paris Cité

École doctorale Sciences Mathématiques de Paris-Centre (386)
IMJ-PRG

L-functions and rational points for Galois twists of modular curves

Par Élie Studnia

Thèse de doctorat de Mathématiques

Dirigée par Loïc MEREL

Présentée et soutenue publiquement le 06/11/2024

Devant un jury composé de :

M^me^ Anna Cadoret, Professeur des Universités	Sorbonne Université	examinatrice
M. Loïc Merel, Professeur des Universités	IMJ-PRG	directeur
M^me^ Giada Grossi, CR	Université Sorbonne Paris Nord	examinatrice
M. Vincent Pilloni, DR	Université Paris-Saclay	examinateur
M. Jan Vonk, Professor	Universiteit Leiden	examinateur
M. Pierre Parent, MCF-HDR	Université de Bordeaux	rapporteur
M. Henri Darmon, Professor	McGill University	rapporteur (excusé)

Institut de mathématiques de Jussieu-Paris Rive gauche. UMR 7586.
Boîte courrier 247
4 place Jussieu
75 252 Paris Cedex 05

Université Paris Cité.
École doctorale de sciences mathématiques de Paris centre.
Boîte courrier 290
4 place Jussieu
75 252 Paris Cedex 05

Résumés

Fonctions L et points rationnels de tordues galoisiennes de courbes modulaires

Résumé

Dans cette thèse, on discute de l'existence de courbes elliptiques sur une base générale pour lesquelles la p-torsion est un schéma en groupes fixé (où p est un nombre premier). On prouve tout d'abord que ce problème est représentable au sens de Katz-Mazur par une courbe affine lisse, puis on décrit une autre manière de construire sa compactification sur un corps, comme la tordue de X(p) par une représentation galoisienne bidimensionnelle modulo p. On étudie ensuite la fonction L d'une telle courbe modulaire tordue sur le corps des rationnels et le signe de l'équation fonctionnelle conjecturalement satisfaite par ses facteurs. Lorsque la représentation galoisienne possède une petite image, on affine cette décomposition et on montre que les fonctions L de chacun des facteurs satisfont des équations fonctionnelles dont on détermine le signe. Grâce au système d'Euler de Beilinson-Flach, et en étendant des résultats de grande image galoisienne dûs à Loeffler, on montre la conjecture de Bloch-Kato en rang zéro pour chaque facteur sans multiplication complexe, et on applique ce résultat pour contrôler explicitement la mauvaise réduction de courbes elliptiques pour laquelle l'image de Galois est contenue dans le normalisateur d'un sous-groupe de Cartan non déployé, sous une hypothèse supplémentaire de non-annulation de certaines fonctions L de Rankin-Selberg, que l'on sait vérifier dans certains cas.

Mots-clés

points rationnels, courbes modulaires, formes modulaires, courbes elliptiques, représentations galoisiennes, fonctions L, systèmes d'Euler, modularité

L-functions and rational points on Galois twists of modular curves

Abstract

In this thesis, we discuss the existence of elliptic curves over a general base scheme for which the p-torsion is a given finite étale scheme, where p is a given prime. We first prove that this problem is representable in the sense of Katz and Mazur by a smooth affine curve, then describe another way to construct the compactification of such a curve over a base field, as a twist of X(p) by a two-dimensional Galois representation modulo p. We then study the L-function of such a twisted modular curve over the field of rationals and compute the sign of the functional equation that its factors are conjectured to satisfy. When the aforementioned Galois representation has small image, we show that this decomposition can be refined further, and we prove that the associated L-functions satisfy a functional equation whose sign we also determine. We then demonstrate the rank zero Bloch-Kato conjecture for every such factor without complex multiplication using the Euler system of Beilinson-Flach elements and extending big Galois image results due to Loeffler. We finally provide an application of such a result by giving an explicit bound on the bad reduction of elliptic curves such that the image of the Galois action on its p-torsion is contained in the normalizer of a nonsplit Cartan subgroup, under the additional hypothesis that certain Rankin-Selberg L-functions do not vanish, which is known to hold in certain cases.

Keywords

Rational points, modular curves, modular forms, Galois representations, Euler systems, elliptic curves, L-functions, modularity

Contents

Introduction **1**

1 Existing work . . . 1
- 1.1 Background . . . 1
- 1.2 Existing work about congruences of elliptic curves . . . 3
- 1.3 Finding rational points on modular curves: methods and results . . . 6

2 Basic results of this thesis (Chapters 1-2) . . . 8
- 2.1 Chapter 1: Moduli problems . . . 8
- 2.2 Chapter 2: Hecke and $\mathrm{GL}_2(\mathbb{F}_p)$-structure of $J(p,p)$ . . . 11

3 Results on the twisted modular Jacobians (Chapters 3-4) . . . 12
- 3.1 Chapter 3: The Tate module of the $J_E^{\alpha}(p)$ . . . 12
- 3.2 Chapter 4: Galois-theoretic root numbers for $(V_{f,\lambda} \otimes R_{f,E})_{\lambda}$ and $(V^{\epsilon}_{f,\lambda,E})_{\lambda}$ 13
- 3.3 Chapter 4: Automorphic properties of the $(V_{f,\lambda} \otimes R_{f,E})_{\lambda}$ and $(V^{\epsilon}_{f,\lambda,E})_{\lambda}$ . . 14

4 When the image of ρ is contained in the normalizer of a nonsplit Cartan subgroup (Chapter 5) . . . 15
- 4.1 Decomposition of the Tate module and functional equation . . . 15
- 4.2 The Bloch-Kato conjecture in rank zero for the factors of $J_E^{\alpha}(p)$ . . . 16
- 4.3 The formal immersion theorem . . . 16
- 4.4 Application to congruences to the CM elliptic curve $y^2 = x^3 - p$ . . . 17

5 Large image results for the Rankin-Selberg convolution of two modular forms (Chapter 6) . . . 18

Résumé de la thèse **21**

1 Résultats de base (Chapitres 1-2) . . . 21
- 1.1 Chapitre 1 : les problèmes de modules . . . 21
- 1.2 Chapitre 2 : la structure de $J(p,p)$ comme module sur l'algèbre de Hecke et $\mathrm{GL}_2(\mathbb{F}_p)$ . . . 23

2 Les jacobiennes modulaires tordues (Chapitres 3-4) . . . 25
- 2.1 Chapitre 3 : le module de Tate de $J_E^{\alpha}(p)$ . . . 25
- 2.2 Chapitre 4 : calcul galoisien des signes d'équation fonctionnelle pour $(V_{f,\lambda} \otimes R_{f,E})_{\lambda}$ et $(V^{\epsilon}_{f,\lambda,E})_{\lambda}$ . . . 27
- 2.3 Chapitre 4 : automorphie de $(V_{f,\lambda} \otimes R_{f,E})_{\lambda}$ and $(V^{\epsilon}_{f,\lambda,E})_{\lambda}$ . . . 27

3 Cas où l'image de ρ est contenue dans le normalisateur d'un sous-groupe de Cartan non déployé (Chapitre 5) . . . 28
- 3.1 Décomposition du module de Tate et équation fonctionnelle . . . 28
- 3.2 La conjecture de Bloch-Kato en rang zéro pour les facteurs de $J_E^{\alpha}(p)$ . . . 29
- 3.3 Le théorème d'immersion formelle . . . 30
- 3.4 Applications aux congruences à la courbe elliptique CM d'équation $y^2 = x^3 - p$ 31

4 Résultats de grande image pour le produit tensoriel de deux formes modulaires (Chapitre 6) . . . 31

1 Moduli spaces and twisted modular curves 35
1.1 Moduli problems . . . 37
1.1.1 Definitions . . . 37
1.1.2 Γ_0-structures and degeneracy maps . . . 41
1.1.3 Degeneracies for $\Gamma_1(N)$-structures . . . 48
1.2 Compactified moduli schemes . . . 55
1.3 Application to our moduli problems . . . 61
1.4 Properties of Galois twists . . . 70
1.4.1 $Y_\rho(N)$ and its rational points . . . 70
1.4.2 Comparison with the X_G . . . 72
1.5 Hecke operators . . . 77
1.5.1 $\Gamma_0(p)$-degeneracies in characteristic p . . . 77
1.5.2 Hecke operators and the Eichler-Shimura relation . . . 78
1.5.3 Link with the point of view of Galois twists . . . 82
1.5.4 The bad Hecke operators for $X_1(N, \Gamma_0(m))$ . . . 83
1.6 The cuspidal subscheme and the q-expansion principle . . . 84

2 The geometric situation 93
2.1 Statement of results . . . 93
2.2 Constructions . . . 94
2.3 Uniformizing $P(p)$ . . . 101
2.4 Uniformizing $X(p,p)$ . . . 111
2.5 Uniformizing u . . . 121
2.6 Connected components of $C(p)$ and $\ker R$ . . . 124

3 Tate modules for the Jacobian of $X(p,p)$ and its twists 129
3.1 Introduction . . . 129
3.2 The Tate module of $P(p)$ . . . 132
3.3 The singular homology of $J(p,p)$ . . . 133
3.4 The Tate module of twists of $J(p,p)$ . . . 134
3.5 Irreducibility of the factors of $\mathcal{T}_\ell J(p,p)_\rho$ . . . 139
3.6 Tate modules of the Jacobians of the connected components of $X(p,p)_\rho$ . . . 145

4 Automorphy, functional equations and root numbers for $L(J_\rho, s)$ 163
4.1 Introduction and statement of results . . . 163
4.2 Relations between classical modular forms and automorphic forms . . . 166
4.3 Basics on the Langlands correspondence . . . 170
4.4 Preparation to the computation of the root numbers . . . 176
4.5 Root numbers for the factors of $T_\ell J_\rho$ . . . 185
4.6 Consequences for elliptic curves . . . 199
4.7 On residual automorphy for the p-torsion of $J_\rho(p)$ . . . 201

5 Representations valued in the normalizer of a nonsplit Cartan subgroup 205
5.1 Statement of results . . . 205
5.2 The Tate module of the $J_{\rho,\xi}(p)$ . . . 208
5.3 Signs of the functional equation for factors of the Tate module of $J_{\rho,\xi}(p)$ . . . 215
5.4 Application to elliptic curves . . . 221
5.5 The Bloch-Kato conjecture for factors of the Tate module of $J_{\rho,\xi}(p)$ . . . 224
5.6 Reminder on the Chabauty-Coleman method . . . 234
5.7 An integrality result on $X_{\rho,\xi}(p)(\mathbb{Q})$ . . . 242
5.8 Diophantine consequences for the elliptic curve $y^2 = x^3 - p$ . . . 253

6 On obstructions to the Euler system method for Rankin-Selberg convolutions 257
6.1 Introduction . . . 257
6.2 The big image theorem for one modular form . . . 259
6.3 Special elements in the image of the convolution of two modular forms . . . 261
6.4 Families of dihedral counter-examples: proof of Theorem 6.D . . . 266
6.5 Examples and counter-examples . . . 270

A Prerequisites from algebraic geometry 275
A.1 Results from descent . . . 275
A.1.1 Sheaves in the fpqc topology . . . 275
A.1.2 Galois twists of schemes . . . 278
A.2 Compactification of finite schemes over the affine line . . . 283
A.3 Refresher on group schemes and Abelian varieties . . . 288
A.3.1 Generalities . . . 288
A.3.2 Image and quotient of Abelian varieties . . . 289
A.3.3 Differentials on Abelian varieties . . . 290
A.3.4 Abelian schemes on Dedekind rings in low ramification . . . 292
A.4 Jacobians of relative curves . . . 293
A.4.1 Functorialities in the Picard groups . . . 293
A.4.2 Degrees and Jacobian varieties . . . 298
A.4.3 Holomorphic differentials on the Jacobian of a curve . . . 305
A.4.4 Jacobians and Galois twists . . . 309

B Representations of $\mathrm{GL}_2(\mathbb{F}_p)$. 311
B.1 Principal series representations . . . 312
B.2 Cuspidal representations . . . 315
B.3 Restriction of representations to smaller subgroups . . . 318
B.4 Splitting of a certain cuspidal representation restricted to $\mathrm{SL}_2(\mathbb{F}_p)$ . . . 322
B.5 Representations of G in characteristic p . . . 324

C Modular forms and local constants 327
C.1 Gauss sums . . . 327
C.2 Twists and local L-factors of newforms . . . 328
C.3 Local constants and twists of newforms . . . 329

Bibliography 333

Introduction

1 Existing work

1.1 Background

Given an elliptic curve $E/\mathbb{Q}$ and an integer $N \geq 1$, the subgroup $E[N]$ of $E(\overline{\mathbb{Q}})$ made with its N-torsion points is endowed with an action of $G_{\mathbb{Q}}$ by group automorphisms. By choosing a basis of the free $\mathbb{Z}/N\mathbb{Z}$-module $E[N]$ of rank two, this defines a continuous group homomorphism $\rho_{E,N} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ which encodes important information on the arithmetic of E.

If $\varphi : E \to F$ is an isogeny of elliptic curves over $\mathbb{Q}$ with degree prime to N, it induces an isomorphism $\rho_{E,N} \simeq \rho_{F,N}$. The Frey-Mazur conjecture originates from the following question asked by Mazur in [112]:

Question 1 *Does there exist an integer $N \geq 7$ and non-isogenous elliptic curves E, F over $\mathbb{Q}$ such that $\rho_{E,N}$ and $\rho_{F,N}$ are conjugate?*

It is thus a statement about a *comparison* of two different Galois representations. Such a problem was already considered by Serre [141, Théorèmes 6", 7], who showed that when E, F are not isogenous over $\overline{\mathbb{Q}}$[1], then the intersection of the fields $\mathbb{Q}(E_{tors})$ and $\mathbb{Q}(F_{tors})$ is a number field. This implies in particular that the set S of integers $N \geq 1$ such that $\rho_{E,N}$ is conjugate to $\rho_{F,N}$ is finite.

Serre also provides a explicit bound on $\max S$ in his paper about Cebotarev's theorem:

Theorem A *(Serre [144, Théorème 21]) Assume the generalized Riemann hypothesis. Let $E, F/\mathbb{Q}$ be non-isogenous elliptic curves and let $N_{E,F}$ denote the product of the primes of bad reduction for E or F. There is a universal constant $c > 0$ such that one has*

$$\max S \leq c \log N_{E,F} (\log \log 2N_{E,F})^6.$$

The key difference with Mazur's question is that Serre's result is *non-uniform*: his bound depends on both elliptic curves E, F, while, in Mazur's question, the bound on N is absolute, i.e. he asks for $N \geq 7$.

A second motivation to discuss Mazur's question arises from the study of ternary Diophantine equations. The historical example is the study of the Fermat equation:

Theorem B *(Frey [55, III.2]) Assume that modular representations satisfy level-lowering[2] and that semi-stable elliptic curves over $\mathbb{Q}$ are modular. Then, for any prime $p \geq 3$, the Fermat equation $x^p + y^p = z^p$ has no rational solution (x, y, z) with $xyz \neq 0$.*

The main idea linking elliptic curves over $\mathbb{Q}$ to Diophantine equations comes from the so-called *Frey-Hellegouarch curve*, first introduced by Hellegouarch [74, 75]. Let $a, b, c \in \mathbb{Z}$ be pairwise coprime integers such that $a + b + c = 0$ and consider the elliptic curve $E/\mathbb{Q}$ with equation $y^2 = x(x - a)(x + b)$ (with discriminant $(4abc)^2$). It can be checked (see for instance

[1] Serre's condition is slightly different, but he writes in *loc.cit.* that he expects it to be equivalent, which was subsequently proved by Faltings [45, Corollary 2 to Theorem 4].

[2] This is Conjecture S in *loc.cit.*, which was proved shortly afterwards by Ribet [134].

[145, §4.1]) that E has good reduction at any prime $p \nmid 2abc$, semi-stable reduction at any odd prime $p \mid abc$. Let p, ℓ be distinct odd prime numbers such that the ℓ-adic valuations of a, b, c are all divisible by p and not all zero. A local study of the elliptic curve $E/\mathbb{Q}_\ell$ [140, IV, Appendix A.1] shows that the representation $\rho_{E,p}$ is unramified at ℓ.

In particular, in the case of the Fermat equation where $(a, b, c) = (u^p, v^p, w^p)$, the representation $\rho_{E,p}$ is only ramified at 2 and p; a more precise study of ramification at these primes (see for instance [145, §4.2]) shows that, in this situation, $\rho_{E,p}$ cannot be modular[3].

In a later work [56], Frey establishes a similar connection between a generalized class of ternary Diophantine equations and isomorphisms between the $\rho_{E,N}$ for various elliptic curves $E/\mathbb{Q}$.

Theorem C *(Frey [56, Proposition 3.5]) Let S be a a finite set of prime numbers, and $\mathbb{Z}_S$ denote the set of $n \in \mathbb{Z}$ such that every prime divisor of n is in S. Let $\mathcal{E}_S$ be the set of isomorphism classes of elliptic curves over $\mathbb{Q}$ such that their conductor is a square-free product of elements of S. Then the following statements are equivalent:*

- *The set of $(x, y, z) \in \mathbb{Z}^3$ such that $(x, y, z) = 1$ and there exists $a, b, c \in \mathbb{Z}_S, p \geq 5$ prime such that $ax^p + by^p + cz^p = 0$ is finite.*
- *There are finitely many elliptic curves $E/\mathbb{Q}$ (up to isomorphism) such that $E[2] \subset E(\mathbb{Q})$ and $\rho_{E,p} \simeq \rho_{E_0,p}$ for some $E_0 \in \mathcal{E}_S$ and some prime $p \geq 5$.*

A theorem of Shafarevich [140, IV, §1.4] shows that, in the statement of Theorem C, $\mathcal{E}_S$ is finite. Moreover, there does not seem to be any conceptual reason for the triviality requirement on the Galois representation $\rho_{E,2}$: up to a small modification that we will discuss later, its presence or absence should not be meaningful. The same applies to the semi-stability condition on E_0. One possible statement of the Frey-Mazur conjecture is the following slight generalization of the second condition of Theorem C.

Conjecture 1 *(See [56, Conjecture 5]) Let $E/\mathbb{Q}$ be an elliptic curve. There are finitely many elliptic curves up to isomorphism $F/\mathbb{Q}$ such that the representations $\rho_{E,p}$ and $\rho_{F,p}$ are conjugate for some prime $p \geq 7$.*

It is in fact expected [53, Conjecture 2.1] that a uniform version of this conjecture holds.

Conjecture 2 *There exists a constant $C_{FM} > 0$ such that for any elliptic curves $E, F/\mathbb{Q}$ such that $\rho_{E,p} \simeq \rho_{F,p}$ for some prime $p > C_{FM}$, E and F are isogenous.*

In [145, §4.3], Serre discusses the following attempt towards solving the Diophantine equation $u^p + v^p + 31w^p = 0$, where $p \geq 5$ is a prime distinct from 31, with *the modular method*. If (u, v, w) is a nontrivial solution, then, up to dividing by their greatest common divisor, we may assume that u, v, w are pairwise coprime. Let (A, B, C) be a permutation of $(u^5, v^5, 31w^5)$ or $(-u^5, -v^5, -31w^5)$ such that B is even (hence divisible by 32) and $A \equiv -1 \pmod 4$. Let E be the elliptic curve with equation $y^2 = x(x - A)(x + B)$: by [145, §4.1], it is semi-stable with full 2-torsion and its primes of bad reduction are exactly those that divide ABC. Its minimal discriminant is $31^2 \left(\frac{ABC}{31 \cdot 2^p}\right)^2 2^{2p-8}$. Therefore, by Serre's Conjecture [87, 88], $\rho_{E,p}$ is the reduction of a newform $f \in \mathcal{S}_2(\Gamma_0(62))$.

There are two Galois orbits of newforms in $\mathcal{S}_2(\Gamma_0(62))$, of which exactly one is rational, corresponding to the newform $f_{\mathbb{Q}}$[4]. A local argument at $\ell \in \{3, 5\}$ as in [145, §4.3 Lemme 1], shows, using the q-expansion of the newform with non-rational q-expansion given by the LMFDB [107] that $f = f_{\mathbb{Q}}$, hence E is congruent modulo p to some elliptic curve of conductor 62. Let E_0 be the only elliptic curve of conductor 62 with full 2-torsion by the LMFDB data [107]: it is given by the minimal Weierstrass equation $y^2 + xy + y = x^3 - x^2 - 21x + 41$ and (minimal) discriminant 62^2. If Conjecture 1 holds for E_0 then, when p is large enough, the elliptic curve E

[3]The importance of level-lowering in this argument is that it states that if $\rho_{E,p}$ is modular, it is so *in the smallest possible level*, which would be 2.

[4]It is the newform F in [145, §4.3 Remarque (3)].

must be isogenous to E_0, hence isomorphic to E_0 since E_0 is the only elliptic curve of conductor 62 with $E_0[2] \subset E_0(\mathbb{Q})$. The minimal discriminants are equal up to a unit, thus $ABC = 31 \cdot 32$, $p = 5$, and $(u, v, w) \in \{(2, -1, -1), (-1, 2, -1), (-2, 1, 1), (1, -2, 1)\}$.[5]

1.2 Existing work about congruences of elliptic curves

In [112], Mazur suggests that Question 1 can be rephrased as a problem about finding rational points on certain twists of the modular curves $X(N)$. Let us make that observation more precise. Let E, F be two elliptic curves over a field K, and $N \geq 1$ be an integer not divisible by the characteristic of K. Then $\rho_{E,N}$ and $\rho_{F,N}$ are conjugate if, and only if, there is an isomorphism $\varphi : E[N] \to F[N]$ of finite étale group schemes over K. Both $E[N]$ and $F[N]$ are endowed with the bilinear perfect alternated Weil pairing $\langle -, - \rangle$, so there is a unique $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$ such that, for any $P, Q \in E[N](\overline{K})$, $\langle \varphi(P), \varphi(Q) \rangle = \alpha \langle P, Q \rangle$. We write $\alpha = \det \varphi$. For instance, if φ comes from an isogeny $E \to F$ of degree d coprime to N, then $\det \varphi = d$.

For $N \geq 3$ and $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$, there exists[6] a smooth projective geometrically connected curve $X_E^\alpha(N)$ with a map $j : X_E^\alpha(N) \to \mathbb{P}^1_K$ over K such that $j^{-1}(\mathbb{A}^1_K)$ parametrizes the isomorphism classes of couples $(F/U, \iota)$, where $F \to U$ is an elliptic curve over the K-scheme U and $\iota : E[N]_U \to F[N]_U$ is an isomorphism of finite étale group schemes with determinant α. In this parametrization, the morphism j computes the j-invariant of the elliptic curve F/U.

Let $Y_E^\alpha(N)$ be the open subscheme $j^{-1}(\mathbb{A}^1_K)$ of $X_E^\alpha(N)$. Its rational points are called the *non-cuspidal* points of $X_E^\alpha(N)$. Conversely, the points of $X_E^\alpha(N) \backslash Y_E^\alpha(N)$ are called the *cusps*. In particular, $X_E^1(N)$ always possesses a K-rational point attached to $(E/K, \mathrm{id})$. Furthermore, an isogeny $\varphi : E \to F$ of elliptic curves over K with degree d coprime to N defines a non-cuspidal K-rational point in $X_E^d(N)$, as well as, for any $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$, an isomorphism $X_F^\alpha(N) \to X_E^{d\alpha}(N)$.

When $K = \mathbb{Q}$, as noted in [112], the curve $X_{E_\mathbb{C}}^\alpha(N)$ is isomorphic to the classical curve $X(N)_\mathbb{C}$: indeed, because $\mathbb{C}$ is an algebraically closed field, the N-torsion subscheme of any elliptic curve over $\mathbb{C}$ is constant. It is in this sense that the $X_E^\alpha(N)$ are twists of $X(N)$. In particular, this lets us compute the genus of $X(N)$: it is zero when $N \leq 5$ (hence the requirement that $p \geq 7$ in Conjecture 1), one when $N = 6$, and at least 3 when $N \geq 7$.

Hence, by Faltings's Theorem [45, Theorem 7], every $X_E^\alpha(N)$ for $N \geq 7$ has finitely many rational points, so that Conjecture 1 is equivalent to

Conjecture 3 *Let $E/\mathbb{Q}$ be an elliptic curve. There is a constant C_E such that for any prime $p > C_E$ and any $\alpha \in \mathbb{F}_p^\times$, the non-cuspidal rational points of $X_E^\alpha(p)$ come from elliptic curves isogenous to E.*

Thus Conjecture 2 is equivalent to

Conjecture 4 *There exists a constant $C > 0$ such that, for any elliptic curve $E/\mathbb{Q}$ and any $\alpha \in \mathbb{F}_p^\times$, for any prime $p > C$, the non-cuspidal rational points of $X_E^\alpha(p)$ come from elliptic curves isogenous to E.*

From now on, we assume, as in the statement of Conjecture 3, that $N = p$ is a prime number.

In order to relate Question 1 to Conjecture 3, it is useful to be able to determine, given two elliptic curves $E, F/\mathbb{Q}$,

[5] Since the submission of this thesis, Samir Siksek told me about the following results. First, as an application of the symplectic congruence criterion (Proposition 2), Halberstadt and Kraus [71, Proposition 2.2] proved that the equation had no solution when $p \equiv 3 \pmod 4$. Using a different argument introduced by Kraus in [96] to study the Diophantine equation $a^3 + b^3 = c^p$ (which works prime by prime and does not seem to have an obvious modular interpretation), Siksek proves in [151, Theorem 12] that the equation has no solution when $11 \leq p \leq 10^6$. These results are discussed in the PhD thesis of Heline Deconinck [34, Chapter 4], which also rules out a further 1/12-th of possible congruence classes for a prime p modulo $3 \cdot 5 \cdot 7 \cdot 11$ such that the equation has a nontrivial solution.

[6] Such a result seems to have been known to Mazur in [112], but we are only aware of partial statements in the literature such as [97, Proposition 1], or [113, I.7] in the case of number fields. We prove a generalization of this statement in Chapter 1.

(i) whether there is an isomorphism of group schemes $E[p] \simeq F[p]$, or in other words whether $\rho_{E,p} \simeq \rho_{F,p}$,
(ii) whenever it is the case, what the determinants of isomorphisms $\iota : E[p] \to F[p]$ are.

Definition *In the situation (i), we say that the elliptic curves E, F are* congruent *modulo p.*

The article [97] by Kraus and Oesterlé seems to be the first one discussing both of these questions and answering Question 1 for $p = 7$. The article points out a practical answer to *disprove* the existence of an isomorphism in many cases: it is sufficient (see Proposition 3 of *loc.cit.*) to find a prime ℓ of common good reduction for E and F such that $a_\ell(E) \not\equiv a_\ell(F) \pmod{p}$. Indeed, one has $a_\ell(E) \equiv a_\ell(F) \pmod{p}$ for every prime ℓ of common good reduction for E and F if and only if the representations $\rho_{E,p}$ and $\rho_{F,p}$ have isomorphic semi-simplifications, which holds when[7] E and F are congruent modulo p. Under the assumptions that E, F are modular[8], the authors of *loc.cit.* make this criterion effective.

Proposition 1 *(Kraus-Oesterlé [97, Proposition 4]) Let E, F be two modular elliptic curves over $\mathbb{Q}$. There is an effective bound $M = M(E, F)$ such that $\rho_{E,p}$ and $\rho_{F,p}$ have the same semi-simplification if, and only if, for any prime $\ell \leq M(E, F)$, the following two conditions are true:*

- *if ℓ is a prime of common good reduction for E, F, one has $a_\ell(E) \equiv a_\ell(F) \pmod{p}$,*
- *if ℓ is a prime of good reduction for exactly one of the curves E, F, and of bad multiplicative reduction for the other one, then one has $a_\ell(E)a_\ell(F) \equiv \ell + 1 \pmod{p}$.*

Replacing $\rho_{E,p}$ with its semi-simplification is usually not a problem: by work of Mazur [112, Theorem 1], the representation $\rho_{E,p}$ is irreducible when $p \geq 11$ and $p \neq 13$, except for a finite number of well-known cases.

The authors of *loc.cit.* also discuss (ii). Indeed, suppose that the group schemes $E[p]$ and $F[p]$ are isomorphic: we can multiply any isomorphism between them by $d \in \mathbb{F}_p^\times$, which multiplies its determinant by d^2. Thus, the set of determinants of isomorphisms $\iota : E[p] \to F[p]$ is a subset of $\mathbb{F}_p^\times$ stable under multiplication by the subgroup $\mathbb{F}_p^{\times 2}$ of squares in $\mathbb{F}_p^\times$.

Definition *Let E, F be two elliptic curves over $\mathbb{Q}$ which are congruent mod p. When there is an isomorphism $\iota : E[p] \to F[p]$ of group schemes of determinant 1, we say that $E[p]$ and $F[p]$ are* symplectically isomorphic*, or that E, F are* symplectically congruent *modulo p. When there is an isomorphism $\iota : E[p] \to F[p]$ of group schemes of determinant in $\mathbb{F}_p^\times \backslash \mathbb{F}_p^{\times 2}$, we say that $E[p]$ and $F[p]$ are* anti-symplectically isomorphic*, or that E, F are* anti-symplectically *congruent modulo p.*

Note that it is possible for two elliptic curves E, F over $\mathbb{Q}$ to be both symplectically congruent modulo p and anti-symplectically congruent modulo p. By [33, Proposition 1.1] and [141, §5.2 (iv)], this is only possible if the image of $\rho_{E,p}$ is contained in a split Cartan subgroup.

In order to find out whether two elliptic curves that are congruent modulo p are symplectically or anti-symplectically congruent modulo p, the authors of [97] consider the invariants of the elliptic curve in *bad reduction*, that is, attached to the restriction of $\rho_{E,p}$, $\rho_{F,p}$ to an inertia group at some prime ℓ.

Proposition 2 *(Kraus-Oesterlé [97, Proposition 2]) Let E, F be two elliptic curves over $\mathbb{Q}$ with minimal discriminants Δ_E, Δ_F, and p, ℓ be two distinct prime numbers such that*

- *the elliptic curves E, F both have bad multiplicative reduction at ℓ,*
- *the group schemes $E[p]$ and $F[p]$ are isomorphic,*
- *$v_{E,\ell} := v_\ell(\Delta_E)$ is not divisible by p.*

[7] This is an equivalence if $\rho_{E,p}$ or $\rho_{F,p}$ is irreducible, which is the "generic" situation, as shown by Theorem F.
[8] which is now known by works of Breuil, Conrad, Diamond, Taylor and Wiles [166, 40, 32, 18].

Then $v_{F,\ell} := v_\ell(\Delta_F)$ is not divisible by p. Moreover, $E[p]$ and $F[p]$ are symplectically isomorphic if and only if $\left(\frac{v_{E,\ell}v_{F,\ell}}{p}\right) = 1$.

Such local criteria have subsequently been developed in other settings, in particular in potential good reduction. We refer to [53] for a list.

Let E, F be elliptic curves over $\mathbb{Q}$ that are congruent modulo p. It is possible by [33, Proposition 1.1] that one cannot determine, using solely local methods, whether the congruence is symplectic or anti-symplectic. A solution, suggested in §1.1 of *loc.cit.*, is to use explicit models for the curves $X_E^\alpha(p)$. More precisely, for small values of p, one can construct part or all of the following data:

- explicit equations for a family $X^\alpha(p)$ of proper curves over the ring $\mathbb{Q}[a,b]_{4a^3+27b^2}$ such that its specialization at the maximal ideal $(a-a_0, b-b_0) \subset \mathbb{Q}[a,b]_{4a^3+27b^2}$ for $(a_0,b_0) \in \mathbb{Q}^2$ yields a model of $X_E^\alpha(p)$ for the elliptic curve $E/\mathbb{Q}$ given by the Weierstrass equation $y^2 = x^3 + a_0x + b_0$.
- explicit equations for the j-invariant map $X^\alpha(p) \to \mathbb{P}^1_{\mathbb{Q}[a,b]_{4a^3+27b^2}}$,
- for any non-cuspidal point $P \in X^\alpha(p)(K)$ above the maximal ideal $(a-a_0, b-b_0)$ for $a_0, b_0 \in K$ for some number field K, corresponding to an isomorphism $E[p] \to E'[p]$ of group schemes over K with determinant α, where E denotes the elliptic curve $y^2 = x^3 + a_0x + b_0$ over K, a specification (for instance using the invariants c_4, c_6 of E') of the K-isomorphism class of E' [9].

When $p \in \{3,5\}$ and $\alpha \in \mathbb{F}_p^{\times 2}$ (the *symplectic case*), this was solved by Rubin and Silverberg [138]. An explicit model for $X_E^1(7)$ was first constructed by Halberstadt and Kraus [72], and an explicit equation for $X_E^{-1}(7)$ was first described by Poonen, Schaefer and Stoll [130]. These formulae were proved by a different method and completed by work of Fisher: he describes equations for $X_E^\alpha(p)$ for any α when $p \in \{3,5\}$ [46], when $p \in \{7,11\}$ [47], when $p = 13$ [48].

As Halberstadt and Kraus demonstrate in [72], explicit models for the curve $X_E^\alpha(p)$ turn out to be convenient means for exhibiting congruences of elliptic curves modulo p, or even families of such congruences. Indeed, they describe an infinite family of 6-uples of pairwise non-isogenous elliptic curves over $\mathbb{Q}$ which are pairwise symplectically congruent modulo 7. In [47] and [48], Fisher constructs infinite families of symplectic congruences for $p \in \{7,11,13\}$ and infinite families of anti-symplectic congruences for $p \in \{7,11,13\}$.

In [33, §3.7], the authors prove that there is only one pair of elliptic curves congruent modulo 17 with both conductors smaller than 500000 (up to quadratic twist), given by the LMFDB labels [107] 3675.e1, 47775.q1, and that the congruence is anti-symplectic. Fisher exhibits in [49] the first known example of symplectic congruence modulo 17, with conductors $279809270 = 2 \cdot 5 \cdot 13 \cdot 59 \cdot 191^2$, and $3077901970 = 2 \cdot 5 \cdot 11 \cdot 13 \cdot 59 \cdot 191^2$, and conjectures in the same article that these are the only congruences between elliptic curves over $\mathbb{Q}$ modulo a prime $q \geq 17$. This conjecture is somewhat supported by [33, Theorem 1.3], which states that this conjecture holds for elliptic curves of conductor at most 500000.

To find the symplectic congruence modulo 17 which we just discussed (and, in fact, the families of congruences modulo 13 of [48], as well as the family of anti-symplectic congruences modulo 11, crucially relying on the work of [98]), Fisher does not in fact use the models for any of the $X_E^1(17)$. Instead, he directly considers a moduli space $Z(p,\alpha)$ for triples (E,F,ι) of elliptic curves such that $\iota : E[p] \to F[p]$ is an isomorphism of determinant α, known as a *modular diagonal surface* first studied by Kani and Schanz [83]. The latter authors prove, among others, the following classification:

Theorem D *(Kani-Schanz [83, Theorem 4])*

- *$Z(p,\alpha)$ is a rational surface if and only if $p \leq 5$ or $p = 7$ and $\alpha \in \mathbb{F}_p^{\times 2}$,*

[9] Indeed, when for instance $j(P)$ is neither 0 or 1728, the previous items only determine E' up to quadratic twist.

- *$Z(p,\alpha)$ is birational to an elliptic K3-surface if and only if $p=7$ and $\alpha \notin \mathbb{F}_p^{\times 2}$,*
- *$Z(p,\alpha)$ is birational to an elliptic surface of Kodaira dimension 1 if and only if $p=11$ and $\alpha \in \mathbb{F}_p^{\times 2}$,*
- *$Z(p,\alpha)$ is a surface of general type in all other cases.*

By studying the geometry of $Z(11,1)$, Kani and Rizzo [82] were able to prove that there were infinitely many families of symplectic congruences of elliptic curves (over $\mathbb{Q}$) modulo 11.

As explained in [83], a consequence of this classification is that when $p \geq 13$, according to Lang's conjecture (see for instance [22, Conjecture B]), the rational points on $Z(p,\alpha)$ should be located on finitely many rational or elliptic curves (i.e. the curves with genus $g \leq 1$) up to finitely many exceptions.

Theorem E *(Bakker-Tsimerman [7, Theorem 29]) Let $N \geq 1$. There is an integer M_N with the following property. Let $p > M_N$ be a prime number, k be an algebraically closed field of characteristic zero. Let B be a smooth projective curve over k of gonality at most N endowed with a nonconstant morphism $B \to Z(p,\alpha)_k$. Then B factors through a Hecke correspondence.*

Even assuming Lang's conjecture, to prove the Frey-Mazur conjecture in this case, one would have to prove that there are no "exceptional" points for large enough p.

1.3 Finding rational points on modular curves: methods and results

There is a long-standing strategy about finding rational points of modular curves, pioneered by Mazur in [111, 112] for the study of the modular curves $X_1(p)$ and $X_0(p)$. An advantage of this approach is that it enables one to find rational points for the curve of interest without need for an explicit model, which has been used to discuss the following question.

Question 2 *(Serre's uniformity question [141, §4.3]) Does there exist a constant $C > 0$ such that for any elliptic curve $E/\mathbb{Q}$ without complex multiplication and any prime $p > C$, the representation $\rho_{E,p}$ is surjective?*

As explained in the beginning of [111], local arguments by Serre [141] show that it is enough to rule out (when $p > 13$) the following three cases:

(a) the representation $\rho_{E,p}$ is reducible,
(b) the image of $\rho_{E,p}$ is contained in the normalizer of a split Cartan subgroup,
(c) the image of $\rho_{E,p}$ is contained in the normalizer of a nonsplit Cartan subgroup.

In all three situations, for a given p, there is a modular curve parametrizing elliptic curves with Galois image contained in the given subgroup. The focus of the articles [111, 112] is (a), (although they prove partial results regarding (b) as well).

Theorem F *(Mazur [112]) Let $E/\mathbb{Q}$ be an elliptic curve such that $\rho_{E,p}$ is reducible for some prime $p > 37$. Then E has complex multiplication by $\mathbb{Q}(\sqrt{-p})$ and in particular one has $p \leq 163$.*

The proof also yields more precise results on the torsion subgroups of elliptic curves.

Theorem G *(Mazur [111]) Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup of $E(\mathbb{Q})$ is isomorphic to one of the following groups: $\mathbb{Z}/n\mathbb{Z}$ for $n \leq 10$ or $n = 12$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ for $n \leq 4$. In particular, if p is a prime such that $E(\mathbb{Q})$ has a p-torsion point, then one has $p \leq 7$.*

Before coming back to Serre's uniformity question, let us mention that Theorem G has been generalized to arbitrary number fields by Merel [116] and made explicit by Parent [128]. The proofs of these statements still follow Mazur's strategy.

Theorem H *(Merel [116], Oesterlé, Parent [128]) Let $d \geq 1$ be an integer. There exists an effectively computable bound $B(d)$ such that for any number field K of degree at most d and any elliptic curve E/K, the torsion subgroup of $E(K)$ has cardinality at most $B(d)$. The prime divisors of $B(d)$ are all at most $(1+3^{d/2})^2$.*

Case (b) in Serre's uniformity question was ruled out for large enough p in [12], and for all $p \geq 11$ except $p = 13$ in [13]. The arguments therein also follow Mazur's strategy. The recent articles [101] (for primes $p \geq 1.4 \cdot 10^7$) and [58] (for all primes, using the calculations of [5] for $p < 100$) use Mazur's strategy to show that in case (c), the image of $\rho_{E,p}$ is *equal* to said normalizer. However, Mazur's approach is more difficult to adapt for this setting for reasons that we will get into.

After describing these applications, we now review Mazur's strategy.

Let X be a compactified modular curve over $\mathbb{Q}$. Then X is endowed with a natural morphism $j : X \to \mathbb{P}^1_{\mathbb{Q}}$ mapping any noncuspidal point of X to the j-invariant of the elliptic curve that it represents. The strategy consists in studying separately the points of $X(\mathbb{Q})$ with non-integral j-invariant and the points of $X(\mathbb{Q})$ with integral j-invariant. In terms of moduli spaces, this amounts to *first* proving that elliptic curves corresponding to a rational point of X have no (or few) primes of potentially multiplicative reduction, *then* treating this case by other methods.

The strategy to rule out the existence of rational points with non-integral j-invariant (or otherwise control them) is to use a *formal immersion argument* following the spirit of [112, Corollary 4.3]. More precisely, let ℓ be a prime number and $P \in X(\mathbb{Q})$ be a point such that $j(P) \notin \mathbb{Z}_{(\ell)}$. Assume for the sake of simplicity that $\ell > 2$ and that X has a smooth proper model $\mathcal{X}$ over $\mathbb{Z}_{(\ell)}$. Then P reduces to a *cuspidal point* $c \in \mathcal{X}(\mathbb{F}_\ell)$.

Let $A/\mathbb{Q}$ be a quotient of the Jacobian of X, so that A is an Abelian variety with good reduction at ℓ with Néron model $\mathcal{A}$ over $\mathbb{Z}_{(\ell)}$, and let $f : X \to A$ be a morphism. Then f extends to a morphism $\mathcal{X} \to \mathcal{A}$ still denoted by f, and we can usually assume that $f(c) = 0$. Then $f(P) \in \mathcal{A}(\mathbb{Q})$ is a point whose reduction modulo ℓ vanishes. By a result of Raynaud [112, Proposition 1.1], this implies that $f(P)$ is either a non-torsion point, or zero.

In practice, one often proves that $f(P)$ is a torsion point by showing that $A(\mathbb{Q})$ is a finite group. In [112], Mazur uses the *Eisenstein quotient* $\widetilde{J}$ of the Jacobian $J_0(p)$ of $X_0(p)$, whose construction and properties – in particular the finiteness of $\widetilde{J}(\mathbb{Q})$ by descent – are discussed in [111]. Since this paper, a different method has emerged thanks to recent progress in the Bloch-Kato conjecture, in particular the work of Kolyvagin-Logachev [94] and Kato [84]. They prove instances of the *Bloch-Kato conjecture*: that is, if the L-function of certain abelian varieties A does not vanish at its central point, then the group $A(\mathbb{Q})$ is finite.

That is why, in [116, 128, 12, 13], the *Eisenstein quotient* is replaced with the *winding quotient*, that is, the largest quotient J_e of $J_0(p)$ such that the L-function of J_e does not vanish at the central point.

In contrast, the argument showing that $f(P)$ is nonzero is geometric and local. The cuspidal subscheme of $\mathcal{X}$ is well-understood, so it is usually feasible to choose f such that $f(c_0) = 0$, for some cuspidal point $c_0 \in X$ whose reduction modulo ℓ is also c. The *formal immersion argument* consists in proving that the ring homomorphism $\widehat{f^\sharp} : \widehat{\mathcal{O}_{A,0_{\mathbb{F}_\ell}}} \to \widehat{\mathcal{O}_{X,c}}$ is surjective. Indeed, this claim implies that $f^\sharp$ is an epimorphism in the category of Noetherian local rings, which implies that the morphism $f : \mathcal{X}(\mathbb{Z}_\ell) \to \mathcal{A}(\mathbb{Z}_\ell)$ is injective in the residue disk of c (which contains c_0 and P): since $f(c_0) = 0_{A_{\mathbb{Q}_\ell}}$, one has $f(P) \neq 0_{A_{\mathbb{Q}}}$.

In applications, the formal immersion argument is convenient because the geometry of modular curves at their cusps is well-understood, including in finite characteristic, thanks to the q-expansion principle, which lets one describe the differential forms near a cusp.

The second part of Mazur's strategy is to handle points $P \in X(\mathbb{Q})$ corresponding to elliptic curves with an integral j-invariant. The method usually differs according to the problem.

In the case of torsion on elliptic curves, it is enough to apply a specialization lemma: indeed, if an elliptic curve E/K with potentially good reduction above a prime $\mathfrak{r}$ of residue characteristic 3 has a p-torsion point (with $p > 7$), then the reduction of this point modulo $\mathfrak{r}$ (in the Néron model $\mathcal{E}$ of E) still has order p. Thus p divides the cardinality of $\mathcal{E}(\mathcal{O}_K/\mathfrak{r})$, which has an explicit bound in terms of the degree of the extension $K/\mathbb{Q}$ using Hasse's theorem (see for instance [128, Proposition 1.3]).

For (a), Mazur studies the *isogeny character* of the elliptic curve and proves that it is of the form $\alpha\omega_p^k$, where α is a character of $G_{\mathbb{Q}}$ of order dividing 12, ω_p is the mod p cyclotomic character of $G_{\mathbb{Q}}$ and $k \in \mathbb{Z}/(p-1)\mathbb{Z}$ can take at most 6 possible values. By comparing the implied congruences with Hasse's theorem, he is then able to prove that either $p \in \{17, 37\}$ or $\mathbb{Q}(\sqrt{-p})$ has class number one.

For (b), the argument in [12] is *Runge's method*, which provides an upper bound on the j-invariant of integral points lying on the modular curve, which can be shown to contradict a lower bound coming from refinements (in this case, due to Pellarin [129]) of Masser-Wüstholz's [110] isogeny bound. This is also the idea used in [13, 101, 58].

Let us now explain why (c) is more difficult to approach with Mazur's strategy. It is known by [25, Theorem 1] that the L-function of every simple isogeny factor of the Jacobian $J_{ns}^+(p)$ of the associated modular curve $X_{ns}^+(p)$ vanishes with odd order. By the Birch and Swinnerton-Dyer conjecture, we thus expect that every isogeny factor of $J_{ns}^+(p)$ has infinitely many rational points. Moreover, the study of integral points of $X_{ns}^+(p)$ with Runge's method does not work, because this method relies on *Runge's condition* [12, §1] – namely, that there are at least two Galois orbits of cusps – which is not satisfied on $X_{ns}^+(p)$.

A different approach has emerged in the past decade to compute modular points on rational curves, the so-called *quadratic Chabauty* method, following ideas of Kim [89, 91, 90].

Unlike Mazur's approach, it seems that no examples have been completely worked out without using an explicit model of the curve to effectively determine the rational points; however, when the curve of interest has a model, the quadratic Chabauty method applies in much greater generality than Mazur's method, since the Jacobian J of the modular curve X does not need to have a quotient with finitely many rational points any more. A somewhat typical condition (see [9, Section 2]) would be that J satisfies

$$\dim J = \operatorname{rk} J(\mathbb{Q}),\ \operatorname{rk} NS(J) > 1.$$

Using this method, the authors of [8] were able to rule out $p = 13$ in cases (b) (and (c), because it turns out that the associated modular curves are isomorphic when $p = 13$), this completing the solution of (b):

Theorem I *(Bilu-Parent [12], Bilu-Parent-Rebolledo [13], Balakrishnan-Dogra-Müller-Tuitman-Vonk [8]) Let $p \geq 11$ be a prime number. Then any elliptic curve $E/\mathbb{Q}$ such that the image of $\rho_{E,p}$ is contained in the normalizer of a split Cartan subgroup (resp. of a nonsplit Cartan subgroup if $p = 13$) has complex multiplication.*

More recently, the authors of [8] determine in [9], among other examples, the rational points of the curve $X_{ns}^+(17)$, but report that computational difficulties arose in the case of $X_{ns}^+(19)$. On the other hand, Dogra and Le Fourn [44] proved that the quadratic Chabauty method could in principle be applied to any $X_{ns}^+(p)$ of genus at least two.

2 Basic results of this thesis (Chapters 1-2)

This thesis is a study of the arithmetic of the modular curves $X_E^\alpha(p)$ for primes $p \geq 7$ and elliptic curves $E/\mathbb{Q}$.

2.1 Chapter 1: Moduli problems

In Chapter 1, we review the theory of moduli problems of elliptic curves as described in the work of Katz and Mazur [86]. The main goal is to give a complete proof of the existence of the modular curves $X_E^\alpha(p)$ over more general bases than fields (generalizing [97, Proposition 2] and [113, §1.7]), as well as their basic geometric properties. In particular, we show that, like classical modular curves, these curves can be endowed with supplementary $\Gamma_0(m)$-structures yielding Hecke operators. Such a result seems to be folklore, but we are not aware of a fleshed-out proof.

When applying Mazur's method to a modular curve X, as we saw, one constructs a morphism f from the modular curve X to a suitable quotients of its Jacobian. One then has to analyze the geometry of f at the cusps, including in finite characteristic. That is why this chapter deals with moduli spaces over bases that are not fields.

Theorem 1 *Let $N \geq 3$ be an integer and R be a regular excellent Noetherian $\mathbb{Z}[1/N]$-algebra. Let G be a finite étale commutative group scheme over R which is étale-locally isomorphic to $(\mathbb{Z}/N\mathbb{Z})^{\oplus 2}$, endowed with a fibrewise perfect bilinear alternating pairing $(-,-)_G : G \times G \to \mu_N$. Then there is a proper smooth R-scheme $X_G(N)$ of relative dimension one satisfying the following properties:*

- *There is a finite locally free map $(j, \det) : X_G(N) \to \mathbb{P}^1_R \times (\mathbb{Z}/N\mathbb{Z})^\times_R$, and the geometric fibres of* det *are connected.*
- *The reduced subscheme attached to the closed subspace $\{j = \infty\}$, called the* cuspidal subscheme*, is finite étale over R and defines an effective Cartier divisor.*
- *For any R-scheme S, $j^{-1}(\mathbb{A}^1_R)(S)$ is functorially isomorphic to the set of equivalence classes of $(E/S, \iota)$, where E/S is a relative elliptic curve, $\iota : G_S \to E[N]$ is an isomorphism of finite étale group schemes over S. Moreover, under this isomorphism, j maps the couple $(E/S, \iota)$ to the j-invariant of E/S, and* det *maps the couple $(E/S, \iota)$ to the unique $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times_R(S)$ such that the fibrewise perfect bilinear alternating pairing*

$$G \times G \xrightarrow{\iota \times \iota} E[N] \times E[N] \xrightarrow{\mathrm{We}} (\mu_N)_S$$

  is exactly $\alpha \cdot (-,-)_G$, where We *denotes the Weil pairing.*
- *The formation of $X_G(N), j, \det$, the cuspidal subscheme, and the above isomorphism of functors commutes with base change.*

For $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$, let $X^\alpha_G(N)$ denote the closed open subscheme $\det^{-1}(\alpha)$ of $X_G(N)$, and $J^\alpha_G(N)$ denote its relative Jacobian over R. For $n \in (\mathbb{Z}/N\mathbb{Z})^\times$, the isomorphism of functors $(E/S, \iota, C) \longmapsto (E/S, n \cdot \iota, C)$ extends to an isomorphism $[n] : X^\alpha_G(N) \to X^{n^2\alpha}_G(N)$.

For every prime number $\ell \nmid N$, for every $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$, there is a Hecke correspondence on $X^\alpha_G(N) \times X^{\ell\alpha}_G(N)$ inducing an endomorphism T_ℓ of $\prod_{\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times} J^\alpha_G(N)$. The various T_ℓ and $[n]$ as previously commute pairwise, and T_ℓ sends the component $J^\alpha_G(N)$ into the component $J^{\ell\alpha}_G(N)$.

By choosing $N = p$ prime, and for G the p-torsion of an elliptic curve endowed with its Weil pairing, we find:

Corollary 1 *Let R be an excellent Dedekind ring*[10] *and E/R be an elliptic curve. Let $p \geq 3$ be a prime invertible in R and $\alpha \in \mathbb{F}_p^\times$. There exists a smooth proper relative curve $X^\alpha_E(p) \to \operatorname{Spec} R$ with geometrically connected fibres endowed with the following datum:*

- *a finite locally free map $j : X^\alpha_E(p) \to \mathbb{P}^1_R$ such that the reduced closed subscheme attached to the subspace $\{j = \infty\}$ is finite étale over R,*
- *for every R-scheme S, a functorial isomorphism between $j^{-1}(\mathbb{A}^1_R)(S)$ and the equivalence classes of pairs $(F/S, \iota)$, where F/S is an elliptic curve and $\iota : E[p]_S \to F[p]$ is an isomorphism of group schemes such that the following two pairings are equal:*

$$E[p]_S \times E[p]_S \xrightarrow{\alpha \cdot \mathrm{We}} (\mu_p)_S, \quad E[p]_S \times E[p]_S \xrightarrow{\iota \times \iota} F[p] \times F[p] \xrightarrow{\mathrm{We}} (\mu_p)_S.$$

- *a relative Jacobian $J^\alpha_E(p)$,*
- *for every prime $\ell \neq p$, Hecke operators $T_\ell : J^\alpha_E(p) \to J^{\ell\alpha}_E(p)$ that pairwise commute,*
- *for every $n \in \mathbb{F}_p^\times$, an isomorphism $[n] : X^\alpha_E(p) \to X^{n^2\alpha}_E(p)$.*

[10] This is for instance the case if $\mathrm{Frac}(R)$ is of characteristic zero, if R is a complete discrete valuation ring, or R is essentially of finite type over a field.

It remains to relate these curves $X_E^\alpha(p)$ to the classical modular curve $X(p)$ attached to the congruence subgroup $\Gamma(p)$.

More precisely, let $X(p,p)$ be the compactification of the moduli scheme parametrizing elliptic curves over a $\mathbb{Z}[1/p]$-scheme along with a basis of their p-torsion subgroup: it is a smooth projective $\mathbb{Z}[1/p]$-scheme of relative dimension one, and is endowed with a left action of the group $\mathrm{GL}_2(\mathbb{F}_p)/\{\pm I_2\}$, a finite locally free morphism $j : X(p,p) \to \mathbb{P}^1_{\mathbb{Z}[1/p]}$ (given by the j-invariant) and the Weil pairing morphism $X(p,p) \to \operatorname{Spec}\mathbb{Z}[1/p,\zeta_p]$, which is smooth proper of relative dimension one with geometrically connected fibres.

When R is a field in which p is invertible and E/R is an elliptic curve, we realize the disjoint reunion of the curves $X_E^\alpha(p)$ as a Galois twist of (geometrically disconnected) modular curve $X(p,p)_R$ over R, and check that this identification is compatible with the structures identified above: the j-invariant and the Hecke operators. While this correspondence is implicitly used by e.g. Wiles [166, p. 543] for the purpose of the $3-5$-switch, and alluded to in the introduction of [163], it has not, to the author's knowledge, been spelled out.

There are several possible definitions of *Galois twist*, and we mean here the following one (which is a special case of Proposition A.1.11):

Definition *Let X be a smooth quasi-projective scheme over a field k with separable closure k_s. Let $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{Aut}(X)$ be a continuous group homomorphism, where $\mathrm{Aut}(X)$ is endowed with the discrete topology. The* twist *of X by ρ is the unique (up to unique isomorphism) smooth quasi-projective k-scheme X' endowed with an isomorphism $j : X'_{k_s} \to X_{k_s}$ of k_s-schemes such that, if $\beta : X'(k_s) \xrightarrow{\sim} X'_{k_s}(k_s) \xrightarrow{j} X_{k_s}(k_s) \xrightarrow{\sim} X(k_s)$ and $g \in \mathrm{Gal}(k_s/k)$, for any $P \in X'(k_s)$, one has $\beta(g \cdot P) = \rho(g)(g \cdot \beta(P))$.*

This construction is functorial in a natural sense (see Proposition A.1.13).

Theorem 2 *Let k be a field with separable closure k_s and $p \geq 3$ be a prime number invertible in k. Let E/k be an elliptic curve and $(P,Q) \in E(k_s)^2$ be a basis of its p-torsion. For each $\sigma \in \mathrm{Gal}(k_s/k)$, let $\rho(\sigma) \in \mathrm{GL}_2(\mathbb{F}_p)$ be the matrix such that $\begin{pmatrix}\sigma(P)\\ \sigma(Q)\end{pmatrix} = \rho(\sigma)\begin{pmatrix}P\\ Q\end{pmatrix}$. Then $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ is a group anti-homomorphism.*

Let $X(p,p)_{\rho^{-1}}$ be the twist of $X(p,p)_k$ by the Galois representation ρ^{-1}. The twist by ρ^{-1} of the morphism

$$(j, \mathrm{We}) : X(p,p)_k \to \mathbb{P}^1_k \times_k \operatorname{Spec} k \otimes \mathbb{Z}[\zeta_p]$$

is a morphism

$$(j, \mathrm{We}_{\rho^{-1}}) : X(p,p)_{\rho^{-1}} \to \mathbb{P}^1_k \times_k S,$$

where S denotes the constant k-scheme whose underlying set is the collection $\mu_p^\times(k_s)$ of primitive p-th roots of unity in k_s. For $\zeta \in \mu_p^\times(k_s)$, let $X_{\rho,\zeta}(p)$ denote the inverse image of the component ζ in $X(p,p)_{\rho^{-1}}$.

Let $\xi = \langle P, Q\rangle_{E[p]} \in \mu_p^\times(k_s)$. For every $a \in \mathbb{F}_p^\times$, there is an isomorphism of $\mathbb{P}^1_k$-schemes $\iota^a_{E,P,Q} : X_E^a(p)_k \to X_{\rho,\xi^a}(p)$ such that for any non-cuspidal point $(F/k_s,\iota) \in X_E^a(p)(k_s)$, one has

$$\iota^a_{E,P,Q}(F/k_s,\iota) = (F/k_s, (\iota(P), \iota(Q))) \in X(p,p)(k_s) \supset X_{\rho,\xi^a}(p)(k_s).$$

Moreover, the disjoint reunion of the $\iota^a_{E,P,Q}$ induces an isomorphism $\iota^J_{E,P,Q}$ between the direct product of the $J_E^a(p)$ and the Galois twist $J(p,p)_{\rho^{-1}}$ by ρ^{-1} of the Jacobian[11] of the curve $X(p,p)$ over k. The Abelian variety $J(p,p)_{\rho^{-1}}$ is endowed (through the twist) of Hecke operator T_ℓ for any prime $\ell \neq p$ and $[n]$ for any $n \in \mathbb{F}_p^\times$ (where $[n]$ maps a couple $(F/S,(A,B))$ – where F/S is an elliptic curve over the k-scheme S and (A,B) is a basis of $F[p](S)$ – to $(F/S,(nA,nB))$).

The isomorphism $\iota^J_{E,P,Q}$ preserves the Hecke operators and the action of $\mathbb{F}_p^\times$.

[11] The notion of Jacobian of a non-geometrically connected curve does not seem entirely standard, but amounts to a minor modification of existing results on smooth proper schemes $C \to S$ of relative dimension one with geometrically connected fibres. We discuss the necessary adaptations in Appendix A.4.

For later use, we also state and prove in this chapter some well-known features of the arithmetic geometry of classical modular curves, namely: the Eichler-Shimura relation, a lemma about the action of the Hecke operator on the cuspidal subscheme, and a q-expansion principle.

2.2 Chapter 2: Hecke and $\mathrm{GL}_2(\mathbb{F}_p)$-structure of $J(p,p)$

In Chapter 2, we study the geometric properties of the modular curve $X(p,p)_{\mathbb{Z}[1/p]}$. Let $J(p,p)$ denote its relative Jacobian. Let $X_1(p,\mu_p)$ denote the base change to $\mathbb{Z}[1/p,\zeta_p]$ of the smooth proper modular curve over $\mathbb{Z}[1/p]$ whose noncuspidal points parametrize couples $(E/S,P)$ up to isomorphism, where E/S is an elliptic curve, P is a point of "exact order p" in the sense of [86, (3.2)], and let $J_1(p,\mu_p)$ denote the Jacobian of the relative curve $X_1(p,\mu_p)\to \operatorname{Spec}\mathbb{Z}[1/p]$; it is endowed with modified Hecke operators T'_ℓ and modified diamond operators $\langle n\rangle$' (in order to take into account the action on $\operatorname{Spec}\mathbb{Z}[1/p,\zeta_p]$, see Definition 2.2.6).

For each $t\in\mathbb{F}_p$ (resp. $t=\infty$), we define a morphism $u_t : J(p,p)\to J_1(p,\mu_p)$ as follows by push-forward functoriality: we map a couple $(E,(P,Q))$ to $(E,tP+Q,\langle P,\,Q\rangle_E)$ (resp. to $(E,P,\langle P,\,Q\rangle_E)$), where $\langle P,\,Q\rangle_E$ is the Weil pairing on $E[p]$.

Let $P(p)$ be the direct product of $p+1$ copies of $J_1(p,\mu_p)$ indexed by $\mathbb{F}_p\cup\{\infty\}$; we can construct an action of $\mathrm{GL}_2(\mathbb{F}_p)$ on $P(p)$ which commutes with every T'_ℓ, and such that the modified diamond $\langle n\rangle'$ is exactly the action of $nI_2\in\mathrm{GL}_2(\mathbb{F}_p)$. Let $u : J(p,p)\to P(p)$ be the direct product of the u_t. Then $C(p):=\ker u=\cap_{t\in\mathbb{F}_p\cup\{\infty\}}\ker u_t$ is a proper group scheme over $\mathbb{Z}[1/p]$, and we let $C^0(p)$ be the (smooth proper over $\mathbb{Z}[1/p]$) Néron model of the connected component of $C(p)_{\mathbb{Q}}$ containing the unit point.

Theorem 3 *The morphism u commutes to the action of $\mathrm{GL}_2(\mathbb{F}_p)$ and the Hecke operators, in the sense that $u\circ T_\ell = T'_\ell\circ u$. Moreover, there exists an explicit morphism $R : P(p)\to P(p)$ equivariant for the T'_ℓ and the action of $\mathrm{GL}_2(\mathbb{F}_p)$ such that the sequence of Abelian schemes over $\mathbb{Z}[1/p]$*

$$0\to C^0(p)\to J(p,p)\xrightarrow{u} P(p)\xrightarrow{R} P(p),$$

is a complex whose fibres are exact up to isogeny. More precisely, for any ring homomorphism $\mathbb{Z}[1/p]\to k$ with a field k, the groups of connected components of $(\ker R)_k$ and $C(p)_k$ are annihilated by $2p(p+1)$.

We also describe the holomorphic differentials on $X(p,p)_{\mathbb{C}}$ along with their action by the Hecke operators and $\mathrm{GL}_2(\mathbb{F}_p)$. Let us first introduce some notation for the rest of this introduction.

Notation for representation of $\mathrm{GL}_2(\mathbb{F}_p)$:

- $\mathcal{D}$ denotes the set of characters $\mathbb{F}_p^\times\to\mathbb{C}^\times$,
- St denotes the Steinberg representation of $\mathrm{GL}_2(\mathbb{F}_p)$: it is of dimension p and can be realized over $\mathbb{Z}$.
- For any $\alpha\in\mathcal{D}$, let St_α denote the twist of St by the character $\alpha(\det)$ of $\mathrm{GL}_2(\mathbb{F}_p)$.
- For any $\alpha,\beta\in\mathcal{D}$, let $\pi(\alpha,\beta)$ denote the principal series representation of $\mathrm{GL}_2(\mathbb{F}_p)$ attached to the characters α,β.

For any left $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-module V, let $V^\vee$ denote the *right* $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-module $\mathrm{Hom}(V,\mathbb{C})$.

Notation for spaces of modular forms:

- $\mathscr{S}$ denotes the collection of $(f,\mathbf{1})$, where $\mathbf{1}\in\mathcal{D}$ is the trivial character, and f is a newform of level p, weight 2, and trivial character.
- $\mathscr{P}$ denotes the collection of (f,χ), where $f\in\mathcal{S}_2(\Gamma_1(p))$ is a normalized newform with nontrivial character χ. The complex conjugation acts freely on $\mathscr{P}$ by exchanging (f,χ) with $(\overline{f},\chi^{-1})$, where $\overline{f}\in\mathcal{S}_2(\Gamma_1(p))$ the normalized newform whose q-expansion is $\sum_{n\geq 1}\overline{a_n(f)}q^n$.

- $\mathscr{P}'$ denotes a set of representatives for $\mathscr{P}$ modulo the complex conjugation.
- $\mathscr{C}$ denotes the collection of (f,χ), where $f \in \mathcal{S}_2(\Gamma_1(p)\cap\Gamma_0(p^2))$ is a normalized newform with character $\chi \in \mathcal{D}$ and such that no twist of f by a character in $\mathcal{D}$ is of level p.
- $\mathscr{C}_M$ denotes the collection of the $(f,\mathbf{1}) \in \mathscr{C}$ such that f has complex multiplication (necessarily by the field $\mathbb{Q}(\sqrt{-p})$, and $p \equiv 3 \pmod 4$).
- $\mathscr{C}_1$ denotes the collection of the $(f,\mathbf{1}) \in \mathscr{C}\backslash\mathscr{C}_M$, and $\mathscr{C}_1'$ is a set of representatives for $\mathscr{C}_1$ modulo twists by the unique quadratic character in $\mathcal{D}$.
- If $f \in \mathcal{S}_k(\Gamma_1(N))$ is a newform with character χ, L is a number field containing the coefficients of f and λ is a maximal ideal of $\mathcal{O}_L$, $V_{f,\lambda}$ is the continuous irreducible representation $G_{\mathbb{Q}} \to \mathrm{GL}_2(L_\lambda)$ such that, for any prime $q \nmid N$ coprime to the residue characteristic of λ, the characteristic polynomial of the arithmetic Frobenius at q is $X^2 - a_q(f)X + q^{k-1}\chi(q)$.

Theorem 4 *There is an identification $H^0(X(p,p)_{\mathbb{C}},\Omega^1) \simeq \bigoplus_{b\in\mathbb{F}_p^\times} \mathcal{S}_2(\Gamma(p)) \otimes \Delta_{b,1}$ compatible with the action of the T_ℓ and of $\mathrm{GL}_2(\mathbb{F}_p)$. Moreover, $H^0(X(p,p)_{\mathbb{C}},\Omega^1)$ decomposes, as a right $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-module endowed with the action of the T_ℓ, as the following direct sum:*

- *for every $(f,\mathbf{1}) \in \mathscr{S}$, for every $\alpha \in \mathcal{D}$, a copy of $\mathrm{St}_\alpha^\vee$,*
- *for every $(f,\chi) \in \mathscr{P}$ modulo complex conjugation, for every $\alpha \in \mathcal{D}$, a copy of $\pi(\alpha,\alpha\chi)^\vee$,*
- *for every $(f,\chi) \in \mathscr{C}$, a copy of $C_f^\vee$, for a certain irreducible cuspidal representation C_f of $\mathrm{GL}_2(\mathbb{F}_p)$ attached to a pair $\{\phi_f, \phi_f^p\}$ of characters of $\mathbb{F}_{p^2}^\times$.*

For every factor as above (with $\alpha = \mathbf{1}$ in the third kind), for any prime number $\ell \neq p$ (resp. any $n \in \mathbb{F}_p^\times$), T_ℓ (resp. nI_2) acts on the factor by multiplication by $a_\ell(f)\alpha(\ell)$ (resp. $\alpha^2(n)\chi(n)$).

3 Results on the twisted modular Jacobians (Chapters 3-4)

3.1 Chapter 3: The Tate module of the $J_E^\alpha(p)$

In Chapter 3, we use the Eichler-Shimura relation and the results of Chapter 2 to describe the Tate module of the Jacobian of $X(p,p)_{\mathbb{Q}}$, then of the $X_E^\alpha(p)$, where $E/\mathbb{Q}$ denotes an elliptic curve.

In fact, the Tate module of Galois twists of $X(p,p)_{\mathbb{Q}}$ has already been discussed by Virdol [163, Theorem 1.1] for the purposes of proving meromorphic continuation for its L-function in certain cases.

Theorem J *(Virdol [163, Theorem 1.1]) Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ be a group homomorphism. One has an equality of L-functions*

$$L(s, X(p,p)_\rho) = \prod_\pi L(s, \rho_{\pi,\ell} \otimes (\widetilde{\varphi_\pi} \circ \rho)),$$

where

- *in the product, the $\pi = \pi_f \otimes \pi_\infty$ are cuspidal automorphic representations of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$ of weight 2, where π_∞ is cohomological and π_f a representation of $\mathrm{GL}_2(\mathbb{A}_{f,\mathbb{Q}})$ such that $\pi_f^{\hat\Gamma(p)} \neq 0$, where $\hat\Gamma(p) \leq \mathrm{GL}_2(\mathbb{A}_{f,\mathbb{Q}})$ is the principal adelic congruence subgroup of level p,*
- *$\rho_{\pi,\ell}$ is the ℓ-adic Galois representation attached to π,*
- *$\widetilde{\varphi_\pi}$ is the representation of $\mathrm{GL}_2(\mathbb{F}_p)$ attached to $\pi_f^{\hat\Gamma(p)}$.*

This chapter differs from the work of Virdol on the following aspects. First, his statement and arguments rely on the adelic language of automorphic representations, which we try to avoid at this point in the text. Our classical approach makes the representations $\widetilde{\varphi_\pi} \circ \rho$ explicit. Second, when the Galois twist comes from the p-torsion of an elliptic curve (as in Theorem 2), Virdol

computes the L-function (in fact, the Tate module) of the product of the $J_E^\alpha(p)$ over all $\alpha \in \mathbb{F}_p^\times$, while we are interested in the Tate modules of each one of the $X_E^\alpha(p)$, for an elliptic curve $E/\mathbb{Q}$.

In the rest of the introduction, $p \geq 7$ is a prime number and $E/\mathbb{Q}$ is an elliptic curve. Fix a basis (P, Q) of the $\mathbb{F}_p$-vector space $E[p](\overline{\mathbb{Q}})$, and let $\xi = \langle P, Q\rangle_{E[p]} \in \mu_p^\times(\overline{\mathbb{Q}})$ (where $\mu_p^\times(\overline{\mathbb{Q}})$ is the set of roots of unity in $\overline{\mathbb{Q}}$ with order p). Let $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_p)$ be the homomorphism given by

$$\forall \sigma \in G_\mathbb{Q},\ \rho(\sigma)\begin{pmatrix}\sigma(P)\\ \sigma(Q)\end{pmatrix} = \begin{pmatrix}P\\ Q\end{pmatrix},$$

so that $\rho'(\sigma) = (\rho(\sigma)^T)^{-1}$ is the matrix of σ in the basis (P, Q), and in particular $\det\rho$ is the inverse of the cyclotomic character modulo p. Note that in particular ρ is the inverse of the homonymous anti-homomorphism in Theorem 2.

We choose a number field $F \subset \mathbb{C}$ which is Galois over $\mathbb{Q}$ and whose ring of integers $\mathcal{O}_F$ contains the following algebraic numbers:

- the $p(p-1)^2(p+1)$-th roots of unity,
- the Fourier coefficients of any f for $(f, \chi) \in \mathscr{S} \cup \mathscr{P} \cup \mathscr{C}$,
- for every $(f, \mathbf{1}) \in \mathscr{C}_M$, for every prime ℓ split in $\mathbb{Q}(\sqrt{-p})$, the roots of the Hecke polynomial $X^2 - a_\ell(f)X + \ell$ of f at ℓ.

For every $(f, \mathbf{1}) \in \mathscr{C}_M$, we choose a compatible system of characters $(\psi_{f,\lambda})_\lambda$ (where λ runs through the maximal ideals of $\mathcal{O}_F$) with $\psi_{f,\lambda} : G_{\mathbb{Q}(\sqrt{-p})} \to F_\lambda^\times$ attached to f.

When $p \equiv 3 \pmod 4$, the restriction to $\mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p)$ of the cuspidal representation V_4 of $\mathrm{GL}_2(\mathbb{F}_p)$ attached to the character of order 4 of $\mathbb{F}_{p^2}^\times$ is the sum of two irreducible subrepresentations C^+ and C^-, which are dual of each other and conjugate of each other under $\mathrm{GL}_2(\mathbb{F}_p)/\mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p)$.

Theorem 5 *Let ℓ be a prime number and λ be a prime ideal of $\mathcal{O}_F$ with residue characteristic ℓ. Then, for any $\alpha \in \mathbb{F}_p^\times$, $\mathcal{T}_\ell J_E^\alpha(p) \otimes_{\mathbb{Z}_\ell} F_\lambda$ decomposes as the direct sum of the following $F_\lambda[G_\mathbb{Q}]$-submodules:*

- *For every $(f, \mathbf{1}) \in \mathscr{S}$, a copy of $V_{f,\lambda} \otimes (\mathrm{St} \circ \rho)$,*
- *For every $(f, \chi) \in \mathscr{P}'$, a copy of $V_{f,\lambda} \otimes (\pi(\mathbf{1}, \chi) \circ \rho)$,*
- *For every $(f, \mathbf{1}) \in \mathscr{C}_1'$, a copy of $V_{f,\lambda} \otimes (C_f \circ \rho)$, where C_f the cuspidal representation of $\mathrm{GL}_2(\mathbb{F}_p)$ attached to $(f, \mathbf{1})$ by Theorem 4,*
- *For every $(f, \mathbf{1}) \in \mathscr{C}_M$, a copy of $V_{f,\lambda,E}^\epsilon := \mathrm{Ind}_{\mathbb{Q}(\sqrt{-p})}^\mathbb{Q} \psi_{f,\lambda} \otimes C^\epsilon(\rho_{|G_{\mathbb{Q}(\sqrt{-p})}})$, where $\epsilon \in \{\pm\}$ only depends on $\xi^{\alpha\mathbb{F}_p^{\times 2}}$.*

The summands of this decomposition are stable under the Hecke operators T_ℓ with $\ell \equiv 1 \pmod p$, and T_ℓ acts on the factor corresponding to (f, χ) by multiplication by $a_\ell(f)$.

Note that the corresponding Galois representations do not depend on the choice of representative in $\mathscr{P}'$ or $\mathscr{C}_1'$ of a given element in $\mathscr{P}$ (or $\mathscr{C}_1'$).

Notation: If $(f, \chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1'$, let $R_{f,E}$ denote the following Artin representation:

- $\mathrm{St} \circ \rho$ if $(f, \chi) \in \mathscr{S}$,
- $\pi(\mathbf{1}, \chi) \circ \rho$ if $(f, \chi) \in \mathscr{P}'$,
- $C_f \circ \rho$ if $(f, \chi) \in \mathscr{C}_1'$.

3.2 Chapter 4: Galois-theoretic root numbers for $(V_{f,\lambda} \otimes R_{f,E})_\lambda$ and $(V_{f,\lambda,E}^\epsilon)_\lambda$

In Chapter 4, we investigate the L-function of the factors of the Tate module of $J_E^\alpha(p)$. After a reminder about the relevant aspects of the Langlands program, we compute the Galois-theoretic

root numbers of the compatible systems $(V_{f,\lambda} \otimes R_{f,E})_\lambda$ (see above for the definition of $R_{f,E}$) and $(V^\epsilon_{f,\lambda,E})_\lambda$ (defined in Theorem 5). For the sake of simplicity, we report here the results when $E/\mathbb{Q}$ has good reduction at p, although the computations in Chapter 4 cover more general cases. The result depends on the following trichotomy about Galois representations of $G_{\mathbb{Q}_p}$ in $\mathrm{GL}_2(\mathbb{F}_p)$.

Definition *Let $\rho_p : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\mathbb{F}_p)$ be a representation whose determinant is the inverse of the cyclotomic character modulo p. We say that ρ_p is*

- wild *if it is wildly ramified,*
- split *if it is the sum of two characters $G_{\mathbb{Q}_p} \to \mathbb{F}_p^\times$,*
- Cartan *if the image of the inertia subgroup is contained in a nonsplit Cartan subgroup.*

The representation ρ_p is in exactly one of these cases.

Theorem 6 *Assume that $E/\mathbb{Q}$ has good reduction at p. Define U as the product, over every prime number ℓ inert in $\mathbb{Q}(\sqrt{-p})$, of the $(-1)^{m_\ell}$, where $m_\ell \in \mathbb{Z}$ is half the conductor exponent of the Artin representation $V_4 \circ \rho$ at ℓ. Then there is a sign ε_p depending only on the finite flat $\mathbb{Z}_p$-scheme $E[p]_{\mathbb{Z}_p}$, $\xi^{\mathbb{F}_p^{\times 2}}$, and the choice of $\psi_{f,\lambda}$ such that the products of the local Deligne-Langlands constants attached to the summands of $\mathcal{T}_\ell J_E^\alpha(p) \otimes F_\lambda$ are given by Table 1.*

	Type of $\rho_{\mid G_{\mathbb{Q}_p}}$		
	Split	Wild	Cartan
$V_{f,\lambda} \otimes R_{f,E}, (f,\mathbf{1}) \in \mathscr{S}$	$(-1)^{(p+1)/2}$	$(-1)^{(p-1)/2} a_p(f)$	$(-1)^{(p+1)/2}$
$V_{f,\lambda} \otimes R_{f,E}, (f,\chi) \in \mathscr{P}'$	$(-1)^{(p-1)/2}$		
$V_{f,\lambda} \otimes R_{f,E}, (f,\mathbf{1}) \in \mathscr{C}'_1$	$(-1)^{(p+1)/2}$	$(-1)^{(p-1)/2}$	$(-1)^{(p+1)/2}$
$V^\epsilon_{f,\lambda,E}, (f,\mathbf{1}) \in \mathscr{C}_M$	$(-1)^{(p+1)/4} U$	$(-1)^{\frac{p+1}{4}} U \epsilon \varepsilon_p$	$(-1)^{\frac{p+1}{4}} U$

Table 1: Global root numbers for summands of the Tate module of $J_E^\alpha(p)$

3.3 Chapter 4: Automorphic properties of the $(V_{f,\lambda} \otimes R_{f,E})_\lambda$ and $(V^\epsilon_{f,\lambda,E})_\lambda$

Using the Rankin-Selberg method, we prove:

Theorem 7 *If $(f,\mathbf{1}) \in \mathscr{S}$ (resp. $(f,\chi) \in \mathscr{P}'$, resp. $(f,\mathbf{1}) \in \mathscr{C}'_1$) and the Artin representation $R_{f,E}$ is automorphic, then the L-function of the self-dual (up to Tate twist) Galois representation $V_{f,\lambda} \otimes R_{f,E}$ has a holomorphic continuation and satisfies a functional equation whose sign is given (when E has good reduction at p) in Table 1.*

For every $(f,\mathbf{1}) \in \mathscr{C}_M$, the L-function of the self-dual (up to Tate twist) Galois representation $V^\epsilon_{f,\lambda,E}$ admits a meromorphic continuation and satisfies a functional equation whose sign is given in Table 1 when $E/\mathbb{Q}$ has good reduction at p.

As in Theorem 6, the assumption that $E/\mathbb{Q}$ has good reduction at p is made in this part of the introduction for convenience: it is not needed in Chapter 4.

When ρ is surjective, the representations $R_{f,E}$ are irreducible Artin representations of large dimension with non-solvable image, and this does not seem to change after restricting the representations to the absolute Galois group of a totally real number field. As such, proving their automorphy does not seem tractable by current methods.

Another approach to understand the $V_{f,\lambda} \otimes R_{f,E}$ might be to reduce them modulo a prime number. We prove, using results in symmetric power functoriality due to Newton and Thorne [127][12] and in tensor product functoriality in a preprint by Arias-de-Reyna and Dieulefait [3], that the $V_{f,\lambda} \otimes R_{f,E}$ are automorphic modulo p.

Let us first reproduce, for reference, Arias-de-Reyna and Dieulefait's result.

[12] A weaker result that is sufficient for our purposes can be found in the published articles [125, 126].

Theorem K *(Arias-de-Reyna – Dieulefait [3, Theorem 1.1]) Let $f \in \mathcal{S}_k(\Gamma(1))$ be a cuspidal modular form and let $\rho_\bullet(f)$ be the attached compatible system of Galois representations. Let $n > 0$ be an integer and π be a regular algebraic cuspidal polarized automorphic representation of $GL_n(\mathbb{A}_\mathbb{Q})$ of level coprime to 3. Let $r_\bullet(\pi)$ be the attached compatible system of Galois representations. Assume that $\rho_\bullet(f) \otimes r_\bullet(\pi)$ is a regular and irreducible compatible system. Then $\rho_\bullet(f) \otimes r_\bullet(\pi)$ is automorphic, i.e. there exists a regular algebraic cuspidal polarized automorphic representation $f \otimes \pi$ of $GL_{2n}(\mathbb{A}_\mathbb{Q})$ such that the compatible system attached to $f \otimes \pi$ is isomorphic to $\rho_\bullet(f) \otimes r_\bullet(\pi)$.*

Theorem 8 *Assume that E has good reduction at 3 and that ρ is onto. Assume furthermore Theorem K holds. There exists a number field $F' \supset F$ and a prime ideal $\mathfrak{p}$ of F' with residue characteristic p such that for any $(f, \chi) \in \mathscr{S} \cup \mathscr{P}'_1 \cup \mathscr{C}'_1$, the semi-simplification of the reduction modulo $\mathfrak{p}$ of $V_{f,\mathfrak{p}} \otimes R_{f,E}$ is the direct sum of the semi-simplifications of the reductions modulo $\mathfrak{p}$ of automorphic Galois representations (with coefficients in $(F')_\mathfrak{p}$).*

While this result is certainly interesting, its practical utility for Diophantine questions seems unclear.

4 When the image of ρ is contained in the normalizer of a nonsplit Cartan subgroup (Chapter 5)

In Chapter 5, we assume that $\rho(G_\mathbb{Q})$ is contained in the normalizer N of a nonsplit Cartan subgroup C. Let $K/\mathbb{Q}$ be the imaginary quadratic field corresponding to the character $G_\mathbb{Q} \to N \to N/C \simeq \{\pm 1\}$. We assume in this introduction that $p \geq 11$ for the sake of simplicity: then K is inert at p by Proposition 5.4.2.

4.1 Decomposition of the Tate module and functional equation

In such a situation, the decomposition we gave in Theorem 5 is not optimal and can be split further. Let us fix, once and for all, a group isomorphism ι between C and $\mathbb{F}_{p^2}^\times$ preserving the norm and the trace. This isomorphism is not quite canonical, but the pair $\{\iota, \iota^p\}$ is: as a consequence, there is a canonical identification between pairs $\{\psi, \psi^p\}$ of characters of C and pairs $\{\phi, \phi^p\}$ of characters of $\mathbb{F}_{p^2}^\times$.

Theorem 9 *Let λ be a prime ideal of $\mathcal{O}_F$ with residue characteristic ℓ. For any $\alpha \in \mathbb{F}_p^\times$, $\mathcal{T}_\ell J_E^\alpha(p) \otimes_{\mathbb{Z}_\ell} F_\lambda$ is the direct sum of the following continuous representations of $G_\mathbb{Q}$ stable under the Hecke operators:*

- *for every $(f, \chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}'_1 \cup \mathscr{C}_M$, a copy of $V_{f,\lambda} \otimes \theta$, where θ is a certain explicit character of $\mathrm{Gal}(K(\mu_p)/\mathbb{Q})$ independent from ρ; there are two possible θ if $(f, \chi) \in \mathscr{P}' \cup \mathscr{C}'_1$ and one otherwise,*
- *for every $(f, \chi) \in \mathscr{S} \cup \mathscr{P}'$, for every pair $\{\psi, \psi^p\}$ of distinct characters $C \to F^\times$ such that $\psi(tI_2) = \chi(t)$ for $t \in \mathbb{F}_p^\times$, a copy of $V_{f,\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi\right) \circ \rho\right]$,*
- *for every $(f, \mathbf{1}) \in \mathscr{C}'_1$ (resp. $(f, \mathbf{1}) \in \mathscr{C}_M$), for every pair $\{\psi, \psi^p\} \neq \{\phi_f, \phi_f^p\}$ of distinct characters $C/\mathbb{F}_p^\times I_2 \to F^\times$ (resp. up to the equivalence relation $\{\psi, \psi^p\} \sim \{\theta, \theta^p\}$ if and only if $\psi\theta^{-1}$ or $\psi^p\theta^{-1}$ has order at most two), a copy of $V_{f,\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi\right) \circ \rho\right]$.*

On each summand, the Hecke operator T_ℓ (for any prime $\ell \equiv 1 \pmod p$) acts by multiplication by $a_\ell(f)$.

Compared to the decomposition of Theorem 5, such summands are much easier to understand, and their properties as Galois representations are better-known. The rest of Chapter 5 applies Mazur's strategy to the question of rational points on $X_E^\alpha(p)$. The first step is to show that the L-functions of the factors described in the previous theorem extend to entire functions, satisfy functional equations, and to determine the sign of said functional equations.

Theorem 10 *Every summand described in Theorem 9 is a self-dual Galois representation (up to Tate twist), and its L-function extends to an entire function and satisfies a functional equation whose sign is -1 except in the following cases:*

- $V_{f,\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi\right) \circ \rho\right]$ *with* $(f, \mathbf{1}) \in \mathscr{S}$ *and* $\left(\mathrm{Ind}_C^N \psi\right) \circ \rho$ *unramified at* p,
- $V_{f,\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi\right) \circ \rho^{-1}\right]$ *with* $(f, \mathbf{1}) \in \mathscr{C}_1' \cup \mathscr{C}_M$ *if the following condition is satisfied. Let* $M/\mathbb{Q}_p$ *denote the unique quadratic unramified extension and* $\mathfrak{a} : \mathrm{Gal}(\overline{\mathbb{Q}_p}/M) \to \widehat{M^\times}$ *be the class field theory reciprocity homomorphism mapping an arithmetic Frobenius to a uniformizer; in particular,* $\mathfrak{a}$ *has a subquotient* $\overline{\mathfrak{a}}$ *mapping the inertia subgroup* $I_p \triangleleft \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ *to* $\mathcal{O}_M^\times/(1+p\mathcal{O}_M) \simeq \mathbb{F}_{p^2}^\times$. *The sign of the functional equation of the representation is one if and only if the pairs* $\{\phi_f \circ \overline{\mathfrak{a}}, \phi_f^p \circ \overline{\mathfrak{a}}\}$ *and* $\{\psi \circ \rho_{|I_p}, \psi^p \circ \rho_{|I_p}\}$ *of characters* $I_p \to F^\times$ *are equal.*

In both cases, E and its quadratic twists have bad reduction at p. In the first case, one has $\rho(I_p) = 3C$, $p \equiv 2, 5 \pmod 9$, and ψ has order exactly 3.

4.2 The Bloch-Kato conjecture in rank zero for the factors of $J_E^\alpha(p)$

The next result of this chapter is the proof of the Bloch-Kato conjecture in analytic rank zero for factors of $J_E^\alpha(p)$. This is achieved using the Beilinson-Flach Euler system constructed by Kings, Loeffler and Zerbes [92] and by weakening the conditions (see for instance [108, Section 4.4]) under which Rankin-Selberg convolutions of modular forms satisfy the required *large image assumptions* – which is among the contents of Chapter 6, which we discuss later.

In the setting of Theorem 9, let $(f,\chi), (f',\chi') \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1' \cup \mathscr{C}_M$, and $\{\psi, \psi^p\}, \{\psi', (\psi')^p\}$ be two pairs of distinct characters $C \to F^\times$. We say that the Galois representations

$$V_{f,\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi\right) \circ \rho\right], V_{f',\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi'\right) \circ \rho\right]$$

are *in the same Galois orbit* if there is a $\sigma \in G_{\mathbb{Q}}$ such that for all but finitely many prime numbers q, one has

$$\mathrm{Tr}\left(\mathrm{Frob}_q \mid V_{f',\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi'\right) \circ \rho\right]\right) = \sigma\left[\mathrm{Tr}\left(\mathrm{Frob}_q \mid V_{f,\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi\right) \circ \rho\right]\right)\right].$$

Theorem 11 *Let V be one of the four-dimensional summands described in Theorem 9, attached to a triple $((f,\chi), \{\psi, \psi^p\})$. For any $\alpha \in \mathbb{F}_p^\times$, there is a natural quotient A stable by the Hecke operators of $J_E^\alpha(p)$ such that $\mathcal{T}_\ell A \otimes_{\mathbb{Z}_\ell} F_\lambda$ identifies with the direct sum of the summands described in Theorem 9 that are in the same Galois orbit as V. Suppose furthermore that f does not have complex multiplication and $L(V,1) \neq 0$, so that $(f,\chi) \in \mathscr{S} \cup \mathscr{C}_1'$.*

Then $A(\mathbb{Q})$ is finite.

To construct the quotient A, one uses the fact that the choice of basis (P,Q) for $E[p]$ defines an isomorphism $\coprod_{\alpha \in \mathbb{F}_p^\times} X_E^\alpha(p)_{\overline{\mathbb{Q}}} \cong X(p,p)_{\overline{\mathbb{Q}}}$, and in particular endows $\coprod_{\alpha \in \mathbb{F}_p^\times} X_E^\alpha(p)_{\overline{\mathbb{Q}}}$ with an action of $\mathrm{GL}_2(\mathbb{F}_p)$.

4.3 The formal immersion theorem

In the last part of the chapter, we assume that the representation V of Theorem 11 is of the first form in Theorem 10, which implies in particular that $p \equiv 2, 5 \pmod 9$.

Fix any cusp $c \in X_E^\alpha(p)(\overline{\mathbb{Q}})$ and let $q \equiv 1 \pmod p$ be a prime number. Then the morphism $x \longmapsto (T_q - q - 1)(x - c) : X_E^\alpha(p)_{\overline{\mathbb{Q}}} \to J_E^\alpha(p)_{\overline{\mathbb{Q}}}$ is in fact defined over $\mathbb{Q}$ and is independent from the choice of c, because $T_q - q - 1$ vanishes on the divisors supported on the cuspidal subscheme, and consider its composition f with the projection $J_E^\alpha(p) \to A$, where A is as in Theorem 11. Using the description of the differentials over $\mathbb{C}$ from Chapter 2, we are able to run

an analogue of Mazur's formal immersion argument (although our actual formulation is closer to the Chabauty-Coleman method, see [115]) for the morphism $f : X_E^{\alpha}(p) \to A$.

Definition *For every cube root of unity $j \in \mathbb{F}_{p^2}^{\times}$, let*

$$u_j = \sum_{\substack{b \in \mathbb{F}_p \\ 1+b\sqrt{-3} \in \mathbb{F}_{p^2}^{\times 3} j}} e^{\frac{2i\pi b}{p}}.$$

We say that a prime number ℓ is exceptional *for p if $\ell \equiv \pm 1 \pmod{p}$ and there is a prime ideal λ of $\mathbb{Z}[e^{2i\pi/p}]$ with residue characteristic ℓ containing every u_j.*

Direct computations with Magma [16] show that for any $p \leq 1500$, the three u_j generate the unit ideal of $\mathbb{Z}[e^{\frac{2i\pi}{p}}]$. We thus tentatively expect that for any p, there are no exceptional primes[13].

Theorem 12 *Assume that $\rho : G_{\mathbb{Q}} \to N$ is surjective with Artin conductor N_ρ. Let $\psi : C \to F^{\times}$ be a character of order 3 and assume that there exists $(f, \mathbf{1}) \in \mathscr{S}$ such that the central value of the L-function of the Galois representation $V_{f,\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi\right) \circ \rho\right]$ is nonzero: this implies in particular that the image by ρ of an inertia subgroup at p is the proper subgroup of C with index 3.*

Let $E'/\mathbb{Q}$ be an elliptic curve congruent to E modulo p. Then the conductor of E' is equal to $p^2 N_\rho L$, where L is a square-free product of exceptional primes that do not divide pN_ρ.

The known results on the effectivity of Serre's open image theorem, such as [168, Theorems 1.5, 1.10], do not seem to rule out the existence of a non-CM elliptic curve E' as in Theorem 12, nor does this result seem to easily imply that E' and E are isogenous, even assuming that E and E' both have conductor $p^2 N_\rho$. [14]

4.4 Application to congruences to the CM elliptic curve $y^2 = x^3 - p$

In [95], Kraus computes the Serre weight of the p-torsion of an elliptic curve with additive reduction. In particular, when $p \equiv 5 \pmod 9$ and E is the elliptic curve E_p with Weierstrass equation $y^2 = x^3 - p$, we can check that:

- $\rho(G_{\mathbb{Q}}) = N$,
- the image by ρ of an inertia subgroup at p is properly contained in C,
- $\left(\mathrm{Ind}_C^N \psi\right) \circ \rho$ is attached to the unique newform $g \in \mathcal{S}_1(\Gamma_1(108))$ with rational coefficients and complex multiplication by $\mathbb{Q}(\sqrt{-3})$.

When p is small, we can check numerically with MAGMA [16] that there are no exceptional primes for p and with PARI/GP [161] that for some $(f, \mathbf{1}) \in \mathscr{S}$ that the Rankin-Selberg L-value $L(f \times g, 1)$ appearing in Theorem 12 is nonzero[15]. In conductor at most 500000, Cremona and Freitas [33, Theorem 1.3] prove that elliptic curves that are congruent modulo some prime $q \geq 19$ are isogenous. This implies:

[13] After the first submission of this thesis, further computations on the IMJ-PRG's computer were carried out with a slightly improved algorithm, showing in approximately 8 hours and 30 GB of memory that there were no exceptional primes for $11 \leq p \leq 5000$ with $p \equiv 2, 5 \pmod 9$.

[14] Since the submission of this thesis, I realized that the main result of [5] implies that, in such a situation, when $p \leq 100$, the elliptic curve E' has complex multiplication.

[15] At the time of submission of this thesis, this was computed for $p = 23, 29$ for the newform g of weight 1, conductor 108, rational coefficients, and with CM by $\mathbb{Q}(\sqrt{-3})$ which appears in Theorem 13. Since then, further computations were made on the IMJ-PRG's calculators with the help of P. Molin, showing that the same non-vanishing result held for all $p \leq 150$ with $p \equiv 2, 5 \pmod 9$. We already know that there are no exceptional primes in this range, this implies in particular that the Corollary immediately below holds for $p = 41, 59$, and remains true if $p = 113, 131, 149$, when the conclusion is replaced with "E' has the same conductor as E_p".

Corollary 1 *Let $p = 23$. If E' is an elliptic curve congruent modulo p to E_p, then E' is isogenous to E_p.*

For arbitrary primes p, one expects that there exists $(f, \mathbf{1})$ such that $L(f \times g, 1) \neq 0$, but this seems difficult to prove. The following result of Michel, proved by analytic number theory, shows that this is indeed the case when p is large enough.

Theorem L *(Michel, [157, Appendix, Theorem 0.1]) Let $g \in \mathcal{S}_1(\Gamma_1(N))$ be a newform with character χ. There exists a constant C_g satisfying the following property: for any prime $p > C_g$ if g does not have real coefficients or $\chi(p) = -1$, there exists $f \in \mathcal{S}_2(\Gamma_0(p))$ such that $L(f \times g, 1) \neq 0$.*

Theorem 13 *There exists a constant $p_0 \geq 11$ satisfying the following property. Let $p \geq p_0$ be a prime number such that $p \equiv 5 \pmod 9$ and E be the elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-3})$ given by the minimal Weierstrass equation $y^2 = x^3 - p$ (with conductor $108mp^2$, where $m = 1$ if $p \equiv 3 \pmod 4$ and $m = 4$ if $p \equiv 1 \pmod 4$). Then, for any elliptic curve E' congruent to E modulo p, the conductor of E' is given by $108mp^2L$, where L is a square-free product of primes $\ell \equiv \pm 1 \pmod p$ that are exceptional for p. In particular, if there are no exceptional primes for p, E' and E have the same conductor and $j(E')$ is an integer.*

5 Large image results for the Rankin-Selberg convolution of two modular forms (Chapter 6)

Chapter 6 is a preprint [155] by the author of this thesis. It arose from the use of theory of Euler systems in the proof of Theorem 11.

Let $\mathcal{O}_K$ be the ring of integers of a finite extension $K/\mathbb{Q}_p$ and T be a free $\mathcal{O}_K$-module of finite rank on which $G_\mathbb{Q}$ has a continuous $\mathcal{O}_K$-linear action. An Euler system for T can be seen as a collection of cohomology classes $c_n \in H^1(\mathbb{Q}(\mu_n), T)$ for certain integers $n \geq 1$ (including 1) satisfying certain norm relations. The theory of Euler systems, as described in the standard references [137, 114], aims to bound the size of Selmer groups attached to $\mathrm{Hom}_{\mathcal{O}_K}(T, K/\mathcal{O}_K(1))$ given an Euler system $(c_n)_n$ for T such that $c_1 \neq 0$. However, the theory requires certain assumptions about the Galois image of $G_\mathbb{Q}$ in $\mathrm{Aut}(T)$, such as variants or strengthenings of the following condition, which we will call the *adapted image condition*: there exists $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$ such that $T/(\sigma - 1)T \otimes_{\mathcal{O}_K} K$ is a one-dimensional vector space.

In [92], Kings, Loeffler and Zerbes construct an Euler system for some of the Galois representations appearing in Theorem 9, and derive the bounds on Selmer groups that we use in the proof of Theorem 11 assuming the adapted image condition. In [108, Section 4.4], Loeffler proves that the adapted image condition is often satisfied:

Theorem M *(Loeffler [108]) Let $f \in \mathcal{S}_k(\Gamma_1(N_f)), g \in \mathcal{S}_1(\Gamma_1(N_g))$ be newforms with respective characters $\varepsilon_f, \varepsilon_g$ such that $k > 1$ and f is not CM. Let L be a number field containing the coefficients of f and g with ring of integers $\mathcal{O}_L$.*

- *If there is a maximal ideal λ of $\mathcal{O}_L$ such that $V_{f,\lambda} \otimes_{L_\lambda} V_{g,\lambda}$ satisfies the adapted image condition, then $\varepsilon_f\varepsilon_g \neq 1$.*
- *Assume that $\varepsilon_f\varepsilon_g \neq 1$ and that N_f and N_g are coprime. Then, for all but finitely many maximal ideals λ of $\mathcal{O}_L$, $V_{f,\lambda} \otimes V_{g,\lambda}$ satisfies the adapted image condition.*

In the same paper, the author suggests the following question.

Question 3 *(Loeffler, [108, Remark 4.4.2]) Consider the notations of Theorem M and assume that $\varepsilon_f\varepsilon_g \neq 1$. Is it true that, for all but finitely many maximal ideals λ of $\mathcal{O}_L$, $V_{f,\lambda} \otimes V_{g,\lambda}$ satisfies the adapted image condition?*

Theorem M does not cover all the cases needed for the proof of Theorem 11: in the second case described in Theorem 10, the conductors of both modular forms are divisible by p^2, so Theorem M does not prove the adapted image condition. This is the motivation for our work on

Question 3. First, we give weaker sufficient conditions under which the answer to Question 3 is positive.

Theorem 14 *Let us keep the notations of Theorem M and assume that $\varepsilon_f\varepsilon_g \neq 1$. The answer to Question 3 is positive if any of the following conditions is satisfied:*

- *For any (primitive) Dirichlet character χ with conductor C such that $f \otimes \chi$ is Galois-conjugate to f, C is coprime to N_g.*
- *Any (primitive) Dirichlet character χ such that $f \otimes \chi$ is Galois-conjugate to f is even.*
- *$\varepsilon_f^2 = \varepsilon_g^2 = 1$ and $f \otimes \varepsilon_g$ is not Galois-conjugate to f.*
- *The group $\varepsilon_g\left(\bigcap_\chi \ker\chi\right)$ contains an element of order 2 but no element of order 4, where χ runs through (primitive) Dirichlet characters such that $f \otimes \chi$ is Galois-conjugate to f.*

This result implies a slight generalization of the twisted Birch and Swinnerton-Dyer conjecture proved in [92, Theorem 11.7.4] for twists of elliptic curves by two-dimensional odd irreducible Artin representations: we show in Corollary 6.3.11 that in the statement of *loc.cit.*, we need no longer assume that the elliptic curve and the Artin representation have coprime conductors.

We also show that the general answer to Question 3 is negative: the following equivalence lets us describe infinite families of counterexamples.

Theorem 15 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a newform of even weight. The following are equivalent:*

- *For any quadratic number field K, the answer to Question 3 is positive for all but finitely couples (f, g), where g is a newform of weight one with real or complex multiplication by K.*
- *The answer to Question 3 is positive for all couples (f, g) where g is a newform of weight one.*
- *Any (primitive) Dirichlet character χ such that $f \otimes \chi$ is Galois-conjugate to f is even.*

We also describe explicit counter-examples not arising from the same obstruction as the one highlighted by the proof of Theorem 15.

Theorem 16 *There exist newforms $f \in \mathcal{S}_2(\Gamma_0(63)), g \in \mathcal{S}_1(\Gamma_1(1452))$ with coefficients respectively in $\mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{-3})$ such that, for all but finitely many prime ideals $\mathfrak{p}$ of $L = \mathbb{Q}(e^{2i\pi/12})$ with residue characteristic $p \equiv 5, 7 \pmod{12}$, $V_{f,\mathfrak{p}} \otimes V_{g,\mathfrak{p}}$ does not satisfy the adapted image condition.*

Acknowledgements I am deeply grateful for the help and support that my supervisor Loïc Merel gave me, as well as his many suggestions, comments and further questions that helped shape this work. I would like to thank the referees Pierre Parent and Henri Darmon for their reviewing this manuscript and their comments. I am also grateful to Farrell Brumley, Anna Cadoret, Pierre-Henri Chaudouard, Laurent Clozel, Pierre Colmez, Fred Diamond, Marc Hindry, Qing Liu, David Loeffler, Barry Mazur, Jean-François Mestre and Pascal Molin for fruitful discussions regarding parts of this thesis, for their patience in answering my questions, and for pointing me towards the relevant literature.

Résumé de la thèse

Ce chapitre est une traduction en français de la deuxième partie de l'introduction et résume le contenu de cette thèse. Les résultats de l'introduction en anglais ne sont pas cités ici ; les références sont internes, renvoient au corps de la thèse ou à la bibliographie.

Étant donné une courbe elliptique $E/\mathbb{Q}$ et un nombre premier $p \geq 7$, il existe une courbe modulaire $X_E^\alpha(p)$ définie sur $\mathbb{Q}$ dont les points non cuspidaux paramétrent les couples (F, ι), où F est une courbe elliptique sur un $\mathbb{Q}$-schéma S et $\iota : E[p]_S \to F[p]$ est un isomorphisme de schémas finis plats. Cette thèse vise à étudier l'arithmétique des courbes $X_E^\alpha(p)$.

1 Résultats de base (Chapitres 1-2)

1.1 Chapitre 1 : les problèmes de modules

Dans le Chapitre 1, nous rappelons la théorie des espaces de modules de courbes elliptiques telle qu'elle est décrite dans le livre de Katz et Mazur [86]. L'objectif de ce chapitre est de donner une preuve complète de l'existence des courbes modulaires $X_E^\alpha(p)$ sur des bases plus générales que des corps, généralisant ainsi [97, Proposition 2] et [113, §1.7], et de décrire brièvement leur géométrie. En particulier, nous montrons que ces courbes peuvent être dotées de $\Gamma_0(m)$-structures supplémentaires qui les munissent de correspondances de Hecke. Un tel résultat semble bien connu, mais il semble relever du folklore et nous n'en avons pas trouvé une preuve détaillée dans la littérature.

L'intérêt de travailler sur des bases géométriques au-delà de celles des corps apparaît lorsque l'on tente d'appliquer la technique de l'immersion formelle introduite par Mazur dans [111]. En effet, cette dernière impose de comprendre la géométrie de morphismes de la courbe modulaire vers certains quotients de sa jacobienne, y compris en caractéristique finie.

Le premier résultat est le suivant.

Théorème 1 *Soient $N \geq 3$ un entier et R une $\mathbb{Z}[1/N]$-algèbre noethérienne régulière et excellente. Soit G un schéma en groupes fini sur R, étale-localement isomorphe à $(\mathbb{Z}/N\mathbb{Z})^{\oplus 2}$, muni d'un accouplement bilinéaire alterné parfait $(-,-)_G : G \times G \to \mu_N$. Il existe un schéma $X_G(N)$ propre et lisse sur R de dimension relative* 1 *satisfaisant les propriétés suivantes :*

- *Il possède un morphisme fini plat $(j, \det) : X_G(N) \to \mathbb{P}^1_R \times (\mathbb{Z}/N\mathbb{Z})^\times_R$ et les fibres de* det *sont géométriquement connexes.*
- *Le sous-schéma fermé réduit de $X_G(N)$ associé au sous-espace fermé $\{j = \infty\}$, appelé le* sous-schéma cuspidal*, est fini étale sur R et définit un diviseur de Cartier effectif.*
- *Le foncteur des points de $j^{-1}(\mathbb{A}^1_R)$ est isomorphe au foncteur qui à un R-schéma S associe l'ensemble des classes d'équivalence de couples $(E/S, \iota)$, où E/S est une courbe elliptique relative, et $\iota : G_S \to E[N]$ est un isomorphisme de S-schémas en groupes. À travers cet isomorphisme, j envoie le couple $(E/S, \iota)$ sur $j(E)$ et* det *sur l'unique $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$ tel que l'accouplement bilinéaire alterné*

$$G \times G \xrightarrow{\iota \times \iota} E[N] \times E[N] \xrightarrow{\mathrm{We}} (\mu_N)_S$$

soit exactement $\alpha \cdot (-,-)_G$, où We *désigne l'accouplement de Weil.*
- *La construction de $X_G(N), j, \det$, du sous-schéma cuspidal, et de l'isomorphisme ci-dessus commute au changement de base.*

Pour $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$, notons $X_G^\alpha(N)$ le sous-schéma ouvert fermé $\det^{-1}(\alpha)$ de $X_G(N)$, et $J_G^\alpha(N)$ la jacobienne de cette courbe relative sur R. Pour tout $n \in (\mathbb{Z}/N\mathbb{Z})^\times$, l'isomorphisme de foncteurs $(E/S, \iota, C) \longmapsto (E/S, n \cdot \iota, C)$ s'étend en un isomorphisme $[n] : X_G^\alpha(N) \to X_G^{n^2\alpha}(N)$.

Pour chaque nombre premier $\ell \nmid N$, pour tout $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$, on dispose d'une correspondance de Hecke sur $X_G^\alpha(N) \times X_G^{\ell\alpha}(N)$ induisant un endomorphisme T_ℓ du schéma abélien $\prod_{\alpha\in(\mathbb{Z}/N\mathbb{Z})^\times} J_G^\alpha(N)$. Tous les T_ℓ et les $[n]$ commutent deux à deux, et T_ℓ envoie la composante $J_G^\alpha(N)$ dans la composante $J_G^{\ell\alpha}(N)$.

Lorsque N est un nombre premier $p \geq 5$ et G désigne la p-torsion d'une courbe elliptique munie de son accouplement de Weil, on obtient :

Corollaire 1 *Soient R un anneau de Dedekind excellent*[16] *et E/R une courbe elliptique. Soit $p \geq 3$ un nombre premier inversible dans R et $\alpha \in \mathbb{F}_p^\times$. Il existe un R-schéma propre et lisse de dimension relative un $X_E^\alpha(p)$ aux fibres géométriquement connexes, muni également des données suivantes :*

- *un morphisme fini localement libre $j : X_E^\alpha(p) \to \mathbb{F}_p^\times$ tel que le sous-schéma fermé réduit associé au sous-espace $\{j = \infty\}$ soit fini étale sur R,*
- *un isomorphisme entre le foncteur des points de $j^{-1}(\mathbb{A}^1_R)$ et le foncteur qui à chaque R-schéma S associe les classes d'équivalence de couples $(F/S, \iota)$, où F/S est une courbe elliptique relative et $\iota : E[p]_S \to F[p]$ est un isomorphisme de schémas en groupes tel que les deux accouplements ci-dessous soient égaux :*

$$E[p]_S \times E[p]_S \xrightarrow{\alpha\cdot \mathrm{We}} (\mu_p)_S, \quad E[p]_S \times E[p]_S \xrightarrow{\iota\times\iota} F[p] \times F[p] \xrightarrow{\mathrm{We}} (\mu_p)_S,$$

- *une jacobienne relative $J_E^\alpha(p)$,*
- *pour chaque nombre premier $\ell \neq p$, des opérateurs de Hecke $T_\ell : J_E^\alpha(p) \to J_E^{\ell\alpha}(p)$ qui commutent deux à deux,*
- *pour chaque $n \in \mathbb{F}_p^\times$, un isomorphisme $[n] : X_E^\alpha(p) \to X_E^{n^2\alpha}(p)$.*

Nous relions ensuite ces $X_E^\alpha(p)$ à la courbe modulaire classique $\Gamma(p)$. Plus précisément, soit $X(p,p)$ la courbe modulaire compacte sur $\mathbb{Z}[1/p]$ dont les sections non-cuspidales paramétrent les courbes elliptiques munies d'une base de leur p-torsion. C'est un $\mathbb{Z}[1/p]$-schéma projectif lisse de dimension relative 1 muni d'une action à gauche du groupe $\mathrm{GL}_2(\mathbb{F}_p)/\{\pm I_2\}$, d'un morphisme fini localement libre $j : X(p,p) \to \mathbb{P}^1_{\mathbb{Z}/[1/p]}$ (donné par le j-invariant), et d'un morphisme d'accouplement de Weil $X(p,p) \to \operatorname{Spec}\mathbb{Z}[1/p, \zeta_p]$, qui est propre, lisse de dimension relative 1 et aux fibres géométriquement connexes.

Si R est un corps de caractéristique distincte de p et E/R est une courbe elliptique, nous pouvons également construire la réunion disjointe des $X_E^\alpha(p)$ comme tordue galoisienne de la courbe modulaire (non géométriquement connexe) $X(p,p)_R$ sur R. Nous vérifions également que cette identification est compatible avec les opérateurs de Hecke et le j-invariant dont nous avons parlé précédemment. L'équivalence des deux constructions est implicitement utilisée dans la preuve de la modularité des courbes elliptiques semi-stables par Wiles [166, p. 543] afin d'effectuer le « 3−5 switch », et semble mentionnée dans l'introduction de [163], mais il ne semble pas qu'elle ait été complètement rédigée.

Il y a plusieurs définitions possibles pour la notion de *tordue galoisienne*. Celle que nous utilisons est la suivante (qui est un cas particulier de la Proposition A.1.11).

[16] C'est par exemple le cas si $\mathrm{Frac}(R)$ est de caractéristique nulle, si R est un anneau de valuation discret complet, ou si R est essentiellement de type fini sur un corps.

Définition *Soit X un schéma lisse et quasi-projectif sur un corps k de clôture séparable k_s. Soit $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{Aut}(X)$ un morphisme de groupes continu, où $\mathrm{Aut}(X)$ est muni de la topologie discrète. Le* tordu *de X par ρ est l'unique k-schéma lisse et quasi-projectif X' muni d'un isomorphisme $j : j : X'_{k_s} \to X_{k_s}$ de k_s-schémas tel que, si β désigne la composition $X'(k_s) \xrightarrow{\sim} X'_{k_s}(k_s) \xrightarrow{j} X_{k_s}(k_s) \xrightarrow{\sim} X(k_s)$ et $g \in \mathrm{Gal}(k_s/k)$, pour tout $P \in X'(k_s)$, l'on a $\beta(g \cdot P) = \rho(g)(g \cdot \beta(P))$.*

Cette construction est fonctorielle dans un sens naturel explicité dans la Proposition A.1.13. On utilisera parfois « tordue » (au féminin) lorsque l'on considère X comme une courbe ou une variété sur le corps k.

Théorème 2 *Soient k un corps de clôture séparable k_s et $p \geq 3$ un nombre premier inversible dans k. Soient E/k une courbe elliptique et $(P, Q) \in E(k_s)^2$ une base de son sous-groupe de p-torsion. Pour chaque $\sigma \in \mathrm{Gal}(k_s/k)$, soit $\rho(\sigma) \in \mathrm{GL}_2(\mathbb{F}_p)$ la matrice telle que $\begin{pmatrix}\sigma(P)\\ \sigma(Q)\end{pmatrix} = \rho(\sigma)\begin{pmatrix}P\\ Q\end{pmatrix}$. Alors $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ est un anti-homomorphisme de groupes.*

Soit $X(p,p)_{\rho^{-1}}$ le tordu de $X(p,p)_k$ par la représentation galoisienne ρ^{-1}. Le tordu par ρ^{-1} du morphisme

$$(j, \mathrm{We}) : X(p,p)_k \to \mathbb{P}^1_k \times_k \operatorname{Spec} k \otimes \mathbb{Z}[\zeta_p]$$

est un morphisme

$$(j, \mathrm{We}_{\rho^{-1}}) : X(p,p)_{\rho^{-1}} \to \mathbb{P}^1_k \times_k S,$$

où S est le k-schéma constant d'ensemble sous-jacent l'ensemble $\mu_p^\times(k_s)$ des racines primitives p-ièmes de l'unité dans k_s. Pour chaque $\zeta \in \mu_p^\times(k_s)$, soit $X_{\rho,\zeta}(p)$ l'image réciproque de la composante ζ de S dans $X(p,p)_{\rho^{-1}}$.

Soit $\xi = \langle P, Q\rangle_{E[p]} \in \mu_p^\times(k_s)$. Pour chaque $a \in \mathbb{F}_p^\times$, on dispose d'un isomorphisme de $\mathbb{P}^1_k$-schémas $\iota^a_{E,P,Q} : X^a_E(p)_k \to X_{\rho,\xi^a}(p)$ tel que pour tout point non-cuspidal $(F/k_s, \iota) \in X^a_E(p)(k_s)$, l'on a

$$\iota^a_{E,P,Q}(F/k_s, \iota) = (F/k_s, (\iota(P), \iota(Q))) \in X(p,p)(k_s) \supset X_{\rho,\xi^a}(p)(k_s).$$

Enfin, la réunion disjointe des $\iota^a_{E,P,Q}$ induit un isomorphisme $\iota^J_{E,P,Q}$ entre le produit des $J^a_E(p)$ et le tordu galoisien $J(p,p)_{\rho^{-1}}$ par ρ^{-1} de la jacobienne[17] de la courbe $X(p,p)_k \to \operatorname{Spec} k$. La variété abélienne $J(p,p)_{\rho^{-1}}$ est munie (à travers sa structure de tordue galoisienne) de l'opérateur de Hecke T_ℓ pour chaque nombre premier $\ell \neq p$ et de l'automorphisme $[n]$ pour chaque $n \in \mathbb{F}_p^\times$ (envoyant le couple $(F/S, (A, B))$ – où F/S est une courbe elliptique relative sur le k-schéma S et (A, B) forme une base de $F[p](S)$ – sur $(F/S, (nA, nB))$).

L'isomorphisme $\iota^J_{E,P,Q}$ préserve les opérateurs de Hecke et l'action de $\mathbb{F}_p^\times$.

Puisque nous nous en servons plus tard dans le manuscrit, nous montrons quelques résultats classiques de la géométrie arithmétique des courbes modulaires, et notamment la relation d'Eichler-Shimura, un principe de q-développement, et une description de l'action des opérateurs de Hecke sur le sous-schéma cuspidal.

1.2 Chapitre 2 : la structure de $J(p,p)$ comme module sur l'algèbre de Hecke et $\mathrm{GL}_2(\mathbb{F}_p)$

Dans le chapitre 2, nous étudions les propriétés géométriques de la courbe modulaire $X(p,p)_{\mathbb{Z}[1/p]}$, dont nous appelons la jacobienne relative $J(p,p)$. Soit $X_1(p,\mu_p)$ le changement de base à $\mathbb{Z}[1/p,\zeta_p]$ de la courbe modulaire propre et lisse sur $\mathbb{Z}[1/p]$ dont les points non-cuspidaux paramètrent les

[17] La notion de jacobienne pour une courbe non géométriquement connexe ne semble pas complètement standard à en juger [119] et [15, Chapters 8-9], mais peut être dégagée au prix de modifications mineures des résultats existants pour les schémas $C \to S$ propres lisses de dimension relative 1 aux fibres géométriquement connexes. Nous décrivons dans l'Appendice A.4 les adaptations nécessaires.

classes d'isomorphisme de couples $(E/S, P)$, où E est une courbe elliptique relative sur le $\mathbb{Z}[1/p]$-schéma S et P un point « d'ordre exact p » au sens de [86, (3.2)], et soit $J_1(p, \mu_p)$ la jacobienne de cette courbe relative sur $\mathbb{Z}[1/p]$. Alors nous munissons $J_1(p, \mu_p)$ d'opérateurs de Hecke modifiés T'_ℓ et d'opérateurs diamants modifiés $\langle n\rangle'$ (voir la Définition 2.2.6), afin de prendre en compte l'action des opérateurs usuels sur la composante $\mathbb{Z}[1/p, \zeta_p]$.

Pour chaque $t \in \mathbb{F}_p$ (resp. $t = \infty$), on définit le morphisme $u_t : J(p,p) \to J_1(p, \mu_p)$ induit par le morphisme $X(p,p) \to X_1(p, \mu_p)$ suivant : on envoie le couple $(E, (P, Q))$ sur $(E, tP + Q, \langle P,\, Q\rangle_E)$ (resp. $(E, P, \langle P,\, Q\rangle_E)$), où $\langle P,\, Q\rangle_E$ désigne l'accouplement de Weil sur $E[p]$.

Soit $P(p)$ le produit de $p+1$ copies de $J_1(p, \mu_p)$ indexées par $\mathbb{F}_p \cup \{\infty\}$. On peut construire une action de $\mathrm{GL}_2(\mathbb{F}_p)$ sur $P(p)$ qui commute à l'action de chaque T'_ℓ, et telle que l'action de $\langle n\rangle'$ soit exactement l'action de $nI_2 \in \mathrm{GL}_2(\mathbb{F}_p)$. On appelle $u : J(p,p) \to P(p)$ le produit des u_t pour $t \in \mathbb{F}_p \cup \{\infty\}$. Alors $C(p) := \ker u = \bigcap_{t\in\mathbb{F}_p\cup\{\infty\}} \ker u_t$ est un schéma en groupes propre sur $\mathbb{Z}[1/p]$, et on note $C^0(p)$ le modèle de Néron de la composante connexe de l'unité de $C(p)_{\mathbb{Q}}$, qui est un schéma en groupes lisse et propre sur $\mathbb{Z}[1/p]$.

Théorème 3 *Le morphisme u commute à l'action de $\mathrm{GL}_2(\mathbb{F}_p)$ et des opérateurs de Hecke, au sens que $u \circ T_\ell = T'_\ell \circ u$ pour chaque nombre premier $\ell \neq p$. De plus, il existe un morphisme explicite $R : P(p) \to P(p)$ commutant à l'action des T'_ℓ et de $\mathrm{GL}_2(\mathbb{F}_p)$ tel que la suite de schémas abéliens sur $\mathbb{Z}[1/p]$*

$$0 \to C^0(p) \to J(p,p) \xrightarrow{u} P(p) \xrightarrow{R} P(p),$$

soit un complexe dont les fibres sont exactes à isogénie près. De plus, pour tout corps k de caractéristique distincte de p, les groupes de composantes connexes de $(\ker R)_k$ et de $C(p)_k$ sont d'exposant divisant $2p(p+1)$.

On décrit aussi les différentielles holomorphes sur $X(p,p)_{\mathbb{C}}$ ainsi que l'action des opérateurs de Hecke et de $\mathrm{GL}_2(\mathbb{F}_p)$ dont elles sont munies. Pour le reste de l'introduction, définissons la notation suivante :

Notations pour les représentations de $\mathrm{GL}_2(\mathbb{F}_p)$:

- $\mathcal{D}$ est l'ensemble des caractères (à valeurs complexes) du groupe abélien $\mathbb{F}_p^\times$,
- St est la représentation de Steinberg de $\mathrm{GL}_2(\mathbb{F}_p)$: elle est de dimension p et peut être réalisée sur $\mathbb{Z}$,
- pour chaque $\alpha \in \mathcal{D}$, St_α est la tordue de la représentation St par le caractère $\alpha(\det)$ de $\mathrm{GL}_2(\mathbb{F}_p)$,
- pour tous $\alpha, \beta \in \mathcal{D}$, $\pi(\alpha, \beta)$ désigne la représentation de série principale de $\mathrm{GL}_2(\mathbb{F}_p)$ associée aux deux caractères α et β.

Si V est un $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-module à gauche, on appelle $V^\vee$ le $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-module à *droite* $\mathrm{Hom}(V, \mathbb{C})$.

Notations pour les espaces de formes modulaires :

- $\mathscr{S}$ est l'ensemble des $(f, \mathbf{1})$, où $\mathbf{1} \in \mathcal{D}$ est le caractère trivial et $f \in \mathcal{S}_2(\Gamma_0(p))$ est propre pour les opérateurs de Hecke et normalisée.
- $\mathscr{P}$ est l'ensemble des (f, χ), où $f \in \mathcal{S}_2(\Gamma_1(p))$ est une forme modulaire propre pour les opérateurs de Hecke, normalisée et de caractère $\chi \in \mathcal{D}$ non trivial. La conjugaison complexe agit sur $\mathscr{P}$ sans point fixe en échangeant (f, χ) et $(\overline{f}, \chi^{-1})$, où $\overline{f} \in \mathcal{S}_2(\Gamma_1(p))$ est la forme modulaire dont le q-développement est $\sum_{n\geq 1} \overline{a_n(f)} q^n$.
- $\mathscr{P}'$ est un ensemble de représentants de $\mathscr{P}$ modulo la conjugaison complexe.
- $\mathscr{C}$ désigne l'ensemble des (f, χ), où $f \in \mathcal{S}_2(\Gamma_1(p) \cap \Gamma_0(p^2))$ est propre pour les opérateurs de Hecke, normalisée, de caractère $\chi \in \mathcal{D}$, et telle qu'aucune tordue de f par un caractère dans $\mathcal{D}$ ne soit de niveau p.
- $\mathscr{C}_M$ est l'ensemble des $(f, \mathbf{1}) \in \mathscr{C}$ tels que f ait multiplication complexe (le corps quadratique imaginaire étant alors nécessairement $\mathbb{Q}(\sqrt{-p})$ avec $p \equiv 3 \pmod 4$).

- $\mathscr{C}_1$ est l'ensemble des $(f, \mathbf{1}) \in \mathscr{C} \backslash \mathscr{C}_M$, et $\mathscr{C}_1'$ est un ensemble de représentants pour $\mathscr{C}_1$ modulo la torsion par l'unique caractère quadratique non trivial contenu dans $\mathcal{D}$.
- Si $f \in \mathcal{S}_k(\Gamma_1(N))$ est une forme propre pour les opérateurs de Hecke, primitive et normalisée, si L est un corps de nombres contenant les coefficients de f et λ un idéal maximal de $\mathcal{O}_L$, $V_{f,\lambda}$ est la représentation irréductible continue L_λ-linéaire de dimension 2 de $G_\mathbb{Q}$ telle que, pour chaque nombre premier $q \nmid N$ distinct de la caractéristique résiduelle de λ, le polynôme caractéristique d'un Frobenius arithmétique à q soit $X^2 - a_q(f)X + q^{k-1}\chi(q)$.

Théorème 4 *Il existe un isomorphisme $H^0(X(p,p)_\mathbb{C}, \Omega^1) \simeq \bigoplus_{b \in \mathbb{F}_p^\times} \mathcal{S}_2(\Gamma(p)) \otimes \Delta_{b,1}$ qui commute à l'action des T_ℓ et de $\mathrm{GL}_2(\mathbb{F}_p)$. De plus, comme $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-module à droite muni de l'action des T_ℓ, $H^0(X(p,p)_\mathbb{C}, \Omega^1)$ est isomorphe à la somme directe suivante :*

- *pour chaque $(f, \mathbf{1}) \in \mathscr{S}$ et chaque $\alpha \in \mathcal{D}$, une copie de $\mathrm{St}_\alpha^\vee$,*
- *pour chaque $(f, \chi) \in \mathscr{P}$ modulo la conjugaison complexe, pour chaque $\alpha \in \mathcal{D}$, une copie de $\pi(\alpha, \alpha\chi)^\vee$,*
- *pour chaque $(f, \chi) \in \mathscr{C}$, un copie de $C_f^\vee$, pour une certaine représentation cuspidale irréductible C_f de $\mathrm{GL}_2(\mathbb{F}_p)$ associée à une paire $\{\phi_f, \phi_f^p\}$ de caractères de $\mathbb{F}_{p^2}^\times$.*

Pour chacun des termes ci-dessus, (où l'on pose $\alpha = \mathbf{1}$ dans le troisième cas), pour tout nombre premier $\ell \neq p$ (resp. pour tout $n \in \mathbb{F}_p^\times$), T_ℓ (resp. nI_2) agit par multiplication par $a_\ell(f)\alpha(\ell)$ (resp. $\alpha^2(n)\chi(n)$).

2 Les jacobiennes modulaires tordues (Chapitres 3-4)

2.1 Chapitre 3 : le module de Tate de $J_E^\alpha(p)$

Dans le chapitre 3, on utilise la relation d'Eichler-Shimura et les résultats du Chapitre 2 afin de décrire le module de Tate de la jacobienne de $X(p,p)_\mathbb{Q}$, puis de celle de $X_E^\alpha(p)$, où $E/\mathbb{Q}$ est une courbe elliptique.

Précédemment, Virdol [163, Theorem 1.1] a obtenu une description du module de Tate de tordues de la courbe $X(p,p)_\mathbb{Q}$ par une représentation $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_p)$, ce qui lui permet (également dans *op.cit.*) de démontrer que la fonction L de cette courbe possède dans certains cas un prolongement méromorphe. Voici son théorème.

Théorème A *(Virdol [163, Theorem 1.1]) Soit $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ un morphisme continu de groupes. On a l'égalité suivante de fonctions L*

$$L(s, X(p,p)_\rho) = \prod_\pi L(s, \rho_{\pi,\ell} \otimes (\widetilde{\varphi_\pi} \circ \rho)),$$

où

- *dans le produit, les $\pi = \pi_f \otimes \pi_\infty$ sont des représentations cuspidales automorphes de $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ de poids 2, où π_∞ est cohomologique et π_f une représentation de $\mathrm{GL}_2(\mathbb{A}_{f,\mathbb{Q}})$ telle que $\pi_f^{\hat{\Gamma}(p)} \neq 0$, et $\hat{\Gamma}(p) \leq \mathrm{GL}_2(\mathbb{A}_{f,\mathbb{Q}})$ désigne le sous-groupe $[I_2 + p\mathcal{M}_2(\mathbb{Z}_p)] \times \prod_{\ell \neq p} \mathrm{GL}_2(\mathbb{Z}_\ell)$,*
- *$\rho_{\pi,\ell}$ est la représentation galoisienne ℓ-adique associée à π,*
- *$\widetilde{\varphi_\pi}$ désigne la représentation du groupe $\mathrm{GL}_2(\mathbb{F}_p)$ associée à $\pi_f^{\hat{\Gamma}(p)}$.*

Ce chapitre se distingue des résultats de Virdol sous plusieurs aspects. D'abord, les énoncés de Virdol sont exprimés dans un langage adélique de représentations automorphes, là où nous gardons pour l'instant un point de vue classique. Ceci permet en particulier de rendre explicites les représentations $\widetilde{\varphi_\pi} \circ \rho$ en termes de formes modulaires.

Deuxièmement, lorsque la représentation ρ du Théorème A provient de la p-torsion d'une courbe elliptique $E/\mathbb{Q}$ (comme dans le cas du Théorème 2), Virdol calcule en réalité la fonction

L (ou plutôt le module de Tate) du produit $\prod_{\alpha\in\mathbb{F}_p^\times} J_E^\alpha(p)$, alors que nous décrivons le module de Tate de chaque $X_E^\alpha(p)$ séparément.

Dans le reste de ce résumé, $p \geq 7$ est un nombre premier et $E/\mathbb{Q}$ est une courbe elliptique. Fixons une base (P, Q) du $\mathbb{F}_p$-espace vectoriel $E[p](\overline{\mathbb{Q}})$ et soit $\xi = \langle P, Q\rangle_{E[p]} \in \mu_p^\times(\overline{\mathbb{Q}})$ (où $\mu_p^\times(\overline{\mathbb{Q}})$ est l'ensemble des racines p-ièmes primitives de l'unité dans $\overline{\mathbb{Q}}$). Soit $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_p)$ le morphisme continu de groupes tel que

$$\forall\sigma \in G_\mathbb{Q},\ \rho(\sigma)\begin{pmatrix}\sigma(P)\\ \sigma(Q)\end{pmatrix} = \begin{pmatrix}P\\ Q\end{pmatrix},$$

de sorte que $\rho'(\sigma) = (\rho(\sigma)^T)^{-1}$ soit la matrice de σ dans la base (P, Q). En particulier, le caractère $\det\rho : G_\mathbb{Q} \to \mathbb{F}_p^\times$ est l'inverse du caractère cyclotomique, et ρ est l'inverse de l'anti-morphisme de groupes appelé ρ dans le Théorème 2.

Soit $F \subset \mathbb{C}$ un corps de nombres galoisien sur $\mathbb{Q}$ et dont l'anneau des entiers $\mathcal{O}_F$ contient les entiers algébriques suivants :

- les racines $p(p-1)^2(p+1)$-ièmes de l'unité,
- les coefficients de Fourier de f, pour tout $(f, \chi) \in \mathscr{S} \cup \mathscr{P} \cup \mathscr{C}$,
- pour chaque $(f, \mathbf{1}) \in \mathscr{C}_M$, pour chaque nombre premier ℓ décomposé dans $\mathbb{Q}(\sqrt{-p})$, les racines du polynôme de Hecke $X^2 - a_\ell(f)X + \ell$ of f at ℓ.

Pour chaque $(f, \mathbf{1}) \in \mathscr{C}_M$, on choisit un système compatible de caractères $(\psi_{f,\lambda})_\lambda$ (où λ parcourt les idéaux maximaux de $\mathcal{O}_F$), où $\psi_{f,\lambda} : G_{\mathbb{Q}(\sqrt{-p})} \to F_\lambda^\times$ est associé à f par la théorie des formes modulaires à multiplication complexe.

Lorsque $p \equiv 3 \pmod 4$, la restriction à $\mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p)$ de la représentation cuspidale V_4 de $\mathrm{GL}_2(\mathbb{F}_p)$ associée à la paire des deux caractères d'ordre 4 de $\mathbb{F}_{p^2}^\times$ est la somme de deux représentations irréductibles C^+ et C^-. Elles sont duales l'une de l'autre et échangées après conjugaison par $\mathrm{GL}_2(\mathbb{F}_p)/\mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p)$.

Théorème 5 *Soient ℓ un nombre premier et λ un idéal premier de $\mathcal{O}_F$ de caractéristique résiduelle ℓ. Alors, pour tout $\alpha \in \mathbb{F}_p^\times$, $\mathcal{T}_\ell J_E^\alpha(p) \otimes_{\mathbb{Z}_\ell} F_\lambda$ se décompose comme la somme directe des sous-$F_\lambda[G_\mathbb{Q}]$-modules suivants :*

- *Pour chaque $(f, \mathbf{1}) \in \mathscr{S}$, une copie de $V_{f,\lambda} \otimes (\mathrm{St} \circ \rho)$,*
- *Pour chaque $(f, \chi) \in \mathscr{P}'$, une copie de $V_{f,\lambda} \otimes (\pi(\mathbf{1}, \chi) \circ \rho)$,*
- *Pour chaque $(f, \mathbf{1}) \in \mathscr{C}_1'$, une copie de $V_{f,\lambda} \otimes (C_f \circ \rho)$, où C_f est la représentation cuspidale de $\mathrm{GL}_2(\mathbb{F}_p)$ associée à $(f, \mathbf{1})$ par le Théorème 4,*
- *Pour chaque $(f, \mathbf{1}) \in \mathscr{C}_M$, une copie de $V_{f,\lambda,E}^\epsilon := \mathrm{Ind}_{\mathbb{Q}(\sqrt{-p})}^\mathbb{Q} \psi_{f,\lambda} \otimes C^\epsilon(\rho_{|G_{\mathbb{Q}(\sqrt{-p})}})$, où $\epsilon \in \{\pm\}$ ne dépend que de $\xi^{\alpha\mathbb{F}_p^{\times 2}}$.*

Les termes de cette décomposition sont stables par les opérateurs de Hecke T_ℓ tels que $\ell \equiv 1 \pmod p$, et un tel opérateur T_ℓ agit sur le terme associé à (f, χ) par multiplication par $a_\ell(f)$.

Remarquons que la représentation galoisienne apparaissant dans le Théorème 5 ne dépend pas du choix de représentant dans $\mathscr{P}'$ ou $\mathscr{C}_1'$.

Lorsque $(f, \chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1'$, soit $R_{f,E}$ la représentation d'Artin suivante :

- $\mathrm{St} \circ \rho$ pour $(f, \chi) \in \mathscr{S}$,
- $\pi(\mathbf{1}, \chi) \circ \rho$ pour $(f, \chi) \in \mathscr{P}'$,
- $C_f \circ \rho$ pour $(f, \chi) \in \mathscr{C}_1'$.

2.2 Chapitre 4 : calcul galoisien des signes d'équation fonctionnelle pour $(V_{f,\lambda} \otimes R_{f,E})_\lambda$ et $(V^\epsilon_{f,\lambda,E})_\lambda$

Dans le chapitre 4, nous discutons les propriétés de les fonctions L des facteurs du module de Tate de $J^\alpha_E(p)$ décrits dans le Théorème 5. Après des rappels sur les représentations automorphes et certains aspects de la correspondance de Langlands, nous calculons les signes d'équation fonctionnelle galoisiens (c'est-à-dire les produits des facteurs ε associés aux représentations galoisiennes locales définis par Deligne et Langlands et décrits par exemple dans [160, §3]) des représentations galoisiennes $V_{f,\lambda} \otimes R_{f,E}$ et $V^\epsilon_{f,\lambda,E}$, où λ parcourt les idéaux maximaux de $\mathcal{O}_F$.

Même si les résultats du chapitre 4 sont plus généraux, nous donnons ici le résultat lorsque $E/\mathbb{Q}$ a bonne réduction en p. Ce signe dépend du comportement de la représentation $\rho_{|G_{\mathbb{Q}_p}}$, que nous divisons en trois possibilités.

Définition *Soit $\rho_p : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\mathbb{F}_p)$ une représentation continue telle que $\det \rho_p$ soit l'inverse du caractère cyclotomique modulo p. On dit que ρ_p est*

- sauvage *si l'inertie sauvage agit non trivialement,*
- diagonale *si ρ_p est la somme directe de deux caractères de $G_{\mathbb{Q}_p}$ à valeurs dans $\mathbb{F}_p^\times$,*
- Cartan *si l'image de l'inertie est contenue dans un sous-groupe de Cartan non déployé de $\mathrm{GL}_2(\mathbb{F}_p)$.*

La représentation ρ_p est dans exactement une des trois situations ci-dessus.

Théorème 6 *Supposons que $E/\mathbb{Q}$ ait bonne réduction en p.*

Soit U le produit, sur chaque nombre premier ℓ inerte dans $\mathbb{Q}(\sqrt{-p})$, des $(-1)^{m_\ell}$, où $m_\ell \in \mathbb{Z}$ est la moitié de la valuation ℓ-adique du conducteur de la représentation d'Artin $V_4 \circ \rho$. Alors il existe un signe ε_p dépendant seulement du schéma en groupes fini plat $E[p]_{\mathbb{Z}_p}$, de $\xi^{\mathbb{F}_p^{\times 2}}$ et du choix de $\psi_{f,\lambda}$ tel que le signe galoisien de l'équation fonctionnelle pour les facteurs apparaissant dans la décomposition de $\mathcal{T}_\ell J^\alpha_E(p) \otimes F_\lambda$ décrite dans le Théorème 5 soit donné dans la table2.

	Type of $\rho_{\|G_{\mathbb{Q}_p}}$		
	Diagonale	Sauvage	Cartan
$V_{f,\lambda} \otimes R_{f,E}, (f,\mathbf{1}) \in \mathscr{S}$	$(-1)^{(p+1)/2}$	$(-1)^{(p-1)/2} a_p(f)$	$(-1)^{(p+1)/2}$
$V_{f,\lambda} \otimes R_{f,E}, (f,\chi) \in \mathscr{P}'$	$(-1)^{(p-1)/2}$		
$V_{f,\lambda} \otimes R_{f,E}, (f,\mathbf{1}) \in \mathscr{C}'_1$	$(-1)^{(p+1)/2}$	$(-1)^{(p-1)/2}$	$(-1)^{(p+1)/2}$
$V^\epsilon_{f,\lambda,E}, (f,\mathbf{1}) \in \mathscr{C}_M$	$(-1)^{(p+1)/4} U$	$(-1)^{\frac{p+1}{4}} U \epsilon \varepsilon_p$	$(-1)^{\frac{p+1}{4}} U$

TABLE 2 : Signes galoisiens d'équation fonctionnelle pour les facteurs de la décomposition de $J^\alpha_E(p)$

2.3 Chapitre 4 : automorphie de $(V_{f,\lambda} \otimes R_{f,E})_\lambda$ and $(V^\epsilon_{f,\lambda,E})_\lambda$

Nous pouvons démontrer grâce à la méthode de Rankin-Selberg que

Théorème 7 *Soit $(f,\mathbf{1}) \in \mathscr{S}$. (resp. $(f,\chi) \in \mathscr{P}'$, resp. $(f,\mathbf{1}) \in \mathscr{C}'_1$) Si la représentation d'Artin est automorphe, alors la fonction L de la représentation galoisienne autoduale (à tordue à la Tate près) $V_{f,\lambda} \otimes R_{f,E}$ possède un prolongement holomorphe et vérifie une équation fonctionnelle dont le signe est donné (lorsque E a bonne réduction en p) par la table 2.*

Pour tout $(f,\mathbf{1}) \in \mathscr{C}_M$, la fonction L de la représentation galoisienne autoduale (à tordue à la Tate près) $V^\epsilon_{f,\lambda,E}$ possède un prolongement méromorphe et vérifie une équation fonctionnelle dont le signe est donné dans la table 2 lorsque $E/\mathbb{Q}$ a bonne réduction en p.

Comme dans le théorème 6, l'hypothèse de bonne réduction en p pour $E/\mathbb{Q}$ est faite pour simplifier l'introduction, et n'est pas utilisée dans le chapitre 4.

Lorsque ρ est surjective, les représentations $R_{f,E}$ sont d'image finie, irréductibles de grande dimension, et leur image n'est pas résoluble. Ceci ne change pas lorsque l'on restreint ρ au groupe de Galois d'un corps de nombres totalement réel. Par conséquent, il semble que les techniques actuelles ne permettent pas de montrer que les représentations $R_{f,E}$ sont automorphes.

Une autre possibilité pour comprendre la représentation $V_{f,\lambda} \otimes R_{f,E}$ pourrait être de la réduire modulo un nombre premier. Nous démontrons, grâce aux deux résultats de fonctorialité de Langlands suivants,

- pour les puissances symétriques pour le groupe GL(2) sur un corps totalement réel démontréee par Newton et Thorne [127][18],
- pour les produits tensoriels de la forme $\mathrm{GL}(2) \times \mathrm{GL}(n)$, montré sous certaines hypothèses dans une prépublication d'Arias-de-Reyna et Dieulefait [3],

que $V_{f,\lambda} \otimes R_{f,E}$ sont automorphes modulo p en un sens que nous précisons.

Pour référence, nous donnons ici une traduction en français de l'énoncé du résultat d'Arias-de-Reyna et Dieulefait.

Théorème B *(Arias-de-Reyna – Dieulefait [3, Theorem 1.1]) Soit $f \in \mathcal{S}_k(\Gamma(1))$ une forme modulaire parabolique propre pour les opérateurs de Hecke et soit $\rho_\bullet(f)$ le système compatible de représentations associé. Soit $n > 0$ un entier et π une représentation automorphe régulière algébrique cuspidale polarisée de $GL_n(\mathbb{A}_\mathbb{Q})$ de niveau premier à 3. Soit $r_\bullet(\pi)$ le système compatible de représentations galoisiennes associé à π. Supposons que $\rho_\bullet(f) \otimes r_\bullet(\pi)$ soit un système compatible régulier et irréductible. Alors $\rho_\bullet(f) \otimes r_\bullet(\pi)$ est automorphe au sens suivant : il existe une représentation automorphe régulière algébrique cuspidale polarisée $f \otimes \pi$ de $GL_{2n}(\mathbb{A}_\mathbb{Q})$ tel que le système compatible de représentations galoisiennes associé à $f \otimes \pi$ soit isomorphe à $\rho_\bullet(f) \otimes r_\bullet(\pi)$.*

Théorème 8 *Supposons que ρ soit surjective et provienne d'une courbe elliptique $E/\mathbb{Q}$ ayant bonne réduction en 3. Supposons de plus que le Théorème B soit vrai. Il existe un corps de nombres $F' \supset F$ et un idéal premier $\mathfrak{p}$ de F' de caractéristique résiduelle p telle que, pour tout $(f, \chi) \in \mathscr{S} \cup \mathscr{P}_1' \cup \mathscr{C}_1'$, la semi-simplification de la réduction modulo $\mathfrak{p}$ de $V_{f,\mathfrak{p}} \otimes R_{f,E}$ soit la somme directe des semi-simplifications de réductions modulo $\mathfrak{p}$ de représentations galoisiennes à coefficients dans $(F')_\mathfrak{p}$ provenant de systèmes compatibles associés à des représentations automorphes régulières algébriques cuspidales et polarisées.*

Bien que ce résultat soit intéressant, il ne semble pas qu'il ait d'application claire à la détermination des points rationnels de $X_E^\alpha(p)$.

3 Cas où l'image de ρ est contenue dans le normalisateur d'un sous-groupe de Cartan non déployé (Chapitre 5)

Dans le chapitre 5, nous supposons que $\rho(G_\mathbb{Q})$ est contenue dans le normalisateur N d'un sous-groupe de Cartan non déployé C. Soit $K/\mathbb{Q}$ le corps quadratique imaginaire correspondant au caractère $G_\mathbb{Q} \to N \to N/C \simeq \{\pm 1\}$. Pour simplifier, nous supposons dans cette introduction que $p \geq 11$. Dans ce cas, la Proposition 5.4.2 assure que K est inerte en p.

3.1 Décomposition du module de Tate et équation fonctionnelle

Dans une telle situation, la décomposition obtenue dans le théorème 5 n'est pas optimale et peut être affinée. Fixons une fois pour toutes un isomorphisme de groupes ι entre C et $\mathbb{F}_{p^2}^\times$ préservant la norme et la trace. L'isomorphisme ι n'est pas canonique, mais la paire $\{\iota, \iota^p\}$ l'est : par conséquent, ι permet d'identifier canoniquement les paires $\{\psi, \psi^p\}$ de caractères de C et les paires $\{\phi, \phi^p\}$ de caractères de $\mathbb{F}_{p^2}^\times$.

[18] Le cas du corps de base $\mathbb{Q}$, qui suffit à nos besoins, est traité dans les articles publiés [125, 126].

Théorème 9 *Soit λ un idéal premier de $\mathcal{O}_F$ de caractéristique résiduelle ℓ. Pour chaque $\alpha \in \mathbb{F}_p^\times$, $\mathcal{T}_\ell J_E^\alpha(p) \otimes_{\mathbb{Z}_\ell} F_\lambda$ est la somme directe des sous-$G_\mathbb{Q}$-modules suivants qui sont stables par les opérateurs de Hecke :*

- *pour chaque $(f,\chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1' \cup \mathscr{C}_M$, une copie de $V_{f,\lambda} \otimes \theta$, où θ est un caractère de $\mathrm{Gal}(K(\mu_p)/\mathbb{Q})$ ne dépendant pas de ρ ou λ ; on somme sur deux caractères θ possibles si $(f,\chi) \in \mathscr{P}' \cup \mathscr{C}_1'$ et un seul sinon,*
- *pour chaque $(f,\chi) \in \mathscr{S} \cup \mathscr{P}'$, pour chaque paire $\{\psi,\psi^p\}$ de caractères distincts $C \to F^\times$ telle que $\psi(tI_2) = \chi(t)$ pour tout $t \in \mathbb{F}_p^\times$, une copie de $V_{f,\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi\right) \circ \rho\right]$,*
- *pour chaque $(f,\mathbf{1}) \in \mathscr{C}_1'$ (resp. $(f,\mathbf{1}) \in \mathscr{C}_M$), pour chaque paire $\{\psi,\psi^p\} \neq \{\phi_f,\phi_f^p\}$ de caractères distincts $C/\mathbb{F}_p^\times I_2 \to F^\times$ (resp. modulo également la relation d'équivalence définie par : $\{\psi,\psi^p\} \sim \{\theta,\theta^p\}$ si et seulement si l'un des caractères $\psi\theta^{-1}$ et $\psi^p\theta^{-1}$ est d'ordre au plus deux), une copie de $V_{f,\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi\right) \circ \rho\right]$.*

L'opérateur de Hecke T_ℓ (pour $\ell \equiv 1 \pmod p$ premier) agit sur un facteur de l'une des formes ci-dessus par multiplication par $a_\ell(f)$.

Lorsque l'on les compare aux facteurs apparaissant dans la décomposition décrite dans le théorème 5, les facteurs décrits ci-dessus sont bien plus simples, et leurs propriétés en tant que représentations galoisiennes bien mieux comprises. Dans le reste du chapitre 5, on applique la stratégie de Mazur dans le but de déterminer les points rationnels de $X_E^\alpha(p)$. Tout d'abord, on montre que les fonctions L des facteurs apparaissant dans le théorème 9 possèdent des prolongements entiers, vérifient des équations fonctionnelles dont on calcule le signe.

Théorème 10 *Chacune des représentations décrites dans le théorème 9 est autoduale (à une torsion à la Tate près), et sa fonction L possède un prolongement analytique et satisfait une équation fonctionnelle de signe -1, sauf dans les cas suivants :*

- *$V_{f,\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi\right) \circ \rho\right]$ pour $(f,\mathbf{1}) \in \mathscr{S}$, lorsque $\left(\mathrm{Ind}_C^N \psi\right) \circ \rho$ est non ramifiée en p,*
- *$V_{f,\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi\right) \circ \rho\right]$ pour $(f,\mathbf{1}) \in \mathscr{C}_1' \cup \mathscr{C}_M$ si la condition suivante est vérifiée. Soit $M/\mathbb{Q}_p$ l'unique extension quadratique non ramifiée et $\mathfrak{a} : \mathrm{Gal}(\overline{\mathbb{Q}_p}/M) \to \widehat{M^\times}$ l'isomorphisme du corps de classe (normalisé de sorte à envoyer un Frobenius arithmétique sur une uniformisante) ; en particulier, $\mathfrak{a}$ possède un sous-quotient $\overline{\mathfrak{a}}$ envoyant le groupe d'inertie $I_p \lhd \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ dans $\mathcal{O}_M^\times/(1+p\mathcal{O}_M) \simeq \mathbb{F}_{p^2}^\times$. Le signe de l'équation fonctionnelle est 1 si et seulement si les paires $\{\phi_f \circ \overline{\mathfrak{a}}, \phi_f^p \circ \overline{\mathfrak{a}}\}$ et $\{\psi \circ \rho_{|I_p}, \psi^p \circ \rho_{|I_p}\}$ de caractères $I_p \to F^\times$ sont égales.*

Dans ces deux cas, E ainsi que ses tordues quadratiques ont mauvaise réduction en p. Dans le premier, on a de plus $\rho(I_p) = 3C$, $p \equiv 2,5 \pmod 9$ et ψ est d'ordre exactement 3.

3.2 La conjecture de Bloch-Kato en rang zéro pour les facteurs de $J_E^\alpha(p)$

Le résultat suivant de ce chapitre est la preuve de la conjecture de Bloch-Kato en rang zéro pour la plupart des facteurs quadri-dimensionnels du module de Tate de $J_E^\alpha(p)$. Pour ce faire, on utilise le système d'Euler des éléments de Beilinson-Flach construit par Kings, Loeffler et Zerbes [92]. Pour pouvoir utiliser les résultats de [92], il est nécessaire de montrer que ces représentations satisfont les *hypothèses de grande image* requises, ce que nous faisons en étendant les résultats de [108, Section 4.4]. Ceci est l'un des points principaux du chaputre 6 sur lequel nous reviendrons.

Nous replaçant dans le cadre du théorème 9, soit $(f,\chi),(f',\chi') \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1' \cup \mathscr{C}_M$, et soient $\{\psi,\psi^p\},\{\psi',(\psi')^p\}$ deux paires de caractères distincts de C à valeurs dans $F^\times$. On dit que les représentations galoisiennes

$$V_{f,\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi\right) \circ \rho\right],\ V_{f',\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi'\right) \circ \rho\right]$$

sont dans la même orbite sous l'action de Galois s'il existe $\sigma \in G_{\mathbb{Q}}$ tel que pour tout nombre premier q sauf un nombre fini, l'on a

$$\mathrm{Tr}\left(\mathrm{Frob}_q \mid V_{f',\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi'\right) \circ \rho\right]\right) = \sigma\left[\mathrm{Tr}\left(\mathrm{Frob}_q \mid V_{f,\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi\right) \circ \rho\right]\right)\right].$$

Notons que cette notion ne dépend pas du choix de λ.

Théorème 11 *Soit V l'un des facteurs quadridimensionnels apparaissant dans le théorème 9 et associé au couple $((f,\chi),\{\psi,\psi^p\})$. Pour chaque $\alpha \in \mathbb{F}_p^\times$, $J_E^\alpha(p)$ possède un quotient A stable par les opérateurs de Hecke tel que $\mathcal{T}_\ell A \otimes_{\mathbb{Z}_\ell} F_\lambda$ s'identifie à la somme directe des facteurs apparaissant dans le théorème 9 qui sont dans la même orbite que V sous l'action de Galois. Supposons de plus que f n'ait pas de multiplication complexe et que $L(V,1) \neq 0$ (ainsi $(f,\chi) \in \mathscr{S} \cup \mathscr{C}_1'$). Alors le groupe $A(\mathbb{Q})$ est fini.*

Pour construire le quotient A, on utilise le fait que le choix de base (P,Q) pour $E[p]$ définit un isomorphisme $\coprod_{\alpha\in\mathbb{F}_p^\times} X_E^\alpha(p)_{\overline{\mathbb{Q}}} \cong X(p,p)_{\overline{\mathbb{Q}}}$, ce qui permet de munir $\coprod_{\alpha\in\mathbb{F}_p^\times} X_E^\alpha(p)_{\overline{\mathbb{Q}}}$ d'une action de $\mathrm{GL}_2(\mathbb{F}_p)$.

3.3 Le théorème d'immersion formelle

Supposons maintenant que la representation V du théorème 11 relève du premier cas du théorème 10, ce qui implique notamment que $p \equiv 2, 5 \pmod 9$.

Soient $c \in X_E^\alpha(p)(\overline{\mathbb{Q}})$ une pointe et $q \equiv 1 \pmod p$ un nombre premier. Le morphisme $x \longmapsto (T_q - q - 1)(x - c) : X_E^\alpha(p)_{\overline{\mathbb{Q}}} \to J_E^\alpha(p)_{\overline{\mathbb{Q}}}$ est en fait défini sur $\mathbb{Q}$ et ne dépend pas du choix de c, parce que $T_q - q - 1$ annule les diviseurs supportés sur le sous-schéma cuspidal. Considérons sa composition f avec la projection $J_E^\alpha(p) \to A$, où A est le quotient défini par le théorème 11. Grâce à notre description des différentielles sur $\mathbb{C}$ de la courbe obtenue dans le chapitre 2, nous pouvons appliquer un argument analogue à l'immersion formelle de Mazur (plutôt formulé dans le langage de la méthode de Chabauty-Coleman décrite dans [115]) au morphisme $f : X_E^\alpha(p) \to A$.

Définition *Pour chaque racine cubique de l'unité $j \in \mathbb{F}_{p^2}^\times$, soit*

$$u_j = \sum_{\substack{b\in\mathbb{F}_p \\ 1+b\sqrt{-3}\in\mathbb{F}_{p^2}^{\times 3} j}} e^{\frac{2i\pi b}{p}}.$$

Nous disons qu'un nombre premier ℓ est exceptionnel *pour p si $\ell \equiv \pm 1 \pmod p$ et $\mathbb{Z}[e^{2i\pi/p}]$ possède un idéal premier λ de caractéristique résiduelle ℓ contenant chaque u_j.*

Des calculs avec Magma [16] montrent que lorsque $p \leq 1500$, les trois u_j engendrent l'idéal unité de $\mathbb{Z}[e^{\frac{2i\pi}{p}}]$. Nous sommes donc tentés de conjecturer qu'il n'y a pas de nombres premiers exceptionnels quel que soit p.

Théorème 12 *Supposons que $\rho : G_{\mathbb{Q}} \to N$ soit surjective et soit N_ρ son conducteur d'Artin. Soit $\psi : C \to F^\times$ un caractère d'ordre 3 et supposons qu'il existe $(f,\mathbf{1}) \in \mathscr{S}$ tel que la valeur centrale de la fonction L de la représentation $V_{f,\lambda} \otimes \left[\left(\mathrm{Ind}_C^N \psi\right) \circ \rho\right]$ soit non nulle : en particulier, l'image par ρ d'un sous-groupe d'inertie en p est le sous-groupe d'indice 3 de C.*

Soit $E'/\mathbb{Q}$ une courbe elliptique telle que les $G_{\mathbb{Q}}$-modules $E[p](\overline{\mathbb{Q}})$ et $E'[p](\overline{\mathbb{Q}})$ soient isomorphes. Alors E' a pour conducteur $p^2 N_\rho L$, où L est un produit de nombres premiers exceptionnels pour p deux à deux distincts et ne divisant pas pN_ρ.

Notons que les résultats effectifs connus sur le théorème d'image ouverte de Serre (par exemple [168, Theorems 1.5, 1.10]), ne permettent pas de montrer à partir de là qu'une courbe E' comme dans le théorème ci-dessus non CM ne pourrait exister. Ces résultats ne semblent pas non plus suffisants pour montrer que E et E' sont isogènes, même à supposer qu'elles sont toutes deux de conducteur $p^2 N_\rho$.

3.4 Applications aux congruences à la courbe elliptique CM d'équation $y^2 = x^3 - p$

Dans [95], Kraus calcule le poids de Serre de la p-torsion d'une courbe elliptique à réduction additive. Lorsque $p \equiv 5 \pmod 9$ et E est la courbe elliptique E_p d'équation de Weierstrass $y^2 = x^3 - p$, on peut vérifier que :

- $\rho(G_{\mathbb{Q}}) = N$,
- l'image par ρ d'un sous-groupe d'inertie en p est le sous-groupe $3C$,
- $\left(\mathrm{Ind}_C^N \psi\right) \circ \rho$ est associée à l'unique forme modulaire primitive $g \in \mathcal{S}_1(\Gamma_1(108))$ à multiplication complexe par $\mathbb{Q}(\sqrt{-3})$ et dont les coefficients de Fourier sont rationnels.

Lorsque p n'est pas trop grand, on peut vérifier numériquement grâce à Magma [16] qu'il n'y a pas de nombres premiers exceptionnels pour p, et avec PARI/GP [161] que, pour au moins un $(f, \mathbf{1}) \in \mathscr{S}$, la valeur centrale de la fonction L de Rankin-Selberg $L(f \times g, 1)$ apparaissant dans le théorème 12 ne s'annule pas. Cremona and Freitas ont montré [33, Theorem 1.3] que deux courbes elliptiques dont les conducteurs sont inférieurs à 500000 et dont les $G_{\mathbb{Q}}$-modules de q-torsion (sur $\overline{\mathbb{Q}}$) sont isomorphes sont nécessairement isogènes lorsque $q \geq 19$. De ces considérations, l'on peut déduire :

Corollaire 1 *Soit $p = 23$ et soit E' une courbe elliptique telle que $E'[p](\overline{\mathbb{Q}})$ et $E_p[p](\overline{\mathbb{Q}})$ sont isomorphes comme $G_{\mathbb{Q}}$-modules. Alors E' et E_p sont isogènes.*

En général, on s'attend à ce qu'il existe $(f, \mathbf{1}) \in \mathscr{S}$ tel que $L(f \times g, 1) \neq 0$, mais cela semble difficile à montrer en toute généralité. Le résultat suivant de Michel, démontré par des techniques de théorie analytique des nombres, montre que tel est le cas lorsque p est assez grand.

Théorème C *(Michel, [157, Appendix, Theorem 0.1]) Soit $g \in \mathcal{S}_1(\Gamma_1(N))$ une forme primitive normalisée et propre pour les opérateurs de Hecke de caractère χ. Il existe une constante C_g vérifiant la propriété suivante : pour tout nombre premier $p > C_g$, si, pour tout $f \in \mathcal{S}_2(\Gamma_0(p))$, l'on a $L(f \times g, 1) = 0$, alors g est à coefficients réels et $\chi(p) = 1$.*

Théorème 13 *Il existe une constante $p_0 \geq 11$ vérifiant la propriété suivante. Soit $p \geq p_0$ un nombre premier congru à 5 modulo 9 et E la courbe elliptique à multiplication complexe par $\mathbb{Q}(\sqrt{-3})$ donnée par l'équation de Weierstrass minimale $y^2 = x^3 - p$ (de conducteur $108mp^2$, où $m = 1$ si $p \equiv 3 \pmod 4$ et $m = 4$ si $p \equiv 1 \pmod 4$). Alors, pour toute courbe elliptique $E'/\mathbb{Q}$ telle que $E'[p](\overline{\mathbb{Q}})$ et $E[p](\overline{\mathbb{Q}})$ soient isomorphes comme $G_{\mathbb{Q}}$-modules, le conducteur de E' est $108mp^2L$, où L est un produit de nombres premiers exceptionnels pour p, deux à deux distincts. En particulier, s'il n'y a pas de nombres premiers exceptionnels pour p, E' est de conducteur $108mp^2$ et $j(E') \in \mathbb{Z}$.*

4 Résultats de grande image pour le produit tensoriel de deux formes modulaires (Chapitre 6)

Le chapitre 6 reproduit presque exactement la pré-publication [155] par l'auteur de cette thèse. Le projet provient de la tentative de l'auteur d'appliquer la théorie des systèmes d'Euler dans la preuve du théorème 11.

Soit $\mathcal{O}_K$ l'anneau de valuation d'une extension finie $K/\mathbb{Q}_p$ et soit T un $\mathcal{O}_K$-module libre de rang fini munie d'une action continue et $\mathcal{O}_K$-lineaire de $G_{\mathbb{Q}}$. On peut voir un système d'Euler pour T comme une collection de classes de cohomologie $c_n \in H^1(\mathbb{Q}(\mu_n), T)$ pour certains entiers $n \geq 1$ (comprenant notamment $n = 1$) satisfaisant certaines compatibilités vis-à-vis de la corestriction. La théorie des systèmes d'Euler, telle qu'elle est décrite dans les références classiques [137, 114], permet de contrôler la taille des groupes de Selmer du $G_{\mathbb{Q}}$-module $\mathrm{Hom}_{\mathcal{O}_K}(T, K/\mathcal{O}_K(1))$ lorsque l'on dispose d'un système d'Euler $(c_n)_n$ pour T tel que $c_1 \neq 0$. Néanmoins, pour pouvoir appliquer cette théorie, l'image de $G_{\mathbb{Q}}$ dans $\mathrm{Aut}(T)$ doit vérifier certaines hypothèses, souvent des variantes

ou renforcements de la condition suivante, que nous appelons *condition d'image adaptée* : il existe $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$ tel que $T/(\sigma-1)T \otimes_{\mathcal{O}_K} K$ soit une droite sur K.

Dans [92], Kings, Loeffler et Zerbes construisent un système d'Euler pour pour certaines des représentations apparaissant dans le théorème 9, et en déduisent les bornes sur la taille du groupe de Selmer utilisées dans la preuve du théorème 11 en supposant que la condition d'image adaptée est vérifiée. Dans [108, Section 4.4], Loeffler montre que cette condition est en fait souvent vérifiée :

Théorème D *(Loeffler [108]) Soient $f \in \mathcal{S}_k(\Gamma_1(N_f)), g \in \mathcal{S}_1(\Gamma_1(N_g))$ deux formes primitives normalisées et propres pour les opérateurs de Hecke de caractères respectifs $\varepsilon_f, \varepsilon_g$ telles que $k > 1$ et f ne soit pas à multiplication complexe. Soit L un corps de nombres contenant les coefficients de f et g, et d'anneau des entiers $\mathcal{O}_L$.*

- *S'il existe un idéal maximal λ de $\mathcal{O}_L$ tel que $V_{f,\lambda} \otimes_{L_\lambda} V_{g,\lambda}$ possède une image adaptée, alors $\varepsilon_f\varepsilon_g \neq 1$.*
- *Supposons que $\varepsilon_f\varepsilon_g \neq 1$ et que N_f et N_g soient premiers entre eux. Alors l'ensemble des idéaux maximaux λ de $\mathcal{O}_L$ tels que $V_{f,\lambda} \otimes V_{g,\lambda}$ n'ait pas d'image adaptée est fini.*

Dans le même article, l'auteur pose la question suivante.

Question 1 *(Loeffler, [108, Remark 4.4.2]) Reprenons les notations du théorème M et supposons que $\varepsilon_f\varepsilon_g \neq 1$. Est-il vrai que, pour tout idéal maximal λ de $\mathcal{O}_L$ sauf éventuellement un nombre fini, $V_{f,\lambda} \otimes V_{g,\lambda}$ ait une image adaptée ?*

Le théorème D ne permet pas à lui seul d'utiliser les résultats sur les systèmes d'Euler requis pour la preuve de 11. Dans la deuxième situation du théorème 10, les conducteurs des deux formes modulaires sont divisibles par p^2, et le théorème D ne peut donc pas montrer que la condition d'image adaptée est vérifiée pour tout idéal premier sauf un nombre fini. C'est là la motivation pour notre étude de la question 1. Nous donnons en premier lieu des conditions suffisantes plus générales sous lesquelles on peut répondre à la question 1 par l'affirmative.

Théorème 14 *Gardons les notations du théorème D et supposons que $\varepsilon_f\varepsilon_g \neq 1$. On peut répondre par l'affirmative à la question 1 si l'une des conditions suivantes est vérifiée :*

- *Pour tout caractère de Dirichlet (primitif) χ de niveau C tel que $f \otimes \chi$ soit conjuguée à f par l'action de $G_\mathbb{Q}$, C et N_g sont premiers entre eux.*
- *Tout caractère de Dirichlet (primitif) χ tel que $f \otimes \chi$ soit conjugué à f par l'action de $G_\mathbb{Q}$ est pair.*
- *$\varepsilon_f^2 = \varepsilon_g^2 = 1$ et $f \otimes \varepsilon_g$ n'est pas conjugué à f par l'action de $G_\mathbb{Q}$.*
- *Le sous-groupe fini $\varepsilon_g\left(\bigcap_\chi \ker\chi\right)$ de $\mathbb{C}^\times$ contient -1 mais pas $\pm i$, où χ parcourt les caractères de Dirichlet (primitifs) tels que $f \otimes \chi$ soit conjuguée à f sous l'action de $G_\mathbb{Q}$.*

Ce résultat permet d'améliorer la conjecture de Birch and Swinnerton-Dyer démontrée dans [92, Theorem 11.7.4] pour les tordues de courbes elliptiques par les représentations d'Artin bidimensionnelles, impaires et irréductibles : nous montrons dans le corollaire 6.3.11 que, dans l'énoncé de *loc.cit.*, nous n'avons plus besoin de supposer que la courbe elliptique et la représentation d'Artin aient des conducteurs premiers.

Nous montrons ensuite que la réponse générale à la question 1 est « non », et décrivons des familles infinies de contre-exemples grâce au résultat suivant.

Théorème 15 *Soit $f \in \mathcal{S}_k(\Gamma_1(N))$ une forme propre pour les opérateurs de Hecke, primitive et normalisée telle que k soit de poids pair. Les conditions suivantes sont équivalentes :*

- *Pour tout corps quadratique K, on peut répondre « oui » à la question 1 pour tout couple (f, g) sauf un nombre fini d'entre eux, où g est une forme modulaire parabolique primitive propre pour les opérateurs de Hecke et normalisée possédant multiplication réelle ou complexe par K.*

- *La réponse à la question 1 est « oui » pour tout couple (f, g), où g est une forme modulaire parabolique de poids un, primitive, propre pour les opérateurs de Hecke et normalisée.*
- *Tout caractère de Dirichlet (primitif) χ tel que $f \otimes \chi$ soit conjugué à f sous l'action de $G_{\mathbb{Q}}$ est pair.*

Nous décrivons également des contre-exemples explicites provenant d'une obstruction différente de celle apparaissant dans la preuve du théorème 15.

Théorème 16 *Il existe des formes modulaires $f \in \mathcal{S}_2(\Gamma_0(63)), g \in \mathcal{S}_1(\Gamma_1(1452))$ propres pour les opérateurs de Hecke, primitives et normalisées, à coefficients respectivement contenus dans $\mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{-3})$ telles que, pour tout idéal maximal $\mathfrak{p}$ de $L = \mathbb{Q}(e^{2i\pi/12})$ de caractéristique résiduelle $p \equiv 5, 7 \pmod{12}$ sauf un nombre fini, $V_{f,\mathfrak{p}} \otimes V_{g,\mathfrak{p}}$ ne vérifie pas la condition d'image adaptée.*

Chapter 1

Moduli spaces and twisted modular curves

The material of this Chapter is not new or particularly difficult: most of these results seem to be folklore, but it is not clear whether they have been precisely spelled out somewhere.

Its purpose is to prove[1] that two constructions for the curve of interest – both as a moduli space (which was already known, and discussed in [97, Proposition 1] or [113, I.7-9]) and a Galois twist (as discussed in [163]) – are equivalent, and moreover that this equivalence respects all the natural constructions one wishes to do for modular curves: Atkin-Lehner automorphisms, adding isogeny structures and Hecke operators. While [97] or [113] sketch the construction of the moduli space when the base ring is a field, we prove that the construction is valid over more general base rings (assumed to be regular excellent Noetherian to consider compactified moduli schemes).

Theorem 1.A *Let $N \geq 3$ be an integer and R be a regular excellent Noetherian $\mathbb{Z}[1/N]$-algebra. Let $m_0, m_1 \geq 1$ be two integers such that m_0, m_1, N are pairwise coprime, m_0 is square-free and $m_1 \in R^\times$, and write $m = m_0 m_1$. Let G be a finite étale commutative group scheme over R which is étale-locally isomorphic to $(\mathbb{Z}/N\mathbb{Z})^{\oplus 2}$. Then there is a proper flat R-scheme $X_G(N, \Gamma_0(m))$ of relative dimension one with geometrically reduced fibres satisfying the following properties:*

- *There is a finite locally free map $j : X_G(N, \Gamma_0(m)) \to \mathbb{P}^1_R$ such that $X_G(N, \Gamma_0(m))$ is smooth over* $\operatorname{Spec} R$ *outside the inverse image under j of the finitely many supersingular j-invariants in a fibre of residue characteristic dividing m_0.*
- *The reduced subscheme attached to the closed subspace $\{j = \infty\}$, called the* cuspidal subscheme*, is finite étale over R and defines an effective Cartier divisor.*
- *For any R-scheme S, $j^{-1}(\mathbb{A}^1_R)(S)$ is functorially isomorphic to the set of equivalence classes of $(E/S, \iota, C')$, where E/S is a relative elliptic curve, $\iota : G_S \to E[N]$ is an isomorphism of finite étale group schemes over S, and C' is a cyclic subgroup scheme of E of degree m in the sense of [86, (1.4), (3.4)][2].*
- *The formation of $X_G(N, \Gamma_0(m)), j$, the cuspidal subscheme, and the above isomorphism of functors commutes with base change.*

Moreover, let $d, t \geq 1$ be integers such that $dt \mid m$, then the morphism of functors

$$D_{d,t} : (E/S, \iota, C) \mapsto ((E/C[d])/S, \pi \circ \iota, C'),$$

where $C[d]$ denotes the "standard" cyclic subgroup of C of order d in the sense of [86, Theorem 6.7.2], $\pi : E \to E/C[d]$ denotes the natural isogeny and C' denotes the subgroup of order t of the cyclic subgroup $\pi(C)$ (see [86, Theorems 6.7.2, 6.7.4]), extends to a finite locally free

[1] following discussions with Loïc Merel and Barry Mazur

[2] This means that C' is finite locally free of degree m over S, and is fppf-locally over S of the form $[P] + [2P] + \ldots + [mP]$ (as a Cartier divisor on E) for some $P \in E(S)$.

morphism of R-schemes $X_G(N,\Gamma_0(m)) \to X_G(N,\Gamma_0(t))$ of constant rank mapping $X_G(N,\Gamma_0(m))$ to $X_G(N,\Gamma_0(t))$.

For any prime $\ell \nmid N$, the correspondence $(D_{1,1}, D_{\ell,1}) : X_G(N,\Gamma_0(\ell)) \to X_G(N) \times X_G(N)$ (where $X_G(N) := X_G(N,\Gamma_0(1))$) induces an endomorphism T_ℓ of the relative Jacobian $J_G(N)$ of $X_G(N)$, and the T_ℓ commute pairwise.

Furthermore, for $n \in (\mathbb{Z}/N\mathbb{Z})^\times$, there is an automorphism $[n]$ of $X_G(N,\Gamma_0(m))$ extending the isomorphism of functors $(E/S,\iota,C) \longmapsto (E/S,n\iota,C)$; $[n]$ commutes to any $D_{d,t}$.

Assume finally that G is endowed with a bilinear alternated pairing $\langle -,-\rangle_G : G \times G \to \mu_N$ which is fibrewise perfect. Then there is a morphism $\det : X_G(N,\Gamma_0(m)) \to (\mathbb{Z}/N\mathbb{Z})^\times_R$ such that for any $(E/S,\iota,C) \in X_G(N,\Gamma_0(m))(S)$, $\det(F/S,\iota,C)$ is the unique $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times_R(S)$ such that the pairings

$$G \times G \xrightarrow{\iota\times\iota} F[N] \times F[N] \overset{\mathrm{We}}{\to} (\mu_N)_S, \quad G_S \times G_S \overset{\alpha\cdot\langle -,-\rangle_G}{\longrightarrow} (\mu_N)_S$$

are equal, where We *denotes the Weil pairing.*

For any $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$, $X_G^\alpha(N,\Gamma_0(m)) := \det^{-1}(\alpha)$ is a proper flat R-scheme with geometrically connected fibres. For any $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$ and $d,t \geq 1$ such that $dt \mid m$, $D_{d,t}$ maps $X_G^\alpha(N,\Gamma_0(m))$ to $X_G^{d\alpha}(N,\Gamma_0(t))$, so that T_ℓ maps $J_G^\alpha(N)$ into $J_G^{\ell\alpha}(N)$. For any $\alpha, n \in (\mathbb{Z}/N\mathbb{Z})^\times$, $[n]$ is an isomorphism $X_G^\alpha(N,\Gamma_0(m)) \to X_G^{\alpha n^2}(N,\Gamma_0(m))$.

Remark As noted in the introduction of this thesis, the notion of relative Jacobian for a proper smooth scheme $X \to \operatorname{Spec} R$ of relative dimension one does not seem to be standard when the morphism does not have geometrically connected fibres, even when R is a field. However, only minor modifications to the classical theory are needed to define and construct Jacobians in this setting, which we describe in Section A.4.2.

Theorem 1.B *Let us keep the notations of Theorem 1.A and assume that R is a field k with separable closure k_s. Let $X(N,N)_k$ denote the curve attached by Theorem 1.A to the constant group $(\mathbb{Z}/N\mathbb{Z})_k^{\oplus 2}$, which is endowed with a left action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ given for any noncuspidal point $(E/S,\iota) \in X(N,N)_k(S)$ by $M \cdot (E/S,\iota) = (E/S, \iota \circ M^T)$.*

Fix a basis (P,Q) of $G(k_s)$, and let $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the function defined by

$$\forall g \in \mathrm{Gal}(k_s/k),\ \rho(g)\begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} g(P) \\ g(Q) \end{pmatrix}.$$

Then ρ is an anti-homomorphism, and let $X(N,N)_{\rho^{-1}}$ denote the Galois twist (see Proposition A.1.11) of $X(N,N)_k$ by the homomorphism $\rho^{-1} : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. The curve $X(N,N)_{\rho^{-1}}$ is also endowed with a finite locally free morphism $j : X(N,N)_{\rho^{-1}} \to \mathbb{P}^1_k$ representing the j-invariant, with Hecke correspondences and an action of $(\mathbb{Z}/N\mathbb{Z})^\times$ coming from the twist by ρ^{-1}.

Then there is a isomorphism of $\mathbb{P}^1_k$-schemes $\iota : X_G(N) \to X(N,N)_{\rho^{-1}}$ such that, for any non-cuspidal $(E/k_s,\varphi) \in X_G(N)(k_s)$, one has

$$\iota((E/k_s,\varphi)) = (E/k_s, (a,b) \mapsto aP + bQ) \in X(N,N)_k(k_s) \simeq X(N,N)_{\rho^{-1}}(k_s).$$

After passing to the Jacobians, this isomorphism preserves the Hecke operators and the action of $[n]$.

If G is endowed with a perfect bilinear alternated pairing $\langle \cdot,\cdot\rangle_G : G \times G \to \mu_N$, then $\det\rho$ is the mod N cyclotomic character and the connected components of $X(N,N)_{\rho^{-1}}$ are smooth projective geometrically connected curves over k, naturally indexed by the primitive N-th roots of unity in k_s, and ι maps $X_G^\alpha(N)$ to the component of $X(N,N)_{\rho^{-1}}$ indexed by $\langle P,Q\rangle_G^\alpha$.

As a preparation for the rest of the text, we also discuss some of the behavior of the curve $X(N)$ over $\mathbb{Z}[1/N]$: we prove an Eichler-Shimura relation (Corollary 1.5.16) and describe in Section 1.6 its cuspidal subscheme and the q-expansion principle.

This chapter is rooted in techniques from algebraic geometry, and in particular descent. Most of the relevant background, which we will use freely, is collected in Appendix A. The main reference for this background remains the online textbook Stacks Project [4]. The main references for the modular aspects are [36] and [86]. For the proof of the Eichler-Shimura relation, we somewhat follow the argument in the proof of [136, Appendix A, Theorem 5.16], but (as noted in *loc.cit.*), it is made significantly simpler by the theory of moduli schemes in characteristic p.

Notation *If R is a ring and S is a set, S_R denotes the constant R-scheme with underlying set S. For any $N \geq 1$,*

- *μ_N denotes the finite flat group scheme $\operatorname{Spec}\mathbb{Z}[X]/(X^n-1)$ over $\mathbb{Z}$, that is, the Cartier dual of the constant group scheme $(\mathbb{Z}/N\mathbb{Z})_{\mathbb{Z}}$,*
- *$\mu_N^\times$ denotes the finite flat $\mathbb{Z}$-scheme $\operatorname{Spec}\mathbb{Z}[X]/\Phi_N(X)$, where $\Phi_N(X)$ is the N-th cyclotomic polynomial, which is étale above $\mathbb{Z}[1/N]$,*
- *$\mathcal{O}_N$ denotes the ring $\mathbb{Z}[1/N,\zeta_N]$, where ζ_N is a primitive N-th root of unity.*

For every $d \mid N$, there is a natural closed immersion $\mu_d^\times \to \mu_N$ (given on coordinate rings by $X \mapsto X$), and the induced map $\coprod_{d|N} \mu_d^\times \to \mu_N$ is an isomorphism over $\mathbb{Z}[1/N]$.

1.1 Moduli problems

1.1.1 Definitions

We recall the framework introduced in [86, Chapter 4].

Given a ring R, we denote by $\mathbf{Ell}_R$ the category defined as follows. Its objects are relative elliptic curves $E \to S$ (which we often denote as E/S), where S is a R-scheme; given two relative elliptic curves $F \to T$ and $E \to S$, with S, T being R-schemes, a morphism $F/T \to E/S$ is a Cartesan diagram of R-schemes

$$\begin{array}{ccc} F & \xrightarrow{\alpha} & E \\ \downarrow & & \downarrow \\ T & \longrightarrow & S \end{array}$$

where α preserves the zero section, so that $F \to E \times_S T$ is an isomorphism *of elliptic curves over T* (by [86, Theorem 2.5.1]).

Note that if R' is a R-algebra, we have a faithful forgetful functor $\mathbf{Ell}_{R'} \to \mathbf{Ell}_R$.

Definition 1.1.1 A *moduli problem over R* is a contravariant functor $\mathscr{P} : \mathbf{Ell}_R \to \mathbf{Set}$. If R' is a R-algebra, the base change $\mathscr{P}_{R'}$ of $\mathscr{P}$ to R is exactly the functor $\mathbf{Ell}_{R'} \to \mathbf{Ell}_R \xrightarrow{\mathscr{P}} \mathbf{Set}$.

Definition 1.1.2 A moduli problem $\mathscr{P}$ over R is *rigid* if for any object E/S of (Ell/R), the action of $\mathrm{Aut}(E/S)$ on $\mathscr{P}(E/S)$ (on the right) is free, that is: for any $\alpha \in \mathscr{P}(E/S)$, any $g \in \mathrm{Aut}_R(E/S)$ with $g \neq \mathrm{id}$, $\mathscr{P}(g)\alpha \neq \alpha$.

Definition 1.1.3 A moduli problem $\mathscr{P}$ over R is *relatively representable* if for any object E/S of $\mathbf{Ell}_R$, the functor $T \in \mathbf{Sch}_S \longmapsto \mathscr{P}(E_T/T) \in \mathbf{Set}$ is representable by a S-scheme $\mathscr{P}_{E/S}$.

Definition 1.1.4 A moduli problem $\mathscr{P}$ over R is *representable* if there is an elliptic curve $\mathcal{E}/\mathscr{M}(\mathscr{P})$ (for some R-scheme $\mathscr{M}(\mathscr{P})$) and some $\alpha \in \mathscr{P}(\mathcal{E}/\mathscr{M}(\mathscr{P}))$ such that, for any object E/S in $\mathbf{Ell}_R$, $f \in \mathrm{Hom}_{\mathbf{Ell}_R}(E/S, \mathcal{E}/\mathscr{M}(\mathscr{P})) \longmapsto \mathscr{P}(f)\alpha \in \mathscr{P}(E/S)$ is an isomorphism. We call $\mathscr{M}(\mathscr{P})$ the moduli scheme, and we say that $(\mathcal{E}/\mathscr{M}(\mathscr{P}), \alpha)$ represents the moduli problem $\mathscr{P}$ (we will often omit α from the notation if it is not relevant).

The following result is formal:

Proposition 1.1.5 *Let $\mathscr{P}$ be a moduli problem over R and let R' be a R-algebra. Let us write $\mathscr{P}' = \mathscr{P}_{R'}$ for the base change of $\mathscr{P}$.*

- *If $\mathscr{P}$ is rigid, then so is $\mathscr{P}'$.*
- *If $\mathscr{P}$ is relatively representable, then any morphism $F/T \to E/S$ in $\mathbf{Ell}_R$ induces a canonical isomorphism $\mathscr{P}_{F/T} \to \mathscr{P}_{E/S} \times_S T$,*
- *If $\mathscr{P}$ is relatively representable, then $\mathscr{P}'$ is relatively representable, and, for any object E/S in $\mathbf{Ell}_{R'}$, we have an isomorphism $\mathscr{P}'_{E/S} \to \mathscr{P}_{E/S}$ of S-schemes.*
- *If $\mathscr{P}$ is representable by $(\mathcal{E}/\mathscr{M}(\mathscr{P}), \alpha)$, then $\mathscr{P}'$ is representable by*

$$(\mathcal{E}_{R'}/\mathscr{M}(\mathscr{P})_{R'}, \mathscr{P}[\mathcal{E}_{R'}/\mathscr{M}(\mathscr{P})_{R'} \to \mathcal{E}/\mathscr{M}(\mathscr{P})]\alpha).$$

In particular, we have a canonical isomorphism $\mathscr{M}(\mathscr{P}') \to \mathscr{M}(\mathscr{P})_{R'}$ (we say that the formation of the moduli scheme commutes with base change).

Let $\mathscr{C}$ be a property of morphisms of schemes. We say that it is *good* if it satisfies the following conditions:

- it is stable under pre- and post-composition by isomorphisms,
- it is stable under arbitary base change,
- it satisfies fpqc descent in the following sense: if $f : X \to Y$ is a morphism such that there exists a fpqc cover by maps $Y_i \to Y$ such that $f_{Y_i} : X \times_Y Y_i \to Y_i$ satisfies the property $\mathscr{C}$, then f satisfies the property $\mathscr{C}$.

All the properties given in Proposition A.1.5 are good.

Definition 1.1.6 Let $\mathscr{P}$ be a relatively representable moduli problem over R and $\mathscr{C}$ be a good property of morphisms of schemes. We say that $\mathscr{P}$ satisfies $\mathscr{C}$ over $\mathbf{Ell}_R$ if for every object E/S in $\mathbf{Ell}_R$, then $\mathscr{P}_{E/S} \to S$ has property $\mathscr{C}$. If $Z \subset \mathbb{A}^1_R$ is a locally closed subscheme of $\mathbb{A}^1_R$, we say that $\mathscr{P}$ satisfies $\mathscr{C}$ above Z if, for every object E/S in $\mathbf{Ell}_R$ such that $j(E/S) \in \mathbb{A}^1_R(S)$ factors through Z, then $\mathscr{P}_{E/S} \to S$ satisfies property $\mathscr{C}$.

Proposition 1.1.7 *Let R be a ring and S_0 be any S-scheme. The moduli problem $[S_0]$ on $\mathbf{Ell}_R$ defined by $E/S \longmapsto \mathrm{Mor}_R(S, S_0)$ is relatively representable; for any relative elliptic curve E/S (S being a R-scheme), $[S_0]_{E/S}$ is naturally isomorphic to $S \times_R S_0$. In particular, if $\mathscr{C}$ is any good property of morphisms of schemes such that $S_0 \to \operatorname{Spec} R$ satisfies $\mathscr{C}$, then $[S_0]$ satisfies $\mathscr{C}$.*

Proof. – This is formal. □

Definition 1.1.8 Let $\mathscr{P}$ be a moduli problem over R, representable by the elliptic curve $\mathcal{E}/\mathscr{M}(\mathscr{P})$. There is a canonical j-invariant map $\mathscr{M}(\mathscr{P}) \to \mathbb{A}^1_R$, given by the j-invariant of $\mathcal{E}$.

One checks formally that

Lemma 1.1.9 *The formation of the j-invariant map commutes with base change of representable moduli problems.*

Proposition 1.1.10 *Let $\mathscr{C}$ be a good property of morphisms of schemes, $\mathscr{P}$ be a relatively representable moduli problem over R, and $\mathscr{P}'$ be the base change of $\mathscr{P}$ to an R-algebra R'. Then*

- *If $\mathscr{P}$ has property $\mathscr{C}$ over $\mathbf{Ell}_R$, then $\mathscr{P}'$ has property $\mathscr{C}$ over $\mathbf{Ell}_{R'}$,*
- *If R' is faithfully flat over R and $\mathscr{P}'$ has property $\mathscr{C}$ over $\mathbf{Ell}_{R'}$, then $\mathscr{P}$ has property $\mathscr{C}$ over $\mathbf{Ell}_R$.*

We finally discuss the situation for morphisms of moduli problems.

Proposition 1.1.11 *Let $T : \mathscr{P} \Rightarrow \mathscr{P}'$ be a natural transformation of relatively representable moduli problems over $\mathbf{Ell}_R$. Then, for every object E/S in $\mathbf{Ell}_R$, T induces a morphism of S-schemes $\mathscr{P}_{E/S} \to \mathscr{P}'_{E/S}$ whose formation commutes with base change. If $\mathscr{P}, \mathscr{P}'$ are representable, then T induces a map $\mathscr{M}(\mathscr{P}) \to \mathscr{M}(\mathscr{P}')$ whose formation commutes with base change.*

We conclude this section with representability results.

Proposition 1.1.12 *([86, (4.3.4)]) Let $\mathscr{P}, \mathscr{P}'$ be relatively representable moduli problems over $\mathbf{Ell}_R$. Then the moduli problem over $\mathbf{Ell}_R$*

$$\mathscr{P} \times \mathscr{P}' : E/S \longmapsto \mathscr{P}(E/S) \times \mathscr{P}'(E/S)$$

(with its natural action on the morphisms in $\mathbf{Ell}_R$) is relatively representable. Moreover, for every object E/S of $\mathbf{Ell}_R$, one has a canonical isomorphism of S-schemes

$$(\mathscr{P} \times \mathscr{P}')_{E/S} \to \mathscr{P}_{E/S} \times_S \mathscr{P}'_{E/S}.$$

If furthermore $\mathscr{P}$ is representable by $(\mathcal{E}/\mathscr{M}(\mathscr{P}), \alpha)$, then $\mathscr{P} \times \mathscr{P}'$ is representable by

$$\left((p')^*\mathcal{E}/\mathscr{P}'_{\mathcal{E}/\mathscr{M}(\mathscr{P})}, ((\mathscr{P}p')(\alpha), \beta)\right),$$

where $p' : \mathscr{P}'_{\mathcal{E}/\mathscr{M}(\mathscr{P})} \to \mathscr{M}(\mathscr{P})$ is the map given by the relative representability of $\mathscr{P}'$, and

$$\beta \in \mathscr{P}'((p')^*\mathcal{E}/\mathscr{P}'_{\mathcal{E}/\mathscr{M}(\mathscr{P})})$$

corresponds to the identity under the identification

$$\mathscr{P}'((p')^*\mathcal{E}/\mathscr{P}'_{\mathcal{E}/\mathscr{M}(\mathscr{P})}) \simeq \mathrm{Hom}_{\mathscr{M}(\mathscr{P})}(\mathscr{P}'_{\mathcal{E}/\mathscr{M}(\mathscr{P})}, \mathscr{P}'_{\mathcal{E}/\mathscr{M}(\mathscr{P})}).$$

Proof. – This is [86, (4.3.4)], but since the proof (essentially an exercise in formalism) is not detailed in the book, we do it here. For the first claim, we simply note that if E/S is an object of $\mathbf{Ell}_R$ and T is any S-scheme, then we have, fonctorially in T,

$$\begin{aligned}(\mathscr{P} \times \mathscr{P}')(E_T/T) &\simeq \mathscr{P}(E_T/T) \times \mathscr{P}'(E_T/T)\\ &\simeq \mathrm{Hom}_S(T, \mathscr{P}_{E/S}) \times \mathrm{Hom}_S(T, \mathscr{P}'_{E/S})\\ &\simeq \mathrm{Hom}_S(T, \mathscr{P}_{E/S} \times_S \mathscr{P}'_{E/S}),\end{aligned}$$

which concludes.

Now let us consider the second claim. For the sake of easier notation, let $B = \mathscr{M}(\mathscr{P})$, $B' = \mathscr{P}'_{\mathcal{E}/\mathscr{M}(\mathscr{P})}$, and $\alpha' = (\mathscr{P}p')(\alpha)$. Given an object E/S of $\mathbf{Ell}_R$, we have an isomorphism $\iota_{E/S}$ of functors on $\mathbf{Sch}_S$: $\iota_{E,S} : \mathscr{P}'(E_T/T) \to \mathrm{Mor}_S(T, \mathscr{P}'_{E/S})$. In particular, β is the inverse image under $\iota_{\mathcal{E}/B}(B')$ of $\mathrm{id}_{B'} \in \mathrm{Mor}_B(B', B')$.

Let F/T be any object of $\mathbf{Ell}_R$: we need to prove that for any $a \in \mathscr{P}(F/T)$, $b \in \mathscr{P}'(F/T)$, there is a unique morphism $f \in \mathbf{Ell}_R(F/T, (p')^*\mathcal{E}/B')$ such that $(\mathscr{P}f)\alpha' = a$, $(\mathscr{P}'f)(\beta) = b$.

Let us pick $a \in \mathscr{P}(F/T)$ and $b \in \mathscr{P}'(F/T)$. There is a morphism $f_1 \in \mathbf{Ell}_R(F/T, \mathcal{E}/B)$ such that $a = (\mathscr{P}f_1)(\alpha)$. Let g_1 be the induced morphism $T \to B$, so that f_1 determines an isomorphism $f_2 : F/T \simeq g_1^*\mathcal{E}/T$. We thus can define $b' = (\mathscr{P}'(f_2^{-1}))(b) \in \mathscr{P}'(\mathcal{E} \times_B T/T)$. Let $(\iota_{\mathcal{E}/B}T)(b') = \widetilde{f_3} \in \mathrm{Mor}_B(T, B')$, and f_3 be the induced morphism $(\widetilde{f_3})^*(p')^*\mathcal{E}/T \to (p')^*\mathcal{E}/B'$ (noting that $\widetilde{f_3}^*(p')^* = (p' \circ \widetilde{f_3})^* = g_1^*$).

By Yoneda's lemma, one has $\widetilde{f_3} = (\iota_{\mathcal{E}/B}\widetilde{f_3})((\iota_{\mathcal{E}/B}B')\beta) = (\iota_{\mathcal{E}/B}T)(\mathscr{P}'f_3)(\beta)$, and therefore $b' = (\mathscr{P}'f_3)\beta$, whence $b = (\mathscr{P}'(f_3 \circ f_2))(\beta)$. Moreover, one has

$$\mathscr{P}(f_3 \circ f_2)(\alpha') = \mathscr{P}(p' \circ f_3 \circ f_2)(\alpha) = \mathscr{P}(f_1)(\alpha) = a.$$

Now, we need to show injectivity. Let $\widetilde{p'} : (p')^*\mathcal{E}/B' \to \mathcal{E}/B$ be the natural morphism. Let $f_1, f_2 \in \mathbf{Ell}_R(F/T, (p')^*\mathcal{E}/B')$ be such that $(\mathscr{P}f_i)(\alpha') = a$, $(\mathscr{P}'f_i)(\beta) = b$. Thus one has $a = (\mathscr{P}f_i)(\alpha') = (\mathscr{P}f_i) \circ (\mathscr{P}\widetilde{p'})(\alpha)$, so that the two maps $\widetilde{p'} \circ f_1 = \widetilde{p'} \circ f_2$. In particular, the two

base maps $\widetilde{f}_i : T \to B'$ attached to the f_i define the same structure of B-scheme on T, and the two isomorphisms $g_i \in \mathbf{Ell}_R(F/T, \widetilde{f}_i^{\,*}(p')^*\mathcal{E}/T)$ induced by f_i are the same, since $\widetilde{f}_i^{\,*}(p')^* = q^*$.

Let f_i' denote the morphism $q^*\mathcal{E}/T \to (p')^*\mathcal{E}$ induced by $\widetilde{f}_i$. We have $f_i = f_i' \circ g_i$, and since $g_1 = g_2$ are isomorphisms, one knows that $(\mathscr{P}' f_i')(\beta)$ is independent from i. Now, $(\mathscr{P}' f_i')(\beta) = (\mathscr{P}' f_i')((\iota_{\mathcal{E}/B}B')^{-1}\mathrm{id}_{B'}) = (\iota_{\mathcal{E}/B}T)^{-1}(\widetilde{f}_i)$. Therefore, $\widetilde{f}_1 = \widetilde{f}_2$, hence $f_1' = f_2'$ and $f_1 = f_2$.

□

Proposition 1.1.13 *Let $\mathscr{C}$ be a good property of morphisms of schemes satisfying in addition the following assumptions:*

- *it is stable under post-composition by surjective smooth affine maps of relative dimension one (resp. by finite flat maps),*
- *if $f : X \to Y$ is a finite étale surjective map and $g : Y \to Z$ is such that $g \circ f$ satisfies $\mathscr{C}$, then g satisfies $\mathscr{C}$.*

Let $\mathscr{P}$ be a representable moduli problem over $\mathbf{Ell}_R$ having property $\mathscr{C}$ over $\mathbf{Ell}_R$ (resp. above some locally closed subscheme Z of $\mathbb{A}^1_R$). Then $\mathscr{M}(\mathscr{P}) \to \operatorname{Spec} R$ has property $\mathscr{C}$ (resp. the j-invariant of $\mathscr{M}(\mathscr{P}) \to \mathbb{A}^1_R$ has property $\mathscr{C}$ above Z).

Proof. – Since everything is Zariski-local with respect to R, we can assume that there is an odd prime ℓ invertible in R. The conclusion then follows from the properties of the following commuting diagram:

$$\begin{array}{ccccc} \mathscr{M}(\mathscr{P}, [\Gamma(\ell))]_R) & \xrightarrow{f_1} & \mathscr{M}([\Gamma(\ell)]_R) & \xrightarrow{\sigma} & \operatorname{Spec} R \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle j_\ell} & \nearrow & \\ \mathscr{M}(\mathscr{P}) & \xrightarrow{j_{\mathscr{P}}} & \mathbb{A}^1_R & & \end{array}$$

Indeed, π_1 is finite étale by [86, Theorem 3.7.1] while f_1 satisfies $\mathscr{C}$ (resp. satisfies $\mathscr{C}$ above Z), and σ is smooth affine of relative dimension one by [86, Corollary 4.7.2], while j_ℓ is finite by [86, Theorem 5.1.1, Proposition 8.2.2] and thus flat (over $\mathbb{Z}[1/\ell]$, this follows from miracle flatness [4, Lemma 00R4], since both schemes are smooth surjective $\mathbb{Z}[1/\ell]$-schemes where every nonempty open subset has dimension 2, and we conclude by base change). □

Corollary 1.1.14 *Let $\mathscr{P}$ be a representable moduli problem over $\mathbf{Ell}_R$.*

- *If $\mathscr{P}$ is affine (resp. quasi-compact) over $\mathbf{Ell}_R$, then $\mathscr{M}(\mathscr{P})$ is affine (resp. quasi-compact).*
- *If $\mathscr{P}$ is surjective (resp. locally quasi-finite, locally of finite type, locally of finite presentation, finite with R Noetherian, flat) over $\mathbf{Ell}_R$, its j-invariant $\mathscr{M}(\mathscr{P}) \to \mathbb{A}^1_R$ is surjective (resp. locally quasi-finite, locally of finite type, locally of finite presentation, finite, flat). In particular, if $\mathscr{P}$ is locally quasi-finite of finite presentation and flat over $\mathbf{Ell}_R$, then $\mathscr{M}(\mathscr{P}) \to \operatorname{Spec} R$ is Cohen-Macaulay [4, Section 00N7] and its nonempty fibres are pure of relative dimension one.*
- *If $\mathscr{P}$ is affine of finite presentation over $\mathbf{Ell}_R$ and étale above some open subscheme $U \subset \mathbb{A}^1_R$, then $j^{-1}(U) \subset \mathscr{M}(\mathscr{P}) \to \operatorname{Spec} R$ is smooth surjective of relative dimension one.*

Proof. – The first point follows from the properties of affine and quasi-compact morphisms by fpqc descent and [4, Lemma 01ZT]. The second point follows from Proposition A.1.5 for fpqc descent, [4, Section 036M, Section 036K] for the "finite étale descent" conditions, and the fact that finite flat morphisms are clearly Cohen-Macaulay. The dimension of the fibres follows from the results of [4, Section 02NM]. For the last statement, we use the Proposition in the same way along with [4, Lemma 036U] to check that the "finite étale descent" condition is satisfied. □

Proposition 1.1.15 *Let $R \to R'$ be a faithfully flat étale map, and let $\mathscr{P}$ be a moduli problem on $\mathbf{Ell}_R$. Assume that:*

- *$\mathscr{P}_{R'}$ is representable and affine,*
- *For all objects E/S of $\mathbf{Ell}_R$, $T \in \mathbf{Sch}_S \longmapsto \mathscr{P}(E_T/T)$ is an fpqc sheaf.*

Then $\mathscr{P}$ is representable.

Proof. – We need to show that $\mathscr{P}$ is relatively representable, affine over $\mathbf{Ell}_R$, and rigid, by [86, (4.7.0)][3].

Let us first show that $\mathscr{P}$ is rigid. Let T be a R-algebra, E/T be an elliptic curve, $\alpha \in \mathscr{P}(E/T)$ and $u \in \mathrm{Aut}(E/T)$ such that $(\mathscr{P}u)(\alpha) = \alpha$. Let $T' = T \otimes_R S$ and α', u' be the base changes of α, u to the elliptic curve $E_{T'}/T'$. Since $\mathscr{P}_S$ is representable, and since $\alpha' \in \mathscr{P}_S(E_{T'}/T')$, and $(\mathscr{P}_S u')(\alpha') = \alpha'$, one has $u' = \mathrm{id}$. Thus the automorphisms id and u of the T-scheme E become equal after a faithfully flat base change with respect to T: so $u = \mathrm{id}$.

Now, we show that $\mathscr{P}$ is relatively representable. Let E/T be an elliptic curve where T is a R-scheme; we want to show that the pre-sheaf on the category of T-schemes $U \longmapsto \mathscr{P}(E_U/U)$ is representable. The hypothesis states that this pre-sheaf is an fpqc sheaf, and its restriction to the subcategory of schemes over $T_{R'} := T \times_R \operatorname{Spec} R'$ ($T_{R'} \to T$ being affine faithfully flat) is representable by a scheme X' affine over $T_{R'}$. By Proposition A.1.4, this sheaf is representable by an affine T-scheme X. □

1.1.2 Γ_0-structures and degeneracy maps

Recall the following definition inspired from [86, §4.14].

Definition 1.1.16 Let $N \geq 1$ be an integer and R be a ring. Let $\mathbf{FGp}_R^N$ be the category defined as follows:

- Its objects are finite flat locally free commutative group schemes G/S, where S is a R-scheme, and G is annihilated by the multiplication by N,
- A morphism $G'/S' \to G/S$ is a Cartesian diagram as below such that the induced map $f : G' \to G \times_S S'$ is an isomorphism of S'-group schemes.

$$\begin{array}{ccc} G' & \xrightarrow{f} & G \\ \downarrow & & \downarrow \\ S' & \longrightarrow & S \end{array}$$

A *level N structure* on a moduli problem $\mathscr{P}$ on $\mathbf{Ell}_R$ is a functor $F : \mathbf{FGp}_R^N \to \mathbf{Set}$ such that $\mathscr{P}$ is the composition of F and $E/S \in \mathbf{Ell}_R \longmapsto E[N]/S \in \mathbf{FGp}_R^N$. Unless it is both relevant and not obvious, when we claim that a moduli problem $\mathscr{P}$ on $\mathbf{Ell}_R$ is of level N, we omit the functor F from the notation.

Definition 1.1.17 Let $\mathscr{P}, \mathscr{P}'$ be moduli problems on $\mathbf{Ell}_R$, endowed with level N structures by the functors F, F'. A morphism of moduli problems of level N is a natural transformation $f : F \Rightarrow F'$. In particular, for every object E/S of $\mathbf{Ell}_R$ and every $\alpha \in \mathscr{P}(E/S) = F(E[N]/S)$, we can define $f(\alpha) \in F'(E[N]/S) = \mathscr{P}'(E/S)$; this construction defines in particular a morphism of functors $\mathscr{P} \Rightarrow \mathscr{P}'$.

Remarks

- If S_0 is a R-scheme, the moduli problem $[S_0]$ on $\mathbf{Ell}_R$ has a natural level one structure.

[3] The statement in the book discusses the case $R = \mathbb{Z}$, but it applies to any case, since the moduli problems used to cover $\mathbf{Ell}_{\mathbb{Z}}$, the "Legendre" and "naïve level three" problems (over $\mathbb{Z}[1/2]$ and $\mathbb{Z}[1/3]$ are still representable by smooth affine curves over $R[1/2]$ and $R[1/3]$ for any ring R, by Proposition 1.1.5), and the argument does not use any property of $\mathbb{Z}$ as a base ring.

- Suppose that $(\mathscr{P}, F)$ is a moduli problem of level N, and $f : E \to E'$ is an isogeny of elliptic curves over a given R-scheme S of degree prime to N. Then f induces an isomorphism of S-group schemes $E[N] \to E'[N]$, thus induces an isomorphism $\mathscr{P}(E/S) \to \mathscr{P}(E'/S)$. When furthermore $E = E'$ and f is the multiplication by some integer $d \equiv 1 \mod N$, f acts trivially on $E[N]$: this means that $(\mathbb{Z}/N\mathbb{Z})^\times$ acts[4] on $\mathscr{P}$; we will denote this action by $[\cdot]$. Note that this action preserves the j-invariant.
- We can define notions of base change similarly to the previous section.
- If $N \geq 1$ is an integer and $\mathscr{P}$ is a moduli problem on $\mathbf{Ell}_R$ endowed with the level N structure F, and M is any multiple of N, then we can endow $\mathscr{P}$ with the natural level M structure $F_{N\to M} : \mathbf{FGp}_R^M \overset{G\mapsto G[N]}{\longrightarrow} \mathbf{FGp}_R^N \overset{F}{\to} \mathbf{Set}$.
- One obviously has $(F_{N\to M})_{M\to M'} = F_{N\to M'}$ if $M \mid M'$.
- If $(\mathscr{P}, F)$ is a moduli problem of level N, $\hat{\mathbb{Z}}^\times$ acts on $\mathscr{P}$ by projecting to $(\mathbb{Z}/N\mathbb{Z})^\times$ and applying $[\cdot]$. If $N \mid M$, then the induced action of $\hat{\mathbb{Z}}^\times$ on $\mathscr{P}$ given by $(\mathscr{P}, F_{N\to M})$ is the same action.
- We thus define, for any integer $m \geq 1$, the category of moduli problems of level coprime to m: its objects are moduli problems endowed with a level n structure for some $n \geq 1$ coprime to m, and a morphism $(\mathscr{P}, F) \to (\mathscr{P}', F')$, when F, F' are respectively level n, n' structures on $\mathscr{P}, \mathscr{P}'$ (with nn' coprime to m) is any natural transformation of functors $F_{n\to d} \Rightarrow F_{n'\to d}$ for some d divisible by n, n' and coprime to m. The composition is defined similarly, if necessary by raising d. The induced morphism $\mathscr{P} \Rightarrow \mathscr{P}'$ is equivariant for the actions of $\hat{\mathbb{Z}}^\times$ (and any $\mathbb{Z}_p^\times$ for $p \mid m$ acts trivially).

Proposition 1.1.18 *Let $\mathscr{P}, \mathscr{P}'$ be moduli problems on $\mathbf{Ell}_R$ of levels N, N'. Then the moduli problem $\mathscr{P} \times \mathscr{P}'$ is endowed with a natural level M structure, where M is the least common multiple of N and N'.*

Proof. – This is formal. □

Definition 1.1.19 Let $m \geq 1$ be an integer. Let us recall the definitions of the basic moduli problems $[\Gamma(m)]_R, [\Gamma_1(m)]_R, [\Gamma_0(m)]_R$ over a ring R, following [86, Chapter 3]. In the case of $[\Gamma_1(m)]_R$ and $[\Gamma(m)]_R$, we will always assume that $m \in R^\times$.

The moduli problem $[\Gamma(m)]_R$ (resp. $[\Gamma_1(m)]_R$) is defined as follows:

- Let E be an elliptic curve over a R-scheme S. Then $[\Gamma(m)]_R(E/S)$ (resp. $[\Gamma_1(m)]_R(E/S)$) is the set of group homomorphisms $\phi : (\mathbb{Z}/m\mathbb{Z})^{\oplus 2} \to E[m]$ (resp. $\phi : \mathbb{Z}/m\mathbb{Z} \to E[m](S)$) such that for any geometric point $\overline{s}$ of S, the induced map $\phi : (\mathbb{Z}/m\mathbb{Z})^{\oplus 2} \to E[m](\overline{s})$ (resp. $\phi : \mathbb{Z}/m\mathbb{Z} \to E[m](\overline{s})$) is an isomorphism (resp. is injective). Equivalently, $[\Gamma(m)]_R(E/S)$ (resp. $[\Gamma_1(m)]_R(E/S)$) denotes the collection of couples $(P, Q) \in E[m](S)$ (resp. of $P \in E[m](S)$) such that for any geometric point $\overline{s}$ of S, the image of (P, Q) in $E[m](\overline{s})$ is a $\mathbb{Z}/m\mathbb{Z}$-basis of this group (resp. the image of P in $E[m](\overline{s})$ has order exactly m).
- Given a morphism $F/T \to E/S$ in $\mathbf{Ell}_R$, the morphism $[\Gamma(m)]_R(E/S) \to [\Gamma(m)]_R(F/T)$ (resp. $[\Gamma_1(m)]_R(E/S) \to [\Gamma_1(m)]_R(F/T)$) is induced by the map $E(S) \to F(T)$.

The moduli problem $[\Gamma_0(m)]_R$ is defined as follows (as in [86, (3.4)]):

- Given an elliptic curve E over some R-scheme S, $[\Gamma_0(m)]_R(E/S)$ denotes the collection of S subgroup schemes C of E that are finite locally free of degree m over S, and admit fppf-locally over S a generator – in the sense that fppf-locally on S, there is a section $P \in C(S)$ such that as Cartier divisors over E, C is equal to $\sum_{i=1}^m [iP]$.
- Given a morphism $F/T \to E/S$ in $\mathbf{Ell}_R$, the morphism $[\Gamma_0(m)]_R(E/S) \to [\Gamma_0(m)]_R(F/T)$ is given by $C \longmapsto C_T$.

[4] Note that this action depends on the choice of F.

Remark [86, (3.4)] also gives another definition for the moduli problem $[\Gamma_0(m)]_R$, as the collection of isomorphism classes of isogenies $E \to E'$ whose kernel is finite locally free of degree m over S and fppf-locally cyclic. The two definitions are equivalent because, for any relative elliptic curve E/S and any subgroup scheme G of E which is finite locally free over S, G is the kernel of a finite locally free isogeny $\pi : E \to E'$ by [4, Lemma 07S7][5].

Proposition 1.1.21 *On any ring R, and for any integer $m \geq 1$, the moduli problems $[\Gamma_0(m)]_R$, $[\Gamma_1(m)]_R$, $[\Gamma(m)]_R$ are relatively representable, finite locally free of constant rank on $\mathbf{Ell}_R$, étale above $\mathbb{Z}[1/m]$ (over $\mathbf{Ell}_R$). They are endowed with natural level m structures. Moreover, the induced action of $\hat{\mathbb{Z}}^\times$ on $[\Gamma_0(m)]_R$ is trivial.*

Proof. – The relative representability and the properties of the moduli problems follow from [86, Lemma 4.12.1, Theorem 5.1.1] and Proposition 1.1.10). The definition of the level m structure follows from the discussion in [86, Chapter 3] (using for instance [86, Proposition 1.10.6]). As for the action of $\hat{\mathbb{Z}}^\times$ on $[\Gamma_0(m)]_R$, note that, for any $d \geq 1$ coprime to m, if E/S is an elliptic curve and $C \leq E[m]$ is a cyclic subgroup of order m (in the sense of [86, (3.4)], that is: a closed subgroup scheme of $E[m]$, finite locally free of rank m over S, admitting a generator fppf-locally on S), then $dC = C$. □

Proposition 1.1.22 *Let R be a ring and $\mathscr{P}$ be a representable moduli problem on $\mathbf{Ell}_R$ of level N. Let m be an integer coprime to N. Then the moduli problem $\mathscr{P} \times [\Gamma_0(m)]_R$ is representable by a scheme $\mathscr{M}(\mathscr{P}, [\Gamma_0(m)]_R)$ endowed with a finite flat map of locally constant rank to $\mathscr{M}(\mathscr{P})$ (which is étale on the invertible locus of m). This moduli problem has a natural level Nm structure.*

Proof. – $[\Gamma_0(m)]_R$ is relatively representable by Proposition 1.1.21, so $\mathscr{P} \times [\Gamma_0(m)]_R$ is representable by Proposition 1.1.12. The level structure is given by Proposition 1.1.18. □

Proposition 1.1.23 *Let m be a positive integer and d, t be integers such that $dt \mid m$. For any representable moduli problem $\mathscr{P}$ on $\mathbf{Ell}_R$ of level N coprime to m, there exists a* degeneracy map *$D_{d,t} : \mathscr{M}(\mathscr{P}, [\Gamma_0(m)]_R) \to \mathscr{M}(\mathscr{P}, [\Gamma_0(t)]_R)$ defined by the following rule. Let E/S be an elliptic curve endowed with a cyclic subgroup C of order[6] m, and $\alpha \in \mathscr{P}(E/S)$. Let C_d be the "standard" cyclic subgroup scheme of C of order d in the sense of [86, Theorem 6.7.2], and let $\pi : E \to E' = E/C_d$ be the cyclic isogeny of degree d. Then $D_{d,t}$ maps $(E/S, \alpha, C)$ to $(E'/S, \pi(\alpha), C')$, where $C' \leq E'[t]$ is the finite flat subgroup scheme over S, cyclic of degree t defined as the standard subgroup of the finite flat cyclic subgroup $\pi(C)$ of E' (which has order m/d by [86, Theorem 6.7.4]).*

Definition 1.1.24 The $D_{d,t}$ defined in Proposition 1.1.23 are the *degeneracy maps*.

Corollary 1.1.25 *We keep the setting of Proposition 1.1.23.*

- *The formation of any $D_{d,t}$ is natural with respect to $\mathscr{P}$ (for morphisms of representable moduli problems of level N coprime to m, such as the action of $(\mathbb{Z}/N\mathbb{Z})^\times$) and commutes with base change.*
- *$D_{1,m}$ is the identity, and every $D_{1,q}$ (for $q \mid m$) is a map of $\mathscr{M}(\mathscr{P})$-schemes (where the structure map comes from Proposition 1.1.22).*
- *Suppose that d, t are divisors of m such that $dt \mid m$, and let r, s be divisors of t such that $rs \mid t$. Then $D_{r,s} \circ D_{d,t} = D_{dr,s}$.*

Proof. – The first two statements are completely formal. The last assertion follows from [86, Theorem 6.7.4]. □

[5] I am grateful to MathOverflow user SashaP for pointing out this result to me.

[6] As in [86], this denotes a finite S-subgroup scheme of E, locally free of degree m over S, and fppf locally cyclic.

Proposition 1.1.26 *Let $F : \mathscr{P} \Rightarrow \mathscr{P}'$ be a morphism of representable moduli problems of level N on $\mathbf{Ell}_R$. Let $m, d, t \geq 1$ be such that $dt \mid m$ and m is coprime to N. Then the following diagram is Cartesian:*

$$\begin{array}{ccc} \mathscr{M}(\mathscr{P}, [\Gamma_0(m)]_R) & \xrightarrow{D_{d,t}} & \mathscr{M}(\mathscr{P}, [\Gamma_0(t)]_R) \\ \downarrow F & & \downarrow F \\ \mathscr{M}(\mathscr{P}', [\Gamma_0(m)]_R) & \xrightarrow{D_{d,t}} & \mathscr{M}(\mathscr{P}', [\Gamma_0(t)]_R) \end{array}$$

Proof. – Let $\tau_1 = (E'/S, \alpha', C') \in \mathscr{M}(\mathscr{P}, [\Gamma_0(t)]_R)(S), \tau_2 = (E/S, \beta, C) \in \mathscr{M}(\mathscr{P}', [\Gamma_0(m)]_R)(S)$ be such that $F(\tau_1) = D_{d,t}(\tau_2) \in \mathscr{M}(\mathscr{P}', [\Gamma_0(t)]_R)(S)$. Then there exists a cyclic isogeny $\pi : E \to E'$ of degree d whose kernel is the standard subgroup C_d of degree d of C, such that C' is the standard cyclic subgroup of degree t of $\pi(C)$ and $F(\alpha') = \pi(\beta)$.

Let $\alpha \in \mathscr{P}(E/S)$ be the inverse image of α' under π, then $(E/S, \alpha, C) \in \mathscr{M}(\mathscr{P}, [\Gamma_0(m)]_R)(S)$ lies above τ_1 and τ_2.

Suppose that $(K/S, \gamma, D) \in \mathscr{M}(P, [\Gamma_0(m)]_R)(S)$ is a point lying over (τ_1, τ_2). Then there is an isomorphism of elliptic curves $f : K \to E$ mapping $F(\gamma)$ to β and D to C. Moroever, there is a cyclic isogeny $g : K \to E'$ of degree d such that $\alpha' = g(\gamma)$, $\ker g$ is the standard subgroup of D of order d, and C' is the standard cyclic subgroup of $g(D)$ of order t.

Then $g, \pi \circ f$ are cyclic isogenies $K \to E'$ with the same kernel. Thus there exists an automorphism ψ of E' such that $\psi \circ g = \pi \circ f$, whence

$$\psi(F(\alpha')) = \psi(F(g(\gamma))) = F(\pi(f(\gamma))) = \pi(f(F(\gamma))) = \pi(\beta) = F(\alpha').$$

Since $\mathscr{P}'$ is representable, it is rigid, hence ψ is the identity. Therefore, $\gamma = f^{-1}(\alpha)$, and $(F/S, \gamma, D)$ is isomorphic to $(E/S, \alpha, C)$, so we are done. □

Lemma 1.1.27 *Let E, F be relative elliptic curves over a basis S, endowed with cyclic subgroups C, D of coprime degrees $c, d \geq 1$. Suppose we are given an isomorphism $\iota : E/C \to F/D$ of elliptic curves (thus endowing F with the structure of finite locally free E/C-scheme of degree d). Then $E \times_{E/C} F$ is an elliptic curve over S.*

Proof. – Since $E, F, E/C$ are proper commutative group schemes over S, so is $G = E \times_{E/C} F$. Moreover, $G \to S$ factors through $G \to F \to S$, with $G \to F$ finite locally free and $F \to S$ smooth of relative dimension one, hence G is a proper flat commutative group scheme over S of relative dimension one.

Moreover, $G_{S[1/c]} \to F_{S[1/c]}$ is the base change of the étale isogeny $E_{S[1/c]} \to (E/C)_{S[1/c]}$, so it is étale and $G_{S[1/c]} \to S$ is smooth of relative dimension one. Similarly, $G \to S$ is smooth above $S[1/d]$ of relative dimension one. Since c, d are coprime, $G \to S$ is a proper smooth commutative group scheme of relative dimension one.

We finally need to check that the geometric fibres of $G \to S$ are connected, so we may assume that S is the spectrum of an algebraically closed field. Let $p : E \to E/C, q : F \to F/D$ be the projections and G^0 be the connected component of G containing the unit: G^0 is an elliptic curve over S.

Suppose that G^0 contains the kernel $\{0_E\} \times_{E/C} D$ of the first projection $G \to E$: then the isogeny of elliptic curves $G_0 \subset G \to E$ is finite locally free of the same degree d as $G \to E$. Since G^0 is a closed open subscheme of G, this implies that $G^0 = G$. The map $(p^\vee \iota^{-1} q, c \cdot \mathrm{id}) : F \to E \times_{E/C} F$ factors through G^0 and its image contains $\{0_E\} \times_{E/C} D$ (which is the image of D), whence the conclusion. □

Proposition 1.1.28 *Let $\mathscr{P}$ be a representable moduli problem of level N on $\mathbf{Ell}_R$. Let $m \geq 1$ be an integer coprime to N. Let $s', t' \geq 1$ be two coprime divisors of m, and $s, t \geq 1$ be divisors*

of s', t' respectively. Then the following diagram is Cartesian:

$$\begin{array}{ccc} \mathscr{M}(\mathscr{P}, [\Gamma_0(m)]_R) & \xrightarrow{D_{s,\frac{m}{s'}}} & \mathscr{M}(\mathscr{P}, [\Gamma_0\left(\frac{m}{s'}\right)]_R) \\ \downarrow{\scriptstyle D_{t,\frac{m}{t'}}} & & \downarrow{\scriptstyle D_{t,\frac{m}{s't'}}} \\ \mathscr{M}(\mathscr{P}, [\Gamma_0\left(\frac{m}{t'}\right)]_R) & \xrightarrow{D_{s,\frac{m}{s't'}}} & \mathscr{M}(\mathscr{P}, [\Gamma_0\left(\frac{m}{t's'}\right)]_R) \end{array}$$

Proof. – It is straightforward to check that the diagram commutes using [86, Lemma 3.5.1, Theorem 6.7.4]. Let s_∞, t_∞ be the greatest divisors of m which have the same prime divisors as s', t' respectively. Then $s_\infty, t_\infty, \frac{m}{s_\infty t_\infty}$ are pairwise coprime positive integers.

If C is a cyclic subgroup of some elliptic curve E/S, let $C[d]$ denote its standard cyclic subgroup of degree d.

Step 1: Surjectivity

Let

$$x_1 = (E_1/S, \alpha_1, C_1) \in \mathscr{M}(\mathscr{P}, [\Gamma_0(\frac{m}{t'})]_R)(S), x_2 = (E_2/S, \alpha_2, C_2) \in \mathscr{M}(\mathscr{P}, [\Gamma_0(\frac{m}{s'})]_R)(S)$$

be such that $D_{s,\frac{m}{s't'}}(x_1) = D_{t,\frac{m}{s't'}}(x_2)$.

Thus, there exists an isomorphism $\iota : E_1/C_1[s] \to E_2/C_2[t]$ identifying the standard cyclic subgroups of order $\frac{m}{s't'}$ of $C_1/C_1[s]$ and $C_2/C_2[t]$ such that

$$(\mathscr{P}\iota)(\alpha_1 \mod C_1[s]) = \alpha_2 \mod C_2[t].$$

Since s, t are pairwise coprime, $E = E_1 \times_{E_1/C_1[s]} E_2$ is a relative elliptic curve over S by Lemma 1.1.27. Let $\pi_i : E \to E_i$ be the natural projection: π_1, π_2 are isogenies of degrees t, s respectively. Let $\alpha \in \mathscr{P}(E/S)$ be such that $(\mathscr{P}\pi_1)(\alpha) = \alpha_1$: then

$$\begin{aligned}(\mathscr{P}\pi_2)(\alpha) \pmod{C_2[t]} &= (\mathscr{P}\iota)((\mathscr{P}\pi_1)(\alpha) \mod C_1[s]) = (\mathscr{P}\iota)(\alpha_1 \mod C_1[s]) \\ &= \alpha_2 \mod C_2[t],\end{aligned}$$

whence $(\mathscr{P}\pi_2)(\alpha) = \alpha_2$.

Since t is coprime to $\frac{m}{t_\infty}$ (resp. s is coprime to $\frac{m}{s_\infty}$), there exists a unique cyclic subgroup C_1' of order $\frac{m}{t_\infty}$ (resp. C_2' of order $\frac{m}{s_\infty}$) of E such that $\pi_1(C_1') = C_1[m/t_\infty]$ (resp. $\pi_2(C_2') = C_2[m/s_\infty]$).

Since $s \mid \frac{m}{t_\infty}$, $t \mid \frac{m}{s_\infty}$ and st is coprime to $\frac{m}{s_\infty t_\infty}$, one has

$$\begin{aligned}\iota(\pi_1\left(C_1'\left[\frac{m}{s_\infty t_\infty}\right]\right) \mod C_1[s]) &= \iota(C_1\left[\frac{m}{s_\infty t_\infty}\right] \mod C_1[s]) \\ &= \iota(C_1 \mod C_1[s])\left[\frac{m}{s_\infty t_\infty}\right] = (C_2 \mod C_2[t])\left[\frac{m}{s_\infty t_\infty}\right] \\ &= C_2\left[\frac{m}{s_\infty t_\infty}\right] \mod C_2[t] = \pi_2\left(C_2'\left[\frac{m}{s_\infty t_\infty}\right]\right),\end{aligned}$$

so that C_1' and C_2' have the same $\frac{m}{s_\infty t_\infty}$-torsion and there exists by [86, Lemma 3.5.1] a cyclic subgroup C of E with degree m such that $C\left[\frac{m}{t_\infty}\right] = C_1', C\left[\frac{m}{s_\infty}\right] = C_2'$.

We claim that

$$D_{s,\frac{m}{s'}}((E, \alpha, C)) = x_2,\ D_{t,\frac{m}{t'}}((E, \alpha, C)) = x_1.$$

It is enough to prove that

$$\ker \pi_1 = C[t],\ \ker \pi_2 = C[s],\ \pi_1(C[t_\infty])[\frac{t_\infty}{t'}] = C_1[\frac{t_\infty}{t'}],\ \pi_2(C[s_\infty])[\frac{s_\infty}{s'}] = C_2[\frac{s_\infty}{s'}].$$

Let $p_1 : E_1 \to E_1/C_1[s]$, $p_2 : E_2 \to E_2/C_2[t]$ be the projections, then

$$p_2 \circ \pi_2(C[t]) = p_2(\pi_2(C[t_\infty])[t]) = p_2(C_2[t_\infty][t]) = p_2(C_2[t]) = 0.$$

Similarly, the kernel of $p_2 \circ \pi_2 = \iota \circ p_1 \circ \pi_1$ contains $C[s]$. Thus $p_2 \circ \pi_2$ is an isogeny of degree st whose kernel contains the cyclic subgroup $C[s] + C[t] = C[st]$ of degree st: hence $C[st] \to \ker p_2 \circ \pi_2$ is a closed immersion of finite locally free S-schemes of same rank. Zariski-locally on S, it is a surjective morphism of two finite free $\mathcal{O}(S)$-modules of same rank, hence an isomorphism, whence $C[st] \to \ker p_2 \circ \pi_2$ is an isomorphism.

Since p_2, π_2 are composable cyclic isogenies of coprime degrees, by [86, Proposition 6.7.10], $\ker \pi_2$ is the standard cyclic subgroup of $\ker p_2 \circ \pi_2 = C[st]$ of degree $\deg \pi_2 = s$, so it is $C[s]$ by [86, Theorem 6.7.4]. Similarly, one has $\ker \pi_1 = C[t]$. The subgroups $\pi_1(C[t_\infty])[\frac{t_\infty}{t'}]$, $C_1[\frac{t_\infty}{t'}]$ are cyclic with degree dividing t_∞. Since p_1 has degree coprime to t_∞, they are equal if $p_1(\pi_1(C[t_\infty])[\frac{t_\infty}{t'}]) = p_1(C_1[\frac{t_\infty}{t'}])$. Now,

$$\begin{aligned} p_1(\pi_1(C[t_\infty])[\frac{t_\infty}{t'}]) &= \iota^{-1}(p_2 \circ \pi_2(C[t_\infty]))[\frac{t_\infty}{t'}] = \iota^{-1}(p_2(C_2[t_\infty])[\frac{t_\infty}{t'}]) \\ &= \iota^{-1}((C_2[t_\infty] \mod C_2[t])[\frac{t_\infty}{t'}]) = \iota^{-1}(C_2 \mod C_2[t])[\frac{m'}{s't'}][\frac{t_\infty}{t'}] \\ &= (C_1 \mod C_1[s])[\frac{m'}{s't'}][\frac{t_\infty}{t'}] = p_1(C_1[\frac{t_\infty}{t'}]), \end{aligned}$$

and the same holds for C_2, which concludes the proof of the claim.

Step 2: Injectivity

Let $z = (F, \beta, D) \in \mathscr{M}(\mathscr{P}, [\Gamma_0(m)]_R)(S)$ be such that $D_{s,\frac{m}{s'}}(z) = x_2, D_{t,\frac{m}{t'}}(z) = x_1$. Let us show that z is the same point as (E, α, C).

Since $D_{t,\frac{m}{t'}}((F, \beta, D)) = x_1$, there is a cyclic isogeny $j_1 : F \to E_1$ of degree t with kernel $D[t]$ such that $(\mathscr{P}j_1)(\beta) = \alpha_1$, $C_1 = j_1(D)[\frac{m}{t'}]$. Similarly, there is a cyclic isogeny $j_2 : F \to E_2$ of degree s with kernel $C[s]$ and such that $(\mathscr{P}j_2)(\beta) = \alpha_2$ and $C_2 = j_2(D)[\frac{m}{s'}]$.

The couple $j := (j_1, j_2) : F \to E = E_1 \times_{E_1/C_1[s]} E_2$ is a morphism of S-elliptic curves with $\pi_1 \circ j = j_1$, so j is an isogeny of degree one, i.e. an isomorphism. In particular,

$$(\mathscr{P}j)(\beta) = (\mathscr{P}\pi_1)^{-1}(\mathscr{P}j_1)(\beta) = (\mathscr{P}\pi_1)^{-1}\alpha_1 = \alpha.$$

The subgroup scheme $C' := j(D)$ of E is cyclic of degree m. To prove that $C = C'$, it is thus enough to find two integers a, b with least common multiple m such that $C'[a] = C[a]$ and $C'[b] = C[b]$. Now, one has $\pi_1(C')[\frac{m}{t'}] = j_1(D)[\frac{m}{t'}] = C_1[\frac{m}{t'}]$, so $\pi_1(C'[\frac{m}{t_\infty}]) = C_1[\frac{m}{t_\infty}] = \pi_1(C[\frac{m}{t_\infty}])$. Since π_1 has degree prime to $\frac{m}{t_\infty}$, one has $C'[\frac{m}{t_\infty}] = C[\frac{m}{t_\infty}]$. Similarly, $C'[\frac{m}{s_\infty}] = C[\frac{m}{s_\infty}]$, whence $C = C'$, which concludes the proof. □

Proposition 1.1.29 *Let m be a positive integer and $d \mid m$ be positive and prime to $\frac{m}{d}$. For any representable moduli problem $\mathscr{P}$ on $\mathbf{Ell}_R$ of level coprime to m, there is an* Atkin-Lehner automorphism *w_d of $\mathscr{M}(\mathscr{P}, [\Gamma_0(m)]_R)$ defined by the following rule. Let E/S be an elliptic curve endowed with a cyclic subgroup C of order m, and $\alpha \in \mathscr{P}(E/S)$. Let $C_d, C_{\frac{m}{d}}$ be the cyclic subgroups of C of respective degrees $d, \frac{m}{d}$, $\pi : E \to E'$ the cyclic isogeny of kernel C_d. Let C' the finite flat S-subgroup scheme of $E'[m]$ of degree m defined as follows: its d-torsion is the kernel of $\pi^\vee$, and its $\frac{m}{d}$-torsion is $\pi(C) = \pi(C_{\frac{m}{d}})$. Then w_d maps $(E/S, \alpha, C)$ to $(E'/S, \pi(\alpha), C')$.*

Furthermore,

- *The formation of any w_d is natural with respect to $\mathscr{P}$ (for morphisms of representable moduli problems of level N coprime to m, such as the action of $(\mathbb{Z}/N\mathbb{Z})^\times$) and commutes with base change,*

– *If $d, d' \mid m$ are positive integers such that d is coprime to $\frac{m}{d}$ and d' is coprime to $\frac{m}{d'}$, then one has $w_d \circ w_{d'} = [\delta] \circ w_{\frac{dd'}{\delta^2}}$, where δ is the greatest common divisor of d, d'.*
– *If $d, t \mid m$ are positive integers such that $dt \mid m$ and d coprime to $\frac{m}{d}$, then $D_{d,t} = D_{1,t} \circ w_d$.*

Proof. – That the definition constructs a morphism of R-schemes of $\mathscr{M}(\mathscr{P}, [\Gamma_0(m)]_R)$ into itself follows from [86, Lemma 3.5.1, Theorem 6.7.4]. In fact, since d and $\frac{m}{d}$ are coprime, we do not need to involve in this case the notion of standard subgroup; we will use freely the combination of these results throughout the proof. The naturality and commutation to base change is immediate. As in the previous proof, if D is a cyclic subgroup of order k of some elliptic curve F/T, and $\ell \geq 1$ is a divisor of k, then $D[\ell]$ denotes the standard cyclic subgroup of D of order ℓ.

Note that the last identity is a direct computation.

To check that the w_d are automorphisms, it is enough to prove that $w_d \circ w_{d'} = [\delta] \circ w_{\frac{dd'}{\delta^2}}$ when d, d' are prime powers, which we now assume.

When $d = d'$, w_d maps a triple $(E/S, \alpha, C)$ to $(E'/S, \pi(\alpha), C')$, where $\pi : E \to E' = E/C[d]$ is the cyclic isogeny of degree d whose kernel is exactly the d-torsion subgroup of C, and C' is the subgroup $\pi(C) + \ker \pi^\vee$ (by [86, Lemma 3.5.1, Theorem 6.7.4]). Thus

$$\begin{aligned} w_d^2(E/S, \alpha, C) &= (E'/C'[d], (\pi^\vee \circ \pi)(\alpha), \pi^\vee(C')) = (E'/\ker \pi^\vee, [d]\alpha, \pi^\vee(\pi(C)) + \ker (\pi^\vee)^\vee) \\ &= (E/S, [d]\alpha, dC + C[d]) = [d](E/S, \alpha, C). \end{aligned}$$

When $d \neq d'$ (so that $d, d', \frac{m}{dd'}$ are pairwise coprime), $w_{d'}$ maps a triple $(E/S, \alpha, C)$ to $(E_1/S, \pi_1(\alpha), C_1)$, where $\pi_1 : E \to E_1$ is the isogeny whose kernel is the d'-torsion of C, and $C_1 = \ker \pi_1^\vee + \pi_1(C)$; then $w_d(E_1/S, \pi_1(\alpha), C_1) = (E_2/S, \pi_2(\pi_1(\alpha)), C_2)$, where $\pi_2 : E_1 \to E_2$ is the isogeny whose kernel is the d-torsion of C_1, and $C_2 = \ker \pi_2^\vee + \pi_2(C_1)$.

Since $\pi_2 \circ \pi_1$ is an isogeny of degree dd', we need to prove that $\ker \pi_2 \circ \pi_1 = C[dd']$, that $C_2 \left[\frac{m}{dd'}\right] = \pi_2(\pi_1(C))$, and that $C_2[dd'] = \ker \pi_1^\vee \circ \pi_2^\vee$.

One has $C_2 \left[\frac{m}{dd'}\right] = C_2 \left[\frac{m}{d}\right] \left[\frac{m}{dd'}\right] = \pi_2(C_1) \left[\frac{m}{dd'}\right]$. Since π_1, π_2 have degree coprime to $\frac{m}{dd'}$, one thus has

$$C_2 \left[\frac{m}{dd'}\right] = \pi_2(C_1 \left[\frac{m}{dd'}\right]) = \pi_2(\pi_1(C) \left[\frac{m}{dd'}\right]) = (\pi_2 \circ \pi_1)(C) \left[\frac{m}{dd'}\right].$$

Since π_1, π_2 have coprime degrees and are cyclic, $\pi_2 \circ \pi_1$ is cyclic by [86, Proposition 6.7.10], and its kernel $K = \pi_1^{-1}(C_1[d]) = \pi_1^{-1}(\pi_1(C)[d])$ is such that $C[d]$ is its (standard) cyclic subgroup of degree d. Thus $K = \pi_1^{-1}(\pi_1(C))[d] = \ker \pi_1 + C[d'] = C[dd']$.

Furthermore, $\ker \pi_1^\vee \circ \pi_2^\vee$ is a cyclic subgroup of E_2 of degree dd'. Since π_1 has degree prime to d, $(\ker \pi_1^\vee \circ \pi_2^\vee)[d] = (\ker \pi_2^\vee)[d] = C_2[d]$. Since π_2 has degree prime to d', $(\ker \pi_1^\vee \circ \pi_2^\vee)[d']$ is equal to the pre-image in $E_2[d']$ under $\pi_2^\vee$ of $\ker \pi_1^\vee = C_1[d']$. Since

$$(\pi_2^\vee)^{-1}(C_1[d']) = (\pi_2^\vee)^{-1}(\pi_2^{-1}(\pi_2(C_1[d']))) = (d)^{-1}C_2[d'] = C_2[d']$$

(where all pre-images are being taken inside the d'-torsion), it follows that $\ker \pi_1^\vee \circ \pi_2^\vee = C_2[dd']$, which concludes. □

Proposition 1.1.30 *Let $\mathscr{P}$ be a representable moduli problem on $\mathbf{Ell}_R$ of level N and $m, m' \geq 1$ be such that N, m, m' are pairwise coprime. Let $\mathscr{P}' = \mathscr{P} \times [\Gamma_0(m)]_R$. There is a natural (with respect to $\mathscr{P}$ and morphisms of moduli problems of level coprime to mm') isomorphism of moduli problems (of level Nmm', and over $\mathscr{P}$) $\mathscr{P}' \times [\Gamma_0(m')]_R \simeq \mathscr{P} \times [\Gamma_0(mm')]_R$.*

Let $d, r, s \geq 1$ be divisors of m' such that d and $\frac{m'}{d}$ are coprime and $rs \mid m'$. Then, under the

above isomorphism, the following diagrams commute:

$$\begin{array}{ccccc}
\mathscr{M}(\mathscr{P}', [\Gamma_0(m')]_R) & \xleftarrow{w_d(\mathscr{P}', [\Gamma_0(m')]_R)} & \mathscr{M}(\mathscr{P}', [\Gamma_0(m')]_R) & \xrightarrow{D_{r,s}(\mathscr{P}', [\Gamma_0(m')]_R)} & \mathscr{M}(\mathscr{P}', [\Gamma_0(s)]) \\
\downarrow\sim & & \downarrow\sim & & \downarrow\sim \\
\mathscr{M}(\mathscr{P}, [\Gamma_0(mm')]_R) & \xleftarrow{w_d(\mathscr{P}, [\Gamma_0(mm')]_R)} & \mathscr{M}(\mathscr{P}, [\Gamma_0(mm')]_R) & \xrightarrow{D_{r,sm}(\mathscr{P}, [\Gamma_0(mm')]_R)} & \mathscr{M}(\mathscr{P}, [\Gamma_0(sm)]_R)
\end{array}$$

Proof. – This is completely formal, using [86, Lemma 3.5.1, Theorem 6.7.4] for the relevant results on cyclic subgroups. □

Corollary 1.1.31 *Let $\mathscr{P}$ be a representable moduli problem on $\mathbf{Ell}_R$ of level N, let $m \geq 1$ be coprime to N, and let $d, t \mid m$ be positive divisors such that $td \mid m$. Then $D_{d,t}$ is finite locally free, and étale above $\mathbb{Z}[1/m]$.*

Proof. – When $d = 1$, finiteness (resp. étaleness above $\mathbb{Z}[1/m]$) follows from the fact that $D_{1,t}$ is a morphism of finite locally free $\mathscr{M}(\mathscr{P})$-schemes (resp. finite étale $\mathscr{M}(\mathscr{P})$-schemes above $\mathbb{Z}[1/m]$) by [86, Theorem 5.1.1]. For arbitrary d, it is formal to check that $D_{1,1} \circ D_{d,t} = D_{1,1} \circ w_d \circ D_{1,d}$, so that the composition $D_{1,1} \circ D_{d,t}$ is finite (resp. étale above $\mathbb{Z}[1/m]$), hence $D_{d,t}$ is finite (resp. étale above $\mathbb{Z}[1/m]$). To prove flatness and finite presentation, first assume that $\mathscr{P} = [\Gamma(\ell)]_{\mathbb{Z}[1/\ell]}$ for some prime $\ell \nmid 2m$.

In this case, finite presentation is automatic, the moduli schemes are regular affine with every nonempty open subset of dimension 2 (because $\mathscr{P}$ is a modular family and the moduli problems $[\Gamma_0(s)]_{\mathbb{Z}}$ are regular by [86, Theorem 5.1.1]), and $D_{d,t}$ is finite, so the miracle flatness theorem [4, Lemma 00R4] applies and we are done.

Let us treat the general case. The claim is Zariski-local with respect to R, so we may assume that there exists a prime $\ell \nmid 2Nm$ invertible in R. Since $[\Gamma(\ell)]_{\mathbb{Z}[1/\ell]}$ is representable finite étale locally of constant rank over $\mathbf{Ell}_{\mathbb{Z}[1/\ell]}$, for any divisor $s \geq 1$ of m, the forgetful map $\mathscr{M}(\mathscr{P} \times [\Gamma(\ell)]_R, [\Gamma_0(s)]_R) \to \mathscr{M}(\mathscr{P}, [\Gamma_0(s)]_R)$ is finite étale surjective. By Proposition 1.1.26, the two squares in the following diagram are Cartesian.

$$\begin{array}{ccccc}
\mathscr{M}(\mathscr{P}, [\Gamma_0(m)]_R) & \longleftarrow & \mathscr{M}(\mathscr{P} \times [\Gamma(\ell)], [\Gamma_0(m)]_R) & \longrightarrow & \mathscr{M}([\Gamma(\ell)]_R, [\Gamma_0(m)]_R) \\
\downarrow D_{d,t} & & \downarrow D_{d,t} & & \downarrow D_{d,t} \\
\mathscr{M}(\mathscr{P}, [\Gamma_0(t)]_R) & \longleftarrow & \mathscr{M}(\mathscr{P} \times [\Gamma(\ell)]_R, [\Gamma_0(t)]_R) & \longrightarrow & \mathscr{M}([\Gamma(\ell)]_R, [\Gamma_0(t)]_R)
\end{array}$$

Therefore, the special case above shows that the rightmost vertical arrow is finite locally free, thus the same holds for the middle vertical arrow by base change, and thus for the leftmost vertical arrow as well by fpqc descent. □

1.1.3 Degeneracies for $\Gamma_1(N)$-structures

Definition 1.1.32 Let $N \geq 1$ be an integer, and $r \mid N$ be a positive divisor. Let R be a $\mathbb{Z}[1/N]$-algebra. The moduli problem $\mathscr{P} = [\Gamma_1'(N, r)]_R$ on $\mathbf{Ell}_R$ is defined as follows: given a relative elliptic curve E/S, $\mathscr{P}(E/S)$ is the collection of couples (P, C), where $P \in E(S)$ has exact order N, C is a cyclic subgroup of E/S of order r such that the image of P in $(E/C)(S)$ has exact order N.

Proposition 1.1.33 *Let $N, r \geq 1$ with $r \mid N$ and R be a $\mathbb{Z}[1/N]$-algebra. Then $\mathscr{P} = [\Gamma_1'(N, r)]_R$ is relatively representable and finite étale of constant rank. It is endowed with a natural level N structure. It is representable if $N \geq 4$.*

Proof. – By Proposition 1.1.10, we may assume that $R = \mathbb{Z}[1/N]$. If $N \geq 4$, since $\mathscr{P}$ is a subfunctor of the representable finite étale moduli problem $\mathscr{P}' = [\Gamma_1(N)]_R \times [\Gamma_0(r)]_R$ (by [86, Corollary 2.7.4, Theorem 5.1.1] and Proposition 1.1.12), $\mathscr{P}$ is rigid.

Next, we show that for any relative elliptic curve E/S, the subsheaf $T \longmapsto \mathscr{P}(E_T/T)$ of $T \longmapsto \mathscr{P}'(E_T/T)$ is representable by a closed open subscheme of $\mathscr{P}'_{E/S}$. We define a map from $\mathscr{P}'_{E/S}$ to a disjoint union of copies S_d of S indexed by divisors d of N as follows: for any $(P,C) \in \mathscr{P}'(E_T/T)$, the image of P in the S-elliptic curve E_T/C is a section of the finite étale T-group scheme $(E_T/C)[N]$ of constant rank. Therefore, its fibrewise order ω is a locally constant function on T, its values divide N, and the formation of ω commutes with respect to base change. Then we map $(P,C) \in \mathscr{P}'(E/S)$ to the structure map $\omega^{-1}(d) \subset T \to S \simeq S_d$ for each $d \mid N$. Thus $\mathscr{P}(E/S)$ corresponds to the inverse image of S_N, whence the conclusion. □

Proposition 1.1.34 *Let $N, r \geq 1$ be integers with $r \mid N$ and R be a $\mathbb{Z}[1/N]$-algebra. Let $\mathscr{P}$ be a relatively representable moduli problem on $\mathbf{Ell}_R$ of level prime to N. Assume that $\mathscr{P}$ is representable or that $N \geq 4$. Let $s, t \geq 1$ be such that $st \mid r$.*

There exists a degeneracy map $D'_{s,t} : \mathscr{M}(\mathscr{P}, [\Gamma'_1(N,r)]_R) \to \mathscr{M}(\mathscr{P}, [\Gamma'_1(N,t)]_R)$ *defined by the following rule. Given an elliptic curve E/S and a couple $(\alpha, (P,C)) \in (\mathscr{P} \times [\Gamma'_1(N,r)]_R)(E/S)$, let C' be the standard subgroup of C of order s, and $\pi : E \to E' := E/C'$ the natural (étale) isogeny. Then $D'_{s,t}$ maps the point $(E/S, \alpha, (P,C))$ to $(E'/S, (\mathscr{P}\pi)(\alpha), (\pi(P), \pi(C)[t]))$, where $\pi(C)[t]$ is the standard cyclic subgroup of order t of the cyclic subgroup $\pi(C)$ of order r/s.*

Proof. – One still needs to check that $\pi(P)$ has exact order N and that the image of $\pi(P)$ in $E'/\pi(C)[t]$ has exact order N. Since N is invertible in R, everything can be checked fibrewise. Note that we have a successive composition $\pi_\infty : E \to E' \to E'/\pi(C)[t] \to E/C$ of étale isogenies, and that $P, \pi_\infty(P)$ both have exact order N, whence the conclusion. □

Lemma 1.1.35 *Let $N, r \geq 1$, R and $\mathscr{P}$ are as in Proposition 1.1.34. Let $s, t, u, v \geq 1$ be integers with $st \mid r$, and $uv \mid t$. Then the composition $D'_{u,v} \circ D'_{s,t}$ is exactly $D'_{su,t}$.*

Proof. – This is a direct verification. □

Proposition 1.1.36 *Let $N, r, s, t \geq 1$ and R be as in Proposition 1.1.34, and let $F : \mathscr{P} \Rightarrow \mathscr{P}'$ be a morphism of relatively representable (representable if $N \leq 3$) moduli problems of level coprime to N over $\mathbf{Ell}_R$. Then the following diagram is Cartesian:*

$$\begin{array}{ccc} \mathscr{M}(\mathscr{P}, [\Gamma'_1(N,r)]_R) & \xrightarrow{D'_{s,t}} & \mathscr{M}(\mathscr{P}, [\Gamma'_1(N,t)]_R) \\ \downarrow F & & \downarrow F \\ \mathscr{M}(\mathscr{P}', [\Gamma'_1(N,r)]_R) & \xrightarrow{D'_{s,t}} & \mathscr{M}(\mathscr{P}', [\Gamma'_1(N,t)]_R) \end{array}$$

Proof. – Let E be an elliptic curve over a R-scheme S and $\alpha \in \mathscr{P}(E/S)$.

Let $(P,C) \in [\Gamma'_1(N,r)]_R(E/S)$, then

$$\begin{aligned} F(D'_{s,t}((E,\alpha,(P,C)))) &= F((E/C[s], \alpha \mod C[s], (P \mod C[s], C[st]/C[s]))) \\ &= (E/C[s], F(\alpha \mod C[s]), (P \mod C[s], C[st]/C[s])), \end{aligned}$$

where $[n]$ means taking the standard cyclic subgroup of order n.

On the other hand, since F has level prime to N, it is functorial with respect of isogenies of degree dividing N, so that

$$\begin{aligned} D'_{s,t}(F((E,\alpha,(P,C)))) &= D'_{s,t}((E, F(\alpha), (P,C))) \\ &= (E/C[s], F(\alpha) \mod C[s], (P \mod C[s], C[st]/C[s])) \\ &= F(D'_{s,t}((E,\alpha,(P,C)))). \end{aligned}$$

Thus the diagram commutes. We then show that for any R-scheme S, the following diagram

is Cartesian.

$$\begin{array}{ccc} \mathscr{M}(\mathscr{P}, [\Gamma'_1(N,r)]_R)(S) & \xrightarrow{D'_{s,t}} & \mathscr{M}(\mathscr{P}, [\Gamma'_1(N,t)]_R)(S) \\ \downarrow F & & \downarrow F \\ \mathscr{M}(\mathscr{P}', [\Gamma'_1(N,r)]_R)(S) & \xrightarrow{D'_{s,t}} & \mathscr{M}(\mathscr{P}', [\Gamma'_1(N,t)]_R)(S) \end{array}$$

Indeed, let

$$x_1 = (E_1, \alpha', (P_1, C_1)) \in \mathscr{M}(\mathscr{P}', [\Gamma'_1(N,r)]_R)(S),\ x_2 = (E_2, \beta, (P_2, C_2)) \in \mathscr{M}(\mathscr{P}, [\Gamma'_1(N,t)]_R)(S)$$

be two points with $F(x_2) = D'_{s,t}(x_1)$. Thus, there exists an isogeny $\pi : E_1 \to E_2$ such that $\ker \pi = C_1[s]$, $(\mathscr{P}'\pi)(\alpha') = F(\beta)$, $\pi(P_1) = P_2$ and $C_2 = \pi(C_1[st])$. In particular, we can define $\alpha = (\mathscr{P}\pi)^{-1}(\beta)$, so that $(\mathscr{P}'\pi)F(\alpha) = F((\mathscr{P}\pi)(\alpha)) = F(\beta) = (\mathscr{P}'\pi)(\alpha')$, hence $F(\alpha) = \alpha'$. Thus $x_0 := (E_1, \alpha, (P_1, C_1)) \in \mathscr{M}(\mathscr{P}, [\Gamma'_1(N,r)]_R)(S)$ is such that $F(x_0) = x_1$. But one immediately checks by construction that $D'_{s,t}(x_0) = x_2$.

Let $y_0 = (E_0, \alpha_0, (P_0, C_0)) \in \mathscr{M}(\mathscr{P}, [\Gamma'_1(N,r)]_R)(S)$ such that $F(y_0) = x_1$ and $D'_{s,t}(y_0) = x_2$. This means that there is an isomorphism $\iota : E_0 \to E_1$ such that $F((\mathscr{P}\iota)(\alpha_0)) = \alpha'$, $\iota(P_0) = P_1$, $\iota(C_0) = C_1$, and an isogeny $g : E_0 \to E_2$ such that $\ker g = C_0[u]$, $\beta = (\mathscr{P}g)(\alpha_0)$, $C_2 = \pi(C_0[uv])$, $P_2 = \pi(P_0)$. Since $\pi \circ \iota$ and g are isogenies with the same kernel and same target, there is an automorphism ψ of E_2 such that $\psi \circ g = \pi \circ \iota$.

Let us prove that ψ is the identity, since $\mathscr{P}' \times [\Gamma_1(N)]_R$ is rigid, it is enough to show that $(\mathscr{P}'g)(F(\alpha_0)) = (\mathscr{P}'\pi) \circ (\mathscr{P}'\iota)(F(\alpha_0))$, and that $g(P_0) = \pi(\iota(P_0))$. Indeed, one has

$$\begin{aligned} (\mathscr{P}'\pi) \circ (\mathscr{P}'\iota)(F(\alpha_0)) = (\mathscr{P}'\pi) \circ F((\mathscr{P}\iota)(\alpha_0)) = (\mathscr{P}'\pi)(\alpha') = F(\beta) = (\mathscr{P}'g)(F(\alpha_0)), \\ \pi(\iota(P_0)) = \pi(P_1) = P_2 = g(P_0). \end{aligned}$$

Thus $\pi \circ \iota = g$. Thus $(\mathscr{P}\iota)(\alpha_0) = (\mathscr{P}\pi)^{-1}(\mathscr{P}g)(\alpha_0) = (\mathscr{P}\pi)^{-1}(\beta) = \alpha$, and $\iota : y_0 \to x_0$ is an isomorphism. □

Corollary 1.1.37 *In the situation of Proposition 1.1.34, $D'_{s,t}$ is finite étale.*

Proof. – Suppose first that $k \geq 3$ is coprime to N, $R = \mathbb{Z}[1/(Nk)]$ and that $\mathscr{P} = [\Gamma(k)]_R$. Consider the following diagram, where f, g are forgetful maps, finite étale (they are compositions of closed open immersions by the proof of Proposition 1.1.33 and forgetting the $[\Gamma_1(N)]_R$ component, which is finite étale):

$$\begin{array}{ccc} \mathscr{M}([\Gamma(k)]_R, [\Gamma'_1(N,r)]_R) & \xrightarrow{f} & \mathscr{M}([\Gamma(k)]_R, [\Gamma_0(r)]_R) \\ \downarrow D'_{s,t} & & \downarrow D_{s,t} \\ \mathscr{M}([\Gamma(k)]_R, [\Gamma'_1(N,t)]_R) & \xrightarrow{g} & \mathscr{M}([\Gamma(k)]_R, [\Gamma_0(t)]_R) \end{array}$$

Since $D_{s,t}$ is finite étale by Corollary 1.1.31, $D'_{s,t}$ is finite étale.

Let us come back to the general case. The statement is Zariski-local with respect to R, so we may assume that some integer $k \geq 3$ coprime to N is invertible in R. Then both squares in the following diagram are Cartesian, with all vertical maps being $D'_{s,t}$:

$$\begin{array}{ccccc} \mathscr{M}([\Gamma(k)]_R, [\Gamma'_1(N,r)]_R) & \longleftarrow & \mathscr{M}([\Gamma(k)]_R, [\Gamma'_1(N,r)]_R, \mathscr{P}) & \xrightarrow{\delta_r} & \mathscr{M}(\mathscr{P}, [\Gamma'_1(N,r)]_R) \\ \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\ \mathscr{M}([\Gamma(k)]_R, [\Gamma'_1(N,t)]_R) & \longleftarrow & \mathscr{M}([\Gamma(k)]_R, [\Gamma'_1(N,t)]_R, \mathscr{P}) & \xrightarrow{\delta_t} & \mathscr{M}(\mathscr{P}, [\Gamma'_1(N,t)]_R) \end{array}$$

By what we already saw, α is étale, thus so is β. Since $[\Gamma(k)]_R$ is finite étale over $\mathbf{Ell}_{\mathbb{Z}[1/k]}$,

δ_r, δ_t are finite étale. Thus, by étale descent, γ is finite étale and we are done. □

Proposition 1.1.38 *Let $N, r, s, t \geq 1$ be as in Definition 1.1.34 and $\mathscr{P}$ be a relatively representable moduli problem of level L coprime to N, representable if $N \leq 3$. Let $m \geq 1$ be coprime to NL. Then, for any $u, v \geq 1$ such that $uv \mid m$, the following diagram is Cartesian:*

$$\begin{array}{ccc} \mathscr{M}(\mathscr{P}, [\Gamma_1'(N,r)]_R, [\Gamma_0(m)]_R) & \xrightarrow{D'_{s,t}} & \mathscr{M}(\mathscr{P}, [\Gamma_1'(N,t)]_R, [\Gamma_0(m)]_R) \\ \downarrow{\scriptstyle D_{u,v}} & & \downarrow{\scriptstyle D_{u,v}} \\ \mathscr{M}(\mathscr{P}, [\Gamma_1'(N,r)]_R, [\Gamma_0(v)]_R) & \xrightarrow{D'_{s,t}} & \mathscr{M}(\mathscr{P}, [\Gamma_1'(N,t)]_R, [\Gamma_0(v)]_R) \end{array}$$

Proof. – Step 1: The diagram commutes.

Let S be a R-scheme, and $x := (E/S, \alpha, (P, C), D) \in \mathscr{M}(\mathscr{P}, [\Gamma_1'(N,r)]_R, [\Gamma_0(m)]_R)(S)$. Let us prove that $D_{u,v}(D'_{s,t}(x)) = D'_{s,t}(D_{u,v}(x))$.

Let $\pi_s : E \to E/C[s]$ be the natural isogeny of degree s. One has

$$D'_{s,t}(x) = (E/C[s], (\mathscr{P}\pi_s)(\alpha), (\pi_s(P), \pi_s(C)[t]), \pi_s(D)),$$

where, as above, $[\cdot]$ denotes the standard cyclic subgroup of given degree. Note that $C[s]+D$ is a cyclic subgroup of E of degree sm by the factorization lemma [86, (3.5)], so $\pi_s(D) = \pi_s(D + C_s)$ is indeed a cyclic subgroup of degree d by [86, Theorem 6.7.4]. Let $\pi_{s,u}$ denote the quotient isogeny $E/C[s] \to (E/(C[s]))/\pi_s(D)[u]$. Then, with $\pi^1 = \pi_{s,u} \circ \pi_s : E \to (E/(C[s]))/(\pi_s(D)[u])$ the cyclic isogeny (by [86, Proposition 6.7.10]) of kernel $C[s] + D[u]$, one has:

$$\begin{aligned} D_{u,v}(D'_{s,t}(x)) &= \Big((E/C[s])/\pi_s(D)[u], \quad (\mathscr{P}\pi_{s,u})(\mathscr{P}\pi_s)(\alpha), ((\pi_{s,u}(\pi_s(P)), \pi_{s,u}(\pi_s(C)[t]))), \\ &\qquad\qquad \pi_{s,u}(\pi_s(D))[v]\Big) \\ &= \Big((E/C[s])/\pi_s(D)[u], \quad (\mathscr{P}\pi^1)(\alpha), (\pi^1(P), \pi^1(C + D[u])[t]), \\ &\qquad\qquad \pi^1(C[s] + D)[t]\Big). \end{aligned}$$

Similarly, if $\pi_u : E \to E/C[u]$ is the natural isogeny and $\pi^2 : E \to (E/D[u])/\pi_u(C)[s]$ is the composition of π_u and the quotient by $\pi_U(C)[s]$, one sees that

$$D'_{s,t}(D_{u,v}(x)) = ((E/D[u])/\pi_u(C)[s], (\mathscr{P}\pi^2)(\alpha), (\pi^2(P), \pi^2(C + D[u])[t]), \pi^2(C[s] + D)[t])$$

Since π^1, π^2 are isogenies from E with the same kernel, there is an isomorphism

$$\iota : (E/(C[s]))/(\pi_s(D)[u]) \to (E/D[u])/\pi_u(C)[s]$$

such that $\iota \circ \pi^1 = \pi^2$, so the diagram commutes.

Step 2: Injectivity

Suppose we have points

$$x = (E, \alpha, (P, C), D), x' = (E', \alpha', (P', C'), D') \in \mathscr{M}(\mathscr{P}, [\Gamma_1'(N,r)]_R, [\Gamma_0(m)]_R)(S)$$

such that $D'_{s,t}(x) = D'_{s,t}(y)$ and $D_{u,v}(x) = D_{u,v}(x')$. Then there are isomorphisms

$$\begin{aligned} &j_s : E/C[s] \to E/C'[s], \quad (\alpha, P, C, D) \mod C[s] \mapsto (\alpha', P', C', D') \mod C'[s], \\ &j_u : E/D[u] \to E'/D'[u], \quad (\alpha, P, C, D) \mod D[u] \mapsto (\alpha', P', C', D') \mod D'[u]. \end{aligned}$$

The assumptions imply that the two compositions

$$c_s : E \to E/C[s] \xrightarrow{j_s} E'/C'[s] \to E'/(C'[s] + D'[u]),$$
$$c_u : E \to E/D[u] \xrightarrow{j_u} E'/D'[u] \to E'/(C'[s] + D'[u])$$

have the same kernel $C[s] + D[u]$, so they differ by an automorphism λ of $E'/(C'[s] + D'[u])$. By construction,

$$(\alpha', P') \mod C'[s] + D'[u] \in (\mathscr{P} \times [\Gamma_1(N)]_R)(E'/(C'[s] + D'[u]))$$

is fixed by the automorphism λ: since $\mathscr{P} \times [\Gamma_1(N)]_R$ is rigid, λ is the identity and $c_s = c_u$.

Since $E' \to E'/C'[s] \times_{E'/(C'[s]+D'[u])} E'/D'[u]$ is an isomorphism (it is a morphism of elliptic curves, and its kernel is contained in $C'[s]$ and in $D'[u]$, so it is a monomorphism thus an isomorphism), the couple $(E \to E/C[s] \xrightarrow{j_s} E'/C'[s], E \to E/D[u] \xrightarrow{j_u} E'/D'[u])$ defines an morphism $j : E \to E'$ of elliptic curves. The composition of j with the cyclic isogeny $E' \to E'/C'[s]$ of degree s is exactly $E \to E/C[s] \xrightarrow{j_s} E'/C'[s]$, which is an isogeny of degree s. So j is not zero on any fibre, hence it is an isogeny of degree $\frac{s}{s} = 1$, i.e. an isomorphism.

Now, $(\mathscr{P}j)(\alpha) \mod C'[s] = (\mathscr{P}j_s)(\alpha \mod C[s]) = \alpha' \mod C'[s]$, and since $\mathscr{P}$ has level prime to s, $(\mathscr{P}j)(\alpha) = \alpha'$. The same reasoning shows that $(\mathscr{P}j)(D) = D'$. To prove that $(\mathscr{P}j)(P) = P'$ and $(\mathscr{P}j)(C) = C'$, one quotients instead by $D'[u]$, since $[\Gamma'_1(N, r)]_R$ has level prime to u.

Step 3: Surjectivity

Let finally

$$x_1 = (E_1, \alpha_1, (P_1, C_1), D_1) \in \mathscr{M}(\mathscr{P}, [\Gamma'_1(N, r)]_R, [\Gamma_0(v)]_R)(S),$$
$$x_2 = (E_2, \alpha_2, (P_2, C_2), D_2) \in \mathscr{M}(\mathscr{P}, [\Gamma'_1(N, t)]_R, [\Gamma_0(m)]_R)(S)$$

be two points with the same image in $\mathscr{M}(\mathscr{P}, [\Gamma'_1(N, t)]_R, [\Gamma_0(v)]_R)(S)$. We want to prove that there exists $x_0 \in \mathscr{M}(\mathscr{P}, [\Gamma'_1(N, r)]_R, [\Gamma_0(m)]_R)(S)$ with $D_{u,v}(x_0) = x_1$, $D'_{s,t}(x_0) = x_2$.

The assumption means that there exists an isomorphism $\iota : E_1/C_1[s] \to E_2/D_2[u]$ mapping $\alpha_1 \mod C_1[s]$ to $\alpha_2 \mod D_2[u]$, $P_1 \mod C_1[s]$ to $P_2 \mod D_2[u]$, $(C_1 \mod C_1[s])[t] = C_2 \mod D_2[u]$, $D_1 \mod C_1[s] = (D_2 \mod D_2[u])[v]$.

The scheme $E_0 = E_1 \times_{E_1/C_1[s]} E_2$ is a relative elliptic curve over S; moreover, the projections $\pi_1 : E_0 \to E_1, \pi_2 : E_0 \to E_2$ are cyclic isogenies of degrees u, s respectively. The assumptions imply that $(\mathscr{P}\pi_1)^{-1}(\alpha_1) = (\mathscr{P}\pi_2)^{-1}(\alpha_2)$ (because they have the same image in $E_1/C_1[s] \simeq E_2/D_2[u]$, through an isogeny of degree su prime to the level of $\mathscr{P}$), and let $\alpha_0 \in \mathscr{P}(E_0/S)$ denote this element. Let $P_0 \in E_0(S)$ be the point (P_1, P_2), then P_0 has exact order N because so have P_1 and P_2. Because u is coprime to r (resp. s is coprime to m), there is a unique cyclic subgroup C_0 (resp. D_0) of E_0 of order r (resp. m) such that $\pi_1(C_0) = C_1$. (resp. $\pi_2(D_0) = D_2$).

We claim that $x_0 = (E_0, \alpha_0, (P_0, C_0), D_0) \in \mathscr{M}(\mathscr{P}, [\Gamma_1(N, r)]_R, [\Gamma_0(m)]_R)(S)$ is such that $D'_{s,t}(x_0) = x_2$ and $D_{u,v}(x_0) = x_1$.

To check that $x_0 \in \mathscr{M}(\mathscr{P}, [\Gamma_1(N, r)]_R, [\Gamma_0(m)]_R)(S)$, the only remaining assertion to check is that $P_0 \mod C_0$ has exact order N. Suppose that (in any geometric fibre) $dP_0 \mod C_0 = 0$: then $dP_0 \in C_0$. Then, after applying π_1, we find that $dP_1 \in C_1$, hence $dP_1 \mod C_1 = 0$, so $N \mid d$, and we are done.

By construction, $\pi_1 : E_0 \to E_1$ (resp. $\pi_2 : E_0 \to E_2$) is an isogeny of degree u (resp. s) mapping P_0 to P_1 (resp. P_2), α_0 to α_1 (resp. α_2) and C_0 to C_1 (resp. D_0 to D_2). So all we need to check is that $\ker \pi_1 = D_0[u]$ and $D_1 = \pi_1(D_0)[v]$, $\ker \pi_2 = C_0[s]$ and $C_2 = \pi_2(C_0)[t]$.

The map $q_1 : E_0 \xrightarrow{\pi_1} E_1 \to E_1/C_1[s]$ is an isogeny of degree su; its kernel contains $C_0[s]$ because $\pi_1(C_0[s]) = \pi_1(C_0)[s] = C_1[s]$. Similarly, the map $q_2 : E_0 \xrightarrow{\pi_2} E_2 \to E_2/D_2[u]$ is an

isogeny of degree su and its kernel contains $D_0[u]$. Since $q_2 = \iota \circ q_1$, q_1 and q_2 have the same kernel Q, which is a subgroup scheme of E (flat over S) of degree su and contains the cyclic subgroup $C_0[s] + D_0[u]$ of degree su. In particular, $C_0[s] + D_0[u] \to Q$ is a closed immersion of finite locally free S-schemes of degree su: it is an isomorphism (by checking the condition after each base change $\operatorname{Spec} \mathcal{O}_{S,s} \to S$, since a surjection of free modules of same rank is an isomorphism). In particular, the q_i are cyclic, and by [86, Proposition 6.7.10], the kernel of π_1 (resp. π_2) is the standard cyclic subgroup of $C_0[s] + D_0[u]$ of degree u (resp. s), i.e. $D_0[u]$ (resp. $C_0[s]$).

Finally, one has

$$q_2(C_0)[t] = \iota(q_1(C_0)[t]) = \iota((\pi_1(C_0) \mod C_1[s])[t]) = \iota((C_1 \mod C_1[s])[t]) = C_2 \mod D_2[u].$$

Now, $\pi_2(C_0)[t]$ and C_2 are two cyclic subgroups of E_2 of order t, and their image through the cyclic isogeny $E_2 \to E_2/D_2[u]$ of degree u coprime to t are the same: hence $\pi_2(C_0[t]) = C_2$. One shows similarly that $\pi_1(D_0) = D_1[v]$. □

Proposition 1.1.39 *Let $N, r \geq 1$, R and $\mathscr{P}$ be as in Definition 1.1.34. Let $s', t' \geq 1$ be coprime divisors of r, and $s, t \geq 1$ be divisors of s', t' respectively. Then the following diagram is Cartesian:*

$$\begin{array}{ccc} \mathscr{M}(\mathscr{P}, [\Gamma_1'(N, r)]_R) & \xrightarrow{D'_{s, \frac{r}{s'}}} & \mathscr{M}(\mathscr{P}, [\Gamma_1'\left(N, \frac{r}{s'}\right)]_R) \\ \downarrow{\scriptstyle D'_{t, \frac{r}{t'}}} & & \downarrow{\scriptstyle D_{t, \frac{r}{s't'}}} \\ \mathscr{M}(\mathscr{P}, [\Gamma_1'\left(N, \frac{r}{t'}\right)]_R) & \xrightarrow{D'_{s, \frac{r}{s't'}}} & \mathscr{M}(\mathscr{P}, [\Gamma_1'\left(N, \frac{r}{s't'}\right)]_R) \end{array}$$

Proof. – This is similar to the proof of Propositions 1.1.38 or 1.1.28. □

Definition 1.1.40 Let $N \geq 1$ be an integer and R be a $\mathbb{Z}[1/N]$-algebra. Let $\mathscr{P}$ be a relatively representable moduli problem over $\mathbf{Ell}_R$ (representable if $N \leq 3$) of level prime to N. Let $d \mid N$ be a positive integer coprime to N/d. We define as follows the morphism

$$w'_d : \mathscr{M}(\mathscr{P}, [\Gamma_1(N)]_R) \times_{\mathbb{Z}[1/N]} (\mu_d^\times)_{\mathbb{Z}[1/N]} \to \mathscr{M}(\mathscr{P}, [\Gamma_1(N)]) \times_{\mathbb{Z}[1/N]} (\mu_d^\times)_{\mathbb{Z}[1/N]}$$

as the following morphism. Given an elliptic curve E/S, $\alpha \in \mathscr{P}(E/S)$, $P \in E(S)$ of exact order N, and $\zeta \in \mu_d^\times(S)$, let $\pi : E \to E' := E/\langle N/d \cdot P \rangle$ be the natural isogeny of degree d. Then one has

$$w'_d((E, \alpha, P, \zeta)) = (E', (\mathscr{P}\pi)(\alpha), Q, \zeta),$$

where $Q \in E'(S)[N]$ is the unique point such that $dQ = \pi(dP)$ and $\langle N/d \cdot P, N/d \cdot Q \rangle_\pi = \zeta$ (by [86, (2.8.2)], $N/d \cdot Q$ is well-defined, hence Q is well-defined since d and N/d are coprime).

Remarks

- In this construction, w'_d is obviously a morphism of $R \otimes_{\mathbb{Z}[1/N]} \mathbb{Z}[1/N, \mu_d]$-schemes, but the $(\mu_d^\times)_{\mathbb{Z}[1/N]}$ cannot be "factored into $\mathscr{P}$" as a moduli problem of level one.
- w'_d has an obvious base change if we replace μ_d with μ_N: in this case, the pairing condition becomes $\langle N/d \cdot P, N/d \cdot Q \rangle_\pi = \zeta^{N/d}$.
- If one specifies instead some $\zeta_0 \in \mu_d^\times(\operatorname{Spec} R)$ (that is, if R is a $\mathbb{Z}[1/N, \zeta_d]$-algebra), then we can define a map $w'_d : \mathscr{M}(\mathscr{P}, [\Gamma_1(N)]_R) \to \mathscr{M}(\mathscr{P}, [\Gamma_1(N)]_R)$ of R-schemes as the base change of Definition 1.1.40 by $\zeta_0 : \operatorname{Spec} R \to \mu_d^\times$, and therefore satisfies the properties detailed in Lemmas 1.1.41, 1.1.43, 1.1.45.

Lemma 1.1.41 *The formation of w'_d commutes with base change and morphisms of moduli problems of level coprime to N.*

Proof. – This is formal. □

Lemma 1.1.42 *With the notations of Definition 1.1.40, let $e = (e_p)_p \in \hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$ be such that $e_p = -1$ if $p \mid d$, and $e_p = d$ if $p \nmid d$. Then one has $w'_d \circ w'_d = [e]$. In particular, w'_d is an isomorphism.*

Proof. – Let E/S be a relative elliptic curve, $\alpha \in \mathscr{P}(E/S)$, $P \in E(S)$ of exact order N, and $\zeta \in \mu_d^\times(S)$. Let $\pi : E \to E' := E/\langle \frac{N}{d} \cdot P \rangle$ be the isogeny, and Q be the point as in Definition 1.1.40, so that $(E'/S, (\mathscr{P}\pi)(\alpha), Q, \zeta) = w'_d(E/S, \alpha, P, \zeta)$. Then $\pi^\vee : E' \to E$ is the degree d isogeny whose kernel is generated by $\frac{N}{d} \cdot Q$. Moreover, one has $\pi^\vee(dQ) = \pi^\vee(\pi(dP)) = d \cdot (dP)$.

Finally, $\langle \frac{N}{d} \cdot Q, -\frac{N}{d} \cdot P \rangle_{\ker \pi^\vee} = \langle \frac{N}{d} \cdot P, \frac{N}{d} \cdot Q \rangle_{\ker \pi} = \zeta$ by [86, (2.8.3)]. Therefore, if $P' \in E(S)$ is the unique point of exact order N such that $dP' = d \cdot dP$, $\frac{N}{d} \cdot P' = -\frac{N}{d} \cdot P$, one has

$$\begin{aligned} w'_d(w'_d((E/S, \alpha, P, \zeta))) &= w'_d((E'/S, (\mathscr{P}\pi)(\alpha), Q, \zeta)) = (E/S, (\mathscr{P}\pi^\vee)(\mathscr{P}\pi)(\alpha), P') \\ &= (E/S, [d]\alpha, e_1 P), \end{aligned}$$

where $e_1 \in (\mathbb{Z}/N\mathbb{Z})^\times$ is congruent to d mod $\frac{N}{d}$ and to -1 mod d. The conclusion follows. □

Lemma 1.1.43 *With the notation of Definition 1.1.40, let $e = (e_p)_p \in \hat{\mathbb{Z}}^\times$. Let $e' = (e'_p)_p \in \hat{\mathbb{Z}}^\times$ be given by $e'_p = e_p$ if $p \nmid d$, and $e'_p = e_p^{-1}$ otherwise. Then $w'_d \circ [e] = [e'] \circ w'_d$.*

Proof. – This is a straightforward computation. □

Lemma 1.1.44 *With the notation of Definition 1.1.40, let $u \in (\mathbb{Z}/d\mathbb{Z})^\times$, and $\underline{u}$ the automorphism of $\mu_d^\times$ whose cyclotomic character is u (it does not act on the component $\mathscr{M}(\mathscr{P}, [\Gamma_1(N)]_P)$). Then one has $\underline{u} \circ [u] \circ w'_d = w'_d \circ \underline{u}$.*

Proof. – This is also a direct computation. □

Lemma 1.1.45 *With the notations of Definition 1.1.40, after extending coefficients to $\mathcal{O}_N$, if $d' \geq 1$ is another divisor of N coprime to $\frac{dN}{d'}$, then $w'_{d'} \circ w'_d = [e] \circ w_{dd'}$, where $e \in (\mathbb{Z}/N\mathbb{Z})^\times$ is congruent to 1 mod $\frac{N}{d'}$ and to d^{-1} mod d'.*

Proof. – Let E/S be a relative elliptic curve, $\alpha \in \mathscr{P}(E/S)$, $\zeta \in \mu_N^\times(S)$ and $P \in E(S)$ be a point of exact order N. Let, for every $t \mid N$, $\zeta_t = \zeta^{N/t} \in \mu_N(S)$, which factors through $\mu_t^\times(S)$.

Then $w'_d((E/S, \alpha, P, \zeta)) = (E'/S, (\mathscr{P}\pi_1)(\alpha), P', \zeta)$, where $\pi_1 : E \to E' := E/\langle \frac{N}{d} \cdot P \rangle$ is the natural cyclic isogeny of degree d, $\langle \frac{N}{d} \cdot P, \frac{N}{d} \cdot P' \rangle_{\pi_1} = \zeta_d$, and $\pi_1(dP) = dP'$.

Let $\pi_2 : E' \to E'' = E'/\langle \frac{N}{d'} \cdot P' \rangle$ denote the natural cyclic isogeny of degree d', and let $Q \in E''[N](S)$ be such that $d'Q = \pi_2(d'P')$ and $\langle \frac{N}{d'} \cdot P', \frac{N}{d'} \cdot Q \rangle = \zeta_{d'}$. Therefore, one has

$$w'_{d'}(w_d((E/S, \alpha, P, \zeta))) = (E''/S, (\mathscr{P}\pi_2)(\mathscr{P}\pi_1)(\alpha), Q, \zeta).$$

Since $\frac{N}{d'} \cdot P' = \frac{N}{dd'} \cdot d \cdot P' = \frac{N}{dd'} \cdot \pi_1(dP) = \pi_1(\frac{N}{d'} \cdot P)$, $\pi = \pi_2 \circ \pi_1$ is the cyclic isogeny (by [86, Proposition 6.7.10]) of degree dd' and of kernel generated by the point $\frac{N}{dd'} \cdot P$ of exact order dd'. In particular, we have $w'_{dd'}((E/S, \alpha, P, \zeta)) = (E''/S, (\mathscr{P}\pi)(\alpha), R, \zeta)$ where $R \in E''(S)$ is another point of exact order N such that $dd'R = \pi(dd'P)$, and $\langle \frac{N}{dd'} \cdot P, \frac{N}{dd'} \cdot R \rangle_\pi = \zeta_{dd'}$.

To conclude, we have the following equalities using [86, (2.8.3),(2.8.4.1)]:

$$\begin{aligned} dd'R = \pi(dd'P) &= \pi_2(\pi_1(dd'P)) = \pi_2(d'\pi_1(dP)) = \pi_2(d'dP') = d\pi_2(d'P') = d(d'Q) = dd'Q, \\ \langle \frac{N}{dd'}P, \frac{N}{dd'}Q \rangle_\pi^{(d')^2} &= \langle \frac{N}{d}P, \frac{N}{dd'}(d'Q) \rangle_{\pi_2 \circ \pi_1} = \langle \frac{N}{d}P, \pi_2^\vee\left(\pi_2\left(\frac{N}{d}P'\right)\right) \rangle_{\pi_1} \\ &= \langle \frac{N}{d}P, d'\frac{N}{d}P' \rangle_{\pi_1} = \zeta_d^{d'} = \zeta_d^{ed'} = \zeta_{dd'}^{e(d')^2}, \\ \langle \frac{N}{dd'}P, \frac{N}{dd'}Q \rangle_\pi^{d^2} &= \langle \frac{N}{d'}Q, \frac{N}{dd'}(dP) \rangle_{\pi_1^\vee \circ \pi_2^\vee}^{-1} = -\langle \frac{N}{d'}Q, \frac{N}{dd'} \cdot \pi_1(dP) \rangle_{\pi_2^\vee}^{-1} \\ &= \langle \frac{N}{d'}Q, \frac{dN}{dd'}P' \rangle_{\pi_2^\vee}^{-1} = \langle \frac{N}{d'}P', \frac{N}{d'}Q \rangle_{\pi_2} = \zeta_{d'} = \zeta_{d'}^{de} = \zeta_{dd'}^{d^2 e}. \end{aligned}$$

□

Proposition 1.1.46 *Let $N \geq 1$ be an integer, R be a $\mathbb{Z}[1/N]$-algebra and $\mathscr{P}$ be a relatively representable moduli problem over $\mathbf{Ell}_R$ (representable if $N \leq 3$) of level L coprime to N. Let $d \geq 1$ be a divisor of N coprime to N/d, $m \geq 1$ be an integer coprime to NL, and $u, v \geq 1$ such that $uv \mid m$. Let $u' \in (\mathbb{Z}/N\mathbb{Z})^\times$ be congruent to u mod d and to 1 mod $\frac{N}{d}$. Then the following diagram is Cartesian:*

$$\begin{array}{ccc} \mathscr{M}(\mathscr{P}, [\Gamma_1(N)]_R, [\Gamma_0(m)]_R) \times_{\mathbb{Z}} \mu_d^\times & \xrightarrow{w'_d} & \mathscr{M}(\mathscr{P}, [\Gamma_1(N)]_R, [\Gamma_0(m)]_R) \times_{\mathbb{Z}} \mu_d^\times \\ \downarrow D_{u,v} & & \downarrow D_{u,v} \\ \mathscr{M}(\mathscr{P}, [\Gamma_1(N)]_R, [\Gamma_0(v)]_R) \times_{\mathbb{Z}} \mu_d^\times & \xrightarrow{[u']\circ w'_d} & \mathscr{M}(\mathscr{P}, [\Gamma_1(N)]_R, [\Gamma_0(v)]_R) \times_{\mathbb{Z}} \mu_d^\times \end{array}$$

Proof. – Since the w'_d are isomorphisms, it is enough to prove that the diagram commutes. Thus, let E/S be a relative elliptic curve and $(E/S, \alpha, P, C, \zeta) \in (\mathscr{M}(\mathscr{P}, [\Gamma_1(N)]_R, [\Gamma_0(m)]_R) \times \mu_d^\times)(S)$.

Let $E' = E/\langle \frac{N}{d} \cdot P \rangle$, $\pi : E \to E'$ the natural isogeny, and $Q \in E'(S)$ the unique point of exact order N such that $dQ = \pi(dP)$ and $\langle \frac{N}{d} \cdot P, \frac{N}{d} \cdot Q \rangle_\pi = \zeta$. Let $P' = P \mod C[u]$, $\pi_C : E/C[u] \to E'' := (E/C[u])/(\langle \frac{N}{d} \cdot P' \rangle)$ be the natural isogeny, and $Q' \in E''(S)$ the unique point of exact order N such that $dQ' = \pi_C(P')$, and $\langle \frac{N}{d} \cdot P', \frac{N}{d} \cdot Q' \rangle_{\pi_C} = \zeta$. Note that π, π_C have degree d prime to m.

It is clear that the only point to prove is that $Q' = u'Q \mod \pi(C)[u]$, i.e. that $dQ' = dQ \mod \pi(C)[u]$ and $\langle \frac{N}{d} \cdot P', \frac{N}{d} \cdot (Q \mod \pi(C)[u]) \rangle_{\pi_C} = \zeta^u$. The first equality is clear because $dQ' = \pi_C(dP')$ and $dQ = \pi(dP)$.

For the second equality, let $p : E \to E/C[u]$ and $p' : E' \to E'/\pi(C)[u]$ be the natural isogenies of degree u, and let $Q'' = p'(Q)$. By a direct computation, $\pi_C \circ (\pi_C^\vee \circ p' - p \circ \pi^\vee) = 0$, thus $\pi_C^\vee \circ p' = p \circ \pi^\vee$. Using [86, (2.8.3),(2.8.4)], we check that

$$\begin{aligned} \langle \frac{N}{d}P', \frac{N}{d}Q'' \rangle_{\pi_C} &= \langle \frac{N}{d}P', \frac{N}{d}Q \rangle_{(p')^\vee \circ \pi_C} = \langle \frac{N}{d}Q, \frac{N}{d}P' \rangle_{(p')^\vee \circ \pi_C}^{-1} \\ &= \langle \frac{N}{d}Q, \frac{N}{d}P' \rangle_{p \circ \pi^\vee}^{-1} = \langle \frac{N}{d}Q, \frac{N}{d}p^\vee(P') \rangle_{\pi^\vee}^{-1} = \langle u\frac{N}{d}P, \frac{N}{d}Q \rangle_\pi = \zeta^u, \end{aligned}$$

whence the conclusion. □

1.2 Compactified moduli schemes

We construct compactified moduli schemes attached to some moduli problems, using the material of Appendix A.2. We follow [86, Chapter 8] for most of the discussion. As in this source, all base rings are assumed to be regular excellent Noetherian. We will always assume that our moduli problems over R are representable and finite over $\mathbf{Ell}_R$ (by Proposition 1.1.10, these conditions are stable under base change). In particular, by [86, Proposition 8.2.2], the j-invariant map of the moduli problems will always be finite (we could also have used Corollary 1.1.14).

Definition 1.2.1 A moduli problem $\mathscr{P}$ over $\mathbf{Ell}_R$ is *normal near infinity* if $\mathscr{M}(\mathscr{P})$ is normal near infinity in the sense of Definition 1.2.1. Lemma A.2.2 tells us that, under our assumptions, this is equivalent to the definition in [86, (8.6.2)].

In this case, we define the *compactified moduli scheme* $\overline{\mathscr{M}}(\mathscr{P})$ as the compactification of the j-invariant morphism $\mathscr{M}(\mathscr{P}) \to \mathbb{A}^1_R$ in the sense of Proposition A.2.9. It is endowed with a finite morphism $\overline{j} : \overline{\mathscr{M}}(\mathscr{P}) \to \mathbb{P}^1_R$ extending the usual j-invariant. Its *cuspidal subscheme* $C_\mathscr{P}$ is the reduced scheme attached to the closed subspace $\{\overline{j} = \infty\}$ of $\overline{\mathscr{M}}(\mathscr{P})$. The proof of Proposition A.2.9 shows that this is equivalent to the construction of [86, (8.6.3)], using [86, Proposition 8.2.2].

Proposition 1.2.2 *Let $\mathscr{P}, \mathscr{P}'$ be representable moduli problems over R, normal near infinity. Let $f : \mathscr{M}(\mathscr{P}) \to \mathscr{M}(\mathscr{P}')$ be any finite map of R-schemes. Then f extends to a finite map $\overline{\mathscr{M}}(\mathscr{P}) \to \overline{\mathscr{M}}(\mathscr{P}')$.*

Definition 1.2.3 If R' is a R-algebra and $\mathscr{P}'$ is a moduli problem over $\mathbf{Ell}_{R'}$, we say that $\mathscr{P}'$ is *normal near infinity over R* if there exists a closed subscheme Z of $\mathbb{A}^1_R$, finite over R, such that $\mathscr{M}(\mathscr{P}')$ is normal outside $j^{-1}(Z_{R'})$.

Corollary 1.2.4 *Suppose that R' is a R-algebra and that we have moduli problems $\mathscr{P}, \mathscr{P}'$ over $\mathbf{Ell}_R, \mathbf{Ell}_{R'}$ respectively. Suppose that $\mathscr{P}$ is normal near infinity, and that $\mathscr{P}'$ is normal near infinity over R and that we have a morphism of moduli problems $\mathscr{P}' \Rightarrow \mathscr{P}_{R'}$. Then the base change map of moduli schemes $\mathscr{M}(\mathscr{P}') \to \mathscr{M}(\mathscr{P})_{R'}$ extends to a morphism of compatified moduli schemes $\overline{\mathscr{M}}(\mathscr{P}') \to \overline{\mathscr{M}}(\mathscr{P})_{R'}$ over $\mathbb{P}^1_{R'}$, and this maps sends $C_{\mathscr{P}'}$ to $(C_{\mathscr{P}})_{R'}$.*

Definition 1.2.5 Suppose that we can take $\mathscr{P}' = \mathscr{P}_{R'}$ in the Corollary 1.2.4. The morphisms $\overline{m} : \overline{\mathscr{M}}(\mathscr{P}') \to \overline{\mathscr{M}}(\mathscr{P})_{R'}$ and $c : C_{\mathscr{P}'} \to (C_{\mathscr{P}})_{R'}$ constructed by this Corollary are called the *base change morphisms* for $\mathscr{P}$ and $R \to R'$. We then say that the formation of the compactified moduli scheme (resp. the cuspidal subscheme) for $\mathscr{P}$ *commutes with the base change* $R \to R'$ if $\overline{m}$ (resp. c) is an isomorphism.

Remark In the situation of Definition 1.2.5, $\overline{m}$ is finite and an isomorphism above $\overline{j}^{-1}(\mathbb{A}^1_{R'})$.

Corollary 1.2.7 *In the situation of the Definition 1.2.5, let Y be a finite R-scheme. Any morphism $\mathscr{M}(\mathscr{P}) \to Y$ of R-schemes extends to $\overline{\mathscr{M}}(\mathscr{P}) \to Y$, and the extension $\overline{\mathscr{M}}(\mathscr{P}') \to Y_{R'}$ is the morphism $\overline{\mathscr{M}}(\mathscr{P}') \xrightarrow{\overline{m}} \overline{\mathscr{M}}(\mathscr{P})_{R'} \to Y_{R'}$.*

Proof. – The existence of the extensions is Corollary A.2.5. The two morphisms agree on the open subscheme $\mathscr{M}(\mathscr{P}')$, $Y_{R'}$ is separated, so they are equal. □

Proposition 1.2.8 *([86, Proposition 8.6.7]) Let $R \to R'$ be a smooth morphism of R_0-algebras and $\mathscr{P}$ be a moduli problem over $\mathbf{Ell}_R$ normal near infinity over R_0. Then $\mathscr{P}_{R'}$ is normal near infinity over R_0. Moreover, the formation of the compactified moduli scheme and the cuspidal subscheme commutes with base change.*

Proof. – Let $Z \subset \mathbb{A}^1_{R_0}$ be a closed subscheme, finite over R_0, such that $\mathscr{M}(\mathscr{P})\backslash j^{-1}(Z_R)$ is normal. Since $\mathscr{M}(\mathscr{P}_{R'}) \to \mathscr{M}(\mathscr{P})$ is smooth, $\mathscr{M}(\mathscr{P}_{R'})$ is normal outside $j^{-1}(Z_{R'})$, hence $\mathscr{P}_{R'}$ is normal near infinity over R and we have well-defined base change morphisms. Since normalization commutes with smooth base change [4, Lemma 03GV], the formation of the compactified moduli scheme commutes with the base change $R \to R'$.

Let us now discuss the formation of the cuspidal subscheme. The isomorphism of $\mathbb{P}^1_{R'}$-schemes $\overline{\mathscr{M}}(\mathscr{P}_{R'}) \to \overline{\mathscr{M}}(\mathscr{P})_{R'}$ induces a surjective closed immersion $\iota : C_{\mathscr{P}_{R'}} \to (C_{\mathscr{P}})_{R'}$. This map will be an isomorphism as long as $(C_{\mathscr{P}})_{R'}$ is reduced. Now, $(C_{\mathscr{P}})_{R'} \to C_{\mathscr{P}}$ is a smooth map to a reduced scheme, hence $(C_{\mathscr{P}})_{R'}$ is reduced, thus ι is an isomorphism. □

Lemma 1.2.9 *Let $R \to R'$ be a finite étale morphism of regular excellent Noetherian rings, and $\mathscr{P}$ be a finite representable moduli problem over $\mathbf{Ell}_R$ normal at infinity. Then the finite representable moduli problem $\mathscr{P}' = \mathscr{P} \times [\operatorname{Spec} R']$ is normal at infinity, and we have natural isomorphisms $\overline{\mathscr{M}}(\mathscr{P}') \to \overline{\mathscr{M}}(\mathscr{P}) \times_R \operatorname{Spec} R'$, $C_{\mathscr{P}'} \to C_{\mathscr{P}} \times_R \operatorname{Spec} R'$.*

Proof. – First, note that by Proposition 1.1.12, $\mathscr{P}'$ is finite representable with moduli scheme $\mathscr{M}(\mathscr{P}) \times_R \operatorname{Spec} R' \to \operatorname{Spec} R$. If $Z \subset \mathscr{M}(\mathscr{P})$ is a closed subscheme finite over $\operatorname{Spec} R$ such that $\mathscr{M}(\mathscr{P})$ is normal outside Z, then $\mathscr{M}(\mathscr{P}')$ is normal outside the closed subscheme $Z_{R'}$ which is finite over R. Hence $\mathscr{P}'$ is normal at infinity. The isomorphism $\mathscr{M}(\mathscr{P}') \to \mathscr{M}(\mathscr{P}) \times_R \operatorname{Spec} R'$ preserves the j-invariants, so it is an isomorphism of $\mathbb{P}^1_R$-schemes. Since relative normalization commutes with smooth base change [4, Lemma 03GV], the relative normalization of $\mathscr{M}(\mathscr{P})_{R'}$ in $\mathbb{P}^1_{R'}$ is exactly $\overline{\mathscr{M}}(\mathscr{P})_{R'}$.

From the commutative diagram

$$\begin{array}{ccc} \mathscr{M}(\mathscr{P}) \times_R \operatorname{Spec} R' & \longrightarrow & \mathscr{M}(\mathscr{P}') \\ \downarrow j & & \downarrow j \\ \mathbb{P}^1_{R'} & \longrightarrow & \mathbb{P}^1_R \end{array}$$

we get a natural morphism $f : \overline{\mathscr{M}}(\mathscr{P}) \times_R \operatorname{Spec} R' \to \overline{\mathscr{M}}(\mathscr{P}')$, which is an isomorphism outside the cuspidal subschemes. Since f is a morphism of finite $\mathbb{P}^1_R$-schemes, f is finite. Furthermore, f is an isomorphism above $\mathscr{M}(\mathscr{P}')$, which is dense and whose inverse image $\mathscr{M}(\mathscr{P}) \times_R \operatorname{Spec} R'$, which is dense. Moreover, all the points of the target (resp. the source) of f in the cuspidal subscheme (resp. in $f^{-1}(C_{\mathscr{P}'})$, i.e. in $C_{\mathscr{P}} \times_R \operatorname{Spec} R'$) are normal: by definition for the target, by étale base change for the source. By Lemma A.2.6, f is an isomorphism.

□

Proposition 1.2.10 *Let $R \to R'$ be a faithfully flat (resp. finite faithfully flat) morphism and $\mathscr{P}$ a moduli problem over $\mathbf{Ell}_R$. If $\mathscr{P}_{R'}$ is normal near infinity over some ring R_0, where R is a R_0-algebra, (resp. normal near infinity), $\mathscr{P}$ is normal near infinity over R_0 (resp. $\mathscr{P}$ is normal near infinity). Moreover, if R' is étale over R, then the formation of the compactified moduli scheme and the cuspidal subscheme for $\mathscr{P}$ commutes with the base change $R \to R'$.*

Proof. – Suppose that $\mathscr{P}_{R'}$ is normal near infinity over R_0: there is a finite subscheme $Z \subset \mathbb{A}^1_{R_0}$ such that $\mathscr{M}(\mathscr{P})\backslash j^{-1}(Z_{R'})$ is normal. Then the map $\mathscr{M}(\mathscr{P}_{R'})\backslash j^{-1}(Z_{R'}) \to \mathscr{M}(\mathscr{P})\backslash j^{-1}(Z_R)$ is faithfully flat from a normal scheme, hence its codomain is a normal scheme. In particular, $\mathscr{P}$ is normal at infinity over R_0.

Suppose now that $\mathscr{P}_{R'}$ is normal near infinity and R' is finite faithfully flat over R. There is a closed subscheme $Z' \subset \mathbb{A}^1_{R'}$, finite over R' (thus affine), such that $\mathscr{M}(\mathscr{P}_{R'})\backslash j^{-1}(Z')$ is normal. Because R is Noetherian, the image Z of Z' in $\mathbb{A}^1_R$ is a closed subscheme, finite over R; by definition, $\mathscr{M}(\mathscr{P}_{R'})\backslash j^{-1}(Z_{R'})$ is contained in $\mathscr{M}(\mathscr{P}_{R'})\backslash j^{-1}(Z')$, hence is normal. Thus $\mathscr{P}_{R'}$ is normal at infinity over R. The previous point shows that $\mathscr{P}$ is normal at infinity over R.

The last point follows from Proposition 1.2.8. □

Definition 1.2.11 Let R' be a R-algebra. A moduli problem $\mathscr{P}$ on $\mathbf{Ell}_{R'}$ is *smooth at infinity over R* if the following properties hold:

- $\mathscr{P}$ is normal near infinity.
- There exists a closed subscheme $Z \subset \mathbb{A}^1_R$, finite over R, such that $\overline{\mathscr{M}}(\mathscr{P}) \to \operatorname{Spec} R'$ is smooth outside $j^{-1}(Z_{R'})$.
- $C_{\mathscr{P}}$ is finite étale over R.

When $R = R'$, we say that $\mathscr{P}$ is smooth at infinity. This is then exactly the notion discussed in [86, Definition 8.6.5].

Remark Since the j-invariant map $\mathscr{M}(\mathscr{P}) \to \mathbb{A}^1_R$ is finite, this definition for $R' = R$ is equivalent to asking that $\mathscr{M}(\mathscr{P}) \to \operatorname{Spec} R$ is smooth at infinity in the sense of Definition A.2.11.

Lemma 1.2.13 *Let R' be an R-algebra. If $\mathscr{P}$ is a moduli problem on $\mathbf{Ell}_{R'}$ which is smooth at infinity over R, then $\mathscr{P}$ is normal near infinity over R.*

Proof. – This is because $\mathscr{M}(\mathscr{P})\backslash j^{-1}(Z_{R'}) \to \operatorname{Spec} R'$ is smooth over a regular ring, hence $\mathscr{M}(\mathscr{P})\backslash j^{-1}(Z_{R'})$ is a regular scheme by [4, Lemma 07NF]. □

Proposition 1.2.14 *([86, Proposition 8.6.6]) Let $R_0 \to R \to R'$ be morphisms of rings. If $\mathscr{P}$ is a moduli problem on $\mathbf{Ell}_R$ which is smooth at infinity over R_0, then $\mathscr{P}_{R'}$ is smooth at infinity over R_0, and the formation of the compactified moduli scheme and the cuspidal subscheme for $\mathscr{P}$ commutes with the base change $R \to R'$. Moreover, the cuspidal subscheme of $\mathscr{P}$ is an effective Cartier divisor in $\overline{\mathscr{M}}(\mathscr{P})$.*

Proof. – This is an immediate consequence of Proposition A.2.12. □

Proposition 1.2.15 *Let $R_0 \to R \to R'$ be morphisms of rings with $R \to R'$ faithfully flat smooth. Let $\mathscr{P}$ be a moduli problem on $\mathbf{Ell}_R$ such that $\mathscr{P}_{R'}$ is smooth at infinity over R_0. Then $\mathscr{P}$ is smooth at infinity over R_0 and the formation of the compactified moduli scheme and the cuspidal subscheme for $\mathscr{P}$ commutes with the base change $R \to R'$.*

Proof. – Let $Z \subset \mathbb{A}^1_{R_0}$ be a closed subscheme, finite over R_0, such that $\mathscr{M}(\mathscr{P}_{R'})$ is smooth over $\operatorname{Spec} R'$ outside the j-invariants in $Z_{R'}$. Now, $\mathscr{P}$ is normal near infinity over R_0 by Proposition 1.2.10, and the formation of the compactified moduli scheme and the cuspidal subscheme commutes with base change by Proposition 1.2.8. In particular, after making the fpqc base change $R \to R'$, $\overline{\mathscr{M}}(\mathscr{P})_R \to \operatorname{Spec} R$ is smooth of relative dimension one outside the j-invariants in Z_R, therefore $\overline{\mathscr{M}}(\mathscr{P}) \to \operatorname{Spec} R$ is smooth of relative dimension one outside the j-invariants in Z_R.

We previously said that the isomorphism of compactified moduli schemes induces an isomorphism of cuspidal subschemes $\iota : C_{\mathscr{P}_{R'}} \to (C_{\mathscr{P}})_{R'}$. Hence $C_{\mathscr{P}} \to \operatorname{Spec} R$ becomes finite étale after the faithfully flat base change $R \to R'$, hence $C_{\mathscr{P}} \to \operatorname{Spec} R$ is finite étale. □

Proposition 1.2.16 *Let R be a regular excellent Noetherian ring and let $\mathscr{P}$ be a finite locally free representable moduli problem on $\mathbf{Ell}_R$ endowed with a level N structure, for some $N \geq 1$, and assume that $\mathscr{P}$ is normal near infinity. Then the action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $\mathscr{M}(\mathscr{P})$ extends to an action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $\overline{\mathscr{M}}(\mathscr{P})$. This action is natural with respect to $\mathscr{P}$ (for morphisms of finite locally free representable moduli problems on $\mathbf{Ell}_R$ normal near infinity and endowed with a level N structure).*

Proof. – This is a direct application of Proposition A.2.9. □

Proposition 1.2.17 *Let $N, m \geq 1$ be coprime integers, R be a regular excellent Noetherian ring, and $\mathscr{P}$ be a finite locally free representable moduli problem on $\mathbf{Ell}_R$ endowed with a level N structure, such that $\mathscr{P} \times [\Gamma_0(m)]_R$ is normal near infinity. Then, for every divisor $d \geq 1$ of m, the moduli problem $\mathscr{P} \times [\Gamma_0(t)]_R$ is normal near infinity. Moreover,*

- *for any $d, t \geq 1$ such that $dt \mid m$, there is a finite map $\overline{\mathscr{M}}(\mathscr{P}, [\Gamma_0(m)]_R) \to \overline{\mathscr{M}}(\mathscr{P}, [\Gamma_0(t)])$ of R-schemes extending the morphism $D_{d,t}$ of Definition 1.1.23. We denote this extension by $D_{d,t}$.*
- *for any $d \geq 1$ dividing m and coprime to m/d, there is an automorphism of R-schemes of $\overline{\mathscr{M}}(\mathscr{P}, [\Gamma_0(m)]_R)$ extending w_d. We denote this extension by w_d.*
- *the formation of $D_{d,t}$ and w_d is natural with respect to $\mathscr{P}$ (for morphisms of representable moduli problems of level N such that their product with $[\Gamma_0(m)]_R$ is normal near infinity).*
- *the relations between the various w_d (for $d \geq 1$ dividing m and coprime to m/d) and $D_{s,t}$ (for various $s, t \geq 1$ such that $st \mid m$) stated in Corollary 1.1.25 and Proposition 1.1.29 still hold.*

Proof. – For any $t \geq 1$ dividing m, $D_{1,t} : \mathscr{M}(\mathscr{P}, [\Gamma_0(m)]_R) \to \mathscr{M}(\mathscr{P}, [\Gamma_0(t)]_R)$ is finite flat surjective. The rest is a direct application of the construction of Proposition A.2.9, since these maps are defined on the (non-compactified) moduli schemes. □

Proposition 1.2.18 *In the situation of Proposition 1.2.2, assume furthermore that f is flat, that $\mathscr{P}, \mathscr{P}'$ are flat near infinity[7] over $\mathbf{Ell}_R$, and that $\overline{\mathscr{M}}(\mathscr{P})$, $\overline{\mathscr{M}}(\mathscr{P}')$ are respectively Cohen-Macaulay and regular at every point of the cuspidal subscheme. Then the compactifications $\overline{f}$ of f and of the j-invariants are finite locally free. These hypotheses are satisfied if f is flat and $\mathscr{P}, \mathscr{P}'$ are smooth at infinity.*

Proof. – After taking a direct factor of R (since it is Noetherian), we can assume that R has no nontrivial idempotents. Since it is regular, R is a domain.

[7] in the sense that there exists an open subscheme $U \subset \mathbb{A}^1_R$ whose complement is finite over $\operatorname{Spec} R$ and such that $\mathscr{P}, \mathscr{P}'$ are flat over $\mathbf{Ell}_R$ above U

Let $x \in \overline{\mathscr{M}}(\mathscr{P})$ be contained in the cuspidal subscheme, y be its image in $\mathbb{P}^1_R$ and z be its image in $\operatorname{Spec} R$. We show that $\dim \mathcal{O}_{\overline{\mathscr{M}}(\mathscr{P}),x} = \dim \mathcal{O}_{\mathbb{P}^1_R,y} = \dim \mathcal{O}_{\operatorname{Spec} R,z} + 1$. This implies in particular that $\dim \mathcal{O}_{\overline{\mathscr{M}}(\mathscr{P}),x} = \dim \mathcal{O}_{\overline{\mathscr{M}}(\mathscr{P}'),f(x)}$. The morphisms $\overline{f}^\sharp : \mathcal{O}_{\mathbb{P}^1_R,y} \to \mathcal{O}_{\overline{\mathscr{M}}(\mathscr{P}),x}$ or $\overline{j}^\sharp : \mathcal{O}_{\overline{\mathscr{M}}(\mathscr{P}'),f(x)} \to \mathcal{O}_{\overline{\mathscr{M}}(\mathscr{P}),x}$ are local, and they are localizations at a maximal ideal of finite morphisms (by Proposition A.2.9); and since their base rings are regular, while the target ring is Cohen-Macaulay, the morphisms are flat by miracle flatness [4, Lemma 00R4].

Let us prove that $\dim \mathcal{O}_{\mathbb{P}^1_R,y} = \dim \mathcal{O}_{\operatorname{Spec} R,z} + 1$. By [4, Lemma 00ON], we are reduced to the case where R is a field. Since y is above the infinity section, it is a closed point of $\mathbb{P}^1$ and the conclusion follows.

Next, we need to prove that $\dim \mathcal{O}_{\mathbb{P}^1_R,y} = \dim \mathcal{O}_{\overline{\mathscr{M}}(\mathscr{P}),x}$. Let $U \subset \mathbb{P}^1_R$ an affine open subscheme containing the cuspidal subscheme such that j is flat above $U \cap \mathbb{A}^1_R$ and $\mathcal{O}(j^{-1}(U))$ is normal. Then $\mathcal{O}(U)$ is a normal domain, so, since $\mathcal{O}(U) \to \mathcal{O}(j^{-1}(U))$ is finite, it is enough to show by [4, Lemma 00ON] that this map satisfies going down. Since $\mathcal{O}(j^{-1}(U))$ is normal Noetherian, it is a finite product of domains, and, by [4, Proposition 00H8], the going down property holds as soon as $\mathcal{O}(U)$ injects in each direct factor of $\mathcal{O}(j^{-1}(U))$. Now, if $C \subset j^{-1}(U)$ is a closed open subscheme, then $j : C \to U$ is still finite flat, and U is irreducible, so $j(C) = U$. Hence $\mathcal{O}(C)$ is faithfully flat over $\mathcal{O}(U)$, and $\mathcal{O}(U) \to \mathcal{O}(C)$ is injective. □

Corollary 1.2.19 *The $D_{d,t}$ defined in Proposition 1.2.17 are finite locally free if for every point $x \in X := \overline{\mathscr{M}}(\mathscr{P}, [\Gamma_0(k)]_R)$ (for any divisor $k \geq 1$ of m) lying in the cuspidal subscheme, the local ring $\mathcal{O}_{X,x}$ is regular, and if $X \to \mathbb{P}^1_R$ is flat above some open subset $U \subset \mathbb{A}^1_R$ with $\mathbb{A}^1_R \backslash U$ finite over R. These conditions are satisfied if every $\mathscr{P} \times [\Gamma_0(k)]_R$ is smooth at infinity.*

To apply Proposition 1.2.17, we thus need concrete criteria in order to decide when the moduli problems $\mathscr{P} \times [\Gamma_0(m)]_R$ are normal near infinity.

Proposition 1.2.20 *Let $\mathscr{P}$ be a finite representable moduli problem over $\mathbf{Ell}_R$, where R is a Noetherian ring. Let $m_0, m_1 \geq 1$ be coprime integers such that m_0 is square-free and $m_1 \in R^\times$, with $m = m_0 m_1$. Let $U \subset \mathbb{A}^1_R$ be an open subset such that its complement Z is finite over* $\operatorname{Spec} R$ *and $\mathscr{P}_{|U}$ is étale over U. Then:*

- *$\mathscr{M}(\mathscr{P}, [\Gamma_0(m)]_R]) \to \operatorname{Spec} R$ is Cohen-Macaulay of relative dimension one with geometrically reduced fibres at every point of $j^{-1}(U)$, and smooth at every point which is not supersingular in residue characteristic $p \mid m_0$.*
- *Assume furthermore that R is regular excellent Noetherian of generic characteristic zero. Then $\mathscr{P} \times_R [\Gamma_0(m)]_R$ is smooth at infinity, the same statement as above holds for its compactified moduli scheme, and $\overline{\mathscr{M}}(\mathscr{P}, [\Gamma_0(m)]_R) \to \overline{\mathscr{M}}(\mathscr{P})$ is finite locally free of constant rank.*
- *If furthermore R' is any regular excellent Noetherian R-algebra, the conclusions of the previous point hold over R'.*

Proof. – The last point follows from the second one using Proposition 1.2.14.

We know that the map $\mathscr{M}(\mathscr{P}, [\Gamma_0(m)]_R) \to \mathscr{M}(\mathscr{P})$ is finite locally free of constant rank (étale over $\mathbb{Z}[1/m]$) and the same argument as Corollary 1.1.14 shows that $j^{-1}(U) \subset \mathscr{M}(\mathscr{P}) \to \operatorname{Spec} R$ is smooth of relative dimension one. Thus, $j^{-1}(U) \subset \mathscr{M}(\mathscr{P}, [\Gamma_0(m)]_R) \to \operatorname{Spec} R$ is Cohen-Macaulay of relative dimension one and smooth above $R[1/m]$.

To prove the claimed smoothness (and reducedness of the geometric fibres), we may therefore assume that R is an algebraically closed field k of characteristic $p \mid m_0$. After replacing $\mathscr{P}$ with $\mathscr{P} \times_R [\Gamma_0(m_0 m_1/p)]_R$, we may assume that $(m_0, m_1) = (p, 1)$.

Fix some prime $\ell \nmid 2m$, then $\mathscr{M}([\Gamma(\ell)]_k, [\Gamma_0(p)]_k, \mathscr{P}) \to \mathscr{M}(\mathscr{P}, [\Gamma_0(p)]_k)$ is finite étale of constant positive rank, hence it is enough to prove the statement for the moduli problem $[\Gamma(\ell)]_k \times [\Gamma_0(p)] \times \mathscr{P}$. The map $\mathscr{M}([\Gamma(\ell)]_k, [\Gamma_0(p)]_k, \mathscr{P}) \to \mathscr{M}([\Gamma(\ell)]_k, [\Gamma_0(p)]_k)$ is finite étale above $j^{-1}(U)$, so we are reduced to the case $\mathscr{P} = [\Gamma(\ell)]_k$. This then follows from [86, Theorem

10.10.3 (5)] (with the same p, $N = \ell$, $\Gamma \leq \mathrm{GL}_2(\mathbb{Z}/p\ell\mathbb{Z})$ being the subgroup of upper-triangular matrices that are trivial mod ℓ), whose assumptions ((a), (b) and balancedness[8]) can be directly checked, and we come back from what *loc. cit.* calls the "canonical problems" to our setting using [86, Proposition 9.1.7].

Note that, to use this statement, we need to base change from $R_0 = \mathbb{Z}[1/\ell]$ (we are dealing with a representable moduli problem, so there is no issue) and check that the moduli problem $[\Gamma_0(p)]_{R_0}$ is indeed the quotient of $[\Gamma(p)]_{R_0}$ by the subgroup of *lower*-triangular matrices (see Remark 1.3.8), which is [86, Theorem 7.4.2].

Now, we discuss the second point. Assume that R is regular excellent Noetherian, and that $\mathscr{P} \times [\Gamma_0(m)]_R$ is smooth at infinity. Then the required smoothness for the compactified moduli scheme follows directly from the first point. The morphism $f : \overline{\mathscr{M}}(\mathscr{P}, [\Gamma_0(m)]_R) \to \overline{\mathscr{M}}(\mathscr{P})$ is finite by assumption, flat away from the cusps because so is the moduli problem $[\Gamma_0(p)]_R$. Away from some finite R-subscheme containing $j^{-1}(Z)$ and the supersingular points in residue characteristic $p \mid m_0$ (using [86, Lemma 12.5.4]), f is a finite map of smooth R-schemes of relative dimension one, so it is flat by miracle flatness.

Thus only the smoothness at infinity remains to prove. We assume that R is regular excellent Noetherian, and (after possibly shrinking it), that U is principal defined by a monic polynomial. If $m_0 = 1$, then the statement follows from [86, Theorem 8.6.8], so we assume $m_0 > 1$. Let $Y_0(m)^R$ be the coarse moduli scheme attached to $[\Gamma_0(m)]_R$, $Y_0(m) := Y_0(m)^{\mathbb{Z}[1/m_1]}$. By [86, Theorem 5.1.1, Lemma 8.1.2], $Y_0(m)$ is normal. By [86, Proposition 8.1.6], we have a canonical morphism of $\mathbb{A}^1_R$-schemes $B : Y_0(m)^R \to Y_0(m) \times_{\mathbb{Z}[1/m_1]} \operatorname{Spec} R$. Let V be a principal open subscheme of $\mathbb{A}^1_{\mathbb{Z}[1/m_1]}$ defined by a monic polynomial which is a multiple of $j(j - 1728)$, and such that V does not contain the supersingular j-invariants in residue characteristic $p \mid m_0$ (see [86, Lemma 12.5.4]). By [86, (8.5.4)], B is an isomorphism above $j^{-1}(V)$.

The open subspace $V' = U \cap V$ of $\mathbb{A}^1_R$ is defined by a monic polynomial, hence it is the complement of a closed subscheme Z' finite over $\operatorname{Spec} R$. Then $\pi : \mathscr{M}(\mathscr{P}, [\Gamma_0(m)]_R) \to Y_0(m)^R$ is finite, and a morphism of smooth R-schemes of relative dimension one above $j^{-1}(V')$, hence by miracle flatness it is flat.

Let us prove that $Y_0(m)$ is smooth at infinity in the sense of Definition A.2.11, and let $X_0(m)$ be its compactification. We apply [86, Theorem 10.10.3 (5)] to each prime $p \mid m_0$, with $N = m_0 m_1/p$, $\Gamma_1 \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, $\Gamma_2 \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ the subgroups consisting of upper-triangular matrices: the assumptions (a) and (b) are trivially satisfied and one checks directly that Γ_1 is balanced. By Proposition A.2.12, for any regular excellent Noetherian $\mathbb{Z}[m_1^{-1}]$-algebra S, that $Y_0(m)^S$ is smooth at infinity, and $X_0(m)^S := \overline{Y_0(m)^S} \to X_0(m)_S$ is an isomorphism away from the (inverse images under finite maps) of the finite R-scheme $j^{-1}(\mathbb{A}^1_R \backslash V_R)$.

Let us temporarily assume that π is étale above $j^{-1}(V)$. Since R has generic residue characteristic zero, we can then apply Proposition A.2.13 to $\mathscr{M}(\mathscr{P}, [\Gamma_0(m)]_R) \to X_0(m)^R$, and the conclusion would follow.

Thus, all we need to do is prove that π is étale above $j^{-1}(V')$. Let k be an algebraically closed field and a R-algebra. It is enough to show that the fibres of $\pi \times_R \operatorname{Spec} k$ above $j^{-1}(V')_k$ are étale. Let $BC : Y_0(m)^k \to Y_0(m)^R_k$ be the canonical base change morphism, which is an isomorphism above $j^{-1}(V')$.

Since, above $j^{-1}(V)$, the formation of the coarse moduli scheme for $[\Gamma_0(m)]$ commutes with base change, and since π is flat above $j^{-1}(V')$, we may thus assume that R is an algebraically closed field k of characteristic c. Let $U' \subset \mathbb{A}^1_k$ be the affine open subset on which $j(j - 1728)$ is invertible. If $c \neq 2$, consider the moduli problem $[U', 1]$ of [86, Theorem 8.4.9], which yields the following commutative diagram of U'-schemes:

[8] This is the reason why m_0 had to be square-free.

$$\begin{array}{ccc} \mathscr{M}(\mathscr{P},[\Gamma_0(m)]_k,[U',1]) & \xrightarrow{\alpha} & \mathscr{M}(\mathscr{P},[\Gamma_0(m)]_k)\times_{\mathbb{A}^1_k} U' \\ \downarrow{\scriptstyle\beta} & & \downarrow{\scriptstyle\pi'} \\ \mathscr{M}([\Gamma_0(m)]_k,[U',1]) & \xrightarrow{\delta} & Y_0(m)^k\times_{\mathbb{A}^1_k} U' \end{array}$$

By [86, Corollary 8.4.10], α, δ are finite étale. By assumption, β is finite étale above $j^{-1}(U \cap U')$. Thus π' is étale above $j^{-1}(U \cap U')$: since $\pi \otimes_R \operatorname{Spec} k = BC \circ \pi'$, and BC is an isomorphism above $j^{-1}(V') \subset j^{-1}(U \cap U')$, $\pi \times_R \operatorname{Spec} k$ is étale above $j^{-1}(V')_k$.

When $c = 2$, the same argument applies by replacing the moduli problem $[U', 1]$ with the moduli problem $[\mu_4]$ of [86, Theorem 8.4.11], and replacing the references to [86, Theorem 8.4.9, Corollary 8.4.10] with references to [86, Theorem 8.4.11, Corollary 8.4.12]. □

Corollary 1.2.21 *Let $\mathscr{P}$ be a finite étale representable moduli problem over $\mathbf{Ell}_R$, for some regular excellent Noetherian ring R of generic characteristic zero. Then, for all coprime $m_0, m_1 \geq 1$ with m_0 square-free and $m_1 \in R^\times$, $\mathscr{P} \times_R [\Gamma_0(m_0 m_1)]_R$ is smooth at infinity.*

Proposition 1.2.22 *Let $N \geq 1$ be an integer, $r \mid N$, and R be a regular excellent Noetherian $\mathbb{Z}[1/N]$-algebra, and $\mathscr{P}$ be a finite locally free relatively representable (representable if $N \leq 3$) moduli problem on $\mathbf{Ell}_R$ with level prime to N, such that $\mathscr{P} \times [\Gamma'_1(N, r)]_R$ is normal near infinity. Then, for every divisor $d \geq 1$ of r, the moduli problem $\mathscr{P} \times [\Gamma'_1(N, d)]_R$ is normal near infinity. Moreover,*

- *for any $s, t \geq 1$ such that $st \mid r$, the morphism $D'_{s,t}$ of Definition 1.1.23 extends to a finite map $D'_{s,t} : \overline{\mathscr{M}}(\mathscr{P}, [\Gamma'_1(N, r)]_R) \to \overline{\mathscr{M}}(\mathscr{P}, [\Gamma'_1(N, t)])$ of R-schemes.*
- *$D'_{s,t}$ is finite locally free if for every $d \mid r$ and every $x \in X := \overline{\mathscr{M}}(\mathscr{P}, [\Gamma'_1(N, d)]_R)$ contained in the cuspidal subscheme, $\mathcal{O}_{X,x}$ is regular. This is in particular the case if every $[\mathscr{P}] \times [\Gamma'_1(N, d)]_R$ is smooth near infinity.*
- *for any $d \geq 1$ dividing N and coprime to N/d, there is an automorphism of R-schemes of $\overline{\mathscr{M}}(\mathscr{P}, [\Gamma_1(N)]_R)$ extending w'_d. We denote this extension by w'_d.*
- *the formation of $D'_{s,t}$ and w'_d is natural with respect to $\mathscr{P}$ (for morphisms of representable moduli problems of level N such that their product with $[\Gamma'_1(N, r)]_R$ or $[\Gamma_1(N)]_R$ is normal near infinity).*
- *the relations between the various w'_d and $D'_{s,t}$ stated in Lemmas 1.1.35, 1.1.43, 1.1.44 (with the suitable extension of scalars) and 1.1.45 still hold.*

Proof. – The proof is analogous to the proof of Proposition 1.2.17 (and Corollary 1.2.19) using the results of Section 1.1.3. □

1.3 Application to our moduli problems

Definition 1.3.1 Let $N \geq 3$ be an integer, S be a $\mathbb{Z}[1/N]$-scheme. A *N-torsion group over S* is a finite étale group G over S which is étale-locally isomorphic to $(\mathbb{Z}/N\mathbb{Z})^{\oplus 2}$.

Definition 1.3.2 A *Weil pairing* for a N-torsion group G is a bilinear alternating pairing $G \times_R G \to \mu_N$ which is fibre-wise perfect. By Cartier duality [147, §4], this alternating pairing induces an morphism w from G to its Cartier dual. Since both groups are finite étale over R, w is finite étale by [4, Lemma 02GW]. Since w is a fibrewise isomorphism, w is an isomorphism. We call the datum of a N-torsion group over R endowed with a Weil pairing a *polarized N-torsion group*.

The moduli problems that we will consider are the following ones:

Definition 1.3.3 Let G be a N-torsion group over a $\mathbb{Z}[1/N]$-algebra R. The moduli problem $\mathscr{P}_G$ on $\mathbf{Ell}_R$ is defined as follows:

– let S be a R-scheme and E/S be an elliptic curve, then $\mathscr{P}_G(E/S)$ is the set of isomorphisms $\iota : G \times_R S \to E[N]$ of S-group schemes,
– for a morphism $F/T \to E/S$ in the category $\mathbf{Ell}_R$, the morphism $\mathscr{P}_G(E/S) \to \mathscr{P}_G(F/T)$ is induced by the isomorphism $F[N] \to E[N] \times_S T$.

It is endowed with a natural structure of moduli problem of level N. In particular, for any $m \geq 1$ coprime to N, the moduli problem $\mathscr{P}_G(\Gamma_0(m)) := \mathscr{P}_G \times [\Gamma_0(m)]_R$ is endowed with a natural level structure of level Nm.

Remark The moduli problem $[\Gamma(N)]_R$ over a $\mathbb{Z}[1/N]$-algebra R is exactly the moduli problem $\mathscr{P}_G$ attached to the constant group scheme $(\mathbb{Z}/N\mathbb{Z})^{\oplus 2}_R$.

Definition 1.3.5 Let G be a polarized N-torsion group with Weil pairing W. Given an isomorphism of S-group schemes $\varphi : G_S \to E[N]$, the map $G_S \times G_S \overset{\varphi\times\varphi}{\to} E[N] \times E[N] \overset{\mathrm{We}}{\to} \mu_N$ is an alternate pairing; therefore it can be written as $\alpha \circ W$, where α is an endomorphism of the S-group scheme μ_N. In particular, α is a locally constant function $S \to (\mathbb{Z}/N\mathbb{Z})^\times$, which we call the determinant of φ and denote $\det \varphi$.

For $u \in (\mathbb{Z}/N\mathbb{Z})^\times$ (resp. and $m \geq 1$ coprime to N), let $\mathscr{P}_{G,u}$ (resp. $\mathscr{P}_{G,u}(\Gamma_0(m))$) denote the subfunctor of $\mathscr{P}_G$ (resp. $\mathscr{P}_G(\Gamma_0(m))$) parametrizing isomorphisms ι (resp. couples (ι, C)) with $\det \iota = u$.

Proposition 1.3.6 *Let G be a N-torsion group over a $\mathbb{Z}[1/N]$-algebra R. Then the moduli problem $\mathscr{P}_G$ satisfies the following properties:*

(*i*) *It is representable and finite étale of constant rank $r_N \geq 1$ over $\mathbf{Ell}_R$, by an elliptic curve $\mathcal{E}_G(N)/Y_G(N)$, with $Y_G(N) \to \operatorname{Spec} R$ smooth affine of relative dimension one,*
(*ii*) *Its j-invariant is finite locally free of constant rank $r'_N \geq 1$, étale on the locus where $j(j-1728)$ is invertible,*
(*iii*) *If R is regular excellent Noetherian, then $\mathscr{P}_G$ is smooth at infinity over $\mathbb{Z}[1/N]$: the formation of its compactified moduli scheme and cuspidal subschemes commutes with any base change,*
(*iv*) *If R is regular excellent Noetherian, the compactified moduli scheme $X_G(N)$ attached to $\mathscr{P}_G$ is smooth proper over $\operatorname{Spec} R$ of relative dimension one,*
(*v*) *If R is regular excellent Noetherian, $X_G(N)$ is a regular scheme and the j-invariant map is finite locally free of rank r'_N,*
(*vi*) *The level N structure on $\mathscr{P}_G$ defines a natural action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $Y_G(N)$ which preserves the j-invariant. When R is regular excellent Noetherian, it extends to an action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $X_G(N)$ (still denoted $[\cdot]$) whose formation commutes with base change.*

Proof. – When G is constant and $R = \mathbb{Z}[1/N]$, (i)-(iv) (apart from the statement about base change) follow from Corollary 1.1.14 and [86, Theorem 5.1.1, Proposition 8.6.8]. Since $X_G(N)$ is smooth proper over $\mathbb{Z}[1/N]$ of relative dimension one, it is regular (with every nonempty open subset of dimension two), hence Cohen-Macaulay, and the j-invariant $X_G(N) \to \mathbb{P}^1_{\mathbb{Z}[1/N]}$ is finite from a Cohen-Macaulay scheme to a regular scheme (every nonempty open subscheme of either having dimension 2), hence is flat by miracle flatness. Finally, (vi) (apart from the commutation with base change) follows from the results on level structures and Proposition A.2.9.

When G is constant over a different base, the results (including the base change statements) follow from Proposition 1.1.10, Corollary 1.1.14, and Proposition 1.2.14.

For general G, there is a faithfully flat étale map $R \to R'$ such that $G_{R'}$ is constant. Since $\mathscr{P}(N)_{R'}$ is representable and affine over $\mathbf{Ell}_{R'}$, and since $T \longmapsto \mathscr{P}_G(E_T/T)$ is a fpqc sheaf on $\mathbf{Sch}_S$ for all objects E/S of $\mathbf{Ell}_R$, Proposition 1.1.15 proves that $\mathscr{P}_G$ is representable. By Proposition 1.1.10, $\mathscr{P}_G$ is finite étale of rank r_N over $\mathbf{Ell}_R$. Thus the moduli scheme is smooth of relative dimension one over R, with finite flat j-invariant of rank r'_N by Corollary 1.1.14 (and base changing to R' for the value of the rank). The j-invariant map $Y_G(N) \to \mathbb{A}^1_R$ is then étale above the invertible locus of $j(j-1728)$ by [86, Corollary 8.4.5].

We use Proposition 1.2.15 (with $R_0 = \mathbb{Z}[1/N]$ and the base change $R \to R'$) to show that $\mathscr{P}_G$ is smooth at infinity over $\mathbb{Z}[1/N]$ and that the formation of its compactified moduli scheme and cuspidal subscheme commutes with the base change $R \to R'$ (and thus with any base change by Proposition 1.2.14). Thus the following diagram is Cartesian:

$$\begin{array}{ccccc} X_{G_{R'}}(N) & \xrightarrow{j'} & \mathbb{P}^1_{R'} & \xrightarrow{\sigma'} & \operatorname{Spec} R' \\ \downarrow & & \downarrow & & \downarrow \\ X_G(N) & \xrightarrow{j} & \mathbb{P}^1_R & \xrightarrow{\sigma} & \operatorname{Spec} R \end{array}$$

Since j' is finite flat and étale away from the cusps and the vanishing locus of $j'(j'-1728)$, and $\sigma' \circ j'$ is smooth proper of relative dimension one, by fpqc descent j is finite flat and étale away from the cusps and the vanishing locus of $j(j-1728)$, and $\sigma \circ j$ is proper smooth of relative dimension one.

(vi) follows from the fact that $Y_G(N) \to X_G(N)$ is an epimorphism (for separated R-schemes), the fact that $\mathscr{P}$ has a natural level N structure, and the fact that the formation of the compactified moduli scheme for $\mathscr{P}_G$, as well as the cuspidal subscheme, commutes with base change. □

Corollary 1.3.7 *If $\mathscr{P}$ is an étale representable moduli problem over $\mathbf{Ell}_R$ (where R is any ring), then its j-invariant $\mathscr{M}(\mathscr{P}) \to \mathbb{A}^1_R$ is étale on the locus where $j(j-1728)$ is invertible.*

Proof. – This statement is Zariski-local over $\operatorname{Spec} R$, so we may assume that some odd prime ℓ is invertible in R. Consider the same commuting diagram as in Proposition 1.1.13:

$$\begin{array}{ccc} \mathscr{M}(\mathscr{P}, [\Gamma(\ell))]_R) & \xrightarrow{f_1} & \mathscr{M}([\Gamma(\ell)]_R) \\ \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle j_\ell} \\ \mathscr{M}(\mathscr{P}) & \xrightarrow{j_{\mathscr{P}}} & \mathbb{A}^1_R \end{array}$$

We just proved that j_ℓ was étale above the locus where $j(j-1728)$ is invertible, and f_1 is étale because $\mathscr{P}$ is. Since π_1 is finite étale, $j_{\mathscr{P}}$ is étale-locally étale above the locus where $j(j-1728)$ is invertible, hence it is étale above this locus by [4, Lemma 036W]. □

Notation *We denote by $\mathcal{E}(N)/Y(N)$ the elliptic curve $\mathcal{E}_{(\mathbb{Z}/N\mathbb{Z})^{\oplus 2}}(N)/Y_{(\mathbb{Z}/N\mathbb{Z})^{\oplus 2}}(N)$. The action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the right on $(\mathbb{Z}/N\mathbb{Z})^{\oplus 2}$ by $\begin{pmatrix} a \\ b \end{pmatrix} \mid M = M^T \begin{pmatrix} a \\ b \end{pmatrix}$ induces a left action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ by automorphisms on $\mathscr{P}(N)$, hence on $Y(N)$.*

Let S be any $\mathbb{Z}[1/N]$-scheme and G be a N-torsion group over S. The datum of an isomorphism $f : (\mathbb{Z}/N\mathbb{Z})^{\oplus 2} \to G$ of group schemes over S is the same (by considering the image under f of the two basis sections) as the datum of two sections $A, B \in G(S)$ such that $(a,b) \in (\mathbb{Z}/N\mathbb{Z})^{\oplus 2} \longmapsto aA + bB \in G(S)$ is injective (thus an isomorphism). Under this identification, for any S-scheme, $Y(N)(S)$ fonctorially identifies with the set of S-isomorphism classes of triples (E, P, Q) where E/S is an elliptic curve, and (P, Q) is a $\mathbb{Z}/N\mathbb{Z}$-basis of $E[N](S)$. Under this identification, a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ maps a S-point (E, P, Q) of $Y(N)$ to $(E, aP + bQ, cP + dQ)$.

In particular, this procedure identifies $[a]$ with the action of the matrix $aI_2 \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Remark In [86] (for instance (10.3)), the authors let $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \mathrm{Aut}((\mathbb{Z}/N\mathbb{Z})^{\oplus 2})$ act on $X(N)$ on the *right*. Our definition of the action (which is on the *left*) of $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is exactly the action of the transpose g^T of g in *loc.cit.*. This will become important when we will write down an explicit description of the cuspidal subscheme in Section 1.6.

Proposition 1.3.9 *Let (P^{univ}, Q^{univ}) be the basis of $\mathcal{E}(N)[N]$ as a finite group scheme over $Y(N)$. Then $\mathrm{We} = \langle P^{univ}, Q^{univ}\rangle_{\mathcal{E}(N)}$ defines a map $\mathrm{We} : Y(N) \to \operatorname{Spec}\mathcal{O}_N$. It extends to a smooth proper map $\mathrm{We} : X(N) \to \operatorname{Spec}\mathcal{O}_N$ with geometrically connected fibres. In particular, $Y(N), X(N)$ are connected, and the geometric fibres of $X(N) \to \operatorname{Spec}\mathbb{Z}[1/N]$ (as well as those of its restriction to $Y(N)$) have exactly $\varphi(N)$ connected components.*

Furthermore, the natural left action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $Y(N)$ extends uniquely to the compactified moduli scheme $X(N)$, preserves the j-invariant, and the following diagram commutes, for any $M \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$:

$$\begin{array}{ccc} X(N) & \xrightarrow{M} & X(N) \\ \downarrow{\scriptstyle \mathrm{We}} & & \downarrow{\scriptstyle \mathrm{We}} \\ \operatorname{Spec}\mathcal{O}_N & \xrightarrow{\det M} & \operatorname{Spec}\mathcal{O}_N \end{array}$$

Proof. – First, $\operatorname{Spec}\mathcal{O}_N \to \operatorname{Spec}\mathbb{Z}[1/N]$ is finite étale. So the extension of We follows from Corollary A.2.5. The extension of the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ follows from the previous results and Proposition A.2.9. Since $X(N) \to \operatorname{Spec}\mathbb{Z}[1/N]$ is smooth proper of relative dimension one, and $\mathcal{O}_N$ is finite étale over $\mathbb{Z}[1/N]$, $\mathrm{We} : X(N) \to \operatorname{Spec}\mathcal{O}_N$ is smooth proper of relative dimension one.

To check that the extension of the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ preserves the j-invariant, it is enough to check it on $Y(N)$, where it is obvious. Checking that the diagram commutes can also be done after restricting to $Y(N)$ (by Proposition A.2.9), where it is an easy computation.

To discuss the geometric fibres of $\mathrm{We} : X(N) \to \operatorname{Spec}\mathcal{O}_N$, we see that $\mathrm{We} : Y(N) \to \operatorname{Spec}\mathcal{O}_N$ is the scheme representing the moduli problem $[\Gamma(N)]^{\mathbb{Z}[\zeta_N]-can}_{\mathcal{O}_N}$ (see [86, Propositions 9.3.1, (9.4.3.1)]), and apply [86, Corollary 10.9.2][9]. □

Lemma 1.3.10 *Let X be a scheme of finite type over a field k, Cohen-Macaulay of relative dimension one. Let $Z \subset X$ be a closed subscheme consisting of finitely many regular points of X. Then $C \in \pi_0(X) \longmapsto C\backslash Z \in \pi_0(X\backslash Z)$ is a bijection.*

Proof. – Suppose that Y is any quasi-compact Noetherian scheme. Then we know that the connected components of Y identify with the connected components of the graph $\mathcal{G}_Y$, whose vertices are the irreducible components of Y, and where two vertices (corresponding to irreducible components $Z \neq Z'$) are linked if and only if they have a nonempty intersection.

Thus, it is enough to prove the exact same statement when "connected components" are replaced with "irreducible components", and show that, given two irreducible components $Y \neq Y'$ of X, Y and Y' meet if and only if $Y\backslash Z$ and $Y'\backslash Z$ meet. Note that since X and $X\backslash Z$ are pure of dimension one, any subspace of either of them is an irreducible component if and only if it is closed, irreducible, and of Krull dimension one.

In particular, given an irreducible component $Y \subset X$, $Y\backslash Z$ is closed in $X\backslash Z$ and is a nonempty open subset of Y (otherwise Y would be contained in the zero-dimensional closed subspace Z, a contradiction), hence is irreducible and of Krull dimension one (because Y is of finite type over a field). Moreover, the reunion of the $Y\backslash Z$, where Y runs through the finitely many irreducible components of X, is exactly $X\backslash Z$, hence the $Y\backslash Z$ are the irreducible components of $X\backslash Z$.

Given two irreducible components $Y, Y' \subset X$, if $Y\backslash Z = Y'\backslash Z$, then $Y \cap Y'$ is a closed subpace of Y (resp. Y') containing the dense open subspace $Y\backslash Z$ (resp. $Y'\backslash Z$), hence $Y \cap Y' = Y = Y'$.

Given two distinct irreducible components $Y, Y' \subset X$, a point $x \in Y \cap Y'$ has the property that $\mathcal{O}_{X,x}$ contains two distinct minimal prime ideals, hence is not regular. Therefore $x \notin Z$.

[9] More directly, we can directly follow the argument given in [36]: by considering the complex uniformization, the base change to $\mathbb{C}$ of $\mathrm{We} : Y(N) \to \operatorname{Spec}\mathcal{O}_N$ is connected, whence $X(N)$ is connected, and it follows that $\mathcal{O}(X(N)) \otimes_{\mathcal{O}_N} \mathbb{C} \simeq \mathbb{C}$. Since $\mathcal{O}(X(N))$ is a finite, normal, integral $\mathcal{O}_N$-algebra, it is exactly $\mathcal{O}_N$, and $\mathcal{O}_{\operatorname{Spec}\mathcal{O}_N} \to \mathrm{We}_*\mathcal{O}_{X(N)}$ is an isomorphism. It follows by cohomology and base change that the formation of $\mathrm{We}_*\mathcal{O}_{X(N)}$ commutes with arbitrary base change, QED.

Thus Y meets Y' if and only if $Y\backslash Z$ meets $Y'\backslash Z$ and the conclusion follows. □

Corollary 1.3.11 *If G is a N-torsion group over any $\mathbb{Z}[1/N]$-algebra R, then the geometric fibres of $Y_G(N) \to \operatorname{Spec} R$ (resp. $X_G(N) \to \operatorname{Spec} R$ if R is regular excellent Noetherian) have exactly $\varphi(N)$ connected components.*

Proof. – The situation when G is constant and $R = \mathbb{Z}[1/N]$ is completely handled by Proposition 1.3.9 and Lemma 1.3.10. Let us discuss the general case. Let R' be a faithfully flat étale R-algebra such that $G_{R'}$ is constant. It is enough to prove the statements for $Y_{G_{R'}}(N) \to \operatorname{Spec} R'$ (resp. $X_{G_{R'}}(N) \to \operatorname{Spec} R'$ if R, and therefore R', is excellent). But $Y_{G_{R'}}(N) \to \operatorname{Spec} R'$ (resp. $X_{G_{R'}}(N) \to \operatorname{Spec} R'$) is a base change of $Y(N) \to \operatorname{Spec} \mathbb{Z}[1/N]$ (resp. $X(N) \to \operatorname{Spec} \mathbb{Z}[1/N]$), so it satisfies the conclusion. □

Proposition 1.3.12 *Suppose that G is a polarized N-torsion group over some $\mathbb{Z}[1/N]$-algebra R. Then the rule $(E/S, \iota) \longmapsto \det \iota \in (\mathbb{Z}/N\mathbb{Z})^\times_S$ defines a morphism $\det : Y_G(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$, which extends to $\det : X_G(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$ if R is regular excellent Noetherian. In either case, one has $\det \circ [u] = u^2 \cdot \det$ for $u \in (\mathbb{Z}/N\mathbb{Z})^\times$. Let, for each $u \in (\mathbb{Z}/N\mathbb{Z})^\times$, $Y_{G,u}(N)$ (resp. $X_{G,u}(N)$ if R is regular excellent Noetherian) the inverse image of u under $\det : Y_G(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$ (resp. $\det : X_G(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$), and $\mathcal{E}_{G,u}(N) = \mathcal{E}_G(N) \times_{Y_G(N)} Y_{G,u}(N)$. Then $\mathcal{E}_{G,u}(N)/Y_{G,u}(N)$ represents $\mathscr{P}_{G,u}$, and $\mathscr{P}_{G,u}$ is a finite étale surjective moduli problem over $\mathbf{Ell}_R$. Moreover, if R is regular excellent Noetherian, $\mathscr{P}_{G,u}$ is normal near infinity and $X_{G,u}$ identifies with the compactified moduli scheme $\overline{\mathscr{M}}(\mathscr{P}_{G,u})$; under this identification, the cuspidal subscheme of $X_{G,u}$ identifies with the inverse image of the cuspidal subscheme of $X_G(N)$ in $X_{G,u}(N)$.*

Proof. – It is clear that det is well-defined. By Corollary A.2.5, it extends to $X_G(N)$ if R is regular excellent Noetherian. If $\alpha \in \mathscr{P}_G$ is such that $(\mathcal{E}_G(N)/Y_G(N), \alpha)$ represents $\mathscr{P}_G$, it is a tautology that $(\mathscr{E}_{G,u}(N), Y_{G,u}(N), \alpha_{|\det^{-1}(u)})$ represents $\mathscr{P}_{G,u}$.

We need to show that $\mathscr{P}_{G,u}$ is finite étale over $\mathbf{Ell}_R$. To do that, consider an elliptic curve E/S where S is a R-scheme. Then there is a morphism of S schemes $\det : (\mathscr{P}_G)_{E/S} \to (\mathbb{Z}/N\mathbb{Z})^\times_S$ given by $(\iota : G_T \to E_T[N]) \longmapsto \det \iota \in (\mathbb{Z}/N\mathbb{Z})^\times_S(T)$. It is clear that $(\mathscr{P}_{G,u})_{E/S} = (\mathscr{P}_G) \times_{(\mathbb{Z}/N\mathbb{Z})^\times_S} u$, where u is the closed open immersion $S \to (\mathbb{Z}/N\mathbb{Z})^\times_S$ onto the component corresponding to u. Thus $(\mathscr{P}_{G,u})_{E/S} \to (\mathscr{P}_G)_{E/S}$ is a closed open immersion of S-schemes into a finite étale S-scheme, whence the conclusion.

To show that $\mathscr{P}_{G,u}$ is surjective, it is enough to show that for any elliptic curve E/k over an algebraically closed field where N is invertible, then $(\mathscr{P}_{G,u})_{E/k}$ is not the empty scheme, that is, that $\mathscr{P}_{G,u}(E/k)$ is not the empty set. Since G_k is constant, this follows from the fact that the Weil pairing $E[N](k) \times E[N](k) \to \mu_N(k)$ is surjective.

A consequence of the previous results is that, when R is regular excellent Noetherian, $Y_{G,u}(N)$ is a normal scheme, hence $\mathscr{P}_{G,u}$ is normal near infinity.

The closed open immersion $Y_{G,u} \to Y_G(N)$ extends to a finite map $\overline{\mathscr{M}}(\mathscr{P}_{G,u}) \to X_G(N)$. It comes from a morphism of moduli problems, so it preserves the j-invariant. Since the image of $Y_{G,u}(N)$ is contained in $X_{G,u}(N)$ and $Y_{G,u}(N)$ is dense in $\overline{\mathscr{M}}(\mathscr{P}_{G,u})$, the finite map $\overline{\mathscr{M}}(\mathscr{P}_{G,u}) \to X_G(N)$ factors through the closed open subscheme $X_{G,u}(N)$. This finite map $f : \overline{\mathscr{M}}(\mathscr{P}_{G,u}) \to X_{G,u}(N)$ is thus between normal schemes, and is an isomorphism above the dense open subscheme $Y_{G,u}(N)$ whose pre-image is dense. By Lemma A.2.6, f is an isomorphism. Since f clearly preserves the j-invariant, f also preserves the cuspidal subschemes.

Since $\det \circ [v] = v^2 \cdot \det$, $[v]$ induces an isomorphism $Y_{G,u}(N) \to Y_{G,uv^2}(N)$ of $\mathbb{A}^1_R$-schemes, which extends by Proposition A.2.9 to an isomorphism $X_{G,u}(N) \to X_{G,uv^2}(N)$ of $\mathbb{P}^1_R$-schemes where R is regular excellent Noetherian. □

Corollary 1.3.13 *Let G be a polarized N-torsion group over some $\mathbb{Z}[1/N]$-algebra R. Then, for any $u \in (\mathbb{Z}/N\mathbb{Z})^\times$:*

(i) *$Y_{G,u}(N) \to \operatorname{Spec} R$ (resp. $X_{G,u}(N) \to \operatorname{Spec} R$ if R is regular excellent Noetherian) is smooth of relative dimension one with connected geometric fibres (resp. proper smooth of relative dimension one with connected geometric fibres).*

(*ii*) *The j-invariant $Y_{G,u}(N) \to \mathbb{A}^1_R$ (resp. $X_{G,u}(N) \to \mathbb{P}^1_R$ if R is regular excellent Noetherian) is finite locally free, étale on the locus where j is defined and $j(j-1728)$ is invertible.*

(*iii*) *If R is regular excellent Noetherian, then $\mathscr{P}_{G,u}$ is smooth at infinity over $\mathbb{Z}[1/N]$ and the formation of its compactified moduli scheme and cuspidal subscheme commute with base change.*

Proof. – (*i*), (*ii*), (*iii*) all follow from Propositions 1.3.6 and 1.3.12, apart from the statement on geometric fibres. For each geometric point x of $\operatorname{Spec} R$, the associated geometric fibres of $(Y_{G,u})_x$ (or $(X_{G,u})_x$) are non-empty, and their disjoint reunion has $\varphi(N) = |(\mathbb{Z}/N\mathbb{Z})^\times|$ connected components by Corollary 1.3.11. It follows that each $(Y_{G,u})_x$ (or $(X_{G,u})_x$) is connected. □

Proposition 1.3.14 *Let $m_0, m_1, N \geq 1$ be pairwise coprime integers with $N \geq 3$ and m_0 square-free. Let $m = m_0 m_1$, G be a N-torsion group over some $\mathbb{Z}[(Nm_1)^{-1}]$-algebra R. Then the following properties hold:*

(*i*) *$\mathscr{P}_G(\Gamma_0(m))$ is representable by a scheme $Y_G(N, \Gamma_0(m))$, it is finite locally free of constant rank $r_{N,m} \geq 1$ over $\mathbf{Ell}_R$, étale above $\mathbb{Z}[1/m]$,*

(*ii*) *$Y_G(N, \Gamma_0(m)) \to \operatorname{Spec} R$ is affine, Cohen-Macaulay of relative dimension one with geometrically reduced fibres, smooth outside the supersingular j-invariants in characteristic $p \mid m_0$, its geometric fibres have $\varphi(N)$ connected components, and the j-invariant $Y_G(N, \Gamma_0(m)) \to \mathbb{A}^1_R$ is finite locally free of rank $r'_{N,m} \geq 1$, étale on the locus where $m_0 j(j-1728)$ is invertible.*

(*iii*) *If R is regular excellent Noetherian, $\mathscr{P}_G(\Gamma_0(m))$ is smooth at infinity over $\mathbb{Z}[(Nm_1)^{-1}]$,*

(*iv*) *If R is regular excellent Noetherian, the compactified moduli scheme $X_G(N, \Gamma_0(m))$ of $\mathscr{P}_G(\Gamma_0(m))$ is Cohen-Macaulay of relative dimension one over $\operatorname{Spec} R$, smooth outside the supersingular j-invariants in characteristic $p \mid m_0$; its geometric fibres are reduced and possess $\varphi(N)$ connected components,*

(*v*) *If R is regular excellent Noetherian, the j-invariant $X_G(N, \Gamma_0(m)) \to \mathbb{P}^1_R$ is finite locally free of constant rank $r'_{N,m}$,*

(*vi*) *The natural action of $(\mathbb{Z}/Nm\mathbb{Z})^\times$ on $\mathscr{P}_G(\Gamma_0(m))$ (as a moduli problem of level Nm) factors through the quotient to $(\mathbb{Z}/N\mathbb{Z})^\times$ and is equivariant for the natural forgetful map $\mathscr{P}_G(\Gamma_0(m)) \to \mathscr{P}_G$. If R is regular excellent Noetherian, it extends as an equivariant action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on the morphism $X_G(N, \Gamma_0(m)) \to X_G(N)$.*

Remark When G is constant, we write $Y_G(N, \Gamma_0(m)) = Y(\mathscr{P}_G, \Gamma_0(m))$ for short, and similarly for the compactified moduli scheme.

Proof. – The representability of the moduli problem follows from Proposition 1.1.12, using [86, Theorem 5.1.1] and Proposition 1.3.6, since we are taking the Cartesian product of $\mathscr{P}_G$ (representable) and $[\Gamma_0(m)]_R$ (relatively representable). It is finite locally free of constant positive rank (only depending on N, m) and étale above $\mathbb{Z}[1/m]$ over $\mathbf{Ell}_R$, because $\mathscr{P}_G$ and $[\Gamma_0(m)]_R$ are. The results of (*ii*) (apart from the number of connected components of the geometric fibres and the "constant rank $r'_{N,m} \geq 1$" part of the j-invariant) are the consequence of Corollary 1.1.14 and the first part of Proposition 1.2.20. In particular, $\mathscr{P}_G(N, \Gamma_0(m))$ is normal near infinity.

When $R = \mathbb{Z}[(Nm_1)^{-1}]$ and G is constant, since $\mathcal{E}(N)/Y(N)$ is a modular family in the sense of [86, §4.11], [86, Theorem 5.1.1] shows that $Y(N, \Gamma_0(m))$ is a regular scheme. Thus, the j-invariant map $X(N, \Gamma_0(m)) \to \mathbb{P}^1_{\mathbb{Z}[(Nm_1)^{-1}]}$ is finite between two regular Noetherian schemes (every nonempty open subset of either having dimension two), hence it is flat by the miracle flatness theorem [4, Lemma 00R4]. It is thus finite locally free of constant rank $r'_{N,m} \geq 1$, since $\mathbb{P}^1_{\mathbb{Z}[(Nm_1)^{-1}]}$ is connected.

In particular, $X(N, \Gamma_0(m)) \to \operatorname{Spec} \mathbb{Z}[(Nm_1)^{-1}]$ is proper flat. Moreover, $Y(N, \Gamma_0(m)) \to \mathbb{A}^1_{\mathbb{Z}}$ is finite locally free $r'_{N,m}$, and by taking arbitrary base change we find that the j-invariant map $Y_G(N, \Gamma_0(m)) \to \mathbb{A}^1_R$ is always of constant rank $r'_{N,m}$ when G is constant. Since G is always

étale-locally constant, it follows that $j : Y_G(N, \Gamma_0(m)) \to \mathbb{A}^1_{\mathbb{Z}[(Nm_1)^{-1}]}$ has rank $r'_{N,m}$ for any N-torsion group G.

When R is regular excellent Noetherian of generic characteristic zero or G is constant, (iii),(iv) (apart from the statement on the number of connected components of the geometric fibres) follow from Proposition 1.2.20 and Corollary 1.2.21.

If G be a N-torsion group over any regular excellent Noetherian $\mathbb{Z}[(Nm_1)^{-1}]$-algebra R, then there is a faithfully flat étale R-algebra R' such that $G_{R'}$ is constant. Thus, by Proposition 1.2.15 $\mathscr{P}_G(\Gamma_0(m))$ is smooth at infinity over $\mathbb{Z}[(Nm)^{-1}]$, and the formation of its compactified moduli scheme and cuspidal subscheme commutes with base change, thus (iii), (iv) (without, once again, the statement on the connected components of the geometric fibres) hold.

The compactification of the j-invariant is a finite map $\overline{j} : X_G(N, \Gamma_0(m)) \to \mathbb{P}^1_R$ of R-schemes, where the source is Cohen-Macaulay of relative dimension one over R, and the target is smooth over R of relative dimension one (with R regular). By miracle flatness, this implies that $\overline{j}$ is flat, hence locally free. Since it has rank $r'_{N,m}$ above the dense open subscheme $\mathbb{A}^1_R$, it is of constant rank $r'_{N,m}$.

The assertion (vi) is formal, using Proposition A.2.9 and the definition of the natural level Nm structure on $\mathscr{P}_G \times [\Gamma_0(m)]_R$, since it is clear that $(\mathbb{Z}/m\mathbb{Z})^\times$ acts trivially on the moduli problem $[\Gamma_0(m)]_R$.

To conclude, it is enough to prove the statement on the number of connected components of geometric fibres of $X(N, \Gamma_0(m)) \to \operatorname{Spec} \mathbb{Z}[(Nm_1)^{-1}]$ (by base change, this will hold whenever G is constant, and any G is étale locally constant). By [4, Lemma 0E0N], we only need to prove it when G is constant over $R = \mathbb{Z}[(Nm)^{-1}]$. It is thus enough to prove in this situation that $X_G(N, \Gamma_0(m)) \to X(N)_{\mathbb{Z}[(Nm)^{-1}]} \overset{\text{We}}{\to} \operatorname{Spec} \mathcal{O}_N[m^{-1}]$ has connected geometric fibres (since this map is proper smooth). This is a consequence of [86, Corollary 10.9.5], by setting $N_1 = N, K = Nm, N_2 = m$ and $\Gamma \leq \mathrm{GL}_2(\mathbb{Z}/Nm\mathbb{Z})$ the subgroup of upper-triangular matrices $M \equiv I_2 \mod N$. □

Corollary 1.3.16 *Let m_0, m_1, m, N, R, G be as in Proposition 1.3.14, and assume that R is Noetherian. Then the following statements hold:*

- (i) *If R is (R_k), $m_0 \in R$ is not a zero divisor, and [$k \leq 1$ or (R/pR is (R_k) for all $p \mid m_0$)], then $Y_G(N, \Gamma_0(m))$ is (R_k),*
- (ii) *If R is (S_k), then so is $Y_G(N, \Gamma_0(m))$,*
- (iii) *If R is reduced (resp. normal) and $m_0 \in R$ is not a zero divisor, $Y_G(N, \Gamma_0(m))$ is reduced (resp. normal),*
- (iv) *If R is regular excellent Noetherian and $m_0 \in R$ is not a zero divisor, then $X_G(N, \Gamma_0(m))$ is normal,*
- (v) *If R is regular excellent Noetherian and R/pR is (R_k) for all $p \mid m_0$, then $X_G(N, \Gamma_0(m))$ is (R_k).*

Proof. – Regularity ascends along smooth maps [4, Lemma 07NF], so $X_G(N, \Gamma_0(m))$ is regular at every point of its cuspidal subscheme. Hence (v) (resp. (iv)) follows from (i) (resp. (iii)). The reunion of (i) and (ii) implies (iii) by, for instance, Serre's criterion for normality (and the analog for reducedness) [4, Lemmas 031R, 031S]. (ii) is a consequence of the fact that $Y_G(N, \Gamma_0(m))$ is Cohen-Macaulay of relative dimension one over $\operatorname{Spec} R$.

Let us finally discuss (i): we assume that $m_0 \in R$ is not a zero divisor. After a faithfully flat étale base change, we can assume that G is constant. Since the kernel of $R \to R \otimes \mathbb{Q}$ is finitely generated, it is contained in the d-torsion of R for some integer $d \geq 1$ prime to Nm. Thus, after taking the Zariski-cover $\operatorname{Spec} R[1/m]$, $\operatorname{Spec} R[1/d]$, we can assume that either $m \in R^\times$ or R is flat over $\mathbb{Z}$. The first case follows from ascending properties of smooth maps, so from now on we assume that R is flat over $\mathbb{Z}$.

Let us first discuss the property (R_0) (resp. (R_1)). Let $U \subset Y(N, \Gamma_0(m))$ the open subset excluding the supersingular j-invariants in characteristic $p \mid m$. Then the complement

of U is finite, hence by the going-down theorem [4, Lemma 00HS] (applied to the flat map $Y_G(N,\Gamma_0(m)) \to Y(N,\Gamma_0(m))$) the complement of U_R in $Y(N,\Gamma_0(m))_R$ cannot contain points of codimension zero or one. Since $U \to \operatorname{Spec}\mathbb{Z}$ is smooth, U_R is (R_0) (resp. (R_1)) and we are done.

Now, we fix some $k \geq 0$ and assume that R and each R/pR (for $p \mid m_0$) is (R_k). The map $Y_G(N,\Gamma_0(m))_R \to Y(N,\Gamma_0(m))$ is affine and flat to a regular base scheme, and the rings of fibres are of the form $R \otimes_{\mathbb{Z}} F$, where F is a finitely generated field extension of a field k which is either finite or $\mathbb{Q}$. We need to prove that these $R \otimes_{\mathbb{Z}} F$ satisfy the property (R_k). By considering the map $R \otimes_{\mathbb{Z}} k \to R \otimes_{\mathbb{Z}} F$, all we need to show is that the fibre rings of $R \otimes_{\mathbb{Z}} k \to R \otimes_{\mathbb{Z}} F$ are (R_k). These fibres are regular by [4, Lemma 0381] since k is perfect and F is finitely generated. □

Definition 1.3.17 If G is constant over R, the following map (denoted We) is the *Weil pairing*:

$$X_G(N,\Gamma_0(m)) \to X_G(N) \simeq X(N)_R \overset{\mathrm{We}}{\to} \operatorname{Spec}\mathcal{O}_N \times_{\mathbb{Z}} \operatorname{Spec} R.$$

If G is polarized, we call det (the determinant) the map $X_G(N,\Gamma_0(m)) \to X_G(N) \overset{\det}{\to} (\mathbb{Z}/N\mathbb{Z})^{\times}_R$.

Corollary 1.3.18 *The maps* We *and* det *from Definition 1.3.17 are flat surjective with connected geometric fibres. In particular, $X(N,\Gamma_0(m))$ and $Y(N,\Gamma_0(m))$ are irreducible.*

Proof. – In the case of the Weil pairing map, it is enough to prove the result when $R = \mathbb{Z}[1/N]$. Then $X(N,\Gamma_0(m)) \to \operatorname{Spec}\mathcal{O}_N \to \operatorname{Spec}\mathbb{Z}[1/N]$ is surjective, and its geometric fibres have $\varphi(N)$ connected components. Since $\operatorname{Spec}\mathcal{O}_N$ is finite étale over $\operatorname{Spec}\mathbb{Z}[1/N]$, $X(N,\Gamma_0(m))$ is proper flat over $\operatorname{Spec}\mathcal{O}_N$ and in particular surjective. If k is an algebraically closed field of characteristic not dividing N, it is easy to see that the geometric fibre of $X(N,\Gamma_0(m))$ at $\mathbb{Z}[1/N] \to k$ is exactly the disjoint reunion of the geometric fibres of $X(N,\Gamma_0(m)) \to \operatorname{Spec}\mathcal{O}_N$ for all $\varphi(N)$ morphisms $\mathcal{O}_N \to k$. All of these $\varphi(N)$ geometric fibres are nonempty, but their disjoint reunion has exactly $\varphi(N)$ connected components: this shows that they must each be connected.

The map $\mathrm{We} : X(N,\Gamma_0(m)) \to \operatorname{Spec}\mathcal{O}_N[1/m_1]$ is smooth with geometrically connected fibres. Therefore $X(N,\Gamma_0(m))_{\mathbb{Q}}$ is a regular connected scheme (hence irreducible), and it is dense in $X(N,\Gamma_0(m))$, whence $X(N,\Gamma_0(m))$ (and thus $Y(N,\Gamma_0(m))$) is irreducible.

For the geometric fibres of det, a similar argument reduces the problem to showing that for any $u \in (\mathbb{Z}/N\mathbb{Z})^{\times}$ and any algebraically closed field k of residue characteristic not dividing N, there is an element in $X(N,\Gamma_0(m))(k)$. Let E/k be any elliptic curve (ordinary if m vanishes in k, for instance with j-invariant taken outside $\mathbb{F}_{p^2}$ by [86, Lemma 12.5.4]), there are isomorphisms of arbitrary determinant $G_k \to E[N](k)$ since $G, E[N]$ are constant étale, and there is an arbitrary finite étale subgroup scheme of $E[m]$, cyclic of order m (if needed by separating the p part, where $p \mid m$ is the characteristic of k). □

Corollary 1.3.19 *In Corollary 1.1.31, the map $D_{d,t}$ is finite locally free of constant rank, which is independent from the moduli problem.*

Proof. – Using the same reduction than the proof of Corollary 1.1.31 (whose notations we keep), it is enough to prove the statement when $\mathscr{P} = [\Gamma(\ell)]_{\mathbb{Z}[1/\ell]}$ with $\ell \nmid 2m$ some prime. Assume more generally that $\mathscr{P} = [\Gamma(k)]_{\mathbb{Z}[1/k]}$ where $k \geq 3$ is any integer prime to m. Then $D_{d,t}$ is a finite locally free morphism $Y(k,\Gamma_0(m)) \to Y(k,\Gamma_0(t))$ between regular irreducible $\mathbb{Z}[1/k]$-schemes, so that it is locally free of constant rank $r_k \geq 1$. By Proposition 1.1.26, for any primes $\ell, \ell' \nmid 2m$, we then have $r_\ell = r_{\ell\ell'} = r_{\ell'}$, and the conclusion follows. □

Corollary 1.3.20 *Let m_0, m_1, m, N, R, G be as in Proposition 1.3.14 and assume that G is polarized. Let $u \in (\mathbb{Z}/N\mathbb{Z})^{\times}$. Then the moduli problem $\mathscr{P}_{G,u}(\Gamma_0(m)) := \mathscr{P}_{G,u} \times_{\mathscr{P}_G} \mathscr{P}_G(\Gamma_0(m))$ over $\mathbf{Ell}_R$ is representable by the closed open subscheme $\det^{-1}(u)$ of $Y_G(N,\Gamma_0(m))$. This moduli problem is finite locally free surjective over $(\mathbf{Ell}_R)$. Moreover, if R is regular excellent Noetherian, $\mathscr{P}_{G,u}(\Gamma_0(m))$ is normal near infinity and the closed open subscheme $X_{G,u}(N,\Gamma_0(m)) = \det^{-1}(u)$*

of $X_G(N,\Gamma_0(m))$ identifies with the compactified moduli scheme $\overline{\mathscr{M}}(\mathscr{P}_{G,u})$; under this identification, the cuspidal subscheme $C_{\mathscr{P}_{G,u}}$ identifies with the inverse image of the cuspidal subscheme of $X_G(N,\Gamma_0(m))$ in $X_{G,u}(N,\Gamma_0(m))$. The $Y_{G,u}(N,\Gamma_0(m))$ (resp. the $X_{G,u}(N,\Gamma_0(m))$) seen as R-schemes, have geometrically connected fibres.

Proof. – The first part is completely formal, apart from the surjectivity. It is enough to show that for any elliptic curve E over an algebraically closed field k where Nm_1 is invertible, $\mathscr{P}_{G,u}(\Gamma_0(m))(E/k)$ is nonempty. This is clear since G is étale, hence constant, and the Weil pairing $E[N]\times E[N]\to\mu_N$ is onto, while, if some prime power $q\mid m$ is invertible in k, we can choose as $\Gamma_0(q)$-structure any cyclic subgroup generated by a point of order q, and if there is a prime p that vanishes in k and divides m, then p prime to m/p and the kernel of the Frobenius (see Section 1.5.1) is a $\Gamma_0(p)$-structure.

The moduli problem $\mathscr{P}_{G,u}$ is normal near infinity because $Y_{G,u}(N,\Gamma_0(m))\to Y_G(N,\Gamma_0(m))$ is a closed open immersion. Its compactification in the sense of Proposition A.2.9 is a finite map $f_u:\overline{\mathscr{M}}(\mathscr{P}_{G,u}(\Gamma_0(m)))\to X_G(N,\Gamma_0(m))$ whose image is contained in the closed open subscheme $\det^{-1}(u)$. In other words, $f_u:\overline{\mathscr{M}}(\mathscr{P}_{G,u}(\Gamma_0(m)))\to X_{G,u}(N,\Gamma_0(m))$ is a finite morphism and is an isomorphism above the dense open subscheme $Y_{G,u}(N,\Gamma_0(m))$ with dense inverse image. Both schemes are normal on the inverse image of the closed subspace $\{1/j=0\}$. By Lemma A.2.6, f_u is an isomorphism, and in particular it induces an isomorphism from $C_{\mathscr{P}_{G,u}(\Gamma_0(m))}$ to the restriction to $C_{\mathscr{P}_G(\Gamma_0(m))}$ to $\det^{-1}(u)$ (since the induced map is an isomorphism on the underlying topological space, while the two subschemes are reduced).

For the last part, by Proposition 1.3.14, the disjoint reunion of the connected components of the geometric fibres of $Y_{G,u}(N,\Gamma_0(m))$ (resp. $X_{G,u}(N,\Gamma_0(m))$) over a geometric point $\overline{x}$ of R (resp. assuming that R is regular excellent Noetherian) over all $u\in(\mathbb{Z}/N\mathbb{Z})^\times$ has exactly $\varphi(N)=|(\mathbb{Z}/N\mathbb{Z})^\times|$ elements. Since every $Y_{G,u}(N,\Gamma_0(m))\to\operatorname{Spec}R$ is surjective, its geometric fibres have to be connected. □

Proposition 1.3.21 *Let $N\geq 3$, R be a $\mathbb{Z}[1/N]$-algebra (resp. R is a regular excellent Noetherian $\mathbb{Z}[1/N]$-algebra) and G be a N-torsion group over R. The collection of $Y_G(N,\Gamma_0(m))$ (resp. $X_G(N,\Gamma_0(m))$), for integers $m=m_0m_1$ coprime to N with $m_0,m_1\geq 1$, m_0 square-free and $m_1\in R^\times$, is endowed with degeneracy maps $D_{d,t}$ and Atkin-Lehner automorphisms as in Propositions 1.1.23 and 1.1.29 (resp. Proposition 1.2.17). They are finite locally free of constant rank, and commute with the action of $(\mathbb{Z}/N\mathbb{Z})^\times$. The relations stated in Corollary 1.1.25 and Proposition 1.1.29 still hold.*

Proof. – This is a direct translation of what we previously did in this more concrete context. The specific statements are Propositions 1.1.23, 1.1.29, 1.2.17, as well as Corollaries 1.1.25, 1.2.19, 1.3.19. □

Proposition 1.3.22 *Let m_0,m_1,m,N,R,G be as in Proposition 1.3.14. Assume that G is constant.*

- *Then $Y(N,\Gamma_0(m))$ has a natural action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ which commutes to every degeneracy map and Atkin-Lehner automorphism. A matrix $\begin{pmatrix}a&b\\c&d\end{pmatrix}$ acts by*

$$(E/S,(P,Q),C)\longmapsto(E/S,(aP+bQ,cP+dQ),C).$$

  Moreover, the action of aI_2 (for $a\in(\mathbb{Z}/N\mathbb{Z})^\times$) is exactly the action of $[a']$ for any $a'\in(\mathbb{Z}/Nm\mathbb{Z})^\times$ congruent to a modulo N.
- *If moreover R is regular excellent Noetherian, this action extends to $X_G(N,\Gamma_0(m))$ and commutes to the extensions of degeneracy maps and Atkin-Lehner automorphisms; moreover, the action of aI_2 is given by any $[a']$ for any $a'\in(\mathbb{Z}/Nm\mathbb{Z})^\times$ congruent to a modulo N.*

Proof. – This follows from the fact that $\mathscr{P}(N)$ has a natural level structure of level N, and that the natural action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $\mathscr{P}(N)$ acts by morphisms of moduli problems of level N, as well as Corollary 1.1.25 and Proposition 1.1.29. The action of scalar matrices is an explicit computation. The second point follows from Proposition A.2.9. □

Proposition 1.3.23 *Let m_0, m_1, m, N, R, G be as in Proposition 1.3.14.*

- *Suppose that G is constant and that $d, t \geq 1$ are such that $dt \mid m$ (resp. $d \geq 1$ divides m and is coprime to m/d). Then $\mathrm{We} \circ D_{d,t} = \underline{d} \circ \mathrm{We}$ (resp. $\mathrm{We} \circ w_d = \underline{d} \circ \mathrm{We}$).*
- *Suppose that G is polarized and that $d, t \geq 1$ are such that $dt \mid m$ (resp. $d \geq 1$ divides m and is coprime to m/d). Then $\det \circ D_{d,t} = d \cdot \det$ (resp. $\det \circ w_d = d \cdot \det$).*
- *When R is regular excellent Noetherian, both identities extend to $X_G(N, \Gamma_0(m))$.*

Proof. – The first two points are direct computations. The third point follows from the previous two and the fact that $S(X_G(N, \Gamma_0(m))) \to S(Y_G(N, \Gamma_0(m)))$ is injective for any separated scheme S by Proposition A.2.9. □

The methods of this section can be applied, *mutans mutandis*, to prove the following statement:

Proposition 1.3.24 *Let $N \geq 5$ be an integer and $m = m_0 m_1$ be coprime to N, with m_0 square-free and coprime to m_1.*

- *For any $\mathbb{Z}[1/(Nm_1)]$-algebra R, the moduli problem $[\Gamma_1(N)]_R \times [\Gamma_0(m)]_R$ is representable, finite flat of constant rank over $\mathbf{Ell}_R$, étale above $R[m_0^{-1}]$. Write $Y_1(N, \Gamma_0(m))_R$ for the moduli scheme. The natural action of $(\mathbb{Z}/Nm\mathbb{Z})^\times$ on $Y_1(N, \Gamma_0(m))$ factors through $(\mathbb{Z}/N\mathbb{Z})^\times$.*
- *$Y_1(N, \Gamma_0(m))_R \to \operatorname{Spec} R$ is affine, Cohen-Macaulay of relative dimension one, smooth outside the supersingular j-invariants in characteristic $p \mid m_0$, with geometrically connected fibres.*
- *When R is regular excellent Noetherian, this moduli problem is smooth at infinity over $\mathbb{Z}[(Nm_1)^{-1}]$, its compactified moduli scheme $X_1(N, \Gamma_0(m))$ is finite locally free of constant rank over $\mathbb{P}^1_R$, proper Cohen-Macaulay of relative dimension one over $\operatorname{Spec} R$ with geometrically connected fibres, and smooth outside the supersingular j-invariants in characteristic $p \mid m_0$. The natural action of $(\mathbb{Z}/Nm\mathbb{Z})^\times$ factors through $(\mathbb{Z}/N\mathbb{Z})^\times$.*
- *The formation of $X_1(N, \Gamma_0(m))$ and its cuspidal subscheme commutes with arbitrary base change of regular excellent Noetherian $\mathbb{Z}[(Nm_1)^{-1}]$-algebras.*

The conclusions of Proposition 1.3.21 apply here after replacing $Y_G(N, \Gamma_0(m))$ with $Y_1(N, \Gamma_0(m))$ (resp. $X_G(N, \Gamma_0(m))$ with $X_1(N, \Gamma_0(m))$ if R is regular excellent Noetherian).

1.4 Properties of Galois twists

In this section, we fix an integer $N \geq 3$ and a field k of characteristic not dividing N with separable closure k_s. We fix a left representation $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

1.4.1 $Y_\rho(N)$ and its rational points

Definition 1.4.1 The group $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on the following diagram of quasi-projective k-schemes (and trivially on the second row)

$$\begin{array}{ccccc} Y(N)_k & \xrightarrow{\text{in}} & X(N)_k & \xleftarrow[\text{cl}]{} & C_N \\ \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle \bar{j}} & & \downarrow \\ \mathbb{A}^1_k & \xrightarrow{\text{in}} & \mathbb{P}^1_k & \xleftarrow[\infty]{} & \operatorname{Spec} k \end{array}$$

Twisting by ρ thus gives a diagram of quasi-projective k-schemes:

$$\begin{array}{ccccc} Y_\rho(N)_k & \xrightarrow{\text{in}} & X_\rho(N) & \xleftarrow[\text{cl}]{} & C_{N,\rho} \\ \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle \bar{j}} & & \downarrow \\ \mathbb{A}^1_k & \xrightarrow{\text{in}} & \mathbb{P}^1_k & \xleftarrow[\infty]{} & \operatorname{Spec} k \end{array}$$

Moreover, the first cell is a Cartesian diagram, $j, \bar{j}$ are finite flat of constant rank, and $C_{N,\rho}$ is finite étale over k. Moreover, $X_\rho(N)$ is smooth over $\operatorname{Spec} k$.

Proof. – This follows from Propositions A.1.11 and A.1.13, as well as the properties of $X(N)$ discussed in the previous section, and the fact that finiteness, flatness, étaleness, smoothness descend along fpqc covers. □

Lemma 1.4.2 *Let E/k be an elliptic curve and $P, Q \in E[N](k_s)$ be such that $E[N](k_s)$ is free over $\mathbb{Z}/N\mathbb{Z}$ with basis (P, Q). For every $\sigma \in \operatorname{Gal}(k_s/k)$, define $D(\sigma) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $D(\sigma)\begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} \sigma(P) \\ \sigma(Q) \end{pmatrix}$. Then $D(\sigma\sigma') = D(\sigma')D(\sigma)$ for all $\sigma, \sigma' \in \operatorname{Gal}(k_s/k)$.*

Proof. – Simple computation. □

From this result, we obtain a description of the rational points of $Y_\rho(N)$.

Proposition 1.4.3 *For any subextension L of k_s/k, $Y_\rho(N)(L)$ is in natural bijection with the L-isomorphism classes of triples (E, P, Q) satisfying the following properties:*

- *E is an elliptic curve defined over L,*
- *$P, Q \in E[N](k_s)$ and $E[N](k_s)$ is free over $\mathbb{Z}/N\mathbb{Z}$ with basis (P, Q),*
- *For all $\sigma \in \operatorname{Gal}(k_s/L)$, $\begin{pmatrix} \sigma(P) \\ \sigma(Q) \end{pmatrix} = \rho^{-1}(\sigma)\begin{pmatrix} P \\ Q \end{pmatrix}$.*

If $x \in Y_\rho(N)(L)$ is given by the triple (E, P, Q), then $j(x) \in \mathbb{P}^1(L)$ is the j-invariant of E.

Proof. – Let $k \subset L \subset k_s$ be a subextension. Then, by [86, (4.3.1)], $Y_\rho(N)(L)$ is in bijection with the triples (E, P, Q), where E is an elliptic curve over k_s, and (P, Q) is a basis of $E[N](k_s)$ such that, for every $\sigma \in \operatorname{Gal}(k_s/L)$, one has $(E, P, Q) \simeq_{\overline{k_s}} (\sigma(E), a\sigma(P) + b\sigma(Q), c\sigma(P) + d\sigma(Q))$, where $\rho(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. In particular, $j(E) \in k_s$ is fixed by G_L, hence we can assume that E is defined over L, and that, for all $\sigma \in G_L$ with $\rho(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, there is a k_s-automorphism t_σ of E_{k_s} mapping (P, Q) to $(a\sigma(P) + b\sigma(Q), c\sigma(P) + d\sigma(Q))$.

We claim that $\sigma \longmapsto t_\sigma^{-1}$ satisfies the cocycle property of Proposition A.1.11. Since the identity involves two k_s-automorphisms of E_{k_s}, it is enough, by rigidity, to check it on $E[N](k_s)$, and hence on P and Q. Let $\sigma, \sigma' \in \operatorname{Gal}(k_s/L)$ and $\rho(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \rho(\sigma') = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Then

$$\begin{aligned} t_{\sigma\sigma'}(P) &= (aa' + bc')\sigma(\sigma'(P)) + (ab' + bd')\sigma(\sigma'(Q)) \\ &= a\sigma(a'\sigma'(P) + b'\sigma'(Q)) + b\sigma(c'\sigma'(P) + d'\sigma'(Q)) = a\sigma(t_{\sigma'}(P)) + b\sigma(t_{\sigma'}(Q)) \\ &= \sigma \circ t_{\sigma'} \circ \sigma^{-1}(a\sigma(P) + b\sigma(Q)) = \sigma t_{\sigma'} \sigma^{-1} t_\sigma(P), \end{aligned}$$

and similarly for Q, hence the cocycle property holds.

Let $E' = E_{t^{-1}}$ be the twisted elliptic curve over L: we still have $P, Q \in E'[N](k_s)$, and (E', P, Q) corresponds to the same point of $Y(N)(k_s)$ as (E, P, Q). Let now $\sigma \in \operatorname{Gal}(k_s/L)$, and write $\rho(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \rho(\sigma)^{-1} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Then one has

$$\sigma_{E'}(P) = t_\sigma^{-1}\sigma_E(P) = t_\sigma^{-1}(a'(a\sigma(P) + b\sigma(Q)) + b'(c\sigma(P) + d\sigma(Q))) = a'P + b'Q,$$

hence $\begin{pmatrix}\sigma_{E'}(P)\\ \sigma_{E'}(Q)\end{pmatrix} = \rho(\sigma)^{-1}\begin{pmatrix}P\\ Q\end{pmatrix}$.

In other words, we proved that every point in $Y_\rho(N)(L)$ came from a triple satisfying the required conditions. Conversely, it is clear that every such triple produces a k_s-rational point on $Y_\rho(N)$ stable under $\mathrm{Gal}(k_s/L)$, hence a L-rational point.

To conclude, all we need to do is show that any two triples $(E,P,Q),(E',P',Q')$ satisfying the requested conditions and representing the same point in $Y(N)(k_s)$ are L-isomorphic. Indeed, these triples are isomorphic over k_s by [86, (4.3.1)], so let $f : E_{K_s} \to E'_{K_s}$ be a k_s-isomorphism mapping (P,Q) to (P',Q'). One easily checks that the induced map $f[N] : E[N](k_s) \to E'[N](k_s)$ commutes to $\mathrm{Gal}(k_s/L)$, hence by rigidity the same holds for f, so that f is defined over L by Corollary A.1.10, and f is by fpqc descent an isomorphism.

The last statement is clear from the construction and the definition of Y_ρ. □

Proposition 1.4.4 *Let $\chi : \mathrm{Gal}(k_s/k) \to \{\pm 1\}$ be a character, and let*

$$\rho' = \chi \otimes \rho : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

The natural k_s-isomorphism between the following two diagrams

$$\begin{array}{ccccc} Y_\rho(N)_k & \xrightarrow{\text{in}} & X_\rho(N)_k & \xleftarrow[\text{cl}]{} & (C_N)_\rho \\ \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle \bar{j}} & & \downarrow \\ \mathbb{A}^1_k & \xrightarrow{\text{in}} & \mathbb{P}^1_k & \xleftarrow[\infty]{} & \operatorname{Spec} k \end{array} \qquad \begin{array}{ccccc} Y_{\rho'}(N)_k & \xrightarrow{\text{in}} & X_{\rho'}(N)_k & \xleftarrow[\text{cl}]{} & (C_N)_{\rho'} \\ \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle \bar{j}} & & \downarrow \\ \mathbb{A}^1_k & \xrightarrow{\text{in}} & \mathbb{P}^1_k & \xleftarrow[\infty]{} & \operatorname{Spec} k \end{array}$$

coming from the definition of a Galois twist is defined over k.

Moreover, for any finite subextension $L \subset k_s$ of k, the induced map $Y_\rho(N)(L) \to Y_{\rho'}(N)(L)$ is described, through the description of Proposition 1.4.3, by the rule $(E,P,Q) \longmapsto (E \otimes \chi, P, Q)$, where $E \otimes \chi$ is the quadratic twist of E by $\chi_{|\mathrm{Gal}(k_s/L)}$.

Proof. – By Corollary A.1.10, since it involves quasi-compact k-schemes, the isomorphism is defined over k as long as it commutes to $\mathrm{Gal}(k_s/k)$. Since $X_\rho(N), X_{\rho'}(N)$ are proper smooth over k, it is enough to check that the induced bijection $Y_\rho(N)(k_s) \to Y_{\rho'}(N)(k_s)$ commutes with the action of $\mathrm{Gal}(k_s/k)$.

Now, given $\sigma \in \mathrm{Gal}(k_s/k)$ and an elliptic curve E/k_s with a basis (P,Q) of $E[N]$, let $x \in Y_\rho(N)(k_s), x' \in Y_\rho(N)(k_s)$ be the geometric points attached to the triple (E,P,Q). If $\rho(\sigma) = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$, then one computes that

$$\begin{aligned}\sigma(x) &= (\sigma(E), a\sigma(P) + b\sigma(Q), c\sigma(P) + d\sigma(Q)),\\ \sigma(x') &= (\sigma(E), \chi(\sigma)(a\sigma(P) + b\sigma(Q)), \chi(\sigma)(c\sigma(P) + d\sigma(Q))).\end{aligned}$$

The two triples are isomorphic (by the automorphism $\chi(\sigma)$ of $\sigma(E)$) and therefore equal as geometric points of $Y_\rho(N)$.

Let now L/k be a subextension of k_s/k and (E,P,Q) be a triple as in Proposition 1.4.3 parametrizing some L-point of $Y_\rho(N)$. Then its image in $Y_{\rho'}(N)(L)$ is parametrized by a triple (E',P',Q') which satisfies the conditions of Proposition 1.4.3 (but for the left representation ρ') and is isomorphic to (E,P,Q) over k_s. This Proposition shows that (E',P',Q') is uniquely determined up to L-isomorphism. It is enough to check that $(E \otimes \chi, P, Q)$ satisfies the requested conditions. □

1.4.2 Comparison with the X_G

Recall the following classical result.

Proposition 1.4.5 *Let k be a field with separable closure k_s. The functor $G \longmapsto G(k_s)$, from finite étale commutative group schemes over k to finite discrete $\mathrm{Gal}(k_s/k)$-modules, is an equivalence of categories.*

Corollary 1.4.6 *Let k be a field with separable closure k_s and N an integer invertible in k. Let G be a finite étale group scheme over k, étale-locally isomorphic to $(\mathbb{Z}/N\mathbb{Z})^{\oplus 2}$. Fix a basis (A, B) of $G(k_s)$ over $\mathbb{Z}/N\mathbb{Z}$, and define, for every $\sigma \in \mathrm{Gal}(k_s/k)$, $D_G(\sigma) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ by $D_G(\sigma)\begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} \sigma(A) \\ \sigma(B) \end{pmatrix}$, so that $\sigma \longmapsto D_G(\sigma)$ is a group anti-homomorphism.*

Let E be an elliptic curve over k. Let $\mathscr{B}_{D_G}(E)$ denote the collection of bases (P, Q) of $E[N](k_s)$ such that for every $\sigma \in \mathrm{Gal}(k_s/k)$, one has $D_G(\sigma)\begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} \sigma(P) \\ \sigma(Q) \end{pmatrix}$. Then

$$\varphi \in \mathrm{Iso}_{k-Gp}(G, E[N]) \longmapsto (\varphi(A), \varphi(B)) \in \mathscr{B}_{D_G}(E)$$

is a bijection.

Proposition 1.4.7 *Let $N \geq 3, m_0, m_1 \geq 1$ be integers such that m_0, m_1, N are pairwise coprime, m_0 is square-free and $m_1 N$ is invertible in k, and let $m = m_0 m_1$. Let $X_\rho(N, \Gamma_0(m))$ denote the twist of $X(N, \Gamma_0(m))_k$ by ρ (since $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $X(N, \Gamma_0(m))$).*

Then, the j-invariant, the Atkin-Lehner automorphisms and the degeneracy maps (from Proposition 1.3.21) can be twisted to finite locally free morphisms between the $X_\rho(N, \Gamma_0(m))$ (or with target $\mathbb{P}^1_k$) satisfying the same relations as Proposition 1.3.21. In particular, the j-invariant $X_\rho(N, \Gamma_0(m)) \to \mathbb{P}^1_k$ is well-defined and $X_\rho(N, \Gamma_0(m))$ is smooth over k at every point, except, when m_0 vanishes in k, the points whose j-invariant is supersingular.

For every subextension L/k of k_s/k, the points $x \in X_\rho(N, \Gamma_0(m))(L)$ with $j(x) \in \mathbb{A}^1_k(L)$ identify with the L-isomorphism classes of quadruples (E, P, Q, C) such that:

- *E is an elliptic curve over L and $P, Q \in E(k_s)$ form a basis of $E[N](k_s)$,*
- *C is a cyclic subgroup of E of degree m,*
- *For all $\sigma \in \mathrm{Gal}(k_s/L)$, $\begin{pmatrix} \sigma(P) \\ \sigma(Q) \end{pmatrix} = \rho^{-1}(\sigma)\begin{pmatrix} P \\ Q \end{pmatrix}$.*

Under this identification, the descriptions of the degeneracy maps (resp. the Atkin-Lehner automorphisms) in Proposition 1.1.23 (resp. Proposition 1.1.29) still apply.

Proof. – The $X(N, \Gamma_0(m))_k$ are proper k-schemes of dimension one hence projective [4, Lemma 0A26], and they have an action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for which the degeneracy maps and Atkin-Lehner involutions are equivariant: the existence and regularity of $X_\rho(N, \Gamma_0(m))$ and twisted degeneracy maps (as well as their relations) is a consequence of Propositions A.1.11, A.1.13, and the previous results on the $X(N, \Gamma_0(m))_k$.

To prove that we identified correctly the rational points of $X_\rho(N, \Gamma_0(m))$ (as well as the claims about the behavior of the degeneracy maps and the Atkin-Lehner automorphisms), it is enough to show that every $(E, P, Q, C) \in X_\rho(N, \Gamma_0(m))(k_s)$ stable under $\mathrm{Gal}(k_s/L)$ is represented by a unique L-isomorphism class of (E', P', Q', C') as in the statement of the Proposition. To this end, we argue as in Proposition 1.4.3.

Let L/k be a subextension of k_s/k. Let us call (E, P, Q, C) a good quadruple over L if the following conditions are satisfied:

- E is an elliptic curve over L and $P, Q \in E(k_s)$ form a basis of $E[N](k_s)$,
- C is a cyclic subgroup of E of degree m,
- For all $\sigma \in \mathrm{Gal}(k_s/L)$, $\begin{pmatrix} \sigma(P) \\ \sigma(Q) \end{pmatrix} = \rho^{-1}(\sigma)\begin{pmatrix} P \\ Q \end{pmatrix}$.

In order to conclude the proof of the Proposition, we only need to show that every non-cuspidal point $(E, P, Q, C) \in X_\rho(N, \Gamma_0(m))(k_s)$ stable under $\mathrm{Gal}(k_s/L)$ is represented by a

unique L-isomorphism class of quadruple (E', P', Q', C') which is good for L. The argument mimics the proof of Proposition 1.4.3.

Let $(E_1, P_1, Q_1, C_1), (E_2, P_2, Q_2, C_2)$ be two good quadruples over L that are k_s-isomorphic. Then there is a k_s-isomorphism $\iota : (E_1)_{k_s} \to (E_2)_{k_s}$ mapping (P_1, Q_1, C_1) to (P_2, Q_2, C_2). For any $\sigma \in \mathrm{Gal}(k_s/L)$, the k_s-automorphism $\iota^{-1} \circ (\mathrm{id} \times \mathrm{Spec}\, \sigma^{-1}) \circ \iota \circ (\mathrm{id} \times \mathrm{Spec}\, \sigma)$ of $(E_1)_{k_s}$ agrees with the identity on $E_1[N]$ (by the assumptions on (P_1, Q_1) and (P_2, Q_2)), hence, by rigidity [86, Corollary 2.7.4], ι commutes with $\mathrm{Gal}(k_s/L)$, hence ι is defined over L by Corollary A.1.10.

By Proposition 1.4.3, a non-cuspidal L-rational point with finite j-invariant on $X_\rho(N, \Gamma_0(m))$ is given by a k_s-isomorphism class of (E, P, Q, C), where E/L is an elliptic curve, $P, Q \in E[N](k_s)$ form a basis of $E[N](k_s)$, one has $\begin{pmatrix}\sigma(P)\\ \sigma(Q)\end{pmatrix} = \rho^{-1}(\sigma)\begin{pmatrix}P\\ Q\end{pmatrix}$ for all $\sigma \in \mathrm{Gal}(k_s/L)$, and $C \leq E_{k_s}$ is a cyclic subgroup of degree m.

Choose $\sigma \in \mathrm{Gal}(L/k_s)$ and let $\rho(\sigma) = \begin{pmatrix}a & b\\ c & d\end{pmatrix}$. Then

$$\begin{aligned}[(E, P, Q, C)] &= \sigma([(E, P, Q, C)]) \\ &= [(E, a\sigma(P) + b\sigma(Q), c\sigma(P) + d\sigma(Q), \sigma(C))] = [(E, P, Q, \sigma(C))],\end{aligned}$$

so there is a k_s-automorphism ι of E_{k_s} preserving (P, Q) and mapping C to $\sigma(C)$. By rigidity, ι is the identity, so $C = \sigma(C)$.

Hence, as a Weil divisor on E_{k_s}, C is invariant by $\mathrm{Gal}(k_s/L)$, so the Weil divisor attached to C comes from a Weil divisor on E_L (with degree m). Since E_L is a regular scheme, C comes from a Cartier divisor C_0 on E_L of degree m. Since $C = (C_0)_{k_s}$ is a subgroup scheme of E_{k_s}, Corollary A.1.10 implies that C_0 is a subgroup scheme of E of degree L. Since C is fppf-locally cyclic, by approximation, C_0 is fppf-locally cyclic, and (E, P, Q, C_0) is a good quadruple for L that represents (E, P, Q, C). □

Proposition 1.4.8 *Let G be a finite étale group scheme over k, étale-locally isomorphic to $(\mathbb{Z}/N\mathbb{Z})^{\oplus 2}$. Choose a basis (A, B) of $G(k_s)$ and define D_G as in Corollary 1.4.6, so that $\sigma \in \mathrm{Gal}(k_s/k) \longmapsto D_G(\sigma)^{-1} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is a group homomorphism. For each integer $m \geq 1$ coprime to N such that $m = m_0 m_1$ with $m_0, m_1 \geq 1$ pairwise coprime, m_0 square-free, m_1 invertible in k, there is a natural isomorphism $\iota_m : X_G(N, \Gamma_0(m)) \to X_{D_G^{-1}}(N, \Gamma_0(m))$ of projective k-schemes. Moreover,*

- *This isomorphism preserves the j-invariant,*
- *This family of isomorphims commutes with the Atkin-Lehner automorphisms and all the degeneracy maps,*
- *Under this isomorphism, if L/k is a subextension of k_s/k and E is an elliptic curve over L, endowed with a cyclic subgroup C of order m and an isomorphism $\varphi : G_L \to E[N]$, the image under ι_m of the $\overline{k}$-point (E, φ, C) is the $\overline{k}$-point $(E, (\varphi(A), \varphi(B)), C)$ of $Y_{D_G^{-1}}(N, \Gamma_0(m))$.*

Proof. – Since (A, B) is a $\mathbb{Z}/N\mathbb{Z}$-basis of $G(k_s)$, the morphism of $\mathbb{A}^1_{k_s}$-schemes (where the j-invariant provides the structure map) $\tau_m : Y_G(N, \Gamma_0(m))_{k_s} \to Y(N, \Gamma_0(m))_{k_s}$ defined by

$$(E/S, \varphi, C) \longmapsto (E/S, \varphi(A), \varphi(B), C)$$

for any k_s-scheme S is an isomorphism. Moreover, τ_m is compatible with the Atkin-Lehner automorphisms and the degeneracy maps. By Proposition A.2.9, it extends to an isomorphism $\overline{\tau}_m : X_G(N, \Gamma_0(m))_{k_s} \to X(N, \Gamma_0(m))_{k_s}$ which is compatible with the Atkin-Lehner automorphisms and the degeneracy maps.

Let us prove that, for any $\sigma \in \mathrm{Gal}(k_s/k)$, the following diagram commutes:

$$\begin{array}{ccc} X_G(N,\Gamma_0(m)) \times_k \operatorname{Spec} k_s & \xrightarrow{\overline{\tau}_m} & X(N,\Gamma_0(m)) \times_k \operatorname{Spec} k_s \\ \downarrow{\scriptstyle (\mathrm{id},\underline{\sigma}^{-1})} & & \downarrow{\scriptstyle D_G^{-1}(\sigma)\circ(\mathrm{id},\underline{\sigma}^{-1})} \\ X_G(N,\Gamma_0(m)) \times_k \operatorname{Spec} k_s & \xrightarrow{\overline{\tau}_m} & X(N,\Gamma_0(m)) \times_k \operatorname{Spec} k_s \end{array}$$

Then the uniqueness of the Galois twist will yield the conclusion. It is enough to check the commutation when restricted to $Y_G(N,\Gamma_0(m))$, because of the properties of compactified moduli schemes (see Proposition A.2.9).

In other words, given two k-morphisms $f : S \to Y_G(N,\Gamma_0(m))$, $g : S \to \operatorname{Spec} k_s$, we need to prove that $D_G^{-1}(\sigma) \circ \mathrm{pr}_1 \circ \tau_m(f,g) = \tau_m(f, \underline{\sigma}^{-1} \circ g)$. Let us write $\tau = \tau_m$ for the sake of brevity.

Suppose that f corresponds to a triple (E,φ,C), where E is an elliptic curve over S, $C \leq E[m]$ a cyclic locally free subgroup scheme of E of degree m, and $\varphi : G_S \to E[N]$ is an isomorphism. Then the first projection p_1 of $\tau(f,g) \in Y(N,\Gamma_0(m))(S)$ corresponds to the triple $(E/S, (\varphi(g^*A), \varphi(g^*B)), C)$. Thus $D_G^{-1}(\sigma) \circ p_1 \in Y(N,\Gamma_0(m))(S)$ is the triple

$$\left(E/S, \varphi\left[g^*\left(\sigma^{-1}(A), \sigma^{-1}(B)\right)\right], C\right) = (E/S, \left[\varphi(A \circ \underline{\sigma}^{-1} \circ g), \varphi(B \circ \underline{\sigma}^{-1} \circ g)\right], C),$$

which is exactly the triple given by $\tau(f, \underline{\sigma}^{-1} \circ g)$, and we are done. □

Lemma 1.4.9 *Let k be a field with characteristic not dividing N. Let $\omega_k : \mathrm{Gal}(k_s/k) \to (\mathbb{Z}/N\mathbb{Z})^\times$ be the mod N cyclotomic character. Let $\mathcal{O}_{N,k}$ be the finite étale k-algebra $k \otimes \operatorname{Spec} \mathcal{O}_N$ (which is a finite étale k-scheme), and define $\rho : \sigma \in \mathrm{Gal}(k_s/k) \longmapsto \mathrm{id} \times \underline{\omega_k(\sigma)^{-1}} \in \mathrm{Aut}_k(\operatorname{Spec} \mathcal{O}_{N,k})$, Then $(\operatorname{Spec} \mathcal{O}_{N,k})_\rho$ is naturally isomorphic to the disjoint union of $\varphi(N)$ copies of k, naturally indexed by $\mathrm{Hom}(\mathcal{O}_N, k_s)$.*

Proof. – Let k' be the extension of k generated by a primitive N-th root of unity ζ. By the construction in the proof of Proposition A.1.11, $(\operatorname{Spec} \mathcal{O}_{N,k})_\rho$ is the spectrum of the sub-algebra of $A = k' \otimes_{\mathbb{Z}} \mathcal{O}_N$ fixed by the automorphisms $\sigma \otimes \underline{\omega_k(\sigma)}$ for all $\sigma \in \mathrm{Gal}(k'/k)$. Choose a morphism $\pi : \mathcal{O}_N \to k'$, and let, for every $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, μ_a be the following homomorphism of k'-algebras:

$$\mu_a : \alpha \otimes \beta \in k' \otimes_{\mathbb{Z}} \mathcal{O}_N \mapsto \alpha \cdot \pi(\underline{a}(\beta)) \in k'.$$

Since A is a finite k'-algebra, the kernel $\mathfrak{m}_a$ of μ_a is a maximal ideal of A. The μ_a are linear forms, so, for any $a, a' \in (\mathbb{Z}/N\mathbb{Z})^\times$, either $\mathfrak{m}_a \neq \mathfrak{m}_{a'}$ or μ_a and $\mu_{a'}$ are collinear. Since the vectors $\begin{pmatrix} \mu_a(1) \\ \mu_a(1 \otimes \zeta) \end{pmatrix} = \begin{pmatrix} 1 \\ \pi(\zeta)^a \end{pmatrix}$ (for $a \in (\mathbb{Z}/N\mathbb{Z})^\times$) are pairwise linearly independent, the $\mathfrak{m}_a$ are pairwise distinct.

By the Chinese reminder theorem [4, Lemma 00DT], the product

$$\Pi = \prod_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} \mu_a : A \to \prod_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} k'$$

is surjective between k'-algebras of the same finite dimension, hence is an isomorphism of k'-algebras.

For the action of $\mathrm{Gal}(k'/k)$ previously defined on A, every μ_a is easily seen to be equivariant, so Π induces an isomorphism of k-algebras $A^{\mathrm{Gal}(k'/k)} \to \prod_{a \in (\mathbb{Z}/N\mathbb{Z})^\times} k$.

To conclude, note that the $\pi \circ \underline{a}$ are exactly the ring homomorphisms $\mathcal{O}_N \to k_s$. □

Proposition 1.4.10 *Consider the situation and notations of Proposition 1.4.8, but assume furthermore that G is polarized. Let $\zeta_k : \mathcal{O}_N \to k_s$ be the image of the polarization of G at (A,B). Then*

(i) $\det D_G$ *is the cyclomotic character mod N,*

(ii) if we let D_G^{-1} act on $\mathcal{O}_{N,k}$ through its determinant as in Lemma 1.4.9, the twist by D_G^{-1} of the map $\mathrm{We} : X(N,\Gamma_0(m))_k \to \operatorname{Spec}\mathcal{O}_{N,k}$ *is*

$$\mathrm{We}_{D_G^{-1}} : (X(N,\Gamma_0(m))_k)_{D_G^{-1}} \to \coprod_{f:\mathcal{O}_N\to k_s} \operatorname{Spec} k,$$

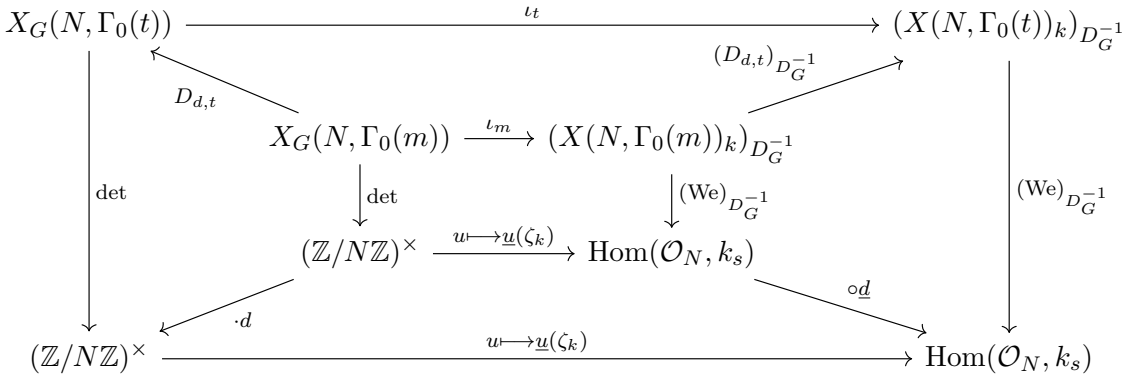
(iii) For $(E,P,Q,C) \in Y(N,\Gamma_0(m))_k(k_s)$, $\mathrm{We}_{D_G^{-1}}(E,P,Q,C)$ belongs to the component

$$\langle P,\, Q\rangle_{E[N]} \in \mu_N(k_s) \simeq \mathrm{Hom}(\mathcal{O}_N, k_s),$$

(iv) the following diagram commutes, where the horizontal arrows are isomorphisms and the bottom line is made with constant k-schemes,

$$\begin{array}{ccc} X_G(N,\Gamma_0(m)) & \xrightarrow{\iota_m} & (X(N,\Gamma_0(m))_k)_{D_G^{-1}} \\ \downarrow{\scriptstyle \det} & & \downarrow{\scriptstyle (\mathrm{We})_{D_G^{-1}}} \\ (\mathbb{Z}/N\mathbb{Z})^\times & \xrightarrow{u\longmapsto \underline{u}(\zeta_k)} & \mathrm{Hom}(\mathcal{O}_N, k_s) \end{array}$$

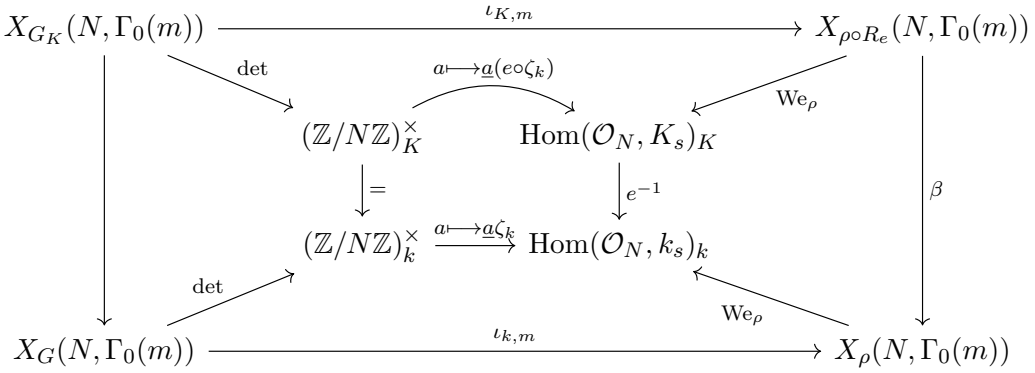
(v) let d,t be divisors of m and $D_{d,t}$ be the associated degeneracy map from Proposition 1.3.21. The following diagram commutes:



Proof. – (i) follows from the theory of the Weil pairing, (ii) directly from Lemma 1.4.9, and (iii) is a tautology. For (iv), the target scheme is a finite disjoint union of copies of $\operatorname{Spec} k$, so it is enough to check commutativity on a Zariski-dense subset of $Y_G(N,\Gamma_0(m))(\overline{k})$ (since the bottom arrow is easily seen to be an isomorphism). The explicit description of ι_m in Proposition 1.4.10 shows that the diagram commutes for $\overline{k}$-points of $Y_G(N,\Gamma_0(m))$ whose projection on $Y_G(N)$ is defined over k_s. To complete the proof of (iv), we just note that $Y_G(N,\Gamma_0(m))_k \to Y_G(N)_k$ is surjective and that $Y_G(N)(k_s)$ is infinite. For (v), the top cell commutes by Proposition 1.4.8, the bottom cell commutes by a direct verification, the outer and inner cells commute by (iv), the left cell commutes by Proposition 1.3.23, which concludes. □

Proposition 1.4.11 *Consider the situation and notations of Proposition 1.4.10, and write $\rho = D_G^{-1}$. Let K be a field extension of k and K_s be a separable closure of K. Fix an embedding $e : k_s \to K_s$. Then ι defines a homomorphism $R_e : \mathrm{Gal}(K_s/K) \to \mathrm{Gal}(k_s/k)$. Then, for some canonical morphism β, the following diagram commutes, and $X_{\rho\circ R_e}(N,\Gamma_0(m)) \xrightarrow{\beta} X_\rho(N,\Gamma_0(m))_K$*

is an isomorphism.



Moreover, this diagram commutes to the degeneracy maps as in Proposition 1.4.10.

Proof. – Note that all horizontal arrows in the diagram are isomorphisms and that both short vertical arrows are. The bottom and top cells commute by Proposition 1.4.10 (because $e(P), e(Q)$ define a basis of the polarized p-torsion group $G_K[p]$ over K, and that the attached representation is $\rho \circ R_e$). The left cell and the center cell commute by definition. Since the horizontal arrows are isomorphisms, there is a unique β such that the outer cell commutes. For this choice of β, the rightmost cell commutes as well. Moreover, since the outer cell commutes, the horizontal maps are isomorphisms, and the leftmost arrow is the base change $k \to K$ map, $X_{\rho\circ R_e}(N,\Gamma_0(m)) \xrightarrow{\beta} X_\rho(N,\Gamma_0(m))_K$ is an isomorphism. □

1.5 Hecke operators

In this section, we are mainly interested in the proper modular curves. Therefore our base rings will always be regular excellent Noetherian.

1.5.1 $\Gamma_0(p)$-degeneracies in characteristic p

Let $N, m, p \geq 1$ be pairwise coprime integers, where p is prime and $N \geq 3$. Let k be a perfect field of characteristic p with separable (hence algebraic) closure k_s and φ be its absolute Frobenius. Let G be a N-torsion group over k and let $\mathscr{P} = \mathscr{P}_G(\Gamma_0(m))$ for the sake of brevity. It is a finite étale representable moduli problem over $\mathbf{Ell}_k$ endowed with a natural structure of level Nm.

By our previous results, the moduli problem $\mathscr{P} \times [\Gamma_0(p)]_k$ is representable by a finite flat $\mathscr{M}(\mathscr{P})$-scheme $\mathscr{M}(\mathscr{P},\Gamma_0(p)) = Y_G(N,\Gamma_0(mp))$ (the structure map to $\mathscr{M}(\mathscr{P}) = Y_G(N,\Gamma_0(m))$ being $D_{1,m}$). Moreover, $\mathscr{P} \times [\Gamma_0(p)]_k$ is smooth at infinity and the compactified moduli scheme $\overline{\mathscr{M}}(\mathscr{P},[\Gamma_0(p)]_k)$ is smooth over k outside the supersingular j-invariants. By [86, Theorem 13.4.7], $Y_G(N,\Gamma_0(mp))$ is the disjoint union of two $\mathscr{M}(\mathscr{P})$-schemes $\mathscr{M}(\mathscr{P})_{(1,0)}$ and $\mathscr{M}(\mathscr{P})_{(0,1)}$ with crossings at the supersingular points.

First, let us recall the usual definitions of Frobenius morphisms in characteristic p.

Definition 1.5.1 Any $\mathbb{F}_p$-scheme X has an *absolute Frobenius* $F_{abs} : X \to X$, which induces the identity on points and $a \longmapsto a^p$ on rings of functions. Given a S-scheme X with structure map σ, where S is a $\mathbb{F}_p$-scheme, we denote by X^φ the S-scheme defined by $X \times_S S$, where the map $S \to S$ is exactly F_{abs}. The *relative Frobenius* of X/S is then the map $(F_{abs,X}, \sigma) : X \to X^\varphi$ of S-schemes. If X is a relative elliptic curve, it is an isogeny of degree p and the dual isogeny is the *Verschiebung* (this is [86, Lemma 12.2.1]). Suppose that $F_{abs} : S \to S$ is an isomorphism, then we can define the S-scheme $X^{\varphi^{-1}} = X \times_S S$, where the map $S \to S$ is exactly F_{abs}^{-1}. Then $(X^{\varphi^{-1}})^\varphi$ naturally identifies with X (as a S-scheme). In particular, if in addition X is a relative elliptic curve over S, there is an isogeny $X \to X^{\varphi^{-1}}$ defined as the dual of the Frobenius $X^{\varphi^{-1}} \to (X^{\varphi^{-1}})^\varphi \simeq X$. We will also call it the Verschiebung.

In particular, we have an Atkin-Lehner automorphism w_p on $\mathscr{M}(\mathscr{P}, \Gamma_0(p))$ and the degeneracy map $D_{p,m} = w_p \circ D_{1,m} : \mathscr{M}(\mathscr{P}, \Gamma_0(p)) \to \mathscr{M}(\mathscr{P})$.

Proposition 1.5.2 *The automorphism w_p preserves the supersingular locus of $\mathscr{M}(\mathscr{P}, \Gamma_0(p))$ and exchanges the ordinary loci of $\mathscr{M}(\mathscr{P})_{(1,0)}$ and $\mathscr{M}(\mathscr{P})_{(0,1)}$.*

Proof. – The fact that the supersingular locus is preserved comes from [86, Corollary 12.3.7] and the definition of w_p. Thus w_p induces an automorphism of the ordinary locus of $\mathscr{M}(\mathscr{P}, \Gamma_0(p))$, which is the disjoint union of the ordinary loci of $\mathscr{M}(\mathscr{P})_{(0,1)}$ and $\mathscr{M}(\mathscr{P})_{(1,0)}$. Both are purely inseparable base changes of the smooth projective geometrically connected curve $\overline{\mathscr{M}}(\mathscr{P})_k \to \operatorname{Spec} k$ with finitely many points removed, thus are irreducible schemes. So either w_p preserves the ordinary loci of $\mathscr{M}(\mathscr{P})_{(0,1)}$ and $\mathscr{M}(\mathscr{P})_{(1,0)}$, or it exchanges them.

Let E be an ordinary elliptic curve over k_s and $\alpha \in \mathscr{P}(E/k_s)$ be a level structure. Consider the triple $(E/k_s, \alpha, \ker F)$, where $F : E \to E^\varphi$ is the Frobenius isogeny and V is its dual. Then $x = (E/k_s, \alpha, \ker F)$ defines a point in the ordinary locus of $\mathscr{M}(\mathscr{P})_{(1,0)}(k_s)$ by [86, Proposition 13.4.4, Theorem 13.4.7]. But $w_p(x) = (E^\varphi/k_s, \alpha', \ker V)$ for some $\alpha' \in \mathscr{P}(E^\varphi/k_s)$, and it is easy to see from [86, (13.4.1-3), Theorem 13.4.7] that $w_p(x)$ is a point in the ordinary locus of $\mathscr{M}(\mathscr{P})_{(0,1)}(k_s)$, whence the conclusion. □

Proposition 1.5.3 *Let $x \in \mathscr{M}(\mathscr{P})(k)$ be an ordinary point corresponding to the couple $(E/k, \alpha)$. Then the following equality of effective Cartier divisors holds:*

$$(D_{p,m})_*(D_{1,m})^* x = \varphi(x) + p \cdot \varphi'(x),$$

where $\varphi(x) \in \mathscr{M}(\mathscr{P})(k)$ is the couple $(E^\varphi/k, F(\alpha))$ with $F : E \to E^\varphi$ the Frobenius isogeny, and $\varphi'(x) \in \mathscr{M}(\mathscr{P})(k)$ is the couple $(E^{\varphi^{-1}}/k, V(\alpha))$ with $V : E \to E^{\varphi^{-1}}$ is the Verschiebung (attached to the elliptic curve $E^{\varphi^{-1}}/k$).

Proof. – By Lemma A.4.8, pushing forward line bundles attached to Cartier divisors supported at normal points is the same as pushing forward said normal points.

Since x is ordinary and the $D_{i,m}$ are finite flat, $(D_{1,m})^* x$ is a Cartier divisor on $\mathscr{M}(\mathscr{P}, [\Gamma_0(p)]_k)$ which is the sum of the inverse images $x_{(1,0)}$ and $x_{(0,1)}$ of x on $\mathscr{M}(\mathscr{P})_{(1,0)}$ and $\mathscr{M}(\mathscr{P})_{(0,1)}$. By [86, (13.5.6)], $x_{(1,0)}$ is the Cartier divisor corresponding to a single (smooth) rational point of $\mathscr{M}(\mathscr{P})_{(1,0)}$; by definition of the $(1,0)$-cyclic moduli problem, one has

$$x_{(1,0)} = (E/k, \alpha, \ker F) \in \mathscr{M}(\mathscr{P})_{(1,0)}(k).$$

Thus $D_{p,m}(x_{(1,0)})$ is exactly the Cartier divisor corresponding to the k-rational point

$$\phi(x) = (E^\varphi, F(\alpha)) \in \mathscr{M}(\mathscr{P})(k).$$

On the other hand, by [86, (13.5.6)], $\mathscr{M}(\mathscr{P})_{(0,1)} \to \mathscr{M}(\mathscr{P})$ is a morphism of degree p and induces a bijection on points with values in any perfect k-algebra. Since x is an ordinary point, $x_{(0,1)}$ is an effective Cartier divisor of degree p, supported on the only point in $y \in \mathscr{M}(\mathscr{P})_{(0,1)}(k)$ such that $D_{1,m}(y) = x$, so that $x_{(0,1)} = p \cdot y$ as effective Cartier divisors. By definition of the $(0,1)$-cyclic moduli problem, it is easy to see that $(E/k, \alpha, \ker V) \in \mathscr{M}(\mathscr{P})_{(0,1)}(k)$ and $D_{1,m}((E/k, \alpha, \ker V)) = x$, so that $y = (E/k, \alpha, \ker V)$. To conclude, it is enough to note that $D_{p,m}(y) = \varphi'(x)$. □

1.5.2 Hecke operators and the Eichler-Shimura relation

Definition 1.5.4 A finite flat representable moduli problem $\mathscr{P}$ over $\mathbf{Ell}_R$ (R being a regular excellent Noetherian ring) of level N *has good Hecke operators* if the following conditions are satisfied for every couple (m_0, m_1) of coprime positive integers that are coprime to N and such that m_0 is square-free, $m_1 \in R^\times$:

– $\mathscr{P} \times_R [\Gamma_0(m_0m_1)]_R$ is smooth at infinity.
– $\overline{\mathscr{M}}(\mathscr{P}, [\Gamma_0(m_0m_1)]_R) \to \operatorname{Spec} R$ is proper, surjective, Cohen-Macaulay of relative dimension one with geometrically reduced fibres.

Lemma 1.5.5

(*i*) *If a finite flat representable moduli problem $\mathscr{P}$ of level N over $\mathbf{Ell}_R$ has good Hecke operators, then $\overline{\mathscr{M}}(\mathscr{P}) \to \operatorname{Spec} R$ is a relative curve, and any (compactified) degeneracy map $D_{d,t}$ is finite locally free of constant rank (independent from $\mathscr{P}$ and R) by Corollary 1.2.19.*

(*ii*) *If a finite flat representable moduli problem $\mathscr{P}$ of level N over $\mathbf{Ell}_R$ has good Hecke operators and $R \to R'$ is finite étale faithfully flat, then $\mathscr{P} \times [\operatorname{Spec} R']$ has good Hecke operators (for the natural level N structure).*

(*iii*) *If a finite flat representable moduli problem $(\mathscr{P}, F)$ of level N over $\mathbf{Ell}_R$ has good Hecke operators and M is a multiple of N, then any base change $R \to R'$ of $(\mathscr{P}, F_{N\to M})$ has good Hecke operators as long as R, R' have the same invertible integers coprime to M.*

(*iv*) *If a finite flat representable moduli problem $\mathscr{P}$ of level N over $\mathbf{Ell}_R$ has good Hecke operators, so does $\mathscr{P} \times [\Gamma_0(m)]_R$ for any $m = m_0m_1$ with $m_0, m_1 \geq 1$, m_0 square-free and $m_1 \in R^\times$ for its natural structure of level Nm_0m_1 moduli problem.*

(*v*) *If $\mathscr{P}$ is a finite étale representable moduli problem of level N over $\mathbf{Ell}_R$ and R has generic characteristic zero, then the two conditions are automatically verified for any base change of R.*

(*vi*) *Let $\mathscr{P}$ be a finite flat representable moduli problem of level N over $\mathbf{Ell}_R$ and R' be a smooth faithfully flat R-algebra (hence regular excellent Noetherian) such that $\mathscr{P}_{R'}$ has good Hecke operators. If moreover $\mathscr{P}_{R'}$ is smooth at infinity over R, then $\mathscr{P}$ has good Hecke operators.*

Proof. – (*i*) follows from Lemma A.4.26 and Corollary 1.2.19, (*ii*) from Lemma 1.2.9, and (*v*) from (mostly) Proposition 1.2.20 and Corollary 1.2.21. (*iii*) and (*iv*) are formal verifications. Finally, (*vi*) follows from Proposition 1.2.15 and Proposition 1.2.20. □

Corollary 1.5.6 *Let R be a regular excellent Noetherian $\mathbb{Z}[1/N]$-algebra with $N \geq 3$ and G be a N-torsion group over R. Let $m_0, m_1 \geq 1$ be coprime integers with product m coprime to N such that m_0 is square-free and $m_1 \in R^\times$. Then $\mathscr{P}_G(\Gamma_0(m))$ (endowed with its natural level Nm structure) and $[\Gamma_1(N)]_R \times_R [\Gamma_0(m)]_R$ (endowed with its natural level Nm structure, assuming that $N \geq 4$) have good Hecke operators.*

Definition 1.5.7 In the above situation, when $m_0 \in R^\times$, the relative curve is smooth. We denote its relative Jacobian[10] by $J_G(N, \Gamma_0(m))$ (resp. $J_1(N, \Gamma_0(m))$).

Definition 1.5.8 We copy for convenience Definition A.4.17. If X is a proper finitely presented S-scheme, $P_{X/S}$ denotes the functor on $\mathbf{Sch}_S$ given by $T \longmapsto \operatorname{Pic}(X \times_S T)$. The *relative Picard functor* of X/S is the sheafification $\operatorname{Pic}_{X/S}$ of $P_{X/S}$ in the fppf topology (see Definition A.3.11). If moreover the fibres of $X \to S$ are pure of dimension one, we define $P^0_{X/S}$ as the sub-presheaf of $P_{X/S}$ such that $P_{X/S}(T)$ is made with the classes of those line bundles $\mathcal{L}$ on $X \times_S T$ such that for every $t \in T$, the line bundle $t^*\mathcal{L}$ on $X_{\kappa(t)}$ has degree zero on every connected component. The fppf-sheafification of $P^0_{X/S}$ is the subsheaf $\operatorname{Pic}^0_{X/S}$ of $\operatorname{Pic}_{X/S}$.

Definition 1.5.9 Let $\mathscr{P}$ be a finite flat representable moduli problem of level N over $\mathbf{Ell}_R$ which has good Hecke operators and $p \nmid N$ be a prime. The Hecke operator T_p denotes the endomorphism $(D_{p,1})_*(D_{1,1})^*$ of any of the functors $P_{\overline{\mathscr{M}}(\mathscr{P})/\operatorname{Spec} R}$, $P^0_{\overline{\mathscr{M}}(\mathscr{P})/\operatorname{Spec} R}$, $\operatorname{Pic}_{\overline{\mathscr{M}}(\mathscr{P})/\operatorname{Spec} R}$, $\operatorname{Pic}^0_{\overline{\mathscr{M}}(\mathscr{P})/\operatorname{Spec} R}$.

Lemma 1.5.10 *With the same notations as before:*

[10] As noted in the introduction of this chapter, the notion of relative Jacobian for a proper smooth scheme $X \to \operatorname{Spec} R$ of relative dimension one does not seem to be standard when the morphism does not have geometrically connected fibres, even when R is a field. However, only minor modifications to the classical theory are needed to define and construct Jacobians in this setting, which we describe in Section A.4.2.

(*i*) *The formation of T_p commutes with arbitrary base change (of regular excellent Noetherian algebras).*

(*ii*) *If the level N structure on $\mathscr{P}$ is given by the functor F and M is any multiple of N coprime to p, then the operator T_p for the level M structure $F_{N\to M}$ on $\mathscr{P}$ is the same.*

(*iii*) *If $m = m_0m_1$ is coprime to Np, with m_0 square-free and coprime to $m_1 \in R^\times$, then, for any $d, t \geq 1$ with $dt \mid m$ (resp. any $d \geq 1$ with $d \mid m$ coprime to m/d), the formation of T_p commutes to the push-forwards and pull-backs by $D_{d,t} : \overline{\mathscr{M}}(\mathscr{P}, [\Gamma_0(m)]_R) \to \overline{\mathscr{M}}(\mathscr{P}, [\Gamma_0(t)]_R)$ (resp. to the push-forwards and pull-backs by the Atkin-Lehner automorphisms w_d of $\overline{\mathscr{M}}(\mathscr{P}, [\Gamma_0(m)]_R)$).*

(*iv*) *Let $C : \mathscr{P} \Rightarrow \mathscr{P}'$ be a flat natural transformation of finite flat representable moduli problems over $\mathbf{Ell}_R$ of level N (for instance, C can be $[a]$ for some $a \in (\mathbb{Z}/N\mathbb{Z})^\times$). Then $C : \overline{\mathscr{M}}(\mathscr{P}) \to \overline{\mathscr{M}}(\mathscr{P}')$ is finite locally free, and the formation of the Hecke operator T_p commutes with the pull-back C^* and the push-forward $[C_*]$.*

Proof. – The first two points are clear. The last three points are applications of Proposition A.4.23 and A.4.25. The Cartesian diagram away from the cusps is given by Propositions 1.1.26 and 1.1.28, the required flatness follows from Proposition 1.2.18 for C and Corollary 1.2.19 for the degeneracy maps.

So we need to show that for any R-scheme T, $\iota : \mathscr{M}(\mathscr{P}, [\Gamma_0(m)]_R)_T \to \overline{\mathscr{M}}(\mathscr{P}, [\Gamma_0(m)]_R)_T$ has scheme-theoretically dense image. The second assertion is true because ι is a finite flat base change of the scheme-theoretically dense inclusion $\mathbb{A}^1_T \to \mathbb{P}^1_T$. □

Corollary 1.5.11 *Let $\mathscr{P} = \mathscr{P}_G(\Gamma_0(m))$, where $N, m_0, m_1 \geq 1$ are coprime integers, $N \geq 3$, m_0 is square-free, R is a regular excellent Noetherian $\mathbb{Z}[(Nm_1)^{-1}]$-algebra, $m = m_0m_1$, and G is the constant N-torsion group over R. Let $p \nmid Nm$ be a prime. Then T_p commutes with the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.*

Proof. – $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts by morphisms of moduli problems of level Nm. □

Proposition 1.5.12 *Let $N, m_0, m_1 \geq 1$ be pairwise coprime integers, with $N \geq 3$ and m_0 square-free. Let R be a regular excellent Noetherian $\mathbb{Z}[(Nm_1)^{-1}]$-algebra and G be a polarized N-torsion group over R. Let $m = m_0m_1$ and $\mathscr{P} = \mathscr{P}_G(N, \Gamma_0(m))$. Let, for each $u \in (\mathbb{Z}/N\mathbb{Z})^\times$, $\mathscr{P}_u = \mathscr{P}_{G,u}(N, \Gamma_0(m))$ and $X_{\mathscr{P},u}$ be the associated compactified moduli scheme. Then there is an isomorphism of functors*

$$\iota : P_{\overline{\mathscr{M}}(\mathscr{P})/\operatorname{Spec} R} \simeq \prod_{u\in(\mathbb{Z}/N\mathbb{Z})^\times} P_{X_{\mathscr{P},u}/\operatorname{Spec} R}$$

(preserving the P^0). Through this isomorphism, the operator T_p decomposes as a direct product over $u \in (\mathbb{Z}/N\mathbb{Z})^\times$ of the morphisms $(D_{p,1})_*(D_{1,1})^* : P_{X_{\mathscr{P},u}/\operatorname{Spec} R} \to P_{X_{\mathscr{P},pu}/\operatorname{Spec} R}$, also denoted by T_p, and preserving the P^0.

In particular, ι sheafifies to an isomorphism

$$\iota : \mathrm{Pic}_{\overline{\mathscr{M}}(\mathscr{P})/\operatorname{Spec} R} \simeq \prod_{u\in(\mathbb{Z}/N\mathbb{Z})^\times} \mathrm{Pic}_{X_{\mathscr{P},u}/\operatorname{Spec} R}$$

preserving the Pic^0, and, through this isomorphism, T_p is the direct sum over $u \in (\mathbb{Z}/N\mathbb{Z})^\times$ of the morphisms $(D_{p,1})_*(D_{1,1})^* : \mathrm{Pic}_{X_{\mathscr{P},u}/\operatorname{Spec} R} \to \mathrm{Pic}_{X_{\mathscr{P},pu}/\operatorname{Spec} R}$.

Proof. – $D_{1,m}$ preserves the map to the constant scheme $(\mathbb{Z}/N\mathbb{Z})^\times$, while $D_{p,m}$ multiplies it by p. We can then mimic the construction of the Hecke operators by considering instead, for each $u \in (\mathbb{Z}/N\mathbb{Z})^\times$, the maps

$$D^u_{1,m} : X_{G,u}(N, \Gamma_0(mp)) \to X_{G,u}(N, \Gamma_0(m)),\ D^u_{p,m} : X_{G,u}(N, \Gamma_0(pm)) \to X_{G,pu}(N, \Gamma_0(m)).$$

□

Proposition 1.5.13 *Let $\mathscr{P}$ be a finite flat representable moduli problem over $\mathbf{Ell}_R$ of level N having good Hecke operators. Let p, q be distinct primes not dividing N. Then T_p and T_q commute.*

Proof. – By Proposition 1.5.10, the following diagram of pre-sheaves commutes (with all applications preserving P^0):

$$\begin{array}{ccc} P_{\overline{\mathscr{M}}(\mathscr{P},[\Gamma_0(p)]_R)/\operatorname{Spec} R} & \xrightarrow{T_q} & P_{\overline{\mathscr{M}}(\mathscr{P},[\Gamma_0(p)]_R)/\operatorname{Spec} R} \\ \downarrow{\scriptstyle [u_*]} & & \downarrow{\scriptstyle [u_*]} \\ P_{\overline{\mathscr{M}}(\mathscr{P})/\operatorname{Spec} R} & \xrightarrow{T_q} & P_{\overline{\mathscr{M}}(\mathscr{P})/\operatorname{Spec} R} \\ \downarrow{\scriptstyle u^*} & & \downarrow{\scriptstyle u^*} \\ P_{\overline{\mathscr{M}}(\mathscr{P},[\Gamma_0(p)]_R)/\operatorname{Spec} R} & \xrightarrow{T_q} & P_{\overline{\mathscr{M}}(\mathscr{P},[\Gamma_0(p)]_R)/\operatorname{Spec} R} \end{array}$$

where u is either $D_{p,m}$ or $D_{1,m}$, whence the conclusion. □

Proposition 1.5.14 *Let $\mathscr{P}$ be a finite flat relatively representable moduli problem over $\mathbf{Ell}_R$ of level L prime to N, where R is a regular excellent Noetherian $\mathbb{Z}[1/N]$-algebra, and assume that $\mathscr{P}$ is representable if $N \leq 3$ and that $\mathscr{P}' = \mathscr{P} \times_R [\Gamma_1(N)]_R$ has good Hecke operators. Let $d \mid N$ be a positive integer coprime to N/d, and $e \mid N/d$ be an integer. Let $p \nmid LN$ be a prime number, and let $p' \in (\mathbb{Z}/de\mathbb{Z})^\times$ be congruent to p mod d and to 1 mod e. Then, on $P_{\overline{\mathscr{M}}(\mathscr{P},[\Gamma_1(N)]_R)\times\mu_{de}^\times/\operatorname{Spec} R}$, one has $([p'])_*(w'_d)_* T_p = T_p (w'_d)_*$.*

Proof. – This is a consequence of Proposition A.4.25. The Cartesian diagrams are given in Proposition 1.1.46, and the maps are finite locally free by Corollary 1.2.19. □

Proposition 1.5.15 *Suppose that $R = \mathbb{F}_p$ and G is a constant N-torsion group over R. Let $m \geq 1$ be an integer coprime to Np. Then the Jacobian $J_G(N, \Gamma_0(m))$ of $X_G(N, \Gamma_0(m))$ is endowed with a Frobenius isogeny F (its absolute Frobenius) of degree p with dual isogeny F', and the following identity holds on $J_G(N, \Gamma_0(m))$:*

$$T_p = F + [p] \cdot F'.$$

Proof. – First, recall that $\mathrm{We} : X_G(N, \Gamma_0(m))_{\mathbb{F}_p} \to \operatorname{Spec} \mathcal{O}_N \otimes \mathbb{F}_p := T$ is the Stein factorization of $X_G(N, \Gamma_0(m)) \to \operatorname{Spec} \mathbb{F}_p$. Let $x, x' \in Y_G(N, \Gamma_0(m))(\overline{\mathbb{F}_p})$ be two ordinary points with $\mathrm{We}(x) = \mathrm{We}(x')$ and let us show that on the divisor $D = x - x'$ of $X_G(N, \Gamma_0(m))_{\overline{\mathbb{F}_p}}$, one has $T_p(D) = (F + [p] \cdot F')(D)$.

By Proposition 1.5.3, we know that $T_p(D) = \varphi(x) - \varphi(x') + p \cdot \varphi'(x) - p \cdot \varphi'(x')$ as Cartier divisors, where we extend φ and φ' by linearity. The goal is thus to show that (in the notation of this Proposition) $F(x - x')$ represents the Cartier divisor $\varphi(x) - \varphi(x')$ and that $[p] \cdot F'(x - x')$ represents the Cartier divisor $p \cdot (\varphi'(x) - \varphi'(x'))$. For the first part, note that $\varphi(x)$ (resp. $F(x - x')$) is exactly the pre-composition of the geometric point x (resp. $x - x'$) by the absolute Frobenius of $\overline{\mathbb{F}_p}$.

For the second part, we can write $x = \varphi(x_1), x' = \varphi(x'_1)$ for some ordinary geometric points $x_1, x'_1 \in Y_G(N, \Gamma_0(m))(\overline{\mathbb{F}_p})$, then one checks directly that $\varphi'(x) = [p] \cdot x_1, \varphi'(x') = [p] \cdot x'_1$, and $F'(x - x') = F'(F(x_1 - x'_1)) = p \cdot (x_1 - x'_1)$, whence the conclusion.

Now, T_p and $F + [p] \cdot F'$ are two endomorphisms of $J_G(N, \Gamma_0(m))$, so there is a greatest closed subscheme Z of $J_G(N, \Gamma_0(m))$ on which they coincide, and Z is a subgroup scheme of $J_G(N, \Gamma_0(m))$. Since $J_G(N, \Gamma_0(m))$ is reduced, it is enough to show that Z contains a Zariski-dense set of $\overline{F_p}$-points of $J_G(N, \Gamma_0(m))$.

By Proposition A.4.30, there exists $r \geq 1$, such that the sum of r difference maps

$$\delta^r : (X_G(N,\Gamma_0(m)) \times_T X_G(N,\Gamma_0(m)))^{\times_{\mathbb{F}_p} r} \to J_G(N,\Gamma_0(m))$$

is surjective. Let $U \subset X_G(N,\Gamma_0(m))_{\mathbb{F}_p}$ be the ordinary locus: then $V := (U \times_T U)^{\times_{\mathbb{F}_p} r}$ is dense in $(X_G(N,\Gamma_0(m)) \times_T X_G(N,\Gamma_0(m)))^{\times_{\mathbb{F}_p} r}$, hence the image in $J_G(N,\Gamma_0(m))$ of $V(\overline{\mathbb{F}_p})$ (which is contained in Z) is Zariski-dense, whence the conclusion. □

Corollary 1.5.16 *Assume that $R = \mathbb{Q}$ and G is a constant N-torsion group over R. Let ℓ be a prime and $p \nmid N\ell$ be another prime. Then, on the ℓ-adic Tate module of $J_G(N)$, one has*

$$\mathrm{Frob}_p^2 - T_p \mathrm{Frob}_p + p[p] = 0.$$

Proof. – Let G_0 be the constant N-torsion group on $\mathbb{Z}[1/N]$. Then $J_G(N)$ is the generic fibre of the Abelian scheme $J_{G_0}(N)$ (to which T_p extends), so the isomorphism $\mathcal{T}_\ell J_G(N) \to \mathcal{T}_\ell J_{G_0}(N)_{\mathbb{F}_p}$ given by the reduction modulo p preserves T_p and is equivariant for the (unramified) Galois action of a decomposition group $D_p \leq G_{\mathbb{Q}}$ above p. The conclusion follows from Proposition 1.5.15. □

1.5.3 Link with the point of view of Galois twists

Using the previous results from this section, the results on Jacobians (Propositions A.4.28, A.4.39, A.4.40) as well as the previous results about twists (Propositions 1.4.8, 1.4.10), the following statements are formal.

Proposition 1.5.17 *Let $N \geq 3$ and k be a field of characteristic not dividing N with separable closure k_s. Let G be a N-torsion group over k. Choose a basis (A,B) of $G(k_s)$ and define D_G as in Corollary 1.4.6, so that $\sigma \in \mathrm{Gal}(k_s/k) \longmapsto D_G(\sigma)^{-1} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is a group homomorphism.*

Let $m_0, m_1 \geq 1$ such that m_0, m_1, N are pairwise coprime to N, m_1 is invertible in k and m_0 is square-free, and $m = m_0 m_1$. The isomorphism $\iota_m : X_G(N,\Gamma_0(m)) \to (X(N,\Gamma_0(m))_k)_{D_G^{-1}}$ of Proposition 1.4.8 extends by push-forward functoriality to an isomorphism of the Jacobians $[(\iota_m)_*] : J_G(N,\Gamma_0(m)) \to (J(N,\Gamma_0(m))_k)_{D_G^{-1}}$, where $(J(N,\Gamma_0(m))_k)_{D_G^{-1}}$ is the Galois twist of the Jacobian $J(N,\Gamma_0(m))_k$ where $\mathrm{Gal}(k_s/k)$ acts by the push-forward action of D_G^{-1}.

The collection of the $[(\iota_m)_*]$ (over all possible m) commutes with the push-forwards and the pull-backs of the twists by ρ of the degeneracy maps and the Atkin-Lehner automorphisms. Moreover, for any prime $p \nmid Nm$, the finite flat maps $D_{1,m}, D_{p,m} : X_\rho(N,\Gamma_0(mp)) \to X_\rho(N,\Gamma_0(m))$ induce an endomorphism $T_p = (D_{p,m})_*(D_{1,m})^*$ of $J_\rho(N,\Gamma_0(m))$, and $[(\iota_m)_*]$ commutes to the action of T_p.

Proposition 1.5.18 *Let us keep the notations of Proposition 1.5.17. Assume furthermore that G is polarized, and let $\zeta_k : \mathcal{O}_N \to k_s$ be the image of the polarization of G at (A,B). For each $\xi \in \mu_N^\times(k_s)$, let $X_\xi(N,\Gamma_0(m))$ be the inverse image of ξ under the morphism*

$$(\mathrm{We})_{D_G^{-1}} : (X(N,\Gamma_0(m))_k)_{D_G^{-1}} \to \coprod_{f:\mathcal{O}_N \to k_s} \mathrm{Spec}\, k$$

defined in Proposition 1.4.10.

Then, for each $u \in (\mathbb{Z}/N\mathbb{Z})^\times$, the isomorphism $\iota_{m,u} : X_{G,u}(N,\Gamma_0(m)) \to X_{\underline{u}\zeta_k}(N,\Gamma_0(m))$ induced by ι_m extends to an isomorphism $[(\iota_{m,u})_*]$ of their Jacobians, such that, for all primes $p \nmid Nm$ invertible in k, the following diagrams commute:

$$\begin{array}{ccc} J_G(N,\Gamma_0(m)) & \xrightarrow{[(\iota_m)_*]} & J_\rho(N,\Gamma_0(m)) \\ \downarrow{=} & & \downarrow{=} \\ \prod_{u\in(\mathbb{Z}/N\mathbb{Z})^\times} J_{G,u}(N,\Gamma_0(m)) & \xrightarrow{[(\iota_{m,u})_*]} & \prod_{u\in(\mathbb{Z}/N\mathbb{Z})^\times} J_{\underline{u}\zeta_k}(N,\Gamma_0(m)) \end{array}$$

$$\begin{array}{ccc} J_{G,u}(N,\Gamma_0(m)) & \xrightarrow{[(\iota_{m,u})_*]} & J_{\underline{u}\zeta_k}(N,\Gamma_0(m)) \\ \downarrow{\scriptstyle T_p=[(D_{p,m})_*]D_{1,m}^*} & & \downarrow{\scriptstyle T_p=[(D_{p,m})_*](D_{1,m})^*} \\ J_{G,pu}(N,\Gamma_0(m)) & \xrightarrow{[(\iota_{m,pu})_*]} & J_{\underline{up}\zeta_k}(N,\Gamma_0(m)) \end{array}$$

1.5.4 The bad Hecke operators for $X_1(N,\Gamma_0(m))$

Proposition 1.5.19 *Let $N, r \geq 1$ with $r \mid N$ and $N \geq 4$ and R be a regular excellent Noetherian $\mathbb{Z}[1/N]$-algebra. Then $\mathscr{P} = [\Gamma_1'(N,r)]_R$ with its level N structure admits good Hecke operators.*

Proof. – By base change, we may assume R is a localization of $\mathbb{Z}[1/N]$. Since this moduli problem is finite étale by Proposition 1.1.33, the conditions are verified by Proposition 1.2.20. □

Proposition 1.5.20 *If $N, r \geq 1$ are such that $r \mid N$, $N \geq 4$ and R is a regular excellent $\mathbb{Z}[1/N]$-algebra, then, for any coprime integers $m_0, m_1 \geq 1$ coprime to N such that $m_1 \in R^\times$ and m_0 square-free, the fibres of $\overline{\mathscr{M}}([\Gamma_1'(N,r)] \times [\Gamma_0(m)]) \to \operatorname{Spec} R$ are geometrically connected.*

Proof. – It is enough to prove that $\overline{\mathscr{M}}([\Gamma_1'(N,r)]_R, [\Gamma_0(m)]_R) \to \operatorname{Spec} R$ has connected geometric fibres when R is a localization of $\mathbb{Z}[1/N]$ (and for any suitable m). By [4, Lemma 0E0N], we may assume that $R = \mathbb{Q}$, and it is then enough to show that for any $m \geq 1$ coprime to N, $\overline{\mathscr{M}}([\Gamma_1'(N,r)]_{\mathbb{Q}}, [\Gamma_0(m)]_{\mathbb{Q}}) \to \operatorname{Spec} \mathbb{Q}$ is geometrically connected.

There is a natural map $Y(N,\Gamma_0(m))_{\mathbb{Q}} \to \mathscr{M}([\Gamma_1'(N,r)]_{\mathbb{Q}}, [\Gamma_0(m)]_{\mathbb{Q}}) \times_{\mathbb{Q}} \operatorname{Spec} \mathbb{Q}(\mu_N)$ (mapping a basis (P,Q) of the N-torsion to the triple $(P, \langle N/r \cdot Q\rangle, \langle P, Q\rangle)$, the latter coordinate being the Weil pairing, and preserving the $\Gamma_0(m)$-structure) and we can easily check (by passing to $\overline{\mathbb{Q}}$) that it is surjective. Thus, the compactification map $X(N,\Gamma_0(m))_{\mathbb{Q}} \to \overline{\mathscr{M}}([\Gamma_1'(N,r)]_{\mathbb{Q}}, [\Gamma_0(m)]_{\mathbb{Q}})_{\mathbb{Q}(\mu_N)}$ of $\mathbb{Q}(\mu_N)$-schemes is surjective. Its source is geometrically connected (as a $\mathbb{Q}(\mu_N)$-scheme), hence $\overline{\mathscr{M}}([\Gamma_1'(N,r)]_{\mathbb{Q}}, [\Gamma_0(m)]_{\mathbb{Q}})_{\mathbb{Q}(\mu_N)} \times_{\mathbb{Q}(\mu_N)} \operatorname{Spec} \overline{\mathbb{Q}}$ is connected, hence $\overline{\mathscr{M}}([\Gamma_1'(N,r)]_{\mathbb{Q}}, [\Gamma_0(m)]_{\mathbb{Q}})$ is geometrically connected as a $\mathbb{Q}$-scheme, whence the conclusion. □

Proposition 1.5.21 *In the situation of Proposition 1.1.34, $D'_{s,t}$ has positive constant rank, independent from $\mathscr{P}$.*

Proof. – Suppose that whenever $k \geq 3$ is coprime to N and invertible in R, $D'_{s,t}$ for the moduli problem $[\Gamma(k)]_R$ is finite étale of constant rank $r_k > 0$. By Proposition 1.1.36, the same holds for any moduli problem on $\mathbf{Ell}_R$ with a morphism to $[\Gamma(k)]_R$. In particular, if $k, k' \geq 3$ are invertible in R and coprime to N, $r_k = r_{kk'} = r_{k'}$. By considering the case where $R = \mathbb{Q}$, we then see that all the r_k are equal to some $\rho > 0$.

Let $\mathscr{P}$ be a relatively representable moduli problem on $\mathbf{Ell}_R$ (representable if $N \leq 3$) of level coprime to N. Choose two coprime integers $k, k' \geq 3$ coprime to N, then $D'_{s,t}$ (for $\mathscr{P}$) has an étale cover by the $D'_{s,t}$ for the two representable moduli problems $\mathscr{P} \times [\Gamma(k)]_{R[1/k]}$ and $\mathscr{P} \times [\Gamma(k')]_{R[1/k']}$. These instances of $D'_{s,t}$ are, by Proposition 1.1.36, base changes of instances of $D'_{s,t}$ for $[\Gamma(k)]_{\mathbb{Z}[1/k]}, [\Gamma(k')]_{\mathbb{Z}[1/k]}$, so they are both finite étale of rank ρ by the above. By descent, it follows that $D'_{s,t}$ for $\mathscr{P}$ is finite étale of rank ρ.

So all we have to do is show that $\mathscr{M}([\Gamma(k)]_R, [\Gamma_1'(N,r)]_R)$ is connected. The morphism

$$(E/S,(P,Q)) \in Y(Nk)_{\mathbb{Z}[1/Nk]} \longmapsto (E/S,(kP,kQ),(NP,\langle \frac{kN}{r} \cdot Q\rangle)) \in \mathscr{M}([\Gamma(k)]_R, [\Gamma_1'(N,r)]_R)$$

is surjective (it is enough to prove it when R is a field), so $\mathscr{M}([\Gamma(k)]_R, [\Gamma_1'(N,r)]_R)$ is connected by Corollary 1.3.9. □

Definition 1.5.22 Let $N \geq 4, r, m_0, m_1 \geq 1$ be integers, with $r \mid N$, N, m_0, m_1 pairwise coprime and m_0 square-free. Let R be a regular excellent Noetherian $\mathbb{Z}[(Nm_1)^{-1}]$-algebra and p be a prime number be such that $pr \mid N$. For any divisor $i \geq 1$ of N, let $Y_1'(i)$ (resp. $X_1'(i)_R$) be the moduli scheme (resp. the compactified moduli scheme) attached to the finite étale representable moduli problem $[\Gamma_1'(N,i)]_R \times_R [\Gamma_0(m)]_R$. For $i \in \{1, p\}$, the degeneracy map $D'_{i,r} : Y_1'(pr)_R \to Y_1'(r)_R$ extends to a map $D'_{i,r} : X_1'(pr)_R \to X_1'(r)_R$.

The operator U_p is the endomorphism $(D'_{p,r})_*(D'_{1,r})^*$ of the functor $P_{X_1'(r)_R/\operatorname{Spec} R}$. In particular, U_p preserves P^0 and U_p extends to an endomorphism U_p of the sheaf $\operatorname{Pic}_{X_1'(r)_R/\operatorname{Spec} R}$ preserving its subsheaf $\operatorname{Pic}^0_{X_1'(r)_R/\operatorname{Spec} R}$.

Proof. – By Proposition A.4.23, we only need to show that $D'_{1,r}, D'_{p,r}$ are finite locally free morphisms of relative curves over R. We know that the $X_1'(N, u, \Gamma_0(m))$ are relative curves over $\operatorname{Spec} R$ with geometrically connected fibres by Proposition 1.5.19. Hence, it is enough to show that the $D'_{*,r}$ are finite locally free. They are the compactifications of finite locally free morphisms of constant rank by Corollaries 1.1.37, 1.5.21, so they are finite, and the flatness follows from Proposition 1.2.18 since the moduli problems are smooth at infinity. □

Proposition 1.5.23 *With the notations of Definition 1.5.22:*

- *The formation of U_p commutes with base change.*
- *If p, q are distinct primes dividing N/r, then U_p and U_q commute.*
- *U_p commutes with any push-forward or pull-back by $D_{u,v}$ (where $uv \mid m$).*
- *In particular, U_p commutes with any T_q for any q coprime to Nm.*

Proof. – The first point is formal. The rest follows from Propositions A.4.23, A.4.25. To apply these results, we first need to check that all the maps involved indeed extend and are finite flat of constant rank, which is the case by Propositions 1.2.17, 1.2.22, 1.5.21 and Corollary 1.2.19. We also need some diagrams to be Cartesian above dense open subschemes, which is proved in the Propositions 1.1.38 and 1.1.39. □

1.6 The cuspidal subscheme and the q-expansion principle

Notation *The ring $\mathbb{Z}((q))$ is the ring of Laurent series with coefficients in $\mathbb{Z}$, or, in other words, $(\mathbb{Z}[[q]])[q^{-1}]$. Let, for any even $k \geq 4$,*

$$E_k = 1 - \frac{2k}{B_k} \sum_{n \geq 1} \left(\sum_{d \mid n} d^{k-1} \right) q^n \in \mathbb{Z}[[q]] \otimes \mathbb{Q}$$

denote the normalized Eisenstein series coming from the classical theory of modular forms [41, Section 1.1, Exercise 1.1.7]. One has $\frac{-2\cdot 4}{B_4} = 240$, $\frac{-2\cdot 6}{B_6} = -504$, so $E_4, E_6 \in \mathbb{Z}[[q]]$.

Definition 1.6.1 The *Tate curve* $\operatorname{Tate}(q)$ is the elliptic curve over $\mathbb{Z}((q))$ with Weierstrass equation

$$y^2 + xy = x^3 + \left(-5\frac{E_4 - 1}{240}\right) x - \frac{1}{12}\left(5\frac{E_4 - 1}{240} + 7\frac{E_6 - 1}{-504}\right)$$

as in [85, (A1.2.3)], endowed with the nowhere-vanishing differential $\omega = \frac{dx}{2y+x} = \frac{dy}{3x^2 - \frac{5}{12}\frac{E_4 - 1}{240} + y}$. It satisfies the following properties:

- Its j-invariant is given by the series $j(q) = \frac{1}{q} + 744 + \cdots$ from classical modular forms (see for instance [41, p. 7]).

– The invariant c_4 (resp. c_6, Δ) attached to this Weierstrass equation is E_4 (resp. $-E_6$, resp. the classical series $\Delta(q) = q\prod_{n\geq 1}(1-q^n)^{24}$).
– For every $N \geq 1$, there is a short exact sequence of finite flat commutative group schemes over $\mathbb{Z}((q))$

$$0 \to \mu_N \xrightarrow{\alpha} \mathrm{Tate}(q)[N] \xrightarrow{\beta} \mathbb{Z}/N\mathbb{Z} \to 0$$

such that, for any $\mathbb{Z}((q))$-algebra R, $\zeta \in \mu_N(R)$, $P \in \mathrm{Tate}(q)[N](R)$, one has

$$\langle \alpha(\zeta),\, P\rangle_{\mathrm{Tate}(q)[N]} = \zeta^{\beta(P)}.$$

This is the same elliptic curve which is called $\mathrm{Tate}(q)$ in [86, (8.8)].

Remark The computation of c_6 does not match the one given in [86, (8.8)]: in *loc.cit.*, the authors write that c_6-invariant of the Tate curve is E_6. This seems to be a mistake (rather than a different definition for the Tate curve): in particular, it implies by [152, Theorem V.5.3] that the specialization of the Tate curve at any $q \in (3\mathbb{Z}_3)^3$ has *nonsplit* multiplicative reduction. Thus [152, Theorem V.3.1] contradicts the claim [86, (8.8, T3)] about the torsion subscheme of the Tate curve. Given that *loc.cit.* refers to [36, 85] and that these both references use the same exact sequence for the torsion of the Tate curve (for instance [36, Construction 1.15]), it seems reasonable that the correction to make is to clarify in [86, (8.8)] that the c_6-invariant of the Tate curve is $-E_6$.

Remark Let R be a regular excellent Noetherian ring and $\mathscr{P}$ be a finite representable moduli problem over $\mathbf{Ell}_R$ normal near infinity. Then the formal completion of $\overline{\mathscr{M}}(\mathscr{P})$ along its cuspidal subscheme is, by [86, Lemma 8.11.2], the normalization of $R[[1/j]]$ in the normal finite $R((1/j))$-scheme $\mathscr{M}(\mathscr{P}) \times_{j,\mathbb{A}^1} \operatorname{Spec} R((1/j))$. Note that there exists a canonical continuous isomorphism $R[[1/j]] \simeq R[[q]]$ defined by $j = j(\mathrm{Tate}(q))$. Thus, the formal completion of $\overline{\mathscr{M}}(\mathscr{P})$ along its cusps is naturally a $R[[q]]$-scheme.

Proposition 1.6.4 *Let R be a regular excellent Noetherian ring and $\mathscr{P}$ be a finite representable moduli problem over $\mathbf{Ell}_R$ normal near infinity. Then the formal completion of $\overline{\mathscr{M}}(\mathscr{P})$ along its cuspidal subscheme is isomorphic, as a $R[[q]]$-scheme, to the normalization of $R[[q]]$ in the finite étale $R((q))$-scheme $\mathscr{P}_{\mathrm{Tate}(q)/R((q))}/\{\pm 1\}$, where $\{\pm 1\}$ is the automorphism group of $\mathrm{Tate}(q)/R((q))$. Moreover, this isomorphism is natural with respect to morphisms of moduli problems.*

Proof. – This is [86, Theorem 8.11.10]. □

The following notation is identical to the one introduced in [86, (10.2)].

Notation *Let $N \geq 3$ and Surj_N denote the set of surjective linear $f : (\mathbb{Z}/N\mathbb{Z})^{\oplus 2} \to \mathbb{Z}/N\mathbb{Z}$. Given $\Lambda \in \mathrm{Surj}_N$, there is a unique vector k_Λ such that $\Lambda(x) = \det(k_\Lambda, x)$ for every $x \in (\mathbb{Z}/N\mathbb{Z})^{\oplus 2}$. Then k_Λ is a generator of* $\ker \Lambda$. *We also* choose *a vector ℓ_Λ such that $\Lambda(\ell_\Lambda) = 1$.*

There is a left action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on Surj_N given by $(g\cdot\Lambda)(x) = \Lambda(g^T x)$ for $x \in (\mathbb{Z}/N\mathbb{Z})^{\oplus 2}$ (seen as a column vector). In the case of $\Lambda : (x, y) \mapsto x$, one sees that $k_\Lambda = (0, -1)$, and we choose $\ell_\Lambda = (1, 0)$.

Proposition 1.6.5 *(See [86, Corollary 10.2.5, (10.3.5)].) Let $N \geq 3$ be an integer, S be a $\mathbb{Z}[1/N]$-scheme and G a finite étale commutative group scheme over S, with $N \cdot G = 0$ and a short exact sequence of abelian fppf sheaves $0 \to \mu_N \to G \xrightarrow{\pi} \mathbb{Z}/N\mathbb{Z} \to 0$. Let G_1 denote the closed subscheme $\pi^{-1}(1)$ of G. There is an isomorphism $[\Gamma(N)]_{G/S} \to \coprod_{\Lambda\in\mathrm{Surj}_N} \mu_N^\times \times_{\mathbb{Z}} G_1$, given for any connected S-scheme T by*

$$\left[\phi : (\mathbb{Z}/N\mathbb{Z})^{\oplus 2}_T \xrightarrow{\sim} G_T\right] \longmapsto \left(\phi(k_{(\pi\circ\phi)(T)}), \phi(\ell_{(\pi\circ\phi)(T)})\right)_{(\pi\circ\phi)(T)},$$

where $\left[(\pi\circ\phi)(T) : (\mathbb{Z}/N\mathbb{Z})^{\oplus 2} \to \mathbb{Z}/N\mathbb{Z}\right] \in \mathrm{Surj}_N$.

Moreover, if T is a connected S-scheme, $\Lambda \in \mathrm{Surj}_N$, $\zeta \in \mu_N(T), X \in G_1(T)$, and $(\zeta, X)_\Lambda$ is the image of $\iota \in [\Gamma(N)]_{G/S}(T)$, then, for $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the image of $g \cdot \iota$ is given by $(\zeta', X')_{\Lambda'}$, where

- $\Lambda' = \Lambda(g^T \cdot)$, $k_{\Lambda'} = (\det g)(g^T)^{-1} k_\Lambda$,
- $\ell_{\Lambda'} = (g^T)^{-1}\ell_\Lambda + n(g,\Lambda)(g^T)^{-1}k_\Lambda$ *for some* $n(g,\Lambda) \in \mathbb{Z}/N\mathbb{Z}$,
- $\zeta' = \zeta^{\det g}$ *and* $X' = X \cdot \zeta^{n(g,\Lambda)}$.

Proof. – This is the same as [86, (10.2), (10.3)], except that the compatibility with the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is a slightly different calculation. □

Corollary 1.6.6 *Let $N \geq 3$ be an integer, $g, g' \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\Lambda \in \mathrm{Surj}_N$. Then one has*

$$\begin{pmatrix} \det g'g & 0 \\ n(g'g,\Lambda) & 1 \end{pmatrix} = \begin{pmatrix} \det g' & 0 \\ n(g', g\cdot\Lambda) & 1 \end{pmatrix} \begin{pmatrix} \det g & 0 \\ n(g,\Lambda) & 1 \end{pmatrix}.$$

Proof. – This is a direct calculation. □

Proposition 1.6.7 *Let $N \geq 3$ be an integer and fix a system $(\Lambda_i)_{i\in I}$ of representatives for $\mathrm{Surj}_N/\{\pm 1\}$. Then the formal completion of $\mathrm{We} : X(N) \to \operatorname{Spec}\mathcal{O}_N$ along its cuspidal subscheme is isomorphic to*

$$\coprod_{i\in I} \operatorname{Spf}(\mathcal{O}_N[[q^{1/N}]]).$$

Moreover, let $(i,g) \in I \times \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, there exists $(j,g') \in I \times \{\pm g\}$ such that $\Lambda_i \circ (g')^T = \Lambda_j$. Then, the action of g is the same as the action of g'; it induces a morphism from the Λ_i component to the Λ_j component, coming from the ring homomorphism $(\zeta_N, q^{1/N}) \longmapsto (\zeta_N^{\det g}, \zeta_N^{n(g',\Lambda_i)} q^{1/N})$.

Proof. – This is a consequence of Proposition 1.6.5, which we applied to the description of the N-torsion group of $\mathrm{Tate}(q)$ over $\mathbb{Z}((q))[N^{-1}]$ [86, (8.8)] (because $-I_2$ acts without any fixed point on Surj_N since $N > 2$). The conclusion then follows from Proposition 1.6.4. Note that the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ must preserve q since q can be written as a formal power series in $1/j$. □

Corollary 1.6.8 *Let $N \geq 3$ be an integer. Then the cuspidal subscheme of $X(N)$ is a finite disjoint reunion of copies of $(\mu_N^\times)_{\mathbb{Z}[1/N]}$ indexed by $\mathrm{Surj}_N/\{\pm 1\}$.*

Proposition 1.6.9 *Let $N \geq 3$ be an integer and $\ell \equiv 1 \mod N$ be a prime. Let $J(N)$ be the relative Jacobian of $X(N) \to \operatorname{Spec}\mathbb{Z}[1/N]$ and $\Delta : X(N) \times_{\operatorname{Spec}\mathcal{O}_N} X(N) \to J(N)$ be the difference map (see Propositions 1.3.9 and A.4.29). Let $\iota : C \to X(N)$ be the cuspidal subscheme. Then $(T_\ell - \ell - 1) \circ \Delta \circ (\iota \times \iota) = 0$.*

Proof. – First, denote by $f : C' \to J(N)$ the morphism $(T_\ell - \ell - 1) \circ \Delta \circ (\iota \times \iota)$, where $C' := C \times_{\operatorname{Spec}\mathbb{Z}[1/N,\zeta_N]} C$ is a finite étale $\mathbb{Z}[1/N]$-scheme. Let D be the scheme-theoretic image of f. Then D is a closed subscheme of $J(N)$, so it is of finite type over $\mathbb{Z}[1/N]$. Since C' is finite over $\mathbb{Z}[1/N]$, it is affine, and the morphism $C' \to D$ is finite surjective: by [4, Lemma 01YQ], D is affine, and thus D is finite over $\mathbb{Z}[1/N]$. Moreover, since $C' \to \mathbb{Z}[1/N]$ is finite étale, $\mathcal{O}(D)$ is torsion-free, so $D \to \mathbb{Z}[1/N]$ is flat and unramified, hence D is finite étale over $\mathbb{Z}[1/N]$. To show that $D \to J(N)$ is the unit section, we only need to check that the fibre of D at ℓ is the unit section of $J(N)_{\mathbb{F}_\ell}$.

Since C is a disjoint reunion of copies of $\mathcal{O}_N$ and $\ell \equiv 1 \mod N$, $C'_{\mathbb{F}_\ell}$ is a finite reunion of copies of $\operatorname{Spec}\mathbb{F}_\ell$. In other words, we want to prove that for any two cuspidal points $x, y \in X(N)(\mathbb{F}_\ell)$ with the same image in $\operatorname{Spec}\mathbb{F}_\ell \otimes \mathbb{Z}[\zeta_N]$, one has $T_\ell(x-y) = (\ell+1)(x-y)$. The conclusion follows from Proposition 1.5.15, since $[\ell]$ acts trivially on $J(N)$, $x - y \in J(N)(\mathbb{F}_\ell)$, and the Frobenius isogeny on $J(N)_{\mathbb{F}_\ell}$ has degree ℓ. □

Proposition 1.6.10 *Let $N \geq 3$ be an integer. Let $\Lambda \in \mathrm{Surj}_N$ and $M = \begin{pmatrix} \alpha & 0 \\ u & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Let $U \subset X(N)$ be the affine inverse image of the open subset $\{j \neq 0, 1728\} \subset \mathbb{P}^1_{\mathbb{Z}[1/N]}$. Then the datum*

$$\Big(\mathrm{Tate}(q), (k_\Lambda, \ell_\Lambda) \longmapsto (\zeta_N^\alpha, q^{1/N}\zeta_N^u)\Big)$$

defines a morphism of $\mathcal{O}_N \otimes \mathbb{Z}[[q]]$-schemes $C_{(M,\Lambda)} : \mathrm{Spec}\, \mathcal{O}_N \otimes \mathbb{Z}[[q^{1/N}]] \to U \times_{\mathbb{Z}[1/j]} \mathrm{Spec}\, \mathbb{Z}[[q^{1/N}]]$ such that the composition

$$\mathrm{Spec}\, \mathcal{O}_N \to \mathrm{Spec}\, \mathcal{O}_N \otimes \mathbb{Z}[[q^{1/N}]] \overset{C_{(M,\Lambda)}}{\longrightarrow} U \times_{\mathbb{Z}[1/j]} \mathrm{Spec}\, \mathbb{Z}[[q^{1/N}]] \overset{\mathrm{We}}{\to} \mathrm{Spec}\, \mathcal{O}_N$$

is given by $\zeta \longmapsto \zeta^\alpha$.

Given a regular excellent Noetherian $\mathbb{Z}[1/N]$-algebra R and $\omega \in H^0(X(N)_R, \Omega^1_{X(N)_R/R})$, there is a unique $f \in \mathcal{O}_N \otimes R[[q^{1/N}]]$ such that, for every $t \geq 1$, the pull-back of ω under the morphism $\mathrm{Spec}\, \mathcal{O}_N \otimes R \otimes \mathbb{Z}[q^{1/N}]/(q^t) \to \mathrm{Spec}\, \mathcal{O}_N \otimes R \otimes \mathbb{Z}[[q^{1/N}]] \overset{C_{(M,\Lambda)}}{\longrightarrow} U_R$ can be written as $f \cdot d(q^{1/N})$.

Proof. – By [86, (8.7),(8.8)], the group of sections of the N-torsion subscheme of $\mathrm{Tate}(q)$ over $\mathcal{O}_N \otimes \mathbb{Z}((q))$ identifies with the group $\zeta_N^{\mathbb{Z}/N\mathbb{Z}} \times q^{\left(\frac{1}{N}\mathbb{Z}\right)/\mathbb{Z}}$.

Consider the morphism $C^0_{(M,\Lambda)} : \mathrm{Spec}\, \mathcal{O}_N \otimes \mathbb{Z}((q^{1/N})) \to Y(N)$ given by the elliptic curve $(\mathrm{Tate}(q), \iota)$, where $\iota : (\mathbb{Z}/N\mathbb{Z})^{\oplus 2} \to \mathrm{Tate}(q)[N](\mathcal{O}_N \otimes \mathbb{Z}((q^{1/N})))$ is the isomorphism mapping the $(k_\Lambda, \ell_\Lambda)$ to $(\zeta_N^\alpha, q^{1/N}\zeta_N^u)$. The post-composition of this morphism with the j-invariant (resp. the Weil pairing) is exactly given by the inclusion $\mathbb{Z}[j] \subset \mathbb{Z}((q))$ (resp. the projection $\mathrm{Spec}\, \mathcal{O}_N \otimes \mathbb{Z}((q)) \to \mathrm{Spec}\, \mathcal{O}_N$). Let $U \subset Y(N)$ denote the inverse image of open subscheme of $\mathbb{P}^1_{\mathbb{Z}[1/N]}$ where $1/j$ is defined and $1728/j - 1$ is invertible, then U is affine since $\mathbb{P}^1_{\mathbb{Z}[1/N]}$ is separated. By [86, (8.11.5)], one has $j(\mathrm{Tate}(q))(j(\mathrm{Tate}(q)) - 1728) \in \mathbb{Z}((q))^\times$, so $C^0_{(M,\Lambda)}$ induces a morphism

$$C^1_{(M,\Lambda)} : \mathrm{Spec}\, \mathcal{O}_N \otimes \mathbb{Z}((q^{1/N})) \to U \times_{\mathrm{Spec}\, \mathbb{Z}[1/j]} \mathrm{Spec}\, \mathbb{Z}[[q]].$$

In $\mathbb{Z}[[q]]$, $\frac{1728}{j} - 1 \in -1 + q\mathbb{Z}[[q]]$ is invertible, so $U \times_{\mathrm{Spec}\, \mathbb{Z}[1/j]} \mathrm{Spec}\, \mathbb{Z}[[q]]$ is a finite $\mathcal{O}_N \otimes \mathbb{Z}[[q]]$-scheme, so the image of $C^1_{(M,\Lambda)}$ factors through the spectrum of the integral closure C of $A := \mathcal{O}_N \otimes \mathbb{Z}[[q]]$ in $B := \mathcal{O}_N \otimes \mathbb{Z}((q^{1/N}))$. The normalization of $\mathbb{Z}[[q]]$ in $\mathbb{Z}((q^{1/N}))$ is clearly $\mathbb{Z}[[q^{1/N}]]$; since normalization commutes with smooth base change [4, Lemma 03GG] and $\mathcal{O}_N$ is smooth over $\mathbb{Z}$, one has $C = \mathcal{O}_N \otimes \mathbb{Z}[[q^{1/N}]]$.

Hence $C^1_{(M,\Lambda)}$ factors through a finite morphism

$$C_{(M,\Lambda)} : \mathrm{Spec}\, \mathcal{O}_N \otimes \mathbb{Z}[[q^{1/N}]] \to U \times_{\mathbb{Z}[1/j]} \mathrm{Spec}\, \mathbb{Z}[[q^{1/N}]].$$

Let R be a regular excellent Noetherian $\mathbb{Z}[N^{-1}]$-algebra. For every integer $t \geq 1$, consider the map $C^R_{(M,\Lambda),t} : \mathrm{Spec}\, \mathcal{O}_N \otimes R \otimes \mathbb{Z}[[q^{1/N}]]/(q^t) \to U_R \times_{\mathbb{Z}[1/j]} \mathrm{Spec}\, \mathbb{Z}[[q^{1/N}]]$. Since

$$\Omega^1_{\left(\mathcal{O}_N \otimes R \otimes \mathbb{Z}[[q^{1/N}]]/(q^t)\right)/R} \simeq \frac{(\mathcal{O}_N \otimes R)[[q^{1/N}]]}{(q^t, Ntq^{t-1/N})} \cdot dq^{1/N},$$

there exists a unique $f_{(M,\Lambda),t}(\omega) \in (\mathcal{O}_N \otimes R)[[q^{1/N}]]/(q^t, Ntq^{t-1/N})$ such that

$$f_{(M,\Lambda),t}(\omega) d(q^{1/N}) = (C^R_{(M,\Lambda),t})^* \omega.$$

To conclude, it is enough to note that $\varprojlim \left[\frac{(\mathcal{O}_N \otimes R)[[q^{1/N}]]}{(q^t, Ntq^{t-1/N})}\right] \simeq (R \otimes \mathcal{O}_N)[[q^{1/N}]]$. □

Definition 1.6.11 In the setting of Proposition 1.6.10, f is the q-expansion of the differential

ω at the cusp datum (M, Λ). Let $C^*_{(M,\Lambda)}$ denote the morphism

$$\omega \in H^0(X(N)_R, \Omega^1_{X(N)_R/R}) \longmapsto f \in \mathcal{O}_N \otimes R[[q^{1/N}]].$$

Lemma 1.6.12 *Consider the setting of Proposition 1.6.10. The formation of the R-linear morphism $C^*_{(M,\Lambda)} : H^0(X(N)_R, \Omega^1_{X(N)_R/R}) \to \mathcal{O}_N \otimes R[[q^{1/N}]]$ of q-expansion at (M, Λ) commutes with base change, and its image is contained in the subring $\mathcal{O}_N \otimes R \otimes (\mathbb{Z}[1/N])[[q^{1/N}]]$. Moreover, if $g \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, then the q-expansion of ω at $\left(\begin{pmatrix} \det g & 0 \\ n(g,\Lambda) & 1 \end{pmatrix} M, g \cdot \Lambda\right)$ (the second coordinate is exactly $\Lambda \circ g^T$) is the same as the q-expansion at (M, Λ) of $g^*\omega$.*

Proof. – The first part of this statement is clear by Proposition A.4.34. To prove the second part of the claim, write

$$M = \begin{pmatrix} \alpha & 0 \\ u & 1 \end{pmatrix}, \; M' = \begin{pmatrix} \det g & 0 \\ n(g,\Lambda) & 1 \end{pmatrix} M = \begin{pmatrix} \alpha \det g & 0 \\ \alpha n(g,\Lambda) + u & 1 \end{pmatrix}.$$

We will show that $C_{(M',g\cdot\Lambda)} = g \circ C_{(M,\Lambda)}$. In the notation of the proof of Proposition 1.6.10, it is enough to check that $C^0_{(M',\Lambda\circ g^T)} = g \circ C^0_{(M,\Lambda)}$.

The morphism $g \circ C^0_{(M,\Lambda)} \in Y(N)(\mathcal{O}_N \otimes \mathbb{Z}((q^{1/N})))$ corresponds to the couple $(\mathrm{Tate}(q), \lambda \circ g^T)$, where $\lambda : (\mathbb{Z}/N\mathbb{Z})^{\oplus 2} \to \mathrm{Tate}(q)[N](\mathcal{O}_N \otimes \mathbb{Z}((q^{1/N})))$ maps $(k_\Lambda, \ell_\Lambda)$ to $(\zeta_N^\alpha, q^{1/N}\zeta_N^u)$. Thus, by Proposition 1.6.5,

$$\begin{aligned}(\lambda \circ g^T)(k_{\Lambda'}) &= \lambda(\det g k_\Lambda) = \zeta_N^{\alpha \det g}, \\ (\lambda \circ g^T)(\ell_{\Lambda'}) &= \lambda(\ell_\Lambda)\lambda(n(g,\Lambda)k_\Lambda) = q^{1/N}\zeta_N^{u+\alpha n(g,\Lambda)},\end{aligned}$$

hence $(\mathrm{Tate}(q), \lambda \circ g^T)$ is exactly the morphism attached to $C_{(M',g\cdot\Lambda)}$. □

Remark By considering a model of $X(N)$ and its cuspidal subscheme over $\mathbb{Z}[\zeta_N]$ (as in, say, [86, Theorem 10.9.1]), one can show that the image of this map is contained in the subring $\mathbb{Z}[\zeta_N] \otimes R \otimes \mathbb{Z}[[q^{1/N}]]$, that is, that the denominators of the q-expansion are bounded. We do not do this here, because it is not relevant to the rest of the text.

Proposition 1.6.14 *In the setting of Proposition 1.6.10, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_N \otimes R$ and $x \in X(N)_R$ be the image of the prime ideal $(\mathfrak{p}, q^{1/N})$ under $C_{(M,\Lambda)}$. Then the local homomorphism $(C_{(M,\Lambda)})^\sharp : \mathcal{O}_{X(N)_R,x} \to (\mathcal{O}_N \otimes R)_\mathfrak{p}[[q^{1/N}]]$ becomes an isomorphism after completion.*

In particular, for any $t \geq 1$,

$$\omega_x \in \mathfrak{m}^t_{X(N)_R,x}\Omega^1_{X(N)_R/R,x} \iff C^*_{(M,\Lambda)}\omega \in (\mathfrak{p}, q^{1/N})^t(\mathcal{O}_N \otimes R)_\mathfrak{p}[[q^{1/N}]].$$

Proof. – We keep the notation of the proof of Proposition 1.6.10.

Let $y \in B := \mathrm{Spec}\,(\mathcal{O}_N \otimes R)_\mathfrak{p} \otimes (\mathbb{Z}[1/N])[[q^{1/N}]]$ be the point corresponding to the prime ideal $(\mathfrak{p}, q^{1/N})$. The scheme morphism $C^{(M,\Lambda)}$ induces a local homomorphism of $R[1/j]_{(1/j)}$-algebras

$$\mu = C^\sharp_{(M,\Lambda)} : \mathcal{O}_{U_R,x} \to \mathcal{O}_{B,y} = (\mathcal{O}_N \otimes R)_\mathfrak{p}[[q^{1/N}]].$$

By Proposition 1.2.14, there exists $j_N \in \mathcal{O}_{U_R,x}$ such that the cuspidal subscheme of U_R is exactly, in a neighborhood of x, cut out by the section j_N. Thus $(j_N) = \sqrt{(1/j)}$ as ideals of $\mathcal{O}_{U_R,x}$. Because U_R is a smooth R-scheme, $\mathcal{O}_{U_R,x}$ is a regular local ring, hence a unique factorization domain by [4, Lemma 0AG0]. The local ring $\mathcal{O}_{U_R,x}/(j_N)$ is the ring of stalks of the cuspidal subscheme at x, so it is a regular local ring. Hence $j_N \in \mathcal{O}_{U_R,x}$ is prime.

The closed subspace cut out by the kernel K of the morphism $\mathcal{O}_{U_R,x} \to \mathcal{O}_{B,y}/(q^{1/N})$ is the cuspidal subspace. Since $\mathcal{O}_{B,y}/(q^{1/N})$ is reduced, $K = j_N\mathcal{O}_{U_R,x}$, so $\mu_q : \mathcal{O}_{U_R,x}/(j_N) \to \mathcal{O}_{B,y}/(q^{1/N})$ is a homomorphism of R-algebras such that, by Proposition 1.6.10, the following diagram commutes, and its vertical maps are localizations at prime ideals with the same restriction to R by Corollary 1.6.8:

$$\begin{array}{ccc} \mathcal{O}_N \otimes R & \xrightarrow{\det M \otimes \mathrm{id}} & \mathcal{O}_N \otimes R \\ \downarrow & & \downarrow \\ \mathcal{O}_{U_R,x}/(j_N) & \xrightarrow{\mu_q} & \mathcal{O}_{B,y}/(q^{1/N}). \end{array}$$

Hence μ_q is an isomorphism. In particular, it implies that $\mathcal{O}_{U_R,x} \to \mathcal{O}_{B,y}/(\mathfrak{p}, q^{1/N})$ is onto. Since $\mathcal{O}_{U_R,x}/(j_N)$ is the ring of stalks at x of the finite étale (over R) cuspidal subscheme of $X(N)_R$, its maximal ideal is generated by $\mathfrak{p}$: hence the maximal ideal of $\mathcal{O}_{U_R,x}$ is generated by $(\mathfrak{p}, j_N)$, and the maximal ideal of $\mathcal{O}_{B,y}$ is generated by $\mu(\mathfrak{m}_{U_R,x})$. Hence $\mathcal{O}_{U_R,x} \to \mathcal{O}_{B,y}/(\mathfrak{p}, q^{1/N})^t$ is onto for every $t \geq 1$.

Thus the completion morphism $\hat{\mu} : \widehat{\mathcal{O}_{U_R,x}} \to (\widehat{\mathcal{O}_N \otimes R})_{\mathfrak{p}}[[q^{1/N}]]$ is a surjective homomorphism of regular local rings by [4, Lemma 07NY]. We show that the two regular local rings have the same dimension, which implies that $\hat{\mu}$ is an isomorphism. By [4, Lemma 07NV], it is enough to show that $\mathcal{O}_{U_R,x}$ and $(\mathcal{O}_N \otimes R)_{\mathfrak{p}}[x]_{(x)}$ have dimension $1 + \dim R_{\mathfrak{p}'}$, where $\mathfrak{p}'$ is the inverse image in R of $\mathfrak{p}$. In fact, both rings are the rings of stalks at a point z of a smooth R-scheme of relative dimension one, z being mapped to the prime ideal $\mathfrak{p}'$, and z being closed in the fibre at $\mathfrak{p}'$. The conclusion then follows from usual dimension theory (for instance [106, Theorem 4.3.12] and [4, Lemma 02G1]).

Therefore, for every $t \geq 1$, $\mu_t : \mathcal{O}_{U_R,x}/\mathfrak{m}_{U_R,x}^t \to \mathcal{O}_{B,y}/(\mathfrak{p}, q^{1/N})^t$ is an isomorphism.

Since the local sections $1/j$ and j_N cut out the same closed subspace of U_R in a neighborhood of x, $1/j \in \mathcal{O}_{U_R,x}^{\times} j_N^s$ for some $s \geq 1$. By Proposition 1.6.7[11], one has $s = N$. Then $\mu(j_N)^N \in \mathcal{O}_{B,y}^{\times} \cdot (1/j) = \mathcal{O}_{B,y}^{\times} q$, therefore $\mu(j_N) \in (\mathcal{O}_N \otimes R)_{\mathfrak{p}}^{\times} q^{1/N} + q^{2/N}\mathcal{O}_{B,y}$.

Now, $\Omega^1_{U_R/R,x}$ is a free $\mathcal{O}_{U_R/R,x}$-module of rank one with basis dj_N by [15, §2.2 Proposition 7]. Write $\omega_x = g dj_N$: then one has $C^*_{(M,\Lambda)}\omega = \frac{d\mu(j_N)}{dq^{1/N}}\mu(g) \cdot dq^{1/N}$, with $\mu(g), \mu(j_N) \in (\mathcal{O}_N \otimes R)_{\mathfrak{p}}[[q^{1/N}]]$ and the derivative $\frac{d\mu(j_N)}{dq^{1/N}}$ is computed formally in $(\mathcal{O}_N \otimes R)_{\mathfrak{p}}[[q^{1/N}]]$.

We saw above that $\frac{d\mu(j_N)}{dq^{1/N}} \in (\mathcal{O}_N \otimes R)_{\mathfrak{p}}[[q^{1/N}]]^{\times}$ was invertible. Therefore, for $t \geq 1$, $\omega_x \in \mathfrak{m}_{U_R,x}^t \Omega^1_{U_R/R,x}$ if and only if $g \in \mathfrak{m}_{U_R,x}^t$, if and only if $\mu(g) \in (\mathfrak{p}, q^{1/N})^t \mathcal{O}_{B,y}$ if and only if $\frac{d\mu(j_N)}{dq^{1/N}}\mu(g) \in (\mathfrak{p}, q^{1/N})^t \mathcal{O}_{B,y}$, whence the conclusion.

□

Proposition 1.6.15 *In the notation of Lemma 1.6.12, the morphism*

$$C^*_{(M,\Lambda)} : H^0(X(N)_R, \Omega^1_{X(N)_R/R}) \to \mathcal{O}_N \otimes R \otimes (\mathbb{Z}[1/N])[[q^{1/N}]]$$

is injective and its cokernel is flat.

Therefore, if S is a regular excellent Noetherian R-algebra, with $R \to S$ injective, the inverse image of $\mathcal{O}_N \otimes R \otimes (\mathbb{Z}[1/N])[[q^{1/N}]]$ under

$$(C^*_{(M,\Lambda)}) : H^0(X(N)_S, \Omega^1_{X(N)_S/S}) \to \mathcal{O}_N \otimes S \otimes (\mathbb{Z}[1/N])[[q^{1/N}]]$$

is exactly $H^0(X(N), \Omega^1_{X(N)_R/R})$.

Proof. – By Proposition A.4.34, and since $\mathbb{Z}[\zeta_N, N^{-1}][[q^{1/N}]]$ is a torsion-free abelian group,

[11] The formal variable q in Proposition 1.6.7 is actually the same as the one in this proof, because $1/j$ can be written as the same formal power series in either variable. However, the $q^{1/N}$ do not have to be the same.

$H^0(X(N)_R, \Omega^1_{X(N)_R/R})$ and $\mathbb{Z}[\zeta_N] \otimes R \otimes (\mathbb{Z}[1/N])[[q^{1/N}]]$ are flat R-modules. The same Proposition implies that $(C^S_{(M,\Lambda)})^* \cong (C^R_{(M,\Lambda)})^* \otimes_R S$ if S is a regular excellent Noetherian R-algebra.

Assume that $(C^{\mathbb{Z}[1/N]}_{(M,\Lambda)})^*$ is injective and remains injective after tensoring with $\mathbb{F}_p$ for any prime $p \nmid N$. Let V denote the cokernel of $C^{\mathbb{Z}[1/N]}_{(M,\Lambda)})^*$: then for any prime $p \nmid N$, one has $\mathrm{Tor}_1^{\mathbb{Z}[1/N]}(\mathbb{F}_p, V) = 0$. Hence V is flat over $\mathbb{Z}[1/N]$, and the sequence

$$0 \to H^0(X(N), \Omega^1_{X(N)/\mathbb{Z}[1/N]}) \to \mathbb{Z}[\zeta_N] \otimes (\mathbb{Z}[1/N])[[q^{1/N}]] \to V \to 0$$

remains exact after tensoring with any $\mathbb{Z}[1/N]$-module, so we are done.

Since $(C^{\mathbb{Z}[1/N]}_{(M,\Lambda)})^*$ is injective if and only if $(C^{\mathbb{Q}}_{(M,\Lambda)})^*$ is injective, it is enough to show that $(C^R_{(M,\Lambda)})^*$ is injective for any field R of characteristic not dividing N.

Thus, let R be any field of characteristic not dividing R, and let $\omega \in H^0(X(N)_R, \Omega^1_{X(N)_R/R})$ be in the kernel of $C^*_{(M,\Lambda)}$. Let $x \in X(N)_R$ be the image under $(C_{(M,\Lambda)} \times R$ of any ideal of the form $(\mathfrak{p}, q^{1/N})$ for some prime ideal $\mathfrak{p} \subset R \otimes \mathbb{Z}[\zeta_N]$. Then, by Proposition 1.6.14, one has $\omega_x \in \cap_{t \geq 1} \mathfrak{m}^t_{X(N)_R,x} \Omega^1_{X(N)_R/R,x}$. Since $\Omega^1_{X(N)_R/R,x}$ is a free $\mathcal{O}_{X(N)_R,x}$-module of rank one, by Krull's theorem [106, Corollary 1.3.13], $\omega_x = 0$.

Since $X(N)_R \to \operatorname{Spec} R$ is smooth of relative dimension one, $\Omega^1_{X(N)_R/R}$ is an invertible $\mathcal{O}_{X(N)_R}$-module, and its global section ω vanishes on some open subscheme $U \subset X(N)_R$ such that U contains the cuspidal subscheme of $X(N)_R$. Then U is dense in the regular scheme $X(N)_R$, so that, for any affine open subscheme V, the restriction $\Omega^1_{X(N)_R/R}(V) \to \Omega^1_{X(N)_R/R}(V \cap U)$ is injective, hence $\omega = 0$. □

Let us finish this section with a lemma that will help us compute the full q-expansion of a differential.

Lemma 1.6.16 *Let $N \geq 3$ be an integer and $c \in (\mathbb{Z}/N\mathbb{Z})^\times$, then*

$$C_{(I_2,(x,y)\mapsto x)} \circ \underline{c} = \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} C_{(I_2,(x,y)\mapsto x)}.$$

Proof. – The $\mathbb{Z}[1/N]$-scheme $X(N)$ is proper smooth and $\mathcal{O}_N \otimes \mathbb{Z}[[q^{1/N}]]$ is reduced, so it is enough to show that $C^0_{(I_2,(x,y)\mapsto x)} \circ \underline{c} = \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} C^0_{(I_2,(x,y)\mapsto x)}$.

Since $k_{(x,y)\mapsto x} = (0,-1)$ and $\ell_{(x,y)\mapsto x} = (1,0)$, $C^0_{(I_2,(x,y)\mapsto x)}$ is the point

$$(\mathrm{Tate}(q), q^{1/N}, \zeta_N^{-1}) \in Y(N)(\mathcal{O}_N \otimes \mathbb{Z}((q^{1/N}))).$$

Thus, the morphisms $C^0_{(I_2,(x,y)\mapsto x)} \circ \underline{c}$, $\begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix} C^0_{(I_2,(x,y)\mapsto x)}$ are attached to the following elliptic curves with level structure over $\mathcal{O}_N \otimes \mathbb{Z}((q^{1/N}))$:

$$(\mathrm{Tate}(q), q^{1/N}, \zeta_N^{-c}),\ (\mathrm{Tate}(q), q^{1/N}, \zeta_N^{-c}),$$

which are equal, whence the conclusion.

□

Lemma 1.6.17 *Let $N \geq 3$ be an integer, (M_1, Λ_1) be a cusp datum and $g \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Then there exists a cusp datum $(M_2, \Lambda_2) = (M_2, \Lambda_1 \circ g^T)$ such that $g \circ C_{(M_1,\Lambda_1)} = C_{(M_2,\Lambda_2)}$.*

Proof. – Since $X(N)$ is a proper $\mathbb{Z}[1/N]$-scheme and $\mathcal{O}_N \otimes \mathbb{Z}[[q^{1/N}]]$ is reduced, it is enough to show that for some cusp datum (M_2, Λ_2), one has $g \circ C^0_{(M_1,\Lambda_1)} = C^0_{(M_2,\Lambda_2)}$.

Let $M_1 = \begin{pmatrix} \alpha_1 & 0 \\ u_1 & 1 \end{pmatrix}$, then $C^0_{(M_1,\Lambda)}$ is the point

$$(\mathrm{Tate}(q), (k_{\Lambda_1}, \ell_{\Lambda_1}) \mapsto (\zeta_N^{\alpha_1}, q^{1/N}\zeta_N^{u_1})) \in Y(N)(\mathcal{O}_N \otimes \mathbb{Z}((q^{1/N}))).$$

Thus $g \circ C^0_{(M_1,\Lambda_1)}$ is the point

$$(\mathrm{Tate}(q), ((g^T)^{-1}k_{\Lambda_1}, (g^T)^{-1}\ell_{\Lambda_1}) \mapsto (\zeta_N^{\alpha_1}, q^{1/N}\zeta_N^{u_1})) \in Y(N)(\mathcal{O}_N \otimes \mathbb{Z}((q^{1/N}))),$$

which is equal by Proposition 1.6.5 to

$$(\mathrm{Tate}(q), (k_{\Lambda_2}, \ell_{\Lambda_2} - n(g,\Lambda_1)k_{\Lambda_2}) \mapsto (\zeta_N^{\alpha_1}, q^{1/N}\zeta_N^{u_1})) \in Y(N)(\mathcal{O}_N \otimes \mathbb{Z}((q^{1/N}))),$$

which is equal to

$$(\mathrm{Tate}(q), (k_{\Lambda_2}, \ell_{\Lambda_2}) \mapsto (\zeta_N^{\alpha_1}, q^{1/N}\zeta_N^{u_1+n(g,\Lambda_1)\alpha_1})) \in Y(N)(\mathcal{O}_N \otimes \mathbb{Z}((q^{1/N}))),$$

which is exactly $C^0_{(M_2,\Lambda_2)}$ with $M_2 = \begin{pmatrix} \alpha_1 & 0 \\ u_1 + n(g,\Lambda_1)\alpha_1 & 1 \end{pmatrix}$.

□

Chapter 2

The geometric situation

2.1 Statement of results

We introduce the objects that we will be working with in this chapter, and state the results that we aim to prove. We refer to the next subsection for a more careful discussion of why (or how) the various constructions sketched here are well-defined, and mostly conform to standard notation.

Let $p \geq 7$ be a prime number.

Let $X(p,p)$ be the compactified modular curve over $\mathbb{Z}[1/p]$ parametrizing the elliptic curves endowed with a full level p structure. This curve possesses an action of $\mathbb{F}_p^\times$ (denoted by $[-]$) and Hecke correspondences T_ℓ for $\ell \neq p$; all of them act on its Jacobian $J(p,p)$, we denote by $\mathbb{T}$ the commutative subring of $\mathrm{End}(J(p,p))$ generated by the T_ℓ and the $[n]$ for any $n \in \mathbb{F}_p^\times$. For every $n \geq 1$ coprime to p, we can define a Hecke operator $T_n \in \mathbb{T}$ by the usual formulas (see Definition 2.2.1). Moreover, there is a natural action of $\mathrm{GL}_2(\mathbb{F}_p)$ on $X(p,p)$, which induces by push-forward functoriality an action of $\mathrm{GL}_2(\mathbb{F}_p)$ on $J(p,p)$ (such that nI_2 acts by $[n]$ for any $n \in \mathbb{F}_p^\times$), which commutes to $\mathbb{T}$. We wish to understand the structure of this action of $\mathbb{T}[\mathrm{GL}_2(\mathbb{F}_p)]$ on $J(p,p)$. This will enable us in later chapters to discuss the Tate module of $J(p,p)$, then of its various twists by Galois representations.

Let $X_1(p)$ be the compactified modular curve over $\mathbb{Z}[1/p]$ parametrizing elliptic curves endowed with a point of order p, and $X_1(p,\mu_p) = X_1(p)_{\mathbb{Z}[1/p,\zeta_p]}$, seen as a smooth projective curve over $\mathbb{Z}[1/p]$. Its non-cuspidal points parametrize triples (E,P,α), where E is a relative elliptic curve over some base S, $P \in E(S)$ is a point of order p, and $\alpha \in \mathcal{O}(S)$ is a primitive p-th root of unity. The curve $X_1(p,\mu_p)$ is endowed with natural Hecke correspondences T_ℓ for primes $\ell \neq p$, U_p and diamond operators $\langle n \rangle$ for $n \in \mathbb{F}_p^\times$ (all coming from $X_1(p)$), as well as an Atkin-Lehner involution w_p. All of them induce endomorphisms of its Jacobian $J_1(p,\mu_p)$: U_p, T_ℓ and the $\langle n \rangle$ pairwise commute, but they do not commute with w_p.

We define modified Hecke operators T'_ℓ (for primes $\ell \neq p$) and modified diamond operators $\langle n \rangle'$ (for $n \in (\mathbb{Z}/p\mathbb{Z})^\times$) on $J_1(p,\mu_p)$ (see Definition 2.2.6). They generate a commutative subring $\mathbb{T}'$ of of $\mathrm{End}(J_1(p,\mu_p))$ that we call the modified Hecke algebra. As above (see Definition 2.2.8), we can define elements $T'_n \in \mathbb{T}'$ for any $n \geq 1$ coprime to p. By construction, $\mathbb{T}'$ commutes with U_p and w_p. Let $P(p)$ be the direct product of $p+1$ copies of $J_1(p,\mu_p)$ indexed by $\mathbb{F}_p \cup \{\infty\}$; we can construct actions of $\mathrm{GL}_2(\mathbb{F}_p)$, U_p and w_p on $P(p)$ which all commute with $\mathbb{T}'$.

For each $t \in \mathbb{F}_p$ (resp. $t = \infty$), we define a morphism $u_t : J(p,p) \to J_1(p,\mu_p)$ as follows by push-forward functoriality: we map a couple $(E,(P,Q))$ to $(E, tP+Q, \langle P, Q\rangle_E)$ (resp. to $(E,P,\langle P, Q\rangle_E)$), where $\langle P, Q\rangle_E$ is the Weil pairing on $E[p]$. The morphism $u : J(p,p) \to P(p)$ is the direct product of the u_t. Then $C(p) := \ker u$ is a proper group scheme over $\mathbb{Z}[1/p]$, and we let $C^0(p)$ be the connected component of $C(p)$ containing the image of the unit section.

We define the endomorphism R of $P(p)$ as follows: given $s,t \in \mathbb{F}_p \cup \{\infty\}$, the morphism $J_1(p,\mu_p)_s \subset P(p) \xrightarrow{R} P(p) \to J_1(p,\mu_p)_t$ is:

- $-U_p$ is $s = t$,
- w_p if $s \neq t$ and $\infty \in \{s, t\}$,
- $\langle s - t \rangle w_p$ if s, t are distinct elements of $\mathbb{F}_p$.

Then R commutes with $\mathbb{T}'$ and $\mathrm{GL}_2(\mathbb{F}_p)$.

Theorem 2.A *The following sequence of Abelian varieties over* $\mathbb{Q}$

$$0 \to C^0(p) \to J(p,p) \xrightarrow{u} P(p) \xrightarrow{R} P(p)$$

is exact up to isogeny. It is equivariant for the Hecke operators (that is, $T_n, \langle n \rangle$ *for* $J(p,p)$ *and* $T'_n, \langle n \rangle'$ *for* $P(p)$*) and for the actions of* $\mathrm{GL}_2(\mathbb{F}_p)$.

Thanks to this exact sequence, we can describe the space of holomorphic differentials on $X(p,p)_{\mathbb{C}}$ as a $(\mathbb{T} \otimes \mathbb{C})[\mathrm{GL}_2(\mathbb{F}_p)]$-module. To do this, we need some information about the representations of $\mathrm{GL}_2(\mathbb{F}_p)$, which is recalled in Appendix B.

Notation

- *The Steinberg representation is denoted by* St.
- *If* $\psi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ *is a caracter,* St_ψ *denotes the twist of* St *by the character* $\psi(\det)$.
- *Given two Dirichlet characters* $\alpha, \beta : \mathbb{F}_p^\times \to \mathbb{C}^\times$*, the principal series representation attached to the pair* $\{\alpha, \beta\}$ *is* $\pi(\alpha, \beta)$.
- *If* V *is a left complex representation of* $\mathrm{GL}_2(\mathbb{F}_p)$*,* $V^\vee := \mathrm{Hom}(V, \mathbb{C})$ *is a right* $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$*-module.*

Theorem 2.B *The right* $(\mathbb{T} \otimes \mathbb{C})[\mathrm{GL}_2(\mathbb{F}_p)]$*-module* $H^0(X(p,p)_{\mathbb{C}}, \Omega^1)$ *is isomorphic to the direct sum of the following modules:*

- *For every Dirichlet character* $\psi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ *and every newform* $f \in \mathcal{S}_2(\Gamma_1(p))$ *with character* χ*, modulo the relation* $(f, \psi) \sim (\overline{f}, \chi\psi)$*, the representation* $\pi(\psi, \chi\psi)^\vee$ *if* $\chi \neq \mathbf{1}$ *and* $\mathrm{St}_\psi^\vee$ *if* $\chi = 1$*. The pull-back by the Hecke operator* T_n *for an integer* $n \geq 1$ *coprime to* p *(resp. by* $m_n := nI_2$ *for* $n \in \mathbb{F}_p^\times$*) acts by multiplication by* $a_n(f)\psi(n)$ *(resp.* $\chi(n)\psi(n)^2$*).*
- *For every newform* $f \in \mathcal{S}_2(\Gamma_0(p^2) \cap \Gamma_1(p))$ *with character* χ*, an irreducible cuspidal representation* $C_f^\vee$ *of* $\mathrm{GL}_2(\mathbb{F}_p)$ *where pulling back by* T_n *(resp. by* m_n*) is multiplication by* $a_n(f)$ *(resp.* $\chi(n)$*).*

Theorem 2.C *For any field* k *of characteristic distinct from* p*, the sequence*

$$J(p,p)_k \xrightarrow{u_k} P(p)_k \xrightarrow{R_k} P(p)_k$$

is exact up to isogeny. Moreover, the groups $2p(p+1)\pi_0(\ker u_k)$ *and* $2p(p+1)\pi_0(\ker R_k)$ *vanish.*

2.2 Constructions

Let $X(p,p)$ (resp. $Y(p,p)$) be the compactified moduli scheme (resp. moduli scheme) attached to the finite étale representable moduli problem $[\Gamma(p)]_{\mathbb{Z}[1/p]}$; it is projective and smooth of relative dimension one over $\mathbb{Z}[1/p]$. We let $J(p,p)$ denote its Jacobian as a relative curve[1] over $\mathbb{Z}[1/p]$.

By Corollary 1.5.6, there are Hecke operators T_ℓ acting on $J(p,p)$ for all primes $\ell \neq p$. Since $\mathrm{GL}_2(\mathbb{F}_p)$ acts on $[\Gamma(p)]_{\mathbb{Z}[1/p]}$ (by a morphism of moduli problems of level p), it acts on $X(p,p)$

[1] In usual sources such as [15] or [119], the Jacobian of a smooth projective curve over some base is usually defined only when the geometric fibres are connected. We provide an extended definition in Appendix A.4.2 and check what properties still hold in this more general setting. Many of the constructions below are defined and studied in detail and greater generality in Chapter 1.

and thus on $J(p,p)$ by push-forward functoriality. Moreover, for any $n \in \mathbb{F}_p^\times$, the action of nI_2 on $X(p,p)$ (hence on $J(p,p)$ by push-forward functoriality) is exactly the natural action of $n \in \mathbb{F}_p^\times$ as an automorphism of moduli problems of level p (see the beginning of Section 1.1.2). By Corollary 1.5.11, the action of $\mathrm{GL}_2(\mathbb{F}_p)$ commutes to any T_ℓ for any prime $\ell \neq p$. Let $\mathbb{T}$ be the commutative sub-algebra of $\mathrm{End}(J(p,p))$ generated by the T_ℓ (for $\ell \neq p$ prime) and the nI_2 for $n \in \mathbb{F}_p^\times$.

Definition 2.2.1 We define the elements $T_n \in \mathbb{T}$ (for $n \geq 1$ coprime to p) in the following way:

- T_1 is the identity,
- for any prime $\ell \neq p$, for any $k \geq 2$, $T_{\ell^k} = T_\ell T_{\ell^{k-1}} - \ell \cdot (\ell I_2) T_{\ell^{k-2}}$.
- for coprime integers $m, n \geq 1$ such that $p \nmid mn$, $T_{mn} = T_m T_n$.

Lemma 2.2.2 *For any integers $n, m \geq 1$ coprime to p and with greatest common divisor δ, one has*

$$T_n T_m = \sum_{d|\delta} d \cdot (dI_2) T_{\frac{mn}{d^2}}.$$

In particular, for all integers $n, m_1, \ldots, m_r \geq 1$ coprime to p, $(nI_2)T_{m_1} \ldots T_{m_r}$ is a $\mathbb{Z}$-linear combination of certain $(q' I_2) \cdot T_q$, where $q', q \geq 1$ are integers such that $q(q')^2 \equiv n^2 m_1 \ldots m_r \pmod{p}$. Thus $\mathbb{T}$ is generated as a group by the T_n.

Proof. – The first part of the statement implies the second part by an easy induction. By multiplicativity, we can assume that n, m are powers of the same prime number $q \neq p$. We can assume that $n \leq m$, and we proceed by induction over n. When $n \leq q$, the identity is a reformulation of $T_q T_m = T_{qm} - q(qI_2)T_{m/q}$, which is the definition of T_{mq}. When $n > q$, one has

$$\begin{aligned} T_n T_m &= T_q T_{n/q} T_m - q(qI_2) T_{n/q^2} T_m = \sum_{d|n/q} d \cdot (dI_2) \cdot T_q T_{\frac{mn}{qd^2}} - \sum_{d|n/q^2} dq \cdot (qdI_2) \cdot T_{\frac{mn}{q^2 d^2}} \\ &= \sum_{d|n/q} d \cdot (dI_2) \cdot (T_{\frac{nm}{d^2}} + q(qI_2) T_{\frac{mn}{q^2 d^2}}) - \sum_{q \leq d|n/q} d \cdot (dI_2) \cdot T_{\frac{mn}{d^2}} \\ &= n \cdot (nI_2) T_{\frac{m}{n}} + \sum_{d|n/q} d \cdot (dI_2) T_{\frac{mn}{d^2}}, \end{aligned}$$

whence the conclusion. □

Write $\mathrm{We} : X(p,p) \to \mathrm{Spec}\, \mathbb{Z}[1/p, \zeta_p]$ for the Weil pairing as defined in Proposition 1.3.9.

We treat elements of $\mathbb{F}_p^{\oplus 2}$ as column vectors, and choose the following system S of representatives for $\mathbb{P}^1(\mathbb{F}_p)$: S is made with the $(t, 1)$ for $t \in \mathbb{F}_p$ and with $(1, 0)$.

Let $X_1(p, \mu_p)$ (resp. $Y_1(p, \mu_p)$) be the compactified moduli scheme (resp. the moduli scheme) attached to the finite étale representable moduli problem $[\Gamma_1(p)]_{\mathbb{Z}[1/p]} \times [\mathbb{Z}[1/p, \mu_p]]$ (of level p): it is projective and smooth of relative dimension one over $\mathbb{Z}[1/p]$, so it has a relative Jacobian $J_1(p, \mu_p)$. By Lemma 1.2.9, $X_1(p, \mu_p)$ is exactly the fibre product $X_1(p) \times_{\mathbb{Z}[1/p]} \mathrm{Spec}\, \mathbb{Z}[1/p, \mu_p]$. By Corollary 1.5.6, there are Hecke operators T_ℓ for $\ell \neq p$ acting on $J_1(p, \mu_p)$. Instead of the notation of Section 1.1.2, we will denote the action of $(\mathbb{Z}/p\mathbb{Z})^\times$ (given by the level p structure) by $\langle \cdot \rangle$ rather than $[\cdot]$.

Given $n \in \mathbb{F}_p^\times$, let $\underline{n}$ be the automorphism of $\mathrm{Spec}\, \mathbb{Z}[1/p, \mu_p]$ with cyclotomic character n. In particular, by base change, $n \longmapsto \underline{n}$ induces another action of $\mathbb{F}_p^\times$ on the $\mathbb{Z}[1/p]$-scheme $X_1(p, \mu_p)$: on non-cuspidal points, it maps $(E/S, P, \alpha)$ to $(E/S, P, \alpha^n)$.

Lemma 2.2.3 *For any $n \in \mathbb{F}_p^\times$, $\langle n \rangle$ is the base change of the classical diamond operator on $X_1(p)$, mapping a non-cuspidal point $(E/S, P)$ to $(E/S, nP)$. Moreover, the actions of the Hecke operators T_ℓ (for $\ell \neq p$ prime), $\langle n \rangle$ and $\underline{n}$ (for $n \in \mathbb{F}_p^\times$) commute.*

Proof. – The commutation with the Hecke operators follow from the fact that both $\langle \cdot \rangle$ and $\underline{\cdot}$ act as morphisms of moduli problems of level p. For the description of $\langle \cdot \rangle$ as well as its commutation

with $\underline{\cdot}$, both claims are formal verifications on non-cuspidal points. The conclusion follows from the fact that the open immersion $Y_1(p,\mu_p) \to X_1(p,\mu_p)$ is scheme-theoretically dense. □

By the results of Section 1.5.4, we have a "bad" Hecke operator U_p acting on $J_1(p,\mu_p)$ commuting to every T_ℓ, $\langle\cdot\rangle$, $\underline{\cdot}$, there is an Atkin-Lehner automorphism w_p (called w'_p in Section 1.5.4) of $X_1(p,\mu_p)$ acting on $J_1(p,\mu_p)$ by push-forward functoriality.

The operator w_p acts in the following way: it maps a non-cuspidal point $(E/S, P, \alpha)$ to $(E'/S, Q, \alpha)$, where $E' = E/\langle P\rangle$, $\pi : E \to E'$ is the natural isogeny, and $Q \in \ker \pi^\vee(S) \subset E'[p](S)$ is the unique point such that $\langle P, Q\rangle_{\ker\pi} = \alpha$ (in the sense of [86, (2.8)]). In particular, by [86, (2.8.6.1)], for any $Q_1 \in E[p](S')$ (with $S' \to S$ étale) such that $\langle P, Q_1\rangle_{E[N]} = \alpha$, then $Q = \pi(Q_1)$.

Lemma 2.2.4 *U_p commutes with the T_ℓ (for $\ell \neq p$ prime), as well as the $\langle n\rangle$ and the $\underline{n}$ for $n \in \mathbb{F}_p^\times$.*

Proof. – For the Hecke operators and the diamonds, it follows from Proposition 1.5.23. For $\underline{\cdot}$, it follows from Proposition A.4.25 and the fact that the following diagram is Cartesian (adopting the notation of Section 1.5.4), for $n \in \mathbb{F}_p^\times$:

$$\begin{array}{ccccc}
\overline{\mathscr{M}}([\Gamma_1(p)],[\mu_p]) & \xleftarrow[D'_{1,1}]{} & \overline{\mathscr{M}}([\Gamma'_1(p,p)],[\mu_p]) & \xrightarrow{D'_{p,1}} & \overline{\mathscr{M}}([\Gamma_1(p)],[\mu_p]) \\
\downarrow{\scriptstyle \underline{n}} & & \downarrow{\scriptstyle \underline{n}} & & \downarrow{\scriptstyle \underline{n}} \\
\overline{\mathscr{M}}([\Gamma_1(p)],[\mu_p]) & \xleftarrow[D'_{1,1}]{} & \overline{\mathscr{M}}([\Gamma'_1(p,p)],[\mu_p]) & \xrightarrow{D'_{p,1}} & \overline{\mathscr{M}}([\Gamma_1(p)],[\mu_p])
\end{array}$$

□

Lemma 2.2.5 *For any $n \in \mathbb{F}_p^\times$, one has $\langle n\rangle w_p \langle n\rangle = w_p$ and $w_p \circ \underline{n} = \underline{n} \circ \langle n\rangle \circ w_p$. Moreover, w_p is an involution and, for any prime $\ell \neq p$, $\langle \ell\rangle w_p T_\ell = T_\ell w_p$.*

Proof. – The behavior with respect to $\langle\cdot\rangle$ has been proved in Section 1.1.3 for moduli schemes and this extends to the compactified moduli scheme by Proposition 1.2.22. Similarly, $w_p \circ w_p$ is the action of $-1 \in \hat{\mathbb{Z}}^\times$; since -1 is an automorphism of any elliptic curve, it acts trivially on moduli schemes, so that $w_p \circ w_p$ is the identity. The identity about Hecke operators is a consequence of Proposition 1.5.14.

For the last equality, it is enough to prove that it holds for non-cuspidal points. If E/S is an elliptic curve and $\alpha \in \mu_p(S)$, $P \in E(S)$ is a point of exact order p, let $\pi : E \to E'$ be the isogeny whose kernel is generated by P. Then $w_p(\underline{n}(E/S,P,\alpha)) = (E', Q, \alpha^n)$, where $Q \in \ker\pi^\vee(S)$ is the unique point such that $\langle -, Q\rangle_{\ker\pi}$ maps P to α^n. Therefore, $w_p(E/S,P,\alpha) = (E'/S, n^{-1}Q, \alpha)$. Hence $\underline{n}\langle n\rangle w_p(E/S,P,\alpha) = w_p(\underline{n}(E/S,P,\alpha))$, whence the conclusion. □

Definition 2.2.6 The *modified* Hecke operator T'_ℓ on $J_1(p,\mu_p)$ is $T'_\ell = \underline{\ell} \circ T_\ell$, for any prime $\ell \neq p$. For any $n \in \mathbb{F}_p^\times$, the operator $\langle n\rangle'$ on $X_1(p,\mu_p)$ is given by $\langle n\rangle \circ \underline{n^2}$. The modified Hecke algebra $\mathbb{T}'$ is the subring of $\mathrm{End}(J_1(p,\mu_p))$ generated by the T'_ℓ (for $\ell \neq p$ prime) and the $\langle n\rangle'$ for $n \in \mathbb{F}_p^\times$.

Lemma 2.2.7 *Every element of $\mathbb{T}'$ commutes with w_p and U_p.*

Proof. – This follows from Lemmas 2.2.4 and 2.2.5. □

Definition 2.2.8 For any $n \geq 1$ coprime to p, we define an element $T'_n \in \mathbb{T}'$ as follow:

- T'_1 is the identity,
- For any prime $\ell \neq p$ and any $k \geq 2$, $T'_{\ell^k} = T'_\ell T'_{\ell^{k-1}} - \ell\langle\ell\rangle' T'_{\ell^{k-2}}$,
- For any integers $m, n \geq 1$ such that p, m, n are pairwise coprime, $T'_{mn} = T'_m T'_n$.

Definition 2.2.9 If $x = (t,1) \in S$ (resp. $x = (1,0) \in S$), the morphism $u_x : X(p,p) \to X_1(p,\mu_p)$ is the compactification (in the sense of Proposition A.2.9) of the morphism

$$(E,(P,Q)) \in Y(p,p)(S) \longmapsto (E, tP+Q, \langle P, Q\rangle_E) \in Y_1(p,\mu_p)(S).$$

Lemma 2.2.10 *Every u_x is finite locally free of constant rank and induces an isomorphism $\mathcal{O}(X_1(p,\mu_p)) \to \mathcal{O}(X(p,p))$.*

Proof. – Any u_x is a morphism of finite $\mathbb{P}^1_{\mathbb{Z}[1/p]}$-schemes (the structure map being the j-invariant in each case), so it is finite. Since $X(p,p), X_1(p,\mu_p)$ are regular schemes where every nonempty open subset has dimension two, u_x is flat by miracle flatness, so it is locally free. Since $X_1(p,\mu_p)$ is connected by Corollary 1.5.20, u_x is locally free of constant rank. The same Corollary implies that $\mathcal{O}(X_1(p,\mu_p)) = \mathbb{Z}[1/p,\zeta_p]$, and Proposition 1.3.9 shows that one also have $\mathcal{O}(X(p,p)) \simeq \mathbb{Z}[1/p,\mu_p]$, whence the conclusion. □

Let $X_1(p,\mu_p)^S$ be the disjoint reunion of $p+1$ copies of $X_1(p,\mu_p)$ indexed by S; by [4, Lemma 03GO], $X_1(p,\mu_p)^S$ can also be seen as the compactification of $p+1$ copies of $Y_1(p,\mu_p)$ indexed by S. Thus, we can also see $X_1(p,\mu_p)^S$ as the compactified moduli scheme attached to the following moduli problem over $\mathbf{Ell}_{\mathbb{Z}[1/p]}$, mapping a relative elliptic curve E/Z to the set $[\Gamma_1(p)](E/Z) \times \mu_p^\times(Z) \times \{f : Z \to S \mid f \text{ locally constant}\}$.

We let $\mathrm{GL}_2(\mathbb{F}_p)$ act on $X_1(p,\mu_p)^S$ as follows: if $M \in \mathrm{GL}_2(\mathbb{F}_p)$, $x, x' \in S, \lambda \in \mathbb{F}_p^\times$ are such that $\lambda(M^T)^{-1}x = x'$, then M acts by

$$X_1(p,\mu_p)_x \simeq X_1(p,\mu_p) \xrightarrow{\det M \circ \langle\lambda\rangle} X_1(p,\mu_p) \simeq X_1(p,\mu_p)_{x'}.$$

A straightforward calculation (using the fact that $\langle -1\rangle$ is the identity) yields:

Lemma 2.2.11 *This defines a left action of $\mathrm{GL}_2(\mathbb{F}_p)$ on $X_1(p,\mu_p)^S$. Moreover,*

- *the matrix $\begin{pmatrix} a & * \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$ preserves the component $X_1(p,\mu_p)_{(0,1)}$ and acts on it by $\underline{ad} \circ \langle d\rangle$,*
- *the matrix $aI_2 \in \mathrm{GL}_2(\mathbb{F}_p)$ acts by $\langle a\rangle'$,*
- *for $t,u \in \mathbb{F}_p$, the matrix $T^t = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$ realizes the obvious isomorphism*

$$X_1(p,\mu_p)_{(u,1)} \simeq X_1(p,\mu_p) \simeq X_1(p,\mu_p)_{(u-t,1)},$$

- *the matrix $W^{-1} := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ realizes the obvious isomorphism*

$$X_1(p,\mu_p)_{(0,1)} \simeq X_1(p,\mu_p) \simeq X_1(p,\mu_p)_{(1,0)}.$$

Now, $X_1(p,\mu_p)^S$ is a disjoint reunion of smooth relative curves, so it is a smooth relative curve, and in particular it has a relative Jacobian $P(p)$ which is naturally the product of the $J_1(p,\mu_p)$ indexed by copies of S. In particular, the action of $\mathrm{GL}_2(\mathbb{F}_p)$ (by automorphisms) on $X_1(p,\mu_p)^S$ extends by push-forward functoriality (by Proposition A.4.23) to an action on $P(p)$.

We also have a diagonal action of $\mathrm{End}(J_1(p,\mu_p))$ on $P(p)$: in particular, $\langle\cdot\rangle$, $\underline{\cdot}$, and $\mathbb{T}'$ generate a commutative subring $\mathbb{T}$ of $P(p)$, which commutes to the action of $\mathrm{GL}_2(\mathbb{F}_p)$ (since this action only permutes the coordinates and applies certain $\langle n\rangle, \underline{m}$, and these operators commute with $\mathbb{T}'$).

By Proposition A.4.23, the sum $u : J(p,p) \to P(p)$ of the push-forwards $[(u_x)_*]$ of the u_x (over $x \in S$) is well-defined.

Lemma 2.2.12 *u commutes to the action of $\mathrm{GL}_2(\mathbb{F}_p)$.*

Proof. – Let $M \in \mathrm{GL}_2(\mathbb{F}_p)$, $\lambda \in \mathbb{F}_p^\times$, and $x, x' \in S$ such that $\lambda(M^T)^{-1}x = x'$. It is enough to show that $M \circ u_x = u_{x'} \circ M$ (as morphisms $X(p,p) \to X_1(p,\mu_p)^S$) by Proposition A.4.23. It is enough to prove this away from the cuspidal points. Let S be a $\mathbb{Z}[1/p]$-scheme and $(E,P,Q) \in Y(p,p)(S)$, then one has

$$\begin{aligned} M \cdot u_x((E,P,Q)) &= M \cdot \left(\left(E, x^T \begin{pmatrix} P \\ Q \end{pmatrix} \right), \langle P,Q\rangle_E, x \right) \\ &= \left(\left(E, \lambda x^T \begin{pmatrix} P \\ Q \end{pmatrix} \right), \langle P,\ Q\rangle_E^{\det M}, x' \right) \\ &= \left(\left(E, (x')^T M \begin{pmatrix} P \\ Q \end{pmatrix} \right), \langle P,\ Q\rangle_E^{\det M}, x' \right) \\ &= u_{x'}(M \cdot (E,P,Q)). \end{aligned}$$

□

Notation for 2×2 matrices: We adopt, in the rest of the text, the following notation for 2×2 matrices.

- For $a, b \in \mathbb{F}_p^\times$, $\Delta_{a,b} \in \mathrm{GL}_2(\mathbb{F}_p)$ denotes the matrix $\mathrm{diag}(a,b)$.
- If $n \in \mathbb{Z}$ is coprime to p, $\delta_n \in SL_2(\mathbb{Z})$ is a matrix congruent to $\Delta_{n^{-1},n}$ modulo p. Sometimes, we will require additional conditions on the choice of δ_n, which we will make explicit.
- If $n \in \mathbb{F}_p^\times$, m_n is the matrix $\Delta_{n,n}$.
- $U \in \mathrm{GL}_2(\mathbb{F}_p)$ is the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and $T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.
- $W \in \mathrm{GL}_2(\mathbb{F}_p)$ is the matrix $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.
- $B \leq \mathrm{GL}_2(\mathbb{F}_p)$ is the subgroup made with upper-triangular matrices.

Notation for representations of $\mathrm{GL}_2(\mathbb{F}_p)$: Throughout the chapter, we will use the well-known classification of complex representations of $\mathrm{GL}_2(\mathbb{F}_p)$) as described in Appendix B. The irreducible complex representations of $\mathrm{GL}_2(\mathbb{F}_p)$ split in four classes:

- The abelian ones, which are all of the form $\psi(\det)$, where $\psi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ is a character.
- The principal series representations $\pi(\alpha,\beta)$ of dimension $p+1$, attached to a pair of distinct characters $\alpha, \beta : \mathbb{F}_p^\times \to \mathbb{C}^\times$.
- The twisted Steinberg representations $\mathrm{St}_\psi = \mathrm{St} \otimes \psi(\det)$ of dimension p, where $\psi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ is a character.
- The cuspidal representations of dimension $p-1$, which are exactly those such that U has no nonzero invariant vector.

For any left $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-module M, we will denote $M^\vee = \mathrm{Hom}_{\mathbb{C}}(M, \mathbb{C})$, which is a right $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-module.

We denote by $\mathcal{D}$ the group of characters $\mathbb{F}_p^\times \to \mathbb{C}^\times$.

Proposition 2.2.13 *Let $M = \begin{pmatrix} a & * \\ 0 & d \end{pmatrix} \in B$ act on $J_1(p,\mu_p)$ by $\underline{ad}\langle d \rangle$. Let V be any $\mathbb{Z}[1/p]$-scheme. There is a unique isomorphism of $\mathbb{Z}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules*

$$\mathbb{Z}[\mathrm{GL}_2(\mathbb{F}_p)] \otimes_{\mathbb{Z}[B]} J_1(p,\mu_p)(V) \to P(p)(V)$$

such that $[I_2] \times J_1(p,\mu_p)(V) \to P(p)(V)$ is simply the inclusion $J_1(p,\mu_p) = J_1(p,\mu_p)_{(0,1)} \to P(p)$ coming from the inclusion $X_1(p,\mu_p)_{(0,1)} \to X_1(p,\mu_p)^S$.

This isomorphism is functorial with respect to V and commutes with $\mathbb{T}$.

Proof. – The morphism $v_0 : J_1(p,\mu_p)(V) = J_1(p,\mu_p)_{(0,1)}(V) \to P(p)(V)$ is an morphism of $\mathbb{Z}[B]$-modules by Lemma 2.2.11, which is functorial in V. Thus it induces a morphism of $\mathbb{Z}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules $v : \mathbb{Z}[\mathrm{GL}_2(\mathbb{F}_p)] \otimes_{\mathbb{Z}[B]} J_1(p,\mu_p)(V) \to P(p)(V)$ which is functorial in V. Now,

$$\mathbb{Z}[\mathrm{GL}_2(\mathbb{F}_p)] \otimes_{\mathbb{Z}[B]} J_1(p,\mu_p)(V) \simeq \bigoplus_{M \in T^{\mathbb{F}_p} \cup \{W^{-1}\}} [M] \otimes J_1(p,\mu_p)(V),$$

and, for any $f \in J_1(p,\mu_p)(V)$, $v([M]\otimes f) = M\cdot v_0(f)$.

Let, for each $x \in S$, ι_x denote the morphism $X_1(p,\mu_p) = X_1(p,\mu_p)_x \subset X_1(p,\mu_p)^S$. Then v_0 is exactly $[(\iota_{(0,1)})_*]$.

If $M = T^t$ (resp. $M = W^{-1}$), then $M \circ [(\iota_{(0,1)})_*] = [(\iota_{(-t,1)})_*]$ (resp. it equals $[(\iota_{(1,0)})_*]$) by Lemma 2.2.11. The conclusion follows from the fact that $\prod_{x\in S}[(\iota_x)_*]J_1(p,\mu_p)^{\times S} \to P(p)$ is an isomorphism. □

Proposition 2.2.14 *For any prime $\ell \neq p$ and any $x \in S$, $[(u_x)_*]\circ T_\ell = T'_\ell \circ [(u_x)_*]$. In particular, $u\circ T_\ell = T'_\ell \circ u$.*

Remark This does *not* follow directly from Proposition 1.5.10, because, while u_x is the compactification of the morphism of moduli problems

$$U_x : \begin{pmatrix} P \\ Q \end{pmatrix} \in [\Gamma(p)]_{\mathbb{Z}[1/p]}(E/Z) \longmapsto \left(x^T \begin{pmatrix} P \\ Q \end{pmatrix}, \langle P, Q\rangle_E \right) \in [\Gamma_1(p)]_{\mathbb{Z}[1/p]} \times [\mu_p^\times](E/Z),$$

this morphism of moduli problems does not respect the level p structure.

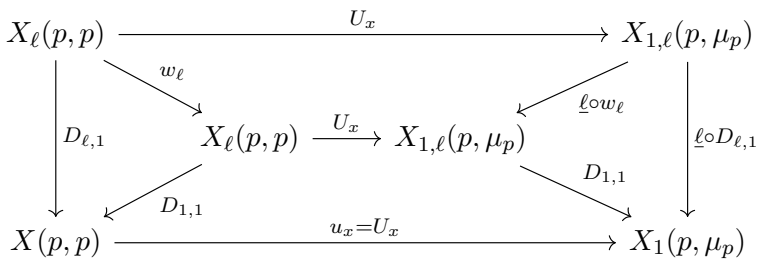
Proof. – Let $X_\ell(p,p)$ (resp. $X_{1,\ell}(p,\mu_p)$) be the compactified moduli scheme attached to the finite flat moduli problem $[\Gamma(p)]_{\mathbb{Z}[1/p]} \times [\Gamma_0(\ell)]$ (resp. $[\Gamma_1(p)]_{\mathbb{Z}[1/p]} \times [\mu_p^\times] \times [\Gamma_0(\ell)]$) over $\mathbf{Ell}_{\mathbb{Z}[1/p]}$. Both moduli problems are smooth at infinity by the results of Section 1.5 and both compactified moduli schemes are relative elliptic curves with global ring of functions $\mathbb{Z}[1/p,\mu_p]$. Consider the following diagram:

$$\begin{array}{ccc} X(p,p) & \xrightarrow{u_x = U_x} & X_1(p,\mu_p) \\ {\scriptstyle D_{1,1}}\uparrow & & {\scriptstyle D_{1,1}}\uparrow \\ X_\ell(p,p) & \xrightarrow{U_x} & X_{1,\ell}(p,\mu_p) \\ \downarrow{\scriptstyle D_{\ell,1}} & & \downarrow{\scriptstyle \underline{\ell}\circ D_{\ell,1}} \\ X(p,p) & \xrightarrow{u_x = U_x} & X_1(p,\mu_p) \end{array}$$

Note that all morphisms are morphisms of finite flat $\mathbb{P}^1_{\mathbb{Z}[1/p]}$-schemes (because all moduli problems are finite flat, so this holds away from the cusps by Corollary 1.1.14; the finiteness above the cusps is by construction, and the flatness at the cusps follows from miracle flatness). The top square is Cartesian away from the cusps, essentially by Proposition 1.1.12, and in particular it commutes (since the inclusion $Y_1(p,\mu_p) \to X_1(p,\mu_p)$ is scheme-theoretically dense).

If we can prove that the bottom square commutes and is Cartesian away from the cusps, then the result follows from Proposition A.4.25.

Consider, then, the following diagram:



All the schemes are relative curves over $\mathbb{Z}[1/p]$ with ring of global functions $\mathcal{O}(\mathbb{Z}[1/p,\mu_p])$, and all the maps (except potentially the U_x) are finite flat by Corollary 1.2.19. Since the moduli problems $[\Gamma(p)], [\Gamma_1(p)], [\mu_p^\times]$ are finite étale over $\mathbf{Ell}_{\mathbb{Z}[1/p]}$, U_x is a flat morphism of moduli problems, so that every U_x in the diagram is flat away from the cusps, and finite (since it is a

morphism of $\mathbb{P}^1_{\mathbb{Z}[1/p]}$-schemes). By miracle flatness (since all the moduli problems are smooth at infinity), it follows that every U_x is finite flat.

Thus, it is enough to show that the diagram commutes and the larger rectangle is Cartesian away from the cusps. Both triangles commute by Proposition 1.2.17. Moreover, the top trapezoid is easily checked to commute away from the cusps, hence it commutes (because we can apply Proposition A.2.9), and the bottom trapezoid is commutative and Cartesian away from the cusps, as we proved above. Moreover, the top trapezoid is automatically Cartesian since two "opposite" maps are isomorphisms, and the conclusion follows. □

Definition 2.2.16 The morphism $R : P(p) \to P(p)$ is defined as follows: for any $x, y \in S$, the map $J_1(p,\mu_p) \xrightarrow{[(\iota_x)_*]} P(p) \xrightarrow{R} P(p) \xrightarrow{\iota_y^*} J_1(p,\mu_p)$ is given by

- $-U_p$ if $x = y$,
- w_p if $x \neq y$ and $(1,0) \in \{x, y\}$,
- $\langle s-t\rangle w_p$ if $x = (s,1), y = (t,1)$ with $s, t \in \mathbb{F}_p$ distinct.

Lemma 2.2.17 *Let ℓ be a prime number. There is a dense open subscheme $U \subset \mathbb{A}^1_{\mathbb{Q}}$ such that for any elliptic curve E over a field K of characteristic 0, if $j(E) \in U$, then the $j(E/C)$ are all pairwise distinct, where C runs through the cyclic subgroups of order ℓ of $E_{\overline{K}}$.*

Proof. – Consider the moduli scheme $Y_1'(N,N)$ with $N = q\ell \geq 4$ (for some integer $q \geq 1$) attached to the moduli problem $[\Gamma_1'(N,N)]_{\mathbb{Q}}$ from Section 1.1.3. By Proposition 1.1.33, Lemma 1.3.10 and Corollary 1.5.20, $Y_1'(N,N)$ is smooth of relative dimension one, affine and integral. Consider the two morphisms $Y_1'(N,N) \to \mathbb{A}^1_{\mathbb{Q}}$ given by

$$(E,P,C) \longmapsto j(E/\langle qP\rangle),\ (E,P,C) \longmapsto j(E/C[\ell]),$$

and let $Z \subset Y_1'(N,N)$ be the closed subscheme on which these morphisms agree: then either $Z = Y_1'(N,N)$ or Z is a discrete union of finitely many closed points – so that the open subset $\mathbb{A}^1 \backslash j(Z)$ works.

All we need to do, then, is find a single elliptic curve E over some algebraically closed field K and independent points $P, Q \in E[\ell]$ such that $j(E/\langle P\rangle) \neq j(E/\langle Q\rangle)$. Let $\tau \in \mathbb{C}$ be a complex number with positive imaginary part, and consider the points $P = \frac{\tau}{\ell}, Q = \frac{1}{\ell}$ of the elliptic curve $E = \frac{\mathbb{C}}{\mathbb{Z}\tau \oplus \mathbb{Z}}$. Then the j-invariant of $E/\langle P\rangle$ is $j(\tau/\ell)$, and the j-invariant of $E/\langle Q\rangle$ is $j(\ell\tau)$. Using the q-expansion of j, it is clear that when $\tau = it$ with $t \to +\infty$, then $j(\tau/\ell) \sim e^{2\pi t/\ell}$, $j(\ell\tau) \sim e^{2\pi\ell t}$, so $j(\tau/\ell) \neq j(\ell\tau)$. □

Proposition 2.2.18 *R commutes with the action of $\mathbb{T}'[\mathrm{GL}_2(\mathbb{F}_p)]$ and $R \circ u = 0$.*

Proof. – Every entry of the matrix of R is $\mathbb{T}'$-equivariant by Lemma 2.2.7, so R commutes to $\mathbb{T}'$.

Next, we show that R commutes to T. A direct computation shows that $T \circ \iota_{(t,1)} = \iota_{(t-1,1)}$ for $t \in \mathbb{F}_p$, while $T \circ \iota_{(1,0)} = \iota_{(1,0)}$. Let $s, t \in \mathbb{F}_p$, then

$$\iota_{(t,1)}^* T \circ R \circ [(\iota_{(s,1)})_*] = (T^{-1} \circ \iota_{(t,1)})^* \circ R \circ [(\iota_{(s,1)})_*] = \iota_{(t+1,1)}^* \circ R \circ [(\iota_{(s,1)})_*],$$
$$\iota_{(t,1)}^* R \circ T \circ [(\iota_{(s,1)})_*] = \iota_{(t,1)}^* \circ R \circ [(T \circ \iota_{(s,1)})_*] = \iota_{(t,1)}^* \circ R \circ [(\iota_{(s-1,1)})_*],$$

and since, for $s, t \in \mathbb{F}_p$, $\iota_{(t,1)}^* R[(\iota_{(s,1)})_*]$ depends only from $s - t \in \mathbb{F}_p/\{\pm 1\}$, we see that $\iota_{(t,1)}^* R \circ T \circ [(\iota_{(s,1)})_*] = \iota_{(t,1)}^* T \circ R \circ [(\iota_{(s,1)})_*]$. Since, for $x \in S$, $\iota_x^* R[(\iota_{(1,0)})_*]$ and $\iota_{(1,0)}^* R[(\iota_x)_*]$ only depend on whether $x = (1,0)$, we also see that $\iota_x^* \circ (R \circ T) \circ [(\iota_{(1,0)})_*] = \iota_x^* \circ (T \circ R) \circ [(\iota_{(1,0)})_*]$.

Thus R commutes with T.

Similar computations using Lemma 2.2.5 show that R also commutes with $\Delta_{a,1}$ for $a \in \mathbb{F}_p^\times$ and W, so that R commutes with $\mathrm{GL}_2(\mathbb{F}_p)$.

Therefore, to prove that $R \circ u = 0$, it is enough to show that $\iota_{(1,0)}^* \circ R \circ u = 0$, that is, that $\sum_{t \in \mathbb{F}_p} w_p \circ [(u_{(t,1)})_*] = U_p \circ u_{(1,0)}$ (as morphisms $J(p,p) \to J_1(p,\mu_p)$). The closed subscheme

Z on which these morphisms agree is a closed subgroup scheme of $J(p,p)$, so, since $J(p,p)$ is smooth, it is enough to show that Z contains a Zariski-dense subset of $J(p,p)(\overline{\mathbb{Q}})$.

By Lemma 2.2.17, let $U \subset D(j(j-1728)) \subset \mathbb{A}^1_{\mathbb{Q}}$ be a nonempty open subscheme such that for any elliptic curve E with j-invariant in U, the j-invariants of the E/C, where C runs through cyclic subgroups of E of order p, are pairwise distinct. For some large $r \geq 1$, the points of $J(p,p)(\overline{\mathbb{Q}})$ in the image of $(j^{-1}(U) \times_{(\mu_N^\times)_{\mathbb{Q}}} j^{-1}(U))^{\times r}$ are Zariski-dense in $J(p,p)(\overline{\mathbb{Q}})$: it is thus enough to show that for any $(E,P,Q),(E',P',Q') \in j^{-1}(U)(\overline{\mathbb{Q}}) \subset Y(p,p)(\overline{\mathbb{Q}})$ such that $\langle P, Q\rangle_E = \langle P', Q'\rangle_{E'}$, $\sum_{t\in\mathbb{F}_p} w_p \circ [(u_{(t,1)})_*]$ and $U_p \circ u_{(1,0)}$ coincide on $[(E,P,Q)]-[(E',P',Q')]$.

In this case, since $[\Gamma_1'(p,p)]_{\mathbb{Q}}, [\Gamma_1(p)]_{\mathbb{Q}}$ are representable finite étale, their moduli schemes are finite étale above U, by [86, Proposition 8.6.8]. Therefore, the pull-back under $D'_{1,1}$ of any Cartier divisor $[(E,S,\alpha)]$ (resp. $[(E',S',\alpha)]$) (where S,S' are points of E,E' of exact order p) is exactly the sum over all cyclic subgroups C of E of degree p and not containing S (resp. C of E' not containing S') of the quadruples $[(E,S,C,\alpha)]$ (resp. $[(E,S,C',\alpha)]$).

Now, the cyclic subgroups of $E[p]$ (resp. $E'[p]$) not containing P (resp. P') are exactly the $tP+Q$ (resp. $tP'+Q'$) over all $t \in \mathbb{F}_p$. If $t \in \mathbb{F}_p$, then by [86, (2.8.6)], $\langle tP+Q, -P \pmod{tP+Q}\rangle_{\langle tP+Q\rangle} = \langle tP+Q, -P\rangle_{E[p]} = \alpha$. Thus, using Lemma A.4.8 (for each map), we have in $\mathrm{Div}(Y_1(p,\mu_p)_{\overline{\mathbb{Q}}})$:

$$\begin{aligned}
&\sum_{t\in\mathbb{F}_p} w_p \circ [(u_{(t,1)})_*]((E,P,Q)-(E',P',Q')) = \sum_{t\in\mathbb{F}_p} w_p((E,tP+Q,\alpha)-(E',tP+Q,\alpha))\\
&= \sum_{t\in\mathbb{F}_p} (E/\langle tP+Q\rangle, -P \pmod{tP+Q}, \alpha) - (E'/\langle tP'+Q'\rangle, -P' \pmod{tP'+Q'}, \alpha)\\
&= \sum_{t\in\mathbb{F}_p} (E/\langle tP+Q\rangle, P \pmod{tP+Q}, \alpha) - \sum_{t\in\mathbb{F}_p} (E'/\langle tP'+Q'\rangle, P' \pmod{tP'+Q'}, \alpha)\\
&= (D'_{p,1})_*(D'_{1,1})^*([(E,P,\alpha)]-[(E',P,\alpha)])\\
&= U_p \circ u_{(1,0)}([(E,P,Q)]-[(E',P',Q')]),
\end{aligned}$$

whence the conclusion.

□

2.3 Uniformizing $P(p)$

In the rest of this section, $\mathbb{H}$ denotes the complex upper half-plane, endowed with the usual action of $\mathrm{GL}_2(\mathbb{R})^+$ by homographies: $\begin{pmatrix} a & b \\ c & d\end{pmatrix}\cdot\tau = \frac{a\tau+b}{c\tau+d}$.

Given an positive integer N, $\Gamma_0(N), \Gamma_1(N), \Gamma(N)$ denotes as usual the subgroup of matrices $M \in SL_2(\mathbb{Z})$ which are respectively upper-triangular modulo N, congruent to $\begin{pmatrix} 1 & * \\ 0 & 1\end{pmatrix}$ modulo N, or congruent to I_2 modulo N.

Proposition 2.3.1 *Let $X_1(p)^{an}$ be the classical compact Riemann surface whose non-cuspidal points are given by the quotient $\Gamma_1(p)\backslash\mathbb{H}$ (see for example [41, Chapter 2]). There exists a morphism of locally ringed spaces $X_1(p)^{an}\times\mathbb{F}_p^\times\times S \to X_1(p,\mu_p)^S$ making $X_1(p)^{an}\times\mathbb{F}_p^\times\times S$ the analytification of $X_1(p,\mu_p)^S_{\mathbb{C}}$ in the sense of [68, Exp. XII, (1.1)]. Under this morphism, a point $(\tau,b,x) \in \mathbb{H}\times\mathbb{F}_p^\times\times S$ is mapped to $\left(\left(\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\mathbb{Z}}, \frac{1}{p}\right), e^{-2i\pi b/p}, x\right) \in X_1(p,\mu_p)^S(\mathbb{C})$. In particular, this uniformization preserves the j-invariant (i.e. maps the algebraic j-invariant to the analytic $j(\tau) = \frac{1}{q} + 744 + 196884q + \ldots$).*

Under this identification, a matrix $M \in \mathrm{GL}_2(\mathbb{F}_p)$ acts as follows: given $x,x' \in S$ and $\lambda \in \mathbb{F}_p^\times$

such that $\lambda(M^T)^{-1}x = x'$*, then the composition*

$$X_1(p)^{an} \times \mathbb{F}_p^\times \simeq X_1(p)^{an} \times \mathbb{F}_p^\times \times \{x\} \xrightarrow{M} X_1(p)^{an} \times \mathbb{F}_p^\times \times \{x'\} \simeq X_1(p)^{an} \times \mathbb{F}_p^\times$$

is exactly $\langle\lambda\rangle \times [\det M]$*, where* $[\det M] : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ *is the multiplication by* $\det M$*.*

Remark The reason for the minus sign comes from the uniformization that we will adopt for $X(p,p)$, and the sign convention for the Weil pairing in [86, (2.8.5.2)].

Since we will in fact need several variants of this result, we prove a generalized version of this statement. It is not a new result by any means, but we include a proof since it is not spelled out in [86] or the otherwise very thorough [136, Appendix A].

Lemma 2.3.3 *Let* $a, b, c \geq 1$ *be pairwise coprime integers with* $a \geq 3$ *or* $b \geq 4$*. Let* X^a *(resp.* X_a*) be the compact connected Riemann surface attached (see for example [41, Chapter 2]) to the congruence subgroup* $\Gamma = \Gamma(a) \cap \Gamma_1(b) \cap \Gamma_0(c)$ *(resp. the compactified moduli scheme attached to the finite étale moduli problem* $[\Gamma(a)]_{\mathbb{C}} \times [\Gamma_1(b)]_{\mathbb{C}} \times [\Gamma_0(c)]_{\mathbb{C}}$*).*

There exists a morphism of locally ringed spaces $\mathrm{An} : X^a \times (\mathbb{Z}/a\mathbb{Z})^\times \to X_a$ *such that, for any* $(\Gamma\tau, v) \in \mathbb{H}/\Gamma \times (\mathbb{Z}/a\mathbb{Z})^\times$*, one has*

$$\mathrm{An}(\Gamma\tau, v) = \left[\left(\frac{\mathbb{C}}{\tau\mathbb{Z} \oplus \mathbb{Z}}, \frac{v\tau}{a}, \frac{1}{a}, \frac{1}{b}, \langle\frac{1}{c}\rangle\right)\right].$$

Moreover, An *satisfies the universal property of an analytification in the sense of [68, Exp. XII, (1.1)], and* $j \circ \mathrm{An}$ *is exactly the modular* j*-invariant.*

Proof. – First, we know by Corollary 1.2.21 that X_a is a smooth projective scheme of dimension one over $\mathbb{C}$. Therefore, its analytification X' is (by [68, Exp. XII, (2.6), (3.1), (3.2)]) a (perhaps disconnected) compact Riemann surface.

Next, we construct a morphism of locally ringed spaces $Y^a \to Y_a$, where $Y^a = \mathbb{H}/\Gamma$ and Y_a is the moduli scheme attached to the finite étale moduli problem $[\Gamma(a)]_{\mathbb{C}} \times [\Gamma_1(b)]_{\mathbb{C}} \times [\Gamma_0(c)]_{\mathbb{C}}$.

Step 1: A "versal" elliptic curve over $\mathbb{H}$*:*

Let $R = \mathcal{O}(\mathbb{H})$ be the ring of holomorphic functions on $\mathbb{H}$. It is a Bezout domain by [51, (26.5)]. In particular, the image of the obvious morphism $\theta : \mathbb{H} \to \operatorname{Spec} R$ of locally ringed spaces is dense, and meets every nonempty closed subscheme of $\operatorname{Spec} R$ cut out by a finitely generated ideal.

Let $G_k(\tau) = \sum_{(m,n)\in\mathbb{Z}^2\setminus\{0\}} (m\tau + n)^{-k}$ for each even $k > 2$. Consider the cubic $\mathcal{E}^{an}$ over R of equation $y^2 = x^3 - 15G_4x - 35G_6$ (that is, $\mathcal{E}^{an}$ is the closed subscheme of $\mathbb{P}^2_R$ with equation $y^2z = x^3 - 15G_4xz - 35G_6z^3$). Its discriminant $\delta \in R$ is $16(4\cdot 15^3 G_4^3 - 35^2 G_6^2)$, so it is a modular form of weight 12 and level 1. The first terms in the q-expansion of δ are given by (using [41, p. 5])

$$\begin{aligned}
\delta(\tau) &= 16 \cdot 4\left(\frac{2\cdot 15\pi^4}{90} + \frac{30(2i\pi)^4}{6}q + O(q^2)\right)^3 - 16\cdot 27\left(\frac{70\pi^6}{945} + \frac{70(2i\pi)^6}{120}q + O(q^2)\right)^2 \\
&= \pi^{12}\left[64\cdot\left(\frac{1}{3} + 80q + O(q^2)\right)^3 - 16\cdot 27\left(\frac{2}{27} - \frac{7\cdot 16}{3}q + O(q^2)\right)^2\right] \\
&= \pi^{12}\left[\frac{64}{27} + \frac{64\cdot 80}{3}q + O(q^2) - \frac{64}{27} + \frac{64\cdot 7\cdot 16}{3} + O(q^2)\right] \\
&= \frac{64\pi^{12}\cdot 16(5+7)}{3}q + O(q^2) = (2\pi)^{12}q + O(q^2),
\end{aligned}$$

hence $\delta = (2\pi)^{12}\Delta$ does not vanish on $\mathbb{H}$ (where Δ is the weight 12 normalized cusp form of

level one). Hence $\mathcal{E}^{an}$ is an elliptic curve over R. Its (algebraic) j-invariant is $-1728\frac{(-60G_4)^3}{\delta} \in R$, which is, by [41, p.7], the modular j-invariant. We know that, for any $\tau \in \mathbb{H}$, by [153, Proposition VI.3.6],

$$z \in \mathbb{C}/(\tau\mathbb{Z} \oplus \mathbb{Z}) \longmapsto [z]_\tau := [\wp_{\tau\mathbb{Z}\oplus\mathbb{Z}}(z) : 2\wp'_{\tau\mathbb{Z}\oplus\mathbb{Z}}(z) : 1] \in (\mathcal{E}^{an} \times_{\operatorname{Spec} R,\tau} \operatorname{Spec} \mathbb{C})(\mathbb{C}) \subset (\mathbb{P}^2_R \times_{\operatorname{Spec} R,\tau} \operatorname{Spec} \mathbb{C})(\mathbb{C})$$

defines an isomorphism.

Let $c, d \in \mathbb{Z}$ and $N \geq 1$ be coprime integers (that is, $c\mathbb{Z} + d\mathbb{Z} + N\mathbb{Z} = \mathbb{Z}$), and $P \in \mathcal{E}^{an}(R)$ be given by $[\wp_{\tau\mathbb{Z}\oplus\mathbb{Z}}\left(\frac{c\tau+d}{N}\right) : 2\wp'_{\tau\mathbb{Z}\oplus\mathbb{Z}}\left(\frac{c\tau+d}{N}\right) : 1]$ (it is a well-defined point, because this can be checked at each $\tau \in \mathbb{H}$). For any $e \mid N$, there is a (universal) closed subscheme Z_e of $\operatorname{Spec} R$ on which $eP = 0$: it is a base change of the diagonal $\mathcal{E}^{an} \to \mathcal{E}^{an} \times_R \mathcal{E}^{an}$, which is a finitely presented closed immersion by [4, Lemma 0818]. Hence $Z_e \to \operatorname{Spec} R$ is a finitely presented closed immersion and Z_e is cut out by a finitely generated ideal. But Z_e does not meet $\theta(\mathbb{H})$ unless $e = N$, in which case $Z_e \supset \theta(\mathbb{H})$. It follows that $P \in \mathcal{E}^{an}(R)$ is a point of exact order N.

Similarly, given functions $f : \mathbb{H} \to \mathbb{C}$, $g : \mathbb{H} \to \mathbb{H}$, we write $[f(\tau)]_{g(\tau)}$ or $[f]_g$ for the point $(\tau \longmapsto [\wp_{g(\tau)\mathbb{Z}\oplus\mathbb{Z}}(f(\tau)) : 2\wp'_{g(\tau)\mathbb{Z}\oplus\mathbb{Z}}(f(\tau)) : 1]) \in \operatorname{Mor}_{\mathbb{C}}(\operatorname{Spec} R, \mathcal{E}^{an})$. When there is no index, it is assumed that g is the identity.

Let R' be the product of copies of R indexed by $(\mathbb{Z}/a\mathbb{Z})^\times$. The enriched elliptic curve

$$\epsilon = \left(\mathcal{E}^{an}_{R'}/R', \left(\left(\left[\frac{v\tau}{a}\right]\right)_{v\in(\mathbb{Z}/a\mathbb{Z})^\times}, \left[\frac{1}{a}\right]_{R'}\right), \left[\frac{1}{b}\right]_{R'}, \langle\left[\frac{1}{c}\right]_{R'}\rangle\right)$$

defines a morphism $\upsilon : \operatorname{Spec} R' \to Y_a$.

Step 2: Passing to the quotient by Γ

Now, there is a natural left action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$, which induces a natural (componentwise) action of $SL_2(\mathbb{Z})$ on $\operatorname{Spec} R'$. Let us show that υ factors through a morphism $\upsilon' : \operatorname{Spec}(R')^\Gamma \to Y_a$. Since Y_a is affine by Proposition 1.1.14, it is enough to show that ϵ is invariant under Γ.

Let $g = \begin{pmatrix} u & v \\ w & t \end{pmatrix} \in \Gamma$. Then $g \cdot \epsilon$ is the elliptic curve E over R' given by the equation

$$y^2 = x^3 - 15G_4\left(\frac{u\cdot+v}{w\cdot+t}\right)x - 35G_6\left(\frac{u\cdot+v}{w\cdot+t}\right) \Leftrightarrow y^2 = x^3 - 15(w\tau+t)^4G_4x - 35(w\tau+d)^6G_6,$$

with attached structure

$$\left(\left[z\frac{g\cdot\tau}{a}\right]_{g\cdot\tau}, \left[\frac{1}{a}\right]_{g\cdot\tau}, \left[\frac{1}{b}\right]_{g\cdot\tau}, \langle\left[\frac{1}{c}\right]_{g\cdot\tau}\rangle\right).$$

Since one can straightforwardly check that, with $(\wp, \wp_g) = (\wp_{\tau\mathbb{Z}\oplus\mathbb{Z}}, \wp_{g\cdot\tau\mathbb{Z}\oplus\mathbb{Z}})$,

$$\wp_g(z) = (w\tau+t)^2\wp((w\tau+t)z), \quad \wp'_g(z) = (w\tau+t)^3\wp((w\tau+t)z),$$

this data is equal to

$$\left(\left[(w\tau+t)^2\wp\left(z\frac{u\tau+v}{a}\right):2(w\tau+z)^3\wp'\left(z\frac{u\tau+v}{a}\right):1\right]\right)_{z\in(\mathbb{Z}/a\mathbb{Z})^\times},$$
$$\left(\left[(w\tau+t)^2\wp\left(\frac{w\tau+t}{a}\right):2(w\tau+z)^3\wp'\left(\frac{w\tau+t}{a}\right):1\right]\right)_{z\in(\mathbb{Z}/a\mathbb{Z})^\times},$$
$$\left(\left[(w\tau+t)^2\wp\left(\frac{w\tau+t}{b}\right):2(w\tau+z)^3\wp'\left(\frac{w\tau+t}{b}\right):1\right]\right)_{z\in(\mathbb{Z}/a\mathbb{Z})^\times},$$
$$\left\langle\left(\left[(w\tau+t)^2\wp\left(\frac{w\tau+t}{c}\right):2(w\tau+z)^3\wp'\left(\frac{w\tau+t}{c}\right):1\right]\right)_{z\in(\mathbb{Z}/a\mathbb{Z})^\times}\right\rangle.$$

Since $(u,v)\equiv(t,w)\equiv(1,0) \pmod a$, since $w\equiv 0 \pmod{bc}$ and $u\equiv t\equiv 1 \pmod b$, this data is equal to

$$\left(\left[(w\tau+t)^2\wp\left(z\frac{\tau}{a}\right):2(w\tau+z)^3\wp'\left(z\frac{\tau}{a}\right):1\right]\right)_{z\in(\mathbb{Z}/a\mathbb{Z})^\times},$$
$$\left(\left[(w\tau+t)^2\wp\left(\frac{1}{a}\right):2(w\tau+z)^3\wp'\left(\frac{1}{a}\right):1\right]\right)_{z\in(\mathbb{Z}/a\mathbb{Z})^\times},$$
$$\left(\left[(w\tau+t)^2\wp\left(\frac{1}{b}\right):2(w\tau+z)^3\wp'\left(\frac{1}{b}\right):1\right]\right)_{z\in(\mathbb{Z}/a\mathbb{Z})^\times},$$
$$\left\langle t\cdot\left(\left[(w\tau+t)^2\wp\left(\frac{1}{c}\right):2(w\tau+z)^3\wp'\left(\frac{1}{c}\right):1\right]\right)_{z\in(\mathbb{Z}/a\mathbb{Z})^\times}\right\rangle.$$

The map $[x:y:z]\in\mathcal{E}^{an}_{R'}\longmapsto[(w\tau+t)^2x:(w\tau+t)^3y:z]\in E'$ is an isomorphism and maps the additional data attached to ϵ to exactly the data above, so $\mathcal{E}^{an}_{R'}$ (with its level Γ structure) is isomorphic to $g^*\mathcal{E}^{an}_{R'}$. Hence υ is invariant by the action of Γ, and υ factors through a morphism $\upsilon':\mathrm{Spec}\,(R')^\Gamma\to Y_a$. Since the ring of functions of $Y^a\times(\mathbb{Z}/a\mathbb{Z})^\times\simeq\Gamma\backslash(\mathbb{H}\times(\mathbb{Z}/a\mathbb{Z})^\times)$ is exactly $(R')^\Gamma$, we get a morphism $\lambda:Y^a\times(\mathbb{Z}/a\mathbb{Z})^\times\to Y_a$ of locally ringed spaces.

Given $(\tau,v)\in\mathbb{H}\times(\mathbb{Z}/a\mathbb{Z})^\times$, $\lambda(\tau,v)$ is by construction the following elliptic curve with level Γ structure

$$y^2=x^3-15G_4(\tau)x-35G_6(\tau),\left(\left[\frac{v\tau}{a}\right]_\tau,\left[\frac{1}{a}\right]_\tau,\left[\frac{1}{b}\right]_\tau,\left\langle\left[\frac{1}{c}\right]_\tau\right\rangle\right).$$

Thus, its uniformization is $\left(\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\mathbb{Z}},\frac{v\tau}{a},\frac{1}{a},\frac{1}{b},\langle\frac{1}{c}\rangle\right)$, and in particular the j-invariant of this elliptic curve is exactly $j(\tau)$, so that $j_{alg}\circ\lambda$ is exactly the modular j-invariant.

Step 3: λ induces a bijection $Y^a\times(\mathbb{Z}/a\mathbb{Z})^\times\to Y_a(\mathbb{C})$

Let $(\tau,z),(\tau,z')\in\mathbb{H}\times(\mathbb{Z}/a\mathbb{Z})^\times$ be such that $\lambda(\tau,z)=\lambda(\tau',z')$. By analytification, there is an isomorphism of complex tori $f:\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\mathbb{Z}}\to\frac{\mathbb{C}}{\tau'\mathbb{Z}\oplus\mathbb{Z}}$ mapping $\frac{z\tau}{a}$ (resp. $\frac{1}{a}$, $\frac{1}{b}$, $\langle\frac{1}{c}\rangle$) to $\frac{z'\tau'}{a}$ (resp. $\frac{1}{a}$, $\frac{1}{b}$, $\langle\frac{1}{c}\rangle$). By [41, Proposition 1.3.2], f is of the form $q\longmapsto mq+t$ where $m,t\in\mathbb{C}$ and $m(\tau\mathbb{Z}\oplus\mathbb{Z})=\tau'\mathbb{Z}\oplus\mathbb{Z}$. Since $f(0)=0$, we can take $t=0$. Since f preserves the Weil pairing, we must have $e^{-2i\pi z/a}=e^{-2i\pi z'/a}$ by [86, (2.8.5.2)], so $z=z'$.

We know that there are $u,v,w,t\in\mathbb{Z}$ such that $\tau'=m(u\tau+v),1=m(w\tau+t)$. In particular,

$ut - vw = \pm 1$. Since $\tau' = \frac{u\tau+v}{w\tau+t} \in \mathbb{H}$, we know that $ut - vw = 1$. Therefore,

$$\begin{aligned} m\frac{z\tau}{a} \equiv \frac{z\tau'}{a} \equiv m\frac{z(u\tau+v)}{a} \pmod{m(\tau\mathbb{Z}\oplus\mathbb{Z})},\\ m\frac{1}{a} \equiv \frac{1}{a} \equiv m\frac{w\tau+t}{a} \pmod{m(\tau\mathbb{Z}\oplus\mathbb{Z})},\\ m\frac{1}{b} \equiv \frac{1}{b} \equiv m\frac{w\tau+t}{b} \pmod{m(\tau\mathbb{Z}\oplus\mathbb{Z})},\\ m\langle\frac{1}{c}\rangle \equiv \langle\frac{1}{c}\rangle \equiv m\langle\frac{w\tau+t}{c}\rangle \pmod{m(\tau\mathbb{Z}\oplus\mathbb{Z})}, \end{aligned}$$

hence $g = \begin{pmatrix} u & v \\ w & t \end{pmatrix} \in \Gamma$ and $g\tau = \tau'$. So $\lambda : Y^a \times (\mathbb{Z}/a\mathbb{Z})^\times \to Y_a(\mathbb{C})$ is injective.

Let E be an elliptic curve over $\mathbb{C}$ and (P_a, Q_a) be a basis of its a-torsion, $P_b \in E(\mathbb{C})$ have exact order b, and $C \leq E$ be a cyclic subgroup of order c. By [153, Theorem VI.5.1] there is some $\tau \in \mathbb{H}$ such that E is isomorphic to the elliptic curve F of equation $y^2 = x^3 - 15G_4(\tau)x - 35G_6(\tau)$, and we can find coefficients $u, v, w, t \in \mathbb{Z}/abc\mathbb{Z}$ such that $ut - wx = \delta \in (\mathbb{Z}/abc\mathbb{Z})^\times$ is congruent to 1 mod bc and such that under the isomorphism $E \to F$, (P_a, Q_a, P_b, C) is mapped to

$$\left(\left[\frac{u\tau+v}{a}\right]_\tau, \left[\frac{w\tau+t}{a}\right]_\tau, \left[\frac{w\tau+t}{b}\right]_\tau, \langle\left[\frac{w\tau+t}{c}\right]_\tau\rangle\right),$$

where $[z]_\tau$ denotes the point $\left[\wp_{\tau\mathbb{Z}\oplus\mathbb{Z}}(z) : 2\wp'_{\tau\mathbb{Z}\oplus\mathbb{Z}}(z) : 1\right]$ for $z \in \mathbb{C}/(\tau\mathbb{Z}\oplus\mathbb{Z})$.

In particular, let $(u_1, v_1) = \delta^{-1}(u, v)$, and pick lifts $u', v', w', t' \in \mathbb{Z}$ of u, v, w, t such that $u't' - w'v' = 1$, and let $\tau' = \frac{u'\tau+v'}{w'\tau+t'}$. Let F' be the complex elliptic curve with equation $y^2 = x^3 - 15G_4(\tau') - 35G_6(\tau')$, so that

$$\alpha : [x : y : z] \in F \mapsto [(w'\tau + t')^2 x : (w'\tau + t')^3 y : z] \in F'$$

is an isomorphism. Then one has

$$\begin{aligned} &\alpha\left(\left[\frac{u\tau+v}{a}\right]_\tau, \left[\frac{w\tau+t}{a}\right]_\tau, \left[\frac{w\tau+t}{b}\right]_\tau, \langle\left[\frac{w\tau+t}{c}\right]_\tau\rangle\right)\\ &= \left(\left[\frac{\delta\tau'}{a}\right]_{\tau'}, \left[\frac{1}{a}\right]_{\tau'}, \left[\frac{1}{b}\right]_{\tau'}, \langle\left[\frac{1}{c}\right]_{\tau'}\rangle\right), \end{aligned}$$

so that $(E, P_a, Q_a, P_b, C) \in Y_a(\mathbb{C})$ is $\lambda((\tau', \delta))$.

Step 4: The analytification of $\lambda : Y^a \times (\mathbb{Z}/a\mathbb{Z})^\times \to Y_a \subset X_a$ extends holomorphically to $X^a \times (\mathbb{Z}/a\mathbb{Z})^\times$

Let Y' be the analytification of Y_a, it is a (possibly disconnected) Riemann surface contained in X' and such that $X' \backslash Y'$ is finite. The morphism λ factors through a holomorphic morphism $\lambda' : Y^a \times (\mathbb{Z}/a\mathbb{Z})^\times \to Y'$, which is bijective by Step 3 and [68, Exp. XII, (1.1)] (hence a biholomorphism, but we will not use it). Let $\iota : Y^a \times \mathbb{Z}/a\mathbb{Z})^\times \xrightarrow{\lambda'} Y' \subset X'$. Our claim is that ι extends holomorphically to $X^a \times (\mathbb{Z}/a\mathbb{Z})^\times$.

Let $c \in (X^a \backslash Y^a) \times (\mathbb{Z}/a\mathbb{Z})^\times$, and let f be any meromorphic function on X'. Let us show that $f \circ \iota$ extends meromorphically to c. Let $\beta : D \to X^a \times (\mathbb{Z}/a\mathbb{Z})^\times$ be a biholomorphism to some open subspace of $X^a \times (\mathbb{Z}/a\mathbb{Z})^\times$, where D is the open unit disk, $\beta(D\backslash\{0\}) \subset Y^a \times (\mathbb{Z}/a\mathbb{Z})^\times$ and $\beta(0) = c$. So it is enough to check that the singularity at 0 of $f \circ \iota \circ \beta$ is not essential. If it were, by Casorati-Weierstrass (see for instance [100, Theorem V.3.2]), there would be a dense $S \subset \mathbb{C}$ such that for any $s \in S$, $(f \circ \iota \circ \beta)^{-1}(s)$ is infinite. Since ι, β are injective and f has finite fibres, and we would get a contradiction.

Hence, for any holomorphic $\phi : X' \to \mathbb{P}^1(\mathbb{C})$, $\phi \circ \iota : Y^a \times (\mathbb{Z}/a\mathbb{Z})^\times$ extends holomorphically

to $X^a \times (\mathbb{Z}/a\mathbb{Z})^\times$. By [51, 14.13], this implies that for any sequence $x_n \in Y^a \times (\mathbb{Z}/a\mathbb{Z})^\times$ converging to some point of $X^a \times (\mathbb{Z}/a\mathbb{Z})^\times$, $\iota(x_n)$ has at most one limit point. Since X' is compact, this implies that ι extends continuously. By picking charts and using Morera's theorem (see for instance [100, Theorem III.7.9], although the book does not mention the relevant corollary: a continuous function on an open subset of $\mathbb{C}$ which is holomorphic outside finitely many points is holomorphic), it is straightforward to check that the continuous extension of ι to $X^a \times (\mathbb{Z}/a\mathbb{Z})^\times$ is holomorphic.

Step 5: ι is isomorphic to the inclusion $Y^a \times (\mathbb{Z}/a\mathbb{Z})^\times \subset X^a \times (\mathbb{Z}/a\mathbb{Z})^\times$.

Since $X^a \times (\mathbb{Z}/a\mathbb{Z})^\times$ is compact, its image under ι is compact and contains a co-finite open subspace of X', so ι is surjective. Since the restriction of ι to the co-finite open subset $Y^a \times (\mathbb{Z}/a\mathbb{Z})^\times$ is injective (by Step 3 and [68, Exp. XII, (1.1)]), the degree of ι with respect to any connected component of X' ([51, 4.24]) is one. Hence ι is an isomorphism.

□

Corollary 2.3.4 *This identification induces an isomorphism of right $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules*

$$\iota_{1,p} : H^0(X_1(p,\mu_p)^S_{\mathbb{C}}, \Omega^1) \to (\mathcal{S}_2(\Gamma_1(p)) \otimes \mathbb{C}[\mathbb{F}_p^\times]) \otimes_{\mathbb{Z}[B]} \mathbb{Z}[\mathrm{GL}_2(\mathbb{F}_p)]$$

such that:

- $\begin{pmatrix} a & * \\ 0 & d \end{pmatrix} \in B$ *acts on* $\mathcal{S}_2(\Gamma_1(p)) \otimes \mathbb{C}[\mathbb{F}_p^\times]$ *by* $\langle d\rangle \otimes [ad]$, *where* $[ad] : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ *is the multiplication by* ad.
- *If* $t \in \mathbb{F}_p$, $M = T^t$ *and* $x = (t,1)$ *(resp.* $M = W$ *and* $x = (1,0)$*), then, for all* $f \in \mathcal{S}_2(\Gamma_1(p)), b \in \mathbb{F}_p^\times$, $\iota_{1,p}^{-1}(f \otimes [b] \otimes M)$ *is the holomorphic differential on* $X_1(p)^{an} \times \mathbb{F}_p^\times \times S$ *which is equal to* $f(\tau)d\tau$ *on the component* (b^{-1}, x) *and zero on the other components.*

Proof. – The uniformization of Proposition 2.3.1 yields by [68, Exp. XII, Corollaire 4.3] an isomorphism of right $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules

$$\iota : H^0(X_1(p,\mu_p)^S_{\mathbb{C}}, \Omega^1) \to \bigoplus_{(b,x)\in\mathbb{F}_p^\times \times S} \mathcal{S}_2(\Gamma_1(p)) \otimes [(b,x)].$$

So all we need to do is construct a $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-isomorphism

$$j : \bigoplus_{(b,x)\in\mathbb{F}_p^\times \times S} \mathcal{S}_2(\Gamma_1(p)) \otimes [(b,x)] \to (\mathcal{S}_2(\Gamma_1(p)) \otimes \mathbb{C}[\mathbb{F}_p^\times]) \otimes_{\mathbb{Z}[B]} \mathbb{Z}[\mathrm{GL}_2(\mathbb{F}_p)]$$

with the correct compatibilities.

Let $x, x' \in S$ and $M \in \mathrm{GL}_2(\mathbb{F}_p)$, then write $\lambda(M^T)^{-1}x = x'$ for some $\lambda \in \mathbb{F}_p^\times$. Then we know that, given a differential $\omega = f(\tau)d\tau$ with support on the component (b,x') of $X_1(p) \times \mathbb{F}_p^\times \times S$, $M^*\omega = (\langle\lambda\rangle)^*(f(\tau)d\tau)$ and has support on the component $(b(\det M)^{-1}, x)$. In other words, we know that $M^*(f \cdot [(b,x')]) = ((\langle\lambda\rangle)^* f) \cdot [(b(\det M)^{-1}, x)]$.

Let us define j by

$$f \cdot (b,(t,1)) \longmapsto f \otimes [b^{-1}] \otimes [T^t], \quad f \cdot (b,(1,0)) \longmapsto [b^{-1}] \otimes [W].$$

Then the second condition is satisfied for $\iota_{1,p} := j \circ \iota$ and $\iota_{1,p}$ is clearly a $\mathbb{C}$-linear isomorphism. It remains to show that the first condition is satisfied and that $\iota_{1,p}$ is a morphism of $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules.

Let $M = \begin{pmatrix} a & * \\ 0 & d \end{pmatrix} \in B$ and $\omega \in H^0(X_1(p,\mu_p)^S_{\mathbb{C}}, \Omega^1)$ be such that its support is contained in the component $(b^{-1},(0,1))$. Since $d(M^T)^{-1}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, the support of the differential

$M^*\omega = (\underline{ad})^*\langle d\rangle^*\omega$ is contained in the component $((abd)^{-1},(0,1))$. Let $\iota_{1,p}(\omega) = f\cdot[(b,(0,1))]$, then one has $\iota_{1,p}(M^*\omega) = (\langle\lambda\rangle)^*f\cdot[(abd,(0,1))]$.

Finally, we need to show that $\iota_{1,p}$ is a morphism of right $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules.

Let $f\in\mathcal{S}_2(\Gamma_1(p)), b\in\mathbb{F}_p^\times$, $x=(t,1)$ and $M=T^t$ (resp. $x=(1,0)$ and $M=W$), and $N\in\mathrm{GL}_2(\mathbb{F}_p)$. Let ω be the differential equal to $f(\tau)d\tau$ on the component (b^{-1},x). Then $N^*\omega$ is the differential $(\langle\lambda\rangle^*f)(\tau)d\tau$ on the component $(b^{-1}(\det N)^{-1},x')$ where $\lambda(N^T)^{-1}x'=x$, that is, $\lambda x'=N^Tx$. Thus $\iota_{1,p}(\omega)=f\otimes[b]\otimes M$, while $\iota_{1,p}(N^*\omega)=(\langle\lambda\rangle^*f)\otimes[b\det N]\otimes N'$, where N' is T^s (resp. W) if $x'=(s,1)$ (resp. $(1,0)$).

Since $\lambda L_2(N')=\lambda x'=N^Tx=C_2(N^TM^T)=L_2(MN)$, we can write $MN=\begin{pmatrix}a&*\\0&\lambda\end{pmatrix}N'$ where $a\lambda=a\lambda\det N'=\det M\det N=\det N$.

Thus

$$\begin{aligned}\iota_{1,p}(\omega)\mid N=(f\otimes[b])\otimes[MN]&=\left((f\otimes[b])\mid\begin{pmatrix}\lambda^{-1}\det N&*\\0&\lambda\end{pmatrix}\right)\otimes[N']\\&=(\langle\lambda\rangle^*f\otimes[\det Nb])\,,\end{aligned}$$

whence the conclusion.

□

Proposition 2.3.5 *Let $\mathcal{S}_2(\Gamma_1(p),\mathbb{F}_p^\times,S)$ denote $(\mathcal{S}_2(\Gamma_1(p))\otimes\mathbb{C}[\mathbb{F}_p^\times])\otimes_{\mathbb{Z}[B]}\mathbb{Z}[\mathrm{GL}_2(\mathbb{F}_p)]$ for the sake of easier notation. Let $\ell\neq p$ be a prime number and $n\in\mathbb{F}_p^\times$. Then the following diagrams commute:*

$$\begin{array}{ccc}H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)&\xrightarrow{\iota_{1,p}}&\mathcal{S}_2(\Gamma_1(p),\mathbb{F}_p^\times,S)\\\downarrow{\scriptstyle T_\ell^*}&&\downarrow{\scriptstyle (T_\ell\otimes\mathrm{id})\otimes\mathrm{id}}\\H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)&\xrightarrow{\iota_{1,p}}&\mathcal{S}_2(\Gamma_1(p),\mathbb{F}_p^\times,S)\end{array}$$

$$\begin{array}{ccc}H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)&\xrightarrow{\iota_{1,p}}&\mathcal{S}_2(\Gamma_1(p),\mathbb{F}_p^\times,S)\\\downarrow{\scriptstyle \langle n\rangle^*}&&\downarrow{\scriptstyle (\langle n\rangle\otimes\mathrm{id})\otimes\mathrm{id}}\\H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)&\xrightarrow{\iota_{1,p}}&\mathcal{S}_2(\Gamma_1(p),\mathbb{F}_p^\times,S)\end{array}\qquad\begin{array}{ccc}H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)&\xrightarrow{\iota_{1,p}}&\mathcal{S}_2(\Gamma_1(p),\mathbb{F}_p^\times,S)\\\downarrow{\scriptstyle \underline{n}^*}&&\downarrow{\scriptstyle (\mathrm{id}\otimes\underline{n})\otimes\mathrm{id}}\\H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)&\xrightarrow{\iota_{1,p}}&\mathcal{S}_2(\Gamma_1(p),\mathbb{F}_p^\times,S)\end{array}$$

In each case, the Hecke operators on the right hand side are those defined analytically, with the convention of [41, Chapter 5.2].

Proof. – Since all arrows are morphisms of right $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules, it is enough to prove the claim when replacing all the diagrams by

$$\begin{array}{ccc}H^0(X_1(p,\mu_p)_{\mathbb{C}},\Omega^1)&\xrightarrow{\iota_{1,p}}&\mathcal{S}_2(\Gamma_1(p))\otimes\mathbb{C}[\mathbb{F}_p^\times]\\\downarrow&&\downarrow\\H^0(X_1(p,\mu_p)_{\mathbb{C}},\Omega^1)&\xrightarrow{\iota_{1,p}}&\mathcal{S}_2(\Gamma_1(p))\otimes\mathbb{C}[\mathbb{F}_p^\times]\end{array}$$

For $\underline{n}$, the statements are straightforward from the construction of $\iota_{1,p}$.

For $\langle n\rangle$, the statement is a direct consequence of the fact that the following diagram commutes:

$$\begin{array}{ccc}(\Gamma_1(p)\backslash\mathbb{H})\times\mathbb{F}_p^\times&\xrightarrow{\Gamma_1(p)\tau\mapsto\Delta_{n^{-1},n}\Gamma_1(p)\tau}&(\Gamma_1(p)\backslash\mathbb{H})\times\mathbb{F}_p^\times\\\downarrow&&\downarrow\\X_1(p,\mu_p)&\xrightarrow{\langle n\rangle}&X_1(p,\mu_p)\end{array}$$

Now, we only discuss Hecke operators. Let $\ell \neq p$ be a prime and $\omega \in H^0(X_1(p,\mu_p)_{\mathbb{C}}, \Omega^1)$ which is nonzero only on the component b^{-1} (for $b \in \mathbb{F}_p^\times$), and is equal to $f(\tau)d\tau$ on this component, for some $f \in \mathcal{S}_2(\Gamma_1(p))$: thus $\iota_{1,p}(\omega) = f \otimes [b]$.

Then $T_\ell^*\omega = (D_{1,1}^*)^*((D_{\ell,1})_*)^*\omega$. Now, by Lemma 2.3.3 (and Lemma 1.2.9), $X_1(p,\mu_p,\Gamma_0(\ell))$ can be uniformized as $[((\Gamma_1(p)\cap\Gamma_0(\ell))\backslash\mathbb{H}^*]\times\mathbb{F}_p^\times$, by mapping (τ,z) to $\left(\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\mathbb{Z}}, \frac{1}{p}, \langle\frac{1}{\ell}\rangle, e^{-2i\pi z/p}\right)$,

and the following diagram commutes:

$$\begin{array}{ccccc} \mathbb{H}\times\mathbb{F}_p^\times & \xleftarrow[M]{} & \mathbb{H}\times\mathbb{F}_p^\times & \xrightarrow{N} & \mathbb{H}\times\mathbb{F}_p^\times \\ \downarrow & & \downarrow & & \downarrow \\ X_1(p,\mu_p) & \xleftarrow[D_{\ell,1}]{} & X_1(p,\mu_p,\Gamma_0(\ell)) & \xrightarrow{D_{1,1}} & X_1(p,\mu_p) \end{array}$$

where $M(\tau,z) = (\delta_\ell\cdot(\ell\tau), z)$, where $\delta_\ell \in \Gamma(\ell)$ is any matrix whose reduction mod p is $\Delta_{\ell^{-1},\ell}$, and $N(\tau,z) = (\tau,z)$. Hence the pull-back of $\omega' = D_{\ell,1}^*\omega$ to (the middle) $\mathbb{H}\times\mathbb{F}_p^\times$ is $\ell(f \mid \delta_\ell)(\ell\tau)d\tau$ on the component b^{-1} and 0 on the other components.

To compute $(D_{1,1}^*)^*\omega'$, we consider the following commutative diagram, where v, v' are uniformizations:

$$\begin{array}{ccccc} \mathbb{H}\times\mathbb{F}_p^\times & \xrightarrow{(g_v)_v} & \coprod_{v\in\mathbb{P}^1(\mathbb{F}_\ell)} \mathbb{H}\times\mathbb{F}_p^\times & \xrightarrow{N} & \mathbb{H}\times\mathbb{F}_p^\times \\ & \searrow^{v'} & \downarrow{\scriptstyle(\pi_v)_v} & & \downarrow{\scriptstyle v} \\ & & X_1(p,\mu_p,\Gamma_0(\ell)) & \xrightarrow{D_{1,1}} & X_1(p,\mu_p) \end{array}$$

Given $v = [c:d] \in \mathbb{P}^1(\mathbb{F}_\ell)$, π_v is the map $\tau \longmapsto \left(\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\mathbb{Z}}, \frac{1}{p}, \langle\frac{c\tau+d}{\ell}\rangle\right)$. Pick, for each $v = [c:d] \in \mathbb{P}^1(\mathbb{F}_p)$, a matrix $M_v \in \Gamma_1(p)$ such that $M_v \equiv \begin{pmatrix} * & * \\ c & d\end{pmatrix} \pmod{\ell}$. Then define π_v, g_v as M_v, M_v^{-1} respectively. By Lemma 2.2.17, the above diagram is Cartesian above a certain co-finite open subscheme U of $X_1(p,\mu_p)$.

Let $D_\ell = \begin{pmatrix}\ell & 0\\ 0 & 1\end{pmatrix}, D'_\ell = \begin{pmatrix}1 & 0\\ 0 & \ell\end{pmatrix} \in \mathcal{M}_2(\mathbb{Z})$. Then, on the component b^{-1} of $v^{-1}(U)$, one has

$$\begin{aligned} v^*(T_\ell^*\omega) = v^*(D_{1,1}^*)^*\omega' &= \sum_{v\in\mathbb{P}^1(\mathbb{F}_\ell)} (g_v^{-1})^*(\ell f \mid \delta_\ell)(\ell\tau)d\tau) \\ &= \sum_{v\in\mathbb{P}^1(\mathbb{F}_\ell)} (f \mid \delta_\ell D_\ell M_v)(\tau)d\tau = \sum_{M\in(\Gamma_0(\ell)\cap\Gamma_1(p))\backslash\Gamma_1(p)} (f \mid \delta_\ell D_\ell)(\tau)d\tau \end{aligned}$$

Here, we always consider the weight two action of $\mathrm{GL}_2(\mathbb{R})^+$, that is,

$$\left(f \mid \begin{pmatrix} a & b\\ c & d\end{pmatrix}\right)(\tau) = \frac{ad-bc}{(c\tau+d)^2} f\left(\frac{a\tau+b}{c\tau+d}\right),$$

so that scalar matrices act trivially. Now, let us show that

$$M \in (\Gamma_0(\ell)\cap\Gamma_1(p))\backslash\Gamma_1(p) \longmapsto \delta_\ell D_\ell M \in \Gamma_1(p)\backslash\Gamma_1(p)D'_\ell\Gamma_1(p)$$

is a bijection.

Let $M \in \Gamma_1(p)$ and $M' = \delta_\ell D_\ell M$. Then, by [150, Lemma 3.29], $M' \in \Gamma_1(p)D'_\ell\Gamma_1(p)$ as long as the following conditions are satisfied: the reductions in $\mathcal{M}_2(\mathbb{F}_p)$ of $D'_\ell\Gamma_1(p)$ and $\Gamma_1(p)D'_\ell$ are equal and contain $M' \pmod p$, and $M' \in \Gamma(1)D'_\ell\Gamma(1)$.

Since $\Gamma(1)D'_\ell\Gamma(1)$ is the set of matrices with integral entries and determinant ℓ, it contains M'. One easily checks that the reduction mod p of $D'_\ell\Gamma_1(p)$ and that of $\Gamma_1(p)D'_\ell$ is exactly

$\begin{pmatrix}1 & * \\ 0 & \ell\end{pmatrix}$, and that $M' \equiv \Delta_{1,\ell} M \equiv \begin{pmatrix}1 & * \\ 0 & \ell\end{pmatrix} \pmod p$. Thus $M' \in \Gamma_1(p) D'_\ell \Gamma_1(p)$.

Now, let $M, M' \in \Gamma_1(p)$. Then

$$\begin{aligned}\delta_\ell D_\ell M \in \Gamma_1(p)\delta_\ell D_\ell M' &\Leftrightarrow M(M')^{-1} \in D_\ell^{-1}\delta_\ell^{-1}\Gamma_1(p)\delta_\ell D_\ell \\ &\Leftrightarrow M(M')^{-1} \in D_\ell^{-1}\Gamma_1(p) D_\ell \cap \Gamma_1(p) \\ &\Leftrightarrow M(M')^{-1} \in \Gamma_1(p) \cap \Gamma_0(\ell) \Leftrightarrow M \in (\Gamma_1(p) \cap \Gamma_0(\ell)) M',\end{aligned}$$

and we are done.

Now, $\upsilon^*(T_\ell^* \omega)$ and $(T_\ell f)(\tau) d\tau$ are holomorphic differentials on $\mathbb{H} \times \mathbb{F}_p^\times$ and they agree except at points contained in finitely many (discrete) $SL_2(\mathbb{Z})$-orbits. Hence they are agree, whence the conclusion. □

Corollary 2.3.6 *Given a normalized newform $f \in \mathcal{S}_2(\Gamma_1(p))$ with character χ, $\psi \in \mathcal{D}$ and $M \in \{T^t \mid t \in \mathbb{F}_p\} \cup \{W\}$, let*

$$u_{f,\psi,M} = \iota_{1,p}^{-1}\left(f \otimes \left(\sum_{t \in \mathbb{F}_p^\times} \psi^{-1}(t)[t]\right) \otimes M\right) \in H^0(X_1(p,\mu_p)^S_{\mathbb{C}}, \Omega^1).$$

Then the $u_{f,\psi,M}$ form a basis of $H^0(X_1(p,\mu_p)^S_{\mathbb{C}}, \Omega^1)$. Moreover, every $u_{f,\psi,M}$ is an eigenvector for the action of $\mathbb{T}$. For a prime $\ell \neq p$, and $n \in \mathbb{F}_p^\times$, one has

$$T_\ell^* u_{f,\psi,M} = a_\ell(f) f, \quad \langle n \rangle^* u_{f,\psi,M} = \chi(n) f, \quad \underline{n}^* u_{f,\psi,M} = \psi(n) f.$$

Proof. – By Proposition 2.3.5, it is a direct verification that

$$T_\ell^* u_{f,\psi,M} = a_\ell(f) f, \underline{n}^* u_{f,\psi,M} = \psi(n), \langle n \rangle^* u_{f,\psi,M} = \chi(n) u_{f,\psi,M}.$$

We show that the $\iota_{1,p}(u_{f,\psi,M})$ form a basis of $(\mathcal{S}_2(\Gamma_1(p)) \otimes \mathbb{C}[\mathbb{F}_p^\times]) \otimes_{\mathbb{Z}[B]} \mathbb{Z}[\mathrm{GL}_2(\mathbb{F}_p)]$, which implies the conclusion. It is enough to prove that the $f \otimes \sum_{t \in \mathbb{F}_p^\times} \psi^{-1}(t)[t]$, where $f \in \mathcal{S}_2(\Gamma_1(p))$ runs through normalized newforms and ψ through elements of $\mathcal{D}$, form a basis of $\mathcal{S}_2(\Gamma_1(p)) \otimes \mathbb{C}[\mathbb{F}_p^\times]$.

The normalized newforms of $\mathcal{S}_2(\Gamma_1(p))$ form a basis by [41, Theorem 5.8.2], since the only cusp form of weight 2 and level 1 is null. Hence, we only need to check that the $e_\psi = \sum_{t \in \mathbb{F}_p^\times} \psi^{-1}(t)[t]$ form a basis of $\mathbb{C}[\mathbb{F}_p^\times]$. There are $p - 1 = \dim_{\mathbb{C}} \mathbb{C}[\mathbb{F}_p^\times]$ of them, so we only need to prove that the e_ψ are linearly independent.

Let $g \in \mathbb{F}_p^\times$ be a generator, then $\underline{g}(e_\psi) = \psi(g) e_\psi$ is an eigenvector for the multiplication by g with eigenvalue $\psi(g)$. Since ψ is a generator, $\psi(g)$ determines ψ, hence the e_ψ are linearly independent. □

Lemma 2.3.7 *Let $f \in \mathcal{S}_2(\Gamma_1(p))$ be a normalized newform with character χ. Then the twists of f by primitive Dirichlet characters are pairwise distinct, and the only primitive Dirichlet characters ψ such that $f \otimes \psi$ has conductor p are $1, \chi^{-1}$.*

Proof. – Let $\psi \neq 1$ be a primitive Dirichlet character such that $f \otimes \psi$ has conductor p. By Corollary C.3.10, ψ must have conductor p, and $\psi\chi, \psi$ must have distinct conductors. This implies that $\chi \neq 1$ and $\psi = \chi^{-1}$. If furthermore $f \otimes \psi = f$, then by comparing characters we see that $\chi = \chi^{-1}$, so that χ is a quadratic character. Since $\chi(-1) = 1$, χ is the character of a real quadratic field and f has real multiplication, which contradicts [132, Theorem 4.5]. □

Definition 2.3.8 Given a normalized newform $f \in \mathcal{S}_2(\Gamma_1(p))$ with character χ and $\psi \in \mathcal{D}$, $H^0(X_1(p,\mu_p)^S_{\mathbb{C}}, \Omega^1)[f,\psi]$ denotes the subspace of $H^0(X_1(p,\mu_p)^S_{\mathbb{C}}, \Omega^1)$ on which every T'_ℓ acts by $a_\ell(f)\psi(\ell)$, and every $\langle n \rangle'$ acts by $\chi(n)\psi(n)^2$ (where $\ell \neq p$ is prime and $n \in \mathbb{F}_p^\times$).

Lemma 2.3.9 *With the same notation, for any integer $n \geq 1$ prime to p, $T'_n - a_n(f)\psi(n)$ annihilates $H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)[f,\psi]$.*

Proof. – This is a direct induction using the classical relations between the Fourier coefficients of a newform (see for instance [41, Proposition 5.8.5]). □

Proposition 2.3.10 *Each $H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)[f,\psi]$ as in Definition 2.3.8 is stable under $\mathbb{T}$, w_p^*, R^* and $\mathrm{GL}_2(\mathbb{F}_p)$. Moreover, $H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)$ is the direct sum of the $H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)[f,\psi]$, where we sum over the couples (f,ψ) as in Definition 2.3.8, and only count exactly one couple among each pair $\{(f,\psi),(\overline{f},\chi\psi)\}$.*

Finally, we have the following isomorphisms of right $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules. If $\chi = 1$,

$$[I_2] \in \pi^\vee(\psi,\psi) \longmapsto \iota_{1,p}^{-1}\left(f \otimes \left(\sum_{t\in\mathbb{F}_p^\times} \psi^{-1}(t)[t]\right) \otimes [I_2]\right) \in H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)[f,\psi]$$

If $\chi \neq 1$,

$$\begin{aligned}\pi^\vee(\psi,\chi\psi)\oplus\pi^\vee(\chi\psi,\psi) &\to H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)[f,\psi],\\ ([I_2],0) &\longmapsto \iota_{1,p}^{-1}\left(f \otimes \left(\sum_{t\in\mathbb{F}_p^\times} \psi^{-1}(t)[t]\right) \otimes [I_2]\right)\\ (0,[I_2]) &\longmapsto \iota_{1,p}^{-1}\left(\overline{f} \otimes \left(\sum_{t\in\mathbb{F}_p^\times} (\chi\psi)^{-1}(t)[t]\right) \otimes [I_2]\right).\end{aligned}$$

Proof. – The stability properties come from the fact that w_p, R and the actions of $\mathbb{T}$ and $\mathrm{GL}_2(\mathbb{F}_p)$ commute with $\mathbb{T}'$. Moreover, the $u_{f,\psi,M}$ from Corollary 2.3.6 form a basis of $H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)$ made with eigenvectors for the action of $\mathbb{T}' \subset \mathbb{T}$. So, as a $\mathbb{C}[\mathbb{T}']$-module, $H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)$ is the direct sum of its eigenspaces.

By Corollary 2.3.6, the eigenspaces are always of the following form: the eigenvalue of T'_ℓ is $a_\ell(f)\psi(\ell)$, and that of $\langle n\rangle'$ is $\chi(n)\psi(n)^2$, where $f \in \mathcal{S}_2(\Gamma_1(p))$ is a normalized newform of character χ and $\psi \in \mathcal{D}$.

Let $f, f' \in \mathcal{S}_2(\Gamma_1(p))$ be normalized newforms with characters χ,χ', and $\psi,\psi' \in \mathcal{D}$, such that the eigenspaces of $H^0(X_1(p,\mu_p)^{\mathbb{C}}_S,\Omega^1)$ attached to (f,ψ) and (f',ψ') are the same. Then for every prime $\ell \neq p$, one has $a_\ell(f)\psi(\ell) = a_\ell(f')\psi'(\ell)$ and for every $n \in \mathbb{F}_p^\times$, one has $\chi(n)\psi(n)^2 = \chi'(n)\psi'(n)^2$. By strong multiplicity one [121, Theorem 4.6.19], the newforms $f\otimes\psi$ and $f'\otimes\psi'$ (see Proposition C.2.2) are thus equal, so f' must be the newform $f\otimes\overline{\psi'}\psi$. By Lemma 2.3.7, this implies that $\psi' = \psi$ (thus $(f,\psi) = (f',\psi')$) or $\psi = \overline{\chi}\psi'$ (so that $(f',\psi') = (\overline{f},\chi\psi)$).

Conversely, if $(f',\psi') \in \{(f,\psi),(\overline{f},\chi\psi)\}$ where $f \in \mathcal{S}_2(\Gamma_1(p))$ is a normalized newform and $\psi \in \mathcal{D}$, then

$$H^0(X_1(p,\mu_p)^{\mathbb{C}}_S,\Omega^1)[f,\psi] = H^0(X_1(p,\mu_p)^{\mathbb{C}}_S,\Omega^1)[f',\psi'].$$

Therefore,

$$H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1) = \bigoplus_{(f,\psi)} H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)[f,\psi],$$

where f runs through normalized newforms in $\mathcal{S}_2(\Gamma_1(p))$, ψ runs through elements of $\mathcal{D}$ and we count exactly one couple among each pair $\{(f,\psi),(\overline{f},\chi\psi)\}$ when f has character $\chi \neq 1$.

Let (f,ψ) be as in Definition 2.3.8, and let χ be the character of f. By what we proved above and Corollary 2.3.6, a basis of $H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)[f,\psi]$ is given by the $u_{f,\psi,M}$ if $\chi = 1$, and the $u_{f,\psi,M}, u_{\overline{f},\chi\psi,M}$ otherwise, where M runs through $\{T^t,\, t \in \mathbb{F}_p\} \cup \{W\}$. Thus, when $\chi = 1$,

$\iota_{1,p}(H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)) = \mathbb{C}f \otimes \sum_{t\in\mathbb{F}_p^\times} \psi^{-1}(t)[t] \otimes_{\mathbb{C}[B]} \mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$, where $\begin{pmatrix} a & * \\ 0 & b \end{pmatrix}$ acts (on the right) on $f \otimes \sum_{t\in\mathbb{F}_p^\times} \psi^{-1}(t)[t]$ by multiplication by $\psi(ab) = \psi(a)\psi(b)$. In this case,

$$[I_2] \in \pi^\vee(\psi,\psi) \longmapsto \iota_{1,p}^{-1}\left(f \otimes \left(\sum_{t\in\mathbb{F}_p^\times} \psi^{-1}(t)[t]\right) \otimes [I_2]\right) \in H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)[f,\psi]$$

is therefore an isomorphism.

When $\chi \neq 1$, $\iota_{1,p}(H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1))[f,\psi]$ is equal to

$$\left(\mathbb{C}\left[f \otimes \sum_{t\in\mathbb{F}_p^\times} \psi^{-1}(t)[t]\right] \oplus \mathbb{C}\left[\overline{f} \otimes \sum_{t\in\mathbb{F}_p^\times} (\chi\psi)^{-1}(t)[t]\right]\right) \otimes_{\mathbb{C}[B]} \mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)],$$

and, given $M = \begin{pmatrix} a & * \\ 0 & b \end{pmatrix}$, one has

$$\left(f \otimes \sum_{t\in\mathbb{F}_p^\times} \psi^{-1}(t)[t]\right) \mid M = \psi(a)(\chi\psi)(b)\left(f \otimes \sum_{t\in\mathbb{F}_p^\times} \psi^{-1}(t)[t]\right),$$

$$\left(\overline{f} \otimes \sum_{t\in\mathbb{F}_p^\times} (\psi\chi)^{-1}(t)[t]\right) \mid M = (\chi\psi)(a)\psi(b)\left(\overline{f} \otimes \sum_{t\in\mathbb{F}_p^\times} (\psi\chi)^{-1}(t)[t]\right),$$

whence the conclusion. □

Lemma 2.3.11 *Let (f,ψ) be as in Definition 2.3.8. Then $H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)[f,\psi]$ is not contained in the kernel of R^*.*

Proof. – Let $\omega' = u_{f,\psi,I_2} \in H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)[f,\psi] \simeq H^0(P(p)_{\mathbb{C}},\Omega^1)[f,\psi]$, and ω its (nonzero) restriction to the closed open subscheme $X_1(p,\mu_p)_{(0,1)}$. Then, if χ denotes the character of f, for any $t \in \mathbb{F}_p$,

$$\iota_{(t,1)}^* R^*(\iota_{(0,1)})_*\omega = (\iota_{(0,1)})^* R[(\iota_{(t,1)})_*]\omega = (\langle t\rangle w_p)^*\omega = \chi(t)w_p^*\omega \neq 0,$$

hence $R^*\omega' \neq 0$, and the conclusion follows. □

2.4 Uniformizing $X(p,p)$

Proposition 2.4.1 *Let $X(p)$ be the classical compact connected Riemann surface whose non-cuspidal points are given by the quotient $\Gamma(p)\backslash\mathbb{H}$ (see for example [41, Chapter 2]). There exists a morphism of locally ringed spaces $X(p) \times \mathbb{F}_p^\times \to X(p,p)_{\mathbb{C}}$, making it the analytification of $X(p,p)_{\mathbb{C}}$ in the sense of [68, Exp. XII, (1.1)]. Under this morphism, a point $(\tau,b) \in \mathbb{H} \times \mathbb{F}_p^\times$ is mapped to the enriched elliptic curve $\left(\frac{\mathbb{C}}{\mathbb{Z}\tau\oplus\mathbb{Z}}, \frac{b\tau}{p}, \frac{1}{p}\right) \in Y(p,p)(\mathbb{C})$.*

This uniformization induces the following action of $\mathrm{GL}_2(\mathbb{F}_p)$ on $X(p)\times\mathbb{F}_p^\times$: for $M \in \mathrm{GL}_2(\mathbb{F}_p)$, $(x,b) \in X(p) \times \mathbb{F}_p^\times$, let $M' = \Delta^{-1}_{b\det M,1} M \Delta_{b,1} \in \mathrm{SL}_2(\mathbb{F}_p)$, then $M \cdot (x,b) = (M' \cdot x, b(\det M)x)$.

Proof. – This is a direct consequence of Lemma 2.3.3. □

Corollary 2.4.2 *This identification induces an isomorphism*

$$\iota_{p,p} : H^0(X(p,p)_{\mathbb{C}},\Omega^1) \to \bigoplus_{b\in\mathbb{F}_p^\times} \mathcal{S}_2(\Gamma(p)) \otimes \Delta_{b,1},$$

where, given $b \in \mathbb{F}_p^\times$ and $f \in \mathcal{S}_2(\Gamma(p))$, $f(\tau)d\tau$ identifies to a holomorphic differential on $X(p)$ (which we will also denote $f(\tau)d\tau$ or f), and $f \otimes \Delta_{b,1}$ denotes the differential equal to $f(\tau)d\tau$ on $X(p) \times \{b^{-1}\}$, and vanishing on the other components.

In particular, for any $M \in \mathrm{GL}_2(\mathbb{F}_p), b \in \mathbb{F}_p^\times, f \in \mathcal{S}_2(\Gamma(p))$, one has

$$M^*(\iota_{p,p}^{-1}(f \otimes \Delta_{b,1})) = \iota_{p,p}^{-1}((f \mid_2 M') \otimes \Delta_{b \det M,1}),$$

where $M' = \Delta_{b,1} M \Delta_{b \det M,1}^{-1} \in \mathrm{SL}_2(\mathbb{F}_p)$.

Proof. – The analytification of $M^*\iota_{p,p}^{-1}(f \otimes \Delta_{b,1})$ is the differential on $X(p) \times \mathbb{F}_p^\times$ given by $M^*(f(\tau)\mathbf{1}_{z=b^{-1}}d\tau)$ for $(\tau, z) \in \mathbb{H} \times \mathbb{F}_p^\times$. Then

$$\begin{aligned} M^*(f(\tau)\mathbf{1}_{z=b^{-1}}d\tau)(\tau,z) &= f(\Delta_{z \det M,1}^{-1} M \Delta_{z,1}\tau)\mathbf{1}_{z \det M = b^{-1}} d(\Delta_{z \det M,1}^{-1} M \Delta_{z,1}\tau) \\ &= (f \mid \Delta_{(b \det M)^{-1} \det M,1}^{-1} M \Delta_{(b \det M)^{-1},1})(\tau)\mathbf{1}_{z=(b \det M)^{-1}}d\tau \\ &= (f \mid \Delta_{b,1} M \Delta_{b \det M,1}^{-1})(\tau)\mathbf{1}_{z=(b \det M)^{-1}}d\tau, \end{aligned}$$

whence the conclusion. □

Now, we prove for later reference (this will be needed in Chapter 5.7.2) that the algebraic q-expansion defined in Chapter 1.6 corresponds to the usual q-expansion after analytification. We first need the following lemma.

Lemma 2.4.3 *Let Y be a smooth proper $\mathbb{C}$-scheme, pure of dimension one, and X be a connected noncompact Riemann surface. Let $\varphi : X \to Y$ be a morphism of locally ringed spaces. Then φ factors through* $\mathrm{Spec}\,\mathcal{O}(X)$.

Proof. – We may assume that Y is connected.

First, we show the following: for any morphism of locally ringed spaces $f : X \to Y$ from a connected Riemann surface to a smooth connected $\mathbb{C}$-scheme, for any open subscheme $U \subset Y$, the image of $f^\sharp : \mathcal{O}(U) \to \mathcal{O}(f^{-1}(U))$ is made with meromorphic functions on X. Indeed, when U, Y, f are fixed, the statement is local with respect to X: since $f^{-1}(Y \backslash U)$ is discrete, we may assume that $f^{-1}(Y \backslash U)$ is a point $x \in X$. Let $\alpha \in \mathcal{O}(U)$. There is an affine open subscheme $V \subset Y$ containing $f(x)$ and a nonzero function $\beta \in \mathcal{O}(V)$ such that $\alpha\beta \in \mathcal{O}(V \cap U)$ extends to a function γ on the open subscheme $(V \cap U) \cup \{f(x)\}$. Then $f^\sharp(\alpha) = \frac{f^\sharp(\gamma)}{f^\sharp(\beta)}$ is a quotient of holomorphic functions near x, whence the conclusion.

Let us come back to the original statement. Let $x, y \in Y$ be two distinct closed points, then $U = Y \backslash \{x\}, V = Y \backslash \{y\}$ are smooth connected affine $\mathbb{C}$-schemes of dimension one by [4, Lemmas 0A24, 0A28], and $X = U \cup V$. Let $A \subset \mathcal{O}(X \backslash \varphi^{-1}(x)), B \subset \mathcal{O}(X \backslash \varphi^{-1}(y))$ be the images of $\mathcal{O}(U)$ and $\mathcal{O}(V)$ respectively: A, B are $\mathbb{C}$-algebras of meromorphic functions on X, so, by Mittag-Leffler's theorem [51, (26.5)], there are functions $\alpha, \beta \in \mathcal{O}(X)$ vanishing exactly on $f^{-1}(x)$ and $f^{-1}(y)$ respectively such that $A \subset \mathcal{O}(X)_\alpha, B \subset \mathcal{O}(X)_\beta$. Since α, β have no common zero, they generate the unit ideal of $\mathcal{O}(X)$ (see [51, Exercise 26.4]).

Hence, $\varphi : X \backslash f^{-1}(x) \to U$ factors through $\mathrm{Spec}\,\mathcal{O}(X)_\alpha$ and $\varphi : X \backslash f^{-1}(y) \to V$ factors through $\mathrm{Spec}\,\mathcal{O}(X)_\beta$, and the two morphisms $\mathrm{Spec}\,\mathcal{O}(X)_\alpha \to U$, $\mathrm{Spec}\,\mathcal{O}(X)_\beta \to V$ agree when restricted to $\mathrm{Spec}\,\mathcal{O}(X)_{\alpha\beta}$ (because they both come from φ). Hence they glue to a morphism $g : \mathrm{Spec}\,\mathcal{O}(X) \to Y$ such that the composition $X \overset{\mathrm{can}}{\to} \mathrm{Spec}\,\mathcal{O}(X) \overset{g}{\to} Y$ is equal to φ above U and above V, hence this composition is φ. □

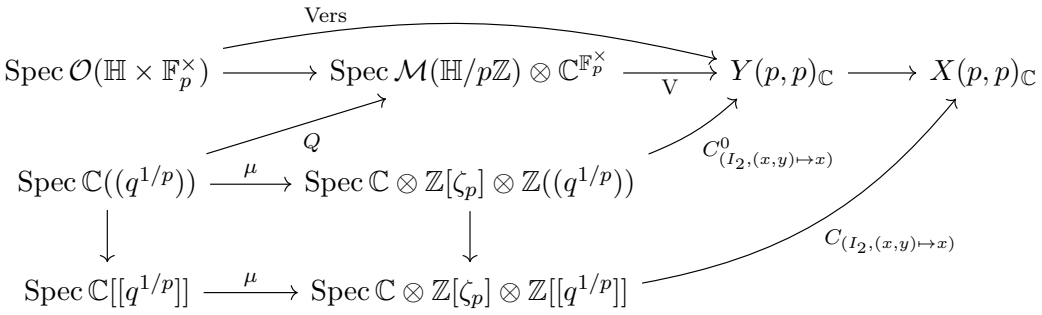
Proposition 2.4.4 *Let $\mu : z \otimes \zeta_p \in \mathbb{C} \otimes \mathbb{Z}[\zeta_p] \longmapsto ze^{\frac{-2i\pi}{p}} \in \mathbb{C}$.*

Let $\omega \in H^0(X(p,p)_{\mathbb{C}}, \Omega^1)$ and let $\sum_{n \geq 0} a_n q^{n/p} \in \mathbb{C}[[q^{1/p}]]$ be the image under μ of its q-expansion at the cusp datum $(I_2, (x,y) \mapsto x)$ (see Definition 1.6.11). Then the $\Delta_{1,1}$ component of $\iota_{p,p}(\omega)$ is $\frac{2i\pi}{p} \sum_{n \geq 0} a_n e^{\frac{2i\pi(n+1)\tau}{p}}$.

Proof. – Step 1: Descending the uniformization.

Let $\mathcal{M}(\mathbb{H}/p\mathbb{Z})$ denote the ring of p-periodic holomorphic functions f on $\mathbb{H}$ that are meromorphic at infinity: in other words, if we write $f(\tau) = g(e^{2i\pi\tau})$, where $g : D(0,1)\backslash\{0\} \to \mathbb{C}$ is a holomorphic function, then the singularity of g at 0 is either removable or a pole.

Consider the following diagram:



In this diagram, the unmarked vertical and horizontal arrows are the natural ones, and the maps $C_{(I_2,(x,y)\mapsto x)}, C^0_{(I_2,(x,y)\mapsto x)}$ are defined in Proposition 1.6.10 and its proof. For the sake of brevity, since we will only consider the cusp datum $(I_2,(x,y)\mapsto x)$, we write C, C^0 instead of $C_{(I_2,(x,y)\mapsto x)}, C^0_{(I_2,(x,y)\mapsto x)}$. So we need to define Vers, V, Q, and check that they make the diagram commute.

The application Vers denotes the versal elliptic curve as defined in the proof of Lemma 2.3.3: to be precise, it is given by the equation $y^2 = x^3 - 15G_4\cdot x - 35G_6$ with $G_4, G_6 \in \mathcal{O}(\mathbb{H}\times\mathbb{F}_p^\times)$ do not depend on the $\mathbb{F}_p^\times$ coordinate, and the level structure is given by

$$(\tau,b)\in\mathbb{H}\times\mathbb{F}_p^\times \longmapsto \left(\left[\wp_{\tau\mathbb{Z}\oplus\mathbb{Z}}\left(\frac{b\tau}{p}\right) : 2\wp'_{\tau\mathbb{Z}\oplus\mathbb{Z}}\left(\frac{b\tau}{p}\right) : 1\right], \left[\wp_{\tau\mathbb{Z}\oplus\mathbb{Z}}\left(\frac{1}{p}\right) : 2\wp'_{\tau\mathbb{Z}\oplus\mathbb{Z}}\left(\frac{1}{p}\right) : 1\right]\right).$$

Now, $G_4, G_6 \in \mathcal{M}(\mathbb{H}/p\mathbb{Z})$, since they are modular forms for $SL_2(\mathbb{Z})$. Moreover, let $c,d\in\mathbb{Z}$ be integers not both divisible by p. Then $\tau \longmapsto \wp'_{\tau\mathbb{Z}\oplus\mathbb{Z}}\left(\frac{c\tau+d}{p}\right)$ is a p-periodic holomorphic function on $\mathbb{H}$, given as the sum of the series

$$-2\sum_{(u,v)\in\mathbb{Z}^2}\left(\frac{c\tau+d}{p}-(u\tau+v)\right)^{-3},$$

which converges uniformly on rectangles of the form $\{|\mathrm{Re}(\tau)|\le D, \mathrm{Im}(\tau)\ge t\}$ for any $D,t>0$. This implies that $\wp'_{\tau\mathbb{Z}\oplus\mathbb{Z}}\left(\frac{c\tau+d}{p}\right)$ converges to a constant as $\mathrm{Im}(\tau)\to\infty$, hence

$$\left[\tau\longmapsto\wp'_{\tau\mathbb{Z}\oplus\mathbb{Z}}\left(\frac{c\tau+d}{p}\right)\right]\in\mathcal{M}(\mathbb{H}/p\mathbb{Z}).$$

The calculation at the start of [41, Section 4.6] shows that $\left[\tau\longmapsto\wp_{\tau\mathbb{Z}\oplus\mathbb{Z}}\left(\frac{c\tau+d}{p}\right)\right]\in\mathcal{M}(\mathbb{H}/p\mathbb{Z})$, so there is a unique morphism $V : \mathrm{Spec}\,\mathcal{M}(\mathbb{H}/p\mathbb{Z})\otimes\mathbb{C}^{\mathbb{F}_p^\times}\to Y(p,p)_{\mathbb{C}}$ making the second row of the diagram commute.

For any $f\in\mathcal{M}(\mathbb{H}/p\mathbb{Z})\otimes\mathbb{C}^{\mathbb{F}_p^\times}$, there is a unique power series $g(q^{1/p}) := Q^\sharp(f)\in\mathbb{C}((q^{1/p}))$ such that for all $\tau\in\mathbb{H}$, one has $f(\tau,1) = g(e^{\frac{2i\pi\tau}{p}})$. The morphism Q in the diagram is the morphism of schemes coming from $Q^\sharp$.

To check that the diagram commutes, we need to write down an isomorphism preserving the

level structure between the Tate curve, given over $\mathbb{C}((q^{1/p}))$ by

$$y^2+xy=x^3-5x\frac{E_4-1}{240}+\frac{1}{12}\left(-5\frac{E_4-1}{240}-7\frac{E_6-1}{-504}\right),$$

and the curve with Weierstrass equation

$$v^2=u^3-15G_4u-35G_6 \Leftrightarrow v^2=u^3-\frac{\pi^4}{3}E_4u-\frac{2\pi^6}{27}E_6.$$

A direct computation with [85, (A1.2.1)] shows that the appropriate change of variables is

$$u=(2i\pi)^2\left(x+\frac{1}{12}\right),\ v=\frac{(2i\pi)^3}{2}(x+2y).$$

Now, let us discuss the level structures. The level structure induced on the Tate curve by $C_{(I_2,(x,y)\mapsto x)}$ is an isomorphism $\phi:(\mathbb{Z}/p\mathbb{Z})^2\longmapsto q^{\left(\frac{1}{p}\mathbb{Z}\right)/\mathbb{Z}}\zeta_p^{\mathbb{Z}/p\mathbb{Z}}$ such that $\phi((0,-1))=\zeta_p$ and $\phi((1,0))=q^{1/p}$. In particular, the image of this level structure under μ is given by $(a,b)\longmapsto e^{\frac{2i\pi}{p}(a\tau+b)}\in\mathbb{C}^*/e^{2i\pi\tau\mathbb{Z}}$, which is isomorphic to $(a,b)\longmapsto\frac{a\tau+b}{p}\in\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\mathbb{Z}}$.

This proves that the diagram that we drew at the beginning of the proof commutes.

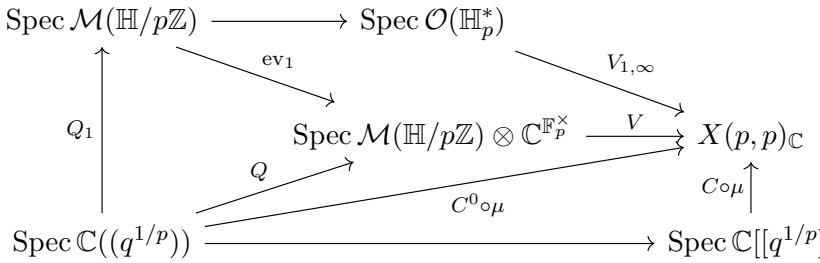
Step 2: Extension of the diagram to infinity.

Let $\mathbb{H}_p^*$ be the Riemann surface $\mathbb{H}/p\mathbb{Z}\cup\{i\infty\}$, where the holomorphic structure near $i\infty$ makes the bijection $\tau\in\mathbb{H}_p^*\longmapsto e^{2i\pi\frac{\tau}{p}}\in D(0,1)$ a biholomorphism. Let $\mathbb{H}_p^*\to X(p,p)^{an}$ be the morphism $\tau\longmapsto(\tau,1)$ with the uniformization of Proposition 2.4.1 (see [41, Chapter 2.4] for the description of the cusps of the analytification). By Lemma 2.4.3, the composition $\mathbb{H}_p^*\to X(p,p)^{an}\to X(p,p)_{\mathbb{C}}$ factors through a morphism $V_{1,\infty}:\operatorname{Spec}\mathcal{O}(\mathbb{H}_p^*)\to X(p,p)_{\mathbb{C}}$.

Let ev_1 be the morphism of schemes attached to the homomorphism of $\mathbb{C}$-algebras

$$\mathcal{M}(\mathbb{H}/p\mathbb{Z})\otimes\mathbb{C}^{\mathbb{F}_p^\times}\simeq\operatorname{Fun}(\mathbb{F}_p^\times,\mathcal{M}(\mathbb{H}/p\mathbb{Z}))\overset{f\mapsto f(1)}{\longrightarrow}\mathcal{M}(\mathbb{H}/p\mathbb{Z}).$$

By Step 1, the following diagram commutes



The morphism $Q_{1,\infty}:\operatorname{Spec}\mathbb{C}((q^{1/p}))\to\operatorname{Spec}\mathcal{O}(\mathbb{H}_p^*)$ actually factors through a morphism $Q_\infty:\operatorname{Spec}\mathbb{C}[[q^{1/p}]]\to\operatorname{Spec}\mathcal{O}(\mathbb{H}_p^*)$ corresponding to the usual q-expansion, mapping the function $\sum_{n\geq0}a_ne^{\frac{2i\pi n\tau}{p}}$ to the series $\sum_{n\geq0}a_nq^{n/p}$.

The morphisms $V_{1,\infty}\circ Q_\infty, C\circ\mu:\operatorname{Spec}\mathbb{C}[[q^{1/p}]]\to X(p,p)_{\mathbb{C}}$ are morphisms of reduced separated $\mathbb{C}$-schemes and agree on the dense open subscheme $\operatorname{Spec}\mathbb{C}((q^{1/p}))$ of the source, hence they are equal. In other words, the following diagram commutes:

$$\begin{array}{ccc} \mathbb{H}_p^* & \xrightarrow{\tau\mapsto(\tau,1)} & X(p,p)^{an} \\ \downarrow & & \downarrow \\ \operatorname{Spec}\mathcal{O}(\mathbb{H}_p^*) & \xrightarrow{V_{1,\infty}} & X(p,p)_{\mathbb{C}} \\ Q_\infty \uparrow & \nearrow_{C\circ\mu} & \\ \operatorname{Spec}\mathbb{C}[[q^{1/p}]] & & \end{array}$$

Step 3: Conclusion.

Let $x \in X(p,p)(\mathbb{C})$ be the image of the maximal ideal of $\operatorname{Spec}\mathbb{C}[[q^{1/p}]]$ under $C\circ\mu$: its inverse image $x^{an} \in X(p,p)^{an}_{\mathbb{C}}$ is the point $(i\infty, 1)$.

For $z \in \mathbb{H}$ and $\gamma \in SL_2(\mathbb{Z})$, if z and $\gamma\cdot z$ have imaginary part greater than one, then $\gamma = \pm\begin{pmatrix}1 & * \\ 0 & 1\end{pmatrix}$. Therefore, the function $e^{\frac{2i\pi\tau}{p}}$ is well-defined as an element of $\mathcal{O}_{X(p,p)^{an}_{\mathbb{C}},(i\infty,1)}$ and is a uniformizer of this discrete valuation ring by the construction of the Riemann surface attached to $\Gamma(p)$ [41, Chapter 2.4]. By Step 2, the following diagram commutes.

$$\begin{array}{ccccc} \mathcal{O}_{X(p,p)_{\mathbb{C}},x} & \longrightarrow & \mathcal{O}_{X(p,p)^{an},x^{an}} & \xrightarrow{e^{\frac{2i\pi}{p}}\mapsto q^{1/p}} & \mathbb{C}[[q^{1/p}]] \\ & \searrow & & \nearrow_{(C\circ\mu)^\sharp} & \end{array}$$

Moreover, by [68, Exp. XII, Théorème 1.1] and Proposition 1.6.14, all three rings are discrete valuation rings (since $X(p,p)_{\mathbb{C}}$ is smooth of relative dimension one over $\mathbb{C}$ and its analytification is a Riemann surface), all three morphisms are local and induce isomorphisms after completing.

Let $\sum_{n\geq 1} b_n e^{\frac{2i\pi n\tau}{p}}$ denote the component of $\Delta_{1,1}$ in $\iota_{p,p}(\omega)$. Since $d\tau = \frac{p}{2i\pi}e^{\frac{-2i\pi}{p}}d(e^{\frac{2i\pi}{p}})$, the pull-back of ω as a holomorphic differential form on $X(p,p)^{an}_{\mathbb{C}}$ can be written locally around x^{an} as $\frac{p}{2i\pi}\left(\sum_{n\geq 0} b_{n+1}e^{\frac{2i\pi n\tau}{p}}\right)\cdot d(e^{\frac{2i\pi\tau}{p}})$. The local diagram commutes, so the pull-back of ω by $C\circ\mu$ as a continuous differential on the analytic space $\operatorname{Spec}\mathbb{C}[[q^{1/p}]]/(q^t)$ is given by $\frac{p}{2i\pi}\left(\sum_{n=0}^{pt} b_{n+1}q^{n/p}\right)d(q^{1/p})$, and we proved the result. □

Corollary 2.4.5 *Let $\omega \in H^0(X(p,p)_{\mathbb{C}},\Omega^1)$ and let $\sum_{n\geq 0} a_n q^{n/p} \in (\mathbb{Z}[\zeta_p]\otimes\mathbb{C})[[q^{1/p}]]$ be its q-expansion at the cusp datum $(I_2,(x,y)\mapsto x)$. Let, for every $a\in\mathbb{F}_p^\times$, $\mu_a : \mathbb{Z}[\zeta_p]\otimes\mathbb{C}\to\mathbb{C}$ be the homomorphism of $\mathbb{C}$-algebras such that $\mu_a(\zeta_p) = e^{-\frac{2i\pi a}{p}}$. Then*

$$\iota_{p,p}(\omega) = \frac{2i\pi}{p}\sum_{a\in\mathbb{F}_p^\times}\left(\sum_{n\geq 1}\mu_a(a_{n-1})e^{\frac{2i\pi n\tau}{p}}\right)\otimes\Delta_{a^{-1},1}.$$

Proof. – For any $t\geq 2$, let C_t be the following composition:

$$\operatorname{Spec}(\mathbb{Z}[\zeta_p]\otimes\mathbb{C})\otimes\mathbb{Z}[[q^{1/p}]]/(q^{t/p}) \to \operatorname{Spec}(\mathbb{Z}[\zeta_p]\otimes\mathbb{C})\otimes\mathbb{Z}[[q^{1/p}]] \xrightarrow{C_{(I_2,(x,y)\mapsto x)}} X(p,p)_{\mathbb{C}}.$$

Then, for any $a\in\mathbb{F}_p^\times$, one has by Lemma 1.6.16

$$\begin{aligned}(\operatorname{Spec}\mu_a)^*C_t^*\omega &= (\operatorname{Spec}\mu_1\circ\underline{a})^*C_t^*\omega = (\operatorname{Spec}\mu_1)^*(\underline{a})^*C_t^*\omega \\ &= (\operatorname{Spec}\mu_1)^*C_t^*(\Delta_{a,1}^*\omega).\end{aligned}$$

Therefore, the power series in front of the $\Delta_{1,1}$ component of $\iota_{p,p}(\Delta_{a,1}^*\omega)$ (hence the $\Delta_{a^{-1},1}$ component of $\iota_{p,p}(\omega)$) is $\frac{2i\pi}{p}\sum_{n\geq 1}\mu_a(a_{n-1})e^{\frac{2i\pi n\tau}{p}}$. □

Corollary 2.4.6 *For every $\psi \in \mathcal{D}$, the subspace of $H^0(X(p,p)_{\mathbb{C}}, \Omega^1)$ on which $\mathrm{GL}_2(\mathbb{F}_p)$ acts by $\psi(\det)$ is trivial.*

Proof. – Let $\omega \in H^0(X(p,p)_{\mathbb{C}}, \Omega^1)$ be such that for all $g \in \mathrm{GL}_2(\mathbb{F}_p)$, $g^*\omega = \psi(\det g)\omega$. Write $\iota_{p,p}(\omega) = \sum_{b\in\mathbb{F}_p^\times} f_b \otimes \Delta_{b,1}$. Then, if $M \in \mathrm{SL}_2(\mathbb{F}_p)$,

$$\sum_{b\in\mathbb{F}_p^\times} f_b \otimes \Delta_{b,1} = \iota_{p,p}(\omega) = \iota_{p,p}(M^*\omega) = M^* \sum_{b\in\mathbb{F}_p^\times} f_b \otimes \Delta_{b,1}$$
$$= \sum_{b\in\mathbb{F}_p^\times} (f_b \mid \Delta_{b,1} M \Delta_{b,1}^{-1}) \mid \Delta_{b,1},$$

so every f_b is in $\mathcal{S}_2(\Gamma(1)) = \{0\}$, so $\omega = 0$. □

Proposition 2.4.7 *Let $\ell \neq p$ be a prime number, then the following diagram commutes, where ℓ maps $\Delta_{b,1}$ to $\Delta_{b\ell,1}$:*

$$\begin{array}{ccc} H^0(X(p,p)_{\mathbb{C}}, \Omega^1) & \xrightarrow{\iota_{p,p}} & \bigoplus_{b\in\mathbb{F}_p^\times} \mathcal{S}_2(\Gamma(p)) \otimes \Delta_{b,1} \\ \downarrow{\scriptstyle T_\ell^*} & & \downarrow{\scriptstyle [\Gamma(p) D_{1,\ell} \Gamma(p)]\otimes \ell} \\ H^0(X(p,p)_{\mathbb{C}}, \Omega^1) & \xrightarrow{\iota_{p,p}} & \bigoplus_{b\in\mathbb{F}_p^\times} \mathcal{S}_2(\Gamma(p)) \otimes \Delta_{b,1} \end{array}$$

Proof. – This is proved in a completely similar way to Proposition 2.3.5. Consider the following commutative diagram of locally ringed spaces, where υ is always the uniformization defined in Lemma 2.3.3:

$$\begin{array}{ccccccc} \mathbb{H}\times\mathbb{F}_p^\times & \xleftarrow{h} & \mathbb{H}\times\mathbb{F}_p^\times & \xrightarrow{(g_w)_w} & \coprod_{w\in\mathbb{P}^1(\mathbb{F}_\ell)} \mathbb{H}\times\mathbb{F}_p^\times & \xrightarrow{h'} & \mathbb{H}\times\mathbb{F}_p^\times \\ \downarrow{\scriptstyle \upsilon} & & & \searrow^{\upsilon} & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \upsilon} \\ Y(p,p)_{\mathbb{C}} & & \xleftarrow[D_{\ell,1}]{} & & Y(p,p,\Gamma_0(\ell))_{\mathbb{C}} & \xrightarrow{D_{1,1}} & Y(p,p)_{\mathbb{C}} \end{array}$$

Here, $h(\tau,z) = (\delta_\ell(\ell\tau), \ell z)$ where $\delta_\ell \in \Gamma(\ell)$ is congruent mod p to $\Delta_{\ell^{-1},\ell}$, $h'(\tau,z) = (\tau,z)$, π maps a point (τ,z) on the component $w = [c:d] \in \mathbb{P}^1(\mathbb{F}_\ell)$ to the class of the elliptic curve $\left(\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\mathbb{Z}}, \frac{z\tau}{p}, \frac{1}{p}, \langle\frac{c\tau+d}{\ell}\rangle\right)$, and $g_v : (\tau,z) \longmapsto (M_v^{-1}\tau, z)$ where $M_v \in \Gamma(p)$ is such that the image in $\mathbb{P}^1(\mathbb{F}_\ell)$ of its second row is v. Note that $(\pi_v)_v$ is a morphism of locally ringed spaces because so is g_v and so is υ.

As in Proposition 2.3.5, the rightmost 2×2 square is Cartesian above a cofinite open subscheme of $Y(p,p)$ (by Lemma 2.2.17) and let

$$D_\ell = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}, \; D'_\ell = \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}.$$

As in the proof of Proposition 2.3.5, it is enough to show that

$$M \in (\Gamma_0(\ell) \cap \Gamma(p))\backslash\Gamma(p) \longmapsto \delta_\ell D_\ell M \in \Gamma(p)\backslash\Gamma(p) D'_\ell \Gamma(p),$$

is bijective, which is proved in a similar way. □

Notation *We denote by Γ' the congruence group $\Gamma_1(p) \cap \Gamma_0(p^2)$. Let $\mathcal{N}_0$ be the collection of (f,χ), where $f \in \mathcal{S}_2(\Gamma_1(p))$ is a normalized newform with character χ, and $\mathcal{N}$ be the reunion of $\mathcal{N}_0$ and the (f,χ), where f is a normalized newform in $\mathcal{S}_2(\Gamma')$ with character χ.*

By Proposition C.2.2, for any $\psi \in \mathcal{D}$, and $(f,\chi) \in \mathcal{N}$, then $(f\otimes\psi, \chi\psi^2) \in \mathcal{N}$.

Proposition 2.4.8 *Let $j : \mathcal{S}_2(\Gamma(p)) \to \mathcal{S}_2(\Gamma')$ be the isomorphism given by $f \longmapsto f \mid \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$: it extends as an isomorphism*

$$j' : \bigoplus_{b \in \mathbb{F}_p^\times} \mathcal{S}_2(\Gamma(p)) \otimes \Delta_{b,1} \to \bigoplus_{b \in \mathbb{F}_p^\times} \mathcal{S}_2(\Gamma') \otimes \Delta_{b,1}.$$

The following collection of vectors is a basis of $H^0(X(p,p)_{\mathbb{C}}, \Omega^1)$ made with eigenvectors for $\mathbb{T}$ and the $\Delta_{a,b}$ (for $a, b \in \mathbb{F}_p^\times$):

- *$u_{f,\psi} := (j' \circ \iota_{p,p})^{-1} \left(f(\tau) \otimes \sum_{t \in \mathbb{F}_p^\times} \psi^{-1}(t)[\Delta_{t,1}] \right)$, where (f, χ) runs through $\mathcal{N}$ and ψ runs through elements of $\mathcal{D}$,*
- *$u^p_{f,\psi} := (j' \circ \iota_{p,p})^{-1} \left(f(p\tau) \otimes \sum_{t \in \mathbb{F}_p^\times} \psi^{-1}(t)[\Delta_{t,1}] \right)$, where (f, χ) runs through $\mathcal{N}_0$ and ψ runs through elements of $\mathcal{D}$.*

In either case, the eigenvalue for the Hecke operator T_ℓ, for $\ell \neq p$ prime (resp. m_n, resp. $\Delta_{n,1}$ for $n \in \mathbb{F}_p^\times$) is $a_n(f)\psi(n)$ (resp. $\psi(n)^2\chi(n)$, resp. $\psi(n)$).

Proof. – For any prime $\ell \neq p$, one can directly check that $j(f \mid [\Gamma(p)\mathrm{diag}(1,\ell)\Gamma(p)]) = T_\ell(j(f))$. By similar verifications, the induced action by $j' \circ \iota_{p,p}$ of $\mathbb{T}[(\Delta_{a,b})_{a,b} \in \mathbb{F}_p^\times]$ on $\bigoplus_{b \in \mathbb{F}_p^\times} \mathcal{S}_2(\Gamma') \otimes \Delta_{b,1}$ is the following: pulling back by T_ℓ (resp. m_n, resp. $\Delta_{n,1}$) acts by $T_\ell \otimes [\ell]$ (resp. $\langle n \rangle \otimes [n^2]$, resp. $\mathrm{id} \otimes [n]$) where $[n]$ is the application $f \otimes \Delta_{b,1} \longmapsto f \otimes \Delta_{bn,1}$.

Now, as we saw in the proof of Corollary 2.3.6, the $\sum_{t \in \mathbb{F}_p^\times} \psi^{-1}(t)[\Delta_{t,1}]$ (where ψ runs through characters in $\mathcal{D}$) form a basis of $\sum_{t \in \mathbb{F}_p^\times} \mathbb{C}[\Delta_{t,1}]$, and these vectors are eigenvectors of any $[n]$ ($n \in \mathbb{F}_p^\times$) with eigenvalue $\psi(n)$. Moreover, the $f(\tau)$ for $(f, \chi) \in \mathcal{N}$ and the $f(p\tau)$ for $(f, \chi) \in \mathcal{N}_0$ form a basis of $\mathcal{S}_2(\Gamma')$ by [41, Theorem 5.8.3], and they are eigenvectors for the Hecke and diamond operators (this follows for instance from the proof of [41, Proposition 5.6.2]). This implies the conclusion. □

Corollary 2.4.9 *The action of $\mathbb{T}$ on $H^0(X(p,p)_{\mathbb{C}}, \Omega^1)$ is diagonalizable. Its eigenspaces, which are stable under the right action of $\mathrm{GL}_2(\mathbb{F}_p)$, are the following form:*

- *Given $(f, \chi) \in \mathcal{N}_0$ and $\psi \in \mathcal{D}$, the subspace on which T_ℓ (resp. m_n) acts with eigenvalue $a_\ell(f)\psi(\ell)$ (resp. $\chi(n)\psi(n)^2$) has dimension p if $\chi = 1$ and $p+1$ otherwise. We let $\Omega^1[f, \psi]$ be this eigenspace.*
- *Given $(f, \chi) \in \mathcal{N}$ such that all the twists of f by Dirichlet characters modulo p have conductor p^2 (we say that f is* twist-primitive*), the subspace on which T_ℓ (resp. m_n) acts with eigenvalue $a_\ell(f)$ (resp. $\chi(n)$) has dimension $p-1$. We let $\Omega^1[f]$ be this eigenspace.*

Proof. – The action of $\mathbb{T}$ on $H^0(X(p,p)_{\mathbb{C}}, \Omega^1)$ is diagonal in the basis of Proposition 2.4.8.

First, we need to show that, for any vector v in this basis, there exist $(f, \chi) \in \mathcal{N}_0$ and $\psi \in \mathcal{D}$ such that for every $\ell \neq p$ and every $n \in \mathbb{F}_p^\times$, $T_\ell^* v = a_\ell(f)\psi(\ell)v$, $m_n^* v = \chi(n)\psi(n)^2$, or there exists $(f, \chi) \in \mathcal{N}$ such that f is twist-primitive and for every $\ell \neq p$ and every $n \in \mathbb{F}_p^\times$, $T_\ell^* v = a_\ell(f)v$ and $m_n^* v = \chi(n)v$.

First, one always has $u^p_{f,\psi} \in \Omega^1[f, \psi]$. Next, let $(f, \chi) \in \mathcal{N}$ and $\psi \in \mathcal{D}$. If f is twist-primitive, then its twist $g = f \otimes \psi \in \mathcal{S}_2(\Gamma')$ is a twist-primitive newform, and one directly checks that $u_{f,\psi} \in \Omega^1[g]$. If f is not twist-primitive, then $f = g \otimes \theta$ for some character $\theta \in \mathcal{D}$ and $(g, \chi\theta^{-2}) \in \mathcal{N}_0$, so that it is easy to check that $u_{f,\psi} \in \Omega^1[g, \psi\theta]$.

Let $(f, \chi) \in \mathcal{N}$ and $\psi \in \mathcal{D}$, assume that either f is twist-primitive and $\psi = \mathbf{1}$, or $(f, \chi) \in \mathcal{N}_0$. Let us count how many vectors in the basis of Proposition 2.4.8 lie in $\Omega^1[f, \psi]$. If $\psi' \in \mathcal{D}$ and $(g, \chi') \in \mathcal{N}$ (resp. $(g, \chi') \in \mathcal{N}_0$), the vector $u_{g,\psi'}$ (resp. $u^p_{g,\psi'}$) lies in $\Omega^1[f, \psi]$ if and only if, for every prime $\ell \neq p$ and every $n \in \mathbb{F}_p^\times$, $a_\ell(g)\psi'(\ell) = a_\ell(f)\psi(\ell)$ and $\chi'(n)\psi'(n)^2 = \chi(n)\psi(n)^2$. When this condition is satisfied, the newforms $g \otimes \psi'$ and $f \otimes \psi$ are equal (by strong multiplicity one [121, Theorem 4.6.19]), so $(g, \psi') = (f \otimes \psi\overline{\psi'}, \psi')$ – and the converse is true.

When $(f,\chi)\in\mathcal{N}_0$, every choice of ψ' (resp. by Lemma 2.3.7, only $\psi'=\psi$ if $\chi=\mathbf{1}$, or only $\psi'\in\{\psi,\chi\psi\}$ if $\chi\neq\mathbf{1}$) determines a suitable couple (g,ψ'). Therefore, $\Omega^1[f,\psi]$ has dimension $p=(p-1)+1$ if $\chi=\mathbf{1}$ and $p+1=(p-1)+2$ otherwise. When f is twist-primitive and $\psi=\mathbf{1}$, g always has conductor p^2, so $\Omega^1[f]$ contains no vector of the form $u^p_{\cdot,\cdot}$. Since every choice of ψ' determines a couple (g,ψ'), such that $u_{g,\psi'}\in\Omega^1[f]$, $\dim\Omega^1[f]=p-1$. □

Definition 2.4.10 We define the sets $\mathscr{S},\mathscr{P},\mathscr{C}$ as follows:

- $\mathscr{S}$ is the set of $(f,\mathbf{1})\in\mathcal{N}_0$ (alternatively, f is a newform with trivial character and conductor p).
- $\mathscr{P}$ is the set of $(f,\chi)\in\mathcal{N}_0$ with χ nontrivial (alternatively, f is a newform with conductor p and nontrivial character).
- $\mathscr{C}$ is the set of $(f,\chi)\in\mathcal{N}$ where f is twist-primitive, that is, every twist of f by a Dirichlet character of conductor p has conductor p^2.

Corollary 2.4.11 *For any $(f,\chi)\in\mathcal{N}_0$ and $\psi\in\mathcal{D}$ (resp. any $(f,\chi)\in\mathcal{N}$ such that f is twist-primitive), for any $n\geq 1$ coprime to p, T_n acts on $\Omega^1[f,\psi]$ (resp. $\Omega^1[f]$) by $a_n(f)\psi(n)$ (resp. $a_n(f)$).*

Proof. – Exactly like in the proof of Lemma 2.3.9, it is a direct induction on n using the definition of T_n and the relations between Fourier coefficients of newforms. □

Corollary 2.4.12 *Let $(f,\chi)\in\mathscr{C}$. Let $\Omega^1[f]$ be the subspace of $H^0(X(p,p),\Omega^1)$ which T_ℓ (resp. m_n) acts by $a_\ell(f)$ (resp. $\chi(n)$). Then $\Omega^1[f]$ is an irreducible cuspidal (right) representation of $\mathrm{GL}_2(\mathbb{F}_p)$ with central character χ. Let, for each $\psi\in\mathcal{D}$, $e_\psi=u_{f_\psi,\psi^{-1}}$ with the notation of Proposition 2.4.8 where f_ψ is the twist of f by ψ.*

Then the e_ψ form a basis of $\Omega^1[f]$. Moreover, the following relations hold (where the notations $\mathfrak{g}$ and λ_p are defined in Appendix C):

- *For $a\in\mathbb{F}_p^\times$, $e_\psi\mid U^a=\sum_\theta\frac{\theta(a)}{p-1}\mathfrak{g}(\overline{\theta})e_{\psi\theta}$, where θ runs through elements of $\mathcal{D}$,*
- *For any $a\in\mathbb{F}_p^\times$, $e_\psi\mid\Delta_{a,1}=\psi^{-1}(a)e_\psi$.*
- *$e_\psi\mid W=\lambda_p(f_\psi)e_{\overline{\chi}/\psi}$.*

Proof. – The second relation is a direct consequence from Proposition 2.4.8. Note that by [121, Theorem 4.6.17], for every $\psi\in\mathcal{D}$, $a_p(f_\psi)=0$.

For any function $\alpha:\mathbb{F}_p^\times\to\mathbb{C}$, one easily computes that

$$\alpha=\frac{1}{p-1}\sum_{\chi\in\mathcal{D}}\left(\sum_{x\in\mathbb{F}_p^\times}\alpha(x)\chi^{-1}(x)\right)\chi.$$

Thus, for every $m\in\mathbb{F}_p^\times$, one has $e^{\frac{2i\pi m}{p}}=\frac{1}{p-1}\sum_{\chi\in\mathcal{D}}\chi(m)\mathfrak{g}(\overline{\chi})$ (where $\mathfrak{g}$ is the Gauss sum, every character being regarded as a mod p Dirichlet character).

Let $\psi \in \mathcal{D}$ and $a \in \mathbb{F}_p^\times$. Let $V = \begin{pmatrix} 1 & 1/p \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{Q})$. Then one has, in $\bigoplus_{t\in\mathbb{F}_p^\times} \mathbb{C}[[q]] \otimes [\Delta_{t,1}]$,

$$\begin{aligned} j'(\iota_{p,p}(e_\psi \mid U^a)) &= \sum_{x\in\mathbb{F}_p^\times} \psi(x) f_\psi \mid_2 V^{xa} \otimes [\Delta_{x,1}] = \sum_{\substack{n\geq 1 \\ x\in\mathbb{F}_p^\times}} \psi(x) a_n(f)\psi(n) e^{\frac{2i\pi}{p}nxa} e^{2i\pi n\tau} \otimes [\Delta_{x,1}] \\ &= \frac{1}{p-1} \sum_{\substack{n\geq 1 \\ (x,\theta)\in\mathbb{F}_p^\times\times\mathcal{D}}} \psi(x) a_n(f)\psi(n)\mathfrak{g}(\overline{\theta})\theta(nxa) e^{2i\pi n\tau} \otimes [\Delta_{x,1}] \\ &= \frac{1}{p-1} \sum_{\theta\in\mathcal{D}} \mathfrak{g}(\overline{\theta})\theta(a) \sum_{\substack{n\geq 1 \\ x\in\mathbb{F}_p^\times}} (\psi\theta)(x)(\psi\theta)(n) a_n(f) e^{2i\pi n\tau} \otimes [\Delta_{x,1}] \\ &= \sum_\theta \frac{\mathfrak{g}(\overline{\theta})\theta(a)}{p-1} f_{\psi\theta} \otimes \sum_{x\in\mathbb{F}_p^\times} (\psi\theta)(x)[\Delta_{x,1}] = \sum_\theta \frac{\theta(a)}{p-1}\mathfrak{g}(\overline{\theta})(j'\circ\iota_{p,p})(e_{\psi\theta}). \end{aligned}$$

Now, one formally has $(j'\circ\iota_{p,p})([h\otimes\Delta_{b,1}] \mid_2 W) = h \mid_2 \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \delta_{b^{-1}} \begin{pmatrix} 0 & -1/p \\ p & 0 \end{pmatrix} \otimes [\Delta_{b,1}]$, so that

$$\begin{aligned} j'(\iota_{p,p}(e_\psi \mid W)) &= \sum_{x\in\mathbb{F}_p^\times} \psi(x)\overline{\psi^2\chi(x)}(f_\psi \mid \begin{pmatrix} 0 & -1 \\ p^2 & 0 \end{pmatrix} \otimes [\Delta_{x,1}] = \lambda_p(f_\psi) \sum_{x\in\mathbb{F}_p^\times} \overline{\chi\psi(x)} f_{\overline{\psi}} \otimes [\Delta_{x,1}] \\ &= \lambda_p(f_\psi) \sum_{x\in\mathbb{F}_p^\times} \overline{\chi\psi(x)} f_{\overline{\psi\chi}} \otimes [\Delta_{x,1}] = \lambda_p(f_\psi) e_{\overline{\psi\chi}}, \end{aligned}$$

so we are done. □

Definition 2.4.13 Given $(f,\chi) \in \mathscr{C}$, we define $C_f = \mathrm{Hom}_{\mathbb{C}}(\Omega^1[f], \mathbb{C})$: it is an irreducible cuspidal left[2] representation of $\mathrm{GL}_2(\mathbb{F}_p)$. By Appendix B.2, C_f is attached to a pair $\{\phi, \phi^p\}$ of characters of $\mathbb{F}_{p^2}^\times$. We will often arbitrarily choose a character in this pair and call it *the* character attached to C_f. Every time that we do this, the result we are interested in does not depend on which character we chose.

Remark Given (f,χ) as in Definition 2.4.13, it turns out that the character of $\mathbb{F}_{p^2}^\times$ attached to C_f characterizes the automorphic representation of $\mathrm{GL}_2(\mathbb{Q}_p)$ attached to f and therefore, by the local Langlands correspondence, the restriction to a decomposition group at p of the Galois representation attached to f. This will prove to be important in later computations of local constants. We will discuss this relationship in more detail later, so let us simply derive, for later reference, a few elementary consequences of the construction.

Corollary 2.4.15 *Let $(f,\chi) \in \mathscr{C}$ and $\psi \in \mathcal{D}$. Then $C_{f\otimes\psi} \simeq C_f \otimes \psi(\det)$. In particular, if ϕ is one of the characters of $\mathbb{F}_{p^2}^\times$ attached to C_f, then $\phi\cdot\psi(N_{\mathbb{F}_{p^2}/\mathbb{F}_p})$ is one of the characters attached to $C_{f\otimes\psi}$.*

Proof. – The second part of the claim is a consequence of the first part and Corollary B.2.8. To prove the first part of the claim, let $(e_\alpha)_{\alpha\in\mathcal{D}}, (e'_\alpha)_{\alpha\in\mathcal{D}}$ be the bases of $\Omega^1[f]$ and $\Omega^1[f\otimes\psi]$ constructed in Corollary 2.4.12.

The $\mathbb{C}$-linear homomorphism $e_\alpha \longmapsto e'_{\alpha\psi^{-1}}$ is a linear isomorphism $\Omega^1[f] \to \Omega^1[f\otimes\psi]$. By Corollary 2.4.12, the induced morphism $\Omega^1[f]\otimes\psi(\det) \to \Omega^1[f\otimes\psi]$ is equivariant for the (right) actions of U, $\Delta_{a,1}$ and W, so it is a $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-isomorphism, and we are done. □

[2]In particular, note that a matrix $M \in \mathrm{GL}_2(\mathbb{F}_p)$ maps $u \in C_f$ to $u(- \mid M)$: in particular, this operation preserves the central character instead of inverting it.

Corollary 2.4.16 *Let $(f,\chi) \in \mathscr{C}$ and $\phi : \mathbb{F}_{p^2}^\times \to \mathbb{C}^\times$ be a character attached to C_f. Then the following identities hold:*

- $\phi_{|\mathbb{F}_p^\times} = \chi$.
- *Let $z \in \mathbb{F}_{p^2}^\times \backslash \mathbb{F}_p^\times$ have trace and norm $a, N \in \mathbb{F}_p^\times$ respectively (this amounts to requiring that $z^2 \notin \mathbb{F}_p^\times$). Then*

$$-\phi(z) - \phi^p(z) = \frac{\chi(a)}{p-1} \sum_{\psi \in \mathcal{D}} \psi\left(\frac{a^2}{N}\right) \lambda_p(f_\psi) \mathfrak{g}(\overline{\chi\psi^2}).$$

- *Let $z \in \mathbb{F}_{p^2}^\times \backslash \mathbb{F}_p$ with norm N such that $z^2 \in \mathbb{F}_p^\times$. Then*

$$-\phi(z) = -\phi^p(z) = \frac{1}{2} \sum_{\psi^2\chi = 1} \psi^{-1}(N) \lambda_p(f_\psi).$$

- *If $\psi \in \mathcal{D}$ satisfies $\psi^2\chi = 1$ and $a \in \mathbb{F}_p^\times \backslash \mathbb{F}_p^{\times 2}$, then $\phi(\sqrt{a}) = -\psi^{-1}(-a)\lambda_p(f_\psi)$.*
- *If $\chi = \mathbf{1}$ and $\lambda \in \mathcal{D}$ is the nontrivial quadratic character, then $\lambda_p(f) = -\lambda(-1)\lambda_p(f_\lambda)$.*

Proof. – For any $a \in \mathbb{F}_p^\times$, aI_2 acts on C_f by $\phi(a)$ by definition of ϕ, and also acts by $\chi(a)$ by construction.

For the second statement, $-\phi(z) - \phi^p(z)$ is the trace of the action of $\begin{pmatrix} 0 & -N \\ 1 & a \end{pmatrix} = \Delta_{N,1} W U^a$ on $\Omega^1[f,1]$ by construction. Let $\psi \in \mathcal{D}$, then

$$\begin{aligned} e_\psi \mid \Delta_{N,1} W U^a &= \psi^{-1}(N) e_\psi \mid W U^a = \psi^{-1}(N)\lambda_p(f_\psi) e_{\overline{\chi}/\psi} \mid U^a \\ &= \frac{\psi^{-1}(N)}{p-1} \lambda_p(f_\psi) \sum_{\theta \in \mathcal{D}} \theta(a)\mathfrak{g}(\overline{\theta}) e_{\theta\overline{\chi}/\psi}. \end{aligned}$$

Since $\theta\overline{\chi}/\psi = \psi$ if and only if $\theta = \chi\psi^2$, the trace of the action of $\Delta_{N,1} W U^a$ on $\Omega^1[f]$ is

$$\sum_\psi \frac{\psi^{-1}(N)}{p-1} \lambda_p(f_\psi) \mathfrak{g}(\overline{\chi\psi^2}) \chi\psi^2(a) = \frac{\chi(a)}{p-1} \sum_\psi \psi\left(\frac{a^2}{N}\right) \lambda_p(f_\psi) \mathfrak{g}(\overline{\chi\psi^2}).$$

For the third statement, since $\phi(-1) = \chi(-1) = 1$, $-\phi(z) = -\phi(z^p) = \frac{1}{2}\mathrm{Tr}(D_{N,1} W \mid \Omega^1[f])$. As above, $e_\psi \mid \Delta_{N,1} W = \psi^{-1}(N)\lambda_p(f_\psi) e_{\overline{\chi}/\psi}$, so the trace is

$$\sum_{\psi = \overline{\psi}/\chi} \psi^{-1}(N)\lambda_p(f_\psi) = \sum_{\psi^2\chi = 1} \psi^{-1}(N)\lambda_p(f_\psi).$$

For the fourth statement, let $a = z^2$. Since $\chi(-1) = 1$, χ has two square roots $\alpha, \beta \in \mathcal{D}$. We already proved that $-\alpha(-a)\lambda_p(f_{\overline{\alpha}}) - \beta(-a)\lambda_p(f_{\overline{\beta}}) = 2\phi(z)$. Since $f_{\overline{\alpha}}, f_{\overline{\beta}} \in \mathcal{S}_2(\Gamma_0(p^2))$, $\lambda_p(f_{\overline{\alpha}})^2 = \lambda_p(f_{\overline{\beta}})^2 = 1$, and $(-\alpha(-a))^2 = (-\beta(-a))^2 = \chi(-a) = \chi(a)$. Thus $\alpha(-a)\lambda_p(f_{\overline{\alpha}})$ and $\beta(-a)\lambda_p(f_{\overline{\beta}})$ have the same square and their sum is not zero, so they are equal.

In particular, if $\chi = \mathbf{1}$, $\phi(z) = -\lambda(-a)\lambda_p(f_\lambda) = -\lambda_p(f)$, since λ and $\mathbf{1}$ are the two elements of $\mathcal{D}$ with square $\mathbf{1}$. The last point follows from the fact that $\lambda(a) = -1$ by definition of λ and a. □

Corollary 2.4.17

– *Let $(f,\mathbf{1}) \in \mathscr{S}$ and $\psi \in \mathcal{D}$. Then $\Omega^1[f,\psi]$ is (as a right $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-module) the dual (in the same sense as Definition 2.4.13) of a twisted Steinberg representation of central character ψ^2.*

– *Let $(f,\chi)\in\mathscr{P}$ and $\psi\in\mathcal{D}$. Then, in the same sense as above, $\Omega^1[f,\psi]$ is the dual of an irreducible principal series representation of $\mathrm{GL}_2(\mathbb{F}_p)$ with central character $\chi\psi^2$.*

Proof. – The claim about the central character is true by construction. Assume that $\Omega^1[f,\psi]$ (in either case) is not irreducible as a $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-module. Then it has an irreducible subrepresentation of dimension at most $\frac{p+1}{2}$. Since $\frac{p+1}{2}<p-1$, the description of irreducible representations of $\mathrm{GL}_2(\mathbb{F}_p)$ shows that this irreducible subrepresentation must be a line, which contradicts Corollary 2.4.6.

Thus $\Omega^1[f,\psi]$ is an irreducible right complex representation of $\mathrm{GL}_2(\mathbb{F}_p)$ of dimension p or $p+1$: it is thus the dual of a Steinberg representation, or of an irreducible principal series representation. □

2.5 Uniformizing u

Proposition 2.5.1 *Let us endow $X_1(p,\mu_p)^S_{\mathbb{C}}$ and $X(p,p)_{\mathbb{C}}$ with the analytifications defined in Propositions 2.3.1 and 2.4.1. Let $(\tau,b)\in\mathbb{H}\times\mathbb{F}_p^\times$. Then, for $x\in S$, the analytification of u_x maps $(\Gamma(p)\tau,b)$ to the following points:*

$$\begin{aligned} x=(t,1),\ t\in\mathbb{F}_p:&\quad u_x(\Gamma(p)\tau,b)=(\Gamma_1(p)T^{bt}\tau,b,x),\\ x=(1,0):&\quad u_x(\Gamma(p)\tau,b)=(\Gamma_1(p)\delta_b W\tau,b,x).\end{aligned}$$

Proof. – Let $t_0,b_0\in\mathbb{Z}$ lifting t,b. One has, using [86, (2.8.5.2)], with $\omega=e^{-\frac{2i\pi b}{p}}$,

$$\begin{aligned} u_{(t,1)}\left(\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\mathbb{Z}},\frac{b\tau}{p},\frac{1}{p}\right)&=\left(\omega,(t,1),\left(\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\mathbb{Z}},\frac{tb\tau+1}{p}\right)\right)\\ &=\left(\omega,(t,1),\left(\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus(t_0b_0\tau+1)\mathbb{Z}},\frac{b_0t_0\tau+1}{p}\right)\right)\\ &=\left(\omega,(t,1),\left(\frac{\mathbb{C}}{\tau'\mathbb{Z}\oplus\mathbb{Z}},\frac{1}{p}\right)\right),\quad \text{with } \tau'=\begin{pmatrix}1&0\\t_0b_0&1\end{pmatrix}\cdot\tau\in\mathbb{H},\\ u_{(1,0)}\left(\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\mathbb{Z}},\frac{b\tau}{p},\frac{1}{p}\right)&=\left(\omega,(1,0),\left(\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\mathbb{Z}},\frac{b\tau}{p}\right)\right)=\left(\omega,(1,0),\langle b\rangle\left(\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\mathbb{Z}},\frac{\tau}{p}\right)\right)\\ &=\left(\omega,(1,0),\langle b\rangle\left(\frac{\mathbb{C}}{\mathbb{Z}\oplus\tau^{-1}\mathbb{Z}},\frac{1}{p}\right)\right)=\left(\omega,(1,0),\langle b\rangle\left(\frac{\mathbb{C}}{-\tau^{-1}\mathbb{Z}\oplus\mathbb{Z}},\frac{1}{p}\right)\right)\\ &=\left(\omega,(1,0),\left(\frac{\mathbb{C}}{\tau'\mathbb{Z}\oplus\mathbb{Z}},\frac{1}{p}\right)\right),\quad \text{with } \tau'=\delta_b\begin{pmatrix}0&-1\\1&0\end{pmatrix}\cdot\tau.\end{aligned}$$

It is then straightforward to compare with the given analytifications. □

Corollary 2.5.2 *Let $u^{*,an}$ be the morphism such that the following diagram commutes (where $\mathcal{S}_2(\Gamma_1(p,\mu_p,S))$ is as in Proposition 2.3.5):*

$$\begin{array}{ccccccc} H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1) & \xrightarrow{\sim} & H^0(P(p)_{\mathbb{C}},\Omega^1) & \xrightarrow{u^*} & H^0(J(p,p),\Omega^1) & \xrightarrow{\sim} & H^0(X(p,p),\Omega^1)\\ \downarrow{\scriptstyle \iota_{1,p}} & & & & & & \downarrow{\scriptstyle \iota_{p,p}}\\ \mathcal{S}_2(\Gamma_1(p),\mathbb{F}_p^\times,S) & & \xrightarrow{\qquad\qquad u^{*,an}\qquad\qquad} & & & & \bigoplus_{b\in\mathbb{F}_p^\times}\mathcal{S}_2(\Gamma(p))\otimes\Delta_{b,1}\end{array}$$

Then $u^{*,an}$ commutes with the given actions of $\mathrm{GL}_2(\mathbb{F}_p)$ and is given by the following formulas:

$$(f,b,t) \in \mathcal{S}_2(\Gamma_1(p)) \times \mathbb{F}_p^\times \times \mathbb{F}_p : u^{*,an}(f \otimes [b] \otimes T^t) = \left(f \mid_2 T^{t/b}\right) \otimes \Delta_{b,1},$$
$$(f,b) \in \mathcal{S}_2(\Gamma_1(p)) \times \mathbb{F}_p^\times : u^{*,an}(f \otimes [b] \otimes W) = (\langle b^{-1}\rangle f) \mid_2 W) \otimes \Delta_{b,1}.$$

Proof. – By construction, for any $x \in S$, if the second row of $M \in \{T^t \mid t \in \mathbb{F}_p\} \cup \{W\}$ is not x, $u^{*,an}$ vanishes on $\mathcal{S}_2(\Gamma_1(p)) \otimes \mathbb{C}[\mathbb{F}_p^\times] \otimes [M]$. So what we need to show instead is that, for any $b \in \mathbb{F}_p^\times$:

$$(f,t) \in \mathcal{S}_2(\Gamma_1(p)) \times \mathbb{F}_p : u^*_{(t,1)}(\iota_{1,p}^{-1}(f \otimes [b] \otimes T^t)) = \iota_{p,p}^{-1}\left(\left(f \mid_2 T^{t/b}\right) \otimes \Delta_{b,1}\right),$$
$$f \in \mathcal{S}_2(\Gamma_1(p)) : u^*_{(1,0)}\left(f \otimes [b] \otimes W\right) = \iota_{p,p}^{-1}\left(((\langle b^{-1}\rangle f) \mid_2 W) \otimes \Delta_{b,1}\right).$$

For both identities, the differentials vanish on all the connected components of $X(p) \times \mathbb{F}_p^\times$ except on the b^{-1} component. Since the differentials are all holomorphic on $X(p)$, it is enough to show equality after pulling-back to $\mathbb{H}$ by $\tau \in \mathbb{H} \longmapsto (\Gamma(p)\tau, b^{-1})$.

Let $t \in \mathbb{F}_p$, and choose lifts $t_0, b_0 \in \mathbb{Z}$ of t, b such that $b_0 \mid t_0$. We then have on $\mathbb{H} \times \{b^{-1}\}$:

$$u^*_{(t,1)}(f(\tau)d\tau) = f(T^{t_0/b_0}\tau)d(T^{t_0/b_0}\tau) = (f \mid_2 T^{t_0/b_0})(\tau)d\tau,$$
$$u^*_{(1,0)}(f(\tau)d\tau) = f(\delta_{b^{-1}}W\tau)d(\delta_{b^{-1}}W\tau) = ((\langle b^{-1}\rangle f) \mid_2 W)(\tau)d\tau.$$

□

Corollary 2.5.3 *There is a commutative diagram of right $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules,*

$$\begin{array}{ccc} H^0(X_1(p,\mu_p)^S_{\mathbb{C}}, \Omega^1) & \xrightarrow{\quad u^* \quad} & H^0(X(p,p)_{\mathbb{C}}, \Omega^1) \\ \downarrow & & \downarrow \\ \mathcal{S}_2(\Gamma_1(p)) \otimes_{\mathbb{Z}[B \cap \mathrm{SL}_2(\mathbb{F}_p)]} \mathbb{Z}[\mathrm{GL}_2(\mathbb{F}_p)] & \longrightarrow & \mathcal{S}_2(\Gamma(p)) \otimes_{\mathbb{Z}[\mathrm{SL}_2(\mathbb{F}_p)]} \mathbb{Z}[\mathrm{GL}_2(\mathbb{F}_p)]. \end{array}$$

where the vertical arrows are isomorphisms, and the bottom arrow is the natural one (given by the inclusion $\mathcal{S}_2(\Gamma_1(p)) \subset \mathcal{S}_2(\Gamma(p))$).

Proof. – The obvious identification $\bigoplus_{b \in \mathbb{F}_p^\times} \mathcal{S}_2(\Gamma(p)) \otimes \Delta_{b,1} \simeq \mathcal{S}_2(\Gamma(p)) \otimes_{\mathbb{C}[\mathrm{SL}_2(\mathbb{F}_p)]} \mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$ is an isomorphism of $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules by definition of the action on the right-hand side, and we let the rightmost map in the diagram be precisely the composition of $\iota_{p,p}$ with this identification. On the other hand, we can identify $(\mathcal{S}_2(\Gamma_1(p)) \otimes \mathbb{C}[\mathbb{F}_p^\times]) \otimes_{\mathbb{C}[B]} \mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$ with $\mathcal{S}_2(\Gamma_1(p)) \otimes_{\mathbb{C}[B \cap \mathrm{SL}_2(\mathbb{F}_p)]} \mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$ as follows: we map $(f \otimes [b]) \otimes M$ to $f \otimes \Delta_{b,1}M$. This construction is well-defined, because if $M = \begin{pmatrix} a & * \\ 0 & d \end{pmatrix} M'$ (with $M, M' \in \mathrm{GL}_2(\mathbb{F}_p)$), then

$$(f \otimes [b]) \otimes M = ((f \otimes [b]) \mid \begin{pmatrix} a & * \\ 0 & d \end{pmatrix}) \otimes M' = ((\langle d\rangle f) \otimes [bad]) \otimes M'$$
$$f \otimes \Delta_{b,1}M = f \otimes \begin{pmatrix} ba & * \\ 0 & d \end{pmatrix} M' = f \otimes \begin{pmatrix} d^{-1} & * \\ 0 & d \end{pmatrix} \Delta_{bad,1}M' = (\langle d\rangle f) \mid \Delta_{bad,1}M'.$$

That this identification is $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-equivariant is then clear, and we let the leftmost vertical map be the composition of $\iota_{1,p}$ with this identification. Now, all we need to do is check that the diagram commutes, which is a direct consequence from the formulae in Corollary 2.5.2. □

Corollary 2.5.4 *The sequence*

$$H^0(P(p)_{\mathbb{C}},\Omega^1)\xrightarrow{R^*}H^0(P(p)_{\mathbb{C}},\Omega^1)\xrightarrow{u^*}H^0(J(p,p)_{\mathbb{C}},\Omega^1)$$

is exact. The image of u^* is exactly the sum of all the non-cuspidal irreducible $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-submodules of $H^0(J(p,p)_{\mathbb{C}},\Omega^1)$. In other words,

$$\operatorname{im}u^*\oplus\bigoplus_{(f,\chi)\in\mathscr{C}}\Omega^1[f]\simeq H^0(J(p,p)_{\mathbb{C}},\Omega^1).$$

Proof. – Let M be a right $\mathbb{C}[\mathrm{SL}_2(\mathbb{F}_p)]$-module and $M'=M\otimes_{\mathbb{C}[\mathrm{SL}_2(\mathbb{F}_p)]}\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$. For

$$m=\sum_{b\in\mathbb{F}_p^\times}m_b\otimes\Delta_{b,1}\in M',$$

one has $m\mid U=\sum_{b\in\mathbb{F}_p^\times}(m_b\mid U^b)\otimes\Delta_{b,1}$, so that

$$(M')^U=\bigoplus_{b\in\mathbb{F}_p^\times}M\otimes\Delta_{b,1}=M^U\otimes_{\mathbb{C}[B\cap\mathrm{SL}_2(\mathbb{F}_p)]}\mathbb{C}[B].$$

Therefore, by Corollary 2.5.3 and the discussion of irreducible representations of $\mathrm{GL}_2(\mathbb{F}_p)$ in Appendix B, the image of u^* is exactly the sum of all irreducible $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-submodules which are subquotients of principal series representations. By Corollaries 2.4.9, 2.4.12, 2.4.17, the image of u^* is the sum of the $\Omega^1[f,\psi]$ for $(f,\chi)\in\mathscr{S}\cup\mathscr{P}$ and $\psi\in\mathcal{D}$.

Let $(f,\chi)\in\mathscr{S}$ (resp. $(f,\chi)\in\mathscr{P}$) and $\psi\in\mathcal{D}$. Let $V_{f,\psi}$ be the $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-submodule of $H^0(P(p)_{\mathbb{C}},\Omega^1)$ where T'_ℓ (resp. $\langle n\rangle'$) acts by multiplication by $a_\ell(f)\psi(\ell)$ (resp. $\chi(n)\psi(n)^2$). Since R^* commutes to $\mathbb{T}'$ and $T'_\ell u=uT_\ell$, one has:

$$\Omega^1[f,\psi]\cap u^*H^0(P(p)_{\mathbb{C}},\Omega^1)=u^*V_{f,\psi},$$
$$V_{f,\psi}\cap R^*H^0(P(p)_{\mathbb{C}},\Omega^1)=R^*V_{f,\psi}.$$

It is thus enough to prove that $V_{f,\psi}\xrightarrow{R^*}V_{f,\psi}\xrightarrow{u^*}\Omega^1[f,\psi]$ is exact.

By Lemma 2.2.18, we know that the sequence is a complex of $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules. By Lemma 2.3.11, R^* is never trivial, and we saw that u^* was surjective. By Corollary 2.4.17, $\Omega^1[f,\psi]$ has length one as a $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-module. By Proposition 2.3.10, $V_{f,\psi}$ has length two as a $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-module, and the conclusion follows.

We already know that $u^*R^*=0$. To show exactness, we may reduce to subspaces where every T_ℓ and every m_n (resp. T'_ℓ, $\langle n\rangle'$) acts by a scalar. Then the relevant submodule of $H^0(J(p,p),\Omega^1)$ has length one over $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$, and is in the image of u^* by the above. But the image of R^* also has length at least one, and we saw that the relevant submodule of $H^0(P(p)_{\mathbb{C}},\Omega^1)$ had length two, whence the desired exactness. □

Corollary 2.5.5 *$H^0(X(p,p)_{\mathbb{C}},\Omega^1)$ is the direct sum of the following right $\mathbb{T}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules, on which every element of $\mathbb{T}$ acts as a scalar:*

- *For $(f,\mathbf{1})\in\mathscr{S}$, and $\psi\in\mathcal{D}$, $\Omega^1[f,\psi]$, which is isomorphic to the twisted Steinberg $\mathrm{St}^\vee_\psi$.*
- *For $(f,\chi)\in\mathscr{P}$ and $\psi\in\mathcal{D}$, modulo the relation $(f,\psi)\sim(\overline{f},\chi\psi)$, $\Omega^1[f,\psi]$, which is isomorphic to the irreducible principal series $\pi(\psi,\chi\psi)^\vee$,*
- *For $(f,\chi)\in\mathscr{C}$, $\Omega^1[f]$ which is the irreducible cuspidal representation $C_f^\vee$.*

In all these cases (with $\chi=\mathbf{1}$ in the first one, and $\psi=\mathbf{1}$ in the last one), the operator T_n acts on the submodule as the scalar $a_n(f)\psi(n)$, and m_n acts by the scalar $\psi(n)^2\chi(n)$.

Proof. – By Corollary 2.5.4 and Proposition 2.3.10, since the action of $\mathbb{T}$ is diagonalizable, $H^0(X(p,p)_{\mathbb{C}},\Omega^1)$ is the direct sum of the $\Omega^1[f]$ for $(f,\chi)\in\mathscr{C}$ and of the images under u^* of the $H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)[f,\psi]$ for $(f,\chi)\in\mathscr{S}\cup\mathscr{P}$ and $\psi\in\mathcal{D}$, modulo the relation $(f,\chi,\psi)\sim(\overline{f},\overline{\chi},\chi\psi)$. The action of $\mathbb{T}$ is given by Corollary 2.4.11.

By Corollaries 2.4.17 and 2.5.4, $\Omega^1[f,\psi]$ is an irreducible quotient of $H^0(X_1(p,\mu_p)^S_{\mathbb{C}},\Omega^1)[f,\psi]$, isomorphic to a twisted Steinberg if $\chi=\mathbf{1}$ and an irreducible principal series otherwise. By Proposition 2.3.10, $\Omega^1[f,\psi]$ is isomorphic to $\mathrm{St}^\vee_\psi$ if $\chi=\mathbf{1}$ and $\pi(\psi,\chi\psi)^\vee$ otherwise (since $\pi(\chi\psi,\psi)$ and $\pi(\psi,\chi\psi)$ are isomorphic $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules). □

2.6 Connected components of $C(p)$ and $\ker R$

Definition 2.6.1 By Proposition 2.2.13, there exists a unique morphism $v:P(p)\to J(p,p)$ of abelian schemes which commutes to the action of $\mathrm{GL}_2(\mathbb{F}_p)$ and such that the morphism $v\circ[(\iota_{(0,1)})_*]:J_1(p,\mu_p)\to J(p,p)$ is exactly $u^*_{(0,1)}$. We write $q=u\circ v$: it is a $\mathrm{GL}_2(\mathbb{F}_p)$-endomorphism of $P(p)$. We denote by $\Delta:P(p)\to P(p)$ the sum of the $\langle n\rangle$.

Lemma 2.6.2 *Let $x,y\in S$. The morphism*

$$J_1(p,\mu_p)\xrightarrow{[(\iota_x)_*]}P(p)\xrightarrow{q}P(p)\xrightarrow{\iota_y^*}J_1(p,\mu_p)$$

is given by:

- *when $x=y$, it is multiplication by p,*
- *when $x\neq y$ and $(1,0)\in\{x,y\}$, it is w_pU_p,*
- *when $x=(s,1),y=(t,1)$ with $s\neq t$, it is $\langle s-t\rangle w_pU_p$.*

In particular, q commutes with Δ.

Proof. – First assume that $x=(0,1)$. When $y=(0,1)$, the morphism is exactly $[u_{(0,1)}]_*u^*_{(0,1)}$, where $u_{(0,1)}:X(p,p)\to X_1(p,\mu_p)$ is a morphism of smooth proper connected curves (over $\mathbb{Z}[1/p]$). By considering its complex analytification from Proposition 2.5.1, $u_{(0,1)}$ has degree p, so that $[u_{(0,1)}]_*u^*_{(0,1)}$ is exactly the multiplication by p.

When $y=(t,1)$ (resp. $y=(1,0)$ and $t=1$), the morphism is exactly $[(u_y)_*]u^*_{(0,1)}$. Consider the following diagram:

$$\begin{array}{ccccc}
X_1(p,\mu_p) & \xleftarrow[u_{(0,1)}]{} & X(p,p) & \xrightarrow{u_y} & X_1(p,\mu_p)\\
\downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle w_p\langle t\rangle^{-1}}\\
X_1(p,\mu_p) & \xleftarrow[D'_{1,1}]{} & X(\Gamma'_1(p,p),\mu_p) & \xrightarrow{D'_{p,1}} & X'_1(p,\mu_p).
\end{array}$$

In this diagram, α is the compactification of the map

$$(E,P,Q)\longmapsto(E,Q,\langle P+t^{-1}Q\rangle,\langle P,\,Q\rangle)\ (\text{resp. }(E,P,Q)\longmapsto(E,Q,\langle P\rangle,\langle P,\,Q\rangle)).$$

It is then direct (using Section 1.1.3, [86, (2.8.2),(2.8.6.1)], and the fact that $\langle -1\rangle$ is trivial) that the diagram commutes away from the cusps with α being an isomorphism, hence, by Proposition A.2.9, the diagram commutes with α being an isomorphism. By Proposition A.4.25, $[(u_y)_*]u^*_{(0,1)}=[((w_p\langle t\rangle^{-1})^{-1})_*]U_p=\langle t\rangle w_pU_p$.

To describe the other coordinates, use the above and notice that the following diagrams

commute (since q is $\mathrm{GL}_2(\mathbb{F}_p)$-equivariant and $\langle -1\rangle$ is trivial), for $s,t\in\mathbb{F}_p$:

$$\begin{array}{ccccccc} J_1(p,\mu_p) & \xrightarrow{[(\iota_{(t,1)})_*]} & P(p) & \xrightarrow{q} & P(p) & \xrightarrow{\iota^*_{(s,1)}} & J_1(p,\mu_p) \\ & \searrow^{\iota} & \uparrow{\scriptstyle T^{-t}} & & \uparrow{\scriptstyle T^{-t}} & \nearrow_{\alpha} & \\ & & P(p) & \xrightarrow{q} & P(p) & & \end{array}$$

$$\begin{array}{ccccccc} J_1(p,\mu_p) & \xrightarrow{[(\iota_{(1,0)})_*]} & P(p) & \xrightarrow{q} & P(p) & \xrightarrow{\iota^*_{(s,1)}} & J_1(p,\mu_p) \\ & \searrow^{\iota} & \uparrow{\scriptstyle W} & & \uparrow{\scriptstyle W} & \nearrow_{\beta} & \\ & & P(p) & \xrightarrow{q} & P(p) & & \end{array}$$

$$\begin{array}{ccccccc} J_1(p,\mu_p) & \xrightarrow{[(\iota_{(1,0)})_*]} & P(p) & \xrightarrow{q} & P(p) & \xrightarrow{\iota^*_{(1,0)}} & J_1(p,\mu_p) \\ & \searrow^{\iota} & \uparrow{\scriptstyle W} & & \uparrow{\scriptstyle W} & \nearrow_{\gamma} & \\ & & P(p) & \xrightarrow{q} & P(p) & & \end{array}$$

where $\alpha=\iota^*_{(s,1)}\circ(T^t)^*=\iota^*_{(s-t,1)}$, $\beta=\iota^*_{(s,1)}\circ(W^{-1})^*=\langle s\rangle\iota^*_{(-1/s,1)}$, and $\gamma=\iota^*_{(1,0)}\circ(W^{-1})^*=\iota^*_{(0,1)}$ and $\iota=[(\iota_{(0,1)})_*]$. □

Lemma 2.6.3 *The uniformization of the automorphism w_p of $X_1(p,\mu_p)$ is given by*

$$(\Gamma_1(p)\tau,b)\longmapsto(\delta_b\Gamma_1(p)\begin{pmatrix}0&-1\\p&0\end{pmatrix}\tau,b).$$

Proof. – Let $\tau\in\mathbb{H}$. Then (τ,b) corresponds to the class of $\left(\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\mathbb{Z}},\frac{1}{p},e^{-2i\pi b/p}\right)$. Let $E=\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\mathbb{Z}}$ and $\pi:E\to E'$ the isogeny whose kernel is $\langle\frac{1}{p}\rangle$. Thus $w_p(\tau,b)$ is the class of the enriched elliptic curve $\left(\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\frac{1}{p}\mathbb{Z}},\pi(Q),e^{-2i\pi b/p}\right)$, where $Q\in E(\mathbb{C})$ is any p-torsion point such that $\langle\frac{1}{p},Q\rangle_{E[p]}=\langle\frac{1}{p},\pi(Q)\rangle_{\pi}=e^{-2i\pi b/p}$. Thus $Q=\frac{-b\tau}{p}$ works, so that $w_p(\tau,b)$ represents the enriched elliptic curve

$$\begin{aligned}\left(\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\frac{1}{p}\mathbb{Z}},\frac{-b\tau}{p},e^{-2i\pi b/p}\right)&\simeq\left(\frac{\mathbb{C}}{\mathbb{Z}\oplus\frac{1}{p\tau}\mathbb{Z}},\frac{-b}{p},e^{-2i\pi b/p}\right)\\&\simeq\left(\frac{\mathbb{C}}{\frac{-1}{p\tau}\mathbb{Z}\oplus\mathbb{Z}},-b\frac{1}{p},e^{-2i\pi b/p}\right)\simeq\langle b\rangle\left(\frac{\mathbb{C}}{\frac{-1}{p\tau}\mathbb{Z}\oplus\mathbb{Z}},\frac{1}{p},e^{-2i\pi b/p}\right),\end{aligned}$$

whence the conclusion. □

Lemma 2.6.4 *The pull-back by U_p on $H^0(J_1(p,\mu_p)_{\mathbb{C}},\Omega^1)\overset{\iota_{1,p}}{\simeq}\mathcal{S}_2(\Gamma_1(p))\otimes\mathbb{C}[\mathbb{F}_p^\times]$ is exactly the classical Hecke operator U_p.*

Proof. – By the proof of Proposition 2.6.2, $U_p=w_p[(u_{(1,0)})_*]u^*_{(0,1)}$ We proceed as in the proof of Proposition 2.4.7. Consider the following diagram:

$$\begin{array}{ccccccc} \mathbb{H}\times\mathbb{F}_p^\times & \xleftarrow[h]{} & \mathbb{H}\times\mathbb{F}_p^\times & \xrightarrow{(g_w)_w} & \coprod_{0\le w<p}\mathbb{H}\times\mathbb{F}_p^\times & \xrightarrow{h'} & \mathbb{H}\times\mathbb{F}_p^\times \\ \downarrow{\scriptstyle \upsilon} & & & \searrow^{\upsilon} & \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\upsilon} \\ Y_1(p,\mu_p)_{\mathbb{C}} & & \xleftarrow[w_pu_{1,0}]{} & & Y(p,p)_{\mathbb{C}} & \xrightarrow{u_{(0,1)}} & Y(p,p)_{\mathbb{C}} \end{array}$$

where $h(\tau,z)=(\frac{\tau}{p},z)$, $h'(\tau,z)=(\tau,z)$, π maps (τ,z) on the copy w of $\mathbb{H}\times\mathbb{F}_p^\times$ to the class of the enriched elliptic curve $\left(\frac{\mathbb{C}}{\tau\mathbb{Z}\oplus\mathbb{Z}},\frac{z(\tau+w)}{p},\frac{1}{p}\right)$, and $g_w(\tau,z)=(\tau-w,z)$.

By Proposition 2.5.1 and Lemma 2.6.3, and, since, for suitable choices of $M,M'\in SL_2(\mathbb{Z})$ congruent to $\Delta_{b^{-1},b}$ mod p, $M\begin{pmatrix}0&-1\\p&0\end{pmatrix}M'\begin{pmatrix}0&-1\\1&0\end{pmatrix}=\begin{pmatrix}1&0\\0&p\end{pmatrix}$, the diagram commutes. Moreover, this diagram is Cartesian above a suitable co-finite open subscheme of $Y_1(p,\mu_p)$.

Therefore, for $(f,b)\in\mathcal{S}_2(\Gamma_1(p))\times\mathbb{F}_p^\times$, one has

$$U_p^*(\iota_{1,p}(f\otimes[b]))=\iota_{1,p}^{-1}\left[\sum_{0\le w<p}f\mid\begin{pmatrix}1&0\\0&p\end{pmatrix}\begin{pmatrix}1&w\\0&1\end{pmatrix}\otimes[b]\right]=\iota_{1,p}^{-1}(U_p(f)\otimes[b]),$$

whence the conclusion. □

Corollary 2.6.5 *The endomorphism $(w_pU_p+1)\Delta$ of $P(p)$ vanishes.*

Proof. – It is enough to show that $(w_pU_p+1)\Delta$ is the null endomorphism of $J_1(p,\mu_p)_{\mathbb{Q}}$ (since this morphism preserves the summands of $P(p)$), and this is equivalent to the fact that the pull-back by $\Delta(w_p+U_p)$ is the trivial endomorphism of $H^0(J_1(p,\mu_p)_{\mathbb{C}},\Omega^1)\overset{\iota_{1,p}}{\simeq}\mathcal{S}_2(\Gamma_1(p))\otimes\mathbb{C}[\mathbb{F}_p^\times]$.

By Proposition 2.3.5, Δ^* acts on $\mathcal{S}_2(\Gamma_1(p))\otimes\mathbb{C}[\mathbb{F}_p^\times]$ as the sum of all the classical diamond operators of $\mathcal{S}_2(\Gamma_1(p))$: thus $\frac{\Delta^*}{p-1}$ is a projection on the subspace $\mathcal{S}_2(\Gamma_0(p))\otimes\mathbb{C}[\mathbb{F}_p^\times]$. Therefore, by Lemma 2.6.3 $w_p^*\Delta^*$ is exactly the composition of Δ^* with the action of $\begin{pmatrix}0&-1\\p&0\end{pmatrix}$.

Thus, by Lemmas 2.6.3, 2.6.4, for every $f\in\mathcal{S}_2(\Gamma_0(p))$, one has

$$(w_p^*+U_p^*)(f\otimes[b])=\left(\sum_{i=0}^{p-1}f\mid\begin{pmatrix}1&i\\0&p\end{pmatrix}+\begin{pmatrix}0&-1\\p&0\end{pmatrix}\right)\otimes[b]:=g\otimes[b].$$

We can check that $\begin{pmatrix}0&-1\\p&0\end{pmatrix}=\begin{pmatrix}1&0\\0&p\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ and the $\begin{pmatrix}1&i\\0&p\end{pmatrix}$ (for $0\le i<p$) form representatives for $\Gamma_0(p)\backslash\Gamma_0(p)\begin{pmatrix}1&0\\0&p\end{pmatrix}\Gamma(1)$, since $\Gamma_0(p)\mathrm{diag}(1,p)\Gamma(1)=\begin{pmatrix}1&0\\0&p\end{pmatrix}\Gamma(1)$. Thus $g\in\mathcal{S}_2(\Gamma(1))=\{0\}$, whence the conclusion. □

Proposition 2.6.6 *There exists an endomorphism r of $P(p)$ commuting with Δ such that $q-(2p-\Delta)=r\circ R$.*

Proof. – We define r such that for any $x,y\in S$, the morphism

$$J_1(p,\mu_p)\overset{[(\iota_x)_*]}{\to}P(p)\overset{r}{\to}P(p)\overset{\iota_y^*}{\to}J_1(p,\mu_p)$$

is equal to

- $w_p\Delta$ when $x=y$,
- $-w_p$ when $x\neq y$ and one of them is $(1,0)$,
- $-\langle s-t\rangle w_p$ when $x=(s,1),y=(t,1)$ with distinct $s,t\in\mathbb{F}_p$.

It is clear that r commutes with Δ.

Given distinct $s, t \in \mathbb{F}_p$,

$$\begin{aligned}
&\iota_{(t,1)}^* \circ r \circ R \circ [(\iota_{(s,1)})_*] \\
&= (-w_p)w_p + (-\langle s-t\rangle w_p)(-U_p) + (w_p\Delta)(\langle s-t\rangle w_p) + \sum_{x\neq s,t} (-\langle t-x\rangle w_p)\langle x-s\rangle w_p \\
&= \langle s-t\rangle w_p U_p + w_p\Delta w_p - 1 - \sum_{x\neq s,t} \langle \frac{t-x}{x-s}\rangle \\
&= \langle s-t\rangle w_p U_p + \Delta - 1 - (\Delta - \langle -1\rangle) = \langle s-t\rangle w_p U_p = \iota_{(t,1)}^* \circ q \circ [(\iota_{(s,1)})_*].
\end{aligned}$$

If $s \in \mathbb{F}_p$,

$$\begin{aligned}
\iota_{(s,1)}^* \circ r \circ R \circ [(\iota_{(1,0)})_*] &= (-w_p)(-U_p) + (w_p\Delta)w_p + \sum_{t\neq s} (-\langle t-s\rangle w_p)w_p = w_pU_p + \Delta - \Delta \\
&= w_pU_p = \iota_{(s,1)}^* \circ q \circ [(\iota_{(1,0)})_*], \\
\iota_{(1,0)}^* \circ r \circ R \circ [(\iota_{(s,1)})_*] &= (w_p\Delta)w_p + (-w_p)(-U_p) + \sum_{t\neq s} (-w_p)(\langle s-t\rangle w_p) \\
&= \Delta + w_pU_p - \sum_{t\neq s} \langle (t-s)^{-1}\rangle = w_pU_p = \iota_{(1,0)}^* \circ q \circ [(\iota_{(s,1)})_*], \\
\iota_{(s,1)}^* \circ r \circ R \circ [(\iota_{(s,1)})_*] &= (-w_p)(w_p) + (w_p\Delta)(-U_p) + \sum_{t\neq s} (-\langle t-s\rangle w_p)(\langle t-s\rangle w_p) \\
&= -p - \Delta = \iota_{(s,1)}^* \circ q \circ [(\iota_{(s,1)})_*] - (2p-\Delta), \\
\iota_{(1,0)}^* \circ r \circ R \circ [(\iota_{(1,0)})_*] &= (w_p\Delta)(-U_p) + \sum_{t\in\mathbb{F}_p} (-w_p)w_p = \Delta - p \\
&= \iota_{(1,0)}^* \circ q \circ [(\iota_{(1,0)})_*] - (2p-\Delta).
\end{aligned}$$

□

Corollary 2.6.7 *The following identities hold:* $(2p-\Delta)q = q^2$, $q \circ r \circ R = r \circ R \circ q = 0$. *Moreover, for any field k with characteristic not dividing p,* $\operatorname{im} q_k$ *has finite index in* $\ker R_k$, *and* $(2p-\Delta)\pi_0(\ker q_k) = (2p-\Delta)\pi_0(\ker R_k) = 0$.

Proof. – Since $R \circ q = R \circ u \circ v = 0$, one has $\operatorname{im}(q_k) \subset \ker R_k$ for any field k with characteristic not dividing p. In particular, $(q - (2p-\Delta))q = r \circ R \circ q = 0$. Moreover, if $y \in \ker R(\overline{k})$, then $q(y) - (2p-\Delta)y = r(R(y)) = 0$, hence $(2p-\Delta)y \in \operatorname{im} q(\overline{k})$. Thus $(2p-\Delta)\ker R_k \subset \operatorname{im} q_k$. Since $\Delta^2 = (p-1)\Delta$, one has $(p+1+\Delta)(2p-\Delta) = 2p(p+1)$ so $2p(p+1)\ker R_k \subset \operatorname{im} q_k$. Thus, $\operatorname{im} q_k$ is the connected component of unity in $\ker R_k$. Since $(2p-\Delta)\ker R_k \subset \operatorname{im} q_k$, we have $(2p-\Delta)\pi_0(\ker R_k) = 0$.

q commutes with Δ, so $0 = q^2 - (2p-\Delta)q = q^2 - q(2p-\Delta) = q \circ r \circ R$. By Proposition 2.6.6, over any field k with characteristic not dividing p, $(2p-\Delta)\ker q_k = (r \circ R)(\ker q_k) \subset \operatorname{im} r_k \circ R_k$. Since $2p(p+1)$ is a multiple of $2p-\Delta$ (so that $2p-\Delta : P(p)_k \to P(p)_k$ is surjective), $\operatorname{im} r_k \circ R_k$ is the connected component of unity of $\ker q_k$, and we are done. □

Corollary 2.6.8 *Over any field k whose characteristic is not p, the exponents of* $\pi_0(\ker u_k)$, $\pi_0(\ker q_k)$, $\pi_0(\ker R_k)$ *divide* $2p(p+1)$.

Proof. – $\operatorname{im} q$ and $\operatorname{im} u$ are abelian subvarieties of $P(p)$, contained with finite index in $\ker R$, so they are equal. Thus, $\operatorname{im} v + \ker u = J(p,p)$. Since the neutral component $(\ker u)^0$ of $\ker u$ has finite index in $\ker u$, $\operatorname{im} v + (\ker u)^0$ contains a multiple of $\operatorname{im} v + \ker u$, so that $\operatorname{im} v + (\ker u)^0 = J(p,p)$. Consequently, $v : \pi_0(\ker q) \to \pi_0(\ker u)$ is surjective. It is thus enough, by the previous Corollary, to show that $2p(p+1) \in \operatorname{End}(P(p))(2p-\Delta)$ (as endomorphisms of $P(p)$), which is true since $2p(p+1) = (p+1+\Delta)(2p-\Delta)$. □

Chapter 3

Tate modules for the Jacobian of $X(p,p)$ and its twists

3.1 Introduction

The purpose of this section is to compute the Tate modules of $J(p,p)$ and $P(p)$, as well as that Jacobians of Galois twists of $X(p,p)$ or $X_1(p,\mu_p)^S$, as a $\mathbb{T}[G_{\mathbb{Q}}]$-module (or $\mathbb{T}'[G_{\mathbb{Q}}]$-module). To this effect, we first describe the Tate modules of $J(p,p)$ (resp. $P(p)$) as $\mathbb{T}[G_{\mathbb{Q}} \times \mathrm{GL}_2(\mathbb{F}_p)]$-modules (resp. $\mathbb{T}'[G_{\mathbb{Q}} \times \mathrm{GL}_2(\mathbb{F}_p)]$), and prove that the general case follows from Proposition A.4.39.

We use the letter $\mathcal{T}$ to denote Tate modules, in order to distinguish them from Hecke operators. In this section and the following ones, ω_p will always denote the mod p cyclotomic character.

Notation *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a newform with primitive character χ. Let F be a number field containing the coefficients of f and $\mathfrak{l}$ be a prime ideal of $\mathcal{O}_F$ with residue characteristic ℓ. Let $T_{f,\mathfrak{l}}$ be a continuous representation $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{F_\mathfrak{l}})$ satisfying the following properties:*

- *$T_{f,\mathfrak{l}}$ is unramified at every prime number $q \nmid N\ell$,*
- *$\det T_{f,\mathfrak{l}} = \chi(\omega_N)\omega^{k-1}$, where ω_N (resp. ω) is the mod N cyclotomic character (resp. the ℓ-adic cyclotomic character),*
- *If $q \nmid \ell N$ is a prime, the characteristic polynomial of the arithmetic Frobenius at q is $X^2 - a_q(f)X + q^{k-1}\chi(q)$,*
- *$V_{f,\mathfrak{l}} := T_{f,\mathfrak{l}} \otimes_{\mathcal{O}_{F_\mathfrak{l}}} F_\mathfrak{l}$ is absolutely irreducible (by [132, Theorem 2.3] when $k \geq 2$ and by [37, Théorème 4.1] when $k = 1$ – see also [37, Théorème 6.1, Remarque 6.5]).*

In particular, while all possible choices for $T_{f,\mathfrak{l}}$ need not be isomorphic over $\mathcal{O}_{F_\mathfrak{l}}$, it is the case for $V_{f,\mathfrak{l}}$.

The determination of the Tate module of $P(p)$ can be easily reduced to that of $J_1(p)$, whose structure is well-known. Recall the following notations from Section 2.

Notation

- *$\mathcal{D}$ denotes the set of Dirichlet characters $(\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$,*
- *$\mathscr{S}$ denotes the set of $(f, \mathbf{1})$ where $f \in \mathcal{S}_2(\Gamma_0(p))$ is a newform,*
- *$\mathscr{P}$ denotes the set of (f,χ), where $f \in \mathcal{S}_2(\Gamma_1(p))$ is a newform with character $\chi \neq \mathbf{1}$,*
- *$\mathscr{C}$ denotes the set of (f,χ), where $f \in \mathcal{S}_2(\Gamma_1(p) \cap \Gamma_0(p^2))$ is a newform with character $\chi \in \mathcal{D}$, and such that no twist of f by a character in $\mathcal{D}$ has conductor p.*
- *For $\alpha \in \mathcal{D}$, St_α is the Steinberg representation of $\mathrm{GL}_2(\mathbb{F}_p)$ twisted by $\alpha(\det)$.*
- *For $\alpha, \beta \in \mathcal{D}$, $\pi(\alpha,\beta)$ is the principal series representation of $\mathrm{GL}_2(\mathbb{F}_p)$ attached to the pair of characters $\{\alpha,\beta\}$.*
- *By Definition 2.4.13, we can attach to any $(f,\chi) \in \mathscr{C}$ a cuspidal representation of $\mathrm{GL}_2(\mathbb{F}_p)$ named C_f.*

We fix, in this introduction, a number field $F \subset \mathbb{C}$ which is Galois over $\mathbb{Q}$ and contains:

- the $p(p^2-1)(p-1)$-th roots of unity (so that any representation of $\mathrm{GL}_2(\mathbb{F}_p)$ can be realized over F),
- the coefficients of every newform of weight 2, level dividing p^2, and character of conductor dividing p,
- for every newform $f \in \mathcal{S}_2(\Gamma_0(p^2))$ with complex multiplication (necessarily by the quadratic imaginary field $K := \mathbb{Q}(\sqrt{-p})$), for every prime number ℓ split in K, the roots of the polynomial $X^2 - a_\ell(f)X + \ell$.

Theorem 3.A *(Proposition 3.2.2) Let $\mathfrak{l} \subset \mathcal{O}_F$ be a maximal ideal with residue characteristic ℓ. There is an isomorphism of $(\mathbb{T} \otimes_{\mathbb{Z}} F_{\mathfrak{l}})[G_{\mathbb{Q}} \times \mathrm{GL}_2(\mathbb{F}_p)]$-modules:*

$$\mathcal{T}_\ell P(p) \otimes_{\mathbb{Z}_\ell} F_{\mathfrak{l}} \to \bigoplus_{\substack{(f,\chi)\in\mathscr{S}\cup\mathscr{P} \\ \psi\in\mathcal{D}}} V_{f\otimes\psi,\mathfrak{l}} \otimes \pi(\psi,\psi\chi).$$

On the factor attached to $((f,\chi),\psi) \in (\mathscr{S}\cup\mathscr{P})\times\mathcal{D}$, the Hecke operator T_n (resp. $\langle n\rangle$) for $n \geq 1$ coprime to p acts by multiplication by $a_n(f)$ (resp. $\chi(n)$).

The case of $J(p,p)$ (as an Abelian variety over $\mathbb{Q}$) also seems known, as a similar claim is made in [163], but we keep to a classical language and our argument seems somewhat different. Since $J(p,p)(\mathbb{C})$ is a complex torus, we can relate its singular cohomology to $H^0(J(p,p)(\mathbb{C}),\Omega^1)$ (for the left and right $\mathbb{T}[\mathrm{GL}_2(\mathbb{F}_p)]$-module structures). Using the results of the previous Chapter, we can determine $H_1(X(p,p)(\mathbb{C}),\mathbb{C})$ as a $\mathbb{T}[\mathrm{GL}_2(\mathbb{F}_p)]$-module. Determining the structure of the Tate module of $J(p,p)$ then amounts to studying the action of $G_{\mathbb{Q}}$, which is given by the Eichler-Shimura relation (Corollary 1.5.16).

Theorem 3.B *(Corollary 3.4.4) Let $\mathfrak{l} \subset \mathcal{O}_F$ be a maximal ideal with residue characteristic ℓ. Then, as a $(\mathbb{T}\otimes F_{\mathfrak{l}})[G_{\mathbb{Q}}\times\mathrm{GL}_2(\mathbb{F}_p)]$-module, $\mathcal{T}_\ell J(p,p)\otimes_{\mathbb{Z}_\ell} F_{\mathfrak{l}}$ is isomorphic to the direct sum of the following modules:*

- *for each $((f,\mathbf{1}),\psi) \in \mathscr{S}\times\mathcal{D}$, a copy of $V_{f\otimes\psi,\mathfrak{l}}\otimes\mathrm{St}_\psi$, on which, for any $n\geq 1$ coprime to p, T_n (resp. nI_2) acts by $a_n(f)\psi(n)$ (resp. $\psi(n)^2$),*
- *for each $((f,\chi),\psi) \in \mathscr{P}\times\mathcal{D}$ modulo the relation $((f,\chi),\psi) \sim ((\overline{f},\overline{\chi}),\chi\psi)$, a copy of $V_{f\otimes\psi,\mathfrak{l}}\otimes\pi(\psi,\psi\chi)$, on which on which, for any $n\geq 1$ coprime to p, T_n (resp. nI_2) acts by $a_n(f)\psi(n)$ (resp. $\psi(n)^2\chi(n)$),*
- *for each $(f,\chi)\in\mathscr{C}$, a copy of $V_{f,\mathfrak{l}}\otimes C_f$, on which, for any $n\geq 1$ coprime to p, T_n (resp. nI_2) acts by $a_n(f)$ (resp. $\chi(n)$),*

A consequence of this result is the description of the Tate module of any Galois twist of $J(p,p)$, also studied by Virdol (his result is reproduced in the general Introduction as Theorem J), but our classical statement seems more explicit.

Corollary 3.C *(Corollary 3.4.9) Let k be a field of characteristic distinct from p and separable closure k_s. Let F be a large enough number field, $\mathfrak{l}\subset\mathcal{O}_L$ be a maximal ideal with residue characteristic ℓ invertible in k. Let $\rho:\mathrm{Gal}(k_s/k)\to\mathrm{GL}_2(\mathbb{F}_p)$ be a continuous group homomorphism. Then, as a $(\mathbb{T}\otimes_{\mathbb{Z}} F_{\mathfrak{l}})[G_k]$-module, $\mathcal{T}_\ell\mathrm{Jac}(X(p,p)_\rho)\otimes_{\mathbb{Z}_\ell}F_{\mathfrak{l}}$ is isomorphic to the direct sum of*

- *for each $((f,\mathbf{1}),\psi)\in\mathscr{S}\times\mathcal{D}$, a copy of $\psi(\omega_p\det\rho)\otimes V_{f,\mathfrak{l}}\otimes\mathrm{St}(\rho)$, on which, for any $n\geq 1$ coprime to p, T_n (resp. nI_2) acts by $a_n(f)\psi(n)$ (resp. $\psi(n)^2$),*
- *for each $((f,\chi),\psi)\in\mathscr{P}\times\mathcal{D}$ modulo the relation $((f,\chi),\psi)\sim((\overline{f},\overline{\chi}),\chi\psi)$, a copy of $\psi(\omega_p\det\rho)\otimes V_{f,\mathfrak{l}}\otimes(\pi(1,\chi)(\rho))$, on which, for any $n\geq 1$ coprime to p, T_n (resp. nI_2) acts by $a_n(f)\psi(n)$ (resp. $\psi(n)^2\chi(n)$),*
- *for each $(f,\chi)\in\mathscr{C}$, a copy of $V_{f,\mathfrak{l}}\otimes C_f(\rho)$, on which, for any $n\geq 1$ coprime to p, T_n (resp. nI_2) acts by $a_n(f)$ (resp. $\chi(n)$).*

When we twist $X(p,p)$ by a Galois representation ρ coming from the p-torsion from an elliptic curve E over some field k (with separable closure k_s and of characteristic distinct from p), or more generally when $\det\rho$ is the inverse of the mod p cyclotomic character, Proposition 1.4.10 implies that the twist $X(p,p)_\rho$ is the disjoint reunion of the $p-1$ smooth projective geometrically connected curves $X_{E[p],a}(p)$ over k (where a runs through $\mathbb{F}_p^\times$), or in general $X_{\rho,\xi}(p)$, when ξ runs through $\mu_p^\times(k_s)$. The remainder of the section is dedicated to the computation of the Tate modules of the Jacobians of these curves.

First, we have to restrict the Hecke algebra $\mathbb{T}$ acting on $J(p,p)$ (hence on $\mathrm{Jac}(X(p,p)_\rho)$) to a certain sub-algebra. Let $\mathbb{T}_1$ denote the subalgebra of $\mathbb{T}$ generated by the $(mI_2)\cdot T_n$ where $n,m\geq 1$ are integers such that $nm^2\equiv 1 \pmod p$. The endomorphism of $J(p,p)_\rho$ induced by $a\in\mathbb{T}_1$ factors as a direct sum of $a_\xi\in\mathrm{End}(\mathrm{Jac}(X_{\rho,\xi}(p)))$ (over $\xi\in\mu_p^\times(k_s)$).

Theorem 3.D *(Corollary 3.6.26) Let ℓ be a prime number and $\mathfrak{l}$ be a prime ideal of $\mathcal{O}_F$ of residue characteristic ℓ. Let $\rho:G_\mathbb{Q}\to\mathrm{GL}_2(\mathbb{F}_p)$ such that $\det\rho=\omega_p^{-1}$. Let $\iota:\overline{\mathbb{Q}}\to k_s$ be a ring homomorphism, inducing a continuous group homomorphism $R_\iota:\mathrm{Gal}(k_s/k)\to\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.*

For $\xi\in\mu_p^\times(k_s)$, $\mathcal{T}_\ell J_{\rho,\xi}(p)\otimes_{\mathbb{Z}_\ell}F_\mathfrak{l}$ is isomorphic as a $(\mathbb{T}_1\otimes F_\mathfrak{l})[G_\mathbb{Q}]$-module to the direct sum of the following factors:

- *$V_{f,\mathfrak{l}}\otimes\mathrm{St}(\rho)$ for every $(f,\chi)\in\mathscr{S}$,*
- *$V_{f,\mathfrak{l}}\otimes\pi(1,\chi)(\rho)$ for every $(f,\chi)\in\mathscr{P}$ modulo complex conjugation,*
- *$V_{f,\mathfrak{l}}\otimes C_f(\rho)$ for every $(f,\chi)\in\mathscr{C}$ modulo twists by characters in $\mathcal{D}$ and such that f does not have complex multiplication,*
- *for every $(f,\chi)\in\mathscr{C}$ modulo twists by characters in $\mathcal{D}$ such that f has complex multiplication, $\mathrm{Ind}_{G_{\mathbb{Q}(\sqrt{-p})}}^{G_\mathbb{Q}}\psi_{f,\mathfrak{l}}\otimes C^+(\rho_{|G_{\mathbb{Q}(\sqrt{-p})}})$, where $\psi_{f,\mathfrak{l}}:G_{\mathbb{Q}(\sqrt{-p})}\to F_\mathfrak{l}^\times$ is one of the CM characters attached to f (which one is selected depends only on ξ) and C^+ is a cuspidal representation of $\mathbb{F}_p^\times\,\mathrm{SL}_2(\mathbb{F}_p)$ defined in Section B.4.*

On every summand, the Hecke operator $(mI_2)\cdot T_n\in\mathbb{T}_1$ (for $n,m\geq 1$ such that $nm^2\equiv 1 \pmod p$) acts by multiplication by $a_n(f)\chi(m)$.

We stated the result for the base field $\mathbb{Q}$, but the body of this Chapter contains a similar version of this result which is valid for an arbitrary base field k. Let us briefly discuss its proof.

When ρ is surjective, this corresponds exactly to the decomposition into irreducible factors of the Tate module of $\mathrm{Jac}(X(p,p)_\rho)$ (by Corollary 3.C and the results of Section 3.5), so the proof is easier. In order to deal with general ρ, we need a stronger version of Theorem 3.D, supplied by Corollary 3.6.18, which keeps track of the action of $\mathrm{SL}_2(\mathbb{F}_p)$. This action preserves the connected components, but is not defined over $\mathbb{Q}$ any more.

The argument for any field k of characteristic zero then works as follows: consider an elliptic curve $E_0/\mathbb{Q}$ with surjective attached Galois representation $\rho_0:G_\mathbb{Q}\to\mathrm{GL}_2(\mathbb{F}_p)$ (given by a basis (P,Q) of its p-torsion and $\xi_0=\langle P,Q\rangle_{E[p]}$). Then $X_{\rho,\xi}(p)$ is a twist of $X_{\rho_0,\xi_0}(p)_k$ by the Galois cocycle $\rho\rho_0^{-1}:\mathrm{Gal}(k_s/k)\to\mathrm{SL}_2(\mathbb{F}_p)$ (where a common choice of embedding $\overline{\mathbb{Q}}\to\overline{k}$ defines a homomorphism $\mathrm{Gal}(\overline{k}/k)\to G_\mathbb{Q}$ and identifies $\mu_p^\times(\overline{\mathbb{Q}})$ with $\mu_p^\times(\overline{k})$). By keeping track the action over $\overline{\mathbb{Q}}$ of $\mathrm{SL}_2(\mathbb{F}_p)$ on all components on $X_{E_0[p],a}(p)$ (or equivalently on the $X_{\rho_0,\xi_0}(p)$), we are able to describe both the action of $G_\mathbb{Q}$ and that of $\mathrm{SL}_2(\mathbb{F}_p)$ on the Tate module of $X_{\rho,\xi}(p)$.

For fields of positive characteristic, the same argument shows that it is enough to establish the stronger version of Theorem 3.D for one representation ρ_0 over the prime field, and we choose one representation ρ_0 which lifts to characteristic zero, in which case the result is already known by specialization[1]. The existence of the curves $X_G(p)$ over rings of mixed characteristic is crucial to this part of the argument.

[1]I am grateful to Anna Cadoret for her answers to my questions regarding this theory.

3.2 The Tate module of $P(p)$

Lemma 3.2.1 *There is an isomorphism of $\mathbb{Z}[\mathrm{GL}_2(\mathbb{F}_p) \times G_{\mathbb{Q}}]$-modules*

$$I : \mathbb{Z}[\mathrm{GL}_2(\mathbb{F}_p)] \otimes_{\mathbb{Z}[B]} (\mathbb{Z}[\mathbb{F}_p^\times] \otimes J_1(p)(\overline{\mathbb{Q}})) \to P(p)(\overline{\mathbb{Q}}),$$

such that:

- $M = \begin{pmatrix} a & * \\ 0 & d \end{pmatrix}$ *acts on $\mathbb{Z}[\mathbb{F}_p^\times] \otimes J_1(p)(\overline{\mathbb{Q}})$ by $\underline{ad} \otimes \langle d \rangle$, where $\underline{ad} \in \mathrm{End}(\mathbb{Z}[\mathbb{F}_p^\times])$ is the morphism $[b] \longmapsto [bad]$.*
- *$\sigma \in G_{\mathbb{Q}}$ acts on $\mathbb{Z}[\mathbb{F}_p^\times] \otimes J_1(p)(\overline{\mathbb{Q}})$ by the tensor product of $\underline{\omega_p(\sigma)}$ and its standard action.*
- *For any $M \in \mathrm{GL}_2(\mathbb{F}_p)$, $a \in \mathbb{F}_p^\times$, $f \in J_1(p)(\overline{\mathbb{Q}})$, $\ell \neq p$ prime, and $n \in \mathbb{F}_p^\times$, one has*

$$I(M \otimes [a] \otimes (T_\ell f)) = T_\ell(M \otimes [a] \otimes f), \quad I(M \otimes [a] \otimes (\langle n \rangle f)) = \langle n \rangle (M \otimes [a] \otimes f).$$

Proof. – By Proposition 2.2.13, it is enough to construct an isomorphism of $\mathbb{Z}[G_{\mathbb{Q}}]$-modules $\mathbb{Z}[\mathbb{F}_p^\times] \otimes J_1(p)(\overline{\mathbb{Q}}) \to J_1(p, \mu_p)(\overline{\mathbb{Q}})$ respecting the T_ℓ, the $\langle n \rangle$, and mapping $\underline{a} \in \mathrm{End}(\mathbb{Z}[\mathbb{F}_p^\times])$ to $\underline{a} \in \mathrm{End}(\mu_p^\times)$.

By Proposition A.4.28, we have an identification of functors $J_1(p, \mu_p)(-) \simeq J_1(p)(- \times_{\mathbb{Z}[1/p]} \mu_p^\times)$ (valued in Abelian groups), where $\mu_p^\times$ is the affine scheme with coordinate ring $\mathbb{Z}[p^{-1}, \zeta_p]$. This identification is natural, so it commutes with Hecke and diamond operators. Moreover, by Proposition A.4.32, the following diagram commutes for any $\mathbb{Q}$-algebra R and any $a \in \mathbb{F}_p^\times$:

$$\begin{array}{ccc} J_1(p, \mu_p)(R) & \xrightarrow{\simeq} & J_1(p)(R \otimes \mathbb{Q}(\mu_p)) \\ \downarrow{\scriptstyle \underline{a}} & & \downarrow{\scriptstyle \underline{a}^{-1}} \\ J_1(p, \mu_p)(R) & \xrightarrow{\simeq} & J_1(p)(R \otimes \mathbb{Q}(\mu_p)) \end{array}$$

Therefore, it is enough to find an isomorphism $\iota : \mathbb{Z}[\mathbb{F}_p^\times] \to J_1(p)(\overline{\mathbb{Q}}) \to J_1(p)(\overline{\mathbb{Q}} \otimes \mathbb{Q}(\mu_p))$ such that the following diagram commutes for each $a \in \mathbb{F}_p^\times$ and each $\sigma \in G_{\mathbb{Q}}$:

$$\begin{array}{ccc} J_1(p)(\overline{\mathbb{Q}} \otimes \mathbb{Q}(\mu_p)) & \xrightarrow{\iota} & \mathbb{Z}[\mathbb{F}_p^\times] \otimes J_1(p)(\overline{\mathbb{Q}}) \\ \downarrow{\scriptstyle \sigma \otimes \underline{a}^{-1}} & & \downarrow{\scriptstyle \underline{a\omega_p(\sigma)} \otimes \sigma} \\ J_1(p)(\overline{\mathbb{Q}} \otimes \mathbb{Q}(\mu_p)) & \xrightarrow{\iota} & \mathbb{Z}[\mathbb{F}_p^\times] \otimes J_1(p)(\overline{\mathbb{Q}}) \end{array}$$

To define this automorphism, we will work in slightly greater generality so as to make the argument clearer. Write $K = \mathbb{Q}(\mu_p)$, $\Gamma = \mathrm{Gal}(K/\mathbb{Q})$, $J = J_1(p)_{\mathbb{Q}}$ and fix an embedding $j : K \to \overline{\mathbb{Q}}$. This defines a group homomorphism of $q : G_{\mathbb{Q}} \to \Gamma$ (when K is a general finite Galois extension of $\mathbb{Q}$, q is only defined up to conjugacy; here, it is absolute, but it is easier to pretend for a while that it isn't). Let $\pi : \overline{\mathbb{Q}} \otimes K \to \overline{\mathbb{Q}}^\Gamma$ such that for each $g \in \Gamma$, $(x, y) \in \overline{\mathbb{Q}} \times K$, $\pi(x \otimes y)(g) = x \cdot j(g(y))$. Then we have the following relations:

$$\pi(x \otimes g(y))(h) = \pi(x \otimes y)(hg),\ \pi(\sigma(x) \otimes y)(g) = \sigma(\pi(x \otimes y)(q(\sigma)^{-1} g)).$$

There is an obvious isomorphism of Abelian groups $\lambda : J(\overline{\mathbb{Q}}^\Gamma) \to \mathbb{Z}[\Gamma] \otimes J(\overline{\mathbb{Q}})$ mapping a point $x \in J(\overline{\mathbb{Q}}^\Gamma)$ to the sum over $g \in \Gamma$ of the $[g] \otimes p_g(x)$, where p_g denotes the projection $\overline{\mathbb{Q}}^\Gamma \to \overline{\mathbb{Q}}$. For any $\sigma \in G_{\mathbb{Q}}$ and $\gamma \in \Gamma$, for any $x \in J(\overline{\mathbb{Q}} \otimes K)$, one has

$$\lambda(\pi((\sigma\otimes\gamma)(x))) = \sum_{h\in\Gamma}[h]\otimes p_h(\pi(\sigma\otimes\gamma)(x)) = \sum_{h\in\Gamma}[h]\otimes\sigma(p_{q(\sigma)^{-1}h\gamma}(\pi(x)))$$
$$= \sum_{h\in\Gamma}[q(\sigma)h\gamma^{-1}]\otimes\sigma(p_h(\pi(x))) = (\mathbf{L}_{q(\sigma)}\mathbf{R}_{\gamma^{-1}}\otimes\sigma)(\lambda(\pi(x))),$$

where $\mathbf{L},\mathbf{R}$ denote the left and right translations on $\mathbb{Z}[\Gamma]$, which pairwise commute. Then $\iota=\lambda\circ\pi$ satisfies the conditions. □

Proposition 3.2.2 *Let ℓ be a prime number and F be a finite extension of $\mathbb{Q}_\ell$ containing all the $(p-1)$-th roots of unity and the coefficients of every newform in $\mathcal{S}_2(\Gamma_1(p))$. Let $\mathfrak{l}$ be the maximal ideal of $\mathcal{O}_F$. We then have an isomorphism of $(\mathbb{T}\otimes_{\mathbb{Z}}F)[G_{\mathbb{Q}}\times\mathrm{GL}_2(\mathbb{F}_p)]$-modules:*

$$\mathcal{T}_\ell P(p)\otimes_{\mathbb{Z}_\ell}F \to \bigoplus_{\substack{(f,\chi)\in\mathscr{S}\cup\mathscr{P}\\ \psi\in\mathcal{D}}} V_{f\otimes\psi,\mathfrak{l}}\otimes\pi(\psi,\psi\chi).$$

On the factor attached to $((f,\chi),\psi)$, T_q (resp. $\langle n\rangle$) acts by $a_q(f)$ (resp. $\chi(n)$).

Proof. – This follows from the previous Lemma and the description of the Tate module of $J_1(p)$ as given by [136, Theorem 5.12] (note the discussion of *loc.cit.* below Definition 5.6; *loc.cit.* does not discuss basic facts about the action of Hecke operators on classical modular forms, which can be found in [41, Chapter 5]). □

3.3 The singular homology of $J(p,p)$

Proposition 3.3.1 *Let A be a (not necessarily commutative) ring acting on some complex torus J. Assume that $H^0(J,\Omega^1)\simeq\bigoplus_i M_i$, where each M_i is a $\mathbb{C}$-vector space on which A acts on the right. Then*

$$H_1(J,\mathbb{C})\simeq\bigoplus_i \mathrm{Hom}_{\mathbb{C}}(M_i,\mathbb{C})\oplus\mathrm{Hom}_{\mathbb{C}}(\overline{M_i},\mathbb{C}),$$

where $\overline{M}:=M\otimes_{\mathbb{C}}\mathbb{C}$, $\mathbb{C}\to\mathbb{C}$ being the complex conjugation.

Proof. – We can write $J=V/\Lambda$, where V is a complex vector space and $\Lambda\subset V$ is a closed discrete subgroup with $V\simeq\Lambda\otimes_{\mathbb{Z}}\mathbb{R}$. Then A acts on Λ and V by group homomorphisms and $\mathbb{C}$-linear maps, and one has, as $A\otimes\mathbb{C}$-modules, one has the following isomorphisms:

$$H_1(J,\mathbb{C})\simeq\Lambda\otimes_{\mathbb{Z}}\mathbb{C}\simeq(\Lambda\otimes_{\mathbb{Z}}\mathbb{R})\otimes_{\mathbb{R}}\mathbb{C}\simeq V\otimes_{\mathbb{R}}\mathbb{C}\simeq V\oplus\overline{V}$$
$$H^0(J,\Omega^1)\simeq\mathrm{Hom}_{\mathbb{C}}(V,\mathbb{C}),$$

The conclusion is then formal. □

Corollary 3.3.2 *The $(\mathbb{T}\otimes\mathbb{C})[\mathrm{GL}_2(\mathbb{F}_p)]$-module $H_1(X(p,p)(\mathbb{C}),\mathbb{C})$ decomposes as the direct sum of two copies of the following $(\mathbb{T}\otimes\mathbb{C})[\mathrm{GL}_2(\mathbb{F}_p)]$-modules:*

- *for each $((f,\mathbf{1}),\psi)\in\mathscr{S}\times\mathcal{D}$, a copy of St_ψ, where T_ℓ acts by $\psi(\ell)a_\ell(f)$,*
- *for each $((f,\chi),\psi)\in\mathscr{P}\times\mathcal{D}$ modulo the relation $(f,\chi,\psi)\sim(\overline{f},\overline{\chi},\psi\chi)$, a copy of $\pi(\psi,\psi\chi)$, where T_ℓ acts by $a_\ell(f)\psi(\ell)$,*
- *for each $(f,\chi)\in\mathscr{C}$, a module isomorphic to C_f, where T_ℓ acts by $a_\ell(f)$.*

Proof. – By Corollary 2.5.5, for each $((f,\chi),\psi)\in(\mathscr{S}\cup\mathscr{P})\times\mathcal{D}$ (resp. $(f,\chi)\in\mathscr{C}$), there is a ring homomorphism $\mu_{f,\psi}:\mathbb{T}\to\mathbb{C}$ (resp. $\mu_f:\mathbb{T}\to\mathbb{C}$) such that

$$\mu_{f,\psi}(T_\ell)=a_\ell(f)\psi(\ell) \qquad (\text{ resp. } \mu_f(T_\ell)=a_\ell(f))$$
$$\mu_{f,\psi}(nI_2)=\chi(n)\psi^2(n) \qquad (\text{ resp. } \mu_f(nI_2)=\chi(n))$$

For each $((f,\chi),\psi) \in (\mathscr{S} \cup \mathscr{P}) \times \mathcal{D}$ (resp. $(f,\chi) \in \mathscr{C}$), let $M_{f,\psi}$ (resp. M_f) be the $(\mathbb{T} \otimes \mathbb{C})[\mathrm{GL}_2(\mathbb{F}_p)]$ which is isomorphic over $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$ to St_ψ if $\chi = \mathbf{1}$ and $\pi(\psi, \chi\psi)$ otherwise (resp. C_f) and on which $\mathbb{T}$ acts through the character $\mu_{f,\psi}$ (resp. μ_f). In particular, $M_{f,\psi}$ and $M_{\overline{f},\chi\psi}$ are isomorphic, and the complex conjugate of $M_{f,\psi}$ (resp. M_f) is $M_{\overline{f},\overline{\psi}}$ (resp. $M_{\overline{f}}$).

By Corollary 2.5.5, $H^0(X(p,p)(\mathbb{C}), \Omega^1) \simeq H^0(J(p,p)(\mathbb{C}), \Omega^1)$ is isomorphic to

$$\left(\bigoplus_{\psi \in \mathcal{D}} {\bigoplus_{(f,\chi) \in \mathscr{S} \cup \mathscr{P}}}' \mathrm{Hom}(M_{f,\psi}, \mathbb{C}) \right) \oplus \bigoplus_{(f,\chi) \in \mathscr{C}} \mathrm{Hom}(M_f, \mathbb{C})$$

as a right $(\mathbb{T} \otimes \mathbb{C})[\mathrm{GL}_2(\mathbb{F}_p)]$-module, where the $'$ means that for each $(f,\chi) \in \mathscr{P}$, we choose exactly one element in $\{(f,\chi), (\overline{f}, \overline{\chi})\}$ to count in the sum (this choice being consistent for all ψ). The conclusion follows from Proposition 3.3.1. □

3.4 The Tate module of twists of $J(p,p)$

Lemma 3.4.1 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a normalized newform with weight $k \geq 2$ and character χ. Let $\mathbb{Q}(\chi) \subset F \subset \mathbb{C}$ be a number field containing the coefficients of f, ℓ a prime number and $\mathfrak{l} \subset \mathcal{O}_F$ a prime ideal of residue characteristic ℓ. Let V be a continuous two-dimensional representation of $G_\mathbb{Q}$ with coefficients in $F_\mathfrak{l}$ such that*

- *V is unramified at all but finitely many primes,*
- *for all but finitely many primes q, the endomorphism $\mathrm{Frob}_q^2 - a_q(f)\mathrm{Frob}_q + q^{k-1}\chi(q)$ of V vanishes, where Frob_q is the arithmetic Frobenius.*

Then V is isomorphic to $V_{f,\mathfrak{l}}$.

Proof. – For each $\sigma \in G_\mathbb{Q}$, denote by P_σ (resp. Q_σ) be the characteristic polynomial of $\sigma \in \mathrm{End}_{F_\mathfrak{l}}(V_{f,\mathfrak{l}})$ (resp. $\sigma \in \mathrm{End}_{F_\mathfrak{l}}(V)$). Given $\sigma \in G_\mathbb{Q}$, we denote by $V(\sigma)$ the endomorphism of V induced by σ.

Now, $\sigma \longmapsto P_\sigma$ and $\sigma \longmapsto Q_\sigma$ are continuous maps. Whenever σ is an arithmetic Frobenius, the assumption implies that $P_\sigma(V(\sigma)) = 0$: by Cebotarev, $P_\sigma(V(\sigma)) = 0$ for each $\sigma \in G_\mathbb{Q}$.

Let $S \leq G_\mathbb{Q}$ be the subgroup of σ such that $V(\sigma)$ is scalar, and $T \leq G_\mathbb{Q}$ be the subgroup of elements σ such that $\det(\sigma \mid V_{f,\mathfrak{l}}) = \det(\sigma \mid V)$. If $\sigma \in G_\mathbb{Q} \backslash S$, the gcd R of P_σ and Q_σ is such that $R(V(\sigma)) = 0$. Since $V(\sigma)$ is not scalar, R must have degree two, so $P_\sigma = Q_\sigma$ and $\sigma \in T$. Hence $G_\mathbb{Q}$ is the reunion of the two closed subgroups S and T, so $G_\mathbb{Q} \in \{S, T\}$.

Let us prove that $G_\mathbb{Q} \neq S$. Assume, for the sake of contradiction, that $G_\mathbb{Q} = S$: in this case, there is a character $\psi : G_\mathbb{Q} \to F_\mathfrak{l}^\times$ corresponding to V, so that, for all $\sigma \in G_\mathbb{Q}$, $\psi(\sigma)$ is a root of P_σ. Let $V' := V_{f,\mathfrak{l}} \otimes \psi^{-1}$: then V' is irreducible and 1 is an eigenvalue of every $V'(\sigma)$ for $\sigma \in G_\mathbb{Q}$. Let $\mathbb{Q}^{ab}$ denote the maximal abelian extension of $\mathbb{Q}$: every $\sigma \in G_{\mathbb{Q}^{ab}}$ acts on V' with determinant 1, so acts unipotently on V'.

Let us prove that V' has a line stable under $G_{\mathbb{Q}^{ab}}$. If it is not the case, there exists $\sigma, \tau \in G_{\mathbb{Q}^{ab}}$ such that $\ker(V'(\sigma) - \mathrm{id}), \ker(V'(\tau) - \mathrm{id})$ are distinct lines. Then, in a suitable basis of V', the matrices of σ, τ are $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$ for some $a, b \in F_\mathfrak{l}^\times$. Then the trace of $V'(\sigma\tau)$ is $2 + ab$, so $\sigma\tau \in G_{\mathbb{Q}^{ab}}$ does not act unipotently on V', whence a contradiction.

So V' contains a line stable under $G_{\mathbb{Q}^{ab}}$: since each $\sigma \in G_{\mathbb{Q}^{ab}}$ acts unipotently on V', $(V')^{G_{\mathbb{Q}^{ab}}}$ is nonzero. Since V' is irreducible, one has $(V')^{G_{\mathbb{Q}^{ab}}} = V'$, so the action of $G_\mathbb{Q}$ on V' is abelian: this contradicts our original assumption, namely that $G_\mathbb{Q} = S$.

Therefore, $G_\mathbb{Q} = T$. Let $\sigma \in G_\mathbb{Q}$, then $(P_\sigma - Q_\sigma) \in K \cdot X$ vanishes when evaluated at $V(\sigma)$, so $P_\sigma = Q_\sigma$. Therefore, since $V_{f,\mathfrak{l}}$ is absolutely irreducible, one has

$$\dim_{F_\mathfrak{l}} \mathrm{Hom}_{F_\mathfrak{l}}(V, V_{f,\mathfrak{l}}) = \dim_{\overline{F_\mathfrak{l}}} \mathrm{Hom}_{\overline{F_\mathfrak{l}}}(V \otimes_{F_\mathfrak{l}} \overline{F_\mathfrak{l}}, V_{f,\mathfrak{l}} \otimes_{F_\mathfrak{l}} \overline{F_\mathfrak{l}}) \geq 1,$$

so there is a nonzero morphism of $F_\mathfrak{l}[G_\mathbb{Q}]$-modules $f : V \to V_{f,\mathfrak{l}}$. Since $V_{f,\mathfrak{l}}$ is irreducible, f is an isomorphism and we are done. □

Notation *From now on, $F \subset \mathbb{C}$ denotes a number field which is Galois over $\mathbb{Q}$ and contains the $p(p-1)^2(p+1)$-th roots of unity and the Fourier coefficients of the newforms in $\mathcal{S}_2(\Gamma_1(p))$ or $\mathcal{S}_2(\Gamma_1(p) \cap \Gamma_0(p^2))$.*

Proposition 3.4.2 *Let ℓ be a prime number and $\mathfrak{l}$ be a prime ideal of $\mathcal{O}_F$ dividing (ℓ). Then $\mathcal{T}_\ell J(p,p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is the direct sum of its eigenspaces for $\mathbb{T}$, which are stable under $G_\mathbb{Q} \times \mathrm{GL}_2(\mathbb{F}_p)$, and are of the following form:*

- *For each $((f,\mathbf{1}),\psi) \in \mathscr{S} \times \mathcal{D}$, a $2p$-dimensional $F_\mathfrak{l}$-vector space on which any T_n acts by $a_n(f)\psi(n)$ (with $n \geq 1$ prime to p), which is isomorphic over $F_\mathfrak{l}[\mathrm{GL}_2(\mathbb{F}_p)]$ to the direct sum of two copies of St_ψ, and over $F_\mathfrak{l}[G_\mathbb{Q}]$ to the sum of p copies of $V_{f\otimes\psi,\mathfrak{l}}$.*
- *For each $((f,\chi),\psi) \in \mathscr{P} \times \mathcal{D}$ modulo the relation $(f,\chi,\psi) \sim (\overline{f},\overline{\chi},\chi\psi)$, a $2(p+1)$-dimensional $F_\mathfrak{l}$-vector space where any T_n acts by $a_n(f)\psi(n)$ (with $n \geq 1$ coprime to p) which is isomorphic over $F_\mathfrak{l}[\mathrm{GL}_2(\mathbb{F}_p)]$ to the direct sum of two copies of $\pi(\psi,\psi\chi)$ and over $F_\mathfrak{l}[G_\mathbb{Q}]$ to the sum of $p+1$ copies of $V_{f\otimes\psi,\mathfrak{l}}$.*
- *For each $f \in \mathscr{C}$, a $2(p-1)$-dimensional vector space where any T_n acts by $a_n(f)$ (with $n \geq 1$ coprime to p) which is isomorphic over $F_\mathfrak{l}[\mathrm{GL}_2(\mathbb{F}_p)]$ to the direct sum of two copies of C_f, and over $F_\mathfrak{l}[G_\mathbb{Q}]$ to the sum of $p-1$ copies of $V_{f,\mathfrak{l}}$.*

Proof. – As a $(\mathbb{T}\otimes F_\mathfrak{l})[\mathrm{GL}_2(\mathbb{F}_p)]$-module, $\mathcal{T}_\ell J(p,p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is isomorphic to $H_1(J(p,p)(\mathbb{C}),F_\mathfrak{l})$. Now, the $\mu_{f,\psi},\mu_f$ (resp. $M_{f,\psi},M_f$) defined in the proof of Corollary 3.3.2 are in fact characters $\mathbb{T} \to F$ (resp. can be defined as modules over $F[\mathrm{GL}_2(\mathbb{F}_p)]$). An easy induction shows that for any $n \geq 1$ coprime to p, $\mu_f(T_n) = a_n(f)$ (resp. $\mu_{f,\psi}(n) = a_n(f)\psi(n)$).

Let us fix a system of representatives $\mathscr{P}'$ for $\mathscr{S} \cup \mathscr{P}$ modulo the complex conjugation. Then $H_1(J(p,p)(\mathbb{C}),F)$ and

$$\left(\bigoplus_{((f,\chi),\psi)\in\mathscr{P}'\times\mathcal{D}} M_{f,\psi} \oplus \bigoplus_{(f,\chi)\in\mathscr{C}} M_f\right)^{\oplus 2}$$

are two $(\mathbb{T}\otimes F)[\mathrm{GL}_2(\mathbb{F}_p)]$-modules that are isomorphic after the base change $F \to \mathbb{C}$, so they are isomorphic. Therefore, one has the isomorphism of $(\mathbb{T}\otimes F_\mathfrak{l})[\mathrm{GL}_2(\mathbb{F}_p)]$-modules

$$\mathcal{T}_\ell J(p,p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l} \simeq \left(\bigoplus_{((f,\chi),\psi)\in\mathscr{P}'\times\mathcal{D}} M_{f,\psi}^{\oplus 2} \oplus \bigoplus_{(f,\chi)\in\mathscr{C}} M_f^{\oplus 2}\right) \otimes_F F_\mathfrak{l}.$$

Since every factor is the eigenspace of some character $\mathbb{T} \to F$, every summand in this decomposition is stable under $G_\mathbb{Q}$.

Let $(f,\chi) \in \mathscr{C}$. The eigenspace $T[f]$ of $T := \mathcal{T}_\ell J(p,p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ for the character μ_f has dimension $2(p-1)$ and is endowed with a continuous action of $\mathrm{GL}_2(\mathbb{F}_p) \times G_\mathbb{Q}$; it is isomorphic over $F_\mathfrak{l}[\mathrm{GL}_2(\mathbb{F}_p)]$ to two copies of C_f. By Proposition B.3.6, for every character $\psi \in \mathcal{D}$, the submodule $T[f,\psi_D]$ of $T[f]$ on which each $\Delta_{a,b}$ (for $a,b \in \mathbb{F}_p^\times$) acts by $\chi(a)\psi(a)\overline{\psi(b)}$ is two-dimensional, stable under $G_\mathbb{Q}$, and $T[f]$ is the direct sum of the $T[f,\psi_D]$.

Now, $T[f,\psi_D]$ is a continuous two-dimensional representation of $G_\mathbb{Q}$ over $F_\mathfrak{l}$. By the Eichler-Shimura relation (Corollary 1.5.16), for any prime $q \nmid p\ell$, the polynomial $X^2 - a_q(f)X + q\chi(q)$ vanishes at the arithmetic Frobenius Frob_q. By Lemma 3.4.1, $T[f,\psi_D]$ is isomorphic to $V_{f,\mathfrak{l}}$ as a $F_\mathfrak{l}[G_\mathbb{Q}]$-module.

Let now $((f,\chi),\psi) \in \mathscr{P}' \times \mathcal{D}$. The eigenspace $T[f,\psi]$ of T for the character $\mu_{f,\psi}$ has dimension $2p$ (or $2(p+1)$ if $\chi \neq \mathbf{1}$) and is endowed with a continuous action of $\mathrm{GL}_2(\mathbb{F}_p) \times G_\mathbb{Q}$; it is isomorphic over $F_\mathfrak{l}[\mathrm{GL}_2(\mathbb{F}_p)]$ to the direct sum of two copies of St_ψ (or $\pi(\psi,\psi\chi)$ if $\chi \neq \mathbf{1}$). By the Eichler-Shimura relation (Corollary 1.5.16), $\mathrm{Frob}_q^2 - a_q(f)\psi(q)\mathrm{Frob}_q + q\chi(q)\psi(q)^2 = 0$ for

each prime $q \nmid p\ell$, so, by Lemma 3.4.1, we are done if we can show that $T[f,\psi]$ is the direct sum of two-dimensional representations of $G_{\mathbb{Q}}$.

In the case of St_ψ, by Lemma B.3.1, we can take the eigenspaces of $T[f,\psi]$ for the action of $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

In the case of $\pi(\psi,\psi\chi)$, let $g \in \mathrm{GL}_2(\mathbb{F}_p)$ be the generator of a Cartan subgroup. For any $1 \leq k \leq p$, g^k is diagonalizable with eigenvalues in $\mathbb{F}_{p^2}\backslash\mathbb{F}_p$, so is not conjugate to any element of B: by [142, §7.2 Proposition 20], it acts on $\pi(\psi,\psi\chi)$ with trace 0. On the other hand, g^{p+1} is a scalar matrix equal to λI_2 for some $\lambda \in \mathbb{F}_p^\times$, hence the eigenvalues of the action of g on $\pi(\psi,\psi\chi)$ are exactly the $(p+1)$-th roots of $(\chi\psi^2)(\lambda)$, each one with multiplicity one. Therefore, $T[f,\psi]$ is the direct sum of the eigenspaces for the action of g, which all have dimension two and are stable under $G_{\mathbb{Q}}$. □

Lemma 3.4.3 *Let V be a finite-dimensional vector space over some non-Archimedean local field K, endowed with continuous K-linear actions of two profinite groups G, H such that*

- *the actions of G and H commute,*
- *there exists finite-dimensional K-vector spaces A, B endowed with K-linear continuous actions of G and H respectively, with A (resp. B) being absolutely irreducible over G (resp. H), such that $V_{|G}$ (resp. $V_{|H}$) is isomorphic to a direct sum of copies of A (resp. B).*

Then there is an isomorphism of $K[G\times H]$-modules $V \simeq (A\otimes B)^{\oplus d}$ for some $d \geq 1$.

Proof. – Let $W \subset V$ be a sub-$K[H]$-module isomorphic to B. Then $U = \mathrm{Hom}_{K[H]}(W,V)$ is a finite-dimensional K-vector space on which G acts (through its action on V). We have a natural evaluation morphism $\epsilon : U \otimes_K W \to V$ which is $K[G\times H]$-linear. Since $V_{|H}$ is a direct sum of copies of W, ϵ is surjective.

Since B is absolutely irreducible, it satisfies Schur's Lemma. Therefore, $\dim_K U = \frac{\dim V}{\dim W}$, so ϵ is a linear surjective morphism between finite dimensional K-vector spaces, so it is an isomorphism.

Now, it is enough to show that U is isomorphic as a $K[G]$-module to a direct sum of copies of A. This is direct, since $U \otimes W_{|G} \simeq V_{|G}$, and $W_{|G}$ is trivial, while $V_{|G}$ is a direct sum of copies of the absolutely irreducible $K[G]$-module A. □

Corollary 3.4.4 *Let ℓ be a prime number and $\mathfrak{l}$ be a prime ideal of $\mathcal{O}_F$ with residue characteristic ℓ. Then $\mathcal{T}_\ell J(p,p)\otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is isomorphic to the direct sum of the following $(\mathbb{T}\otimes F_\mathfrak{l})[G_{\mathbb{Q}}\times\mathrm{GL}_2(\mathbb{F}_p)]$-submodules:*

- *for each $((f,\mathbf{1}),\psi) \in \mathscr{S}\times\mathscr{D}$, a copy of $V_{f\otimes\psi,\mathfrak{l}}\otimes\mathrm{St}_\psi$, on which, for any $n\geq 1$ coprime to p, T_n (resp. nI_2) acts by $a_n(f)\psi(n)$ (resp. $\psi(n)^2$),*
- *for each $((f,\chi),\psi) \in \mathscr{P}\times\mathscr{D}$ modulo the relation $((f,\chi),\psi) \sim ((\overline{f},\overline{\chi}),\chi\psi)$, a copy of $V_{f\otimes\psi,\mathfrak{l}}\otimes\pi(\psi,\psi\chi)$, on which on which, for any $n\geq 1$ coprime to p, T_n (resp. nI_2) acts by $a_n(f)\psi(n)$ (resp. $\psi(n)^2\chi(n)$),*
- *for each $(f,\chi)\in\mathscr{C}$, a copy of $V_{f,\mathfrak{l}}\otimes C_f$, on which, for any $n\geq 1$ coprime to p, T_n (resp. nI_2) acts by $a_n(f)$ (resp. $\chi(n)$),*

Remark It seems interesting to study the integral behavior of the decomposition when $\ell = p$.

More precisely, one can consider the following situation. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_F$ dividing p. Fix $((f,\chi),\psi)\in(\mathscr{S}\cup\mathscr{P})\times\mathcal{D}$: the largest quotient $\mathcal{T}_{f,\psi}$ of $\mathcal{T}_pJ(p,p)\otimes_{\mathbb{Z}_p}\mathcal{O}_{F_\mathfrak{p}}$ on which $\mathbb{T}$ acts by the character $\mu_{f,\psi}$ is a free $\mathcal{O}_{F_\mathfrak{p}}$-module of rank $2p$ (or $2(p+1)$ when χ is nontrivial), which is (after tensoring with $\mathbb{Q}$) the direct sum of two copies of St_ψ (or $\pi(\psi,\psi\chi)$). But what is its isomorphism class as a $\mathcal{O}_{F_\mathfrak{p}}$-module?

Fix a uniformizer ϖ for $F_\mathfrak{p}$. When χ is trivial, p is not an Eisenstein prime by [111, II (9.7), (14.2)], so $T_{f,\mathfrak{p}}/\varpi$ is absolutely irreducible. Therefore, the isomorphism class of $T_{f,\mathfrak{p}}$ as a

$\mathcal{O}_{F_\mathfrak{p}}[G_\mathbb{Q}]$-module is well-defined. Similarly, St_ψ/ϖ is absolutely irreducible, so there is a unique (up to isomorphism) $\mathcal{O}_{F_\mathfrak{p}}[\mathrm{GL}_2(\mathbb{F}_p)]$-module which is free of rank p over $\mathcal{O}_{F_\mathfrak{p}}$ and isomorphic to St_ψ over $F_\mathfrak{p}$.

Using the absolute irreducibilities on both sides, one can check that $\mathcal{T}_{f,\psi}$ is, over $\mathcal{O}_{F_\mathfrak{p}}[\mathrm{GL}_2(\mathbb{F}_p)]$, the direct sum of two copies of St_ψ. The argument of Lemma 3.4.3 can be adapted (using the residual irreducibility of the two representations) so that its conclusion still holds, that is, $\mathcal{T}_{f,\psi} \simeq \mathrm{St}_\psi \otimes T_{f\otimes\psi,\mathfrak{p}}$.

When χ is not trivial, the argument does not work any more, because the $\mathbb{Z}_p[\mathrm{GL}_2(\mathbb{F}_p)]$-module $\pi(\psi,\psi\chi)$ is not residually irreducible, nor is it isomorphic to $\pi(\psi\chi,\psi)$ (while the two modules are isomorphic over $\mathbb{Q}_p[G]$), and $T_{f,\mathfrak{p}}/\varpi$ need not be residually irreducible (or $T_{f,\psi}$ need not be uniquely defined up to $\mathcal{O}_{F_\mathfrak{p}}[G_\mathbb{Q}]$-isomorphism).

However, when $T_{f,\mathfrak{p}}/\varpi$ is absolutely irreducible (so that $T_{f,\mathfrak{p}}$ defines a unique isomorphism class of $\mathcal{O}_{F_\mathfrak{p}}[G_\mathbb{Q}]$-module), we can see by decomposing according to the eigenspaces of a nonsplit Cartan subgroup C (as in the proof of Proposition 3.4.2) that $\mathcal{T}_{f,\psi}$ is a direct sum of $p+1$ copies of $T_{f,\mathfrak{p}}$. This is then enough to prove (with an adaptation of the argument of Lemma 3.4.3) that $\mathcal{T}_{f,\psi} \simeq T_{f,\psi} \otimes \pi'$, where π' is a $\mathcal{O}_{F_\mathfrak{p}}[\mathrm{GL}_2(\mathbb{F}_p)]$-module isomorphic to either $\pi(\psi,\psi\chi)$ or $\pi(\psi\chi,\psi)$.

Since $\pi(\psi\chi,\psi)_{\mathbb{F}_p}, \pi(\psi,\psi\chi)_{\mathbb{F}_p}$ have the same semi-simplification, but are defined by different (nonsplit) exact sequences (see Appendix B.5), one way to decide between $\pi(\psi,\psi\chi)_{\mathcal{O}_K}$ and $\pi(\psi\chi,\psi)_{\mathcal{O}_K}$ would be to describe explicitly the image in singular homology of the sum of the u_x: $H_1(X(p,p)(\mathbb{C}),\mathbb{F}_p) \to \bigoplus_{x\in S} H_1(X_1(p)(\mathbb{C}) \times \mathbb{F}_p^\times, \mathbb{F}_p)$, but this does not seem straightforward.

The case of cuspidal representations adds another difficulty (since $T_{f,\mathfrak{p}}$ also needs not be residually irreducible in this case, so this notation may refer to several non-isomorphic $\mathcal{O}_{F_\mathfrak{p}}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules): given $(f,\chi) \in \mathscr{C}$, it is not clear how many isomorphism classes of $\mathcal{O}_{F_\mathfrak{p}}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules M which are free of finite rank over $\mathcal{O}_{F_\mathfrak{p}}$ and such that $M \otimes_\mathbb{Z} \mathbb{Q} \simeq C_f$.

Lemma 3.4.6 *Let k be a field with characteristic q and separable closure k_s. Let $\mathbb{Q}_{\{q\}'}$ be the maximal extension of $\mathbb{Q}$ which is unramified at q (so $\mathbb{Q}_{\{0\}'} = \overline{\mathbb{Q}}$), and $\mathcal{O}_{\mathbb{Q}_{\{q\}'}}$ be the ring of algebraic integers of $\mathbb{Q}_{\{q\}'}$.*

- *There exists a ring homomorphism $\iota : \mathcal{O}_{\mathbb{Q}_{\{q\}'}} \to k_s$.*
- *Any ring homomorphism $\iota : \mathcal{O}_{\mathbb{Q}_{\{q\}'}} \to k_s$ defines a continuous group homomorphism $R_\iota : \mathrm{Gal}(k_s/k) \to \mathrm{Gal}(\mathbb{Q}_{\{q\}'}/\mathbb{Q})$. When $q > 0$, $\ker\iota$ is a maximal ideal, and the image of R_ι is its decomposition subgroup.*
- *If $\iota' : \mathcal{O}_{\mathbb{Q}_{\{q\}'}} \to k_s$ is another ring homomorphism, there exists a $\sigma \in \mathrm{Aut}(\mathbb{Q}_{\{q\}'}/\mathbb{Q})$ such that $\iota' = \iota\circ\sigma$, and $R_{\iota'} = \sigma^{-1}R_\iota\sigma$.*

Proof. – When $q = 0$, the existence of an embedding $\overline{\mathbb{Q}} \to k_s$ follows from classical Galois theory. When $q > 0$, there exists a maximal ideal $\mathfrak{q} \in \mathcal{O}_{\mathbb{Q}_{\{q\}'}}$ with residue characteristic q. Since $\mathcal{O}_{\mathbb{Q}_{\{q\}'}}$ contains all the roots of unity with order prime to q and is integral over $\mathbb{Z}$, $\mathcal{O}_{\mathbb{Q}_{\{q\}'}}/\mathfrak{q}$ is the algebraic closure of $\mathbb{F}_q$, and there exists an embedding $\mathcal{O}_{\mathbb{Q}_{\{q\}'}}/\mathfrak{q} \to k_s$ by Galois theory again.

Let us fix a morphism $\iota : \mathcal{O}_{\mathbb{Q}_{\{q\}'}} \to k_s$.

Let us check that $\iota(\mathcal{O}_{\mathbb{Q}_{\{q\}'}})$ is stable under $\mathrm{Gal}(k_s/k)$. Any element in $\iota(\mathcal{O}_{\mathbb{Q}_{\{q\}'}})$ is a root of some irreducible monic polynomial $f \in \mathbb{Z}[t]$. Conversely, let $f \in \mathbb{Z}[t]$ be a monic irreducible polynomial of degree d and $x \in k_s$ be a root of f. If $f \pmod q$ is not separable (which implies necessarily that $q > 0$), then, by considering its decomposition in irreducible factors in $\mathbb{F}_q[t]$, there exists a monic polynomial $g \in \mathbb{Z}[t]$ such that $\sqrt{(f \pmod q)} = (g \pmod q)$ and $g \pmod q$ is separable. In particular, x is still a root of g. After replacing f with one of the irreducible monic factors of g in $\mathbb{Z}[t]$, we can therefore assume that $f \pmod q$ is separable. Then the roots of f are contained in $\mathcal{O}_{\{q\}'}$, so we can write $f(t) = \prod_{i=1}^d (t - y_i)$ with $y_i \in \mathcal{O}_{\{q'\}}$. Thus, in k_s, $(f \pmod q)(t) = \prod_{i=1}^d (t - \iota(y_i))$, so x is one of the y_i.

Thus $\iota(\mathcal{O}_{\mathbb{Q}_{\{q\}'}})$ is exactly the subset of elements of k_s that are roots of irreducible monic $f \in \mathbb{Z}[t]$. In particular, it is stable under $\mathrm{Gal}(k_s/k)$.

Let $\mathfrak{q} = \ker \iota$, then, by definition, the group of automorphisms of $(\mathcal{O}_{\{q\}'}, \mathfrak{q})$ identifies with the automorphism group of $\mathcal{O}_{\mathbb{Q}_{\{q\}'}}/\mathfrak{q} \simeq \iota(\mathcal{O}_{\mathbb{Q}_{\{q\}'}})$. Thus, any $t \in \mathrm{Gal}(k_s/k)$ induces an automorphism of $\iota(\mathcal{O}_{\mathbb{Q}_{\{q\}'}})$, and there is therefore a unique automorphism $R_\iota(t) \in \mathrm{Gal}(\mathbb{Q}_{\{q\}'}/\mathbb{Q})$ preserving $(\mathcal{O}_{\{q\}'}, \mathfrak{q})$ such that for any $z \in \mathcal{O}_{\{q\}'}$, $\iota(R_\iota(t)(z)) = t(\iota(z))$.

Let $\sigma \in \mathrm{Gal}(\mathbb{Q}_{\{q\}'}/\mathbb{Q})$ and $\iota' = \iota \circ \sigma$. One can check directly that $R_{\iota\circ\sigma} = \sigma^{-1} R_\iota \sigma$.

Let $\iota' : \mathcal{O}_{\mathbb{Q}_{\{q\}'}} \to k_s$ be another ring homomorphism with kernel $\mathfrak{q}$. The above argument shows that ι' and ι have the same image in k_s, thus $(\iota')^{-1}\iota$ is an automorphism of $\mathcal{O}_{\mathbb{Q}_{\{q\}'}}/\mathfrak{q}$, which lifts to an automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}_{\{q\}'}/\mathbb{Q})$ preserving $(\mathcal{O}_{\{q\}'}, \mathfrak{q})$. Hence $\iota' = \iota \circ \sigma$.

Let $\iota' : \mathcal{O}_{\mathbb{Q}_{\{q\}'}} \to k_s$ be another ring homomorphism with kernel $\mathfrak{q}'$. There exists some $\sigma \in \mathrm{Gal}(\mathbb{Q}_{\{q\}'}/\mathbb{Q})$ such that $\sigma(\mathfrak{q}) = \mathfrak{q}'$, so $\iota" := \iota' \circ \sigma : \mathcal{O}_{\mathbb{Q}_{\{q\}'}} \to k_s$ has kernel $\mathfrak{q}$: by the previous paragraph, we can write $\iota" = \iota \circ \sigma'$ for some $\sigma' \in \mathrm{Gal}(\mathbb{Q}_{\{q'\}}/\mathbb{Q})$, hence $\iota' = \iota \circ \sigma' \circ \sigma^{-1}$, and we are done. □

Corollary 3.4.7 *Let us keep the notations of the previous lemma, and fix a ring homomorphism $\iota : \mathcal{O}_{\mathbb{Q}_{\{q\}'}} \to k_s$ with kernel $\mathfrak{q}$. Let A be an abelian scheme over $\mathbb{Z}_{\{}(q)\}$. Let ℓ be a prime number distinct from q. Then, for any $n \geq 1$, the obvious homomorphisms*

$$A[\ell^n](\mathcal{O}_{\mathbb{Q}_{\{q\}'}} \otimes \mathbb{Z}_{(q)}) \to A_{\mathbb{Q}}[\ell^n](\mathbb{Q}_{\{q\}'}), \qquad A_{\mathbb{Q}}[\ell^n](\mathbb{Q}_{\{q\}'}) \to A_{\mathbb{Q}}[\ell^n](\overline{\mathbb{Q}}),$$
$$A[\ell^n](\mathcal{O}_{\mathbb{Q}_{\{q\}'}} \otimes \mathbb{Z}_{(q)}) \to A[\ell^n]\left((\mathcal{O}_{\mathbb{Q}_{\{q\}'}})_{\mathfrak{q}}/\mathfrak{q}\right) \xrightarrow{\iota} (A_k)[\ell^n](k_s),$$

are isomorphisms.

Proof. – When $q = 0$, this is simply the fact that $A[\ell^n](\overline{\mathbb{Q}}) \xrightarrow{\iota} (A_k)[\ell^n](k_s)$ is an isomorphism for any abelian variety A over $\mathbb{Q}$, which is classical (see [118, Theorem 8.2, Remark 8.4]). When $q > 0$, the map labelled ι is an isomorphism for the same reason (since $\iota : (\mathcal{O}_{\mathbb{Q}_{\{q\}'}})_{\mathfrak{q}}/\mathfrak{q} \to k_s$ is a morphism of separably closed fields), and the other maps are isomorphisms by the Néron-Ogg-Shafarevich criterion [146, §1]. □

Definition 3.4.8 Let k be a field with characteristic prime to p and separable closure k_s, and $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{F}_p)$. We define the smooth projective curve (that is, pure one-dimensional scheme) $X_\rho(p)$ over k as the twist of $X(p,p)_k$ by the action of ρ (this is closer to the notation of Definition 1.4.7). Its Jacobian variety (in the sense of Proposition A.4.28) is denoted by $J_\rho(p)$.

Corollary 3.4.9 *Let k be a field of characteristic distinct from p and separable closure k_s. Let $F, \ell, \mathfrak{l}$ be as in Corollary 3.4.4 such that $\ell \in k^\times$. Let $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ be a continuous group homomorphism. Then, as a $(\mathbb{T} \otimes_{\mathbb{Z}} F_{\mathfrak{l}})[G_k]$-module, $\mathcal{T}_\ell J_\rho(p) \otimes_{\mathbb{Z}_\ell} F_{\mathfrak{l}}$ is isomorphic to the direct sum of*

- *for each $((f, \mathbf{1}), \psi) \in \mathscr{S} \times \mathscr{D}$, a copy of $\psi(\omega_p \det \rho) \otimes V_{f,\mathfrak{l}} \otimes \mathrm{St}(\rho)$, on which, for any $n \geq 1$ coprime to p, T_n (resp. nI_2) acts by $a_n(f)\psi(n)$ (resp. $\psi(n)^2$),*
- *for each $((f,\chi),\psi) \in \mathscr{P} \times \mathscr{D}$ modulo the relation $((f,\chi),\psi) \sim ((\overline{f},\overline{\chi}),\chi\psi)$, a copy of $\psi(\omega_p \det \rho) \otimes V_{f,\mathfrak{l}} \otimes (\pi(1,\chi)(\rho))$, on which, for any $n \geq 1$ coprime to p, T_n (resp. nI_2) acts by $a_n(f)\psi(n)$ (resp. $\psi(n)^2\chi(n)$),*
- *for each $(f,\chi) \in \mathscr{C}$, a copy of $V_{f,\mathfrak{l}} \otimes C_f(\rho)$, on which, for any $n \geq 1$ coprime to p, T_n (resp. nI_2) acts by $a_n(f)$ (resp. $\chi(n)$).*

Proof. – This follows essentially from Corollary 3.4.4 using [163, Proposition 2.2], but let us spell the argument out. Fix some algebraic closure $\overline{k}$ of k. By Proposition A.4.39, $J_\rho(p)$ identifies with the twist of $J(p,p)_k$ by ρ (by the push-forward functoriality) and inherits its action by $\mathbb{T}$ by

Proposition A.1.13. By Propositions A.1.11 and A.1.13, the following diagram commutes, with all the maps commuting to $\mathbb{T}$:

$$\begin{array}{ccc} J_\rho(p)(\overline{k}) & \xrightarrow{j_{J(p,p)_k}} & J(p,p)(\overline{k}) \\ \downarrow\sigma & & \downarrow\rho(\sigma)\circ\sigma \\ J_\rho(p)(\overline{k}) & \xrightarrow{j_{J(p,p)_k}} & J(p,p)(\overline{k}), \end{array}$$

with $j_{J(p,p)_k}$ a morphism of abelian varieties by Proposition A.4.39, and all the maps in the diagram commute with $\mathbb{T}$ by Proposition A.1.13. In particular, $j_{J(p,p)_k}$ identifies $\mathcal{T}_q J_\rho(p)$ with $\mathcal{T}_q J(p,p)_k$ as $\mathbb{T}$-module, and the G_k-actions coincide if we let $\sigma \in G_k$ act on $\mathcal{T}_q J(p,p)_k$ by the composition of its natural action and $\rho(\sigma)$.

By the previous remark and Corollary 3.4.4, the induced structure of $(\mathbb{T}\otimes F_\mathfrak{l})[\mathrm{Gal}(k_s/k)]$-module on $\mathcal{T}_\ell J(p,p)_k \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is exactly the one described in the statement of this Corollary. □

Remark Each of the factors in the decomposition is invariant if we replace ρ with one of its quadratic twists. This fact is also a direct consequence of Proposition 1.4.4 after compactifying.

3.5 Irreducibility of the factors of $\mathcal{T}_\ell J(p,p)_\rho$

Let $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ be a continuous group homomorphism, where k is a field of characteristic distinct from p with separable closure k_s, and assume that $\det\rho = \omega_p^{-1}$ (we recall that ω_p is the mod p cyclotomic character). By Proposition 1.4.10, the twist of $X(p,p)_k$ by ρ has exactly $p-1$ connected components $X_{\rho,\alpha}(p)$ (each one of them geometrically connected) for $\alpha \in \mu_p^\times(k_s)$, so the twist of $J(p,p)_k$ by ρ has $p-1$ summands indexed by $\alpha \in \mu_p^\times(k_s)$, corresponding to the Jacobian varieties of the $X_{\rho,\alpha}(p)$. In particular, the direct sum of the Tate modules of the Jacobians of the $X_{\rho,\alpha}(p)$ is given by Corollary 3.4.9.

Our goal is to exploit the decomposition given by Corollary 3.4.9 to describe the Tate modules of the Jacobians of the $X_{\rho,\alpha}(p)$.

Lemma 3.5.1 *Let G be a finite group and $q \nmid 6|G|$ be a prime number. Then any closed subgroup $H \leq \mathrm{SL}_2(\mathbb{Z}_q)\times G$ whose first projection is onto is equal to $\mathrm{SL}_2(\mathbb{Z}_q)\times G_1$ for some subgroup $G_1 \leq G$.*

Proof. – First, we show that $U := \begin{pmatrix}1&1\\0&1\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}_q)$ satisfies $(U, e_G) \in H$. Let $D \subset \mathbb{Z}_q$ consisting of those $a \in \mathbb{Z}_q$ such that $\left(\begin{pmatrix}1&a\\0&1\end{pmatrix}, e_G\right) \in H$. Then D is a closed subgroup of $\mathbb{Z}_q$. The assumption implies that $(U,g) \in H$ for some $g \in G$. Then $(U^{|G|}, e_G) = (U,g)^{|G|} \in H$, so $|G| \in D$, so $\overline{|G|\mathbb{Z}} \subset D$. Since $q \nmid |G|$, $|G|\mathbb{Z}$ is dense in $\mathbb{Z}_q$, so $1 \in D$ and $(U, e_G) \in H$.

For each $m \in \mathrm{SL}_2(\mathbb{Z}_q)$, the above argument shows that $(U, e_G) \in (m,1)^{-1}H(m,1)$, so $(mUm^{-1}, e_G) \in H$. Therefore, the subset S of those $M \in \mathrm{SL}_2(\mathbb{Z}_q)$ such that $(M, e_G) \in H$ is a closed subgroup containing every conjugate of U, so $S = \mathrm{SL}_2(\mathbb{Z}_q)$ and $\mathrm{SL}_2(\mathbb{Z}_q)\times\{e_G\} \subset H$, whence the conclusion. □

Lemma 3.5.2 *Let k be a field, V, W be two k-vector spaces of finite dimension, and $f : G \to H$ be a group homomorphism. Suppose that H acts on the k-vector spaces V and W in such a way that $V_{|G}$ is absolutely irreducible and $f(G)$ acts trivially on W. Then any subrepresentation of $V \otimes_k W$ (over $k[H]$) is of the form $V \otimes_k W'$ for some subrepresentation $W' \leq W$.*

Proof. – Under these assumptions, V satisfies Schur's Lemma. Therefore, the morphism

$$w \in W \longmapsto (- \otimes w) \in \mathrm{Hom}_{f(G)}(V, V \otimes_k W)$$

is an injective k-linear map between finite dimensional k-vector spaces of same dimension, hence is an isomorphism.

Let $X \subset V \otimes_k W$ be any $k[H]$-submodule such that X does not contain $V \otimes w$ for any $w \neq 0$. Then there is no nonzero $k[f(G)]$-morphism $V_{|f(G)} \to X_{|f(G)}$. However, $X_{|f(G)}$ embeds in a sum of copies of the absolutely irreducible representation $V_{|f(G)}$, so any irreducible $k[f(G)]$-module of X is isomorphic to $V_{|f(G)}$. So X cannot have any irreducible $k[f(G)]$-submodule, so $X = 0$.

Let $X \subset V \otimes_k W$ be any $k[H]$-submodule. Then $W' = \{w \in W,\ X \supset V \otimes w\}$ is a $k[H]$-submodule of W, and $V \otimes_k W' \subset X$. Then $X' = X/(V \otimes_k W') \subset V \otimes_k (W/W')$ satisfies the assumptions of the above paragraph, so $X' = 0$ and $X = V \otimes_k W'$. □

Proposition 3.5.3 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a normalized newform without complex multiplication of weight $k \geq 2$, F be a number field containing the coefficients of f, $\mathfrak{l}$ be a maximal ideal of $\mathcal{O}_F$ with residue characteristic ℓ, and $\lambda \in \mathcal{O}_{F_\mathfrak{l}}$ be a uniformizer. Let L be a number field and $\sigma : G_L \to \mathrm{GL}_n(\mathcal{O}_F)$ be an absolutely irreducible Artin representation. Then the representation $\sigma \otimes V_{f,\mathfrak{l}}$ is irreducible as a $F_\mathfrak{l}[G_L]$-module. Moreover, if ℓ is large enough (with respect to f, L and $|\sigma(G_L)|$), then $(\sigma \otimes_{\mathcal{O}_F} T_{f,\mathfrak{l}})/\lambda$ is an irreducible $(\mathcal{O}_{F_\mathfrak{l}}/\lambda)[G_{L(\mu_{\ell^\infty})}]$-module.*

Proof. – Let $M \supset L$ be the number field such that $\ker \sigma = G_M$. By [132, Proposition 4.4], $(V_{f,\mathfrak{l}})_{|G_M}$ is irreducible. It is absolutely irreducible, because otherwise one of the following two impossible situations occurs:

- $V_{f,\mathfrak{l}} \otimes \overline{F_\mathfrak{l}}$ has a unique $\overline{F_\mathfrak{l}}$-line stable under G_M, so this line is stable under $\mathrm{Gal}(\overline{F_\mathfrak{l}}/F_\mathfrak{l})$, so this line is of the form $D \otimes \overline{F_\mathfrak{l}}$ for some line $D \subset V_{f,\mathfrak{l}}$ stable under G_M, which is impossible.
- $V_{f,\mathfrak{l}} \otimes \overline{F_\mathfrak{l}}$ is the sum of two characters, so $V_{f,\mathfrak{l}}$ is an abelian representation of G_M, thus contradicting [132, Proposition 4.4].

Let W be a $F_\mathfrak{l}$-vector space on which G_L acts by σ. By Lemma 3.5.2 (for $G_M \to G_L$), any $F_\mathfrak{l}[G_L]$-submodule of $V_{f,\mathfrak{l}} \otimes W$ is of the form $V_{f,\mathfrak{l}} \otimes W'$ for some subrepresentation W' of W. Since W is absolutely irreducible, W' is either zero or W, so $V_{f,\mathfrak{l}} \otimes W'$ is irreducible.

Let us assume that $M/\mathbb{Q}$ is unramified above ℓ and $\ell \nmid 30|\sigma(G_L)|$ (this holds for all but finitely many ℓ). Let $\Gamma \subset \mathrm{GL}_2(\mathcal{O}_{F_\mathfrak{l}}) \times \mathrm{GL}_n(\mathcal{O}_K)$ be the image of $G_{L(\mathbb{Q}(\mu_{\ell^\infty}))}$ in $\mathrm{Aut}(T_{f,\mathfrak{l}}) \times \mathrm{Aut}(T_\sigma)$, where T_σ is some free $\mathcal{O}_F$-module of finite rank on which G_L acts by σ.

Now, Γ is a closed subgroup of $\mathrm{GL}_2(\mathcal{O}_{F_\mathfrak{l}}) \times \mathrm{im}(\sigma)$ (the second factor is a finite group), and, by [108, Theorem 2.2.2], its first projection contains a conjugate of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ when ℓ is large enough. Since ℓ is unramified in $M/\mathbb{Q}$, the Galois extensions $L(\mu_{\ell^\infty})$ and M are linearly disjoint over L, so the second projection of Γ is exactly $\mathrm{im}(\sigma)$. By Lemma 3.5.1, Γ contains a conjugate of $\mathrm{SL}_2(\mathbb{Z}_\ell) \times \mathrm{im}(\sigma)$.

To show the conclusion, it is enough to show that $(T_{f,\mathfrak{l}} \otimes_{\mathcal{O}_F} T_\sigma)/\mathfrak{l}$ is an absolutely irreducible Γ-module. Consider the space $R = \overline{\mathbb{F}_\ell}^{\oplus 2}$ endowed with its natural action of $\mathrm{SL}_2(\mathbb{Z}_\ell)$: it is then enough to show that $R \otimes_{\mathcal{O}_F} (T_\sigma/\mathfrak{l})$ is an irreducible $\overline{\mathbb{F}_\ell}[\mathrm{SL}_2(\mathbb{Z}_\ell) \times \mathrm{im}(\sigma)]$-module.

The action of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ on R is (absolutely) irreducible, and, by our choice of ℓ, the action of $\mathrm{im}(\sigma)$ on $T_\sigma/\mathfrak{l}$ is absolutely irreducible. We can then apply Lemma 3.5.2 to the morphism $\mathrm{SL}_2(\mathbb{Z}_\ell) \subset \mathrm{SL}_2(\mathbb{Z}_\ell) \times \mathrm{im}(\sigma)$, whence the conclusion. □

Corollary 3.5.4 *In the situation of Corollary 3.4.9, if k is a number field and ρ is onto, then all the given decomposition factors are absolutely irreducible, except when $p \equiv 3 \pmod 4$, f is a CM modular form and one of the following two conditions is satisfied:*

- *$k \supset \mathbb{Q}(\sqrt{-p})$,*
- *$\omega_p \det \rho : G_k \to \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$ is trivial.*

.

Proof. – Since $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is onto, the representations $\mathrm{St}(\rho), \pi(1,\chi)(\rho), C_f(\rho)$ are absolutely irreducible, so, when f is not CM, we can apply Proposition 3.5.3 and the conclusion follows.

If f is CM, then there is a nontrivial Dirichlet character ϵ such that $f \otimes \epsilon = f$. By considering the character of f, $\epsilon^2 = 1$, so ϵ is a quadratic character. By [132, Theorem 4.5], ϵ is the character of an imaginary quadratic field, so $\epsilon(-1) = -1$. By Corollary C.3.10, since f has conductor p^2 and its character has conductor at most p, the level of ϵ must be a power of p. Since $p > 2$, ϵ is the unique nontrivial quadratic character of $\mathbb{F}_p^\times$, that is, $\epsilon = \left(\frac{\cdot}{p}\right)$ is the character of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$. Then $\left(\frac{-1}{p}\right) = \epsilon(-1) = -1$ so $p \equiv 3 \pmod 4$.

When none of the two conditions are verified, let $\psi, \psi' : G_{\mathbb{Q}(\sqrt{-p})} \to \overline{F_\mathfrak{l}}^\times$ be the two characters attached to $V_{f,\mathfrak{l}}$ (see [132, Theorem 4.5]). Let $k_1 = k(\sqrt{-p})$: then $\rho(G_{k_1})$ is a normal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ with index at most 2, and is not $\mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p)$ (otherwise $\det \rho : G_k \to \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$ is trivial or agrees with ω_p), so $\rho(G_{k_1}) = \mathrm{GL}_2(\mathbb{F}_p)$.

Therefore, $(V_{f,\mathfrak{l}} \otimes C_f(\rho))_{|G_{k_1}} \simeq [\psi \otimes C_f(\rho_{|G_{k_1}})] \oplus [\psi' \otimes C_f(\rho_{|G_{k_1}})]$, and the two factors are irreducible. Assume that $V_{f,\mathfrak{l}} \otimes C_f(\rho)$ was reducible, and let M be an irreducible subrepresentation. Up to exchanging ψ, ψ', we can assume that $M_{|G_{k_1}} \simeq \psi \otimes C_f(\rho_{|G_{k_1}})$. After conjugating by G_k, we also have $M_{|G_{k_1}} \simeq \psi' \otimes C_f(\rho_{|G_{k_1}})$. By taking determinants, we see that $\left(\frac{\psi}{\psi'}\right)^{p-1} = 1$. This is impossible since, by [132, Theorem 4.3], $\frac{\psi}{\psi'}$ has infinite image. □

Before discussing in more detail the case where $(f,\chi) \in \mathscr{C}$ is a CM modular form, let us recall the properties of CM modular forms. This statement is well-known: for instance, it seems implied by [132]. But since *loc. cit.* (or any other text I was able to locate) does not explicitly provide or prove such an statement, we do it here.

Proposition 3.5.5 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a normalized newform with complex multiplication by some imaginary quadratic field K, where $k \geq 2$. There exists a number field $F \subset \mathbb{C}$ containing the image of K and the coefficients of f, and two locally constant characters $\psi_\sigma, \psi_\tau : \mathbb{A}_{K,f}^\times \to F^\times$ satisfying the following properties (where $\mathrm{Hom}(K,F) = \{\sigma,\tau\}$ and $\mathbb{A}_{K,f}^\times$ is the group of finite idèles of K):*

- *for any $x \in K^\times$ and $i \in \{\sigma,\tau\}$, one has $\psi_i(x) = i(x)^{k-1}$,*
- *both ψ_i are trivial on $\prod_{v \nmid N} \mathcal{O}_{K_v}^\times$,*
- *pre-composing by the action of $\mathrm{Aut}(K/\mathbb{Q})$ exchanges the two ψ_i,*
- *for any prime ideal λ of $\mathcal{O}_F$ with residue characteristic ℓ, for each $i \in \{\sigma,\tau\}$, the continuous character*
$$x = (x_p)_p \in (\mathbb{A}_{\mathbb{Q},f} \otimes K)^\times \simeq \mathbb{A}_{K,f}^\times \mapsto \psi_i(x) i(x_\ell)^{1-k} \in F_\lambda$$
is trivial on $K^\times$ and corresponds under the global class field theory reciprocity morphism[2] to a character $\psi_{i,\lambda} : G_K \to F_\lambda^\times$ such that $V_{f,\lambda} \simeq \mathrm{Ind}_K^{\mathbb{Q}} \psi_{i,\lambda}$.

In other words, $(\psi_{\sigma,\lambda})_\lambda, (\psi_{\tau,\lambda})_\lambda$ form compatible systems over F in the sense of Definition 4.5.2.

In particular, for any maximal ideal λ of $\mathcal{O}_F$, for any prime number q split in K and coprime to $N\lambda$, if $q\mathcal{O}_K = \mathfrak{q}\mathfrak{q}'$, then $\psi_\sigma(\mathfrak{q}), \psi_\sigma(\mathfrak{q}')$ are the two roots of $X^2 - a_q(f)X + q^{k-1}\chi(q)$, where χ is the character of f.

Proof. – By [132, Theorem 4.5], there is an integer $m \geq 1$ divisible by $N\Delta_{K/\mathbb{Q}}$, a character $\psi : J^m \to \mathbb{C}^\times$ and an embedding $\sigma : K \to \mathbb{C}$ such that:

- J^m is the group of fractional ideals of $\mathcal{O}_K$ coprime to m,
- for any $x \in K^\times$ prime to m and congruent to 1 modulo m, $\psi((x)) = \sigma(x)^{k-1}$,

[2] normalized so as to map a uniformizer to an arithmetic Frobenius

- for any prime number q split in K and coprime to m, let $\mathfrak{q},\mathfrak{q}'$ denote the prime ideals of $\mathcal{O}_K$ dividing q, then $\psi(\mathfrak{q})+\psi(\mathfrak{q}')=a_q(f)$,
- the character χ of f is the product of the Dirichlet character ε attached to $K/\mathbb{Q}$ and the character $a\in(\mathbb{Z}\setminus\cup_{p|m}p\mathbb{Z})\longmapsto a^{1-k}\psi((a))$, which is a Dirichlet character modulo m.

Now, the subgroup of J^m made with principal ideals generated by elements $x\in K^\times$ congruent to 1 modulo m has finite index. Therefore, for any fractional ideal I of K coprime to m, one has $|\psi(I)|=(\mathbf{N}_{K/\mathbb{Q}}I)^{\frac{k-1}{2}}$.

By [123, Corollary VII.6.14], ψ extends to a continuous character $\psi_0:\mathbb{A}_K^\times/K^\times\to\mathbb{C}^\times$ such that, for any $z\in(K\otimes\mathbb{R})^\times$, one has $\psi_0(z)=\sigma(z)^{1-k}$. Because $\mathcal{O}_K^\times$ is finite, $K^\times$ is a discrete subgroup of $\mathbb{A}_{K,f}^\times$, so we can consider the restriction ψ_σ of ψ_0 to $\mathbb{A}_{K,f}^\times$. Thus $\psi_\sigma:\mathbb{A}_{K,f}^\times\to\mathbb{C}^\times$ satisfies the following properties:

- ψ_σ is trivial on $\prod_{v|m}(1+m\mathcal{O}_{K_v})\prod_{v\nmid m}\mathcal{O}_{K_v}^\times$,
- for any $z\in K^\times$, $\psi_\sigma(z)=\sigma(z)^{k-1}$,
- if $q\nmid Nm$ is a prime number split in K and $\mathfrak{q},\mathfrak{q}'$ are the two prime ideals above q, if $z\in K_\mathfrak{q}$, $z'\in K_{\mathfrak{q}'}$ are uniformizers, then $\psi_\sigma(z)+\psi_\sigma(z')=a_q(f)$ and $\psi_\sigma(z)\psi_\sigma(z')=\chi(q)q^{k-1}$,
- if $n\in\mathbb{Z}$ is an integer coprime to m, and z is the idèle equal to n at every place $v\nmid m$ and equal to 1 at other places, then $\psi_\sigma(z)=\varepsilon(n)\chi(n)$.

Let $\tau:K\to\mathbb{C}$ be the other embedding and ψ_τ be the conjugate of ψ_σ under the action of $\mathrm{Gal}(K/\mathbb{Q})$.

Let $q\nmid m$ be a prime number split in K. Let $\mathfrak{q},\mathfrak{q}'$ denote the prime ideals of $\mathcal{O}_K$ dividing q and fix uniformizers $z\in K_\mathfrak{q}, z'\in K_{\mathfrak{q}'}$. The numbers $\psi_\sigma(z),\psi_\sigma(z')$ are roots of $X^2-a_q(f)X+q^{k-1}\chi(q)$, so they are algebraic. Let F_0 be a number field containing K, $a_q(f)$, $\chi(q)$ and $\psi_\sigma(z),\psi_\sigma(z')$. There exists an integer $n\geq1$ such that $\mathfrak{q}^n,(\mathfrak{q}')^n$ are principal with generators $x,x'\in1+m\mathcal{O}_K$, so that

$$\psi_\sigma(z)^n=\psi_\sigma(x)=\sigma(x)^{k-1},\quad \psi_\sigma(z')^n=\psi_\sigma(x')=\sigma(x')^{k-1},$$

whence

$$\psi_\sigma(z)\mathcal{O}_{F_0}=\sigma(\mathfrak{q})^{k-1}\mathcal{O}_{F_0},\ \psi_\sigma(z')\mathcal{O}_{F_0}=\sigma(\mathfrak{q}')^{k-1}\mathcal{O}_{F_0}.$$

In particular, $\frac{\psi_\sigma(z)}{\psi_\sigma(z')}$ is not an algebraic integer.

Let $\theta:\mathbb{A}_{K,f}^\times\to\mathbb{C}^\times$ be a locally constant character satisfying the following properties:

- There are $\alpha,\beta\in\mathbb{Z}$ such that for any $x\in K^\times$, $\theta(x)=\sigma(x)^\alpha\tau(x)^\beta$,
- For all but finitely many primes $q\nmid Nm$ split in K, if $\mathfrak{q},\mathfrak{q}'$ are the two ideals of $\mathcal{O}_K$ dividing q and $z\in K_\mathfrak{q}$, $z'\in K_{\mathfrak{q}'}$ are uniformizers, then

$$(X-\theta(z))(X-\theta(z'))=X^2-a_q(f)X+q^{k-1}\chi(q).$$

Let us prove that $\theta\in\{\psi_\sigma,\psi_\tau\}$.

Let $I\subset m\mathcal{O}_K$ be a nonzero ideal such that for any finite place v of $\mathcal{O}_K$, $\theta(1+I\mathcal{O}_{K_v})=\{1\}$. Moreover, $x\in\mathbb{A}_{K,f}^\times\mapsto|\theta(x)|\|x\|_{\mathbb{A}_{K,f}}^{\frac{\alpha+\beta}{2}}\in\mathbb{R}^{+\times}$ is equal to 1 on the finite index subgroup $K^\times\prod_{v|I}(1+\mathcal{O}_{K_v})\prod_{v\nmid I}\mathcal{O}_{K_v}^\times$ of $\mathbb{A}_{K,f}^\times$. Since $\mathbb{R}^{+\times}$ is uniquely divisible, for any $x\in\mathbb{A}_{K,f}^\times$, one has $|\theta(x)|\|x\|_{\mathbb{A}_{K,f}}^{\frac{\alpha+\beta}{2}}=1$. By taking for x a uniformizer of a split prime ideal $\mathfrak{q}\subset\mathcal{O}_K$ with residue caracteristic q coprime to Im, we see that $\alpha+\beta=k-1$.

By the Dirichlet density theorem [123, Theorem VII.13.2], we can find infinitely many primes $q\nmid m$ such that $q\mathcal{O}_K=\mathfrak{q}\mathfrak{q}'$ with $\mathfrak{q},\mathfrak{q}'$ distinct ideals of $\mathcal{O}_K$, and such that $\mathfrak{q}$ is a principal ideal generated by some $x\in1+I\mathcal{O}_K$. For all but finitely many such q, $\theta(x)=\sigma(x)^\alpha\tau(x)^\beta$ is a root of $X^2-a_q(f)X+q^{k-1}\chi(q)$, so $\theta(x)\in\{\psi_\sigma(x),\psi_\tau(x)\}=\{\sigma(x)^{k-1},\tau(x)^{k-1}\}$. Since $\frac{\sigma(x)}{\tau(x)}$ is not a root of unity, we see that $(\alpha,\beta)\in\{(0,k-1),(k-1,0)\}$.

After pre-composing θ by the action of $\mathrm{Gal}(K/\mathbb{Q})$, we may assume that $(\alpha,\beta)=(k-1,0)$, so that $\psi_f\theta^{-1}:\frac{\mathbb{A}_{K,f}^\times}{K^\times\prod_{v|I}(1+I\mathcal{O}_{K_v})\prod_{v\nmid I}\mathcal{O}_{K_v}^\times}\to\mathbb{C}^\times$ is a well-defined character from a finite group, so its image is contained in the roots of unity.

Let $q\nmid m\mathbf{N}_{K/\mathbb{Q}}(I)$ be a prime number that splits in K with $q\mathcal{O}_K=\mathfrak{q}\mathfrak{q}'$. Let $z\in K_\mathfrak{q}$, $z'\in K_{\mathfrak{q}'}$ be uniformizers and assume that $\theta(z),\theta(z')$ are the two roots of $X^2-a_q(f)X+q^{k-1}\chi(q)$. Then $\theta(z)\in\{\psi_\sigma(z),\psi_\sigma(z')\}$ is equal to $\psi(z)$ up to a root of unity. We saw that $\frac{\psi_\sigma(z)}{\psi_\sigma(z')}$ is not a root of unity, hence $\theta(z)=\psi_\sigma(z)$. By Dirichlet's density theorem [123, Theorem VII.13.2], one then has $\theta=\psi_\sigma$.

Let $F\subset\mathbb{C}$ be the number field generated by the image in $\mathbb{C}$ of F and K. Applying the above argument to any $\mathrm{Aut}(\mathbb{C}/F)$-conjugate of ψ_σ, we see that ψ_σ (hence ψ_τ) takes all its values in $F^\times$.

Let now λ be a prime ideal of $\mathcal{O}_F$ with residue characteristic ℓ. By [132, Theorem 4.5], $V_{f,\lambda}$ is a semi-simple continuous abelian representation of G_K, so it decomposes as the sum of two continuous characters $\alpha,\beta:G_K\to\overline{F_\lambda}$ that are unramified away from $N\ell$. Let, for $i\in\{\sigma,\tau\}$ (defining a morphism $K\otimes\mathbb{Q}_\ell\to F_\lambda$),

$$\psi_{i,\lambda}:x=(x_\ell)\in(K\otimes\mathbb{A}_{\mathbb{Q},f})^\times\simeq\mathbb{A}_{K,f}^\times\mapsto\psi_i(x)i(x_\ell)^{1-k}\in F_\lambda.$$

Then $\psi_{i,\lambda}$ is a continuous character $\mathbb{A}_K^\times/K^\times\prod_{v\nmid m\ell}\mathcal{O}_{K_v}^\times\to F_\lambda^\times$.

Note that we have an exact sequence

$$0\to(K\otimes\mathbb{R})^\times\to\mathbb{A}_K^\times/K^\times\to\mathbb{A}_{K,f}^\times/K^\times\to1$$

of locally compact Abelian groups, where $(K\otimes\mathbb{R})^\times\simeq\mathbb{C}^\times$ is connected, and the profinite group $\prod_{v|36m}(1+36m\mathcal{O}_{K_v})^\times\prod_{v\nmid36m}\mathcal{O}_{K_v}^\times$ is an open subgroup of $\mathbb{A}_{K,f}^\times/K^\times$, so the latter is locally profinite hence totally disconnected. Hence $(K\otimes\mathbb{R})^\times$ is the connected component of unity in $\mathbb{A}_K^\times/K^\times$.

By [73, Proposition 15.42], the class field theory reciprocity isomorphism thus identifies $\frac{\mathbb{A}_{K,f}^\times}{K^\times\prod_{v\nmid m\ell}\mathcal{O}_{K_v}^\times}$ with the abelianization of the Galois group $G_{K,m\ell}$ of K unramified outside $m\ell$ (by mapping a uniformizer at a place $v\nmid m\ell$ to an arithmetic Frobenius). Let $\psi'_{i,\lambda}:G_K\to F_\lambda^\times$ be the character corresponding to $\psi_{i,\lambda}$ under this identification: $\psi'_{i,\lambda}$ is unramified outside $m\ell$.

Thus, for any prime $q\nmid m\ell$ split in K, if $\mathfrak{q}$ denotes a prime ideal of $\mathcal{O}_K$ above q, then $\psi'_{i,\lambda}(\mathrm{Frob}_\mathfrak{q})$ is the value of ψ_i at a uniformizer of $\mathfrak{q}$ (in $K_\mathfrak{q}$), so it is a root of $X^2-a_q(f)X+q^{k-1}\chi(q)$, so it is either $\alpha(\mathrm{Frob}_\mathfrak{q})$ or $\beta(\mathrm{Frob}_\mathfrak{q})$. In other words, the function $(\psi'_{i,\lambda}-\alpha)(\psi'_{i,\lambda}-\beta):G_{K,m\ell}\to\overline{F_\lambda}$ vanishes at the Frobenius of every prime ideal in K which is prime to $m\ell$ and split in $K/\mathbb{Q}$. By Cebotarev's theorem [123, Neukirch VII.13.4], $(\psi'_{i,\lambda}-\alpha)(\psi'_{i,\lambda}-\beta)=0$, hence $G_{K,m\ell}$ is the reunion of one of the two subgroups $\{\alpha=\psi'_{i,\lambda}\}$ and $\{\beta=\psi'_{i,\lambda}\}$. Note that $\psi_{\sigma,\lambda}\neq\psi_{\tau,\lambda}$ by considering the behavior at the place ℓ, and we already know that $\alpha\neq\beta$. Therefore, $\{\alpha,\beta\}=\{\psi'_{\sigma,\lambda},\psi'_{\tau,\lambda}\}$, whence the conclusion. □

Notation *From now on (unless specified otherwise), we assume that the number field $F\subset\mathbb{C}$ satisfies furthermore the following property: for every $(f,\chi)\in\mathscr{C}$ with complex multiplication (necessarily by $\mathbb{Q}(\sqrt{-p})$ and $p\equiv3\pmod4$), for every prime q split in $\mathbb{Q}(\sqrt{-p})$, F contains the roots of the Hecke polynomial $X^2-a_q(f)X+q\chi(q)$.*

To each such $(f,\chi)\in\mathscr{C}$, one can thus attach the two compatible systems $(\psi_{\sigma,\mathfrak{l}})_{\mathfrak{l}\in\mathrm{Max}(\mathcal{O}_F)}$ (for $\sigma\in\mathrm{Hom}(K,F)$) of characters $G_{\mathbb{Q}(\sqrt{-p})}\to F_\mathfrak{l}$. We mean this affirmation in the sense of Definition 4.5.2, but for the remainder of the chapter, it is enough to note that for any prime ideal $\mathfrak{q}$ of $\mathbb{Q}(\sqrt{-p})$ with residue charateristic distinct from p, $\psi_{\sigma,\mathfrak{l}}(\mathrm{Frob}_\mathfrak{q})$ does not depend on the choice of a maximal ideal $\mathfrak{l}$ of $\mathcal{O}_F$ with residue characteristic coprime to $\mathfrak{q}$.

For the remainder of the text, we will in fact denote these two compatible systems by $(\psi_{f,\pm,\mathfrak{l}})_\mathfrak{l}$,

where the assignment of $\pm$ is arbitrary.

Proposition 3.5.6 *Let $(f,\chi) \in \mathscr{C}$ with f CM, so that $p \equiv 3 \pmod 4$ and f has complex multiplication by $\mathbb{Q}(\sqrt{-p})$. Let $\chi_1 \in \mathcal{D}$ be such that $\chi_1^2 = \chi$, and let $f_1 = f \otimes \chi_1^{-1}$. Then $(f_1, \mathbf{1}) \in \mathscr{C}$ is independent from the choice of χ_1, and C_{f_1} is the representation V_4 of Section B.4.*

Let $\mathfrak{l}$ be a prime ideal of $\mathcal{O}_F$ with residue characteristic ℓ, and $\psi, \psi' : G_{\mathbb{Q}(\sqrt{-p})} \to F_{\mathfrak{l}}^\times$ be the two continuous characters (conjugate under $G_\mathbb{Q}/G_{\mathbb{Q}(\sqrt{-p})}$) such that $(V_{f_1,\mathfrak{l}})_{|G_{\mathbb{Q}(\sqrt{-p})}}$ is the direct sum of ψ and ψ'.

Let k be a field with separable closure k_s on which $p\ell$ is invertible. For any subextension k'/k of k_s/k, let $G_{k'} = \mathrm{Gal}(k_s/k')$. Note that there is a unique conjugacy class e of morphisms from G_k to the maximal quotient $G_{\mathbb{Q},p\ell}$ of the absolute Galois group of $\mathbb{Q}$ which is unramified outside $p\ell$. Let $\alpha \in k_s$ be any root of the polynomial $X^2 - X - \frac{p+1}{4}$. Let $\rho : G_k \to \mathrm{GL}_2(\mathbb{F}_p)$ be any representation. Then the following statements hold:

(i) If $\det\rho \subset \mathbb{F}_p^{\times 2}$, then $C_f(\rho) \simeq \chi_1(\det\rho) \otimes (C^+(\rho) \oplus C^-(\rho))$, where C^+ and C^- are the representations V^+ and V^- defined in Section B.4.

(ii) If $\alpha \in k$, then the image of e is contained in $G_{\mathbb{Q}(\sqrt{-p}),p\ell}$ and

$$(V_{f,\mathfrak{l}} \circ e) \otimes C_f(\rho) \simeq \chi_1(\omega_p \det\rho) \otimes [(\psi(e) \otimes V_4(\rho)) \oplus (\psi'(e) \otimes V_4(\rho))].$$

(iii) When e has open image and $\rho(G_k)$ contains a conjugate of the Borel subgroup (i.e. the subgroup of upper-triangular matrices), both summands in the decomposition (ii) are irreducible and they are not isomorphic.

(iv) If $\alpha \notin k$ and $\omega_p \det\rho : G_k \to \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$ is trivial, let $e_1 = e_{|G_{k(\alpha)}}$, then, for any $\epsilon \in \{\pm\}$,

$$(V_{f,\mathfrak{l}} \circ e) \otimes C_f(\rho) \simeq \chi_1(\omega_p \det\rho) \otimes \bigoplus_{\theta \in \{\psi\circ e_1, \psi'\circ e_1\}} \mathrm{Ind}_{k(\alpha)}^k(\theta \otimes C^\epsilon(\rho_{|G_{k(\alpha)}})).$$

(v) In the situation of (iv), if e has open image and $\rho(G_k)$ contains a conjugate of the Borel subgroup, the two summands in the decomposition of $V_{f,\mathfrak{l}} \otimes C_f(\rho)$ are irreducible.

Proof. – We already saw in the proof of Corollary 3.5.4 why $p \equiv 3 \pmod 4$ and $f \otimes \left(\frac{\cdot}{p}\right) = f$. Since the character χ_1 is defined up to multiplication by $\left(\frac{\cdot}{p}\right)$, $f \otimes \chi_1^{-1}$ is independent from the choice of χ_1. It is then clear using Proposition C.2.2 that $(f_1, \mathbf{1}) \in \mathscr{C}$.

Let $\phi : \mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times$ be one of the two characters attached to C_{f_1}. Since $f_1 = f_1 \otimes \left(\frac{\cdot}{p}\right)$, by Corollaries 2.4.15 and B.2.8, $\phi \cdot \left(\frac{N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\cdot)}{p}\right) \in \{\phi, \phi^p\}$. The only possibility is $\phi \cdot \left(\frac{N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\cdot)}{p}\right) = \phi^p$, so $\phi^2 = (\phi^p)^2$, hence $\phi^4 = \phi^{2(p+1)-2p+2} = 1$. Since ϕ does not factor through the norm, $\phi^2 \neq 1$, so ϕ has order 4 and $C_{f_1} \simeq V_4$.

This implies by Corollary 2.4.15 that $C_f \simeq \chi_1(\det) \otimes C_{f_1}$. (i) is then a direct consequence of Proposition B.4.1.

The decomposition in (ii) is a consequence of the theory of complex multiplication described in Proposition 3.5.5 (or see [132, Proposition 4.4, Theorem 4.5]). For (iii), the irreducibility follows from Proposition B.3.7, and the two summands are not isomorphic because $\frac{\psi}{\psi'}$, hence $\frac{\psi(e)}{\psi'(e)}$ has infinite image by [132, Theorem 4.3].

From now on, assume that $\alpha \notin k$ and that $(\omega_p \det\rho)(G_k) \subset \mathbb{F}_p^{\times 2}$, and fix $\epsilon \in \{\pm\}$. Let

$k_1 = k(\alpha)$, $e_1 = e_{|G_{k_1}}$. Then

$$\begin{aligned}(V_{f,\mathfrak{l}} \circ e) \otimes C_f(\rho) &\simeq \chi_1(\det \rho\omega_p) \otimes (V_{f_1,\mathfrak{l}} \circ e) \otimes C_{f_1}(\rho) \\ &\simeq \chi_1(\omega_p \det \rho) \otimes (V_{f_1,\mathfrak{l}} \circ e) \otimes \mathrm{Ind}_{k_1}^k C^\epsilon(\rho_{|G_{k_1}}) \\ &\simeq \chi_1(\omega_p \det \rho) \otimes \mathrm{Ind}_{k_1}^k \left[(V_{f_1,\mathfrak{l}} \circ e_1) \otimes C^\epsilon(\rho_{|G_{k_1}})\right] \\ &\simeq \chi_1(\omega_p \det \rho) \otimes \mathrm{Ind}_{k_1}^k \left[((\psi \oplus \psi') \circ e_1) \otimes C^\epsilon(\rho_{|G_{k_1}})\right] \\ &\simeq \chi_1(\omega_p \det \rho) \otimes \bigoplus_{\theta \in \{\psi \circ e_1, \psi' \circ e_1\}} \theta \otimes C^\epsilon(\rho_{|G_{k_1}}),\end{aligned}$$

which proves (iv).

Assume that $\rho(G_k)$ contains a conjugate of the Borel subgroup. The claim is that for any $\theta \in \{\psi \circ e_{|G_{k_1}}, \psi' \circ e_{|G_{k_1}}\}$ and $\epsilon \in \{\pm\}$, $W = \mathrm{Ind}_{k_1}^k \theta \otimes C^\epsilon(\rho_{|G_{k_1}})$ is irreducible. Since $\psi \circ e_{|G_{k_1}}, \psi' \circ e_{|G_{k_1}}$ are conjugate under G_k/G_{k_1} and the same holds for $C^+(\rho_{|G_{k_1}}), C^-(\rho_{|G_{k_1}})$, we may assume $\theta = \psi \circ e_{|G_{k_1}}$, so that

$$W_{|G_{k_1}} \simeq \left[(\psi \circ e_{|G_{k_1}}) \otimes C^\epsilon(\rho_{|G_{k_1}})\right] \oplus \left[(\psi' \circ e_{|G_{k_1}}) \otimes C^{-\epsilon}(\rho_{|G_{k_1}}).\right]$$

Both summands are irreducible by Proposition B.4.3.

So if $M \subset W$ is a proper nonzero irreducible G_k-submodule, then $M_{|G_{k_1}}$ is isomorphic to $(\psi \circ e_{|G_{k_1}}) \otimes C^\epsilon(\rho_{|G_{k_1}})$ or its conjugate under G_k/G_{k_1}. Since $M_{|G_{k_1}}$ is isomorphic to its conjugate under G_k/G_{k_1}, we find that

$$(\psi \circ e_{|G_{k_1}}) \otimes C^\epsilon(\rho_{|G_{k_1}}) \simeq (\psi' \circ e_{|G_{k_1}}) \otimes C^{-\epsilon}(\rho_{|G_{k_1}}).$$

Thus $\frac{\psi}{\psi'}$ is trivial on the finite-index subgroup $e(G_{k_1} \cap \ker \rho)$ of $G_{\mathbb{Q}(\sqrt{-p})}$, which contradicts [132, Theorem 4.3]. □

3.6 Tate modules of the Jacobians of the connected components of $X(p,p)_\rho$

Let E be an elliptic curve over a field k with characteristic distinct from p. Let k_s be a separable closure of k and (P,Q) be a basis of $E[p](k_s)$. In the terminology of Section 1.3, $E[p]$ with its Weil pairing is a polarized p-torsion group[3] over $\operatorname{Spec} k$.

Let, for each $\sigma \in \mathrm{Gal}(k_s/k)$, $\rho_1(\sigma) \in \mathrm{GL}_2(\mathbb{F}_p)$ be the matrix such that $\rho_1(\sigma)\begin{pmatrix}P\\Q\end{pmatrix} = \begin{pmatrix}\sigma(P)\\\sigma(Q)\end{pmatrix}$. By Lemma 1.4.2, $\rho_1 : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ is an anti-homomorphism, hence $\rho = \rho_1^{-1}$ is a group homomorphism with determinant ω_p^{-1}.

By Proposition 1.4.10, we have a commutative diagram of k-schemes, where the bottom schemes are constant, the horizontal arrows are isomorphisms, and the fibres of the vertical morphisms are smooth projective geometrically connected k-schemes of dimension one:

$$\begin{array}{ccc} X_{E[p]}(p) & \longrightarrow & X(p,p)_\rho \\ \downarrow \det & & \downarrow \mathrm{We}_\rho \\ \mathbb{F}_p^\times & \xrightarrow{a \mapsto \underline{a}(\langle P,Q\rangle)} & \mathrm{Hom}_k(k \otimes_{\mathbb{Z}} \mathbb{Z}[1/p,\zeta_p], k_s). \end{array}$$

[3] that is, a finite étale group scheme over $\operatorname{Spec} k$, étale locally isomorphic to $\mathbb{F}_p^{\oplus 2}$, endowed with a (fibrewise) perfect alternated bilinear pairing $E[p] \times E[p] \to \mu_p$.

In fact, Proposition 1.4.10 tells that we have a similar diagram for any ρ such that $\det\rho = \omega_p^{-1}$, since such a representation encodes precisely a polarized p-torsion group over k. In particular, $X(p,p)_\rho$ is the reunion of $p-1$ smooth projective geometrically connected k-schemes of dimension one, indexed by the $\mathbb{F}_p^\times$-torsor $\mathrm{Hom}_k(k\otimes_{\mathbb{Z}}\mathbb{Z}[1/p,\mu_p],k_s) = \mu_p^\times(k_s)$ (because the rightmost vertical map does not depend on the choice of basis of $G(k_s)$).

Definition 3.6.1 Recall from Definition 3.4.8 that if k is a field of characteristic not dividing p with separable closure k_s and $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ is a group homomorphism with $\det\rho = \omega_p^{-1}$, we denote by $X_\rho(p)$ the smooth proper k-scheme of dimension one $(X(p,p)_k)_\rho$. It is endowed (by Proposition 1.4.10) with a canonical morphism to the disjoint union of copies of $\mathrm{Spec}\,k$ indexed by $\mu_p^\times(k_s)$; given $\xi \in \mu_p^\times(k_s)$, we denote by $X_{\rho,\xi}(p)$ the inverse image under said morphism of ξ.

Lemma 3.6.2 *Let $f \in \mathcal{S}_k(\Gamma_1(N)), g \in \mathcal{S}_{k'}(\Gamma_1(N'))$ be normalized newforms and $M > 1$ be an integer such that, for every prime number $\ell \equiv 1 \pmod M$ and coprime to NN', one has $a_\ell(f) = a_\ell(g)$. Then $k = k'$ and f, g are twists one of the other.*

Proof. – We may assume that $NN' \mid M$. Let us fix a prime number $p \mid M$, a number field $F \subset \mathbb{C}$ containing the coefficients of f and g as well as the $\varphi(M)$-th roots of unity, and a prime ideal $\mathfrak{p}$ of $\mathcal{O}_F$ with residue characteristic p. We consider the $\mathfrak{p}$-adic representations V_f, V_g of $G_{\mathbb{Q},M}$ attached to f and g respectively, where the index M indicates that the representations are unramified at any prime not dividing M.

For every prime $\ell \equiv 1 \pmod M$, $\mathrm{Tr}(\mathrm{Frob}_\ell \mid V_f) = a_\ell(f) = a_\ell(g) = \mathrm{Tr}(\mathrm{Frob}_\ell \mid V_g)$. By Cebotarev, the Frob_ℓ (for $\ell \equiv 1 \pmod M$) are dense in $G_{\mathbb{Q}(\mu_M),M}$, so the representations $V_{f,M} = (V_f)_{|G_{\mathbb{Q}(\mu_M),M}}, V_{g,M} = (V_g)_{|G_{\mathbb{Q}(\mu_M),M}}$ have the same traces, hence the same characteristic polynomials. By considering their determinants, we find that $k = k'$.

Moreover, $V_{f,M}$ and $V_{g,M}$ are semi-simple (they have finite image when $k = 1$, and it is [132, Proposition 4.2] when $k > 1$), so they are isomorphic, hence the $\mathrm{Gal}(\mathbb{Q}(\mu_M)/\mathbb{Q})$-module $H := \mathrm{Hom}_{G_{\mathbb{Q}(\mu_M),M}}(V_f, V_g)$ is nonzero.

Therefore, there exists a character $\psi : \mathrm{Gal}(\mathbb{Q}(\mu_M)/\mathbb{Q}) \to F^\times$ such that for some nonzero $u \in H$, $\sigma(u) = \psi(\sigma)u$ for all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\mu_M)/\mathbb{Q})$. Thus u corresponds to a nonzero $G_{\mathbb{Q}}$-homomorphism $V_{f,\mathfrak{p}} \to V_{g\otimes\psi,\mathfrak{p}}$. Since both representations are irreducible, u is an isomorphism and $f = g \otimes \psi$ by strong multiplicity one. □

Notation *We denote by λ the character $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \to \{\pm 1\}$, it is the unique quadratic Dirichlet character of conductor p.*

Finally, given a prime ℓ, the ring $\mathcal{O}_{\{\ell\}'}$ denotes the ring of integers of the maximal extension $\mathbb{Q}_{\{\ell\}'}$ of $\mathbb{Q}$ which is unramified at ℓ. When $\ell = 0$, $\mathcal{O}_{\{\ell\}'}$ denotes the ring $\overline{\mathbb{Z}}$ of algebraic integers.

Definition 3.6.3 The subalgebra $\mathbb{T}_1$ is the subalgebra of $\mathbb{T}$ generated by the $T_n \cdot (qI_2)$, where $n, q \geq 1$ are integers such that $nq^2 \equiv 1 \pmod p$. In fact, the $T_n \cdot (qI_2)$ generate $\mathbb{T}_1$ as a group, by Lemma 2.2.2.

For later use, we also define larger endomorphism algebras of $\mathbb{T}[\mathrm{GL}_2(\mathbb{F}_p)]$ that will usually be non-commutative or act non-rationally on twists of $J(p,p)$.

Definition 3.6.4 Let $G, H \leq \mathrm{GL}_2(\mathbb{F}_p)$ be subgroups. We denote by $\mathbb{T}_{1,G}(H)$ the subring of $\mathbb{T}[\mathrm{GL}_2(\mathbb{F}_p)]$ generated by the $(T_n \cdot (mI_2))u$, where:

- $n \geq 1$ is coprime to p,
- $u \in \mathbb{Z}[G]$ is a formal linear combination of matrices of determinant $(nm^2)^{-1} \in \mathbb{F}_p^\times$,
- u commutes to H.

Note that $\mathbb{T}_{1,G}(H)$ is generated as a group by the $T_n u$ as above, by Lemma 2.2.2, and that its subring $\mathbb{T}_1$ is central. When H contains only scalar matrices, we write $\mathbb{T}_{1,G}(H) := \mathbb{T}_{1,G}$.

The interest of the $\mathbb{T}_{1,G}(H)$ is the following:

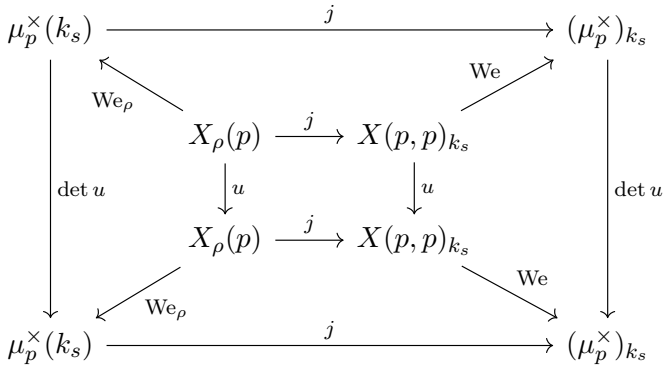
Lemma 3.6.5 *Let k be a field such that p is invertible in k, and let k_s be its separable closure. Let $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ be a group homomorphism with $\det\rho = \omega_p^{-1}$. Then:*

- *$\mathbb{T}[\mathrm{GL}_2(\mathbb{F}_p)]$ naturally embeds in $\mathrm{End}_{k_s}\left(\prod_\xi J_{\rho,\xi}(p)\right)$,*
- *for any $M \in \mathrm{GL}_2(\mathbb{F}_p)$ and any $\xi \in \mu_p^\times$, M acts by a morphism $J_{\rho,\xi}(p)_{k_s} \to J_{\rho,\xi^{\det M}}(p)_{k_s}$ of abelian varieties over k_s,*
- *the image of $\mathbb{T}_{1,\mathrm{GL}_2(\mathbb{F}_p)}$ in $\mathrm{End}(J_\rho(p)_{k_s})$ is contained in $\prod_{\xi\in\mu_p^\times(k_s)} \mathrm{End}_{k_s}(J_{\rho,\xi}(p)_{k_s})$,*
- *the image of $\mathbb{T}_{1,\mathrm{GL}_2(\mathbb{F}_p)}(\mathrm{im}\,\rho)$ in $\mathrm{End}(J_\rho(p)_{k_s})$ is contained in $\prod_{\xi\in\mu_p^\times(k_s)} \mathrm{End}_k(J_{\rho,\xi}(p))$.*

Proof. – By Proposition A.4.39, $\prod_\xi J_{\rho,\xi}(p)$ is the twist of $J(p,p)_k$ by ρ, which means that $\mathbb{T}[\mathrm{GL}_2(\mathbb{F}_p)]$ tautologically embeds in $\mathrm{End}_{k_s}\left(\prod_\xi J_{\rho,\xi}(p)\right)$.

Moreover, any $z \in \mathbb{T}[\mathrm{GL}_2(\mathbb{F}_p)]$ commuting to $\mathrm{im}\,\rho$ has a twist z_ρ as an endomorphism of $\prod_\xi J_{\rho,\xi}(p)$ by Proposition A.1.13.

To conclude, it is enough to show by Proposition 1.5.18 that for any $u \in \mathrm{GL}_2(\mathbb{F}_p)$, u naturally induces a morphism of k_s-schemes: $X_{\rho,\xi}(p)_{k_s} \to X_{\rho,\xi^{\det u}}(p)_{k_s}$. In other words, we have to show that the leftmost cell in the following diagram commutes:



Note that all vertical and horizontal arrows in this diagram are isomorphisms. The top and bottom cells commute because of the properties of twists (Proposition A.1.13 and Proposition 1.4.10), and the same holds for the outer cell. The rightmost cell commutes because of Proposition 1.3.9. The inner cell commutes by definition, so we are done.

□

Definition 3.6.6 Let k be a field with characteristic distinct from p and separable closure k_s. Let $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ be a continuous group homomorphism such that $\det\rho = \omega_p^{-1}$. Let $\Gamma \leq \mathrm{GL}_2(\mathbb{F}_p)$ be a subgroup such that $\mathrm{im}\,\rho$ is contained in the normalizer of Γ. We denote by $\mathbb{T}_{1,\Gamma,\rho}$ the subalgebra of $\mathbb{T}[\Gamma \rtimes_\rho \mathrm{Gal}(k_s/k)]$ generated by the $(T_n \cdot (mI_2))(M,\sigma)$, for $n, m \geq 1, M \in \Gamma, \sigma \in \mathrm{Gal}(k_s/k)$ such that $m^2 n \det M \equiv 1 \pmod p$. It acts by group homomorphisms on $J_{\rho,\xi}(p)(k_s)$ for every $\xi \in \mu_p^\times(k_s)$.

The given elements generate $\mathbb{T}_{1,\Gamma,\rho}$ as a group and $\mathbb{T}_1$ is a central subring of $\mathbb{T}_{1,\Gamma,\rho}$.

Since we have to work with each connected component separately, we will consider $\mathbb{T}_1$-module structures rather than $\mathbb{T}$-module structures.

Definition 3.6.7 For the sake of easier notation, we will write:

- $\mathscr{P}'$ for a system of representatives of $\mathscr{P}$ modulo the complex conjugation,
- $\mathscr{C}_M$ for the $(f,\mathbf{1}) \in \mathscr{C}$ with f CM,

– $\mathscr{C}_1'$ for a system of representatives of $(f,\mathbf{1}) \in \mathscr{C}$ with f not CM and modulo twists by λ.

If $(f,\chi) \in \mathscr{S} \cup \mathscr{P} \cup \mathscr{C}$ and M is a $(\mathbb{T}_1 \otimes F)$-module, its *f-eigenspace* denotes the greatest submodule of M on which every $(nI_2)\cdot T_m$ (for $m,n \geq 1$ coprime to p such that $mn^2 \equiv 1 \pmod p$) acts by $a_m(f)\chi(n)$.

Lemma 3.6.8 *Let M be a $(\mathbb{T}_1 \otimes F)$-module.*

– *Let $(f,\chi) \in \mathscr{S} \cup \mathscr{P} \cup \mathscr{C}$. The functor mapping a $(\mathbb{T} \otimes F)$-module M to its f-eigenspace is exact.*
– *If $(f,\chi) \in \mathscr{P}$ (resp. in $\mathscr{C}$), the f-eigenspace of M is the same as the f'-eigenspace of M, where $(f',\chi') \in \mathscr{P}'$ is either (f,χ) or its complex conjugate (resp. $(f',\chi') \in \mathscr{C}_1' \cup \mathscr{C}_M$ is the unique element such that f' is a twist of f).*
– *M is the direct sum of its f-eigenspaces over all $(f,\chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1' \cup \mathscr{C}_M$.*

Proof. – Let ℓ be any prime number. Then $A := \mathbb{T}_1 \otimes_{\mathbb{Z}} F$ acts faithfully on

$$T := \mathcal{T}_\ell J(p,p) \otimes_{\mathbb{Z}} F \simeq \bigoplus_{\mathfrak{l}|\ell} \mathcal{T}_\ell J(p,p) \otimes_{\mathbb{Z}_\ell} F_{\mathfrak{l}}.$$

By Proposition 3.4.4, T is the sum of the following A-submodules:

- for each $((f,\chi),\psi) \in \mathscr{S} \times \mathcal{D}$, a nonzero submodule where, for any $n,m \geq 1$ coprime to p such that $n^2m \equiv 1 \pmod p$, $(nI_2)\cdot T_m$ acts by $\psi^2(n)a_m(f)\psi(m) = \psi(mn^2)a_m(f) = a_m(f)$,
- for each $((f,\chi),\psi) \in \mathscr{P} \times \mathcal{D}$ (modulo the relation $((f,\chi),\psi) \sim ((\overline{f},\overline{\chi}),\psi\chi)$), a nonzero submodule where, for any $m,n \geq 1$ coprime to p such that $n^2m \equiv 1 \pmod p$, $(nI_2)\cdot T_m$ acts by $\psi^2(n)\chi(n)a_m(f)\psi(m) = \chi(n)a_m(f)$,
- for each $(f,\chi) \in \mathscr{C}$, a nonzero submodule where, for any $m,n \geq 1$ coprime to p such that $n^2m \equiv 1 \pmod p$, $(nI_2)\cdot T_m$ acts by $\chi(n)a_m(f)$.

Let $m,n \geq 1$ be integers coprime to p such that $n^2m \equiv 1 \pmod p$.

For any $(f,\chi) \in \mathscr{P}$, one has $\overline{\chi}(n)a_m(\overline{f}) = \overline{\chi}(nm)a_m(f) = \chi(n)a_m(f)$.

For any $((f,\chi),\psi) \in \mathscr{C} \times \mathcal{D}$, one has $(\chi\psi^2)(n)a_m(f\otimes\psi) = \psi(mn^2)\chi(n)a_m(f) = \chi(n)a_m(f)$. Therefore, T is the sum of its f-eigenspaces over $(f,\chi) \in \Upsilon := \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1' \cup \mathscr{C}_M$.

By Lemma 3.6.2, the eigenspaces attached to any distinct two elements of Υ are distinct. So T is the direct sum, over all $(f,\chi) \in \Upsilon$ of its f-eigenspaces, which are all nonzero.

By construction, for every $(f,\chi) \in \Upsilon$, there is a character $\mu_f : \mathbb{T}_1 \to F$ mapping $(nI_2)\cdot T_m$ (for $m,n \geq 1$ coprime to p such that $n^2m \equiv 1 \pmod p$ is nonzero) to $\chi(n)a_m(f)$, and A acts on T through the F-algebra homomorphism $A \to \prod_{(f,\chi)\in\Upsilon} A/\ker\mu_f$. Since the F-algebra homomorphisms $\mu_f : A \to F$ are pairwise distinct, they have pairwise distinct kernels (which are maximal ideals), so that $A \to \prod_{(f,\chi)\in\Upsilon} A/\ker\mu_f$ is onto. Since $A \to \mathrm{End}_F(T)$ is injective, $A \to \prod_{(f,\chi)\in\Upsilon} A/\ker\mu_f$ is an isomorphism.

In particular, taking the f-eigenspace is exactly equivalent to tensoring with $A \to A/\ker\mu_f$, which is a flat ring homomorphism, whence the conclusion. □

Corollary 3.6.9 *Let $\mathfrak{l}$ be a maximal ideal of $\mathcal{O}_F$ with residue characteristic ℓ. Let k be a field with separable closure k_s, where $p\ell$ is invertible and $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ be a continuous group homomorphism with $\det\rho = \omega_p^{-1}$. Let $\mathcal{O}$ be the ring of integers of the maximal extension of $\mathbb{Q}$ unramified at the characteristic of k, whose Galois group over $\mathbb{Q}$ is $G_{\mathbb{Q},k}$. Fix a ring homomorphism $\iota : \mathcal{O} \to k_s$ and let $e : \mathrm{Gal}(k_s/k) \to G_{\mathbb{Q},k}$ be the attached group homomorphism by Lemma 3.4.6. If $p \equiv 3 \pmod 4$, we denote by $\alpha \in k_s$ a root of the polynomial $X^2 - X - \frac{p+1}{4}$.*

Then the eigenspaces under $\mathbb{T}_1$ of $\mathcal{T}_\ell J(p,p)_\rho \otimes_{\mathbb{Z}_\ell} F_{\mathfrak{l}}$ are the following $(\mathbb{T}_1 \otimes F_{\mathfrak{l}})[\mathrm{Gal}(k_s/k)]$-modules:

– *for $(f,\mathbf{1}) \in \mathscr{S}$, the f-eigenspace is the sum of $p-1$ copies of $(V_{f,\mathfrak{l}} \circ e) \otimes \mathrm{St}(\rho)$,*

– *for* $(f,\chi)\in\mathscr{P}'$, *the* f*-eigenspace is the sum of* $p-1$ *copies of* $(V_{f,\mathfrak{l}}\circ e)\otimes\pi(\mathbf{1},\chi)(\rho)$,
– *for* $(f,\mathbf{1})\in\mathscr{C}_1'$, *the* f*-eigenspace is the sum of* $p-1$ *copies of* $(V_{f,\mathfrak{l}}\circ e)\otimes C_f(\rho)$,
– *for* $(f,\mathbf{1})\in\mathscr{C}_M$, *the* f*-eigenspace is the sum of* $\frac{p-1}{2}$ *copies of*

(i) $\bigoplus_{r\in\{\pm\}}\mathrm{Ind}_{k(\alpha)}^{k}\left[(\psi_{f,r,\mathfrak{l}}\circ e)\otimes C^r(\rho_{|G_{k(\sqrt{-p})}})\right]$ *if* $\omega_p(\mathrm{Gal}(k_s/k))\not\subset\mathbb{F}_p^{\times 2}$ *or equivalently* $\alpha\notin k$ *(if* k *does not have characteristic two, this is equivalent to asking that* $\sqrt{-p}\notin k$*),*

(ii) $\bigoplus_{\theta\in\{\psi_{f,+,\mathfrak{l}}\circ e,\psi_{f,-,\mathfrak{l}}\circ e\}}\mathrm{Ind}_{k(\alpha)}^{k}\left[\theta\otimes C^r(\rho_{|G_{k(\sqrt{-p})}})\right]$ *otherwise (either choice of* $r\in\{\pm\}$ *leads to the same result).*

Proof. – By Lemma 3.6.8, the direct sum of the $\mathbb{T}_1$-eigenspaces for $(f,\chi)\in\mathscr{S}\cup\mathscr{P}'\cup\mathscr{C}_1'\cup\mathscr{C}_M$ is $\mathcal{T}_\ell J(p,p)_\rho\otimes_{\mathbb{Z}_\ell}F_{\mathfrak{l}}$.

Let $((f,\chi),\psi)\in(\mathscr{S}\cup\mathscr{P}')\times\mathcal{D}$. Let V be a $(\mathbb{T}\otimes F)$-module such that for all primes $q\neq p$ (resp. all $n\in\mathbb{F}_p^\times$), T_q (resp. nI_2) acts by $a_q(f)\psi(q)$ (resp. $\chi(n)\psi^2(n)$). Then, for all primes $q\neq p$ and all $n\in\mathbb{F}_p^\times$ with $n^2q\equiv 1\pmod p$, $(nI_2)\cdot T_q$ acts on V by

$$\chi(n)\psi^2(n)a_q(f)\psi(q)=\psi(qn^2)a_q(f)\chi(n)=a_q(f)\chi(n),$$

so V is its own f-eigenspace as a $(\mathbb{T}_1\otimes F)$-module.

Thus, for the eigenspaces attached to elements of $\mathscr{S}\cup\mathscr{P}'$, the claim follows from Corollary 3.4.9.

Let $(f,\chi)\in\mathscr{C}$, then f is the twist by some $\psi\in\mathcal{D}$ of a certain $(g,\mathbf{1})\in\mathscr{C}_1'\cup\mathscr{C}_M$. Let V be a $(\mathbb{T}\otimes F)$-module such that for all primes $q\neq p$ (resp. all $n\in\mathbb{F}_p^\times$), T_q (resp. nI_2) acts by $a_q(f)$ (resp. $\chi(n)$). Then, for all primes $q\neq p$ and all $n\in\mathbb{F}_p^\times$ with $n^2q\equiv 1\pmod p$, $(nI_2)\cdot T_q$ acts on V by $\chi(n)a_q(f)=\psi^2(n)a_q(g)\psi(g)=a_q(g)$, so V is its own f-eigenspace as a $(\mathbb{T}_1\otimes F)$-module.

The application $((f,\mathbf{1}),\psi)\in\mathscr{C}_1'\times\mathcal{D}\longmapsto(f\otimes\psi,\psi^2)\in\mathscr{C}$ is injective and its image is exactly the collection of non-CM modular forms. Moreover, if $(f,\mathbf{1})\in\mathscr{C}_1'\cup\mathscr{C}_M$ and $\psi\in\mathscr{D}$, then, by Corollaries 2.4.15 and B.2.8, one has

$$\begin{aligned}(V_{f\otimes\psi,\mathfrak{l}}\circ e)\otimes C_{f\otimes\psi}(\rho)&\simeq(V_{f,\mathfrak{l}}\circ e)\otimes(\psi(\omega_p)\circ e)\otimes\psi(\det\rho)\otimes C_f(\rho)\\&\simeq\psi(\omega_p\det\rho)\otimes(V_{f,\mathfrak{l}}\otimes e)\otimes C_f(\rho)\simeq(V_{f,\mathfrak{l}}\circ e)\otimes C_f(\rho),\end{aligned}$$

so by Corollary 3.4.9 the description of the eigenspace is correct for all $f\in\mathscr{C}_1'$.

Any $(f,\mathbf{1})\in\mathscr{C}_M$ has exactly $\frac{p-1}{2}$ twists in $\mathscr{C}$, so the f-eigenspace is the direct sum of $\frac{p-1}{2}$ copies of $(V_{f,\mathfrak{l}}\circ e)\otimes C_f(\rho)$. When $\alpha\in k$, this representation decomposes as the stated eigenspace by Propositions 3.5.6(ii) and B.4.1. When $\alpha\notin k$, $[(V_{f,\mathfrak{l}}\circ e)\otimes C_f(\rho)]^{\oplus\frac{p-1}{2}}$ decomposes as the stated eigenspace by Proposition 3.5.6(iv). □

Definition 3.6.10 Let $\mathfrak{l}\subset\mathcal{O}_F$ be a maximal ideal with residue characteristic ℓ. Let k be a field with separable closure k_s and such that $p\ell\in k^\times$. Let $\iota:\mathcal{O}_{\{q\}'}\to k_s$ be a ring homomorphism, which defines a continuous group homomorphism $e:\mathrm{Gal}(k_s/k)\to\mathrm{Gal}(\mathbb{Q}_{\{\ell\}'}/\mathbb{Q})$. Let $\rho:\mathrm{Gal}(k_s/k)\to\mathrm{GL}_2(\mathbb{F}_p)$ be a continuous group homomorphism with $\det\rho=\omega_p^{-1}$. For $(f,\chi)\in\mathscr{S}\cup\mathscr{P}\cup\mathscr{C}$, let $R_{f,\mathfrak{l}}(\rho)$ denote the representation:

- $(V_{f,\mathfrak{l}}\circ e)\otimes\mathrm{St}(\rho)$ if $(f,\chi)\in\mathscr{S}$,
- $(V_{f,\mathfrak{l}}\circ e)\otimes\pi(1,\chi)(\rho)$ if $(f,\chi)\in\mathscr{P}$,
- $(V_{f,\mathfrak{l}}\circ e)\otimes C_f(\rho)$ if $(f,\chi)\in\mathscr{C}$.

The above proof implies that $R_{f,\mathfrak{l}}(\rho)$ does not change if we twist f by a character in $\mathcal{D}$.

Remark The homomorphism e is defined up to conjugation, so the isomorphism class of $R_{f,\mathfrak{l}}(\rho)$ does not depend on the choice of ι. However, as we will see, this does not make the choice of ι irrelevant to our description of the Tate modules.

Proposition 3.6.12 *Let k be a number field and $\rho : G_k \to \mathrm{GL}_2(\mathbb{F}_p)$ be a surjective continuous group homomorphism with $\det\rho = \omega_p^{-1}$. Let ℓ be a prime number and $\mathfrak{l} \subset \mathcal{O}_F$ be a prime ideal of residue characteristic ℓ. For each $\xi \in \mu_p^\times(\overline{k})$, $\mathcal{T}_\ell[\mathrm{Jac}(X_{\rho,\xi})] \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is a $(\mathbb{T}_1 \otimes F_\mathfrak{l})[G_k]$-module, so its eigenspaces (for $\mathbb{T}_1 \otimes F$) are the following irreducible $(\mathbb{T}_1 \otimes F_\mathfrak{l})[G_k]$-modules:*

- *for $(f,\chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1'$, the f-eigenspace is $R_{f,\mathfrak{l}}(\rho)$,*
- *for $(f,\mathbf{1}) \in \mathscr{C}_M$, the f-eigenspace is isomorphic to $\mathrm{Ind}_{k(\sqrt{-p})}^k \psi_{f,r_{f,\rho}(\xi),\mathfrak{l}} \otimes C^+(\rho_{|G_{k(\sqrt{-p})}})$, where $r_{f,\rho} : \xi \in \mu_p^\times(\overline{k})/\mathbb{F}_p^{\times 2} \longmapsto r_{f,\rho}(\xi) \in \{\pm\}$ is a bijection that only depends on f and ρ.*

Proof. – For each $v \in \mathbb{F}_p^\times$, the automorphism vI_2 of $X(p,p)$ (which commutes with Hecke correspondences) induces an isomorphism $vI_2 : X_{\rho,\xi} \to X_{\rho,v^2\xi}$, so that the isomorphism class of $\mathcal{T}_\ell[\mathrm{Jac}(X_{\rho,\xi})] \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ as a $(\mathbb{T}_1 \otimes F_\mathfrak{l})[G_k]$-module only depends on the class of ξ in $\mu_p^\times(\overline{k})/\mathbb{F}_p^{\times 2}$.

For each $v \in \mathbb{F}_p^\times$, the automorphism $\Delta_{v,1}$ of $X(p,p)$ (which also commutes with Hecke correspondences) induces an isomorphism $\Delta_{v,1} : (X_{\rho,\xi})_{\overline{k}} \to (X_{\rho,v\xi})_{\overline{k}}$ respecting the Hecke correspondences, so the isomorphism class of $\mathcal{T}_\ell[\mathrm{Jac}(X_{\rho,\xi})] \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ as a $(\mathbb{T}_1 \otimes F_\mathfrak{l})$-module does not depend on ξ.

By Corollary 3.6.9, the eigenspaces of the $(\mathbb{T}_1 \otimes F_\mathfrak{l})[G_k]$-module $\bigoplus_{\xi \in \mu_p^\times(\overline{k})} \mathcal{T}_\ell[\mathrm{Jac}(X_{\rho,\xi})] \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ are:

- for $(f,\chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1'$, the direct sum of $p-1$ copies of $R_{f,\mathfrak{l}} := R_{f,\mathfrak{l}}(\rho)$,
- for each $(f,\mathbf{1}) \in \mathscr{C}_M$, the direct sum of $\frac{p-1}{2}$ copies of $R_{f,\mathfrak{l}} := R_{f,+,\mathfrak{l}} \oplus R_{f,-,\mathfrak{l}}$, with $R_{f,\epsilon,\mathfrak{l}} := \mathrm{Ind}_{k(\sqrt{-p})}^k \psi_{f,\epsilon,\mathfrak{l}} \otimes C^+(\rho_{|G_{k(\sqrt{-p})}})$.

The $R_{f,\mathfrak{l}}$ (resp. $R_{f,r,\mathfrak{l}}$) are defined over F in the following sense: for any prime ideal $\mathfrak{q} \subset \mathcal{O}_k$ such that ρ is unramified at $\mathfrak{q}$ and the residue characteristic of $\mathfrak{q}$ is coprime to $p\mathfrak{l}$, $\mathrm{Tr}(\mathrm{Frob}_\mathfrak{q} \mid R_{f,\mathfrak{l}})$ (resp. $\mathrm{Tr}(\mathrm{Frob}_\mathfrak{q} \mid R_{f,r,\mathfrak{l}})$) is in $\mathcal{O}_F$ and does not depend on $\mathfrak{l}$ (in other words, they form a compatible system with coefficients in F in the sense of Definition 4.5.2).

The $R_{f,\mathfrak{l}}$ (for $(f,\chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1'$) and the $R_{f,\pm,\mathfrak{l}}$ (for $(f,\chi) \in \mathscr{C}_M$) are irreducible $F_\mathfrak{l}[G_k]$-modules by Corollary 3.5.4 and Proposition 3.5.6.

Let $(f,\chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1'$. For each $\xi \in \mu_p^\times(\overline{k})$, let $T[f,\xi]$ denote the f-eigenspace of $\mathcal{T}_\ell[\mathrm{Jac}(X_{\rho,\xi})] \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$. Then the $p-1$ different $T[f,\xi]$ have the same dimension over $F_\mathfrak{l}$, and their sum is isomorphic to $R_{f,\mathfrak{l}}^{\oplus(p-1)}$, which is a sum of $p-1$ irreducible $(\mathbb{T} \otimes F_\mathfrak{l})[G_k]$-modules, so we must have $T[f,\xi] \simeq R_{f,\mathfrak{l}}$ for each ξ.

Let $(f,\mathbf{1}) \in \mathscr{C}_M$. For each $\xi \in \mu_p^\times(\overline{k})$, let $T[f,\xi]$ be the f-eigenspace of $\mathcal{T}_\ell[\mathrm{Jac}(X_{\rho,\xi})] \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$. We know that

$$\bigoplus_\xi T[f,\xi] \simeq (R_{f,\mathfrak{l}} \oplus R_{f,-,\mathfrak{l}})^{\oplus(p-1)/2},$$

that all the summands on the right-hand side being irreducible, and all the $T[f,\xi]$ have the same dimension over $F_\mathfrak{l}$. Thus each $T[f,\xi]$ is isomorphic to $R_{f,r_{f,\mathfrak{l},\xi},\mathfrak{l}}$, for some sign $r_{f,\mathfrak{l},\xi}$.

Let us fix some $\xi_0 \in \mu_p^\times(\overline{k})$, and let $r_{f,\mathfrak{l}} = r_{f,\mathfrak{l},\xi_0}$. Thus $T[f,\xi_0]$ is isomorphic to $R_{f,r_{f,\mathfrak{l}},\mathfrak{l}}$. Since the isomorphism class of $T[f,\xi]$ only depends on the class of ξ in $\mu_p^\times(\overline{k})/\mathbb{F}_p^{\times 2}$, every $T[f,u^2\xi_0]$ is isomorphic to $R_{f,r_{\mathfrak{l}},\mathfrak{l}}$. Therefore every $T[f,u\xi_0]$ with $u \notin \mathbb{F}_p^{\times 2}$ is isomorphic to $R_{f,-r_{f,\mathfrak{l}},\mathfrak{l}}$.

We now need to show that $(r_{f,\mathfrak{l}})_{f \in \mathscr{C}_M}$ does not depend on $\mathfrak{l}$.

To prove this, let $(r_f)_{f\in\mathscr{C}_M}, (r'_f)_{f\in\mathscr{C}_M}$ be two distinct families of signs, and let us show that there are infinitely many prime ideals $\mathfrak{q} \subset \mathcal{O}_k$ (unramified for ρ and with residual characteristic coprime to $p\ell$) such that the traces of the action of $\mathrm{Frob}_\mathfrak{q}$ on $\bigoplus_f R_{f,r_f,\mathfrak{l}}$ and $\bigoplus_f R_{f,r'_f,\mathfrak{l}}$ has distinct traces.

Let $M \in \mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p)$ be a non-scalar matrix with characteristic polynomial $(X-a)^2$ for some $a \in \mathbb{F}_p^\times$. Write $\alpha = \mathrm{Tr}(M \mid C^+)$ and $\beta = \mathrm{Tr}(M \mid C^-)$, so that $\alpha\beta(\alpha-\beta) \in F^\times$.

Let $\mathfrak{q}$ be any prime such that ρ is unramified at $\mathfrak{q}$, $\rho(\mathrm{Frob}_\mathfrak{q}) \in \mathbb{F}_p^\times M$, and the residue characteristic of $\mathfrak{q}$ is coprime to $p\ell$. We compute that

$$\mathrm{Tr}(\mathrm{Frob}_\mathfrak{q} \mid \bigoplus_f R_{f,r_f,\mathfrak{l}}) = \alpha \sum_f \psi_{f,r_f,\mathfrak{l}}(\mathrm{Frob}_\mathfrak{q}) + \beta \sum_f \psi_{f,-r_f,\mathfrak{l}}(\mathrm{Frob}_\mathfrak{q})$$
$$\mathrm{Tr}(\mathrm{Frob}_\mathfrak{q} \mid \bigoplus_f R_{f,r'_f,\mathfrak{l}}) = \alpha \sum_f \psi_{f,r'_f,\mathfrak{l}}(\mathrm{Frob}_\mathfrak{q}) + \beta \sum_f \psi_{f,-r'_f,\mathfrak{l}}(\mathrm{Frob}_\mathfrak{q}).$$

If, for all but finitely many $\mathfrak{q}$ as above, these two traces are equal, one then has

$$\alpha \sum_f \Big[\psi_{f,r_f,\mathfrak{l}}(\mathrm{Frob}_\mathfrak{q}) - \psi_{f,r'_f,\mathfrak{l}}(\mathrm{Frob}_\mathfrak{q})\Big] = \beta \sum_f \Big[\psi_{f,-r_f,\mathfrak{l}}(\mathrm{Frob}_\mathfrak{q}) - \psi_{f,-r'_f,\mathfrak{l}}(\mathrm{Frob}_\mathfrak{q})\Big]$$

for all but finitely many $\mathfrak{q}$ as above. Fix some $g \in G_k$ such that $\rho(g) = M$. Then, by Cebotarev's theorem, for any $h \in H := \ker \rho : G_k \to \mathrm{PGL}_2(\mathbb{F}_p) \triangleleft G_{k(\sqrt{-p})}$,

$$\alpha \sum_f \Big[\psi_{f,r_f,\mathfrak{l}}(gh) - \psi_{f,r'_f,\mathfrak{l}}(gh)\Big] = \beta \sum_f \Big[\psi_{f,-r_f,\mathfrak{l}}(gh) - \psi_{f,-r'_f,\mathfrak{l}}(gh)\Big].$$

Since $G_{k(\sqrt{-p})}/H \simeq \mathrm{PSL}_2(\mathbb{F}_p)$ is a perfect group, $H \to G^{ab}_{k(\sqrt{-p})}$ is surjective. Thus, the following identity holds on $G^{ab}_{k(\sqrt{-p})}$:

$$\alpha \sum_f \Big[\psi_{f,r_f,\mathfrak{l}} - \psi_{f,r'_f,\mathfrak{l}}\Big] = \beta \sum_f \Big[\psi_{f,-r_f,\mathfrak{l}} - \psi_{f,-r'_f,\mathfrak{l}}\Big].$$

The $\psi_{f,r,\mathfrak{l}}$ (over all possible f and r) are pairwise distinct characters (because, by [132, Theorem 4.3], $\frac{\psi_{f,+,\mathfrak{l}}}{\psi_{f,-,\mathfrak{l}}} : G_{\mathbb{Q}(\sqrt{-p})} \to F_\mathfrak{l}^\times$ has infinite image), and $\alpha\beta(\alpha-\beta) \in F^\times$, this implies that $r_f = r'_f$ for all f.

Now, let $\mathfrak{l}, \mathfrak{l}' \subset \mathcal{O}_F$ be two distinct maximal ideals with residue characteristics ℓ, ℓ', $\xi \in \mu_p^\times(\overline{k})$. Let $\mathfrak{q} \subset \mathcal{O}_F$ be any prime ideal such that ρ is unramified at $\mathfrak{q}$ and $\mathfrak{q}$ is coprime to $p\ell\ell'$. We can then compute in F that

$$\begin{aligned}
\mathrm{Tr}(\mathrm{Frob}_\mathfrak{q} \mid \bigoplus_f R_{f,r_{f,\mathfrak{l},\xi},\mathfrak{l}}) &= \mathrm{Tr}(\mathrm{Frob}_\mathfrak{q} \mid \mathcal{T}_\ell \mathrm{Jac}(X_{\rho,\xi})) - \sum_{(f,\chi)\in\mathscr{S}\cup\mathscr{P}'\cup\mathscr{C}'_1} \mathrm{Tr}(\mathrm{Frob}_\mathfrak{q} \mid R_{f,\mathfrak{l}}) \\
&= \mathrm{Tr}(\mathrm{Frob}_\mathfrak{q} \mid \mathcal{T}_{\ell'} \mathrm{Jac}(X_{\rho,\xi})) - \sum_{(f,\chi)\in\mathscr{S}\cup\mathscr{P}'\cup\mathscr{C}'_1} \mathrm{Tr}(\mathrm{Frob}_\mathfrak{q} \mid R_{f,\mathfrak{l}'}) \\
&= \mathrm{Tr}(\mathrm{Frob}_\mathfrak{q} \mid \bigoplus_f R_{f,r_{f,\mathfrak{l}',\xi},\mathfrak{l}'}) = \mathrm{Tr}(\mathrm{Frob}_\mathfrak{q} \mid \bigoplus_f R_{f,r_{f,\mathfrak{l}',\xi},\mathfrak{l}}).
\end{aligned}$$

By the above argument, this identity implies that

$$(r_{f,\mathfrak{l},\xi})_{(f,\mathbf{1})\in\mathscr{C}_M} = (r_{f,\mathfrak{l}',\xi})_{(f,\mathbf{1})\in\mathscr{C}_M},$$

whence the conclusion. □

To be able to handle a representation ρ over an arbitrary field, we need to keep track of the action of $\mathrm{GL}_2(\mathbb{F}_p)$ compatibly with the action of $G_\mathbb{Q}$. To do that, we need ways to describe representations of profinite groups when they are only well-known on open subgroups.

Lemma 3.6.13 *Let G be a profinite group and $K \triangleleft G$ be an open subgroup. Let V_1, V_2 be two finite-dimensional continuous representations of G over a p-adic field F. Assume that $(V_1)_{|K}$ is*

absolutely irreducible and $(V_2)_{|K}$ is a direct sum of copies of $(V_1)_{|K}$. Then there is a representation W of G/K over F such that $V_2 \simeq V_1 \otimes W$.

Proof. – By the assumptions, the $F[G/K]$-module $W := \mathrm{Hom}_{F[K]}(V_1, V_2)$ has dimension $\frac{\dim V_2}{\dim V_1}$ over F, and the obvious map $V_1 \otimes W \to V_2$ (which is G-equivariant) is onto. Since it is a linear morphism between F-vector space of the same finite dimension, it is an isomorphism. □

Lemma 3.6.14 *Let G be a profinite group, $G_2 \triangleleft G$ be an open subgroup of index two, and $K \triangleleft G$ an open subgroup contained in G_2. Let F be a p-adic field and $\psi, \psi' : G_2 \to F^\times$ be continuous characters, conjugate under G/G_2, such that $\psi^{-1}\psi'$ has infinite image. Let V be a finite-dimensional continuous representation of G over F such that $V_{|K}$ is isomorphic to a direct sum of copies of $\left[\mathrm{Ind}_{G_2}^G \psi\right]_{|K}$. Then there exists a continuous finite-dimensional representation W of G_2/K over F such that $V \simeq \mathrm{Ind}_{G_2}^G[\psi \otimes W]$.*

Proof. – Let $W = \mathrm{Hom}_{F[K]}(\psi, V)$, then W is a finite-dimensional $F[G_2/K]$-module and its dimension over F is exactly $\frac{\dim V}{2}$. The canonical morphism $u : \psi \otimes W \to V$ is $F[G_2]$-linear, and its image is exactly the ψ-isotypic component V_2 of $V_{|K}$. Then the induced morphism $f : \mathrm{Ind}_{G_2}^G[\psi \otimes W] \to V$ is $F[G]$-equivariant between finite-dimensional F-vector spaces of same dimension. Its image contains the sub-G-module generated by V_2, which is V, so f is onto, so f is an isomorphism. □

Lemma 3.6.15 *Let k be a field with characteristic not p and $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ be a continuous group homomorphism with $\det \rho = \omega_p^{-1}$. Then the actions of $\mathrm{GL}_2(\mathbb{F}_p)$ and $\mathrm{Gal}(k_s/k)$ by $\mathbb{T}$-endomorphisms of $J_\rho(p)(k_s)$ factor through the group $\mathrm{GL}_2(\mathbb{F}_p) \rtimes_\rho \mathrm{Gal}(k_s/k)$, whose product law is $(M, g)(M', g') = (M\rho(g)M'\rho(g)^{-1}, gg')$.*

Proof. – For any $N \in \mathrm{GL}_2(\mathbb{F}_p)$ and any $\sigma \in \mathrm{Gal}(k_s/k)$, the following diagrams are commutative by Proposition A.1.11, and the actions of $\mathrm{Gal}(k_s/k)$ and $\mathrm{GL}_2(\mathbb{F}_p)$ commute on $J(p,p)(k_s)$.

$$\begin{array}{ccc} J_\rho(p)(k_s) & \xrightarrow{j} & J(p,p)(k_s) \\ \downarrow N & & \downarrow N \\ J_\rho(p)(k_s) & \xrightarrow{j} & J(p,p)(k_s) \end{array} \qquad \begin{array}{ccc} J_\rho(p)(k_s) & \xrightarrow{j} & J(p,p)(k_s) \\ \downarrow \sigma & & \downarrow \rho(\sigma)\circ\sigma \\ J_\rho(p)(k_s) & \xrightarrow{j} & J(p,p)(k_s). \end{array}$$

Thus, for any $M \in \mathrm{GL}_2(\mathbb{F}_p)$ and $\sigma \in \mathrm{Gal}(k_s/k)$, the $\mathbb{T}$-endomorphism of $J_\rho(p)(k_s)$ induced by $\sigma \circ M$ is the same as the one induced by $\rho(\sigma)M\rho(\sigma)^{-1}\sigma$, and the conclusion follows. □

Proposition 3.6.16 *In the situation of Proposition 3.6.12, write $G_{k,\rho} := \mathrm{SL}_2(\mathbb{F}_p) \rtimes_\rho \mathrm{Gal}(\overline{k}/k)$ for the sake of easier notation and $\widetilde{\rho}$ be the homomorphism $(M, \sigma) \in G_{k,\rho} \mapsto M\rho(\sigma) \in \mathrm{GL}_2(\mathbb{F}_p)$. It is endowed with a natural morphism to G_k, which we omit from the notation. When $p \equiv 3 \pmod 4$, we denote by G_2 the subgroup $\mathrm{SL}_2(\mathbb{F}_p) \rtimes_\rho \mathrm{Gal}(\overline{k}/k(\sqrt{-p})) = \widetilde{\rho}^{-1}(\mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p))$.*

For each $\xi \in \mu_p^\times(\overline{k})$, $\mathcal{T}_\ell[\mathrm{Jac}(X_{\rho,\xi})] \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is a $(\mathbb{T}_1 \otimes F_\mathfrak{l})[G_{k,\rho}]$-module, so its eigenspaces (for $\mathbb{T}_1 \otimes F$) are the following irreducible $(\mathbb{T}_1 \otimes F_\mathfrak{l})[G_{k,\rho}]$-modules:

- *for $(f, \chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1'$, the f-eigenspace is $V_{f,\mathfrak{l}} \otimes \mathrm{St}(\widetilde{\rho})$,*
- *for $(f, \chi) \in \mathscr{P}'$, the f-eigenspace is $V_{f,\mathfrak{l}} \otimes \pi(\mathbf{1}, \chi)(\widetilde{\rho})$,*
- *for $(f, \mathbf{1}) \in \mathscr{C}_1'$, the f-eigenspace is $V_{f,\mathfrak{l}} \otimes C_f(\widetilde{\rho})$,*
- *for $(f, \mathbf{1}) \in \mathscr{C}_M$, there exists a bijection $r_{f,\rho} : \xi \in \mu_p^\times(\overline{k})/\mathbb{F}_p^{\times 2} \longmapsto r_f(\xi) \in \{\pm\}$ (which is independent from $\mathfrak{l}$) such that the f-eigenspace is isomorphic to $\mathrm{Ind}_{G_2}^G \psi_{f,r,\mathfrak{l}} \otimes C^+(\widetilde{\rho}_{|G_2})$.*

Proof. – For $(f, \chi) \in \mathscr{S}$ (resp. $(f, \chi) \in \mathscr{P}'$, resp. $(f, \chi) \in \mathscr{C}_1'$), let $E_{f,\mathfrak{l},\xi}$ be the f-eigenspace of $\mathcal{T}_\ell[\mathrm{Jac}(X_{\rho,\xi})] \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ as a $(\mathbb{T}_1 \otimes F_\mathfrak{l})[G_{k,\rho}]$-module. Let furthermore $R_{f,\mathfrak{l}}(\widetilde{\rho})$ denote the $(\mathbb{T}_1 \otimes F_\mathfrak{l})[G_{k,\rho}]$-module $V_{f,\mathfrak{l}} \otimes \mathrm{St}(\widetilde{\rho})$ (resp. $V_{f,\mathfrak{l}} \otimes \pi(1, \chi)(\widetilde{\rho})$, resp. $V_{f,\mathfrak{l}} \otimes C_f(\widetilde{\rho})$).

By Proposition 3.6.12, all the $E_{f,\mathfrak{l},\xi}$ are isomorphic, as $(\mathbb{T}_1 \otimes F_\mathfrak{l})[G_k]$-modules, to $R_{f,\mathfrak{l}}(\widetilde{\rho})$, and both are irreducible as $F_\mathfrak{l}[G_k]$-modules. In particular, the $E_{f,\mathfrak{l},\xi}$ and the $R_{f,\mathfrak{l}}(\widetilde{\rho})$ are all irreducible as $(\mathbb{T}_1 \otimes F_\mathfrak{l})[G_{k,\rho}]$-modules.

The direct sum of the $E_{f,\mathfrak{l},\xi}$ is the f-eigenspace of $\mathcal{T}_\ell J_\rho(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$, which is isomorphic over $(\mathbf{T}_1 \otimes_{\mathbb{Z}} F_\mathfrak{l})[G_{k,\rho}]$ by Corollaries 3.4.4 and 3.6.9 to $R_{f,\mathfrak{l}}(\widetilde{\rho})^{\oplus(p-1)}$. By uniqueness of the decomposition into irreducible factors, for every ξ, one has $E_{f,\mathfrak{l},\xi} \simeq R_{f,\mathfrak{l}}(\widetilde{\rho})$.

Let now $(f,\mathbf{1}) \in \mathscr{C}_M$. For $r \in \{\pm\}$, let $R_{f,r,\mathfrak{l}}(\widetilde{\rho}) = \mathrm{Ind}_{G_2}^{G} \psi_{f,r,\mathfrak{l}} \otimes C^+(\widetilde{\rho}_{|G_2})$ as a $(\mathbb{T}_1 \otimes F_\mathfrak{l})[G_{k,\rho}]$-module (where $(mI_2)\cdot T_n$ acts by $a_n(f)$ for any $n,m \geq 1$ with $nm^2 \equiv 1 \pmod p$). Let $E_{f,\mathfrak{l},\xi}$ be, for any $\xi \in \mu_p^\times(\overline{k})$, the f-eigenspace of $\mathcal{T}_\ell J_{\rho,\xi}(p)$ as a $(\mathbb{T}_1 \otimes F_\mathfrak{l})[G_{k,\rho}]$-module.

We know by Proposition 3.6.12 that $E_{f,\mathfrak{l},\xi}$ and $R_{f,r_{f,\rho}(\xi),\mathfrak{l}}(\widetilde{\rho})$ are isomorphic when restricted to $\{1\} \times G_k$, and that they are irreducible as $F_\mathfrak{l}[G_k]$-modules. Therefore, the $E_{f,\mathfrak{l},\xi}$ and $R_{f,r,\mathfrak{l}}(\widetilde{\rho})$ are irreducible $F_\mathfrak{l}[G_{k,\rho}]$-modules.

Moreover, $\bigoplus_{\xi \in \mu_p^\times(\overline{k})} E_{f,\mathfrak{l},\xi}$ is the f-eigenspace of $\mathcal{T}_\ell J_\rho(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$, which is isomorphic by Corollaries 3.4.4 and 3.6.9 to

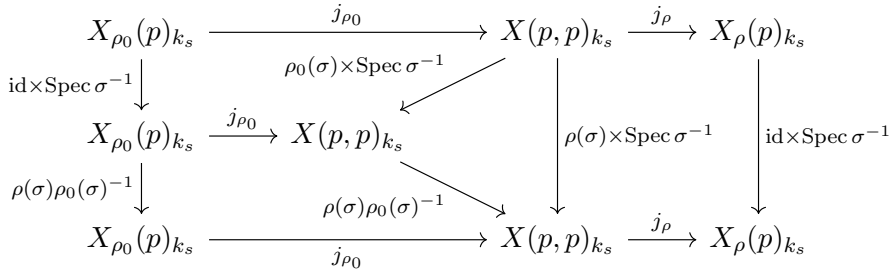
$$V_{f,\mathfrak{l}} \otimes C_f(\widetilde{\rho})^{\oplus(p-1)} \simeq \mathrm{Ind}_{G_2}^{G_{k,\rho}}(\psi_{f,+,\mathfrak{l}} \oplus \psi_{f,-,\mathfrak{l}}) \otimes C^+(\widetilde{\rho})^{\oplus\frac{p-1}{2}} \simeq R_{f,+,\mathfrak{l}}(\widetilde{\rho})^{\oplus\frac{p-1}{2}} \oplus R_{f,-,\mathfrak{l}}(\widetilde{\rho})^{\oplus\frac{p-1}{2}}.$$

Therefore, there exists a morphism $r : \mu_p^\times(k_s) \to \{\pm\}$ such that all of its fibres have cardinality $\frac{p-1}{2}$ and every $E_{f,\mathfrak{l},\xi}$ is isomorphic to one $R_{f,r(\xi),\mathfrak{l}}(\widetilde{\rho})$. For any $n \in \mathbb{F}_p^\times$, $nI_2 : E_{f,\mathfrak{l},\xi} \to E_{f,\mathfrak{l},\xi^{n^2}}$ is an isomorphism of $(\mathbb{T}_1 \otimes F_\mathfrak{l})[G_{k,\rho}]$-modules; therefore, we may choose r so that it is a bijection $\mu_p^\times(k_s)/\mathbb{F}_p^{\times 2} \to \{\pm 1\}$.

□

Lemma 3.6.17 *Let k be a field with characteristic distinct from p and k_s be a separable closure for k. Let $\rho, \rho_0 : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ be two continuous group homomorphisms with $\det\rho = \det\rho_0 = \omega_p^{-1}$. Then the function $\rho\rho_0^{-1} : \mathrm{Gal}(k_s/k) \to \mathrm{SL}_2(\mathbb{F}_p)$ is a cocycle in the sense of Proposition A.1.11; for any $\xi \in \mu_p^\times(k_s)$, the twist of $X_{\rho_0,\xi}(p)$ is $X_{\rho,\xi}(p)$, and this identification is compatible with the action of $\mathbb{T}_{1,\{1\}}$ on the Jacobians.*

Proof. – For any $\sigma \in \mathrm{Gal}(k_s/k)$, consider the following diagram:



This diagram implies that $\sigma \in \mathrm{Gal}(k_s/k) \longmapsto \rho(\sigma)\rho_0(\sigma)^{-1} \in \mathrm{SL}_2(\mathbb{F}_p) \to \mathrm{Aut}_{k_s}(X_{\rho_0}(p))$ satisfies the cocycle relation of Proposition A.1.11, and that $X_\rho(p)$ is the twist of $X_{\rho_0}(p)$ by this cocycle. Moreover, by Lemma 3.6.5, because it takes its values in $\mathrm{SL}_2(\mathbb{F}_p)$, this cocycle leaves invariant the morphism to the constant k-scheme with underlying set $\mu_p^\times(k_s)$ defined in Proposition 1.4.10. Thus the twist of $X_{\rho_0}(p) \to \mu_p^\times(k_s)$ by the cocycle $\rho\rho_0^{-1}$ is exactly $X_\rho(p) \to \mu_p^\times(k_s)$.

Therefore, for every $\xi \in \mu_p^\times(k_s)$, $X_{\rho,\xi}(p)$ is the twist of $X_{\rho_0,\xi}(p)$ by the cocycle

$$\rho\rho_0^{-1} : \mathrm{Gal}(k_s/k) \to \mathrm{SL}_2(\mathbb{F}_p) \subset \mathrm{Aut}_{k_s}(X_{\rho_0,\xi}(p)).$$

This twist preserves (by definition) the geometric actions of $\mathrm{GL}_2(\mathbb{F}_p)$, and by Propositions A.4.39, A.4.40, it also preserves the actions of $\mathbb{T}$. □

Corollary 3.6.18 *Let $\mathfrak{l} \subset \mathcal{O}_F$ be a maximal ideal with residue characteristic ℓ. Let k_s be a separable closure of k and $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ such that $\det \rho = \omega_p^{-1}$. Let k be a field of characteristic zero with separable closure $\iota : \overline{\mathbb{Q}} \to k_s$ be a ring homomorphism, inducing a continuous group homomorphism $R_\iota : \mathrm{Gal}(k_s/k) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $G_{k,\rho}$ be the group $\mathrm{SL}_2(\mathbb{F}_p) \rtimes_\rho \mathrm{Gal}(k_s/k)$, which is endowed with a group homomorphism $\widetilde{\rho} : (M,\sigma) \in G_{k,\rho} \longmapsto M\rho(\sigma)$.*

Then, for $(f,\chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1' \cup \mathscr{C}_M$ and $\xi \in \mu_p^\times(k_s)$, the f-eigenspace of $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is isomorphic as a $F_\mathfrak{l}[G_{k,\rho}]$-module to the following:

- *$V_{f,\mathfrak{l}}(R_\iota) \otimes \mathrm{St}(\widetilde{\rho})$ when $(f,\chi) \in \mathscr{S}$,*
- *$V_{f,\mathfrak{l}}(R_\iota) \otimes \pi(1,\chi)(\widetilde{\rho})$ when $(f,\chi) \in \mathscr{P}'$,*
- *$V_{f,\mathfrak{l}}(R_\iota) \otimes C_f(\widetilde{\rho})$ when $(f,\chi) \in \mathscr{C}_1'$,*
- *when $(f,\chi) \in \mathscr{C}_M$, let $k' = k(\sqrt{-p}) \subset k_s$, and $G_{k',\rho} = \mathrm{SL}_2(\mathbb{F}_p) \rtimes_\rho \mathrm{Gal}(k_s/k')$. There is a unique $r \in \{\pm\}$ depending only in $\iota^{-1}(\xi)$ such that the eigenspace is isomorphic to:*
  - *$\mathrm{Ind}_{G_{k',\rho}}^{G_{k,\rho}} \psi_{f,r,\mathfrak{l}}(R_\iota) \otimes C^+(\widetilde{\rho}_{|G_{k',\rho}})$ if $k' \neq k$,*
  - *$\bigoplus_{s\in\{\pm\}} \psi_{f,rs,\mathfrak{l}}(R_\iota) \otimes C^s(\widetilde{\rho})$ if $k = k'$.*

Proof. – If $\overline{L}$ is a separable closure of some field extension L/k endowed with a k-embedding $\iota' : k_s \to \overline{L}$, there is a natural a group homomorphism $R_{\iota'} : \mathrm{Gal}(\overline{L}/L) \to \mathrm{Gal}(k_s/k)$. For any $\zeta \in \mu_p^\times(k_s)$, it is then direct to see that $X_{\rho,\zeta}(p)_L$ is naturally isomorphic to $X_{\rho\circ R_{\iota'},\iota'(\zeta)}(p)_L$. In particular, if the description is correct for ρ, it is correct for $\rho \circ R_{\iota'}$.

Therefore, by Lemma 3.6.17, to prove the Proposition, it is enough to find a single representation $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_p)$ with determinant ω_p^{-1} for which the claim is correct. Thanks to Proposition 3.6.16, it is enough to find a single surjective representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ with $\det \rho = \omega_p^{-1}$.

By [141, Cor. 1 à Prop. 21], if $E/\mathbb{Q}$ is a semi-stable elliptic curve with good reduction at 2 – such as the elliptic curve with LMFDB label [107] 11.*a*3 and Weierstrass equation $y^2 - y = x^3 - x^2$ – then, for any basis (P,Q) of $E[p]$, the group homomorphism $\sigma \longmapsto \rho(\sigma)$ (defined for any $\sigma \in G_\mathbb{Q}$ by $\rho(\sigma)\begin{pmatrix}\sigma(P)\\ \sigma(Q)\end{pmatrix} = \begin{pmatrix}P\\ Q\end{pmatrix}$ – it is a group homomorphism by Lemma 1.4.2) satisfies the requirements. □

Remark Let $E/\mathbb{Q}$ be an elliptic curve and fix a basis (P,Q) of its p-torsion module. Let $\zeta = \langle P, Q\rangle \in \mu_p^\times(\overline{\mathbb{Q}})$ and $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_p)$ the group homomorphism given by

$$\forall g \in G_\mathbb{Q},\ \begin{pmatrix}g(P)\\ g(Q)\end{pmatrix} = \rho(g)^{-1}\begin{pmatrix}P\\ Q\end{pmatrix}.$$

For any $\alpha \in \mathbb{F}_p^\times$, $X_E^\alpha(p)$ identifies with $X_{\rho,\zeta^\alpha}(p)$ in a way that respects the Hecke correspondences. Can one describe the CM eigenspaces of the Tate module of $\mathrm{Jac}(X_E^\alpha(p)) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ in a way which is independent from the choice of ρ?

A possible approach could be to reparametrize the CM eigenspaces in the following more canonical way. First, the two compatible systems of characters $\psi_{f,\pm,\mathfrak{l}}$ can be parametrized in a choice-free way by the two embeddings $\mathbb{Q}(\sqrt{-p}) \to F$. Second, a completely choice-free parametrization for the set of representations $\{C^+, C^-\}$ of $\mathbb{F}_p^\times SL(V)$ (where V is a two-dimensional vector space over $\mathbb{F}_p$, with $p \equiv 3 \pmod 4$) with coefficients in F is by the pairs $([U],\xi)$, where $[U]$ represents a conjugacy class of unipotent element in $SL(V)$ and $\xi \in \mu_p^\times(F)/\mathbb{F}_p^{\times 2}$ corresponds to the eigenvalues of the representation at any element in $[U]$. Note that the pair $([U],\xi)$ describes the same representation as $([U^{-1}],\xi^{-1})$.

Let $\rho_E : G_\mathbb{Q} \to GL(E[p])$ be the Galois representation attached to E. Fix any basis (P,Q) of $E[p](\overline{\mathbb{Q}})$. It defines the conjugacy class $[U]$ of the unipotent automorphism $(P,Q) \mapsto (P, P+Q)$ of $E[p]$, and the root of unity $\xi = \langle P, Q\rangle \in \mu_p^\times(\overline{\mathbb{Q}})$. Then $\xi^{\mathbb{F}_p^{\times 2}}$ is defined over[4] $\mathbb{Q}(\sqrt{-p}) \subset \overline{\mathbb{Q}}$, so,

[4]Note how the following inclusion is necessary to even define ψ_σ.

for any embedding $\sigma : \mathbb{Q}(\sqrt{-p}) \to F$, it makes sense to define $\sigma(\xi)$ as an element of $\mu_p^\times(F)/\mathbb{F}_p^{\times 2}$. Thus, for $(f, \mathbf{1}) \in \mathscr{C}_M$, the f-eigenspaces of $\mathcal{T}_\ell \mathrm{Jac}(X_E^1(p)) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ and $\mathcal{T}_\ell \mathrm{Jac}(X_E^{-1}(p)) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ are given (up to re-ordering) by the couple

$$\mathcal{E}_{f,E} := \left(\mathrm{Ind}_{\mathbb{Q}(\sqrt{-p})}^{\mathbb{Q}}\left[\psi_\sigma \otimes C_{[U],\sigma(\xi)}((\rho_E)_{|G_{\mathbb{Q}(\sqrt{-p})}})\right], \mathrm{Ind}_{\mathbb{Q}(\sqrt{-p})}^{\mathbb{Q}}\left[\psi_\sigma \otimes C_{[U],\sigma(\xi)^{-1}}((\rho_E)_{|G_{\mathbb{Q}(\sqrt{-p})}})\right]\right),$$

where $\sigma : \mathbb{Q}(\sqrt{-p}) \to F$ is an embedding. Note that $\mathcal{E}_{f,E}$ is independent from the choices of σ and of the basis (P, Q). Hence, it seems logical (and can probably be proved in the same way as Corollary 3.6.18) that one of the following is true:

- either, for every elliptic curve $E/\mathbb{Q}$, $\mathcal{E}_{f,E}$ is equal to the couple made with the f-eigenspaces of $\mathcal{T}_\ell \mathrm{Jac}(X_E^1(p)) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ and $\mathcal{T}_\ell \mathrm{Jac}(X_E^{-1}(p)) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ in this order,
- or, for every elliptic curve $E/\mathbb{Q}$, $\mathcal{E}_{f,E}$ is equal to the couple made with the f-eigenspaces of $\mathcal{T}_\ell \mathrm{Jac}(X_E^{-1}(p)) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ and $\mathcal{T}_\ell \mathrm{Jac}(X_E^1(p)) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ in this order.

It seems numerically possible (when p is small enough for $X_E^\alpha(p)$ to have an explicit model, for a given elliptic curve E) to decide which alternative is correct, but we were not able to find any general argument to privilege one choice over the other in general. In particular, is there any reason to believe that the same alternative is correct, no matter what $(f, \mathbf{1}) \in \mathscr{C}_M$ or p are?

We now want to prove the equivalent of Corollary 3.6.18 in positive characteristic. The same argument as the previous proof shows that it is enough to prove the result for a single representation $\rho : \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \to \mathrm{GL}_2(\mathbb{F}_p)$. Using the ideas of Proposition 3.6.16 does not work for several reasons: because $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ is pro-cyclic, $(V_{f,\mathfrak{l}})_{|\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)}$ is never absolutely irreducible, and ρ cannot be surjective because $\mathrm{GL}_2(\mathbb{F}_p)$ is not solvable.

The idea is to take for ρ the restriction of a global representation to a decomposition subgroup, and this idea is better expressed using the relative curves $X_{G,u}(p)$ as in Section 1.3 and fundamental groups. First, we carefully specify the relationship between Galois groups and fundamental groups in the following Lemma (which is a simple verification).

Definition 3.6.20 Let X be a scheme and $\mathbf{FinÉt}_X$ denote the category of finite étale surjective X-schemes. Let $\overline{x} : \mathrm{Spec}\,\Omega \to X$ be a geometric point (that is, Ω is an algebraically closed field), the *fundamental group* $\pi_1(X, \overline{s})$ is the group of automorphisms of the functor $\mathbf{FinÉt}_X \to \mathbf{FinSet}$ given by $U \longmapsto U_{\overline{x}}$.

Lemma 3.6.21 *Let k be a field with separable closure k_s. For every finite étale k-scheme Y, let Y_{k_s} denote the underlying set of the finite étale k_s-scheme $Y \times_k \mathrm{Spec}\,k_s$, and let ι_Y denote the bijection $Y(k_s) \to Y \times_k \mathrm{Spec}\,k_s$ defined as follows: for $f : \mathrm{Spec}\,k_s \to Y$, $\iota_Y(f)$ is the image of the morphism $\mathrm{Spec}\,k_s \xrightarrow{(f,\mathrm{id})} Y \times_k \mathrm{Spec}\,k_s$. Then the collection of the ι_Y is an isomorphism of functors $\mathbf{FinÉt}_k \to \mathbf{FinSet}$. Moreover, for any finite étale k-scheme Y and every $\sigma \in \mathrm{Gal}(k_s/k)$, the following diagram commutes:*

$$\begin{array}{ccc} Y(k_s) & \xrightarrow{P \longmapsto (P \circ \mathrm{Spec}\,\sigma)} & Y(k_s) \\ \downarrow{\scriptstyle \iota_Y} & & \downarrow{\scriptstyle \iota_Y} \\ Y \times_k \mathrm{Spec}\,k_s & \xrightarrow{\mathrm{id} \times \mathrm{Spec}\,\sigma^{-1}} & Y \times_k \mathrm{Spec}\,k_s \end{array}$$

In particular, if α is the geometric point $\mathrm{Spec}\,\Omega \to \mathrm{Spec}\,k$ for some algebraically closed extension Ω of k_s, this defines a morphism $\mathrm{Gal}(k_s/k) \to \pi_1(\mathrm{Spec}\,k, \alpha)$: for every finite étale k-scheme Y, any $\sigma \in \mathrm{Gal}(k_s/k)$ acts on the set of points Y_α (which is the same as the set of points of Y_{k_s}) by $\mathrm{id} \times \mathrm{Spec}\,\sigma^{-1}$.

Remark In the situation of Definition 3.6.20, let $x \in X$ be the image of $\overline{x}$, $\kappa(x)$ denote its residue field and $\overline{\kappa(x)}$ be the separable closure of $\kappa(x)$ in Ω. Lemma 3.6.21 means that $g \in \mathrm{Gal}(\overline{\kappa(x)}/\kappa(x)) \longmapsto (\mathrm{id} \times \mathrm{Spec}\, g^{-1}) \in \pi_1(X, \overline{x})$ is a group homomorphism and that it is compatible with the expected Galois actions on $X(\overline{\kappa(x)})$.

The following Lemma describes how to apply the formalism of fundamental groups in our situation.

Lemma 3.6.23 *Let ℓ be a prime number, $\mathfrak{l}$ be a prime ideal of $\mathcal{O}_F$ containing ℓ. Let S be an affine, connected, regular excellent Noetherian $\mathbb{Z}[(p\ell)^{-1}]$-scheme. Let G be a polarized p-torsion group over S and let, for each $u \in \mathbb{F}_p^\times$, $X_u := X_{G,u}(p)$ (see Section 1.3), which is a smooth proper S-scheme of relative dimension one with connected geometric fibres.*

Let $\mathcal{O}_{p\ell}$ be the ring of integers of the maximal algebraic extension $\mathbb{Q}_{\{p,\ell\}}$ of $\mathbb{Q}$ which is unramified outside p and ℓ. Let $\overline{s}$ be a geometric point of S above a topological point $s \in S$. Choose a morphism $\iota_{\overline{s}} : \mathcal{O}_{p\ell} \to \kappa(\overline{s})$: it defines a morphism $R_\iota : \pi_1(S, \overline{s}) \to \mathrm{Gal}(\mathbb{Q}_{\{p,\ell\}}/\mathbb{Q})$ (whose conjugacy class does not depend on $\iota_{\overline{s}}$).

Let (P, Q) be a basis of $G(\kappa(\overline{s}))$ with $\zeta = \langle P, Q\rangle_G \in \mu_p^\times(\kappa(\overline{s}))$. For each $g \in \pi_1(S, \overline{s})$, let $D(g) \in \mathrm{GL}_2(\mathbb{F}_p)$ be the unique matrix such that $\begin{pmatrix} g(P) \\ g(Q) \end{pmatrix} = D(g) \begin{pmatrix} P \\ Q \end{pmatrix}$. Then

$$\rho_{\overline{s}} := D^{-1} : \pi_1(S, \overline{s}) \to \mathrm{GL}_2(\mathbb{F}_p)$$

is a group homomorphism.

The mod p cyclotomic character ω_p is also a well-defined homomorphism $\pi_1(S, \overline{s}) \to \mathbb{F}_p^\times$. Its restriction to $\mathrm{Gal}(\overline{\kappa(s)}/\kappa(s))$ is the usual mod p cyclotomic character; moreover, $\det \rho_{\overline{s}} = \omega_p^{-1}$.

Let $\overline{\kappa(s)}$ denote the separable closure of $\kappa(s)$ in $\kappa(\overline{s})$, then $\rho_s := (\rho_{\overline{s}})_{|\mathrm{Gal}(\overline{\kappa(s)}/\kappa(s))}$ identifies with the representation attached to the basis (P, Q) of the polarized p-torsion group G_s over $\kappa(s)$, and $(R_{\iota_{\overline{s}}})_{|\mathrm{Gal}(\overline{\kappa(s)}/\kappa(s))}$ is exactly the group homomorphism R_ι defined in Lemma 3.4.6. Furthermore, every $(X_u)_s$ is isomorphic to $X_{\rho_s, \zeta^u}(p)$, and the extension of this isomorphism to the Jacobians of these curves respects the Hecke correspondences.

Let S_0 be a finite étale connected S-scheme endowed with a geometric point $\overline{s}_0$ lifting $\overline{s}$ such that P, Q lift to $G(S_0)$. There is a natural action of $\mathrm{SL}_2(\mathbb{F}_p)$ on $X_{G,u}(p) \times_S S_0$ for any u such that the isomorphism $(X_{G,u} \times_S S_0) \times_{S_0} \overline{s}_0 \simeq X_{G_{\overline{s}},u} \to X_{\rho_s,\zeta^u}(p) \times_{\kappa(s)} \overline{s}$ of Proposition 1.4.10 is $\mathrm{SL}_2(\mathbb{F}_p)$-equivariant.

Moreover, for any $u \in \mathbb{F}_p^\times$, the actions of $\mathbb{T}_1$, $\pi_1(S, \overline{s})$ and $\mathrm{SL}_2(\mathbb{F}_p)$ on $\mathcal{T}_\ell J_{\rho_s,\zeta^u}(p)$ factor through the algebra $\mathbb{T}_1[\mathrm{SL}_2(\mathbb{F}_p) \rtimes_\rho \pi_1(S, \overline{s})]$.

If we replace (P, Q) with a different basis $\begin{pmatrix} P' \\ Q' \end{pmatrix} = M \begin{pmatrix} P \\ Q \end{pmatrix}$ (for $M \in \mathrm{GL}_2(\mathbb{F}_p)$), then the new representation is exactly $M\rho_{\overline{s}}M^{-1}$; for $N \in \mathrm{SL}_2(\mathbb{F}_p)$, the action of N attached to the new basis (P', Q') is $(MNM)^{-1}_{(P,Q)}$, where the subscript means that we consider the action of the matrix attached to the basis (P, Q).

If we replace $\iota_{\overline{s}}$ with another ring homomorphism $\iota = \iota_{\overline{s}} \circ \sigma$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}_{\{p,\ell\}}/\mathbb{Q})$, then $R_\iota = \sigma^{-1} R_{\iota_{\overline{s}}} \sigma$.

If $\overline{s'}$ is another geometric point of S, there is a (non-canonical) isomorphism I between the functors $\mathbf{FinÉt}_S \to \mathbf{FinSet}$ given by $Y \longmapsto Y_{\overline{s}}$, $Y \longmapsto Y_{\overline{s'}}$. Let $(P', Q', \zeta', \overline{s'}_0)$ be the image of $(P, Q, \zeta, \overline{s_0})$ under I (in particular, this uniquely defines an action of $\mathrm{SL}_2(\mathbb{F}_p)$ on $X_{G,u}(p) \times_S \kappa(\overline{s'})$). Moreover, $I(\iota_{\overline{s}})$ defines a ring homomorphism $\iota_{\overline{s'}} : \mathcal{O}_{p\ell} \to \kappa(\overline{s'})$ and also induces an isomorphism $\pi_1(I) : \pi_1(S, \overline{s}) \to \pi_1(S, \overline{s'})$, in such a way that $\rho_{\overline{s}} = \rho_{\overline{s}} \circ \pi_1(I)$. The

following diagram commutes:

$$\begin{array}{ccc} \pi_1(S,\overline{s}) & \xrightarrow{R_{\iota_{\overline{s}}}} & \mathrm{Gal}(\mathbb{Q}_{\{p,\ell\}}/\mathbb{Q}) \\ \downarrow{\scriptstyle \pi_1(I)} & & \downarrow{\scriptstyle \mathrm{id}} \\ \pi_1(S,\overline{s'}) & \xrightarrow{R_{\iota_{\overline{s'}}}} & \mathrm{Gal}(\mathbb{Q}_{\{p,\ell\}}/\mathbb{Q}) \end{array}$$

For every $u \in \mathbb{F}_p^\times$, I induces an isomorphism $\mathcal{T}_\ell \mathrm{Jac}(X_u)_{\overline{s}} \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l} \to \mathcal{T}_\ell \mathrm{Jac}(X_u)_{\overline{s'}} \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ of $(\mathbb{T}_1 \otimes F_\mathfrak{l})[\mathrm{SL}_2(\mathbb{F}_p) \rtimes_{\rho_{\overline{s}}} \pi_1(S,\overline{s})]$-module (whose action on $\mathrm{Jac}(X_u)_{\overline{s'}}$ is given through $\pi_1(I)$).

Proof. – That D is an anti-homomorphism (and thus that $\rho_{\overline{s}}$ is a group homomorphism) is a direct verification similar to Lemma 1.4.2.

Let $E \subset \mathrm{Frac}(\mathcal{O}_{p\ell})$ be a finite Galois extension of $\mathbb{Q}$ which is unramified outside $p\ell$. Then $\mathrm{Spec}\,\mathcal{O}_E[(p\ell)^{-1}]$ is a finite étale $\mathbb{Z}[(p\ell)^{-1}]$-scheme, so $\pi_1(S,\overline{s})$ acts on the topological space $\mathrm{Spec}\,\mathcal{O}_E[(p\ell)^{-1}] \times_{\mathbb{Z}} S \times_S \overline{s} \simeq (\mathrm{Spec}\,\mathcal{O}_E)_{\overline{s}}$. The choice of $\iota_{\overline{s}}$ amounts to specifying a point $i \in (\mathrm{Spec}\,\mathcal{O}_E)_{\overline{s}}$, with $i = [\iota_{\overline{s}} \otimes 1 : \mathcal{O}_E \otimes \kappa(\overline{s}) \to \kappa(\overline{s})]$. By definition, $(\mathrm{Spec}\,\mathcal{O}_E)_{\overline{s}}$ is endowed with actions of $\mathrm{Gal}(E/\mathbb{Q})$ (right) and $\pi_1(S,\overline{s})$ (left) that commute. Since $\mathrm{Gal}(E/\mathbb{Q})$ is the automorphism group of $(\mathrm{Spec}\,\mathcal{O}_E)_{\overline{s}}$, we can define a homomorphism $\pi_1(S,\overline{s}) \to \mathrm{Gal}(E/\mathbb{Q})$ by mapping $g \in \pi_1(S,\overline{s})$ to the unique $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ such that $(\mathrm{Spec}\,\sigma \times \mathrm{id})i = g(i)$.

This morphism is clearly compatible with extensions $E' \supset E$, so this defines a homomorphism $R_{\iota_{\overline{s}}} : \pi_1(S,\overline{s}) \to \mathrm{Gal}(\mathbb{Q}_{p\ell}/\mathbb{Q})$. Note that when $g = \mathrm{Spec}\,\alpha^{-1}$ with $\alpha \in \mathrm{Gal}(\overline{\kappa(s)}/\kappa(s))$, then

$$\begin{aligned} g(i) &= \ker[\iota_{\overline{s}} \circ (\mathrm{id} \times \alpha^{-1})] = \ker[\alpha \circ \iota_{\overline{s}} \circ (\mathrm{id} \times \alpha^{-1})] \\ &= \ker[\iota_{\overline{s}} \circ (R_{\iota_{\overline{s}}}(\alpha) \times \alpha)] \circ (\mathrm{id} \times \alpha^{-1})] \\ &= \ker[\iota_{\overline{s}} \circ (R_{\iota_{\overline{s}}}(\alpha) \times \mathrm{id})] = (\mathrm{Spec}\,R_{\iota_{\overline{s}}}(\alpha) \times \mathrm{id})i, \end{aligned}$$

where the $R_{\iota_{\overline{s}}}(\alpha)$ is in the sense of Lemma 3.4.6, so our notation makes sense.

For any $g \in \pi_1(S,\overline{s})$, g acts on the finite discrete group $(\mu_p)_{k_s}$, so this automorphism is given by some $\underline{a}$ for $a \in \mathbb{F}_p^\times$. The mod p cyclotomic character is simply $g \longmapsto a$. Since we came from the finite étale $\mathbb{Z}[p^{-1}]$-scheme $(\mu_p)_{\mathbb{Z}[1/p]}$, this character factors through $\pi_1(S,\overline{s}) \to G_{\mathbb{Q},p}$ (this map is only defined up to conjugacy, but since ω_p is a character, it does not depend from the representative of the conjugacy class).

For any field k with separable closure k_s such that $p \in k^\times$, for any $\sigma \in \mathrm{Gal}(k_s/k)$, for any $f \in \mu_p^\times(k_s)$, $f \circ \mathrm{Spec}\,\sigma = \sigma \circ f^\sharp = f^\sharp \circ \underline{\omega_p(\sigma)}$. This implies by Lemma 3.6.21 that the mod p cyclotomic character on $\pi_1(S,\overline{s})$ is the composition of $\pi_1(S,\overline{s}) \to G_{\mathbb{Q},p\ell} \xrightarrow{\omega_p} \mathbb{F}_p^\times$, and that its restriction to any Galois group is the usual mod p cyclotomic character.

This discussion implies in particular that $\det D = \omega_p$, thus $\det \rho_{\overline{s}} = \omega_p^{-1}$.

For every $n \geq 1$ and $u \in \mathbb{F}_p^\times$, $\mathrm{Jac}(X_u)[\ell^n]$ is a finite étale S-group scheme with an action of $\mathbb{T}_1$. So $\pi_1(S,\overline{s})$ acts on the finite $\mathbb{T}_1$-module $\mathrm{Jac}(X_u)[\ell^n]_{\overline{s}}$. We can then take the inverse limit over all $n \geq 1$ and tensor with $F_\mathfrak{l}$.

Most of the claimed compatibilities are direct verifications, using Propositions 1.4.10 and 1.5.18 as well as Lemmas 3.6.5, 3.6.21 and 3.6.15. The existence of I is [156, Proposition 5.5.1]. We elaborate on the construction of $\iota_{\overline{s'}}$ and the fact that $R_{\iota_{\overline{s}}} = R_{\iota_{\overline{s}}} \circ \pi_1(I)$.

Let $E/\mathbb{Q}$ be a finite Galois extension unramified outside $p\ell$. Then

$$i' = I(\ker[\iota_{\overline{s}} : \mathcal{O}_E \otimes \kappa(\overline{s}) \to \kappa(\overline{s})])$$

is a point of $\mathrm{Spec}\,\mathcal{O}_E \otimes \kappa(\overline{s'})$, so is the kernel of a unique morphism $\iota_{\overline{s'}} : \mathcal{O}_E \otimes \kappa(\overline{s'}) \to \kappa(\overline{s'})$ of

$\kappa(\overline{s'})$-algebras. The following diagram commutes and commutes to the action of $\mathrm{Gal}(E/\mathbb{Q})$.

$$\begin{array}{ccc} \mathrm{Spec}\,(\mathcal{O}_E)_{\overline{s}} & \xrightarrow{g} & \mathrm{Spec}\,(\mathcal{O}_E)_{\overline{s}} \\ \downarrow I & & \downarrow I \\ \mathrm{Spec}\,(\mathcal{O}_E)_{\overline{s'}} & \xrightarrow{g} & \mathrm{Spec}\,(\mathcal{O}_E)_{\overline{s'}} \end{array}$$

Hence $R_{\iota_{\overline{s}}}$ and $R_{\iota_{\overline{s'}}} \circ \pi_1(I)$ have the same projections in $\mathrm{Gal}(E/\mathbb{Q})$, whence $R_{\iota_{\overline{s}}} = R_{\iota_{\overline{s'}}} \circ \pi_1(I)$. □

Proposition 3.6.24 *Let $\mathfrak{l}$ be a maximal ideal of $\mathcal{O}_F$ with residue characteristic ℓ, and S be a connected regular excellent Noetherian affine $\mathbb{Z}[(p\ell)^{-1}]$-scheme of characteristic zero. Let G be a polarized p-torsion group over S and let, for each $u \in \mathbb{F}_p^\times$, $X_u := X_{G,u}(p)$ (see Section 1.3), which is a smooth proper S-scheme of relative dimension one with connected geometric fibres.*

Let $\mathcal{O}_{p\ell}$ be the ring of integers of the maximal algebraic extension $\mathbb{Q}_{\{p,\ell\}}$ of $\mathbb{Q}$ unramified outside p and ℓ. Let $\overline{s}$ be a geometric point of S above a topological point $s \in S$; fix a morphism $\iota_{\overline{s}} : \mathcal{O}_{p\ell} \to \kappa(\overline{s})$, which induces a morphism $R_\iota : \pi_1(S,\overline{s}) \to \mathrm{Gal}(\mathbb{Q}_{\{p,\ell\}}/\mathbb{Q})$.

Let (P,Q) be a basis of $G(\kappa(\overline{s}))$ with $\zeta = \langle P, Q\rangle_G \in \mu_p^\times(\kappa(\overline{s}))$, and, for each $g \in \pi_1(S,\overline{s})$, $\rho_{\overline{s}}(g) \in \mathrm{GL}_2(\mathbb{F}_p)$ be the unique matrix such that $\begin{pmatrix} g(P) \\ g(Q)\end{pmatrix} = \rho_{\overline{s}}^{-1}(g)\begin{pmatrix} P \\ Q\end{pmatrix}$.

Thus $\rho_{\overline{s}} : \pi_1(S,\overline{s}) \to \mathrm{GL}_2(\mathbb{F}_p)$ is a group homomorphism with determinant ω_p^{-1}.

Let S_0 be a finite étale connected S-scheme endowed with a geometric point $\overline{s}_0$ lifting $\overline{s}$ such that P,Q lift to $G(S_0)$. When $p \equiv 3 \pmod 4$, let S_2 be the finite étale S-scheme corresponding to the $\pi_1(S,\overline{s})$-set $\{\pm\}$, where the action is by $\left(\frac{\omega_p}{p}\right)$. Then, for a suitable geometric point $\overline{s}_2$ of S_2, the map $(S_0,\overline{s}_0) \to (S,\overline{s})$ factors through $(S_2,\overline{s_2})$. Note that $S_2 = S \times_{\mathbb{Z}} \mathrm{Spec}\,\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$.

Let $G_{\overline{s},\rho} = \mathrm{SL}_2(\mathbb{F}_p) \rtimes_{\rho_{\overline{s}}} \pi_1(S,\overline{s})$ and $\widetilde{\rho_{\overline{s}}} : (M,g) \in G_{\overline{s},\rho} \longmapsto M\rho_{\overline{s}}(g) \in \mathrm{GL}_2(\mathbb{F}_p)$, and $G_2 = \widetilde{\rho_{\overline{s}}}^{-1}(\mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p)) \simeq \mathrm{SL}_2(\mathbb{F}_p) \rtimes_{\rho_{\overline{s}}} \pi_1(S_2,\overline{s}_2)$.

Then, for each $u \in \mathbb{F}_p^\times$, the eigenspaces of the $(\mathbb{T}_1 \otimes F_\mathfrak{l})[G_{\overline{s},\rho}]$-module $\mathcal{T}_\ell\mathrm{Jac}(X_u)_{\overline{s}} \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ are:

- *for $(f,\mathbf{1}) \in \mathscr{S}$, a copy of $R_{f,\mathfrak{l}} := (V_{f,\mathfrak{l}} \circ R_{\iota_{\overline{s}}}) \otimes \mathrm{St}(\widetilde{\rho_{\overline{s}}})$,*
- *for $(f,\chi) \in \mathscr{P}'$, a copy of $R_{f,\mathfrak{l}} := (V_{f,\mathfrak{l}} \circ R_{\iota_{\overline{s}}}) \otimes (\pi(1,\chi))(\widetilde{\rho_{\overline{s}}})$,*
- *for $(f,\mathbf{1}) \in \mathscr{C}_1'$, a copy of $R_{f,\mathfrak{l}} := (V_{f,\mathfrak{l}} \circ R_{\iota_{\overline{s}}}) \otimes C_f(\widetilde{\rho_{\overline{s}}})$,*
- *for $(f,\mathbf{1}) \in \mathscr{C}_M$, there is a sign r depending only on $\iota^{-1}(\zeta)$ such that it is:*
  - *if $S_2 \to S$ is an isomorphism, a copy of $\bigoplus_{v\in\{\pm\}} (\psi_{f,rv,\mathfrak{l}} \circ R_{\iota_{\overline{s}}}) \otimes C^v(\widetilde{\rho_{\overline{s}}})$.*
  - *if $S_2 \to S$ is not an isomorphism, a copy of*

$$R_{f,r,\mathfrak{l}} := \mathrm{Ind}_{\pi_1(S_2,\overline{s}_2)}^{\pi_1(S,\overline{s})} \left[(\psi_{f,r,\mathfrak{l}} \circ R_{\iota_{\overline{s}}}) \otimes C^+((\widetilde{\rho_{\overline{s}}})_{|\pi_1(S_2,\overline{s}_2)})\right].$$

Proof. – Assume first that $s \in S$ is the generic point. The map $\mathrm{Gal}(\overline{\kappa(s)}/\kappa(s)) \to \pi_1(S,\overline{s})$ is surjective [156, Remark 5.7.12] and the kernel of this morphism acts trivially on every $\mathcal{T}_\ell\mathrm{Jac}(X_u)$ by definition: therefore, by Corollary 3.6.18, the result holds for any $(u,\mathfrak{l})$.

The claim then holds for every possible choice of $(\overline{s},P,Q,\iota_{\overline{s}},S_0,S_2)$ and any $(u,\mathfrak{l})$ thanks to the discussion of Lemma 3.6.23. □

Corollary 3.6.25 *The statement of Corollary 3.6.18 holds if we only assume that the characteristic of k is not p or ℓ after the following modifications are made:*

- *if the characteristic of k is $q \neq 0$, then let $\mathcal{O}_{\{p,\ell\}}$ be the ring of integers of the maximal algebraic extension $\mathbb{Q}_{\{p,\ell\}}$ of $\mathbb{Q}$ which is unramified outside p,ℓ, and ι is a ring homomorphism $\mathcal{O}_{\{p,\ell\}} \to k_s$ inducing a morphism $R_\iota : \mathrm{Gal}(k_s/k) \to \mathrm{Gal}(\mathbb{Q}_{\{p,\ell\}}/\mathbb{Q})$.*
- *if $p \equiv 3 \pmod 4$ and k has characteristic 2, then k' is the subextension of k_s generated by the roots of $X^2 - X - \frac{p+1}{4}$, so that $\mathrm{Gal}(k_s/k') = \omega_p^{-1}(\mathbb{F}_p^{\times 2})$.*

Proof. – When the characteristic of k is zero, this was already proved, so we assume that k has positive characteristic q. By the same argument as the proof of Corollary 3.6.18, it is enough to prove the result for *one* representation of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.

When $q \neq 11$, we apply Proposition 3.6.27 to $S = \operatorname{Spec} \mathbb{Z}[(11p\ell)^{-1}]$ and G being the p-torsion group of the elliptic curve E/S with Weierstrass equation given by $y^2 - y = x^3 - x^2$ (LMFDB [107] label 11.a3) at a geometric point in the special fibre at q, and then we restrict to its absolute Galois group.

When $q = 11$, we apply Proposition 3.6.27 to $S = \operatorname{Spec} \mathbb{Z}[(14p\ell)^{-1}]$ and G being the p-torsion group of the elliptic curve E/S with Weierstrass equation given by $y^2 + xy + y = x^3 - x$ (LMFDB label 14.a5) at a geometric point in the special fibre at q, and then we restrict to the absolute Galois group. □

Corollary 3.6.26 *Let $\mathfrak{l}$ be a maximal ideal of $\mathcal{O}_F$ with residue characteristic ℓ and k be a field with separable closure k_s and residue characteristic distinct from p, ℓ. Let $\mathcal{O}$ be the ring of integers of the maximal algebraic extension $\mathbb{Q}_{\{p,\ell\}}$ of $\mathbb{Q}$ unramified outside p, ℓ and $\iota : \mathcal{O} \to k_s$ be a ring homomorphism, inducing a continuous group homomorphism $R_\iota : \mathrm{Gal}(k_s/k) \to \mathrm{Gal}(\mathbb{Q}_{\{p,\ell\}}/\mathbb{Q})$.*

Let $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ be a continuous group homomorphism with $\det \rho = \omega_p^{-1}$. Then, for any $\xi \in \mu_p^\times(k_s)$, as a $(\mathbb{T}_1 \otimes F_\mathfrak{l})[\mathrm{Gal}(k_s/k)]$-module, $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is isomorphic to the following direct sum:

- *for every $(f,\chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1'$, a copy of $R_{f,\mathfrak{l}}(\rho)$, on which, for all $n, m \geq 1$ such that $nm^2 \equiv 1 \pmod p$, $T_n \cdot (mI_2)$ acts by $\chi(m)a_n(f)$,*
- *for $(f,\chi) \in \mathscr{C}_M$, let k' be the subextension of k_s/k generated by the roots of the polynomial $X^2 - X - \frac{p+1}{4}$. There exists a sign r depending only on $\iota^{-1}(\xi)/\mathbb{F}_p^{\times 2}$ such that the factor (on which, for any $n, m \geq 1$ with $nm^2 \equiv 1 \pmod p$) is:*
  - $\mathrm{Ind}_{\mathrm{Gal}(k_s/k')}^{\mathrm{Gal}(k_s/k)}(\psi_{f,r,\mathfrak{l}} \circ R_\iota) \otimes C^+(\rho_{|\mathrm{Gal}(k_s/k')})$, *when $k' \neq k$,*
  - $\bigoplus_{v \in \{\pm\}} (\psi_{f,rv,\mathfrak{l}} \circ R_\iota) \otimes C^v(\rho_{|\mathrm{Gal}(k_s/k')})$ *when $k' = k$.*

Proposition 3.6.27 *The statement of Proposition 3.6.24 holds* as is *when S is not assumed to have characteristic zero.*

Proof. – This is exactly similar to the proof of Proposition 3.6.24 after replacing Corollary 3.6.18 with Corollary 3.6.25. □

We conclude this section by discussing the action of $\mathbb{T}_{1,\{1\}}$ on the Tate modules of the connected components.

Proposition 3.6.28 *Let k be a field with characteristic $q \neq p$, $\mathfrak{l}$ be a maximal ideal of $\mathcal{O}_F$ with residue characteristic $\ell \neq q$. Let k_s be a separable closure of k and $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{GL}_2(\mathbb{F}_p)$ be group homomorphism such that $\det \rho = \omega_p^{-1}$. Let $\xi \in \mu_p^\times(k_s)$. Let $\mathcal{O}$ be the ring of integers of the maximal algebraic extension $\mathbb{Q}_{\{p,\ell\}}/\mathbb{Q}$ unramified outside $p\ell$ and fix an embedding $\iota : \mathcal{O} \to k_s$. This determines a group homomorphism $R_\iota : \mathrm{Gal}(k_s/k) \to \mathrm{Gal}(\mathbb{Q}_{\{p,\ell\}}/\mathbb{Q})$.*

Let $n \geq 1, M \in \mathrm{GL}_2(\mathbb{F}_p), \sigma \in \mathrm{Gal}(k_s/k)$ be such that $n \det M \equiv 1 \pmod p$. Then:

- *For any $(f,\chi) \in \mathscr{S}$ (resp. $(f,\chi) \in \mathscr{P}'$, resp. $(f,\chi) \in \mathscr{C}_1'$), for any $r \geq 1$, the action of $(T_n M\sigma)^r$ on the f-eigenspace of $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is $a_n(f)^r \mu_r \mathrm{Tr}(R_\iota(\sigma^r) \mid V_{f,\mathfrak{l}})$, where μ_r is the trace of the action of $(M\rho(\sigma))^r$ on St (resp. on $\pi(1,\chi)$, resp. on C_f),*
- *If $(f,\chi) \in \mathscr{C}_M$, $T_n M = 0$ if $n \notin \mathbb{F}_p^{\times 2}$. Otherwise, for any $r \geq 1$, the action of $(T_n M\sigma)^r$ on the f-eigenspace of $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is*
  - *if $\omega_p(\sigma)^r \notin \mathbb{F}_p^{\times 2}$, it is 0,*
  - *if r is even and $\omega_p(\sigma) \notin \mathbb{F}_p^{\times 2}$, let V_4 be the representation of $\mathrm{GL}_2(\mathbb{F}_p)$ described in Section B.4, the result is*

$$\frac{1}{2} a_n(f)^r \mathrm{Tr}(\sigma^r \mid V_{f,\mathfrak{l}}) \mathrm{Tr}((M\rho(\sigma))^r \mid V_4),$$

- *if $\omega_p(\sigma) \in \mathbb{F}_p^{\times 2}$ and s is the sign attached to $\iota^{-1}(\xi)$ defined in Corollary 3.6.25;*

$$a_n(f)^r \left[\psi_{f,s,\mathfrak{l}}(R_\iota(\sigma^r))\mathrm{Tr}((M\rho(\sigma))^r \mid C^+) + \psi_{f,-s,\mathfrak{l}}(R_\iota(\sigma^r))\mathrm{Tr}((M\rho(\sigma))^r \mid C^-)\right].$$

Proof. – When $M \in \mathrm{SL}_2(\mathbb{F}_p)$, the claim is contained in Proposition 3.6.25. When $\det M \in \mathbb{F}_p^{\times 2}$, there exists $M_1 \in \mathrm{SL}_2(\mathbb{F}_p)$ and $m \in \mathbb{F}_p^\times$ such that $M = mM_1$: hence $nm^2 \equiv 1 \pmod p$. Therefore $(T_n M\sigma)^r = (T_n(mI_2)M_1\sigma)^r = (T_n \cdot (mI_2))^r (M_1\sigma)^r$ acts on the f-eigenspace by $(a_n(f)\chi(m))^r (M_1\sigma)^r$, and we are thus reduced to the case of $\mathrm{SL}_2(\mathbb{F}_p)$ (because χ is the central character of the representation of $\mathrm{GL}_2(\mathbb{F}_p)$).

Now, assume that $M \notin \mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p)$. When $(f,\chi) \in \mathscr{C}_M$, $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is a submodule of the f-eigenspace of $\mathcal{T}_\ell J_\rho(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$, on which T_n acts by $a_n(f) = 0$ by Corollary 3.4.4. So we assume that $(f,\chi) \notin \mathscr{C}_M$.

Let $\tau_{(M,\sigma),\xi,r}$ be the trace of the action of $(T_n M\sigma)^r$ on the f-eigenspace of $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$. Clearly, $\tau_{(M,\sigma),\xi,r}$ only depends on the $\mathrm{SL}_2(\mathbb{F}_p) \rtimes_\rho \mathrm{Gal}(k_s/k)$-conjugacy class of (M,σ). Since $\det M \in \mathbb{F}_p^{\times 2}$, $\mathbb{F}_p[M]$ contains matrices of every possible determinant. When $N \in \mathrm{GL}_2(\mathbb{F}_p)$ commutes to M, $(N\rho(\sigma)^{-1},\sigma) \in \mathrm{GL}_2(\mathbb{F}_p) \rtimes_\rho \mathrm{Gal}(k_s/k)$ commutes to (M,σ). Therefore, the $\mathrm{SL}_2(\mathbb{F}_p) \rtimes_\rho \mathrm{Gal}(k_s/k)$-conjugacy class of (M,σ) is, in fact, its $\mathrm{GL}_2(\mathbb{F}_p) \rtimes_\rho \mathrm{Gal}(k_s/k)$-conjugacy class.

For any $\xi_1 \in \mu_p^\times(k_s)$, any $(N,\sigma') \in \mathrm{GL}_2(\mathbb{F}_p) \rtimes_\rho \mathrm{Gal}(k_s,k)$ induces isomorphisms from the f-eigenspace of $\mathcal{T}_\ell J_{\rho,\xi_1}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ to that of $\mathcal{T}_\ell J_{\rho,\xi_1^{\det N}}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ which commute to T_n: therefore, $\tau_{(N,\sigma')(M,\sigma')^r(N,\sigma')^{-1},\xi^{\det N},r} = \tau_{(M,\sigma),\xi,r}$. Hence $\tau_{(M,\sigma),\xi,r}$ does not depend on ξ.

Therefore, $(p-1)\tau_{M,\xi,r}$ is exactly the trace of $(T_n M\sigma)^r$ acting on the f-eigenspace of $\mathcal{T}_\ell J(p,p)_\rho$, which is, by Proposition A.4.39, the trace of $(T_n M\rho(\sigma)\sigma)^r$ acting on $\mathcal{T}_\ell J(p,p)_k$. By Corollary 3.4.4 (and Lemma 3.6.2, Corollary 3.4.7), this trace is

$$\begin{aligned}&\sum_{\psi \in \mathcal{D}} \mathrm{Tr}(R_\iota(\sigma^r) \mid V_{f\otimes\psi,\mathfrak{l}}) a_n(f\otimes\psi)^r \psi(\det(M\rho(\sigma))^r)\mathrm{Tr}(M^r \mid R_f)\\ &= 2(p-1)a_n(f)^r \mathrm{Tr}((M\rho(\sigma))^r \mid R_f),\end{aligned}$$

where R_f is St if $(f,\chi) \in \mathscr{S}$, $\pi(1,\chi)$ if $(f,\chi) \in \mathscr{P}'$, and C_f if $(f,\chi) \in \mathscr{C}_1'$. □

Corollary 3.6.29 *Let $\rho, k, k_s, q, \ell, \mathfrak{l}, \iota, R_\iota$ be as Proposition 3.6.28. Let $(f,\chi) \in \mathscr{S}$ (resp. $(f,\chi) \in \mathscr{P}'$, resp. $(f,\chi) \in \mathscr{C}_1'$), and let $Q_f = \mathrm{St}$ (resp. $Q_f = \pi(\mathbf{1},\chi)$, resp. $Q_f = C_f$). Assume that $V_{f,\mathfrak{l}} \circ R_\iota$ is semisimple, for instance if the image of R_ι is open.*

Let $G_{k,\rho} = \mathrm{GL}_2(\mathbb{F}_p) \rtimes_\rho \mathrm{Gal}(k_s/k)$, and $\widetilde{\rho} : (M,g) \in G_{k,\rho} \longmapsto M\rho(g)$. Let $\widetilde{R}_\iota$ be the homomorphism $(M,g) \in G_{k,\rho} \longmapsto R_\iota(g)$.

Then, for any $\xi \in \mu_p^\times(k_s)$, the f-eigenspace of $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is a semi-simple $\mathbb{T}_{1,\mathrm{GL}_2(\mathbb{F}_p),\rho} \otimes F_\mathfrak{l}$-module, and it is isomorphic to the restriction of the $\mathbb{T}[G_{k,\rho}] \otimes F_\mathfrak{l}$-module $(V_{f,\mathfrak{l}} \circ \widetilde{R}_\iota) \otimes Q_f(\widetilde{\rho})$, where $T_n \in \mathbb{T}$ (resp. nI_2) for $n \geq 1$ coprime to p acts by $a_n(f)$ (resp. $\chi(n)$).

Proof. – First, by Proposition 3.4.4, there is a ring homomorphism $\mathbb{T} \to F$ mapping T_n (resp. nI_2) to $a_n(f)$ (resp. $\chi(n)$). Thus the $(\mathbb{T} \otimes F_\mathfrak{l})[G_{k,\rho}]$-module $(V_{f,\mathfrak{l}} \circ \widetilde{R}_\iota) \otimes Q_f(\widetilde{\rho})$ described in the statement is well-defined. Let us prove that it is semi-simple: it is enough to show that it is semi-simple as a continuous representation of $G_{k,\rho}$ with coefficients in $F_\mathfrak{l}$.

By [21, §2.7 Lemma], it is enough to show that $(V_{f,\mathfrak{l}} \circ \widetilde{R}_\iota) \otimes Q_f(\widetilde{\rho})$ is semi-simple as a $F_\mathfrak{l}[\mathrm{Gal}(k_s/k)]$-module[5]. This is the case, because this module is the direct sum of a certain number of copies of $V_{f,\mathfrak{l}} \circ R_\iota$, which is semi-simple by assumption (if R_ι has an image of finite index, it is a consequence of [132, Theorem 4.4]).

By Proposition 3.6.28, the f-eigenspace $E_{f,\mathfrak{l},\xi}$ of $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is a $\mathbb{T}_{1,\mathrm{GL}_2(\mathbb{F}_p),\rho} \otimes F_\mathfrak{l}$-module with the same traces as $(V_{f,\mathfrak{l}} \circ \widetilde{R}_\iota) \otimes Q_f(\widetilde{\rho})$. So the semi-simplification of $E_{f,\mathfrak{l}}$ is exactly $(V_{f,\mathfrak{l}} \circ \widetilde{R}_\iota) \otimes Q_f(\widetilde{\rho})$.

[5] As previously, the reference discusses only complex smooth representations, but their argument applies *as is*.

Now, $\bigoplus_\xi E_{f,\mathfrak{l},\xi}$ is the f-eigenspace of $\mathcal{T}_\ell J_{\rho,\xi}(p)\otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$, which is, by Corollary 3.4.4 and Proposition A.4.39, isomorphic over $(\mathbb{T}\otimes F_\mathfrak{l})[G_{k\rho}]$ to $\bigoplus_{\psi\in\mathcal{D}}(\psi(\omega_p\det\widetilde{\rho})\otimes(V_{f,\mathfrak{l}}\circ\widetilde{R}_\iota)\otimes C_f(\widetilde{\rho})$, where T_n (resp. nI_2) acts on the summand ψ by $a_n(f)\psi(n)$ (resp. $\chi(n)\psi(n)^2$) for any $n\geq 1$ coprime to p.

Therefore, one has the following isomorphism of $\mathbb{T}_{1,\mathrm{GL}_2(\mathbb{F}_p),\rho}\otimes F_\mathfrak{l}$-modules:

$$\bigoplus_\xi E_{f,\mathfrak{l},\xi}\simeq\Big((V_{f,\mathfrak{l}}\circ\widetilde{R}_\iota)\otimes Q_f(\widetilde{\rho})\Big)^{\oplus(p-1)},$$

whence every $E_{f,\mathfrak{l},\xi}$ is semi-simple and the conclusion follows. □

Chapter 4

Automorphy, functional equations and root numbers for $L(J_\rho, s)$

4.1 Introduction and statement of results

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ be a continuous representation such that $\det \rho = \omega_p^{-1}$ is the inverse of the cyclotomic character modulo p. Then $X_\rho(p) := X(p,p)_\rho$ is a smooth projective $\mathbb{Q}$-scheme of relative dimension one, and is, by Proposition 1.4.10, the reunion of smooth projective geometrically connected $\mathbb{Q}$-schemes $X_{\rho,\xi}(p)$ indexed by $\xi \in \mu_p^\times(\overline{\mathbb{Q}})$. The Jacobian of $X_{\rho,\xi}(p)$ is noted $J_{\rho,\xi}(p)$.

We will use the following notation from Sections 2 and 3:

Notation

- $\mathcal{D}$ *denotes the set of Dirichlet characters* $(\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$,
- $\mathscr{S}$ *denotes the set of* $(f, \mathbf{1})$ *where* $f \in \mathcal{S}_2(\Gamma_0(p))$ *is a newform,*
- $\mathscr{P}$ *denotes the set of* (f, χ)*, where* $f \in \mathcal{S}_2(\Gamma_1(p))$ *is a newform with character* $\chi \neq \mathbf{1}$*,*
- $\mathscr{P}'$ *denotes a set of representatives in* $\mathscr{P}$ *for* $\mathscr{P}$ *modulo the complex conjugation,*
- $\mathscr{C}$ *denotes the set of* (f, χ)*, where* $f \in \mathcal{S}_2(\Gamma_1(p) \cap \Gamma_0(p^2))$ *is a newform with character* $\chi \in \mathcal{D}$*, and such that no twist of* f *by a character in* $\mathcal{D}$ *has conductor* p*,*
- $\mathscr{C}_1'$ *denotes a set of representatives of the form* $(f, \mathbf{1})$ *for the* $(f, \chi) \in \mathscr{C}$ *modulo twists such that* f *does not have complex multiplication.*
- $\mathscr{C}_M$ *denotes the collection of* $(f, \mathbf{1}) \in \mathscr{C}$ *such that* f *has complex multiplication. In this case,* $p \equiv 3 \pmod 4$ *and* f *has complex multiplication by* $\mathbb{Q}(\sqrt{-p})$*.*
- $\mathbb{T}_1$ *denotes the subalgebra of* $\bigoplus_{\xi \in \mu_p^\times(\overline{\mathbb{Q}})} \mathrm{End}(J_{\rho,\xi}(p))$ *generated by the* $(mI_2) \cdot T_n$ *such that* $n, m \geq 1$ *are integers such that* $nm^2 \equiv 1 \pmod p$*.*
- *For* $\alpha \in \mathcal{D}$*,* St_α *is the Steinberg representation of* $\mathrm{GL}_2(\mathbb{F}_p)$ *twisted by* $\alpha(\det)$*.*
- *For* $\alpha, \beta \in \mathcal{D}$*,* $\pi(\alpha, \beta)$ *is the principal series representation of* $\mathrm{GL}_2(\mathbb{F}_p)$ *attached to the characters* α, β*.*
- *Given* $(f, \chi) \in \mathscr{C}$*, we can attach by Definition 2.4.13 a cuspidal representation of* $\mathrm{GL}_2(\mathbb{F}_p)$ *named* C_f*.*
- ω_p *denotes the cyclotomic character modulo* p*.*

The varieties $J_{\rho,\xi}(p)$ are Abelian varieties over $\mathbb{Q}$: according to a conjecture akin to the Birch and Swinnerton-Dyer conjecture, the L-functions of the eigenspaces (for the Hecke algebra $\mathbb{T}_1$) of its Tate module are entire, and their vanishing orders at $s = 1$ match the ranks of the eigenspaces of $J_{\rho,\xi}(p)(\mathbb{Q}) \otimes \mathbb{Q}$ for $\mathbb{T}_1$.

By Theorem 3.D, after extending scalars to a sufficiently large extension $F_\mathfrak{l}$ of $\mathbb{Q}_\ell$ (where ℓ is a prime that may be equal to p), the Tate module of $J_{\rho,\xi}(p)$ splits as a direct sum of $(\mathbb{T}_1 \otimes F_\mathfrak{l})[G_{\mathbb{Q}}]$-submodules (which we call *eigenspaces* for $\mathbb{T}_1$, because $\mathbb{T}_1$ acts on them through a ring homomorphism $\mathbb{T}_1 \to F_\mathfrak{l}$) of the following form:

- $V_{f,\mathfrak{l}} \otimes \mathrm{St}(\rho)$, where $(f, \mathbf{1}) \in \mathscr{S}$,
- $V_{f,\mathfrak{l}} \otimes \pi(1,\chi)(\rho)$, where $(f,\chi) \in \mathscr{P}'$,
- $V_{f,\mathfrak{l}} \otimes C_f(\rho)$, where $(f,\chi) \in \mathscr{C}_1'$,
- $\mathrm{Ind}_{G_{\mathbb{Q}(\sqrt{-p})}}^{G_\mathbb{Q}} \psi_{f,\mathfrak{l}} \otimes C^+(\rho_{|G_{\mathbb{Q}(\sqrt{-p})}})$, for $(f,\mathbf{1}) \in \mathscr{C}_M$, where $\psi_{f,\mathfrak{l}} : G_{\mathbb{Q}(\sqrt{-p})} \to F_\mathfrak{l}^\times$ is a character attached to f and C^+ is a cuspidal representation of $\mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p)$ described in Section B.4.

The summand attached to some $(f,\chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1' \cup \mathscr{C}_M$ is called the *f-eigenspace* of the Tate module of $J_{\rho,\xi}(p)$. The f-eigenspaces, for $(f,\mathbf{1}) \in \mathscr{C}_M$, are referred to as the *CM eigenspaces* of the Tate module of the $J_{\rho,\xi}(p)$. The other eigenspaces are the *non-CM eigenspaces*.

It is naturally expected that these L-functions satisfy functional equations of the form $s \longleftrightarrow 2-s$. If we can prove it and determine the constant (in fact, the *sign*, by Lemma 4.4.1), we may deduce the partiy of the vanishing order at $s=1$ of said factor. It seems reasonable to assume that these vanishing orders are "often" 0 or 1, and finding out their parity amounts to determining whether the corresponding eigenspace of $J_{\rho,\xi}(p)(\mathbb{Q}) \otimes_\mathbb{Z} F$ vanishes or not.

In general, proving that the L-function of a ℓ-adic Galois representation is entire and satisfies a functional equation requires automorphy lifting theorems. In our setting, such an automorphy result seems to be beyond reach for several reasons. First, the presence of large Artin representations means that our automorphic representations will not be regular (see for example [26, Definition 1.6]), in which case the usual patching methods will not work. To the author's knowledge, even the mechanism by which a large-dimensional Artin representation of $G_\mathbb{Q}$ can be attached to an automorphic form is completely unknown in general. This is because there seems to be no clear Shimura variety attached to this situation, and, again to the author's knowledge, this means that the recent progress in higher Hida theory [17] cannot be applied to such a situation.

In our situation, in the "generic" case (say, ρ is surjective and comes from the p-torsion of an elliptic curve $E[p]$), the common technique of base change to work over a better-behaved number field does not seem to work. For GL(2) (that is, two-dimensional Galois representations) base change from $\mathbb{Q}$ to any totally real number field is known by [42, 43], and base change for a *solvable* extension of totally real fields is well-known [59, Proposition 4.25], but neither seems to simplify the situation. Indeed, since $\rho(G_\mathbb{Q})$ contains the perfect group $\mathrm{SL}_2(\mathbb{F}_p)$, for any number field K such that $\rho(G_K)$ contains $\mathrm{SL}_2(\mathbb{F}_p)$ and any solvable extension L/K, $\rho(G_L)$ contains the r-th derived subgroup of $\rho(G_K)$, which contains $\mathrm{SL}_2(\mathbb{F}_p)$. Furthermore, since ρ maps the complex conjugation to a conjugate of $\Delta_{1,-1} \in \mathrm{GL}_2(\mathbb{F}_p)$, if F is any totally real number field (which we may assume is Galois), F is fixed under every complex conjugation, so $\rho(G_F)$ is a normal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ containing $\Delta_{1,-1}$, so contains $\det^{-1}(\{\pm 1\})$, and in particular contains $\mathrm{SL}_2(\mathbb{F}_p)$.

A related idea is to use Brauer's theorem on induced characters in order to do away with the Artin representations, but, for instance in the case of $V_{f,\mathfrak{p}} \otimes \mathrm{St}(\rho)$, it is the virtual difference of the representations $\mathrm{Ind}_K^\mathbb{Q} V_{f,\mathfrak{p}} - V_{f,\mathfrak{p}}$ with $G_K = \rho^{-1}(B)$. The previous paragraph shows that K is not a solvable extension of a totally real field, so that the base changed representation $(V_{f,\mathfrak{p}})_{|K}$ is not known (to the best of the author's knowledge) to be automorphic or possess an entire L-function.

Thus, we can only properly study the L-function of $J_\rho(p)$ in specific situations, where for instance ρ is not surjective. This is carried out in the next Chapter when the image of ρ is contained in the normalizer of a nonsplit Cartan subgroup.

If we instead *assume* that the involved Artin representations are automorphic (in a sufficiently strong sense, see Definition 4.5.1), we can show that the L-functions of the factors of $J_\rho(p)$ are entire and satisfy functional equations whose sign can be computed on the Galois side by the theory of Rankin-Selberg products [27, Theorem 9.1]. This is the goal of the first part of this section, after reminders about the Langlands correspondence and the dictionary between modular

forms and automorphic representations.

Theorem 4.1.1 *(Lemma 4.4.1, Propositions 4.5.5 and 4.5.6)*

- *For every eigenspace V in the Tate module of each $J_{\rho,\xi}(p)$, V is isomorphic to $V^*(1)$.*
- *The L-function of any CM eigenspace of the Tate module of $J_{\rho,\xi}(p)$ is well-defined, extends meromorphically to the complex plane and satisfies the expected functional equation, whose sign is given by the product of the local Deligne-Langlands constants.*
- *Let $(f,\chi) \in \mathscr{S}$ (resp. $(f,\chi) \in \mathscr{P}'$, $(f,\chi) \in \mathscr{C}_1'$, $(f,\chi) \in \mathscr{C}_M$). Assume that the Artin representation $\mathrm{St} \circ \rho$ (resp. $\pi(1,\chi) \circ \rho$, resp. $C_f \circ \rho$, resp. $C^+ \circ \rho_{|\mathbb{Q}(\sqrt{-p})}$) is automorphic in the sense of Definition 4.5.1 (with the obvious adjustments over $\mathbb{Q}(\sqrt{-p})$). Then the L-function of the f-eigenspace of the Tate module of $J_{\rho,\xi}(p)$ extends holomorphically to the complex plane and satisfies the expected functional equation (whose sign is given by the product of the local Deligne-Langlands constants).*

To compute the (expected) signs of the functional equation satisfied by the L-functions of the eigenspaces, we need to introduce a distinction depending on the behavior of ρ as a representation of $G_{\mathbb{Q}_p}$, which is expanded on in Proposition 4.4.7.

Definition 4.1.2 We say that ρ is

- *split* if the image of a decomposition subgroup at p is contained in a subgroup conjugate in $\mathrm{GL}_2(\mathbb{F}_p)$ to the group of diagonal matrices,
- *wild* if it is not tamely ramified at p,
- *a-Cartan* if the restriction to an inertia subgroup of ρ is irreducible. In this case, the image by ρ of an inertia subgroup at p is the index a subgroup of a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$, and a is an odd divisor of $\frac{p+1}{2}$.

Definition 4.1.3 Suppose that ρ is a-Cartan, and let $C \leq \mathrm{GL}_2(\mathbb{F}_p)$ be a nonsplit Cartan subgroup such that the image of ρ under an inertia subgroup I_p at p is aC. Let $E/\mathbb{Q}_p$ be the unique quadratic unramified extension. Choose one of the two isomorphisms $\iota : C \to \mathbb{F}_{p^2}^\times$ respecting the trace and norm. The associated *reciprocity index* (see Definition 4.4.12) is the index of the largest subgroup of I_p on which $\iota \circ \rho_{|I_p}$ agrees with the class field theory isomorphism $G_E \to \widehat{E^\times}/(1+p\mathcal{O}_E)$ (mapping an arithmetic Frobenius to a uniformizer).

Remark By the link between class field theory and the fundamental characters [141, Proposition 3], if ρ is a-Cartan, then 1 is one of its reciprocity indices if and only if ρ^* has Serre weight 2 (in the sense of [145, §2.2]).

In fact, if $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ has determinant ω_p^{-1} and is a-Cartan, then a is the greatest common divisor of $k-1$ and p^2-1, where k is the Serre weight of ρ (it is the same result if k denotes the Serre weight of ρ^*) by [145, §2.2].

The following result is a simplified version of Proposition 4.5.7, which also describes the somewhat more complicated result for the CM eigenspaces.

Theorem 4.1.5 *For $(f,\mathbf{1}) \in \mathscr{C}_1'$, let ω_f be the order of the character of $\mathbb{F}_{p^2}^\times$ attached to f. If ρ is a-Cartan, let $n_{f,\rho} \in \{0,1\}$ be equal to 1 if and only if $\frac{p+1}{\omega_f}$ is divisible by a but $\frac{2(p+1)}{\omega_f}$ is not divisible by any of the two reciprocity indices of ρ.*

Then product of the local constants attached to the non-CM eigenspaces of the Tate module of $J_{\rho,\xi}(p)$ (that is, the expected sign of the functional equation satisfied by their L-function) is given in Table 4.1.

In Section 4.6, we discuss the application of Theorem 4.1.5 when ρ comes from an elliptic curve and $p \to \infty$.

We also study $J_\rho(p)[p]$ as a $\mathbb{F}_p[G_{\mathbb{Q}}]$-module, which has a very explicit semi-simplification. We show in Section 4.7 that, thanks to recent progress in Langlands functoriality due to Arias-de-Reyna and Dieulefait in the preprint [3], and to Newton and Thorne [127], $J_\rho(p)[p] \otimes_{\mathbb{F}_p} \overline{\mathbb{F}_p}$ has

	Type of $\rho_{\mid G_{\mathbb{Q}_p}}$		
	Split	Wild	a-Cartan
$V_{f,\mathfrak{l}} \otimes \mathrm{St}(\rho), (f, \mathbf{1}) \in \mathscr{S}$	$(-1)^{(p+1)/2}$	$(-1)^{(p-1)/2} a_p(f)$	$(-1)^{(p+a)/2}$
$V_{f,\mathfrak{l}} \otimes \pi(\mathbf{1}, \chi)(\rho), (f, \chi) \in \mathscr{P}'$	$(-1)^{(p-1)/2}$		
$V_{f,\mathfrak{l}} \otimes C_f(\rho), (f, \mathbf{1}) \in \mathscr{C}'_1$	$(-1)^{(p+1)/2}$	$(-1)^{(p-1)/2}$	$(-1)^{(p+1)/2+n_{f,\rho}}$

Table 4.1: Signs of the functional equation for eigenspaces of $J_{\rho,\xi}(p)$

the same semi-simplification as a direct sum of mod p reductions of automorphic p-adic Galois representations. However, the practical utility of such a result is unclear.

Theorem 4.1.6 *(Proposition 4.7.2) Assume that ρ^* is surjective, or that it is irreducible with Serre weight in $\{2, p+1\}$, and that its Artin conductor N is coprime to 3. Let V be a non-CM eigenspace of the p-adic Tate module of $J_{\rho,\xi}(p)$. Assume furthermore that [3, Theorem 1.1] (that is, Theorem K) holds. Then there exists regular algebraic cuspidal unitary automorphic representations $\pi_1, \dots, \pi_r$ of $\mathrm{GL}(n_i)$ over $\mathbb{Q}$ and continuous representations $V_1, \dots, V_r$ of $G_{\mathbb{Q}}$ with coefficients in $F_{\mathfrak{p}}$ (where $F \subset \mathbb{C}$ is a sufficiently large number field and $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}_F$ with residue characteristic p) such that the following two conditions are satisfied:*

- *For every i, $L(V_i, s)$ and $L(\pi_i, s)$ are well-defined formal products that agree up to shifting s and perhaps finitely many Euler factors.*
- *The semi-simplifications of the mod $\mathfrak{p}$ reductions of $\bigoplus_i V_i$ and V are isomorphic $\overline{\mathbb{F}_p}[G_{\mathbb{Q}}]$-modules.*

I am grateful to Pierre-Henri Chaudouard and Laurent Clozel for their answers to my questions about the Langlands Correspondence, Rankin-Selberg convolutions, and automorphy lifting theorems.

4.2 Relations between classical modular forms and automorphic forms

The material in this Section is not new, but we spell it out carefully as a preparation to the computations of Section 4.5. Our references for the theory of automorphic forms are the books of Gelbart [60] and Bump [20], and we use [21] for its clear description of local representations of GL(2). Some of what we discuss is also covered in, for instance, [109, §2, §3].

Let $\psi : (\mathbb{Z}/M\mathbb{Z})^\times \to \mathbb{C}^\times$ be a primitive Dirichlet character. We can, for instance by [20, Proposition 3.1.2], attach to ψ a finite-order continuous character $\psi_{\mathbb{A}} : \mathbb{A}_{\mathbb{Q}}^\times / \mathbb{Q}^\times \prod_{q \nmid M} \mathbb{Z}_q^\times \to \mathbb{C}^\times$ such that, for every prime $q \nmid M$, $\psi(q)$ is the image under $\psi_{\mathbb{A}}$ of the unique idèle $(z_v)_v$ such that $z_v = 1$ if $v \neq q$ and $z_q = q$. In particular, the character $\prod_{q \mid M} \mathbb{Z}_q^\times \subset \mathbb{A}_{\mathbb{Q}}^\times \xrightarrow{\psi_{\mathbb{A}}} \mathbb{C}^\times$ is exactly ψ^{-1}. Moreover, if $p \mid M$ is a prime, and $(z_v)_v$ is the idèle such that $z_v = 1$ for $v \neq p$ and $z_p = p$, then $\psi_{\mathbb{A}}(z) = \psi'_p(p)$, where $\psi = \psi_p \psi'_p$, where $\psi_p, \psi'_p : (\mathbb{Z}/M\mathbb{Z})^\times \to \mathbb{C}^\times$ are Dirichlet characters whose conductors are a power of p and prime to p respectively.

Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a normalized newform. We can attach to f a cuspidal unitary automorphic representation π_f of $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$. The representation π_f is the restricted tensor product, over all places v of $\mathbb{Q}$, of smooth admissible representations $\pi_{f,v}$ of $\mathrm{GL}_2(\mathbb{Q}_v)$.

To describe the features of this correspondence, we need to introduce additive characters for all the local fields involved. When p is a prime, we define the additive character

$$\theta_p : \mathbb{Q}_p \to \mathbb{Q}_p/\mathbb{Z}_p \subset \mathbb{Q}/\mathbb{Z} \xrightarrow{\exp(2i\pi\cdot)} \mathbb{C}^\times.$$

When $F/\mathbb{Q}_p$ is a finite extension, we write $\theta_F = \theta_p \circ \mathrm{Tr}_{F/\mathbb{Q}_p}$, and η_F (or η_p when $F = \mathbb{Q}_p$) for the character $\theta_F(\cdot/p)$, which has *level one* in the sense of [21, §1.7] when $F/\mathbb{Q}_p$ is tamely

ramified (see for instance [123, Theorem III.2.6]), that is, η_F vanishes on the maximal ideal of $\mathcal{O}_F$, but not on $\mathcal{O}_F$.

The default character of $\mathbb{R}$ is $\theta_\infty : x \in \mathbb{R} \longmapsto \exp(-2i\pi x)$ and if F is a finite extension of $\mathbb{R}$, we let $\theta_F = \theta_\infty \circ \mathrm{Tr}_{F/\mathbb{R}}$. Thanks to this condition, for any number field F, $\prod_v \theta_v$ is a nontrivial additive character of $\mathbb{A}_F/F$.

For any local field F, we denote by $\|\cdot\|_F$ the normalized absolute value.

Proposition 4.2.1 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a normalized newform with primitive character χ.*

(i) For any place v of $\mathbb{Q}$, $\pi_{f,v}$ has central character $(\chi_{\mathbb{A}})_{|\mathbb{Q}_v^\times}$.
(ii) Let ψ be any Dirichlet character and v be any place of $\mathbb{Q}$, then $\pi_{f\otimes\psi,v} \simeq \pi_{f,v} \otimes (\psi_{\mathbb{A}})_{|\mathbb{Q}_v^\times}(\det)$.
(iii) For any $p \nmid N$, let $\alpha, \beta \in \mathbb{C}^\times$ be the two roots of $X^2 - a_p(f)X + p^{k-1}\chi(p)$, then $\pi_{f,p}$ is the principal series representation attached to the two unramified unitary characters $p \longmapsto \alpha p^{(1-k)/2}$, $p \longmapsto \beta p^{(1-k)/2}$ of $\mathbb{Q}_p^\times$.
(iv) Let $L_\infty(f,s) = 2(2\pi)^{-s}\Gamma(s)$, then, for any place v of $\mathbb{Q}$, $L_v\left(f, s + \frac{k-1}{2}\right) = L(\pi_{f,v}, s)$.
(v) If p is a prime number, $\varepsilon(\pi_{f,p}, s, \theta_p) = p^{-v_p(N)\left(s-\frac{1}{2}\right)}\varepsilon_p(f)$, in the sense of Definition C.3.6.
(vi) $\varepsilon(\pi_{f,\infty}, s, \theta_{\mathbb{R}}) = (-i)^k$.
(vii) If $k \geq 2$, then $\pi_{f,\infty}$ is the discrete holomorphic series *of weight k, that is, the representation $\sigma(|x|^{(k-1)/2}, |x|^{(1-k)/2}\mathfrak{s})$, where $\mathfrak{s}$ is the sign function. If $k = 1$, then $\pi_{f,\infty}$ is the* limit of discrete holomorphic series *$\pi(|x|^{1/2}, |x|^{-1/2})$.*

Proof. – [60, Theorem 5.19 (a)] attaches to f a certain automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ which appears in $L_0^2(\mathrm{GL}_2(\mathbb{Q})\backslash \mathrm{GL}_2(\mathbb{A}_\mathbb{Q}), \psi)$ for a certain continuous character $\psi : \mathbb{A}_\mathbb{Q}^\times/\mathbb{Q}^\times \to \mathbb{C}^\times$. By [20, Theorems 3.3.3, 3.3.4], this representation factors as a restricted tensor product of local representations. By [60, Theorem 5.19] and the discussion at the beginning of Section 5C of *loc.cit.*, π has conductor N: in particular, it is enough to test (v) at $s = 1/2$ by [60, Remark 6.13 (ii)]. We define π_f as the *contragredient* of this representation (which is the one constructed in, say, [20, Section 3.6]), which has the correct central character (and factorizes as a restricted tensor product), which concludes for (i).

The discussion at the beginning of [60, Section 5C] shows that, when $p \nmid N$, $\pi_{f,p}$ is the principal series representation attached to two unramified characters μ_1, μ_2 of $\mathbb{Q}_p^\times$, with $\mu_i = \|\cdot\|^{-s_i}$,

$$\mu_1\mu_2 = (\chi_{\mathbb{A}})_{|\mathbb{Q}_p^\times}, \quad \mu_1(p) + \mu_2(p) = p^{(1-k)/2}a_p(f).$$

Hence

$$p^{s_1+\frac{k-1}{2}} + p^{s_2+\frac{k-1}{2}} = a_p(f), \quad p^{\left(s_1+\frac{k-1}{2}\right)+\left(s_2+\frac{k-1}{2}\right)} = p^{k-1}\chi(p),$$

thus $\mu_1(p)p^{(k-1)/2}, \mu_2(p)p^{(k-1)/2}$ are the two roots of $X^2 - a_p(f)X + p^{k-1}\chi(p)$. This proves (iii) and (iv) for finite places at primes not dividing N.

For (vii), the situation when $k \geq 2$ is discussed at the beginning of [60, Section 5C], and for $k = 1$ it is [61, Remark 2.5.2]. This implies in particular (iv) at the infinite place.

In particular, if ψ is a Dirichlet character, the automorphic representations $\pi_f \otimes \psi_{\mathbb{A}}(\det)$ and $\pi_{f\otimes v}$ have the same components at infinity and the sane components at all but finitely many places, so they are isomorphic by strong multiplicity one [20, Theorem 3.3.6].

Now, the function $R(f,s) = \frac{L\left(\pi_f, s-\frac{k-1}{2}\right)}{L(f,s)}$ can be written, by [60, Theorem 6.15], as a product $\prod_{p|N}\frac{1-a_pp^{-s}}{1-b_pp^{-s}}$, with $|a_p| \leq p^{(k-1)/2}$ by [121, Theorem 4.6.17] and $|b_p| \leq p^{(k-1)/2}$ because $\pi_{f,p}$ is unitary (and the L-factors of ramified representations have degree at most 1 in p^{-s}). By Proposition C.3.2 and [60, Theorem 6.18], we have a functional equation $R(f,s) = \alpha R(\overline{f}, k-s)$, where $R(\overline{f}, s)$ is defined similarly and is of the form $\prod_{p|N}\frac{1-a'_pp^{-s}}{1-b'_pp^{-s}}$ with $|a'_p|, |b'_p| \leq p^{(k-1)/2}$, and $\alpha \in \mathbb{C}^\times$. In particular, for each p, there is a constant $\alpha_p \in \mathbb{C}^\times$ such that

$$(1 - a_p p^{-s})(1 - b'_p p^{s-k}) = \alpha_p (1 - b_p p^{-s})(1 - a'_p p^{s-k}), \quad \prod_p \alpha_p = \alpha.$$

By computing the coefficients in p^s and p^{-s}, we see that $b'_p = \alpha_p a'_p$ and $a_p = \alpha_p b_p$, so that, by computing the constant coefficient, we find

$$1 + \alpha_p^2 \frac{a'_p b_p}{p^k} = \alpha_p (1 + \frac{a'_p b_p}{p^k}),$$

so either $\alpha_p = 1$ or $a'_p b_p \neq 0$ and $\alpha_p = \frac{p^k}{a'_p b_p}$, so that either $\alpha_p = 1$ or $|\alpha_p| > 1$.

Let us show that the product of the α_p has module one. Indeed, the local constants in the functional equation for modular forms have module one by Propositions C.3.1 and C.3.2. On the automorphic side, this follows from [60, Theorem 6.18] and [80, Proposition 2.21.2 (ii)] for cuspidal representations, and [80, Propositions 3.5, 3.6] reduce the claim to the case of GL(1) for unitary characters by [60, Theorem 4.27][1] which follows from the explicit formula [160, (3.6.3)].

Therefore, every α_p is equal to one, so $a_p = b_p$ and we are done. This proves (iv) in full generality.

To establish (v), we already saw that it was enough to prove it at $s = 1/2$, which is claimed in [103, (2.12)]. All that remains to do is prove (vi), which is a consequence of the automorphic functional equation [60, Theorem 6.18], (v), and the modular functional equation from Proposition C.3.2 and Corollary C.3.5. □

The above properties are sufficient to determine the global dictionary, both from a global point of view (using the modular [121, Theorem 4.6.19] and automorphic [20, Theorem 3.3.6] multiplicity one theorems) and from a local point of view (using the converse theorem [21, §27.1] characterizing irreducible smooth representations by the L-factors and ε-factors attached to their twists). But we are interested in describing the correspondence more precisely in certain specific cases.

Proposition 4.2.2 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a normalized newform, and χ be its primitive Dirichlet character with conductor M.*

- *Let $p \mid N$ be prime such that $p^2 \nmid NM$. Then $\pi_{f,p}$ is the twist of the Steinberg representation of $\mathrm{GL}_2(\mathbb{Q}_p)$ by the unramified character $p \longmapsto a_p(f)p^{1-k/2}$.*
- *Let $p \mid N$ be prime and coprime to N/M. Then $\pi_{f,p}$ is the principal series representation of $\mathrm{GL}_2(\mathbb{Q}_p)$ attached to the characters $\alpha, \beta : \mathbb{Q}_p^\times \to \mathbb{C}^\times$ such that α is unramified and maps p to $a_p(f)p^{(1-k)/2}$, and $\alpha\beta = (\chi_{\mathbb{A}})_{|\mathbb{Q}_p^\times}$.*

Proof. – In the first case, Proposition 4.2.1 implies that $L(\pi_{f,p}, s) = 1 - a_p(f)p^{-(k-1)/2-s}$ with $a_p(f)^2 = p^{k/2-1}\chi(p)$ (Proposition C.2.1), so that $\pi_{f,p}$ is not cuspidal by [21, §24.5]. However, for any non trivial Dirichlet character ψ whose conductor is a p-th power, $a_p(f \otimes \psi) = 0$ by Corollary C.3.10, so $L(\pi_{f,p} \otimes (\psi_{\mathbb{A}})_{|\mathbb{Q}_p^\times}(\det), s) = 1$. Assume that $\pi_{f,p}$ is a principal series representation attached to two characters α, β of $\mathbb{Q}_p^\times$. Since $L(\pi_{f,p}, s) \neq 1$, by [21, §23.4, 26.1], we may assume that α is unramified. But then, there is a nontrivial character $\gamma : \mathbb{Q}_p^\times / p^{\mathbb{Z}} \to \mathbb{C}^\times$ such that $\beta\gamma$ is unramified, so that $L(\pi_{f,p} \otimes \gamma(\det), s) \neq 1$. By construction, we may write $\gamma = \psi_{|\mathbb{A}})_{|\mathbb{Q}_p^\times}$ for some nontrivial Dirichlet character ψ of conductor some power of p: this is a contradiction. So $\pi_{f,p}$ is a twist of the Steinberg representation, and by considering its L-function (using [21, §26.1]) the twisting character must map p to $a_p(f)p^{1-k/2}$.

In the second case, $L(\pi_{f,p}, s) = 1 - a_p(f)p^{-s-(k-1)/2} \neq 1$ by Proposition C.2.1, so as above $\pi_{f,p}$ is not cuspidal. Assume that $\pi_{f,p}$ is a twist of a Steinberg representation by the character ϕ:

[1] The definitions of [60] and [80] are compatible.

since $L(\pi_{f,p}, s) \neq 1$, ϕ is unramified, and the computation above shows that $\phi(p) = a_p(f)p^{1-k/2}$. One then has $L(\pi_{f\otimes\overline{\chi},p}, s) = L(\pi_{f,p} \otimes (\chi_{\mathbb{A}})_{|\mathbb{Q}_p^\times}(\det), s) = L(\phi(\chi_{\mathbb{A}})_{|\mathbb{Q}_p^\times}, s + 1/2) = 1$ because the character is ramified. Yet one has $L(\pi_{f\otimes\overline{\chi},p}, s) = L_p(\overline{f}, s+(k-1)/2) = 1-\overline{a_p(f)}p^{-s-(k-1)/2} \neq 1$, so we have a contradiction. Thus $\pi_{f,p}$ is the principal series induced from two characters α, β. By considering its L-function, we can assume that α is unramified and maps p to $a_p(f)p^{(1-k)/2}$. Moreover, $\alpha\beta$ is the central character of $\pi_{f,p}$, which is exactly $(\chi_{\mathbb{A}})_{|\mathbb{Q}_p^\times}$. □

Proposition 4.2.3 *Let $(f, \chi) \in \mathscr{C}$. Let $E/\mathbb{Q}_p$ be the unique unramified quadratic extension. There is a character $\alpha : E^\times/(1 + p\mathcal{O}_E) \to \mathbb{C}^\times$, unique up to $E/\mathbb{Q}_p$-conjugation, such that $\pi_{f,p}$ is the representation π_α from [21, §19.1] (so α does not factor through the norm $E^\times \to \mathbb{Q}_p^\times$). Moreover, for each $u \in \mathbb{Z}_p^\times$, $\alpha(u) = \overline{\chi}(u)$ and $\alpha(p) = 1$. If $\psi \in \mathcal{D}$, then the character thus attached to $(f \otimes \psi, \chi\psi^2) \in \mathscr{C}$ is exactly $\alpha \cdot \overline{\psi(N_{E/\mathbb{Q}_p})}$, with the convention that $\psi(p) = 1$.*

Remark If $\chi \in \mathcal{D}$, the character $\mathbb{Q}_p^\times \to \mathbb{C}^\times$ that maps p to 1 and agrees with $\overline{\chi}$ on $\mathbb{Z}_p^\times$ is exactly $(\chi_{\mathbb{A}})_{|\mathbb{Q}_p^\times}$.

Proof. – By [21, §24.3] and Proposition 4.2.1, one has $n(\pi_{f,p}, \theta_p) = 2$ so $n(\pi_{f,p}, \eta_p) = 0$. Let us now show that $\pi_{f,p}$ is cuspidal. By [21, §27.2] and Proposition 4.2.1, it is enough to show that for any Dirichlet character ψ whose conductor is a power P of p, one has $a_p(f \otimes \psi) = 0$. When $\psi \neq \overline{\chi}$, $f \otimes \psi$ has conductor P^2 by Corollary C.3.10, so by Proposition C.2.1 one has $a_p(f \otimes \psi) = 0$. Finally, $a_p(f \otimes \overline{\chi}) = a_p(\overline{f}) = \overline{a_p(f)} = 0$.

By [21, (25.2.3)], since η_p has level one, $\pi_{f,p}$ has normalized level zero, and the claim is a consequence of [21, §19.1 Proposition] (and the above remark for the central character and the behavior under twists). □

Corollary 4.2.5 *Let $(f, \chi) \in \mathscr{C}$ and $E/\mathbb{Q}_p$ be the quadratic unramified extension. By Proposition 4.2.3, let $\alpha : E^\times \to \mathbb{C}^\times$ be the character attached to $\pi_{f,p}$. Then the cuspidal representation C_f is attached to the character $\overline{\alpha}_{|\mathcal{O}_E^\times}$.*

Proof. – To ease notation, write $\tau = \mathrm{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}$ and $\nu = N_{\mathbb{F}_{p^2}/\mathbb{F}_p}$. For any $\psi \in \mathcal{D}$, using (in this order), Proposition 4.2.1, Proposition 4.2.3, and [21, §24.3, 25.2, 25.4, 23.7],

$$\begin{aligned}\lambda_p(f \otimes \psi) = \varepsilon_p(f \otimes \psi) &= \varepsilon(\pi_{f\otimes\psi,p}, \frac{1}{2}, \theta_p) = \varepsilon(\pi_{\alpha\cdot\overline{\psi}(N_{E/\mathbb{Q}_p})}, \frac{1}{2}, \eta_p) \\ &= \frac{-p}{(p^4)^{1/2}} \sum_{u\in(\mathcal{O}_E/p)^\times} \overline{\alpha}(u)\psi(\nu(u))\eta_p(\tau(u)).\end{aligned}$$

Let $M \in \mathrm{GL}_2(\mathbb{F}_p)$ be a generator of some nonsplit Cartan subgroup, and let $a, N \in \mathbb{F}_p^\times$ be its trace and determinant, respectively. Let $g \in (\mathcal{O}_E/p)^\times$ be one of the two elements with trace

a and norm N. One has $\overline{\alpha}(g)\overline{\alpha}(g^p) = \overline{\alpha}(\nu(g)) = \chi(N) = \phi(g)\phi(g^p)$ and, by Corollary 2.4.16,

$$\begin{aligned}
\mathrm{Tr}(M \mid C_f) &= \frac{\chi(a)}{p-1} \sum_{\psi \in \mathcal{D}} \psi\left(\frac{a^2}{N}\right) \lambda_p(f_\psi) \mathfrak{g}(\overline{\chi\psi^2}) \\
&= \frac{-\chi(a)}{p(p-1)} \sum_{\psi \in \mathcal{D}} \psi\left(\frac{a^2}{N}\right) \sum_{t \in (\mathcal{O}_E/p)^\times} \overline{\alpha}(t)\psi(\nu(t)) e^{2i\pi \frac{\tau(t)}{p}} \sum_{u \in \mathbb{F}_p^\times} \overline{\chi\psi^2}(u) e^{2i\pi u/p} \\
&= \frac{-1}{p(p-1)} \sum_{u \in \mathbb{F}_p^\times} \sum_{t \in (\mathcal{O}_E/p)^\times} \sum_{\psi \in \mathcal{D}} \overline{\alpha}(\frac{at}{-u}) e^{2i\pi \frac{u}{p}\left(1 - \frac{1}{a}\tau(\frac{at}{-u})\right)} \psi\left(\frac{1}{N}\nu(\frac{at}{-u})\right) \\
&= \frac{-1}{p} \sum_{\substack{t \in (\mathcal{O}_E/p)^\times \\ \nu(t) = N}} \sum_{u \in \mathbb{F}_p^\times} \overline{\alpha}(t) e^{2i\pi \frac{u}{p}\left(1 - \frac{\tau(t)}{a}\right)} = \frac{-1}{p} \sum_{\substack{t \in (\mathcal{O}_E/p)^\times \\ \nu(t) = N}} \sum_{u \in \mathbb{F}_p} \overline{\alpha}(t) e^{2i\pi \frac{u}{p}\left(1 - \frac{\tau(t)}{a}\right)} \\
&= - \sum_{\substack{t \in (\mathcal{O}_E/p)^\times \\ \tau(t) = a \\ \nu(t) = N}} \overline{\alpha}(t) = -\alpha(g) - \alpha(g^p),
\end{aligned}$$

so that $\overline{\alpha}(g) \in \{\phi(g), \phi^p(g)\}$, whence $\{\overline{\alpha}_{|\mathcal{O}_E^\times}, \overline{\alpha}^p_{|\mathcal{O}_E^\times}\} = \{\phi, \phi^p\}$. □

4.3 Basics on the Langlands correspondence

The following discussion of Weil groups is somewhat terse. We refer the reader wishing for more detail to Tate's article [160].

In this paragraph, all our local fields are assumed to be of characteristic zero.

To a non-Archimedean local field F one attaches a *Weil group* W_F: it is a topological group endowed with a reciprocity isomorphism $\mathfrak{a}_F : W_F^{ab} \to F^\times$ and a continuous homomorphism $W_F \to G_F$. Moreover, $\mathfrak{a}_F$ is the restriction of the class field theory isomorphism $G_F \to \hat{F^\times}$, which is normalized so that it maps a *geometric* Frobenius to a uniformizer of F. The Weil group is constructed as follows in [160]: let k be the residue field of F, then W_F is the subgroup of G_F made with the $\sigma \in G_F$ such that the image of σ in $\mathrm{Gal}(\overline{k}/k)$ is an integer power of the Frobenius (arithmetic or geometric). The topology on W_F is defined by the following properties:

- $I_F \subset W_F$ is an open subgroup,
- the topologies induced on I_F by $I_F \leq W_F$ and $I_F \leq G_F$ are the same,
- the image of the map $W_F \to G_F \to G_k$ is exactly $\langle F \rangle \simeq \mathbb{Z}$, where F is the Frobenius. We require that the induced map $W_F \to \langle F \rangle \simeq \mathbb{Z}$ be continuous, where $\mathbb{Z}$ is endowed with the discrete topology.

Finally, we denote by $\|\cdot\| : W_F \to \mathbb{R}^{+\times}$ the continuous group homomorphism given by the composition $W_F \xrightarrow{\mathfrak{a}_F} F^\times \xrightarrow{\|\cdot\|} \mathbb{R}^{+\times}$. In particular, it maps an *arithmetic* Frobenius to the cardinality of the residue field of $\mathcal{O}_F$.

When F is a local Archimedean field, there is also a definition of a topological group W_F along with its morphism to G_F, a reciprocity isomorphism $\mathfrak{a}_F : W_F^{ab} \to F^\times$ and a continuous group homomorphism $\|\cdot\| : W_F \to \mathbb{R}^{+\times}$. When F is complex, W_F is exactly $F^\times$; when F is real, $W_F = \overline{F}^\times \cup j\overline{F}^\times$, where $j^2 = -1$ and conjugation by j on $\overline{F}^\times$ is the nontrivial automorphism in $\mathrm{Gal}(\overline{F}/F)$.

Its definition is less explicit, but any number field F also has a Weil group W_F. It is endowed with a reciprocity isomorphism $\mathfrak{a}_F : W_F^{ab} \to \mathbb{A}_F^\times / F^\times$, and with a surjective homomorphism to G_F such that $\mathbb{A}_F^\times / F^\times \to W_F^{ab} \to G_F^{ab}$ is exactly the class field theory surjection (normalized like $\mathfrak{a}$: that is, it maps a uniformizer to a geometric Frobenius.

The Weil group is well-behaved with respect to extensions of local fields or number fields, as well as localizations at various places. We refer to [160, §1] for more information.

Definition 4.3.1 When F is a local field (resp. a global field), a *representation* of W_F over a field K of characteristic 0 (resp. over $\mathbb{C}$) is a group homomorphism $W_F \to \mathrm{GL}(V)$ for some finite-dimensional K-vector space V with open kernel (resp. a continuous homomorphism $W_F \to \mathrm{GL}(V)$, where $\mathrm{GL}(V)$ is endowed with its Archimedean topology).

Definition 4.3.2 When F is local non-Archimedean, a *Deligne representation* of W_F with coefficients in a field K of characteristic zero is a couple (ρ, N), where ρ is a representation of W_F on a finite-dimensional K-vector space V and N is a (necessarily nilpotent) endomorphism of V such that, for any $w \in W_F$, $\rho(w)N\rho(w)^{-1} = \|w\|N$. We say that (ρ, N) is a semi-simple Deligne representation if ρ is a semi-simple representation of W_F. If needed, a representation of W_F corresponds to the Deligne representation $(\rho, 0)$ of W_F.

The interest of Deligne representations is captured by the following result [160, (4.2.1)]:

Proposition 4.3.3 *Let F be a finite extension of $\mathbb{Q}_p$ and E be a finite extension of $\mathbb{Q}_\ell$ where p, ℓ are distinct primes. Choose a Frobenius $\phi \in W_F$ and a pro-ℓ-tame inertia character $t_\ell : I_F \to \mathbb{Q}_\ell$. To any Deligne representation (ρ, N) of W_F on a finite-dimensional E-vector space V, one can attach $\rho_E : \phi^n\sigma \in W_F \longmapsto \rho(\phi^n\sigma)\exp(t_\ell(\sigma)N) \in \mathrm{GL}_E(V)$ (where $\sigma \in I_F$ and $n \in \mathbb{Z}$), which is a continuous group homomorphism $W_F \to \mathrm{GL}(V)$ (where $\mathrm{GL}(V)$ is endowed with the ℓ-adic topology).*

This operation defines a bijection between the isomorphism classes of Deligne representations of W_F over E and the continuous representations of W_F over E, and it is independent from the choices of t_ℓ and ϕ.

Remark In [62, Definition 12.2.1], complex Deligne representations (or Weil-Deligne representations) are continuous representations of $W_F \times \mathrm{SL}_2(\mathbb{C})$ over a finite-dimensional $\mathbb{C}$-vector space such that their $\mathrm{SL}_2(\mathbb{C})$-component is algebraic. These two formalisms are equivalent, as is described in [64, §2.1].

Let V be a continuous representation of a p-adic field F with coefficients in a ℓ-adic field E. We denote the Weil-Deligne representation attached to $V_{|W_F}$ by $\mathrm{D}(V)$, if necessary by adding F or E as an index. Usually, the choice of E is immaterial, F is $\mathbb{Q}_p$ for some prime p, and V comes from a continuous representation of $G_{\mathbb{Q}}$ over E, and we will shorten $\mathrm{D}\left(V_{|G_{\mathbb{Q}_p}}\right)$ in $\mathrm{D}_p(V)$.

To complex representations (resp. Deligne representations) of W_F when F is an Archimedean (resp. non-Archimedean) local field, Deligne and Langlands attach L- and ε-factors, which are meromorphic functions of a complex variable s. The definition of the local ε also requires the datum of a nontrivial additive character ψ of $(F, +)$. While we will state the definition of the L-factors, the definition of the ε is more involved, and we simply recall some of their properties in Proposition 4.3.7 for easier manipulation. We refer to [160] and [21, Chapter 7] for more information. We follow the normalization of the latter, called "Langlands's local constants" in [160, (3.6)].

Definition 4.3.5 Let F be a non-Archimedean local field with Weil group W_F, inertia group I_F, geometric Frobenius ϕ, and let q be the cardinality of the residue field. For $t \geq -1$, let I_F^t denote the higher inertia subgroup in upper numbering (see [143, Chapter IV], for instance).

If (ρ, N) is a Deligne representation of W_F on some finite-dimensional complex vector space V, its L-function is the meromorphic function (see [160, (4.1.5)] or [21, (31.3.1)])

$$L(V, s) = \det(1 - q^{-s}\rho(\phi) \mid (\ker N)^{I_F})^{-1}.$$

If ρ is a representation of W_F in a characteristic zero field, then its conductor exponent $f(\rho)$ is given by the formula in [35, (4.5)] (an equivalent definition is in [139, §4]). It is not too difficult,

using [143, VI.2 Exercise 1a] as an intermediate step, to deduce that

$$f(\rho) = \int_{-1}^{\infty} \dim V/V^{I_F^t}\, dt.$$

(this formula appears in [165, Definition 3.1.27]; because upper numbering commutes with quotients, the formula does not have to involve the kernel of ρ).

If V is a Deligne representation of W_F, there is a modified formula for $a(V)$ in [160, (4.1.5)].

We can then do the following direct computation using Proposition 4.3.3.

Lemma 4.3.6 *Let E, F be two non-Archimedean local fields with coprime residue characteristics. Let V be a finite dimensional E-vector space endowed with a continuous action $\rho : G_F \to \mathrm{GL}_E(V)$. Let I_F denote the inertia group of G_F and I_F^t denote the higher ramification groups in upper numbering. Then:*

- *Fix an embedding $E \to \mathbb{C}$. Then $L(\mathrm{D}(V^*) \otimes_E \mathbb{C}, s)$ is exactly the evaluation of the rational fraction $\det(1 - t\rho(\mathrm{Frob}_F) \mid V_{I_F}) \in E(t) \subset \mathbb{C}(t)$ at q^{-s}, where q is the cardinality of the residue field of F and V_{I_F} is the space of* co-invariants *of V under the inertia.*
- *$f(\mathrm{D}(V)) = f(\mathrm{D}(V^*)) = \int_{-1}^{\infty} \dim_E(V/V^{I_F^t})\, dt$.*

Proposition 4.3.7 *Let F be a non-Archimedean local field with uniformizer ϖ, $s \in \mathbb{C}$ and $\psi : F \to \mathbb{C}^\times$ be nontrivial additive character. Let n_ψ be the largest integer n such that $\psi_{|\varpi^{-n}\mathcal{O}_F}$ is trivial (so if F is unramified over $\mathbb{Q}_p$, then $n_{\theta_F} = 0$). Let V be a complex Deligne representation of W_F with conductor exponent $f(V)$. Then:*

- *For any $a = \mathfrak{a}_F(\alpha) \in F^\times$, $\varepsilon(V, s, \psi(a\cdot)) = \det V(\alpha)\|a\|^{s-\frac{1}{2}}\varepsilon(V, s, \psi)$.*
- *Write $-1 = \mathfrak{a}_F(c)$, then $\varepsilon(V, s, \psi)\varepsilon(V^*, 1-s, \psi) = \det \rho(c)$.*
- *For any $s' \in \mathbb{C}$, $\varepsilon(V, s + s', \psi) = \varepsilon(V \otimes \|\cdot\|^{s'}, s, \psi)$.*
- *Let E/F be a finite extension and assume that $V = \mathrm{Ind}_E^F V_1$. Then there is a constant $\lambda_{E/F}(\psi)$ depending only on E/F and ψ (not on V_1) such that*

$$\varepsilon(V, s, \psi) = \varepsilon(V_1, s, \psi \circ \mathrm{Tr}_{E/F})\lambda_{E/F}(\psi)^{\dim V_1}.$$

- *The map $W \longmapsto \varepsilon(V \otimes W, s, \psi)$ (where W is a representation of W_F) is additive.*[2]
- *For any unramified $\chi : F^\times \to \mathbb{C}^\times$, $\varepsilon(V \otimes \chi(\mathfrak{a}_F), s, \psi) = \varepsilon(V, s, \psi)\chi(\varpi^{n_\psi \dim V + f(V)})$.*
- *Let W be an unramified representation of W_F and $\phi \in W_F$ be a geometric Frobenius, then*

$$\varepsilon(V \otimes W, s, \psi) = \varepsilon(V, s, \psi)^{\dim W} \det W(\phi^{n_\psi \dim V + f(V)}).$$

- *For any unramified $\chi : F^\times \to \mathbb{C}^\times$, $\varepsilon(\chi(\mathfrak{a}_F), s, \psi) = \chi(\varpi^{n_\psi})\|\varpi\|^{n_\psi(s-1/2)}$.*
- *With $V = \chi(\mathfrak{a}_F)$ for some $\chi : F^\times \to \mathbb{C}^\times$, for any $y \in \varpi^{f(V)+n_\psi}\mathcal{O}_F^\times$,*

$$\varepsilon(V, s, \psi) = \chi(y)\|\varpi\|^{(s-1/2)(f(V)+n_\psi)} \frac{\sum_{u \in (\mathcal{O}_F/\varpi^{f(V)})^\times} \chi^{-1}(u)\psi\left(\frac{u}{y}\right)}{\left|\sum_{u \in (\mathcal{O}_F/\varpi^{f(V)})^\times} \chi^{-1}(u)\psi\left(\frac{y}{u}\right)\right|}.$$

The first five claims also hold when F is Archimedean.

Proof. – These are easy computations using [160, §3.6] and [160, §29.4]. □

Remark In particular, this implies that the conductor exponent of a Deligne representation V of W_F is exactly the $n(V, \psi)$ of [21, §29.4 Proposition] with $\psi : F/\mathcal{O}_F \to \mathbb{C}^\times$ an additive character whose restriction to $\varpi_F^{-1}\mathcal{O}_F/\mathcal{O}_F$ (ϖ_F being a uniformizer of F) is nontrivial.

[2] This is false if we assume only that W is a Deligne representation.

These relations imply the following reformulation of [160, Theorem (3.5.3)]:

Proposition 4.3.9 *Let K be a number field with absolute discriminant Δ and V be a complex, finite-dimensional representation of W_K with absolute conductor M. Let $\Lambda(V,s), \Lambda(V^*,s)$ be the formal products $(M|\Delta|)^{s/2}\prod_v L(V_{|W_v},s), (M|\Delta|)^{s/2}\prod_v L(V^*_{|W_v},s)$ respectively (over all places of K). These formal products are convergent in some right-half plane, define holomorphic functions on this half-plane which extend as meromorphic functions on $\mathbb{C}$, and satisfy, for any nontrivial additive character $\psi = \prod_v \psi_v : \mathbb{A}_K/K \to \mathbb{C}^\times$, the functional equation*

$$\Lambda(V,s) = \prod_v \varepsilon(V_{|W_v}, \frac{1}{2}, \psi_v)\Lambda(V^*, 1-s).$$

The *local Langlands correspondence* is the following result: for any $n \geq 1$ and any local field F, there exists a bijection between the isomorphism classes of complex irreducible smooth admissible representations of $\mathrm{GL}_n(F)$ and the isomorphism classes of semi-simple n-dimensional Deligne representations of W_F. This correspondence preserves the L and ϵ constants on either side, as well as those of pairs (corresponding to the Rankin-Selberg convolution on the automorphic side and to the tensor product for representations of W_F), it respects the determinants, twists by characters of $F^\times$ (via $\mathfrak{a}_F$) and taking contragredients. A formal statement can be found in the beginning of [24] or in [62, Chapter 12.4].

Let us first spell out the situation for Dirichlet characters, since we will need it.

Lemma 4.3.10 *Let $\omega : G_{\mathbb{Q}} \to \hat{\mathbb{Z}}^\times$ be the cyclotomic character and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a primitive Dirichlet character. Then, for any prime number p, $\mathrm{D}_p(\chi(\omega)) = \overline{\chi}_{\mathbb{A}} \circ \mathfrak{a}_{\mathbb{Q}_p}$.*

Proof. – If $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ lies in the inertia group, it is known by [139, §3, Theorem 2] (note the different normalization for the class field theory isomorphism) that $\mathfrak{a}_{\mathbb{Q}_p}(\sigma) = \pi_p(\omega(\sigma))$, where $\pi_p : \hat{\mathbb{Z}}^\times \to \mathbb{Z}_p^\times$ is the projection. Moreover, ω acts trivially on the maximal unramified extension of $\mathbb{Q}_p$, which contains all the roots of unity in $\overline{\mathbb{Q}_p}^\times$ of order prime to p. Since $(\overline{\chi}_{\mathbb{A}})_{|\mathbb{Z}_p^\times}$ is exactly the p-part of χ (that is, a character $\chi_p : \mathbb{Z}_p^\times \to \mathbb{C}^\times$ such that the conductor of the Dirichlet character $\chi'_p = \chi\chi_p^{-1}$ is prime to p), the claimed equality holds for σ.

Let $F \in \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ be an inverse image under $\mathfrak{a}_{\mathbb{Q}_p}$ of $\frac{1}{p}$ (so that F is an *arithmetic* Frobenius). By [139, §3, Theorem 2], $\pi_p(\omega(F)) = 1$ and for any $q \neq p$, $\pi_q(\omega(F)) = p$, so that $\chi(\omega(F)) = \chi'_p(p)$. Now, we compute that

$$(\overline{\chi}_{\mathbb{A}})_{|\mathbb{Q}_p^\times}\left(\frac{1}{p}\right) = \prod_{\ell \neq p}(\overline{\chi}_{\mathbb{A}})_{|\mathbb{Z}_\ell^\times}(p) = \prod_{\ell \neq p}\chi_\ell(p) = \chi'_p(p).$$

□

Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a newform and p be a prime number. We can attach Deligne representations of $W_{\mathbb{Q}_p}$ to f in two seemingly distinct manners. A first possibility is to fix a number field $F \subset \mathbb{C}$ containing the coefficients of f and a prime ideal $\lambda \subset \mathcal{O}_F$ prime to p, then consider $\mathrm{D}_p(V_{f,\lambda}) \otimes_{F_\lambda} \mathbb{C}$ for some F-embedding of F_λ into $\mathbb{C}$. A second possibility is to consider the image $\sigma_{f,p}$ of $\pi_{f,p}$ under the local Langlands correspondence.

When $p \nmid N$, $\sigma_{f,p}$ and $(V_{f,\lambda})_{|W_{\mathbb{Q}_p}}$ are both sums of unramified characters of $W_{\mathbb{Q}_p}$, so relating them is not difficult. The same relation still holds at primes $p \mid N$ (but p coprime to λ), but this is significantly more delicate, and is the *local-global compatibility* proved by Carayol in [23].

Proposition 4.3.11 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a normalized newform. Let $E \subset \mathbb{C}$ be a number field containing the coefficients of f and $\lambda \subset \mathcal{O}_E$ a prime ideal.*

– *Let p be a prime number prime to λ and $\sigma : E_\lambda \to \mathbb{C}$ be a E-homomorphism. The isomorphism class of $\mathrm{D}_p\left(V^*_{f,\lambda}\right) \otimes_{E_\lambda} \mathbb{C}$ does not depend on the choice of λ or σ. We denote*

it by $D_{f,p}$ or sometimes $(V_f^*)_{|W_{\mathbb{Q}_p}}$.
- *The complex Deligne representation $\sigma_{f,p}$ of $W_{\mathbb{Q}_p}$ attached by the local Langlands correspondence to $\pi_{f,p}$ is $D_{f,p} \otimes \|\cdot\|^{(k-1)/2}$. In particular, $\varepsilon_p(f) = \varepsilon(D_{f,p}, \frac{k}{2}, \theta_p)$.*
- *The complex representation $\sigma_{f,\infty}$ of $W_{\mathbb{R}}$ attached to $\pi_{f,\infty}$ is exactly $\|\cdot\|^{(k-1)/2} \otimes \mathrm{Ind}_{W_{\mathbb{C}}}^{W_{\mathbb{R}}} z^{1-k}$.*
- *Let $\chi : (\mathbb{Z}/M\mathbb{Z})^\times \to E^\times$ be a primitive Dirichlet character and p be a prime. Then $D_{f,p} \otimes \chi_{\mathfrak{A}}(\mathfrak{a}_{\mathbb{Q}_p}) = D_{f\otimes\chi,p}$.*

Proof. – Let us first discuss the place at infinity. By Proposition 4.2.1, when $k \geq 2$, $\pi_{f,\infty}$ is the discrete holomorphic series of weight k $(\sigma(|x|^{(k-1)/2}, |x|^{(1-k)/2}\mathfrak{s}))$, so that by [61, §3.1] $\sigma_{f,\infty}$ is exactly the induced to $W_{\mathbb{R}}$ of the character $z \longmapsto \left(\frac{z}{|z|}\right)^{k-1}$ of $W_{\mathbb{C}}$. When $k \geq 1$, the same reference tells us that $\sigma_{f,\infty}$ is exactly $\mathbf{1} \oplus \mathfrak{s}$, where $\mathfrak{s}$ denotes the morphism $\mathfrak{s} \circ \mathfrak{a}_{\mathbb{R}} : W_{\mathbb{R}} \to \{\pm 1\}$.

When $k = 1$, the $V_{f,\lambda}^*$ all have finite image and come from the same odd representation $G_{\mathbb{Q}} \to \mathrm{GL}_2(F)$. In particular, its representation to $G_{\mathbb{R}}$ is exactly $1 \oplus \epsilon$, with ϵ the unique nontrivial character of $G_{\mathbb{R}}$, and thus its restriction to $W_{\mathbb{R}}$ is the correct one.

Now, we only discuss finite places. First, assume that $k \geq 2$ is even (resp. $k \geq 2$ is odd). Carayol's theorem [23, Theorem A] states that there is a finite extension E' of E_λ and a continuous two-dimensional representation $\sigma' : G_{\mathbb{Q}} \to \mathrm{GL}_2(E')$ such that, for any finite place $v \neq \ell$ (where ℓ is the residue characteristic of λ) of $\mathbb{Q}$, $\mathrm{D}_v(\sigma')$ is associated to $\pi_{f,v}$ (resp. $\pi_{f,v} \otimes \|\det\|^{-1/2}$, see the normalization in [23, §0.2]) under the so-called *Hecke correspondence* – a different normalization of the Langlands correspondence. Let $w \in \{0, 1\}$ be an integer with the same parity as k.

Fix an arbitrary E-embedding $E' \to \mathbb{C}$. Let $q \nmid N\ell$ be a prime, $I_q \leq G_{\mathbb{Q}}$ be an inertia group at q and Frob_q an arithmetic Frobenius at q. Then, for any $s \in \mathbb{Z}$,

$$\begin{aligned}\det(1 - q^{-s}\mathrm{Frob}_q \mid (\sigma')^{I_q}) &= L(\|\cdot\|^s \cdot \mathrm{D}_q\left((\sigma')^*\right))^{-1} = L\left(\pi_{f,q} \otimes \|\det\|^{-w/2}, s + \frac{1}{2}\right)^{-1} \\ &= \left(1 - \frac{a_q}{q^{k/2}} q^{-s+w/2} + \chi(q) q^{-2s-1+w}\right) \\ &= \det(1 - q^{-s}\mathrm{Frob}_q \mid V_{f,\lambda}(-(k-w)/2)),\end{aligned}$$

so that σ' is unramified outside ℓN and, by Cebotarev, $\sigma' \simeq V_{f,\lambda}(-(k-w)/2) \otimes_{E_\lambda} E'$. This implies in particular that, whenever $p \neq \ell$,

$$\sigma_{f,p} \simeq \|\cdot\|^{(w-1)/2} \otimes \mathrm{D}_p\left((\sigma')^*\right) \otimes_{E'} \mathbb{C} \simeq \left[\mathrm{D}_p\left(V_{f,\lambda}^*\right) \otimes_{E_\lambda} \mathbb{C}\right]\left(\frac{(k-w)+(w-1)}{2}\right),$$

whence the conclusion (where $V(z)$ denotes the twist of V by $\|\cdot\|^z$).

Regardless of the value of k, let χ be a Dirichlet character and p is a prime number distinct from the residue characteristic of λ. Write ω for the cyclotomic character. Then

$$D_{f\otimes\chi,p} = \mathrm{D}_p\left(V_{f\otimes\chi,\lambda}^*\right) = \mathrm{D}_p\left(V_{f,\lambda}^* \otimes \overline{\chi}(\omega)\right) = \mathrm{D}_p\left(V_{f,\lambda}^*\right) \otimes \mathrm{D}_p\left(\overline{\chi}(\omega)\right) = D_{f,p} \otimes \chi_{\mathbb{A}}(\mathfrak{a}_{\mathbb{Q}_p}).$$

When $k = 1$, while the result is certainly known, it is not covered by Carayol's theorem. Since we will need it, we give an elementary proof. Every $V_{f,\lambda}$ has finite image and is realizable over E by [37, Remarque 6.5 and footnote], so Cebotarev's theorem shows that these representations are all isomorphic to some $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(E) \subset \mathrm{GL}_2(\mathbb{C})$. We show that for all primes p, one has $\varepsilon_p(f) = \varepsilon(\mathrm{D}_p(\rho^*), \frac{1}{2}, \theta_p)$: using the compatibility with twists that we have just proved, the equality of conductors between ρ^* and f [37, Theorem 4.6] and the converse theorem [21, §27.1], we are done.

Let $p \mid N$ be a prime. Let S be the set of primes $q \mid N$ distinct from p. Let χ be the character of f, and, for each $q \mid N$, $\chi = \chi_q \chi_q'$, where the conductor of χ_q is a power of q and the conductor of χ_q' is coprime to q.

For each $q \in S'$, choose an odd integer $n_q > v_q(N) + 2$ such that the property of [21, §29.4 Proposition (4)] is satisfied for $\mathrm{D}_q(\rho^*)$ and the additive character θ_q. Let now ψ be an even Dirichlet character of conductor $M = \prod_{q \in S'} q^{n_q}$, and write as above $\psi = \prod_q \psi_q$, $\psi'_q = \psi\overline{\psi_q}$, where the conductor of ψ_q is q^{n_q}, and let us write $\sigma = \rho \otimes \chi$.

If $\omega : G_{\mathbb{Q}} \to \hat{\mathbb{Z}}^\times$ is the cyclotomic character, one can check directly that, for any primitive Dirichlet character φ, and any prime q, $\overline{\varphi}(\omega)_{|W_{\mathbb{Q}_q}} = \varphi_{\mathbb{A}}(\mathfrak{a}_{\mathbb{Q}_q})$.

Let $q \in S'$ and $Q = q^{n_q}$. Then, for a certain $c_q \in \mathbb{Q}_q^\times$,

$$\begin{aligned}\varepsilon(\mathrm{D}_q(\sigma^*), \frac{1}{2}, \theta_q) &= \varepsilon(\psi_{\mathbb{A}}(\mathfrak{a}_{\mathbb{Q}_q}) \otimes \mathrm{D}_p(\rho^*), \frac{1}{2}, \theta_q) \\ &= \det \mathrm{D}_q(\rho^*)(\mathfrak{a}_{\mathbb{Q}_q}^{-1}(c_q))^{-1} \varepsilon((\psi_{\mathbb{A}})_{|\mathbb{Q}_q^\times}, \frac{1}{2}, \theta_q)^2,\end{aligned}$$

where, for all $x \in 1 + q^{(n_q+1)/2}\mathbb{Z}_q$, $\overline{\psi_q}(1+x) = (\psi_{\mathbb{A}})_{|\mathbb{Q}_q^\times}(1+x) = \theta_p(c_q x)$. In particular, $c_q = \frac{z_q}{Q}$ for some $z_q \in \mathbb{Z}_q^\times$. Since $\det \rho = \overline{\chi}_{\mathbb{A}}(\mathfrak{a}_{\mathbb{Q}_q})$, one has

$$\det \mathrm{D}_q(\rho^*)(\mathfrak{a}_{\mathbb{Q}_q}^{-1}(c_q))^{-1} = (\overline{\chi}_{\mathbb{A}})_{|\mathbb{Q}_q^\times}(\frac{z_q}{Q}) = \chi_q(z_q)\overline{\chi'_q(Q)}.$$

Finally, by [160, (3.6.3)]

$$\varepsilon((\psi_{\mathbb{A}})_{|\mathbb{Q}_q^\times}, \frac{1}{2}, \theta_q) = (\psi_{\mathbb{A}})_{|\mathbb{Q}_q^\times}(Q)\frac{\mathfrak{g}(\psi_q)}{|\mathfrak{g}(\psi_q)|} = \psi'_q(Q)\frac{\mathfrak{g}(\psi_q)}{|\mathfrak{g}(\psi_q)|},$$

whence

$$\varepsilon(\mathrm{D}_q(\sigma^*), \frac{1}{2}, \theta_q) = \chi_q(z_q)\overline{\chi'_Q}(Q)\psi'_q(Q)^2\frac{\mathfrak{g}(\psi_q)^2}{Q}.$$

Now, by Proposition C.3.9 and the proof of Lemma C.1.4,

$$\varepsilon_q(f \otimes \psi_q) = \overline{\chi'_q}(Q)\psi_q(-1)\frac{\mathfrak{g}(\chi_q\psi_q)}{\mathfrak{g}(\overline{\psi_q})} = \overline{\chi'_q}(Q)\psi_q(-1)\chi_q(-(-z_q))\frac{\mathfrak{g}(\psi_q)}{\mathfrak{g}(\overline{\psi_q})},$$

thus by Proposition C.3.4 and Lemma C.1.2,

$$\begin{aligned}\varepsilon_q(f \otimes \psi) = \psi'_q(Q)^2\varepsilon_q(f \otimes \psi_q) &= \psi'_q(Q)^2\overline{\chi'_q}(Q)\psi_q(-1)\chi_q(z_q)\frac{\mathfrak{g}(\psi_q)}{\mathfrak{g}(\overline{\psi_q})} \\ &= \psi'_q(Q)^2\overline{\chi'_q}(Q)\chi_q(z_q)\frac{\mathfrak{g}(\psi_q)}{\overline{\mathfrak{g}(\psi_q)}} = \varepsilon(\mathrm{D}_q(\sigma^*), \frac{1}{2}, \theta_q).\end{aligned}$$

By Proposition C.3.2, the constant of $f \otimes \psi$ at infinity is $-i$. Since ρ is an odd Artin representation, by [160, §3.2], one has

$$\varepsilon_\infty(\sigma_\infty^*, \frac{1}{2}, \theta_\infty) = \varepsilon_{\mathbb{R}}(\mathbf{1}, \frac{1}{2}, \theta_\infty)\varepsilon_{\mathbb{R}}(\mathfrak{s}, \frac{1}{2}, \theta_\infty) = \mathbf{1}(-1) \cdot 1 \cdot \mathfrak{s}(-1) \cdot i = -i,$$

Since the global L-functions of σ^* (in the convention of [160]) and $f \otimes \psi$ are equal by [37, Théorème 4.6], we must have $\varepsilon_p(f \otimes \psi) = \varepsilon(\mathrm{D}_p(\sigma^*), \frac{1}{2}, \theta_p)$.

By Proposition C.3.4, $\varepsilon_p(f \otimes \psi) = \psi(p^{v_p(N)})\varepsilon_p(f)$. On the other hand, by [160, (3.6.5)],

$$\varepsilon(\mathrm{D}_p(\sigma^*), \frac{1}{2}, \theta_p) = \varepsilon(\mathrm{D}_{\rho^*}(\otimes)\psi_{\mathbb{A}}(\mathfrak{a}_{\mathbb{Q}_p}), \frac{1}{2}, \theta_p) = \psi(p^{v_p(N)})\varepsilon(\mathrm{D}_{\rho^*}(,)\frac{1}{2}, \theta_p),$$

whence the desired equality. □

Remark In the case $k = 1$, our argument is essentially a mimic of Deligne's proof of the existence of local constants (as exposed in for instance [21, Chapter 7]).

Corollary 4.3.13 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a newform with primitive character χ, $p \mid N$ be a prime and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ whose image under the cyclotomic character is $c = (c_q)_q \in \hat{\mathbb{Z}}^\times$. Write $\chi = \chi_p\chi'_p$, where the conductor of χ_p is a power of p and that of χ'_p is prime to p. Then $D_{\sigma(f),p} \simeq D_{f,p} \otimes_{\mathbb{C},\sigma} \mathbb{C}$ (for any extension of σ as an automorphism of $\mathbb{C}$) and one has*

$$\varepsilon_p(\sigma(f)) = \sigma(\varepsilon_p(f))\sigma(\chi_p(c_p))\frac{\sigma(p^{kv_p(N)/2})}{p^{kv_p(N)/2}}.$$

Proof. – We extend σ to an automorphism of $\mathbb{C}$. Let $F/\mathbb{Q}$ be a finite Galois extension containing the coefficients of f with $F \subset \mathbb{C}$. For any maximal ideal $\mathfrak{l} \subset \mathcal{O}_F$ with residue characteristic $\ell \neq p$, for any F-embedding $F_\mathfrak{l} \to \mathbb{C}$,

$$\begin{aligned} D_{\sigma(f),p} \otimes_{F_\mathfrak{l}} \mathbb{C} &\simeq \mathrm{D}_p\left(V^*_{\sigma(f),\mathfrak{l}}\right) \otimes_{F_\mathfrak{l}} \mathbb{C} \simeq \mathrm{D}_p\left(V^*_{f,\sigma^{-1}(\mathfrak{l})} \otimes_{F_{\sigma^{-1}(\mathfrak{l})},\sigma} F_\mathfrak{l}\right) \otimes F_\mathfrak{l}\mathbb{C} \\ &\simeq D_{f,p} \otimes_{\mathbb{C},\sigma} \mathbb{C}, \end{aligned}$$

hence $D_{\sigma(f),p} \simeq \sigma(D_{f,p})$.

Let η be the unramified character of $W_{\mathbb{Q}_p}$ mapping a Frobenius to $\frac{\sigma(\sqrt{p})}{\sqrt{p}}$. By the discussion around [160, (3.6.10)] and in its notation, one has

$$\begin{aligned} \varepsilon_p(\sigma(f)) &= \varepsilon(D_{\sigma(f),p}, \frac{k}{2}, \theta_p) = \varepsilon_1(\sigma(D_{f,p})\|\cdot\|^{k/2}, \theta_p) \\ &= \sigma(\varepsilon_1(D_{f,p}\|\cdot\|^{k/2}\eta^{kv_p(N)}, \sigma^{-1}\circ\theta_p)) = \sigma(\varepsilon_1(D_{f,p}\|\cdot\|^{k/2}, \eta^k, \theta_p(c_p^{-1}\cdot))) \\ &= \sigma(\varepsilon(D_{f,p}\otimes\eta^k, \frac{k}{2}, \theta_p(c_p^{-1}\cdot))) = \sigma\left[\det D_{f,p}(\mathfrak{a}^{-1}_{\mathbb{Q}_p}(c_p^{-1}))\varepsilon(D_{f,p}\otimes\eta^k, \frac{k}{2}, \theta_p)\right] \\ &= \sigma\left[\det D_{f,p}(\mathfrak{a}^{-1}_{\mathbb{Q}_p}(c_p^{-1}))\left(\frac{\sigma(\sqrt{p})}{\sqrt{p}}\right)^{kv_p(N)}\varepsilon(D_{f,p}, \frac{k}{2}, \theta_p)\right] \\ &= \sigma(\varepsilon_p(f))\frac{\sigma(p^{kv_p(N)/2})}{p^{kv_p(N)/2}}\sigma(\det D_{f,p}(\mathfrak{a}^{-1}_{\mathbb{Q}_p}(c_p^{-1}))). \end{aligned}$$

Let ω_N denote the mod N cyclotomic character. One has

$$\det D_{f,p} = \mathrm{D}_p\left(\det V^*_{f,\mathfrak{l}}\right) = \|\cdot\|^{1-k}\mathrm{D}_p\left(\chi^{-1}(\omega_N)\right) = \|\cdot\|^{1-k}\chi_\mathbb{A}\circ\mathfrak{a}_{\mathbb{Q}_p},$$

so that $\det D_{f,p}(\mathfrak{a}^{-1}_{\mathbb{Q}_p}(c_p^{-1})) = \chi_\mathbb{A}(c_p^{-1}) = \overline{\chi_p}(c_p^{-1}) = \chi_p(c_p)$. □

4.4 Preparation to the computation of the root numbers

This section is dedicated to various lemmas about the representations involved in Section 4.5. They will help in the computation, so we factor them out for clarity.

From now on, $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_p)$ is a continuous representation with $\det\rho = \omega_p^{-1}$. Let F be a number field as in Section 3.6, that is: it contains the $p(p-1)^2(p+1)$-th roots of unity, the coefficients of all the newforms in $\mathscr{S} \cup \mathscr{P} \cup \mathscr{C}$, and, for each prime ℓ such that $\ell \in \mathbb{F}_p^{\times 2}$ and every $(f, \mathbf{1}) \in \mathscr{C}_M$, F contains the roots of $X^2 - a_\ell(f)X + \ell$. We say that such a number field is *large enough*.

Lemma 4.4.1 *For any maximal ideal $\lambda \subset \mathcal{O}_F$,*

- *for any $(f, \mathbf{1}) \in \mathscr{S}$, $S := V_{f,\lambda} \otimes \mathrm{St}(\rho)$ satisfies $S^*(1) \simeq S$*
- *for any $(f, \chi) \in \mathscr{P}$, $P := V_{f,\lambda} \otimes \pi(1, \chi)(\rho)$ satisfies $P^*(1) \simeq P$.*
- *for any $(f, \chi) \in \mathscr{C}$, $C := V_{f,\lambda} \otimes C_f(\rho)$ satisfies $C^*(1) \simeq C$.*

– *for any* $(f,\mathbf{1})\in\mathscr{C}_M$, *any* $\epsilon\in\{\pm\}$, *any of the two characters* $\psi: G_{\mathbb{Q}(\sqrt{-p})}\to F_\mathfrak{l}$ *attached to* f, $I:=\mathrm{Ind}_{G_{\mathbb{Q}(\sqrt{-p})}}^{G_\mathbb{Q}}\psi\otimes C^\epsilon(\rho_{|G_{\mathbb{Q}(\sqrt{-p})}})$ *satisifes* $I^*(1)\simeq I$.

Proof. – Using the results of Appendix B (Corollary B.1.10 for $\mathscr{S}$, Lemma B.1.9 and Proposition B.1.4 for $\mathscr{P}$ and Corollaries B.2.8, B.2.9 for $\mathscr{C}$), one has:

$$\begin{aligned}
S^*(1)&\simeq V_{f,\lambda}^*(1)\otimes\mathrm{St}^*(\rho)\simeq V_{f,\lambda}\otimes\mathrm{St}(\rho), && (f,\mathbf{1})\in\mathscr{S}\\
P^*(1)&\simeq V_{f,\lambda}^*(1)\otimes\pi(1,\chi)^*(\rho)\simeq V_{f,\lambda}\otimes\overline{\chi}(\omega_p)\otimes\pi(1,\chi^{-1})(\rho)\\
&\simeq V_{f,\lambda}\otimes\chi(\det\rho)\otimes\pi(1,\chi^{-1})(\rho)\simeq V_{f,\lambda}\otimes\pi(\chi,1)(\rho), && (f,\chi)\in\mathscr{P}\\
C^*(1)&\simeq V_{f,\lambda}^*(1)\otimes C_f^*(\rho)\simeq V_{f,\lambda}\otimes\chi(\det\rho)\otimes C_{\overline{f}}(\rho)\\
&\simeq V_{f,\lambda}\otimes C_{\overline{f}\otimes\chi}(\rho)\simeq C, && (f,\chi)\in\mathscr{C}.
\end{aligned}$$

Let now $(f,\mathbf{1})\in\mathscr{C}_M$ and $\psi,\psi': G_{\mathbb{Q}(\sqrt{-p})}\to F_\mathfrak{l}^\times$ be the two characters attached to f: thus $\psi\psi'=\det V_{f,\lambda}$ is the cyclotomic character. Thus

$$(\psi\otimes C^\epsilon(\rho_{|G_{\mathbb{Q}(\sqrt{-p})}}))^*(1)\simeq\psi^{-1}\otimes\psi\psi'\otimes(C^\epsilon)^*(\rho_{|G_{\mathbb{Q}(\sqrt{-p})}})\simeq\psi'\otimes C^{-\epsilon}(\rho_{|G_{\mathbb{Q}(\sqrt{-p})}}).$$

Since $G_{\mathbb{Q}(\sqrt{-p})}=\rho^{-1}(\mathbb{F}_p^\times\,\mathrm{SL}_2(\mathbb{F}_p))$, $\psi\otimes C^\epsilon(\rho_{|G_{\mathbb{Q}(\sqrt{-p})}}))^*(1)$ is by Proposition B.4.1 the conjugate under $G_\mathbb{Q}/G_{\mathbb{Q}(\sqrt{-p})}$ of $\psi\otimes C^\epsilon(\rho_{|G_{\mathbb{Q}(\sqrt{-p})}})$, whence the conclusion. □

Lemma 4.4.2 *Let* $f\in\mathcal{S}_k(\Gamma_1(N))$ *be a normalized newform with character* χ, *and* $p\mid N$ *be a prime number not dividing* N/p *or the conductor of* χ. *Then* $D_{f,p}$ *is the couple* (ρ,N), *where* $\rho: W_{\mathbb{Q}_p}\to\mathrm{GL}_2(\mathbb{C})$ *is the unramified representation such that the geometric Frobenius acts by* $a_p(f)\begin{pmatrix}1&0\\0&p\end{pmatrix}$ *and* N *acts by* $\begin{pmatrix}0&1\\0&0\end{pmatrix}$.

Proof. – By Proposition 4.2.2, $\pi_{f,p}$ is the twist by the unramified character $p\longmapsto p^{1-k/2}a_p(f)$ of the Steinberg representation of $\mathrm{GL}_2(\mathbb{Q}_p)$. By [21, §33.3], $\sigma_{f,p}$ is the couple (σ,N) such that σ is the sum of the unramified characters $\phi\longmapsto\alpha p^{-1/2}$, $\phi\longmapsto\alpha p^{1/2}$, with $\alpha=p^{1-k/2}a_p(f)$. Since $\phi N\phi^{-1}=p^{-1}N$, after conjugating if necessary we may assume that

$$\sigma(\phi)=\begin{pmatrix}\alpha p^{-1/2}&0\\0&\alpha p^{1/2}\end{pmatrix},\quad N=\begin{pmatrix}0&1\\0&0\end{pmatrix}.$$

By Proposition 4.3.11, $D_{f,p}$ is the twist of $\sigma_{f,p}$ by the unramified character $\|\cdot\|^{(1-k)/2}$, which maps ϕ to $p^{(k-1)/2}$. □

Lemma 4.4.3 *Let* $(f,\chi)\in\mathscr{P}$. *Then* $D_{f,p}$ *is the direct sum of two characters of* $W_{\mathbb{Q}_p}$.

Proof. – By Proposition 4.2.2, $\pi_{f,p}$ is an irreducible principal series representation, so we just need to apply [21, §33.3]. □

Lemma 4.4.4 *Let* $(f,\chi)\in\mathscr{C}$. *Let* $E/\mathbb{Q}_p$ *be the unique quadratic unramified extension. Let* $\phi: E^\times/(1+p\mathcal{O}_E)\to\mathbb{C}^\times$ *be the character such that* $\{\phi_{|\mathcal{O}_E^\times},\phi^p_{|\mathcal{O}_E^\times}\}$ *is attached to the cuspidal representation* C_f *and* $\phi(p)=-p$. *Then* $D_{f,p}\simeq\left(\mathrm{Ind}_{W_E}^{W_{\mathbb{Q}_p}}\overline{\phi}\circ\mathfrak{a}_E,0\right)$.

Proof. – We saw that $\pi_{f,p}$ was the representation π_α for some character $\alpha: E^\times/(1+p\mathcal{O}_E)\to\mathbb{C}^\times$ such that $\overline{\alpha}_{|\mathcal{O}_E^\times}$ was attached to C_f and $\alpha(p)=1$. By the "tame" Langlands correspondence of [21, §34.4], $\sigma_{f,p}\simeq\left(\mathrm{Ind}_{W_E}^{W_{\mathbb{Q}_p}}(\alpha\eta)\circ\mathfrak{a}_E,0\right)$, with $\eta: E^\times/\mathcal{O}_E^\times\to\mathbb{C}^\times$ nontrivial and quadratic. Since

$$(\|\cdot\|_{W_{\mathbb{Q}_p}})_{|W_E}=\|\cdot\|_{\mathbb{Q}_p}\circ\mathfrak{a}_{\mathbb{Q}_p}\circ(W_E\subset W_{\mathbb{Q}_p})=\|\cdot\|_{\mathbb{Q}_p}\circ N_{E/\mathbb{Q}_p}\circ\mathfrak{a}_E=\|\cdot\|_E\circ\mathfrak{a}_E=\|\cdot\|_{|W_E},$$

one has

$$D_{f,p} \simeq \sigma_{f,p} \otimes \|\cdot\|^{-1/2} \simeq (\mathrm{Ind}_{W_E}^{W_{\mathbb{Q}_p}}(\alpha\eta\|\cdot\|_E^{-1/2}) \circ \mathfrak{a}_E, 0),$$

with $\alpha(p)\eta(p)\|p\|_E^{-1/2} = 1 \cdot (-1) \cdot (p^{-2})^{-1/2} = -p$, whence the conclusion. □

Definition 4.4.5 Given a newform $f \in \mathcal{S}_k(\Gamma_1(N))$, we let $D_{f,\infty}$ (or $\mathrm{D}_\infty\left(V_{f,\lambda}^*\right)$, for any maximal ideal λ of any $\mathcal{O}_F$, where $F \subset \mathbb{C}$ is a number field containing the coefficients of f) be the complex representation of $W_{\mathbb{R}}$ given by $\mathrm{Ind}_{W_{\mathbb{C}}}^{W_{\mathbb{R}}} z^{1-k}$.

Proposition 4.4.6 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a newform with primitive character χ. Let F be a number field containing the coefficients of f and $\lambda \subset \mathcal{O}_F$ a maximal ideal.*

(i) Let $\sigma : G_{\mathbb{Q}} \to \mathrm{GL}_2(n)\mathbb{C}$ be an Artin representation and c be the complex conjugation. Then one has

$$\varepsilon(\mathrm{D}_\infty(\sigma), \frac{1}{2}, \theta_\infty)\varepsilon(\mathrm{D}_\infty(\sigma^*), \frac{1}{2}, \theta) = \det\sigma(c), \quad \varepsilon(\mathrm{D}_\infty((V_{f,\lambda} \otimes \sigma)^*), \frac{k}{2}, \theta_\infty) = (-i)^{kn}.$$

(ii) Let p be a prime number prime to λ such that $D_{f,p}$ is the direct sum of two characters α, β of $\mathbb{Q}_p^\times$, and $\sigma : G_{\mathbb{Q}_p} \to \mathrm{GL}_n(\mathbb{C})$ be a continuous representation such that $\sigma^* \simeq \sigma \otimes \chi$. Then $\alpha(-1)^n = \beta(-1)^n$ and

$$\varepsilon(\mathrm{D}_p((V_{f,\lambda} \otimes \sigma)^*), \frac{k}{2}, \theta_p) = \alpha(-1)^n\varepsilon(\mathrm{D}_p(\sigma), \frac{1}{2}, \theta_p)\varepsilon(\mathrm{D}_p(\sigma^*), \frac{1}{2}, \theta_p).$$

(iii) Let $p \mid N$ be a prime number prime to λ and the conductor of χ, and such that $p^2 \nmid N$. Let $\sigma : G_{\mathbb{Q}_p} \to \mathrm{GL}_n(\mathbb{C})$ be a continuous representation such that $\sigma^* \simeq \sigma \otimes \chi$. Let $I_p \leq G_{\mathbb{Q}_p}$ be the inertia group and Frob_p be an arithmetic Frobenius, then

$$\varepsilon(\mathrm{D}_p((V_{f,\lambda} \otimes \sigma)^*), \frac{k}{2}, \theta_p) = \varepsilon(\mathrm{D}_p(\sigma), \frac{1}{2}, \theta_p)\varepsilon(\mathrm{D}_p(\sigma^*), \frac{1}{2}, \theta_p)\det(-p^{1-k/2}a_p(f)\mathrm{Frob}_p \mid \sigma^{I_p}).$$

Proof. – (i): The first equality is the local functional equation. For the second equality, σ is an Artin representation, so the representation $\mathrm{D}_\infty(\sigma)$ of $W_{\mathbb{R}}$ factors through the quotient $W_{\mathbb{R}} \to G_{\mathbb{R}}$ and is the sum of the characters $\mathbf{1}$ and $\mathfrak{s}$. Since $\varepsilon(D_{f,\infty}, \frac{k}{2}, \theta_\infty) = (-i)^k$, all we need to do is prove that $D_{f,\infty} \otimes \mathfrak{s} \simeq D_{f,\infty}$. This is true because $D_{f,\infty}$ is induced from the subgroup $W_{\mathbb{C}}$ of index two and $\mathfrak{s}$ is a character of $W_{\mathbb{R}}/W_{\mathbb{C}}$.

Now, we consider the situation of (ii) let p be a prime number coprime to λ and assume that $D_{f,p}$ is the direct sum of the characters α, β of $\mathbb{Q}_p^\times$, and that $\sigma : G_{\mathbb{Q}_p} \to \mathrm{GL}_n(\mathbb{C})$ is a continuous representation such that $\sigma^* \otimes \sigma \otimes \chi$. In particular, after taking $\det \mathrm{D}_p(-)$ and evaluating at $\mathfrak{a}_{\mathbb{Q}_p}^{-1}(-1)$, we see that when n is odd, $(\overline{\chi}_{\mathbb{A}})_{|\mathbb{Q}_p^\times}(-1) = 1$.

One has $(\alpha\beta) \circ \mathfrak{a}_{\mathbb{Q}_p} = \det D_{f,p} = (\|\cdot\|^{k-1}\overline{\chi}_{\mathbb{A}} \circ \mathfrak{a}_{\mathbb{Q}_p})^{-1} = \|\cdot\|^{1-k}\chi_{\mathbb{A}}(\mathfrak{a}_{\mathbb{Q}_p})$, so $\alpha(-1)^n = \beta(-1)^n$. Write $\alpha = \alpha_0\|\cdot\|^{(1-k)/2}, \beta = \beta_0\|\cdot\|^{(1-k)/2}$, $\beta_0(\overline{\chi}_{\mathbb{A}})_{\mathbb{Q}_p^\times} = \alpha_0^{-1}$, then one has

$$\begin{aligned}
\varepsilon(\mathrm{D}_p((V_{f,\lambda} \otimes \sigma)^*), \frac{k}{2}, \theta_p) &= \varepsilon(\mathrm{D}_p(\sigma^*) \otimes \alpha_0(\mathfrak{a}_{\mathbb{Q}_p}), \frac{1}{2}, \theta_p)\varepsilon(\mathrm{D}_p(\sigma^*) \otimes \beta_0(\mathfrak{a}_{\mathbb{Q}_p}), \frac{1}{2}, \theta_p) \\
&= \varepsilon(\mathrm{D}_p(\sigma^*) \otimes \alpha_0(\mathfrak{a}_{\mathbb{Q}_p}), \frac{1}{2}, \theta_p)\varepsilon(\mathrm{D}_p(\sigma) \otimes ((\overline{\chi}_{\mathbb{A}})\beta_0)(\mathfrak{a}_{\mathbb{Q}_p}), \frac{1}{2}, \theta_p) \\
&= \varepsilon(\mathrm{D}_p(\sigma^*) \otimes \alpha_0(\mathfrak{a}_{\mathbb{Q}_p}), \frac{1}{2}, \theta_p)\varepsilon(\mathrm{D}_p(\sigma) \otimes \alpha_0^{-1}(\mathfrak{a}_{\mathbb{Q}_p}), \frac{1}{2}, \theta_p) \\
&= \det\sigma^* \otimes \alpha_0(\mathfrak{a}_{\mathbb{Q}_p})(\mathfrak{a}_{\mathbb{Q}_p}^{-1}(-1)) = \alpha_0(-1)^n \det\sigma(\mathfrak{a}_{\mathbb{Q}_p}^{-1}(-1)) \\
&= \alpha(-1)^n\varepsilon(\mathrm{D}_p(\sigma), \frac{1}{2}, \theta_p)\varepsilon(\mathrm{D}_p(\sigma^*), \frac{1}{2}, \theta_p).
\end{aligned}$$

Now we prove (iii). Assume instead that p does not divide the conductor of χ and $v_p(N) = 1$. Let $\alpha : W_{\mathbb{Q}_p} \to \mathbb{C}^\times$ be the unramified character mapping a geometric Frobenius ϕ to $a_p(f)$. Then $D_{f,p} = (\rho, N)$, with $N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\rho = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha\|\cdot\|^{-1} \end{pmatrix}$. By [21, §31.3][3],

$$\begin{aligned}
&\varepsilon(\mathrm{D}_p((V_{f,\lambda}\otimes\sigma)^*), \frac{k}{2}, \theta_p) = \varepsilon(D_{f,p}\otimes \mathrm{D}_p(\sigma^*), \frac{k}{2}, \theta_p) \\
&= \varepsilon((\alpha\oplus\alpha\|\cdot\|^{-1})\otimes \mathrm{D}_p(\sigma^*), \frac{k}{2}, \theta_p) \\
&\qquad \times \frac{L(\mathrm{D}_p(\sigma)\otimes\alpha^{-1}, \frac{2-k}{2})L(\mathrm{D}_p(\sigma)\otimes\alpha^{-1}\|\cdot\|, \frac{2-k}{2})L(\mathrm{D}_p(\sigma^*)\otimes\alpha, \frac{k}{2})}{L(\mathrm{D}_p(\sigma^*)\otimes\alpha, \frac{k}{2})L(\mathrm{D}_p(\sigma^*)\otimes\alpha\|\cdot\|^{-1}, \frac{k}{2})L(\mathrm{D}_p(\sigma)\otimes\alpha^{-1}\|\cdot\|, \frac{2-k}{2})} \\
&= \varepsilon((\alpha\oplus\alpha\|\cdot\|^{-1})\otimes \mathrm{D}_p(\sigma^*), \frac{k}{2}, \theta_p)\frac{L(\mathrm{D}_p(\sigma)\otimes\alpha^{-1}, 1-k/2)}{L(\mathrm{D}_p(\sigma^*)\otimes\alpha\|\cdot\|^{-1}, k/2)}.
\end{aligned}$$

Because σ has finite image, if $I \leq W_{\mathbb{Q}_p}$ denotes the inertia subgroup,

$$\begin{aligned}
&\frac{L(\mathrm{D}_p(\sigma)\otimes\alpha^{-1}, 1-\frac{k}{2})}{L(\mathrm{D}_p(\sigma^*)\otimes\alpha\|\cdot\|^{-1}, \frac{k}{2})} = \frac{\det(1-\sigma^*(\phi)\alpha(\phi)\|\phi\|^{-1}p^{-k/2} \mid (\sigma^*)^I)}{\det(1-\sigma(\phi)\alpha^{-1}(\phi)p^{k/2-1} \mid \sigma^I)} \\
&= \frac{\det(1-\sigma(\phi^{-1})\alpha(\phi)p^{1-k/2} \mid \sigma^I)}{\det(1-\sigma(\phi)\alpha^{-1}(\phi)p^{k/2-1} \mid \sigma^I)} = \det(-p^{1-k/2}\sigma(\phi^{-1})\alpha(\phi) \mid \sigma^I) \\
&= \det(-p^{1-k/2}\sigma(\mathrm{Frob}_p)a_p(f) \mid \sigma^I).
\end{aligned}$$

On the other hand, the properties of local constants imply that, for any two unramified characters β, γ of $W_{\mathbb{Q}_p}$, $\varepsilon((\beta\oplus\gamma)\otimes \mathrm{D}_p(\sigma^*), \frac{k}{2}, \theta_p)$ only depends on $\beta\gamma$. Therefore, since $\alpha^2\|\cdot\|^{-1}$ is the unramified character $\chi_{\mathbb{A}}(\mathfrak{a}_{\mathbb{Q}_p})\|\cdot\|^{1-k} : \phi \longmapsto p^{k-1}\chi(p)$,

$$\begin{aligned}
&\varepsilon(\mathrm{D}_p((V_{f,\lambda}\otimes\sigma)^*), \frac{k}{2}, \theta_p) \\
&= \varepsilon(\mathrm{D}_p(\sigma^*)\otimes(\|\cdot\|^{(1-k)/2}\oplus\|\cdot\|^{(1-k)/2}\chi_{\mathbb{A}}(\mathfrak{a}_{\mathbb{Q}_p})), \frac{k}{2}, \theta_p)\det(-p^{1-k/2}\sigma(\mathrm{Frob}_p)a_p(f) \mid \sigma^I) \\
&= \varepsilon(\mathrm{D}_p(\sigma^*), \frac{1}{2}, \theta_p)\varepsilon(\mathrm{D}_p(\sigma^*\otimes\overline{\chi}), \frac{1}{2}, \theta_p)\det(-p^{1-k/2}\sigma(\mathrm{Frob}_p)a_p(f) \mid \sigma^I),
\end{aligned}$$

whence the conclusion. □

To study the local constants at the place p, we need first to study the shape of representations $G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\mathbb{F}_p)$.

Proposition 4.4.7 *Let $p \geq 5$ be a prime. Write $G = G_{\mathbb{Q}_p}$ and let $I \triangleleft G$ the inertia subgroup. Let $\rho : G \to \mathrm{GL}_2(\mathbb{F}_p)$ be a continuous group homomorphism with $\det\rho = \omega_p^{-1}$. Then exactly one of the following statements is true:*

- *ρ is not tamely ramified. There are characters $q, \beta : G \to \mathbb{F}_p^\times$ and a cocycle $\nu : G \to \mathbb{F}_p(q)$ that does not vanish on the wild inertia subgroup such that ρ is conjugate to a representation of the form $\sigma \longmapsto \beta(\sigma)\begin{pmatrix} q(\sigma) & \nu(\sigma) \\ 0 & 1 \end{pmatrix}$.*
- *ρ is conjugate to a representation of the form $\sigma \longmapsto \begin{pmatrix} \alpha(\sigma) & 0 \\ 0 & \beta(\sigma) \end{pmatrix}$ for some characters $\alpha, \beta : G \to \mathbb{F}_p^\times$, and $\det : \rho(I) \to \mathbb{F}_p^\times$ is an isomorphism.*

[3] This formula yields the same result as [160, (4.1.5)], because for a Deligne representation (ρ, N) on a $\mathbb{C}$-vector space V, $(z, f) \in ((V/\ker N)\otimes\|\cdot\|^{-1}) \times V^*/\ker N^* \longmapsto f(Nz) \in \mathbb{C}$ is a perfect duality of representations of W_F.

– *There exists a nonsplit Cartan subgroup $C \leq \mathrm{GL}_2(\mathbb{F}_p)$ such that $\rho^{-1}(C)$ is exactly the Galois group of the unramified quadratic extension of $\mathbb{Q}_p$. Moreover, $\rho(I)$ is a subgroup of C of index $a \mid \frac{p+1}{2}$ prime to $p-1$.*

Proof. – First, let us check that all statements are pairwise incompatible. Clearly, the first condition is not compatible with any of the other two, in which ρ is tamely ramified. In the second situation, $\rho(I)$ has order $p-1$, while, in the third situation, $\rho(I)$ has order $\frac{p^2-1}{a} \geq \frac{p^2-1}{(p+1)/2} = 2(p-1)$, so they are incompatible too.

Now, we show that one of the three statements holds.

Since the wild inertia subgroup $I^+ \triangleleft G$ is a pro-p-group, the image of I^+ is either trivial (then ρ is tamely ramified) or conjugate to the subgroup $U^{\mathbb{Z}} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

Suppose we are in the latter case. Then (after conjugating so that $\rho(I^+) = U^{\mathbb{Z}}$), $\rho(G)$ is contained in the normalizer of $U^{\mathbb{Z}}$, which is the group of upper-triangular matrices, so we can write $\rho(\sigma) = \beta(\sigma) \begin{pmatrix} q(\sigma) & \nu(\sigma) \\ 0 & 1 \end{pmatrix}$ for some characters $q, \beta : G \to \mathbb{F}_p^\times$, and $\nu : G \to \mathbb{F}_p$. It can be directly checked that $\nu : G \to \mathbb{F}_p(q)$ is a cocycle, and since $\rho(I^+)$ is nontrivial, $\nu(I^+) = \mathbb{F}_p$.

So assume from now on that ρ is tamely ramified. Let s be a pro-generator of the pro-cyclic group I/I^+, which has a pro-order prime to p, so that $\det \rho(s)$ generates $\det \rho(I) = \omega_p^{-1}(I) = \mathbb{F}_p^\times$. Therefore, $\rho(s) \in \mathrm{GL}_2(\mathbb{F}_p)$ is non scalar and its order is prime to p, hence it is either diagonalizable in $\mathrm{GL}_2(\mathbb{F}_p)$, or a non-scalar element of some nonsplit Cartan subgroup C.

In the former situation, after conjugating, we can assume that $\rho(s) = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ with $\alpha \neq \beta$, so that $\rho(x^p) = \rho(x)$ for any $x \in I$. In particular, if $z \in G$ is an arithmetic Frobenius, $\rho(z)\rho(x)\rho(z)^{-1} = \rho(zxz^{-1}) = \rho(x^p) = \rho(x)$, so $\rho(G)$ is contained in the centralizer subgroup of $\rho(s)$, which consists of the diagonal matrices and is abelian. Therefore, $\rho(I)$ is a quotient of the image of I in G^{ab}, which is $\mathbb{Z}_p^\times$. Since $\rho(I)$ is cyclic with order prime to p, it follows that $\rho(I)$ is a quotient of $\mathbb{F}_p^\times$. Since $\det : \rho(I) \to \mathbb{F}_p^\times$ is surjective by the assumption on ρ, it is an isomorphism.

We now assume that $\rho(s)$ is a non-scalar element of some nonsplit Cartan group C. Then $\rho(I)$ is a subgroup of C, so it is cyclic of index $a \mid p^2 - 1$. Since $\det C = \mathbb{F}_p^\times = \det \rho(I)$, we have $(p+1)C = (p+1)\rho(I)$, so that the greatest common divisor $(p+1)a$ and p^2-1 is exactly $p+1$. Thus a is coprime to $p-1$: it is odd, so coprime to $2(p-1)$ and $a \mid \frac{p+1}{2}$. An explicit computation shows that the normalizer of $\frac{p+1}{2}C$ in $\mathrm{GL}_2(\mathbb{F}_p)$ is exactly the normalizer N of C, so that $\rho(G) \subset N$.

If $\rho(G) \subset C$, then the image of ρ is commutative, so that $\rho(I)$ is a quotient of the image of I in G^{ab}, which is $\mathbb{Z}_p^\times$. Since $\rho(I)$ is cyclic with order prime to p, $\rho(I)$ is a quotient of $\mathbb{F}_p^\times$, which is impossible since $|\rho(I)| = \frac{p^2-1}{a} \geq \frac{p^2-1}{(p+1)/2} = 2(p-1)$. So $\rho^{-1}(C)$ is the Galois group of some quadratic unramified extension of $\mathbb{Q}_p$, that is, of *the* quadratic unramified extension of $\mathbb{Q}_p$. □

Definition 4.4.8 In the situation of Proposition 4.4.7, we say that ρ is

- *wild* if it is not tamely ramified,
- *split* if it is conjugate to a representation of the form $\sigma \longmapsto \begin{pmatrix} \alpha(\sigma) & 0 \\ 0 & \beta(\sigma) \end{pmatrix}$ for some characters $\alpha, \beta : G \to \mathbb{F}_p^\times$,
- *a-Cartan* if $\rho(G)$ is contained in the normalizer N of a Cartan subgroup C, with $\rho^{-1}(C)$ the Galois group of the quadratic unramified extension of $\mathbb{Q}_p$ and $\rho(I)$ is a cyclic subgroup of C of index $a \mid \frac{p+1}{2}$ coprime to $p-1$.

Note that being wild, split, or a-Cartan only depends on the conjugacy class of ρ.

Lemma 4.4.9 *Let $q, \beta : G_{\mathbb{Q}_p} \to \mathbb{F}_p^\times$ be characters and $\nu : G_{\mathbb{Q}_p} \to \mathbb{F}_p(q)$ be a cocycle whose restriction to the wild inertia subgroup does not vanish. Let $\rho(\sigma) = \beta(\sigma)\begin{pmatrix} q(\sigma) & \nu(\sigma) \\ 0 & 1 \end{pmatrix}$ for every $\sigma \in G_{\mathbb{Q}_p}$ and assume that $\det \rho = \omega_p^{-1}$. Let $G = G_{\mathbb{Q}_p}$, $I \lhd G$ be the inertia subgroup, $I^+ \lhd G$ the wild inertia subgroup. Then:*

- *the image of $(q\beta, \beta) : I/I^+ \to (\mathbb{F}_p^\times)^2$ is cyclic with order $p-1$,*
- *the extension $L/\mathbb{Q}_p$ defined by $G_L = \ker q$ is tamely ramified of degree dividing $p-1$,*
- *$f_{L/\mathbb{Q}_p}$ is odd and $v_2(e_{L/\mathbb{Q}_p}) = v_2(p-1)$,*
- *$\nu_{|G_L}$ is a wildly ramified character of conductor exponent c such that $c-1$ is coprime to $e_{L/\mathbb{Q}_p}$,*
- *$q_{|I}$ is the $(c-1)$-th power of the tame inertia character of $\mathrm{Gal}(L/\mathbb{Q}_p)_0$, so that $q_{|I}$ is equal to the $\frac{(c-1)(p-1)}{e}$-th power of the mod p cyclotomic character,*
- *$c \leq e + 1 + \frac{e}{p-1}$,*
- *L is linearly disjoint from the quadratic unramified extension E of $\mathbb{Q}_p$ and the Langlands constant $\lambda_{LE/\mathbb{Q}_p}(\theta_p)$ is $(-1)^{(p+1)/2}$,*
- *Let $M \in \mathrm{GL}_2(\mathbb{F}_p)$ be such that $M\rho M^{-1} = \beta' \begin{pmatrix} q' & \nu' \\ 0 & 1 \end{pmatrix}$, then one has*

$$(\beta', q') = (\beta, q), \quad \nu'_{|G_L} \in \left(\frac{\det M}{p}\right) \mathbb{F}_p^{\times 2} \nu_{|G_L}.$$

Proof. – $\sigma \longmapsto \begin{pmatrix} (q\beta)(\sigma) & 0 \\ 0 & 1 \end{pmatrix}$ is a split representation, so the first claim follows from Proposition 4.4.7. Let now be $L/\mathbb{Q}_p$ the extension such that $\ker q = G_L$, and $E/\mathbb{Q}_p$ be the unique quadratic unramified extension. Since $H := \mathrm{Gal}(L/\mathbb{Q}_p)$ identifies with the image of q, it is a cyclic group of order dividing $p-1$, so that $L/\mathbb{Q}_p$ is tamely ramified.

Let $a : \mathbb{Q}_p^\times/(1+p\mathbb{Z}_p) \to \mathbb{F}_p^\times$ be such that $a \circ \mathfrak{a}_{\mathbb{Q}_p} = q$, so that $\ker a = N_{L/\mathbb{Q}_p} L^\times$. Since $(q\beta^2)(I) = \det \rho(I) = \mathbb{F}_p^\times$, $q(I) \not\subset \mathbb{F}_p^{\times 2}$, thus $a(\mathbb{Z}_p^\times) \not\subset \mathbb{F}_p^{\times 2}$, so that $\mathbb{F}_p^\times/a(\mathbb{Z}_p^\times)$ has odd cardinality. Since $|a(\mathbb{Z}_p^\times)| = e_{L/\mathbb{Q}_p}$ (which we denote e for short), $v_2(e) = v_2(p-1)$. In particular, $v_2(e) \leq v_2(|H|) \leq v_2(p-1)$, so $v_2(|H|) = v_2(e) = v_2(p-1)$ and $f_{L/\mathbb{Q}_p}$ is odd, therefore E and L are linearly disjoint.

$\nu : G_L \to \mathbb{F}_p$ is a morphism, and its restriction to the wild inertia subgroup is onto. Therefore, its conductor exponent c is at least 2. Write $\nu_{|G_L} = \nu_0 \circ \mathfrak{a}_L$, for some group homomorphism $\nu_0 : L^\times \to \mathbb{F}_p$. For $x \in G, y \in G_L$, we can see that $\nu(xyx^{-1}) = q(x)\nu(y)$, so, for any $\sigma \in H$ and $x \in L^*$, $\nu_0(\sigma(x)) = q(\sigma)\nu_0(x)$.

Let $K \subset L$ be the maximal subextension which is unramified over $\mathbb{Q}_p$: there are uniformizers $\pi \in K, \varpi \in L$, with $\varpi^e = \pi$. Let $H_0 = \mathrm{Gal}(L/K)$ be the inertia subgroup of H, and, for $s \in H_0$, $\kappa(s) = \frac{s(\varpi)}{\varpi} \pmod{\varpi\mathcal{O}_L}$: $\kappa : H_0 \to k_L^\times$ is an injective homomorphism, where k_L is the residue field of L. Since $e = |H_0| \mid p-1$, κ is in fact an injective homomorphism $\kappa : H_0 \to \mathbb{F}_p^\times$.

By definition of $c \geq 2$, $\nu_0 : \frac{1+\varpi^{c-1}\mathcal{O}_L}{1+\varpi^c\mathcal{O}_L} \to \mathbb{F}_p(q)$ is a surjective character. But, as a $k_L[H_0]$-module, $\frac{1+\varpi^{c-1}\mathcal{O}_L}{1+\varpi^c\mathcal{O}_L}$ is isomorphic to $k_L(\kappa^{c-1})$, so $\kappa^{c-1} = q$. Since $q : H_0 \to \mathbb{F}_p^\times$ is injective, $c-1$ is coprime to e, and in particular c is odd.

Suppose that $e < p-1$. Then by [123, II.5.5], there is a group isomorphism $\varpi\mathcal{O}_L \to 1+\varpi\mathcal{O}_L$ mapping $\varpi^r\mathcal{O}_L$ to $1+\varpi^r\mathcal{O}_L$ for any $r \geq 1$. Therefore, $1+\varpi^{e+1}\mathcal{O}_L = (1+\varpi\mathcal{O}_L)^p \subset \ker \nu$, so $c \leq e+1$. If $e = p-1$, then there is a group isomorphism $\varpi^2\mathcal{O}_L \to 1+\varpi^2\mathcal{O}_L$ mapping $\varpi^r\mathcal{O}_L$ to $1+\varpi^r\mathcal{O}_L$ for any $r \geq 2$. We see as above that $(1+\varpi^{p+1}\mathcal{O}_L) \subset (1+\varpi^2\mathcal{O}_L)^p$, so $c \leq p+1$. In either case, $c \leq e+1+\frac{e}{p-1}$.

The fact that $\kappa = (\omega_p)_{|I}^{\frac{p-1}{e}}$ is a direct consequence of [141, Propositions 1, 3] (because κ is the character θ_e, while $\theta_{p-1} = (\omega_p)_{|I}$ because of the normalization of the class theory isomorphism).

All that remains to do is compute the Langlands constant $\lambda_{LE/\mathbb{Q}_p}(\theta_p)$. Write $p^* = (-1)^{\frac{p-1}{2}}p$. Since H is cyclic, it contains at most one character of order two. Moreover, $q^{-1}(\mathbb{F}_p^{\times 2})/G_L$ is an index two subgroup of H, corresponding to a certain quadratic extension M of $\mathbb{Q}_p$ contained in L. On the other hand, $q^{-1}(\mathbb{F}_p^{\times 2}) = (\det\rho)^{-1}(\mathbb{F}_p^{\times 2}) = G_{\mathbb{Q}(\sqrt{p^*})}$, so $M = \mathbb{Q}_p(\sqrt{p^*})$. Thus, H has a unique character with order two, which we denote by χ_2; it is the character of the quadratic extension $\mathbb{Q}_p(\sqrt{p^*})/\mathbb{Q}_p$, and is also $\omega_p^{(p-1)/2}$.

Let $\psi : H \to \mathbb{C}^\times$ be any character (in particular, ψ is at most tamely ramified) and η be the unique quadratic unramified character of $G_{\mathbb{Q}_p}$: then $\varepsilon(\psi\eta, \frac{1}{2}, \theta_p)$ is $\varepsilon(\psi, \frac{1}{2}, \theta_p)\eta_\psi$, where η_ψ is 1 if ψ is unramified and -1 otherwise. Since H has exactly $[L : \mathbb{Q}_p] - f_{L/\mathbb{Q}_p} = f_{L/\mathbb{Q}_p}(e-1) \notin 2\mathbb{Z}$ ramified characters, one has

$$\begin{aligned}\lambda_{LE/\mathbb{Q}_p}(\theta_p) &= \frac{\varepsilon(\mathrm{Ind}_{LE}^{\mathbb{Q}_p}\mathbf{1}, \frac{1}{2}, \theta_p)}{\varepsilon(\mathbf{1}, \frac{1}{2}, \theta_{EL})} = \prod_{\chi : H\to\mathbb{C}^\times} \varepsilon(\chi, \frac{1}{2}, \theta_p)\varepsilon(\chi\eta, \frac{1}{2}, \theta_p) \\ &= \prod_{\chi : H\to\mathbb{C}^\times} \varepsilon(\chi, \frac{1}{2}, \theta_p)\varepsilon(\chi, \frac{1}{2}, \theta_p)\eta_\chi = -\prod_{\chi : H\to\mathbb{C}^\times} \varepsilon(\chi, \frac{1}{2}, \theta_p)\varepsilon(\chi^{-1}, \frac{1}{2}, \theta_p) \\ &= -\prod_{\chi : H\to\mathbb{C}^\times} \chi(\mathfrak{a}_{\mathbb{Q}_p}^{-1}(-1)).\end{aligned}$$

Since H is cyclic with even order, the product of its characters is exactly χ_2. Then $\chi_2(\mathfrak{a}_{\mathbb{Q}_p}^{-1})$ is the Teichmüller lift of $\omega_p^{(p-1)/2}(\mathfrak{a}_{\mathbb{Q}_p}^{-1}(-1)) = (-1)^{(p-1)/2}$, thus $\lambda_{LE/\mathbb{Q}_p}(\theta_p) = (-1)^{\frac{p+1}{2}}$.

Let now $\beta', q' : G_{\mathbb{Q}_p} \to \mathbb{F}_p^\times$ be characters $\nu' : G_{\mathbb{Q}_p} \to \mathbb{F}_p(q')$ be a cocycle such that, for some $M \in \mathrm{GL}_2(\mathbb{F}_p)$, $M\rho M^{-1} = \beta'\begin{pmatrix} q' & \nu' \\ 0 & 1\end{pmatrix}$. Since the wild inertia subgroup I^+ is a pro-p-group, $\beta_{|I^+} = q_{|I^+} = 1$, and $M\rho M^{-1}$ is not tamely ramified (because ρ isn't), so $\nu' : I^+ \to \mathbb{F}_p$ is a nonzero group homomorphism. In particular, we have $M\begin{pmatrix} 1 & \nu_{|I^+} \\ 0 & 1\end{pmatrix}M^{-1} = \begin{pmatrix} 1 & \nu'_{|I^+} \\ 0 & 1\end{pmatrix}$: a direct computation shows that $M = \begin{pmatrix} u & v \\ 0 & w\end{pmatrix}$ for some $u, w \in \mathbb{F}_p^\times$ and $v \in \mathbb{F}_p$. This implies that $(\beta q, \beta) = (\beta' q', \beta')$, hence $(\beta, q) = (\beta', q')$, and another direct computation shows that $\frac{u}{w}\nu_{|G_L} = \nu'_{|G_L}$, hence $\nu'_{|G_L} \in (\det M)\mathbb{F}_p^{\times 2}\nu_{|G_L}$. □

Corollary 4.4.10 *With the same notation as in Lemma 4.4.9, let $1 \le n \le p-1$ the smallest positive integer such that $q_{|I} = (\omega_p^n)_{|I}$. Then, unless $L = \mathbb{Q}_p(\mu_p)$ and $n = 1$, the space of possible cocycles ν (up to coboundaries) is one-dimensional and $c - 1 = \frac{ne}{p-1}$. When $n = 1$ and $L = \mathbb{Q}_p(\mu_p)$, the space of possible cocycles ν is 2-dimensional and $c \in \{2, p+1\}$, and the subspace of cocycles ν for which $c = 2$ is a line. Moreover, in this situation, one has $c = 2$ if and only if $\begin{pmatrix} \omega_p & \nu \\ 0 & 1\end{pmatrix}$ is* peu ramifiée *in the sense of [145, §2.4], if and only if this representation comes from a finite flat subgroup over $\mathbb{Z}_p$.*

Proof. – By local Tate duality and the computation of the local Euler-Poincaré characteristic [124, (7.2.6),(7.3.1)],

$$\dim H^1(\mathbb{Q}_p, \mathbb{F}_p(q)) = \dim H^0(\mathbb{Q}_p, \mathbb{F}_p(q)) + \dim H^2(\mathbb{Q}_p, \mathbb{F}_p(q)) + 1 = 1 + \dim H^0(\mathbb{Q}_p, \mathbb{F}_p(\omega_p q^{-1})),$$

so $\dim H^1(\mathbb{Q}_p, \mathbb{F}_p(q))$ is equal to one if $q \neq \omega_p$ and two otherwise.

By Lemma 4.4.9, $n \equiv (c-1)\frac{p-1}{e} \pmod{p-1}$, and $c - 1 \le e + \frac{e}{p-1}$. If $e < p-1$, then $c - 1 \le e$, so $n, (c-1)\frac{p-1}{e}$ are congruent modulo $p-1$ and in the interval $[1, p-1]$, so they are equal. If $e = p-1$, then $c \le p+1$ and $n \equiv c - 1 \pmod{p-1}$. So unless $c = p+1$, $1 \le n, c-1 \le p-1$

are congruent modulo $p-1$ hence equal. So the only possibility for $n \neq (c-1)\frac{p-1}{e}$ is if $e = p-1$ and $n = 1$: in this case $c \in \{2, p+1\}$.

When $e = p-1$ and $n = 1$, assume that $L \neq \mathbb{Q}_p(\mu_p)$. Then consider the following diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & 1+\varpi^2\mathcal{O}_L & \xrightarrow{\subset} & 1+\varpi\mathcal{O}_L & \longrightarrow & \mathbb{F}_p & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \alpha:x\mapsto x^p} & & \downarrow{\scriptstyle \beta:x\mapsto x^p} & & & & \\ 1 & \longrightarrow & 1+\varpi^{p+1}\mathcal{O}_L & \xrightarrow{\subset} & 1+\varpi^p\mathcal{O}_L & \longrightarrow & \mathbb{F}_p & \longrightarrow & 1 \end{array}$$

By the snake lemma, since β is injective (as $\mu_p \not\subset L$) and α is an isomorphism, γ is injective, hence an isomorphism. Thus β is onto, and every element in $1+\varpi^p\mathcal{O}_L$ is a p-th power. Therefore $c \leq p$ and therefore $c = 2$. When $L = \mathbb{Q}_p(\mu_p)$ and $n = 1$, one has $q = \omega_p$. The rest of the assertions is contained in [145, §2.4, 2.8]. □

Lemma 4.4.11 *Let $\rho : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\mathbb{F}_p)$ be a continuous representation with $\det\rho = \omega_p^{-1}$. Assume that ρ is a-Cartan: let C be a Cartan subgroup with normalizer N such that $\rho(G_{\mathbb{Q}_p}) \subset N$ and $\rho^{-1}(C)$ is the subgroup of $G_{\mathbb{Q}_p}$ corresponding to the unramified quadratic extension $E/\mathbb{Q}_p$. There is a unique character $\sigma : E^\times/(1+p\mathcal{O}_E) \to C$ such that $\rho_{|G_E} = \sigma \circ \mathfrak{a}_E$. One has $\sigma(p) = -I_2$ and $\sigma(x) = x^{-1}I_2$ for each $x \in \mathbb{F}_p^\times$. Hence $\rho(G_E)$ is the image by ρ of the inertia subgroup. Let $i, j : (\mathcal{O}_E/p)^\times \to C$ be the two natural isomorphisms that respect the trace and the norm, and, for $k \in \{i, j\}$, let b_k be the index in C of the subgroup $\{s \in (\mathcal{O}_E/p)^\times \mid \sigma(s) = k(s)^{-1}\}$. Then each b_k is divisible by a, each $\frac{p^2-1}{b_k}$ is prime to a, and the least common multiple of b_i, b_j is $p+1$.*

Proof. – The existence of σ is a consequence of local class field theory, and it is clear that a is the index of $\sigma(\mathcal{O}_E^\times)$ in C. For any $x = \mathfrak{a}_E(s) \in \mathcal{O}_E^\times$,

$$\sigma(N_{E/\mathbb{Q}_p}x) = \sigma(x^{p+1}) = \rho(s)^{p+1} = \omega_p^{-1}(s)I_2 = ((N_{E/\mathbb{Q}_p}\mathfrak{a}_E)(s))^{-1}I_2 = (N_{E/\mathbb{Q}_p}x)^{-1}I_2,$$

so, for any $y \in \mathbb{F}_p^\times$, $\sigma(y) = y^{-1}I_2$. Let $F \in G_{\mathbb{Q}_p}$ be an arithmetic Frobenius mapped under $\mathfrak{a}_{\mathbb{Q}_p}$ to p^{-1}: then $\rho(F) \in N\backslash C$, so $\rho(F)^2 = -\det\rho(F_p)I_2 = -\omega_p^{-1}(F_p)I_2 = -I_2$. Since F^2 is the image of F under the transfer map $G_{\mathbb{Q}_p}^{ab} \to G_E^{ab}$, one has $\mathfrak{a}_E(F^2) = \mathfrak{a}_{\mathbb{Q}_p}(F) = p^{-1}$, thus $\sigma(p) = -1$.

Let $I \triangleleft G_{\mathbb{Q}_p}$ be the inertia subgroup. Since $\rho(I)$ has even cardinality, it contains the unique element of C with order 2, which is $-I_2$. Since G_E is generated by I and F^2, $\rho(G_E) = \rho(I)$, so that $\rho(I)$ is a subgroup of $\rho(G_{\mathbb{Q}_p})$ of index two.

For $k \in \{i, j\}$, let $U_k = \{s \in (\mathcal{O}_E/p)^\times \mid \sigma(s) = k(s)^{-1}\}$: it is a subgroup of $(\mathcal{O}_E/p)^\times$ and let b_k denote its index in C. We saw that $\mathbb{F}_p^\times \subset U_k$, hence $b_k \mid p+1$. Moreover, since $j = i^p$, $U_i \cap U_j \subset \{s \in (\mathcal{O}_E/p)^\times \mid s^{p-1} = 1\} = (p+1)C$, so $p+1$ is the greatest common multiple of b_i and b_j. Moreover,

$$ab_kC = b_k\sigma(\mathcal{O}_E^\times) = \sigma(U_k) = k(U_k)^{-1} = b_kC,$$

so that the greatest common divisor of ab_k and p^2-1 is b_k, hence a and $\frac{p^2-1}{b_k}$ are coprime. Since a divides $b_k\frac{p^2-1}{b_k}$, a divides each b_k. □

Definition 4.4.12 The pair $\{b_i, b_j\}$ of integers attached to ρ as in Lemma 4.4.11 is called the *set of reciprocity indices* for ρ. This pair only depends on ρ up to conjugacy.

Proposition 4.4.13 *Let $\rho : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\mathbb{F}_p)$ be an a-Cartan representation. Let $E/\mathbb{Q}_p$ be the quadratic unramified extension, C a nonsplit Cartan subgroup such that $\rho^{-1}(C) = G_E$. Let $\psi : C \to \mathbb{C}^\times$ be a character and $\psi(\rho) = \mathrm{Ind}_{G_E}^{G_{\mathbb{Q}_p}}[\psi \circ \rho]$.*

(i) Assume that $\psi_{|\mathbb{F}_p^\times} = 1$ and let $(f, \mathbf{1}) \in \mathscr{S}$. Then $\psi(\rho)$ is self-dual and

$$\varepsilon(D_{f,p} \otimes \mathrm{D}_p(\psi(\rho)^*), 1, \theta_p) = r\varepsilon(\psi(\rho), \frac{1}{2}, \theta_p)^2,$$

where $r \in \{\pm 1\}$ is equal to -1 if and only if $\psi^a = 1$, that is, if and only if $\psi(\rho)$ is unramified.

(ii) Let $(f, \chi) \in \mathscr{P}$ and assume that for all $a \in \mathbb{F}_p^\times$, $\psi(aI_2) = \chi(a)$. Then

$$\varepsilon(D_{f,p} \otimes \mathrm{D}_p(\psi(\rho)^*), 1, \theta_p) = \varepsilon(\psi(\rho), \frac{1}{2}, \theta_p)\varepsilon(\psi(\rho)^*, \frac{1}{2}, \theta_p)$$

(iii) Let $(f, \mathbf{1}) \in \mathscr{C}$ and assume that $\psi_{|\mathbb{F}_p^\times} = 1$. Let $\phi : (\mathcal{O}_E/p)^\times \to \mathbb{C}^\times$ be any of the two characters attached to C_f. Then

$$\varepsilon(D_{f,p} \otimes \mathrm{D}_p(\psi(\rho)^*), 1, \theta_p) =: r \in \{\pm 1\},$$

and $r = -1$ if and only if $\overline{\psi} \circ \rho_{|I_p} \in \{\phi \circ \mathfrak{a}_E, \phi^p \circ \mathfrak{a}_E\}$.

Proof. – Write $I_p \triangleleft G_{\mathbb{Q}_p}$ for the inertia subgroup, and $F \in G_{\mathbb{Q}_p}$ be an arithmetic Frobenius such that $\mathfrak{a}_{\mathbb{Q}_p}(F_p) = p^{-1}$. Let N be the normalizer of C, so that $\rho(F_p) = -I_2$ by Lemma 4.4.11. Note that $\psi(\rho)^* \simeq \overline{\psi}(\rho)$, and that $\psi^p(\rho) \simeq \psi(\rho)$, since the action of N/C on C by conjugation is given by taking p-th powers.

(i): Since $\psi(\mathbb{F}_p^\times) = 1$, $\psi^{p+1} = 1$, so $\psi(\rho)^* \simeq \overline{\psi}(\rho) \simeq \psi^p(\rho) \simeq \psi(\rho)$. By Proposition 4.4.6 (iii), we need to check that $\delta = \det(-a_p(f)F \mid \psi(\rho)^I)$ is 1 if $\psi(\rho)$ is ramified and -1 otherwise. Now, $\psi(\rho)_{|I_p} \simeq (\psi \oplus \psi^p) \circ \rho_{|I_p}$, so it has determinant one. Therefore, either $\psi(\rho)^{I_p}$ is zero, or it is $\psi(\rho)$. Since $F \notin G_E$, $\mathrm{Tr}(F \mid \psi(\rho)) = 0$, so $\delta = \det(F \mid \psi(\rho)^I)$ is -1 if $\psi(\rho)$ is unramified and 1 otherwise.

(ii): One has

$$\psi(\rho) \otimes \chi \simeq \psi^p(\rho) \otimes \overline{\chi}(\det \rho) \simeq (\psi^p \overline{\chi}(\det))(\rho) \simeq (\psi^p \overline{\psi}^{p+1})(\rho) \simeq \overline{\psi}(\rho),$$

and $D_{f,p}$ is the sum of two characters α, β by Lemma 4.4.4, so we can apply Proposition 4.4.6 (ii), which yields the result since $\alpha(-1)^2 = 1$.

(iii): Let ϕ_0 be the unique extension of ϕ to $E^\times$ such that $\phi_0(p) = -p$. The representation $\rho_{|G_E}$ can be uniquely written as $\sigma \circ \mathfrak{a}_E$ for some character $\sigma : E^\times/(1 + p\mathcal{O}_E) \to C$. By Lemma 4.4.11, $\sigma_{|\mathbb{F}_p^\times}$ is the inverse of the identity and $\sigma(p) = -I_2$. We saw that $\lambda_{E/\mathbb{Q}_p}(\theta_p) = 1$, so that, by Lemma 4.4.4, one has

$$\begin{aligned}\varepsilon(D_{f,p} \otimes \mathrm{D}_p(\psi(\rho)^*), 1, \theta_p) &= \varepsilon((\overline{\phi_0} \otimes (\overline{\psi}(\sigma) \oplus \overline{\psi}^p(\sigma)) \circ \mathfrak{a}_E), 1, \theta_E) \\ &= \prod_{\zeta \in \{\psi(\sigma), \psi^p(\sigma)\}} \varepsilon(\overline{\phi_0\zeta}, 1, \theta_E) = \prod_{\zeta \in \{\psi(\sigma), \psi^p(\sigma)\}} \varepsilon(\overline{\phi_0\zeta}\|\cdot\|^{1/2}, \frac{1}{2}, \theta_E).\end{aligned}$$

If $(\zeta\phi_0)_{|\mathcal{O}_E^\times}$ is nontrivial, then $(\zeta\phi_0)_{|\mathcal{O}_E^\times}$ is a nontrivial character of $\mathcal{O}_E^\times/\mathbb{Z}_p^\times(1 + p\mathcal{O}_E)$, so

$$\varepsilon(\overline{\phi_0\zeta}\|\cdot\|^{1/2}, \frac{1}{2}, \theta_E) = \phi_0(p)\|p\|_E^{1/2}\zeta(p)\frac{\sum_{u \in (\mathcal{O}_E/p)^\times}(\phi_0\zeta)(u)\theta_E\left(\frac{u}{p}\right)}{\left|\sum_{u \in (\mathcal{O}_E/p)^\times}(\phi_0\zeta)(u)\theta_E\left(\frac{u}{p}\right)\right|} = -\zeta(p)(\phi_0\zeta)(\sqrt{a}),$$

for any $a \in \mathbb{F}_p^\times \backslash \mathbb{F}_p^{\times 2}$ by Lemma C.1.5. Since $(\phi_0)_{|\mathbb{F}_p^\times} = \psi_{|\mathbb{F}_p^\times} = 1$, when $\psi \circ \rho_{|I_p} \notin \{\overline{\phi} \circ \mathfrak{a}_E, \overline{\phi}^p \circ \mathfrak{a}_E\}$ one has $\varepsilon(D_{f,p} \otimes \mathrm{D}_p(\psi(\rho)^*), 1, \theta_p) = 1$.

If $(\psi(\sigma)\phi_0)_{|\mathcal{O}_E^\times}$ is trivial, then $\varepsilon(\overline{\phi_0\psi(\sigma)}\|\cdot\|^{1/2}, \frac{1}{2}, \theta_E) = 1$. Moreover, $\psi^p(\sigma)\phi_0 = \psi_0^{-(p-1)}$ is

not trivial on $\mathcal{O}_E^\times$, otherwise it would factor through the norm. Then

$$\begin{aligned}\varepsilon(D_{f,p}\otimes \mathrm{D}_p\left(\psi(\rho)^*\right),1,\theta_p) &= -\psi^p(\sigma(p))(\phi_0\psi^p(\sigma))(\sqrt{a}) = -\psi(-1)\psi^{p-1}(\sigma(\sqrt{a}))\\ &= -\psi^{(p-1)/2}(\sigma(a)) = -1.\end{aligned}$$

□

4.5 Root numbers for the factors of $T_\ell J_\rho$

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ be a continuous representation with determinant ω_p^{-1}. We are interested in the L-functions for the factors of $J_\rho(p)$.

Definition 4.5.1 An *irreducible* Artin representation $\sigma : G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ is *automorphic* if there exists a unitary cuspidal smooth automorphic representation $\pi \simeq \bigotimes'_v \pi_v$ of $\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})$ such that, at every place v of $\mathbb{Q}$, the local Langlands correspondence (say, as in [24] for finite places) attaches π_v to $\sigma^*_{W_{\mathbb{Q}_v}}$.

We say that an Artin representation $\sigma : G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$ is *automorphic* if all its irreducible components are automorphic.

For example, in this sense, every odd two-dimensional representation is automorphic by Serre's conjecture [87, 88] and Proposition 4.3.11.

To make some notation easier, let us use the following definitions.

Definition 4.5.2 Let E, F be number fields. A compatible system of Galois representations of G_E over F is the datum, for each maximal ideal $\lambda \subset \mathcal{O}_F$, of a continuous semi-simple finite-dimensional representation V_λ of G_E over F_λ such that the family $(F_\lambda)_\lambda$ satisfies the following conditions:

- There exists a finite set S of finite places of E such that, for any maximal ideal λ of $\mathcal{O}_F$ with residue characteristic ℓ, V_λ is unramified at every place of E outside S and not dividing ℓ.
- For every finite place v of E, there exists a Deligne representation $\mathrm{D}_v(V)$ of W_{E_v} over F such that for any maximal ideal λ of $\mathcal{O}_F$ with residue characteristic prime to v, one has $V_v \otimes_F F_\lambda \simeq \mathrm{D}_v(V_\lambda)$.

Remark There are many possible notions of compatible systems in the literature, such as the ones given in [59, 2.30–2.32]. Our notion is closer to what *loc.cit.* calls a strongly compatible system, but we do not require any p-adic Hodge-theoretic condition. Similarly, while it would be convenient to treat infinite places on the same footing as finite places, for instance by using motives as sketched in [160, §4], we can do so by hand.

With this definition, compatible systems contain Artin representations, the cyclotomic character $(\mathbb{Q}_p(1))_p$, and the $V_f := (V_{f,\lambda})_\lambda$ attached to modular forms. They are stable under the usual operations of sum, tensor product, taking duals, restriction, induction, conjugation under automorphisms of E, and extensions of scalars.

In particular, the $R_f(\rho) := (R_{f,\mathfrak{l}}(\rho))_\mathfrak{l}$ as in Definition 3.6.10 form a compatible system over F. In fact, when $(f,\chi) \in \mathscr{S} \cup \mathscr{P}'$ (resp. $(f,\chi) \in \mathscr{C}'_1$), $R_f(\rho)$ is defined with coefficients over the subfield of $\mathbb{C}$ generated by the coefficients of f (resp. by the coefficients of f and $\mathbb{Q}(i,\phi_f)^+$ by Proposition B.2.11)[4].

By Proposition 3.5.5, if $(\psi_{f,\lambda})_\lambda$ denotes one of the compatible systems over $G_{\mathbb{Q}(\sqrt{-p})}$ attached to some $(f,\mathbf{1}) \in \mathscr{C}_M$, $\left(\mathrm{Ind}^{\mathbb{Q}}_{\mathbb{Q}(\sqrt{-p})}\left[\psi_{f,\lambda}\otimes C^\epsilon(\rho_{|G_{\mathbb{Q}(\sqrt{-p})}})\right]\right)_\lambda$ also forms a compatible system.

Definition 4.5.4 Let $V := (V_\lambda)_\lambda$ be a compatible system of representations of G_E over a number field F. Suppose given an embedding $F \to \mathbb{C}$. Then V has a global L-function (at least

[4]This is because $\pi(1,\chi)$ (resp. St) can be realized over $\mathbb{Q}(\chi)$ (resp. $\mathbb{Q}$).

as a formal Dirichlet series), a global conductor ideal $\mathfrak{f}_V \subset \mathcal{O}_E$ and an absolute conductor N_V defined as

$$L(V,s) := \prod_v L(\mathrm{D}_v(V^*), s), \quad \mathfrak{f}_V = \prod_v \mathfrak{p}_v^{f(\mathrm{D}_v(V^*))}, \quad N_V = N_{E/\mathbb{Q}}\mathfrak{f}_V.$$

where the product runs over finite places of E, and, at a finite place v with associated maximal ideal $\mathfrak{p}_v$, the L-factor or conductor exponent can be computed, by Lemma 4.3.6, either on the Deligne representation or on any V_λ with λ coprime to the residue characteristic of v.

Proposition 4.5.5 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ a normalized newform and $Y : G_\mathbb{Q} \to \mathrm{GL}_d(\mathbb{C})$ be an automorphic Artin representation. The function*

$$\Lambda(V_f \otimes Y, s) = M^{s/2} 2^d (2\pi)^{-ds} \Gamma(s)^d L(V_f \otimes Y, s),$$

where M and $L(V_f \otimes Y, s)$ are the conductor and the L-function, respectively, of the compatible system $(V_{f,\lambda} \otimes Y)_\lambda$ (where λ runs through maximal ideals of the ring of integers of a number field containing the coefficients of f and on which Y is realizable) extends meromorphically to $\mathbb{C}$ and satisfies the following functional equation:

$$\Lambda(V_f \otimes Y, s) = \prod_v \varepsilon(D_{f,v} \otimes \mathrm{D}_v(Y^*), \frac{k}{2}, \theta_v) \cdot \Lambda(Y^* \otimes V_{\overline{f}}, k-s).$$

When $k > 1$, or $k = 1$ and Y has no irreducible component isomorphic to V_f^*, then $\Lambda(V_f \otimes Y, s)$ extends to an entire function. We call $\prod_v \varepsilon(D_{f,v} \otimes \mathrm{D}_v(Y^*), \frac{k}{2}, \theta_v)$ the Galois-theoretic root number *of the compatible system $V_f \otimes Y$.*

Proof. – We can assume that Y is irreducible and attached to a cuspidal unitary smooth automorphic representation π_Y. Since $(\mathrm{D}_\infty(Y^*))_{|W_\mathbb{C}}$ is a sum of copies of the trivial representation, while $D_{f,\infty}$ is induced from $W_\mathbb{C}$, it follows that $\Lambda(V_f \otimes Y, s) = L\left(\pi_f \times \pi_Y, s - \frac{k-1}{2}\right)$. To reach the conclusion, we can simply apply the theory of the Rankin-Selberg convolution [62, Theorem 11.7.1], while noting that by [24] the local Langlands correspondence preserves the L-factors of products of pairs. □

While we do not know that the Artin representations appearing in $\mathcal{T}_\ell J_\rho(p)$ are automorphic, we do know that the expected functional equation is, by Lemma 4.4.1, of the form $\Lambda(s) = \epsilon\Lambda(2-s)$, so that ϵ (the *global root number*) is a sign which can be (in most cases) computed.

There is one situation where we can be more specific, as is already pointed out in [163, §3.1]: it is that of the CM forms.

Proposition 4.5.6 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a newform with complex multiplication by an imaginary quadratic field K such that $k \geq 2$. Let $F \supset K$ be a number field such that there exists a compatible system $\psi = (\psi_v)_v$ of characters of G_K over F such that $\mathrm{Ind}_K^\mathbb{Q}\psi = V_f$ (see Proposition 3.5.5), and $Y : G_K \to \mathrm{GL}_d(F)$ be an Artin representation. Let $\mathrm{D}_\infty(\psi^*)$ denote the character $z \in W_\mathbb{C} \longmapsto z^{1-k}$, I be the compatible system $\mathrm{Ind}_K^\mathbb{Q}(Y \otimes \psi)$ and M be its conductor. Then the function $\Lambda(I,s) := M^{s/2}2^d(2\pi)^{-ds}\Gamma(s)^d L(I,s)$ admits a meromorphic continuation to the complex plane and satisfies the following functional equation:*

$$\Lambda(I,s) = \prod_v \varepsilon(\mathrm{D}_v(\psi^*) \otimes \mathrm{D}_v(Y^*), \frac{k}{2}, \theta_{K_v}) \Lambda(I^*(k-1), k-s).$$

We call $\prod_v \varepsilon(\psi(\mathfrak{a}_{K_v}) \otimes \mathrm{D}_v(Y^*), \frac{k}{2}, \theta_{K_v})$ the global root number *of the compatible system I.*

Proof. – We fix an embedding of F in $\mathbb{C}$. By [132, (3.5), Theorem 4.5], there is a continuous

character $\psi_0 : \mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times$ such that for any prime ideal $\mathfrak{p}$ with residue characteristic coprime to N and any place v with residue characteristic coprime to p, ψ_0 maps any uniformizer at the place $\mathfrak{p}$ to $\psi_v(\mathrm{Frob}_\mathfrak{p})$ (which is an element of F), where $\mathrm{Frob}_\mathfrak{p}$ is an arithmetic Frobenius. Moreover, for $z \in \mathbb{C}^\times$, $(\psi_0)(z) = z^{1-k}$.

Let V be the complex representation of $W_\mathbb{Q}$ defined by $\psi_0(\mathfrak{a}) \otimes Y^*$. After checking L-factors at every place and computing conductor exponents (as in [123, Chapter VII: 10.4, 11.2, 11.7, 12.1]), we see that $\Lambda(I, s)$ is exactly $\Lambda(V, s)$ in the notation of Proposition 4.3.9, and that $\Lambda(I^*(k-1), s)$ is exactly $\Lambda(V^*, s-(k-1))$, so that the claim is a direct consequence of the functional equation for representations of W_K [160, (3.5.4)]. □

As announced, the goal of this section is the computation of the Galois-theoretic root numbers attached to the factors of $J_\rho(p)$.

Proposition 4.5.7 *Let F be a large enough number field in the sense of Section 4.4. Let $\mathfrak{l}$ be a maximal ideal of $\mathcal{O}_F$ with residue characteristic ℓ.*

Let, for every $(f, \mathbf{1}) \in \mathscr{C}_1'$, ϕ_f be one character of $\mathbb{F}_{p^2}^\times$ attached to f and ω_f be its order. Then, if ρ is a-Cartan, let $n_{f,\rho} \in \{0, 1\}$ be the integer equal to one if, and only if, $\frac{p+1}{\omega_f}$ is divisible by a and $\frac{2(p+1)}{\omega_f}$ is not divisible by any of the two reciprocity indices of ρ.

Moreover, for $(f, \mathbf{1}) \in \mathscr{C}_M$, let, for each prime ℓ inert in $\mathbb{Q}(\sqrt{-p})$, m_ℓ be one half of the conductor exponent of $V_4(\rho)$ (it is an integer for all ℓ and equal to zero for all but finitely many), and let $U = \prod_\ell (-1)^{m_\ell}$.

The global root numbers for the eigenspaces of $T_\ell J_\rho(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ are given in Table 4.2.

The entry in the "CM row" of the table means the following. Let $K = \mathbb{Q}(\sqrt{-p})$ and let $\psi : \mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times$ one of the two continuous characters attached to f by Proposition 3.5.5. We compute the L-function of $\mathrm{Ind}_{\mathbb{Q}(\sqrt{-p})}^\mathbb{Q} \psi(\mathfrak{a}_K) \otimes (C^\epsilon)^*(\rho_{|G_K})$ in the normalization of [160] (that is, we consider the situation of Proposition 4.5.6 with $Y = C^\epsilon(\rho_{|G_K})$).

Furthermore, when $\rho_{|G_{\mathbb{Q}_p}}$ is wild, it is $\mathrm{SL}_2(\mathbb{F}_p)$-conjugate to a representation of the form $\beta \otimes \begin{pmatrix} q & \nu \\ 0 & 1 \end{pmatrix}$, where $\beta, q : G_{\mathbb{Q}_p} \to \mathbb{F}_p^\times$ are characters and $\nu : G_{\mathbb{Q}_p} \to \mathbb{F}_p(q)$ is a cocycle whose restriction to the wild inertia subgroup is nonzero. Let $G_L = \ker q$, $d = [L : \mathbb{Q}_p]$ and $\nu_0 : G_L \to \mathbb{F}_p$ be the character given by $\nu = \nu_0(\mathfrak{a}_L)$, whose conductor exponent n is even. There is an element $\gamma \in L^\times$ with normalized valuation $1 - n$ such that, for any $x \in \mathcal{O}_L$ with valuation at least $\frac{n}{2}$, $e^{\frac{2i\pi}{p}\nu_0(1+x)} = \eta_L(\gamma x)$. Let K_p denote the completion of K at its unique place dividing p and $\gamma_0 = N_{L/K_p}\gamma \in K_p^\times$. Then $\varepsilon_\mathfrak{p}(\psi, \nu) = i\psi(\gamma_0)\|\gamma_0\|^{1/2} \in \{\pm 1\}$.

	Type of $\rho_{\|G_{\mathbb{Q}_p}}$		
	Split	Wild	a-Cartan
$R_{f,\mathfrak{l}}(\rho), (f, \mathbf{1}) \in \mathscr{S}$	$(-1)^{(p+1)/2}$	$(-1)^{(p-1)/2} a_p(f)$	$(-1)^{(p+a)/2}$
$R_{f,\mathfrak{l}}(\rho), (f, \chi) \in \mathscr{P}$	$(-1)^{(p-1)/2}$		
$R_{f,\mathfrak{l}}(\rho), (f, \mathbf{1}) \in \mathscr{C}_1'$	$(-1)^{(p+1)/2}$	$(-1)^{(p-1)/2}$	$(-1)^{(p+1)/2+n}$
CM factors	$(-1)^{(p+1)/4} U$	$(-1)^{\frac{d+2}{4}} U \epsilon \varepsilon_\mathfrak{p}(\psi, \nu)$	$(-1)^{\frac{p+2a-1}{4}} U$

Table 4.2: Global root numbers for factors of $J_\rho(p)$

Proof. – Throughout the proof, we choose a decomposition subgroup $G_{\mathbb{Q}_p}$ of $G_\mathbb{Q}$, $I_p \leq G_{\mathbb{Q}_p}$ is the inertia subgroup, $I_p^+ \leq I_p$ is the wild inertia subgroup, and $F_p \in G_{\mathbb{Q}_p}$ is an arithmetic Frobenius such that $\mathfrak{a}_{\mathbb{Q}_p}(F_p) = \frac{1}{p}$. The unique quadratic unramified extension of $\mathbb{Q}_p$ is denoted by E, and we call $c \in G_\mathbb{Q}$ the complex conjugation.

For $(f, \chi) \in \mathscr{P}$:

Write $P = \pi(1,\chi)\circ\rho$. Then

$$P^* \simeq \pi(1,\chi)^*\circ\rho \simeq \pi(1,\chi^{-1})\circ\rho \simeq \chi^{-1}(\det\rho)\otimes(\pi(\chi,1)\circ\rho) \simeq \chi\otimes P.$$

By Proposition 4.4.6 (i), $\varepsilon(D_{f,\infty}\otimes \mathrm{D}_\infty(P^*),1,\theta_\infty) = (-i)^{2(p+1)} = 1$.

For any finite place $v\nmid p$, $D_{f,v}$ is the sum of two characters (when $v\neq p$, $D_{f,v}$ is unramified, and when $v=p$ it is Lemma 4.4.3), so by Proposition 4.4.6 (ii), one has

$$\varepsilon(D_{f,v}\otimes \mathrm{D}_v(P^*),1,\theta_v) = \varepsilon(\mathrm{D}_v(P\oplus P^*),1,\theta_v).$$

Therefore,

$$\begin{aligned}\prod_v \varepsilon(D_{f,v}\otimes \mathrm{D}_v(P^*),1,\theta_v) &= \prod_{q<\infty}\varepsilon(\mathrm{D}_v(P\oplus P^*),\frac{1}{2},\theta_v) = \varepsilon(\mathrm{D}_\infty(P\oplus P^*),\frac{1}{2},\theta_\infty)^{-1}\\ &= \det(c\mid P)^{-1}\end{aligned}$$

Since $\rho(c)\sim\Delta_{1,-1}$, $P(c)^2$ is the identity and $P(c)$ has trace 2 by Proposition B.1.11, so $\det(c\mid P) = (-1)^{(p-1)/2}$.

For $(f,\chi)\in\mathscr{S}$:

Let $S = \mathrm{St}\circ\rho$. Since St is self-dual, S is self-dual too. Therefore, by Proposition 4.4.6 (ii), for any finite place $v\neq p$, $D_{f,v}$ is the sum of two unramified characters, so

$$\varepsilon(D_{f,v}\otimes \mathrm{D}_v(S^*),1,\theta_v) = \varepsilon(\mathrm{D}_v(S\oplus S^*),\frac{1}{2},\theta_v).$$

By Proposition 4.4.6, it follows that

$$\begin{aligned}\prod_v \varepsilon(D_{f,v}\otimes \mathrm{D}_v(S^*),1,\theta_v) &= (-i)^{2p}\varepsilon_p(D_{f,p}\otimes \mathrm{D}_p(S\oplus S^*),1,\theta_p)\prod_{v\neq p,\infty}\varepsilon(\mathrm{D}_v(S\oplus S^*),\frac{1}{2},\theta_v)\\ &= -\det(-a_p(f)F_p\mid S^{I_p})\prod_{v\neq\infty}\varepsilon(\mathrm{D}_v(S\oplus S^*),\frac{1}{2},\theta_v)\\ &= -\det(-a_p(f)F_p\mid S^{I_p})\varepsilon(\mathrm{D}_\infty(S\oplus S^*),\frac{1}{2},\theta_v)^{-1}\\ &= -\det(c\mid S)\det(-a_p(f)F_p\mid S^{I_p}).\end{aligned}$$

By Proposition B.1.11, $S(c)$ has trace 1 and order 2, so $\det(c\mid S) = (-1)^{(p-1)/2}$. Therefore,

$$\prod_v \varepsilon(D_{f,v}\otimes \mathrm{D}_v(S^*),1,\theta_v) = (-1)^{(p+1)/2}\det(-a_p(f)F_p\mid S^{I_p}).$$

When $\rho_{|G_{\mathbb{Q}_p}}$ is wild:

After conjugating ρ (which does not cause any issue), we may assume that ρ maps the wild inertia subgroup I_p^+ to $U^{\mathbb{Z}} = \begin{pmatrix}1 & *\\ 0 & 1\end{pmatrix}$. Then $\rho(G_{\mathbb{Q}_p})$ is contained in the normalizer of $U^{\mathbb{Z}}$, which is the group B of upper-triangular matrices. Lemma B.3.1 therefore implies that $S^{I_p} = S^{G_{\mathbb{Q}_p}}$ is a line, so that $\det(-a_p(f)F_p\mid S^{I_p}) = -a_p(f)$, whence the conclusion.

When $\rho_{|G_{\mathbb{Q}_p}}$ is split:

After conjugating ρ, we may assume that for $s\in G_{\mathbb{Q}_p}$, $\rho(s) = \begin{pmatrix}\alpha(s) & 0\\ 0 & \beta(s)\end{pmatrix}$ for some

characters $\alpha, \beta : G_{\mathbb{Q}_p} \to \mathbb{F}_p^\times$. By Lemma B.3.3, $S_{|G_{\mathbb{Q}_p}} \simeq \mathbf{1} \oplus \bigoplus_{\chi \in \mathcal{D}} \chi\left(\frac{\alpha}{\beta}\right)$.

Let a be the cardinality of $\rho(I_p) \pmod{\mathbb{F}_p^\times I_2}$. Then $S^{I_p}_{|G_{\mathbb{Q}_p}} \simeq \mathbf{1} \oplus \bigoplus_{\chi \in \mathcal{D}, \chi^{(p-1)/a}=1} \chi\left(\frac{\alpha}{\beta}\right)$, so that

$$\det(-a_p(f)F_p \mid S^{I_p}) = (-a_p(f))^{1+\frac{p-1}{a}} \prod_{\chi \in \mathcal{D}, \chi^{\frac{p-1}{a}}=1} \chi\left(\frac{\alpha}{\beta}(F_p)\right).$$

To prove that this quantity is one, it is enough to show that $\frac{p-1}{a}$ is odd (because $a_p(f)^2 = 1$ and the factors with χ and χ^{-1} in the product cancel out). Now, $\frac{p-1}{a}$ is the cardinality of the group $\rho(I_p) \cap \mathbb{F}_p^\times I_2$. Since $\det : \rho(I_p) \to \mathbb{F}_p^\times$ is an isomorphism by Proposition 4.4.7, $-I_2 \notin \rho(I_p)$, so $\rho(I_p) \cap \mathbb{F}_p^\times I_2$ does not have an element of order 2: thus $\rho(I_p) \cap \mathbb{F}_p^\times I_2$ has odd order, and we are done.

When $\rho_{|G_{\mathbb{Q}_p}}$ is a-Cartan:

Let C be a nonsplit Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ with normalizer N such that $\rho(G_{\mathbb{Q}_p}) \subset N$ and $\rho^{-1}(C) = G_E$. Our assumption states that $\rho(aI_p) = \rho(G_E) = aC$ by Lemma 4.4.11. By Proposition B.3.4, since $\det \rho(I_p) = \mathbb{F}_p^\times$, it follows that

$$S^{I_p}_{|G_{\mathbb{Q}_p}} \simeq \bigoplus_{\psi^a=1}{}' \mathrm{Ind}_E^{\mathbb{Q}_p} \psi \circ \rho_{|G_E} \simeq \mathbf{1}^{\oplus \frac{a-1}{2}} \oplus \epsilon^{\oplus \frac{a-1}{2}},$$

where the first direct sum is over characters $\psi : C/\mathbb{F}_p^\times \to \mathbb{C}^\times$ such that $\psi^2 \neq 1$, $\psi^a = 1$, and we only count one character among ψ and ψ^{-1}, so that there are $\frac{a-1}{2}$ terms in the sum, and ϵ is the character $\mathrm{Gal}(E/\mathbb{Q}_p) \xrightarrow{\sim} \{\pm 1\}$.

Thus $\det(-a_p(f)F_p \mid S^{I_p}) = (-a_p(f))^{a-1}(-1)^{\frac{a-1}{2}} = (-1)^{\frac{a-1}{2}}$ and we are done.

For $(f, \mathbf{1}) \in \mathscr{C}_1'$:

Let $W = C_f(\rho)$, so that, as in the proof of Lemma 4.4.1, $W^* = W$. Let $\phi : E^\times/(1+p\mathcal{O}_E) \to \mathbb{C}^\times$ be attached to f as in Lemma 4.4.4, and ω the order of $\phi_{|\mathcal{O}_E^\times} : (\mathcal{O}_E/p)^\times/\mathbb{F}_p^\times \to \mathbb{C}^\times$.

First, we compute that $\varepsilon(D_{f,\infty} \otimes \mathrm{D}_\infty(W^*), 1, \theta_\infty) = (-i)^{2(p-1)} = 1$ by Proposition 4.4.6 (i). For any finite place $v \neq p$, $D_{f,p}$ is the direct sum of two unramified characters so, by Proposition 4.4.6 (ii), $\varepsilon(D_{f,v} \otimes \mathrm{D}_v(W^*), 1, \theta_v) = \varepsilon(\mathrm{D}_v(W \oplus W^*), \frac{1}{2}, \theta_v)$. Therefore, using Lemma B.2.10 as above,

$$\begin{aligned}
\prod_v \varepsilon(D_{f,v} \otimes \mathrm{D}_v(W^*), 1, \theta_v) &= \frac{\varepsilon(D_{f,p} \otimes \mathrm{D}_p(W^*), 1, \theta_p)}{\varepsilon(\mathrm{D}_p(W \oplus W^*), \frac{1}{2}, \theta_p)} \varepsilon(\mathrm{D}_\infty(W \oplus W^*), \frac{1}{2}, \theta_\infty)^{-1} \\
&= \frac{\varepsilon(D_{f,p} \otimes \mathrm{D}_p(W^*), 1, \theta_p)}{\det(c \mid W) \det W(\mathfrak{a}_{\mathbb{Q}_p}^{-1}(-1))} \\
&= \varepsilon(D_{f,p} \otimes \mathrm{D}_p(W^*), 1, \theta_p) \left(\frac{\det \rho(c)}{p}\right) \left(\frac{\det \rho(\mathfrak{a}_{\mathbb{Q}_p}^{-1}(-1))}{W}\right) \\
&= \varepsilon(D_{f,p} \otimes \mathrm{D}_p(W^*), 1, \theta_p)(-1)^2 = \varepsilon(D_{f,p} \otimes \mathrm{D}_p(W^*), 1, \theta_p).
\end{aligned}$$

$\rho_{|G_{\mathbb{Q}_p}}$ is split:

After conjugating, we may assume that $\rho(s) = \begin{pmatrix} \alpha(s) & 0 \\ 0 & (\omega_p^{-1}\alpha^{-1})(s) \end{pmatrix}$ for some character $\alpha : G_{\mathbb{Q}_p} \to \mathbb{F}_p^\times$. Write $\alpha = \alpha_0 \omega_p^t$, for some $t \in \mathbb{Z}/(p-1)\mathbb{Z}$ and some unramified character $\alpha_0 : G_{\mathbb{Q}_p} \to \mathbb{F}_p^\times$. By Proposition B.3.6, one has

$$D_{f,p} \otimes \mathrm{D}_p\left(W^*\right) \simeq \bigoplus_{\psi \in \mathcal{D}} \overline{\psi}(\alpha_0^2) \otimes \mathrm{D}_p\left(\left(V_{f,\lambda} \otimes \psi(\omega_p^{2t-1})\right)^*\right) \simeq \bigoplus_{\psi \in \mathcal{D}} \overline{\psi}(\alpha_0^2) \otimes D_{f \otimes \psi^{2t-1}, p},$$

hence, since $\prod_{\psi \in \mathcal{D}} \psi^2 = \mathbf{1}$,

$$\begin{aligned}\varepsilon(D_{f,p} \otimes \mathrm{D}_{W^*}(,)\,1, \theta_p) &= \prod_{\psi \in \mathcal{D}} \varepsilon(\overline{\psi}(\alpha_0^2) \otimes D_{f \otimes \psi^{2t-1}, p}, 1, \theta_p) = \prod_{\psi \in \mathcal{D}} \overline{\psi}(\alpha_0^2(F_p^{-2}))\varepsilon(D_{f \otimes \psi^{2t-1}, p}, 1, \theta_p) \\ &= \prod_{\psi \in \mathcal{D}} \psi(\alpha_0(F_p))^4 \varepsilon_p(f \otimes \psi^{2t-1}) = \prod_{\psi \in \mathcal{D}} \lambda_p(f \otimes \psi^{2t-1}).\end{aligned}$$

For any $\psi \in \mathcal{D}$, by Proposition C.3.1, $\lambda_p(f \otimes \psi^{2t-1})\lambda_p(f \otimes \overline{\psi}^{2t-1}) = 1$ because f has real coefficients. Therefore, if $\lambda \in \mathcal{D}$ is the nontrivial quadratic character, Corollary 2.4.16 implies that $\varepsilon(D_{f,p} \otimes \mathrm{D}_p\left(V^*\right), 1, \theta_p) = \lambda_p(f)\lambda_p(f \otimes \lambda) = (-1)^{\frac{p+1}{2}}$, and we are done.

$\rho_{|G_{\mathbb{Q}_p}}$ is a-Cartan:

Let $C \leq \mathrm{GL}_2(\mathbb{F}_p)$ be a Cartan subgroup with normalizer N such that $\rho(G_{\mathbb{Q}_p}) \subset N$ and $\rho^{-1}(C) = G_E$. Let $\lambda \in \mathcal{D}$ be the nontrivial quadratic character and $\epsilon : \mathrm{Gal}(E/\mathbb{Q}_p) \xrightarrow{\sim} \{\pm 1\}$. By Lemma 4.4.11, let $\sigma : E^\times/(1+p\mathcal{O}_E) \to C$ be the group homomorphism such that $\rho_{|G_E} = \sigma \circ \mathfrak{a}_E$, with $\sigma(p) = -I_2$ and $\sigma(x) = x^{-1}I_2$ for $x \in \mathbb{F}_p^\times$. Fix an isomorphism $\iota : C \to (\mathcal{O}_E/p)^\times$ preserving the trace and the norm, and let b_ι, b_{ι^p} be the two reciprocity indices.

By Proposition B.3.8, in the notation of Proposition 4.4.13,

$$W_{|G_{\mathbb{Q}_p}} \simeq \bigoplus_{\chi \in \{1,\lambda\}} \chi(\omega_p^{-1})\epsilon^{r_\chi} \oplus \bigoplus_{\psi}{}' \psi(\rho_{|G_{\mathbb{Q}_p}}),$$

where $r_\chi \in \{0,1\}$ depends on χ, ϕ and ψ runs through the characters $C/\mathbb{F}_p^\times \to \mathbb{C}^\times$, where $\psi \notin \{\phi, \phi^p\}$, $\psi^2 \neq \mathbf{1}$, and we count exactly one character in each pair $\{\psi, \psi^{-1}\}$.

If $\chi \in \{1, \lambda\}$,

$$\begin{aligned}\varepsilon(D_{f,p} \otimes \mathrm{D}_p\left((\chi(\omega_p^{-1}) \otimes \epsilon^{r_\chi})^*\right), 1, \theta_p) &= \varepsilon(D_{f \otimes \chi^{-1}, p} \otimes \epsilon^{r_\chi}, 1, \theta_p) = \epsilon^{r_\chi}(F_p^{-2})\varepsilon(D_{f \otimes \chi^{-1}, p}, 1, \theta_p) \\ &= \varepsilon_p(f \otimes \chi^{-1}) = \lambda_p(f \otimes \chi^{-1}) = \lambda_p(f \otimes \chi).\end{aligned}$$

By Corollary 2.4.16 and Proposition 4.4.13,

$$\varepsilon(D_{f,p} \otimes \mathrm{D}_{W^*}(,)\,1, \theta_p) = (-1)^{\frac{p+1}{2}+m},$$

where $m \in \{0,1\}$ has the same parity as the number of $\psi : C/\mathbb{F}_p^\times \to \mathbb{C}^\times$ such that $\psi \neq \phi, \phi^p$, $\psi^2 \neq 1$, and $\psi \circ \sigma \circ \mathfrak{a}_E$ coincides with either $\overline{\phi} \circ \mathfrak{a}_E$ or $\overline{\phi}^p \circ \mathfrak{a}_E$ on I_p, and we count one character in each pair $\{\phi, \psi^p\}$.

Thus, m has the same parity as the number of $\psi : C/\mathbb{F}_p^\times \to \mathbb{C}^\times$ with order at most 3 and distinct from $\phi \circ \iota, \phi^p \circ \iota$ and such that $\psi \circ \sigma$ coincides with $\overline{\phi}$ on $(\mathcal{O}_E/p)^\times$. If $\psi : C/\mathbb{F}_p^\times \to \mathbb{C}^\times$ is a character with order at most 2 such that $\psi \circ \sigma$ coincides with $\overline{\phi}$ on $(\mathcal{O}_E/p)^\times$, then $\phi^2_{|\mathcal{O}_E^\times} = 1$. Then ϕ factors through the norm $E^\times \to \mathbb{Q}_p^\times$, which is impossible.

Therefore, m has the same parity as the number of $\psi : C/\mathbb{F}_p^\times \to \mathbb{C}^\times$ distinct from $\phi \circ \iota, \phi^p \circ \iota$ and such that $\psi \circ \sigma$ coincides with $\overline{\phi}$ on $(\mathcal{O}_E/p)^\times$.

Since $\sigma(\mathcal{O}_E^\times) = aC$, there exists some $\psi : C/\mathbb{F}_p^\times \to \mathbb{C}^\times$ such that $\overline{\phi}_{|\mathcal{O}_E^\times} = \psi \circ \sigma_{|\mathcal{O}_E^\times}$ if and only if ϕ is a a-th power, or equivalently if $\omega \mid \frac{p+1}{a}$. In this case, there are exactly a characters ψ satisfying the above condition, where a is odd. Otherwise, $m = 0$.

Assume that $\psi = \phi \circ \iota$ and $\psi = \phi^p \circ \iota$ both satisfy $\psi \circ \sigma_{|\mathcal{O}_E^\times} = \overline{\phi}_{|\mathcal{O}_E^\times}$. Then $\overline{\phi}_{|\mathcal{O}_E^\times} = \overline{\phi}^p_{|\mathcal{O}_E^\times}$, so $\phi^{p-1}_{|\mathcal{O}_E^\times} = \phi^{p+1}_{|\mathcal{O}_E^\times} = 1$, so $\phi^2_{|\mathcal{O}_E^\times} = 1$, which we already saw was impossible.

For $i \in \{1, p\}$, $\psi := \phi^i \circ \iota$ satisfies $(\psi \circ \iota) \circ \sigma_{|\mathcal{O}_E^\times} = \overline{\phi}_{|\mathcal{O}_E^\times}$ if and only if ϕ vanishes on the subgroup $\{\iota^i(\sigma(x))x \mid x \in (\mathcal{O}_E/p)^\times\}$ of $(\mathcal{O}_E/p)^\times$ (with cardinality b_{ι^i}), if and only if $\omega \mid \frac{p^2-1}{b_{\iota^i}}$. Since $p \equiv -1 \pmod{\omega}$ and $b_{\iota^i} \mid p+1$, $\omega \mid \frac{p^2-1}{b_{\iota^i}}$ if and only if $\omega \mid \frac{2(p+1)}{b_{\iota^i}}$.

When $\rho_{|G_{\mathbb{Q}_p}}$ is wild:

By Lemma 4.4.9, after conjugating, we can assume that $\rho_{|G_{\mathbb{Q}_p}} = \beta \begin{pmatrix} q & \nu \\ 0 & 1 \end{pmatrix}$, for some characters $\beta, q : G_{\mathbb{Q}_p} \to \mathbb{F}_p^\times$ such that the extension $L/\mathbb{Q}_p$ cutting out $\ker q$ is tamely ramified with ramification index e such that $v_2(e) = v_2(p-1)$, and for some cocycle $\nu : G_{\mathbb{Q}_p} \to \mathbb{F}_p(q)$ is a cocycle whose restriction to I_p^+ is surjective, and such that the conductor exponent $n \geq 2$ of the wildly ramified character $\nu_{|G_L} : G_L \to \mathbb{F}_p^\times$ is such that $n-1$ is coprime to e (so n is even).

Write $\nu = \nu_0 \circ \mathfrak{a}_L$ for some character $\nu_0 : L^\times \to \mathbb{F}_p$. By the proof of Lemma 4.4.9, for any $\sigma \in \mathrm{Gal}(L/\mathbb{Q}_p)$, $\nu_0(\sigma(x)) = q(x)\nu_0(\sigma)$. A consequence is that the restriction of ν_0 to any proper subfield of L vanishes.

Let $K \subset L$ be the largest subextension which is unramified over $\mathbb{Q}_p$, and let $\pi \in K, \varpi \in L$ be uniformizers such that $\varpi^e = \pi$. Thus $e\nu_0(\varpi) = \nu_0(\pi) = 0$, so $\nu_0(\varpi) = 0$, and $\nu_0(\mathbb{Q}_p^\times) = \{0\}$.

By Proposition B.3.7, if B denotes the subgroup of upper-triangular matrices and $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, then

$$(C_f)_{|B} = \mathrm{Ind}_{\mathbb{F}_p^\times U^{\mathbb{Z}}}^B \left[a \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \longmapsto e^{2i\pi b/p} \right].$$

Since $\begin{pmatrix} a & * \\ 0 & b \end{pmatrix} \in B/\mathbb{F}_p^\times U^{\mathbb{Z}} \longmapsto ab^{-1} \in \mathbb{F}_p^\times$ is an isomorphism, by Mackey's formula [142, Proposition 22] and Lemma 4.4.4,

$$\begin{aligned}
\mathrm{D}_p(W^*) &\simeq \bigoplus_{t \in \mathbb{F}_p^\times / q(G_{\mathbb{Q}_p})} \mathrm{Ind}_L^{\mathbb{Q}_p} e^{-2i\pi t\nu_0/p} \circ \mathfrak{a}_L \\
D_{f,p} \otimes \mathrm{D}_p(W^*) &\simeq \bigoplus_{t \in \mathbb{F}_p^\times / q(G_{\mathbb{Q}_p})} \mathrm{Ind}_{LE}^{\mathbb{Q}_p} \left[(e^{-2i\pi t\nu_0/p} \circ \mathfrak{a}_L) \otimes \overline{\phi} \circ \mathfrak{a}_E \right] \\
&\simeq \bigoplus_{t \in \mathbb{F}_p^\times / q(G_{\mathbb{Q}_p})} \mathrm{Ind}_{LE}^{\mathbb{Q}_p} \left[(e^{-2i\pi t\nu_0(N_{LE/L})/p} \cdot \overline{\phi}(N_{LE/E})) \circ \mathfrak{a}_{LE} \right].
\end{aligned}$$

Since $v_2(e) = v_2(p-1)$, $[\mathbb{F}_p^\times : q(G_{\mathbb{Q}_p})]$ is odd, so

$$\begin{aligned}
\varepsilon(D_{f,p} \otimes \mathrm{D}_p(W^*), 1, \theta_p) &= \lambda_{LE/\mathbb{Q}_p}(\theta_p)^{[\mathbb{F}_p^\times : q(G_{\mathbb{Q}_p})]} \prod_{t \in \mathbb{F}_p^\times / q(G_{\mathbb{Q}_p})} \varepsilon(e^{\frac{-2i\pi t}{p}\nu_0(N_{LE/L})} \cdot \overline{\phi}(N_{LE/E}), 1, \theta_E) \\
&= (-1)^{(p+1)/2} \prod_{t \in \mathbb{F}_p^\times / q(G_{\mathbb{Q}_p})} \varepsilon(e^{\frac{-2i\pi t}{p}\nu_0(N_{LE/L})} \cdot \overline{\phi}(N_{LE/E}), 1, \eta_{LE}(p\cdot)) \\
&= (-1)^{(p+1)/2} \prod_{t \in \mathbb{F}_p^\times / q(G_{\mathbb{Q}_p})} e^{\frac{-2i\pi t}{p}\nu_0(p^2)} \overline{\phi}(p^{[L:\mathbb{Q}_p]}) \|p\|_{LE}^{1/2} \varepsilon(e^{\frac{-2i\pi t}{p}\nu_0(N_{LE/L})} \cdot \overline{\phi}(N_{LE/E}), 1, \eta_{LE}) \\
&= (-1)^{(p+1)/2} \prod_{t \in \mathbb{F}_p^\times / q(G_{\mathbb{Q}_p})} \varepsilon(e^{\frac{-2i\pi t}{p}\nu_0(N_{LE/L})} \cdot \overline{\phi}(N_{LE/E}), 1, \eta_{LE}).
\end{aligned}$$

Let us fix, from now on, some $t \in \mathbb{F}_p^\times$. There exists some $\gamma \in L^\times$ such that for every $x \in \varpi^{n/2}\mathcal{O}_L$, $e^{2i\pi\nu_0(x)/p} = \eta_L(\gamma x)$. Then γ is a well-defined element of $\varpi^{1-n}\mathcal{O}_L/\varpi^{1-n/2}\mathcal{O}_L$ and it has valuation exactly $1-n$ (since L is tamely ramified, η_L vanishes on $\varpi\mathcal{O}_L$ but not on $\mathcal{O}_L$).

For any $\sigma \in \mathrm{Gal}(L/\mathbb{Q}_p)$ and $q_0 \in \mathbb{Z}_p^\times \cap \mathbb{N}$ lifting $q(\sigma)$, for any $x \in \varpi^{n/2}\mathcal{O}_L$,

$$\begin{aligned}\eta_L(q_0\sigma(\gamma)x) = \eta_L(q_0\gamma\sigma^{-1}(x)) = e^{2i\pi\nu_0(1+q_0\sigma^{-1}(x))/p} = e^{2i\pi\nu_0((1+\sigma^{-1}(x))^{q_0})/p}\\ = e^{2i\pi q(\sigma)\nu_0(\sigma^{-1}(1+x))/p} = e^{2i\pi\nu_0(1+x)/p} = \eta_L(\gamma x),\end{aligned}$$

so $\sigma(\gamma) \equiv q(\sigma)^{-1}\gamma \pmod{\varpi^{1-n/2}\mathcal{O}_L}$.

Write $\gamma = \varpi^{1-n}\zeta$ for some $\zeta \in (\mathcal{O}_L/\varpi^{n/2})^\times$. In the computation above, if we take $\sigma \in I_{\mathbb{Q}_p}$, by Lemma 4.4.9, we see that $\zeta \in (\mathcal{O}_L/\varpi^{n/2})^\times$ is fixed by $\mathrm{Gal}(L/K)$. Since $\mathrm{Gal}(L/K)$ has order prime to p and $1+\varpi^{n/2}\mathcal{O}_L$ is a pro-p-group, $H^1(\mathrm{Gal}(L/K), 1+\varpi^{n/2}\mathcal{O}_L) = \{0\}$. Thus $H^0(\mathrm{Gal}(L/K), \mathcal{O}_L^\times) \to H^0(\mathrm{Gal}(L/K), (\mathcal{O}_L/\varpi^{n/2})^\times)$ is onto and we can take $\gamma = \varpi^{1-n}\zeta$ for $\zeta \in \mathcal{O}_K^\times$. Since $1-n$ and $e = [L:K]$ are coprime, $\mathrm{Tr}_{L/K}(\gamma) = \zeta\mathrm{Tr}_{L/K}(\varpi^{1-n}) = 0$, so $\eta_L(\gamma) = 1$. Moreover, we have $\nu_0(\gamma) = (1-n)\nu_0(\varpi) + \nu_0(\zeta) = 0$.

The extension LE/L is unramified, so that $N_{LE/L} : \frac{1+\varpi^r\mathcal{O}_{LE}}{1+\varpi^{r+1}\mathcal{O}_{LE}} \to \frac{1+\varpi^r\mathcal{O}_L}{1+\varpi^{r+1}\mathcal{O}_L}$ is onto. Hence the conductor exponent of the character $e^{-2i\pi t\nu_0(N_{LE/L})/p}$ is n. Moreover, for any $z \in 1+\varpi\mathcal{O}_{LE}$, $N_{LE/E}(z) \in (1+\varpi\mathcal{O}_{LE}) \cap \mathcal{O}_E = 1+p\mathcal{O}_E$, hence $\overline{\phi}(N_{LE/E})$ has conductor exponent two, so the conductor exponent of its product with $e^{-2i\pi t\nu_0(N_{LE/L})/p}$ is n.

Let finally $a \in \mathcal{O}_{LE}$, $a' \in \mathcal{O}_{LE}$ its unique conjugate under $\mathrm{Gal}(LE/L)$, and $x = \varpi^{n/2}a$. Then

$$\begin{aligned}\overline{\phi}(N_{LE/E}(1+x))e^{-2i\pi t\nu_0(N_{LE/L}(1+x))/p} &= e^{-\frac{2i\pi t}{p}\nu_0(1+(a+a')\varpi^{n/2}+aa'\varpi^n)} = \left(e^{\frac{2i\pi}{p}\nu_0(1+\mathrm{Tr}_{LE/L}(x))}\right)^{-t}\\ &= \eta_L(\gamma\mathrm{Tr}_{EL/L}(x))^{-t} = \eta_{LE}(-t\gamma x).\end{aligned}$$

We can then apply [21, §23.6 Proposition] (note that by their definition of level in [21, §1.8], the character has level $n-1$):

$$\begin{aligned}&\varepsilon(e^{-2i\pi t\nu_0(N_{LE/L})/p}\cdot\overline{\phi}(N_{LE/E}), 1, \eta_{LE})\\ &= p^{-\frac{2(n-1)f_{L/\mathbb{Q}_p}}{2}} e^{\frac{2i\pi t}{p}\nu_0(N_{LE/L}(-t\gamma))}\cdot\overline{\phi}^{-1}(N_{LE/E}(-t\gamma))\eta_{LE}(-t\gamma)\\ &= p^{-(n-1)f_{L/\mathbb{Q}_p}} e^{\frac{2i\pi t}{p}\nu_0(t^2\gamma^2)}\overline{\phi}^{-1}(N_{L/\mathbb{Q}_p}(-t\zeta\varpi^{1-n}))\\ &= p^{-(n-1)f_{L/\mathbb{Q}_p}}\phi(p)^{(n-1)f_{L/\mathbb{Q}_p}} = -1,\end{aligned}$$

and therefore $\varepsilon(D_{f,p}\otimes \mathrm{D}_p(W^*), 1, \theta_p) = -(-1)^{(p+1)/2} = (-1)^{(p-1)/2}$.

When $(f, \mathbf{1}) \in \mathscr{C}_M$:

Let ψ be one of the two compatible systems of Galois representations of $K := \mathbb{Q}(\sqrt{-p})$ with coefficients in (completions of) F attached to f and ϵ be a sign. Let $\psi^0 : \mathbb{A}_K^\times/K^\times \to \mathbb{C}^\times$ be the continuous adelic character of K attached to f as in [132, (3.5)], normalized so that for any two finite places v of K, λ of F, where the residue characteristic of v is coprime to $p\lambda$, ψ^0 maps a uniformizer at v to the image of the arithmetic Frobenius by ψ_λ, and ψ^0 maps a complex number $z \in \mathbb{C}^\times$ to $\sigma(z)^{1-k}$ for some embedding $\sigma : K \to \mathbb{C}$.

Since f has real coefficients, $\overline{\psi^0}$ is the other complex character attached to f, and $\overline{\psi^0} = \psi^0\circ\tau$, where τ is the automorphism of $K/\mathbb{Q}$. Thus the character $|\psi^0|^2 : \mathbb{A}_K^\times/K^\times \to \mathbb{R}^{+\times}$ maps any uniformizer at a split prime v of K to its residue characteristic and any complex number z to $\sigma(z)^{-1}\overline{\sigma(z)}^{-1}$, so that $\|\psi^2\| = \|\cdot\|_{\mathbb{A}}^{-1}$.

Let $\mathfrak{p}$ denote the only prime ideal of K above p.

Because f has conductor p^2, ψ has conductor $\mathfrak{p}$ and ψ^0 is trivial on the compact open subgroup $(1+\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}})\prod_{v\nmid p}\mathcal{O}_{K_v}^\times$. As we saw, the global root number for the compatible system

$\mathrm{Ind}_K^{\mathbb{Q}}[\psi \otimes C^\epsilon(\rho_{|G_K})]$ is $\prod_v \varepsilon(\psi^0(\mathfrak{a}_{K_v}) \otimes \mathrm{D}_v\left((C^\epsilon)^*(\rho_{|G_K})\right), 1, \theta_{K_v})$, where the product is over all places v of K.

The infinite place:

The representation $\psi^0(\mathfrak{a}_{\mathbb{C}}) \otimes \mathrm{D}_\infty\left((C^\epsilon)^*(\rho_{|G_K})\right)$ of $W_{\mathbb{C}}$ is the sum of $p-1$ copies of the character z^{-1} (for some continuous automorphism z of $\mathbb{C}$) of $W_{\mathbb{C}} \simeq \mathbb{C}^\times$, so, by [160, (3.2.5), (3.6.1)], the local constant is $(-\varepsilon(z^{-1}, 1, e^{2i\pi \mathrm{Tr}_{\mathbb{C}/\mathbb{R}}}))^{\frac{p-1}{2}} = (-i)^{\frac{p-1}{2}} = i(-i)^{\frac{p+1}{2}} = i(-1)^{\frac{p+1}{4}}$.

Split places:

Let ℓ be a prime that splits in K and let v, v' be the two places of K above ℓ. For $w \in \{w, w'\}$, let I_w be the conductor ideal of $C^\epsilon(\rho_{|G_K})$ at w. We view it, when relevant, as an ideal of $\mathcal{O}_K$ which is a power of the maximal ideal defining w. The representations $C^\epsilon(\rho_{|G_{K_w}})$ and $C^{-\epsilon}(\rho_{|G_{K_w}})$ are dual of each other by Proposition B.4.1, so they have the same conductor ideal. But $C^{-\epsilon}(\rho_{|G_K})$ is the conjugate by $\mathrm{Gal}(K/\mathbb{Q})$ of $C^\epsilon(\rho_{|G_K})$, so that $I_{v'}$ is the image under $\mathrm{Gal}(K/\mathbb{Q})$ of the conductor ideal of $C^{-\epsilon}(\rho_{|G_{K_v}})$, which is I_v: so $I_{v'} = \tau(I_v)$, so the ideals have the same norm.

Therefore, $\psi^0(I_v)\psi^0(I_{v'}) = \psi^0(I_v\tau(I_v)) = (\psi^0\overline{\psi^0})(I_v) = \mathbf{N}I_v$, and

$$\begin{aligned}
&\prod_{w\in\{v,v'\}} \varepsilon(\psi^0(\mathfrak{a}_{K_w}) \otimes \mathrm{D}_w\left((C^\epsilon)^*(\rho_{|G_K})\right), 1, \theta_{K_w}) \\
&= \prod_{w\in\{v,v'\}} \psi(I_w)(\mathbf{N}I_w)^{-1/2}\varepsilon(\mathrm{D}_w\left((C^\epsilon)^*(\rho_{|G_K})\right), \frac{1}{2}, \theta_{K_w}) \\
&= \psi(I_vI_{v'})(\mathbf{N}I_v)^{-1} \prod_{w\in\{v,v'\}} \varepsilon(\mathrm{D}_w\left((C^\epsilon)^*(\rho_{|G_K})\right), \frac{1}{2}, \theta_{K_w}) = \prod_{w\in\{v,v'\}} \varepsilon(\mathrm{D}_w\left((C^\epsilon)^*(\rho_{|G_K})\right), \frac{1}{2}, \theta_{K_w}).
\end{aligned}$$

Inert places:

Let ℓ be a prime number which is inert in K and let $\lambda = \ell\mathcal{O}_K$ be the unique prime ideal above ℓ. Let λ^{n_ℓ} be the conductor ideal of $C^\epsilon(\rho_{G_{K_\lambda}})$, which we also view as an idèle of K (supported at λ) when useful. Using the link between conductors and local constants, and the behavior of the latter with respect to induced representations, the conductor exponent of $C(\rho)$ at ℓ is then $2n_\ell$. By [132, (3.5)], since f has trivial character, $(\psi^0)_{|K_\lambda}(\ell) = -\ell$, so

$$\begin{aligned}
&\varepsilon(\psi^0(\mathfrak{a}_{K_\lambda}) \otimes \mathrm{D}_\lambda\left((C^\epsilon)^*(\rho_{|G_K})\right), 1, \theta_{K_\lambda}) = \psi^0(\lambda)(\ell^2)^{-\frac{n_\ell}{2}}\varepsilon(\mathrm{D}_\lambda\left((C^\epsilon)^*(\rho_{|G_K})\right), \frac{1}{2}, \theta_{K_\lambda}) \\
&= (\psi^0)_{|K_\lambda}(\ell)^{n_\ell}\ell^{-n_\ell}\varepsilon(\mathrm{D}_\lambda\left((C^\epsilon)^*(\rho_{|G_K})\right), \frac{1}{2}, \theta_{K_\lambda}) = (-1)^{n_\ell}\varepsilon(\mathrm{D}_\lambda\left((C^\epsilon)^*(\rho_{|G_K})\right), \frac{1}{2}, \theta_{K_\lambda}).
\end{aligned}$$

Temporary conclusion:

The root number is thus

$$i(-1)^{\frac{p+1}{4}} \frac{\varepsilon(\psi^0(\mathfrak{a}_{K_\mathfrak{p}}) \otimes \mathrm{D}_\mathfrak{p}\left((C^\epsilon)^*(\rho_{|G_K})\right), 1, \theta_{K_\mathfrak{p}})}{\varepsilon(\mathrm{D}_\mathfrak{p}\left((C^\epsilon)^*(\rho_{|G_K})\right), \frac{1}{2}, \theta_{K_\mathfrak{p}})} \prod_v \varepsilon(\mathrm{D}_v\left((C^\epsilon)^*(\rho_{|G_K})\right), \frac{1}{2}, \theta_{K_v}) \prod_{\left(\frac{\ell}{p}\right)=-1} (-1)^{n_\ell},$$

where the first product, which we denote by Π, is over the finite places v of K. Since $C^\epsilon(\rho_{|G_K})$ is an Artin representation, its restriction to $W_{\mathbb{C}}$ is trivial, and thus Π is the global root number of (the compatible system attached to) the Artin representation $C^\epsilon(\rho_{|G_K})$, hence of (the compatible system attached to) the Artin representation $\mathrm{Ind}_K^{\mathbb{Q}} C^\epsilon(\rho_{|G_K}) = V_4(\rho)$ in the notation of Section B.4. Since V_4 can be realized over $\mathbb{R}$ by Proposition B.2.11, a theorem of Frohlich and Queyrut

[57] states that $\Pi = 1$.

Hence our global root number is

$$i(-1)^{\frac{p+1}{4}} \frac{\varepsilon(\psi_{\mathfrak{p}}^0(\mathfrak{a}_{K_\mathfrak{p}}) \otimes \mathrm{D}_\mathfrak{p}\left((C^\epsilon)^*(\rho_{|G_K})\right), 1, \theta_{K_\mathfrak{p}})}{\varepsilon(\mathrm{D}_\mathfrak{p}\left((C^\epsilon)^*(\rho_{|G_K})\right), \frac{1}{2}, \theta_{K_\mathfrak{p}})} \prod_{\left(\frac{\ell}{p}\right)=-1} (-1)^{\frac{m_\ell}{2}},$$

where m_ℓ is the conductor exponent at ℓ of $V_4(\rho)$.

Before delving in the computation of the local constants at $\mathfrak{p}$, let us discuss $\psi_\mathfrak{p}^0 := \psi_{|K_\mathfrak{p}}^0$. This character is trivial over $1 + \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$ and is not constant over $\mathcal{O}_{K_\mathfrak{p}}^\times$. Moreover, we know that for $x \in K_\mathfrak{p}^\times$, $\psi_\mathfrak{p}^0(N_{K_\mathfrak{p}/\mathbb{Q}_p}(x)) = \|x\|_{K_\mathfrak{p}}^{-1}$. Since ψ^0 is trivial over $K^\times \prod_{v \neq \mathfrak{p}} \mathcal{O}_{K_v}^\times$, we see that $\psi_\mathfrak{p}^0(x) = \sigma(x)$ for $x \in \pm\sqrt{-p}^\mathbb{Z}$.

For $x \in \mathcal{O}_{K_\mathfrak{p}}^\times$, $x \equiv \tau(x) \pmod{\mathfrak{p}}$, so $1 = \|x\|_{K_\mathfrak{p}}^{-1} = \psi_\mathfrak{p}^0(N_{K_\mathfrak{p}/\mathbb{Q}_p} x) = \psi_\mathfrak{p}^0(x^2)$, so $\psi_\mathfrak{p}^0$ is a nontrivial quadratic character $(\mathcal{O}_{K_\mathfrak{p}}/\mathfrak{p})^\times \to \mathbb{C}^\times$, and therefore, for $x \in \mathcal{O}_{K_\mathfrak{p}}^\times$, $\psi_\mathfrak{p}^0(x) = \left(\frac{x \pmod{\mathfrak{p}}}{p}\right)$.

When $\rho_{|G_{\mathbb{Q}_p}}$ is split:

After conjugating ρ by $\mathrm{SL}_2(\mathbb{F}_p)$, we may assume that there are characters $\alpha, \beta : G_{\mathbb{Q}_p} \to \mathbb{F}_p^\times$ such that $\rho(\sigma) = \begin{pmatrix} \alpha(\sigma) & 0 \\ 0 & \beta(\sigma) \end{pmatrix}$ for every $\sigma \in G_{\mathbb{Q}_p}$. Then $\alpha\beta = \omega_p^{-1}$ and $G_{K_\mathfrak{p}}$ is the kernel of $\alpha\beta : G_{\mathbb{Q}_p} \to \mathbb{F}_p^\times/\mathbb{F}_p^{\times 2}$. Write $\alpha = \alpha_0(\mathfrak{a}_{\mathbb{Q}_p})$ and $\beta = \beta_0(\mathfrak{a}_{\mathbb{Q}_p})$. By Proposition B.4.4,

$$C^\epsilon(\rho_{|G_{K_\mathfrak{p}}}) \simeq \bigoplus_{\chi : \mathbb{F}_p^{\times 2} \to \mathbb{C}^\times} \chi \circ \left(\frac{\alpha}{\beta}\right)_{|G_{K_\mathfrak{p}}}$$

$$\mathrm{D}_\mathfrak{p}\left((C^\epsilon(\rho_{|G_{K_\mathfrak{p}}}))^*\right) \simeq \bigoplus_{\chi : \mathbb{F}_p^{\times 2} \to \mathbb{C}^\times} \chi \circ \left(\frac{\alpha_0}{\beta_0}\right) \circ N_{K/\mathbb{Q}_p} \circ \mathfrak{a}_{K_\mathfrak{p}}.$$

Since $p \equiv 3 \pmod 4$, all the characters in the above sum (except the trivial character) come in pairs $\{\chi, \chi^{-1}\}$. Since

$$\varepsilon(\chi \circ \left(\frac{\alpha_0}{\beta_0}\right) \circ N_{K/\mathbb{Q}_p} \circ \mathfrak{a}_{K_\mathfrak{p}}, \frac{1}{2}, \theta_{K_\mathfrak{p}}) \varepsilon(\chi^{-1} \circ \left(\frac{\alpha_0}{\beta_0}\right) \circ N_{K/\mathbb{Q}_p} \circ \mathfrak{a}_{K_\mathfrak{p}}, \frac{1}{2}, \theta_{K_\mathfrak{p}}) = \chi \circ \frac{\alpha_0}{\beta_0} \circ N_{K/\mathbb{Q}_p}(-1) = 1,$$

and $\varepsilon(\mathbf{1}, \frac{1}{2}, \theta_{K_\mathfrak{p}}) = 1$, we get

$$\varepsilon(\mathrm{D}_\mathfrak{p}\left((C^\epsilon(\rho_{|G_{K_\mathfrak{p}}}))^*\right), \frac{1}{2}, \theta_{K_\mathfrak{p}}) = 1.$$

Let $\chi : \mathbb{F}_p^{\times 2} \to \mathbb{C}^\times$ be a nontrivial character and $\gamma = \chi\left(\frac{\alpha_0}{\beta_0}\right) : \mathbb{Q}_p^\times \to \mathbb{C}^\times$. Recall that $\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p) = \{\mathrm{id}, \tau\}$ acts on $W_{K_\mathfrak{p}}$ by conjugation, and that this action preserves the local constants. Then one has

$$\begin{aligned}
&\varepsilon(\psi_\mathfrak{p}^0(\mathfrak{a}_{K_\mathfrak{p}}) \otimes \gamma(N_{K/\mathbb{Q}_p}\mathfrak{a}_{K_\mathfrak{p}}), 1, \theta_{K_\mathfrak{p}}) \varepsilon(\psi_\mathfrak{p}^0(\mathfrak{a}_{K_\mathfrak{p}}) \otimes \gamma^{-1}(N_{K/\mathbb{Q}_p}\mathfrak{a}_{K_\mathfrak{p}}), 1, \theta_{K_\mathfrak{p}}) \\
&= \varepsilon(\psi_\mathfrak{p}^0(\mathfrak{a}_{K_\mathfrak{p}}) \otimes \gamma(N_{K/\mathbb{Q}_p}\mathfrak{a}_{K_\mathfrak{p}}), 1, \theta_{K_\mathfrak{p}}) \varepsilon(\psi_\mathfrak{p}^0(\mathfrak{a}_{K_\mathfrak{p}})\| \cdot \|^1 \otimes \gamma^{-1}(N_{K/\mathbb{Q}_p}\mathfrak{a}_{K_\mathfrak{p}}), 0, \theta_{K_\mathfrak{p}}) \\
&= \varepsilon(\psi_\mathfrak{p}^0(\mathfrak{a}_{K_\mathfrak{p}}) \otimes \gamma(N_{K/\mathbb{Q}_p}\mathfrak{a}_{K_\mathfrak{p}}), 1, \theta_{K_\mathfrak{p}}) \varepsilon((\overline{\psi}_\mathfrak{p}^0)^{-1}(\mathfrak{a}_{K_\mathfrak{p}}) \otimes \gamma^{-1}(N_{K/\mathbb{Q}_p}\mathfrak{a}_{K_\mathfrak{p}}), 0, \theta_{K_\mathfrak{p}}) \\
&= \varepsilon(\psi_\mathfrak{p}^0(\mathfrak{a}_{K_\mathfrak{p}}) \otimes \gamma(N_{K/\mathbb{Q}_p}\mathfrak{a}_{K_\mathfrak{p}}), 1, \theta_{K_\mathfrak{p}}) \varepsilon((\psi_\mathfrak{p}^0)^{-1}(\mathfrak{a}_{K_\mathfrak{p}}) \circ \tau \otimes \gamma^{-1}(N_{K/\mathbb{Q}_p}\mathfrak{a}_{K_\mathfrak{p}}) \circ \tau, 0, \theta_{K_\mathfrak{p}} \circ \tau) \\
&= \varepsilon(\psi_\mathfrak{p}^0(\mathfrak{a}_{K_\mathfrak{p}}) \otimes \gamma(N_{K/\mathbb{Q}_p}\mathfrak{a}_{K_\mathfrak{p}}), 1, \theta_{K_\mathfrak{p}}) \varepsilon((\psi_\mathfrak{p}^0)^{-1}(\mathfrak{a}_{K_\mathfrak{p}}) \otimes \gamma^{-1}(N_{K/\mathbb{Q}_p}\mathfrak{a}_{K_\mathfrak{p}}), 0, \theta) \\
&= \psi_\mathfrak{p}^0(-1)\gamma(N_{K_\mathfrak{p}/\mathbb{Q}_p}(-1)) = -1.
\end{aligned}$$

Since there are $\frac{1}{2}\left(\frac{p-1}{2}-1\right)=\frac{p-3}{4}$ pairs $\{\chi,\chi^{-1}\}$ of characters of $\mathbb{F}_p^{\times 2}$, it follows by the classical computation of the Gauss sum (Proposition C.1.3)

$$\begin{aligned}
&\varepsilon(\psi_{\mathfrak{p}}^0(\mathfrak{a}_{K_{\mathfrak{p}}})\otimes \mathrm{D}_{\mathfrak{p}}\left((C^\epsilon(\rho_{|G_{K_{\mathfrak{p}}}}))^*\right),1,\theta_{K_{\mathfrak{p}}})=(-1)^{\frac{p-3}{4}}\varepsilon(\psi_{\mathfrak{p}}^0(\mathfrak{a}_{K_{\mathfrak{p}}})\|\cdot\|^{1/2},\frac{1}{2},\theta_{K_{\mathfrak{p}}})\\
&=(-1)^{\frac{p-3}{4}}\times\sigma(p)(p^{-2})^{\frac{1}{2}}\frac{\sum_{x\in(\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p})^\times}(\psi_{\mathfrak{p}}^0)^{-1}(x)\theta_{K_{\mathfrak{p}}}\left(\frac{x}{p}\right)}{\left|\sum_{x\in(\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p})^\times}(\psi_{\mathfrak{p}}^0)^{-1}(x)\theta_{K_{\mathfrak{p}}}\left(\frac{x}{p}\right)\right|}=(-1)^{\frac{p-3}{4}}\frac{\sum_{x\in\mathbb{F}_p^\times}\left(\frac{x}{p}\right)e^{\frac{4i\pi}{p}x}}{\left|\sum_{x\in\mathbb{F}_p^\times}\left(\frac{x}{p}\right)e^{\frac{4i\pi}{p}x}\right|}\\
&=(-1)^{\frac{p-3}{4}}\left(\frac{2}{p}\right)i=-i,
\end{aligned}$$

whence the conclusion.

When $\rho_{|G_{\mathbb{Q}_p}}$ is a-Cartan:

Let $D\leq \mathrm{GL}_2(\mathbb{F}_p)$ be a nonsplit Cartan subgroup such that $\rho(I_p)=\rho(G_E)=aD$ (by Lemma 4.4.11) and let N be the normalizer of D. Let $D_2=D\cap\mathbb{F}_p^\times\,\mathrm{SL}_2(\mathbb{F}_p)$ and $N_2=N\cap\mathbb{F}_p^\times\,\mathrm{SL}_2(\mathbb{F}_p)$. Note that a is an odd divisor of $\frac{p+1}{2}$, so $a\mid\frac{p+1}{4}$.

Let $\eta:\mathrm{Gal}(K_{\mathfrak{p}}E/K_{\mathfrak{p}})\to\{\pm1\}$ be a character, trivial if and only if $p\equiv 3 \pmod 8$. Let X be a set of characters $\chi:D_2/\mathbb{F}_p^\times\to\mathbb{C}^\times$ with order at least 3 such that for any $\chi:D_2/\mathbb{F}_p^\times\to\mathbb{C}^\times$, X contains exactly one of the characters χ and $\chi^p=\chi^{-1}$. By Proposition B.4.5,

$$C^\epsilon(\rho_{|G_{K_{\mathfrak{p}}}})\simeq\eta\oplus\bigoplus_{\chi\in X}\mathrm{Ind}_{K_{\mathfrak{p}}E}^{K_{\mathfrak{p}}}\left[\chi\circ\rho_{|G_{K_{\mathfrak{p}}E}}\right].$$

Since $\theta_{K_{\mathfrak{p}}}$ is trivial on $\sqrt{-p}^{-1}\mathcal{O}_{K_{\mathfrak{p}}}$ but not on $p^{-1}\mathcal{O}_{K_{\mathfrak{p}}}$, and $\psi_{\mathfrak{p}}^0$ has conductor ideal $\mathfrak{p}$, one has

$$\begin{aligned}
\varepsilon(\overline{\eta},\frac{1}{2},\theta_{K_{\mathfrak{p}}})&=\overline{\eta}(\mathfrak{a}_{K_{\mathfrak{p}}}^{-1}(\sqrt{-p}))=(-1)^{\frac{p-3}{4}}\\
\varepsilon(\psi_{\mathfrak{p}}^0(\mathfrak{a}_{K_{\mathfrak{p}}})\otimes\overline{\eta},\frac{1}{2},\theta_{K_{\mathfrak{p}}})&=\overline{\eta}(\mathfrak{a}_{K_{\mathfrak{p}}}^{-1}(\sqrt{-p}^{1+1}))\varepsilon(\psi_{\mathfrak{p}}^0(\mathfrak{a}_{K_{\mathfrak{p}}})\|\cdot\|^{1/2},\frac{1}{2},\theta_{K_{\mathfrak{p}}})\\
&=\psi_{\mathfrak{p}}^0(p)\|p\|^{1/2}\frac{\sum_{x\in(\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p})^\times}(\psi_{\mathfrak{p}}^0)^{-1}(u)\theta_{K_{\mathfrak{p}}}\left(\frac{u}{p}\right)}{\left|\sum_{x\in(\mathcal{O}_{K_{\mathfrak{p}}}/\mathfrak{p})^\times}(\psi_{\mathfrak{p}}^0)^{-1}(u)\theta_{K_{\mathfrak{p}}}\left(\frac{u}{p}\right)\right|}=i\left(\frac{2}{p}\right)=(-1)^{\frac{p+1}{4}}i.
\end{aligned}$$

Write $\rho_{|W_E}=\sigma\circ\mathfrak{a}_E$ for some character $\sigma:E^\times/(1+p\mathcal{O}_E)\to D$ with image aD, so that one has $\sigma(p)=-I_2$ and, for each $x\in\mathbb{F}_p^\times$, $\sigma(x)=x^{-1}I_2$. Let $\chi\in X$ and define

$$\begin{aligned}
\varepsilon_\chi&:=\frac{\varepsilon(\psi_{\mathfrak{p}}^0(\mathfrak{a}_{K_{\mathfrak{p}}})\otimes\mathrm{D}_{\mathfrak{p}}\left(\mathrm{Ind}_{K_{\mathfrak{p}}E}^{K_{\mathfrak{p}}}\left[\chi\circ\rho_{|G_{K_{\mathfrak{p}}E}}\right]^*\right),1,\theta_{K_{\mathfrak{p}}})}{\varepsilon(\mathrm{D}_{\mathfrak{p}}\left(\mathrm{Ind}_{K_{\mathfrak{p}}E}^{K_{\mathfrak{p}}}\left[\chi\circ\rho_{|G_{K_{\mathfrak{p}}E}}\right]^*\right),1,\theta_{K_{\mathfrak{p}}})}\\
&=\frac{\varepsilon((\psi_{\mathfrak{p}}^0\circ N_{K_{\mathfrak{p}}E/K_{\mathfrak{p}}})(\mathfrak{a}_{K_{\mathfrak{p}}E})\otimes(\overline{\chi}\circ\rho_{|W_{K_{\mathfrak{p}}E}}),1,\theta_{K_{\mathfrak{p}}E})}{\varepsilon(\overline{\chi}\circ\rho_{|W_{K_{\mathfrak{p}}E}},\frac{1}{2},\theta_{K_{\mathfrak{p}}E})}\\
&=\frac{\varepsilon(\psi_{\mathfrak{p}}^0(N_{K_{\mathfrak{p}}E/K_{\mathfrak{p}}})\cdot\overline{\chi}(\sigma\circ N_{K_{\mathfrak{p}}E/E}),1,\theta_{K_{\mathfrak{p}}E})}{\varepsilon(\overline{\chi}(\sigma\circ N_{K_{\mathfrak{p}}E/E}),\frac{1}{2},\theta_{K_{\mathfrak{p}}E})}
\end{aligned}$$

Since $K_{\mathfrak{p}}E/K_{\mathfrak{p}}$ is unramified, $\psi_{\mathfrak{p}}^0(N_{K_{\mathfrak{p}}E/K_{\mathfrak{p}}})$ is the only character of order two of $(\mathcal{O}_{K_{\mathfrak{p}}E}/\mathfrak{p})^\times$. Since $N_{K_{\mathfrak{p}}E/E}((K_{\mathfrak{p}}E)^\times)$ is the subgroup generated by p and the squares of $\mathcal{O}_E^\times$, one has

$$(\sigma\circ N_{K_{\mathfrak{p}}E/E})(\mathcal{O}_{K_{\mathfrak{p}}E}^\times)=(\sigma\circ N_{K_{\mathfrak{p}}E/E})((K_{\mathfrak{p}}E)^\times)=aD_2.$$

We have to distinguish three cases:

(a) $\overline{\chi}(\sigma \circ N_{K_\mathfrak{p}E/E})$ is trivial on the units, hence trivial. This is equivalent to $\chi(aD_2) = \{1\}$, or equivalently to $\chi^a = 1$. Since a is odd, there are $\frac{a-1}{2}$ such characters.

(b) $(\overline{\chi} \circ \sigma \circ N_{K_\mathfrak{p}E/E})(\mathcal{O}_{K_\mathfrak{p}E}^\times) = \{\pm 1\}$: in this case, the restrictions to $\mathcal{O}_{K_\mathfrak{p}E}^\times$ of $\psi_\mathfrak{p}^0(N_{K_\mathfrak{p}E/K_\mathfrak{p}})$ and $(\overline{\chi} \circ \sigma \circ N_{K_\mathfrak{p}E/E})$ are two nontrivial characters $(\mathcal{O}_{EK_\mathfrak{p}}/\mathfrak{p})^\times \to \{\pm 1\}$, so they are equal, and their product is the unramified character mapping the uniformizer $\sqrt{-p}$ to $-p$. This case occurs whenever $\chi^a \neq 1$ but $\chi^{2a} = 1$. There are $\frac{2a-2}{2} - \frac{a-1}{2} = \frac{a-1}{2}$ such characters.

(c) In the remaining $\frac{p-3}{4} - (a-1) = \frac{p+1}{4} - a$ cases, $\psi_\mathfrak{p}^0(N_{K_\mathfrak{p}E/K_\mathfrak{p}}) \cdot \overline{\chi}(\sigma \circ N_{K_\mathfrak{p}E/E})$ and $\overline{\chi}(\sigma \circ N_{K_\mathfrak{p}E/E})$ are both characters $(K_\mathfrak{p}E)^\times/(1 + \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}E}) \to \mathbb{C}^\times$, and neither vanishes on $\mathcal{O}_{K_\mathfrak{p}E}^\times$.

We let $k = \mathcal{O}_E/p$ and $T, \nu : k \to \mathbb{F}_p$ denote the trace and norm, respectively. Let

$$\alpha : (K_\mathfrak{p}E)^\times/\mathbb{Z}_p^\times(1 + \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}E}) \to \mathbb{C}^\times$$

denote any ramified character. Since -1 is not a square in $\mathbb{F}_p^\times$, $\theta_{K_\mathfrak{p}E}$ is trivial on $\sqrt{-p}^{-1}\mathcal{O}_{K_\mathfrak{p}E}$ but not on $p^{-1}\mathcal{O}_{K_\mathfrak{p}E}$, we can apply Lemma C.1.5, so that

$$\begin{aligned}
\varepsilon(\alpha, s, \theta_{K_\mathfrak{p}E}) = \varepsilon(\alpha\|\cdot\|^{s-\frac{1}{2}}, \frac{1}{2}, \theta_{K_\mathfrak{p}E}) &= \alpha(p)\|p\|^{s-\frac{1}{2}} \frac{\sum_{x \in (\mathcal{O}_{EK_\mathfrak{p}}/\mathfrak{p})^\times} \alpha^{-1}(x)\theta_{K_\mathfrak{p}E}(x/p)}{\left|\sum_{x \in (\mathcal{O}_{EK_\mathfrak{p}}/\mathfrak{p})^\times} \alpha^{-1}(x)\theta_{K_\mathfrak{p}E}(x/p)\right|} \\
&= \alpha(p)p^{-4s+2} \frac{\sum_{x \in k^\times} \alpha^{-1}(x) e^{\frac{4i\pi}{p}T(x)}}{\left|\sum_{x \in k^\times} \alpha^{-1}(x) e^{\frac{4i\pi}{p}T(x)}\right|} \\
&= p^{-4s+2}\alpha(p) \frac{\sum_{x \in k^\times} \alpha^{-1}(x) e^{\frac{2i\pi}{p}T(x)}}{\left|\sum_{x \in k^\times} \alpha^{-1}(x) e^{\frac{2i\pi}{p}T(x)}\right|} \\
&= p^{-4s+2}\alpha(p)\alpha^{-1}(\sqrt{-1}) = p^{-4s+2}\alpha(p\sqrt{-1}).
\end{aligned}$$

When α is instead unramified, one has

$$\varepsilon(\alpha, s, \theta_{K_\mathfrak{p}E}) = \varepsilon(\alpha\|\cdot\|^{s-\frac{1}{2}}, \frac{1}{2}, \theta_{K_\mathfrak{p}E}) = \alpha(\sqrt{-p})p^{1-2s}.$$

Note that in all cases, the kernels of $\psi_\mathfrak{p}^0(N_{K_\mathfrak{p}E/K_\mathfrak{p}})$ and $(\overline{\chi} \circ \sigma \circ N_{K_\mathfrak{p}E/E})$ both contain $\sqrt{-1}^\mathbb{Z}\mathbb{Z}_p^\times(1 + \mathfrak{p}\mathcal{O}_{K_\mathfrak{p}E})$. Moreover, $(\overline{\chi} \circ \sigma \circ N_{K_\mathfrak{p}E/E})(p) = \overline{\chi}(\sigma(p^2)) = 1$.

Therefore, in all three cases, $\varepsilon_\chi = \varepsilon(\psi_\mathfrak{p}^0(N_{K_\mathfrak{p}E/K_\mathfrak{p}}) \cdot \overline{\chi}(\sigma \circ N_{K_\mathfrak{p}E/E}), 1, \theta_{K_\mathfrak{p}E})$.

(a): in this case, $\varepsilon_\chi = \varepsilon(\psi_\mathfrak{p}^0(N_{K_\mathfrak{p}E/K_\mathfrak{p}}), 1, \theta_{K_\mathfrak{p}E}) = \psi_\mathfrak{p}^0(N_{K_\mathfrak{p}E/K_\mathfrak{p}}(p\sqrt{-1}))p^{-2} = 1$.

(b): in this case, $\varepsilon_\chi = \varepsilon(\sqrt{-p} \longmapsto -p, 1, \theta_{K_\mathfrak{p}E}) = -pp^{1-2} = -1$.

(c): in this case,

$$\varepsilon_\chi = \varepsilon(\psi_\mathfrak{p}^0(N_{K_\mathfrak{p}E/K_\mathfrak{p}}) \cdot \overline{\chi}(\sigma \circ N_{K_\mathfrak{p}E/E}), 1, \theta_{K_\mathfrak{p}E}) = p^{-4+2}\psi_\mathfrak{p}^0(N_{K_\mathfrak{p}E/K_\mathfrak{p}}(p)) = p^{-2}\psi_\mathfrak{p}^0(p^2) = 1.$$

Finally, the global root number is $i(-1)^{\frac{p+1}{4}} U \frac{(-1)^{\frac{p+1}{4}} i}{(-1)^{\frac{p-3}{4}}} (-1)^{\frac{a-1}{2}} = (-1)^{\frac{p+2a-1}{4}} U$.

When $\rho_{|G_{\mathbb{Q}_p}}$ is wild:

Let us discuss why the result is well-defined. There are three aspects: we can change the decomposition subgroup at p, we can conjugate $\rho_{|G_{\mathbb{Q}_p}}$ by some matrix such that it remains of the form $\beta \begin{pmatrix} q & \nu \\ 0 & 1 \end{pmatrix}$, and we can change γ. We first explain why the second does not matter, then

discuss the first change. The independence of the result with respect to the choice of γ will be dealt with at the end of the proof.

Indeed, let $M \in \mathrm{GL}_2(\mathbb{F}_p)$ be such that $M\left(\beta\begin{pmatrix} q & \nu \\ 0 & 1\end{pmatrix}\right)M^{-1} = \beta'\begin{pmatrix} q' & \nu' \\ 0 & 1\end{pmatrix}$. By Lemma 4.4.9, we see that $(\beta, q) = (\beta', q')$ and that $\nu'_{|G_L} = r\nu_{G_L}$, where $r = \frac{M_{1,1}}{M_{2,2}} \in \det M\mathbb{F}_p^{\times 2}$.

Let $\gamma \in L^\times, \gamma_0 \in K_\mathfrak{p}^\times$ be attached to $\nu_{|G_L}$. Fix some $r_0 \in \mathbb{Z}_p^\times$ lifting r, then $\gamma' = r_0\gamma$ works for $\nu'_{|G_L}$, and thus we may take $\gamma'_0 = r_0^{[L:K_\mathfrak{p}]}\gamma_0$. Since $v_2([L:K_\mathfrak{p}]) = v_2([L:\mathbb{Q}_p]) - 1 = v_2(p-1) - 1 = 0$, the class of $r_0^{[L:K_\mathfrak{p}]}$ in $\mathbb{F}_p^\times$ is a square if and only if r is, if and only if $\det M \in \mathbb{F}_p^{\times 2}$.

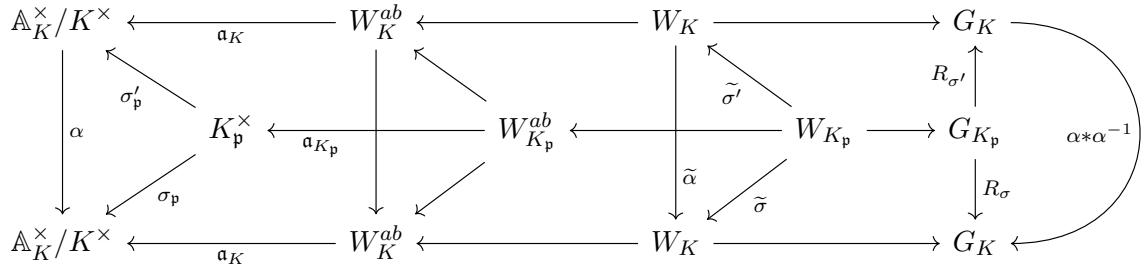
In particular, $\psi^0_\mathfrak{p}(\gamma'_0)\|\gamma'_0\|^{1/2} = \left(\frac{\det M}{p}\right)\psi^0_\mathfrak{p}(\gamma_0)\|\gamma_0\|^{1/2}$. This is what we wanted to prove, because $C^\epsilon(M\rho_{|G_K}M^{-1}) = C^{\left(\frac{\det M}{p}\right)\epsilon}(\rho_{|G_K})$ by Proposition B.4.1.

Now, we discuss the behavior with respect to changing the embedding $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}_p}$. Let $\sigma, \sigma' : \overline{\mathbb{Q}} \to \overline{G_{\mathbb{Q}_p}}$ be two embeddings inducing homomorphisms $R_\sigma, R_{\sigma'} : G_{\mathbb{Q}_p} \to G_\mathbb{Q}$. Then $\sigma' = \sigma \circ \alpha$ for some $\alpha \in G_\mathbb{Q}$, hence $R_{\sigma'}(t) = \alpha^{-1}R_\sigma(t)\alpha$ for every $t \in G_{\mathbb{Q}_p}$. The morphism $\rho \circ R_\sigma$ (resp. $\rho \circ R_{\sigma'}$) is $\mathrm{SL}_2(\mathbb{F}_p)$-conjugate to $\beta_\sigma\begin{pmatrix} q_\sigma & \nu_\sigma \\ 0 & 1\end{pmatrix}$ (resp. $\beta_{\sigma'}\begin{pmatrix} q_{\sigma'} & \nu_{\sigma'} \\ 0 & 1\end{pmatrix}$).

Therefore, the morphisms $\beta_\sigma\begin{pmatrix} q_\sigma & \nu_\sigma \\ 0 & 1\end{pmatrix}, \beta_{\sigma'}\begin{pmatrix} q_{\sigma'} & \nu_{\sigma'} \\ 0 & 1\end{pmatrix} : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\mathbb{F}_p)$ are $\mathrm{SL}_2(\mathbb{F}_p)$-conjugate if $\det\rho(\alpha) \in \mathbb{F}_p^{\times 2}$ and conjugate by a matrix in $\mathrm{GL}_2(\mathbb{F}_p)\backslash\mathbb{F}_p^{\times 2}\mathrm{SL}_2(\mathbb{F}_p)$ otherwise. Note that $\det\rho(\alpha) \in \mathbb{F}_p^{\times 2}$ if and only if $\omega_p(\alpha) \in \mathbb{F}_p^{\times 2}$, if and only if $\alpha \in G_K$, that is, if and only if $\sigma_{|K} = \sigma'_{|K}$.

By Lemma 4.4.9, $(\beta_\sigma, q_\sigma) = (\beta_{\sigma'}, q_{\sigma'})$, the extension L is the same in both cases, and $(\nu_{\sigma'})_{|G_L} = r(\nu_\sigma)_{|G_L}$ for some $r \in \mathbb{Z}_p^\times$ which is a square if and only if $\omega_p(\alpha)$ is one.

Moreover, using the material of [160, §1], one sees that there are morphisms $\widetilde{\sigma}, \widetilde{\sigma'} : W_{K_\mathfrak{p}} \to W_K$, and an automorphism $\widetilde{\alpha}$ of W_K such that the following diagram commutes, where the unmarked maps are the natural ones:



The claim we want to prove is thus $\psi^0(\sigma_\mathfrak{p}(\gamma_0)) = \psi^0(\sigma'_\mathfrak{p}(\gamma'_0))$, where $\gamma \in L^\times, \gamma_0 \in K_\mathfrak{p}^\times$ are attached to $(\nu_\sigma)_{|G_L}$ and $\gamma' = r\gamma, \gamma'_0 = r^{[L:K_\mathfrak{p}]}\gamma_0 \in K_\mathfrak{p}$ are attached to $(\nu_{\sigma'})_{|G_L}$. As above, $[L:K_\mathfrak{p}]$ is odd, so $r^{[L:K_\mathfrak{p}]}$ is a square if and only if $\omega_p(\alpha) \in \mathbb{F}_p^{\times 2}$. Since γ_0 has odd valuation (as we will see later in the proof),

$$\begin{aligned}\psi^0(\sigma_\mathfrak{p}(\gamma_0)) = \psi^0 \circ \alpha \circ \sigma'_\mathfrak{p}(r^{-[L:K_\mathfrak{p}]}\gamma'_0) &= \psi^0_\mathfrak{p}(r)^{-[L:K_\mathfrak{p}]}\psi^0_\mathfrak{p}(\sigma'_\mathfrak{p}(\gamma'_0))\frac{\overline{\psi^0_\mathfrak{p}}}{\psi^0_\mathfrak{p}}(\sigma'_\mathfrak{p}(\gamma'_0)) \\ &= \left(\frac{\omega_p(\alpha)}{p}\right)\psi^0(\sigma'_\mathfrak{p}(\gamma'_0))\left(\frac{\omega_p(\alpha)}{p}\right),\end{aligned}$$

so we are done.

Now, we can compute the sign after fixing a decomposition subgroup and conjugating ρ by a matrix in $\mathrm{SL}_2(\mathbb{F}_p)$ so that it has the form $\beta\begin{pmatrix} q & \nu \\ 0 & 1\end{pmatrix}$.

After conjugating by a matrix in $\mathrm{SL}_2(\mathbb{F}_p)$, we may assume that $\rho_{|G_{\mathbb{Q}_p}} = \beta \otimes \begin{pmatrix} q & \nu \\ 0 & 1 \end{pmatrix}$ with $\beta, q : G_{\mathbb{Q}_p} \to \mathbb{F}_p^\times$ characters and $\nu : G_{\mathbb{Q}_p} \to \mathbb{F}_p(q)$ a cocycle. Define $L, \nu_0, n, \gamma, \zeta, e, \omega, \varpi$ as in the case "$(f, \mathbf{1}) \in \mathscr{C}_1'$ and $\rho_{|G_{\mathbb{Q}_p}}$ wild". The maximal unramified subextension of K is denoted by L_0 to avoid a conflict of notation. Since $q\beta^2 = \omega_p^{-1}$, one has $q^{-1}(\mathbb{F}_p^{\times 2}) = \omega_p^{-1}(\mathbb{F}_p^{\times 2}) = G_{K_\mathfrak{p}}$, so $G_{K_\mathfrak{p}}$ is contained in L and $[\mathbb{F}_p^{\times 2} : q(G_{K_\mathfrak{p}})] = [\mathbb{F}_p^\times : q(G_{\mathbb{Q}_p})]$.

By Proposition B.4.3 and Mackey's formula,

$$\mathrm{D}_\mathfrak{p}\left(C^\epsilon(\rho_{|G_{K_\mathfrak{p}}})^*\right) \simeq \bigoplus_{t \in \mathbb{F}_p^{\times 2}/q(G_{K_\mathfrak{p}})} \mathrm{Ind}_L^{K_\mathfrak{p}}\left[e^{\frac{-2i\pi t\epsilon}{p}\nu_0} \circ \mathfrak{a}_L\right].$$

Therefore,

$$\varepsilon_q := \frac{\varepsilon(\psi_\mathfrak{p}^0(\mathfrak{a}_{K_\mathfrak{p}}) \otimes \mathrm{D}_\mathfrak{p}\left((C^\epsilon)^*(\rho_{|G_K})\right), 1, \theta_{K_\mathfrak{p}})}{\varepsilon(\mathrm{D}_\mathfrak{p}\left((C^\epsilon)^*(\rho_{|G_K})\right), \frac{1}{2}, \theta_{K_\mathfrak{p}})} = \prod_{t \in \mathbb{F}_p^{\times 2}/q(G_{K_\mathfrak{p}})} \frac{\varepsilon((\psi_\mathfrak{p}^0(N_{L/K_\mathfrak{p}})e^{\frac{-2i\pi t\epsilon}{p}\nu_0}) \circ \mathfrak{a}_L, 1, \theta_L)}{\varepsilon(e^{\frac{-2i\pi t\epsilon}{p}\nu_0} \circ \mathfrak{a}_L, \frac{1}{2}, \theta_L)}$$

$$= \prod_{t \in \mathbb{F}_p^{\times 2}/q(G_{K_\mathfrak{p}})} \frac{\varepsilon((\psi_\mathfrak{p}^0(N_{L/K_\mathfrak{p}})e^{\frac{-2i\pi t\epsilon}{p}\nu_0})\|\cdot\|^{\frac{1}{2}}, \frac{1}{2}, \theta_L)}{\varepsilon(e^{\frac{-2i\pi t\epsilon}{p}\nu_0}, \frac{1}{2}, \theta_L)}.$$

As in the $\mathscr{C}_1'$ case, $\psi_\mathfrak{p}^0(N_{L/K_\mathfrak{p}})$ is trivial on $1 + \varpi\mathcal{O}_L$. Since $[L : K_\mathfrak{p}]$ divides $\frac{[L:\mathbb{Q}_p]}{2} \mid \frac{p-1}{2}$ which is odd, $N_{L/K_\mathfrak{p}}(\mathcal{O}_L^\times)$ is a subgroup of $\mathcal{O}_K^\times$ with odd index, so it contains an element which is not a square, and $\psi_\mathfrak{p}^0(N_{L/K_\mathfrak{p}})$ does not vanish on $\mathcal{O}_L^\times$. So $\psi_\mathfrak{p}^0(N_{L/K_\mathfrak{p}})$ has level zero in the sense of [21, §1.8]. On the other hand, we saw in Lemma 4.4.9 that ν_0 had positive level $n-1$ in the sense of [21, §1.8].

It is clear from the definition of γ that whenever $x \in \varpi^{n/2}\mathcal{O}_L$, $e^{\frac{-2i\pi t\epsilon}{p}\nu_0}(1+x) = \theta_L\left(\frac{-t\epsilon\gamma}{p}x\right)$, so, by the stability theorem [21, §23.8], one has

$$\varepsilon_q^{-1} = \prod_{t \in \mathbb{F}_p^{\times 2}/q(G_{K_\mathfrak{p}})} \psi_\mathfrak{p}^0(N_{L/K_\mathfrak{p}}\frac{-t\epsilon\gamma}{p})\|\frac{-t\epsilon\gamma}{p}\|^{1/2} = \left(-\epsilon\psi_\mathfrak{p}^0(N_{L/K_\mathfrak{p}}\gamma)\|\gamma\|^{1/2}\right)^{[\mathbb{F}_p^{\times 2}:q(G_{K_\mathfrak{p}})]},$$

Let $\gamma_0 = N_{L/K_\mathfrak{p}}(\gamma) \in \mathfrak{p}^{f_{L/K_\mathfrak{p}}(1-n)}\mathcal{O}_{K_\mathfrak{p}}^\times$ with $\gamma_0 \in L^\times$. Since

$$f_{L/K_\mathfrak{p}}(1-n)[\mathbb{F}_p^{\times 2} : q(G_{K_\mathfrak{p}})] = \frac{(p-1)(1-n)}{e}$$

is an odd integer, it follows that

$$\varepsilon_q^{-1} = -\epsilon(-1)^{\frac{[\mathbb{F}_p^{\times 2}:q(G_{K_\mathfrak{p}})]-1}{2}}[\psi_\mathfrak{p}^0(\gamma_0)\|\gamma_0\|^{1/2}] \in \{\pm i\}.$$

Note that $[\mathbb{F}_p^{\times 2} : q(G_{K_\mathfrak{p}})] = [\mathbb{F}_p^\times : q(G_{\mathbb{Q}_p})] = \frac{p-1}{[L:\mathbb{Q}_p]}$ and by Lemma 4.4.9, $p - 1 \equiv [L : \mathbb{Q}_p] \equiv 2 \pmod 4$.

Let $d = [L : \mathbb{Q}_p]$. The global sign is thus

$$\epsilon\left(\prod_{\left(\frac{\ell}{p}\right)=-1}(-1)^{n_\ell}\right)(-1)^{\frac{p+1}{4}+\frac{p-1-d}{2d}}\left[i\psi_\mathfrak{p}^0(\gamma_0)\|\gamma_0\|^{1/2}\right].$$

Now, since $d \equiv p-1 \equiv 2 \pmod 4$,

$$\begin{aligned}\frac{p+1}{4} + \frac{p-1-d}{2d} &= \frac{\frac{d}{2}(p+1)+p-1-d}{2d} = \frac{\left(\frac{d}{2}+1\right)(p-1)}{2d} \\ &= \frac{(p-1)\left(\frac{d}{2}+1\right)}{4\frac{d}{2}} \equiv \frac{(p-1)\left(\frac{d}{2}+1\right)}{4} \pmod 2 \\ &\equiv \frac{p-1}{2}\frac{d+2}{4} \equiv \frac{d+2}{4} \pmod 2.\end{aligned}$$

In the above, we saw that γ_0 had indeed odd valuation. Moreover, if we replace γ with another allowed $\gamma' \in L^\times$, then $\gamma' \in (1+\varpi^{n/2}\mathcal{O}_L)\gamma$, so $N_{L/K_\mathfrak{p}}\left(\frac{\gamma'}{\gamma}\right) \in 1+\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}} \subset \ker \psi^0_\mathfrak{p}$. □

Remark It is surprising and not obvious *a priori*, that, except for the CM factors, the global root number for $R_f(\rho)$ only depends from $a_p(f)$ (which, by Proposition C.2.1, encodes whether (f,χ) is in $\mathscr{S}$, $\mathscr{P}'$, or $\mathscr{C}$), on the restriction of ρ to an inertia group at p, and on $p \pmod 4$. While it seems natural *a posteriori* that $a_p(f)$ and the restriction of ρ to an inertia group at p contribute to the sign, the relevance of $p \pmod 4$ seems less easy to explain.

4.6 Consequences for elliptic curves

In this Section, we fix an elliptic curve $E/\mathbb{Q}$, and consider, for any prime $p \geq 7$, the representation $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_p)$ given by $\rho(\sigma)\begin{pmatrix}\sigma(P)\\ \sigma(Q)\end{pmatrix} = \begin{pmatrix}P\\Q\end{pmatrix}$ for some basis (P,Q) of $E[p]$ (as in Proposition 1.4.8). By the results of [141], we know that either E has complex multiplication, or, for all but finitely many p, $\rho(G_\mathbb{Q}) = \mathrm{GL}_2(\mathbb{F}_p)$. This is another reason why Proposition 3.6.12 and the sign computation of the previous section are important: they describe, in some sense, the situation for all but finitely many p.

The following result is a standard estimate of the cardinalities of $\mathscr{S}, \mathscr{P}, \mathscr{C}$:

Lemma 4.6.1 *The following estimates fold, for any $p \geq 5$ and any $\epsilon \in \{\pm 1\}$:*

$$|\mathscr{S}| \in \frac{p+1}{12} + \left[-\frac{7}{6}, 0\right], \qquad |\mathscr{P}| \in \frac{(p-11)(p-3)}{24} + \left[0, \frac{7}{6}\right],$$

$$\left|\frac{1}{2}|\mathscr{S}| - \left|\{(f,\chi) \in \mathscr{S} \mid a_p(f) = \epsilon\}\right|\right| \leq \frac{3\sqrt{p}\ln 11e^2p}{2\pi}, \qquad |\mathscr{P}'| = \frac{1}{2}|\mathscr{P}|,$$

$$|\mathscr{C}| \in \frac{(p-1)(p^2-2p-27)}{48} + \frac{p-1}{2}\left[0, \frac{7}{6}\right], \qquad |\mathscr{C}'_1| + \frac{1}{2}|\mathscr{C}_M| \in \frac{p^2-2p-27}{48} + \left[0, \frac{7}{6}\right],$$

$$|\mathscr{C}_M| \in \{0, h(\mathbb{Q}(\sqrt{-p}))\}, \qquad |\mathscr{C}_M| \leq \frac{\sqrt{p}\ln 4e^2p}{\pi}.$$

Proof. – $|\mathscr{S}|$ is the genus of $X_0(p)$, which is known to be in $\frac{p+1}{2} - \left[0, \frac{7}{6}\right]$ (for instance [41, Exercise 3.1.4]). Furthermore, $|\mathscr{S}| + |\mathscr{P}|$ is the genus of $X_1(p)$, which is given in [41, Figure 3.4], and $|\mathscr{P}'| = \frac{1}{2}|\mathscr{P}|$. Moreover, by Corollaries 2.4.2 and 2.5.5, one has

$$\begin{aligned}&(p-1)\left(|\mathscr{C}| + \frac{p-1}{2}\mathscr{S} + \frac{p+1}{2}\dim_\mathbb{C} \mathcal{S}_2(\Gamma_1(p))\right) \\ &= p(p-1)|\mathscr{S} + (p+1)(p-1)|\mathscr{P}'| + (p-1)|\mathscr{C}| = (p-1)\dim_\mathbb{C} \mathcal{S}_2(\Gamma(p)),\end{aligned}$$

which yields successive estimates for $\mathscr{P}, \mathscr{P}', \mathscr{C}$.

Next, by considering the possible twists, $|\mathscr{C}| = \frac{p-1}{2}|\mathscr{C}_M| + (p-1)|\mathscr{C}_1'|$. So all we have to do is compute $|\mathscr{C}_M|$. We know that it is zero if $p \equiv 1 \pmod 4$, so we assume $p \equiv 3 \pmod 4$. By [132, Theorem 4.5], $|\mathscr{C}_M|$ is exactly the number of continuous characters $\mathbb{A}_K^\times / K^\times \to \mathbb{C}^\times$ (with $K := \mathbb{Q}(\sqrt{-p})$) that are equal to $z \longmapsto \sigma(z)^{-1}$ for $z \in (K \otimes \mathbb{R})^\times$ and some fixed isomorphism $\sigma : K \otimes \mathbb{R} \to \mathbb{C}$, are trivial on $(1 + \sqrt{-p}\mathcal{O}_{K_p}) \prod_{v \nmid \sqrt{-p}\infty} \mathcal{O}_{K_v}^\times$, and are given on $\mathcal{O}_{K_p}$ (as in the proof of Theorem 4.5.7) by the unique nontrivial character $(\mathcal{O}_{K_p}/\sqrt{-p})^\times \to \{\pm 1\}$.

If there exists such a character (that is, if $|\mathscr{C}_M| > 0$), then $|\mathscr{C}_M|$ is exactly the number of characters $\mathbb{A}_K^\times / \mathbb{C}^\times K^\times \prod_v \mathcal{O}_{K_v}^\times \to \mathbb{C}^\times$, therefore $|\mathscr{C}_M|$ is the class number $h(\mathbb{Q}(\sqrt{-p}))$ of $\mathbb{Q}(\sqrt{-p})$. By [1, Lemma 4.3], one has $h(\mathbb{Q}(\sqrt{-p})) \leq \frac{\sqrt{p}\ln 4e^2 p}{\pi}$.

Since $|\mathscr{S}| = \sum_\epsilon |\{(f,\chi) \in \mathscr{S} \mid a_p(f) = \epsilon\}|$, it is enough to conclude to prove that

$$\frac{1}{2}|\mathscr{S}| - \frac{3\sqrt{p}\ln 11e^2 p}{2\pi} \leq |\{(f,\chi) \in \mathscr{S} \mid a_p(f) = -1\}| \leq \frac{1}{2}|\mathscr{S}|.$$

We mimic the argument of [1, Section 4]. By Proposition C.3.3, the cardinality of the set $\{(f,\chi) \in \mathscr{S} \mid a_p(f) = -1\}$ is equal to the dimension of the subspace of $\mathcal{S}_2(\Gamma_0(p))$ fixed under the Atkin-Lehner involution w_p, hence is equal to the genus of the quotient $X_0^+(p)$ of $X_0(p)$ by w_p. Note that if $p \geq 5$ is congruent to 1 modulo 4, $\mathbb{Q}(\sqrt{-p})$ never has class number one by genus theory (since $\mathbb{Q}(i, \sqrt{p})$ is a quadratic extension of $\mathbb{Q}(\sqrt{-p})$ which is everywhere unramified). By applying the Riemann-Hurwitz formula as in Proposition 4.4 of *loc.cit.*, we find using Theorem 4.2 and Lemma 4.3 of *loc.cit.* that

$$2|\mathscr{S}| - 2 = 2(2|\mathscr{S}^-| - 2) + |\mathrm{Fix}(w_p)| \in 4|\mathscr{S}^-| - 2 + \left[0, \frac{\sqrt{p}\ln 4e^2 p}{\pi} + \frac{\sqrt{4p}\ln 16e^2 p}{\pi}\right].$$

The conclusion follows since

$$\begin{aligned}\frac{\sqrt{p}\ln 4e^2 p}{\pi} + \frac{\sqrt{4p}\ln 16e^2 p}{\pi} &\leq \frac{\sqrt{p}}{\pi}\left[\ln 4e^2 p + \ln 16e^4 p^2\right] \leq \frac{\sqrt{p}}{\pi}\ln 2^{10} e^6 p^3 \\ &\leq \frac{3\sqrt{p}\ln 11e^2 p}{\pi}.\end{aligned}$$

□

Lemma 4.6.2 *Suppose E has good ordinary (resp. good supersingular) reduction at p. Then $\rho_{|G_{\mathbb{Q}_p}}$ is split or wild (resp. 1-Cartan, and one of its reciprocity indices is one).*

Proof. – This follows from the local study of Serre [141, §1.11]. More precisely, the case "split or wild" for good ordinary reduction is exactly the discussion "b) or c)" in the Corollary to Proposition 11 of *loc.cit.* For good supersingular reduction, Proposition 12 of *loc.cit.* shows that the image of the inertia subgroup is a nonsplit Cartan subgroup, so that ρ is 1-Cartan. Moreover, the Corollary to Proposition 12 of *loc.cit.* shows using Proposition 3 that 1 is a reciprocity index for $\rho_{|G_{\mathbb{Q}_p}}$ (because Serre's normalization of class field theory isomorphism is the inverse of ours). □

Corollary 4.6.3 *As $p \to \infty$, uniformly in $E, \ell, \xi \in \mu_p^\times(\overline{\mathbb{Q}})$ as long as E has good reduction at p, the asymptotics for the number of eigenspaces for $(\mathbb{T}_1 \otimes \overline{\mathbb{Q}_\ell})$ of $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} \overline{\mathbb{Q}_\ell}$ with a given sign are given in Table 4.3. Recall that the eigenspaces corresponding to $(f,\chi) \in \mathscr{C}_M$ have dimension $p-1$ (and there are $O(\sqrt{p}\log p)$ of them), and the ones corresponding to non-CM newforms have dimension in $\{2p-2, 2p, 2p+2\}$.*

	Type of $\rho_{\mid G_{\mathbb{Q}_p}}$		
	Split	Wild	a-Cartan
$(-1)^{\frac{p-1}{2}}$	$\frac{p^2}{48}+O(p)$	$\frac{p^2}{24}+O(p)$	$\frac{p^2}{48}+O(p)$
$(-1)^{\frac{p+1}{2}}$	$\frac{p^2}{48}+O(p)$	$\frac{p}{24}+O(\sqrt{p}\log p)$	$\frac{p^2}{48}+O(p)$

Table 4.3: Asymptotic number of eigenspaces in the Tate module of $J_{\rho,\xi}(p)$ with a given global root number

4.7 On residual automorphy for the p-torsion of $J_\rho(p)$

Let F be a number field as in Section 4.4, that is: it contains the $p(p-1)^2(p+1)$-th roots of unity, the coefficients of all the newforms in $\mathscr{S}\cup\mathscr{P}\cup\mathscr{C}$, and, for each prime ℓ split in $\mathbb{Q}(\sqrt{-p})$ and every $(f,\mathbf{1})\in\mathscr{C}_M$, F contains the roots of $X^2-a_\ell(f)X+\ell$. Fix a prime ideal $\mathfrak{p}\subset\mathcal{O}_F$ with residue characteristic p, and an embedding $\mathcal{O}_F/\mathfrak{p}\to\overline{\mathbb{F}_p}$.

For instance, any character $\chi:\mathbb{F}_p^\times\to\mathbb{C}^\times$ takes its values in $\mathcal{O}_F^\times$, so can be reduced modulo $\mathfrak{p}$ to a character $\chi_\mathfrak{p}:\mathbb{F}_p^\times\to\overline{\mathbb{F}_p}^\times$. Since $\chi_\mathfrak{p}$ takes its values in the $(p-1)$-torsion of $\overline{\mathbb{F}_p}^\times$, that is, in $\mathbb{F}_p^\times$. Thus $\chi_\mathfrak{p}$ is an endomorphism of the group $\mathbb{F}_p^\times$, so it is of the form $x\longmapsto x^{a_\chi}$ for some integer $1\le a_\chi\le p-1$.

Similarly, let $\phi:\mathbb{F}_{p^2}^\times\to\mathbb{C}^\times$ be a character. It takes its values in $\mathcal{O}_F^\times$, so we can consider its reduction $\phi_\mathfrak{p}:\mathbb{F}_{p^2}^\times\to(\mathcal{O}_F/\mathfrak{p})^\times\subset\overline{\mathbb{F}_p}^\times$. Since $\phi_\mathfrak{p}$ takes its values in the (p^2-1)-torsion of $\overline{\mathbb{F}_p}^\times$, which is $\mathbb{F}_{p^2}^\times$. Thus, $\phi_\mathfrak{p}:\mathbb{F}_{p^2}^\times\to\mathbb{F}_{p^2}^\times$ can be uniquely written as $x\longmapsto x^{a+bp}$, with $0\le a,b<p$ and $(a,b)\neq(p-1,p-1)$. For instance, $a\equiv b\pmod 2$ if and only if ϕ is even.

Replacing ϕ with ϕ^p amounts to exchanging a and b, and ϕ factors through the norm $\mathbb{F}_{p^2}^\times\to\mathbb{F}_p^\times$ if and only if it is the case for $\phi_\mathfrak{p}$, which is the case if and only if $a=b$. Assuming that ϕ does not factor through the norm, we set $b_\phi=\min(a,b), a_\phi=\max(a,b)$. Note that these quantities only depend on the pair $\{\phi,\phi^p\}$, so in particular, they are independent from the embeddings $\mathcal{O}_F/\mathfrak{p}\subset\overline{\mathbb{F}_p}$, $\mathbb{F}_{p^2}\subset\overline{\mathbb{F}_p}$.

Let $\rho:G_\mathbb{Q}\to\mathrm{GL}_2(\mathbb{F}_p)$ be a representation such that $\det\rho=\omega_p^{-1}$, and let $\rho^*:G_\mathbb{Q}\to\mathrm{GL}_2(\mathbb{F}_p)$ denote its contragredient: thus $\det\rho^*=\omega_p$.

Proposition 4.7.1 *The $\overline{\mathbb{F}_p}[G_\mathbb{Q}]$-module $J_\rho(p)[p](\overline{\mathbb{Q}})\otimes_{\mathbb{F}_p}\overline{\mathbb{F}_p}$ has the same semi-simplification as the following direct sum of $\overline{\mathbb{F}_p}[G_\mathbb{Q}]$-modules:*

- $\left[\bigoplus_{(f,\mathbf{1})\in\mathscr{S}}T_{f,\mathfrak{p}}/\mathfrak{p}\otimes\mathrm{Sym}^{p-1}\rho^*\right]^{\oplus(p-1)}$,
- $\left[\bigoplus_{(f,\chi)\in\mathscr{P}'}(T_{f,\mathfrak{p}}/\mathfrak{p})\otimes\left[\mathrm{Sym}^{p-1-a_\chi}\rho^*\oplus(\omega_p^{-a_\chi}\otimes\mathrm{Sym}^{a_\chi}\rho^*)\right]\right]^{\oplus(p-1)}$,
- $\bigoplus_{(f,\chi)\in\mathscr{C}}T_{f,\mathfrak{p}}/\mathfrak{p}\otimes\left[(\omega_p^{1-a_f}\otimes\mathrm{Sym}^{a_f-b_f-2}\rho^*)\oplus(\omega_p^{-b_f}\otimes\mathrm{Sym}^{(p-1)-(a_f-b_f)}\rho^*)\right]$, *where b_f,a_f are the two integers attached to the character $\phi_f:\mathbb{F}_{p^2}^\times\to\mathcal{O}_F^\times$ (so that $0\le b_f<a_f\le p$).*

Proof. – Let $\chi:\mathbb{F}_p^\times\to\mathcal{O}_F^\times$ be a nontrivial character, then, by Lemma B.0.1 and Proposition B.1.4,

$$\pi(1,\chi)(\rho)\simeq\pi(1,\chi)^{\circ *}(\rho^*)\simeq\chi(\det)^{-1}\pi(1,\chi)(\rho^*)\simeq\pi(\chi^{-1},1)(\rho^*).$$

By Corollary B.5.8, the semi-simplification of $\pi(\chi_\mathfrak{p}^{-1},1)(\rho^*)$ is the direct sum of $\omega_p^{-a_\chi}\otimes\mathrm{Sym}^{a_\chi}\rho^*$ and of $\mathrm{Sym}^{p-1-a_\chi}\rho^*$.

The $\mathbb{F}_p[\mathrm{GL}_2(\mathbb{F}_p)]$-module St is isomorphic to Sym^{p-1}, so, by Lemma B.0.1, one has

$$\mathrm{St}(\rho)=\mathrm{St}^{\circ *}(\rho^*)\simeq\mathrm{St}(\rho^*)\simeq\mathrm{Sym}^{p-1}\rho^*.$$

Now, if $(f,\chi)\in\mathscr{C}$, $C_f(\rho)=C_f^{\circ *}(\rho^*)=\chi^{-1}(\det\rho^*)\otimes C_f(\rho^*)\simeq\chi^{-1}(\omega_p)\otimes C_f(\rho^*)$. By [131, Lemma 4.2], the semi-simplification of $C_\phi\pmod\mathfrak{p}$ is the direct sum of $\omega_p^{b_\phi+1}\otimes\mathrm{Sym}^{a_\phi-b_\phi-2}R$

and $\omega_p^{a_\phi - b_\phi} \otimes \mathrm{Sym}^{(p-1)-(a_\phi-b_\phi)} R$, where R is the tautological representation of $\mathrm{GL}_2(\mathbb{F}_p)$. Since $\chi^{-1}(\omega_p) = \omega_p^{-a_f-b_f}$, we can then apply Corollary 3.4.9. □

The shape of this decomposition suggests that we can use results in Langlands functoriality to prove that the components described in the previous propositions are mod p reductions of Galois representations attached to automorphic representations. The ones we will use are [127, Theorem A] for symmetric power functoriality, and the so far unpublished preprint [3, Theorem 1.1] for $\mathrm{GL}_2 \times \mathrm{GL}_n$ functoriality.

Proposition 4.7.2 *Assume that ρ^* is onto, or is irreducible with Serre weight in $\{2, p+1\}$, and that its Artin conductor N is coprime to 3. Let V be a $\overline{\mathbb{F}_p}[G_\mathbb{Q}]$-module of dimension $2r$ over $\overline{\mathbb{F}_p}$ which is one of the summands appearing in Proposition 4.7.1. Then, there exists a regular algebraic cuspidal polarized automorphic representation π of $\mathrm{GL}_{2r}(\mathbb{A}_\mathbb{Q})$ with coefficients in some number field F' and a prime ideal $\mathfrak{p}_0$ of residue characteristic p such that, if $V_{\pi,\mathfrak{p}_0}$ is the $\mathfrak{p}_0$-adic representation of $G_\mathbb{Q}$ attached to π, then the reduction mod $\mathfrak{p}_0$ of $V_{\pi,\mathfrak{p}_0}$ has the same semi-simplification as V (for a suitable embedding $\mathcal{O}_{F'}/\mathfrak{p}_0 \to \overline{\mathbb{F}_p}$).*

Proof. – By Proposition 4.7.1, $V \simeq T_{f,\mathfrak{p}}/\mathfrak{p} \otimes \mathrm{Sym}^a \rho^* \otimes u(\omega_p)$ for some $(f,\chi) \in \mathscr{S} \cup \mathscr{P} \cup \mathscr{C}$, where $u : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ is the reduction mod $\mathfrak{p}$ of a character $u_0 : \mathbb{F}_p^\times \to \mathcal{O}_F^\times$. Clearly, one has $a = r-1$.

Let us show that ρ^* is attached to a non-CM modular form $g \in \mathcal{S}_k(\Gamma_1(N'))$ for some integer N' coprime to $3p$. By Serre's conjecture (now a theorem [87, 88]), ρ^* is attached to a normalized newform $g_1 \in \mathcal{S}_k(\Gamma_1(N))$ such that $k \equiv 2 \pmod{p-1}$. If g_1 is not CM, we can take $(g, N') = (g_1, N)$. Otherwise, ρ^* is irreducible and its Serre weight k lies in $\{2, p+1\}$. By Cebotarev's theorem, there is a prime $q > 3Np$ such that $\rho^*(\mathrm{Frob}_q)$ is conjugate to the image under ρ^* of the complex conjugation. In particular, $q \equiv -1 \pmod{p}$, so the characteristic polynomial of $\rho^*(\mathrm{Frob}_q)$ is $(X-1)(X-q)$. Hence, by Diamond's theorem[5] [135, Theorem 5.1], ρ^* arises from an eigenform in $\mathcal{S}_k(\Gamma_1(N) \cap \Gamma_0(q))$ with level divisible by q. By [135, Theorem 4.2], ρ^* arises from a newform $g \in \mathcal{S}_k(\Gamma_1(N) \cap \Gamma_0(q))$. By Proposition 4.2.2, $\pi_{g,q}$ is the twist of a Steinberg representation. Therefore, by Proposition 4.3.11 and the construction of the local Langlands correspondence in [21, (33.3)], $D_{g,q}$ is a special representation of $W_{\mathbb{Q}_q}$, so g cannot have complex multiplication, and we let $(g, N') = (g, Nq)$.

Let $F' \subset \mathbb{C}$ be a number field containing F and the Fourier coefficients of g. Let $\mathfrak{p}_0$ be a prime ideal of $\mathcal{O}_{F'}$ above $\mathfrak{p}$ such that for almost every prime q, $a_q(g) \pmod{\mathfrak{p}_0} = \mathrm{Tr}(\rho^*(\mathrm{Frob}_q))$.

The argument of [135, §2] shows that, after multiplying by a power of the Eisenstein series $E_{p-1} \in 1 + \frac{p}{T}\mathbb{Z}[[q]]$ (where T is an integer coprime to p) or enlarging F' if necessary, there is a normalized eigenform $f_1 \in \mathcal{S}_{k'}(\Gamma(1))$ with coefficients in F' such that, for all primes $\ell \neq p$, $a_\ell(f_1) \equiv a_\ell(f \otimes u_0) \mod \mathfrak{p}_0$, and such that $k' > (a+1)(k+1)$. In particular, f_1 does not have complex multiplication and g is not in the Galois orbit of a twist of f_1.

By this construction, V and $[T_{f_1,\mathfrak{p}_0} \otimes \mathrm{Sym}^a T_{g,\mathfrak{p}_0}]/\mathfrak{p}_0$ has the same semi-simplification as V.

By [127, Theorem A], there is an regular algebraic cuspidal polarized automorphic representation π_g of $\mathrm{GL}_2(r)\mathbb{A}_\mathbb{Q}$ whose attached λ-adic representation is $\mathrm{Sym}^a V_{g,\lambda}$ for all maximal ideals $\lambda \subset \mathcal{O}_{F'}$: in particular, π_g is unramified away from the primes dividing $N'p$, so its level is coprime by 3. The conclusion follows if we can apply [3, Theorem 1.1], so all we need to do is check its hypotheses of regularity and irreducibility.

For any maximal ideal $\lambda \subset \mathcal{O}_{F'}$, the Hodge-Tate weights of $V_{f_1,\lambda} \otimes \mathrm{Sym}^a V_{g,\lambda}$ are pairwise distinct, so the compatible system $(V_{f_1,\lambda} \otimes \mathrm{Sym}^a V_{g,\lambda})_\lambda$ is regular.

By [108, Theorem 3.2.2], for any large enough prime ℓ and any prime ideal $\lambda \supset \mathcal{O}_{F'}$ with residue characteristic ℓ, the image of $G_{\mathbb{Q}(\mu_{\ell^\infty})}$ on $V_{f_1,\lambda} \oplus V_{g,\lambda}$ contains (for a suitable choice of

[5] I am grateful to Fred Diamond for suggesting to approach this question under the lens of level-raising congruences and for directing me towards his theorem.

bases) $\mathrm{SL}_2(\mathbb{Z}_\ell) \oplus \mathrm{SL}_2(\mathbb{Z}_\ell)$, so by Lemma 3.5.2 $V_{f_1,\lambda} \otimes \mathrm{Sym}^a V_{g,\lambda}$ is irreducible (because the action of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ on $\mathrm{Sym}^t(\overline{\mathbb{Q}_\ell}^{\oplus 2})$ is irreducible[6]). □

Remarks

- [3, Remark 1.4] suggests that the assumption $3 \nmid N$ is not necessary, but does not prove it.
- The purpose of the other assumptions on ρ^* is to make sure that it is attached to a non-CM modular form in characteristic zero. It seems likely [39] that the other assumptions can be weakened, but we have not been able to prove it.

[6]This well-known fact can be shown as follows: the action of $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ on an irreducible subrepresentation is unipotent, so this irreducible subrepresentation must contain some nonzero vector in $\ker(U - \mathrm{id})$. Such a vector is, up to a scalar, $x = \begin{pmatrix} 1 \\ 0 \end{pmatrix}^k$, and the U^T-translates of x generate $V := \mathrm{Sym}^t(\overline{\mathbb{Q}_\ell}^{\oplus 2})$, because $\dim V = t + 1$ and $(U^T - \mathrm{id})^t x \neq 0$, $(U^T - \mathrm{id})^{t+1} = 0$.

Chapter 5

Representations valued in the normalizer of a nonsplit Cartan subgroup

5.1 Statement of results

Throughout this chapter, $p \geq 7$ is a prime and $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is a continuous representation such that $\det \rho = \omega_p^{-1}$, and $\rho(G_{\mathbb{Q}})$ is contained in the normalizer N of a nonsplit Cartan subgroup C. We call K the imaginary quadratic field such that $G_K = \rho^{-1}(C)$ (see Proposition 5.2.1). The goal of this section is to find out what more information we can tell about the various curves $X_{\rho,\xi}(p)$.

The reason why we give this case a particular focus is that when $p \geq 17$ is a prime and $E/\mathbb{Q}$ is an elliptic curve, one of the following statements is true, by [111, 112, 12, 13]:

- E has complex multiplication,
- $p = 17$ (resp. $p = 37$) and E is a quadratic twist of an elliptic curve in the LMFDB isogeny class [107] with label 14450.b (resp. 1225.b),
- The image of the group homomorphism $G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$ is contained in the normalizer of a nonsplit Cartan subgroup,
- The group homomorphism $G_{\mathbb{Q}} \to \mathrm{Aut}(E[p])$ is onto.

Serre's uniformity question [141, §4.3], still currently open, asks whether the third case is redundant, at least for large enough primes p. This amounts to asking whether, for a large enough prime p, the rational points of a certain modular curve $X_{ns}^+(p)$ only correspond to cusps or CM points. An affirmative answer is suggested by the main theorem of [8], which uses a new method for the determination of rational points, the *Chabauty-Kim* method, and shows that for elliptic curves $E/\mathbb{Q}$ without complex multiplication, the action of $G_{\mathbb{Q}}$ on $E[13]$ is either reducible, surjective, or has image contained in an exceptional subgroup. In [9], a similar method is used in §5.1 to describe all the elliptic curves corresponding to this last case, and in §5.5 the authors show that the third case is redundant for $p = 17$. They run into computational issues for $p = 19$, but [44, Theorem 1, Remark 1] proves that the method can in principle be made to work for all primes $p \geq 13$.

In order to describe the results of this section, let us recall the following notation from the previous sections.

Notation for spaces of modular forms:

- $\mathcal{D}$ denotes the set of Dirichlet characters $(\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{C}^\times$,
- $\mathscr{S}$ denotes the set of $(f, \mathbf{1})$ where $f \in \mathcal{S}_2(\Gamma_0(p))$ is a newform,
- $\mathscr{P}$ denotes the set of (f, χ), where $f \in \mathcal{S}_2(\Gamma_1(p))$ is a newform with character $\chi \neq \mathbf{1}$,

- $\mathscr{P}'$ denotes a set of representatives for $\mathscr{P}$ modulo the involutive action of the complex conjugation,
- $\mathscr{C}$ denotes the set of (f,χ), where $f \in \mathcal{S}_2(\Gamma_1(p)\cap\Gamma_0(p^2))$ is a newform with character $\chi \in \mathcal{D}$, and such that no twist of f by a character in $\mathcal{D}$ has conductor p,
- $\mathscr{C}_1'$ denotes a set of representatives of the form $(f,\mathbf{1})$ for the $(f,\chi)\in\mathscr{C}$ modulo twists such that f does not have complex multiplication.
- $\mathscr{C}_M$ denotes the collection of $(f,\mathbf{1})\in\mathscr{C}$ such that f has complex multiplication. In this case, $p\equiv 3 \pmod 4$ and f has complex multiplication by $\mathbb{Q}(\sqrt{-p})$.

Notation for representations of $\mathrm{GL}_2(\mathbb{F}_p)$:

- $I_2 \in \mathrm{GL}_2(\mathbb{F}_p)$ is the identity matrix.
- For $\alpha\in\mathcal{D}$, St_α is the Steinberg representation of $\mathrm{GL}_2(\mathbb{F}_p)$ twisted by $\alpha(\det)$.
- For $\alpha,\beta\in\mathcal{D}$, $\pi(\alpha,\beta)$ is the principal series representation of $\mathrm{GL}_2(\mathbb{F}_p)$ attached to the characters α,β.
- Given $(f,\chi)\in\mathscr{C}$, we can attach by Definition 2.4.13 a cuspidal representation of $\mathrm{GL}_2(\mathbb{F}_p)$ named C_f.

Notation for Hecke algebras:

- $\mathbb{T}$ is the subalgebra of $\mathrm{End}\left(\prod_{\xi\in\mu_p^\times(\overline{\mathbb{Q}})} J_{\rho,\xi}(p)\right)$ generated by the Hecke operators T_n and the (mI_2), where $n\geq 1$ is coprime to p and $m\in\mathbb{F}_p^\times$.
- $\mathbb{T}_1$ is the subalgebra of $\mathbb{T}$ generated by the Hecke operators $(mI_2)\cdot T_n$, where $m,n\geq 1$ are integers such that $mn^2\equiv 1 \pmod p$. It is contained in $\bigoplus_{\xi\in\mu_p^\times(\overline{\mathbb{Q}})}\mathrm{End}(J_{\rho,\xi}(p))$.

Let $f\in\mathcal{S}_k(\Gamma_1(N))$ be a normalized newform with character χ and with coefficients contained in the ring of integers $\mathcal{O}_L$ of a number field L. Let λ be a maximal ideal of $\mathcal{O}_L$, then $V_{f,\lambda}$ denotes the continuous irreducible representation $G_\mathbb{Q}\to\mathrm{GL}_2(L_\lambda)$ such that for any prime q coprime to $N\lambda$, the characteristic polynomial of the arithmetic Frobenius Frob_q is $X^2-a_q(f)X+q^{k-1}\chi(q)$.

We choose a number field $F\subset\mathbb{C}$ which is Galois over $\mathbb{Q}$ and whose ring of integers $\mathcal{O}_F$ contains the following algebraic numbers:

- the $p(p-1)^2(p+1)$-th roots of unity,
- the Fourier coefficients of any f for $(f,\chi)\in\mathscr{S}\cup\mathscr{P}\cup\mathscr{C}$,
- for every $(f,\mathbf{1})\in\mathscr{C}_M$, for every prime ℓ split in $\mathbb{Q}(\sqrt{-p})$, the roots of the Hecke polynomial $X^2-a_\ell(f)X+\ell$ of f at ℓ.

Our first step is to describe the Tate module of $J_{\rho,\xi}(p)$ (for $\xi\in\mu_p^\times(\overline{\mathbb{Q}})$) as a Galois-module.

Theorem 5.A *(See Proposition 5.2.5) Let $\mathfrak{l}$ be a maximal ideal of $\mathcal{O}_F$ with residue characteristic ℓ. For any $\xi\in\mu_p^\times(\overline{\mathbb{Q}})$, $\mathcal{T}_\ell J_{\rho,\xi}(p)\otimes_{\mathbb{Z}_\ell}F_\mathfrak{l}$ is isomorphic to the direct sum of $(\mathbb{T}_1\otimes F_\mathfrak{l})[G_\mathbb{Q}]$-modules of the following form:*

- *$V_{f,\mathfrak{l}}\otimes\alpha(\rho)$, where $(f,\chi)\in\mathscr{S}\cup\mathscr{P}'\cup\mathscr{C}_1'\cup\mathscr{C}_M$, and $\alpha:N\to F^\times$ is a character such that $\alpha(tI_2)=\chi(t)$ for $t\in\mathbb{F}_p^\times$.*
- *$V_{f,\mathfrak{l}}\otimes\left[\mathrm{Ind}_C^N\psi\right](\rho)$, $(f,\chi)\in\mathscr{S}\cup\mathscr{P}'\cup\mathscr{C}_1'\cup\mathscr{C}_M$, where $\psi:C\to F^\times$ is a character such that $\psi^{p-1}\neq\mathbf{1}$, $\psi(tI_2)=\chi(t)$ for every $t\in\mathbb{F}_p^\times$, and, if $(f,\chi)\in\mathscr{C}_1'\cup\mathscr{C}_M$, ψ is not one of the two characters attached to f.*

The Hecke operator $(mI_2)\cdot T_n$ acts on each summand by $\chi(m)a_n(f)$. Moreover, for every submodule V as above, one has $V^*(1)\simeq V$ as $F_\mathfrak{l}[G_\mathbb{Q}]$-submodules.

As a corollary, the L-function of $J_{\rho,\xi}(p)$ splits into factors according to the decomposition given in Theorem 5.A. By the classical Rankin-Selberg method, we can show that these factors extend as entire functions on the complex plane and satisfy a functional equation, whose signs we compute.

We report here the computation of this sign when K is inert at p (which is the case for the application to elliptic curves when $p \geq 11$, see Lemma 5.4.2).

Theorem 5.B *(See Corollary 5.2.6 and Section 5.3) Let F be a large enough number field and $\mathfrak{l} \subset \mathcal{O}_F$ be a maximal ideal of residue characteristic ℓ, and fix $\xi \in \mu_p^\times(\overline{\mathbb{Q}})$. Let V be one of the summands of $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ (as a $F_\mathfrak{l}[G_\mathbb{Q}]$-module) described in Theorem 5.A. Then the L-function of V extends to an entire function on the complex plane and satisfies the predicted functional equation. When K is inert at p, the signs of these functional equations are the following:*

- *If V is two-dimensional, or four-dimensional with $(f,\chi) \in \mathscr{P}'$, the sign of the functional equation is -1.*
- *If V is four-dimensional with $(f,\mathbf{1}) \in \mathscr{S}$, the sign is 1 if, and only if, the representation $\left[\mathrm{Ind}_C^N \psi\right](\rho)$ is unramified at p.*
- *If V is four-dimensional with $(f,\mathbf{1}) \in \mathscr{C}_1' \cup \mathscr{C}_M$, let $\phi : \mathbb{F}_{p^2}^\times \to F^\times$ be the character attached to f, I_p be an inertia subgroup at p, and $\mathfrak{a} : I_p \to \mathbb{F}_{p^2}^\times$ be given by the class field theory reciprocity homomorphism (for E and normalized so that it maps an arithmetic Frobenius to a uniformizer). The sign of the functional equation is 1 if, and only if*[1]*, $\phi \circ \mathfrak{a}$ is one of the characters $\psi(\rho_{|I_p}), \psi^p(\rho_{|I_p})$.*

Corollary 5.C *(Corollary 5.4.5) When ρ comes from an elliptic curve with good reduction at p, then the signs of all the functional equations in Theorem 5.B are equal to -1. In particular, in this case, the central value of the L-function of all the factors described in Theorem 5.A vanishes.*

Nonetheless, in certain situations, the signs of some factors of the Tate module of $J_{\rho,\xi}(p)$ can be equal to one, and it is then possible for their central L-value to not vanish. In such a situation, thanks to the Euler systems constructed by Kato [84] and Kings, Loeffler and Zerbes [92], we can prove some cases of the Bloch-Kato conjecture in rank zero. In the case of two-dimensional factors, the result is a direct application of Kato's work; however, in the case of four-dimensional factors, applying the Euler system method requires that a certain *large image* condition be satisfied. This verification is carried out in Chapter 6.

Theorem 5.D *(See Section 5.5) Let F be a large enough number field and $\mathfrak{l} \subset \mathcal{O}_F$ be a maximal ideal of residue characteristic ℓ, and fix $\xi \in \mu_p^\times(\overline{\mathbb{Q}})$. Let V be one of the summands of $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ (as a $F_\mathfrak{l}[G_\mathbb{Q}]$-module) described in Theorem 5.A such that $L(V,1) \neq 0$.*

(i) Suppose that V is of the form $V_{f,\mathfrak{l}} \otimes \alpha(\rho)$, for some character $\alpha : N \to F^\times$. Then, for all but finitely many $\mathfrak{l}$, the divisible $\mathcal{O}_{F_\mathfrak{l}}$-linear Selmer group attached to V is finite.

(ii) Suppose that V is of the form $V_{f,\mathfrak{l}} \otimes \left[\mathrm{Ind}_C^N \psi\right](\rho)$ for some character $\psi : C \to F^\times$ with $(f,\mathbf{1}) \notin \mathscr{C}_M$. Then, for all but finitely many $\mathfrak{l}$ with residue characteristic ℓ such that f is ordinary at $\mathfrak{l}$ and that $\psi^{p-1}(\mathrm{Frob}_\ell) \neq 1$, the divisible $\mathcal{O}_{F_\mathfrak{l}}$-linear Selmer group attached to V is finite.

The finiteness of the Mordell-Weil group in a suitable quotient of the Jacobian is the main ingredient to apply Mazur's *formal immersion argument*. It was first used in [112, Corollary 4.3] and then became a standard technique in the determination of rational points on modular curves without reference to a model (see for instance [116, 12, 13, 101]). We use here a more explicit version of this argument, inspired by Coleman's approach to the Chabauty method [28], which was explained to me by Samuel Le Fourn.

Definition 5.1.1 Let $p \equiv 2,5 \pmod 9$ be a prime number. We say that a prime number ℓ is *exceptional* for p if $\ell \equiv \pm 1 \pmod p$ and there exists a prime ideal λ of $\mathbb{Z}[e^{2i\pi/p}]$ with residue

[1] Since the first submission of this thesis, I realized that this criterion could be written in a clearer way: it is equivalent to ask $\psi^{k-1} \in \{\phi_f, \phi_f^p\}$, where k is the Serre weight of the contragredient of ρ.

characteristic ℓ such that, for every cube root of unity $j \in \mathbb{F}_{p^2}^{\times}$,

$$u_j := \sum_{\substack{b \in \mathbb{F}_p \\ 1+b\sqrt{-3} \in \mathbb{F}_{p^2}^{\times 3} j}} e^{\frac{2i\pi b}{p}} \in \lambda.$$

Direct computations with Magma [16] show that for any $p \leq 1500$, the three u_j generate the unit ideal of $\mathbb{Z}[e^{\frac{2i\pi}{p}}]$. We thus tentatively expect that for any p, there are no exceptional primes[2].

Theorem 5.E *(Theorem 5.7.2) Assume that*

- $\rho : G_{\mathbb{Q}} \to N$ *is surjective of conductor* N_ρ,
- *the image under* ρ *of an inertia group at* p *is* $3C$,
- $X_{\rho,\xi}(p)$ *has a non-cuspidal rational point corresponding to an elliptic curve* E *over* $\mathbb{Q}$ *for some* ξ,
- *there exists* $(f, \mathbf{1}) \in \mathscr{S}$ *such that, if* $\psi : C \to F^{\times}$ *is a character with order* 3, *and* g *is the weight one holomorphic newform attached to the irreducible odd Artin representation* $\left[\mathrm{Ind}_C^N \psi\right](\rho)$, *then* $L(f \times g, 1) \neq 0$.

Then $p \equiv 2, 5 \pmod 9$ *and the conductor of* E *is of the form* $p^2 N_\rho L$, *where* L *is a square-free product of exceptional primes for* p *that do not divide* pN_ρ.

By our previous discussion about Serre's uniformity question, it is expected that the elliptic curve E has complex multiplication when $p \geq 13$ (in particular, it has potentially good reduction everywhere and $L = 1$), but this remains an open question. The recent works of Le Fourn and Lemos [101] then Furio and Lombardo [58] show that unless E has complex multiplication, one has $\rho(G_{\mathbb{Q}}) = N$. By Lemma 5.4.1, the image of an inertia subgroup at p is either C or $3C$, and the latter case can only occur if $p \equiv 2, 5 \pmod 9$.

Using the computation of the Serre weight of the p-torsion of an elliptic curve by Kraus [95], we find that, for the elliptic curve E_p with Weierstrass equation $y^2 = x^3 - p$ for $p \equiv 5 \pmod 9$, the Artin representation appearing in Theorem 5.E is the one attached to the unique newform $g \in \mathcal{S}_1(\Gamma_1(108))$ with rational coefficients and CM by $\mathbb{Q}(\sqrt{-3})$. For $p = 23$, I checked numerically in PARI/GP with the help of Pascal Molin the non-vanishing of $L(f \times g, 1)$ for some $(f, \mathbf{1}) \in \mathscr{S}$, which implies the following result. [3]

Corollary 5.F *Let* $p = 23$. *Any elliptic curve* $E/\mathbb{Q}$ *congruent modulo* p *to the elliptic curve* E_p *is isogenous to* E_p.

Using a result of analytic number theory of Michel [157, Appendix, Theorem 0.1] pointed out to me by Farrell Brumley, the conclusion of Theorem 5.E holds for all but finitely many E_p, in the following sense.

Theorem 5.G *(Proposition 5.8.4) There exists a constant* $p_0 \geq 11$ *such that, for any prime* $p \geq p_0$ *congruent to* 5 *modulo* 9, *for any elliptic curve* $E'/\mathbb{Q}$ *such that* $E'[p](\overline{\mathbb{Q}})$ *is isomorphic, as a* $G_{\mathbb{Q}}$*-module, to the* p*-torsion of the elliptic curve* E_p *with Weierstrass equation* $y^2 = x^3 - p$. *Then the conductor of* E' *is of the form* $108mp^2L$, *where* L *is a square-free product of exceptional primes for* p, *and* $m = 1$ *if* $p \equiv 3 \pmod 4$ *and* $m = 4$ *if* $p \equiv 1 \pmod 4$.

5.2 The Tate module of the $J_{\rho,\xi}(p)$

Before discussing the object of this section, we describe the representation ρ in more detail.

[2] Since the first submission of this thesis, this claim has been verified for $p \leq 5000$.

[3] Since the submission of this thesis, I was able to carry out further numerical computations, showing that the non-vanishing condition held for $23 \leq p \leq 150$ and $p \equiv 5 \pmod 9$. Therefore, the proof of Corollary 5.F carries over to $p = 41, 59$.

Proposition 5.2.1 *There exists an imaginary quadratic field $K/\mathbb{Q}$ such that $\rho^{-1}(C) = G_K$, and K is inert or ramified at p. Moreover,*

- *If $K/\mathbb{Q}$ is unramified at p, then ρ is a-Cartan (see Proposition 4.4.7) for some odd $a \mid \frac{p+1}{2}$. In particular, $[C : \rho(G_K)] \mid a$.*
- *If $p \equiv 1 \pmod 4$ and $K/\mathbb{Q}$ is ramified at p, then ρ is $\frac{p+1}{2}$-Cartan and $\rho(I_p \cap G_K) = \mathbb{F}_p^\times I_2$ for any inertia subgroup $I_p \leq G_\mathbb{Q}$ at p.*
- *If $p \equiv 3 \pmod 4$ and $K/\mathbb{Q}$ is ramified at p, then ρ is split and $\rho(G_{\mathbb{Q}_p} \cap G_K) \in \{\mathbb{F}_p^{\times 2} I_2, \mathbb{F}_p^\times I_2\}$.*

Proof. – Since $\det \rho = \omega_p^{-1}$ is an odd character, the image of the complex conjugation under ρ is conjugate to $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, so that $\rho(G_\mathbb{Q}) \not\subset C$, and $\rho^{-1}(C)$ is thus an open subgroup of $G_\mathbb{Q}$ with index two not containing the complex conjugation: it corresponds to an imaginary quadratic field K.

Fix an embedding $G_{\mathbb{Q}_p} \leq G_\mathbb{Q}$, let $I_p \leq G_{\mathbb{Q}_p}$ be the inertia subgroup. The group N does not contain any element of order p, so ρ is tamely ramified at p, so it cannot be wild (see Proposition 4.4.7).

If p splits in K, then the restriction of ρ to a decomposition subgroup at p is contained in C, so Proposition 4.4.7 implies that ρ is split: $\rho(G_{\mathbb{Q}_p}) \subset C$ is comprised of matrices which are diagonalizable over $\mathbb{F}_p$, $\rho(G_{\mathbb{Q}_p}) \subset \mathbb{F}_p^\times I_2$, hence $\mathbb{F}_p^\times = \omega_p^{-1}(G_{\mathbb{Q}_p}) \subset \det \mathbb{F}_p^\times I_2$, a contradiction. So K is inert or ramified at p.

Assume that $\rho_{|G_{\mathbb{Q}_p}}$ is split. Then $\rho(G_{\mathbb{Q}_p})$ is a subgroup of N made with matrices with eigenvalues in $\mathbb{F}_p^\times$. Thus $\rho(G_{\mathbb{Q}_p}) \cap C = \rho(G_{\mathbb{Q}_p} \cap G_K)$ is scalar. Moreover, by Proposition 4.4.7, $\rho(I_p)$ is a cyclic subgroup of order $p-1$ and has surjective determinant, so it is not scalar: hence $\rho(I_p) \not\subset C$, $\rho(I_p) \cap C = \rho(I_p)^2$, and K is ramified at p. Thus $\rho(I_p) \cap C$ is a cyclic subgroup of order $\frac{p-1}{2}$ of $\mathbb{F}_p^\times I_2$, so $\rho(I_p) \cap C = \mathbb{F}_p^{\times 2} I_2$ and $\mathbb{F}_p^{\times 2} = \det \rho(I_p)^2 = \det \rho(I_p) \cap C = \det \mathbb{F}_p^{\times 2} I_2 = \mathbb{F}_p^{\times 4}$ so $p \equiv 3 \pmod 4$.

Assume that ρ is a-Cartan and $K/\mathbb{Q}$ is ramified at p. Let $E/\mathbb{Q}_p$ denote the quadratic unramified extension, there is a Cartan subgroup $D \leq \mathrm{GL}_2(\mathbb{F}_p)$ such that $\rho(I_p) = aD$, and $\rho(I_p \cap G_K)$ is an index two subgroup of aD contained in C, so it is equal to $2aD \subset C$. Because C is cyclic, this implies $2aD = 2aC$. Moreover, any $z \in N \backslash C$, $\mathrm{Tr}(N) = 0$, so $N^2 = -(\det N) I_2$ and every element in $aD \backslash C$ has order dividing $2(p-1)$. So aD is contained in the reunion of the two subgroups $2aD$ and its subgroup of $2(p-1)$-torsion. Since a is odd, $aD \neq 2aD$, so aD is its subgroup of $2(p-1)$-torsion, thus a is a multiple of $\frac{p^2-1}{2(p-1)} = \frac{p+1}{2}$. Thus $a = \frac{p+1}{2}$; since a is odd, one has $p \equiv 1 \pmod 4$, and $\rho(I_p) \cap C = 2aD = (p+1)D = \mathbb{F}_p^\times I_2$.

The conclusion follows. □

Notation *For the rest of the chapter, ϵ is the unique nontrivial character of $N/C \simeq \{\pm 1\}$: then $\epsilon_K = \epsilon \circ \rho$ is the Galois character attached to the imaginary quadratic field K, and we let M be the conductor of the corresponding primitive Dirichlet character. The group homomorphism $G_K \to C$ induced by ρ is denoted ρ_K.*

Definition 5.2.2 For $(f, \chi) \in \mathscr{S} \cup \mathscr{P} \cup \mathscr{C}$, we define H_f as the following set of complex characters of N, and $H_f(\rho)$ as the collection of the $\alpha \circ \rho$ for $\alpha \in H_f$:

- If $(f, \chi) \in \mathscr{S}$, then H_f consists of the single character $\left(\frac{\det}{p}\right) \epsilon_K^{\mathbf{1}(p \equiv 3 \pmod 4)}$. Thus $H_f(\rho)$ contains the single character $\left(\frac{\omega_p}{p}\right) \epsilon_K^{\mathbf{1}(p \equiv 3 \pmod 4)}$.
- If $(f, \chi) \in \mathscr{P}$, then H_f contains the two characters $\psi(\det) \epsilon^{\mathbf{1}(\psi(-1)=-1)}$, for every $\psi \in \mathcal{D}$ such that $\psi^2 = \chi$. Thus $H_f(\rho)$ consists of the two characters $\overline{\psi}(\omega_p) \epsilon_K^{\mathbf{1}(\psi(-1)=-1)}$ where ψ is as in the previous sentence.

- If $(f,\chi) \in \mathscr{C}$ and f does not have complex multiplication, then H_f contains the two characters $\psi(\det)\epsilon^r$, for every $\psi \in \mathcal{D}$ such that $\psi^2 = \chi$, and $r \in \mathbb{Z}/2\mathbb{Z}$ is such that $(-1)^r\lambda_p(f \otimes \overline{\psi}) = 1$. Thus $H_f(\rho)$ consists of the two characters $\overline{\psi}(\omega_p)\epsilon_K^r$, for (ψ, r) as in the previous sentence.
- If $(f,\chi) \in \mathscr{C}$ and f has complex multiplication, then H_f (resp. $H_f(\rho)$) consists of the character $\psi(\det)\epsilon^{\frac{p-3}{4}}$ (resp. $\overline{\psi}(\omega_p)\epsilon_K^{\frac{p-3}{4}}$), where $\psi \in \mathcal{D}$ is the only *even* character such that $\psi^2 = \chi$.

We also define the set $\mathcal{I}_f$ of characters of C, endowed with the equivalence relation $\sim$, as follows:

- For $(f,\chi) \in \mathscr{S} \cup \mathscr{P}$, $\mathcal{I}_f$ is the set of characters $C \to \mathbb{C}^\times$ such that $\psi^p \neq \psi$ and $\psi(aI_2) = \chi(a)$ for all $a \in \mathbb{F}_p^\times$. We write $\alpha \sim \beta$ if $\alpha \in \{\beta, \beta^p\}$.
- For $(f,\chi) \in \mathscr{C}$ such that f has no complex multiplication, $\mathcal{I}_f$ is the set of characters $\psi : C \to \mathbb{C}^\times$ such that $\psi^p \neq \psi$, $\psi(aI_2) = \chi(a)$ for all $a \in \mathbb{F}_p^\times$, and ψ is not one of the two characters of C attached to C_f. We write $\alpha \sim \beta$ if $\alpha \in \{\beta, \beta^p\}$.
- For $(f,\chi) \in \mathscr{C}_M$, $\mathcal{I}_f$ is the set of characters $\psi : C \to \mathbb{C}^\times$ such that $\psi^{2(p-1)} \neq 1$ and $\psi(aI_2) = \chi(a)$ for every $a \in \mathbb{F}_p^\times$. We write $\alpha \sim \beta$ if $\alpha\beta^{-1}$ or $\alpha\beta^{-p}$ has order dividing 2.

Remarks

– For $\alpha : C \to \mathbb{F}_p^\times$, $\mathrm{Ind}_K^{\mathbb{Q}}\alpha(\rho_K)$ is reducible if and only if $\alpha(\rho_K) = \alpha^p(\rho_K)$, i.e. if and only if $\alpha^{p-1}(\rho_K) = 1$.
– For any $(f,\chi) \in \mathscr{S} \cup \mathscr{P} \cup \mathscr{C}$, for any $\sigma \in G_{\mathbb{Q}}$, there are bijections $\alpha \in H_f \longmapsto \sigma\circ\alpha \in H_\sigma(f)$, $\psi \in \mathcal{I}_f \longmapsto \sigma \circ \psi \in \mathcal{I}_\sigma(f)$, by Corollaries 4.2.5 and 4.3.13.
– For any $(f,\chi) \in \mathscr{C}$ and $\alpha \in \mathcal{D}$, there are bijections $\beta \in H_f \to \alpha\beta(\det) \in H_{f\otimes\alpha}$ and $\psi \in \mathcal{I}_f \longmapsto \beta(\det)\psi \in \mathcal{I}_{f\otimes\beta}$. This is a consequence of Corollaries 2.4.15 and B.2.8.

Lemma 5.2.3 *Let $(f,\chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1' \cup \mathscr{C}_M$.*

– *For any $\psi \in H_f(\rho)$, the newform $f \otimes \psi$ has trivial character*[4].
– *For any $\psi \in \mathcal{I}_f$, one has $\left[\mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)\right]^* \simeq \left[\mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)\right] \otimes \chi(\omega_p)$.*
– *For any $\psi \in \mathcal{I}_f$, one has $\det \mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K) = \epsilon_K\overline{\chi}(\omega_p)$.*

Proof. – The first point follows directly from the description of $H_f(\rho)$: the square of any $\alpha \in H_f(\rho)$ is $\overline{\chi}(\omega_p)$. For the second point, since $G_K = \rho^{-1}(C)$ and N/C acts on C by $z \longmapsto z^p$, one has

$$\begin{aligned}\left[\mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)\right]^* &\simeq \left[\mathrm{Ind}_K^{\mathbb{Q}}\psi^p(\rho_K)\right]^* \simeq \left[\mathrm{Ind}_K^{\mathbb{Q}}\overline{\psi}^p(\rho_K)\right] \\ &\simeq \left[\mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)\cdot\overline{\psi}(\rho_K^{p+1})\right] \simeq \left[\mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)\cdot\overline{\psi}(\omega_p^{-1}I_2)\right] \\ &\simeq \psi(\omega_p I_2)\otimes\left[\mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)\right] \simeq \chi(\omega_p)\otimes\left[\mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)\right].\end{aligned}$$

For the third point, the restriction to G_K of $\det \mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)$ is the product of the conjugates under $G_{\mathbb{Q}}/G_K$ of $\psi(\rho_K)$, so it is $\psi(\rho_K)\cdot\psi^p(\rho_K) = \psi(\rho_K^{p+1}) = \psi(\omega_p^{-1}I_2) = \overline{\chi}(\omega_p)$. Therefore, $\det \mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K) \in \{\overline{\chi}(\omega_p), \epsilon_K\overline{\chi}(\omega_p)\}$. Moreover, the image under $\det \mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)$ of the complex conjugation c is a symmetry with trace 0 (since K is imaginary), so the eigenvalues of the complex conjugation are 1 and -1 (with multiplicity on each), and its determinant is -1. Since $\overline{\chi}(\omega_p(c)) = 1$ and $\epsilon_K(c) = -1$, the determinant has to be $\epsilon_K\overline{\chi}(\omega_p)$. □

[4] As always, we identify characters of $G_{\mathbb{Q}}$ and Dirichlet characters by means of the cyclotomic character $G_{\mathbb{Q}} \to \hat{\mathbb{Z}}^\times$.

We define the group homomorphism $\widetilde{\rho} : (M,\sigma) \in N \rtimes_\rho G_{\mathbb{Q}} \longmapsto M\rho(\sigma) \in N$ and $\widetilde{\rho_K}$ as the induced morphism $\widetilde{\rho}^{-1}(C) \to C$.

Recall the following objects from Chapter 3, introduced in Definitions 3.6.4, 3.6.6.

Notation *We call $\mathbb{T}_{1,N}(N)$ the subalgebra of $\mathrm{End}\left(\prod_{\xi\in\mu_p^\times(\overline{\mathbb{Q}})} J_{\rho,\xi}(p)_{\overline{\mathbb{Q}}}\right)$ generated by the $T_n u$, where $n \geq 1$ is an integer coprime to p, $u \in \mathbb{Z}[N]$ commutes to N and is a linear combination of matrices of determinant $n^{-1} \in \mathbb{F}_p^\times$. This subalgebra is contained in $\bigoplus_{\xi\in\mu_p^\times(\overline{\mathbb{Q}})} \mathrm{End}(J_{\rho,\xi}(p))$.*

We denote by $\mathbb{T}_{1,N,\rho}$ the subalgebra of $\mathbb{T}[N \rtimes_\rho G_{\mathbb{Q}}]$ generated by the $(T_n \cdot (mI_2))(M,\sigma)$, for $n,m \geq 1, M \in N, \sigma \in G_{\mathbb{Q}}$ such that $m^2 n \det M \equiv 1 \pmod p$. It acts by group homomorphisms on $J_{\rho,\xi}(p)(\overline{\mathbb{Q}})$ for every $\xi \in \mu_p^\times(\overline{\mathbb{Q}})$.

Proposition 5.2.4 *For any $\xi \in \mu_p^\times(k_s)$, for any $(f,\chi) \in \mathscr{S} \cup \mathscr{P} \cup \mathscr{C}_1' \cup \mathscr{C}_M$, the f-eigenspace in $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is isomorphic as a $\mathbb{T}_{1,N,\rho} \otimes_{\mathbb{Z}} F_\mathfrak{l}$-module to the restriction to $\mathbb{T}_{1,N,\rho} \otimes F_\mathfrak{l}$ of the following $(\mathbb{T} \otimes F_\mathfrak{l})[N \rtimes_\rho G_{\mathbb{Q}}]$-module:*

$$\left[\bigoplus_{\alpha\in H_f} V_{f,\mathfrak{l}} \otimes \alpha(\widetilde{\rho})\right] \oplus \left[\bigoplus_{\psi\in\mathcal{I}_f/\sim} V_{f,\mathfrak{l}} \otimes \mathrm{Ind}_{\widetilde{\rho}^{-1}(C)}^{N\rtimes_\rho G_{\mathbb{Q}}} \psi(\widetilde{\rho_K})\right],$$

where $T_n \in \mathbb{T}$ (resp. $nI_2 \in \mathbb{T}$) for $n \geq 1$ coprime to p acts by $a_n(f)$ (resp. $\chi(n)$).

Proof. – First case: $(f,\chi) \notin \mathscr{C}_M$.

By Corollary 3.6.29, the f-eigenspace of $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is isomorphic as a $\mathbb{T}_{1,\mathrm{GL}_2(\mathbb{F}_p),\rho} \otimes F_\mathfrak{l}$-module to the restriction to $\mathbb{T}_{1,\mathrm{GL}_2(\mathbb{F}_p),\rho} \otimes F_\mathfrak{l}$ of $V_{f,\mathfrak{l}} \otimes R_f(\widetilde{\rho})$, where R_f is St if $(f,\chi) \in \mathscr{S}$, $\pi(\mathbf{1},\chi)$ if $(f,\chi) \in \mathscr{P}'$, and C_f if $(f,\chi) \in \mathscr{C}_1'$, and T_n (resp. nI_2) for any $n \geq 1$ coprime to p acts by $a_n(f)$.

The goal is then simply to describe the decomposition of $(R_f)_{|N}$ into irreducible representations. It is enough to show that $\mathrm{St}_{|N}$ (resp. $\pi(1,\chi)_{|N}$, resp. $C_f(\rho)_{|N}$) is isomorphic to $\bigoplus_{\psi\in H_f} \psi \oplus \bigoplus_{\psi\in\mathcal{I}_f/\sim} \mathrm{Ind}_C^N \psi$ (the latter sum is well-defined because if $\psi,\psi' \in \mathcal{I}_f$ are such that $\psi \sim \psi'$, then ψ is conjugate to ψ' by N/C).

When $(f,\chi) \in \mathscr{S}$, this is a consequence from Lemma B.3.4. When $(f,\chi) \in \mathscr{P}'$, this also follows directly from Lemma B.3.5.

When $(f,\chi) = (f,\mathbf{1}) \in \mathscr{C}_1'$, we apply Proposition B.3.8. The summands made from induced representations correspond to each other, so what we need to prove is that the (abelian) characters match. Let $\phi_f : C \to \mathbb{C}^\times$ be one of the two characters attached to C_f, then, by Proposition B.3.8, the two characters appearing in $(C_f)_{|N}$ are the $\psi\epsilon^r$, where $\psi \in \mathcal{D}$ runs through the characters such that $\psi^2(u) = \phi_f(uI_2)$ for each $u \in \mathbb{F}_p^\times$, and r is such that $(-1)^r\psi(-1)$ is -1 if $\phi_f(u) = \psi(u^2)$ for every $u \in \sqrt{\mathbb{F}_p^\times I_2}$, and 1 otherwise. Fix some $a \in \mathbb{F}_p^\times \backslash \mathbb{F}_p^{\times 2}$, then it is clear that $(-1)^r\psi(-1) = -\frac{\phi_f(\sqrt{a})}{\psi(a)}$, so $(-1)^r = -\frac{\phi_f(\sqrt{a})}{\psi(-a)} = \lambda_p(f\otimes\alpha) \in \{\pm 1\}$ by Corollary 2.4.16.

Second case: $(f,\chi) \in \mathscr{C}_M$.

By Corollary 3.6.25, as a $\mathbb{T}_1[\mathrm{SL}_2(\mathbb{F}_p) \rtimes_\rho G_{\mathbb{Q}}]$-module, the f-eigenspace of $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is isomorphic, for some sign r only depending on $\xi^{\mathbb{F}_p^{\times 2}}$, to

$$\mathrm{Ind}_{\mathrm{SL}_2(\mathbb{F}_p)\rtimes_\rho G_{\mathbb{Q}(\sqrt{-p})}}^{\mathrm{SL}_2(\mathbb{F}_p)\rtimes_\rho G_{\mathbb{Q}}} \psi_{f,r,\mathfrak{l}} \otimes C^+(\widetilde{\rho_K}) \simeq \mathrm{Ind}_{\mathrm{SL}_2(\mathbb{F}_p)\rtimes_\rho G_{\mathbb{Q}(\sqrt{-p})}}^{\mathrm{SL}_2(\mathbb{F}_p)\rtimes_\rho G_{\mathbb{Q}}} \psi_{f,+,\mathfrak{l}} \otimes C^r(\widetilde{\rho_K}),$$

where the extensions of $\widetilde{\rho}$ (resp. $\widetilde{\rho_K}$) to $\mathrm{SL}_2(\mathbb{F}_p) \rtimes_\rho G_{\mathbb{Q}}$ (resp. $\mathrm{SL}_2(\mathbb{F}_p) \rtimes_\rho G_{\mathbb{Q}(\sqrt{-p})}$) are given by $(M,g) \longmapsto M\rho(g) \in \mathrm{GL}_2(\mathbb{F}_p)$.

For any $\psi,\psi' \in \mathcal{I}_f$, the character $\psi^2_{|C\cap\mathrm{SL}_2(\mathbb{F}_p)}$ is by definition nontrivial, and $\psi \sim \psi'$ if and only if the restrictions of ψ,ψ' to $C \cap \mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p)$ are equal or p-th powers one of the other, that

is, if and only if the restrictions of ψ, ψ' to $C \cap \mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p)$ are conjugate under the action of N. Therefore, by Proposition B.4.5, one has

$$C^r_{|N\cap\mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p)} \simeq \left[\epsilon^{\frac{p-3}{4}} \oplus \bigoplus_{\chi\in\mathcal{I}_f/\sim} \left(\mathrm{Ind}_C^N \chi\right)\right]_{|N\cap\mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p)},$$

and the conclusion follows since $V_{f,\mathfrak{l}} = \mathrm{Ind}^{\mathbb{Q}}_{\mathbb{Q}(\sqrt{-p})}\psi_{f,r,\mathfrak{l}}$. □

Proposition 5.2.5 *Let $\mathfrak{l} \subset \mathcal{O}_F$ be a maximal ideal with residue characteristic ℓ.For any $\xi \in \mu_p^\times(\overline{\mathbb{Q}})$, and any $(f,\chi) \in \mathscr{S} \cup \mathscr{P} \cup \mathscr{C}'_1 \cup \mathscr{C}_M$, the f-eigenspace in $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is isomorphic (as a $F_\mathfrak{l}[G_\mathbb{Q}]$-module) to*

$$\left[\bigoplus_{\alpha\in H_f(\rho)} V_{f,\mathfrak{l}}\otimes\alpha\right] \oplus \left[\bigoplus_{\psi\in\mathcal{I}_f/\sim} V_{f,\mathfrak{l}} \otimes \mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)\right].$$

The summands of this decomposition are isomorphic to their Tate-twisted duals and do not depend on the choice of representatives for $\mathcal{I}_f/\sim$. Each summand is stable under the (geometric) action of $\mathbb{T}_{1,N}\otimes F_\mathfrak{l}$, is isomorphic to the direct sum of two copies of the same irreducible $\mathbb{T}_{1,N}\otimes F_\mathfrak{l}$-module, and two distinct summands have non-isomorphic attached $\mathbb{T}_{1,N}\otimes F_\mathfrak{l}$-modules. Moreover, every summand is irreducible as a $F_\mathfrak{l}[G_\mathbb{Q}]$-module, except in the following cases:

- *$\psi \in \mathcal{I}_f$ is such that $\psi(\rho_K)^{p-1} = 1$. In this case, $\mathrm{Ind}_K^\mathbb{Q}\psi(\rho_K)$ is the sum of two finite order characters $\alpha_\psi, \beta_\psi : G_\mathbb{Q} \to F^\times$. Moreover, $\alpha_\psi\beta_\psi = \epsilon_K\overline{\chi}(\omega_p)$ and $\alpha_\psi\beta_\psi^{-1} = \epsilon_K$. In this case, $V_{f,\mathfrak{l}}\otimes\alpha_\psi, V_{f,\mathfrak{l}}\otimes\beta_\psi$ are irreducible and isomorphic to their Tate-twisted duals.*
- *When $(f,\mathbf{1}) \in \mathscr{C}_M$, $\theta : G_K \to F_\mathfrak{l}^\times$ one of the two characters attached to f, and $\psi \in \mathcal{I}_f$ such that $\psi(\rho_K)^{p-1} \neq 1$:*
  - *If $K \neq \mathbb{Q}(\sqrt{-p})$ and $\psi(\rho_K)^4 = 1$, $V_{f,\mathfrak{l}} \simeq \mathrm{Ind}_K^\mathbb{Q}\psi(\rho_K)$ is the direct sum of two irreducible representations $\mathrm{Ind}^\mathbb{Q}_{\mathbb{Q}(\sqrt{-p})}\theta\otimes\alpha_\psi$, $\mathrm{Ind}^\mathbb{Q}_{\mathbb{Q}(\sqrt{-p})}\theta\otimes\beta_\psi$, where the characters α_ψ, β_ψ are the two lifts to $G_{\mathbb{Q}(\sqrt{-p})}$ of the quadratic character $\psi(\rho_K)_{|G_{K(\sqrt{-p})}}$. Taking the Tate-twisted dual exchanges these two representations.*
  - *When $(f,\mathbf{1}) \in \mathscr{C}_M$ (so that $p \equiv 3 \pmod 4$), $K = \mathbb{Q}(\sqrt{-p})$ and $\psi \in \mathcal{I}_f$ is such that $\psi(\rho_K)^{p-1} \neq 1$, let $\theta : G_K \to F_\mathfrak{l}^\times$ denote one of the characters attached to f. Then $V_{f,\mathfrak{l}}$ decomposes as the direct sum of the two following irreducible representations, both of which are isomorphic to their Tate-twiste duals: $\mathrm{Ind}_K^\mathbb{Q}\theta\otimes\psi(\rho_K)$ and $\mathrm{Ind}_K^\mathbb{Q}\theta\otimes\psi^p(\rho_K)$.*

Proof. – Let $(f,\chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}'_1 \cup \mathscr{C}_M$.

The group N/C acts on C by $z \mapsto z^p$, so, for any $\psi \in \mathcal{I}_f$, $G_\mathbb{Q}/G_K$ exchanges $\psi(\rho_K)$ and $\psi^p(\rho_K)$: therefore $\mathrm{Ind}_K^\mathbb{Q}\psi(\rho_K) \simeq \mathrm{Ind}_K^\mathbb{Q}\psi^p(\rho_K)$.

Furthermore, let $\alpha : C \to \{\pm 1\}$ be the unique character of order two. Then $\alpha(\rho_K) = \left(\frac{\det\rho_K}{p}\right)$ is the restriction to G_K of the character $\left(\frac{\omega_p}{p}\right)$, and therefore $\mathrm{Ind}_K^\mathbb{Q}(\alpha\psi)(\rho_K) \simeq \left(\frac{\omega_p}{p}\right)\otimes\mathrm{Ind}_K^\mathbb{Q}\psi(\rho_K)$. Since $V_{f,\mathfrak{l}}\otimes\left(\frac{\omega_p}{p}\right) \simeq V_{f,\mathfrak{l}}$ if $(f,\mathbf{1}) \in \mathscr{C}_M$, it follows that $V_{f,\mathfrak{l}}\otimes\mathrm{Ind}_K^\mathbb{Q}(\alpha\psi)(\rho_K) \simeq V_{f,\mathfrak{l}}\otimes\mathrm{Ind}_K^\mathbb{Q}\psi(\rho_K)$.

This proves that the given decomposition is independent from a choice of representatives for $\mathcal{I}_f/\sim$. By Lemma 5.2.3, all the summands are isomorphic to their Tate-twisted duals (since $V_{f,\mathfrak{l}} \simeq V^*_{f,\mathfrak{l}}(1)\otimes\chi(\omega_p)$).

The decomposition itself is a specialization of Proposition 5.2.4, which also implies the claimed stability under the geometric action of $\mathbb{T}_{1,N}\otimes F_\mathfrak{l}$. The Proposition also implies that the action of $\mathbb{T}_{1,N}$ on the summand $V_{f,\mathfrak{l}}\otimes\alpha(\rho)$ for $\alpha \in H_f$ (resp. $V_{f,\mathfrak{l}}\otimes\mathrm{Ind}_C^N\psi(\rho_K)$ for $\psi \in \mathcal{I}_f$) is the restriction to $\mathbb{T}_{1,N}$ of the action of $\mathbb{T}[N]$ on $\alpha^{\oplus 2}$ (resp. $\left[\mathrm{Ind}_C^N\psi\right]^{\oplus 2}$), where T_n (resp. mI_2) acts by multiplication by $a_n(f)$.

The claims that we need to prove are the following:

(i) For $\alpha \in H_f$, the datum of the $a_n(f)\chi(m)\alpha(M)$ for $n, m \geq 1$ and $M \in N$ such that $nm^2 \det M \equiv 1 \pmod{p}$ determines α.
(ii) For any $\psi \in \mathcal{I}_f$, $\mathrm{Ind}_C^N \psi$ is an irreducible $(\mathbb{T}_{1,N} \otimes F_\mathfrak{l})$-module,
(iii) For any $\psi, \psi' \in \mathcal{I}_f$, if $\mathrm{Ind}_C^N \psi$ and $\mathrm{Ind}_C^N \psi'$ are isomorphic $(\mathbb{T}_{1,N} \otimes F_\mathfrak{l})$-modules, then $\psi \sim \psi'$.

A result of Serre [144, Corollaire 2 au Théorème 15] states that if f is not CM, then, for any $u \in \mathbb{F}_p^\times$, there are infinitely many prime numbers $q \equiv u \pmod{p}$ such that $a_q(f) \neq 0$. This result implies directly (i) when $(f, \chi) \notin \mathscr{C}_M$, and H_f is a singleton when f is CM, so (i) is always true.

This result also shows that when $(f, \chi) \notin \mathscr{C}_M$ and under the assumptions of (iii), the representations $\mathrm{Ind}_C^N \psi$ and $\mathrm{Ind}_C^N \psi'$ of N over F are isomorphic, which implies that $\psi' \in \{\psi, \psi^p\}$ thus ψ, ψ'.

Let us prove (iii) when $(f, \chi) \in \mathscr{C}_M$. Indeed, under the assumptions of (iii), the representations $\mathrm{Ind}_C^N \psi, \mathrm{Ind}_C^N \psi'$ are isomorphic when reduced to $N \cap \mathrm{SL}_2(\mathbb{F}_p)$. This implies that the characters $\psi_{|C \cap \mathrm{SL}_2(\mathbb{F}_p)}, \psi'_{|C \cap \mathrm{SL}_2(\mathbb{F}_p)}$ are conjugate by N. This implies that $\psi \sim \psi'$.

Now, let us prove (ii). Let $\psi \in \mathcal{I}_f$ be such that $\mathrm{Ind}_C^N \psi$ is a reducible $(\mathbb{T}_{1,N} \otimes F_\mathfrak{l})$-module: its semi-simplification is the sum of characters $\alpha, \beta : \mathbb{T}_{1,N} \otimes F_\mathfrak{l} \to F_\mathfrak{l}$; both of them map $T_n \cdot (mI_2)$ to $a_n(f)\chi(m)$ for any $n, m \geq 1$ such that $nm^2 \equiv 1 \pmod{p}$. Therefore, $\mathrm{Ind}_C^N \psi$ is reducible as a $C \cap \mathrm{SL}_2(\mathbb{F}_p)$-module, which implies that $\psi^{p-1}_{|C \cap \mathrm{SL}_2(\mathbb{F}_p)} = \mathbf{1}$. Since, by construction, $\psi^{p-1}_{|\mathbb{F}_p^\times} = 1$, we see that $\psi^{2(p-1)} = \mathbf{1}$. In particular, if $\chi = \mathbf{1}$, then $\psi^4 = \mathbf{1}$, and therefore $(f, \chi) \notin \mathscr{C}_M$.

Let $M \in N$; by Serre's result, there exists a prime number $n \geq 1$ such that $n \det M \equiv 1 \pmod{p}$ and $a_n(f) \neq 0$. We let M act on $\mathrm{Ind}_C^N \psi$ (recall its only structure is that of a $\mathbb{T}_{1,N}$-module) by $a_n(f)^{-1} \cdot T_n M$. Since $(T_n M)^{p^2-1}$ acts by $T_n^{p^2-1} = a_n(f)^{p^2-1} \neq 0$ (by Lemma 2.2.2), T_n, M are automorphisms. Let $m \geq 1$ be an integer such that $m \det M \equiv 1 \pmod{p}$, let us show that $T_m M \in \mathbb{T}_{1,N}$ acts by $a_m(f)M$.

Indeed, by Serre's result, there exists a prime $q \nmid nmp$ such that $a_q(f) \neq 0$ and $q \equiv \det M \pmod{p}$. Then $(T_n T_q)(T_m M) = T_{mq}(T_n M)$ acts by $a_{nq}(f)(T_m M) = a_n(f)a_q(f)(T_m M)$ and $a_{mq}(f)a_n(f)M = a_n(f)a_m(f)a_q(f)M$, so that $T_m M$ acts by $a_m(f)M$.

It is straightforward to check that this construction defines a group action of N on the $(\mathbb{T}_{1,N} \otimes F_\mathfrak{l})$-module $\mathrm{Ind}_C^N \psi$, whose traces are exactly that of N on $\mathrm{Ind}_C^N \psi$; since this $(\mathbb{T}_{1,N} \otimes F_\mathfrak{l})$-module was reducible, it implies that $\mathrm{Ind}_C^N \psi$ is reducible as a $F_\mathfrak{l}[N]$-module, which is impossible by definition of $\mathcal{I}_f$.

Now, we discuss the irreducibility conditions for the Galois representations.

Let $\psi \in \mathcal{I}_f$. By Mackey's criterion [142, Proposition 23], $\mathrm{Ind}_K^\mathbb{Q} \psi(\rho_K)$ is irreducible if and only if $\psi(\rho_K)$ is disjoint from its conjugate under $G_\mathbb{Q}/G_K$, which is $\psi^p(\rho_K)$, as we saw. This is equivalent to $\psi(\rho_K) \neq \psi^p(\rho_K)$, or equivalently $\psi^{p-1}(\rho_K) \neq 1$.

When $\psi^{p-1}(\rho_K) = 1$, $\mathrm{Ind}_K^\mathbb{Q} \psi(\rho_K)$ is the direct sum of two characters α_ψ, β_ψ whose restriction to G_K is $\psi(\rho_K)$. Therefore, $\alpha_\psi = \beta_\psi \epsilon_K$, and $\alpha_\psi \beta_\psi = \epsilon_K \overline{\chi}(\omega_p)$ (by the third claim in Lemma 5.2.3), so that $\alpha_\psi^2 = \beta_\psi^2 = \overline{\chi}(\omega_p)$. Therefore the representations $V_{f,\mathfrak{l}} \otimes \alpha_\psi, V_{f,\mathfrak{l}} \otimes \beta_\psi$ are irreducible and isomorphic to their Tate-twisted duals, and their sum is $V_{f,\mathfrak{l}} \otimes \mathrm{Ind}_K^\mathbb{Q} \psi(\rho_K)$.

When $\psi^{p-1}(\rho_K) \neq 1$ and $(f, \chi) \notin \mathscr{C}_M$, by Proposition 3.5.3, $V_{f,\mathfrak{l}} \otimes \mathrm{Ind}_K^\mathbb{Q} \psi(\rho_K)$ is irreducible.

Now, we assume that $\psi^{p-1}(\rho_K) \neq 1$ and $(f, \chi) = (f, \mathbf{1}) \in \mathscr{C}_M$. Let $\theta : G_{\mathbb{Q}(\sqrt{-p})} \to F_\mathfrak{l}^\times$ be one of the characters attached to f and θ' be its conjugate under $G_\mathbb{Q}/G_K$, so that

$$V_{f,\mathfrak{l}} \otimes \mathrm{Ind}_K^\mathbb{Q} \psi(\rho_K) \simeq \mathrm{Ind}_{\mathbb{Q}(\sqrt{-p})}^\mathbb{Q} \left\{ \theta \otimes \left[\mathrm{Ind}_K^\mathbb{Q} \psi(\rho_K) \right]_{|G_{\mathbb{Q}(\sqrt{-p})}} \right\}.$$

By Mackey's criterion, this representation is irreducible if and only if $\theta \otimes \left[\mathrm{Ind}_K^\mathbb{Q} \psi(\rho_K) \right]_{|G_{\mathbb{Q}(\sqrt{-p})}}$ is irreducible and is not isomorphic to its conjugate under $G_\mathbb{Q}/G_{\mathbb{Q}(\sqrt{-p})}$, which is the representa-

tion $\theta' \otimes \left[\mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)\right]_{|G_{\mathbb{Q}(\sqrt{-p})}}$. Over a finite index normal subgroup of $G_{\mathbb{Q}(\sqrt{-p})}$, these representations are isomorphic to $\theta^{\oplus 2}, (\theta')^{\oplus 2}$ respectively. Since $\frac{\theta}{\theta'}$ has infinite image by [132, Theorem 4.3], $\theta \otimes \left[\mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)\right]_{|G_{\mathbb{Q}(\sqrt{-p})}}$ is not isomorphic to its conjugate under $G_{\mathbb{Q}}/G_{\mathbb{Q}(\sqrt{-p})}$.

Thus $V_{f,\mathfrak{l}} \otimes \mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)$ is irreducible if and only if $I := \left[\mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)\right]_{|G_{\mathbb{Q}(\sqrt{-p}}}$ is irreducible. This condition is false when $K = \mathbb{Q}(\sqrt{-p})$, which we will treat separately, so we assume for the time being that $K \neq \mathbb{Q}(\sqrt{-p})$. Then $I \simeq \mathrm{Ind}_{K(\sqrt{-p})}^{\mathbb{Q}(\sqrt{-p})}\psi((\rho_K)_{|K(\sqrt{-p})})$ is reducible, by Mackey's criterion, if and only if $\psi((\rho_K)_{|G_{K(\sqrt{-p})}}) = \psi^p((\rho_K)_{|G_{K(\sqrt{-p})}})$, which is equivalent to $\psi^{p-1}((\rho_K)_{|G_{K(\sqrt{-p})}}) = 1$. Since $G_{K(\sqrt{-p})} = \rho^{-1}(C \cap \mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p))$, this is equivalent to $\psi^{2(p-1)}(\rho_K) = 1$.

If I is reducible, since $\psi^{p+1} = 1$, one has $\psi^4(\rho_K) = 1$. Let α, β be the two lifts of $\psi(\rho_K)_{|G_{K(\sqrt{-p})}}$ to $G_{\mathbb{Q}(\sqrt{-p})}$, so that $I \simeq \alpha \oplus \beta$, $\alpha = \beta\epsilon_K$ and $\alpha\beta = \det I = \epsilon_K$. In particular, α, β are quadratic characters. Suppose that α is its own conjugate under $\mathrm{Gal}(\mathbb{Q}(\sqrt{-p})/\mathbb{Q})$: then it extends to a character $\alpha_0 : G_{\mathbb{Q}} \to \mathbb{C}^\times$ whose kernel contains $\rho^{-1}(4C)$. Thus α_0 factors through ρ. Let $g \in G_{\mathbb{Q}} \backslash G_K$, then $\rho(g)^2$ is scalar so $g^2 \in G_{K(\sqrt{-p})}$ and $\alpha_0(g)^2 = \alpha_0(g^2) = \psi(\rho_K(g)^2) = 1$, so that $\alpha_0^2 = 1$. In particular, the character $g \in \rho(G_K) \longmapsto \psi(g)\alpha_0(g)^{-1}$ is trivial on the index-two subgroup $\rho(G_K) \cap \mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p)$ but takes the values $\pm i$, whence a contradiction. Thus $\mathrm{Gal}(\mathbb{Q}(\sqrt{-p})/\mathbb{Q})$ exchanges α and β, and

$$\left[\mathrm{Ind}_{\mathbb{Q}(\sqrt{-p})}^{\mathbb{Q}}\theta \otimes \alpha\right]^*(1) \simeq \mathrm{Ind}_{\mathbb{Q}(\sqrt{-p})}\mathbb{Q}\theta^{-1}(1) \otimes \alpha^{-1} \simeq \mathrm{Ind}_{\mathbb{Q}(\sqrt{-p})}^{\mathbb{Q}}\theta' \otimes \alpha \simeq \mathrm{Ind}_{\mathbb{Q}(\sqrt{-p})}^{\mathbb{Q}}\theta \otimes \beta.$$

Now assume that $K = \mathbb{Q}(\sqrt{-p})$. Then

$$\begin{aligned} V_{f,\mathfrak{l}} \otimes \mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K) &\simeq \mathrm{Ind}_K^{\mathbb{Q}}\theta \otimes [\psi(\rho_K) \oplus \psi^p(\rho_K)] \\ &\simeq \left[\mathrm{Ind}_K^{\mathbb{Q}}\theta \otimes \psi(\rho_K)\right] \oplus \left[\mathrm{Ind}_K^{\mathbb{Q}}\theta \otimes \psi^p(\rho_K)\right]. \end{aligned}$$

Since $(\theta\psi(\rho_K))^*(1) = \theta'\psi^{-1}(\rho_K) = \theta'\psi^p(\rho_K)$ is the conjugate under $\mathrm{Gal}(K/\mathbb{Q})$ of $\theta\psi(\rho_K)$, the summands above are the Tate twists of their duals. Since $\theta \otimes \psi(\rho_K)$ is isomorphic over some open subgroup of G_K to θ, and since $\frac{\theta}{\theta'}$ has infinite image, Macley's criterion implies that both summands are irreducible.

□

Proposition 5.2.6 *Let V be any of the following compatible systems:*

(a) $(V_{f,\mathfrak{l}} \otimes \alpha)_\mathfrak{l}$ *for* $(f,\chi) \in \mathscr{E} := \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1' \cup \mathscr{C}_M$ *and* $\alpha \in H_f(\rho)$,
(b) $(V_{f,\mathfrak{l}} \otimes \alpha)_\mathfrak{l}$ *for* $(f,\chi) \in \mathscr{E}$ *and* $\alpha : G_{\mathbb{Q}} \to F^\times$ *extending* $\psi(\rho_K)$ *for some* $\psi \in \mathcal{I}_f$ *such that* $\psi(\rho_K)^{p-1} = 1$,
(c) $\left(V_{f,\mathfrak{l}} \otimes \mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)\right)_\mathfrak{l}$ *for* $(f,\chi) \in \mathscr{E}$ *and* $\psi \in \mathcal{I}_f$,
(d) if $K = \mathbb{Q}(\sqrt{-p})$ *and* θ *is a compatible system of characters of* G_K *attached to* $(f,\chi) \in \mathscr{C}_M$, $\mathrm{Ind}_K^{\mathbb{Q}}[(\theta\psi)(\rho_K)]$ *for* $\psi \in \mathcal{I}_f$.
(e) if $K \neq \mathbb{Q}(\sqrt{-p})$, *when* θ *is a compatible system of characters of* $G_{\mathbb{Q}(\sqrt{-p})}$ *attached to* $(f,\chi) \in \mathscr{C}_M$, $\psi \in \mathcal{I}_f$ *is such that* $\psi(\rho_K)^4 = 1$ *and* $\psi(\rho_K)^{p-1} \neq 1$, *the compatible system* $\left(\mathrm{Ind}_{\mathbb{Q}(\sqrt{-p})}^{\mathbb{Q}}\theta \otimes \alpha\right)_\mathfrak{l}$, *where* $\alpha : G_{\mathbb{Q}(\sqrt{-p})} \to \mathbb{C}^\times$ *extends* $\psi(\rho_K)_{|G_{K(\sqrt{-p})}}$.

Let M be the conductor of V. Then

$$\Lambda(V,s) := M^{s/2}[2(2\pi)^{-s}\Gamma(s)]^{\dim V/2}L(V,s)$$

is defined on a right half-plane, extends to an entire function and satisfies the functional equation

$$\Lambda(V,s) = \varepsilon(V)\Lambda(V^*(1), 2-s),$$

where $\varepsilon(V) \in \mathbb{C}^\times$. *Moreover,* $\varepsilon(V) = \prod_v \varepsilon_v$, *where*

- *In cases (a) and (b),* v *runs through the places of* $\mathbb{Q}$ *and* $\varepsilon_v = \varepsilon_v(f \otimes \alpha)$ *when* v *is finite, and* $\varepsilon_v(\infty) = (-i)^2 = -1$.
- *In case (c),* v *runs through all places of* $\mathbb{Q}$ *and* $\varepsilon_v = \varepsilon(D_{f,v} \otimes \mathrm{D}_v\left(\left(\mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)\right)^*\right), 1, \theta_{\mathbb{Q}_v})$.
- *In case (d),* v *runs through the places of* $\mathbb{Q}(\sqrt{-p})$ *and* $\varepsilon_v = \varepsilon(\mathrm{D}_v\left((\theta\psi(\rho_K))^*\right), 1, \theta_{K_v})$ *for* v *finite and* $\varepsilon_\infty(z^{-1}, 1, \theta_{\mathbb{C}})$.
- *In case (e),* v *runs through the places of* $\mathbb{Q}(\sqrt{-p})$ *and* $\varepsilon_v = \varepsilon(\mathrm{D}_v\left((\theta\alpha)^*\right), 1, \theta_{K_v})$ *for* v *finite and* $\varepsilon_\infty(z^{-1}, 1, \theta_{\mathbb{C}})$.

In all cases except (e), one has $V^*(1) \simeq V$ *and* $\varepsilon(V) \in \{\pm 1\}$.

The definition of the $D_{f,v}$ as Weil-Deligne representations is recalled in Section 4.3.

Proof. – In the first two cases, $V = V_{f\otimes\alpha,\mathfrak{l}}$ since α identifies with a Dirichlet character by the Kronecker-Weber theorem. The conclusion follows by Proposition C.3.2 (for the correct functional equation), Corollary C.3.5 (for the constant in the functional equation), and Proposition 4.3.11 (for the correct Galois-theoretic interpretation).

In the third case, this follows from the Rankin-Selberg functional equation (Proposition 4.5.5), and the fact that $\mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)$ is automorphic, because it is odd (and therefore either attached to a cuspidal weight one modular form, or the direct sum of two characters of $G_{\mathbb{Q}}$ of finite order). In the fourth and fifth cases, the result follows from Proposition 4.5.6.

The claimed self-duality is proved in Proposition 5.2.5, and it implies that $\varepsilon(V)^2 = 1$. □

5.3 Signs of the functional equation for factors of the Tate module of $J_{\rho,\xi}(p)$

Proposition 5.3.1 *Let* $(f,\chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1' \cup \mathscr{C}_M$, *and* $\alpha \in H_f(\rho)$. *Let* $V = (V_{f,\mathfrak{l}} \otimes \alpha)_{\mathfrak{l}\in\mathrm{Max}(\mathcal{O}_F)}$. *The global root number of the compatible system* V *(as defined in Proposition 5.2.6) is:*

- *equal to* $-\lambda_p(f\otimes\overline{\psi})$ *(resp.* $(-1)^{\frac{p+1}{4}}$*) if* K *is ramified at* p, $(f,\chi) \in \mathscr{C}_1'$ *(resp.* $(f,\chi) \in \mathscr{C}_M$*) and* $\alpha \in \epsilon_K^{\mathbb{Z}}\overline{\psi}(\omega_p)$.
- *equal to* $\eta(-p)a_p(f)$ *if* K *is ramified at* p, $(f,\chi) \in \mathscr{S}$ *and* $p \equiv 3 \pmod 4$, *where* η *the quadratic Dirichlet character with conductor coprime to* p *such that* $\epsilon_K\eta$ *has conductor* p.
- *equal to* -1 *otherwise.*

Proof. – We can write $\alpha = \beta(\omega_p)\gamma(\omega)$, where $\beta \in \mathcal{D}$, γ are Dirichlet characters with values in F, the conductor of γ is coprime to p, and $\omega : G_{\mathbb{Q}} \to \hat{\mathbb{Z}}^\times$ is the cyclotomic character. In all cases, $\gamma^2 = \mathbf{1}$ and $\beta^2\chi = \mathbf{1}$. Let P_1 be the conductor of the newform $f\otimes\beta$ (with trivial character), so P_1 is a power of p. By Propositions C.3.2 and Corollary C.3.8, the global root number of V is $(-i)^2\lambda_p(f\otimes\beta)\gamma(-P_1)$.

Suppose that $\beta \neq \mathbf{1}$ and that $(f,\chi) \in \mathscr{S} \cup \mathscr{P}'$. Then, by Propositions C.3.2 and C.3.9, $P_1 = p^2$ and $\lambda_p(f\otimes\beta) = \beta(-1)$, so the global root number of V is $-\alpha(\omega^{-1}(-1)) = -\alpha(c)$, where c is the complex conjugation.

When $(f,\chi) \in \mathscr{S} \cup \mathscr{P}'$, after checking every case, we can see that $\beta = \mathbf{1}$ if and only if $K/\mathbb{Q}$ is ramified at p, $p \equiv 3 \pmod 4$, and $(f,\chi) \in \mathscr{S}$. If one of these conditions is not satisfied, we can check case by case that $\alpha(c) = 1$. When $K/\mathbb{Q}$ is ramified at p, $p \equiv 3 \pmod 4$ and $(f,\chi) \in \mathscr{S}$, $\beta = \mathbf{1}$, so $P_1 = p$, $\lambda_p(f) = -a_p(f)$ by Propositions C.3.3 and C.2.1, so the global root number of V is $a_p(f)\gamma(p)$.

When $(f,\chi) \in \mathscr{C}_1' \cup \mathscr{C}_M$, then $(f \otimes \beta, \mathbf{1}) \in \mathscr{C}$, so $P_1 = p^2$, and the global root number of V is $-\gamma(-1)\lambda_p(f \otimes \beta)$.

If $(f,\chi) \in \mathscr{C}_1'$ and $K/\mathbb{Q}$ is inert at p, then $\beta = \overline{\psi}$ and $\gamma = \epsilon_K^r$ for some quadratic $\psi \in \mathcal{D}$, and $(-1)^r\lambda_p(f \otimes \overline{\psi}) = 1$, so that $\gamma(-1) = \lambda_p(f \otimes \beta)$, thus the global root number of V is -1.

If $(f,\chi) \in \mathscr{C}_1'$ and $K/\mathbb{Q}$ is ramified at p, $\beta = \overline{\psi}\lambda^r$ and $\gamma = \eta^r$ for some quadratic $\psi \in \mathcal{D}$, $(-1)^r\lambda_p(f \otimes \overline{\psi}) = 1$, and $\epsilon_K = \lambda\eta$, so, by Corollary 2.4.16,

$$-\gamma(-1)\lambda_p(f \otimes \beta) = -\eta(-1)^r(-\lambda(-1))^r\lambda_p(f \otimes \overline{\psi}) = -\lambda_p(f \otimes \overline{\psi}).$$

If $(f,\chi) \in \mathscr{C}_M$, $f = f \otimes \beta$, so we would like to compute $\lambda_p(f)$. Let $E/\mathbb{Q}_p$ be the unique quadratic unramified extension and $\phi : E^\times/(1+p\mathcal{O}_E) \to \mathbb{C}^\times$ be the character such that $\phi(p) = -p$ and $\phi_{|\mathcal{O}_E^\times}$ has order 4: then, by Lemma 4.4.4, Proposition 3.5.6 and Lemma C.1.5,

$$\begin{aligned}\lambda_p(f) = \varepsilon_p(f) &= \varepsilon(\mathrm{Ind}_E^{\mathbb{Q}_p}\phi(\mathfrak{a}_E), 1, \theta_p) = \lambda_{E/\mathbb{Q}_p}(\theta_p)\varepsilon(\phi(\mathfrak{a}_E)\|\cdot\|^{1/2}, \frac{1}{2}, \theta_E)\\ &= \phi_0(p)\|p\|^{1/2}\frac{\sum_{u\in(\mathcal{O}_E/p)^\times}\phi^{-1}(u)e^{\frac{2i\pi}{p}\mathrm{Tr}_{E/\mathbb{Q}_p}(u)}}{\left|\sum_{u\in(\mathcal{O}_E/p)^\times}\phi^{-1}(u)e^{\frac{2i\pi}{p}\mathrm{Tr}_{E/\mathbb{Q}_p}(u)}\right|}\\ &= -\phi(\sqrt{-1}) = -(-1)^{\frac{p^2-1}{8}} = -(-1)^{\frac{p-1}{2}\frac{p+1}{4}} = -(-1)^{\frac{p+1}{4}} = (-1)^{\frac{p-3}{4}}.\end{aligned}$$

When $K/\mathbb{Q}$ is inert at p, $\gamma = \epsilon_K^{\frac{p-3}{4}}$, so the global root number of V is $-(-1)^{\frac{p-3}{4}}(-1)^{\frac{p-3}{4}} = -1$.

When $K/\mathbb{Q}$ is ramified at p, $\epsilon_K = \lambda\eta$, where the conductor of η is coprime to p, so $\gamma = \eta^{\frac{p-3}{4}}$. Now, $\eta(-1) = \lambda(-1)(\lambda\eta)(-1) = 1$, and the global root number of V is $-(-1)^{\frac{p-3}{4}} = (-1)^{\frac{p+1}{4}}$. □

The results are gathered in Table 5.1:

	$(f,\mathbf{1}) \in \mathscr{S}$	$(f,\chi) \in \mathscr{P}'$	$(f,\mathbf{1}) \in \mathscr{C}_1'$	$(f,\mathbf{1}) \in \mathscr{C}_M$
$p \nmid M$	-1			
$p \mid M$, $p \equiv 1 \pmod 4$	-1		$-\lambda_p(f \otimes \overline{\psi})$	None
$p \mid M$, $p \equiv 3 \pmod 4$	$a_p(f)\eta(-p)$	-1	$-\lambda_p(f \otimes \overline{\psi})$	$(-1)^{\frac{p+1}{4}}$

Table 5.1: Functional equation signs for factors of $J_{\rho,\xi}(p)$ of the form $V_f \otimes \alpha$, where $\alpha = \overline{\psi}(\omega_p)\epsilon_K^r \in H_f(\rho)$

Lemma 5.3.2 *Let $(f,\mathbf{1}) \in \mathscr{S} \cup \mathscr{C}_1' \cup \mathscr{C}_M$ and $\psi \in \mathcal{I}_f(\rho)$. Assume that $K/\mathbb{Q}$ is ramified at p.*

- *If $p \equiv 3 \pmod 4$, then $\psi(\rho_K)$ vanishes on a decomposition subgroup at p.*
- *If $p \equiv 1 \pmod 4$, then $\psi(\rho_K)$ is an unramified character of order at most 2, mapping an arithmetic Frobenius to $\psi(\sqrt{a})$ for any $a \in \mathbb{F}_p^\times \backslash \mathbb{F}_p^{\times 2}$.*

Proof. – We fix a decomposition group $G_{\mathbb{Q}_p} \subset G_{\mathbb{Q}}$, let $I_p \leq G_{\mathbb{Q}_p}$ be the inertia group. If $p \equiv 3 \pmod 4$, by Proposition 5.2.1, $\rho(G_K \cap G_{\mathbb{Q}_p})$ is scalar, so is contained in the kernel of ψ. Thus we may assume that $p \equiv 1 \pmod 4$.

Therefore, ρ is $\frac{p+1}{2}$-Cartan by Proposition 5.2.1. By Lemma 4.4.11, $\rho(G_{\mathbb{Q}_p})/\rho(I_p)$ has cardinality two, and so does $\rho(I_p)/\rho(I_p \cap G_K)$: since $\rho(I_p \cap G_K) = \mathbb{F}_p^\times I_2$, $|\rho(G_{\mathbb{Q}_p})| = 4(p-1)$. By Lemma 4.4.11, $\rho(G_{\mathbb{Q}_p})$ is not commutative, so $\rho(G_{\mathbb{Q}_p}) \not\subset C$ and $\rho(G_{\mathbb{Q}_p} \cap G_K)$ is an index two subgroup of $\rho(G_{\mathbb{Q}_p})$. Hence $\rho(G_{\mathbb{Q}_p} \cap G_K) \subset C$ has cardinality $2(p-1)$ and contains $\mathbb{F}_p^\times I_2 = \rho(I_p \cap G_K)$. The conclusion follows. □

Proposition 5.3.3 *Let $(f,\chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1' \cup \mathscr{C}_M$. Let $\psi \in \mathcal{I}_f(\rho)$ be such that $\psi(\rho_K)^{p-1} = 1$, and let $\alpha, \beta : G_{\mathbb{Q}} \to F^\times$ be the two characters extending $\psi(\rho_K)$, and α_0, β_0 be the associated*

Dirichlet characters. The global root numbers of the compatible systems $V_f \otimes \alpha, V_f \otimes \beta$ are given by Table 5.2. The pair of the two root numbers is given by Table 5.3.

	$(f,\mathbf{1}) \in \mathscr{S}$	$(f,\chi) \in \mathscr{P}'$	$(f,\mathbf{1}) \in \mathscr{C}_1'$	$(f,\mathbf{1}) \in \mathscr{C}_M$
$p \nmid G$	$\gamma(-p)a_p(f)$	None	$-\gamma(-1)\lambda_p(f)$	$\gamma(-1)(-1)^{\frac{p+1}{4}}$
$p \mid G$	$-\gamma(-1)$		$\gamma(-1)\lambda_p(f)$	$\gamma(-1)(-1)^{\frac{p+1}{4}}$

Table 5.2: Functional equation signs for factors of $J_{\rho,\xi}(p)$ of the form $V_f \otimes \gamma$, where γ is one of the characters of $G_{\mathbb{Q}}$ extending $\psi(\rho_K)$ for $\psi \in \mathcal{I}_f$ such that $\psi(\rho_K)^{p-1} = 1$, and γ has conductor G.

	$(f,\mathbf{1}) \in \mathscr{S}$	$(f,\chi) \in \mathscr{P}'$	$(f,\mathbf{1}) \in \mathscr{C}_1'$	$(f,\mathbf{1}) \in \mathscr{C}_M$
$p \nmid M, \psi(\rho_K)_{\mid I_p} = 1$	$\alpha_0(-p)a_p(f)$	None	$\{\pm 1\}$	
$p \nmid M, \psi(\rho_K)_{\mid I_p} \neq 1$	$\{\pm 1\}$			
$p \mid M$	$\alpha_0(-1)\{1, \alpha_0(p)a_p(f)\}$	$\{\pm 1\}$	$\{-\alpha_0(-1)\lambda_p(f)\}$	$\{\alpha_0(-1)(-1)^{\frac{p+1}{4}}\}$

Table 5.3: Given a factor of the Tate module of $J_{\rho,\xi}(p)$ of the form $V_f \otimes \mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)$ with $\psi(\rho_K)^{p-1} = 1$, the pair of signs of the functional equations of the two compatible systems $V_f \otimes \alpha, V_f \otimes \beta$, where α, β are the characters of $G_{\mathbb{Q}}$ extending $\psi(\rho_K)$. In this table, α_0 denotes the primitive Dirichlet character attached to any character among α, β which is unramified at p.

Proof. – By Proposition 5.2.5, one $\alpha\beta = \varepsilon_K\overline{\chi}(\omega_p)$ and $\alpha\beta^{-1} = \epsilon_K$, which implies $\alpha_0^2 = \beta_0^2 = \overline{\chi}$. Since $\psi(\rho_K)$ takes its values in a subgroup of μ_{p^2-1}, it is tamely ramified above p. Since $K/\mathbb{Q}$ is tamely ramified at p, α, β are also tamely ramified at p, and the p-adic valuations of the conductors of α_0, β_0 are at most one.

Let $\gamma \in \{\alpha_0, \beta_0\}$, we can write $\gamma = \delta\eta$, where η is a quadratic character with conductor prime to p and $\delta \in \mathcal{D}$ is such that $\delta^2\chi = \mathbf{1}$.

Suppose that $\delta \neq \mathbf{1}$ and $(f,\chi) \in \mathscr{S} \cup \mathscr{P}'$. Then, by Proposition C.3.9, $f \otimes \delta \in \mathcal{S}_2(\Gamma_0(p^2))$ is a newform with functional equation sign $-\delta(-1)$ by Proposition C.3.2. By Corollary C.3.8, the sign of the functional equation for $f \otimes \gamma = (f \otimes \delta) \otimes \eta$ is $-\delta(-1)\eta(-p^2) = -\gamma(-1)$.

When $(f,\chi) \in \mathscr{S} \cup \mathscr{P}'$, $\delta = \mathbf{1}$ if and only if the conductor of γ is coprime to p. Since $\delta^2\chi = \mathbf{1}$, this is only possible when $(f,\chi) \in \mathscr{S}$ and one of α, β is unramified at p. When $K/\mathbb{Q}$ is inert at p, $\alpha\beta^{-1} = \epsilon_K$, so α is unramified at p if and only if β is, if and only if $\mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)$ is unramified at p. When $K/\mathbb{Q}$ is ramified at p and $(f,\chi) \in \mathscr{S}$, since $\alpha^2 = \beta^2 = \mathbf{1}$ and $\alpha\beta = \epsilon_K$, exactly one among the characters α, β is unramified at p.

So assume that $(f,\chi) \in \mathscr{S}$ and $\delta = \mathbf{1}$. Then, by Proposition C.3.2 and Corollary C.3.8, the sign of the functional equation for $f \otimes \gamma$ is $-\eta(-p)\lambda_p(f) = \eta(-p)a_p(f)$ by Proposition C.2.1.

Suppose now that $(f,\chi) = (f,\mathbf{1}) \in \mathscr{C}_1' \cup \mathscr{C}_M$. Then $(f \otimes \delta, \mathbf{1}) \in \mathscr{C}$, so the sign of the functional equation for $f \otimes \gamma = (f \otimes \delta) \otimes \eta$ is

$$(-i)^2\eta(-p^2)\lambda_p(f \otimes \delta) = -\eta(-1)\lambda_p(f \otimes \delta) = -\gamma(-1)\delta(-1)\lambda_p(f \otimes \delta).$$

By Corollary 2.4.16, this is equal to $\gamma(-1)\lambda_p(f)$ if δ is nontrivial, and $-\gamma(-1)\lambda_p(f)$ if δ is trivial. As we saw in the proof of Proposition 5.3.1, when f is CM, $\lambda_p(f) = (-1)^{\frac{p-3}{4}}$.

This explains how Table 5.2 is filled. Now, we discuss the contents of Table 5.3. Since $\alpha_0^2 = \beta_0^2 = \overline{\chi}$, if χ is not trivial, then it is necessary for α_0, β_0 to both be ramified at p. When $K/\mathbb{Q}$ is unramified at p, then the conductor of the quotient character $\alpha_0\beta_0^{-1}$ (which is the Dirichlet character attached to the quadratic extension $K/\mathbb{Q}$) is coprime to p, so α is ramified at p if and only if β is ramified at p. In this case, one has $\alpha_0(-1)\beta_0(-1)^{-1} = \epsilon_K(c) = -1$, where c is the complex conjugation, which accounts for the first two rows of the table except when $(f,\chi) \in \mathscr{S}$ and $\psi(\rho_K)$ is unramified at p. In this case, note that $\frac{\alpha_0}{\beta_0}(-p) = \epsilon_K(c\mathrm{Frob}_p) = (-1) \cdot (-1) = 1$.

When $p \mid M$, by Proposition 5.2.1, $\rho_K(I_p \cap G_K)$ is scalar. When $(f,\chi) \in \mathscr{P}'$, α and β are both ramified at p, thus the two signs are $-\alpha_0(-1), -\beta_0(-1)$, whose quotient is $\epsilon_K(c) = -1$.

Otherwise, $\chi = \mathbf{1}$, so $\psi(\rho_K(I_p \cap G_K))$ is trivial, so the restriction to an inertia subgroup I_p at p of α, β is quadratic. Since $\alpha = \beta\epsilon_K$, and the restriction to I_p of ϵ_K is a nontrivial quadratic character, exactly one among the characters α, β is unramified at p, and we can assume that it is α. The remaining entries in the table follow from noting that $-\beta_0(-1) = \alpha_0(-1)$, using the results previously written in Table 5.2, and the fact that $\alpha_0(-p) = \psi(\sqrt{a})$ for any $a \in \mathbb{F}_p^\times \backslash \mathbb{F}_p^{\times 2}$. Moreover, $\alpha_0(p) = \psi(\rho_K(\mathrm{Frob}_K))$, so it is equal to $\psi(\sqrt{a})$ for any $a \in \mathbb{F}_p^\times \backslash \mathbb{F}_p^{\times 2}$ if $p \equiv 1 \pmod 4$ and is equal to 1 otherwise. □

Proposition 5.3.4 *Let $(f,\chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1' \cup \mathscr{C}_M$. Let $\psi \in \mathcal{I}_f(\rho)$ be such that $\psi(\rho_K)^{p-1} \neq 1$. Then the global root number of the compatible system $(V_{f,\mathrm{l}} \otimes \mathrm{Ind}_K^{\mathbb{Q}} \psi(\rho_K)$ is given by the following:*

- *When $(f,\chi) \in \mathscr{S}$ and $K/\mathbb{Q}$ is unramified at p, the sign is 1 if and only if $\psi(\rho_K)$ is unramified at p.*
- *When $(f,\chi) \in \mathscr{S}$ and $K/\mathbb{Q}$ is ramified at p, the sign is $a_p(f)\psi(\sqrt{a})$ (where $a \in \mathbb{F}_p^\times \backslash \mathbb{F}_p^{\times 2}$) if $p \equiv 1 \pmod 4$, and $a_p(f)$ if $p \equiv 3 \pmod 4$.*
- *When $(f,\chi) \in \mathscr{P}'$, the sign is -1.*
- *When $(f,\chi) \in \mathscr{C}_1' \cup \mathscr{C}_M$ and $K/\mathbb{Q}$ is unramified at p, the sign is 1 if and only if the restriction of $\psi(\rho_K)$ to an inertia subgroup at p is the same as that of $\overline{\phi}(\mathfrak{a}_E)$ or $\overline{\phi}^p(\mathfrak{a}_E)$, where $E/\mathbb{Q}_p$ is the quadratic unramified extension.*
- *When $(f,\chi) \in \mathscr{C}_1' \cup \mathscr{C}_M$ and $K/\mathbb{Q}$ is ramified at p, the sign is 1.*

Proof. – For easier notation, we write $\Psi := \mathrm{Ind}_K^{\mathbb{Q}} \psi(\rho_K)$ and $\epsilon_K = \epsilon_{K,p}(\omega_p)\epsilon'_{K,p}(\omega)$, where $\omega : G_{\mathbb{Q}} \to \hat{\mathbb{Z}}^\times$ is the cyclotomic character, $\epsilon_{K,p} \in \mathcal{D}$ and $\epsilon'_{K,p}$ has conductor coprime to p. We fix a decomposition subgroup at p, thereby inducing an injection $G_{\mathbb{Q}_p} \subset G_{\mathbb{Q}}$, and we denote by $I_p \triangleleft G_{\mathbb{Q}_p}$ the inertia subgroup and by $\mathrm{Frob}_p \in G_{\mathbb{Q}_p}$ an arithmetic Frobenius with $\mathfrak{a}_{\mathbb{Q}_p}(\mathrm{Frob}_p) = \frac{1}{p}$.

We apply Proposition 5.2.6. By Proposition 4.4.6(i), the constant at infinity is $(-i)^{2\cdot 2} = 1$ in all cases. By Proposition 4.4.6(ii) and Lemma 5.2.3, the constant at a prime $\ell \neq p$ is exactly $\varepsilon(\mathrm{D}_\ell(\Psi \oplus \Psi^*), \frac{1}{2}, \theta_\ell)$.

Therefore, the global root number is

$$\begin{aligned}
&\varepsilon(D_{f,p} \otimes \mathrm{D}_p(\Psi^*), 1, \theta_p) \prod_{\ell \neq p\infty} \varepsilon(\mathrm{D}_\ell(\Psi \oplus \Psi^*), \frac{1}{2}, \theta_\ell) \\
&= \frac{\varepsilon(D_{f,p} \otimes \mathrm{D}_p(\Psi^*), 1, \theta_p)}{\varepsilon(\mathrm{D}_\infty(\Psi \oplus \Psi^*), \frac{1}{2}, \theta_\infty)\varepsilon(\mathrm{D}_p(\Psi \oplus \Psi^*), \frac{1}{2}, \theta_p)} = \frac{\varepsilon(D_{f,p} \otimes \mathrm{D}_p(\Psi^*), 1, \theta_p)}{\det \Psi(c) \det \Psi(\mathfrak{a}_{\mathbb{Q}_p}^{-1}(-1))}.
\end{aligned}$$

By Lemma 5.2.3, $\det \Psi = \epsilon_K \overline{\chi}(\omega_p)$, so $\det \Psi(c) = -1$, and $\det \Psi(\mathfrak{a}_{\mathbb{Q}_p}^{-1}(-1)) = \epsilon_{K,p}(-1)$. Thus $\epsilon_{K,p}(-1) \in \{-1, 1\}$, and it is equal to -1 if and only if $K/\mathbb{Q}$ is ramified at p and $p \equiv 3 \pmod 4$.

When $(f,\chi) \in \mathscr{P}'$:
By Proposition 4.4.6(ii) and Lemma 5.2.3, one has therefore

$$\varepsilon(D_{f,p} \otimes \mathrm{D}_p(\Psi^*), 1, \theta_p) = \varepsilon(\mathrm{D}_p(\Psi \oplus \Psi^*), \frac{1}{2}, \theta_p) = \det \Psi(\mathfrak{a}_{\mathbb{Q}_p}^{-1}) = \epsilon_{K,p}(-1),$$

whence the conclusion.

When $(f,\chi) \in \mathscr{S}$:
By Proposition 4.4.6(iii) and Lemma 5.2.3, one has

$$\varepsilon(D_{f,p} \otimes \mathrm{D}_p(\Psi^*), 1, \theta_p) = \varepsilon(\mathrm{D}_p(\Psi \oplus \Psi^*), \frac{1}{2}, \theta_p) \det(-a_p(f)\mathrm{Frob}_p \mid \Psi^{I_p}),$$

so the global root number is $-\det(-a_p(f)\mathrm{Frob}_p \mid \Psi^{I_p})$.

When $K/\mathbb{Q}$ is unramified at p, $\det\Psi = \epsilon_K$ is trivial on I_p, so Ψ^{I_p} is either the entire space of Ψ or zero. In the latter case, the global root number is therefore -1. In the former case, the global root number is $-(-a_p(f))^2\det\Psi(\mathrm{Frob}_p) = -\epsilon_K(\mathrm{Frob}_p) = -(-1) = 1$.

When $K/\mathbb{Q}$ is ramified at p, $\Psi_{|G_{\mathbb{Q}_p}} \simeq \mathrm{Ind}_{K\mathbb{Q}_p}^{\mathbb{Q}_p}\psi(\rho_K)_{|G_{K\mathbb{Q}_p}}$ and we can apply Lemma 5.3.2.

When $p \equiv 3 \pmod 4$, $\psi(\rho_K)_{|G_{K\mathbb{Q}_p}}$ is the trivial character, so $\Psi_{|G_{\mathbb{Q}_p}}$ is the direct sum of the trivial character and the (ramified) nontrivial character of $\mathrm{Gal}(K\mathbb{Q}_p/\mathbb{Q}_p)$. Thus

$$-\det(-a_p(f)\mathrm{Frob}_p \mid \Psi^{I_p}) = -(-a_p(f)) = a_p(f).$$

When $p \equiv 1 \pmod 4$, then, by Lemma 5.3.2, $\psi(\rho_K)_{|G_{K\mathbb{Q}_p}}$ is the unramified character mapping an arithmetic Frobenius to $\psi(\sqrt{a})$ for any $a \in \mathbb{F}_p^\times\backslash\mathbb{F}_p^{\times 2}$. So $\Psi_{|G_{\mathbb{Q}_p}}$ is the direct sum of the two characters α, β of $G_{\mathbb{Q}_p}$ extending $\psi(\rho_K)_{|G_{K\mathbb{Q}_p}}$. Since $\alpha\beta^{-1}$ is the nontrivial character of $\mathrm{Gal}(K\mathbb{Q}_p/\mathbb{Q}_p)$, at most one of these characters is unramified, and the unramified character of $G_{\mathbb{Q}_p}$ mapping an arithmetic Frobenius to $\psi(\sqrt{a})$ is one of α, β. Thus

$$-\det(-a_p(f)\mathrm{Frob}_p \mid \Psi^{I_p}) = -(-a_p(f)\psi(\sqrt{a})) = a_p(f)\psi(\sqrt{a}).$$

When $(f,\chi) \in \mathscr{C}$:

Let $E/\mathbb{Q}_p$ be the unique quadratic unramified extension and $\phi : E^\times/(1+p\mathcal{O}_E) \to \mathbb{C}^\times$ be a character such that $\phi_{|(\mathcal{O}_E/p)^\times}$ is attached to C_f and $\phi(p) = -p$. The case where $K/\mathbb{Q}$ is unramified at p is a consequence of Proposition 4.4.13(iii) (because $\epsilon_{K,p}(-1) = 1$), so we may assume that $K/\mathbb{Q}$ is ramified at p. Let $\mathfrak{p}$ be the unique prime ideal of K above p, and K_p be the $\mathfrak{p}$-adic completion of K and $\tau : \mathrm{Gal}(K_p/\mathbb{Q}_p) \to \{\pm 1\}$ the unique nontrivial character.

We denote by $\lambda \in \mathcal{D}$ the unique nontrivial quadratic Dirichlet character of conductor p.

The subgroup of norms $N_{K_p/\mathbb{Q}_p}K_p^\times \subset \mathbb{Q}_p^\times$ has valuation group $\mathbb{Z}$ and index 2, so its intersection with $\mathbb{Z}_p^\times$ is $\mathbb{Z}_p^{\times 2}$. Hence the subgroup of norms $N_{EK_p/\mathbb{Q}_p}(EK_p)^\times \subset \mathbb{Q}_p^\times$ has index 4, valuation group $2\mathbb{Z}$, contains $p^2 \in N_{E/\mathbb{Q}_p}E^\times \cap N_{K_p/\mathbb{Q}_p}K_p^\times$, and contains $\mathbb{Z}_p^{\times 2}$: hence $N_{EK_p/\mathbb{Q}_p}(EK_p)^\times = p^{2\mathbb{Z}}\mathbb{Z}_p^{\times 2}$ is the subgroup of norms of $E(\sqrt{-p})$ and $EK_p = E(\sqrt{-p})$. Thus $\tau_{|G_E} = \left(\frac{\omega_p}{p}\right)$.

When $p \equiv 3 \pmod 4$, $\psi(\rho_K)_{|G_{K_p}}$ is trivial by Lemma 5.3.2, so $\Psi_{|G_{\mathbb{Q}_p}} = \mathbf{1} \oplus \tau$. Since $D_{f,p}$ is induced from E, one has

$$D_{f,p} \otimes \mathrm{D}_p(\Psi^*) = D_{f,p} \otimes \left[\mathbf{1} \oplus \left(\frac{\omega_p}{p}\right)\right] = D_{f,p} \oplus D_{f\otimes\lambda,p},$$

hence

$$\varepsilon(D_{f,p} \otimes \mathrm{D}_p(\Psi^*), 1, \theta_p) = \epsilon_p(f)\epsilon_p(f\otimes\lambda) = \lambda_p(f)\lambda_p(f\otimes\lambda) = -\lambda(-1) = (-1)^{\frac{p+1}{2}} = -\epsilon_{K,p}(-1)$$

by Corollary 2.4.16, whence the conclusion.

When $p \equiv 1 \pmod 4$, $\psi(\rho_K)_{|G_{K_p}}$ is the unramified character $\mathrm{Frob}_K \longmapsto \psi(\sqrt{a})$ (for any $a \in \mathbb{F}_p^\times\backslash\mathbb{F}_p^{\times 2}$) with order dividing 2 by Lemma 5.3.2. Then $\Psi_{|G_{\mathbb{Q}_p}}$ is the direct sum of the unramified character $\eta : \mathrm{Frob}_p \in G_{\mathbb{Q}_p} \longmapsto \psi(\sqrt{a}) \in \{\pm 1\}$ and $\eta\tau$. Since $D_{f,p}$ is induced from E and $\Psi_{|G_E}$ is isomorphic to the restriction to G_E of $\mathbf{1} \oplus \left(\frac{\omega_p}{p}\right)$, one has as above

$$\varepsilon(D_{f,p}\otimes \mathrm{D}_p\left(\Psi^*\right),1,\theta_p)=\varepsilon(D_{f,p}\otimes(\mathbf{1}\oplus\left(\frac{\omega_p}{p}\right)^{-1}),1,\theta_p)=\varepsilon(D_{f,p}\oplus D_{f\otimes\lambda,p},1,\theta_p)$$
$$=\epsilon_p(f)\epsilon_p(f\otimes\lambda)=\lambda_p(f)\lambda_p(f\otimes\lambda)=-\lambda(-1)=(-1)^{\frac{p+1}{2}}=-\epsilon_{K,p}(-1)$$

by Corollary 2.4.16, whence the conclusion. □

Corollary 5.3.5 *Assume that $K/\mathbb{Q}$ is unramified at p. Then, among the irreducible factors of $\mathcal{T}_\ell J_{\rho,\xi}(p)\otimes_{\mathbb{Z}_\ell}F_\mathfrak{l}$ that are isomorphic to their Tate-twisted duals described in Proposition 5.2.5, the following ones have global root number $+1$:*

- *When $[C:\rho(G_K)]>1$ and $(f,\chi)\in\mathscr{P}'$, there exists $\psi\in\mathcal{I}_f$ such that $\psi(\rho_K)^{p-1}=\{1\}$. Let $\alpha:G_\mathbb{Q}\to F^\times$ be the (unique) odd character which extends $\psi(\rho_K)$, then $V_{f,\mathfrak{l}}\otimes\alpha$ works.*
- *When $\rho(G_K)=C$, $[C:\rho(I_p)]>1$ and $(f,\mathbf{1})\in\mathscr{S}$, there exists $\psi\in\mathcal{I}_f$ with $\psi(\rho_K)^{p-1}\neq\{1\}$ and $\psi(I_p)=\{1\}$. Then $V_{f,\mathfrak{l}}\otimes\mathrm{Ind}_K^\mathbb{Q}\psi(\rho_K)$ works.*
- *When $\rho(I_p)=C$ and b,b' are the two reciprocity indices of $\rho_{|G_{\mathbb{Q}_p}}$, for any $(f,\chi)\in\mathscr{C}_1'\cup\mathscr{C}_M$ such that b,b' do not divide $\frac{p+1}{\omega}$, where ω is the order of the character $\phi:C/\mathbb{F}_p^\times\to\mathbb{C}^\times$ attached to f, then there exists $\psi\in\mathcal{I}_f$ such that $V_{f,\mathfrak{l}}\otimes\mathrm{Ind}_K^\mathbb{Q}\psi(\rho_K)$ works.*

Proof. – In the first case, we know that $\rho(G_K)=a'C$ with $a'\mid a$; by Proposition 4.4.7, $a\mid\frac{p+1}{2}$ is coprime to $p-1$, thus $a'\mid\frac{p+1}{2}$ is odd. In particular, $\mathbb{F}_p^\times I_2\subset\rho(G_K)$ and $[C:\rho(G_K)]>2$. Let $\gamma\in\mathcal{D}$ with square χ and $\gamma_0=\gamma(\det):C\to F^\times$. Then $(\gamma_0)(tI_2)=\chi(t)$ for any $t\in\mathbb{F}_p^\times$.

The characters $\beta:C\to F^\times$ such that $\beta(tI_2)=\chi(t)$ for every $t\in\mathbb{F}_p^\times$ are exactly the $\gamma_0\psi$, where ψ runs through the characters $C/\mathbb{F}_p^\times\to F^\times$. For any $\psi:C/\mathbb{F}_p^\times\to F^\times$, one has

$$\beta:=\gamma_0\psi\in\mathcal{I}_f\Leftrightarrow\beta^{p-1}\neq\mathbf{1}\Leftrightarrow\psi^{p-1}\neq\mathbf{1}\Leftrightarrow\psi^2\neq\mathbf{1},$$
$$\beta(\rho_K)^{p-1}=\{1\}\Leftrightarrow\psi(\rho_K)^{p-1}=\{1\}\Leftrightarrow\psi^2(\rho_K)=\{1\}.$$

The group $C/(\mathbb{F}_p^\times\rho(G_K))=C/\rho(G_K)$ is cyclic with cardinality at least 3, so there is a character $\psi:C\to F^\times$ such that $\psi(\mathbb{F}_p^\times\rho(G_K))=\{1\}$ and $\psi^2\neq\mathbf{1}$. Then $\gamma_0\psi\in\mathcal{I}_f$ is such that $(\gamma_0\psi)(\rho_K)^{p-1}=\{1\}$, so that there are two characters $\alpha,\beta:G_\mathbb{Q}\to\mathbb{C}^\times$ extending $(\gamma_0\psi)(\rho_K)$. Their ratio is the odd character ϵ_K, so exactly one among α and β is odd. Since $\psi(\rho_K)$ takes its values in $F^\times$ and $G_\mathbb{Q}$ is generated by G_K and the complex conjugation, α,β also take their values in $F^\times$. The conclusion follows from Proposition 5.3.3.

In the second case, $\rho(I_p)=aC$ for some odd $a\mid\frac{p+1}{2}$ which is greater than one. So $[C:\rho(I_p)]>2$ and $\rho(I_p)\supset\mathbb{F}_p^\times$. Therefore, there exists a character $\psi:C/\rho(I_p)\to F^\times$ with order at least 3. Then $\psi(\rho_K)^{p-1}\neq\{1\}$, so $V_{f,\mathfrak{l}}\otimes\mathrm{Ind}_K^\mathbb{Q}\psi(\rho_K)$ is irreducible and isomorphic to its Tate-twisted dual. Since $\psi(\rho(I_p))=\{1\}$, the conclusion follows from Proposition 5.3.4.

In the third case, let $E/\mathbb{Q}_p$ be the quadratic unramified extension and fix an isomorphism $\iota:C\to(\mathcal{O}_E/p)^\times$ preserving the trace and norm. Let $\sigma:E/(1+p\mathcal{O}_E)\to C$ be such that $\rho_{|W_E}=\sigma(\mathfrak{a}_E)$. By Lemma 4.4.11, $\sigma(x)=x^{-1}I_2$ for every $x\in\mathbb{F}_p^\times$. After exchanging b,b' if needed, the following equalities hold:

$$\{x\in C\mid x\sigma(\iota(x))=I_2\}=bC,\quad\{x\in C\mid x\sigma(\iota^p(x))=I_2\}=b'C.$$

Let $\phi:C\to F^\times$ be one of the characters attached to C_f and ω be its order. It is enough to prove the following implication, by Proposition 5.3.4: if b,b' do not divide $\frac{p+1}{\omega}$, then there exists $\psi:C/\mathbb{F}_p^\times\to F^\times$ such that $\psi\circ\sigma\circ\iota=\overline{\phi}$ and $\psi\notin\{\phi,\phi^p\}$.

Since $\rho(I_p)=C$, $\sigma\circ\iota$ is an automorphism of C, so we need to show that $\overline{\phi}\notin\{\phi\circ\sigma\circ\iota,\phi\circ\sigma\circ\iota^p\}$.

Let (b_1, b_p) denote (b, b'), for any $j \in \{1, p\}$,

$$\overline{\phi} = \phi \circ \sigma \circ \iota^j \Leftrightarrow \phi\left(\{x\sigma(\iota^j(x)) \mid x \in C\}\right) = \{1\} \Leftrightarrow \phi\left(\frac{p^2-1}{b_j}C\right) = \{1\}$$
$$\Leftrightarrow \omega \mid \frac{p+1}{b_j}(p-1) \Leftrightarrow \omega \mid \frac{2(p+1)}{b_j},$$

whence the conclusion. □

5.4 Application to elliptic curves

The following result (which is independent from the setting defined at the beginning of the Chapter) comes essentially from [167, Proposition 1.13]. In view of Corollary 5.3.5, we have formulated it as a purely local result, because the image of the inertia group at p also affects the sign computation.

Lemma 5.4.1 *Let $p \geq 7$ be a prime. Let $E/\mathbb{Q}_p$ be an elliptic curve and $\rho : G_{\mathbb{Q}_p} \to \mathrm{GL}_2(\mathbb{F}_p)$ be a representation attached to the choice of a basis for $E[p]$ (in the sense of Proposition 1.4.10, that is, $\det \rho = \omega_p^{-1}$). Assume that ρ is a-Cartan. Then there exists a tamely ramified extension $L/\mathbb{Q}_p$ satisfying the following properties:*

- *The ramification index $e_{L/\mathbb{Q}_p}$ properly divides 12,*
- *E_L/L has good supersingular reduction,*
- *One of the reciprocity indices of ρ (see Lemma 4.4.11) divides $e_{L/\mathbb{Q}_p}$,*
- *$a \in \{1, 3\}$,*
- *If $a = 3$, then $p \equiv 2, 5 \pmod 9$ and the action of the inertia group I_p on $E[2]$ is cyclic with order 3.*

Proof. – If $j(E) \notin \mathbb{Z}_p$, by [141, Proposition 13], a subgroup of index two of $\rho(I_p)$ is contained in a nonsplit Cartan subgroup and in a subgroup conjugate to $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$. Therefore $\{I_2\}$ has index at most two in $\rho(I_p)$, so $2 \geq |\rho(I_p)| \geq 2(p-1)$, whence a contradiction. So $j(E) \in \mathbb{Z}_p$ and E has potentially good reduction at p by [153, Proposition VII.5.5]. By [146, Theorem 2, Corollary 2], the image of I_p in $\mathrm{Aut}(E[m])$ is a quotient of the tame inertia group and does not depend on the choice of an integer $m \geq 3$ coprime to p. In particular, said image is cyclic with cardinality e such that $\mathrm{GL}_2(\mathbb{F}_3)$ and $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ contain cyclic subgroups of cardinality e. This implies that $e \in \{1, 2, 3, 4, 6\}$.

Let $L/\mathbb{Q}_p$ be a finite extension such that I_L is exactly the subgroup of I_p of index e, which is the kernel of its action on $E[m]$ for every $m \geq 3$ coprime to p: so $L/\mathbb{Q}_p$ has ramification index e and is tamely ramified. By the Néron-Ogg-Shafarevich criterion [146, Theorem 1], E_L/L has good reduction. By [141, Proposition 11][5], if E_L/L has good ordinary reduction, then $\rho(I_L)$ is contained in a nonsplit Cartan subgroup and is conjugate to a subgroup of the form $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$, hence is trivial. Then $2(p-1) \leq |\rho(I_p)| \leq [I_p : I_L] = e \leq 6$, which is a contradiction.

Hence E_L/L has good supersingular reduction. We can then apply the discussion of [141, §1.10, §1.11 (2)]. Since ρ is tamely ramified, the denominators of the valuations of the elements of $E[p](\overline{\mathbb{Q}_p})$ are coprime to p; since $e \leq 6 < p$, the Newton polygon of the formal group attached to E_L is the line $(1, e) \to (p^2, 0)$, so, by Proposition 10 of *loc.cit.* (and taking into account the change of conventions with respect to Serre's) $\rho_{|I_L}$ is given by the $(-e)$-th power of a fundamental character of level two for L.

Let $D \leq \mathrm{GL}_2(\mathbb{F}_p)$ be a nonsplit Cartan subgroup with $\rho(I_p) = aD = \rho(G_F)$, where $F/\mathbb{Q}_p$ is the quadratic unramified extension, by Lemma 4.4.11. Let us fix an identification ι of D with

[5] Note that our convention for ρ is different than that of Serre.

$(\mathcal{O}_F/p)^\times$ preserving the trace and the norm. What we just wrote is that, after if necessary replacing ι with ι^p, $\rho_{|I_p}(z) = \iota(\mathfrak{a}_F(z))^{-1}$ for any $z \in I_L$, so one of the reciprocity indices of ρ divides e, so $a \in \{1,2,3,4,6\}$. Since a is odd, $a \in \{1,3\}$.

We proved in Lemma 4.4.11 that a was coprime to $\frac{p^2-1}{b}$ for any reciprocity index b of ρ, hence a is coprime to $\frac{p^2-1}{e}$. Thus, if $a = 3$, then $e \in \{3,6\}$, $a \mid \frac{p+1}{2}$ and $\frac{p^2-1}{e}$ is not divisible by 3. Therefore, $v_3(p+1) = 1$ so $p \equiv 2,5 \pmod 9$.

Since I_p/I_L is cyclic, the action of I_p on $E[2]$ is a cyclic quotient of $\mathbb{Z}/e\mathbb{Z}$ by a 2-group (since the group of automorphisms of $E[4]$ fixing $E[2]$ is a 2-group) and it embeds in $\mathrm{GL}_2(\mathbb{F}_2)$, so the action of I_p on $E[2]$ is cyclic with order 3. □

Next, we show that in most situations, the extension $K/\mathbb{Q}$ is inert at p.

Lemma 5.4.2 *Assume that $\rho_{|G_{\mathbb{Q}_p}}$ comes from an elliptic curve $E/\mathbb{Q}_p$ and that K is ramified. Then $p = 7$ and there exists a finite extension $L/\mathbb{Q}_p$ such that E_L/L has good ordinary reduction and $e_{L/\mathbb{Q}_p} \in \{3,6\}$.*

Proof. – If $p \equiv 1 \pmod 4$, by Lemma 5.2.1, ρ is $\frac{p+1}{2}$-Cartan. By Proposition 5.4.1, $\frac{p+1}{2} \leq a$, so $p \leq 7$. Since $p \equiv 1 \pmod 4$, one has $p = 5$, which we excluded. So we assume that $p \equiv 3 \pmod 4$: thus ρ is split and $\rho(G_{\mathbb{Q}_p} \cap G_K)$ is scalar.

If $j(E) \notin \mathbb{Z}_p$, then, by [141, Proposition 13], $\rho(I_p)$ is conjugate to a subgroup of $\pm \begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$. Since $\rho(I_p \cap G_K)$ is scalar, we see that $\rho(I_p \cap G_K) \subset \{\pm I_2\}$, hence $4 \geq |\rho(I_p)| = p-1$ by Proposition 4.4.7, a contradiction. As in the proof of Lemma 5.4.1, there is a finite extension $L/\mathbb{Q}_p$ with ramification index $e \in \{1,2,3,4,6\}$ such that E_L/L has good reduction.

If this reduction is supersingular, by the same argument as in the proof of Lemma 5.4.1, $\rho_{|I_L}$ agrees with $\left((\mathfrak{a}_F)_{|I_L}\right)^{-1} : I_L \to (\mathcal{O}_F/p)^\times$, where $F/\mathbb{Q}_p$ is the quadratic unramified extension. Thus $|\rho(I_L)| = \frac{p^2-1}{e}$, but $|\rho(I_L)| \leq |\rho(I_p)| = p-1$, so $e \geq p+1 \geq 8$, which is impossible.

Hence E_L/L has good ordinary reduction. By [141, Proposition 11], $\rho_{|I_L}$ is given by $\begin{pmatrix} 1 & * \\ 0 & \omega_p^{-1} \end{pmatrix}$. Therefore $\omega_p^{-1}(I_L \cap G_K) = \{1\}$, hence $p-1 \mid 2e$. Therefore $p = 7$ and $e \in \{3,6\}$. □

Lemma 5.4.3 *Assume that ρ comes from a elliptic curve $E/\mathbb{Q}$ with complex multiplication by K and that $p \neq 7$. Then $K/\mathbb{Q}$ is inert at p, and E acquires good reduction at p after a finite extension of $\mathbb{Q}_p$ with ramification index dividing 4 if $K = \mathbb{Q}(i)$, 6 if $K = \mathbb{Q}(j)$, 2 otherwise. In particular, unless $K = \mathbb{Q}(j)$, $\rho_{G_{\mathbb{Q}_p}}$ is 1-Cartan.*

Proof. – Let I_p be an inertia group at p. Since $p \neq 7$, Lemma 5.4.2 implies that $K/\mathbb{Q}$ is inert at p, so by Lemma 5.4.1 there is a finite extension $L/\mathbb{Q}_p$ with ramification index $e \in \{1,2,3,4,6\}$ such that e is the cardinality of the image of I_p on $E[m]$ for any $m \geq 3$ coprime to p, by [146, Theorem 2]. Our goal is to show that if $K \neq \mathbb{Q}(i)$ (resp. $K \neq \mathbb{Q}(j)$), then $e \mid 6$ (resp. $e \mid 4$).

If $K \neq \mathbb{Q}(i)$ (resp. $K \neq \mathbb{Q}(j)$), there is an odd prime $\ell \equiv 3 \pmod 4$ (resp. $\ell \equiv 2 \pmod 3$) which splits in K. The image J of I_p in $\mathrm{Aut}_{\mathbb{Z}_\ell}(\mathcal{T}_\ell E)$ is a cyclic group with cardinality e and commutes to the image in $\mathcal{M}_2(\mathbb{Z}_\ell)$ of the diagonalizable subgroup $\mathcal{O}_K \otimes \mathbb{Z}_\ell$, so $J = g \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} g^{-1}$ for some characters $\alpha, \beta : I_p \to \mathbb{Z}_\ell^\times$ and $g \in \mathrm{GL}_2(\mathbb{Z}_\ell)$. Thus J is cyclic of order e and embeds in the torsion subgroup of $(\mathbb{Z}_\ell^\times)^2$, which is isomorphic to $(\mathbb{F}_\ell^\times)^{\oplus 2}$. By comparing exponents, we see that $e \mid \ell - 1$, so $e \neq 4$ thus $e \mid 6$ (resp. e prime to 3 thus $e \mid 4$). □

Proposition 5.4.4 *Assume that $p > 7$ and $\rho_{|G_{\mathbb{Q}_p}}$ comes from an elliptic curve $E/\mathbb{Q}_p$. Then $K/\mathbb{Q}$ is inert at p, $\rho_{|G_{\mathbb{Q}_p}}$ is a-Cartan for some $a \in \{1,3\}$, and let $b \in \{1,2,3,4,6\}$ be its smallest reciprocity index (which is divisible by a) and let b' be the other reciprocity index. Let $(f, \mathbf{1}) \in \mathscr{C}_1'$ (resp. $(f, \mathbf{1}) \in \mathscr{C}_M$), let $\phi : C/\mathbb{F}_p^\times I_2 \to \mathbb{C}^\times$ be a character attached to C_f, and let ω be the order of ϕ. Let I (resp. $I/2$) be the number of $\psi \in \mathcal{I}_f/\sim$ such that the global root number of the compatible system $V_f \otimes \mathrm{Ind}_K^{\mathbb{Q}} \psi(\rho_K)$ is equal to $+1$. Then one has:*

- $I \in \{0, \min(a, 2)\}$,
- $I > 0$ *only if* $b \geq 3$ *and* $a\omega \mid p+1$,
- *When* $b = 4$, $I = 1$ *if and only if* $v_2(\omega) = v_2(p+1)$ *and* $(\omega, v_2(p+1)) \neq (4, 2)$.
- *When* $b = 3$, $I = 1$ *if and only if* $v_3(\omega) = v_3(p+1)$ *and* $(\omega, v_3(p+1)) \notin \{(3,1),(6,1)\}$.

Proof. – $K/\mathbb{Q}_p$ is inert at p by Lemma 5.4.2, so all the claims before the study case by case follow from Lemma 5.4.1 and Lemma 4.4.11. Let $F/\mathbb{Q}_p$ be the quadratic unramified extension and $\sigma : F^\times/(1+p\mathcal{O}_F) \to C$ be such that $\rho_{|W_F} = \sigma(\mathfrak{a}_F)$. We fix an isomorphism $\iota : C \to (\mathcal{O}_F/p)^\times$ preserving the trace and the norm such that $\{x \in C \, x\sigma(\iota(x)) = I_2\} = bC$. By definition, the image of $\sigma \circ \iota$ is aC (thus it contains $\mathbb{F}_p^\times I_2 = (p+1)C$), and, by Lemma 4.4.11, $\sigma(x) = x^{-1}I_2$ for every $x \in \mathbb{F}_p^\times$, so $x \in C/\mathbb{F}_p^\times I_2 \longmapsto x\sigma(\iota(x)) \in C$ is well-defined.

By Proposition 5.3.4, I is the number of characters $\psi \in \mathcal{I}_f$ such that $\psi \circ \sigma \circ \iota = \overline{\phi}$, because $z \longmapsto z^p$ is an involution of $\mathcal{I}_f$ without any fixed point. Let thus Φ be the set of $\psi : C/\mathbb{F}_p^\times I_2 \to \mathbb{C}^\times$ such that $\psi \circ \sigma \circ \iota = \overline{\phi}$.

If $\psi \in \Phi$, then ω divides the order of ψ, so $\psi^2 \neq 1$. Thus I is the difference of the cardinalities of Φ and of $\Phi \cap \{\phi, \phi^p\}$.

Now, Φ is nonempty if, and only if, $\ker\phi \supset \ker\sigma \circ \iota$. By definition, $\ker\phi = \omega C$, while $[C : \ker\sigma \circ \iota] = |(\sigma \circ \iota)(C)| = \frac{p^2-1}{a}$, so $\Phi \neq \varnothing$ if and only if $\omega C \supset \frac{p^2-1}{a}C$, if and only if $a\omega \mid p^2 - 1$.

Suppose that $a\omega \mid p^2 - 1$. One has $v_2(a\omega) = v_2(\omega) \leq v_2(p+1)$, $a \mid p+1$ is coprime to $p-1$ and $\omega \mid p+1$: write $\omega = 2^z\omega'$ for some odd ω', then a, ω' are odd and divide $p+1$, so they are coprime to $p-1$: hence $a\omega' \mid (p+1)(p-1)$ is coprime to $p-1$, therefore $a\omega' \mid p+1$, hence $a\omega \mid p+1$. The converse is obvious, so $\Phi \neq \varnothing$ if, and only if, $a\omega \mid p+1$.

When $a\omega \mid p+1$, $|\Phi|$ is the number of characters $\psi : C/\mathbb{F}_p^\times I_2 \to \mathbb{C}^\times$ such that $\ker\psi$ contains $\sigma(\iota(C)) = aC$. Therefore, $|\Phi| = a$. Since $\overline{\phi} \neq \overline{\phi}^p$, Φ does not contain both ϕ and ϕ^p, so $I \in \{|\Phi|, |\Phi| - 1\}$.

Now, since $\omega \mid p+1$ and $b \mid p+1$,

$$\begin{aligned}\phi \in \Phi &\Leftrightarrow \phi\left(\{x\sigma(\iota(x)) \mid x \in C\}\right) = \{1\} \Leftrightarrow \phi\left(\frac{p^2-1}{b}C\right) = \{1\} \\ &\Leftrightarrow \omega \mid \frac{p^2-1}{b} \Leftrightarrow \omega \mid \frac{2(p+1)}{b}.\end{aligned}$$

Let b' be the other reciprocity index of $\rho_{|G_{\mathbb{Q}_p}}$, so that $a \mid b'$ and the least common multiple of b and b' is $p+1$. Then, similarly,

$$\phi^p \in \Phi \Leftrightarrow \phi\left(\{x\sigma(\iota^p(x)) \mid x \in C\}\right) = \{1\} \Leftrightarrow \phi\left(\frac{p^2-1}{b'}C\right) = \{1\} \Leftrightarrow \omega \mid \frac{2(p+1)}{b'}.$$

If $a = 3$ and $I \neq 0$, then $|\Phi| = 3$ so $a\omega \mid p+1$. By Lemma 5.4.1, this implies that $v_3(p+1) = 1$ and $b \in \{3, 6\}$, so ω is coprime to 3 and ω divides $3\frac{2(p+1)}{b} = (p+1)\frac{6}{b}$, thus $\omega \mid \frac{2(p+1)}{b}$ and $\phi \in \Phi$. Hence $I = 2$.

So from now on we assume that $a = 1$, so that $a\omega \mid p+1$, thus $|\Phi| = 1$ and $I \in \{0, 1\}$. When $b \leq 2$, $b\omega \mid p+1$, so $\phi \in \Phi$ and $I = 0$.

There exists some integer t such that $\sigma(\iota(x)) = t \cdot x$ for all $x \in C$. Then $\frac{p^2-1}{b}$ (resp. $\frac{p^2-1}{b'}$) is the greatest common divisor of $p^2 - 1$ and $t + 1$ (resp. $p^2 - 1$ and $pt + 1$). Moreover, $a = 1$, so t is coprime to $p^2 - 1$.

When $b = 4$, note first that $p \equiv 3 \pmod 4$. Then $\phi \in \Phi$ if and only if $\omega \mid \frac{p+1}{2}$, which is equivalent to $v_2(\omega) < v_2(p+1)$. The least common multiple of b, b' is $p+1$, so $\frac{p+1}{4} \mid b'$ and $b' = p+1$ if $v_2(p+1) > 2$. Thus, when $v_2(p+1) > 2$, $I = 1$ if and only if $v_2(\omega) = v_2(p+1)$. When $v_2(p+1) = 2$, the greatest common divisor of $p^2 - 1$ and $t+1$ is $\frac{p^2-1}{4}$, so $v_2(t+1) = 1$, and $t \equiv 1 \pmod 4$. Thus $pt + 1$ and $p^2 - 1$ are divisible by 4, so their greatest common divisor

$\frac{p^2-1}{b'}$ is also divisible by 4, so $v_2(b') \leq 1$ and $b' \in \{\frac{p+1}{4}, \frac{p+1}{2}\}$. Therefore, the greatest common divisor of $\frac{2(p+1)}{b'}$ and $p+1$ is 4.

Therefore, $I = 1$ if and only if $v_2(\omega) = v_2(p+1)$ and $(\omega, v_2(p+1)) \neq (4,2)$.

When $b \in \{3,6\}$, note first that $p \equiv 2 \pmod 3$. Then $\phi \in \Phi$ if and only if $\omega \mid \frac{2(p+1)}{b}$, which is equivalent to $v_3(\omega) < v_3(p+1)$. Moreover, b' is divisible by $\frac{p+1}{b}$, so, if $\phi^p \in \Phi$, one has $v_3(\omega) = v_3(p+1)$ and $\omega \mid \frac{2(p+1)}{b'}$, so b' is coprime to 3 and $v_3(p+1) = v_3(b) = 1$.

Assume now that $v_3(\omega) = v_3(p+1) = 1$. Then $\frac{p^2-1}{b}$ (which is the greatest common divisor of $t+1$ and p^2-1) is coprime to 3, so $t \not\equiv -1 \pmod 3$. Since t is coprime to p^2-1, $t \equiv 1 \pmod 3$ and the greatest common divisor of $tp+1$ and p^2-1, which is $\frac{p^2-1}{b'}$, is divisible by 3. Hence b' is coprime to 3 and $b' \in \{\frac{p+1}{3}, \frac{p+1}{6}\}$. If $b' = \frac{p+1}{3}$, then $\frac{2(p+1)}{b'} = 6$. If $b' = \frac{p+1}{6}$, since $p+1$ is the least common multiple of b, b', $v_2(p+1) = v_2(b) \leq 1$, so $p \equiv 1 \pmod 4$, hence the greatest common divisor of $\frac{2(p+1)}{b'} = 12$ and $p+1$ is 6.

Therefore, $I = 1$ if and only if $v_3(\omega) = v_3(p+1)$ and $(\omega, v_3(p+1)) \notin \{(3,1),(6,1)\}$.

□

Corollary 5.4.5 *Assume that $p > 7$ and that $\rho_{|G_{\mathbb{Q}_p}}$ comes from an elliptic curve $E/\mathbb{Q}_p$ with good reduction at p up to quadratic twist. Then, in the decomposition of Proposition 5.2.5, all the given factors are irreducible and isomorphic to their Tate-twisted duals, and their global root numbers are all -1.*

Proof. – By Lemma 5.4.1, $\rho_{|G_{\mathbb{Q}_p}}$ is 1-Cartan and its smallest reciprocity index is at most 2. By Lemma 5.4.2, $K/\mathbb{Q}$ is inert at p, so, in the decomposition of Proposition 5.2.5, all the given factors are irreducible and isomorphic to their Tate-twisted duals. Indeed, the only possible exceptions are situations where $(f,\chi) \in \mathscr{S} \cup \mathscr{P}' \cup \mathscr{C}_1' \cup \mathscr{C}_M$ (resp. $(f,\mathbf{1}) \in \mathscr{C}_M$) and ψ is a character in $\mathcal{I}_f$ such that $\psi(\rho_K)^{p-1} = \{1\}$ (resp. $\psi(\rho_K)^2 \neq \{1\}$, $\psi(\rho_K)^4 = \{1\}$). But since $\rho_{|G_{\mathbb{Q}_p}}$ is 1-Cartan and $K/\mathbb{Q}$ is inert at p, $\rho(G_K) = C$, so this implies $\psi^{p-1} = \mathbf{1}$, which is impossible by definition of $\mathcal{I}_f$ (resp. $\psi^4 = \mathbf{1}$, which means that ψ is one of the characters attached to f, and this is impossible by Definition of $\mathcal{I}_f$).

The fact that all the global root numbers are -1 can be read off Table 5.1 for the factors of the form $V_f \otimes H_f(\rho)$, and off Proposition 5.4.4 for the factors of the form $V_f \otimes \mathrm{Ind}_K^{\mathbb{Q}} \psi(\rho_K)$. □

Remarks

(i) The main result of [101] is that when $p > 1.4 \cdot 10^7$, and ρ comes from an elliptic curve $E/\mathbb{Q}$ without complex multiplication, then $\rho(G_{\mathbb{Q}}) = N$. The bound has been improved to $p > 37$ in the preprint [58].

(ii) It is worth pointing out once again that if ρ comes from an elliptic curve $E/\mathbb{Q}$, then E defines a rational point on the modular curve $X_{ns}^+(p)$ (see for instance [44]). Whether such points with non-CM j-invariants exist for any $p > 13$ is an open question.

(iii) Proposition 5.4.4 suggests the following question: which divisors of $p+1$ arise as orders of ϕ_f for $(f,\mathbf{1}) \in \mathscr{C}_1'$? It seems possible to at least gather numerical evidence thanks to the work of Loeffler and Weinstein [109].

5.5 The Bloch-Kato conjecture for factors of the Tate module of $J_{\rho,\xi}(p)$

The goal of this section is to prove that the factors of the Tate module of $J_{\rho,\xi}(p)$ attached to non-CM modular forms satisfy some version of the Bloch-Kato conjecture in rank zero.

Lemma 5.5.1 *Let $(f,\chi) \in \mathscr{S} \cup \mathscr{C} \cup \mathscr{P}$, $\sigma \in G_{\mathbb{Q}}$ and χ be a primitive Dirichlet character. Assume that $(f',\chi') := (\sigma(f) \otimes \gamma, \sigma(\chi)\gamma^2) \in \mathscr{S} \cup \mathscr{P} \cup \mathscr{C}$. Then has $\gamma \in \mathcal{D}$ and the following holds:*

- *If $(f,\chi)\in\mathscr{S}$, then $\gamma=\mathbf{1}$ and $(f',\mathbf{1})\in\mathscr{S}$.*
- *If $(f,\chi)\in\mathscr{P}$, then $\gamma\in\{\mathbf{1},\sigma(\chi^{-1})\}$ and $(f',\sigma(\chi)\gamma^2)\in\mathscr{P}$.*
- *If $(f,\chi)\in\mathscr{C}$, then $(f',\gamma^2\sigma(\chi))\in\mathscr{C}$ and f' has complex multiplication if and only if f does.*

Proof. – This follows from Lemma 2.3.7 and Corollary C.3.10, as well as the definition of $\mathscr{C}$.□

Proposition 5.5.2 *For every $(f,\chi)\in\mathscr{S}\cup\mathscr{P}\cup\mathscr{C}$, let V_f denote the one-dimensional F-vector space on which N acts trivially and $\mathbb{T}$ acts thusly: T_n (resp. nI_2) acts by $a_n(f)$ (resp. $\chi(n)$). Let $(f,\chi)\in\mathscr{S}\cup\mathscr{P}\cup\mathscr{C}$.*

Let $\alpha\in H_f$. There is a prime ideal $I\subset\mathbb{T}_{1,N}(N)$ such that for any $(f',\chi')\in\mathscr{S}\cup\mathscr{P}\cup\mathscr{C}$:

- *for any $\alpha'\in H_{f'}$, $I\cdot(V_{f'}\otimes\alpha')$ is zero if, for some $\sigma\in G_{\mathbb{Q}}$ and $\gamma\in\mathcal{D}$, one has $(f',\alpha')=(\sigma(f)\otimes\gamma,\sigma(\alpha)\gamma(\det))$, and $V_{f'}\otimes\alpha'$ otherwise.*
- *for any $\psi\in\mathcal{I}_{f'}$, $I\cdot(V_{f'}\otimes_F\mathrm{Ind}_C^N\psi)=V_{f'}\otimes_F\mathrm{Ind}_C^N\psi$.*

Let $\psi\in\mathcal{I}_f$. There is a prime ideal $I\subset\mathbb{T}_{1,N}(N)$ such that for any $(f',\chi')\in\mathscr{S}\cup\mathscr{P}\cup\mathscr{C}$:

- *For any $\psi'\in\mathcal{I}_{f'}$, $I\cdot(V_{f'}\otimes_F\mathrm{Ind}_C^N\psi')=0$ if, for some $\sigma\in G_{\mathbb{Q}}$ and $\gamma\in\mathcal{D}$, one has $f'=\sigma(f)\otimes\gamma$ and $\psi'\sim\sigma(\psi)\gamma(\det)$. Otherwise, $I\cdot(V_{f'}\otimes_F\mathrm{Ind}_C^N\psi')=V_{f'}\otimes_F\mathrm{Ind}_C^N\psi'$.*
- *For any $\alpha\in H_{f'}$, $I\cdot(V_{f'}\otimes\alpha)=V_{f'}\otimes\alpha$.*

Proof. – *Step 1: Preliminaries.*

The space V_f is well-defined by (for instance) Corollary 2.5.5.

Let $(f',\chi')\in\mathscr{S}\cup\mathscr{P}\cup\mathscr{C}$. For $\alpha'\in H_{f'}$ (resp. $\psi'\in\mathcal{I}_{f'}$), let $M_{f',\alpha'}$ (resp. $M_{f',\psi'}$) denote the $(\mathbb{T}\otimes F)[N]$-module $V_{f'}\otimes\alpha'$ (resp. $V_{f'}\otimes\mathrm{Ind}_C^N\psi'$). Note that if $\psi_1,\psi_2\in\mathcal{I}_{f'}$ are such that $\psi_1\sim\psi_2$, then M_{f',ψ_1} and M_{f',ψ_2} are isomorphic as $\mathbb{T}[N]$-modules.

Let $\mathcal{M}$ be the collection of all the $M_{f',\alpha'}$ and $M_{f',\psi'}$ as above. Every $M\in\mathcal{M}$ is an absolutely irreducible $F[N]$-module. Therefore, by Schur's Lemma, $\mathbb{T}_{1,N}(N)$ (which is central in $\mathbb{T}[N]$) acts on M by a F-valued character, which we call in the rest of this proof the *central character*. Replacing M with $M\otimes_{F,\sigma}F$ (for $\sigma\in G_{\mathbb{Q}}$) means post-composing the central character with σ^{-1}.

Let $(f',\chi')\in\mathscr{S}\cup\mathscr{P}\cup\mathscr{C}$ and $\alpha'\in H_{f'}$ (resp. $\alpha'\in\mathcal{I}_{f'}$). It can be checked directly on generators that for every $\sigma\in G_{\mathbb{Q}}$ and every $g\in\mathbb{T}[N]$, $\mathrm{Tr}(g\mid M_{\sigma(f'),\sigma\circ\alpha'})=\sigma(\mathrm{Tr}(g\mid M_{f',\alpha'}))$. Therefore, the central character of $M_{\sigma(f'),\sigma(\alpha')}$ is the post-composition of that of $M_{f',\alpha'}$ with σ.

If in fact $(f',\chi')\in\mathscr{C}$ and $\gamma\in\mathcal{D}$, it can be checked on the generators that $M_{f'\otimes\gamma,\gamma(\det)\alpha'}$ and $M_{f',\alpha'}$ have the same traces for the actions of $\mathbb{T}_{1,N}$, so that they have the same central character.

Let now $\alpha\in H_f$ (resp. $\alpha\in\mathcal{I}_f$). Let $I_\alpha\subset\mathbb{T}_{1,N}(N)$ be the kernel of the central character of $M_{f,\alpha}$ (which is a ring homomorphism $\mathbb{T}_{1,N}(N)\to F$, so that I_α is a prime ideal). We will prove that, for any $M_{f',\alpha'}\in\mathcal{M}$, one of the following is true:

- There exists $(\sigma,\gamma)\in G_{\mathbb{Q}}\times\mathcal{D}$ such that $f'=\sigma(f)\otimes\gamma$ and $\alpha'=\sigma(\alpha)\gamma(\det)$ (resp. $\alpha'\sim\sigma(\alpha)\gamma(\det)$) . Then $I_\alpha M_{f',\alpha'}=0$,
- $IM_{f',\alpha'}=M_{f',\alpha'}$.

If this claim is true, this clearly finishes the proof. Moreover, the implication in first clause is straightforward, since, if $(f',\alpha')=(\sigma(f)\otimes\gamma,\sigma(\alpha)\gamma(\det))$ (resp. $f'=\sigma(f)\otimes\gamma$ and $\alpha'\sim\sigma(\alpha)\gamma(\det)$), the central character of $M_{f',\alpha'}$ is the post-composition with σ of the central character of $M_{f,\alpha}$. Since $IM_{f',\alpha'}$ is a $F[N]$-submodule of $M_{f',\alpha'}$, it is always $M_{f',\alpha'}$ or zero. Therefore, all that remains to prove is that if $I_\alpha M_{f',\alpha'}=0$ for $\alpha'\in H_{f'}\cup\mathcal{I}_{f'}$, then $\alpha'\in H_{f'}$ (resp. $\alpha'\in\mathcal{I}_{f'}$) and there exists $\sigma\in G_{\mathbb{Q}}$ and a Dirichlet character $\gamma\in\mathcal{D}$ such that $f'=\sigma(f)\otimes\gamma$ and $\alpha'=\sigma(\alpha)\gamma(\det)$ (resp. $\alpha'\sim\sigma(\alpha)\gamma(\det)$).

Thus, from now on, we assume that $(f',\chi')\in\mathscr{S}\cup\mathscr{P}\cup\mathscr{C}$ and $\alpha'\in H_{f'}\cup\mathcal{I}_{f'}$ and that $I_\alpha M_{f',\alpha'}=0$. If we need another generic element of $\mathscr{S}\cup\mathscr{P}\mathscr{C}$, we will denote it by (g,θ), and let $\beta\in H_g\cup\mathcal{I}_g$.

Step 2: $\alpha' \in H_{f'}$ (resp. $\alpha' \in \mathcal{I}_{f'}$).

Let $h \in C$ be a generator. Then h^{p-1} generates the cyclic group $C \cap \mathrm{SL}_2(\mathbb{F}_p)$. If $\beta \in H_g$, then we can check that in each case, $\beta(h^{p-1}) = 1$. Thus the element $h^{p-1} + h^{1-p} - 2 \in \mathbb{T}_{1,N}(N)$ annihilates $M_{g,\beta}$. Now, if $\beta \in \mathcal{I}_g$, $\beta(g^{p-1})$ is a $(p+1)$-th root of unity; it is distinct from 1 because $\beta^{p-1} \neq \mathbf{1}$ by the definitions. Then the action of $h^{p-1} + h^{1-p} - 2$ on $M_{g,\beta}$ is given by a nonzero algebraic integer.

Hence, if $\alpha \in H_f$, I_α contains $h^{p-1} + h^{1-p} - 2$, so $(h^{p-1} + h^{1-p} - 2)M_{f',\alpha'} = 0$, so $\alpha' \in H_{f'}$.

If $\alpha \in \mathcal{I}_f$, there is a monic polynomial $\Pi \in \mathbb{Z}[t]$ with $\Pi(0) \neq 0$ such that $\Pi(h^{1-p}+h^{p-1}-2) \in I_\alpha$, hence $\Pi(h^{1-p}+h^{p-1}-2)M_{f',\alpha'} = 0$. Therefore h^{p-1} does not act trivially on $M_{f',\alpha'}$, thus $\alpha' \in \mathcal{I}_{f'}$.

Step 3: We may assume that $f' = f$ and that $M_{f,\alpha'}$ has the same central character as $M_{f,\alpha}$.

$(\mathbb{T}_{1,N}(N) \otimes \mathbb{Q})/I_\alpha$ is a $\mathbb{Q}$-algebra. It embeds in F by two ring homomorphisms $\iota_{f,\alpha}$ and $\iota_{f',\alpha'}$ (given by the central characters of $M_{f,\alpha}$ and $M_{f',\alpha'}$): the images of $\iota_{f,\alpha}, \iota_{f',\alpha'}$ are sub-$\mathbb{Q}$-algebras of F, so they are fields. The morphism $\iota_{f',\alpha'} \circ \iota_{f,\alpha}^{-1} : \mathrm{im}\, \iota_{f,\alpha} \to \mathrm{im}\, \iota_{f',\alpha'}$ is an isomorphism, so it extends as an automorphism $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$. Thus the central character of $M_{f',\alpha'}$ is the post-composition with σ of the central character of $M_{f,\alpha}$. In particular, $M_{\sigma^{-1}(f'),\sigma^{-1}\circ\alpha'}$ has the same central character as $M_{f,\alpha}$, so $I_\alpha M_{\sigma^{-1}(f'),\sigma^{-1}\circ\alpha} = 0$.

By evaluating the central character, we see that for any $n \equiv 1 \pmod{p}$, $a_n(\sigma^{-1}(f')) = a_n(f)$, so, by Lemma 3.6.2, there exists a character $\gamma \in \mathcal{D}$ such that $f = \sigma^{-1}(f') \otimes \gamma$. Thus $M_{f,\sigma^{-1}(\alpha')\gamma(\det)}$ has the same central character as $M_{f,\alpha}$.

In this step, we assume that the problem is solved whenever $f = f'$ and $M_{f,\alpha}, M_{f',\alpha'}$ have the same central character. Therefore, there exists $\tau \in G_{\mathbb{Q}}$ such that $\tau(f) = f$ and $\sigma^{-1}(\alpha')\gamma(\det) = \tau(\alpha)$ (resp. $\sigma^{-1}(\alpha')\gamma(\det) \sim \tau(\alpha)$). Then one checks that $f' = \sigma(\tau(f)) \otimes \sigma(\gamma^{-1})$ and $\alpha' = \sigma(\tau(\alpha))\sigma(\gamma^{-1}(\det))$ (resp. $\alpha' \sim \sigma(\tau(\alpha))\sigma(\gamma^{-1}(\det))$), whence the conclusion.

Step 4: One has $\alpha' = \alpha$ (resp. $\alpha' \sim \alpha$).

We first assume that f has no complex multiplication.

It is enough to prove that for every $h \in N$, the trace of the action of h on the F-vector spaces $M_{f,\alpha'}$ and $M_{f,\alpha}$ is the same. By checking the definitions, characters of H_f are determined by their restrictions to C. Moreover, if $\psi \in \mathcal{I}_f$ and $h \in N$, then the action of h on $M_{f,\psi}$ is zero. So it is enough to check the equality for $h \in C$.

In this case, let q be a prime number such that $q \det h \equiv 1 \pmod{p}$, then $T_q(h+h^p) \in \mathbb{T}_{1,N}(N)$. Since $M_{f,\alpha}$ and $M_{f,\alpha'}$ have the same central character, one has $a_q(f)\alpha(h) = a_q(f)\alpha'(h)$ (resp. $a_q(f)(\alpha(h) + \alpha(h)^p) = a_q(f)(\alpha'(h) + \alpha'(h)^p)$). By a result of Serre [144, Cor. 2 au Théorème 15], we can choose q such that $a_q(f) \neq 0$, so $\mathrm{Tr}(h \mid M_{f,\alpha}) = \mathrm{Tr}(h \mid M_{f,\alpha'})$, and we are done.

When f has complex multiplication, H_f contains a single character, so we may assume that $\alpha, \alpha' \in \mathcal{I}_f$. By definition of $\sim$, it is enough to check that for any $h \in C$ with $\det h \in \mathbb{F}_p^{\times 2}$, $\mathrm{Tr}(h \mid M_{f,\alpha}) = \mathrm{Tr}(h \mid M_{f,\alpha'})$. For such an h, there exists an integer $n \geq 1$ such that $n^2 \det h = 1$, so that $(nI_2)(h + h^p) \in \mathbb{T}_{1,N}(N)$, and therefore $\chi(n)\mathrm{Tr}(h \mid M_{f,\alpha}) = \chi(n)\mathrm{Tr}(h \mid M_{f,\alpha'})$, whence the conclusion. □

Lemma 5.5.3 *Let $I \subset \mathbb{T}_{1,N}(\rho(G_{\mathbb{Q}}))$ (resp. $I \subset \mathbb{T}_{1,N}(N)$) be a subgroup. Then, for any $\xi \in \mu_p^\times(\overline{\mathbb{Q}})$, the abelian variety $A_I := J_{\rho,\xi}(p)/IJ_{\rho,\xi}(p)$ over $\mathbb{Q}$ is well-defined. Moreover, $(A_I)_{\overline{\mathbb{Q}}}$ is endowed with an action of $\mathbb{T}_{1,\rho(G_{\mathbb{Q}})}$ (resp. $\mathbb{T}_{1,N}$) which extends to an action of $\mathbb{T}_{1,\rho(G_{\mathbb{Q}}),\rho}$ (resp. $\mathbb{T}_{1,N,\rho}$) on $A_I(\overline{\mathbb{Q}})$. Finally, A_I only depends (up to $\mathbb{Q}$-isomorphism) on $I(\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_{\mathfrak{l}})$ for any maximal ideal $\mathfrak{l} \subset \mathcal{O}_F$ with residue characteristic ℓ.*

Proof. – Since $\mathbb{T}$ is a finitely generated abelian group, so is I. By Lemma 3.6.5, $\mathbb{T}_{1,N}(\rho(G_{\mathbb{Q}}))$ acts on $J_{\rho,\xi}(p)$. Hence $IJ_{\rho,\xi}(p)$ is an abelian subvariety of $J_{\rho,\xi}(p)$ by Proposition A.3.12, and the quotient A_I is well-defined with an exact sequence $0 \to I \cdot J_{\rho,\xi}(p)(\overline{\mathbb{Q}}) \to J_{\rho,\xi}(p)(\overline{\mathbb{Q}}) \to A_I(\overline{\mathbb{Q}}) \to 0$ by Proposition A.3.13.

The fact that $\mathbb{T}_{1,\rho(G_{\mathbb{Q}})}$ (resp. $\mathbb{T}_{1,N}$) acts on $(A_I)_{\overline{\mathbb{Q}}}$ comes from Lemma 3.6.5 and the fact that

I commutes to $\mathbb{T}_{1,\rho(G_{\mathbb{Q}})}$ (resp. $\mathbb{T}_{1,N}$). The relationship of this action to that of $G_{\mathbb{Q}}$ is given by Lemma 3.6.15.

If I' is another subgroup such that $I(\mathcal{T}_\ell J_{\rho,\xi}(p)\otimes_{\mathbb{Z}_\ell} F_{\mathfrak{l}}) = I'(\mathcal{T}_\ell J_{\rho,\xi}(p)\otimes_{\mathbb{Z}_\ell} F_{\mathfrak{l}})$, then, after replacing I' with $I+I'$, we may assume that $I\subset I'$. Then $IJ_{\rho,\xi}(p)\subset I'J_{\rho,\xi}(p)$ are Abelian subvarieties of $J_{\rho,\xi}(p)$ such that

$$\mathcal{T}_\ell IJ_{\rho,\xi}(p)\otimes_{\mathbb{Z}_\ell} F_{\mathfrak{l}} = I(\mathcal{T}_\ell J_{\rho,\xi}(p)\otimes_{\mathbb{Z}_\ell} F_{\mathfrak{l}}) = I'(\mathcal{T}_\ell IJ_{\rho,\xi}(p)\otimes_{\mathbb{Z}_\ell} F_{\mathfrak{l}}) = \mathcal{T}_\ell I'J_{\rho,\xi}(p)\otimes_{\mathbb{Z}_\ell} F_{\mathfrak{l}},$$

so that $IJ_{\rho,\xi}(p)$ and $I'J_{\rho,\xi}(p)$ have the same dimension. They are therefore equal. □

Corollary 5.5.4 *Let $\mathscr{E}=\mathscr{E}'=\mathscr{S}$ (resp. $(\mathscr{E},\mathscr{E}')=(\mathscr{P},\mathscr{P}')$, resp. $(\mathscr{E},\mathscr{E}')=(\mathscr{C}\backslash\mathscr{C}_M,\mathscr{C}'_1)$, resp. $\mathscr{E}=\mathscr{E}'=\mathscr{C}_M$). Let $\pi:\mathscr{E}\to\mathscr{E}'$ be the identity (resp. picking the representative modulo complex conjugation, resp. picking the representative modulo twists by characters in $\mathcal{D}$, resp. the identity). Let $(f,\chi)\in\mathscr{E}$ and $\alpha\in H_f$. There exists a prime ideal $I\subset\mathbb{T}_{1,N}(N)$ satisfying the following properties:*

- *The Abelian variety $A_I=J_{\rho,\xi}(p)/IJ_{\rho,\xi}(p)$ over $\mathbb{Q}$ is well-defined,*
- *A_I is endowed with an action of $\mathbb{T}_{1,N}$ over $\overline{\mathbb{Q}}$ which extends to an action of $\mathbb{T}_{1,N,\rho}$ on $A_I(\overline{\mathbb{Q}})$,*
- *For any maximal ideal $\mathfrak{l}\subset\mathcal{O}_F$ with residue characteristic ℓ, $\mathcal{T}_\ell A_I\otimes_{\mathbb{Z}_\ell}F_{\mathfrak{l}}$ is isomorphic to the restriction to $\mathbb{T}_{1,N,\rho}\otimes F_{\mathfrak{l}}$ of the $(\mathbb{T}\otimes F_{\mathfrak{l}})[N\rtimes_\rho G_{\mathbb{Q}}]$-module*

$$\prod_{\substack{(f',\chi')\in\mathscr{E}'\\ \alpha'\in H_{f'}}} V_{f',\mathfrak{l}}\otimes\alpha'(\rho),$$

  where T_n (resp. nI_2, resp. $M\in N$) acts on the factor $V_{f',\mathfrak{l}}\otimes\alpha'(\rho)$ by $a_n(f')$ (resp. $\chi'(n)$, resp. $\alpha'(M)$), and we only take the product over triples (f',χ',α') such that, for some $\sigma\in\mathrm{Aut}(F/\mathbb{Q})$ and some $\gamma\in\mathcal{D}$, one has $f'=\sigma(f)\otimes\gamma$ and $\alpha'=\sigma(\alpha)\gamma(\det)$. In particular, one has $(V_{f',\mathfrak{l}}\otimes\alpha'(\rho))_{\mathfrak{l}}=\sigma\left[(V_{f,\mathfrak{l}}\otimes\alpha(\rho))_{\mathfrak{l}}\right]$.
- *Let $\mathfrak{l}\subset\mathcal{O}_F$ be a maximal ideal, and consider the character $\mathbb{T}_{1,N}(N)\to F_{\mathfrak{l}}$ given by the action of $\mathbb{T}_{1,N}(N)$ on $V_{f,\mathfrak{l}}\otimes\alpha$. Then $\mathcal{T}_\ell A_I\otimes_{\mathbb{T}_{1,N}(N)}F_{\mathfrak{l}}\simeq V_{f,\mathfrak{l}}\otimes\alpha(\rho)$.*

Moreover, the abelian subvariety $IJ_{\rho,\xi}(p)$ (and therefore A_I) does not depend on the choice of I.

Proof. – Proposition 5.2.4 yields the structure of $\mathcal{T}_\ell J_{\rho,\xi}(p)\otimes_{\mathbb{Z}_\ell}F_{\mathfrak{l}}$ as a $\mathbb{T}_{1,N,\rho}$-module. The first two items are true for any subgroup $I\subset\mathbb{T}_{1,N}(N)$ by Lemma 5.5.3; a prime ideal I satisfying the third item is then given by Proposition 5.5.2.

Thus, only the fourth item needs to be checked. It amounts to checking the following assertion: let $\sigma\in G_{\mathbb{Q}},\sigma\in\mathcal{D}$, $(f',\chi')\in\mathscr{E}'$ and $\alpha'\in H_{f'}$ be such that $(f',\alpha')=(\sigma(f)\otimes\gamma,\sigma(\alpha')\gamma(\det)$ and such that $\mathbb{T}_{1,N}(N)$ acts on $V_{f,\mathfrak{l}}\otimes\alpha$ and $V_{f',\mathfrak{l}}\otimes\alpha'$ by the same $F_{\mathfrak{l}}$-valued character, and let us show that $(f,\alpha)=(f',\alpha')$.

Indeed, for any $n\equiv 1\pmod p$, T_n acts on the first module by $a_n(f)$ and by $a_n(f')$ on the second one, so one has $a_n(f)=a_n(f')$. By Lemma 3.6.2, f' is a twist of f. By construction of $\mathscr{E}'$, this implies that $f=f'$. Then $\alpha=\alpha'$ by Step 4 of the proof of Proposition 5.5.2. □

Proposition 5.5.5 *In the situation of Proposition 5.5.4, assume that $L(f\otimes\alpha(\rho),1)\neq 0$. Then for all (f',α') appearing in the product of the above Proposition, $L(f'\otimes\alpha'(\rho),1)\neq 0$. Moreover, for any prime q, the q-divisible Bloch-Kato Selmer group $\mathrm{Sel}(A_I,A[q^\infty])$ is finite, and this Selmer group is zero for all but finitely many q. In particular, $A_I(\mathbb{Q})$ is is finite.*

Proof. – The non-vanishing comes from the fact that the newforms attached to the $f'\otimes\alpha'(\rho)$ are Galois-conjugate to the newform attached to $f\otimes\alpha(\rho)$ (and these constructions define newforms by Proposition C.2.2), so we can apply [149, Theorem 1]. The result is then a consequence of [84, Theorem 14.2] and its CM analogue, proved in §15 of *loc.cit.*. □

Proposition 5.5.6 *Define $\widetilde{\rho} : (M, g) \in N \rtimes_\rho G_{\mathbb{Q}} \longmapsto N\rho(g)$ and $\widetilde{\rho_K} : \widetilde{\rho}^{-1}(C) \to C$. Let $\pi, \mathscr{E}, \mathscr{E}', (f, \chi)$ be as in Corollary 5.5.4. Let $\psi \in \mathcal{I}_f$. There exists a prime ideal $I \subset \mathbb{T}_{1,N}(N)$ satisfying the following properties:*

- *The Abelian variety $A_I = J_{\rho,\xi}(p)/IJ_{\rho,\xi}(p)$ over $\mathbb{Q}$ is well-defined,*
- *A_I is endowed with an action of $\mathbb{T}_{1,N}$ over $\overline{\mathbb{Q}}$ which extends to an action of $\mathbb{T}_{1,N,\rho}$ on $A_I(\overline{\mathbb{Q}})$,*
- *For any maximal ideal $\mathfrak{l} \subset \mathcal{O}_F$ with residue characteristic ℓ, $\mathcal{T}_\ell A_I \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ is isomorphic to the restriction to $\mathbb{T}_{1,N,\rho} \otimes F_\mathfrak{l}$ of the $(\mathbb{T} \otimes F_\mathfrak{l})[N \rtimes_\rho G_{\mathbb{Q}}]$-module*

$$\prod_{(f',\chi') \in \mathscr{E}', \psi' \in \mathcal{I}_{f'}/\sim} V_{f',\mathfrak{l}} \otimes \mathrm{Ind}_K^{\mathbb{Q}} \psi'(\widetilde{\rho}_K),$$

where:

- *we sum over triples (f', χ', ψ') such that there exists $\sigma \in \mathrm{Aut}(F/\mathbb{Q})$ and $\gamma \in \mathcal{D}$ such that $(f', \psi') = (\sigma(f) \otimes \gamma, \sigma(\psi) \otimes \gamma(\det))$. In particular, in such a situation, for any maximal ideal $\mathfrak{l}$ of $\mathcal{O}_F$, for all but finitely many prime numbers q,*

$$\mathrm{Tr}\left(\mathrm{Frob}_q \mid V_{f',\mathfrak{l}} \otimes \mathrm{Ind}_K^{\mathbb{Q}} \psi'(\rho_K)\right) = \sigma\left[\mathrm{Tr}\left(\mathrm{Frob}_q \mid V_{f,\mathfrak{l}} \otimes \mathrm{Ind}_K^{\mathbb{Q}} \psi(\rho_K)\right)\right].$$

- *T_n (resp. nI_2) acts on the factor $V_{f',\mathfrak{l}} \otimes \mathrm{Ind}_K^{\mathbb{Q}} \psi'(\widetilde{\rho}_K)$ by $a_n(f')$ (resp. $\chi'(n)$).*

- *Let $\mathfrak{l} \subset \mathcal{O}_F$ be a maximal ideal, and consider the character $\mathbb{T}_{1,N}(N) \to F_\mathfrak{l}$ given by the action of $\mathbb{T}_{1,N}(N)$ on $V_{f,\mathfrak{l}} \otimes \mathrm{Ind}_C^N \psi$. Then $\mathcal{T}_\ell A_I \otimes_{\mathbb{T}_{1,N}(N)} F_\mathfrak{l} \simeq V_{f,\mathfrak{l}} \otimes \mathrm{Ind}_C^N \psi(\rho_K)$.*

Moreover, the abelian subvariety $IJ_{\rho,\xi}(p)$ (and therefore A_I) does not depend on the choice of I.

Proof. – By mimicking the proof of Corollary 5.5.4, the only two statements to prove are that I is a prime ideal and the following: let $(f', \chi') \in \mathscr{E}'$, $\psi' \in \mathcal{I}_{f'}$, $\sigma \in G_{\mathbb{Q}}$ and $\gamma \in \mathcal{D}$, and assume that $(f', \psi') = (\sigma(f) \otimes \gamma, \sigma(\psi)\gamma(\det))$. Assume furthermore that $\mathbb{T}_{1,N}(N)$ acts by the same $F_\mathfrak{l}$-valued character on $V_{f,\mathfrak{l}} \otimes \mathrm{Ind}_C^N \psi$ and $V_{f',\mathfrak{l}} \otimes \mathrm{Ind}_C^N \psi'$. Then $f = f'$ and $\psi \sim \psi'$.

As in the proof of Corollary 5.5.4, by considering the action of T_n for $n \equiv 1 \pmod{p}$, we see that $a_n(f) = a_n(f')$, so by Lemma 3.6.2, f is a twist of f'. By Step 4 in the proof of Proposition 5.5.2, one has $\psi \sim \psi'$. □

Proposition 5.5.7 *Let us consider the situation of Proposition 5.5.6.*

(i) Assume that $\psi(\rho_K)^{p-1} \neq \mathbf{1}$. Then the Artin representation $\mathrm{Ind}_K^{\mathbb{Q}} \psi(\rho_K)$ is attached to a newform $g \in \mathcal{S}_1(\Gamma_1(D))$.

(ii) Assume moreover that $L(f \times g, 1) \neq 0$. Let $(\sigma, \gamma) \in G_{\mathbb{Q}} \times \mathcal{D}$ be such that

$$(f', \chi') = (\sigma(f) \otimes \gamma, \sigma(\chi)\gamma^2) \in \mathscr{E}'.$$

Let $\psi' = \sigma(\psi)\gamma(\det) \in \mathcal{I}_{f'}$. Then the Artin representation $\mathrm{Ind}_K^{\mathbb{Q}} \psi'(\rho_K)$ is attached to the newform $g' = \sigma(g) \otimes \gamma \in \mathcal{S}_1(\Gamma_1(D'))$, and one has $L(f' \otimes g', 1) \neq 0$.

(iii) Assume furthermore that f does not have complex multiplication and $K \neq \mathbb{Q}(\sqrt{-p})$. Let $\mathcal{Q}$ be a set of maximal ideals $\mathfrak{q} \subset \mathcal{O}_F$ with residue characteristic q satisfying the following conditions:

- *$q \nmid 6pD\delta$, where δ is the cardinality of the image of $\mathrm{Ind}_K^{\mathbb{Q}} \psi(\rho_K)(G_{\mathbb{Q}})$ in $\mathrm{PGL}_2(F)$.*
- *$\mathrm{Ind}_K^{\mathbb{Q}} \psi(\mathrm{Frob}_q)$ is not scalar,*
- *f is ordinary at $\mathfrak{q}$.*

Then, the set of prime numbers which are residue characteristics of some $\mathfrak{q} \in \mathcal{Q}$ has density $1 - \delta^{-1}$. Moreover, for all but finitely many $\mathfrak{q} \in \mathcal{Q}$, if $\mathfrak{q}_0$ denotes the inverse image of

$\mathfrak{q}$ under the character $\mathbb{T}_{1,N}(N) \to F_{\mathfrak{q}}$ attached to (f,ψ), the Bloch-Kato Selmer group $\mathrm{Sel}(\mathbb{Q}, A_I[\mathfrak{q}_0^\infty])$ is finite. In particular, $A_I(\mathbb{Q})$ is finite.

Remark There are several possible normalizations for the Rankin-Selberg L-function attached to two newforms f, g of weights $k \geq l$.

- The *imprimitive Rankin-Selberg L-function* $L^{imp}(f,g,s)$ is the meromorphic continuation of the series $\sum_{n\geq 1} a_n(f)a_n(g)n^{-s}$; it is denoted by $D(s,f,g)$ in [148].
- We define *Rankin-Selberg-Li L-function* by the construction of [103, §2]: more precisely, by Theorem 2.1 of *loc.cit.*, there is a primitive Dirichlet character γ such that the couple $(g\otimes\gamma, \overline{f}\otimes\gamma)$ satisfies the conditions (A), (B), (C) of *loc.cit.*, and the Rankin-Selberg-Li L-function attached to f, g is exactly the meromorphic continuation $L^{RSL}(f,g,s)$ of $s \longmapsto L_{g\otimes\gamma,\overline{f}\otimes\gamma}(s-\frac{k+l}{2}+1)\prod_{q|M'}\theta_q(s-\frac{k+l}{2}+1)^{-1}$ in the notation of *loc.cit.* (the shift in s is solely to ensure that the functional equations for $L^{imp}(f,g,s)$ and $L^{RSL}(f,g,s)$ are of the form $s \leftrightarrow k+l-1-s$).
- The *Rankin-Selberg L-function* is the meromorphic continuation $L(f\times g, s)$ of the Euler product $\prod_p L(D_{f,p}\otimes D_{g,p}, p^{-s})$.

The following Lemma proves that, for the purposes of Proposition 5.5.7, any of these L-functions works.

Lemma 5.5.9 *Let $f \in \mathcal{S}_k(\Gamma_1(A)), g \in \mathcal{S}_l(\Gamma_1(B))$ be two newforms with characters χ_f, χ_g and weights $k \geq l$ such that $\chi_f\chi_g$ is nontrivial. Let s be a complex number with $\mathrm{Re}\, s \geq \frac{k+l-1}{2}$. Then $L^{imp}(f,g,s), L^{RSL}(f,g,s), L(f\times g, s)$ are all defined, and they are either all zero, or all nonzero.*

Proof. – We first show that for any prime p, the series $\sum_{n\geq 0} a_{p^n}(f)a_{p^n}(g)p^{-ns}$ is absolutely convergent and its sum is nonzero. Indeed, we know that the following formal identities hold:

$$\sum_{n\geq 0} a_{p^n}(f)p^{-ns} = [(1-\alpha p^{-s})(1-\alpha' p^{-s})]^{-1}, \quad ,\sum_{n\geq 0} a_{p^n}(g)p^{-ns} = [(1-\beta p^{-s})(1-\beta' p^{-s})]^{-1}$$

where $\alpha, \alpha', \beta, \beta'$ are algebraic integers such that $|\alpha|, |\alpha'| \leq p^{\frac{k-1}{2}}$ and $|\beta|, |\beta'| \leq p^{\frac{l-1}{2}}$ by the Ramanujan conjecture. Then, by [148, Lemma 1], the following formal identity holds:

$$\sum_{n\geq 0} a_{p^n}(f)a_{p^n}(g)p^{-ns} = \frac{1-\alpha\alpha'\beta\beta' p^{-2s}}{(1-\alpha\beta p^{-s})(1-\alpha\beta' p^{-s})(1-\alpha'\beta p^{-s})(1-\alpha'\beta' p^{-s})}.$$

When $\Re s > \frac{k+l}{2} - 1$, $u \in \{\alpha, \alpha'\}$, $v \in \{\beta, \beta'\}$, one has $|uvp^{-s}| < p^{\frac{k+l-2}{2}} p^{-\frac{k+l}{2}+1} < 1$, so, in the right half-plane $\{\Re s > \frac{k+l}{2} - 1\}$, the previous formal identity holds in $\mathbb{C}$ and none of the factors in the right-hand side vanishes.

As a consequence, for any primitive Dirichlet character γ, the claim for the couple (f,g) and the couple $(f\otimes\gamma, g\otimes\overline{\gamma})$ are equivalent. Therefore, by [103, Theorem 2.1], we may assume that $(g, \overline{f})$ satisfies the conditions A), B), C) of *loc.cit.*.

It is well-known that $\frac{1}{\Gamma}$ extends to an entire function [100, Chapter XV, §2], and that, for any $s \in \mathbb{C}$ with $\Re s \geq 1$, $L(\chi_g\overline{\chi_f}, s) \neq 0$ (for instance by combining [78, Theorem 5.10] with the results of [123, Section VII.2]). By [103, Theorem 2.2] and the ensuing discussion, it is enough to show that, in the notation of *loc.cit.*, for any $s \in \mathbb{C}$ with $\Re s \geq \frac{1}{2}$, one has $\theta_q(s) \neq 0$. This is done by inspecting all cases with the help of Proposition C.2.1. □

Before coming back to Proposition 5.5.7, we discuss the cohomology of Abelian varieties over local fields. This material seems standard, but we spell it out for the sake of completeness.

Lemma 5.5.10 *Let A be an Abelian variety over a non-Archimedian local field K of characteristic zero. Let $A^\vee$ be the dual abelian variety.*

(i) Let $n \geq 1$. Local Tate duality and the Weil pairing induce a perfect pairing

$$H^1(\mathrm{Gal}(\overline{K}/K), A[n]) \times H^1(\mathrm{Gal}(\overline{K}/K), A^\vee[n]) \to \mathbb{Q}/\mathbb{Z}.$$

(ii) Let $n \geq 1$ and $H^1_\kappa(K, A[n])$ be the image of the Kummer map $A(K)/nA(K) \to H^1(K, A[n])$. Then $H^1_\kappa(K, A[n])$ and $H^1_\kappa(K, A^\vee[n])$ are orthogonal complements under local Tate duality.

(iii) Assume that q is a prime number distinct from the residue characteristic of K. Then, as $r \to \infty$, the length of the cokernel of

$$\mu_{A,r} : H^1(\mathrm{Gal}(K^{nr}/K), (\mathcal{T}_q A)(K^{nr})) \to H^1(\mathrm{Gal}(K^{nr}/K), A[q^r](K^{nr}))$$

is bounded. If A has good reduction, this cokernel is trivial.

(iv) Assume that q is a prime number distinct from the residue characteristic of K. Then, one has

$$\sup_{r \geq 1} \left[\mathrm{len}_{\mathbb{Z}_q} \left(\frac{H^1(\mathrm{Gal}(K^{nr}/K), A[q^r](K^{nr})) + H^1_\kappa(K, A[q^r])}{H^1(\mathrm{Gal}(K^{nr}/K), A[q^r](K^{nr})) \cap H^1_\kappa(K, A[q^r])} \right) \right] < \infty,$$

and this length is always zero when A has good reduction.

Proof. – (i) is a consequence of [118, §12, §16] and local Tate duality [124, Theorem 7.2.15]. For (ii), we show that $H^1_\kappa(K, A[n])$ and $H^1_\kappa(K, A^\vee[n])$ are orthogonal and that the product of their cardinalities is $|H^1(K, A[n])|$. Let g be the dimension of A. By the local Euler-Poincaré characteristic calculation [124, Theorem 7.3.1], the calculation of the degree of $A[n]$ [118, Theorem 8.2], and [120, Lemma I.3.3]

$$\begin{aligned} |H^1(K, A[n])| &= |H^0(K, A[n])||H^2(K, A[n])|\|n^{2g}\|_K^{-1} = |A[n](K)||A^\vee[n]|\|n^g\|_K^{-1}\|n^g\|_K^{-1} \\ &= |A(K)/nA(K)||A^\vee(K)/nA^\vee(K)| = |H^1_\kappa(K, A[n])||H^1_\kappa(K, A^\vee[n])| \end{aligned}$$

To prove that $H^1_\kappa(K, A[n])$ and $H^1_\kappa(K, A^\vee[n])$ are orthogonal to one another, we use the fact that the pairing $H^r(K, A(\overline{K})) \times H^{1-r}(K, A^\vee(\overline{K})) \to \mathbb{Q}/\mathbb{Z}$ (for $r = 0, 1$) of [120, Corollary I.3.4] is compatible with the local duality pairing.

We deal with (iii). When A has good reduction, the cokernel of $\mu_{A,r}$ is, by the Néron-Ogg-Shafarevich criterion [146, Theorem 1], exactly equal to

$$\mathrm{coker}\left[H^1(\mathrm{Gal}(K^{nr}/K), \mathcal{T}_q A) \to H^1(\mathrm{Gal}(K^{nr}/K), A[q^r])\right] \subset H^2(\mathrm{Gal}(K^{nr}/K), \mathcal{T}_q A).$$

Since $\mathrm{Gal}(K^{nr}/K) \simeq \hat{\mathbb{Z}}$ has cohomological dimension one, $\mu_{A,r}$ is trivial.

In general, let M', M, M_2 be the kernel, image, and cokernel of $(\mathcal{T}_q A)(K^{nr}) \to A[q^r](K^{nr})$. We have the following exact sequences:

$$\begin{aligned} H^1(\mathrm{Gal}(K^{nr}/K), (\mathcal{T}_q A)(K^{nr})) \to H^1(\mathrm{Gal}(K^{nr}/K), M) \to H^2(\mathrm{Gal}(K^{nr}/K), M'), \\ H^1(\mathrm{Gal}(K^{nr}/K), M) \to H^1(\mathrm{Gal}(K^{nr}/K), A[q^r](K^{nr})) \to H^1(\mathrm{Gal}(K^{nr}/K), M_2) \end{aligned}$$

which means that the length of the cokernel of $\mu_{A,r}$ is bounded by the sum of the lengths of $H^2(\mathrm{Gal}(K^{nr}/K), M') = 0$ and $H^1(\mathrm{Gal}(K^{nr}/K), M_2)$. By [164, Lemma 1], the length of the cokernel of $\mu_{A,r}$ is at most the length of M_2. Now, by the cohomology long exact sequence for the inertia group of K, M_2 injects into $H^1(\mathrm{Gal}(\overline{K}/K^{nr}), \mathcal{T}_q A)[q^r]$, so it is enough to prove that $H^1(\mathrm{Gal}(\overline{K}/K^{nr}), \mathcal{T}_q A)$ is a finitely generated $\mathbb{Z}_q$-module.

Let I_q be the pro-q-quotient of the tame inertia quotient of $\mathrm{Gal}(\overline{K}/K^{nr})$, corresponding to an extension K^{q-tr}. Then the kernel of $\mathrm{Gal}(\overline{K}/K^{nr}) \to I_q$ has supernatural order coprime to q, so, by the inflation-restriction exact sequence, $H^1(\mathrm{Gal}(\overline{K}/K^{nr}), \mathcal{T}_q A) \simeq H^1(I_q, (\mathcal{T}_q A)(K^{q-tr}))$. Since $I_q \simeq \mathbb{Z}_q$ is pro-cyclic, it is standard (the same argument as [164, Lemma 1] works) that $H^1(I_q, (\mathcal{T}_q A)(K^{q-tr}))$ is exactly the group of co-invariants of $(\mathcal{T}_q A)(K^{q-tr})$ under I_q. In particular, it is a subquotient of $\mathcal{T}_q A$ so is finitely generated, and we are done.

Now, we prove (iv). By [120, Proposition I.3.8], there is an injection

$$\frac{H^1(\mathrm{Gal}(K^{nr}/K), A[q^r](K^{nr}))}{H^1(\mathrm{Gal}(K^{nr}/K), A[q^r](K^{nr})) \cap H^1_\kappa(K, A[q^r])} \to H^1(\mathrm{Gal}(K^{nr}/K), A(K^{nr})) \simeq H^1(\mathrm{Gal}(K^{nr}/K), \pi_0),$$

where π_0 is the finite abelian group of geometric connected components of the special fibre of the Néron model of A. Thus

$$\sup_{r\geq 1}\left[\mathrm{len}_{\mathbb{Z}_q}\left(\frac{H^1(\mathrm{Gal}(K^{nr}/K), A[q^r](K^{nr}))}{H^1_\kappa(K, A[q^r]) \cap H^1(\mathrm{Gal}(K^{nr}/K), A[q^r](K^{nr}))}\right)\right] < \infty$$

and the same holds when A is replaced with $A^\vee$. By local Tate duality, the following modules have the same length,

$$\frac{H^1(\mathrm{Gal}(K^{nr}/K), A^\vee[q^r](K^{nr}))}{H^1_\kappa(K, A^\vee[q^r]) \cap H^1(\mathrm{Gal}(K^{nr}/K), A^\vee[q^r](K^{nr}))}, \quad \frac{H^1(\mathrm{Gal}(K^{nr}/K), A[q^r](K^{nr})) + H^1_\kappa(K, A[n])}{H^1(\mathrm{Gal}(K^{nr}/K), A[q^r](K^{nr}))},$$

which proves the claim in arbitrary reduction.

When A has good reduction, the Néron model of A is an Abelian scheme, so π_0 is the trivial group and $H^1(\mathrm{Gal}(K^{nr}/K), A[q^r](K^{nr})) \subset H^1_\kappa(K, A[q^r])$. By [164, Lemma 1] and [120, Lemma I.3.3], one has

$$H^1(\mathrm{Gal}(K^{nr}/K), A[q^r](K^{nr}))| = |A[q^r](K)| = |A(K)/q^r A(K)| = |H^1_\kappa(K, A[q^r])|,$$

and $H^1(\mathrm{Gal}(K^{nr}/K), A[q^r](K^{nr})) = H^1_\kappa(K, A[q^r])$.

□

We can now prove Proposition 5.5.7.

Proof. – (i): By Lemma 5.2.3, the Artin representation $\psi_\rho := \mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)$ is odd. By Proposition 5.2.5, ψ_ρ is irreducible, so it is attached to a newform $g \in \mathcal{S}_1(\Gamma_1(D))$.
(ii): The definition of ψ' shows that the representation $\mathrm{Ind}_K^{\mathbb{Q}}\psi'(\rho_K)$ is attached to the newform $g' := \sigma(g) \otimes \gamma \in \mathcal{S}_1(D')$. Since $\gamma \in \mathcal{D}$, $D' \mid Dp^2$ by Proposition C.2.2.

The compatible system of representations of $G_{\mathbb{Q}}$ attached to $f \otimes g$ (resp. $f' \otimes g'$) is given by $\left(V_{f,\mathfrak{l}} \otimes \mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)\right)_\mathfrak{l}$ (resp. $\sigma\left[\left(V_{f,\mathfrak{l}} \otimes \mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)\right)_\mathfrak{l}\right]$). Moreover, by Lemma 5.2.3, the product of the central characters of f and g is ϵ_K, so the imprimitive Rankin-Selberg L-series for $f \otimes g$ and $f' \otimes g'$ are, up to finitely many Euler factors (which are inconsequential by the proof of Lemma 5.5.9), conjugates by $G_{\mathbb{Q}}$. By Lemma 5.5.9, one has $L^{imp}(f \otimes g, 1) \neq 0$, so, by [148, Theorem 3], $L^{imp}(f' \otimes g', s) \neq 0$, and therefore $L(f' \otimes g', s) \neq 0$.

(iii): The goal is to apply the properties of the Beilinson-Flach Euler system constructed in [92]: we are essentially proving an analogue of Theorem 11.7.4, but the fact that we deal with a more general modular form rather than an elliptic curve makes the proof slightly more technical.

Step 1: Description of the Selmer conditions.

First, for definiteness, we make the Selmer condition explicit. The algebra $\mathbb{T}' := \mathbb{T}_{1,N}(N)/(I)$ is a subring of the ring of endomorphisms of A_I; by Proposition 5.5.6, $\mathbb{T}'$ is a domain and a finite free $\mathbb{Z}$-module. Thus, $\mathbb{T}' \otimes_{\mathbb{Z}} \mathbb{Z}_q$ is a finite reduced $\mathbb{Z}_q$-algebra without $\mathbb{Z}_q$-torsion. Since $\mathbb{Z}_q$ is Henselian, $\mathbb{T}' \otimes_{\mathbb{Z}} \mathbb{Z}_q$ is a finite product of local rings [4, Lemmas 04GG, 04GM], and the summands are exactly the $\widehat{\mathbb{T}'_{\mathfrak{q}'}}$, where $\mathfrak{q}'$ runs through ideals of $\mathbb{T}'$ dividing q.

Thus, any $(\mathbb{T}' \otimes_{\mathbb{Z}} \mathbb{Z}_q)$-module M is the direct sum of components that are $\widehat{\mathbb{T}'_{\mathfrak{q}'}}$-modules. We define $\mathcal{T}_{\mathfrak{q}_0}A_I, \mathcal{T}_{\mathfrak{q}_0}A_I^\vee$ as the $\widehat{\mathbb{T}'_{\mathfrak{q}_0}}$-components of $\mathcal{T}_qA_I, \mathcal{T}_qA_I^\vee$. If M is in fact a torsion $\mathbb{Z}_q$-module,

then the $\widehat{\mathbb{T}'_{\mathfrak{q}'}}$-component of M is exactly $M[(\mathfrak{q}')^\infty]$.

The Bloch-Kato condition at a place $v \neq q$ (resp. $v = q$) for $\mathcal{T}_{\mathfrak{q}_0} A_I$ is the *simple* (see [92, Definition 11.2.3]) local condition whose image in H^1 is given by the inverse image under the inclusion $H^1(\mathbb{Q}_v, \mathcal{T}_{\mathfrak{q}_0} A_I) \to H^1(\mathbb{Q}_v, \mathcal{T}_{\mathfrak{q}_0} A_I \otimes_{\mathbb{Z}_q} \mathbb{Q}_q)$ of the unramified classes (resp. the crystalline classes $H^1_f(\mathbb{Q}_v, \mathcal{T}_{\mathfrak{q}_0} A_I \otimes_{\mathbb{Z}_q} \mathbb{Q}_q)$ in the sense of [14, (3.7.2)] when $v = q$).

The Bloch-Kato condition at a place $v \neq q$ (resp. $v = q$) for $A_I[\mathfrak{q}_0^\infty]$ is the simple local condition whose image in H^1 is given by the image of the unramified (resp. crystalline) classes under the morphism $H^1(\mathbb{Q}_v, \mathcal{T}_{\mathfrak{q}_0} A_I \otimes_{\mathbb{Z}_q} \mathbb{Q}_q) \to H^1(\mathbb{Q}_v, \mathcal{T}_{\mathfrak{q}_0} A_I \otimes \mathbb{Q}_q/\mathbb{Z}_q) \simeq H^1(\mathbb{Q}_v, A_I[\mathfrak{q}_0^\infty])$.

We make the same definitions for the dual abelian variety $A_I^\vee$ of A_I, which is also endowed with an action of $\mathbb{T}'$. Now, since $A_I^\vee[\mathfrak{q}_0^\infty]$ is the (Tate-twisted) dual of $\mathcal{T}_{\mathfrak{q}_0} A_I$ by [118, §11, §16], local duality [14, Proposition 3.8][6] tells us that $H^1_f(\mathbb{Q}_v, A_I^\vee[\mathfrak{q}_0^\infty])$ and $H^1_f(\mathbb{Q}_v, \mathcal{T}_{\mathfrak{q}_0} A_I)$ are the orthogonal complements of each other.

Note that $H^1_f(\mathbb{Q}_q, A_I[\mathfrak{q}_0^\infty])$ is exactly the kernel of $H^1(\mathbb{Q}_q, A_I[\mathfrak{q}_0^\infty]) \to H^1(\mathbb{Q}_q, A_I(\overline{\mathbb{Q}_v}))$. Indeed, it is enough to prove the same result after replacing $\mathfrak{q}_0^\infty$ with q^∞, and this is exactly [14, Example 3.11].

After removing finitely many primes q, we may and do assume that $\mathbb{T}' \otimes \mathbb{Z}_{(q)}$ is a *regular* semi-local ring, so the same holds for $\mathbb{T}' \otimes \mathbb{Z}_q$. This implies by Proposition 5.5.6 that $\mathcal{T}_q A_I$ is a locally free $(\mathbb{T}' \otimes \mathbb{Z}_q)$-module of rank four, so by [4, Lemma 02M9] it is free of rank four.

Step 2: The Beilinson-Flach Euler system applies.

With the notation of [92, §11.2], our first step is to prove that the Nekovář cohomology group $\widetilde{H}^2(\mathbb{Z}[(6pDq)^{-1}], \mathcal{T}_{\mathfrak{q}_0} A_I; \Delta^{BK})$ is finite, where Δ^{BK} is the Bloch-Kato Selmer condition.

It is enough to show that $\widetilde{H}^2(\mathbb{Z}[(6pDq)^{-1}], \mathcal{T}_{\mathfrak{q}_0} A_I \otimes_{\widehat{\mathbb{T}'_{\mathfrak{q}_0}}} \mathcal{O}_{F_\mathfrak{q}}; \Delta^{BK})$ is finite. By Proposition 5.5.6, there is an injective $\mathcal{O}_{F_\mathfrak{q}}[G_\mathbb{Q}]$-homomorphism $\mathcal{T}_{\mathfrak{q}_0} A_I \otimes_{\widehat{\mathbb{T}'_{\mathfrak{q}_0}}} \mathcal{O}_{F_\mathfrak{q}} \to T_{f,\mathfrak{q}} \otimes_{\mathcal{O}_{F_\mathfrak{q}}} T_{g,\mathfrak{q}}$ with finite cokernel.

Therefore, by the long exact sequence of Nekovář cohomology, $\widetilde{H}^2(\mathbb{Z}[(6pDq)^{-1}], \mathcal{T}_{\mathfrak{q}_0} A_I; \Delta^{BK})$ is finite if, and only if, $\widetilde{H}^2(\mathbb{Z}[(6pDq)^{-1}], T_{f,\mathfrak{q}} \otimes_{\mathcal{O}_{F_\mathfrak{q}}} T_{g,\mathfrak{q}}; \Delta^{BK})$ is finite.

We are done if we can apply [92, Theorem 11.7.3] [7], but there are several issues:

(a) We need to check the assumptions of [92, Hypothesis 11.1.1].
(b) We need to check that Hyp(BI) [92, Hypothesis 11.1.2] is satisfied.
(c) We need to check Hyp(NEZ) [92, Hypothesis 11.1.4].

For (a), f and g are ordinary at $\mathfrak{q}$ and have weights 2 and 1 respectively. Moreover, $q \geq 5$ is coprime to the levels of f and g by definition. The newform f is q-distinguished by [92, Remark 7.2.7], and, since it does not have complex multiplication, after removing finitely many q, it is non-Eisenstein modulo $\mathfrak{q}$ by [133, Theorem 3.1]. If we furthermore assume that q does not divide $p-1$ times the cardinality of the image of $\mathrm{Ind}_K^\mathbb{Q} \psi(\rho_K)$ (this only removes a finite number of primes), then q does not divide the cardinality of the image of $G_\mathbb{Q}$ in $\mathrm{End}(T_{g,\mathfrak{q}})$, and therefore $T_{g,\mathfrak{q}}/\mathfrak{q}$ is irreducible, so that g is not Eisenstein at $\mathfrak{q}$.

Finally, suppose that g is not q-distinguished: then the two eigenvalues of Frob_q acting on $T_{g,\mathfrak{q}}$ agree modulo $\mathfrak{q}$. Let ζ be the quotient of the two eigenvalues of Frob_q. By definition of δ, ζ is a δ-th root of unity and we just assumed that $\zeta \equiv 1 \pmod{\mathfrak{q}}$. Since δ and q are coprime, $\zeta = 1$ and Frob_q acts on $T_{g,\mathfrak{q}}$ by a scalar, which contradicts our definition of $\mathcal{Q}$.

(c) is not an issue by the discussion below [92, Hypothesis 11.1.4]. That leaves (b). Because f has no complex multiplication, we can apply Proposition 6.3.6 (up to removing finitely many $\mathfrak{q}$): we only need to show that (after removing finitely many $\mathfrak{q}$, if necessary) there is a $\sigma \in G_\mathbb{Q}(\mu_{q^\infty})$ such that the co-invariants of $T_{f,\mathfrak{q}} \otimes_{\mathcal{O}_{F_\mathfrak{q}}} T_{g,\mathfrak{q}}$ under σ are free of rank one over $\mathcal{O}_{F_\mathfrak{q}}$. We wish to

[6] The authors of *loc.cit.* seem to omit this definition even though they are using it. This definition is from [137, Remark I.3.6].

[7] It seems that the statement contains a slight typo: the statement should be about $M_\mathcal{O}(f \otimes g)^*(\tau^{-1})$ rather than $M_\mathcal{O}(f \otimes g)(\tau^{-1})$

apply Proposition 6.3.8: because the character of g is the quadratic Dirichlet character attached to K, in this case, we need to check that K is not contained in the number field H defined in Section 6.3. By Lemma 2.3.7, either $(f,\mathbf{1})\in\mathscr{C}_1'$, or $K=\mathbb{Q}$. In the latter case, if α is a Dirichlet character such that $f\otimes\alpha$ is Galois-conjugate to f, then, by Proposition C.3.10, $\alpha\in\mathcal{D}$ and $\alpha^2=1$. Hence $H\subset\mathbb{Q}(\sqrt{-p})$ does not contain K. In Proposition 6.3.8, since the character of g has square $\mathbf{1}$, the first possibility is not satisfied. Therefore the element σ as stated exists.

Thus $\widetilde{H}^2(\mathbb{Z}[(6pDq)^{-1}],\mathcal{T}_{\mathfrak{q}_0}A_I,\Delta^{BK})$ is finite.

Therefore, by [92, Proposition 11.2.9], $\mathrm{Sel}(\mathbb{Q},A_I^\vee[\mathfrak{q}_0^\infty])$ is finite.

Step 3: Finiteness of $\mathrm{Sel}(\mathbb{Q},A_I[\mathfrak{q}_0^\infty])$.

Let $s\geq r\geq 0$, and consider the short exact sequence $0\to A_I^\vee[q^r]\to A_I^\vee[q^s]\overset{q^{r\vee}}{A}_I[q^{s-r}]\to 0$ of $G_{\mathbb{Q},qpD}$-modules. It induces a long exact sequence

$$0\to A_I^\vee[q^{s-r}](\mathbb{Q})/q^rA_I^\vee[q^s](\mathbb{Q})\to H^1(G_{\mathbb{Q},qpD},A_I^\vee[q^r])\to H^1(G_{\mathbb{Q},qpD},A_I^\vee[q^s]).$$

By the Mordell-Weil theorem, if we take $r\geq r_q$ and $s\geq s+r_q$ for some $r_q>0$, it implies that $\ker\left[H^1(G_{\mathbb{Q},pqD},A_I^\vee[q^r])\to H^1(G_{\mathbb{Q},pqD},A_I^\vee[q^\infty])\right]$ has bounded length as a $\mathbb{Z}_q$-module.

Therefore, by Lemma 5.5.10, the Selmer group $H^1_{\mathcal{L}}(G_{\mathbb{Q},pqD},A_I^\vee[q^r][\mathfrak{q}_0^\infty])$ has bounded length as a $\mathbb{Z}_q$-module as $r\to\infty$, where $\mathcal{L}$ denotes the following collection of local conditions:

- at places $v\neq q$, $\mathcal{L}_v$ is the set of unramified cohomology classes.
- at $v=q$, $\mathcal{L}_q$ is the projection to the $\mathfrak{q}_0$-component of the image of the Kummer map $A_I^\vee(\mathbb{Q}_q)/q^rA_I^\vee(\mathbb{Q}_q)\to H^1(\mathbb{Q}_q,A_I^\vee[q^r])$. That this local condition yields the result is a consequence of [14, Example 3.11].

We now apply the Greenberg-Wiles formula [124, Theorem 8.7.9] to the Galois module $A_I^\vee[q^r][\mathfrak{q}_0^\infty]$. By the Mordell-Weil theorem, [164, Lemma 1] and Lemma 5.5.10, it follows that for large enough r,

$$\frac{|H^1_{\mathcal{L}}(\mathbb{Q},A_I^\vee[q^r][\mathfrak{q}^\infty])|}{|H^1_{\mathcal{L}^\vee}(\mathbb{Q},A_I[q^r][\mathfrak{q}^\infty])|}=\frac{|A_I^\vee(\mathbb{Q})[\mathfrak{q}_0^\infty]||\left(A_I^\vee(\mathbb{Q}_q)/q^rA_I^\vee(\mathbb{Q}_q)\right)[\mathfrak{q}_0^\infty]|}{|A_I(\mathbb{Q})[\mathfrak{q}_0^\infty]||A_I^\vee(\mathbb{R})[q^r][\mathfrak{q}_0^\infty]|},$$

where $\mathcal{L}^\vee$ is defined exactly in the same way as $\mathcal{L}$, but after replacing $A_I^\vee$ with A_I.

We claim that

$$\ln|\left(A_I^\vee(\mathbb{Q}_q)/q^rA_I^\vee(\mathbb{Q}_q)\right)[\mathfrak{q}_0^\infty]|=2er\ln q+O(1),\ \ln|A_I^\vee(\mathbb{R})[q^r][\mathfrak{q}_0^\infty]|=2er\ln q+O(1),$$

where e is the dimension of $\mathbb{T}'/\mathfrak{q}_0$ as a $\mathbb{F}_q$-vector space.

By the theory of the q-adic exponential, there is a $\mathbb{T}'\otimes\mathbb{Z}_q$-submodule $M\subset A_I^\vee(\mathbb{Q}_q)$ such that $A_I^\vee(\mathbb{Q}_q)/M$ is finite and $M\otimes_{\mathbb{Z}_q}\mathbb{Q}_q\simeq T_0(A_I^\vee)_{\mathbb{Q}_q}$. Thus M is free of rank two over $\mathbb{T}'\otimes\mathbb{Z}_q$, which implies that $\ln|\left(A_I^\vee(\mathbb{Q}_q)/q^rA_I^\vee(\mathbb{Q}_q)\right)[\mathfrak{q}_0^\infty]|=O(1)+\ln|(M/q^rM)[\mathfrak{q}_0^\infty]|=2re+O(1)$.

Similarly, by the theory of real Lie groups, $A_I^\vee(\mathbb{R})$ is a compact Abelian Lie group, so there is an exact sequence $0\to\Lambda\overset{\exp}{\to}A_I^\vee(\mathbb{R})\to C\to 0$ of $\mathbb{T}'$-modules with C finite and $\Lambda\otimes\mathbb{Z}_q\simeq\mathcal{T}_qA_I^\vee(\mathbb{R})$ a free $(\mathbb{T}'\otimes\mathbb{Z}_q)$-module of rank two. Thus

$$\ln|A_I^\vee(\mathbb{R})[q^r][\mathfrak{q}_0^\infty]|=O(1)+\ln|(M/q^rM)[\mathfrak{q}_0^\infty]|=2re\ln q+O(1).$$

Therefore, $H^1_{\mathcal{L}^\vee}(\mathbb{Q},A_I[q^r][\mathfrak{q}_0^\infty])$ has bounded length as $r\to\infty$. By Lemma 5.5.10, we can replace the system of local conditions $\mathcal{L}^\vee$ at the finitely many places $v\neq q$ of bad reduction by the local condition "lies in the image of $A_I(\mathbb{Q}_v)$ under the local Kummer map". Hence $\mathrm{Sel}(\mathbb{Q},A_I[q^r])[\mathfrak{q}_0^\infty]$ has bounded length as $r\to\infty$, thus $\mathrm{Sel}(\mathbb{Q},A_I[q^\infty])[\mathfrak{q}_0^\infty]$ is finite.

Recall that the Kummer exact sequence yields an injection $A_I(\mathbb{Q})\otimes\mathbb{Q}_q/\mathbb{Z}_q\to\mathrm{Sel}(\mathbb{Q},A_I[q^\infty])$, so that $\left(A_I(\mathbb{Q})\otimes\mathbb{Q}_q/\mathbb{Z}_q\right)[\mathfrak{q}_0^\infty]$ is finite. Since this group is divisible, it is zero. Therefore the

finitely generated $\widehat{\mathbb{T}'_{\mathfrak{q}_0}}$-module $A_I(\mathbb{Q}) \otimes_{\mathbb{T}'} \widehat{\mathbb{T}'_{\mathfrak{q}_0}}$ is q-divisible, so it is zero. Since $\widehat{\mathbb{T}'_{\mathfrak{q}_0}}$ is flat over $\mathbb{T}'$, there is no injective homomorphism $\mathbb{T}' \to A_I(\mathbb{Q})$. Thus, by the Mordell-Weil theorem, $\mathrm{Ann}_{\mathbb{T}'}(A_I(\mathbb{Q}))$ is a nonzero ideal. Since $\mathbb{T}'$ is a domain, every proper quotient of $\mathbb{T}'$ is finite, hence $A_I(\mathbb{Q})$ is finite.

Step 4: Density estimate.

Since we considered all the primes in $\mathcal{Q}$ except for possibly finitely many, by Cebotarev's theorem, we need to prove that the set of residue characteristics of prime ideals at which f is ordinary has density one. Now, let $q \neq p$ be a prime number which is unramified in F and such that f is not ordinary at any prime ideal $\mathfrak{q} \subset \mathcal{O}_F$ with residue characteristic q. Then, for all $\mathfrak{q} \subset \mathcal{O}_F$ with residue characteristic q, $a_q(f) \in \mathfrak{q}\mathcal{O}_F$. Then $a_q(f) \in \cap_{\mathfrak{q}|q} \mathfrak{q}\mathcal{O}_F = q\mathcal{O}_F$. Every complex embedding of $a_q(f) \in \mathcal{O}_F$ has absolute value at most $2\sqrt{q}$, which implies that $a_q(f) = 0$. By Serre's result [144, Cor. 2 au Théorème 15], the set of prime numbers q such that $a_q(f) = 0$ has density zero, because f has no complex multiplication. □

Remark Even if we do not assume any longer that $L(f \times g, 1) \neq 0$, the results of Chapter 6 are sufficient to prove that Hyp(BI) [92, Hypothesis 11.1.2] holds. Using [92, Theorem 11.6.6], a similar argument to the proof of Proposition 5.5.7 shows that the rank of $A_I(\mathbb{Q})$ over $\mathbb{T}'$ is bounded above by the vanishing order of the q-adic Rankin-Selberg L-function.

Suppose now that ρ comes from an elliptic curve with good reduction at p. One could make the following heuristic reasoning:

(a) For "many" four-dimensional factors present in the decomposition of $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\lambda$, their complex L-function will vanish with order exactly one (since the sign of its functional equation is -1).
(b) Hence, for "many" of these factors, the corresponding q-adic Rankin-Selberg L-function will vanish at the central value with order one.
(c) Thus, a "large" quotient A of $J_{\rho,\xi}(p)$ will satisfy that $\mathrm{rk}\, A(\mathbb{Q}) \leq \frac{\dim A}{2}$.
(d) And therefore, one may apply the Chabauty-Coleman method (see [115] for an account, or the following sections for an application in rank zero) to $X_{\rho,\xi}(p)$ for the quotient A, thus determining all its rational points.

All of these steps, apart from (c) which we just discussed, seem to be difficult. For example, in positive rank, one cannot rule out as easily with the Chabauty-Coleman method the existence of a rational point in the residue disk of a cusp, in the way that this works in rank zero (see the following sections).

5.6 Reminder on the Chabauty-Coleman method

The goal of this section is to state and prove the result that we will need for the next section. It is worth noting that this construction is somewhat *ad hoc*. The so-called "tiny" integrals were generalized – and, in particular, given meaning across residue disks – by Coleman [29] in the abelian setting.

Definition 5.6.1 Let K be a non-Archimedean local field with residue field k and X be a proper $\mathcal{O}_K$-scheme. By the valuative criterion for properness [4, Lemma 0XB5], for any finite extension L/K, the natural morphism $\mathrm{Mor}_{\mathcal{O}_K}(\mathrm{Spec}\, \mathcal{O}_L, X) \to \mathrm{Mor}_K(\mathrm{Spec}\, L, X)$ is a bijection.

Let L/K be a finite extension and $\varpi \in \mathcal{O}_L$ be a uniformizer. Given a point $x \in X(L)$, x is the restriction of a point $x_0 \in X(\mathcal{O}_L)$. The *reduction* of x is the point $\mathrm{red}(x) \in X_k$ of the special fibre of X which is the image under x_0 of the unique closed point of $\mathrm{Spec}\, \mathcal{O}_L$. The point $\mathrm{red}(x)$ is also endowed with a morphism $\mathrm{Spec}\, \mathcal{O}_L/\varpi \to \mathrm{Spec}\, \kappa(\mathrm{red}(x))$; we will explicitly mention it when and how we need this additional data.

Given a closed point $x \in X_k$, its *residue disk* $]x[$ is the set of closed points $y \in X_K$ (in particular, $y \in X_K(\kappa(y))$, with $\kappa(y)/K$ a finite extension) such that $\mathrm{red}(y) = x$. If L/K is a finite extension, $\varpi \in \mathcal{O}_L$ is a uniformizer, and x is endowed with a morphism $\operatorname{Spec} \mathcal{O}_L/\varpi \to \operatorname{Spec} \kappa(x)$ of $\mathcal{O}_K$-schemes, we denote by $]x[(L)$ the set of L-points of X whose reduction (as $\operatorname{Spec} \mathcal{O}_L/\varpi$-points, as defined in the above paragraph) is x.

Lemma 5.6.2 *Let K be a finite extension of $\mathbb{Q}_p$ for some prime number p, and $\varpi \in \mathcal{O}_K$ be a uniformizer: write $k = \mathcal{O}_K/\varpi$. Let X be a $\mathcal{O}_K$-scheme of finite type and $x \in X_k$ be a closed point such that X is smooth of relative dimension d at x. Then $\mathcal{O}_{X,x}$ is a regular ring of dimension $d+1$, and there exists $t_1, \dots, t_d \in \mathcal{O}_{X,x}$ such that $(\varpi, t_1, \dots, t_d)$ generate its maximal ideal. Moreover,*

- *Let K' be the finite unramified extension of K with residue field $\kappa(x)$. There is a unique homomorphism of local $\mathcal{O}_K$-algebras $\mathcal{O}_{K'} \to \widehat{\mathcal{O}_{X,x}}$ inducing the identity on the residue fields, and it induces an isomorphism $\mathcal{O}_{K'}[[T_1, \dots, T_d]] \to \widehat{\mathcal{O}_{X,x}}$ (where T_i is mapped to t_i).*
- *Let L/K be a finite extension and $\varpi_L \in \mathcal{O}_L$ be a uniformizer. Fix a homomorphism $\psi : \operatorname{Spec} \mathcal{O}_L/\varpi_L \to \operatorname{Spec} \kappa(x)$ of $\mathcal{O}_K$-schemes: this defines a unique homomorphism of K-algebras $K' \to L$. Moreover, let H be the set of local homomorphisms of local $\mathcal{O}_K$-algebras $\mathcal{O}_{X,x} \to \mathcal{O}_L$ preserving ψ, then $f \in H \longmapsto (f(t_i))_{1 \le i \le d} \in (\varpi_L \mathcal{O}_L)^d$ is a bijection.*

Proof. – The statement is local: after replacing X with an open subscheme containing x, we may assume that X is a smooth affine $\mathcal{O}_K$-scheme of relative dimension d. This implies by [4, Lemma 07NF] that $\mathcal{O}(X)$ is a regular ring, hence $\mathcal{O}_{X,x}$ is a regular local ring. Moreover, by base change, if k denotes the residue field of $\mathcal{O}_K$, $X_k \to \operatorname{Spec} k$ is smooth of relative dimension d, so $\mathcal{O}(X) \otimes_{\mathcal{O}_K} k$ is a regular ring, hence $\mathcal{O}_{X,x}/(\varpi)$ is regular. Moreover, by [4, Lemma 0AFF], there exists a connected open subscheme $x \in U \subset X_k$ of dimension d; since U is regular, it is an integral scheme. By [106, Proposition 2.5.19], the function field of U has transcendence degree d. By the dimension formula [4, Lemma 02JU, Lemma 02JB], $\dim \mathcal{O}_{X,x}/(\varpi) = d$, whence $\dim \mathcal{O}_{X,x} = d+1$.

As a consequence, $\mathcal{O}_{X,x}$ is a regular local ring of dimension $d+1$, and by [106, Corollary 4.2.15], there are $t_1, \dots, t_d \in \mathfrak{m}_{X,x}$ such that $(\varpi, t_1, \dots, t_d)$ is a basis of $\mathfrak{m}_{X,x}/\mathfrak{m}_{X,x}^2$. By Nakayama, $(\varpi, t_1, \dots, t_d)$ generate $\mathfrak{m}_{X,x}$.

The residue field $\kappa(x)$ at x is the residue field of the closed point $x \in X_k$, where X_k is a finite type k-scheme, so that $\kappa(x)$ is a finite extension of k, whence $\kappa(x)$ is a finite field. Let K'/K be the finite unramified extension such that $\kappa(x)$ identifies with the residue field of K'. Then $\mathcal{O}_{K'}$ is an étale $\mathcal{O}_K$-algebra, so it is formally étale by [4, Lemma 04FF]. Therefore, for any $r \ge 1$, any homomorphism of $\mathcal{O}_K$-algebras $\mathcal{O}_{K'} \to \mathcal{O}_{X,x}/\mathfrak{m}_{X,x}^r$ lifts uniquely to a homomorphism of $\mathcal{O}_K$-algebras $\mathcal{O}_{K'} \to \mathcal{O}_{X,x}/\mathfrak{m}^{r+1}$. Hence there is a canonical homomorphism of $\mathcal{O}_K$-algebras $\mathcal{O}_{K'} \to \widehat{\mathcal{O}_{X,x}}$ which induces an isomorphism on the residue fields.

There is a natural homomorphism $f : \mathcal{O}_{K'}[T_1, \dots, T_d] \to \widehat{\mathcal{O}_{X,x}}$ mapping every T_i to t_i. It maps any element outside $(\varpi, T_1, \dots, T_d)$ to an element of $\mathcal{O}_{K'}^\times + \mathfrak{m}_{X,x}\widehat{\mathcal{O}_{X,x}} \subset \widehat{\mathcal{O}_{X,x}}^\times$, so f induces a morphism $f' : \mathcal{O}_{K'}[T_1, \dots, T_d]_{(\varpi, T_1, \dots, T_d)} \to \widehat{\mathcal{O}_{X,x}}$. Since $\mathfrak{m}_{X,x}$ is generated by $(\varpi, t_1, \dots, t_d)$, f' induces a surjection $\mathcal{O}_{K'}[T_1, \dots, T_d]/(\varpi, T_1, \dots, T_d)^n \to \mathcal{O}_{X,x}/\mathfrak{m}_{X,x}^n$ for any $n \ge 1$. By [4, Lemma 00NO], this surjection is between $\mathbb{Z}_p$-modules with the same finite length, so it is an isomorphism. Therefore f' is a completion.

Let L/K be a finite extension, $\varpi_L \in \mathcal{O}_L$ a uniformizer, and endow x with a morphism $\operatorname{Spec} \mathcal{O}_L/\varpi_L \xrightarrow{\psi} \operatorname{Spec} \kappa(x)$. The $\mathcal{O}_K$-algebra $\mathcal{O}_{K'}$ is formally étale, so the homomorphism $\kappa(x) \to \mathcal{O}_L/\varpi_L$ lifts uniquely to a $\mathcal{O}_K$-homomorphism $\mathcal{O}_{K'} \to \mathcal{O}_L$. By definition, H is the

set of commutative diagrams

$$\begin{array}{ccc} \mathcal{O}_{X,x} & \xrightarrow{y^\sharp} & \mathcal{O}_L \\ \downarrow & & \downarrow \\ \kappa(x) & \xrightarrow{\psi^\sharp} & \mathcal{O}_L/\varpi_L \end{array}$$

where $y^\sharp$ is a local homomorphism and the two vertical arrows are the reductions in the quotient field. Thus $f \in H \longmapsto \widehat{f} \in \mathrm{Hom}_{\mathcal{O}_{K'}}(\widehat{\mathcal{O}_{X,x}}, \mathcal{O}_L)$ is a bijection. Since $\widehat{\mathcal{O}_{X,x}}$ is a ring of formal power series in the variables $t_1, \ldots, t_d$, $f \in \mathrm{Hom}_{\mathcal{O}_{K'}}(\widehat{\mathcal{O}_{X,x}}, \mathcal{O}_L) \longmapsto (f(t_i))_{1\leq i\leq d} \in (\varpi_L \mathcal{O}_L)^d$ is a bijection, whence the conclusion. □

Definition 5.6.3 In the situation of Lemma 5.6.2, any $(t_1, \ldots, t_d)$ such that the maximal ideal of $\mathcal{O}_{X,x}$ is generated by $(\varpi, t_1, \ldots, t_d)$ is called *a system of parameters* for X at x.

Corollary 5.6.4 *Let K be a finite extension of $\mathbb{Q}_p$ with uniformizer ϖ and X be a proper $\mathcal{O}_K$-scheme. Let $x \in X$ be a closed point (in the special fibre of X) such that $X \to \mathrm{Spec}\,\mathcal{O}_K$ is smooth at x. Let $(t_1, \ldots, t_d)$ be a system of parameters at x, and fix a finite extension L/K with uniformizer ϖ_L and a homomorphism $\mathrm{Spec}\,\mathcal{O}_L/\varpi_L \to \mathrm{Spec}\,\kappa(x)$. Then*

$$y \in]x[\,(L) \longmapsto (y^\sharp(t_i))_{1\leq i\leq d} \in (\varpi_L \mathcal{O}_L)^d$$

is a bijection, where $y^\sharp$ is the ring homomorphism $\mathcal{O}_{X,x} \to \mathcal{O}_L$ given by the valuative criterion for properness and the definition of $]x[\,(L)$.

Proof. – This is an application of Lemma 5.6.2; the fact that $y \in]x[\,(L) \longmapsto y^\sharp \in H$ (with notation as in this Lemma) is a bijection is exactly the valuative criterion for properness. □

Lemma 5.6.5 *Let K be a finite extension of $\mathbb{Q}_p$ for some prime p. Let X be a $\mathcal{O}_K$-scheme of finite type and $x \in X$ be a closed point in the special fibre at which X is smooth of relative dimension e. Let $(t_1, \ldots, t_e)$ be a system of parameters at x. Then $\Omega^1_{X/\mathcal{O}_K,x}$ is a free $\mathcal{O}_{X,x}$-module of rank e with basis $dt_1, \ldots, dt_e$. Moreover, there is a unique continuous derivation $\hat{d} : \widehat{\mathcal{O}_{X,x}} \to \Omega^1_{X/\mathcal{O}_K,x} \otimes_{\mathcal{O}_{X,x}} \widehat{\mathcal{O}_{X,x}}$ extending $d : \mathcal{O}_{X,x} \to \Omega^1_{X/\mathcal{O}_K,x}$.*

If $\varpi \in \mathcal{O}_K$ is a uniformizer, for any $z_1, \ldots, z_e \in \widehat{\mathcal{O}_{X,x}}$ such that $(\varpi, z_1, \ldots, z_e)$ generate the maximal ideal of $\widehat{\mathcal{O}_{X,x}}$, the $\hat{d}z_1, \ldots, \hat{d}z_e$ form a basis of $\Omega^1_{X/\mathcal{O}_K,x} \otimes_{\mathcal{O}_{X,x}} \widehat{\mathcal{O}_{X,x}}$.

Proof. – There is a natural local homomorphism $\pi : \mathcal{O}_K[T_1, \ldots, T_e]_{(\varpi,T_1,\ldots,T_e)} \to \mathcal{O}_{X,x}$; by construction, the maximal ideal of $\mathcal{O}_{X,x}$ is generated by the image under π of the maximal ideal of $\mathcal{O}_K[T_1, \ldots, T_e]_{(\varpi,T_1,\ldots,T_e)}$. By Lemma 5.6.2, the completion $\mathcal{O}_K[T_1, \ldots, T_d]_{(\varpi,T_1,\ldots,T_d)} \to \widehat{\mathcal{O}_{X,x}}$ is finite free hence flat: since $\widehat{\mathcal{O}_{X,x}}$ is faithfully flat over $\mathcal{O}_{X,x}$ [4, Lemma 00MC], π is flat. The residue fields of the source and range of π are both finite, so the field extension induced by π on the residue fields is finite separable.

Let $U \subset X$ be a affine open subscheme containing x such that every t_i is contained in $\mathcal{O}_X(U)$: there is a morphism $f : U \to \mathbb{A}^e_{\mathcal{O}_K}$ of $\mathcal{O}_K$-schemes attached to $T_i \longmapsto t_i$. The morphism f is between affine $\mathcal{O}_K$-schemes of finite type, so it is of finite type, and it is étale at x by [4, Lemma 02GU (6)]: therefore, after reducing U if necessary, we may assume that f is étale. By [15, Proposition 2.5], the map $\Omega^1_{\mathbb{A}^e_{\mathcal{O}_K}/\mathcal{O}_K, 0_{\mathcal{O}_K/\varpi}} \otimes_{\mathcal{O}_K[T_1,\ldots,T_e]_{(\varpi,T_1,\ldots,T_e)}} \mathcal{O}_{X,x} \to \Omega^1_{X/\mathcal{O}_K,x}$ is an isomorphism: hence $\Omega^1_{X/\mathcal{O}_K,x}$ is free of rank e over $\mathcal{O}_{X,x}$ with basis $dt_1, \ldots, dt_e$.

By the product rule, $d(\mathfrak{m}^r_{X,x}\mathcal{O}_{X,x}) \subset \mathfrak{m}^{r-1}_{X,x}\Omega^1_{X/\mathcal{O}_K,x}$. So d extends to a continuous derivation $\hat{d} : \widehat{\mathcal{O}_{X,x}} \to \varprojlim \Omega^1_{X/\mathcal{O}_K,x}/\mathfrak{m}^r_{X,x}\Omega^1_{X/\mathcal{O}_K,x} \simeq \Omega^1_{X/\mathcal{O}_K,x} \otimes_{\mathcal{O}_{X,x}} \widehat{\mathcal{O}_{X,x}}$.

Now, let $z_1, \ldots, z_e \in \widehat{\mathcal{O}_{X,x}}$ be such that $(\varpi, z_1, \ldots, z_e)$ generates the maximal ideal of $\widehat{\mathcal{O}_{X,x}}$. To prove that $(\hat{d}z_1, \ldots, \hat{d}z_e)$ is a basis of the free $\widehat{\mathcal{O}_{X,x}}$-module (of rank e) $\Omega^1_{X/\mathcal{O}_K,x} \otimes_{\mathcal{O}_{X,x}} \widehat{\mathcal{O}_{X,x}}$, it is enough to prove that they form a basis of $\Omega^1_{X/\mathcal{O}_K,x}/\mathfrak{m}_{X,x}$ as a $\kappa(x)$-vector space of dimension

e. Indeed, if $z_i' \in \mathcal{O}_{X,x}$ has the same image in $\mathcal{O}_{X,x}/\mathfrak{m}_{X,x}^2$, then dz_i' and $\hat{d}z_i$ have the same image in $\Omega^1_{X/\mathcal{O}_K,x}/\mathfrak{m}_{X,x}$. Since $(\varpi, z_1, \dots, z_e)$ is a basis of $\mathfrak{m}_{X,x}\widehat{\mathcal{O}_{X,x}}/\mathfrak{m}_{X,x}^2\widehat{\mathcal{O}_{X,x}}$, so is $(\varpi, z_1', \dots, z_e')$; thus $(\varpi, z_1', \dots, z_e')$ is a basis of $\mathfrak{m}_{X,x}/\mathfrak{m}_{X,x}^2$, whence, by Nakayama, the z_i' form a system of parameters, and the dz_i form a basis of $\Omega^1_{X/\mathcal{O}_K,x}/\mathfrak{m}_{X,x}$, whence the conclusion. □

Corollary 5.6.6 *With the same notations as in Lemma 5.6.5, let $(t_1, \dots, t_e)$ be a system of parameters at x and K'/K be the finite unramified extension such that the residue field of K' is $\kappa(x)$. Let $P \in \mathcal{O}_{K'}[[T_1, \dots, T_e]]$, then $\hat{d}(P(t_1, \dots, t_e)) = \sum_{i=1}^e \frac{\partial P}{\partial T_i}(t_1, \dots, t_e)dt_i$.*

Proof. – When P is a scalar $\lambda \in \mathcal{O}_{K'}$ which is a root of unity, there is an irreducible polynomial, then $\lambda^{p^u-1} = 1$ for some $u \geq 1$, so $(p^u - 1)\hat{d}\lambda = 0$, so $\hat{d}\lambda = 0$. The same holds when P is a scalar $\lambda \in \mathcal{O}_K$. Therefore the result is true when P is constant. Moreover, the result is true when $P(T_1, \dots, T_d) = T_i$ for some $i \geq 0$. Therefore, by the product rule, the result is correct whenever P is a polynomial. By continuity, the result is correct. □

Definition 5.6.7 In the situation of Lemma 5.6.5, assume that $e = 1$, and let t be a parameter of X at x (i.e. $\mathfrak{m}_{X,x} = (\varpi, t)$). Let K'/K be the finite unramified extension such that the residue field of K' identifies with $\kappa(x)$. Let $M \subset \Omega^1_{X/\mathcal{O}_K,x}$ be a sub-$\mathcal{O}_K$-module. Then there exists a sub-$\mathcal{O}_K$-module $J \subset \mathcal{O}_{K'}[[T]]$ such that the image of M in $\Omega^1_{X/\mathcal{O}_K,x} \otimes_{\mathcal{O}_{X,x}} \widehat{\mathcal{O}_{X,x}}$ is $\{P(t)dt,\, P \in J\}$. The *ideal of first coefficients* $I \subset \mathcal{O}_K$ of M is the inverse image in $\mathcal{O}_K$ of the ideal of $\mathcal{O}_{K'}$ generated by the $P(0)$ for $P \in J$.

Lemma 5.6.8 *In the situation of Definition 5.6.7, the ideal of first coefficients does not depend on the choice of t. Moreover, if there is a finite extension L/K such that $X \to \operatorname{Spec}\mathcal{O}_K$ factors through a morphism $f : X \to \operatorname{Spec}\mathcal{O}_L$ which is smooth of relative dimension one at x, then L/K is unramified, so that $\Omega^1_{X/\mathcal{O}_K,x} \to \Omega^1_{X/\mathcal{O}_L,x}$ is an isomorphism, and the ideal of first coefficients of M for $X \to \operatorname{Spec}\mathcal{O}_L$ is generated by the ideal of first coefficients of M for $X \to \operatorname{Spec}\mathcal{O}_K$.*

Proof. – If $t' \in \mathcal{O}_{X,x}$ is another element such that (ϖ, t') generate $\mathfrak{m}_{X,x}$, then there is a $P \in T\mathcal{O}_{K'}[[T]]$ such that $P'(0) \in \mathcal{O}_{K'}^\times$ and the identity $t' = P(t)$ holds in $\widehat{\mathcal{O}_{X,x}}$. Let J_t (resp. $J_{t'}$) be the sub-$\mathcal{O}_K$-module of $\mathcal{O}_{K'}[[T]]$ attached to M and the parameter t (resp. t'). For any $Q \in \mathcal{O}_K[[T]]$, one has, in $\Omega^1_{X/\mathcal{O}_K,x} \otimes_{\mathcal{O}_{X,x}} \widehat{\mathcal{O}_{X,x}}$,

$$Q(t')dt' = Q(P(t))\hat{d}P(t) = (Q \circ P)(t)P'(t)dt = P'(t)(Q \circ P)(t)dt.$$

Thus $J_t = \{P'(T)Q(P(T)) \mid Q \in J_{t'}\}$. The conclusion follows since $P(0) = 0$ and $P'(0) \in \mathcal{O}_{K'}^\times$.

Suppose that $X \to \operatorname{Spec}\mathcal{O}_K$ factors through a morphism $f : X \to \operatorname{Spec}\mathcal{O}_L$ for some finite extension L/K such that f is smooth at x. Then after replacing X with an open subscheme, we may assume that $X \to \operatorname{Spec}\mathcal{O}_K$ and $X \to \operatorname{Spec}\mathcal{O}_L$ are smooth of relative dimension one. Since $x \in X$ lies in the special fibre for $X \to \operatorname{Spec}\mathcal{O}_K$, $p \notin \mathcal{O}_{X,x}^\times$, so $f(x)$ is the closed point $s \in \operatorname{Spec}\mathcal{O}_L$, thus f is smooth and surjective. By [4, Lemma 05B5], $\operatorname{Spec}\mathcal{O}_L \to \operatorname{Spec}\mathcal{O}_K$ is smooth. Since this morphism is étale at the generic point, it is smooth of relative dimension zero i.e. étale, and L/K is unramified.

We thus have an exact sequence $\Omega^1_{\mathcal{O}_L/\mathcal{O}_K,s} \otimes_{\mathcal{O}_L} \mathcal{O}_{X,x} \to \Omega^1_{X/\mathcal{O}_K,x} \to \Omega^1_{X/\mathcal{O}_L,x} \to 0$; since $\mathcal{O}_L$ is étale over $\mathcal{O}_K$, the natural map $\Omega^1_{X/\mathcal{O}_L,x} \to \Omega^1_{X/\mathcal{O}_K,x}$ is thus an isomorphism. In particular, J_K and J_L (with the same notation as in the beginning of the proof) are the same, and the ideal of first coefficients over K (resp. over L) is generated by ϖ^n, where n is the minimum of the valuations of the $P(0)$ for $P \in J_K$ (resp. $P \in J_L = J_K$), whence the conclusion. □

Lemma 5.6.9 *Let $f : X' \to X$ be a morphism of $\mathcal{O}_K$-schemes, and let $x' \in X'$ be a closed point of the closed fibre such that X' and X are smooth of relative dimension one over $\mathcal{O}_K$ at x' and $x = f(x)$ respectively. Assume that f is smooth at x'. Let $M \subset \Omega^1_{X/\mathcal{O}_K,x}$ be a sub-$\mathcal{O}_K$-module.*

Let $f^*M \subset \Omega^1_{X'/\mathcal{O}_K,x'}$ be the sub-$\mathcal{O}_K$-module made with the $(f^*\omega)_{x'}$. Then M and f^*M have the same ideal of first coefficients.

Proof. – Let $t \in \mathcal{O}_{X,x}$ be a parameter, it is enough to show that $f^\sharp(t) \in \mathcal{O}_{X',x'}$ is a parameter. Now, f is smooth at x', so f is smooth at x' of relative dimension zero, so f is étale at x'. Hence $\mathcal{O}_{X,x} \to \mathcal{O}_{X',x'}$ is unramified, whence the conclusion. □

Now, we turn to integration.

Lemma 5.6.10 *Let us keep the notations of Lemma 5.6.5, and let $\sum_{i=1}^e P_i(t_1,\dots,t_e)dt_i \in \operatorname{im}\hat{d}$. For any $1 \leq i,j \leq e$, one has $\frac{\partial P_i}{\partial T_j} = \frac{\partial P_j}{\partial T_i}$.*

Furthermore, if $P_1,\dots,P_e \in \mathcal{O}_K[[T_1,\dots,T_e]]$ are such that for any $1 \leq i,j \leq e$, $\frac{\partial P_i}{\partial T_j} = \frac{\partial P_j}{\partial T_i}$, then there exists a formal series $Q := \sum_{r\geq 1}\frac{1}{r}Q_r(T_1,\dots,T_e) \in K[[T_1,\dots,T_e]]$ such that:

- *for any $1 \leq i \leq e$, one has $P_i = \frac{\partial Q}{\partial T_i}$,*
- *for every $j \geq 1$, $Q_j \in \mathcal{O}_K[T_1,\dots,T_e]$ is a homogeneous polynomial of degree j,*
- *for any $R \in K[[T_1,\dots,T_e]]$ such that $\left(\frac{\partial R}{\partial T_i}\right)_{1\leq i\leq e} = (P_i)_{1\leq i\leq e}$, one has $R = Q + R(0)$.*

Proof. – That the image of $\hat{d}$ is contained in the $\mathcal{O}_{K'}$-submodule of $\sum_{i=1}^e P_i(t_1,\dots,t_e)dt_i$ as stated is a direct application of Corollary 5.6.6. Now, let $P_1,\dots,P_e \in \mathcal{O}_K[[T_1,\dots,T_e]]$ such that for any $1 \leq i,j \leq e$, $\frac{\partial P_i}{\partial T_j} = \frac{\partial P_j}{\partial T_i}$. For every $r \geq 0$, let P_i^r be the homogeneous component of P_i of degree r. Since $\frac{\partial}{\partial T_i}$ maps homogeneous polynomials of degree r to homogeneous polynomials of degree $r-1$, one has, for any $r \geq 0$ and any $1 \leq i,j \leq e$, $\frac{\partial P_i^r}{\partial T_j} = \frac{\partial P_j^r}{\partial T_i}$. Let, for every $r \geq 1$, $Q_r = \sum_{i=1}^e T_i P_i^{r-1}(T_1,\dots,T_e)$: then $Q_r \in \mathcal{O}_K[[T_1,\dots,T_e]]$is homogeneous of degree r, and one has

$$\frac{\partial Q_r}{\partial T_i} = P_i^{r-1} + \sum_{j=1}^e T_j \frac{\partial P_j^{r-1}}{\partial T_i} = P_i^{r-1} + \sum_{j=1}^e T_j \frac{\partial P_i^{r-1}}{\partial T_j} = P_i^{r-1} + (r-1)P_i^{r-1} = rP_i^{r-1}.$$

Thus $\frac{\partial Q}{\partial T_i} = P_i$ for every $1 \leq i \leq e$. Furthermore, if $R \in K[[T_1,\dots,T_e]]$ is such that $\frac{\partial R}{\partial T_i} = P_i$ for every $1 \leq i \leq e$, then every derivative of the formal power series $R - Q \in K[[T_1,\dots,T_e]]$ vanishes. Hence $R - Q$ is constant, whence the conclusion.

□

Proposition 5.6.11 *Let $K/\mathbb{Q}_p$ be a finite extension and X be a proper $\mathcal{O}_K$-scheme. Let $x \in X$ be a closed point in the special fibre such that X is smooth at x of relative dimension d. Let $(t_1,\dots,t_d)$ be a system of parameters at x. Let K'/K be the finite unramified extension whose residue field is $\kappa(x)$ and consider a finite extension L/K with uniformizer ϖ_L endowed with a field homomorphism $\kappa(x) \to \mathcal{O}_L/\varpi_L$. Let $\omega \in \Omega^1_{X/\mathcal{O}_K,x}$ be a* closed *differential and let $A,B \in]x[(L)$.*

We define the tiny integral *$\int_A^B \omega$ as follows: in $\Omega^1_{X/\mathcal{O}_K,x} \otimes_{\mathcal{O}_{X,x}} \widehat{\mathcal{O}_{X,x}}$, there is a decomposition $\omega = \sum_{i=1}^e P_i(t_1,\dots,t_d)dt_i$ for some $P_i \in \mathcal{O}_{K'}[[T_1,\dots,T_d]]$ such that $\frac{\partial P_i}{\partial T_j} = \frac{\partial P_j}{\partial T_i}$ for every $1 \leq i,j \leq d$. Let $Q \in K'[[T_1,\dots,T_d]]$ be as in Lemma 5.6.10, then*

$$\int_A^B \omega := Q(B^\sharp(t_1),\dots,B^\sharp(t_d)) - Q(A^\sharp(t_1),\dots,A^\sharp(t_d)).$$

This quantity is well-defined and does not depend on the choice of $(t_1,\dots,t_d)$ (or Q). In fact, the formula remains correct for any $t_1,\dots,t_d \in \mathfrak{m}_{X,x}\widehat{\mathcal{O}_{X,x}}$ for which $\omega = \sum_{i=1}^d F_i(t_1,\dots,t_d)\hat{dt}_i$ for some $F_i \in \mathcal{O}_{K'}[[T_1,\dots,T_d]]$ such that $\frac{\partial F_i}{\partial T_j} = \frac{\partial F_j}{\partial T_i}$.

Proof. – The differential $d : \Omega^1_{X/\mathcal{O}_K,x} \to \Omega^2_{X/\mathcal{O}_K,x}$ maps $\mathfrak{m}^r_{X,x}\Omega^1_{X/\mathcal{O}_K,x}$ into $\mathfrak{m}^{r-1}_{X,x}\Omega^2_{X/\mathcal{O}_K,x}$, so it extends to a differential $\Omega^1_{X/\mathcal{O}_K,x}\otimes_{\mathcal{O}_{X,x}}\widehat{\mathcal{O}_{X,x}} \to \Omega^2_{X/\mathcal{O}_K,x}\otimes_{\mathcal{O}_{X,x}}\widehat{\mathcal{O}_{X,x}} \simeq \Lambda^2_{\widehat{\mathcal{O}_{X,x}}}\left[\Omega^1_{X/\mathcal{O}_K,x}\otimes_{\mathcal{O}_{X,x}}\widehat{\mathcal{O}_{X,x}}\right]$; it also satisfies the product rule.

We can write $\omega = \sum_{i=1}^d a_i dt_i$ for all $1 \leq i \leq d$, where $a_i \in \mathcal{O}_{X,x}$. Therefore, one has $\sum_{i=1}^r da_i \wedge dt_i = 0$. We can write, in $\widehat{\mathcal{O}_{X,x}}$, $a_i = P_i(t_1, \ldots, t_d)$ for some $P_i \in \mathcal{O}_{K'}[[T_1, \ldots, T_d]]$, and the condition $\sum_{i=1}^r da_i \wedge dt_i = 0$ means that for any $1 \leq i, j \leq d$, one has $\frac{\partial P_i}{\partial T_j} = \frac{\partial P_j}{\partial T_i}$.

Let $Q = \sum_{r\geq 1}\frac{1}{r}Q_r(T_1, \ldots, T_d) \in K'[[T_1, \ldots, T_d]]$ be as in Lemma 5.6.10. Let L/K' be a finite extension with uniformizer ϖ_L, let us show that for any $b_1, \ldots, b_d \in \varpi_L\mathcal{O}_L$, $Q(b_1, \ldots, b_d)$ is well-defined. Indeed, one has $\|Q_r(b_1, \ldots, b_d)\|_L \leq \|\varpi_L\|_L^r$, while $\|r\|_L \geq \frac{1}{r^{[L:\mathbb{Q}_p]}}$. Thus, for any $r \geq 1$, $\|r^{-1}Q_r(b_1, \ldots, b_d)\|_L \leq \frac{\|\varpi_L\|_L^r}{r^{[L:\mathbb{Q}_p]}}$, and the right-hand side goes to zero, so the series $\sum_{r\geq 1}\frac{1}{r}Q_r(b_1, \ldots, b_d)$ converges in L.

Let $(t'_1, \ldots, t'_d)$ be another parameter system. There exists $V_1, \ldots, V_d \in \mathcal{O}_{K'}[[T_1, \ldots, T_d]]$ such that $t_i = V_i(t'_1, \ldots, t'_d)$: thus

$$\omega = \sum_{1\leq i,j\leq d} P_i(V_1, \ldots, V_d)(t'_1, \ldots, t'_d))\frac{\partial V_i}{\partial T_j}(t'_1, \ldots, t'_d)dt'_j.$$

Let $P'_j = \sum_{1\leq i\leq d} P_i(V_1, \ldots, V_d)\frac{\partial V_i}{\partial T_j} \in \mathcal{O}_{K'}[[T_1, \ldots, T_d]]$, then

$$\omega = \sum_{j=1}^d P'_i(t'_1, \ldots, t'_d)dt'_j.$$

The formal series $Q' := Q(V_1, \ldots, V_d) \in K'[[T_1, \ldots, T_d]]$ satisfies $\frac{\partial Q'}{\partial T_i} = P'_i$, so all we need to prove that, for any $A \in]x[(L)$,

$$Q'(A^\sharp(t'_1), \ldots, A^\sharp(t'_d)) = Q(A^\sharp(t_1), \ldots, A^\sharp(t_d)).$$

To prove this, we need to show the following:

(i) For any $1 \leq i \leq d$, $A^\sharp(t_i) = V_i(A^\sharp(t'_1), \ldots, A^\sharp(t'_d))$.
(ii) For any $x_1, \ldots, x_d \in \varpi_L\mathcal{O}_L$, for any $S \in \mathcal{O}_{K'}[T_1, \ldots, T_d]$, one has

$$[S \circ (V_1, \ldots, V_d)](x_1, \ldots, x_d) = S(V_1((x_i)_{1\leq i\leq d}), \ldots, V_d((x_i)_{1\leq i\leq d})).$$

(iii) For any $x_1, \ldots, x_d \in \varpi_L\mathcal{O}_L$, one has

$$\lim_{r\to\infty}\left[\sum_{r\geq 1}\frac{1}{r}[Q_r \circ (V_1, \ldots, V_d)](x_1, \ldots, x_d)\right] = Q'(x_1, \ldots, x_d).$$

(iv) For any $x_1, \ldots, x_d \in \varpi_L\mathcal{O}_L$, one has

$$\lim_{r\to\infty}\left[\sum_{r\geq 1}\frac{1}{r}[Q_r(A^\sharp(t_1), \ldots, A^\sharp(t_d))\right] = Q(x_1, \ldots, x_d).$$

(iv) was proved earlier. For (ii), the set of S such that the identity holds true is a subring of $\mathcal{O}_{K'}[T_1, \ldots, T_d]$ containing $\mathcal{O}_{K'}$ and every T_i, so it is all of $\mathcal{O}_{K'}[T_1, \ldots, T_d]$.

As to (i), fix some $r \geq 1$ and let $z \in \mathcal{O}^\times_{X,x}$ be such that its image in $\kappa(x)^\times$ is a generator of this multiplicative group. There is a polynomial $\Pi \in \mathcal{O}_K[Z, T_1, \ldots, T_d]$ such that

$V_i - \Pi \in (\varpi_K, T_1, \dots, T_d)^r$, with $\varpi_K \in \mathcal{O}_K$ a uniformizer: thus $t_i - \Pi(z, t'_1, \dots, t'_d) \in \mathfrak{m}^r_{X,x}$, hence $A^\sharp(t_i) - \Pi(A^\sharp(z), A^\sharp(t'_1), \dots, A^\sharp(t'_d)) \in \varpi_L^r \mathcal{O}_L$. The assumption on $V_i - \Pi$ implies that

$$\Pi(A^\sharp(z), A^\sharp(t'_1), \dots, A^\sharp(t'_d)) - V_i(A^\sharp(t'_1), \dots, A^\sharp(t'_d)) \in \varpi_L^r \mathcal{O}_L,$$

hence $A^\sharp(t_i) - V_i(A^\sharp(t'_1), \dots, A^\sharp(t'_d)) \in \varpi_L^r \mathcal{O}_L$. Since r was arbitrary, this completes the proof of (i).

Finally, let us prove (iii). By construction,

$$Q' = \sum_{r \geq 1} \frac{1}{r} Q_r \circ (V_1, \dots, V_d), \quad Q_r \circ (V_1, \dots, V_d) \in \frac{1}{r}(T_1, \dots, T_d)^r \mathcal{O}_{K'}[[T_1, \dots, T_d]].$$

Therefore, it is enough to show that

$$\left\| \frac{1}{r}[Q_r \circ (V_1, \dots, V_d)](x_1, \dots, x_d) \right\|_L \leq \frac{\|\varpi_L\|_L^r}{r^{[L:\mathbb{Q}_p]}},$$

because the right-hand side is summable as $r \to \infty$. Let $x'_i = V_i((x_j)_{1 \leq j \leq d}) \in \varpi_L \mathcal{O}_L$ for every $1 \leq i \leq d$. The series $Q_r \in \mathcal{O}_{K'}[[T_1, \dots, T_d]]$ is a homogeneous polynomial of degree r, hence

$$\|[Q_r \circ (V_1, \dots, V_d)](x_1, \dots, x_d)\| = \|Q_r(x'_1, \dots, x'_d)\| \leq \|\varpi_L\|_L^r,$$

and the bound follows.

The proof of the claim that the formula remains correct if $(t_i)_i$ is not assumed to be a parameter system is exactly the same. □

Proposition 5.6.12 *Let $K/\mathbb{Q}_p$ be a finite extension and X be a proper $\mathcal{O}_K$-scheme. Let $x \in X$ be a closed point in the special fibre such that X is smooth at x of relative dimension d. Let K'/K be the finite unramified extension whose residue field is $\kappa(x)$ and let L/K be a finite extension with uniformizer ϖ_L endowed with a field homomorphism $\kappa(x) \to \mathcal{O}_L/\varpi_L$. The following properties hold true:*

- *Additivity: if $A, B, C \in]x[(L)$ and $\omega \in \Omega^1_{X/\mathcal{O}_K,x}$ is closed, then $\int_A^C \omega = \int_A^B \omega + \int_B^C \omega$.*
- *Linearity: for any $A, B \in]x[(L)$, $\lambda, \lambda' \in \mathcal{O}_K$, for any closed 1-forms $\omega, \omega' \in \Omega^1_{X/\mathcal{O}_K,x}$, one has $\int_A^B \lambda\omega + \lambda'\omega' = \lambda \int_A^B \omega + \lambda' \int_A^B \omega'$.*
- *Continuity: if $A, B \in]x[(L)$, $\omega \in \mathfrak{m}^r_{X,x}\Omega^1_{X/\mathcal{O}_K,x}$ is closed, then $\| \int_A^B \omega\| \leq \|\varpi_L\|_L^{n(r)}$, where $n(r) \in \mathbb{Z}$ only depends on L and $n(r) \underset{r \to +\infty}{\longrightarrow} +\infty$.*
- *Fonctoriality in L: let L'/K be another finite extension with uniformizer $\varpi_{L'}$ endowed with a homomorphism $\kappa(x) \to \mathcal{O}_{L'}/\varpi_{L'}$ and let $\sigma : L \to L'$ be a field homomorphism respecting the given morphisms $\kappa(x) \to \mathcal{O}_L/\varpi_L, \kappa(x) \to \mathcal{O}_{L'}/\varpi_{L'}$. Then, for any $A, B \in]x[(L)$, $\sigma(A), \sigma(B) \in]x[(L')$ and, for any closed $\omega \in \Omega^1_{X/\mathcal{O}_K,x}$, one has $\sigma\left(\int_A^B \omega\right) = \int_{\sigma(A)}^{\sigma(B)} \omega$.*
- *Fonctoriality in X: let $f : X \to Y$ be a morphism of proper $\mathcal{O}_K$-schemes, and assume that Y is smooth at the point $y = f(x) \in Y$ (which is automatically closed and contained in the closed fibre). Let $\omega \in \Omega^1_{Y,y}$ be a closed differential and $A, B \in]x[(L)$. Then $f(A), f(B) \in]y[(L)$ (where $\kappa(y) \to \mathcal{O}_L/\varpi_L$ factors through $f^\sharp : \kappa(y) \to \kappa(x)$), $f^*\omega \in \Omega^1_{X,x}$ is closed, and $\int_A^B f^*\omega = \int_{f(A)}^{f(B)} \omega$.*
- *Base change: let $X' = X \times_{\mathcal{O}_K} \operatorname{Spec} \mathcal{O}_L$ and $f : X' \to X$ be the natural projection. The field homomorphism $\kappa(x) \to \mathcal{O}_L/\varpi_L$ defines a unique point $x'_0 \in X'(\mathcal{O}_L)$, and let $x' \in f^{-1}(\{x\})$ be the image of the closed point: x' is a closed point in the closed fibre of X', and X' is smooth over $\operatorname{Spec} \mathcal{O}_L$ at x. Let $A, B \in]x[(L)$ and $\omega \in \Omega^1_{X/\mathcal{O}_K,x}$ be closed, then A, B have*

unique lifts $A', B' \in]x'[(L)$, *and* $\int_A^B \omega = \int_{A'}^{B'} f^*\omega$.

Proof. – Mirroring the construction and proof in Proposition 5.6.11, this reduces to statements on formal power series. □

Corollary 5.6.13 *Consider the situation of Proposition 5.6.11 with* $d = 1$ *and* $e < p-1$, *where* e *is the ramification index of* $L/\mathbb{Q}_p$. *Suppose that there exists distinct* $A, B \in]x[(L)$ *such that* $\int_A^B \omega = 0$. *Then the ideal of first coefficients of* $\mathcal{O}_K \cdot \omega$ *is not* $\mathcal{O}_K$.

Proof. – Let t be a parameter for X at x: we can write $\omega = P(t)dt$ in $\Omega^1_{X/\mathcal{O}_K,x} \otimes_{\mathcal{O}_{X,x}} \widehat{\mathcal{O}_{X,x}}$ for some $P = \sum_{n\geq 0} c_n T^n \in \mathcal{O}_K[[t]]$. Let $a = A^\sharp(t), b = B^\sharp(t) \in \varpi_L \mathcal{O}_L$. Then $a \neq b$ by Corollary 5.6.4, and by assumption

$$c_0(a-b) = \sum_{n\geq 1} \frac{c_{n+1}}{n+1}(b^{n+1} - a^{n+1}).$$

Let us show for any $n \geq 2$, one has $\left\|\frac{a^n - b^n}{n}\right\|_L < \|a-b\|_L$. Since $p \neq 2$, the statement is true for $n = 2$, so we may assume $n \geq 3$. We need to prove that $\left\|\sum_{i=0}^{n-1} a^i b^{n-1-i}\right\|_L < \|n\|_L$. It is enough to check that $v_L(n) < n-1$, where v_L is the valuation on L normalized so that $v_L(L^\times) = \mathbb{Z}$. Let $q = p^r$ be the greatest power of p which is not greater than n. Then $v_L(n) < (p-1)v_p(n) \leq (p-1)r \leq (1+(p-1)r) - 1 \leq (1+(p-1))^r - 1 \leq n-1$, whence the conclusion.

In particular, $\|c_0(b-a)\|_L = \left\|\sum_{n\geq 1} \frac{c_{n+1}}{n+1}(b^{n+1} - a^{n+1})\right\|_L < \|b-a\|_L$, whence $v_L(c_0) > 0$. □

Proposition 5.6.14 *Let* $K/\mathbb{Q}_p$ *be a finite extension with residue field* k *and* A *be an Abelian scheme over* $\mathcal{O}_K$. *Let* 0_k *(resp.* 0_K*) be the unit point in the special fibre (resp. the generic fibre) of* A. *Let* $\omega \in H^0(A, \Omega^1)$, *and let* L/K *be a finite extension. Then* ω *is closed,* $]0_k[(L)$ *is a finite index subgroup of* $A(L)$, *and* $P \in]0_k[(L) \longmapsto \int_{0_K}^P \omega_{0_k} \in L$ *is a group homomorphism.*

Proof. – Let $\varpi_L \in \mathcal{O}_L$ be a group homomorphism. The reduction map is functorial with respect to proper $\mathcal{O}_K$-schemes, so red : $A(L) \to A(\mathcal{O}_L/\varpi_L)$ is a group homomorphism. Since $]0_k[(L) = \mathrm{red}^{-1}(\{0_k\})$ by definition, $]0_k[(L)$ is a subgroup of $A(L)$, and $A(L)/]0_k[(L)$ injects in $A_k(\mathcal{O}_L/\varpi_L)$. Since $\mathcal{O}_L/\varpi_L$ is a finite extension of the finite field k, $A_k(\mathcal{O}_L/\varpi_L)$ is finite, hence so is $A(L)/]0_k[(L)$.

Note that $H^0(A, \Omega^1_{A/\mathcal{O}_K})$ embeds in $H^0(A_K, \Omega^1_{A_K/K})$ and is made of translation-invariant differentials by Proposition A.4.33. Hence the differential ω is closed by Proposition A.3.22. By additivity, we have to show that for any $P, Q \in]0_k[(L)$, $\int_0^Q \omega = \int_P^{P+Q} \omega$. By base change, we may assume that $L = K$. Let $\tau : X \in A \longmapsto X + P \in A$ be the translation. Then $\int_0^Q \omega = \int_0^Q \tau^*\omega = \int_{\tau(0)}^{\tau(Q)} \omega = \int_P^{P+Q} \omega$, whence the conclusion. □

The following result is the goal of the section. It is a version of Mazur's *formal immersion argument*, first described in the proof of [112, Corollary 4.3], and then an important fixture in the determination of rational points on modular curves. Our formulation is perhaps less geometric, with its emphasis on differentials satisfying a *rational* condition (as opposed to an *integral* one), but it is convenient one for the purposes of the next section.

Proposition 5.6.15 *Let* A *be an Abelian scheme over* $\mathbb{Z}_p$ *for some odd prime* p, X *be a smooth proper* $\mathbb{Z}_p$*-scheme of relative dimension one, and* $f : X \to A$ *be a morphism of* $\mathbb{Z}_p$*-schemes. Let* $x_0 \in X(\mathbb{Z}_p)$ *be such that* $f(x_0) = 0_A$ *and* $x \in X$ *be the image under* x_0 *of the closed point of* $\operatorname{Spec} \mathbb{Z}_p$. *Let* $M \subset \Omega^1_{X/\mathbb{Z}_p,x}$ *be the set of stalks of differentials* $\omega \in H^0(X, \Omega^1)$ *such that* $\omega = f^*\omega_1$ *for some* $\omega_1 \in H^0(A_{\mathbb{Q}_p}, \Omega^1)$.

Assume that the ideal of first coefficients of M *is* $\mathbb{Z}_p$. *Then* $f :]x[(\mathbb{Q}_p) \to A(\mathbb{Q}_p) \otimes \mathbb{Q}$ *is injective. In particular,* $\{x_0\} =]x[(\mathbb{Q}_p) \cap f^{-1}(A(\mathbb{Q}_p)_{tors})$.

Proof. – Let $y, y' \in]x[(\mathbb{Q}_p)$ and $d \geq 1$ be such that $d(f(y) - f(y')) = 0$. Let $\omega \in M$ be such that the ideal of first coefficients of $\mathbb{Z}_p \cdot \omega$ is $\mathbb{Z}_p$: there exists $n \geq 1$ and $\omega_1 \in H^0(A, \Omega^1)$ such that $p^n\omega = (f^*\omega_1)_x$. Then

$$\int_y^{y'} \omega = p^{-n} \int_{f(y)}^{f(y')} \omega_1 = p^{-n} \left(\int_0^{f(y')} \omega_1 - \int_0^{f(y)} \omega_1 \right) = p^{-n} \int_0^{f(y')-f(y)} \omega_1$$
$$= \frac{1}{p^n d} \int_0^{d(f(y')-f(y))} \omega_1 = \frac{1}{p^n d} \int_0^0 \omega_1 = 0.$$

This contradicts Corollary 5.6.13. □

Proposition 5.6.16 *Let A be an abelian variety over $\mathbb{Q}$ with good reduction at an odd prime p, X be a smooth proper $\mathbb{Z}_{(p)}$-scheme of relative dimension one. Let $\mathcal{A}$ be the Néron model of A over $\mathbb{Z}_{(p)}$. Let $f : X_{\mathbb{Q}} \to A$ be a scheme morphism and $P \in X(\mathbb{Q}_p)$ be such that $f(P) = 0_A$. Then P lifts to some $P_0 \in X(\mathbb{Z}_p)$. Let $x \in X$ be the image under P_0 of the closed point of* $\operatorname{Spec} \mathbb{Z}_p$.

Suppose that $A(\mathbb{Q})$ is finite and that some $Q \in X(\mathbb{Q})$ distinct from P specializes to x. Then, for every $\omega \in H^0(X, \Omega^1_{X/\mathbb{Z}_{(p)}}) \cap f^*H^0(A, \Omega^1_{A/\mathbb{Q}})$, $\omega_x \in \mathfrak{m}_{X,x}\Omega^1_{X/\mathbb{Z}_{(p)},x}$.

Proof. – That P lifts to P_0 is exactly the valuative criterion for properness. Let $\mathcal{A}$ be the Néron model of A over $\mathbb{Z}_{(p)}$; it is an Abelian scheme, and f extends to a morphism of $\mathbb{Z}_{(p)}$-schemes $X \to \mathcal{A}$, and let $\hat{f} : X_{\mathbb{Z}_p} \to \mathcal{A}_{\mathbb{Z}_p}$ be its base change to $\mathbb{Z}_p$. Then x identifies with a closed point $\hat{x} \in X_{\mathbb{Z}_p}$ of the special fibre, and $P, Q \in]\hat{x}[(\mathbb{Q}_p)$ are distinct points. Moreover, $\hat{f}(P) = 0_{A_{\mathbb{Q}_p}}$ and $\hat{f}(Q) = f(Q) \in A(\mathbb{Q}) \subset \mathcal{A}(\mathbb{Q}_p)$ is a torsion point.

By Proposition 5.6.15, for any $\omega \in H^0(X_{\mathbb{Z}_p}, \Omega^1_{X/\mathbb{Z}_p}) \cap f^*H^0(A_{\mathbb{Q}_p}, \Omega^1_{A/\mathbb{Q}_p})$, one has

$$\omega_{\hat{x}} \in \mathfrak{m}_{X_{\mathbb{Z}_p},\hat{x}}\Omega^1_{X_{\mathbb{Z}_p}/\mathbb{Z}_p,\hat{x}}.$$

Let $\beta : X_{\mathbb{Z}_p} \to X$ be the base change morphism and let $\omega \in H^0(X, \Omega^1_{X/\mathbb{Z}_{(p)}}) \cap f^*H^0(A, \Omega^1_{A/\mathbb{Q}})$. By the previous paragraph, $(\beta^*\omega)_{\hat{x}} \in \mathfrak{m}_{X_{\mathbb{Z}_p},\hat{x}}\Omega^1_{X_{\mathbb{Z}_p}/\mathbb{Z}_p,\hat{x}}$. The morphism

$$\beta^* : \Omega^1_{X/\mathbb{Z}_{(p)},x} \otimes_{\mathcal{O}_{X,x}} \mathcal{O}_{X_{\mathbb{Z}_p},\hat{x}} \to \Omega^1_{X_{\mathbb{Z}_p}/\mathbb{Z}_p,\hat{x}}$$

is an isomorphism of free modules of rank one, so $\omega_x \in \mathfrak{m}_{X,x}\Omega^1_{X/\mathbb{Z}_{(p)},x}$.

□

5.7 An integrality result on $X_{\rho,\xi}(p)(\mathbb{Q})$

Let us recall the definition of exceptional prime given in the introduction of this Chapter.

Definition 5.7.1 Let $p \equiv 2, 5 \pmod 9$ be a prime number. We say that a prime number ℓ is *exceptional* for p if $\ell \equiv \pm 1 \pmod p$ and there exists a prime ideal λ of $\mathbb{Z}[e^{2i\pi/p}]$ with residue characteristic ℓ such that, for every cube root of unity $j \in \mathbb{F}_{p^2}^{\times}$,

$$u_j = \sum_{\substack{b \in \mathbb{F}_p \\ 1+b\sqrt{-3} \in \mathbb{F}_{p^2}^{\times 3} j}} e^{\frac{2i\pi b}{p}} \in \lambda.$$

The goal of this section is to prove the following result.

Theorem 5.7.2 *Let $K/\mathbb{Q}$ be an imaginary quadratic field inert at p and $N \leq \mathrm{GL}_2(\mathbb{F}_p)$ be the normalizer of a nonsplit Cartan subgroup C. Let $\rho : G_{\mathbb{Q}} \to N$ be a surjective continuous group*

homomorphism such that $G_K = \rho^{-1}(C)$, $\det\rho = \omega_p^{-1}$, *and* ρ *is* 3*-Cartan, so that* $3 \mid p+1$. *Let* $\psi : C/\mathbb{F}_p^\times \to F^\times$ *be a character of order* 3 *and* $g \in \mathcal{S}_1(\Gamma_1(M_{3,\rho}))$ *be the newform attached to the odd irreducible Artin representation* $\mathrm{Ind}_K^{\mathbb{Q}}\psi(\rho_K)$. *Assume furthermore that:*

- $X_{\rho,\xi}(\mathbb{Q})$ *contains a non-cuspidal point for some* $\xi \in \mu_p^\times(\overline{\mathbb{Q}})$, *corresponding to some elliptic curve* $E/\mathbb{Q}$,
- *there exists* $(f, \mathbf{1}) \in \mathscr{S}$ *such that* $L(f \times g, 1) \neq 0$.

Then the conductor of E *is equal to* $p^2 M_\rho L$, *where* M_ρ *is the Artin conductor of* ρ *(in the sense of Serre [145]), and* L *is a square-free product of exceptional primes that do not divide* $M_\rho p$.

Remarks

- The recent works of [101, 58] show that the case where one has in fact $\rho(G_K) = 3C$ is impossible, unless E has CM. One could say that we replaced the global condition $\rho(G_K) \neq C$ with a local condition $\rho(I_p) \neq C$.
- By construction, one has $p \nmid M_{3,\rho}$, and, in this situation, the sign of the functional equation of $L(f \times g, s)$ is $+1$.
- It follows from [157, Appendix, Thm 0.1] that there is a bound p_0 depending only on $M_{3,\rho}$ such that if $p \geq p_0$, there exists $(f, \mathbf{1}) \in \mathscr{S}$ such that $L(f \times g, 1) \neq 0$. We will use this result to give a more concrete application of Theorem 5.7.2 in Section 5.8.
- It seems plausible [19] that the bound $p_0(M_{3,\rho})$ can be made effective. Can one expect a bound that does not depend on $M_{3,\rho}$?
- The curve $X_{\rho,\xi}(p)$ has genus at least two: by Faltings' theorem, it contains finitely many rational points. Theorem 5.7.2 thus holds for *some* set of "exceptional primes": what is nontrivial is that we manage to make these primes explicit.
- Let $j \in \mathbb{F}_{p^2}^\times$ be a primitive third root of unity. Numerical computations with MAGMA [16] show that for $p \leq 1500$, the norms of $u_1, u_j, u_1 - u_j, u_j - u_{j^2}$ generate the unit ideal of $\mathbb{Z}$, so there is no exceptional prime. However, the running time of the code grows quickly[8] around $p \geq 1200$, making a direct computation of exceptional primes harder for larger primes p. We thus expect[9] that there are no exceptional primes for any prime $p \geq 11$ congruent to 2 or 5 modulo 9.
- Suppose that ρ comes from an elliptic curve $E_0 \neq E$: the theorem shows that the conductor of E_0 is also of the form $p^2 M_\rho L'$, where L' is a product of exceptional primes $\ell \equiv \pm 1 \pmod{p}$ that are coprime to M_ρ. Even if $L = L' = 1$, proving that E and E_0 are isogenous still seems difficult.

Here is an outline of the proof.

The first step is to show that the conductor of E is of the form $p^2 M_\rho L$, where L is a square-free product of primes $\ell \equiv \pm 1 \pmod{p}$ not dividing pM_ρ. This is accomplished by using Lemmas 5.7.3 (for the primes distinct from p) and Lemma 5.4.1 at p. The second step is to construct a suitable quotient A_I of $J_{\rho,\xi}(p)$ with expected finite Mordell-Weil group: this is done using Corollary 5.5.6 and Proposition 5.5.7. For the rest of the argument, we fix odd primes $q \equiv 1 \pmod{p}$, $\ell \mid L$ with $\ell \equiv \pm 1 \pmod{p}$ not exceptional, an embedding $\iota : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}_\ell}$ inducing a group homomorphism $R_\iota : G_{\mathbb{Q}_\ell} \to G_{\mathbb{Q}}$, and a polarized p-torsion group G over $\mathbb{Z}_{(\ell)}$ such that $X_{G,1}(p)_{\mathbb{Q}} \simeq X_{\rho,\xi}(p)$.

In particular, the rational point of $X_{\rho,\xi}(p)$ reduced modulo ℓ to a point $c_0 \in X_{G,1}(p)(\mathbb{F}_\ell)$ lying in the cuspidal subscheme of $X_{G,1}(p)$. Since this cuspidal subscheme is étale, there is a unique section $c \in X_{G,1}(p)(\mathbb{Z}_\ell)$ of the cuspidal subscheme lifting c_0.

[8] The computation up to $p \leq 1200$ takes slightly under 9 minutes; the computation up to $p \leq 1500$ takes slightly under 30 minutes.

[9] As written elsewhere, further computations since this thesis was submitted established that the claim still held for $11 \leq p \leq 5000$.

The morphism $f : P \in X_{G,1}(p)_{\mathbb{Z}_{(\ell)}} \mapsto (T_q - q - 1)(P - c) \in (A_I)_{\mathbb{Z}_{(\ell)}}$ is well-defined over $\mathbb{Q}$, because, even if c is not rational, $T_q - q - 1$ annihilates the difference of any two cusps by Proposition 1.6.9. So f is well-defined over $\mathbb{Z}_{(\ell)}$.

Finally, we prove that the ideal of first coefficients of the collection of stalks at c_0 of differentials $\omega \in H^0(X_{G,1}(p)_{\mathbb{Z}_\ell}, \Omega^1)$ such that, for some $n \geq 1$, $\ell^n\omega_1 \in f^*H^0((A_I)_{\mathbb{Q}_\ell}, \Omega^1)$ is all of $\mathbb{Z}_\ell$. Then $E, c \in]c_0[(\mathbb{Q}_\ell)$ are mapped by f to torsion points, which contradicts Corollary 5.6.15.

Throughout this argument, we will use without mention basic facts about differentials on Abelian schemes and relative Jacobians proved in Appendix A.4.3.

Lemma 5.7.3 *Let ℓ, p be distinct primes with $p > 3$. Let $E/\mathbb{Q}_\ell$ be an elliptic curve with conductor exponent n_E. Write G_ℓ (resp. I_ℓ) for the absolute Galois group of $\mathbb{Q}_\ell$ (resp. its inertia subgroup). Then the conductor exponent $n_{E,p}$ of $E[p]$ (as a G_ℓ-representation) is contained in $\{n_E - 1, n_E\}$. If $n_{E,p} < n_E$, then $(n_{E,p}, n_E) = (0, 1)$. In this case, the ℓ-adic valuations of the j-invariant and the minimal discriminant of E are divisible by p; moreover, one has $\mathrm{Tr}(\mathrm{Frob}_\ell \mid E[p]) \equiv a_\ell(E)(\ell + 1) \pmod p$ (with $a_\ell(E) = 1$ if E has split multiplicative reduction and $a_\ell(E) = -1$ if E has nonsplit multiplicative reduction).*

Proof. – Let s_E (resp. $s_{E,p}$) be the Swan conductor exponents of $E[p]$ (resp. $\mathcal{T}_pE$). Then one has by definition

$$n_E = s_E + 2 - \mathrm{rk}_{\mathbb{Z}_p} H^0(I_\ell, \mathcal{T}_pE), \quad n_{E,p} = s_{E,p} + 2 - \dim_{\mathbb{F}_p} H^0(I_\ell, E[p]).$$

Since $p \neq \ell$, one has $s_E = s_{E,p}$. Moreover, the homomorphism

$$\tau : H^0(I_\ell, \mathcal{T}_pE) \otimes_{\mathbb{Z}_p} \mathbb{F}_p \to H^0(I_\ell, E[p])$$

is injective, hence $n_E \geq n_{E,p}$, and equality holds if and only if τ is onto.

Let us assume that $H^0(I_\ell, E[p])$ is nonzero. Then, in a suitable basis of $\mathcal{T}_pE$, the image of the action of I_ℓ is contained in the pro-p-group $\mathrm{SL}_2(\mathbb{Z}_p) \cap \begin{pmatrix} 1 + p\mathbb{Z}_p & * \\ p\mathbb{Z}_p & 1 + p\mathbb{Z}_p \end{pmatrix}$, so this action factors through the tame inertia quotient and $s_E = s_{E,p} = 0$. Moreover, the image of the action of I_ℓ is a pro-cyclic subgroup of $\mathrm{SL}_2(\mathbb{Z}_p) \cap \begin{pmatrix} 1 + p\mathbb{Z}_p & * \\ p\mathbb{Z}_p & 1 + p\mathbb{Z}_p \end{pmatrix}$: let $A \in \mathrm{SL}_2(\mathbb{Z}_p)$ be a pro-generator of this image.

Since the action of G_ℓ by conjugation on the tame inertia quotient of I_ℓ is the multiplication by ℓ, A^ℓ is similar to A. In particular, if α is an eigenvalue of A, then the characteristic polynomial of A is $(X - \alpha)(X - \alpha^{-1})$, and α^ℓ is also an eigenvalue of A: thus $\alpha^\ell \in \{\alpha, \alpha^{-1}\}$. Since α is contained in a quadratic extension of $\mathbb{Q}_p$ and $p > 3$, the multiplicative order of α is not divisible by p. Since $(X - \alpha)(X - \alpha^{-1}) \equiv (X - 1)^2 \pmod p$ because $A \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod p$, the reduction of α modulo p is 1. Therefore, by Hensel's lemma, one has $\alpha = 1$, so A is similar in $\mathrm{GL}_2(\mathbb{Z}_p)$ to $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ for some $a \in \mathbb{Z}_p$, and $n_E \leq 1$.

On the other hand, if $H^0(I_\ell, E[p]) = 0$, then $H^0(I_\ell, \mathcal{T}_pE) \otimes_{\mathbb{Z}_p} \mathbb{F}_p \to H^0(I_\ell, E[p])$ is an isomorphism so $n_E = n_{E,p}$.

Thus, when $n_E \neq n_{E,p}$, $H^0(I_\ell, E[p])$ and $n_{E,p} \leq n_E \leq 1$, hence $(n_{E,p}, n_E) = (0, 1)$ and $E[p]$ is invariant under I_ℓ. Assume that this is the case: then E has multiplicative reduction and $j(E) \notin \mathbb{Z}_\ell$. By [152, Theorems V.5.2, V.5.3], there exists $q_E \in \ell\mathbb{Z}_\ell \backslash \{0\}$ such that, for any extension $K/\mathbb{Q}_p$, if E' denotes the elliptic curve E if E has split multiplicative reduction, and its unramified quadratic twist otherwise, $E'(K) \simeq K^\times / q_E^{\mathbb{Z}}$. If $\eta : G_\ell \to \{\pm 1\}$ denotes the unramified character mapping Frob_ℓ to $a_\ell(E)$, one has $E[p] \simeq \eta \otimes \begin{pmatrix} \omega_p & * \\ 0 & 1 \end{pmatrix}$ as G_ℓ-modules.

In particular, since $E[p]$ is fixed under I_ℓ, $q_E \in (\mathbb{Q}_\ell^{nr})^{\times p}$, hence $p \mid v_\ell(q_E)$. Moreover, one has $\mathrm{Tr}(\mathrm{Frob}_\ell \mid E[p]) \equiv a_\ell(E)(\ell + 1) \pmod p$. By [152, Chapter IV.9, Theorem V.3.1],

$v_\ell(q_E) = v_\ell(\Delta_E) = -v_\ell(j(E))$, whence the conclusion. □

Corollary 5.7.4 *Under the assumptions of Theorem 5.7.2, the conductor of E is of the form $p^2 M_\rho L$, where L is a square-free product of prime numbers $\ell \equiv \pm 1 \pmod{p}$ not dividing pM_ρ. Moreover, for every $\ell \mid L$, $j(E) \notin \mathbb{Z}_{(\ell)}$.*

Proof. – What is not given in Lemma 5.7.3 is the conductor exponent at p and the fact that $\ell \equiv \pm 1 \pmod{p}$, if ℓ is a prime dividing the conductor of E but not pM_ρ. By Lemma 5.4.1, E has potentially good reduction at p but bad reduction at p (since ρ is 3-Cartan), thus the conductor exponent of ρ at p is 2. If E has bad reduction at the prime $\ell \nmid pM_\rho$, then, by Lemma 5.7.3, E has multiplicative reduction at ℓ. Therefore, $j(E) \notin \mathbb{Z}_\ell$ by [153, Propositions VII.5.4, VII.5.5], and, by [152, Theorems V.5.2, V.5.3], Frob_ℓ acts on $E[p]$ by a matrix similar to $\pm \begin{pmatrix} \ell & * \\ 0 & 1 \end{pmatrix}$. If this matrix is contained in C, then one has $\ell \equiv 1 \pmod{p}$; if this matrix is in $N\backslash C$, its trace is zero and $\ell \equiv -1 \pmod{p}$. □

Remark The condition that $\ell \equiv \pm 1 \pmod{p}$ implies in particular that $\ell \geq 2p - 1 \geq 20$; it can be found in [168, Theorem 1.5, Proposition 1.8]. We will mostly use this result to assume that $\ell \neq 2$, since the formal immersion argument at this prime is more intricate.

From now on, we assume that $p \equiv 2, 5 \pmod{9}$, so that $C \simeq C[3] \oplus 3C$. Let $(f, \mathbf{1}) \in \mathscr{S}$ and $\psi \in \mathcal{I}_f$ be a character of order three, and V_f be the one-dimensional F-vector space on which $\mathbb{T}[N]$ acts as follows: T_n (resp. nI_2, resp. $A \in N$) acts by $a_n(f)$ (resp. 1, resp. 1). Then the ring $\mathbb{T}_{1,N}(N)$ acts on $V_f \otimes_F \mathrm{Ind}_C^N \psi$ by a character $\mathbb{T}_{1,N}(N) \to F$, and we denote its kernel by $\mathfrak{I}$. We let $\mathfrak{I}_f$ denote the inverse image of $\mathfrak{I}$ in $\mathbb{T}_1$.

Let h be the weight one newform attached to the odd irreducible Artin representation $\left(\mathrm{Ind}_C^N \psi\right) \circ \rho$.

Let $\ell \equiv \pm 1 \pmod{p}$ be a prime at which ρ is unramified. There exists a polarized p-torsion group Γ over $\mathbb{Z}_{(\ell)}$ endowed with a basis (P, Q) of $\Gamma(\overline{\mathbb{Q}})$ such that for any $\sigma \in G_\mathbb{Q}$, $\rho(\sigma) \begin{pmatrix} \sigma(P) \\ \sigma(Q) \end{pmatrix} = \begin{pmatrix} P \\ Q \end{pmatrix}$. Let $\xi_0 = \langle P, Q \rangle_\Gamma \in \mu_p^\times(\overline{\mathbb{Q}})$. After replacing $\overline{\mathbb{Q}}$ with a suitably large number field and using the valuative criterion for properness, we see that there are $P_0, Q_0 \in \Gamma(\overline{\mathbb{Z}}_{(\ell)})$ extending P, Q (where $\overline{\mathbb{Z}}_{(\ell)} = \overline{\mathbb{Z}} \otimes \mathbb{Z}_{(\ell)}$).

In particular, by Propositions 1.4.10 and 1.5.18, for any $t \in \mathbb{F}_p^\times$, $X_{\Gamma,t}(p)_\mathbb{Q}$ is naturally isomorphic to $X_{\rho,t\xi_0}(p)$, and this identification respects the Hecke operators.

Lemma 5.7.6 *Let $q \equiv 1 \pmod{p}$ be a prime, $\mathbb{Q} \subset H \subset \overline{\mathbb{Q}}$ be a number field, and $c \in X_{\rho,\xi}(H)$ be a point in the cuspidal subscheme for some $\xi \in \mu_p^\times(\overline{\mathbb{Q}})$. Then the morphism*

$$P \in X_{\rho,\xi}(p)_H \longmapsto (T_q - q - 1)(P - c) \in J_{\rho,\xi}(p)_H$$

descends to a morphism $X_{\rho,\xi}(p) \to J_{\rho,\xi}(p)$, and this morphism is independent from the choice of c.

Proof. – Since $X_{\rho,\xi}(p), J_{\rho,\xi}(p)$ are smooth proper geometrically connected $\mathbb{Q}$-schemes, by Corollary A.1.10, it is enough to show that $P \in X_{\rho,\xi}(p)(\overline{\mathbb{Q}}) \longmapsto (T_q - q - 1)(P - c) \in J_{\rho,\xi}(\overline{\mathbb{Q}})$ commutes with the action of $G_\mathbb{Q}$. Since $T_q - (q+1) \in \mathrm{End}(J_{\rho,\xi}(p))$, all we need to do is show that, for any two $c, c' \in X_{\rho,\xi}(p)(\overline{\mathbb{Q}})$ contained in the cuspidal subscheme, one has $(T_q - q - 1)(c - c') = 0$. This is exactly Proposition 1.6.9. □

Remark In fact, this morphism is independent from the choice of ρ.

Lemma 5.7.8 *Let A be an Abelian variety over a field k and I be a subgroup of $\mathrm{End}_k(A)$. Let $\pi : A \to A/IA$ be the quotient homomorphism. Then $\pi^* H^0(A/IA, \Omega^1)$ is exactly the I-torsion subspace of $H^0(A, \Omega^1)$.*

Proof. – Let $A' = A/IA$. For $V \in \{A, A'\}$, there is a perfect pairing $\mathrm{Lie}(V) \times H^0(V, \Omega^1_{V/k}) \to k$ (by Corollary A.3.15). The differentials in $\pi^* H^0(A', \Omega^1_{A'/k})$ are clearly in the I-torsion submodule of $H^0(A, \Omega^1_{A/k})$; their image is exactly the orthogonal of $\ker \pi : \mathrm{Lie}(A) \to \mathrm{Lie}(A')$, which is the orthogonal of $I \cdot \mathrm{Lie}(A)$, which is the I-torsion submodule of $H^0(A, \Omega^1_{A/k})$, whence the conclusion. □

Proposition 5.7.9 *Assume that $X_{\rho,\xi}(p)$ has a non-cuspidal rational point P corresponding to an elliptic curve $E/\mathbb{Q}$ with conductor $p^2 M_\rho L$ by Corollary 5.7.4 such that $\ell \mid L$. Assume furthermore that $L(f \times h, 1) \neq 0$.*

Then, there exists a point $c \in X_{\rho,\xi}(p)$ lying in the special fibre of the cuspidal subscheme such that for any $\omega \in H^0(X_{\Gamma,t}(p), \Omega^1_{X_{\Gamma,t}(p)/\mathbb{Z}_{(\ell)}})$, if $\mathfrak{I} \cdot \omega = 0$, then $\omega_c \in \mathfrak{m}_{X_{\Gamma,t}(p),c}\, \Omega^1_{X_{\Gamma,t}(p)/\mathbb{Z}_{(\ell)},c}$.

Proof. – Let $c_0 \in X_{\Gamma,t}(p)$ be the reduction of $E \in X_{\Gamma,t}(p)(\mathbb{Q})$ modulo ℓ. Since $j(E) \notin \mathbb{Z}_{(\ell)}$ by Corollary 5.7.4, c_0 lies in the cuspidal subscheme of $X_{\Gamma,t}(p)$. The cuspidal subscheme of $X_{\Gamma,t}(p)$ is finite étale over $\mathbb{Z}_{(\ell)}$, so there is a $c \in X_{\Gamma,t}(p)(\overline{\mathbb{Q}})$ and a prime ideal $\mathfrak{l} \subset \overline{\mathbb{Z}}$ of residue characteristic ℓ such that c_0 is the reduction of c modulo $\mathfrak{l}$. For the same reason, $c_\mathfrak{l} \in X_{\Gamma,t}(p)(\overline{\mathbb{Q}}_\mathfrak{l})$ factors through some $c'_\mathfrak{l} \in X_{\Gamma,t}(p)(\mathbb{Q}_\ell)$.

Let $A = J_{\rho,\xi}(p)/\mathfrak{I}$: it is an Abelian variety over $\mathbb{Q}$ with good reduction at ℓ (since it is a quotient of $J_{\rho,\xi}(p)$ which has good reduction at ℓ by the Néron-Ogg-Shafarevich criterion [146, Theorem 1] and the description of its Tate module given in Proposition 5.2.5), and let $\mathcal{A}$ be its Néron model over $\operatorname{Spec} \mathbb{Z}_{(\ell)}$.

Let $q \equiv 1 \pmod{p}$ be a prime and $f : X_{\Gamma,t}(p) \to \mathcal{A}$ be the morphism extending

$$x \in X_{\Gamma,t}(p)_\mathbb{Q} \simeq X_{\rho,\xi}(p) \longmapsto ((T_q - q - 1)(x - c) \pmod{\mathfrak{I}}) \in A_\mathbb{Q}$$

as in Lemma 5.7.6.

By Proposition 5.5.7, $A(\mathbb{Q})$ is a finite group, so we can apply Corollary 5.6.16: for any $\omega \in H^0(X_{\Gamma,t}(p), \Omega^1_{X_{\Gamma,t}(p)/\mathbb{Z}_{(\ell)}}) \cap f^* H^0(A, \Omega^1_{A/\mathbb{Q}})$, one has $\omega_{c_0} \in \mathfrak{m}_{X_{\Gamma,t}(p),c_0} \Omega^1_{X_{\Gamma,t}(p)/\mathbb{Z}_{(\ell)},c_0}$.

The conclusion follows once we prove that $H^0(X_{\Gamma,t}(p), \Omega^1_{X_{\Gamma,t}(p)/\mathbb{Z}_{(\ell)}}) \cap f^* H^0(A, \Omega^1_{A/\mathbb{Q}})$ is exactly the $\mathfrak{I}$-torsion submodule of $H^0(X_{\Gamma,t}(p), \Omega^1_{X_{\Gamma,t}(p)/\mathbb{Z}_{(\ell)}})$.

Since both submodules are saturated in $H^0(X_{\Gamma,t}(p), \Omega^1_{X_{\Gamma,t}(p)/\mathbb{Z}_{(\ell)}})$, it is enough to see that $f^* H^0(A, \Omega^1_{A/\mathbb{Q}})$ is the $\mathfrak{I}$-torsion submodule of $H^0(X_{\Gamma,t}(p)_\mathbb{Q}, \Omega^1_{X_{\Gamma,t}(p)_\mathbb{Q}/\mathbb{Q}})$.

By Proposition A.4.35, it is enough to show that $T_q - q - 1 : J_{\rho,\xi}(p) \to J_{\rho,\xi}(p)$ is an isogeny (note that it commutes to $\mathfrak{I}$) and that $\pi^* H^0(A, \Omega^1_{A/\mathbb{Q}})$ is exactly the $\mathfrak{I}$-torsion submodule of $H^0(J_{\rho,\xi}(p), \Omega^1_{J_{\rho,\xi}(p)/\mathbb{Q}})$. The second part is a consequence of Lemma 5.7.8.

By Corollary 2.4.9, the action of T_q on $H^0(J_{\rho,\xi}(p), \Omega^1_{J_{\rho,\xi}(p)/\mathbb{Q}}) \otimes_\mathbb{Q} F$ is diagonalizable and all its complex eigenvalues are of the form $a_q(f)$ for $(f, \chi) \in \mathscr{S} \cup \mathscr{P} \cup \mathscr{C}$, so that $|a_q(f)| \leq 2\sqrt{q} < q+1$, thus $T_q - q - 1 : \mathbb{T}_1 \to \mathbb{T}_1$ is injective. Hence $T_q - q - 1$ divides (in $\mathbb{T}_1$) some positive integer Q. By [118, §8], $T_q - q - 1$ is an isogeny, and we are done. □

Lemma 5.7.10 *Let $X \to \operatorname{Spec} R$ be a smooth proper morphism of relative dimension one. Let $c \in X$ and $V \subset H^0(X, \Omega^1_{X/R})$ be a subset. Let R' be a R-algebra, $\beta : X_{R'} \to X_R$ be the natural homomorphism and $c' \in X_{R'}$ be such that $\beta(c') = c$. Then the following are equivalent:*

- *There exists $\omega \in V$ such that $\omega_c \notin \mathfrak{m}_{X,c}\, \Omega^1_{X/R,c}$.*
- *There exists $\omega \in V$ such that $(\beta^* \omega)_{c'} \notin \mathfrak{m}_{X_{R'},c'}\, \Omega^1_{X_{R'}/R',c'}$.*

Proof. – Since $X \to \operatorname{Spec} R$ is smooth of relative dimension one, we know that $\Omega^1_{X_R/R,c}$ is free of rank one over $\mathcal{O}_{X_R/R,c}$ and that the natural map $\Omega^1_{X/R,c} \otimes_{\mathcal{O}_{X,c}} \mathcal{O}_{X_{R'},c'} \to \Omega^1_{X_{R'}/R',c'}$ (given by β^*) is an isomorphism. Thus, for $\omega \in V$, $\omega_c \notin \mathfrak{m}_{X,c} \Omega^1_{X/R,c}$ if and only if ω_c is a basis of $\Omega^1_{X/R,c}$, if and only if $(\beta^* \omega)_{c'}$ is a basis of $\Omega^1_{X_{R'}/R',c'}$, if and only if $(\beta^* \omega)_{c'} \notin \mathfrak{m}_{X_{R'},c'} \Omega^1_{X_{R'}/R',c'}$. □

Corollary 5.7.11 *Assume that $X_{\rho,\xi}(p)$ has a non-cuspidal rational point P corresponding to an elliptic curve $E/\mathbb{Q}$ with conductor $p^2M_\rho L$ by Corollary 5.7.4 such that $\ell \mid L$ and that $L(f \times h, 1) \neq 0$. Then, for any flat local homomorphism $\mathbb{Z}_{(\ell)} \to R$, there exists $c \in X(p,p)_R$ lying in the special fibre of the cuspidal subscheme such that for any $\omega \in H^0(X(p,p)_R, \Omega^1_{X(p,p)_R/R})$ such that $\mathfrak{I} \cdot \omega = 0$, one has $\omega_c \in \mathfrak{m}_{X(p,p)_R,c}\,\Omega^1_{X(p,p)_R/R,c}$.*

Proof. – It is a consequence of Lemma 5.7.10 and Proposition 5.7.9, as long as we can show that the $\mathfrak{I}$-torsion submodule of $H^0(X(p,p)_R, \Omega^1_{X(p,p)_R/R})$ is generated by the $\mathfrak{I}$-torsion submodule of $H^0(X(p,p)_{\mathbb{Z}_{(\ell)}}, \Omega^1_{X(p,p)_{\mathbb{Z}_{(\ell)}}/\mathbb{Z}_{(\ell)}})$. This is true because R is flat over $\mathbb{Z}_{(\ell)}$ (so in particular $H^0(X(p,p)_{\mathbb{Z}_{(\ell)}}, \Omega^1_{X(p,p)_{\mathbb{Z}_{(\ell)}}/\mathbb{Z}_{(\ell)}}) \otimes_{\mathbb{Z}_{(\ell)}} R \to H^0(X(p,p)_R, \Omega^1_{X(p,p)_R/R})$ is an isomorphism). □

Lemma 5.7.12 *Let $K/\mathbb{Q}$ be a field extension and $\omega \in H^0(X_{\rho,\xi}(p)_K, \Omega^1_{X_{\rho,\xi}(p)_K/K})$. Fix a generator $g \in C$ and let $\zeta_3 = g^{\frac{p^2-1}{3}}$. Then $\mathfrak{I} \cdot \omega = 0$ if and only if the following conditions are satisfied:*

- *ω is the sum of its projections $\omega_{f'}$ to the f'-eigenspaces for $f' \in G_\mathbb{Q} \cdot f$ (one always has $(f', \mathbf{1}) \in \mathscr{S}$),*
- *$\omega \mid (1 + \zeta_3 + \zeta_3^2) = 0$,*
- *$\omega \mid [g^{3(p-1)} + g^{3(1-p)} - 2] = 0$,*
- *for any prime q such that $q \det g \equiv 1 \pmod p$ and $a_q(f) \neq 0$, choose integers B, n_i, m_i with $B, n_i > 0$ and $n_i \equiv 1 \pmod p$ such that $-Ba_q(f) = \sum_i m_i a_{n_i}(f)$. For every $f' \in G_\mathbb{Q} \cdot f$, one has $B\omega_{f'} \mid T_q(g + g^p) = (\sum_i m_i a_{n_i}(f'))\,\omega_{f'}$.*

Moreover, the $\mathfrak{I}$-torsion submodule of $H^0(X_{\rho,\xi}(p)_K, \Omega^1_{X_{\rho,\xi}(p)_K/K})$ has dimension $2|G_\mathbb{Q} \cdot f|$.

Proof. – Because the action of $\mathbb{T}_{1,N}(N) \supset \mathfrak{I}$ is defined over $\mathbb{Q}$, it is enough to show the result when $K = \mathbb{Q}$. For the dimension, it is enough to check, by the proof of Proposition 5.7.9, that $\dim J_{\rho,\xi}(p)/\mathfrak{I}J_{\rho,\xi}(p) = 2|G_\mathbb{Q} \cdot f|$. Since the only other Galois conjugate of $\psi : C/\mathbb{F}_p^\times \to F^\times$ is $\psi^2 = \psi^p$, the conclusion follows from the description of the Tate module of $J_{\rho,\xi}(p)/\mathfrak{I}J_{\rho,\xi}(p)$ by Proposition 5.5.6.

The four conditions are necessary, because (by inspecting the Tate module of A by Proposition 5.5.6) $1 + \zeta_3 + \zeta_3^2, g^{3(p-1)} + g^{3(1-p)} - 2, \sum_i m_i T_{n_i} - BT_q(g + g^p)$ are all contained in $\mathfrak{I}$, and the first condition is equivalent to $\mathfrak{I}_f \cdot \omega = 0$.

The claim is that the reunion of all four conditions is sufficient. In other words, it is enough to prove that A is the quotient of $J_{\rho,\xi}(p)$ by $\mathfrak{I}_f, 1 + \zeta_3 + \zeta_3^2, g^{3(p-1)} + g^{3(1-p)} - 2\mathrm{id}$, and $\sum_i m_i T_{n_i} - BT_q(g + g^p)$ (for q, m_i, n_i as given).

It is enough to show that $\ker[\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l} \to \mathcal{T}_\ell A \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}]$ is exactly the submodule generated by the sum of the images of $\mathcal{I}_f, 1+\zeta_3+\zeta_3^2, g^{3(p-1)}+g^{3(1-p)}-2I_2$, and $\sum_i m_i T_{n_i} - BT_q(g+g^p)$.

We use the description of Proposition 5.2.4 (and argue as in Proposition 5.5.2). The image of $\mathfrak{I}_f$ is made with those eigenspaces of $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ which are attached to newforms that are not Galois-conjugate to f. The image of $1 + \zeta_3 + \zeta_3^2$ is exactly made with the representations on which ζ_3 acts as a matrix of order 3 instead of the identity – among others, it contains the spaces corresponding to H_f. Similarly, the image of $g^{3(p-1)} + g^{3(1-p)} - 2I_2$ is exactly made with those subspaces where $g^{3(p-1)}$ does not act trivially.

Thus, the summands of $\mathcal{T}_\ell J_{\rho,\xi}(p) \otimes_{\mathbb{Z}_\ell} F_\mathfrak{l}$ which are not contained in (equivalently, do not meet) the image of $(\mathfrak{I}_f, 1+\zeta_3+\zeta_3^2, g^{3(p-1)}+g^{3(1-p)}-2I_2)$ are those of the form $V_{f',\mathfrak{l}} \otimes \mathrm{Ind}_{\widetilde{\rho}^{-1}(C)}^{N \rtimes_\rho G_\mathbb{Q}} \psi_1(\widetilde{\rho_K})$ with $(f', \mathbf{1}) \in \mathscr{S}$, $f' \in G_\mathbb{Q} \cdot f$, $\psi_1 \in \mathcal{I}_{f'}/\sim$, $\psi_1(\zeta_3) \neq 1$, $\psi_1(g)^{3(p-1)} = 1$ hence $\psi_1(g)^6 = 1$.

Thus, in this situation, either $\psi_1 \in \{\psi, \psi^2\}$, or $\psi_1 \in \{\psi_6, \psi_6^p\}$ with $\psi_6 = \left(\frac{\det}{p}\right)\psi$. The goal is to show that for $(q, B, (m_i)_i, (n_i)_i)$ as above, $\sum_i m_i T_{n_i} - BT_q(g + g^p) \in \mathbb{T}_{1,N}(N)$ vanishes when applied to $V_{f',\mathfrak{l}} \otimes \mathrm{Ind}_{\widetilde{\rho}^{-1}(C)}^{N \rtimes_\rho G_\mathbb{Q}} \psi(\widetilde{\rho_K})$ but is surjective when applied to $V_{f',\mathfrak{l}} \otimes \mathrm{Ind}_{\widetilde{\rho}^{-1}(C)}^{N \rtimes_\rho G_\mathbb{Q}} \psi_6(\widetilde{\rho_K})$.

Indeed, $\sum_i m_i T_{n_i}$ acts on $V_{f',\mathfrak{l}} \otimes \mathrm{Ind}_{\widetilde{\rho}^{-1}(C)}^{N \rtimes_\rho G_{\mathbb{Q}}} \psi_1(\widetilde{\rho_K})$ by multiplication by

$$\sum_i m_i a_{n_i}(f') = \sigma\left(\sum_i m_i a_{n_i}(f)\right) = \sigma(-Ba_q(f)) = -Ba_q(f').$$

However, $BT_q(g+g^p)$ acts on $V_{f',\mathfrak{l}} \otimes \mathrm{Ind}_{\widetilde{\rho}^{-1}(C)}^{N \rtimes_\rho G_{\mathbb{Q}}} \psi(\widetilde{\rho_K})$ by $Ba_q(f')(j+j^2) = -Ba_q(f')$, where j is a primitive third root of unity. On the other hand, $BT_q(g+g^p)$ acts on $V_{f',\mathfrak{l}} \otimes \mathrm{Ind}_{\widetilde{\rho}^{-1}(C)}^{N \rtimes_\rho G_{\mathbb{Q}}} \psi_6(\widetilde{\rho_K})$ acts by $-Ba_q(f')(j+j^2) = Ba_q(f')$.

Therefore, we are done if there *exists* one instance of $(B, q, (m_i)_i, (n_i)_i)$ as above. The existence of q follows from Serre's theorem [144, Cor. 2 au Théorème 15]. The $a_n(f)$ are algebraic integers: as in Proposition 5.5.2, the $B, (m_i)_i, (n_i)_i$ as above exist provided that $a_q(f)$ is in the number field generated by the $a_n(f)$ with $n \equiv 1 \pmod{p}$.

Let $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ fixing all the $a_n(f)$ for $n \equiv 1 \pmod{p}$. Then $\sigma(f) \in \mathcal{S}_2(\Gamma_0(p))$ is a newform. By Lemmas 3.6.2, $\sigma(f)$ is a twist of f; by Lemma 2.3.7, $\sigma(f) = f$, hence $\sigma(a_q(f)) = a_q(f)$, whence the conclusion. □

Proposition 5.7.13 *Let $a \in \mathbb{F}_p^\times$, and write $X(p,p)_a$ for the connected component $X(p) \times \{a\}$ of $X(p,p)_{\mathbb{C}}$ (see Proposition 2.4.1). By Corollary 2.4.2, $\iota_{p,p}$ identifies $H^0(X(p,p)_a, \Omega^1)$ with $\mathcal{S}_2(\Gamma(p)) \otimes \Delta_{a^{-1},1}$ as right $\mathbb{C}[\mathbb{T}_{1,\mathrm{GL}_2(\mathbb{F}_p)}]$-modules.*

Fix a generator $g \in C$ and let $\zeta_3 = g^{\frac{p^2-1}{3}} \in C \cap \mathrm{SL}_2(\mathbb{F}_p)$ with order 3. Then, a generating family for the $H^0(X(p,p)_a, \Omega^1)[\mathfrak{I}]$ is given by

$$\mathcal{F}_a := \left(\left(f'\left(\frac{\tau}{p}\right) \otimes \Delta_{a^{-1},1} \right) \mid \sum_{r=0}^{\frac{p+1}{3}-1} \Delta_{(\det g)^{-3r},1}\, g^{3r} \zeta_3^i \right)_{\substack{f' \in G_{\mathbb{Q}} \cdot f \\ i \in \{0,1,2\}}},$$

where we recall that $\Delta_{a,b}$ denotes the matrix $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$.

The relations within $\mathcal{F}_a$ are generated by the collection, for every $f' \in G_{\mathbb{Q}} \cdot f$, of

$$\sum_{i=0}^{2} \left[\left(f'\left(\frac{\tau}{p}\right) \otimes \Delta_{a^{-1},1} \right) \mid \sum_{r=0}^{\frac{p+1}{3}-1} \Delta_{(\det g)^{-3r},1}\, g^{3r} \zeta_3^i \right] = 0.$$

Proof. – Fix a homomorphism $\iota : \overline{\mathbb{Q}} \to \mathbb{C}$ mapping ξ_0 to $e^{-\frac{2i\pi}{p}}$. By Proposition 1.4.11, $X(p,p)_a$ identifies with $X_{\mathbf{id},\iota(\underline{a}\underline{\xi}_0)} \simeq \left(X_{\rho,\underline{a}\underline{\xi}_0}\right)_{\mathbb{C}}$.

We will prove that the only $\mathbb{C}$-linear relations within $\mathcal{F}_a$ are the ones given in the statement of the Proposition, and that the span of $\mathcal{F}_a$ (over $\mathbb{C}$) is contained in the $\mathfrak{I}$-torsion submodule of $H^0(X_{\rho,\underline{a}\underline{\xi}_0}(p)_{\mathbb{C}}, \Omega^1)$. Since the dimensions match by Lemma 5.7.12, this is enough to conclude.

For any $f' \in G_{\mathbb{Q}} \cdot f$ and $a \in \mathbb{F}_p^\times$, let

$$u_{f',a} = f'\left(\frac{\tau}{p}\right) \otimes \Delta_{a,1}.$$

Step 1: Let us show that the function $r \in \mathbb{Z} \longmapsto u_{f',a}^r := u_{f',a} \mid \Delta_{(\det g)^{-r},1}\, g^r$ factors through

$\mathbb{Z}/(p+1)\mathbb{Z}$. Indeed, let $r, s \in \mathbb{Z}$, then

$$\begin{aligned} u_{f',a} \mid \Delta_{(\det g)^{-r-(p+1)s},1} g^{r+(p+1)s} &= u_{f',1} \mid \Delta_{a,1}\Delta_{(\det g)^{-r-2s},1} \cdot ((\det g)^s I_2) \cdot g^r \\ &= u_{f',1} \mid \Delta_{(\det g)^{-s},(\det g)^s}\Delta_{a,1}\Delta_{(\det g)^{-r},1}\, g^r \\ &= u_{f',1} \mid \Delta_{a,1}\Delta_{(\det g)^{-r},1}\, g^r = u_{f',a} \mid \Delta_{(\det g)^{-r},1}\, g^r, \end{aligned}$$

whence the conclusion.

Step 2: The only relations between the $u^r_{f',a}$ are that $\sum_{r\in\mathbb{Z}/(p+1)\mathbb{Z}} u^r_{f',a} = 0$.

Let $q \equiv 1 \pmod p$ be a positive integer and $f' \in G_{\mathbb{Q}} \cdot f$. Then $T_q(u^r_{f',a}) = a_q(f')u^r_{f',a}$. Moreover, by Lemmas 3.6.2 and 2.3.7, the collection $(a_q(f'))_{q\equiv 1 \pmod p}$ determines f'. Therefore, let, for every $(f',a) \in (G_{\mathbb{Q}} \cdot f) \times \mathbb{F}_p^\times$, $U_{f',a}$ be the $\mathbb{C}[\mathrm{SL}_2(\mathbb{F}_p)]$-module generated by $u_{f',a}$, then the $U_{f',a}$ are in direct sum. Thus, it is enough to show that for any $f' \in G_{\mathbb{Q}} \cdot f$, the only relations in the family $(u^r_{f',a})_{r,a}$ are that $\sum_{r\in\mathbb{Z}/(p+1)\mathbb{Z}} u^r_{f',a} = 0$ for any a. Thus, fix $f' \in G_{\mathbb{Q}} \cdot f$.

For any $\chi \in \mathcal{D}$, let

$$\hat{u}_{f',\chi} = \sum_{a\in\mathbb{F}_p^\times} \chi^{-1}(a) u_{f',a} \in \Omega^1[f',\chi]\backslash\{0\}$$

in the sense of Corollary 2.5.5. For any $X = \begin{pmatrix} a & 0 \\ b & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)$, a direct verification shows that $\hat{u}_{f',\chi} \mid X = \chi(\det X)\hat{u}_{f',\chi}$. Therefore, by Corollary 2.4.6, the $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-module generated by $\hat{u}_{f',\chi}$ is isomorphic to St_χ: thus, the $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules generated by the $\hat{u}_{f',\chi}$ (where $\chi \in \mathcal{D}$ varies) form a direct sum.

Moreover, for any $r \in \mathbb{Z}/(p+1)\mathbb{Z}$, one has

$$\sum_{a\in\mathbb{F}_p^\times} \chi^{-1}(a) u^r_{f',a} = \hat{u}_{f',\chi} \mid \Delta_{(\det g)^{-r},1}\, g^r = \chi(\det g)^{-r} \hat{u}_{f',\chi} \mid g^r.$$

By Lemma B.3.2, the only (nontrivial) relation in the family $\left(\sum_{a\in\mathbb{F}_p^\times} \chi^{-1}(a) u^r_{f',a}\right)_{r\in\mathbb{Z}/(p+1)\mathbb{Z}}$ (χ being fixed) is that their sum vanishes. The preceding remarks show that the relations in the family $(\hat{u}_{f',\chi} \mid \Delta_{(\det g)^{-r},1}\, g^r)_{\substack{r\in\mathbb{Z}/(p+1)\mathbb{Z} \\ \chi\in\mathcal{D}}}$ are generated by the fact that for any χ,

$$\sum_{r\in\mathbb{Z}/(p+1)\mathbb{Z}} \hat{u}_{f',\chi} \mid \Delta_{(\det g)^{-r},1}\, g^r = 0.$$

Since $u_{f',a} = \frac{1}{p-1}\sum_{\chi\in\mathcal{D}} \chi(a)\hat{u}_{f',\chi}$, the family $(u^r_{f',a})_{a,r}$ has rank $(p-1)(p+1) - |\mathcal{D}| = p(p-1)$, so it has exactly $p-1$ relations, and, for any $a \in \mathbb{F}_p^\times$, $\sum_{r\in\mathbb{Z}/(p+1)\mathbb{Z}} u^r_{f',a} = 0$. Hence these are all the relations in the family $(u^r_{f',a})_{(a,r)\in\mathbb{F}_p^\times\times\mathbb{Z}/(p+1)\mathbb{Z}}$, whence the conclusion.

Step 3: The span of $\mathcal{F}_a$ has dimension $2|G_{\mathbb{Q}} \cdot f|$ and the only relations between the vectors of $\mathcal{F}_a$ are those given in the statement.

Fix $a \in \mathbb{F}_p^\times$. For $i \in \{0,1,2\}$ and $f' \in G_{\mathbb{Q}} \cdot f$, let $v_{f',a,i} = \sum_{r\in 3\mathbb{Z}/(p+1)\mathbb{Z}} u^r_{f',a^{-1}} \mid \zeta_3^i$, so that $\mathcal{F}_a = (v_{f',a,i})_{\substack{f'\in G_{\mathbb{Q}}\cdot f \\ i\in\{0,1,2\}}}$.

Since $p-1 \mid \frac{p^2-1}{3}$, one has $(\det g)^{\frac{p^2-1}{3}} = 1$. Moreover, $\frac{p^2-1}{3} \equiv \frac{p+1}{3} \pmod{p+1}$, so, for $r \in \mathbb{Z}$, one has $u^r_{f',a^{-1}} \mid \zeta_3^i = u^{r+i\frac{p+1}{3}}_{f',a^{-1}}$ by Step 1. Hence

$$v_{f',a,i} = \sum_{r\in 3\mathbb{Z}/(p+1)\mathbb{Z}} u^{r+i\frac{p+1}{3}}_{f',a^{-1}}.$$

Since $\frac{p+1}{3}$ is not divisible by 3, the conclusion follows from Step 2.

Step 4: The vectors of $\mathcal{F}_a$ are contained in the $\mathfrak{I}$-torsion submodule.

We use the criterion of Lemma 5.7.12. Let $f' \in G_{\mathbb{Q}} \cdot f$ and $i \in \{1,2\}$, write $f' = \sigma(f)$ for some $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$. For any $m, n \geq 1$ such that $m^2 n \equiv 1 \pmod{p}$, $(mI_2) \cdot T_n$ acts on $v_{f',a,i}$ by multiplication by $a_n(f') = \sigma(a_n(f))$. By definition of $\mathfrak{I}_f$, $\mathfrak{I}_f$ thus annihilates every $v_{f',a,i}$.

Since $\frac{p+1}{3}$ is coprime to 3, one has

$$v_{f',i} \mid (1 + \zeta_3 + \zeta_3^2) = \sum_{r \in \mathbb{Z}/(p+1)\mathbb{Z}} u^r_{f',a^{-1}} = 0.$$

Moreover, for any $r \in \mathbb{Z}$, $\Delta_{(\det g)^{-r-3(p-1)},1}\, g^{r+3(p-1)} = \Delta_{(\det g)^{-r},1}\, g^r g^{3(p-1)}$. Therefore, one has $u^r_{f,a^{-1}} \mid g^{3(p-1)} = u^{r+3(p-1)}_{f,a^{-1}}$, which implies that $v_{f',a,i} \mid g^{3(p-1)} = v_{f',a,i}$.

Finally, write $-Ba_q(f) = \sum_j w_j a_{n_j}(f)$, where q is a prime such that $a_q(f) \neq 0$ and $q \det g \equiv 1 \pmod{p}$, the w_j are integers, the n_j are positive integers congruent to 1 modulo p, and $B > 0$ is an integer. We need to show that $Bv_{f',a,i} \mid T_q(g + g^p) = \sum_j w_j a_{n_j}(f') \cdot v_{f',a,i}$ for each $(f', a, i) \in (G_{\mathbb{Q}} \cdot f) \times \mathbb{F}_p^\times \times \{0,1,2\}$. Indeed, let $f' = \sigma(f)$, then

$$\begin{aligned}
&Bv_{f',a,i} \mid T_q(g+g^p) = Ba_q(f') \sum_{r \in 3\mathbb{Z}/(p+1)\mathbb{Z}} u_{f',a^{-1}q} \mid \Delta_{(\det g)^{-r},1}\, g^r \zeta_3^i (g+g^p) \\
&= Ba_q(f') \sum_{r \in 3\mathbb{Z}/(p+1)\mathbb{Z}} u_{f',a^{-1}} \mid \left[\Delta_{(\det g)^{-r-1},1} g^{r+1+i\frac{p+1}{3}} + \Delta_{(\det g)^{-r-p},1}\, g^{r+p+i\frac{p+1}{3}}\right] \\
&= Ba_q(f') \sum_{r \in 3\mathbb{Z}/(p+1)\mathbb{Z}} u^{r+i\frac{p+1}{3}+1}_{f',a^{-1}} + u^{r+i\frac{p+1}{3}-1}_{f',a^{-1}} \\
&= -Ba_q(f') v_{f',a,i} = \sigma(-Ba_q(f)) v_{f',a,i} \\
&= \sigma\left(\sum_j w_j a_{n_j}(f)\right) v_{f',a,i} = \left(\sum_j w_j a_{n_j}(f')\right) v_{f',a,i},
\end{aligned}$$

whence the conclusion. □

Lemma 5.7.14 *Let $a \in \mathbb{F}_p^\times$, $\gamma = \begin{pmatrix} u & v \\ * & * \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_p)$ and $(f', \mathbf{1}) \in \mathscr{S}$. Then*

$$\begin{aligned}
\left(f'\left(\frac{\tau}{p}\right) \otimes \Delta_{a,1}\right) \mid \gamma &= \sum_{n \geq 1} a_n(f) e^{\frac{2in\pi}{p}\frac{av}{u}} e^{\frac{2i\pi n\tau}{p}} \otimes \Delta_{a,1} && \text{if } u \neq 0, \\
&= -pa_p(f) \sum_{n \geq 1} a_n(f) e^{2i\pi n\tau} \otimes \Delta_{a,1} && \text{otherwise.}
\end{aligned}$$

Proof. – One has

$$\left(f'\left(\frac{\tau}{p}\right) \otimes \Delta_{a,1}\right) \mid \gamma = \left[f'\left(\frac{\tau}{p}\right) \mid \begin{pmatrix} u & av \\ a^{-1}w & x \end{pmatrix}\right] \otimes \Delta_{a,1}.$$

Since $f'\left(\frac{\tau}{p}\right)$ is invariant under the right action of the lower-triangular matrices in $\mathrm{SL}_2(\mathbb{F}_p)$, when $u \neq 0$, we may assume that $\begin{pmatrix} u & av \\ a^{-1}w & x \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, in which case the conclusion is clear. Similarly, when $u = 0$, we may assume that $\begin{pmatrix} u & av \\ a^{-1}w & x \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Then, by Proposition

C.3.3,

$$f'\left(\frac{\tau}{p}\right) \mid \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = pf \mid \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = p\lambda_p(f)f = -pa_p(f)f.$$

□

Let us now fix an element $j \in \mathbb{F}_{p^2}^\times$ with order 3 (hence $j \notin \mathbb{F}_p^\times$). There is a unique $\mathbb{F}_p$-basis (α, β) of $\mathbb{F}_{p^2}$ such that, for any $x = \begin{pmatrix} u & v \\ * & * \end{pmatrix} \in C$, $u\alpha + v\beta$ has the same characteristic polynomial as x, and such that, if moreover $x = \zeta_3$, one has $u\alpha + v\beta = j$. We say that (α, β) is the *adapted* basis of $\mathbb{F}_{p^2}$.

Definition 5.7.15 Given a $\mathbb{F}_p$-basis $\mathcal{B} = (u, v)$ of $\mathbb{F}_{p^2}$ and a third root of unity $j \in \mathbb{Z}/3\mathbb{Z}$, let

$$\Sigma_{\mathcal{B},t} = \sum_{\substack{au+bv \in \mathbb{F}_{p^2}^{\times 3} j^t / \mathbb{F}_p^\times \\ a \neq 0}} e^{\frac{2i\pi b/a}{p}} \in \mathbb{Z}[\zeta_p].$$

Remark Since $p \equiv -1 \pmod 3$, -3 is not a square in $\mathbb{F}_p^\times$, and one can check directly that $\Sigma_{(1,\sqrt{-3}),t} = u_{j^t}$.

Lemma 5.7.17 *The following statements hold true:*

- *When $\mathcal{B}$ is a fixed $\mathbb{F}_p$-basis of $\mathbb{F}_{p^2}$, the only $\mathbb{Z}$-linear relation between the $\Sigma_{\mathcal{B},t}$ is that their sum is zero.*
- *Let (u, v) be a basis of $\mathbb{F}_{p^2}$, $\lambda \in \mathbb{F}_p$ and $t \in \mathbb{Z}/3\mathbb{Z}$, then $\Sigma_{(u+\lambda v,v),t} = e^{-2i\pi\lambda/p}\Sigma_{(u,v),t}$.*
- *Let (u, v) be a basis of $\mathbb{F}_{p^2}$, $s, t \in \mathbb{Z}/3\mathbb{Z}$ and $\alpha \in \mathbb{F}_{p^2}^{\times 3} j^s$. Then $\Sigma_{(\alpha u,\alpha v),t+s} = \Sigma_{(u,v),t}$.*
- *Let (u, v) be a basis of $\mathbb{F}_{p^2}$, $t \in \mathbb{Z}/3\mathbb{Z}$ and $a, b \in \mathbb{F}_p^\times$. Then $\Sigma_{(au,bv),t} = \underline{ab^{-1}}(\Sigma_{(u,v),t})$.*

Proof. – Let $\mathcal{B} = (u, v)$. For every $w \in \mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times$, let $\omega(w) = e^{\frac{2i\pi}{p}ba^{-1}}$ if $w = (au + bv)\mathbb{F}_p^\times$ with $a \neq 0$, and $\omega(w) = 0$ otherwise. We claim that the only $\mathbb{Z}$-linear relation between the $\omega(w)$ for $w \in \mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times$ is that $\omega(\sqrt{-3}) = 0$ (since $p \equiv -1 \pmod 3$, $-3 \notin \mathbb{F}_p^\times$) and $\sum_w \omega(w) = 0$. Indeed, it is direct to check that $\omega : \mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times \to \mu_p(\mathbb{C}) \cup \{0\}$ is a bijection. Now, note that $\Sigma_{\mathcal{B},t} = \sum_{w \in \mathbb{F}_p^{\times 2} j^t/\mathbb{F}_p^\times} \omega(w)$, whence the conclusion.

The other claims are direct computations. □

Corollary 5.7.18 *Let $\ell \neq p$ be a prime. The following are equivalent:*

- *ℓ is exceptional.*
- *For any $\mathbb{F}_p$-basis $\mathcal{B}$ of $\mathbb{F}_{p^2}$, there exists a prime ideal $\lambda \subset \mathbb{Z}[\zeta_p]$ dividing ℓ such that the $\Sigma_{\mathcal{B},t} \pmod\lambda$ are all zero.*
- *There exists a $\mathbb{F}_p$-basis $\mathcal{B}$ of $\mathbb{F}_{p^2}$ such that ℓ divides the norm of the (nonzero) ideal $(\Sigma_{\mathcal{B},0}, \Sigma_{\mathcal{B},1}, \Sigma_{\mathcal{B},2})$.*
- *For any $\mathbb{F}_p$-basis $\mathcal{B}$ of $\mathbb{F}_{p^2}$, ℓ divides the norm of the (nonzero) ideal $(\Sigma_{\mathcal{B},0}, \Sigma_{\mathcal{B},1}, \Sigma_{\mathcal{B},2})$.*
- *For any primitive p-th root of unity $\zeta \in \overline{\mathbb{F}_\ell}$, there exists a third root of unity $j \in \mathbb{F}_{p^2}^\times$ such that*

$$\sum_{\substack{t \in \mathbb{F}_p \\ 1+t\sqrt{-3} \in \mathbb{F}_{p^2}^{\times 3} j}} \zeta^t \neq 0.$$

Proof. – Let $\mathcal{B}$ be any $\mathbb{F}_p$-basis of $\mathbb{F}_{p^2}$. Let $\lambda \subset \mathbb{Z}[\zeta_p]$ be a prime ideal. Then the $\Sigma_{\mathcal{B},t} \pmod\lambda$ are all zero if and only if the ideal $I_{\mathcal{B}} := (\Sigma_{\mathcal{B},0}\Sigma_{\mathcal{B},1}, \Sigma_{\mathcal{B},2})$ is contained in λ. Thus, given a prime number ℓ, there exists a prime ideal $\lambda \subset \mathbb{Z}[\zeta_p]$ with residue characteristic ℓ such that the $\Sigma_{\mathcal{B},t} \pmod\lambda$ are all zero if and only if the norm of $I_{\mathcal{B}}$ is divisible by ℓ.

To conclude, thanks to Remark 5.7.16, it is enough to prove that the Galois orbit of the ideal $I_{\mathcal{B}}$ does not depend on $\mathcal{B}$. Indeed, write $\mathcal{B} = (u, v)$ and let $\mathcal{B}' = (u', v')$ be another basis. Then, by Lemma 5.7.17, $I_{\mathcal{B}} = I_{\frac{v'}{v}\mathcal{B}} = I_{\left(\frac{v'u}{v}, v'\right)}$. We can write $\frac{v'u}{v} = au' + bv'$ for $(a, b) \in \mathbb{F}_p^\times \times \mathbb{F}_p$, so that, by Lemma 5.7.17, $I_{\mathcal{B}'} = I_{(u',v')} = I_{(u'+ba^{-1}v',v')} = \underline{a}^{-1} I_{(au'+bv',v')} = \underline{a}^{-1} I_{\mathcal{B}}$. □

Proposition 5.7.19 *Let (α, β) be the adapted basis of $\mathbb{F}_{p^2}$. Let $a \in \mathbb{F}_p^\times$ and $M \in \mathrm{SL}_2(\mathbb{F}_p)$, write $\begin{pmatrix}\alpha'\\ \beta'\end{pmatrix} = M^{-1}\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$. Then, for any $f' \in G_{\mathbb{Q}} \cdot f$, $a \in \mathbb{F}_p^\times$ and $i \in \{0, 1, 2\}$, one has*

$$(M\Delta_{a,1})^* \left[\left(f'\left(\frac{\tau}{p}\right) \otimes \Delta_{a^{-1},1} \right) \mid \sum_{r=0}^{\frac{p+1}{3}-1} \Delta_{(\det g)^{-3r},1}\, g^{3r} \zeta_3^i \right] = \left(\sum_{n \geq 1} a_n(f') E_n e^{\frac{2i\pi n\tau}{p}} \right) \otimes \Delta_{1,1},$$

where

- *$E_n \in \mathbb{Z}[\zeta_p]$ for every $n \geq 1$,*
- *If $p \nmid n$, then $E_n = \underline{a^{-1}n}(\Sigma_{(\alpha',\beta'),i})$,*
- *If $p \mid n$, one has $E_n = -\frac{2(p+1)}{3}$ if $\beta' \in \mathbb{F}_{p^2}^{\times 3} j^i$, and $E_n = \frac{p+1}{3}$ otherwise.*

Proof. – First, note that

$$\begin{aligned}(M\Delta_{a,1})^* &\left[\left(f'\left(\frac{\tau}{p}\right) \otimes \Delta_{a^{-1},1} \right) \mid \sum_{r=0}^{\frac{p+1}{3}-1} \Delta_{(\det g)^{-3r},1}\, g^{3r} \zeta_3^i \right] \\ &= \left(\sum_{r=0}^{\frac{p+1}{3}-1} f'\left(\frac{\tau}{p}\right) \mid \Delta_{(a(\det g)^{3r})^{-1},1}\, g^{3r} \zeta_3^i M \Delta_{a,1} \right) \otimes \Delta_{1,1}.\end{aligned}$$

For $0 \leq r < \frac{p+1}{3}$, the classes in $\mathbb{P}^1(\mathbb{F}_p)$ of the first rows of the $g^{3r}\zeta_3^i$ are the same as the classes of the $(u, v) \in \mathbb{P}^1(\mathbb{F}_p)$ such that $u\alpha + v\beta \in \mathbb{F}_{p^2}^{\times 3} j^i$. Now, if $g^{3r}\zeta_3^i = z\begin{pmatrix}u & v\\ * & *\end{pmatrix}$, then the first row of $\Delta_{(a(\det g)^{3r})^{-1},1}\, g^{3r}\zeta_3^s M\Delta_{a,1}$ is proportional to $(u', v') := (a(u[M]_{1,1} + v[M]_{2,1}), u[M]_{1,2} + v[M]_{2,2})$, which are exactly the coordinates of $u\alpha + v\beta$ in the basis $(a^{-1}\alpha', \beta')$.

By Lemma 5.7.14, when $p \nmid n$, we obtain the expression $E_n = \underline{n}\Sigma_{(\alpha'/a,\beta),i} = \underline{na^{-1}}\Sigma_{(\alpha',\beta'),i}$ by Lemma 5.7.17. When $p \mid n$, Lemma 5.7.14 implies that the n-th coefficient in the q-expansion of $f'\left(\frac{\tau}{p}\right) \mid \Delta_{(a(\det g)^{3r})^{-1},1}\, g^{3r}\zeta_3^i M\Delta_{a,1}$ is $a_n(f')$ if $u' \neq 0$, and $-pa_n(f')$ if $u' = 0$. By the above, $u' = 0$ occurs as a term for $g^{3r}\zeta_3^i M$ (for some $0 \leq r < \frac{p+1}{3}$) if and only if $\beta' \in \mathbb{F}_{p^2}^{\times 3} j^i$. The conclusion follows. □

The following consequence of this computation is enough to finish the proof of Proposition 5.7.2, by Corollary 5.7.11. For this proof, we need the precise definition of the algebraic q-expansion given in Section 1.6, as well as its link to the complex uniformization spelled out in Proposition 2.4.4.

Proposition 5.7.20 *Let $\ell \equiv \pm 1 \pmod{p}$ be a non-exceptional prime number and $\mathfrak{l} \subset \mathcal{O}_F$ be a prime ideal with residue characteristic ℓ. Then, for every $c \in X(p,p)_{\mathcal{O}_{F,\mathfrak{l}}}$ lying in the special fibre of the cuspidal subscheme, there exists a differential $\omega \in H^0(X(p,p)_{\mathcal{O}_{F,\mathfrak{l}}}, \Omega^1_{X(p,p)_{\mathcal{O}_{F,\mathfrak{l}}}/\mathcal{O}_{F,\mathfrak{l}}})$ such that $\mathfrak{I} \cdot \omega = 0$, and $\omega_c \notin \mathfrak{m}_{X(p,p)_{\mathcal{O}_{F,\mathfrak{l}},c}}\, \Omega^1_{X(p,p)_{\mathcal{O}_{F,\mathfrak{l}}}/\mathcal{O}_{F,\mathfrak{l},c}}$.*

Proof. – By Proposition 1.6.14 and Corollary 1.6.8, it is enough to show the following: for any $\Lambda \in \mathrm{Surj}_p$, there is a cusp datum (M, Λ) such that, for any maximal ideal λ of the finite étale $\mathcal{O}_{F,\mathfrak{l}}$-algebra $R := \mathbb{Z}[1/p, \zeta_p] \otimes \mathcal{O}_{F,\mathfrak{l}}$, there exists a differential $\omega \in H^0(X(p,p)_{\mathcal{O}_{F,\mathfrak{l}}}, \Omega^1_{X(p,p)_{\mathcal{O}_{F,\mathfrak{l}}}/\mathcal{O}_{F,\mathfrak{l}}})$

such that $\mathfrak{I} \cdot \omega = 0$ and the first coefficient of $C^*_{(M,\Lambda)}\omega \in R \otimes (\mathbb{Z}[1/p])[[q^{1/p}]]$ is not contained in λ.

Let $\Lambda \in \mathrm{Surj}_p$. Let $\gamma \in \mathrm{SL}_2(\mathbb{F}_p)$ be such that $\Lambda = \Lambda_0 \circ \gamma^T$, where $\Lambda_0 : (x, y) \in \mathbb{F}_p^{\oplus 2} \mapsto x \in \mathbb{F}_p$. Let (M, Λ) be a cusp datum such that $C_{(M,\Lambda)} = \gamma \circ C_{(I_2,\Lambda_0)}$ by Lemma 1.6.17. Thus, for any differential $\omega \in H^0(X(p,p)_{\mathbb{C}}, \Omega^1_{X(p,p)_{\mathbb{C}}/\mathbb{C}})$, one has $C^*_{(M,\Lambda)}\omega = C^*_{(I_2,\Lambda_0)}(\gamma^*\omega)$.

Since γ^* is an automorphism of $H^0(X(p,p)_{\mathcal{O}_{F,\mathfrak{l}}}, \Omega^1_{X(p,p)_{\mathcal{O}_{F,\mathfrak{l}}}/\mathcal{O}_{F,\mathfrak{l}}})$, it is enough to prove the following statement by Proposition 1.6.15: for any maximal ideal λ of $\mathbb{Z}[\zeta_p] \otimes \mathcal{O}_{F,\mathfrak{l}}$, there exists $\omega \in H^0(X(p,p)_{\mathbb{C}}, \Omega^1_{X(p,p)_{\mathbb{C}}/\mathbb{C}})$ such that $\mathfrak{I} \cdot \omega = 0$, the q-expansion of $\gamma^*\omega$ is contained in $R \otimes (\mathbb{Z}[1/p])[[q^{1/p}]]$, and its first coefficient is not contained in λ.

Since the automorphisms of $\mathbb{Z}[\zeta_p]$ act transitively on the set of maximal ideals of R, it is enough to prove the following statement by Lemma 1.6.16: let $\lambda_0 \subset \mathbb{Z}[\zeta_p] \otimes \mathcal{O}_{F,\mathfrak{l}}$ be the kernel of the morphism $\zeta_p \otimes z \in \mathbb{Z}[\zeta_p] \otimes \mathcal{O}_{F,\mathfrak{l}} \mapsto ze^{-\frac{2i\pi}{p}} \in \mathbb{C}$ of $\mathcal{O}_F$-algebras. Then, for every $a \in \mathbb{F}_p^\times$, there exists $\omega \in H^0(X(p,p)_{\mathbb{C}}, \Omega^1_{X(p,p)_{\mathbb{C}}/\mathbb{C}})$ such that

$$\mathfrak{I} \cdot \omega = 0, \quad C^*_{(I_2,\Lambda_0)}\left(\Delta^*_{1,a}\gamma^*\omega\right) = C^*_{(I_2,\Lambda_0)}\left[(\gamma\Delta_{1,a})^*\omega\right] \in (R \backslash \lambda_0) + q^{1/p}(R \otimes (\mathbb{Z}[1/p])[[q^{1/p}]]).$$

We take

$$\omega_i = \iota_{p,p}^{-1}\left(\left(f'\left(\frac{\tau}{p}\right) \otimes \Delta_{a^{-1},1}\right) \mid \sum_{r=0}^{\frac{p+1}{3}-1} \Delta_{(\det g)^{-3r},1}\, g^{3r}\zeta_3^i\right)$$

for each $i \in \{0, 1, 2\}$.

The differential ω_i is annihilated by $\mathfrak{I}$ by Proposition 5.7.13. By Proposition 5.7.19 and Corollary 2.4.5, one has

$$C^*_{(I_2,\Lambda_0)}\left[(\gamma\Delta_{1,a})^*\omega_i\right] = C^*_{(I_2,\Lambda_0)}\left[(\gamma\Delta_{a^{-1},a}\Delta_{a,1})^*\omega_i\right] \in R \otimes (\mathbb{Z}[1/p])[[q^{1/p}]].$$

By Propositions 5.7.19 and 2.4.4, the image in $(\mathbb{Z}[\zeta_p] \otimes \mathcal{O}_{F,\mathfrak{l}})_{\lambda_0}$ of the first coefficient of $C^*_{(I_2,\Lambda_0)}\left[(\gamma\Delta_{1,a})^*\omega_i\right]$ is $\Sigma_{(\alpha,\beta),i}$ for a certain $\mathbb{F}_p$-basis (α, β) of $\mathbb{F}_{p^2}$. Since ℓ is not exceptional, one of the $\Sigma_{(\alpha,\beta),i}$ is not contained in λ_0, so the corresponding ω_i suits the conditions. □

5.8 Diophantine consequences for the elliptic curve $y^2 = x^3 - p$

In this section, $p \geq 11$ is a prime such that $p \equiv 5 \pmod 9$.

Lemma 5.8.1 *The Weierstrass equation $y^2 = x^3 - p$ over $\mathbb{Z}$ is minimal with discriminant $-2^4 \cdot 3^3 \cdot p^2 = -432p^2$ is minimal. It defines an elliptic curve $E_p/\mathbb{Q}$ with complex multiplication by $\mathbb{Z}[e^{2i\pi/3}]$ and conductor $108p^2$ if $p \equiv -1 \pmod 4$ and $432p^2$ if $p \equiv 1 \pmod 4$.*

Proof. – By [153, Chapter III.1], the discriminant of the Weierstrass equation is

$$\Delta = -\frac{(-216)^2(-4p)^2}{1728} = -2^{-6} \cdot 2^6 \cdot 3^{-3} \cdot 3^6 \cdot 2^4 \cdot p^2 = -2^4 \cdot 3^3 \cdot p^2 = -432p^2.$$

Since it is not divisible by a twelfth power, the Weierstrass equation is minimal by [153, Remark VII.1.1]. The elliptic curve E_p has complex multiplication by $\mathbb{Z}[e^{2i\pi/3}]$, since $(x, y) \longmapsto (xe^{2i\pi/3}, y)$ is an automorphism of $(E_p)_{\mathbb{Q}(e^{2i\pi/3})}$ of order 3. We compute that $j(E_p) = 0$, hence E_p has potentially good reduction everywhere by [153, Proposition VII.5.5], thus multiplicative reduction nowhere by [153, Proposition VII.5.4], therefore $2, 3, p$ are primes of additive reduction for E_p. In particular, $36p^2$ divides the conductor N_p of E_p and $v_p(N_p) = 2$ by [152, Theorem IV.10.2].

To compute the conductor exponents at 2 and 3, we apply Tate's algorithm [152, Theorem IV.9.4]. At 3, we stop of Step 3 of *loc.cit.* and the reduction type is II with conductor exponent $v_3(\Delta) = 3$. At 2, we stop at Step 3 if $p \equiv 1 \pmod 4$ – in which case the reduction is Type II

and the conductor exponent is $v_2(\Delta) = 4$ – and at Step 5 if $p \equiv -1 \pmod 4$ – in which case the reduction is of type IV and the conductor exponent is $v_2(\Delta) - 2 = 2$. □

Proposition 5.8.2 *The image of $G_{\mathbb{Q}}$ in $\mathrm{Aut}(E_p[p])$ is exactly the normalizer N of a nonsplit Cartan subgroup C. Moreover, the image of an inertia subgroup I_p at p is exactly $3C$.*

Proof. – The image of $\mathbb{Z}[e^{2i\pi/3}]$ in $\mathrm{End}(E_p[p]) \simeq \mathcal{M}_2(\mathbb{F}_p)$ is exactly $C \cup \{0\}$ for some nonsplit Cartan subgroup C, because $\mathbb{F}_p$ does not contain a primitive third root of unity.

Let $f : G_{\mathbb{Q}} \to \mathrm{Aut}(E_p[p])$ be the morphism. For any prime number q, let $I_q \leq G_{\mathbb{Q}}$ be an inertia subgroup at q. Now, $f(G_{\mathbb{Q}(\mu_3)})$ commutes with the image of $\mathbb{Z}[e^{2i\pi/3}] = \mathrm{End}_{\mathbb{Q}[e^{2i\pi/3}]}(E_p)$ in $\mathrm{End}(E_p[p])$, so $f(G_{\mathbb{Q}(\mu_3)}) \subset C$. Hence $f(G_{\mathbb{Q}})$ is contained in the normalizer N of C.

By Lemma 5.7.3, the conductor exponent of the $\mathbb{F}_p[G_{\mathbb{Q}}]$-module $E_p[p]$ at 3 is the same as the conductor of E_p, hence is 3. In particular, the action of the inertia at 3 on the p-torsion is wildly ramified, so $f(I_3)$ (hence $f(G_{\mathbb{Q}})$) contains an element of order 3. By Lemma 5.4.1, $f(I_p) \supset 3C$. By Proposition 5.2.1, $f(G_{\mathbb{Q}}) \not\subset C$. In particular, $f(G_{\mathbb{Q}})/3C$ is a subgroup of $N/3C \simeq \mathfrak{S}_3$ containing an element of order 3 and not equal to the cyclic subgroup of order 3. Hence $f(G_{\mathbb{Q}}) = N$.

Since $f(I_p) \subset C$, $f_{|I_p}$ is isomorphic to the representation $\begin{pmatrix} \chi^{k-1} & 0 \\ 0 & \chi^{p(k-1)} \end{pmatrix} : I_p \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$, where k is the Serre weight of f (see [145, §2.2]) and $\chi : I_p \to \mathbb{F}_{p^2}^\times$ is the fundamental character of inertia of level 2, which is a surjection $I_p \to \mathbb{F}_{p^2}^\times$. By [95, Théorème 1], the Serre weight of the representation f is $\frac{p^2+6p+5}{6} = \frac{(p+1)(p+5)}{6}$. We can write $p = 18t+5$, then the Serre weight of f is $\frac{(18t+6)(18t+10)}{6} = (3t+1)(18t+10) \equiv 1 \pmod 3$. Therefore, $\chi^{k-1}(I_p)$ is contained in the cubes of $\mathbb{F}_{p^2}^\times$, whence $f(I_p) \subset 3C$. □

Proposition 5.8.3 *Let $C \leq \mathrm{GL}_2(\mathbb{F}_p)$ be a nonsplit Cartan subgroup with normalizer N. Let (P, Q) be a basis of $E_p[p](\overline{\mathbb{Q}})$ such that the morphism $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ satisfying*

$$\rho(\sigma) \begin{pmatrix} \sigma(P) \\ \sigma(Q) \end{pmatrix} = \begin{pmatrix} P \\ Q \end{pmatrix}$$

has image N. Let $\psi : C \to F^\times$ be a character of order 3, and g be the modular form attached to the odd, irreducible, Artin representation $\left(\mathrm{Ind}_C^N \psi\right) \circ \rho$. Then g is given by the LMFDB label [107] 108.1.c.a[10].

Proof. – We already saw that $\left(\mathrm{Ind}_C^N \psi\right) \circ \rho$ was attached to a weight one modular form g with complex multiplication by $\mathbb{Q}(\sqrt{-3})$. The nebentypus of g is exactly the character of $\mathbb{Q}(\sqrt{-3})$, since $\det\left[\mathrm{Ind}_C^N \psi\right]$ is the unique nontrivial character of N/C. Since the traces of the representation $\mathrm{Ind}_C^N \psi$ of N are $2, 0, -1$, g has rational coefficients by strong multiplicity one [121, Theorem 4.6.19].

By Proposition 5.8.2, $\rho_g := \left(\mathrm{Ind}_C^N \psi\right) \circ \rho$ is unramified at p, so by [37, Théorème 4.6] the conductor of g is exactly the conductor of the Galois representation ρ_g, which is only ramified at 2 and 3. Let us now determine the conductor exponents.

We start at 3. Since ψ realizes an isomorphism of the 3-torsion subgroup of C on $\psi(C)$, the reduction modulo p of ρ_g has the same restriction to the wild inertia subgroup at 3 as $E_p[p]$. Therefore, the Swan conductor exponent of $E_p[p]$ at 3 and the Swan conductor exponent of g at 3 are equal. Moreover, E_p has additive reduction at 3, so the tame part of the conductor exponent of E_p is 2. Since the subgroup C has no invariants in the representation $\mathrm{Ind}_C^N \psi$, the tame part of the conductor exponent of g at 3 is also equal to 2, so the conductor exponent of g at 3 is 3.

Now, we discuss the prime 2. Because $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$ is unramified at 2, the image under ρ of an inertia subgroup I_2 at 2 is contained in C. This implies that ρ_g is tamely ramified at 2, and

[10] Its q-expansion is $q - q^7 - q^{13} - q^{19} + q^{25} + 2q^{31} + \cdots$

that its conductor exponent is zero if $\rho(I_2)$ does not meet the 3-torsion subgroup in C, and 2 if $\rho(I_2)$ contains the 3-torsion subgroup of C. Since E_p has potentially good reduction at 2 and C is cyclic, by [146, Corollary 1 to Theorem 2], the conductor exponent of ρ_g is zero (resp. 2) if E_p acquires good reduction at 2 on an extension of $\mathbb{Q}_2$ with ramification index coprime to 3 (resp. divisible by 3).

If $L/\mathbb{Q}_2$ is the extension on which E_p acquires good reduction, then the normalized valuation over L of the minimal discriminant of E over $\mathbb{Q}_2$ is divisible by 12 by the formulas of [153, Chapter III.1], which implies that $v_L(2) \in 3\mathbb{Z}$, so the conductor of g is 108.

By the LMFDB [107], there is exactly one newform with rational coefficients and complex multiplication by $\mathbb{Q}(\sqrt{-3})$ in $\mathcal{S}_1(\Gamma_1(108))$, whence the conclusion.

□

Proposition 5.8.4 *There exists a constant $p_0 \geq 11$ such that, for any prime $p \geq p_0$ congruent to 5 modulo 9, for any elliptic curve E' such that $E'[p](\overline{\mathbb{Q}})$ is isomorphic, as a $G_{\mathbb{Q}}$-module, to the p-torsion of the elliptic curve E_p. Then the conductor of E' is of the form $108mp^2L$, where L is a square-free product of exceptional primes for p, and $m = 1$ if $p \equiv 3 \pmod 4$ and $m = 4$ if $p \equiv 1 \pmod 4$.*

Proof. – By Theorem 5.7.2, the conclusion of the Proposition holds if there is $f \in \mathcal{S}_2(\Gamma_0(p))$ such that $L(f \times g, 1) \neq 0$, where g is the newform with LMFDB label [107] 108.1.*c.a* as in Proposition 5.8.3. That there exists such an f is given by a result of analytic number theory due to Michel [157, Appendix, Theorem 0.1], since in this case the sign of the functional equation for $L(f \times g, s)$ is $+1$. □

Remark For small enough p, one can also test the non-vanishing of the Rankin-Selberg L-value required by Theorem 5.7.2 numerically. Thanks to the help of Pascal Molin, I was able to check in PARI/GP that the conclusion of Theorem 5.7.2 held when $p = 23$. In this case, we can also check directly that there are no exceptional primes, so the conductor of E' is $108p^2 = 57132$. By [33, Theorem 1.3], the only elliptic curves of conductor $108p^2$ congruent modulo p to E_p are isogenous to E_p. Therefore[11], for $p = 23$, any elliptic curve congruent modulo p to E_p is isogenous to E_p.

[11] Further computations after the submission of this thesis showed that there were no exceptional primes for p when $p \equiv 2, 5 \pmod 9$ and $11 \leq p \leq 5000$, and that the conclusion of Theorem 5.7.2 held for p and the elliptic curve E_p when $23 \leq p \leq 150$ and $p \equiv 5 \pmod 9$. Thus, any elliptic curve congruent modulo $p \in \{23, 41, 59, 113, 131, 149\}$ to E_p has the same conductor as E_p and integral j-invariant. Finally, [33, Theorem 1.3] also applies for $p = 59$ and $p = 41$ (the latter after a suitable quadratic twist).

Chapter 6

On obstructions to the Euler system method for Rankin-Selberg convolutions

6.1 Introduction

Let $k, N \geq 1$ be integers. We denote by $\mathcal{S}_k(\Gamma_1(N))$ the space of cuspidal holomorphic modular forms with level $\Gamma_1(N)$. Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a cuspidal newform with character ε_f, and L be a number field containing its coefficients. Given a prime ideal $\mathfrak{p} \subset \mathcal{O}_L$, we can attach to f a free $\mathcal{O}_{L_\mathfrak{p}}$-module T_f of rank two endowed with a continuous linear action of $G_\mathbb{Q} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Works of Momose [122] and Ribet [133] show that, when f has no complex multiplication and $k \geq 2$, the image of $G_\mathbb{Q}$ in $\mathrm{Aut}(T_f) \cong \mathrm{GL}_2(\mathcal{O}_{L_\mathfrak{p}})$ contains a conjugate of $\mathrm{SL}_2(\mathbb{Z}_p)$ for all but finitely many $\mathfrak{p}$. More recently, Loeffler [108] proved an *adelic* open image theorem for such newforms, the analog of that of Serre [141] for elliptic curves without complex multiplication.

Let $g \in \mathcal{S}_l(\Gamma_1(M))$ be another newform with character ε_g; after enlarging L if necessary, we assume that its Fourier coefficients are contained in L. As above, we attach to g a free $\mathcal{O}_{L_\mathfrak{p}}$-module of rank two T_g endowed with a continuous linear action of $G_\mathbb{Q}$. Let $T := T_f \otimes_{\mathcal{O}_{L_\mathfrak{p}}} T_g$. The other goal of [108] was to study the image of $G_\mathbb{Q}$ in $\mathrm{Aut}(T)$. In particular, Loeffler proves that, when the following conditions are satisfied:

- $k, l \geq 2$,
- neither f nor g has complex multiplication,
- f and g are not twists one of another,
- $\varepsilon_f \varepsilon_g \neq 1$,

then, for all but finitely many $\mathfrak{p}$, there exists a $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{p^\infty}))$ such that $T/(\sigma - 1)T$ is free of rank one. Loeffler also discusses the case of $k \geq 2, l = 1$ and asks the following question:

Question 6.1.1 *(Loeffler, see [108, Remark 4.4.2]) Assume that $k \geq 2$, $l = 1$, f does not have complex multiplication, and $\varepsilon_f \varepsilon_g \neq 1$. Then does there exist, for all but finitely many $\mathfrak{p}$, $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$ such that $T/(\sigma - 1)T$ is free of rank one?*

Loeffler proves in [108, Proposition 4.4.1] that the answer is positive when N and M are coprime.

Here is a few of the weaker sufficient conditions one can use to answer the question in the affirmative.

Theorem 6.A *The answer to Question 6.1.1 is positive when any of the following conditions hold:*

- *For any (primitive) Dirichlet character χ with conductor C such that $f \otimes \chi$ is Galois-conjugate to f, C is coprime to M (in particular when f has no inner twist).*
- *Any (primitive) Dirichlet character χ such that $f \otimes \chi$ is Galois-conjugate to f is even.*
- *$\varepsilon_f^2 = \varepsilon_g^2 = 1$ and $f \otimes \varepsilon_g$ is not Galois-conjugate to f.*
- *The group $\varepsilon_g\left(\bigcap_\chi \ker\chi\right)$ contains an element of order 2 but no element of order 4, where χ runs through (primitive) Dirichlet characters such that $f \otimes \chi$ is Galois-conjugate to f.*

As a consequence, we obtain the following instance of the Bloch-Kato conjecture, which extends [92, Theorem 11.7.4] by removing some assumptions.

Recall the following definition:

Definition 6.1.2 Let E be an elliptic curve over a number field K, and p be a prime number. The p^∞-Selmer group of E is the subgroup

$$\mathrm{Sel}_{p^\infty}(E/K) = \ker\left[H^1(K, E[p^\infty]) \to \prod_v H^1(K_v, E(\overline{F_v}))\right],$$

where v runs over the finite places of K and the map is induced by localizing at the place v and the inclusion $E[p^\infty] \subset E$.

Theorem 6.B *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication and ρ be an odd two-dimensional irreducible representation of $G_\mathbb{Q}$, with splitting field K and coefficients in some number field L_0 with ring of integers $\mathcal{O}$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}$ with residue characteristic p. Suppose that the following assumptions hold:*

1. *p is coprime to $30N_\rho N_E$, where N_E (resp. N_ρ) is the conductor of E (resp. ρ),*
2. *if ρ has dihedral projective image D, then the maximal cyclic subgroup of D is not a p-group,*
3. *the map $G_\mathbb{Q} \to \mathrm{Aut}(T_pE)$ given by the Galois action on the p-adic Tate module of E is onto,*
4. *E is ordinary at p and $\rho(\mathrm{Frob}_p)$ has distinct eigenvalues mod $\mathfrak{p}$.*

If $L(E, \rho, 1) \neq 0$, then the group $\mathrm{Hom}_{\mathbb{Z}_p[\mathrm{Gal}(\mathrm{F}/\mathbb{Q})]}(\rho, \mathrm{Sel}_{p^\infty}(E/F))$ is finite.

We show, less constructively:

Theorem 6.C *If one replaces "for all but finitely many $\mathfrak{p}$" with "for infinitely many $\mathfrak{p}$" in Question 6.1.1, then the answer is positive.*

We also show that the general answer to Question 6.1.1 is negative. Among other counter-examples, we find:

Theorem 6.D *(See Section 6.4) Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a newform with character ε_f without complex multiplication. Suppose that one of the following conditions holds:*

- *k is even and there exists a primitive Dirichlet character χ such that $f \otimes \chi$ is Galois-conjugate to χ.*
- *$k \geq 3$ is odd, and there exist two Dirichlet characters χ_1, χ_2 such that each $f \otimes \chi_i$ is Galois-conjugate to f, and none of the restrictions to $\ker\varepsilon_f$ of $\chi_1, \chi_2, \chi_1\chi_2$ are trivial.*

Then there exist infinitely many dihedral newforms $g \in \mathcal{S}_1(\Gamma_1(M))$ such that the answer to Question 6.1.1 for (f, g) is negative.

Theorem 6.E *There exist newforms $f \in \mathcal{S}_2(\Gamma_0(63)), g \in \mathcal{S}_1(\Gamma_1(1452))$ with coefficients respectively in $\mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{-3})$ satisfying the following property: for all but finitely many prime ideals $\mathfrak{p}$ of $L = \mathbb{Q}(e^{2i\pi/12})$ with residue characteristic $p \equiv 5, 7 \pmod{12}$, there is no $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$ such that $\ker\left(\sigma - \mathrm{id} \mid T_{f,\mathfrak{p}} \otimes_{\mathcal{O}_{L_\mathfrak{p}}} T_{g,\mathfrak{p}}\right) \otimes_{\mathcal{O}_{L_\mathfrak{p}}} L_\mathfrak{p}$ is a $L_\mathfrak{p}$-line.*

Remarks

(i) The statement of Theorem 6.B can be generalized by replacing elliptic curves with, for instance, abelian varieties attached to newforms of weight 2, with only minimal changes to the proof. One would need to adapt the big image hypothesis, for instance by ensuring that the conclusion of Theorem 6.A holds.

(ii) As explained in [92, Remark 11.7.5(i)], applying Theorem 6.B at a single prime shows that $\mathrm{Hom}_{\mathcal{O}[G_{\mathbb{Q}}]}(\rho, E(K)\otimes\mathcal{O})$ is zero. When generalizing Theorem 6.B to more general modular forms, Theorem 6.C would imply that, provided that the special value is not zero, the relevant Mordell-Weil group is torsion. The point of Theorem 6.B is to prove that, in addition, the ρ-part of $Ш(E/K)[p^\infty]$ is finite for a positive density of such primes p.

(iii) When $f \in \mathcal{S}_k(\Gamma_1(N))$, and $g \in \mathcal{S}_l(\Gamma_1(M))$ are newforms with characters $\varepsilon_f, \varepsilon_g$ respectively, then the Dirichlet character $\varepsilon_f\varepsilon_g$ has the same parity as $k+l$. In particular, when k is even and $l=1$, $\varepsilon_f\varepsilon_g$ is odd, so cannot be trivial. The counter-examples in Theorem 6.D and 6.E are thus non trivial.

(iv) In the counter-example of Theorem 6.E, g has complex multiplication, f has even weight and an odd inner twist. While the answer to Question 6.1.1 is negative, this does not follow from the proof of Theorem 6.D. Further counter-examples are given in Section 6.5.

The existence of a σ as in Question 6.1.1 is important, because it seems necessary to apply the theory of Euler systems (see for instance [114]), which aims to bound Selmer groups assuming the nonvanishing of certain p-adic L-functions. For the Galois-modules that we consider in this article, the Euler system would typically be the system of Beilinson-Flach elements constructed in [92]. We do not see any reason why, for all our couples (f,g) of counter-examples, the central archimedian Rankin-Selberg L-value $L(f\otimes g, 1)$ should vanish.

Hence, consider a couple (f,g) that is a counter-example to Question 6.1.1 and assume that $L(f\otimes g,1)\neq 0$. Should one expect that, as in [92, Theorem 11.7.3], for almost all primes p ordinary for f and g and such that f,g are p-distinguished[1], the Nekovář cohomology group $\widetilde{H}^2\left(\mathcal{O}_L\left[\frac{1}{N_fN_gp}\right], T_f\otimes T_g; \Delta^{BK}\right)$ is finite[2]? However, how to go about proving such a statement without the theory of Euler systems does not seem clear at all.

Acknowledgements I would like thank Loïc Merel for encouraging me to work on this project. His careful reading and many comments helped me vastly improve the original version of this text. I would also like to thank David Loeffler for his help regarding the application of these results to the twisted Birch and Swinnerton-Dyer conjecture.

6.2 The big image theorem for one modular form

We first recall well-known results on twists and Galois conjugates of modular forms. This lets us define inner twists, who are crucial to stating the large image theorem for one modular form.

The results on twists are mostly taken from [104], the lemmas on inner twists come from [122], and the presentation of the results on Galois images of this section comes almost entirely from [108, Section 2].

First, we recall the definition and well-known properties (see [104, 121]) of twists of newforms by Dirichlet characters.

Proposition 6.2.1 *Let $f\in\mathcal{S}_k(\Gamma_1(N))$ be a newform with character ε_f of conductor M. Let χ be a primitive Dirichlet character of conductor C. There exists a unique new, cuspidal eigenform $f\otimes\chi\in\mathcal{S}_2(\Gamma_1(L))$ such that, for every prime number $p\nmid NC$, $a_p(f\otimes\psi)=a_p(f)\psi(p)$. We say that $f\otimes\chi$ is the* twist *of f by χ. Moreover:*

[1] In the situation of Theorem 6.E, this last property holds for example when $p\equiv 5 \pmod{12}$, or when $p\equiv 7 \pmod{12}$ and $\left(\frac{p}{11}\right)=-1$.

[2] The statement of the theorem in *loc. cit.* seems to contain a slight typo; one should (probably) read $M_{\mathcal{O}}(f\otimes g)^*$ instead of $M_{\mathcal{O}}(f\otimes g)$.

(a) *The character of $f \otimes \chi$ is the primitive Dirichlet character associated to $\varepsilon_f \chi^2$.*
(b) *L divides the least common multiple P of N, CM, C^2.*
(c) *For every prime number $q \nmid C$, $v_q(L) = v_q(N)$.*
(d) *Let q be a prime number, and write $\chi = \chi_q \chi'$, where the conductor of χ_q is a power of q and that of χ' is coprime to q. Then $v_q(L)$ only depends on f and χ_q.*

Remark If ψ comes from the primitive Dirichlet character ψ_0, we will also denote by $f \otimes \psi$ the newform $f \otimes \psi_0$.

Proposition 6.2.3 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ and write its q-expansion $f(\tau) = \sum_{n \geq 1} a_n(f) q^n$. Let σ be any automorphism of $\mathbb{C}$. Then $\sigma(f)(\tau) = \sum_{n \geq 1} \sigma(a_n(f)) q^n \in \mathcal{S}_k(\Gamma_1(N))$. Moreover:*

(a) *If f has character ε_f, then $\sigma(f)$ has character $\sigma \circ \varepsilon_f$.*
(b) *If f is a newform, $\sigma(f)$ is a newform.*
(c) *If f is a newform, there is a number field containing all its coefficients.*

Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a newform with primitive character ε_f. Write its q-expansion as $f(\tau) = \sum_{n \geq 1} a_n(f) q^n$, and $L = \mathbb{Q}(a_n(f) \mid n \geq 1)$.

Let now $\gamma : L \to \mathbb{C}$ be a field homomorphism and χ be a primitive Dirichlet character. We say that f has an *inner twist* by (γ, χ) if the newforms $\gamma(f)$ and $f \otimes \chi$ are equal.

Lemma 6.2.4 *In such a situation, one can write $\chi = \lambda \varepsilon_f^t$, where $t \in \mathbb{Z}$ and λ is quadratic. Moreover, the conductor of χ divides N and $\gamma(L) = L$.*

Proof. – Apart from the bound on the conductor of χ, this is [122, Lemma 1.5 (i)].

Let C be the conductor of χ, and let p be a prime such that $v_p(C) > v_p(N)$. Then by [104, Theorem 4.1] and Proposition C.2.2(e), the p-adic valuation of the conductor of $f \otimes \chi$ is $v_p(N)$, and is also $2v_p(C)$, and we get a contradiction. □

Let Γ_f denote the set of (γ, χ) by which f has an inner twist.

Proposition 6.2.5 *The formula $(\alpha, \chi) \cdot (\beta, \psi) = (\alpha \circ \beta, \chi \alpha(\psi))$ endows Γ_f with an abelian group law. Moreover, the group homomorphism*

$$\pi : (\gamma, \chi) \in \Gamma_f \longmapsto \gamma \in \mathrm{Aut}(L)$$

satisfies exactly one of the following properties:

- *π is injective with abelian image. Then the fixed field of $\mathrm{im}(\pi)$ (which we identify to Γ_f) is a field F such that L/F is abelian with Galois group $\mathrm{im}(\pi) \cong \Gamma_f$.*
- *There exists some $(\mathrm{id}, \eta) \in \Gamma_f$ where η is the character of a quadratic field K which is only ramified at primes dividing N. If $k \geq 2$, then K is imaginary.*

Proof. – Checking that we have indeed defined a group law on Γ_f such that π is a homomorphism is formal.

Let $(\sigma, \alpha), (\tau, \beta) \in \Gamma_f$. Then we can write $\alpha = \alpha_2 \varepsilon^a$, $\beta = \beta_2 \varepsilon^b$, with $a, b \in \mathbb{Z}$ and α_2, β_2 quadratic. Then $\tau(\alpha)\alpha^{-1} = (\tau(\varepsilon)\varepsilon^{-1})^a = (\beta^2)^a = \varepsilon^{2ab}$: by symmetry $\tau(\alpha)\beta = \alpha\sigma(\beta)$. Because $\mathrm{Aut}(\mathbb{C})$ acts through an abelian quotient on $\mathbb{Q}(\varepsilon)$, a straightforward computation shows that Γ_f is abelian.

If π is injective, its image is an abelian subgroup of $\mathrm{Aut}(L)$. It is clear that L/F is finite separable. Since $\mathrm{Aut}_F(L) \supset \mathrm{im}(\pi)$, one has $[L : F] \geq |\mathrm{im}(\pi)|$. Conversely, if $\alpha \in L$ is a primitive element over F, the monic polynomial $R(X) = \prod_{\gamma \in \mathrm{im}(\pi)} (X - \gamma(\alpha)) \in L[X]$ vanishes at α and is stable under $\mathrm{im}(\pi)$, so lies in $F[X]$. Thus $[L : F] \leq [F(\alpha) : F] \leq \deg R \leq |\mathrm{im}(\pi)|$, which concludes.

Suppose that π is non-injective. Then there exists a nontrivial Dirichlet character χ such that $f \otimes \chi = f$. Thus $\varepsilon \chi^2 = \varepsilon$, so χ is quadratic. The rest follows from [132, (4.4, 4.5)] in weight $k \geq 2$. □

In the latter case, we say that f has *complex* (resp. *real*) *multiplication by* K if K is imaginary (resp. real). This is often shortened as "CM" (resp. "RM"), and we will omit K from the notation if it does not matter.

If f does not have CM, let F be the subfield of L fixed by the image of π, and let $H/\mathbb{Q}$ be the abelian field extension such that $G_H = \bigcap_{(\gamma,\chi)\in\Gamma_f} \ker\chi$, where χ is viewed as a character of $G_\mathbb{Q}$ through the cyclotomic character $G_\mathbb{Q} \to \hat{\mathbb{Z}}^\times$.

Let $\mathfrak{p} \subset \mathcal{O}_L$ be a prime ideal with finite residue characteristic p. It is well-known (see [132]) that there exists a group homomorphism $\rho_{f,\mathfrak{p}} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathcal{O}_{L_\mathfrak{p}})$ satisfying the following properties:

- $\rho_{f,\mathfrak{p}}$ is continuous, irreducible, and unramified away from pN.
- $\det\rho_{f,\mathfrak{p}} = \varepsilon\omega_p^{k-1}$, where ω_p is the p-adic cyclotomic character.
- For every prime $\ell \nmid pN$, $\mathrm{Tr}\,\rho_{f,\mathfrak{p}}(\mathrm{Frob}_\ell) = a_\ell(f)$, where Frob_ℓ is the arithmetic Frobenius.

Proposition 6.2.6 *(Momose [122, Theorem 4.2], Ribet [133, §3], Ghate–González-Jiménez–Quer [63, Corollary 4.7])*

Assume moreover that $p \nmid 2N$ is unramified in L and f does not have CM. Then $\rho_{f,\mathfrak{p}}(G_H)$ has a $\mathrm{GL}_2(\mathcal{O}_{L_\mathfrak{p}})$-conjugate contained in $\{M \in \mathrm{GL}_2(\mathcal{O}_{F_\mathfrak{p}}), \det M \in \mathbb{Z}_p^\times\}$.

Furthermore, for all but finitely many $\mathfrak{p}$, after conjugating $\rho_{f,\mathfrak{p}}$ by a suitable element of $\mathrm{GL}_2(\mathcal{O}_{L_\mathfrak{p}})$, the group homomorphism $(\rho_{f,\mathfrak{p}},\omega_p) : G_H \to \mathrm{GL}_2(\mathcal{O}_{F_\mathfrak{p}}) \times_{\mathcal{O}_{F_\mathfrak{p}}^\times} \mathbb{Z}_p^\times$ is onto (where the left map in the fibre product is the determinant, and the right one is $x \in \mathbb{Z}_p^\times \longmapsto x^{k-1} \in \mathcal{O}_{F_\mathfrak{p}}^\times$).

Proof. – This is [108, Theorem 2.2.2]. □

6.3 Special elements in the image of the convolution of two modular forms

Let p be an odd prime. Let $\mathcal{O}$ be the ring of integers of a finite extension K of $\mathbb{Q}_p$, with uniformizer ϖ and residue field k. Let T be a free $\mathcal{O}$-module of finite rank, endowed with a continuous and $\mathcal{O}$-linear action of $G_\mathbb{Q}$. Let G be the image in $\mathrm{Aut}(T)$ of $G_{\mathbb{Q}(\mu_{p^\infty})}$. Consider the following statements:

(N) $-\mathrm{id} \in G$.
(gI) $T \otimes_\mathcal{O} K$ is an irreducible $K[G]$-module.
(rI) $T \otimes_\mathcal{O} k$ is an irreducible $k[G]$-module.
(wE) There exists $u \in G$ such that $\ker(u-\mathrm{id}) \otimes K$ has dimension one.
(sE) There exists $u \in G$ such that $T/(u-1)T$ is free of rank one.

Definition 6.3.1 We say that T has Galois image *of Euler type* if it satisfies (N), (gI) and (wE). T has *Euler-adapted* Galois image if it satisfies (N), (rI) and (sE).

Note that (rI) implies (gI) (since any reducible $K[G]$-submodule can be reduced in k), and that (sE) implies (wE).

The statements (gI) and (wE) are the two parts of $\mathrm{Hyp}(\mathbb{Q}(\mu_{p^\infty}), T\otimes K)$ in the notation of [108, Section 4.1]. Similarly, (rI) and (sE) constitute in the same way $\mathrm{Hyp}(\mathbb{Q}(\mu_{p^\infty}), T)$. The condition (N) is not mentioned explicitly in [108], but is used in applications of this article to Euler systems, such as [92, Section 11]. Since it is not difficult to study, we include it here.

Let $k \geq 2$. Let $f \in \mathcal{S}_k(\Gamma_1(N_f))$, $g \in \mathcal{S}_1(\Gamma_1(N_g))$ be newforms with characters ε_f and ε_g, such that f has no complex multiplication. Let L, F, H be the number fields associated to f in the previous section, and $L_0 \subset \mathbb{C}$ be a number field containing L and all the coefficients of g.

If $\mathfrak{p} \subset \mathcal{O}_{L_0}$ is a prime ideal, we can construct the representation $T_{f,\mathfrak{p}}$ of $G_\mathbb{Q}$ as in the previous section by extension of scalars: it is a free $\mathcal{O}_{(L_0)_\mathfrak{p}}$-module of rank 2 with a continuous linear

action of $G_{\mathbb{Q}}$. When the residue characteristic of $\mathfrak{p}$ does not divide $2N_f$ or the discriminant of L, we endow $T_{f,\mathfrak{p}}$ with a basis such that the image of G_H is contained in $\mathrm{GL}_2(\mathcal{O}_{F_\mathfrak{p}})$.

By the work of Deligne and Serre [37, Théorèmes 4.1, 4.6, footnote p.521], there is an odd irreducible Artin representation $\rho_g : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{L_0})$ attached to g, and $\rho'_g : G_{\mathbb{Q}} \to \mathrm{PGL}_2(L_0)$ the corresponding projective representation, and we denote $Q = |\rho'_g(G_{\mathbb{Q}})|$. Let T_g be a free $\mathcal{O}_{L_0}$-module of rank 2 where $G_{\mathbb{Q}}$ acts as ρ_g. Let $T_{f,g,\mathfrak{p}} = T_{f,\mathfrak{p}} \otimes_{\mathcal{O}_{L_0}} T_g$.

Definition 6.3.2 A prime ideal $\mathfrak{p} \subset L_0$ is *good* for (f, g) if the following conditions are satisfied:

- Its residue characteristic p does not divide $30N_fN_g$ or ramify in L.
- $(T_{f,\mathfrak{p}}, \omega_p) : G_H \to \mathrm{GL}_2(\mathcal{O}_{F_\mathfrak{p}})^\times \times_{\mathcal{O}_{F_\mathfrak{p}}^\times} \mathbb{Z}_p^\times$ is surjective, where the fibre product maps are the determinant and the $(k-1)$-th power.

Proposition 6.3.3 *Let $\mathfrak{p}$ be a good prime. Then the image of $G_{H(\mu_{p^\infty})}$ in $\mathrm{Aut}(T_{f,\mathfrak{p}}) \times \mathrm{Aut}(T_g)$ is $\mathrm{SL}_2(\mathcal{O}_{F_\mathfrak{p}}) \times \rho_g(G_H)$.*

Proof. – Let I denote this image, and $K/\mathbb{Q}$ be the Galois extension such that $G_K = \ker \rho_g$. It is clear that $I \subset \mathrm{SL}_2(\mathcal{O}_{F_\mathfrak{p}}) \times \rho_g(G_H)$. Let $p_1 : I \to \mathrm{SL}_2(\mathcal{O}_{F_\mathfrak{p}})$, $p_2 : I \to \rho_g(G_H)$ be the two projections. Because $\mathfrak{p}$ is a good prime, p_1 is surjective. Moreover, p_2 is onto if and only if $H(\mu_{p^\infty}) \cap K \subset H$. Now, $H(\mu_{p^\infty}) \cap KH$ is a finite extension of H, so it is contained in $H(\mu_{p^n}) \cap KH$ for some n. Because $p \nmid N_f$, $H/\mathbb{Q}$ is unramified at p, so $H(\mu_{p^n})$ is totally ramified over H above p. Since $p \nmid N_g$, KH is unramified over H above p. We conclude that $H(\mu_{p^\infty}) \cap K \subset H(\mu_{p^\infty}) \cap KH = H$.

Therefore, all we need to do is show that I contains $\mathrm{SL}_2(\mathcal{O}_{F_\mathfrak{p}}) \times \{1\}$.

If $\rho_g(G_{\mathbb{Q}})$ is solvable, then $\rho'_g(G_{\mathbb{Q}})$ is dihedral or isomorphic to A_4 or S_4. In particular, $p_2(I^{(4)}) = p_2(I)^{(4)}$ is trivial (the derived subgroup of a compact group is, by definition, the closure of the subgroup generated by its commutators; here, we do this operation four times). Since $p > 3$, $\mathrm{SL}_2(\mathcal{O}_{F_\mathfrak{p}})$ is its own derived subgroup. Indeed, by [69, (1.2.11)], it is generated by transvections, and, if $\lambda, u \in \mathcal{O}_{F_\mathfrak{p}}$ are such that $\lambda(\lambda^2 - 1)$ is a unit, the following identity holds:

$$\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} 1 & \frac{u}{\lambda^2-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} 1 & \frac{-u}{\lambda^2-1} \\ 0 & 1 \end{pmatrix}.$$

Hence $p_1(I^{(4)}) = p_1(I)^{(4)} = \mathrm{SL}_2(\mathcal{O}_{F_\mathfrak{p}})$. Thus $I \supset I^{(4)} = \mathrm{SL}_2(\mathcal{O}_{F_\mathfrak{p}}) \times \{1\}$, and we are done.

Otherwise, one has $\rho'_g(G_{\mathbb{Q}}) \cong A_5$. Let $K_5 \subset K$ be such that $G_{K_5} = \ker \rho'_g$, and let $I_5 \subset I$ be the image of $G_{HK_5} = G_H \cap G_{K_5}$. It is enough to show that I_5 contains $\mathrm{SL}_2(\mathcal{O}_{F_\mathfrak{p}}) \times \{1\}$. Since $\rho_g(G_{HK_5}) \subset \rho_g(G_{K_5})$ is composed of scalar matrices, $p_2(I'_5)$ is trivial: as above, we just need to show that $p_1(I_5) = \mathrm{SL}_2(\mathcal{O}_{F_\mathfrak{p}})$.

Since $K_5/\mathbb{Q}$ has Galois group A_5, it does not contain any nontrivial abelian extension of $\mathbb{Q}$. Since $H/\mathbb{Q}$ is abelian, one has $H \cap K_5 = \mathbb{Q}$. Therefore, $p_1(I_5)$ is an open subgroup of $p_1(I) = \mathrm{SL}_2(\mathcal{O}_{F_\mathfrak{p}})$ with index dividing $|\mathrm{Gal}(HK_5/H)| = |A_5| = 60$. Let $z \in p_1(I)$ be any element conjugate to $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ (with a nonzero a): since $p > 5$, z is in the closed subgroup generated by $z^{|A_5|} \in p_1(I_5)$, hence $z \in p_1(I_5)$. Since $\mathrm{SL}_2(\mathcal{O}_{F_\mathfrak{p}})$ is generated by such elements z, $p_1(I_5) = p_1(I)$, which concludes.

□

Corollary 6.3.4 *Let $\mathfrak{p}$ be a good prime with residue characteristic p and $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$. There exists $\alpha \in L^\times \cap \mathcal{O}_{L_\mathfrak{p}}^\times$ such that for all $(\gamma, \chi) \in \Gamma_f$, one has $\gamma(\alpha) = \chi(\sigma)\alpha$. Moroever, the image of $\sigma G_{H(\mu_{p^\infty})}$ in $\mathrm{Aut}(T_{f,\mathfrak{p}}) \times \mathrm{Aut}(T_g)$ is $\left[\begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1}\varepsilon_f(\sigma) \end{pmatrix} \mathrm{SL}_2(\mathcal{O}_{F_\mathfrak{p}})\right] \times [\rho_g(\sigma)\rho_g(G_H)]$.*

Proof. – Let us briefly recall why α exists. For any $\gamma \in \mathrm{Gal}(L/F)$, there is a unique primitive Dirichlet character χ_γ such that $(\gamma, \chi_\gamma) \in \Gamma_f$. The map $\gamma \in \mathrm{Gal}(L/F) \longmapsto \chi_\gamma(\sigma) \in L^\times$ is a

cocycle: by Hilbert 90 (for instance [143, §X.1, Proposition 2]), it can be written as $\gamma \longmapsto \gamma(\beta)\beta^{-1}$ for some $\beta \in L^\times$. Since p is unramified in L, there is some $t \in \mathbb{Z}$ such that $\alpha = p^t\beta$ lies in $\mathcal{O}_{L_\mathfrak{p}}^\times$ and satisfies the required conditions.

By Proposition 6.3.3, the image in $\mathrm{Aut}(T_{f,\mathfrak{p}}) \times \mathrm{Aut}(T_g)$ of $\sigma G_{H(\mu_{p^\infty})}$ is $I_\sigma \times [\sigma\rho_g(G_H)]$, where I_σ is the image in $\mathrm{Aut}(T_{f,\mathfrak{p}})$ of $\sigma G_{H(\mu_{p^\infty})}$. Now, $I_\sigma = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1}\varepsilon_f(\sigma) \end{pmatrix} \mathrm{SL}_2(\mathcal{O}_{F_\mathfrak{p}})$ by [108, Corollary 2.2.3]. □

Lemma 6.3.5 *Let V, W be finite-dimensional vector spaces over a field k, and G_1, G_2 be subgroups of $GL(V)$ and $GL(W)$, acting irreducibly on V and W respectively. Let Γ be a subgroup of $GL(V)\times GL(W)$, containing $G_1 \times \{\mathrm{id}\}$ and such that its second projection is G_2. Then $V \otimes W$ is an irreducible $k[\Gamma]$-module.*

Proof. – Let $U \subset V \otimes W$ be a proper $k[\Gamma]$-submodule. Because G_1 acts irreducibly on V, U is contained in $V \otimes \ker\alpha$ for some nonzero $\alpha \in W^* := \mathrm{Hom}(W, k)$. Since $\Gamma \supset G_1 \times \{1\}$, the subspace $W' = \{\alpha \in W^*, \alpha(U) = 0\}$ is nonzero and stable under Γ. Since W^* is irreducible under G_2, $W' = W^*$, so that $U = 0$. □

Proposition 6.3.6 *If $\mathfrak{p}$ is a good prime, $T_{f,g,\mathfrak{p}}$ satisfies conditions (N) and (gI). Moreover, if $Q/2$ is not a power of p, then condition (rI) holds.*

Proof. – Proposition 6.3.3 shows that $G_H(\mu_{p^\infty})$ contains an element σ acting by $-I_2$ on $T_{f,\mathfrak{p}}$ and I_2 on T_g, which proves condition (N).

The condition (gI) follows from Proposition 6.3.3 and Lemma 6.3.5.

If $\rho_g(G_\mathbb{Q})$ acts absolutely irreducibly on $T_g/\mathfrak{p}$, then Proposition 6.3.3 and Lemma 6.3.5 imply condition (rI). Because of the complex conjugation, it is enough to show that $\rho_g(G_\mathbb{Q})$ acts irreducibly on $T_g/\mathfrak{p}$.

Suppose that $\rho_g(G_\mathbb{Q})$ acts reducibly on $T_g/\mathfrak{p}$. Then the semisimplification of this action is the direct sum of characters α and β of $\rho_g(G_\mathbb{Q})$. Thus $\gamma = \alpha/\beta$ is a character of $\rho_g(G_\mathbb{Q})$ and its kernel K consists of matrices whose reduction modulo $\mathfrak{p}$ is of the form $\begin{pmatrix} \alpha & * \\ 0 & \alpha \end{pmatrix}$. In particular, we have an exact sequence $0 \to K \to \rho_g(G_\mathbb{Q}) \to C \to 0$, where C is cyclic with order prime to p.

Let $h \in K$. Then h acts on $T_g/\mathfrak{p}$ with characteristic polynomial $(X-u)^2$, for some $u \in (\mathcal{O}_{L_0}/\mathfrak{p})^\times$ with Teichmüller lift $u_0 \in \mathcal{O}_{(L_0)_\mathfrak{p}}^\times$ be. Then $h' := u_0^{-1}h \in \mathrm{GL}_2(\mathcal{O}_{(L_0)_\mathfrak{p}})$ has finite order and lies in a conjugate of the pro-p-group $\{M \in \mathrm{GL}_2(\mathcal{O}_{(L_0)_\mathfrak{p}}), M \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{\mathfrak{p}}\}$. It follows that the order of h' is a power of p, so that h^{p^n} is scalar for some $n \geq 1$.

Hence the image of K in $\mathrm{PGL}_2(\mathcal{O}_{L_0}/\mathfrak{p})$ is a p-group, and $\rho_g'(G_\mathbb{Q})$ is an extension of a cyclic subgroup C' of order prime to p by a p-group. Since $p > 5$, this is only possible if $\rho_g'(G_\mathbb{Q})$ is a non-abelian dihedral group. Since $\rho_g'(G_\mathbb{Q})^{\mathrm{ab}}$ then has exponent 2, C' has order 2, so that $Q = |\rho_g'(G_\mathbb{Q})|/2$ is a power of p.

□

Proposition 6.3.7 *Assume that $\varepsilon_f\varepsilon_g \neq 1$. Then there exists a number field $F \subset L_1 \subset L_0$ such that, for all but finitely many good primes $\mathfrak{p} \subset \mathcal{O}_{L_0}$ such that the extension L_1/F splits totally at the prime $\mathfrak{p} \cap \mathcal{O}_F$, then $T_{f,g,\mathfrak{p}}$ has Euler-adapted Galois image. In particular, the set of such primes has positive lower density.*

Proof. – Let $\sigma \in G_\mathbb{Q}$ be such that $(\varepsilon_f\varepsilon_g)(\sigma) \neq 1$ and $\rho_g(\sigma)$ has distinct eigenvalues u, v. By Corollary 6.3.4, $(\gamma, \chi) \in \Gamma_f \longmapsto \chi(\sigma)$ is easily seen to be a cocycle $\mathrm{Gal}(L/F) \to L^\times$, so the above expression can be written as $\gamma(\alpha)/\alpha$ for some $\alpha \in L^\times$. Let $L_1 = F(\alpha, \varepsilon_f(\sigma), u, v)$. Let $p \nmid 30N_fN_g\varphi(N_f)\varphi(N_g)|\rho_g(G_\mathbb{Q})|$ and $\mathfrak{p}$ be a good prime with residue characteristic p such that L_1/F is totally split at $\mathfrak{p}$.

There exists $\sigma' \in G_{\mathbb{Q}(\mu_{p^\infty})}$ such that $\rho_g(\sigma) = \rho_g(\sigma')$ and $\sigma' \in \sigma G_H$. By Corollary 6.3.4, the action of σ' on $T_{f,\mathfrak{p}}$ can be chosen to be any matrix in $\Delta_{\alpha,\alpha^{-1}\varepsilon_f(\sigma)}\mathrm{SL}_2(\mathcal{O}_{F_\mathfrak{p}})$. By our choice of $\mathfrak{p}$, the action of σ' on $T_{f,\mathfrak{p}}$ can be chosen to be any matrix in $\mathrm{GL}_2(\mathcal{O}_{F_\mathfrak{p}})$ with determinant $\varepsilon_f(\sigma)$.

If $u^2 \neq \varepsilon_f(\sigma)^{-1}$, then we choose σ' such that it acts on $T_{f,\mathfrak{p}}$ as $\Delta_{u^{-1},u\varepsilon_f(\sigma)}$. Then the eigenvalues of σ' on $T_{f,g,\mathfrak{p}}$ are $1, u^2\varepsilon_f(\sigma), (\varepsilon_f\varepsilon_g)(\sigma), u/v$: 1 is distinct from all the others, hence (by our choice of p), not congruent to any of the others mod $\mathfrak{p}$, and σ' works.

If $u^2 = \varepsilon_f(\sigma)^{-1}$, we choose σ' such that it acts on $T_{f,\mathfrak{p}}$ as $u^{-1}U$: such a σ' works. □

Given $a, b \in K^\times$ for some field K, let us denote $\Delta_{a,b} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ and $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Proposition 6.3.8 *Let $\mathfrak{p} \subset L_0$ be a good prime. Assume that $-1 \in \varepsilon_g(G_H)$. If g has multiplication by the (real or imaginary) quadratic field K, assume that $K \not\subset H$. Then one of the following holds:*

- *$\rho_g(G_H)$ is a proper subgroup of $\rho_g(G_\mathbb{Q})$, $-1 \in \varepsilon_g(G_H)^2$, $\rho'_g(G_\mathbb{Q})$ is a dihedral group of order $2n$ with $n > 2$, and if n is even, then n is not divisible by 4 and $\rho'_g(G_H) \neq \rho'_g(G_\mathbb{Q})$.*
- *$T_{f,g,\mathfrak{p}}$ satisfies (sE).*

Proof. – Suppose that $\rho_g(G_H)$ contains a matrix M with $\det M = -1$ whose projective image has order 2. Then M^2 is scalar, so $M \sim \Delta_{a,b}$ for some $a, b \in \mathbb{C}^\times$ with $a = -b$ and $ab = -1$, where $A \sim B$ means that there exists $P \in \mathrm{GL}_2(\mathbb{C})$ such that $A = PBP^{-1}$. Therefore $M \sim \Delta_{1,-1}$, and, by Proposition 6.3.3, there is a $\sigma \in G_{H(\mu_{p^\infty})}$ acting on $T_{f,\mathfrak{p}}$ by U and on T_g by M: then σ fulfills the condition (sE). So we would like to find such a matrix M.

Note that when $\rho_g(G_H)$ contains the image c of the complex conjugation, $M = c$ works.

Let $Z \leq \rho_g(G_H)$ be the subgroup of scalar matrices. Consider the surjective determinant map $\delta : \rho'_g(G_H) = \rho_g(G_H)/Z \to \varepsilon_g(G_H)/\det Z$. We are done if we can find $x \in \rho_g(G_H)/Z$ with order 2 such that $\delta(x) = -\det Z$.

Assume that $\rho'_g(G_H)$ is isomorphic to A_4 or A_5. Since the derived subgroup of such a group has odd index, $\varepsilon_g(G_H)/\det Z$ has odd cardinality, so $-1 \in \det Z$ and δ is trivial on classes of order 2: any such class works.

If $\rho'_g(G_H) \cong S_4$, we can consider two cases. If $-\det Z$ is in the image of a class of A_4, the same reasoning as above works. If not, since $S'_4 = A_4$, δ vanishes on A_4, and therefore the natural inclusion $\{\pm 1\} \to \varepsilon_g(G_H)/\det Z$ is an isomorphism, and δ is simply the signature homomorphism. In particular, the class of a transposition in $\rho'_g(G_H)$ works.

Assume that $\rho'_g(G_H) \cong \mathbb{F}_2^{\oplus 2}$ (for instance if $\rho'_g(G_\mathbb{Q})$ is abelian). Then the domain of δ has exponent two and δ has cyclic image, so its image is cyclic of order 1 or 2. Hence δ has a non trivial kernel and is surjective, so any non trivial class in $\delta^{-1}(-\det Z)$ works.

Finally, let $D = \rho'_g(G_\mathbb{Q})$ and $D_H = \rho'_g(G_H)$: we just need to treat the case where D and D_H are dihedral, because $D_H \supset D'$. Let $C \leq D$ be the cyclic subgroup. The hypothesis implies that $D_H \not\subset C$, so D_H is dihedral with cyclic subgroup $D_H \cap C$ of index 2. Since $H/\mathbb{Q}$ is abelian, $D_H \supset D' = 2C$. In particular, the abelianization of D_H has exponent 2, so the image of δ has either 1 or 2 elements. We are done if the image of δ is trivial, so assume that $\det Z = \varepsilon_g(G_H)^2$. If $-1 \notin \det Z$, since D_H is generated by $D_H \backslash C$, there is a class in $D_H \backslash C$ whose image under δ is the coset of -1.

In other words, we just need to treat the case where $\det Z = \varepsilon_g(G_H)^2$, $-1 \in \det Z$ and $\ker \delta$ is contained in $C \cap D_H$. When $4 \mid |C|$ or $D_H = D$ and C has even order, $C \cap D_H$ contains an element of order 2. □

The above Proposition focuses entirely on elements similar to tensors $U \otimes \Delta_{1,-1}$. But other elements could work as well: in the following Proposition, we replace the -1 with other roots of unity $\beta \neq 1$.

Proposition 6.3.9 *Let $\mathfrak{p} \subset L_0$ be a good prime with residue characteristic p. Assume that there exists an odd prime $q \mid |\rho'_g(G_\mathbb{Q})|$ such that $q \neq p$ and $\varepsilon_g(G_H)$ contains an element of order q. Then one of the following statements holds:*

- *$q = 3$ divides $[H : \mathbb{Q}]$, $\rho'_g(G_\mathbb{Q})$ is isomorphic to A_4, $\rho'_g(G_H)$ is isomorphic to $\mathbb{F}_2^{\oplus 2}$.*

- *$q = 3$, $\rho'_g(G_\mathbb{Q})$ and $\rho'_g(G_H)$ are isomorphic to A_4, $e^{2i\pi/9} \in \varepsilon_g(G_H)$, and the projection $\rho_g(G_H) \cap \mathrm{SL}_2(L_0) \to \rho'_g(G_H)$ is not surjective.*
- *$T_{f,g,\mathfrak{p}}$ satisfies (sE).*

Proof. – As above, let $Z \leq \rho_g(G_H)$ be the subgroup of central matrices. When convenient, we will identify Z to a subgroup of $\mathbb{C}^\times$. Assume that Z contains q-th roots of unity, and let $M \in \rho_g(G_H) \cap \mathrm{SL}_2(L_0)$ have order q in $\mathrm{PGL}_2(L_0)$. Then $M^q = \{\pm I_2\}$, so that $M \sim t\Delta_{u,u^{-1}}$, where t is a sign, and u is a primitive q-th root of unity. Since $uI_2 \in Z$, $uM \sim t\Delta_{u^2,1}$ (with $u^2 \not\equiv 1 \pmod{\mathfrak{p}}$) is also in $\rho_g(G_H)$. The tensor $(tU) \otimes (uM)$ then shows (sE), and we already know that the other hypotheses hold.

The first step is to show that, except in specific cases, Z contains all the q-th roots of unity, and $\rho_g(G_H) \cap \mathrm{SL}_2(L_0)$ contains an element whose projective image has order q.

Consider, as before, the surjective determinant map $\delta : \rho'_g(G_H) \to \varepsilon(G_H)/\det Z$. Note that δ is trivial on the derived subgroup of $\rho'_g(G_\mathbb{Q})$ (which is contained in $\rho'_g(G_H)$).

If $\rho'_g(G_\mathbb{Q})$ is isomorphic to A_5 or S_4, or dihedral, then its derived subgroup has index coprime to q. Therefore, $\rho'_g(G_H)$ contains all the elements of order q of $\rho'_g(G_\mathbb{Q})$, and $\varepsilon(G_H)/\det Z = \mathrm{im}(\delta)$ is q-torsion free. Since q is an odd prime and $\varepsilon_g(G_H)$ contains some q-th root of unity, Z contains all the q-th roots of unity. Finally, since its image is q-torsion free, δ maps elements of order q to the identity, so they have lifts in $\rho_g(G_H) \cap \mathrm{SL}_2(L_0)$.

Assume now that $\rho'_g(G_\mathbb{Q})$ is isomorphic to A_4: then $q = 3$. Moreover, since A'_4 is the bitransposition subgroup (with index 3 in A_4), $\rho'_g(G_H)$ can be $\mathbb{F}_2^{\oplus 2}$ or A_4, and $\varepsilon_g(G_H)/\det Z$ is trivial in the former case, and has order 1 or 3 in the latter.

If $\rho'_g(G_H) \cong A_4$ and $\varepsilon_g(G_H)/\det Z$ is trivial, then, as above, Z contains all third roots of unity, and $\rho_g(G_H) \cap \mathrm{SL}_2(L_0)$ contains an element whose projective image has order 3: the argument above shows that we have Euler-adapted Galois image.

All we need to do is show that if $e^{2i\pi/9} \notin \varepsilon_g(G_H)$, $\rho'_g(G_H) \cong A_4$ and $\varepsilon_g(G_H)/\det Z$ has order 3, then we have Euler-adapted Galois image. Since $\varepsilon_g(G_H)$ is cyclic, under the previous assumptions, $|\det Z|$ (hence $|Z|$) is coprime to 3, and $\varepsilon_g(G_H) \setminus \det Z$ contains an element of order 3. In other words, there is some $x \in \rho_g(G_H)$ such that $\det x$ is a third root of unity. If the projective image of x is not a 3-cycle, then x^2 is scalar, and its determinant is also a primitive third root of unity, which we excluded. Therefore (up to replacing x with x^2), we may assume that x^3 is scalar, that x is not, and $\det x = j$. Let t be a multiple of the order of x^3 in Z which is congruent to 1 mod 3: replacing x with x^t if necessary, we may assume that $\det x = j$, x is not scalar, and $x^3 = I_2$. It follows that $x \sim \Delta_{1,j}$. As above, the tensor $U \otimes x$ shows that (sE) holds. □

Corollary 6.3.10 *If any of the following conditions hold, then $T_{f,g,\mathfrak{p}}$ has Euler-adapted Galois image for all but finitely many primes $\mathfrak{p}$:*

(i) $\rho_g(G_H)$ contains the image under ρ_g of the complex conjugation
(ii) $-1 \in \varepsilon_g(G_H)$ and $\rho_g(G_H)$ and $\rho_g(G_\mathbb{Q})$ have the same projective image, which is not a dihedral group of order $2n$ with $n > 1$ odd.
(iii) $\varepsilon_g(G_H)$ contains -1 but not i.
(iv) ε_f^2 is the trivial character, $\varepsilon_g(G_\mathbb{Q})$ contains an element of odd prime order $q \mid |\rho'_g(G_\mathbb{Q})|$, and, if $\rho'_g(G_\mathbb{Q}) \cong A_4$, then $\rho_g(G_\mathbb{Q}) \cap \mathrm{SL}_2(L_0) \to \rho'_g(G_\mathbb{Q})$ is onto.

Proof. – Condition (i) comes from Proposition 6.3.3 and proved like in Proposition 6.3.8. Conditions (ii) and (iii) follow from the Proposition 6.3.8. For condition (iv), assume that f has an inner twist by (γ, χ), then $\varepsilon_f = \gamma(\varepsilon_f) = \varepsilon_f \chi^2$, so that χ is a quadratic character. Therefore, $\mathrm{Gal}(H/\mathbb{Q})$ is a $\mathbb{F}_2$-vector space, which rules out both exceptional cases of Proposition 6.3.9. □

Corollary 6.3.11 *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication and ρ be a two-dimensional odd irreducible Artin representation of $G_\mathbb{Q}$, with splitting field K. Let $L_0/\mathbb{Q}$ be*

a finite extension containing all the eigenvalues of Frobenius for ρ and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_L$ with residue characteristic p. Suppose that the following technical hypotheses hold:

(i) p is coprime to $30N_\rho N_E$, where N_E (resp. N_ρ) is the conductor of E (resp. ρ).
(ii) If ρ has projective dihedral image, then the cyclic subgroup is not a p-group.
(iii) The p-adic Tate module of E is a surjective representation $G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$.
(iv) E is ordinary at p and $\rho(\mathrm{Frob}_p)$ has distinct eigenvalues mod $\mathfrak{p}$.

If $L(E,\rho,1) \neq 0$, then the group $\mathrm{Hom}_{\mathbb{Z}_p[\mathrm{Gal}(\mathrm{K}/\mathbb{Q})]}(\rho, \mathrm{Sel}_{p^\infty}(E/K))$ is finite.

Proof. – This is [92, Theorem 11.7.4] without the assumption on the coprimality of conductors. Let $f \in \mathcal{S}_2(\Gamma_0(N_E))$ and $g \in \mathcal{S}_1(\Gamma_1(N_\rho))$ be the normalized newforms associated to E and ρ: then $L(E,\rho,1)$ is the automorphic Rankin-Selberg L-value $L(f \otimes g, 1)$ (it has a classical definition in [103, Section 2], which we are going to use). We can apply without any modifications the proof of [92, Theorems 11.7.3, 11.7.4], as long as the following facts hold:

(a) $T_pE \otimes \rho$ has Euler-adapted Galois image.
(b) The p-adic L-value $L_p(f,g,1)$ does not vanish.

Since the modular form f associated to the elliptic curve E has no inner twists, $H = \mathbb{Q}$ and Proposition 6.3.8 shows that $T_{f,g,\mathfrak{p}}$ has Euler-adapted Galois image. Now, we check the non-vanishing of $L_p(f,g,1)$.

First, the L-value $L(f,g,1)$ from [92, §2.7] differs from the value $L(f \otimes g, 1)$ by finitely many Euler factors at primes $q \mid N_E N_\rho$, described in [103, Section 2]. In *loc. cit.*, some of them are denoted as θ_q; the others come from replacing the local sum $\sum_{n\geq 0} a_{q^n}(f)a_{q^n}(g)q^{-ns}$ with $\sum_{n\geq 0} a_{q^n}(f\otimes\chi)a_{q^n}(g\otimes\overline{\chi})q^{-ns}$ for some Dirichlet character χ chosen so that $f\otimes\chi, \overline{g}\otimes\chi$ satisfy the hypotheses (A), (B), (C) of *loc. cit.*. Note also that *loc. cit.* uses a different normalization: their $s = 1/2$ is our $s = 1$. By checking every case, one sees that none of these factors vanish at $s = 1$. It follows that $L(f,g,1) \neq 0$, where $L(f,g,1)$ is defined in [92, §2.7].

Finally, we use the interpolation property of [92, Theorem 2.7.4]: the p-adic L-value does not vanish as long as (following the notations of *loc. cit.*) $\mathcal{E}(f)$, $\mathcal{E}^*(f)$, and $\mathcal{E}(f,g,1)$ do not vanish. $\mathcal{E}(f)$ does not vanish because the two Frobenius eigenvalues of f at p have modulus $\sqrt{p}$, by the Hasse-Weil bound. $\mathcal{E}^*(f)$ does not vanish because f is ordinary at p, so exactly one of the Frobenius eigenvalues at p is a p-unit, thus the two cannot be equal. Finally, $\mathcal{E}^*(f,g,1) \neq 0$ because the Frobenius eigenvalues of f and g have modulus respectively $\sqrt{p}$ and 1 (for any complex embedding), so $L_p(f,g,1) \neq 0$ and we are done. □

6.4 Families of dihedral counter-examples: proof of Theorem 6.D

In this Section, we keep the notations from Section 6.3, but furthermore assume that $\varepsilon_g = \varepsilon_f^{-1}\varepsilon$, where ε is the character of some quadratic number field $K \subset H$ such that g has CM by K: in particular, ε factors through $\mathrm{Gal}(H/\mathbb{Q})$.

We are interested in the following question: given a good prime ideal $\mathfrak{p}$ of $\mathcal{O}_{L_0}$ for the couple (f,g), when does $T_{f,g,\mathfrak{p}}$ satisfy (wE)?

We first recall the following fact, already identified as a general obstruction in [108, Proposition 4.1.1].

Lemma 6.4.1 *Let $M, N \in \mathrm{GL}_2(K)$ be matrices over a field K such that $\det M \det N = 1$. Then $\ker[M \otimes N - 1]$ is never a line.*

Proof. – The problem is clearly solved if M or N is scalar. We now assume that neither M nor N is scalar and that 1 is an eigenvalue of $M \otimes N$. Assume that $M \sim \alpha U$ for some $\alpha \in K^\times$. Then α^{-1} is an eigenvalue of N. Since $\det M \det N = 1$, the characteristic polynomial of N is $(X - \alpha^{-1})^2$. As N is not scalar, $N \sim \alpha^{-1}U$. It is easy to see that $U \otimes U - 1$ has rank two, so $\ker(M \otimes N - 1)$ is not a line. Thus, we can (and do) assume that M has distinct eigenvalues

m, m' and N has distinct eigenvalues n, n'. Then the endomorphism $M \otimes N$ is diagonalizable with eigenvalues $mn, m'n', m'n, nm'$. Since $1 = (mn)(m'n') = (mn')(m'n)$, there is never exactly one of these eigenvalues which is equal to one. □

As noted by Loeffler, this lemma implies that, for any couple (f', g') of newforms, $T_{f',g',\mathfrak{p}}$ cannot satisfy (wE) if the product of the characters of f', g' is trivial, whence the requirement that $\varepsilon_f \varepsilon_g \neq 1$ in Question 6.1.1.

Define the map $\mathcal{B} : \mathrm{Gal}(H/\mathbb{Q}) \times G_F \to \{\pm 1\}$ as follows: let $(\sigma, \tau) \in \mathrm{Gal}(H/\mathbb{Q}) \times G_F \to \{\pm 1\}$. By Corollary 6.3.4, there is some $\alpha \in L^\times$ such that $\gamma(\alpha) = \chi(\sigma)\alpha$ for all $(\gamma, \chi) \in \Gamma_f$. Since $\gamma(\varepsilon_f) = \chi^2 \varepsilon_f$, one has $\nu := \frac{\alpha^2}{\varepsilon_f(\sigma)} \in F^\times$. Then $\mathcal{B}(\sigma, \tau) = \frac{\tau(\sqrt{\nu})}{\sqrt{\nu}}$.

Proposition 6.4.2 *$\mathcal{B}$ is a bilinear pairing, and factors through a finite quotient of G_F. Moreover, for every $\sigma \in \mathrm{Gal}(H/\mathbb{Q})$, $\mathcal{B}(\sigma, \cdot) : G_F \to \{\pm 1\}$ is unramified away from $2 \cdot \mathrm{disc}(L/F)$.*

Proof. – The bilinearity is a straightforward verification. To prove the rest of the statement, note that if $\tau \in \mathrm{Gal}(\overline{F}/L(\sqrt{\mu}))$ (where μ is the group of roots of unity that are values of ε_f), then $\mathcal{B}(\cdot, \tau) = 1$. □

Let $\mathfrak{p} \subset \mathcal{O}_{L_0}$ be good prime ideal for (f, g), we write $\mathcal{B}_\mathfrak{p} = \mathcal{B}(\cdot, \mathrm{Frob}_\mathfrak{p}) : \mathrm{Gal}(H/\mathbb{Q}) \to \{\pm 1\}$. Denote by M the subgroup of $\mathrm{Gal}(H/\mathbb{Q})$ made by those $\sigma \in \mathrm{Gal}(H/\mathbb{Q})$ such that $\mathcal{B}(\sigma, \cdot) = 1$. By Cebotarev, M is thus the intersection of the kernels of the $\mathcal{B}_\mathfrak{p}$.

Proposition 6.4.3 *Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_{L_0}$ of residue characteristic p, good for (f, g). Then the following are equivalent:*

- *$T_{f,g,\mathfrak{p}}$ satisfies (wE),*
- *$T_{f,g,\mathfrak{p}}$ satisfies (sE),*
- *$\mathcal{B}_\mathfrak{p} \neq \varepsilon$.*

Proof. – Suppose that $T_{f,g,\mathfrak{p}}$ satisfies (wE): there exists $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$ such that $\ker(\sigma - 1 \mid T_{f,g,\mathfrak{p}})$ is a line. Let $\alpha \in L^\times \cap \mathcal{O}_{L,\mathfrak{p}}^\times$ be associated to σ by Corollary 6.3.4. The action of σ on $T_{f,\mathfrak{p}}, T_g$ is given by some matrices $M \in \mathrm{GL}_2(\mathcal{O}_{(L_0)_\mathfrak{p}}), N \in \mathrm{GL}_2(\mathcal{O}_{L_0})$ respectively. By the assumption on σ and Lemma 6.4.1, one has $1 \neq \det M \det N = \varepsilon_f(\sigma)\varepsilon_f(\sigma)^{-1}\varepsilon(\sigma)$, so $\sigma \notin G_K$. Therefore, N^2 is scalar and $\det N = -\varepsilon_f(\sigma)^{-1}$. Let $\omega \in L_0$ be a square root of $\varepsilon_f(\sigma)^{-1}$, then the two eigenvalues of N are ω and $-\omega$.

By Corollary 6.3.4, we can write $M = \alpha^{-1}\varepsilon_f(\sigma)M'$, where $M' \in \mathrm{GL}_2(\mathcal{O}_{F_\mathfrak{p}})$ has determinant $\frac{\alpha^2}{\varepsilon_f(\sigma)}$. Thus $\alpha\omega^2$ is an eigenvalue of $M' \otimes \Delta_{\omega,-\omega}$, so that one of the eigenvalues of M' is $\pm\omega\alpha$. Since $(\pm\omega\alpha)^2 = \det M'$, one has $\pm\alpha\omega = \frac{1}{2}\operatorname{Tr} M' \in F_\mathfrak{p}$, so $\mathcal{B}(\sigma, \mathrm{Frob}_\mathfrak{p}) = 1 \neq \varepsilon(\sigma)$.

Suppose conversely that $\mathcal{B}(\cdot, \mathrm{Frob}_\mathfrak{p}) \neq \varepsilon$. Then $\ker \mathcal{B}(\cdot, \mathrm{Frob}_\mathfrak{p})$ is not contained in $\ker \varepsilon$, otherwise ε would be a power of $\mathcal{B}_\mathfrak{p}$: but ε is clearly distinct from $\mathcal{B}_\mathfrak{p}^i$ for $i \in \{0, 1\}$ and $\mathcal{B}_\mathfrak{p}^2 = 1$. Hence, there exists $s \in \mathrm{Gal}(H/\mathbb{Q})$ such that $\varepsilon(s) = -1$ and $\mathcal{B}_\mathfrak{p}(s) = 1$. By Corollary 6.3.4, let $\alpha \in \mathcal{O}_{L,\mathfrak{p}}^\times$ such that for all $(\gamma, \delta) \in \Gamma_f$, $\gamma(\alpha) = \delta(s)\alpha$. Since $\gamma(\varepsilon_f) = \delta^2\varepsilon_f$, one has $\nu := \frac{\alpha^2}{\varepsilon_f(\sigma)} \in F^\times$, hence $\nu \in \mathcal{O}_{F,\mathfrak{p}}^\times$. Since $\mathcal{B}_\mathfrak{p}(s) = 1$, ν is a square in $F_\mathfrak{p}$. Therefore, $\varepsilon_f(\sigma)^{-1} = \nu\alpha^{-2}$ has a square root ω in $L_\mathfrak{p}$.

Still by Corollary 6.3.4, we can choose $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$ such that $\sigma_{|H} = s$ and such that σ acts on $T_{f,\mathfrak{p}}$ by the matrix $\alpha^{-1}\varepsilon_f(s)\begin{pmatrix}\nu & 1\\ 0 & \nu\end{pmatrix}$.

Moreover, $\varepsilon(\sigma) = -1$, so $\rho_g'(\sigma) \in \mathrm{PGL}_2(\mathcal{O}_{L_0})$ has order two. Since $\det \rho_g(\sigma) = -\varepsilon_f(\sigma)^{-1}$, and $p \neq 2$, $\rho_g(\sigma)$ is $\mathrm{GL}_2(\mathcal{O}_{(L_0)_\mathfrak{p}})$-conjugate to $\Delta_{\omega,-\omega}$. Therefore, σ acts on $T_{f,g,\mathfrak{p}}$ by $\begin{pmatrix}1 & a & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & -1 & *\\ 0 & 0 & 0 & -1\end{pmatrix}$ with $a \in \mathcal{O}_{(L_0)_\mathfrak{p}}^\times$: hence $T_{f,g,\mathfrak{p}}/(\sigma - 1)T_{f,g,\mathfrak{p}}$ is free of $\mathcal{O}_{(L_0)_\mathfrak{p}}$-rank one. □

Corollary 6.4.4 *The answer to Question 6.1.1 for (f,g) is negative if, and only if, $\varepsilon(M)=1$.*

Proof. – By Cebotarev and the previous Proposition, the answer to Question 6.1.1 for (f,g) is positive if and only if ε cannot be written as a $\mathcal{B}(\cdot,\tau)$ for any $\tau\in G_F$. Because B is bilinear with values in an $\mathbb{F}_2$-vector space, the set of the $\mathcal{B}(\cdot,\tau)$ for $\tau\in G_F$ is exactly the set of homomorphisms $f:\mathrm{Gal}(H/\mathbb{Q})\to\{\pm1\}$ such that $f(M)=1$, whence the conclusion. □

Proposition 6.4.5 *Let $H_0\subset H$ be the subfield such that $G_{H_0}=\ker\varepsilon_f$. Assume that one of the following holds:*

(a) *k is even and H is not totally real,*
(b) *k is odd and $[H:H_0]>2$,. then $(*)$ holds unless perhaps if $[H:H_0]=2$, $\sigma_0\in\mathrm{Gal}(H/H_0)$ is the unique nontrivial element, L contains a fourth root of unity i, and, with c the complex conjugation, for all $(\gamma,\delta)\in\Gamma_f$, $\gamma(i)=\delta(\sigma_0 c)i$.*
(c) *k is odd, $[H:H_0]=2$, and ε_f does not take its values in $L^{\times 2}$ (for instance if L does not contain a fourth root of unity i),*
(d) *k is odd, $[H:H_0]=2$, $i\in L$, and for all $(\gamma,\delta)\in\Gamma_f$, $\gamma(i)=\delta(-1)i$,*
(e) *k is odd, $\mathrm{Gal}(H/H_0)$ contains a unique nontrivial element σ_0, $i\in L$ and, for some $(\gamma,\delta)\in\Gamma_f$, one has $\gamma(i)\neq\delta(\sigma_0)\delta(-1)i$.*

Then there exists a nontrivial character $\varepsilon:\mathrm{Gal}(H/\mathbb{Q})/M\to\{\pm1\}$ mapping the complex conjugation c to $(-1)^{k-1}$.
Moreover, when k is odd, $[H:H_0]=2$, $i\in L$ but is not a value of ε_f, then the existence of such a ε is equivalent to the last clause of (e). Under the same assumptions, if $\varepsilon_f^2=1$, then (d) and (e) are equivalent.

Proof. – Remember that L is the number field generated by the coefficients of f, so it is a subfield of $\mathbb{C}$. Note that $\mathcal{B}$ realizes an isomorphism from $\mathrm{Gal}(H/\mathbb{Q})/M$ to a subgroup B of the $\mathbb{F}_2$-vector space $\mathrm{Hom}(G_F,\mathbb{F}_2)$, so $\mathrm{Gal}(H/\mathbb{Q})/M$ has exponent 2.

Suppose first that k is even and H is not totally real. Let $c\in\mathrm{Gal}(H/\mathbb{Q})$ be the image of the complex conjugation and let $\alpha\in L^\times$ be associated to c as in Corollary 6.3.4. It is enough to prove that $c\notin M$. Since k is even, $\varepsilon_f(c)=1$, so one has $\mathcal{B}(c,\tau)=\frac{\tau(\alpha)}{\alpha}$ for all $\tau\in G_F$. In particular, for every $(\gamma,\delta)\in\Gamma_f$, one has $\mathcal{B}(c,\gamma)=\delta(-1)$. Since H is not totally real, there is some δ such that $\delta(-1)=-1$, so $c\notin M$, whence the conclusion.

Now suppose that k is odd. The goal is to show that there exists a nontrivial character $\mathrm{Gal}(H/\mathbb{Q})/\langle M,c\rangle\to\{\pm1\}$. To do that, we need to show that $\mathrm{Gal}(H/\mathbb{Q})\supsetneq\langle M,c\rangle$, or in other words that $B\supsetneq\{1,\mathcal{B}(c,\cdot)\}$.

Let $\sigma\in M$ be such that $\varepsilon_f(\sigma)=1$: let α be associated to σ by Corollary 6.3.4. Then, for all $\tau\in G_F$, $\tau(\alpha)=\alpha$, hence $\alpha\in F^\times$. Therefore, for all $(\gamma,\delta)\in\Gamma_f$, $\alpha=\gamma(\alpha)=\delta(\sigma)\alpha$, so $\delta(\sigma)=1$, whence $\sigma_{|H}=\mathrm{id}$. Thus, $(\pi,\varepsilon_f):\mathrm{Gal}(H/\mathbb{Q})\to F^\times/F^{\times 2}\times\mathbb{C}^\times$ is injective.

In particular, $\sigma\in\mathrm{Gal}(H/H_0)\longmapsto\mathcal{B}(\sigma,\cdot)$ is injective, so that $|B|\geq[H:H_0]$, so we are done if $[H:H_0]>2$.

Now suppose that $[H:H_0]=2$ and let σ_0 be the unique nontrivial element of $\mathrm{Gal}(H/H_0)$. Let $\sigma\in M$: then the $\alpha\in L^\times$ associated to σ by Corollary 6.3.4 is such that $\frac{\alpha^2}{\varepsilon_f(\sigma)}\in F^{\times 2}$, so $\varepsilon_f(\sigma)\in L^{\times 2}$.

Since $\mathrm{Gal}(H_0/\mathbb{Q})$ is isomorphic to the image of ε_f which contains -1, it is a group with even cardinality. Moreover, since $\sigma_0\notin M$, σ_0 is not a double in $\mathrm{Gal}(H/\mathbb{Q})$. It follows that $\mathrm{Gal}(H/\mathbb{Q})\cong\mathbb{Z}/2\mathbb{Z}\sigma_0\oplus\mathbb{Z}/n\mathbb{Z}\sigma$, where n is the cardinality of the image of ε_f, and σ is such that $\varepsilon_f(\sigma)$ has order n. Hence, representatives for $\mathrm{Gal}(H/\mathbb{Q})/M$ are given (possibly with repetitions) by $\sigma_0,\sigma_0\sigma,\sigma,\mathrm{id}$. Since $\varepsilon_f(\sigma)=\varepsilon_f(\sigma\sigma_0)$ is a generator of the image of ε_f, the previous paragraph shows that unless ε_f takes its values in $L^{\times 2}$, $\sigma,\sigma_0\sigma\notin M$, hence $|B|=4$ are we are done.

In particular, if i is not a value taken by ε_f, but $i\in L$, the above considerations show that representatives for $\mathrm{Gal}(H/\mathbb{Q})$ are given by $\mathrm{id},\sigma_0,c,\sigma_0 c$. So $\mathrm{Gal}(H/\mathbb{Q})$ is generated by M and c if and only if $\sigma_0 c\in M$, which is equivalent to the statement that for all $(\gamma,\delta)\in\Gamma_f$, $\gamma(i)=\delta(\sigma_0)\delta(-1)i$.

In general, when (e) holds, one has $\sigma_0 c \notin M$, so, since $\sigma_0 \notin M$, σ_0 is not in the subgroup generated by M and c, so the conclusion follows. Furthermore, (d) is a stronger condition than (e), since it implies that $c \in M$.

Suppose finally that $\varepsilon_f^2 = 1$ and (e) holds. The discussions above show that the 2-torsion subgroup of $\mathrm{Gal}(H/\mathbb{Q})$ is a set of representatives for $\mathrm{Gal}(H/\mathbb{Q}) \otimes \mathbb{F}_2$. We have an injective homomorphism $(\gamma, \delta) \in \Gamma_f \longmapsto \delta \in \mathrm{Hom}(\mathrm{Gal}(H/\mathbb{Q}), \{\pm 1\})$, so that every homomorphism $\Gamma_f \to \{\pm 1\}$ is of the form $(\gamma, \delta) \longmapsto \delta(\sigma)$ for some element $\sigma \in \mathrm{Gal}(H/\mathbb{Q})$ of order dividing 2. In particular, we know that some $\sigma \in \{\sigma_0, c, \sigma_0 c\}$ is associated to $(\gamma, \delta) \longmapsto \frac{\gamma(i)}{i}$: but then i is the α associated by Corollary 6.3.4 to σ. By taking the couple (c, ε_f^{-1}), we know that $\sigma \neq \sigma_0$, so $\sigma \in \{c, \sigma_0 c\}$, and by the above discussion, it means that exactly one of $c, \sigma_0 c$ is in M. □

Remarks

(i) Let $f \in \mathcal{S}_2(\Gamma_0(63))$ be a newform with LMFDB [107] label 63.2.$a.b$[3]: it has coefficients in $\mathbb{Q}(\sqrt{3})$, an inner twist by the quadratic character ε of $K = \mathbb{Q}(\sqrt{-3})$ and no complex multiplication. The newform $g \in \mathcal{S}_1(\Gamma_1(675))$ with LMFDB label 675.1.$c.b$ has rational coefficients, character ε and complex multiplication by K. The argument shows that (after possibly removing a finite number of primes) $T_{f,g,\mathfrak{p}}$ does not satisfy (wE) when the residue characteristic is congruent to $5, 7$ mod 12.

(ii) Consider a newform $f \in \mathcal{S}_3(\Gamma_1(75))$ with LMFDB label 75.3.$d.b$. Then $L = \mathbb{Q}(i, \sqrt{5})$, $F = \mathbb{Q}$, $H_0 = \mathbb{Q}(\sqrt{-15})$, $H = \mathbb{Q}(j, \sqrt{5})$. Then it can be checked that $\mathrm{Gal}(H/\mathbb{Q})$ is generated by M and c. When ε is the character of the unique real quadratic field contained in H and g is a weight one newform with character $\varepsilon\varepsilon_f^{-1}$ and with real multiplication by ε, property (sE) then holds for all but finitely many $T_{f,g,\mathfrak{p}}$, even though Theorem 6.A does not apply.

(iii) When k is even, H_0 is necessarily totally real. However, H can be totally real and larger than H_0. This is what happens for the newform $f \in \mathcal{S}_2(\Gamma_0(289))$ with LMFDB label 289.2.$a.f$: indeed, $H_0 = \mathbb{Q}$, but $H = \mathbb{Q}(\sqrt{17})$. By Theorem 6.A, the answer to Question 6.1.1 is positive for f and any weight one newform.

(iv) For a newform $f \in \mathcal{S}_3(\Gamma_1(24))$ with LMFDB label 24.3.$h.c$, the condition (c) of Proposition 6.4.5 is satisfied: indeed, in this situation $L = \mathbb{Q}(\sqrt{2}, \sqrt{-7})$ does not contain i, while $H = \mathbb{Q}(\sqrt{2}, j)$, and $H_0 = \mathbb{Q}(\sqrt{-6})$ is such that $[H : H_0] = 2$. Indeed, B contains the two distinct nontrivial elements $\mathcal{B}(c, \cdot)$ and $\mathcal{B}(\mathrm{Frob}_5, \cdot)$ (they are the Kummer characters associated to $\sqrt{14}$ and $\sqrt{2}$ respectively), so that M is trivial and $\mathrm{Gal}(H/\mathbb{Q})$ is larger than $\{\mathrm{id}, c\}$.

(v) For a newform $f \in \mathcal{S}_3(\Gamma_1(64))$ with LMFDB label 64.3.$d.a$, we have $L = \mathbb{Q}(\mu_{12})$ and $F = \mathbb{Q}$; moreover, $H = \mathbb{Q}(\mu_8)$ and $\mathrm{Gal}(H/H_0)$ corresponds to the subgroup $\{1, 3\}$ of $(\mathbb{Z}/8\mathbb{Z})^\times$. Because $a_{63}(f) \in iF^\times$, the condition (d) of Proposition 6.4.5 is verified.

(vi) Even when $i \in L$ is not a value of ε_f, it is not true that (e) implies (d). A counter-example is given by the newform $f \in \mathcal{S}_3(\Gamma_1(324))$ with LMFDB label 324.3.$f.s$[4]. In this situation, ε_f has conductor 36 and order 6, while L has degree 16 and $|\Gamma_f| = 8$, so that $F = \mathbb{Q}(\sqrt{57})$.

(vii) Consider a newform $f \in \mathcal{S}_3(\Gamma_1(21))$ with LMFDB label 21.3.$h.b$. In this case, one has $|\Gamma_f| = 4$, but $H = H_0 = \mathbb{Q}(j)\mathbb{Q}(\mu_7)^+$. In fact, $F = \mathbb{Q}$, $L = \mathbb{Q}(j, \sqrt{-5})$, and one can directly compute that $B = \{\mathcal{B}(\mathrm{id}, \cdot), \mathcal{B}(c, \cdot)\}$.

Corollary 6.4.6 *Suppose that the hypotheses of Proposition 6.4.5 hold, and let ε be the character given by the conclusion Proposition 6.4.5. Let g be a weight one newform with complex (or real) multiplication by ε and with character $\varepsilon\varepsilon_f^{-1}$. Then the answer to Question 6.1.1 for the couple (f, g) is negative.*

[3]Technically, these labels refer to a Galois orbit of newforms; however, the choice of embedding does not matter in all the situations below, so we omit it.

[4]With the tools dicussed here, this verification is not difficult using the LMFDB data and MAGMA [16]; we omit it for the sake of brevity.

The following result completes the proof of Theorem 6.D.

Proposition 6.4.7 *Let ε be the character of the imaginary (resp. real) quadratic field K, and χ be an even (resp. odd) primitive Dirichlet character. There exist infinitely many weight one newforms g with complex (resp. real) multiplication by K, and character $\varepsilon\chi$.*

Proof. – This statement is easier to establish using Galois representations. Let C be the conductor of χ, n be the exponent of χ and D be a positive multiple of Cn. Let K' the abelian extension of K whose group of norms is $K^\times \prod_v M_v$, where M_v is $\mathbb{C}^\times$ when v is a complex place, $\mathbb{R}_+^\times$ when v is a real place, $1 + D\mathcal{O}_{K_v}$ at every place v dividing D, and $\mathcal{O}_{K_v}^\times$ at all other finite places. We claim that χ vanishes on the kernel of the transfer map $V : G_{\mathbb{Q}}^{ab} \to \mathrm{Gal}(K'/K)$. It follows that $\sigma \in G_{\mathbb{Q}} \longmapsto \chi(\sigma)$ extends (through V) to at least $\frac{[K':K]}{\varphi(n)}$ characters $\psi : G_K \to \mathrm{Gal}(K'/K) \to \mathbb{C}^\times$. The Artin representation $\rho_\psi := \mathrm{Ind}_K^{\mathbb{Q}}\psi$ has determinant $\varepsilon\psi(V) = \varepsilon\chi$ and it uniquely determines ψ (up to conjugation by $\mathrm{Gal}(K/\mathbb{Q})$), so this construction produces at least $\frac{[K':K]}{2\varphi(n)}$ pairwise non-isomorphic Artin representations as requested. It is easy to see that we can choose D so that $[K' : K]$ is arbitrarily large, whence the conclusion. □

6.5 Examples and counter-examples

So far, we have identified in Theorem 6.A and in Section 6.3 some sufficient conditions to ensure a positive answer to Question 6.1.1. On the other hand, the situation studied in Section 6.4 provides in some cases families of counter-examples. The purpose of this Section is to study some situations where the results of neither Section applies. We provide a few counterexamples which do not stem from Section 6.4. We also showcase additional examples proving that, while the exceptional cases highlighted in Propositions 6.3.8 and 6.3.9 can occur, they are not necessarily incompatible with Euler-adapted Galois images. Some of these counter-examples are explicit: as in the examples of Section 6.4, we will then always refer to newforms by their LMFDB label [107]. While this label only refers to the equivalence class of the modular forms under the action of $G_{\mathbb{Q}}$, the arguments work regardless of the choice of embedding of the modular forms in $\mathbb{C}$.

Proposition 6.5.1 *Assume that $\mathfrak{p}$ is a good prime, and that (f, g, p) falls in one of the following cases:*

(a) f is 961.2.a.b, g is 3875.1.d.a, and $p \equiv 13, 37, 83, 107 \pmod{120}$.
(b) f is 1849.2.a.g, g is 688.1.b.b, and $p \equiv 7, 17 \pmod{24}$.
(c) f is 1849.2.a.g, g is 2107.1.b.b, and $p \equiv 11, 13 \pmod{24}$.
(d) f is 63.2.a.b, g is 1452.1.e.d and $p \equiv 5, 7 \pmod{12}$.
(e) f is 189.2.a.f, g is 3468.1.i.a and $p \equiv \pm 5, \pm 43, \pm 67 \pmod{168}$.

Then $T_{f,g,\mathfrak{p}}$ does not satisfy (wE).

Remark In all these counter-examples, f is a non-CM newform of weight 2 with trivial character with coefficients in a quadratic number field, g is always a newform of weight 1 with quadratic character, except in case (e) where its character has order 4. In particular, $\varepsilon_f\varepsilon_g \neq 1$. Moreover, g never has complex multiplication by $\varepsilon_g\varepsilon_f$, so these counter-examples are not covered by Lemma 6.4.1 or the construction of Section 6.4. Finally, the field extension $H/\mathbb{Q}$ (associated to f in the notation of Section 6.2) is quadratic. The corresponding situations are:

(a) $\rho'_g(G_{\mathbb{Q}}) \cong A_5$, $\varepsilon_g(G_H) = 1$.
(b) $\rho'_g(G_{\mathbb{Q}}) \cong S_4$, $\varepsilon_g(G_H) = 1$.
(c) $\rho'_g(G_{\mathbb{Q}}) \cong A_4$, $\varepsilon_g(G_H) = 1$.
(d) $\varepsilon_g(G_H) = 1$ and g has CM by a field distinct from H.
(e) $i \in \varepsilon_g(G_H)$, g has CM by a field distinct from H, $\rho'_g(G_{\mathbb{Q}}) = \rho'_g(G_H)$ is a dihedral group of order 6.

Proof. –

(a) According to the LMFDB, ε_g is the quadratic character of conductor 31, $L = \mathbb{Q}(\sqrt{2})$, f is not CM and has an inner twist by ε_g, so that $F = \mathbb{Q}$ and $H = \mathbb{Q}(\sqrt{-31})$. Since $\varepsilon_g(G_H) = 1$, Lemma 6.4.1 shows that any $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}$ satisfying (wE) cannot lie in $G_{H(\mu_{p^\infty})}$.

Let D be the derived subgroup of $\rho_g(G_\mathbb{Q})$. Since g is of A_5-type, $D \subset \mathrm{SL}_2(L_0)$ is a finite group whose projective image is A_5. In particular, it has even order, hence contains $-I_2$. Thus we have an exact sequence $1 \to \{\pm I_2\} \to D \to A_5 \to 1$. Moreover, $\rho_g(G_\mathbb{Q})$ is generated by D and its scalar matrices; since $\det \rho_g(G_\mathbb{Q}) = \{\pm 1\}$, its scalar matrices are $\pm iI_2, \pm I_2$, and $D = \rho_g(G_\mathbb{Q}) \cap \mathrm{SL}_2(L_0)$. Since $D \subset \rho_g(G_{H(\mu_{p^\infty})}) \subset \rho_g(G_\mathbb{Q})$, and $\varepsilon_g(G_H) = 1$, $\rho_g(G_{H(\mu_{p^\infty})}) = D$.

Let $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})} \backslash G_{H(\mu_{p^\infty})}$. By Corollary 6.3.4, σ acts on $T_{f,\mathfrak{p}}$ by a matrix in $\Delta_{\sqrt{2},1/\sqrt{2}} \mathrm{SL}_2(\mathbb{Z}_p)$ (so, a matrix in $\mathrm{GL}_2(\mathbb{Z}_p)$ with determinant 2, divided by $\sqrt{2}$), and, by the above, on T_g by a matrix of iD. So we need to show that if $M \in \mathrm{GL}_2(\mathbb{Z}_p)$ has determinant 2 and $N \in D$, then $\ker\left[M \otimes N - i\sqrt{2}\right]$ is never a line (over $\overline{\mathbb{Q}_p}$).

Note that $p \equiv 3, 5 \pmod 8$, so that M always has two distinct eigenvalues α and $\alpha' = 2/\alpha$, with $2/\alpha + \alpha \in \mathbb{Z}_p$. Moreover, $p \equiv \pm 1 \pmod{12}$, so that $\sqrt{3} \in \mathbb{Z}_p$, hence $\sqrt{6} \notin \mathbb{Z}_p$. Finally, $p \not\equiv \pm 1 \pmod 5$, so $\sqrt{5} \notin \mathbb{Z}_p$.

If N is scalar, it is clear that $M \otimes N$ does not work.

If the projective image of N is a bitransposition, then N is not scalar, N^2 is scalar and $\det N = 1$, so that $N \sim \Delta_{i,-i}$. Then the four eigenvalues of $M \otimes N$ are $i\alpha, -i\alpha, i\alpha', -i\alpha'$. If any of them is $i\sqrt{2}$, it means that α or α' is $\pm\sqrt{2}$. Hence $\alpha = \alpha'$, a contradiction.

If the projective image of N is a 3-cycle, then N is not scalar, N^3 is scalar, and $\det N = 1$, so that $N \sim \Delta_{j,j^2}$. Thus, the four eigenvalues of $M \otimes N$ are $\alpha j, \alpha j^2, \alpha' j, \alpha' j^2$. Suppose that any of them is $i\sqrt{2}$. Up to exchanging α and α', α is $ij^2\sqrt{2}$ or $ij\sqrt{2}$. In either case,

$$\alpha + \alpha' = \pm\sqrt{2}(ij^2 - ij) = \pm i\sqrt{2}(j^2 - j) = \pm\sqrt{6} \in \mathbb{Z}_p, \text{a contradiction.}$$

If the projective image of N is a 5-cycle, then N is not scalar, N^5 is scalar, and $\det N = 1$, so that $N \sim \Delta_{u,u^{-1}}$ where u is a primitive fifth root of unity. It is thus enough to show that $u^{-1}\alpha$ cannot equal $i\sqrt{2}$ (up to renaming u and exchanging α and α'). If this were the case, we would have $\alpha + 2/\alpha = i(u - u^{-1})\sqrt{2} \in \mathbb{Z}_p$, hence $(u - u^{-1})^2 \in \mathbb{Z}_p$. Let $v = (u - u^{-1})^2$: then

$$(5+2v)^2 = (2u^2+2u^{-2}+1)^2 = 4u^4+4u^{-4}+1+8+4u^2+4u^{-2} = 4(1+u+u^2+u^3+u^4)+5 = 5,$$

this implies that $\sqrt{5} \in \mathbb{Z}_p$, which is a contradiction.

(b) According to the LMFDB, in this case, $L = \mathbb{Q}(\sqrt{6})$, the projective image of ρ_g is S_4 and ε_g is the unique non trivial quadratic character of conductor 43. Moreover, f has no CM and an inner twist by ε_g, so that $F = \mathbb{Q}$ and $H = \mathbb{Q}(\sqrt{-43})$. Moreover, the coefficient field of g is $\mathbb{Q}(\sqrt{-2})$, so that g has no coefficient equal to $\pm 2i$. Therefore, $\rho_g(G_\mathbb{Q})$ does not contain $\pm iI_2$, and its scalar matrices are contained in $\pm I_2$. Now, the derived subgroup of $\rho_g(G_\mathbb{Q})$ contains $\rho_g(G_H)$, is contained in $\mathrm{SL}_2(L_0)$ and has projective image A_4, so that it contains an element of even order: so $\rho_g(G_\mathbb{Q}) \cap L_0^\times I_2 = \{\pm I_2\}$, and $\rho_g(G_H) = \rho_g(G_{H(\mu_{p^\infty})})$ lives in an exact sequence $1 \to \{\pm I_2\} \to \rho_g(G_H) \to A_4 \to 1$.

As above, any σ satisfying (wE) cannot lie in $G_{H(\mu_{p^\infty})}$. Let $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})} \backslash G_H$. By the above, $\rho_g(\sigma)$ has determinant -1 and $\rho'_g(\sigma)$ has order 2 or 4: so $\rho_g(\sigma)$ is similar to $\Delta_{1,-1}$ or to $\Delta_{u,-u^{-1}}$, where u is a primitive 8-th root of unity. By Corollary 6.3.4, σ acts on $T_{f,\mathfrak{p}}$ by a matrix of $\Delta_{\sqrt{6},1/\sqrt{6}} \mathrm{SL}_2(\mathbb{Z}_p) = \frac{1}{\sqrt{6}} \mathrm{GL}_2(\mathbb{Z}_p)_{\det=6}$.

So we want to prove that if $M \in \mathrm{GL}_2(\mathbb{Z}_p)$ has determinant 6 and $N \in \mathrm{GL}_2(L_0)$ is similar to $\Delta_{1,-1}$ or $\Delta_{u,-u^{-1}}$ for some primitive eighth root of unity u, then $\ker(M \otimes N - \sqrt{6})$ is not a line.

Note that $\sqrt{2} \in \mathbb{Z}_p$ and $\sqrt{3} \notin \mathbb{Z}_p$, so $\sqrt{6} \notin \mathbb{Z}_p$. Hence M has distinct eigenvalues α, β with product 6, so we can rule out $N \sim \Delta_{1,-1}$. Suppose that $N \sim \Delta_{u,-u^{-1}}$ works, where u is a primitive 8-th root of unity. Then (up to relabelling the eigenvalues) $\alpha = u^{-1}\sqrt{6}$, and

$\mathrm{Tr}(u) = \alpha + 6/\alpha = \sqrt{6}(u + u^{-1}) \in \mathbb{Z}_p$. Since $(u + u^{-1})^2 = u^2 + u^{-4}u^2 + 2 = u^2(1-1) + 2 = 2$, $\mathrm{Tr}(u)^2 = 3 \cdot 4 \notin \mathbb{Z}_p^{\times 2}$, a contradiction.

(c) According to the LMFDB, L, F, H and ε_g are as above (so ε_g is the quadratic character of $H/\mathbb{Q}$), and $\rho_g'(G_\mathbb{Q}) \cong A_4$, while $\rho_g(G_\mathbb{Q})$ has cardinality 48: its scalar subgroup is $\{\pm iI_2, \pm I_2\}$. Thus, $\rho_g'(G_H)$ is a subgroup of index at most 2 of A_4, so is A_4: hence $\rho_g(G_H)$ is a subgroup of $\mathrm{SL}_2(L_0)$ whose projective image is A_4, and $\rho_g(G_\mathbb{Q}\backslash G_H) = i\rho_g(G_H)$.

As above, we want to show that if $M \in \mathrm{GL}_2(\mathbb{Z}_p)$ has determinant 6 and $N \in \rho_g(G_H)$ (so $\det N = 1$), then $\ker\left(M \otimes N - i\sqrt{6}\right)$ is never a line. Write α and $\beta = 6/\alpha$ for the two eigenvalues of M. Because of our choice of p, $\mathbb{Z}_p^{\times 2}$ does not contain 6 or 2.

If N is scalar, then $N = \pm I_2$, and the result is clear.

If the projective image of N is a bitransposition, $N \sim \Delta_{i,-i}$, and thus (up to relabelling), $i\alpha = \pm i\sqrt{6}$, so $\alpha = \beta = \pm\sqrt{6}$, which we excluded.

If the projective image of N is a 3-cycle, then $N \sim \Delta_{j,j^2}$, and thus $\alpha \in \{ij\sqrt{6}, ij^2\sqrt{6}\}$. Thus $\mathrm{Tr}(M) = \alpha + 6/\alpha = \pm i\sqrt{6}(j - j^2) = \pm 3\sqrt{2}$ does not lie in $\mathbb{Z}_p$, a contradiction.

(d) In this case, $L = \mathbb{Q}(\sqrt{3})$, $F = \mathbb{Q}$, $H = \mathbb{Q}(j)$ and ε_g is the character of $H/\mathbb{Q}$, but g has complex multiplication by $\mathbb{Q}(\sqrt{-11})$. Moreover, the field of coefficients of g is $\mathbb{Q}(j)$ and its projective image is the dihedral group of order 12. Thus, the only scalar matrices contained in $\rho_g(G_\mathbb{Q})$ are $\pm I_2$, and $\det : \rho_g'(G_\mathbb{Q}) \to \{\pm 1\}$ is well-defined, with kernel $\rho_g'(G_H)$ (the latter is contained in the former, and the latter has index at most 2 in $\rho_g'(G_\mathbb{Q})$).

So $\rho_g'(G_H)$ is a subgroup of index 2 of $\rho_g(G_\mathbb{Q})$ which is not cyclic. Thus, elements of $\rho_g(G_\mathbb{Q})\backslash\rho_g(G_H)$ fall in two categories: matrices N with $\det N = -1$ and projective order 2 (thus $N \sim \Delta_{1,-1}$), and matrices N with $\det N = -1$ and projective order 6. Such a matrix $N \in \rho_g(G_\mathbb{Q})$ is of the form $\Delta_{u,-u^{-1}}$, with $u^6 = u^{-6}$ and $u^3 \neq -u^{-3}$, so $u^6 = 1$. Since N^2 is not scalar, $u \in \{\pm j, \pm j^2\}$.

Exactly like above, we need to show that for any matrix $M \in \mathrm{GL}_2(\mathbb{Z}_p)$ with $\det M = 3$, for any N as above, $\ker(M \otimes N - \sqrt{3})$ cannot be a line.

If $N \sim \Delta_{1,-1}$, this follows exactly like above from the fact that $3 \notin \mathbb{Z}_p^{\times 2}$. Otherwise, if the statement is false, M has an eigenvalue α such that $\{\alpha j, \alpha j^2\}$ meets $\{\pm\sqrt{3}\}$. Thus, $\mathrm{Tr}(M) = \alpha + 3/\alpha = \pm\sqrt{3}(j + j^2) = \pm\sqrt{3} \notin \mathbb{Z}_p$, hence a contradiction.

(e) In this case, $L = \mathbb{Q}(\sqrt{7}), F = \mathbb{Q}$ and $H = \mathbb{Q}(\sqrt{-3})$; g has complex multiplication by $\mathbb{Q}(\sqrt{-51})$, ε_g is a character of conductor 51 and order 4, and $\rho_g'(G_\mathbb{Q}) \cong S_3$. Since $\varepsilon_g(2893) = \pm i$, $\varepsilon_g(G_H) = \{\pm 1, \pm i\} = \varepsilon_g(G_\mathbb{Q})$. The LMFDB shows that $\rho_g(G_\mathbb{Q})$ is isomorphic to $S_3 \times \mathbb{Z}/8\mathbb{Z}$. Its center (which is scalar, by Schur's lemma), is thus the set of 8-th roots of unity, and $\rho_g(G_\mathbb{Q}) \cap \mathrm{SL}_2(L_0) \to \rho_g'(G_\mathbb{Q})$ is onto with kernel $\{\pm I_2\}$.

The LMFDB data stipulates that $\ker \rho_g' \not\subset G_H$, so $\rho_g'(G_H) = \rho_g'(G_\mathbb{Q})$. Using MAGMA [16], we can alse see that $\ker \rho_g \subset G_H$, so that $[\rho_g(G_\mathbb{Q}) : \rho_g(G_H)] = 2$.

For the sake of easier notation, write $C \subset \rho_g(G_\mathbb{Q})$ for the pre-image of the non-trivial elements of the cyclic subgroup of order 3 of $\rho_g'(G_\mathbb{Q})$.

Since $\rho_g(G_H)$ and $\rho_g(G_\mathbb{Q})$ have the same determinant and projective image, we can split elements of $\rho_g(G_H)$ in six categories: $\{\pm iI_2, \pm I_2\}$, scalar matrices of order 8, matrices in C with determinant ± 1, matrices in C with determinant $\pm i$, matrices outside C with determinant ± 1, matrices outside C with determinant $\pm i$. Then $\rho_g(G_H)$ is exactly made with the matrices of the first, third, and last categories.

As above, we need to show that if $(M, N) \in \mathrm{SL}_2(\mathbb{Z}_p) \times \rho_g(G_H)$, $\ker[M \otimes N - 1]$ is never a line, and that, if $(M, N) \in \mathrm{GL}_2(\mathbb{Z}_p) \times [\rho_g(G_\mathbb{Q})\backslash\rho_g(G_H)]$ is such that $\det M = 7$, then $\ker\left[M \otimes N - \sqrt{7}\right]$ is never a line again.

Note that by our choice of p, $\mathbb{Z}_p$ contains none of $\sqrt{2}, \sqrt{3}, \sqrt{7}$, and $7! \in \mathbb{Z}_p^\times$.

Let $M \in \mathrm{SL}_2(\mathbb{Z}_p)$ (with eigenvalues α and $1/\alpha$) and $N \in \rho_g(G_H)$ be such that $\ker(M \otimes N - 1)$ is a line. Clearly, N is not scalar, and $\det N \neq 1$. Note that $\mathrm{Tr}(M) = \alpha + 1/\alpha \in \mathbb{Z}_p$.

Suppose that $N \in C$. Then $\det N = -1$, so that $N \sim \pm i\Delta_{j,j^2}$. Thus (up to exchanging α and $1/\alpha$) $\alpha \in \{\pm ij, \pm ij^2\}$. Thus $\mathrm{Tr}(M) = \alpha + 1/\alpha = \pm i(j - j^2) = \pm\sqrt{3} \notin \mathbb{Z}_p$, so we get a

contradiction.

So $N \notin C$: thus $\det N = \pm i$ and N^2 is scalar. So $N \sim \Delta_{u,-u}$, where $-u^2 = \pm i$, thus u is a primitive 8-th root of unity. Then $\alpha = \pm u^{-1}$, so $\mathrm{Tr}(M) = \alpha + 1/\alpha = \pm(u + 1/u) = \pm\sqrt{2} \notin \mathbb{Z}_p$, so we get a contradiction.

Let now $M \in \mathrm{GL}_2(\mathbb{Z}_p), N \in \rho_g(G_\mathbb{Q})\backslash\rho_g(G_H)$ such that $\det M = 7$ and $\ker(M \otimes N - \sqrt{7})$ is a line. Let α and $7/\alpha$ be the distinct eigenvalues of M (since $\sqrt{7} \notin \mathbb{Z}_p$). Clearly, N is not scalar, and $\det N \neq 1$.

Suppose that $N \in C$: then $\det N = \pm i$, so that $N \sim u\Delta_{j,j^2}$ for some primitive 8-th root of unity u. So $\alpha \in \{\sqrt{7}ju^{-1}, \sqrt{7}j^2u^{-1}\}$. Thus there is some primitive 24-th root of unity ω such that $\alpha = \sqrt{7}\omega$. Then $\mathrm{Tr}(M)^2 = 7(\omega + 1/\omega)^2 \in \mathbb{Z}_p$, so $\omega^2 + \omega^{-2} \in \mathbb{Z}_p$. Now, $(\omega^2+\omega^{-2})^2 = \omega^4+2+\omega^{-4} = 2-(\omega^8+\omega^{-8}) = 2-(-1) = 3$ (since ω^8, ω^{-8} are the two primitive third roots of unity, and $\omega^{12} = -1$): but $3 \notin \mathbb{Z}_p^{\times 2}$, a contradiction.

So $N \notin C$ and $\det N = -1$, then $N \sim \Delta_{1,-1}$, so we get $\alpha = 7/\alpha$, a contradiction. □

The proposition below, on the other hand, shows that, even in the exceptional case of Proposition 6.3.8, the representation can still have Euler-adapted Galois image.

Proposition 6.5.3 *Let $f \in \mathcal{S}_2(\Gamma_0(63)), g \in \mathcal{S}_1(\Gamma_1(675))$ be newforms with respective labels 63.2.a.b and g be 675.1.g.a. Then $T_{f,g,\mathfrak{p}}$ has Euler-adapted Galois image for every good prime $\mathfrak{p}$.*

Remark In this case, $L = \mathbb{Q}(\sqrt{3}), F = \mathbb{Q}, H = \mathbb{Q}(\sqrt{-3})$, and ε_g is a character of conductor 5 and order 4. Moreover, $\rho_g'(G_\mathbb{Q})$ is the dihedral group of order 12, and g has complex multiplication by $\mathbb{Q}(\sqrt{-15}) \neq H$. Furthermore, the number field LMFDB data shows that $\ker\rho_g' \subset G_H$, so $[\rho_g'(G_\mathbb{Q}) : \rho_g'(G_H)] = [\rho_g(G_\mathbb{Q}) : \rho_g(G_H)] = 2$. Since $a_{139}(g) = \pm 2i$, $iI_2 \in \rho_g(G_H) \subset \rho_g(G_\mathbb{Q})$. Since the coefficient field of g is $\mathbb{Q}(i, \sqrt{6})$, it does not contain the primitive 8-th root of unity, and the scalar matrices of $\rho_g(G_\mathbb{Q})$ are exactly $\pm iI_2, \pm I_2$. Finally, $\varepsilon_g(G_H) = \varepsilon_g(G_\mathbb{Q}) = \{\pm i, \pm 1\}$, since ε_g and H have prime conductors.

It seems that we are in the "exceptional" case of Proposition 6.3.8. However, it turns out that (sE) still holds for every good prime $\mathfrak{p}$.

Proof. – Let us fix such a prime $\mathfrak{p}$. By the proof of Proposition 6.3.8, since $iI_2 \in \rho_g(G_H)$, we are done if $\rho_g(G_H)$ contains an element whose projective image has order 2 and determinant ± 1. So we may assume that the elements of $\rho_g(G_H)$ whose projective image lies outside the maximal cyclic subgroup have determinant $\pm i$.

Let N be such a matrix: then $N \sim \Delta_{u,-u}$, for some u such that $u^2 = \pm i$. Since $(u+1/u)^2 = 2$, if $\sqrt{2} \in \mathbb{Z}_p$, then there exists $M \in \mathrm{SL}_2(\mathbb{Z}_p)$ similar to $\Delta_{u,u^{-1}}$. So there exists $\sigma \in G_{H(\mu_{p^\infty})}$ such that σ acts on $T_{f,\mathfrak{p}}$ (resp. T_g) by M (resp. N). Then $M \otimes N$ has four eigenvalues: $1, -1, i, -i$. So σ shows that (sE) holds. Hence, we now assume that $\sqrt{2} \notin \mathbb{Z}_p$.

Suppose that the restriction of the determinant map $\delta : \rho_g'(G_\mathbb{Q}) \to \varepsilon_g(G_\mathbb{Q})/\{\pm 1\} \cong \mathbb{F}_2$ to the cyclic subgroup is trivial. Since the complex conjugation also lies in $\ker\delta$, δ is trivial, and thus is not onto, a contradiction. Hence, δ maps the unique element of order 2 of the cyclic subgroup (which does not belong to $\rho_g'(G_H)$) to the coset $\{\pm i\}$. Considering the complex conjugation, we see that $\rho_g(G_\mathbb{Q})\backslash\rho_g(G_H)$ contains elements of projective order 2 with determinant -1 and i.

Let $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}\backslash G_H$: then Corollary 6.3.4 shows that σ acts on $T_{f,\mathfrak{p}}$ as $M/\sqrt{3}$, where $M \in \mathrm{GL}_2(\mathbb{Z}_p)$ has determinant 3. If $\sqrt{3} \in \mathbb{Z}_p$, then we can find $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}\backslash G_H$ acting on $T_{f,\mathfrak{p}}$ by U, and on T_g by a matrix of determinant -1 whose projective image has order 2 (hence is similar to $\Delta_{1,-1}$), and we conclude like in the proof of Proposition 6.3.8.

So we may assume that $\sqrt{2}, \sqrt{3} \notin \mathbb{Z}_p$, and therefore that $\sqrt{6} \in \mathbb{Z}_p$. Let $N \in \rho_g(G_\mathbb{Q})\backslash\rho_g(G_H)$ have determinant i and be such that its projective image has order 2: then $N \sim \Delta_{u,-u}$ for some primitive 8-th root of unity u. Then $\sqrt{3}u+\sqrt{3}u^{-1} = \pm\sqrt{6} \in \mathbb{Z}_p$: hence there exists $M \in \mathrm{GL}_2(\mathbb{Z}_p)$ with eigenvalues $\sqrt{3}u, \sqrt{3}u^{-1}$. Thus, there exists $\sigma \in G_{\mathbb{Q}(\mu_{p^\infty})}\backslash G_H$ such that σ acts on $T_{f,\mathfrak{p}}$ (resp. T_g) by $M/\sqrt{3}$ (resp. N). Hence, the eigenvalues of σ acting on $T_{f,g,\mathfrak{p}}$ are $\pm 1, \pm i$ as above, so (sE) holds. □

Remark This argument can be somewhat generalized. If $\rho_g(G_{\mathbb{Q}})$ is dihedral with order $4n$ with $n > 1$ odd, if $[\rho_g(G_{\mathbb{Q}}) : \rho_g(G_H)] = [\rho'_g(G_{\mathbb{Q}}) : \rho'_g(G_H)] = 2$ and H is not the CM field of g, if $\varepsilon_g(G_H) = \varepsilon_g(G_{\mathbb{Q}}) = \{\pm 1, \pm i\}$, and there is some $\sigma \in G_{\mathbb{Q}} \backslash G_H$ such that $\varepsilon_f(\sigma) = 1$ and $\rho_g(\sigma) \notin \rho_g(G_H)$, then (sE) will hold.

Appendix A

Prerequisites from algebraic geometry

This Appendix collects the background from algebraic geometry which is useful to the discussion of moduli schemes and Galois twists in Chapter 1. This background comes in four rather different collections of results. The first part is about descent and its various applications. The main reference here is the online textbook Stacks Project [4]. The second part collects results on one possible compactification method for schemes that are finite over the affine line over a suitable basis. This is necessary to discuss compatified modular curves as in Chapter 1. The third part is about the classical properties of abelian varieties and abelian schemes. I am grateful to Discord user topos_theory_egirl for making me aware of the article [2] and for correcting my simplistic intuition for abelian schemes. The last part of this appendix discusses Jacobians. It is well-known (while it does not seem to be directly stated, it is easily deduced from various results in [15, Chapter 8]) that relative proper smooth curves admit well-behaved Jacobians when their geometric fibres are connected. But it is necessary, in our setting, to slightly adapt this material in order to deal with relative curves whose fibres are not geometrically connected. I would like to thank Qing Liu for his help with this adaptation.

A.1 Results from descent

A.1.1 Sheaves in the fpqc topology

Recall the following definition [4, Definition 022B]: let T be a scheme, and $(\pi_i)_{i\in I}$ be a family of flat scheme morphisms to T, with $\pi_i : T_i \to T$. This family is a *fpqc covering* if for every affine open subscheme $U \subset T$, there is a finite set F, a map $j : F \to I$, and affine open subsets $W_f \subset T_{j(f)}$ for each $f \in F$, such that $U = \bigcup_{f\in F} \pi_{j(f)}(W_f)$.

Theorem A.1.1 *(see [4, Lemma 023Q]) Let S be a scheme, and T be a S-scheme. Then the functor $V \in \mathbf{Sch}_S \longmapsto \mathrm{Mor}_S(V,T)$ satisfies the sheaf property for fpqc covers.*

Proof. – Given a scheme A, let F_A be the pre-sheaf $T \in \mathbf{Sch} \longmapsto \mathrm{Mor}(T,A)$. By *loc. cit.*, it satisfies the sheaf property for fpqc covers. The forgetful functor $\omega_S : \mathbf{Sch}_S \to \mathbf{Sch}$ maps an fpqc cover to an fpqc cover, so the presheaves $F'_T := F_T \circ \omega_T, F'_S := F_S \circ \omega_S$ on $\mathbf{Sch}_S$ satisfy the sheaf property for fpqc covers. Let G be the sheaf on $\mathbf{Sch}_S$ given by the following: for all S-schemes T, $G(T)$ has a single element (and the restriction map is the trivial one). There are natural morphisms of sheaves $G \to F'_S$ (sending the point of $G(V)$ to the structure map $V \to S$), $F'_T \to F'_S$ (composing with the structure map $T \to S$), and the functor that we are studying is exactly $V \longmapsto F'_T(V) \times_{F'_S(V)} G(V)$, which formally satisfies the sheaf property for fpqc covers.□

Proposition A.1.2 *Let S be a scheme, and U, V be two S-schemes. The functor*

$$T \in \mathbf{Sch}_S \longmapsto \mathrm{Mor}_T(U_T, V_T)$$

satisfies the sheaf property for fpqc covers. The subfunctor mapping a S-scheme T to the set of

T-isomorphisms $U_T \to V_T$ also satisfies the sheaf property for fpqc covers.

Proof. – The first functor is isomorphic to $T \in \mathbf{Sch}_S \longmapsto \mathrm{Mor}_S(U_T, V)$. It is formal to check that the functor $T \in \mathbf{Sch}_S \longmapsto U \times_S T \in \mathbf{Sch}_S$ preserves fpqc covers, and we are done.

For the second functor, it is clear from the above that it is separated – two sections that agree on a fpqc cover are equal. Let $\pi_i : T_i \to T$ for $i \in I$ be an fpqc cover, and $\alpha : U_T \to V_T$ be a T-morphism such that for each $i \in I$, $\alpha \times_T T_i : U_{T_i} \to V_{T_i}$ is an isomorphism; it is enough to prove that α is an isomorphism. This is exactly [4, Lemma 02L4] since the $V_{T_i} \to V_T$ are a fpqc cover, and $\alpha \times_T T_i$ is the base change of α by $V_{T_i} \to V_T$. □

Proposition A.1.3 *Let S be a scheme, and U, V be two S-group schemes. The functors*

$$\underline{Mor}_{S-Gp}(U, V) : T \in \mathbf{Sch}_S \longmapsto \mathrm{Mor}_{T-Gp}(U_T, V_T),$$
$$\underline{Iso}_{S-Gp}(U, V) : T \in \mathbf{Sch}_S \longmapsto \mathrm{Iso}_{T-Gp}(U_T, V_T)$$

satisfy the sheaf property for fpqc covers.

Proof. – We deal with the first functor first. Let $F_1 = \underline{Mor}_S(U, V), F_2 = \underline{Mor}_S(U \times U, V)$ be fpqc sheaves. We can define two morphisms $\alpha, \beta : F_1 \to F_2$ as follows: given a S-scheme T and a T-map $\varphi : U_T \to V_T$, $\alpha(\varphi) = m_{V_T} \circ (\varphi \times \varphi)$, where m_{V_T} is the multiplication of the group scheme V_T over T, and $\varphi \times \varphi : U_T \times_T U_T \to V_T \times_T V_T$. We define $\beta(\varphi) = \varphi \circ m_{U_T}$. Then given $u \in \underline{Mor}_S(U, V)(T)$, $u \in \underline{Mor}_{S-Gp}(U, V)(T)$ if and only if $\alpha(u) = \beta(u)$. The conclusion follows formally.

The second functor corresponds to the intersection in $\underline{Mor}_S(U, V)$ of the two subsheaves $\underline{Mor}_{S-Gp}(U, V)$ and $\underline{Iso}_S(U, V)$: it is thus a fpqc sheaf. □

Proposition A.1.4 *Let S be a scheme, and $T \to S$ be a fpqc cover. Let F be a fpqc sheaf on $\mathbf{Sch}_S$ such that its restriction to the category $\mathbf{Sch}_T$ is representable by an affine T-scheme X[1]. Then F is representable by an affine S-scheme X', and $X \simeq X' \times_S T$.*

Proof. –

Step 1: $S = \mathrm{Spec}\, A$

After refining T, we may assume that $T = \mathrm{Spec}\, B$, where $A \to B$ is faithfully flat, and $X = \mathrm{Spec}\, C$, where C is some B-algebra. The hypothesis implies that there exists some $\alpha \in F(X)$ satisfying the following property: for every T-scheme Z with structure map $g : Z \to T$, the map $f \longmapsto \mathrm{Mor}_T(Z, X) \to F(f)\alpha \in F(Z)$ is an isomorphism.

Let $f_1 \in \mathrm{Mor}_T(X \times_S T, X)$ (where $X \times_S T$ is a T-scheme by the second projection) be the unique T-homomorphism such that $F(f_1)\alpha = F(X \times_S T \overset{\mathrm{pr}_1}{\to} X)\alpha$. This defines a map $\pi = (\sigma, f_1) : X \times_S T \to T \times_S X$ of $T \times_S T$-schemes, where $\sigma : X \to T$ is the structure map.

We define the map of T-schemes $f_2 : T \times_S X \to X$ (where $T \times_S X$ is a T-scheme by first projection) such that $F(f_2)\alpha = F(T \times_S X \overset{\mathrm{pr}_2}{\to} X)\alpha$. We then define $\pi' = (f_2, \sigma) : T \times_S X \to X \times_S T$, which is a map of $T \times_S T$-schemes.

Then $\pi \circ \pi'$ is an endomorphism of the $T \times_S T$-scheme $T \times_S X$, so its first component is the first projection $T \times_S X \to T$. Its second component p_2 is a morphism of T-schemes (on the source, through the T-scheme structure on X); furthermore, we have

$$F(p_2)\alpha = F(\pi')F(f_1)\alpha = F(\pi')F(\mathrm{pr}_1)\alpha = F(\mathrm{pr}_1 \circ \pi')\alpha = F(f_2)\alpha = F(\mathrm{pr}_2)\alpha.$$

Since p_2, pr_2 are two maps of T-schemes $T \times_S X \to X$ *for the same T-structure*, it follows that $p_2 = \mathrm{pr}_2$, and $\pi \circ \pi'$ is the identity.

One similarly proves that $\pi' \circ \pi$ is the identity, hence π, π' are isomorphisms of $T \times_S T$-schemes.

Now, let us show that the following two compositions of $T^{\times_S 3}$-morphisms are the same:

[1] That is, the map $X \to T$ is affine.

$$T \times_S T \times_S X \overset{\mathrm{id}\times_S\pi'}{\to} T \times_S X \times_S T \times \overset{\pi'\times\mathrm{id}}{\to} X \times_S T \times_S T,$$
$$\pi'_{13} = (f_2 \circ \mathrm{pr}_{13}, \mathrm{id}, \sigma \circ \mathrm{pr}_{13}) : T \times_S T \times_S X \to X \times_S \times_S T$$

It is clear that the projections on the second and third components are the same (since these are morphisms of $T^{\times_S 3}$-schemes), so all we need to do is prove that the first components of the two morphisms are equal. It is simple to compute that these first components are respectively $f_2 \circ (\mathrm{id} \times f_2)$ and $f_2 \circ \mathrm{pr}_{13}$.

Since these morphisms are morphisms of T-schemes for the same structure (projection on the first component on the source), it is thus enough to prove that $F(f_2 \circ (\mathrm{id} \times f_2))\alpha = F(f_2 \circ \mathrm{pr}_{13})\alpha$.

Now,

$$\begin{aligned} F(f_2 \circ \mathrm{pr}_{13})\alpha &= F(\mathrm{pr}_{13})F(f_2)\alpha = F(\mathrm{pr}_{13})F(\mathrm{pr}_2)\alpha = F(\mathrm{pr}_2 \circ \mathrm{pr}_{13})\alpha \\ &= F(\mathrm{pr}_3 : T \times_S \times_S X \to X)\alpha, \\ F(f_2 \circ (\mathrm{id} \times f_2))\alpha &= F(\mathrm{id} \times f_2)F(f_2)\alpha = F(\mathrm{pr}_2 \circ (\mathrm{id} \times f_2))\alpha = F(f_2 \circ \mathrm{pr}_{23})\alpha \\ &= F(\mathrm{pr}_{23})F(f_2)\alpha = F(\mathrm{pr}_{23})F(\mathrm{pr}_2)\alpha = F(\mathrm{pr}_3)\alpha. \end{aligned}$$

We can thus apply [4, Proposition 023N][2]. This Proposition implies that we can assume that, for some T-isomorphism $(\chi, \sigma) : X \to Y \times_S T$ we have a commutative diagram of $T \times_S T$-schemes:

$$\begin{array}{ccc} T \times_S X & \xrightarrow{\pi'} & X \times_S T \\ \downarrow{\scriptstyle \mathrm{id}\times(\chi,\sigma)} & & \downarrow{\scriptstyle (\sigma,\chi)\times\mathrm{id}} \\ T \times_S (Y \times_S T) & \xrightarrow{\mathrm{can}} & (T \times_S Y) \times_S T \end{array}$$

Let $\alpha' = F((\chi, \sigma)^{-1})\alpha \in F(Y \times_S T)$. Then the following statement holds:

For any T-scheme $g : Z \to T$, $f \in \mathrm{Mor}_S(Z, Y) \longmapsto F((f, g))\alpha' \in F(Z)$ is a bijection. $(*)$

Moreover, the following diagram is easily checked to commute (the indices on T just describe what the lower arrows do):

$$\begin{array}{ccccc} X & \xleftarrow[\mathrm{pr}_2]{} & T \times_S X & \xrightarrow{f_2} & X \\ \downarrow{\scriptstyle (\sigma,\chi)} & & \downarrow{\scriptstyle \mathrm{id}\times(\chi,\sigma)} & & \downarrow{\scriptstyle (\sigma,\chi)} \\ Y \times_S T_2 & \longleftarrow & T_1 \times_S (Y \times_S T_2) & \longrightarrow & Y \times_S T_1 \end{array}$$

Therefore, the pull-backs of α' under both projections $Y \times_S T \times_S T \to Y \times_S T$ are the same. Hence, α' is the pull-back of a class $\alpha_0 \in F(Y)$. Thus, we have a natural homomorphism $f \in \mathrm{Mor}_S(Z, Y) \longmapsto F(f)\alpha_0 \in F(Z)$ of fpqc sheaves on $\mathbf{Sch}_S$. By $(*)$, the application is an isomorphism whenever there is a map $g : Z \to T$ of S-schemes. Since every S-scheme has an fpqc cover by T-schemes, the above morphism is an isomorphism of fpqc sheaves.

Step 2: Glueing affine data

By Step 1, for every affine open subset $U \subset S$, there exists an affine U-scheme X'_U and some $\alpha_U \in F(X'_U)$ such that for every U-scheme V, $f \in \mathrm{Mor}_U(V, X'_U) \longmapsto F(f)\alpha_U \in F(V)$ is a bijection. Moreover, for every inclusion $V \subset U$ of affine open subsets of S, there is a unique map $j_{VU} : X'_V \to X'_U$ of U-schemes such that $F(j_{VU})\alpha_U = \alpha_V$.

Let us prove that every j_{VU} is an open immersion. There is a class $\beta_T \in F(X)$ such that for every T-scheme Z, $f \in \mathrm{Mor}_T(Z, X) \longmapsto F(f)\beta_T \in F(Z)$ is an isomorphism. In particular, for any affine open $U \subset S$, there is a unique morphism of T-schemes $f_U : X'_U \times_S T \to X$ such that

[2]This proposition is formulated for modules over rings, but the explicit construction shows that it works for algebras as long as the descent datum is also a ring homomorphism, hence it works for affine schemes as well.

$F(f_U)\beta_T$ is $F(X'_U \times_S T \to X'_U)\alpha_U$. Since f_U factors through $f^0_U : X'_U \times_S T \to X \times_S U$ which is an isomorphism of T-schemes (by relating its functor of T-points to F), hence f_U is an open immersion.

Given affine open subsets $V \subset U$ of S, one easily sees that $f_U \circ (j_{VU} \times \mathrm{id}_T) = f_V$. Therefore $j_{VU} \times \mathrm{id}_T$ is an open immersion, hence j_{VU} is one too by [4, Lemma 02L3].

Finally, the definition implies easily that, given affine open subsets $W \subset V \subset U$ of S, $j_{VU} \circ j_{WV} = j_{WU}$, so that the (X'_U, j_{VU}) is a glueing data in the sense of [4, Section 01JA]. Therefore, by *loc. cit.*, the X_U glue to an S-scheme X', the α_U to some $\alpha \in F(X')$, and the f_U to some morphism $f : X' \times_S T \to X$, which is an isomorphism after base changing to any affine open subset of S, hence is an isomorphism, and such that $F(f)\beta_T = F(X' \times_S T \to X')\alpha$.

Exactly like in Step 1, this α produces a homomorphism of fpqc sheaves $\phi : \underline{\mathrm{Mor}}_S(-, X') \to F$ on $\mathbf{Sch}_S$, and $\phi(Z)$ is an isomorphism for every S-scheme admitting a map to T. Since every S-scheme has a fpqc cover by a T-scheme, it follows that ϕ is an isomorphism. □

We conclude this section by discussing some examples of ascending and descending properties.

Proposition A.1.5 *Let $\mathcal{P}$ be one of the following properties of morphisms of schemes: isomorphism, surjective, affine, quasi-compact, closed immersion, open immersion, locally of finite type, locally of finite presentation, locally quasi-finite, finite, flat, étale, smooth of relative dimension d, Cohen-Macaulay of relative dimension d, proper.*

Let $f : X \to Y$ be a morphism of schemes and assume that there is a fpqc cover $Y_i \to Y$ such that the base change of f by any $Y_i \to Y$ satisfies property $\mathcal{P}$. Then f satisfies property $\mathcal{P}$.

Proof. – See [4, Section 02YJ]. □

Proposition A.1.6 *Let $R \to S$ be a faithfully flat morphism of local rings. Suppose that S is Noetherian (resp. Noetherian and (R_k), resp. Noetherian and (S_k), resp. reduced, resp. normal, resp. Cohen-Macaulay, resp. regular), then R is Noetherian (resp. Noetherian and (R_k), resp. Noetherian and (S_k), resp. reduced, resp. normal, resp. Cohen-Macaulay, resp. regular).*

Proof. – See [4, Section 033D]. □

Proposition A.1.7 *Let $R \to S$ be a flat morphism of rings. Then the following properties hold:*

- *If R, S are Noetherian, R is (R_k) (resp. (S_k), resp. reduced, resp. normal) and every $S \otimes \kappa(\mathfrak{p})$ (for $\mathfrak{p} \in \operatorname{Spec} R$) is (R_k) (resp. (S_k), resp. reduced, resp. normal), then S is (R_k) (resp. (S_k), resp. reduced, resp. normal).*
- *If S is a smooth R-algebra and R is reduced (resp. normal, resp. regular), then S is reduced (resp. normal, resp. regular).*

Proof. – See [4, Section 0336]. □

A.1.2 Galois twists of schemes

Lemma A.1.8 *Let V be a vector space over a field L, and $\mathrm{Gal}(L/k)$ act semi-linearly on V, where L/k is finite Galois. Then the natural map $V^{\mathrm{Gal}(L/k)} \otimes_k L \to V$ is an isomorphism of L-vector spaces.*

Proof. – To ease notation, write $G = \mathrm{Gal}(L/k)$. Let $(w_i)_i$ be a finite family of vectors of V^G which is k-free. Let us show that this family is free over L in V. Indeed, suppose that we have $\lambda_i \in L$ such that $\sum_i \lambda_i w_i = 0$. Multiplying this equation by a fixed $\alpha \in L$ and applying $\sum_{g \in G} g$, we find that $\sum_i \tau(\alpha\lambda_i) w_i = 0$, where $\tau : L \to k$ is the trace map. Since the w_i are k-free, we find that for all i and all $\alpha \in L$, $\tau(\alpha\lambda_i) = 0$. This implies that every $\lambda_i = 0$, and we are done. Thus the map $V^G \otimes_k L \to V$ is injective.

By the normal basis theorem, we know that there are $\lambda_g \in L$ for each $g \in G$ such that for all $g, h \in G$, $g(\lambda_h) = \lambda_{gh}$, and such that $(\lambda_g)_g$ is a basis of L as a k-vector space. Let us show that

the family of the vectors $w_h := (\lambda_{gh})_{g\in G}$ (for $h \in G$) is a basis of L^G. Since this family has the correct cardinality, it is enough to show that it is free. So let $\mu_h \in L$ for each $h \in G$ such that $\sum_h \mu_h\lambda_{gh} = 0$ for each $g \in G$. Then, for any $\alpha \in L$ and $g \in G$, we have $\sum_{h\in G} g^{-1}(\alpha\mu_h)\lambda_h = 0$. By taking the sum over $g \in G$, we find that $\sum_{h\in G} \tau(\alpha\mu_h)\lambda_h = 0$. Thus every $\tau(\alpha\mu_h)$ vanishes, thus every μ_h vanishes.

In particular, there is a L-linear combination of the w_h which is the indicator function of the unit element of G. It follows that there is a L-linear combination of the $v_h := \sum_{g\in G} \lambda_{gh} g(v) \in V^G$ which is mapped to v. Hence the map is onto. □

Lemma A.1.9 *Let L/K be a finite Galois extension, and U, V be two K-schemes. There is a natural action of* $\mathrm{Gal}(L/K)$ *on* $\mathrm{Mor}_L(U_L, V_L)$. *The base change map*

$$f \in \mathrm{Mor}_K(U, V) \longmapsto f \times \mathrm{id}_L \in \mathrm{Mor}_L(U_L, V_L)^{\mathrm{Gal}(L/K)}$$

is an isomorphism.

Proof. – This map is clearly well-defined. Since, $\mathrm{Spec}\, L \to \mathrm{Spec}\, K$ is a fpqc cover, the base change map is injective by Proposition A.1.2. To prove surjectivity, it is enough to show that if $f \in \mathrm{Mor}_L(U_L, V_L)^{\mathrm{Gal}(L/K)}$, and $\pi_1, \pi_2 : \mathrm{Spec}\, L \times_k \mathrm{Spec}\, L \to \mathrm{Spec}\, L$ are the projections, then $\pi_1^* f = \pi_2^* f$. Let us assume that there is an isomorphism of L-algebras $L \otimes_k L \simeq L^{\oplus \mathrm{Gal}(L/K)}$ (where L acts on the left side by multiplication on the right factor), so it is enough to show that for any $\tau : \mathrm{Spec}\, L \to \mathrm{Spec}\, L \times_k \mathrm{Spec}\, L$, one has $\tau^*\pi_1^* f = \tau^*\pi_2^* f$. In other words, one only needs to show that given $\sigma \in \mathrm{Gal}(L/K)$ inducing a map $\underline{\sigma} : \mathrm{Spec}\, L \to \mathrm{Spec}\, L$, $\underline{\sigma}^* f$ does not depend on the choice of σ. This is exactly the assumption.

So we only need to prove that there is a L-algebra isomorphism $\mu : L \otimes_k L \simeq L^{\oplus \mathrm{Gal}(L/K)}$. Indeed, for each $\sigma \in \mathrm{Gal}(L/K)$, define $\mu_\sigma : a \otimes b \longmapsto \sigma(a)b$: this is clearly a surjective homomorphism of L-algebras for the given structure on $L \otimes_k L$: let us prove that $\mu = \bigoplus_{\sigma\in \mathrm{Gal}(L/K)} \mu_\sigma$ works. By computing the dimensions, it is enough to show that μ is surjective.

It this wasn't the case, there would be nonzero scalars $\lambda_\sigma \in L$ for each $\sigma \in \mathrm{Gal}(L/K)$ such that $\sum_\sigma \lambda_\sigma\mu_\sigma = 0$. In other words, one would have, for every $a \in L$ and $n \geq 0$, $\sum_\sigma \lambda_\sigma \sigma(a^n) = 0$. So, for every polynomial $P \in L[X]$ and every $a \in L$, we would have $\sum_\sigma \lambda_\sigma P(\sigma(a)) = 0$. If $a \in L$ is chosen to be a primitive element, the $\sigma(a)$ are pairwise distinct, and it follows that all the λ_σ are zero. □

Corollary A.1.10 *Let L/K an algebraic Galois extension and U, V be two quasi-compact K-schemes. There is a natural action of* $\mathrm{Gal}(L/K)$ *on* $\mathrm{Mor}_L(U_L, V_L)$. *The base change map*

$$f \in \mathrm{Mor}_K(U, V) \longmapsto f \times \mathrm{id}_L \in \mathrm{Mor}_L(U_L, V_L)^{\mathrm{Gal}(L/K)}$$

is an isomorphism.

Proof. – As above, the map is well-defined and injective. Let $f : U \times_K L \to V \times_K L$ be a morphism of L-schemes which is $\mathrm{Gal}(L/K)$-invariant. Because V, U are quasi-compact, there is a finite Galois subextension $K \subset L' \subset L$ such that f is a base change of some $f' \in \mathrm{Mor}_{L'}(U_{L'}, V_{L'})$. Since the base change map $\mathrm{Mor}_{L'}(U_{L'}, V_{L'}) \to \mathrm{Mor}_L(U_L, V_L)$ is injective by Proposition A.1.2 and equivariant for $\mathrm{Gal}(L/K)$, f' is fixed under the action of $\mathrm{Gal}(L'/K)$, so is the base change of some $f_0 \in \mathrm{Mor}_K(U, V)$. □

Proposition A.1.11 *Let k be a field with separable closure k_s. For $\sigma \in \mathrm{Gal}(k_s/k)$, denote by $\underline{\sigma}$ the associated automorphism of* $\mathrm{Spec}\, k_s$, *so that* $\mathrm{Gal}(k_s/k)$ *acts on the right on* $\mathrm{Spec}\, k_s$. *Let X be a k-scheme and assume that X is quasi-projective over some k-algebra A*[3]. *Let G be a finite group acting on X_{k_s} by k_s-scheme automorphisms, and $\rho : \mathrm{Gal}(k_s/k) \to G$ be a continuous map satisfying the following cocycle condition: for all $\sigma, \sigma' \in \mathrm{Gal}(k_s/k)$,*

$$\rho(\sigma\sigma') = \rho(\sigma) \circ (\mathrm{id}, \underline{\sigma^{-1}}) \circ \rho(\sigma') \circ (\mathrm{id}, \underline{\sigma}).$$

[3]By quasi-projective, we mean that there is a k-immersion $\iota : X \to \mathbb{P}^n_A$ for some $n \geq 1$.

Then, there is a unique (up to unique isomorphism) couple (X_ρ, j_X) satisfying the following properties:

- *X_ρ is a k-scheme,*
- *$j_X : X_\rho \times_k \operatorname{Spec} k_s \to X \times_k \operatorname{Spec} k_s$ is an isomorphism of k_s-schemes,*
- *for any $\sigma \in \operatorname{Gal}(k_s/k)$, the following diagram commutes:*

$$\begin{array}{ccc} X_\rho \times_k \operatorname{Spec} k_s & \xrightarrow{j_X} & X \times_k \operatorname{Spec} k_s \\ \downarrow{\scriptstyle (\mathrm{id},\underline{\sigma}^{-1})} & & \downarrow{\scriptstyle \rho(\sigma)\circ(\mathrm{id},\underline{\sigma}^{-1})} \\ X_\rho \times_k \operatorname{Spec} k_s & \xrightarrow{j_X} & X \times_k \operatorname{Spec} k_s \end{array}$$

In particular, the following diagram commutes, for any $\sigma \in \operatorname{Gal}(k_s/k)$:

$$\begin{array}{ccc} X_\rho(k_s) & \xrightarrow{j_X} & X(k_s) \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \rho(\sigma)\circ\sigma} \\ X_\rho(k_s) & \xrightarrow{j_X} & X(k_s) \end{array}$$

Let $\mathcal{C}$ be a property of morphisms of k-schemes which is étale-local on the base and stable by pre- and post-composition by isomorphisms (for instance, any of the properties listed in Proposition A.1.5). If $X \to \operatorname{Spec} k$ satisfies $\mathcal{C}$, then so does $X_\rho \to \operatorname{Spec} k$. If $X \to \operatorname{Spec} k$ is projective (resp. quasi-projective), so is $X_\rho \to \operatorname{Spec} k$.

Remark When G acts in fact on X by k-automorphisms, the cocycle condition simply means that $\rho : \operatorname{Gal}(k_s/k) \to G$ is a group homomorphism.

Proof. – Note that the last diagram follows formally from the assumptions (see also Lemma 3.6.21). The second to last assertion is formal, and the last assertion follows from [4, Lemma 0BDE].

Step 1: Uniqueness up to isomorphism.

Assume that (U, j_U) and (V, j_V) are two pairs satisfying the requested conditions. Let $j = j_V^{-1} \circ j_U$: then $j : U_{k_s} \to V_{k_s}$ is an isomorphism of k_s-schemes such that for any $\sigma \in \operatorname{Gal}(k_s/k)$, the following diagram commutes:

$$\begin{array}{ccc} U \times_k \operatorname{Spec} k_s & \xrightarrow{j} & V \times_k \operatorname{Spec} k_s \\ \downarrow{\scriptstyle (\mathrm{id},\underline{\sigma}^{-1})} & & \downarrow{\scriptstyle (\mathrm{id},\underline{\sigma}^{-1})} \\ U \times_k \operatorname{Spec} k_s & \xrightarrow{j} & V \times_k \operatorname{Spec} k_s \end{array}$$

Since U, V are quasi-compact, it follows from Corollary A.1.10 that j is in fact the base change of a map of k-schemes $j_1 : U \to V$. This j_1 becomes an isomorphism after the fpqc base change $V \times_k k_s \to V$, hence is an isomorphism.

Step 2: Uniqueness of the isomorphism.

Suppose now that u is an automorphism of a pair (X_ρ, j_X) satisfying the given conditions. Then, tautologically, $u \times \mathrm{id}_{k_s}$ is the identity. By Proposition A.1.2, it follows that u is the identity.

Step 3: Existence and fonctoriality in the affine case.

Assume that X is the spectrum of some k-algebra A. Since ρ maps the unit element to the identity and acts through a finite quotient of $\operatorname{Gal}(k_s/k)$, there is a finite Galois extension L/k such that $\rho(\operatorname{Gal}(k_s/L))$ is trivial. After enlarging L, since G is finite and X is quasi-compact, we may assume that G acts by automorphisms of L-schemes on $X \times_k L$.

Thus, ρ induces a right action $\rho^\sharp$ of G on $A \otimes_k L$ by L-automorphisms. Let τ_2 denote the natural left action of $\mathrm{Gal}(L/k)$ on $A \otimes_k L$. The cocycle condition is equivalent to

$$\rho^\sharp(\sigma\sigma') = \tau_2(\sigma)\rho^\sharp(\sigma')\tau_2(\sigma)^{-1}\rho^\sharp(\sigma).$$

For $\sigma \in \mathrm{Gal}(L/k)$, let $\tau(\sigma) = \rho^\sharp(\sigma)^{-1}\tau_2(\sigma) \in \mathrm{Aut}_k(L)$. It is straightforward to check that τ defines a semi-linear action of $\mathrm{Gal}[L/k)$ on $A \otimes_k L$. Let thus $B = (A \otimes_k L)^{\mathrm{im}(\tau)}$. By Lemma A.1.8, the natural homomorphism of L-algebras $c : B \otimes_k L \to A \otimes_k L$ is an isomorphism.

We then define $X_\rho = \mathrm{Spec}\, B$ and j_X by the map induced by $A \otimes_k k_s \overset{c^{-1}\otimes_L k_s}{\to} B \otimes_k k_s$; checking that the diagram commutes is then formal.

Note that this construction is functorial: if we have a morphism of affine k-schemes $f : X \to Y$ such that $f \times_k \mathrm{Spec}\, k_s$ is equivariant for the action of the group G, the definition produces a map $f_\rho : X_\rho \to Y_\rho$. Moreover, X_ρ (resp. f_ρ) acquires all the properties of X (resp. f) that are étale-local on the base (for instance, all those listed in Proposition A.1.5).

Step 4: The global twist exists if there are enough good open subsets

Let $U \subset X$ be an open subset; we say that U is *good* if it is affine and stable under G. Let $\mathrm{GoodAff}(X)$ be the partially ordered set of good affine opens of X. Let $\mathrm{LocTw}(X)$ be the category of pairs (T, j), where T is a k-scheme and $j : T \times_k \mathrm{Spec}\, k_s \to X \times_k \mathrm{Spec}\, k_s$ is an open immersion of k_s-schemes, in which the morphisms are open immersions.

Then there is a functor $\mathrm{Tw}_\rho : U \mapsto (U_\rho, j_U)$ from $\mathrm{GoodAff}(X)$ to $\mathrm{LocTw}(X)$. Assume that X can be covered with good open subsets. Because Tw_ρ preserves Zariski-coverings, it defines a glueing data in the sense of [4, Section 01JA], and thus the U_ρ glue to a scheme X_ρ endowed with a k_s-isomorphism $j_X : X_\rho \times_k \mathrm{Spec}\, k_s \to X \times_k \mathrm{Spec}\, k_s$.

Step 5: Existence of good open subsets

Finally, it remains to see that X can be covered by good affine open subsets. Note that it is enough to prove that, for all $x \in X$, there is an affine open subset containing all the G-translates of X. Indeed, since X is separated, we can then take the intersection of the G-translates of this affine open subset.

So all we need to do is the following: show, given any finite $F \subset X$, that there is an affine open subset $U \subset X$ containing F. Indeed, consider the open subset $U' \subset \mathbb{P}^n_A$ such that $\iota : X \to U'$ is a closed immersion, and let I be a homogeneous ideal of $A[x_0, \ldots, x_n]$ (with $I \subset (x_0, \ldots, x_n)$) whose vanishing locus is exactly $\mathbb{P}^n_A \backslash U'$. It is enough to show that there is some homogeneous $f \in I$ of positive degree that does not vanish at any $x \in \iota(F)$. Every $x \in \iota(F)$ defines a homogeneous prime ideal $\mathfrak{p}_x \subset (x_0, \ldots, x_n)A[x_0, \ldots, x_n]$, and we thus seek to prove that $I_+ \not\subset \bigcup_{x \in \iota(F)} \mathfrak{p}_x$, where $I_+ \subset I$ is the subset of homogeneous elements of positive degree, given that we know that $I \not\subset \mathfrak{p}_x$ for all x. This is exactly the graded prime avoidance lemma [4, Lemma 00JS], so we are done. □

Proposition A.1.13 *Let X, Y be two k-schemes that are quasi-projective over some k-algebras A, B, and G be a group acting on $X_{k_s} := X \times_k \mathrm{Spec}\, k_s, Y_{k_s} := Y \times_k \mathrm{Spec}\, k_s$ by k_s-isomorphisms, and $f : X \to Y$ be a map such that $f \times_k \mathrm{id}_{k_s}$ is G-equivariant. Let $\rho : \mathrm{Gal}(k_s/k) \to G$ be a continuous map with the cocycle property of Proposition A.1.11 (when post-composed with the actions of G on X_{k_s} or Y_{k_s}). There is a unique map $f_\rho : X_\rho \to Y_\rho$ of k-schemes such that the following diagram commutes:*

$$\begin{array}{ccc} X_\rho \times_k \mathrm{Spec}\, k_s & \xrightarrow{j_X} & X \times_k \mathrm{Spec}\, k_s \\ \downarrow{\scriptstyle f_\rho \times_k \mathrm{id}_{k_s}} & & \downarrow{\scriptstyle f \times_k \mathrm{id}_{k_s}} \\ Y_\rho \times_k \mathrm{Spec}\, k_s & \xrightarrow{j_Y} & Y \times_k \mathrm{Spec}\, k_s \end{array}$$

Moreover, f_ρ acquires all the properties of f that are étale-local on the base. The construction $X \longmapsto (X_\rho, j_X), f \longmapsto f_\rho$ is then functorial in the obvious meaning, and it preserves arbitrary limits.

Proof. – Suppose $f : X \to Y$ is a morphism of quasi-projective k-schemes, such that f is equivariant for the action of a finite group G, and that we are given a continuous $\rho : \mathrm{Gal}(k_s/k) \to G$.

Let $f^0_\rho : X_\rho \times_k \operatorname{Spec} k_s \to Y_\rho \times_k \operatorname{Spec} k_s$ be given by $j_Y^{-1} \circ (f \times_k \mathrm{id}_{k_s}) \circ j_X$. Then it is formal to see that $f^0_\rho \in \mathrm{Mor}_{k_s}((X_\rho)_{k_s}, (Y_\rho)_{k_s})^{\mathrm{Gal}(k_s/k)}$. Since X_ρ, Y_ρ are quasi-projective over k, they are quasi-compact and we can apply Proposition A.1.10 to see that f^0_ρ is the base change of a k-homomorphism $f_\rho : X_\rho \to Y_\rho$.

Note that the diagram uniquely prescribes the image of f_ρ in $\mathrm{Mor}_{k_s}(X_{k_s}, Y_{k_s})$, which uniquely defines f_ρ by Proposition A.1.2.

The proof of fonctoriality is identical.

Let $\mathscr{D}$ be a diagram of quasi-projective k-schemes (all the maps being equivariant for some action of G) and X be its limit in the category $\mathbf{Sch}_k$. Suppose that X is quasi-projective. Then, for any k_s-scheme T, the following diagram commutes, where the maps are isomorphisms:

$$\begin{array}{ccccccc}
\mathrm{Mor}_k(T, X) & \longrightarrow & \mathrm{Mor}_{k_s}(T, X_{k_s}) & \xrightarrow{j_X} & \mathrm{Mor}_{k_s}(T, (X_\rho)_{k_s}) & \longrightarrow & \mathrm{Mor}_k(T, X_\rho) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\varprojlim_{D\in\mathscr{D}} \mathrm{Mor}_k(T, D) & \longrightarrow & \varprojlim_{D\in\mathscr{D}} \mathrm{Mor}_{k_s}(T, D_{k_s}) & \xrightarrow{(j_D)_D} & \varprojlim_{D\in\mathscr{D}} \mathrm{Mor}_k(T, (D_\rho)_{k_s}) & \longrightarrow & \varprojlim_{D\in\mathscr{D}} \mathrm{Mor}_k(T, D_\rho)
\end{array}$$

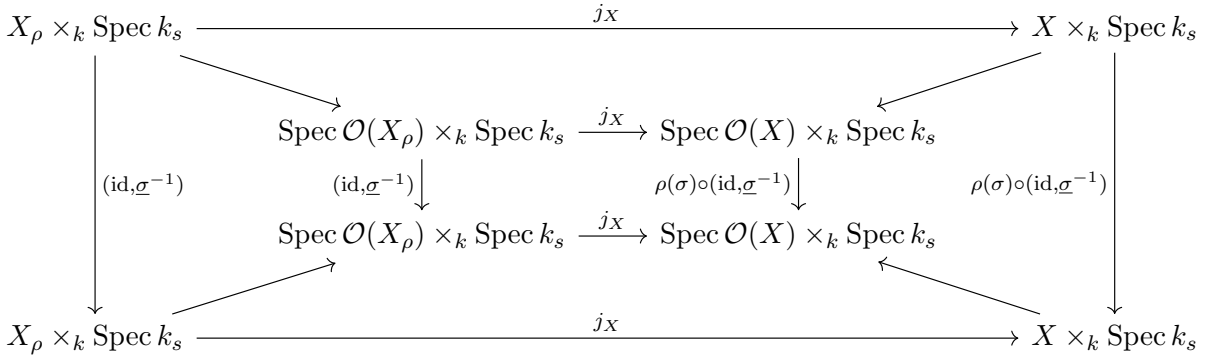
Now, $F_{\mathscr{D}_\rho} : T \in \mathbf{Sch}_k \longmapsto \varprojlim_{D\in\mathscr{D}} \mathrm{Mor}_k(T, D_\rho)$, $F_{X_\rho} : T \in \mathbf{Sch}_k \longmapsto \mathrm{Mor}_k(T, X_\rho)$ are fpqc sheaves by Theorem A.1.1. By fonctoriality, we have a map $\lambda : F_{X_\rho} \to F_{\mathscr{D}_\rho}$; the diagram shows that $\lambda(T) : F_{X_\rho}(T) \to F_{\mathscr{D}_\rho}(T)$ is an isomorphism for every k_s-scheme T. Since every k-scheme has an fpqc cover by k_s-schemes, it follows that λ is an isomorphism. □

Corollary A.1.14 *Let k be a field with separable closure k_s, and X be a quasi-projective k-scheme. Let $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{Aut}(X \times_k \operatorname{Spec} k_s)$ satisfying the cocycle condition. Then the induced action of ρ on $\mathrm{Aut}(\operatorname{Spec} \mathcal{O}(X) \times_k \operatorname{Spec} k_s)$ satisfies the cocycle condition of Proposition A.1.11. Moreover, the twist of $\operatorname{Spec} \mathcal{O}(X)$ by ρ naturally identifies with $\operatorname{Spec} \mathcal{O}(X_\rho)$.*

Proof. – For each $\sigma \in \mathrm{Gal}(k_s/k)$, the commutative diagram

$$\begin{array}{ccc}
X_\rho \times_k \operatorname{Spec} k_s & \xrightarrow{j_X} & X \times_k \operatorname{Spec} k_s \\
\downarrow{\scriptstyle (\mathrm{id}, \underline{\sigma}^{-1})} & & \downarrow{\scriptstyle \rho(\sigma)\circ(\mathrm{id}, \underline{\sigma}^{-1})} \\
X_\rho \times_k \operatorname{Spec} k_s & \xrightarrow{j_X} & X \times_k \operatorname{Spec} k_s
\end{array}$$

induces, by taking the spectra of the rings of global functions (since k_s is flat over k), a commutative diagram



where the unlabeled arrow are canonical morphisms $Y \to \operatorname{Spec} \mathcal{O}(Y)$, and this is enough to conclude. □

A.2 Compactification of finite schemes over the affine line

In this section, our base rings will be assumed to be regular, excellent, and Noetherian (unless explicitly specified otherwise – the rings of sections of *schemes*, on the other hand, are not required to satisfy these conditions). The goal is to state some properties needed to construct compactified moduli schemes and work with morphisms between them.

Definition A.2.1 We say that a R-scheme of finite type X is *normal near infinity* if there is a closed subscheme $Z \subset X$ finite over R such that $X \backslash Z$ is a normal scheme and $X \backslash Z \to \operatorname{Spec} R$ is surjective.

Lemma A.2.2 *Suppose we are given a finite R-map $j : X \to \mathbb{A}^1_R$. Then X is normal near infinity if, and only if, there is a monic $f \in R[t]$ such that X is normal on the locus where $f(j)$ is invertible.*

Proof. – The assumptions imply that X is a R-scheme of finite type. For ($\Leftarrow$), it is clear that $Z = j^{-1}(V(f))$ fits the definition. Let us assume that X is normal near infinity and let Z be the closed subscheme given by the definition. Then the scheme-theoretic image H of Z in $\mathbb{A}^1_R$ is affine. Moreover $\mathcal{O}(H)$ injects into $\mathcal{O}(Z)$, so, since R is Noetherian, H is finite over R. Thus, if x denotes the coordinate function on $\mathbb{A}^1_R$, there is a monic $f \in R[t]$ such that $f(x)_{|H} = 0$. Then X is normal on $j^{-1}(D(f))$. □

Corollary A.2.3 *Suppose we are given a finite R-map $j : X \to \mathbb{A}^1_R$ and $f_1, \dots, f_r \in R$ that generate the unit ideal. Then X is normal near infinity if and only if every $X_{R_{f_i}}$ is normal near infinity (as a R_{f_i}-scheme of finite type).*

Proof. – The forward implication is clear, so let us discuss the reverse implication. For every i, we have an ideal I_i of $R[x]_{f_i}$ containing a monic polynomial and such that every point of $X_{R_{f_i}} \backslash j^{-1}(V(I_i))$ is normal. Let $I \subset R[x]$ be the sum of the inverse images under $R \to R_{f_i}$ of the I_i, so we only need to prove that I contains a monic polynomial. But it is clear that the subset $J \subset R$ which is the reunion of $\{0\}$ and the leading coefficients of polynomials in I is an ideal. Since each I_i contains a monic polynomial, each J_{f_i} is R_{f_i}, hence $J = R$ and I contains a monic polynomial. □

Proposition A.2.4 *Let $j : X \to \mathbb{A}^1_R$ be a finite map, where X is normal near infinity. There is a canonical Cartesian diagram*

$$\begin{array}{ccc} X & \xrightarrow{j} & \mathbb{A}^1_R \\ \downarrow & & \downarrow \\ \overline{X} & \xrightarrow{\overline{j}} & \mathbb{P}^1_R \end{array}$$

such that $\overline{j}$ is finite and $\overline{X}$ is normal in a neighborhood of $\overline{X} \backslash X$. Moreover, $X \to \overline{X}$ is an open immersion with dense image. For any separated scheme Y and any open subscheme $U \subset \overline{X}$, $Y(U) \to Y(X \cap U)$ is injective. By taking $Y = \mathbb{A}^1$, we see that $\mathcal{O}(U) \to \mathcal{O}(U \cap X)$ is injective.

Moreover, let R' be any (regular, excellent, Noetherian) R-algebra and $j' : X' \to \mathbb{A}^1_{R'}$ be a finite map, with X' normal near infinity. Assume that there is a closed subscheme[4] Z' of $\mathbb{A}^1_R$, finite over R, such that X' is normal at every point not above Z', and that we have a commutative

[4]Note, in the following, the R instead of R'.

diagram

$$\begin{array}{ccc} X' & \xrightarrow{f} & X \\ \downarrow{\scriptstyle j'} & & \downarrow{\scriptstyle j} \\ \mathbb{A}^1_{R'} & \longrightarrow & \mathbb{A}^1_R \end{array}$$

Then f extends uniquely to a map $\overline{f} : \overline{X'} \to \overline{X}$ such that the following diagram commutes:

$$\begin{array}{ccc} \overline{X'} & \xrightarrow{\overline{f}} & \overline{X} \\ \downarrow{\scriptstyle \overline{j'}} & & \downarrow{\scriptstyle \overline{j}} \\ \mathbb{P}^1_{R'} & \longrightarrow & \mathbb{P}^1_R \end{array}$$

Proof. – First, we construct $\overline{X}$. Fix a closed subscheme Z of $\mathbb{A}^1_R$ finite over R such that $X \backslash j^{-1}(Z)$ is normal. Let Y be the relative normalization of $X \backslash j^{-1}(Z) \xrightarrow{j} \mathbb{A}^1_R \subset \mathbb{P}^1_R$. Because R is excellent, $\mathbb{P}^1_R$ is Nagata by [4, Lemma 07QV, Lemma 035A] so Y is finite over $\mathbb{P}^1_R$ by [4, Lemma 03GR] ($X \backslash Z$ is normal, hence reduced). By [4, Lemma 035L], Y is normal.

By [4, Lemma 035K], $Y \times_{\mathbb{P}^1_R} (\mathbb{A}^1_R \backslash Z)$ is exactly the normalization of $X \backslash j^{-1}(Z) \xrightarrow{j} \mathbb{A}^1_R \backslash Z$. Since this map is finite, by [4, Lemma 03GP], $Y \times_{\mathbb{P}^1_R} (\mathbb{A}^1_R \backslash Z) \to \mathbb{A}^1_R \backslash Z$ is exactly isomorphic to $X \backslash j^{-1}(Z) \to \mathbb{A}^1_R \backslash Z$. Thus, we can glue $Y \backslash j^{-1}(Z) \to \mathbb{P}^1_R \backslash Z$ and $X \to \mathbb{A}^1_R$ together, and this defines $\overline{X}$.

Note that the construction of $\overline{X}$ does not depend on the choice of Z.

$X \to \overline{X}$ is an open immersion by construction, and it has dense image by [4, Lemma 0AXP]. Moreover, $\overline{X}$ is normal, hence reduced, on a neighborhood of any point of $\overline{X} \backslash X$. Let U be any open subscheme of $\overline{X}$. Since X is dense, $X \cap U$ is a nonempty open subscheme of U; furthermore, if $V \subset U$ is any open subscheme, $V \cap X$ is nonempty and contained in $(X \cap U) \cap V$. Thus $X \cap U \to U$ is an open immersion with dense image and such that all points of $U \backslash X$ are normal hence reduced.

Let Y be a separated scheme and $u, v : U \to Y$ be two morphisms that agree on $U \cap X$. By [4, Lemma 01KM], there is a closed subscheme $U_1 \subset U$ containing $U \cap X$ such that u, v agree on U_1. Thus the surjective closed immersion $U_1 \to X$ is an isomorphism above $U \cap X$. Since U is reduced at every point outside X, $U_1 = U$ thus $u = v$.

To construct $\overline{f}$, let Y' denote the relative normalization of $X' \backslash (j')^{-1}((Z' \cup Z)_{R'}) \to \mathbb{P}^1_{R'}$; since we have a commutative diagram

$$\begin{array}{ccc} X' \backslash (j')^{-1}((Z' \cup Z)_{R'}) & \xrightarrow{j'} & \mathbb{P}^1_{R'} \\ \downarrow{\scriptstyle f} & & \downarrow \\ X \backslash j^{-1}(Z' \cup Z) & \xrightarrow{j} & \mathbb{P}^1_R \end{array}$$

we have a natural map $\overline{f} : Y' \backslash Y$ above $j^{-1}(Z' \cup Z)$. We can then glue it with $f : X' \to X$. □

Corollary A.2.5 *Let $j : X \to \mathbb{A}^1_R$ be a finite map with X normal near infinity. Let Y be a finite R-scheme, and let $g : X \to Y$ a R-morphism. Then g extends uniquely as to map $\overline{g} : \overline{X} \to Y$.*

Proof. – The uniqueness follows from Proposition A.2.4. Fix a closed subscheme $Z \subset \mathbb{A}^1_R$ finite over R such that $X \backslash j^{-1}(Z)$ is normal. Suppose that, for any normal integral affine open subscheme $U \subset \overline{X} \backslash j^{-1}(Z)$, $X \cap U \to Y$ extends to $U \to Y$. Then, if U, V are normal integral affine open subschemes of $\overline{X} \backslash j^{-1}(Z)$, these extensions coincide on $U \cap V$, because they coincide on $U \cap V \cap X$. All these extensions glue together, by construction, with $X \to Y$, so they all glue together and construct the extension $\overline{X} \to Y$.

So let $U \subset \overline{X} \backslash j^{-1}(Z)$ be a normal integral affine open subscheme. By definition, g defines a map $g^\sharp : \mathcal{O}(Y) \to \mathcal{O}(X) \to \mathcal{O}(X \cap U)$. Because U is normal integral affine and $X \cap U$ is an open subscheme of U, $\mathcal{O}(U) \to \mathcal{O}(X \cap U)$ is injective between normal domains and is an isomorphism on function fields. The image of $g^\sharp$ is thus made with elements in the fraction ring of $\mathcal{O}(U)$ and which are integral over R, hence over $\mathcal{O}(U)$. So the image of $g^\sharp$ lands in the subring $\mathcal{O}(U)$, that is, g extends to a map $U \to Y$ and we are done. □

We now wish to show that the compactification previously constructed is canonical, and that a much wider class of morphisms can be extended.

Lemma A.2.6 *Let $f : Z \to X$ be a finite morphism of finite type R-schemes. Suppose that $Y \subset X$ is a dense open subscheme such that $f^{-1}(Y) \to Y$ is an isomorphism, $f^{-1}(Y)$ is dense in Z, every $\mathcal{O}_{Z,z}$ for $z \notin f^{-1}(Y)$ is reduced, and every $\mathcal{O}_{X,x}$ for $x \notin Y$ is normal. Then f is an isomorphism.*

Proof. – First, we easily reduce to the case where X and Z are affine.

Let $x \in X \backslash Y$, and let $z' \in Z$ be a point whose image in X specializes to x. Then $f(\overline{\{z'\}})$ is closed in X and contains a point specializing to x; hence there exists a specialization $z \in Z$ of z' whose image in Z is x. In particular, $\mathcal{O}_{Z,z'}$ is a localization of $\mathcal{O}_{Z,z}$, hence is reduced.

Thus, it is enough to check the claim after changing base by every $\mathcal{O}_{X,x}$ where $x \notin Y$. So we can assume that $Z = \operatorname{Spec} B$, $X = \operatorname{Spec} A$ with A a local normal domain, B is reduced, and Y is the open subscheme given by the complement of the vanishing locus of some nonzero ideal I. Furthermore, we know that for every non-zero $f \in I$, $A[f^{-1}] \to B[f^{-1}]$ is an isomorphism. In particular, $A \to B[f^{-1}]$ is injective, so that $A \to B$ is injective. Since $f^{-1}(Y)$ is dense in Z, we know that for every non-zero $g \in B$, gI is nonzero in B.

Let now $x \in B$ be nonzero: then the ideal xI is nonzero, so there is some $f \in I$ such that $fI \neq 0$. Then, if $r \geq 1$, $f^r x$ is a divisor of $(fx)^r$ which is nonzero (since B is reduced): thus the image of x in B_f is nonzero. Let now $x, y \in B$ be nonzero, then $\{t \in I \mid tx = 0\}, \{t \in I \mid ty = 0\}$ are two proper additive subgroups of I, hence their reunion does not contain I, and we can find $f \in I$ such that x, y have nonzero images in B_f. Since $B_f \simeq A_f$ is a domain, xy has nonzero image in B_f, so $xy \neq 0$. Thus B is a domain.

Therefore, $A \to B$ is finite injective and is an isomorphism on fraction fields. Since A is normal, $A \to B$ is an isomorphism. □

Proposition A.2.7 *Let $\alpha, \beta : X \to \mathbb{A}^1_R$ be two finite maps, where X is a R-scheme of finite type normal near infinity. By Proposition A.2.4, α, β compactify in two finite maps $\overline{\alpha} : X_\alpha \to \mathbb{P}^1_R$, $\overline{\beta} : X_\beta \to \mathbb{P}^1_R$. There is a unique R-isomorphism $\iota : X_\alpha \to X_\beta$ such that the following diagram commutes:*

$$\begin{array}{ccc} X & \xrightarrow{\mathrm{id}} & X \\ \downarrow{\scriptstyle \overline{\alpha}} & & \downarrow{\scriptstyle \overline{\beta}} \\ X_\alpha & \xrightarrow{\iota} & X_\beta \end{array}$$

Proof. – First, note that it is enough to construct a R-map $\iota_{\alpha,\beta}$ making the diagram commute: because then, we can similarly construct $\iota_{\beta,\alpha}$, so $\iota_{\beta,\alpha} \circ \iota_{\alpha,\beta}$ is an endomorphism of X_α which induces the identity on X; by Proposition A.2.4, it is the identity. Similarly, $\iota_{\alpha,\beta} \circ \iota_{\beta,\alpha}$ is the identity endomorphism of X_β so that $\iota_{\alpha,\beta}$ is an isomorphism.

Next, we consider the diagonal inclusion $X \to X \times_R X \to X_\alpha \times_R X_\beta$. Let Z be its scheme-theoretic image. Z is a closed subscheme of $X_\alpha \times_R X_\beta$, hence the first projection $p_1 : Z \to X_\alpha$ is proper.

If p_1 is an isomorphism, we are done, since we can consider the composition $p_2 \circ p_1^{-1}$, where p_2 is the second projection $Z \to X_\alpha \times_R X_\beta \to X_\beta$.

We will show that p_1 is finite and that the dense open subscheme X of X_α satisfies all the conditions of Lemma A.2.6, whence the conclusion.

First, we know that X_α is normal at every point not in X. Moreover, by [4, Lemma 01R8], $Z \cap X \times_R X_\beta$ is the scheme-theoretic image of the diagonal inclusion $X \to X \times_R X_\beta$, which is a closed immersion (as a section of the proper morphism $X \times_R X_\beta \to X$). Thus $X \to Z \cap (X \times_R X_\beta)$ is an isomorphism of inverse $p_1^{-1}(X) \to X$. Note that the image of X in Z, which is $p_1^{-1}(X)$, is dense in Z by [4, Lemma 01RB].

Let $W \subset X$ be a closed subscheme, finite over R, such that every point of $X \backslash W$ is normal (hence reduced). Then $p_1^{-1}(X_\alpha \backslash W)$ is the scheme-theoretic image of $X \backslash W \to (X_\alpha \backslash W) \times_R X_\beta$. Since $X \backslash W$ is reduced, $Z \backslash p_1^{-1}(W)$ is reduced by [4, Lemma 056B]. In particular, Z is reduced at every point not in $p_1^{-1}(X)$.

All that remains to do now is prove that p_1 is finite. To do that, it is enough to show that it has finite fibres by [4, Lemma 02LS], so we only need to prove that for every $x \in X_\alpha \backslash X$, $p_1^{-1}(\{x\})$ is finite. To do this, we exhibit a closed subscheme $T \subset X_\alpha \times X_\beta$ such that the diagonal inclusion factors through T, and such that the fibre of $T \to X_\alpha \times_R X_\beta \to X_\alpha$ at every $x \in X_\alpha$ is finite (since then $p_1 : Z \to X_\alpha$ is the composition of the closed immersion $Z \to T$ and of the map $T \to X_\alpha$).

The morphism α is finite, so X is affine. Let s denote the coordinate on $\mathbb{A}^1_R$. Let $a, b \in \mathcal{O}(X)$ denote the images of s under α, β. Since β is finite, there is an integer $n \geq 1$ and polynomials $Q_0, \dots, Q_{n-1} \in R[t]$ such that $a^n + \sum_{i=0}^{n-1} Q_i(b) a^i = 0$. Let $d \geq 0$ be the maximum of the degrees of the Q_i, and define the homogeneous polynomials $\widetilde{Q_i}(v_0, v_1) = v_1^d Q_i(v_0/v_1) \in R[v_0, v_1]$ of degree d. Let $P \in R[u_0, u_1, v_0, v_1]$ be the bi-homogeneous polynomial of bi-degee (n, d) given by $P = u_0^n v_1^d + \sum_{i=0}^{n-1} \widetilde{Q_i}(v_0, v_1) u_0^i u_1^{n-i}$. Then the image of X in $X_\alpha \times X_\beta \overset{(\overline{\alpha}, \overline{\beta})}{\to} \mathbb{P}^1_R \times_R \mathbb{P}^1_R$ is contained in $(\overline{\alpha}, \overline{\beta})^{-1}(V(P))$.

To conclude, since β is finite, it is enough to check that $V(P) \to \mathbb{P}^1_R \times_R \mathbb{P}^1_R \overset{p_1}{\to} \mathbb{P}^1_R$ has finite fibres above points $x \in \mathbb{P}^1_R \backslash \mathbb{A}^1_R$. This is equivalent to asking that $P(1, 0, v_0, v_1) \in k[v_0, v_1]$ has finitely many zeroes in $\mathbb{P}^1_k$, for a R-algebra k which is a field, which is clear. □

Proposition A.2.8 *Let X, Y be two R-schemes normal near infinity and admitting finite maps $\alpha : X \to \mathbb{A}^1_R, \beta : Y \to \mathbb{A}^1_R$. Let $\overline{\alpha} : X_\alpha \to \mathbb{P}^1_R$, $\overline{\beta} : Y_\beta \to \mathbb{P}^1_R$ be the maps given by Proposition A.2.4, where X (resp. Y) is an open subscheme of X_α (resp. Y_β). Let $f : X \to Y$ be any finite map of R-schemes. Then there is a unique map $\overline{f} : X_\alpha \to Y_\beta$ making the following diagram commute:*

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \downarrow & & \downarrow \\ X_\alpha & \xrightarrow{\overline{f}} & Y_\beta \end{array}$$

Moreover, $\overline{f}$ is finite, and maps any $x \in X_\alpha \backslash X$ into $Y_\beta \backslash Y$.

Proof. – Consider the finite map $\alpha' : X \to Y \overset{\beta}{\to} \mathbb{A}^1_R$ of R-schemes and let $X_{\alpha'}$ be the associated compactification by Proposition A.2.4. By Proposition A.2.7, we have an isomorphism $\iota : X_\alpha \to X_{\alpha'}$ preserving X, and by Proposition A.2.4 we have a natural extension $\overline{f_{\alpha'}} : X_{\alpha'} \to Y_\beta$. It is a map of finite $\mathbb{P}^1_R$-schemes, so is finite. Thus $\overline{f} = \overline{f_{\alpha'}} \circ \iota$ satisfies all the requested conditions. The uniqueness follows from Proposition A.2.4 since Y_β is separated. □

Proposition A.2.9 *Let $\mathbf{ACrv}_R$ be the category whose objects are R-schemes of finite type, normal near infinity and admitting a finite map to $\mathbb{A}^1_R$, and whose morphisms are finite maps of R-schemes. Let $\mathbf{PCrv}_R$ be the category of proper R-schemes that are normal near infinity, its morphisms being finite R-maps. There is a* normal compactification functor $\mathbf{ACrv}_R \to \mathbf{PCrv}_R$, *denoted by $X \longmapsto \overline{X}$, $f \longmapsto \overline{f}$, satisfying the following properties:*

- *Every object X of $\mathbf{ACrv}_R$ has a natural open immersion of R-schemes $X \longmapsto \overline{X}$ with dense image,*
- *For every object X of $\mathbf{ACrv}_R$, every separated scheme Y and every open subset $U \subset \overline{X}$, $Y(\overline{X}) \to Y(X)$ is injective,*

- *For any morphism $f : X \to Y$ in $\mathbf{ACrv}_R$, $\overline{f}$ sends any point in $\overline{X}\backslash X$ into $\overline{Y}\backslash Y$,*
- *$\overline{X}$ is normal at every point $x \notin X$,*
- *$\overline{\mathbb{A}^1_R} = \mathbb{P}^1_R$,*

Lemma A.2.10 *Let $f : X \to Y$ be a morphism in $\mathbf{ACrv}_R$. Then $\overline{f} : \overline{X} \to \overline{Y}$ is the relative normalization of $X \to Y \subset \overline{Y}$.*

Proof. – Let $f' : \overline{X}' \to \overline{Y}$ be the relative normalization of $X \to Y \subset \overline{Y}$. Because X, Y are objects of $\mathbf{ACrv}_R$, $f : X \to Y$ is finite and R is Noetherian, there is a closed subscheme $Z \subset Y$, finite over R, such that $X\backslash f^{-1}(Z), Y\backslash Z$ are normal schemes. Note by [4, Lemma 035K, Lemma 035L], $\overline{X}'\backslash(f')^{-1}(Z)$ is normal and $X \to \overline{X'} \times_{\overline{Y}} Y$ is an isomorphism. In particular, by [4, Lemma 03GR], f' is finite above $\overline{Y}\backslash Z$ and is finite above Y, hence is finite.

Since $\overline{X} \to \overline{Y}$ is finite, by the universal property of relative normalization, there is a unique $\overline{Y}$-morphism $g : \overline{X}' \to \overline{X}$, and this morphism is the identity above X. This morphism is finite (since $\overline{X}', \overline{X}$ are finite $\overline{Y}$-schemes), the points in $\overline{X}\backslash X$ (resp. their inverse images under g) are normal points of $\overline{X}$ (resp. $\overline{X}'$). Finally, X is a dense open subscheme of $\overline{X}$ by construction and of $\overline{X}'$ by [4, Lemma 0AXP]. We conclude using Lemma A.2.6. □

Let us conclude this section with a convenient notion of smoothness at infinity.

Definition A.2.11 Let R be a regular excellent Noetherian ring. An object Y of $\mathbf{ACrv}_R$ is *smooth at infinity* if there exists a closed subscheme $Z \subset Y$, finite over $\operatorname{Spec} R$, such that $\overline{Y}\backslash Z \to \operatorname{Spec} R$ is smooth of relative dimension one, and the scheme $(\overline{Y}\backslash Y)^{red}$ is finite étale over $\operatorname{Spec} R$.

Proposition A.2.12 *Let $R \to S$ be a morphism of regular excellent Noetherian rings, and Y be an object of $\mathbf{ACrv}_R$ which is smooth at infinity. Then Y_S is an object of $\mathbf{ACrv}_S$ which is smooth at infinity, and there is a canonical morphism $\overline{Y_S} \to \overline{Y} \times_R \operatorname{Spec} S$. This morphism is an isomorphism. Moreover, this isomorphism realizes an isomorphism $(\overline{Y_S}\backslash Y_S)^{red} \to (\overline{Y}\backslash Y)^{red} \times_R \operatorname{Spec} S$. Furthermore, $(\overline{Y}\backslash Y)^{red}$ is a relative effective Cartier divisor on $\overline{Y} \to \operatorname{Spec} R$, in the sense of [4, Definition 062T].*

Proof. – By definition, there is a closed subscheme $Z \subset Y$ such that $Y \to \operatorname{Spec} R$ is smooth outside Z, and a finite map $f : Y \to \mathbb{A}^1_R$. Hence $Y_S \to S$ is smooth outside Z_S, so that Y_S is normal outside Z_S, which is a closed subscheme of Y_S finite over S. Moreover $f_S : Y_S \to \mathbb{A}^1_S$ is finite. Thus Y_S is an object in $\mathbf{ACrv}_S$. By Proposition A.2.4, there is a map $c : \overline{Y_S} \to \overline{Y} \times_R \operatorname{Spec} S$, which is an isomorphism above the dense open subset $Y \times_R \operatorname{Spec} S$. Moreover, the inverse image of $Y \times_R \operatorname{Spec} S$ is dense, and its complement is made of normal points of $\overline{Y_S}$ (by construction of the compactification). Since $\overline{Y} \times_R S \to \operatorname{Spec} S$ is smooth at every point not in Y_S, every such point is normal. Thus c is an isomorphism by Lemma A.2.6.

In particular, c induces a surjective closed immersion of schemes $(\overline{Y_S}\backslash Y_S)^{red} \to (\overline{Y}\backslash Y)^{red} \times_R S$. In order to show that it is an isomorphism, it is enough to show that the domain and the target are reduced. For the domain, it is a tautology; for the target, it follows from the fact that $(\overline{Y}\backslash Y)^{red}$ is étale over R.

For the assertion about relative effective Cartier divisors, since $(\overline{Y}\backslash Y)^{red} \to \operatorname{Spec} R$ is finite étale, it is enough by [4, Lemma 062Y] to prove the statement after everything is base changed to a field. Using what we showed above, it is equivalent to proving the assertion assuming that R is a field.

For every $y \in \overline{Y}\backslash Y$, since $\overline{Y}\backslash Z$ is normal, we can find an open subset $y \in U_y$ of $\overline{Y}$ contained in $(Y \cup \{y\})\backslash Z$, and some $t_y \in \mathcal{O}_{\overline{Y}}(U_y)$ which is a uniformizer at y and a unit at every other point of U. Consider then the subsheaf $\mathcal{L}$ of the sheaf of meromorphic functions $\mathcal{K}_{\overline{Y}}$ on $\overline{Y}$ defined as follows: $\mathcal{L}_{|Y} = \mathcal{O}_Y$, $\mathcal{L}_{|U_y} = t_y^{-1}\mathcal{O}_{U_y}$. Then $\mathcal{L}$ is an effective Cartier divisor, and the associated closed subscheme is exactly $(\overline{Y}\backslash Y)^{red}$. □

Proposition A.2.13 *Let R be a regular excellent Noetherian ring and Y be an object in $\mathbf{ACrv}_R$, smooth at infinity. Let $Z \subset Y$ be a closed subscheme, finite over $\operatorname{Spec} R$, such that $Y \setminus \operatorname{Spec} R$ is smooth outside Z. Assume that there is a finite morphism $f : X \to Y$ of R-schemes which is étale above $Y \setminus Z$. Then X is an object of $\mathbf{ACrv}_R$, f is a morphism of $\mathbf{ACrv}_R$. If furthermore f is tamely ramified in codimension one over $\overline{Y}$* [5]*, then $\overline{X} \setminus j^{-1}(Z) \to \operatorname{Spec} R$ is smooth of relative dimension one, and X is smooth at infinity. Moreover, $\overline{X} \setminus f^{-1}(Z) \to \overline{Y} \setminus Z$ is finite locally free.*

Proof. – For the first part, since $f^{-1}(Z)$ is finite over $\operatorname{Spec} R$, and $X \setminus f^{-1}(Z) \to Y \setminus Z$ is finite étale, $X \setminus f^{-1}(Z)$ is normal, so that X (resp. f) is an object (resp. a morphism) of $\mathbf{ACrv}_R$.

By Lemma A.2.10, $\overline{f} : \overline{X} \to \overline{Y}$ is the relative compactification of $X \xrightarrow{f} Y \to \overline{Y}$. We now apply Abhyankar's Lemma [4, Lemma 0EYG, 0EYH]: étale locally on $\overline{Y} \setminus Z$, the map $\overline{f}_Z : \overline{X} \setminus f^{-1}(Z) \to \overline{Y} \setminus Z$ is given by finitely many copies of $A \to A[x]/(x^e - f)$, where $e \in A^\times$, and f cuts exactly the inverse image in A of $(\overline{Y} \setminus Y)^{red}$: in particular, A is smooth of relative dimension one over $\operatorname{Spec} R$ and A/fA is étale over $\operatorname{Spec} R$[6].

It implies that $\overline{f}_Z$ is finite locally free, since these properties are étale local on the base. To establish that $\overline{X} \setminus f^{-1}(Z)$ is smooth of relative dimension one over $\operatorname{Spec} R$, by [4, Lemma 036U], it is enough to show that under these assumptions, $R \to A' := A[x]/(x^e - f)$ is smooth of relative dimension one. Since A' is free over A, A' is flat over R, so it is enough to show that for any algebraically closed field k endowed with a R-algebra structure, $A'_k := A' \otimes_R k$ is normal.

Let $A_k = A \otimes_R k$, it is smooth over k of relative dimension one, hence is a Dedekind ring, A_k/fA_k is étale over k, and $A'_k = A_k[x]/(x^e - f)$. Since $A'_k[1/f]$ is étale over $A_k[1/f]$, it is enough to prove that, if $\mathfrak{m}$ is maximal ideal of A_k containing f, then $(A'_k)_\mathfrak{m} = (A_k)_\mathfrak{m}[x]/(x^e - f)$ is a normal ring. In this situation, $(A_k)_\mathfrak{m}$ is a discrete valuation ring, and, since A_k/fA_k is a direct product of copies of k, f is a uniformizer. It is then a standard exercice to check that $A'_k)_\mathfrak{m}$ is normal.

This local description implies that étale-locally on $\overline{Y} \setminus Z$, $(\overline{X} \setminus X)^{red}$ is given by copies of $A[x]/\sqrt{(x^e - f, fA)} = A[x]/(x) \simeq A$. Thus, $(\overline{X} \setminus X)^{red}$ is smooth over $\operatorname{Spec} R$ by [4, Lemma 036U], and it is also finite over $\operatorname{Spec} R$, hence it is finite étale. □

A.3 Refresher on group schemes and Abelian varieties

A.3.1 Generalities

Definition A.3.1 A group scheme over a field k is the datum of a k-scheme A endowed with three morphisms $m : A \times_k A \to A$, $i : A \to A$, $e \in A(k)$ of k-schemes such that, for any k-scheme S, $A(S)$ is a group for the composition law $A(S) \times A(S) \xrightarrow{m} A(S)$, where the unit element is $S \to \operatorname{Spec} k \xrightarrow{e} A$, and the inverse map is $A(S) \xrightarrow{i} A(S)$. The group scheme (A, m, i, e) is an Abelian variety if A is a smooth proper connected k-scheme. In general, the datum of (m, i, e) will be implicit in the notation, and we will denote $m : A(S) \times A(S) \to A(S)$ by $+$ (or $\cdot$), $i : A(S) \to A(S)$ by $t \longmapsto -t$ (or $t \longmapsto t^{-1}$), and e by 0_A (or 1_A, or e_A).

Proposition A.3.2 *Let A, B be Abelian varieties over a field k, and $f : A \to B$ a homomorphism of k-schemes such that $f(0_A) = 0_B$. Then f is a morphism of Abelian varieties, that is, for any k-scheme S, the function $f : A(S) \to B(S)$ is a group homomorphism.*

Proof. – By [118, Corollary 2.2], f is the composition of a homomorphism of Abelian varieties with a translation. Since $f(0_A) = 0_B$, the translation is trivial, so f is a homomorphism of Abelian varieties. □

Proposition A.3.3 *In Definition A.3.1, the group law on $A(S)$ is commutative.*

[5] In the sense of [4, Section 0BSE].

[6] This is not stated as such in the reference, but follows directly from the proof.

Proof. – This is [118, Corollary 2.4]. Proposition A.3.2 implies that $i : A \to A$ is a homomorphism of Abelian varieties, so that, for any k-scheme S, $A(S)$ is a group whose inversion map is a group homomorphism: it is thus an Abelian group, whence the conclusion. □

Definition A.3.4 Given a morphism $f : A \to B$ of Abelian varieties over a field k, the kernel of f is the scheme $\ker f = f^{-1}(0_B) = \{0_B\} \times_B A$.

Proposition A.3.5 *Let A, B be Abelian varieties over a field k and $f : A \to B$ be a morphism of Abelian varieties. Then f is flat if and only if f is surjective. In this case, one has $\dim f^{-1}(0_A) = \dim A - \dim B$.*

Proof. – Because A is reduced, the scheme-theoretic image of f is a reduced closed subscheme of B. Since f is surjective, the scheme-theoretic image of f is B. By [2, Lemma 2.3.3.2], f is flat. Conversely, if f is flat, then f is open; but f is proper because A is proper over k, so f is closed, whence f is surjective.

The k-schemes A, B are proper and irreducible. Hence, if f is flat surjective, then, by [106, Corollary 4.3.14], $f^{-1}(0_B)$ is pure of dimension $\dim A - \dim B$. Let C be the connected component of 0_A in the closed group subscheme $f^{-1}(0_B)$ of A: by [4, Proposition 0B7R], C is irreducible (as are A, B). Therefore $\dim C = \dim f^{-1}(0_B) = \dim A - \dim B$. □

Proposition A.3.6 *An Abelian variety A over a field k is projective.*

Proof. – This is [118, Theorem 7.1]. □

Definition A.3.7 An isogeny of Abelian varieties over a field k is a morphism $f : A \to B$ of Abelian varieties which is surjective with finite kernel. Its *degree* is the degree of the finite k-scheme $\ker f$.

Proposition A.3.8 *The following are equivalent, given a morphism $f : A \to B$ of Abelian varieties over k:*

- *f is an isogeny,*
- *$\ker f$ is finite and $\dim B = \dim A$,*
- *f is surjective and $\dim B$ and $\dim A$,*
- *f is finite flat surjective.*

Proof. – This is [118, Theorem 8.1]. □

Proposition A.3.9 *Let A be an Abelian variety of dimension g over k and $n \geq 1$ be an integer. The morphism of multiplication by n $[n]_A : A \to A$ is an isogeny of degree n^{2g}. It is étale if and only if n is invertible in k.*

Proof. – This is [118, Theorem 8.2]. □

A.3.2 Image and quotient of Abelian varieties

Lemma A.3.10 *Let G be a group scheme over a field k and $j : H \to G$ be an immersion of group schemes over k. Then j is a closed immersion. If G is an Abelian variety, the group scheme law on H is commutative.*

Proof. – Since $H(S) \to G(S)$ is an injective group homomorphism for any k-scheme S, so the group law on H is commutative for H if the group law of G is. The morphism j is a closed immersion by [4, Lemma 047T]. □

To define quotients of Abelian varieties, we need to specify the meaning of this term, or the category in which the quotient is taken. The usual definition uses the fppf topology. More precisely, every scheme is naturally a sheaf on the fppf site, and the quotient is taken in the (Abelian) category of fppf sheaves.

Definition A.3.11 We define the fppf topology as in [4, Definition 021M]: a collection of maps $\pi_i : T_i \to T$ is an fppf-covering if each π_i is flat, locally of finite presentation, and $\cup_i \pi_i(T_i) = T$. It is equivalent to the definition of [38, Exp. IV, §6.3].

Proposition A.3.12 *Let $f : A \to B$ be a morphism of Abelian varieties over a field k. There exists an Abelian variety C, a faithfully flat morphism $\pi : A \to C$ and a closed immersion $\iota : C \to B$ of Abelian varieties over k such that $f = \iota \circ \pi$.*

Proof. – By [38, Exp. V, Théorème 10.1.2], $C := A/\ker f$ is representable by a group scheme over k of finite type and we can write $f = \iota \circ \pi$, where $\pi : A \to C$ is faithfully flat of finite type and $\iota : C \to B$ is a monomorphism. The group scheme C is separated by [4, Lemma 047L]. It is is geometrically regular by descent [4, Lemma 07NG], so C is smooth over k by [15, §2.2, Proposition 15]. Moreover, C is proper connected since $\pi : A \to C$ is surjective. Hence C is an Abelian variety. Therefore, ι is a proper monomorphism hence a closed immersion by [4, Lemma 04XV]. □

Proposition A.3.13 *Let A be an Abelian variety over a field k and H be a closed subgroup scheme of A. Then there exists an Abelian variety B over k and a flat homomorphism of Abelian varieties $f : A \to B$ such that $\ker f = H$. Moreover, B represents the sheaf A/H in the fpqc topology.*

Proof. – By [2, Théorème 4.C], the quotient $B := A/H$ of fppf sheaves is representable by a group scheme over k. The group scheme B is separated by [4, Lemma 047L]. We can then apply [38, Exp. V, Théorème 10.1.2] to the natural surjective morphism $f : A \to B$ (with kernel H): there is a factorization $f = \iota \circ \pi$, where $\pi : A \to B' := A/H$ is faithfully flat of finite presentation, and $\iota : B' \to B$ is the natural monomorphism. Then ι is the identity, so that f is faithfully flat of finite presentation. As in the previous proof, B is geometrically regular and, by [38, Exp. V, Proposition 9.1], it is a k-scheme of finite type, so it is smooth. Since $f : A \to B$ is surjective, B is proper over k and connected, so it is an Abelian variety. □

A.3.3 Differentials on Abelian varieties

Proposition A.3.14 *Let G be a group scheme over a base k. Then the natural homomorphism $H^0(G, \Omega^1_{G/k}) \otimes_{\mathcal{O}_G(G)} \mathcal{O}_G \to \Omega^1_{G/k}$ is an isomorphism.*

Proof. – By [105, Proposition 1.1(b)], $\Omega^1_{G/k}$ is the pull-back of some k-vector space, which directly implies the statement. □

Corollary A.3.15 *Let A be an Abelian variety over a field k. The pairing*

$$\langle \cdot, \cdot \rangle_A : (\omega, t) \in H^0(A, \Omega^1_{A/k}) \times T_{0_A} G \longmapsto \omega(0_A)(t) \in k$$

is perfect. This pairing is natural in the following sense: if $f : A \to B$ is a morphism of Abelian varieties over k, then $\langle \cdot, f(-) \rangle_B = \langle f^* \cdot, - \rangle_A$.

Proof. – The k-scheme A is proper and geometrically integral, so $k \to \mathcal{O}_A(A)$ is an isomorphism. Hence, by Proposition A.3.14, the evaluation at zero map $H^0(G, \Omega^1_{G/k}) \to \left(\mathfrak{m}_{G,0}/\mathfrak{m}^2_{G,0}\right)$ is an isomorphism. We conclude using the definition of tangent space. That the pairing is natural is a direct verification. □

Corollary A.3.16 *Let $f : A \to B$ be a closed immersion (resp. a smooth morphism) of Abelian varieties over a field k. Then $f^* : H^0(B, \Omega^1_{B/k}) \to H^0(A, \Omega^1_{A/k})$ is surjective (resp. injective).*

Proof. – This is a consequence of Corollary A.3.15 and [105, Proposition 1.1 (a,c)]. □

Corollary A.3.17 *Let $f : A \to B$ be a morphism of Abelian varieties and assume that the connected component of unity C of $\ker f$ is an Abelian variety over k (equivalently, that it is*

smooth). Then the image of $f^* : H^0(B, \Omega^1_{B/k}) \to H^0(A, \Omega^1_{A/k})$ *is exactly the kernel of the restriction map* $H^0(A, \Omega^1_{A/k}) \to H^0(C, \Omega^1_{C/k})$.

Proof. – This is a consequence of Corollary A.3.15 and [105, Proposition 1.1 (a,d)]. □

Let us recall the following result.

Proposition A.3.18 *Every group scheme over a field of characteristic zero is smooth. Every surjective morphism* $f : A \to B$ *of group schemes of finite type over a field* k *of characteristic zero is smooth.*

Proof. – The first part of the claim is Cartier's theorem [4, Lemma 047N]. For the second claim, f is flat by [2, Lemma 2.3.3.2], and moreover $\ker f$ is a group scheme of finite type over k, so it is smooth. Therefore, the smooth locus of f contains 0_A. Let $U \subset A$ be an open subscheme such that $f_{|U}$ is smooth. Consider the following commutative diagram:

$$\begin{array}{ccccc} A \times_k U & \xrightarrow{(\mathrm{id},f)} & A \times_k B & \xrightarrow{(\mathrm{pr}_1,f)} & A \times_k B \\ \downarrow{\scriptstyle +_A} & & & & \downarrow{\scriptstyle f(\mathrm{pr}_1)+\mathrm{pr}_2} \\ A & & \xrightarrow{\qquad\qquad f \qquad\qquad} & & B \end{array}$$

The morphism $A \times_k B \xrightarrow{f(\mathrm{pr}_1)+\mathrm{pr}_2} B$ is the composition of $A \times_k B \xrightarrow{(\mathrm{id},f(\mathrm{pr}_1)+\mathrm{pr}_2)} A \times_k B$ (which is an isomorphism) with the smooth second projection. Thus, the map $f : A \to B$ becomes smooth after pre-composing with the smooth surjective morphism $+_A : A \times_k U \to A$: it is smooth by [4, Lemma 036U]. □

Corollary A.3.19 *Let* A *be an Abelian variety over a field* k. *Let* $m, p, q : A \times_k A \to A$ *be the multiplication, the first projection, and the second projection, respectively. Then, for* $\omega \in H^0(A, \Omega^1_{A/k})$, *one has* $m^*\omega = p^*\omega + q^*\omega$.

Proof. – By Corollary A.3.15, it is enough to show that for any $t \in T_{(0_A,0_A)}(A \times_k A)$, one has

$$m_*(t) = p_*(t) + q_*(t).$$

Let $\iota_1, \iota_2 : A \to A \times_k A$ be the two inclusions $(\mathrm{id}, 0_A)$ and $(0_A, \mathrm{id})$ respectively. When $t = (\iota_1)_* t_1$ (for $t_1 \in T_{0_A}A$), the identity is correct, since $m \circ \iota_1 = p \circ \iota_1 = \mathrm{id}$ while $q \circ \iota_1$ is the zero morphism. Similarly, the identity holds when t is in the image of $(\iota_2)_*$. Thus, the linear map $m_* - p_* - q_* : T_{(0_A,0_A)}(A \times_k A) \to T_{0_A}A$ vanishes on the sum of the images of the tangent maps to ι_1 and ι_2 at 0_A, so it vanishes. □

Corollary A.3.20 *Let* A *be an Abelian variety over a field* k. *Then the pull-back by elements of* $\mathrm{End}(A)$ *endows* $H^0(A, \Omega^1_{A/k})$ *with the structure of a* $(k, \mathrm{End}(A))$*-bimodule.*

Proof. – This is direct. □

Corollary A.3.21 *Let* A *be an Abelian variety over a field* k *and* $\omega \in H^0(A, \Omega^1_{A/k})$. *Then* ω *is translation-invariant.*

Proof. – Let $a \in A(k)$ and $t_a : x \in A \longmapsto x + a \in A$. Then, by Corollary A.3.19,

$$t_a^*\omega = \mathrm{id}^*\omega + a^*\omega = \omega + 0 = \omega.$$

Indeed, $a^*\omega$ is the pull-back by the structure morphism $A \to \mathrm{Spec}\, k$ of a differential in $\Omega^1_{k/k}$, so is zero. □

Proposition A.3.22 *Let* A *be an Abelian variety over a field* k *of characteristic distinct from* 2. *Then for every* $\omega \in H^0(A, \Omega^1_{A/k})$, *one has* $d\omega = 0$.

Proof. – By Proposition A.3.14, $\Omega^2_{A/k}$ is also trivial, so that $H^0(A, \Omega^2_{A/k})$ naturally identifies (by evaluation at 0_A) with $\Lambda^2(T_{0_A}A)^*$ as k-vector spaces. It follows that pull-back by

$[2] : A \to A$ acts by multiplication by 4 on $H^0(A, \Omega^2_{A/k})$. Let now $\omega \in H^0(A, \Omega^2_{A/k})$, then $4d\omega = [2]^* d\omega = d([2]^*\omega) = 2d\omega$, hence $d\omega = 0$ since $2 \in k^\times$. □

A.3.4 Abelian schemes on Dedekind rings in low ramification

In this section, R denotes a localization of $\mathbb{Z}[1/2]$.

Lemma A.3.23 *Let $f : A \to B$ be a morphism of Abelian schemes over R. Suppose that $f_{\mathbb{Q}} : A_{\mathbb{Q}} \to B_{\mathbb{Q}}$ is a closed immersion. Then f is a closed immersion.*

Proof. – This is proved as in the Steps 1-3 of [112, Proposition 1.2]: as in Step 1, there exists $r \geq 1$ and $g_{\mathbb{Q}} : B_{\mathbb{Q}} \to A_{\mathbb{Q}}$ such that $g_{\mathbb{Q}} \circ f_{\mathbb{Q}} = [r]_A$. By the Néron model property, $g_{\mathbb{Q}}$ extends to a morphism $g : B \to A$ of Abelian schemes. Then $g \circ f$ is an endomorphism of A which agrees with $[r]_A$ on the (dense) generic fibre: since A is a separated scheme, $g \circ f = [r]_A$. Thus f is quasi-finite and is between two proper R-schemes, so it is proper, hence f is finite. Suppose that f is not a closed immersion: then, by Nakayama's Lemma, f is not a closed immersion on some special fibre. Since $\ker f$ is a finite R-scheme, it is killed by some $m \geq 1$. But by [112, Proposition 1.1], $f : A[m] \to B[m]$ is a closed immersion for every m, whence the conclusion. □

Remark In the proof, if we do not assume that 2 is invertible in R, the proof shows that f is a finite morphism which is a closed immersion away from 2.

Proposition A.3.25 *Let $H \to G$ be a closed immersion of commutative group schemes over R. Assume that G is of finite type over R and that H is flat. Then the quotient G/H (in the category of fppf sheaves) is representable by a separated scheme of finite type over R and $G \to G/H$ is faithfully flat of finite presentation.*

Proof. – By [2, Theorem 4.C], the quotient sheaf (in the fppf topology) $K := G/H$ exists as a commutative group scheme over R. By [38, Exp. V, Theorem 10.1.2] (applied with $X = K$ and the unit section), the natural morphism $G \to K$ factors through $G \xrightarrow{\pi} G/H \xrightarrow{\iota} K$ with π faithfully flat of finite presentation, G/H locally of finite type over R, and ι a monomorphism. The morphism ι is the identity, and G is quasi-compact, thus so is G/H. Hence G/H is a group scheme of finite type over R.

Let us check that G/H is separated. It is enough to check $\Delta : G/H \to G/H \times_S G/H$ is a closed immersion. Since the following diagram

$$\begin{array}{ccc} G \times_S H & \xrightarrow{(g,h)\mapsto(g,gh)} & G \times_S G \\ \downarrow{\scriptstyle \mathrm{pr}_1} & & \downarrow \\ G/H & \xrightarrow{\Delta} & G/H \times_S G/H \end{array}$$

is Cartesian, it is enough to show by fppf descent that $\iota : (g, h) \in G \times_S H \mapsto (g, gh) \in G \times_S G$ is a closed immersion. Let $f : (g, g') \in G \times_S G \longmapsto (g, g^{-1}g') \in G \times_S G$. Then f is an isomorphism, and $f \circ \iota : (g, h) \in G \times_S H \longmapsto (g, h) \in G \times_S G$ is a base change of the closed immersion $H \to G$, so is a closed immersion. Hence ι is a closed immersion, thus Δ is a closed immersion and G/H is separated. □

Proposition A.3.26 *Let $f : A \to B$ be a morphism of Abelian schemes over R. There exists a factorization $f = \iota \circ \pi$, where $\pi : A \to C$ is a faithfully flat morphism of Abelian schemes, and ι is a closed immersion.*

Proof. – Let C be the Néron model over R of the scheme-theoretic image C_0 of $f_{\mathbb{Q}}$ (this is well-defined by Proposition A.3.12 and [15, §1.4 Theorem 3]). Then $f_{\mathbb{Q}}$ factors as $\iota_0 \circ \pi_0$, where $\pi_0 : A_{\mathbb{Q}} \to C_0, \iota_0 : C_0 \to B_{\mathbb{Q}}$ are morphisms of Abelian varieties with π_0 flat and ι_0 a closed immersion. Then π_0, ι_0 extend to morphisms $\pi : A \to C, \iota : C \to B$ of Abelian schemes. Since $\iota \circ \pi$ agrees with f on the (dense) generic fibre of the separated scheme A, one has $f = \iota \circ \pi$.

Moreover, ι is a closed immersion by Lemma A.3.23. All we need to do is prove that π is flat and surjective. Now, π is between proper R-schemes, so it is proper, thus it has closed image. Moreover, the image of π contains the generic fibre of C, so π is surjective. By [2, Lemma 2.3.3.2], every fibre of π is flat, so, by the "critère de platitude par fibres" [4, Lemma 039D], π is faithfully flat. □

Proposition A.3.27 *Let $f : A \to B$ be a morphism of Abelian schemes over R. Then $\ker f$ is a proper flat group scheme over R, and there is a short exact (for the fppf topology) sequence $0 \to C \to \ker f \to H \to 0$, where H is the finite flat R-group scheme $\operatorname{Spec}\mathcal{O}(\ker f)$, C is an Abelian scheme over R and $C \to \ker f$ is a closed immersion.*

Proof. – Write $f = \iota \circ \pi$ with $\pi : A \to D$ proper faithfully flat, $\iota : D \to B$ a closed immersion and D an Abelian scheme over R by Proposition A.3.26. Then $\ker f = \ker \pi = A \times_{D,0_D} \operatorname{Spec} R$ is proper flat over $\operatorname{Spec} R$. Let $\Gamma = \operatorname{Spec}\mathcal{O}(\ker f)$,

Let C be the Néron model over R of the connected component of unity C_0 of the generic fibre of $\ker f$. By the Néron-Ogg-Shafarevich criterion [146, Theorem 1], C_0 has good reduction at every maximal ideal of v, so C is an Abelian scheme over R (in particular, it is faithfully flat, thus so is $\ker f$). By the Néron mapping property, there is a morphism of Abelian schemes $j : C \to A$ extending the inclusion $C_0 \subset A_{\mathbb{Q}}$, and it is a closed immersion by Lemma A.3.23. The morphisms $0_B : C \to B$ and $f \circ j$ agree on the generic fibre, so they are equal, and j factors through $\ker f$.

By Proposition A.3.25, the quotient sheaf (in the fppf topology) $H := \ker f/C$ exists as a separated commutative group scheme of finite type over R, and $\pi' : \ker f \to H$ is faithfully flat with finite presentation. Since $\ker f$ is proper faithfully flat over R, the "critère de platitude par fibres" [4, Lemma 039D] implies that H is proper flat over R. By [4, Lemma 0D4J] the dimension of its fibres is constant. By construction, the generic fibre of H has finitely many points, so H is proper quasi-finite flat over $\operatorname{Spec} R$, hence H is finite flat over $\operatorname{Spec} R$.

Finally, since $\ker f$ is a proper flat group scheme over $\operatorname{Spec} R$, $\mathcal{O}(\ker f)$ is a finite torsion-free R-algebra, hence it is flat and the natural map $\mathcal{O}(\ker f) \otimes_R \mathcal{O}(\ker f) \to \mathcal{O}(\ker f \times_R \ker f)$ is an isomorphism. This implies that $\operatorname{Spec}\mathcal{O}(\ker f)$ is a finite flat group scheme over R and $\ker f \to \operatorname{Spec}\mathcal{O}(\ker f)$ is a morphism of flat group schemes. Since C is an Abelian scheme over R, $\mathcal{O}(C) \simeq R$, thus $C \to \ker f \to \operatorname{Spec}\mathcal{O}(\ker f)$ is the zero homomorphism. Thus $\ker f \to \operatorname{Spec}\mathcal{O}(\ker f)$ factors through $H \to \operatorname{Spec}\mathcal{O}(\ker f)$.

Thus, the composition of ring homomorphisms $\mathcal{O}(\ker f) \to \mathcal{O}(H) \to \mathcal{O}(\ker f)$ is the identity, hence $\mathcal{O}(\ker f) \to \mathcal{O}(H)$ is injective. Moreover, since $H(\overline{\mathbb{Q}})$ is exactly the group of connected components of $(\ker f)_{\overline{\mathbb{Q}}}$, one has $\dim \mathcal{O}(H) \otimes \overline{\mathbb{Q}} = \dim \mathcal{O}(\ker f) \otimes \overline{\mathbb{Q}}$, so $\mathcal{O}(H)$ and $\mathcal{O}(\ker f)$ are free R-modules of same rank. Hence $\mathcal{O}(H) \to \mathcal{O}(\ker f)$, being surjective, is an isomorphism, and therefore $\ker f \to H$ is exactly the Stein factorization of $\ker f \to \operatorname{Spec} R$. □

A.4 Jacobians of relative curves

A.4.1 Functorialities in the Picard groups

Lemma A.4.1 *Let A be a ring and B a finite locally free A-algebra of constant rank r, and M be a finite locally free B-module of constant rank d. There exists $f_1, \dots, f_r \in A$ generating the unit ideal such that, for each f_i, B_{f_i} is a free A_{f_i}-module and M_{f_i} is a free B_{f_i}-module.*

Proof. – Since M is a flat A-module of finite presentation, it is locally free and has constant rank dr. Let $\mathfrak{p} \in \operatorname{Spec} A$, then $M_{\mathfrak{p}}$ is a finite locally free module of rank r over the semi-local ring $B_{\mathfrak{p}}$. By [4, Lemma 02M9], $M_{\mathfrak{p}}$ is free of rank r over $B_{\mathfrak{p}}$. Hence there exists $m_1, \dots, m_r \in M$ such that $\pi : (b_1, \dots, b_r) \in B \longmapsto \sum_{i=1}^r b_i m_i \in M$ is an isomorphism after tensoring by $\mathfrak{p}$.

By Nakayama, there exists some $f \in A \backslash \mathfrak{p}$ such that the map $\pi \otimes_A A_f$ is surjective. By [4, Lemma 0519], $\ker \pi \otimes_A A_f$ is finitely generated and vanishes when tensoring with $A_{\mathfrak{p}}$, so

by Nakayama, it vanishes after tensoring with A_{fg} for some $g \in A\backslash\mathfrak{p}$. Thus $\pi \otimes_A A_{fg}$ is an isomorphism, whence the conclusion. □

Lemma A.4.2 *Let A be a ring and M be an invertible B-module, where B is a finite locally free A-algebra of constant rank. Then $P = \mathrm{Hom}_A(\det_A B, \det_A M)$ is an invertible A-module. For any $m \in M$, let $\phi_m : B \to M$ be the B-linear morphism mapping 1 to m, then the A-linear homomorphism $\Phi : [m] \in A[M] \longmapsto \det_A \phi_m \in P$ is onto, and its kernel is generated by the $[bm] - N_{B/A}(b)[m]$ for all $b \in B, m \in M$.*

Proof. – By Lemma A.4.1, $\operatorname{Spec} A$ can be covered by principal open subschemes $D(f)$ such that B_f is free over A_f and M_f is free over B_f. In the rest of the proof, we will call such open subschemes *good*. In particular, M is locally free over A.

Since B, M are locally free A-modules, P is an invertible A-module. Since M is invertible over B, B and M have the same constant rank over A, hence Φ is well-defined, and it is clear that $\Phi([bm] - N_{B/A}(b)[m]) = 0$ for all $b \in B, m \in M$. So let $J \subset A[M]$ be the submodule of $A[M]$ generated by the $[bm] - N_{B/A}(b)[m]$ for all $b \in B, m \in M$. The goal is to prove that the sequence

$$0 \to J \to A[M] \xrightarrow{\Phi} P \to 0$$

is exact.

Let $D(f) \subset \operatorname{Spec} A$ be a good principal open subscheme. Let us prove that $\Phi \otimes_A A_f$ is surjective with kernel generated over A_f by J. Indeed, there exists some $m \in M$ such that $b \in B_f \longmapsto bm \in M_f$ is an isomorphism. In particular, $\det_A \phi_m : \det_A B \to \det_A M$ is an isomorphism after tensoring by A_f. It follows that P_f has $\frac{\det_A \phi_m}{1}$ as a A_f-basis, thus $\Phi \otimes_A A_f$ is surjective.

Let $m' \in M$ be any element: since M_f is free over B_f with basis m, there exists $r \geq 1$ and $b \in B$ such that $m' = \frac{b}{f^r} m$ in M_f. Therefore, for some $s \geq 1$, $bf^s m = f^{r+s} m'$ in M, so that $N_{B/A}(b) f^{sd}[m] - f^{(r+s)d}[m'] \in J$, so $[m'] \in J_f + \frac{N_{B/A}(b)}{f^{rd}}[m]$, whence the conclusion. □

Corollary A.4.3 *Let $f : Y \to X$ be a finite locally free map and $\mathcal{L}$ be an invertible $\mathcal{O}_Y$-module. Let $\mathcal{N} : f_*\mathcal{O}_Y \to \mathcal{O}_X$ be the norm map. Let $(U_i)_i$ be a basis of the topology of X constituted by affine open subsets such that $f : f^{-1}(U_i) \to U_i$ has constant rank. Then $f_*\mathcal{L}$ is a locally (with respect to the space X) free $f_*\mathcal{O}_Y$-module, and $\mathcal{P} := \det f_*\mathcal{L} \otimes (\det f_*\mathcal{O}_Y)^{-1}$ is an invertible $\mathcal{O}_X$-module. Given any quasi-coherent $\mathcal{O}_X$-module $\mathcal{M}$, to uniquely define a morphism $\alpha : \mathcal{P} \to \mathcal{M}$ of $\mathcal{O}_X$-modules, it suffices to do the following:*

- *describe a rule attaching to any $s \in \mathcal{L}(f^{-1}(U_i))$ some $\phi(s) \in \mathcal{M}(U_i)$,*
- *check that for any $b \in \mathcal{O}_Y(f^{-1}(U_i)), s \in \mathcal{M}(f^{-1}(U_i))$, $\phi(bs) = \mathcal{N}(b)\phi(s)$,*
- *check that for any $U_j \subset U_i$ and any $s \in \mathcal{L}(f^{-1}(U_i))$, $\phi(s)_{|U_j} = \phi(s_{|f^{-1}(U_j)})$.*

Then, for all $s \in \mathcal{L}(f^{-1}(U_i))$, α maps the determinant of the map $f_*s : (f_*\mathcal{O}_Y)_{|U} \to (f_*\mathcal{L})_{|U}$ of locally free $\mathcal{O}_U$-modules to $\phi(s)$.

Proof. – This is a formal consequence of the previous result. □

Proposition A.4.4 *Let $f : Y \to X$ be a finite locally free morphism of schemes and $\mathcal{L}$ be an invertible module. The formation of $f_*\mathcal{L}$ commutes with arbitrary base change. Moreover, the formation of the norm morphism $f_*\mathcal{O}_Y \to \mathcal{O}_X$ commutes with arbitrary base change.*

Proof. – This is classical, see for instance [4, Lemma 02KG,Lemma 0BD2]. □

Proposition A.4.5 *Let $\mathcal{M}, \mathcal{N}$ be two invertible modules over a scheme Y, and assume that $f : Y \to X$ is finite locally free. Let $\omega = \det f_*\mathcal{O}_Y$. Write $\mathcal{M}' = \underline{Hom}_{\mathcal{O}_X}(\omega, \det f_*\mathcal{M})$, and let us adopt a similar notation for $\mathcal{N}'$. There exists a canonical isomorphism of invertible $\mathcal{O}_X$-modules*

$$T : \mathcal{M}' \otimes_{\mathcal{O}_X} \mathcal{N}' \to \underline{Hom}_{\mathcal{O}_X}(\omega, \det f_*\mathcal{M} \otimes \mathcal{N}).$$

For any open subset $U \subset X$ and any $m \in \mathcal{M}(f^{-1}(U)), n \in \mathcal{N}(f^{-1}(U))$, T maps $\det f_*m \otimes \det f_*n$ *to* $\det f_*(m \otimes n)$. *Moreover, the formation of T commutes with any base change with respect to X.*

Proof. – The uniqueness is clear by the property. Note that to check the property, we may assume that U is affine and $f^{-1}(U) \to U$ has constant rank. To construct T, consider the rule mapping some $s \in \mathcal{M}(f^{-1}(U))$ to the determinant of the morphism $f_*(m \otimes -) : (f_*\mathcal{N})_{|U} \to (f_*(\mathcal{M} \otimes \mathcal{N}))_{|U}$ of locally free $\mathcal{O}_U$-modules of same rank. By Corollary A.4.3, this rule defines a morphism $\mathcal{M}' \to \underline{Hom}_{\mathcal{O}_X}(\det f_*\mathcal{N}, \det f_*(\mathcal{M} \otimes \mathcal{N}))$.

Since $\det f_*\mathcal{N}$, $\mathcal{P} := \det f_*(\mathcal{M} \otimes \mathcal{N})$ are invertible, this is equivalent to defining a morphism $\mathcal{M}' \otimes \mathcal{N}' \to \underline{Hom}_{\mathcal{O}_X}(\omega, \mathcal{P})$. One can then easily check that this morphism satisfies the stated property. To see that T is an isomorphism, it is enough to check that it is surjective. We can work Zariski-locally on X and assume that X is affine, $f_*\mathcal{M}, f_*\mathcal{N}, f_*(\mathcal{M} \otimes \mathcal{N})$ are free over $f_*\mathcal{O}_Y$ and that $f_*\mathcal{O}_Y$ is free over $\mathcal{O}_X$. The conclusion follows by choosing bases m, n of $\mathcal{M}, \mathcal{N}$. □

Proposition A.4.6 *Let $f : X \to Y, g : Y \to Z$ be finite locally free morphisms of schemes, of constant rank. Let $\mathcal{L}$ be a line bundle on X. Then there is a canonical isomorphism*

$$\underline{Hom}_{\mathcal{O}_Z}(\det (g_*f_*)\mathcal{O}_X, \det g_*f_*\mathcal{L}) \to \underline{Hom}_{\mathcal{O}_Z}(\det g_*(\det f_*\mathcal{O}_X), \det g_*(\det f_*\mathcal{L}))$$

given by the following rule: for any open subset $U \subset X$ and any $s \in \mathcal{L}(f^{-1}(g^{-1}(U)))$, it maps $\det (g \circ f)_*s$ *to* $\det g_*(\det f_*s)$. *The formation of this isomorphism commutes with base change.*

Proof. – That the morphism exists follows from Corollary A.4.3. The commutation with base change is easy (using in Corollary A.4.3 an affine cover coming from the original $X \to Y \to Z$). Since its domain and range are invertible $\mathcal{O}_Z$-modules, we only need to prove that the morphism is surjective. This is easy by choosing local sections s generating $\mathcal{L}(f^{-1}(g^{-1}(U)))$ over $\mathcal{O}_X(f^{-1}(g^{-1}(U)))$, so that $\det g_* \det f_*s$ is a basis of the range above U. □

Proposition A.4.7 *Let $f : Y \to X$ be a morphism of schemes, finite free of constant rank. Then*

$$f^* : \mathcal{L} \in \mathrm{Pic}(X) \longmapsto f^*\mathcal{L} \in \mathrm{Pic}(Y),\ [f_*] : \mathcal{L} \in \mathrm{Pic}(Y) \longmapsto \det f_*\mathcal{M} \otimes (\det f_*\mathcal{O}_Y)^{-1}$$

are functorial group homomorphisms.

Proof. – This is clear for f^*. It is clear that id_* is exactly the identity. That f_* is a group homomorphism follows from Proposition A.4.5. To show functoriality, let $f : X \to Y$ and $g : Y \to Z$ be finite morphisms, locally free of constant rank, and $\mathcal{L}$ be a line bundle on X. Then, using Proposition A.4.6,

$$\begin{aligned}[g_*][f_*]\mathcal{L} &\simeq [g_*](\det f_*\mathcal{L} \otimes (\det f_*\mathcal{O}_X)^{-1}) \simeq [g_*](\det f_*\mathcal{L}) \otimes ([g_*]((\det f_*\mathcal{O}_X)^{-1}))^{-1} \\ &\simeq \det g_* \det(f_*\mathcal{L}) \otimes (\det g_* \det(f_*\mathcal{O}_X))^{-1} \\ &\simeq \det (g \circ f)_*\mathcal{L} \otimes (\det (g \otimes f)_*\mathcal{O}_X)^{-1}.\end{aligned}$$

□

Lemma A.4.8 *Let $f : X \to Y$ be a finite flat morphism of finite type reduced schemes over a field k, with X, Y pure of dimension one (hence Cohen-Macaulay). Let $\mathcal{L}$ be a line bundle on X contained in $\mathcal{K}_X$, so that it defines a Cartier divisor on X. Then the line bundle $\mathcal{M} = [f_*]\mathcal{L}$ on Y has a natural embedding into $\mathcal{K}_Y$, which defines a Cartier divisor on Y. Let S_X (resp. S_Y) be the finite set of (closed points) $x \in X$ (resp. $y \in Y$) such that $\mathcal{L}_{X,x} \neq \mathcal{O}_{X,x}$ (resp. $\mathcal{M}_{Y,y} \neq \mathcal{O}_{Y,y}$). Then $S_Y \subset f(S_X)$. If moreover every point of S_X is normal, then every point of $f(S_Y)$ is normal, and, for every $y \in S_Y$,* $\mathrm{mult}_y\mathcal{M} = \sum_{x \in f^{-1}(y) \cap S_X} \mathrm{mult}_x\mathcal{L} \cdot [\kappa(x) : \kappa(y)]$, *where the multiplicity is defined as in [106, Definition 7.1.27].*

Proof. – We may assume that Y is connected, so that f has constant rank d. Our assumptions

imply that the only functions on X, Y are that are not regular at every point are those that vanish at some generic point. In particular, the sheaves of meromorphic functions on X, Y are well-behaved [4, Lemma 0EMF]. Moreover, given an affine open subscheme $U \subset Y$, a section in $\mathcal{O}_X(f^{-1}(U))$ is a regular element (resp. invertible) if and only if its norm over $\mathcal{O}_Y(U)$ is a regular element (resp. invertible). This implies that the norm $f_*\mathcal{O}_X \to \mathcal{O}_Y$ induces compatible $f_*\mathcal{G}_X \to \mathcal{G}_Y$ for $\mathcal{G} = \mathcal{K}, \mathcal{K}^\times, \mathcal{O}^\times$. Note that since f is flat, we have a pull-back of meromorphic functions [4, Lemma 02OU]. The natural map $(f_*\mathcal{K}_X^\times)/(f_*\mathcal{O}_X^\times) \to f_*(\mathcal{K}_X^\times/\mathcal{O}_X^\times)$ is an isomorphism (by checking at the stalks and using the fact that the sheaves of meromorphic functions are well-defined).

Therefore, we have a homomorphism of sheaves in Abelian groups $\nu : f_*(\mathcal{K}_X^\times/\mathcal{O}_X^\times) \to \mathcal{K}_Y^\times/\mathcal{O}_Y^\times$. The embedding $\mathcal{L} \subset \mathcal{K}_X$ corresponds to a section $s_\mathcal{L}$ of $\mathcal{K}_X^\times/\mathcal{O}_X^\times$, and let $s_\mathcal{M}$ be its image in $\mathcal{K}_Y^\times/\mathcal{O}_Y^\times$. Then $s_\mathcal{M}$ defines a line bundle $\mathcal{M}$ on Y. The claim that we wish to prove is that $\mathcal{M} \simeq (\det f_*\mathcal{O}_X)^{-1} \otimes \det f_*\mathcal{L}$.

We define a map $\alpha : (\det f_*\mathcal{O}_X)^{-1} \otimes \det f_*\mathcal{L} \to \mathcal{M}$ as follows: given any affine open subset $U \subset Y$ small enough such that $\mathcal{L}(f^{-1}(U))$ is free over $\mathcal{O}_X(f^{-1}(U))$, for any $s \in \mathcal{L}(U)$, we write $s = fs_1$ for some $f \in \mathcal{O}_X(f^{-1}(U))$, where s_0 is any $\mathcal{O}_X(f^{-1}(U))$-basis of $\mathcal{L}(f^{-1}(U))$, and we map $\det f_*s$ to $N_{X/Y}(fs_1) \in \mathcal{O}_Y(U)s_\mathcal{M} = \mathcal{M}(U)$. This does not depend on the choice of factorization of $s = fs_0$, and satisfies the compatibility properties of Corollary A.4.3. One can also check locally that α is surjective, thus an isomorphism, proving the first part of the claim.

Note that if $s_{\mathcal{L},z} = 1$ (equivalently, $\mathcal{L}_{X,z} = \mathcal{O}_{X,z}$ as subgroups of $\mathcal{K}_{X,z}$, or $z \notin S_X$) for all $z \in f^{-1}(y)$ for some $y \in Y$, then $f_*\mathcal{O}_X$ and $f_*\mathcal{L}$ are quasi-coherent subsheaves of $f_*\mathcal{K}_X$ (itself quasi-coherent) whose stalks agree at x, hence their stalks agree in a neighborhood of y. Therefore, the stalk of $f_*s_\mathcal{L}$ at y is trivial, hence so is the stalk of $s_\mathcal{M}$ at y. This implies that $S_Y \subset f(S_X)$.

If every point x of S_X is normal, then for any $y \in S_Y$, $y = f(x)$ for some $x \in S_X$, so that $\mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ is faithfully flat with $\mathcal{O}_{X,x}$ normal. Thus $\mathcal{O}_{Y,y}$ normal.

The final part of the statement is local with respect to Y; since S_Y is contained in the normal points of Y, we may restrict to affine open subsets contained in the interiors of the irreducible components of Y, thereby assuming that Y is integral. We are then reduced to the following problem: let A be an integral k-algebra of dimension one, and $\mathfrak{m}$ be a maximal ideal such that $A_\mathfrak{m}$ is normal. Let B be a finite flat reduced A-algebra. Let $s \in (B_{reg}^{-1}B)^\times$, and S be the set of maximal ideals of B above $\mathfrak{m}$ such that $sB_\mathfrak{p} \neq B_\mathfrak{p}$. Assume that $B_\mathfrak{p}$ for $\mathfrak{p} \in S$ is normal. Then $v_\mathfrak{m}(N_{B/A}(s)) = \sum_{\mathfrak{p}\in S} f_\mathfrak{p} v_\mathfrak{p}(s \cdot 1_{B_\mathfrak{p}})$, where $f_\mathfrak{p}$ is the degree of the extension of residue fields $A/\mathfrak{m} \to B/\mathfrak{p}$. In other words, $f_\mathfrak{p} \dim_k A/\mathfrak{m} = \dim_k B/\mathfrak{p}$.

Note that both sides of the identity to prove are additive with respect to s (seen as an element of the group $(B_{reg}^{-1}B)^\times$).

By the prime avoidance lemma, for every $\mathfrak{p} \in S$, we can find some $u_\mathfrak{p} \in B$ contained in $\mathfrak{p}$, but not in $\mathfrak{p}^2$ or in any other prime ideal of B lying above $\mathfrak{m}$ or (0). Then $u_\mathfrak{p} \in B_{reg}$, and $u_\mathfrak{p}$ is a generator of $\mathfrak{p}B_\mathfrak{p}$. Let $s' = s \cdot \prod_{\mathfrak{p}\in S} u_\mathfrak{p}^{-v_\mathfrak{p}(s)}$, then $s' \in (B_{reg}^{-1}B)^\times$ is such that for each maximal $\mathfrak{p}$ of B above $\mathfrak{m}$, $s'B_\mathfrak{p} = B_\mathfrak{p}$. Thus $s' : B/\mathfrak{m} \to B/\mathfrak{m}$ is injective between finite dimensional k-vector spaces, hence surjective. Thus the multiplication by s' is an endomorphism of the free $A_\mathfrak{m}$-module of finite rank $B_\mathfrak{m}$ which is surjective after tensoring by $A/\mathfrak{m}$. Hence it is an isomorphism by Nakayama's Lemma, and its determinant (which is $N_{B/A}(s')$) is invertible.

Thus the identity holds for s'. It is therefore enough to prove the identity assuming that $s = u_\mathfrak{p}$, $S = \{\mathfrak{p}\}$ for some $\mathfrak{p}$, ie that $v_\mathfrak{m}(N_{B/A}(u_\mathfrak{p})) = f_\mathfrak{p}$. Since the multiplication by $u_\mathfrak{p}$ is an injective endomorphism of the free $A_\mathfrak{m}$-module of finite rank $B_\mathfrak{m}$, with $A_\mathfrak{m}$ being a discrete valuation ring, it is given in suitable bases of $B_\mathfrak{m}$ by a diagonal matrix with diagonal $(\alpha_i)_{1\leq i\leq n}$ of nonzero elements of $A_\mathfrak{m}$. Then one has

$$\begin{aligned} f_{\mathfrak{p}} &= \mathrm{len}_{A/\mathfrak{m}}(B/\mathfrak{p}) = \mathrm{len}_{A/\mathfrak{m}}(B_{\mathfrak{m}}/u_{\mathfrak{p}}B_{\mathfrak{m}}) \\ &= \mathrm{len}_{A/\mathfrak{m}}\left(\bigoplus_{i=1}^{n} A/\alpha_i A\right) = \sum_{i=1}^{n} \mathrm{len}_{A/\mathfrak{m}}(A/\alpha_i) = \sum_{i=1}^{n} v_{\mathfrak{m}}(\alpha_i) \\ &= v_{\mathfrak{m}}\left(\prod_{i=1}^{n} \alpha_i\right) = v_{\mathfrak{m}}(\det[u_{\mathfrak{p}} : B_{\mathfrak{m}} \to B_{\mathfrak{m}}]) = v_{\mathfrak{m}}(N_{B/A}(u_{\mathfrak{p}})), \end{aligned}$$

whence the conclusion. □

Remark This lemma states, in other words, that the notion of push-forward we defined functions as the natural push-forward at the level of Weil divisors.

Proposition A.4.10 *Consider the following commutative diagram of schemes, where all the maps are finite locally free:*

$$\begin{array}{ccc} Y & \xrightarrow{f} & X \\ \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle u} \\ Y' & \xrightarrow{f'} & X' \end{array}$$

There are then two morphisms $\mathrm{Pic}(Y') \to \mathrm{Pic}(X)$*, given by* $u^*[(f')_*]$ *and* $[f_*]v^*$*. These morphisms are equal if, for any affine open subscheme* $U \subset X'$*, and any* $b \in \mathcal{O}_{Y'}((f')^{-1}(U))$*, one has* $u^\sharp(N_{Y'/X'}(b)) = N_{Y/X}(v^\sharp(b))$*.*

This hypothesis is verified if there exists an open subscheme $U \subset X'$ *such that the diagram is Cartesian above* U *and* $\mathcal{O}_{X'} \to \iota_*\mathcal{O}_{X'_U}$ *is injective, where* ι *is the open immersion* $U \to X'$*.*

Proof. – We first prove the second part of the statement. Since Y', Y, X are flat over X', the morphisms $\mathcal{O}_Z \to \iota_*\mathcal{O}_{Z_U}$ are injective for all each $Z \in \{X, Y', Y\}$; it follows that the norms satisfy the required compatibility.

Now we discuss the first part. Let $\mathcal{L}$ be a line bundle on X, then one directly shows that

$$\begin{aligned} u^*[(f')_*]\mathcal{L} &\simeq u^*\underline{Hom}_{\mathcal{O}_{X'}}(\det(f')_*\mathcal{O}_{Y'}, \det(f')_*\mathcal{L}), \\ [f_*]v^*\mathcal{L} &\simeq \underline{Hom}_{\mathcal{O}_X}(\det f_*\mathcal{O}_Y, \det f_* v^*\mathcal{L}). \end{aligned}$$

We first define our morphism $\Psi : u^*[(f')_*]\mathcal{L} \to [f_*]v^*\mathcal{L}$ by adjunction: it is enough to define a morphism of quasi-coherent sheaves

$$\Phi : \underline{Hom}_{\mathcal{O}_{X'}}(\det(f')_*\mathcal{O}_{Y'}, \det(f')_*\mathcal{L}) \to \underline{Hom}_{\mathcal{O}_X}(\det f_*\mathcal{O}_Y, \det f_* v^*\mathcal{L}).$$

For any affine open subset $U \subset X'$, and $s \in \mathcal{L}((f')^{-1}(U))$, we map $\det(f')_* s$ to $\det f_*(v^*s)$, where $v^*s \in (v^*\mathcal{L})(v^{-1}((f')^{-1}(U))) = \mathcal{L}(f^{-1}(u^{-1}(U)))$, so f_*v^*s defines a morphism of locally free $\mathcal{O}_{u^{-1}(U)}$-modules of same rank $(f_*\mathcal{O}_Y)_{|u^{-1}(U)} \to (f_*v^*\mathcal{L})_{|u^{-1}(U)}$. The assumption on the norm shows Corollary A.4.3 applies and that Φ, hence Ψ, is well-defined.

To show that our morphism is an isomorphism, we work Zariski-locally on X', so we can assume that we are given finite free A-algebras B, C, a $B \otimes_A C$-algebra D (corresponding respectively to X', Y', X, Y) which is locally free over B and C, a free B-module M of rank one (corresponding to $\mathcal{L}$), and such that, for any $b \in B$, the image in C of $N_{B/A}(b)$ is exactly $N_{D/C}(b)$, where N denotes the norm.

In this situation, $\Psi : \mathrm{Hom}_A(\det_A B, \det_A M) \otimes_A C\mathrm{Hom}_C(\det_C D, \det_C M \otimes_B D)$, is given by $\det_A m \otimes 1 \longmapsto \det_C m \otimes_B D$ for any $m \in M$, where m is identified with the A-homomorphism of locally free A-modules of same rank $B \to M$ mapping any $b \in B$ to bm. Let $m \in M$ be a B-basis, then the source of Ψ (resp. its codomain) is free over C of basis $\det_A m$ (resp. $\det_C m \otimes_B D$), so that Ψ is indeed an isomorphism. □

A.4.2 Degrees and Jacobian varieties

Definition A.4.11 Let k be a field and X be a proper k-scheme, pure of dimension one. The degree of a locally free module $\mathcal{L}$ on X of rank $r : \pi_0(X) \to \mathbb{N}$ is the function $\pi_0(X) \to \mathbb{Z}$ given, for every (open and closed) connected component C of X, by

$$\deg \mathcal{L}(C) = \chi(C, \mathcal{L}_{|C}) - r(C)\chi(C, (\mathcal{O}_X)_{|C}),$$

where χ denotes the Euler-Poincaré characteristic.

Note that this definition differs slightly from [4, Section 0AYQ], because we treat connected components separately instead of adding the results up. This is why we recall some elementary statements about degrees.

Proposition A.4.12 *In the situation of Definition A.4.11,* $\mathcal{L}$ *and* $\det \mathcal{L}$ *have the same degree, where* $\det \mathcal{L}$ *is the line bundle on* X *whose restriction to any connected component* C *is given by* $\Lambda^{r(C)}\mathcal{L}$*. Moreover,* deg *defines a group homomorphism* $\mathrm{Pic}(X) \to \mathbb{Z}^{\pi_0(X)}$*.*

Proof. – The first statement is exactly the content of [4, Lemma 0DJ5], applied to each connected component of X separately. For the second claim, let $\mathcal{L}, \mathcal{M}$ be line bundles on X. Then one has

$$\deg \mathcal{L} + \deg \mathcal{M} = \deg(\mathcal{L} \oplus \mathcal{M}) = \deg\left[\det(\mathcal{L} \oplus \mathcal{M})\right] = \deg(\mathcal{L} \otimes \mathcal{M}).$$

□

Lemma A.4.13 *In the situation of Definition A.4.11, if* X *is connected and* $\mathcal{L}$ *is the sheaf of ideals defining a closed subscheme* Z*, finite over* k *of degree* d*, then* $\deg \mathcal{L} = -d$*.*

Proof. – Let $\iota : Z \to X$ be the natural closed immersion: we have an exact sequence

$$0 \to \mathcal{L} \to \mathcal{O}_X \to \iota_* \mathcal{O}_Z \to 0,$$

which implies that

$$\chi(X, \mathcal{O}_X) = \chi(X, \mathcal{L}) + \chi(X, \iota_* \mathcal{O}_Z) = \chi(X, \mathcal{L}) + \chi(Z, \mathcal{O}_Z).$$

Since Z is finite over $\operatorname{Spec} k$, it is a discrete topological space and $\chi(Z, \mathcal{O}_Z) =$ has finite support, $\chi(Z, \iota_* \mathcal{O}_Z) = \dim_k H^0(Z, \mathcal{O}_Z) = d$, and the conclusion follows. □

Lemma A.4.14 *Let* X *be a proper* k*-scheme, pure of dimension one, and* $\mathcal{L}$ *be a line bundle on* X *with degree zero. Then, for any field extension* k' *of* k *and any connected component* C *of* $X_{k'}$*, the degree of* $f^*\mathcal{L}$ *(where* f *is the morphism* $X_{k'} \to X$*) is zero. Conversely, if* $\mathcal{L}$ *is a line bundle on* X *such that for any connected component* C *of* $X_{k'}$*,* $\deg f^*\mathcal{L}(C) = 0$*, then* $\mathcal{L}$ *has degree zero on any connected component of* X*.*

Proof. – First, by [4, Lemma 0B59], one has $\sum_C \deg f^*\mathcal{L}(C) = \deg \mathcal{L}(D)$, where C runs through the connected components of $X_{k'}$ above a fixed connected component D of X. This proves immediately the "converse" statement.

We can assume that X is connected. Assume first that k' is Galois over k, potentially of infinite degree. Then $\mathrm{Gal}(k'/k)$ acts transitively on $\pi_0(X_{k'})$ (see for instance [106, Exercise 3.2.10]), so that $\deg f^*\mathcal{L}(C)$ is an integer δ that does not depend on C. Therefore, if n is the number of connected components of $X_{k'}$, $\deg \mathcal{L} = n\delta$, hence $\delta = 0$.

When k'/k is algebraic and separable, we can embed it in its Galois closure k''/k. Then, on any connected component C of $X_{k''}$, where $f' : X_{k''} \to X$ is the base change morphism, one has $\deg (f')^*\mathcal{L}(C) = 0$. The "converse" statement applied to the extension k''/k' and the line bundle $f^*\mathcal{L}$ shows that $f^*\mathcal{L}$ has degree zero on each connected component.

When k'/k is purely inseparable, $X_{k'} \to X$ is a homeomorphism, hence $X_{k'}$ is connected and $C = X_{k'}$, and the statement is true. Pulling these results together, this proves the claim when k'/k is algebraic.

In general, let $k_1 \supset k'$ be an algebraically closed field and $k'' \subset k_1$ the algebraic closure of k in k_1. To prove the claim, using the "converse" for the extension k_1/k', we may assume that $k' = k_1$. By the above, we may assume that $k = k''$. In this case, the connected components of X are geometrically connected and the result follows from the first identity. □

Lemma A.4.15 *Let k be a field, $f : Y \to X$ be a finite flat map of pure one-dimensional proper k-schemes. Let $\mathcal{M}$ be a line bundle on Y of degree zero. Then $[f_*]\mathcal{M}$ has degree zero. Let $\mathcal{L}$ be a line bundle on X. Then, given connected components C of Y, C' of X containing $f(C)$, $\deg(f^*\mathcal{L})(C') = (\deg f_C) \cdot (\deg \mathcal{L})(C)$, where $f_C : C \to C'$ is the finite flat map induced by f.*

Proof. – This is a well-known consequence of the results from [4, Section 0AYQ]. Since our notion of degree is not quite the same, we include a proof for the sake of completeness.

Let $\mathcal{M}$ be a line bundle on Y, and C be any connected component of X. Then

$$\deg \det[f_*\mathcal{M}](C) = (\deg f_*\mathcal{M})(C) = \chi(C, f_*\mathcal{M}) - \chi(C, \mathcal{O}_C) = \chi(f^{-1}(C), \mathcal{M}) - \chi(C, \mathcal{O}_C).$$

Hence, if $\mathcal{M}$ has degree zero, $\deg \det[f_*\mathcal{M}](C) = \chi(f^{-1}(C), \mathcal{O}_Y) - \chi(C, \mathcal{O}_C)$, and the conclusion follows from Proposition A.4.12.

Let $\mathcal{L}$ be a line bundle on X of degree zero. Let $C \subset Y$ be a component (endowed with the reduced scheme structure) and $C' \subset X$ the unique irreducible component (endowed with the reduced scheme structure) containing $f(C)$. Then $f_C : C \to C'$ is finite between integral proper k-schemes of dimension one. Moreover, f is finite flat hence open, so $f(C)$ contains a nonempty open subset of C', whence f_C is surjective. Thus $\deg (f^*\mathcal{L})_{|C} = \deg f_C \deg \mathcal{L}_{|C'}$ by [4, Lemma 0YAZ]. The conclusion follows from using [4, Lemma 0AYW] on every connected component of Y.

Let $\mathcal{L}$ be a line bundle on X of degree zero. Let $C \subset Y$ be a connected component and $C' \subset X$ the unique connected component containing $f(C)$. Then $f_C : C \to C'$ is finite flat between proper connected k-schemes of dimension one, hence locally free of constant degree c. Then

$$\begin{aligned}\deg f^*\mathcal{L}(C) &= \chi(C, f^*\mathcal{L}) - \chi(C, \mathcal{O}_C) = \chi(C', (f_C)*(f_C)^*\mathcal{L}) - \chi(C', (f_C)_*\mathcal{O}_C) \\ &= \deg((f_C)_*(f_C)^*\mathcal{L})(C') + c\chi(C', \mathcal{O}_{C'}) - \chi(C', (f_C)_*\mathcal{O}_C) \\ &= (\deg \mathcal{L} \otimes (f_C)_*\mathcal{O}_C)(C) - \deg (f_C)_*\mathcal{O}_C = c \deg \mathcal{L}(C),\end{aligned}$$

where the last equality is [4, Lemma 0AYX]. □

Lemma A.4.16 *Let $\pi : X \to S$ be a proper, finitely presented morphism with Stein factorization [4, Theorem 03H2] $X \xrightarrow{f} S' \to S$. For any S-scheme T, if $X_T \to T' \to T$ denotes the Stein factorization of $X_T \to T$, there is a canonical morphism $\sigma : T' \to S' \times_S T$ such that the following diagram commutes:*

$$\begin{array}{ccccc} X_T & \longrightarrow & T'T & \longrightarrow & \\ \downarrow{=} & & \downarrow{\sigma} & & \downarrow{=} \\ X \times_S T & \longrightarrow & S' \times_S T & \longrightarrow & S \times_S T \end{array}$$

If T is flat over S, σ is an isomorphism.

Proof. – This comes down to the definition and properties of the Stein factorization, as well as the existence of a base change morphism $(\pi_*\mathcal{O}_X)_T \to (\pi_T)_*\mathcal{O}_{X_T}$, which is an isomorphism when T is flat over S. □

Definition A.4.17 Let X be a proper finitely presented S-scheme. The *relative Picard presheaf* of X is the functor $P_{X/S}$ on $\mathbf{Sch}_S$ given by $T \longmapsto \mathrm{Pic}(X \times_S T)$. The *relative Picard functor* of X/S is the sheafification $\mathrm{Pic}_{X/S}$ of $P_{X/S}$ in the fppf topology. If moreover $X \to S$ has pure fibres of dimension one, we define $P^0_{X/S}$ as the sub-presheaf of $P_{X/S}$ constituted by the classes of those line bundles $\mathcal{L}$ on $X \times_S T$ such that for every $t \in T$, the line bundle $t^*\mathcal{L}$ on $X_{\kappa(t)}$ has

degree zero on every connected component. Its fppf-sheafification is the *relative Picard functor of degree zero* $\mathrm{Pic}^0_{X/S}$ for X/S.

Remarks

- By Lemma A.4.14, when the fibres of $X \to S$ are pure of dimension one, $P^0_{X/S}$ is indeed a sub-presheaf of $P_{X/S}$ and the quotient pre-sheaf $P_{X/S}/P^0_{X/S}$ is separated for fppf covers.
- The functors $P_{X/S}, \mathrm{Pic}_{X/S}$ match the one described in [15, §8.1, Definition 2]. By Lemma A.4.14, $\mathrm{Pic}^0_{X/S}$ identifies with the smallest subsheaf of $\mathrm{Pic}_{X/S}$ containing $P^0_{X/S}$.

Lemma A.4.18 *Let X be a proper k-scheme, pure of dimension one, and S be a finite k-scheme. Let $f : X \to S$ be a morphism of k-schemes and $\mathcal{L}$ be a line bundle on S. Then $\mathcal{L}$ is trivial. In particular, $f^*\mathcal{L}$ has degree* 0.

Proof. – S is a finite k-scheme, so it is affine and the spectrum of a finite product of Artinian local rings. Hence any line bundle on S is trivial. In particular, $f^*\mathcal{L}$ is the trivial line bundle on X, thus its degree is zero on every connected component of X. □

Lemma A.4.19 *Let X be a proper finitely presented S-scheme and S' be any S-scheme. Let $f : X_{S'} \to T$ be a morphism of S'-schemes, with T finite locally free over S'. Then $f^* \mathrm{Pic}(T)$ is in the kernel of $P_{X/S}(S') \to \mathrm{Pic}_{X/S}(S')$.*

Proof. – Let $\mathcal{L}$ be a line bundle on T. By Lemma A.4.1, there is an affine open cover U_i of S' such that $\mathcal{L}|T \times_{S'} U_i$ is free. In particular, the image of $f^*\mathcal{L}$ in $P_{X/S}(U_i)$, hence in $\mathrm{Pic}_{X/S}(U_i)$, vanishes. Since $\mathrm{Pic}_{X/S}$ is a fppf-sheaf, the class of $\mathcal{L}$ in $\mathrm{Pic}_{X/S}(S')$ vanishes. □

Definition A.4.20 A relative curve is a map $\pi : C \to S$ satisfying the following properties:

- π is proper, finitely presented, flat of relative dimension one with geometrically reduced fibres, and surjective,
- $\pi_*\mathcal{O}_C$ is a quasi-coherent finite étale $\mathcal{O}_C$-algebra, and its formation commutes with arbitrary base change.

Proposition A.4.21 *The property "relative curve" is stable under arbitrary base change and fpqc-local on S. Moreover, if $C \to S$ is a relative curve, the formation of the Stein factorization $C \to T \to S$ [4, Theorem 03H2] commutes with arbitrary base change. Moreover, $T \to S$ is finite étale, $f : C \to T$ is proper flat of relative dimension one, its geometric fibres are reduced and connected, and the formation of $f_*\mathcal{O}_C$ commutes with arbitrary base change (with respect to T).*

Proof. – The first statement is a formal verification using the fact that the formation of push-forwards of quasi-coherent sheaves commutes to flat base change and the fact that the formation of $\pi_*\mathcal{O}_C$ commutes to arbitrary base change.

The fact that $T \to S$ is finite étale follows from the definition. Since f is the composition $C = C \times_T T \to C \times_S T \to T$ of a closed open immersion with a proper flat morphism of relative dimension one, it is proper flat of relative dimension one. The fibres of f are geometrically connected by [4, Theorem 03H2]. This theorem also implies that the formation of the Stein factorization commutes to arbitrary base change (of S-schemes), since the formation of $\pi_*\mathcal{O}_C$ commutes to arbitrary base change by definition.

Let U be a T-scheme (with structure map σ). Note that the following diagram commutes, both squares are Cartesian, and j is a closed open immersion since $T \to S$ is finite étale:

$$\begin{array}{ccccc} C \times_T U & \longrightarrow & C \times_S U & \longrightarrow & C \\ \downarrow{\scriptstyle f_{T,U}} & & \downarrow{\scriptstyle f_U} & & \downarrow{\scriptstyle f} \\ U & \xrightarrow{j=(\sigma,\mathrm{id})} & T \times_S U & \longrightarrow & T \end{array}$$

It follows in particular that the natural morphism $\sigma^* f_* \mathcal{O}_C \to (f_{U,T})^* \mathcal{O}_{C\times_T U}$ is an isomorphism, that is, the formation of $f_*\mathcal{O}_C$ commutes with arbitrary base change with respect to T. Since $\mathcal{O}_T \to f_*\mathcal{O}_C$ is an isomorphism, this map remains an isomorphism after any base change of T-scheme. □

Proposition A.4.22 *Let $X \to S$ be a relative curve with Stein factorization $X \xrightarrow{f} T \to S$. The pre-sheaf $P'_{X/S} : U \longmapsto P_{X/S}(U)/f^* \operatorname{Pic}(T \times_S U)$ is separated for fppf covers, and the sheafification map $P_{X/S} \to \operatorname{Pic}_{X/S}$ factors through $P'_{X/S}$. The pre-sheaf*

$$P'^0_{X/S} : U \longmapsto P^0_{X/S}(U)/f^* \operatorname{Pic}(T \times_S U)$$

is a sub-presheaf of $P'_{X/S}$, and the sheafification map $P^0_{X/S} \to \operatorname{Pic}^0_{X/S}$ factors through $P'^0_{X/S}$. Moreover, if there exists a section of $X \to T$, then $P'_{X/S}, P'^0_{X/S}$ are sheaves in the fppf topology.

Proof. – That $P'^0_{X/S}$ is a sub-presheaf of $P'_{X/S}$ follows from Lemma A.4.18. That the sheafification $P_{X/S} \to \operatorname{Pic}_{X/S}$ factors through $P'_{X/S}$ (and the same statement for the degree-zero pre-sheaves) follows from Lemma A.4.19, since T is finite étale locally free over S and the formation of the Stein factorization commutes with arbitrary base change in this case, by Proposition A.4.21.

That $P'_{X/S}$ is separated is a reformulation of the seesaw theorem [4, Lemma 0BDP] for (base changes of) the morphism $\pi : X \to T$, using Proposition A.4.21 (since $\mathcal{O}_T \to \pi_*\mathcal{O}_X$ is a universal isomorphism).

Thanks to Proposition A.4.21, to prove the final statement, it is enough to show that $P'_{X/S}(S)$ satisfies the glueing property. Let $\sigma : T \to X$ be a morphism of T-schemes, let I be a set and $(\pi_i : S_i \to S)_{i\in I}$ be a fppf covering. Let, for each $i \in I$, $L_i \in P'_{X/S}(S_i)$ such that, for each $i, j \in I$, L_i and L_j have the same image in $P'_{X/S}(S_i \times_S S_j)$. We want to find some $s \in P'_{X/S}(S)$ such that each s_i is the restriction of S.

Let $i \in I$, pick some line bundle $\mathcal{L}$ on $X \times_S S_i$ in the class of s_i, and let $\mathcal{L}_i = \mathcal{L} \otimes (f^*\sigma^*\mathcal{L})^{\otimes -1}$. Then there is an isomorphism $\rho_i : \mathcal{O}_{T\times_S S_i} \to \sigma^*\mathcal{L}_i$, and $\mathcal{L}_i$ is still in the class of s_i.

Let $i, j \in I$, and let $\mathcal{L}'_i$ (resp. $\mathcal{L}'_j$) be the pull-back of $\mathcal{L}_i$ (resp. $\mathcal{L}_j$) under the projection $X \times_S S_i \times_S S_j \to X \times_S S_i$ (resp. $X \times_S S_i \times_S S_j \to X \times_S S_j$): by assumption, there is a line bundle $\mathcal{M}$ on $T \times_S S_i \times_S S_j$ and an isomorphism $\iota_{i,j} : \mathcal{L}'_i \to \mathcal{L}'_j \otimes f^*\mathcal{M}$. After pulling back by $\sigma \times_S S_i \times_S S_j$, we see that $\mathcal{M}$ is trivial. Since $\mathcal{O}_T \to f_*\mathcal{O}_X$ is a universal isomorphism, we may then pick $\iota_{i,j}$ such that the following diagram commutes:

$$\begin{array}{ccc} \mathcal{O}_{T\times_S S_i\times_S S_j} & \xrightarrow{\text{id}} & \mathcal{O}_{T\times_S S_i\times_S S_j} \\ \downarrow \rho_i & & \downarrow \rho_j \\ (\sigma \times S_i \times S_j)^*\mathcal{L}'_i & \xrightarrow{(\sigma^*\times_S S_i\times_S S_j)\iota_{i,j}} & (\sigma \times S_i \times S_j)^*\mathcal{L}'_i \end{array}$$

This rigidification ensures that $(\mathcal{L}_i, \iota_{i,j})$ satisfies a cocycle relation: that is, for every $i, j, k \in I$, if $\mathcal{L}'_i$ now denotes the pull-back of $\mathcal{L}_i$ under $X \times_S S_i \times_S S_j \times_S S_k \to X \times_S S_i$, and similarly for j, k, then $(\iota_{j,k} \times_S S_i) \circ (\iota_{i,j} \times_S S_k) = (\iota_{i,k} \times S_j)$. Thus, this collection defines a line bundle on the small fppf site of X, which must therefore come from a (Zariski) line bundle on X by descent [4, Proposition 023T]. The desired class s is exactly the class of this line bundle. □

Proposition A.4.23 *Let $f : X \to Y$ be a finite locally free morphism of proper finitely presented S-schemes. Then f induces functorial homomorphisms of pre-sheaves of abelian groups $f^* : P_{Y/S} \to P_{X/S}, [f_*] : P_{X/S} \to P_{Y/S}$. If f has constant rank d, one has $[f_*]f^* = d$. If X, Y have pure fibres (over S) of dimension one, $f^*, [f_*]$ induce morphisms between the P^0.*

Proof. – The construction of the morphisms of pre-sheaves is a consequence of Proposition A.4.7, using Lemma A.4.15 to check that both morphisms preserve the sub-presheaf P^0 when the fibres of $X \to S, Y \to S$ are pure of dimension one. If f has constant rank d, it is enough to show

that $[f_*]f^* \in \mathrm{End}(\mathrm{Pic}(Y))$ is the multiplication by d. If $\mathcal{L}$ is a line bundle on Y, then, by the projection formula,

$$\begin{aligned}[f_*]f^*\mathcal{L} &\simeq \det f_*f^*\mathcal{L} \otimes (\det f_*\mathcal{O}_X)^{-1} \simeq \det(\mathcal{L} \otimes f_*\mathcal{O}_X) \otimes (\det f_*\mathcal{O}_X)^{-1} \\ &\simeq \mathcal{L}^{\otimes d} \otimes \det f_*\mathcal{O}_X \otimes (\det f_*\mathcal{O}_X)^{-1} \simeq \mathcal{L}^{\otimes d}.\end{aligned}$$

□

Lemma A.4.24 *Let X be a proper finitely presented S-scheme, and $i_1, \dots, i_r$ be closed open immersions $X_i \to X$, such that X is the disjoint reunion of the $i_j(X_j)$. Then*

$$(i_1^*, \dots, i_r^*) : P_{X/S} \to \bigoplus_{j=1}^{r} P_{X_j/S}$$

is an isomorphism. Its inverse is the sum of the $[(i_j)_*]$.

Proof. – This is a formal verification. □

Proposition A.4.25 *In the situation of Proposition A.4.10, assume that all maps are morphisms of proper finitely presented S-schemes. Then $u^*[(f')_*]$ and $[f_*]v^*$ both define morphisms of functors $P^{Y'/S} \to P^{X/S}$ mapping $P^0_{Y'/S}$ to $P^0_{X/S}$. These morphisms are equal if there is an open subscheme $\iota : U \to X'$ such that, for any S-scheme T, $\mathcal{O}_{X_T} \to (\iota_T)_*\mathcal{O}_{U_T}$ is injective.*

Proof. – This is a direct consequence of Proposition A.4.10 using Proposition A.4.23. □

Lemma A.4.26 *If $\pi : C \to S$ is flat proper of relative dimension one with geometrically reduced fibres and surjective over a locally Noetherian scheme, then π is a relative curve.*

Proof. – By [66, (7.8.6-7), (7.7.5.3)], $\pi_*\mathcal{O}_C$ is a coherent locally free $\mathcal{O}_S$-algebra and its formation commutes with any base change. Let S' be the relative spectrum of $\pi_*\mathcal{O}_C$ over S, so that $C \to S' \to S$ is the Stein factorization of π by [4, Theorem 03H0].

Let us show that S' is finite étale over S (in particular reduced locally Noetherian). We already saw that S' was finite flat over S. To prove that it is étale, since the formation of $\pi_*\mathcal{O}_C$ commutes with arbitrary base change, we may assume that S is the spectrum of an algebraically closed field k. Then $\mathcal{O}(C)$ is a finite reduced k-algebra, hence is an unramified k-algebra, whence the conclusion. □

Lemma A.4.27 *Let $\pi : C \to S$ be a relative curve. Then, fppf-locally over S, C is the disjoint reunion of flat proper S-schemes C_i with geometrically connected fibres and such that $C_i(S) \neq \varnothing$.*

Proof. – Let $C \to S' \to S$ denote the Stein factorization; by working Zariski-locally over S, we may assume that $S' \to S$ has constant rank r. Let T be any flat finitely presented S-scheme. By Proposition A.4.21, $C_T \to T$ is a disjoint union of flat proper T-schemes $C_{T,i}$ with geometrically connected fibres and such that $C_{T,i}(T)$ is nonempty if, and only if, $S' \times_S T$ is (as a T-scheme) the disjoint reunion of closed open subschemes of T and $C \times_S T \to S' \times_S T$ has a nonempty section.

By [4, Lemma 04HN], there exists a fppf-covering family $T_i \to S$ by affine schemes such that $S' \times_S T_i$ is, as a T_i-scheme, the disjoint reunion of finitely many copies of T_i. So, after replacing S with any T_i, we may assume that S is affine and S' is (as a S-scheme) the disjoint reunion of finitely many copies of S, called S_i for $1 \leq i \leq r$. Let $C_i = C \times_{S'} S_i$: it is a proper flat S-scheme with geometrically connected fibres.

Now, for a S-scheme T, the morphism $C \times_S T \to S' \times_S T$ has a section if and only if, for every i, the morphism $C_i \times_S T \to T$ has a section. By [67, Corollaire (17.16.2)], there is a faithfully flat quasi-finite finitely presented affine S-scheme T_i such that $C_i \times_S T_i \to T_i$ has a section. Let T be the fibre product of the T_i over S (for $1 \leq i \leq r$): then T is a faithfully flat quasi-finite finitely presented affine S-scheme and $C_i \times_S T \to T$ has a section for all i, whence the conclusion.

□

Proposition A.4.28 *Let $\pi : C \to S$ be a smooth relative curve and $C \xrightarrow{f} T \to S$ be its Stein factorization. The sheaf* $\mathrm{Pic}^0_{C/S}$ *is representable by an Abelian scheme over S, the* relative Jacobian *of J of C/S, whose construction commutes with any base change with respect to S.*

Proof. – We will use the presheaves P', P'^0 introduced in Proposition A.4.22.

Since $f : C \to T$ is proper smooth with geometrically connected fibres, the fppf sheaf $\mathrm{Pic}^0_{C/T}$ is, by [15, §9.4, Proposition 4], representable by an Abelian T-scheme J_0. It is a direct verification that $P'_{C/S}$ is the push-forward under $T \to S$ of $P'_{C/T}$, that is, that $P'_{C/S}(-) \simeq P'_{C/T}(- \times_S T)$. Moroever, it is clear using Lemma A.4.14 that this isomorphism preserves the sub-presheaf P'^0.

Thus, there is formally a natural transformation $\Lambda : P'_{C/S}(-) \Rightarrow \mathrm{Pic}_{C/T}(- \times_S T)$ (preserving the degree-zero subfunctor). Since the Weil restriction commutes with any base change [15, §7.6, p. 192], for any S-scheme S' such that $C_{S'} \to T \times_S S'$ has a section, Λ is an isomorphism when restricted to the full subcategory of $\mathbf{Sch}_S$ whose objects are schemes that admit a S-morphism to S'.

Let us prove that S has a fppf cover by S-schemes S_i such that $C \times_S S_i \to T \times_S S_i$ has a section. By [4, Lemma 04HN], after replacing S with a jointly surjective collection of étale maps, we can assume that T is the disjoint union of copies of S, so that C is the disjoint reunion of smooth relative curves $f_i : C_i \to S$ with geometrically connected fibres. We are then done if, fppf locally on S, each f_i admits a section. This is classical, see for instance [67, Corollaire (17.16.3)].

Since, by [15, §7.6, Proposition 3], $\mathrm{Pic}_{C/T}(- \times_S T)$ is a fppf sheaf on $\mathbf{Sch}_S$, Λ is thus a sheafification map. Hence, $\mathrm{Pic}^0_{C/S}$ is representable (by an Abelian S-scheme) iff $J_0(T \times_S -)$ is representable (by an Abelian S-scheme).

For any $s \in S$, since T is étale over S, $T_{\kappa(s)}$ is a finite discrete reunion of residue fields of points of T. Then $(J_0)_{\kappa(s)} = J_0 \times_T T_{\kappa(s)}$ is a finite disjoint reunion of Abelian varieties over some finite extensions of $\kappa(s)$. In particular, any finite subset of points in $(J_0)_{\kappa(s)}$ is contained in an affine open subset. Since $T \to S$ is finite locally free, the Weil restriction is representable by Proposition [15, §7.6, Theorem 4] by some S-scheme J.

Let S' be any S-scheme, and let $S_i \to S$ be the fppf cover discussed above such that each $C \times_S S_i \to T \times_S S_i$ has a section.

There is a natural morphism $\mathrm{Pic}^0_{C\times_S S'/S'} \Rightarrow \mathrm{Pic}^0_{C/S}$ of fppf sheaves on $\mathbf{Sch}_{S'}$ obtained by sheafifying the natural composition $P^0_{C\times_S S'/S'} \simeq P^0_{C/S}(\omega) \Rightarrow \mathrm{Pic}^0_{C/S}(\omega)$, where $\omega : \mathbf{Sch}_{S'} \to \mathbf{Sch}_S$ is the forgetful functor. So we have a natural map $\beta_{S'/S} : J_{C\times_S S'/S'} \to J_{C/S} \times_S S'$.

Note that this map is an isomorphism by the properties of sheafification if S' is flat and locally of finite presentation over S, or if $C(T)$ has a section (since in this case P^0 is a sheaf). It follows that every $\beta_{S'/S} \times_S S_i$ is an isomorphism, so $\beta_{S'/S}$ is an isomorphism. Therefore, the formation of $\mathrm{Pic}^0_{C/S}$ commutes with base change.

Since $\mathrm{Pic}^0_{C/S}$ is a functor in Abelian groups, J is naturally a commutative group scheme over S. By [15, §7.6, Proposition 5], J is proper smooth over S, thus, to prove that it is an Abelian scheme, all we need to do is prove that its fibres are connected. Since the construction commutes with base change, we may assume that S is the spectrum of an algebraically closed field k, so that T is a finite disjoint union of copies of $\operatorname{Spec} k$. Then C is the disjoint reunion of smooth projective connected curves C_i over k, and that as abelian fppf-sheaves, so, by Lemma A.4.24, $P^0_{C/\operatorname{Spec} k}$ is isomorphic to the direct sum of the $P^0_{C_i/\operatorname{Spec} k}$. The associated sheaf is represented by the direct product of the (classically) well-defined Jacobians J_i of the C_i, which are known to be Abelian varieties over k (for instance [15, §9.4, Theorem 4]), hence their product is an Abelian variety over k as well. □

Proposition A.4.29 *Let $\pi : C \to S$ be a smooth relative curve with Stein factorization $C \xrightarrow{f} T \to S$ and relative Jacobian J. There exists a difference map $\delta : C \times_T C \to J$ such*

that the following diagrams commute:

$$\begin{array}{ccc} C & \xrightarrow{(\mathrm{id},\mathrm{id})} & C \times_T C \\ \downarrow{\scriptstyle 0} & \swarrow{\scriptstyle \delta} & \\ J & & \end{array} \qquad \begin{array}{ccc} C \times_T C \times_T C & \xrightarrow{((p_1,p_2),(p_2,p_3))} & (C \times_T C) \times_S (C \times_T C) \\ \downarrow{\scriptstyle (p_1,p_3)} & & \downarrow{\scriptstyle (\delta,\delta)} \\ C \times_T C & \xrightarrow{\delta} J \xleftarrow[\delta]{} & J \times_S J. \end{array}$$

and such that moreover, for any geometric points $x_1, x_2 : S' \to C$ with $f(x_1) = f(x_2)$, $\delta(x_1 - x_2)$ is the class of the line bundle $\mathcal{L} = \mathcal{I}_{x_2} \otimes \mathcal{I}_{x_1}^{-1}$ where $\mathcal{I}_{x_i}$ is the sheaf of ideals attached to the relative effective Cartier divisor for $C_{S'} \to S'$ defined by the section x_i (see [4, Definition 062T]).

In particular, if S is an algebraically closed field, then $\mathcal{L}$ is the line bundle on X which is trivial outside the connected component containing x_1, x_2 and attached to the Weil divisor $[x_1] - [x_2]$ on this component.

Proof. – If the general definition is correct, the rest of the statements follows easily. So we need to show that the sections x_i define relative effective Cartier divisors and that $\mathcal{L}$ has fibrewise degree zero. The first part follows from [86, Lemma 1.2.2], and the second part is [86, Lemma 1.2.7] using the fact that degrees are additive. □

Proposition A.4.30 *Let $\pi : C \to S$ be a smooth relative curve with Stein factorization $C \xrightarrow{f} T \to S$ and relative Jacobian $J \to S$. Assume that $C \to S$ has a bounded above genus g (for instance if S is quasi-compact). Let $\delta : C \times_T C \to J$ be the difference map. Then the product over S of g copies of the difference function $\delta^g : (C \times_T C)^g \to J$ is surjective.*

Proof. – By Lemma A.4.27, after replacing S with a fppf-covering, we may assume that C is a disjoint reunion of smooth proper S-schemes C_i of relative dimension one such that $C_i \to S$ has a section and the fibres of $C_i \to S$ have genus at most g. In particular, the relative Jacobian J_i of each C_i/S is well-defined, and all we need to show is that for every i, $\delta^g : (C_i \times_S C_i)^g \to J_i$ is surjective.

This can be verified on the fibres of these two S-schemes, so we may assume that S is the spectrum of an algebraically closed field and that C is connected. By [15, §9.3, Lemma 6], the image of δ^g contains an open subscheme of J. Since δ^g is a morphism between two proper S-schemes, it has closed image, hence it is surjective. □

Corollary A.4.31 *In the situation of Proposition A.4.23, assume that X, Y are smooth and that the push-forward by f is well-defined. Then, if J_X, J_Y denote the Jacobians and δ_X, δ_Y the difference maps, the following diagram commutes:*

$$\begin{array}{ccc} X \times_{T_X} X & \xrightarrow{f \times f} & Y \times_{T_Y} Y \\ \downarrow{\scriptstyle \delta_X} & & \downarrow{\scriptstyle \delta_Y} \\ J_X & \xrightarrow{[f_*]} & J_Y \end{array}$$

Proof. – This amounts to proving the following variant of Lemma A.4.8. Let $f : X \to Y$ be a finite locally free morphism of relative curves over S and let $s \in X(S)$. Then $[f_*]$ maps the ideal attached to the relative effective Cartier divisor s to the ideal attached to the relative effective Cartier divisor defined by $f(s) \in Y(S)$.

This statement can in turn easily be reduced to the following situation, using Lemma A.4.3: let R be a ring and B be a finite locally free A-algebra, where A, B are smooth of relative dimension one over R. Let $I \subset B$ be an ideal such that $R \to B/I$ is an isomorphism, then I is locally principal, the kernel of $A \to B/I$ is a locally principal ideal J generated by the $N_{B/A}(x)$ for $x \in I$, and $R \to A/J$ is an isomorphism.

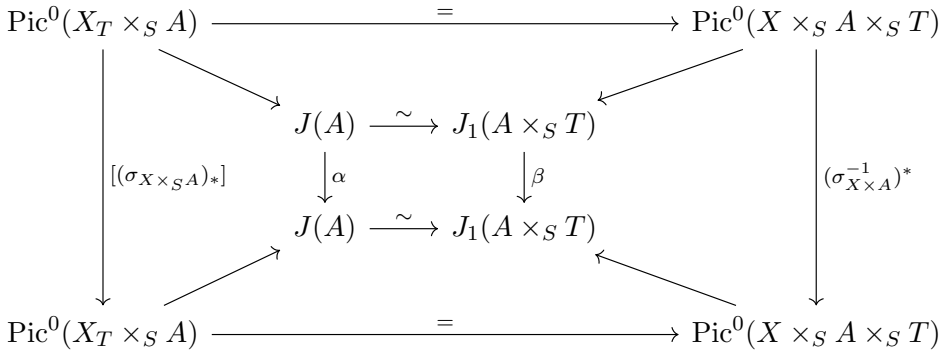
The ideals I, J are locally principal and generated by regular elements due to [86, Lemma 1.2.2], and the fact that $R \to A/J$ is an isomorphism is formal; in particular, $A/J \to B/I$ is an isomorphism. So the only remaining statement is the one about the norm. We can work Zariski-locally on A, and thus assume that B is free over A of finite rank, I is generated by some regular element $g \in B$, and J by some regular element $h \in A$. Since $A/J \to B/I$ is still an isomorphism, its zero-th Fitting ideal is both $hA = J$ and $N_{B/A}(g)A$, whence the conclusion is [4, Lemma 07Z8]. □

Proposition A.4.32 *Let $X \to S$ be a relative curve with geometrically connected fibres and σ be an S-automorphism of some finite étale S-scheme T. Let J_1 be the relative Jacobian of $X \to S$, and J be the relative Jacobian of $X_T \to S$. For any S-scheme A, the following diagram commutes:*

$$\begin{array}{ccc} J(A) & \xrightarrow{\sim} & J_1(A \times_S T) \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ J(A) & \xrightarrow{\sim} & J_1(A \times_S T) \end{array}$$

In this diagram, the horizontal arrows are given by the fact that J is the restriction of scalars of $J_1 \times_S T$ over T/S (by Proposition A.4.28), α is the pushforward of $\mathrm{id} \times \sigma : X \times_S T \to X \times_S T$, and $\beta : f \longmapsto f \circ (\mathrm{id} \circ \sigma^{-1})$.

Proof. – This statement is fppf-local with respect to A, so we may assume by [67, Corollaire (17.16.2)] that $X \to S$ has a section. Therefore, in the following diagram, the diagonal maps are surjective by Proposition A.4.22:



By definition of J and J_1, the leftmost and rightmost cells commute. The top and bottom cells commute by the proof of Proposition A.4.28. We can check that the outer cell commutes. Therefore the inner cell commutes.

□

A.4.3 Holomorphic differentials on the Jacobian of a curve

Proposition A.4.33 *Let $f : G \to S$ be an Abelian scheme over a locally Noetherian scheme S. Then $f_*\Omega^1_{G/S}$ is a locally free $\mathcal{O}_S$-module, its sections are translation-invariant differential forms on G_U/U (for open subschemes $U \subset S$) and its formation commutes with base change. Moreover, $\mathrm{End}_S(G)$ acts on the right on $f_*\Omega^1_{G/S}$.*

Proof. – This is essentially the proof of [15, §4.2 Proposition 1], but the argument is easier in this case.

Because f is smooth, $\Omega^1_{G/S}$ is locally free of rank d. Let $e : S \to G$ be the unit section.

Let us prove that for any locally free $\mathcal{O}_S$-module $\mathcal{F}$ of finite rank, the morphism $\mathcal{F} \to f_*f^*\mathcal{F}$ is an isomorphism. The statement is Zariski-local over S, it is enough to prove that $\mathcal{O}_S \to f_*\mathcal{O}_G$ is an isomorphism. Because f is proper flat with geometrically reduced fibres, by [66, (7.8.6-7),

(7.7.5.3)], $f_*\mathcal{O}_G$ is a coherent locally free $\mathcal{O}_S$-algebra and its formation commutes with any base change. Since f has geometrically connected fibres, $\mathcal{O}_S \to f_*\mathcal{O}_G$ becomes an isomorphism after any base change to a geometric fibre. Hence $\mathcal{O}_S \to f_*\mathcal{O}_G$ is an isomorphism.

Let $m, p_1, p_2 : G \times_S G \to S$ denote the product, the first and second projections respectively. Let us prove that, for any open subscheme $U \subset S$ and any $\omega \in \Omega^1_{G/S}(G_U)$, one has $m^*\omega = p_1^*\omega + p_2^*\omega$. We can and do assume $S = U$. Moreover, we also know by [15, §2.1 Proposition 4] that $H^0(G \times_S G, \Omega^1_{G\times_S G/S}) = \bigoplus_{i=1}^2 H^0(G \times_S G, p_i^*\Omega^1_{G/S})$.

Now, $H^0(G \times_S G, p_i^*\Omega^1_{G/S}) \simeq H^0(G, (p_i)_*p_i^*\Omega^1_{G/S})$; since $p_i : G \times_S G \to G$ is an Abelian scheme, one has $(p_i)_*p_i^*\Omega^1_{G/S} \simeq \Omega^1_{G/S}$, hence $H^0(G \times_S G, \Omega^1_{G\times_S G/S}) \simeq \bigoplus_{i=1}^2 p_i^* H^0(G, \Omega^1_{G/S})$.

In particular, we can write $m^*\omega = p_1^*\omega_1 + p_2^*\omega_2$ for $\omega_1, \omega_2 \in H^0(G, \Omega^1_{G/S})$. By pulling back by $(\mathrm{id}, 0)$ (resp. $(0, \mathrm{id})$) one sees that $\omega_1 = \omega_2 = \omega$. This implies that $\mathrm{End}_S(G)$ acts on the right on $f_*\Omega^1_{G/S}$, and that any global differential on G/S is translation-invariant.

Now, it remains to prove that $f_*\Omega^1_{G/S}$ is a locally free $\mathcal{O}_S$-module and that its formation commutes with base change. Indeed, by [105, Proposition 1.1 (b)], there is a natural isomorphism $f^*e^*\Omega^1_{G/S} \to \Omega^1_{G/S}$. Applying f_*, one gets a natural isomorphism $e^*\Omega^1_{G/S} \to f_*\Omega^1_{G/S}$, hence $f_*\Omega^1_{G/S}$ is locally free of rank $\dim(A/S)$. Since the formation of $e^*\Omega^1_{G/S}$ commutes with base change, the same holds for $f_*\Omega^1_{G/S}$, whence the conclusion. □

Proposition A.4.34 *Let $f : X \to S$ be a smooth relative curve over a Noetherian scheme S and $\mathcal{F}$ be a locally free coherent sheaf over X. For every $j \geq 0$, $R^j f_*\mathcal{F}$ is a locally free coherent $\mathcal{O}_S$-module whose formation commutes with an arbitrary base change of locally Noetherian schemes. Moreover, for $j \in \{0, 1\}$, there is a natural isomorphism*

$$R^{1-j} f_*(\mathcal{F}^\vee \otimes \Omega^1_{X/S}) \to \underline{Hom}_{\mathcal{O}_Y}(R^j f_*\mathcal{F}, \mathcal{O}_X).$$

Proof. – First, let $\mathcal{F}$ be a locally free coherent sheaf on X. By [93, Lemma 3], one has $R^i f_*\mathcal{F} = 0$ for every $i \geq 2$ (and this holds for every base change of f to another locally Noetherian scheme). Apply [31, Lemma 5.1.1] with $m = 1$, this implies that the formation of $R^1 f_*\mathcal{F}$ commutes with base change of locally Noetherian schemes. Moreover, apply [31, Theorem 5.1.2] with $m = 1$: the formation of $f_*(\mathcal{F}^\vee \otimes \Omega^1_{X/S})$ commutes with base change (since the dualizing sheaf for a smooth relative curve identifies with the sheaf of differentials, see the discussion after [31, Corollary 3.5.2]). Since $\mathcal{F}$ was assumed to be locally free and coherent, this means that for every locally free coherent sheaf $\mathcal{F}$ on X, and every $i \geq 0$ (hence for every $i \in \mathbb{Z}$), the formation of $R^i f_*\mathcal{F}$ commutes with base change. By [31, Lemma 5.1.1], this implies that $R^i f_*\mathcal{F}$ is a locally free coherent $\mathcal{O}_S$-module for every $i \in \mathbb{Z}$. The conclusion then follows from re-applying [31, Theorem 5.1.2]. □

Proposition A.4.35 *Let $f : X \to S$ be a smooth relative curve over a locally Noetherian scheme S with relative Jacobian $F : J \to S$. There is an isomorphism $\rho_X : F_*\Omega^1_{J/S} \to f_*\Omega^1_{X/S}$ whose formation commutes with base change and satisfies the following property: let $X \to S' \to S$ be the Stein factorization, T be a Noetherian S-scheme and $x : T \to X$ be a morphism of S-schemes, thus making T a S'-scheme. Then $F_*\Omega^1_{J_T/T} \overset{\rho_{X\times_S T}}{\to} f_*\Omega^1_{X_T/T} \to f_*\Omega^1_{(X\times_{S'} T)/T}$ is exactly given by the restriction through the "difference to x" map $\Delta(\cdot, x) : X \times_{S'} T \to J \times_S T$. In particular, the formation of ρ_X commutes with base change.*

Moreover, if $g : Y \to S$ is a smooth relative curve and with Jacobian $G : J' \to S$ and

$h : X \to Y$ is finite locally free, then the following diagram commutes:

$$\begin{array}{ccc} G_*\Omega^1_{J'/S} & \xrightarrow{\rho_Y} & g_*\Omega^1_{Y/S} \\ \downarrow{\scriptstyle [h_*]^*} & & \downarrow{\scriptstyle h^*} \\ F_*\Omega^1_{J/S} & \xrightarrow{\rho_X} & f_*\Omega^1_{X/S} \end{array}$$

Proof. – It is enough to prove the result when S is Noetherian.

Let $(S_i)_i$ be an fppf-covering of S. If either part of the claim holds after making a base change to each S_i and each $S_i \times_S S_j$, then the claim holds over S, by descent.

Let us first assume that f has geometrically connected fibres. Then, the first part of the claim is the content of [31, (B.4.5)] and its discussion, because all the global differentials on (base changes of) J/S are translation-invariant by [15, §4.2, Corollary 3]. The second part of the claim (when g has geometrically connected fibres) clearly holds when $X(S)$ is not empty by definition of ρ_X, ρ_Y and Corollary A.4.31.

Therefore, the first part of the claim (resp. the second part of the claim) remains true whenever X is (resp. X, Y are) the reunion of several smooth proper S-schemes X_i (resp. X_i, Y_i) of relative dimension one with geometrically connected fibres such that $X_i(S) \neq \varnothing$ for every i (resp. $X_i(S) \neq \varnothing, Y_i(S) \neq \varnothing$ for every i).

The general case reduces to this special case after an fppf base change by Lemma A.4.27. □

Corollary A.4.36 *Let $f : X \to S$ be a smooth relative curve over a locally Noetherian scheme with relative Jacobian J. Then $f_*\Omega^1_{X/S}$ is endowed with a natural structure of sheaf of right* $\mathrm{End}_S(J)$*-modules.*

Proof. – This is direct. □

Definition A.4.37 Let $f : X \to S$, $g : Y \to S$ be smooth relative curves over a locally Noetherian base scheme S with relative Jacobians $F : J_X \to S, G : J_Y \to S$, and let $h : X \to Y$ be a finite locally morphism of S-schemes. The trace map attached to h is the natural map $\mathrm{Tr}_h : f_*\Omega^1_{X/S} \to g_*\Omega^1_{Y/S}$ such that the following diagram commutes.

$$\begin{array}{ccc} F_*\Omega^1_{J_X/S} & \xrightarrow{\rho_X} & f_*\Omega^1_{X/S} \\ \downarrow{\scriptstyle (h^*)^*} & & \downarrow{\scriptstyle \mathrm{Tr}_h} \\ G_*\Omega^1_{J_Y/S} & \xrightarrow{\rho_Y} & g_*\Omega^1_{Y/S}. \end{array}$$

Proposition A.4.38 *In the notation of Definition A.4.37, the formation of* Tr_h *commutes with base change and it is functorial in h. Moreover, this trace map is the image on global sections of the usual trace map $h_*\Omega^1_{X/S} \to \Omega^1_{Y/S}$ coming from duality theory [31, (2.7.36)] given on an affine open $U \subset Y$ by $a \cdot d(h^*(b)) \in \Omega^1_{X/S}(h^{-1}(U)) \longmapsto \mathrm{Tr}_{\mathcal{O}_X(h^{-1}(U))/\mathcal{O}_Y(U)}(a) \cdot db \in \Omega^1_{Y/S}$.*

Proof. – The first part of the claim is direct. Let $\mathrm{Tr}^\delta : f_*\Omega^1_{X/S} \to g_*\Omega^1_{Y/S}$ denote the map coming from Definition A.4.37 and $\mathrm{Tr}^\theta : h_*\Omega^1_{X/S} \to \Omega^1_{Y/S}$ the map coming from duality. The formula we have written is correct by the explicit computation in [31, (2.7.41)].

We want to show that $\mathrm{Tr}^\delta = g_*\mathrm{Tr}^\theta$. The formation of both Tr^δ and $g_*\mathrm{Tr}^\theta$ commutes with base change with respect to S and is fppf-local with respect to S, so, by Lemma A.4.27, so we may assume that S is affine, connected, and X, Y are reunions of smooth proper S-schemes of relative dimension one with geometrically connected fibres and nontrivial sections.

It is enough to check the identity on every pair $h : X' \to Y'$ separately, where $X' \to X, Y' \to Y$ are closed open subschemes such that the geometric fibres of $X' \to S$, $Y' \to S$ are connected, so we may and do assume that $X \to S, Y \to S$ have geometrically connected fibres. In particular, $\mathcal{O}_S \to g_*\mathcal{O}_Y \to f_*\mathcal{O}_X$ are isomorphisms, thus, by [93, (1.1)], $R^1f_*\Omega^1_{X/S}, R^1g_*\Omega^1_{Y/S}$ are free $\mathcal{O}_S$-modules of rank one.

Write $h^\sharp$ for the morphism $\mathcal{O}_Y \to h_*\mathcal{O}_X$ induced by h, and let $R^1(h)$ denote the composition

$$R^1g_*\mathcal{O}_Y \xrightarrow{(R^1g_*)(h^\sharp)} (R^1g_*)(h_*\mathcal{O}_X) \xrightarrow{\sim} R^1(g_* \circ h_*)\mathcal{O}_X = R^1f_*\mathcal{O}_X,$$

where the second map is an isomorphism because h is finite.

Take the dual for Grothendieck duality of the diagram in [105, Proposition 1.3(c)]: by [31, Theorem B.4.1], this diagram is of the form

$$\begin{array}{ccc} F_*\Omega^1_{J_X/S} & \xrightarrow{\rho_X} & f_*\Omega^1_{X/S} \\ \downarrow{\scriptstyle (h^*)^*} & & \downarrow{\scriptstyle (R^1(h))^\vee} \\ G_*\Omega^1_{J_Y/S} & \xrightarrow{\rho_Y} & g_*\Omega^1_{Y/S} \end{array}$$

In particular, Tr^δ is equal to $(R^1(h))^\vee$. We want to show that $(R^1(h))^\vee$ is equal to Tr^θ. The adjoint for Grothendieck duality of $(R^1g_*)(h^\sharp)$ is the morphism $g_*\underline{\mathrm{Hom}}_Y(h_*\mathcal{O}_X, \Omega^1_{Y/S}) \to g_*\Omega^1_{Y/S}$ of evaluation at one. To prove the claim, it is thus enough to show that there exists an isomorphism $\iota : f_*\Omega^1_{X/S} \to g_*\underline{\mathrm{Hom}}_Y(h_*\mathcal{O}_X, \Omega^1_{Y/S})$ such that $\mathrm{ev}_{1\in(h_*\mathcal{O}_X)(Y)} \circ \iota = \mathrm{Tr}^\theta$ and the following diagram commutes:

$$\begin{array}{ccc} (R^1g_*)(h_*\mathcal{O}_X) & \longrightarrow & \mathrm{Hom}(g_*\underline{\mathrm{Hom}}_Y(h_*\mathcal{O}_X, \Omega^1_{Y/S}), \mathcal{O}_S) \\ \downarrow & & \downarrow{\scriptstyle \iota^*} \\ R^1f_*\mathcal{O}_X & \longrightarrow & \mathrm{Hom}(f_*\Omega^1_{X/S}, \mathcal{O}_S). \end{array}$$

Consider the following commutative diagram, as in the proof of [93, Theorem 15][7]:

$$\begin{array}{ccc} g_*\underline{\mathrm{Hom}}_Y(h_*\mathcal{O}_X, \Omega^1_{Y/S}) & \xrightarrow{\cup} & \underline{\mathrm{Hom}}_S((R^1g_*)(h_*\mathcal{O}_X), R^1g_*\Omega^1_{Y/S}) \\ \downarrow\sim & & \downarrow\sim \\ g_*\underline{\mathrm{Hom}}_Y(h_*\mathcal{O}_X, g^!\mathcal{O}_S) & \xrightarrow{\cup} & \underline{\mathrm{Hom}}_S((R^1g_*)(h_*\mathcal{O}_X), R^1g_*g^!\mathcal{O}_S) \\ \downarrow\sim & & \downarrow{\scriptstyle \mathrm{Tr}_g} \\ \underline{\mathrm{Hom}}_S((R^1g_*)(h_*\mathcal{O}_X), \mathcal{O}_S) & \xrightarrow{\cup} & \underline{\mathrm{Hom}}_S((R^1g_*)(h_*\mathcal{O}_X), \mathcal{O}_S) \\ \downarrow\sim & & \downarrow\sim \\ \underline{\mathrm{Hom}}_S(R^1f_*\mathcal{O}_X, \mathcal{O}_S) & \xrightarrow{\cup} & \underline{\mathrm{Hom}}_S(R^1f_*\mathcal{O}_X, \mathcal{O}_S) \\ \downarrow\sim & & \uparrow{\scriptstyle \mathrm{Tr}_f} \\ f_*f^!\mathcal{O}_S & \xrightarrow{\cup} & \underline{\mathrm{Hom}}_S(R^1f_*\mathcal{O}_X, R^1f_*f^!\mathcal{O}_S) \\ \downarrow\sim & & \uparrow\sim \\ f_*\Omega^1_{X/S} & \xrightarrow{\cup} & \underline{\mathrm{Hom}}_S(R^1f_*\mathcal{O}_X, R^1f_*\Omega^1_{X/S}) \end{array}$$

[7] The analogue of $f^!, g^!$ in [31] is given by $f^\sharp, g^\sharp$; the difference is that *loc.cit.* works in the derived category, shifts the complexes and possibly uses different sign conventions. All of these changes cancel out in the final result, since we are working with a finite map of smooth relative curves.

Its first column defines an isomorphism $\iota : f_*\Omega^1_{X/S} \to g_*\underline{\mathrm{Hom}}_Y(h_*\mathcal{O}_X, \Omega^1_{Y/S})$ which is indeed adjoint to the isomorphism $(R^1g_*)(h_*\mathcal{O}_X) \simeq R^1f_*\mathcal{O}_X$. All we need to do is check that the evaluation of ι at $1 \in (h_*\mathcal{O}_X)(Y)$ is exactly the trace homomorphism.

By construction, $\mathrm{Tr}^\delta : h_*\Omega^1_{X/S} \to \Omega^1_{Y/S}$ is the unique morphism such that

$$(R^1g_*)\mathrm{Tr}^\delta : (R^1g_*)(h_*\Omega^1_{X/S}) \to R^1g_*\Omega^1_{Y/S}$$

induces the identity map on $\mathcal{O}_S$ after identifying

$$(R^1g_*)(h_*\Omega^1_{X/S}) \simeq R^1f_*\Omega^1_{X/S} \simeq \mathcal{O}_S, R^1g_*\Omega^1_{Y/S} \simeq \mathcal{O}_S.$$

Now, for any quasi-coherent sheaf $\mathcal{G}$ on X, consider as in the proof of [93, Theorem 15] the following chain of isomorphisms

$$\begin{aligned}\mathrm{Hom}_X(\mathcal{G}, \Omega^1_{X/S}) &\simeq \mathrm{Hom}_X(\mathcal{G}, f^!\mathcal{O}_S) \simeq \mathrm{Hom}_S(R^1f_*\mathcal{G}, \mathcal{O}_S) \simeq \mathrm{Hom}_S((R^1g_*)(h_*\mathcal{G}), \mathcal{O}_S)\\ &\simeq \mathrm{Hom}_Y(h_*\mathcal{G}, g^!\mathcal{O}_S) \simeq \mathrm{Hom}_Y(h_*\mathcal{G}, \Omega^1_{Y/S}).\end{aligned}$$

Moreover, there is a functorial isomorphism

$$\mathrm{Hom}_{h_*\mathcal{O}_X}(h_*\mathcal{G}, \underline{\mathrm{Hom}}_{\mathcal{O}_Y}(h_*\mathcal{O}_X, \Omega^1_{Y/S})) \to \mathrm{Hom}_{\mathcal{O}_Y}(h_*\mathcal{G}, \Omega^1_{Y/S})$$

given by the evaluation at 1. Therefore, if $\tau : h_*\Omega^1_{X/S} \to \Omega^1_{Y/S}$ denotes the image of $\mathrm{id}_{\Omega^1_{X/S}}$ (for $\mathcal{G} = \Omega^1_{X/S}$), then $g_*\tau$ is equal to the composition of ι and the evaluation at 1. It is then easy to check that $R^1g_*\tau = R^1g_*\mathrm{Tr}^\delta$, so $\tau = \mathrm{Tr}^\delta$, whence the conclusion. □

A.4.4 Jacobians and Galois twists

Proposition A.4.39 *Let X be a proper smooth k-scheme of relative dimension one, with Jacobian variety J, where k is a field with separable closure k_s. Let $\rho : \mathrm{Gal}(k_s/k) \to \mathrm{Aut}_{k_s}(X_{k_s})$ be a function satisfying the cocycle relation of Proposition A.1.11. Let $\mathrm{Aut}_{k_s}(X_{k_s})$ act on J by push-forward functoriality. Let $\Delta : X \times_{\mathrm{Spec}\,\mathcal{O}(X)} X \to J$ be the difference morphism, which is equivariant for the action of $\mathrm{Aut}_{k_s}(X_{k_s})$. Then its twist $\Delta_\rho : X_\rho \times_{\mathrm{Spec}\,\mathcal{O}(X_\rho)} X_\rho \to J_\rho$ by ρ identifies J_ρ with the Jacobian variety of X_ρ.*

Proof. – Let $j_X : X_\rho \times_k \mathrm{Spec}\,k_s \to X \times_k \mathrm{Spec}\,k_s$ be the k_s-isomorphism from Proposition A.1.11, J_ρ be the Jacobian variety of X_ρ over k. The formation of J_ρ commutes with base change, so push-forward functoriality yields an isomorphism $j_J : J_\rho \times_k \mathrm{Spec}\,k_s \to J \times_k \mathrm{Spec}\,k_s$ of Abelian varieties over k_s.

The following diagram commutes for each $\sigma \in \mathrm{Gal}(k_s/k)$ by Proposition A.4.25 and the fact that the formation of the Jacobian commutes with base change:

$$\begin{array}{ccc}(J_\rho)_{k_s} & \xrightarrow{j_J} & J_{k_s}\\ \downarrow{\scriptstyle (\mathrm{id},\underline{\sigma^{-1}})} & & \downarrow{\scriptstyle [\rho(\sigma)_*]\circ(\mathrm{id},\underline{\sigma^{-1}})}\\ (J_\rho)_{k_s} & \xrightarrow{j_J} & J_{k_s}\end{array}$$

Therefore, by Proposition A.1.11, (J_ρ, j_J) is the twist of J by ρ. The rest of the statement follows from Proposition A.1.13 and Corollary A.4.31, because the twist of $\mathrm{Spec}\,\mathcal{O}(X)$ by ρ is exactly $\mathrm{Spec}\,\mathcal{O}(X_\rho)$. □

Proposition A.4.40 *Let $f : X \to Y$ be a finite locally free morphism of proper smooth k-schemes of relative dimension one, k being a field with separable closure k_s. Let J_X, J_Y be the Jacobians of X, Y. Let G be a finite group acting on the k_s-schemes X_{k_s}, Y_{k_s} equivariantly for f,*

and let $\rho : \mathrm{Gal}(k_s/k) \to G$ *be a function satisfying the cocycle property when post-composed with the actions of* G *on* X_{k_s} *and* Y_{k_s} *(as in Proposition A.1.13). Then the twist by* ρ *of* $f^* : J_Y \to J_X$ *(resp. the push-forward* $[f_*] : J_X \to J_Y$*) identifies with the pull-back* $(f_\rho)^* : J_{Y_\rho} \to J_{X_\rho}$ *(resp. the push-forward* $[(f_\rho)_*]$*).*

Appendix B

Representations of $\mathrm{GL}_2(\mathbb{F}_p)$.

The purpose of this Appendix is to recall the representation theory of $G = \mathrm{GL}_2(\mathbb{F}_p)$ when $p \geq 5$. Most of the following is well-known, but is worth stating in full for its applications to the main work. We follow mainly [81], [11] and [21, §6].

Notation

- $B \leq \mathrm{GL}_2(\mathbb{F}_p)$ *is the subgroup of upper-triangular matrices,*
- $U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $W = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$,
- $S' = \{W\} \cup \{T^t,\, t \in \mathbb{F}_p\}$ *is a natural system of representatives for* G/B,
- *given* $a, b \in \mathbb{F}_p^\times$, *we write* $\Delta_{a,b} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$.

The following relations hold:

$$\begin{aligned} a,b,t \in \mathbb{F}_p^\times : \quad & \Delta_{a,b} T^t = T^{tb/a} \Delta_{a,b}\,; && \Delta_{a,b} W = W \Delta_{b,a} \\ s,t \in \mathbb{F}_p, u := st+1 \neq 0 : \quad & U^s T^t = T^{t/(1+st)} \begin{pmatrix} u & s \\ 0 & u^{-1} \end{pmatrix} && \\ s \in \mathbb{F}_p^\times : \quad & U^s T^{-1/s} = W \begin{pmatrix} -s^{-1} & 1 \\ 0 & -s \end{pmatrix}; && U^s W = T^{1/s} \begin{pmatrix} s & -1 \\ 0 & s^{-1} \end{pmatrix} \end{aligned}$$

If V is a free R-module with finite rank on which G acts on the left (resp. right), V^* denotes the contragredient, that is, $V^* = \mathrm{Hom}_R(V, R)$, where $g \cdot f = f(g^{-1}\cdot)$. It is still a left (resp. right) representation of G. Let $V^{\circ *}$ denote the left (resp. right) R-module V on which every $g \in G$ acts as $(g^{-1})^T$. Finally, $V^\vee$ denotes the *right* (resp. *left*) representation of G given by $\mathrm{Hom}_R(V, R)$, where $f \cdot g = f(g\cdot)$.

Lemma B.0.1 *Let M be a left $R[G]$-module and $\chi : \mathbb{F}_p^\times \to R^\times$ be such that for every $n \in \mathbb{F}_p^\times$, nI_2 acts on M by multiplication by $\chi(n)$. Then $M^{\circ *} \simeq M \otimes \chi^{-1}(\det)$.*

Proof. – Consider the function $f : x \in M^{\circ *} \longmapsto (W \cdot_M x) \in M \otimes \chi^{-1}(\det)$, which is clearly an isomorphism of R-modules. For any $g \in G$, any $x \in M^{\circ *}$, one has

$$\begin{aligned} f(g \cdot_{M^{\circ *}} x) &= f((g^T)^{-1} \cdot_M x) = f((\det g^{-1} I_2) W^{-1} g W \cdot_M x) = \chi(\det g)^{-1} W \cdot_M (W^{-1} g W \cdot_M x) \\ &= \det g^{-1} g \cdot_M (Wx) = g \cdot_{M \otimes \chi^{-1}(\det)} f(x), \end{aligned}$$

whence the conclusion. □

B.1 Principal series representations

Let R be a $\mathbb{Z}\left[\frac{1}{p^2-1}, \mu_{p-1}\right]$-algebra without nontrivial idempotents. In particular, if $\omega \in R^\times$ is such that $\omega^{p-1} = 1$, then either $\omega = 1$ or $\omega - 1$ is invertible. Indeed, we can find polynomials $A, B \in \mathbb{Z}\left[\frac{1}{p-1}, X\right]$ such that $A(X)(X^{p-1}-1)+B(X)(X-1)^2 = X-1$. Thus $B(\omega)(\omega-1)^2 = \omega-1$, so that, if $\omega \neq 1$, then $(\omega-1)B(\omega)$ is a nonzero idempotent, hence is equal to 1, and $\omega - 1 \in R^\times$.

Let $\psi, \chi : \mathbb{F}_p^\times \to R$ be two characters and $R(\psi, \chi)$ be a free R-module of rank 1, and let $\begin{pmatrix} a & * \\ 0 & b \end{pmatrix} \in B$ act on $R(\psi, \chi)$ by $\psi(a)\chi(b)$. Then $\pi(\psi, \chi)$ denotes the left $R[G]$-module $R[G] \otimes_{\mathbb{R}[B]} R(\psi, \chi)$. When $R = \mathbb{C}$, these representations are the *principal series* of $\mathrm{GL}_2(\mathbb{F}_p)$.

Proposition B.1.1 *Fix a generator g of $R(1,1)$. The* Steinberg representation St *of G is the quotient $\pi(1,1)/\sum_{M \in G/B} M \otimes g$.* St *is free of rank p as a R-module, and the exact sequence $0 \to R \to \pi(1,1) \to \mathrm{St} \to 0$ splits.*

Proof. – In the exact sequence, $\nu : R \to \pi(1,1)$ is the map $1 \longmapsto \sum_{M \otimes G/B} M \otimes g$. So it is enough to construct a $R[G]$-retraction $r : \pi(1,1) \to R$ of ν and show that $\ker R$ is free over R. Take $r : M \otimes g \longmapsto (p+1)^{-1}$, and note that $\ker r$ has the $M \otimes g - I_2 \otimes g$ as a basis, where M runs through $S' \backslash \{I_2\}$. □

Proposition B.1.2 *The R-module $\mathrm{End}_{R[G]}(\pi(1,1))$ is free of rank two. In particular, $\mathrm{End}_{R[G]}\mathrm{St}$ is a free R-module of rank one, so that, if R is a field and $p \in R^\times$, then* St *is absolutely irreducible.*

Proof. – Fix a generator g of $R(\mathbf{1}, \mathbf{1})$. By construction of $\pi(1,1)$,

$$\rho : u \in \mathrm{End}_{R[G]}(\pi(1,1)) \longmapsto u(I_2 \otimes g) \in \pi(1,1)^B$$

is an isomorphism. Since $I_2 \otimes g \in \pi(1,1)^B$, it is enough to show that the submodule of $\sum_{M \in S' \backslash \{I_2\}} R \cdot M \otimes g$ made with its elements fixed by B is free of rank one.

Let $x = \sum_{t \in \mathbb{F}_p^\times} c_t T^t \otimes g + c_\infty W \in \pi(1,1)^B$ for some $c_t, c_\infty \in R$. Then, for any $a \in \mathbb{F}_p^\times$, $x = \Delta_{1,a} x = \sum_{t \in \mathbb{F}_p^\times} c_t T^{at} \otimes g + c_\infty W \otimes g$, so that the c_t for $t \in \mathbb{F}_p^\times$ are constant.

Moreover, one computes that $x = Ux = c_\infty T \otimes g + c_1 W \otimes g + \sum_{t \in \mathbb{F}_p^\times \backslash \{-1\}} c_1 T^{t/(t+1)} \otimes g$, so that $c_\infty = c_1$. Hence $\pi(1,1)^B$ is contained in $R(I_2 \otimes g) + R\sum_{M \in S'} M \otimes g$, and it easy to check that the reverse inclusion holds.

Note that $\rho(\mathrm{id}) = I_2 \otimes g$, and that $\rho^{-1}\left(\sum_{M \in S'} M \otimes g\right)$ is a projection onto $\pi(1,1)^G$. □

Write St_ψ for the twisted representation $\mathrm{St} \otimes \psi(\det)$, for some character $\psi : \mathbb{F}_p^\times \to R^\times$.

Proposition B.1.3 *Let $\psi, \chi : \mathbb{F}_p^\times \to R^\times$ be distinct characters. Then $\mathrm{End}_{R[G]}(\pi(\psi, \chi))$ is free of rank one. Thus, if R is a field and $p \in R^\times$, $\pi(\psi, \chi)$ is absolutely irreducible.*

Proof. – As in the previous Proposition, if we fix a generator g of $R(\psi, \chi)$, we have a injective homomorphism $\rho : u \in \mathrm{End}_{R[G]}(\pi(\psi, \chi)) \longmapsto u(I_2 \otimes g) \in \pi(\psi, \chi)$, the image of which is exactly the submodule $\Upsilon = \{v \in \pi(\psi, \chi) \mid \forall M \in B,\ Mv = \psi([M]_{1,1})\chi([M]_{2,2})v\}$. The goal is to show that $\Upsilon = R(I_2 \otimes g)$.

Let $x = \sum_{t \in \mathbb{F}_p} c_t T^t \otimes g + c_\infty W \otimes g \in \Upsilon$. For any $a \in \mathbb{F}_p^\times$,

$$\chi(a)x = \Delta_{1,a} x = \sum_{t \in \mathbb{F}_p} \chi(a) c_t T^{at} \otimes g + \psi(a) c_\infty W \otimes g,$$

so that, by identifying coefficients, $c_a = c_1$ and for any $a \in \mathbb{F}_p^\times$, $(\psi(a) - \chi(a))c_\infty = 0$. Let $a \in \mathbb{F}_p^\times$ be such that $\psi(a) \neq \chi(a)$, and let $\omega = \frac{\psi(a)}{\chi(a)}$. By construction, $\omega \neq 1$, $\omega^{p-1} = 1$, and $(\omega - 1)c_\infty = 0$: $\omega - 1$ is invertible and $c_\infty \neq 0$. Now,

$$x = Ux = c_0 I_2 \otimes g + \sum_{t \in \mathbb{F}_p^\times \backslash \{-1\}} c_1 \frac{\psi}{\chi}(t+1) T^{\frac{t}{t+1}} \otimes g + (\psi\chi)(-1) \cdot c_1 W \otimes g,$$

whence $c_1 = 0$ and $x \in R(I_2 \otimes g)$. Thus, $\Upsilon \subset R(I_2 \otimes g)$, and the reverse inclusion is clear. □

Proposition B.1.4 *Let $\psi, \chi, \theta : \mathbb{F}_p^\times \to R^\times$ be characters. Then $\pi(\psi\theta, \chi\theta)$ is canonically isomorphic to $\pi(\psi, \chi) \otimes \det\theta$.*

Proof. – Let g, g' be generators of $R(\psi, \chi), R(\psi\theta, \chi\theta)$. The morphism

$$rI_2 \otimes g' \in R(\psi\theta, \chi\theta) \longmapsto rI_2 \otimes g \in \pi(\psi, \chi) \otimes \det\theta$$

is a $R[B]$-morphism, so it induces a $R[G]$-morphism $u : \pi(\psi\theta, \chi\theta) \to \pi(\psi, \chi) \otimes \det\theta$. The image of u is the $R[G]$-submodule generated by $u(I_2 \otimes g') = I_2 \otimes g$, hence u is surjective. Since u is R-linear and surjective between two free R-modules of same rank, hence it is an isomorphism.□

Proposition B.1.5 *Let $\psi_1, \chi_1, \psi_2, \chi_2 : \mathbb{F}_p^\times \to R$ and assume that $R(\psi_1, \chi_1), R(\psi_2, \chi_2)$ have the same traces. Then $\{\psi_1, \chi_1\} = \{\psi_2, \chi_2\}$.*

Proof. – Left multiplication by $\Delta_{1,a}$ (for $a \in \mathbb{F}_p^\times \backslash \{0, 1\}$) acts on G/B as follows: the $T^t B$ for $t \in \mathbb{F}_p^\times$ are permuted without any fixed point, and $\Delta_{1,a} W = W \Delta_{a,1}$. Thus, the trace of the action of $\Delta_{1,a}$ on $R(\psi_i, \chi_i)$ is $\chi_i(a) + \psi_i(a)$. Moreover, the matrix aI_2 acts on $R(\psi_i, \chi_i)$ by multiplication by $\psi_i(a)\chi_i(a)$. Since $p + 1 \in R^\times$, we can then check that $\psi_1 + \chi_1 = \psi_2 + \chi_2$ and $\psi_1\chi_1 = \psi_2\chi_2$. Thus $(\psi_1 - \psi_2)(\psi_1 - \chi_2) = 0$. Since $\psi_1 - \psi_2, \psi_1 - \chi_2$ take their values in $R^\times \cup \{0\}$. Therefore, the reunion of the two subgroups $\{\psi_1 = \psi_2\}, \{\psi_1 = \chi_2\}$ of $\mathbb{F}_p^\times$ is $\mathbb{F}_p^\times$, hence one has $\psi_1 = \psi_2$ (thus $\chi_1 = \chi_2$) or $\psi_1 = \chi_2$ (thus $\chi_1 = \psi_2$). □

Proposition B.1.6 *Let $\psi, \chi : \mathbb{F}_p^\times \to R^\times$ be two distinct characters, $g \in R(\chi, \psi)$ be a generator, and*

$$v = W \otimes g + \sum_{a \in \mathbb{F}_p^\times} \frac{\psi}{\chi}(a)(T)^a \otimes g \in \pi(\chi, \psi).$$

Then

$$u \in \mathrm{Hom}_{R[G]}(\pi(\psi, \chi), \pi(\chi, \psi)) \longmapsto u(I_2 \otimes g) \in Rv$$

is an isomorphism. Let $u^\circ : \pi(\psi, \chi) \to \pi(\chi, \psi)$ be such that $u^\circ(I_2 \otimes g) = v$, then:

- *if $p \in R^\times$, u° is an isomorphism.*
- *if $\mathbb{F}_p \subset R$, then u° is neither injective nor onto, its kernel and cokernel are free of same positive rank.*

Proof. – It is clear that $u \in \mathrm{Hom}_{R[G]}(\pi(\psi, \chi), \pi(\chi, \psi)) \longmapsto u(I_2 \otimes g)$ is an isomorphism onto the submodule $\Upsilon \subset \pi(\chi, \psi)$ on which B acts by the character $R(\psi, \chi)$. For any $a \in \mathbb{F}_p^\times$, aI_2 acts on $\pi(\chi, \psi)$ by multiplication by $(\psi\chi)(a)$; thus Υ is the submodule of the $x \in \pi(\chi, \psi)$ such that $Ux = x$ and $\Delta_{1,a} x = \chi(a)x$. We compute:

$$\begin{aligned}
\Delta_{1,a} v &= W\Delta_{a,1} \otimes g \sum_{t \in \mathbb{F}_p^\times} \frac{\psi}{\chi}(t) T^{ta} \Delta_{1,a} \otimes g = \chi(a) W \otimes g + \chi(a) \sum_{t \in \mathbb{F}_p^\times} \psi(t)\psi(a)\chi^{-1}(ta) T^{ta} \otimes g \\
&= \chi(a) v, \\
Uv &= T \otimes g + \sum_{t \neq 0, -1} \frac{\chi}{\psi}(t+1) \frac{\psi}{\chi}(t) T^{t/(t+1)} \otimes g + \frac{\psi}{\chi}(-1)\psi\chi(-1) W \otimes g \\
&= W \otimes g + T \otimes g + \sum_{t \neq 0, 1} \frac{\psi}{\chi}(t) T^t \otimes g = v,
\end{aligned}$$

thus $Rv \subset \Upsilon$. If the inclusion is strict, then, by substracting the correct multiple of v, there exists some $x = \sum_{t\in\mathbb{F}_p} c_t T^t \otimes g \in \Upsilon\backslash\{0\}$. Now, for each $a \in \mathbb{F}_p^\times$, $\chi(a)x = \Delta_{1,a}x = \sum_{t\in\mathbb{F}_p} \psi(a)c_t T^{ta} \otimes g$: after identifying the coefficients, we see that $c_a = \frac{\psi}{\chi}(a)c_1$ and $c_0 = 0$. Since

$$x = Ux \in \sum_{t\in\mathbb{F}_p} RT^t \otimes g + \frac{\psi}{\chi}(-1)\psi\chi(-1)c_1 W \otimes g,$$

one has $c_1 = 0$ thus $x = 0$, thus contradicting our assumption.

Now, we discuss u°. We can check that

$$\begin{aligned}\sum_{s\in\mathbb{F}_p} T^s v &= \sum_{a\in\mathbb{F}_p^\times, s\in\mathbb{F}_p} \frac{\psi}{\chi}(a)T^{a+s} \otimes g + \sum_{s\in\mathbb{F}_p} T^s W \otimes g \\ &= \sum_{t\in\mathbb{F}_p}\sum_{a\in\mathbb{F}_p^\times} \frac{\psi}{\chi}(a)\cdot T^t \otimes g + \sum_{s\in\mathbb{F}_p} WU^{-s} \otimes g \\ &= pW \otimes g,\end{aligned}$$

thus the cokernel of u° is of p-torsion. Therefore, if $p \in R^\times$, u° is a surjective map of free R-modules of same finite rank, hence an isomorphism.

Now assume that $\mathbb{F}_p \subset R$. Then, since $X^{p-1} - 1 = \prod_{1\le i<p}(X - i)$, ψ, χ must take their values in $\mathbb{F}_p^\times$, so all the constructions are defined over $\mathbb{F}_p$ (and obtained after extending scalars by $\mathbb{F}_p \to R$). Over $\mathbb{F}_p$, we just computed that $u^\circ\left(\sum_{s\in\mathbb{F}_p} T^s \otimes g\right) = \sum_{s\in\mathbb{F}_p} T^s v = 0$, hence u° is not injective. Since u° is linear between two $\mathbb{F}_p$-vector spaces of dimension $p+1$, it is not surjective either, and its kernel and cokernel have the same finite rank. This claim is stable under the faithfully flat extension of scalars $\mathbb{F}_p \to R$. □

Remark What this result says is that $\pi(\chi,\psi)$ is symmetric with respect to (ψ,χ) in characteristic zero (or more generally distinct from p), but not in characteristic p.

Lemma B.1.8 *Let $\psi, \chi : \mathbb{F}_p^\times \to R^\times$ be characters, then $\pi(\psi,\chi)^{\circ *} \simeq \pi(\chi^{-1},\psi^{-1})$. In particular, with $\psi = \chi = 1$, we get an isomorphism $\mathrm{St}^{\circ *} \to \mathrm{St}$.*

Proof. – As in the previous proofs, $u \in \mathrm{Hom}_G(\pi(\chi^{-1},\psi^{-1}), \pi(\psi,\chi)^{\circ *}) \longmapsto u(I_2 \otimes g)$ is a bijection onto the sub-R-module Υ made with those $x \in \pi(\psi,\chi)^{\circ *}$ such that any $M \in B$ satisfies $Mx = \chi^{-1}([M]_{1,1})\psi^{-1}([M]_{2,2})x$. In other words, Υ is the set of those $x \in \pi(\psi,\chi)$ such that $\Delta_{a,b}x = \chi(a)\psi(b)x$ for all $a, b \in \mathbb{F}_p^\times$ and $T^{-1}x = x$. The module Υ contains $x = W \otimes g$ since $W\Delta_{a,b} = \Delta_{b,a}W$ and $T^{-1}W = WU$. Let $u : \pi(\chi^{-1},\psi^{-1}) \to \pi(\psi,\chi)^{\circ *}$ be such that $u(I_2 \otimes g) = W \otimes g$: then u is a $R[G]$-morphism, and its image contains $W \otimes g$ and is a $R[G]$-module, so u is onto. Since u is R-linear between free R-modules of same rank, u is an isomorphism. □

Lemma B.1.9 *Let $\psi, \chi : \mathbb{F}_p^\times \to R^\times$ be characters, then $\pi(\chi^{-1},\psi^{-1})$ and $\pi(\chi,\psi)^*$ are isomorphic.*

Proof. – As above, we only need to exhibit some $f \in \mathrm{Hom}_R(\pi(\chi,\psi), R)$ such that $f(U^{-1}\cdot) = f$, $f(\Delta_{a,b}^{-1}\cdot) = \chi^{-1}(a)\psi^{-1}(b)f$, and such that the $R[G]$-module generated by f is $\mathrm{Hom}_R(\pi(\chi,\psi), R)$. Let g be a generator of $R(\chi,\psi)$, and $f : \pi(\chi,\psi) \to R$ mapping $I_2 \otimes g$ to 1 and $M \otimes g$ to 0 for any $M \in S'\backslash\{T^t,\, t \in \mathbb{F}_p^\times\} \cup \{W\}$. It is then formal to check that f satisfies the requested conditions. □

Corollary B.1.10 *The isomorphism of Lemma B.1.9 induces (when $\psi = \chi$) an isomorphism $\mathrm{St}_{\psi^{-1}} \to \mathrm{St}_\psi^*$.*

Proof. – It is enough to show the result when $\chi = \psi = \mathbf{1}$, and in this case one has $\pi(\mathbf{1},\mathbf{1}) = \mathrm{St} \oplus \mathbf{1}$. Assume that the induced map $\mathbf{1} \to \pi(\mathbf{1},\mathbf{1}) \to \pi(\mathbf{1},\mathbf{1})^* \to \mathrm{St}^*$ vanishes. Then the composition

$\mathrm{St} \to \pi(\mathbf{1},\mathbf{1}) \to \pi(\mathbf{1},\mathbf{1})^* \to \mathrm{St}^*$ is R-linear and onto between free R-modules of same rank, hence is an isomorphism.

So the goal is to show that any G-equivariant morphism $\mathrm{St} \to R$ vanishes. It is enough to show that a G-equivariant morphism $\pi(\mathbf{1},\mathbf{1}) \to R$ vanishing at $\nu := \sum_{M \in B\backslash G} M \cdot g$ (where g is a generator of $R(1,1)$) is zero, or, in other words, that a G-equivariant $f : \pi(\mathbf{1},\mathbf{1}) \to R$ is determined by $f(\nu)$. Note that f is determined by $f(g)$, and $f(\nu) = f((p+1)g) \in R^\times f(g)$ by construction. □

Proposition B.1.11 *Let $\alpha, \beta : \mathbb{F}_p^\times \to R^\times$ be characters, $a, b \in \mathbb{F}_p^\times$ be distinct, and $C \leq G$ be a nonsplit Cartan subgroup.*

- *$aI_2 \in \mathrm{GL}_2(\mathbb{F}_p)$ acts on $\pi(\alpha,\beta)$ (resp. St_α) by multiplication by $(\alpha\beta)(a)$ (resp. $\alpha^2(a)$).*
- *The trace of U acting on $\pi(\alpha,\beta)$ (resp. St_α) is 1 (resp. 0).*
- *The trace of $\Delta_{a,b}$ acting on $\pi(\alpha,\beta)$ (resp. St_α) is $\alpha(a)\beta(b) + \alpha(b)\beta(a)$ (resp. $\alpha(ab)$).*
- *The trace of $g \in C\backslash\mathbb{F}_p^\times I_2$ acting on $\pi(\alpha,\beta)$ (resp. St_α) is 0 (resp. $-\alpha(\det g)$).*

Proof. – The statements about St_α follow from the fact that $\pi(\alpha,\alpha) \simeq \alpha(\det) \oplus \mathrm{St}_\alpha$. The first point is because $\mathbb{F}_p^\times I_2$ is central and that aI_2 acts by $(\alpha\beta)(a)$ on $R(\alpha,\beta)$. For the second point, note that $\pi(\alpha,\beta)$ has a basis made with the vectors e_M for $M \in G/B$ and that for $N \in G$, $N \cdot e_M$ is a unit multiple of e_{NM}.

Thus, the trace of any matrix $N \in \mathrm{GL}_2(\mathbb{F}_p)$ acting on $\pi(\alpha,\beta)$ is the sum, over all elements $x \in G/B$ stable under left multiplication by N, of the $\alpha([P]_{1,1})\beta([P]_{2,2})$, where $Nx' = x'P$, $P \in B$ and $x' \in G$ lifts x. The claims then follow from the following facts: the left multiplication by any $g \in C\backslash\mathbb{F}_p^\times I_2$ has no fixed point in G/B (since nonscalar elements of C do not have eigenvalues in $\mathbb{F}_p$), while B is the only fixed point of the left multiplication by U on G/B, and left multiplication by $\Delta_{a,b}$ on G/B has the two fixed points B and WB, with $\Delta_{a,b}I_2 = I_2\Delta_{a,b}$, $\Delta_{a,b}W = W\Delta_{b,a}$. □

B.2 Cuspidal representations

In this section, we assume that R is a field of characteristic zero containing the $p(p^2-1)(p-1)$-th roots of unity.

The $\psi(\det)$, the St_ψ, and the $\pi(\psi,\chi)$ (we say of all these representations that they *come from principal series*) form exactly $2(p-1) + \frac{(p-1)(p-2)}{2} = \frac{(p-1)(p+2)}{2}$ pairwise non-isomorphic irreducible representations of G. When counting against the conjugacy classes of G, we see that we are missing $\frac{p(p-1)}{2}$ isomorphism classes of irreducible representations of G.

Moreover, the sum of the squared dimensions of these missing irreducible representations is

$$(p-1)^2p(p+1) - (p-1) - (p-1)p^2 - \frac{(p-1)(p-2)(p+1)^2}{2} = \frac{p(p-1)^3}{2}.$$

Lemma B.2.1 *Let V be an irreducible representation of G. Then $V^U \neq 0$ if and only if V comes from principal series.*

Proof. – If $V = \psi(\det)$ or $V = \pi(\chi,\psi)$, $V^U \neq 0$ by construction. If $V = \mathrm{St}_\psi$, then there is a surjective morphism $\pi(\psi,\psi) \to \mathrm{St}_\psi$ (by Proposition B.1.1. Since the space of $\pi(\psi,\psi)$ is generated by some element fixed under U, the same holds for St_ψ.

Conversely, if V is irreducible and $V^U \neq 0$, then there is a character $\alpha : B/\langle U\rangle \to R^\times$ such that V^U contains a nonzero element x on which B acts by α. If $\alpha(M) = \psi([M]_{1,1})\chi([M]_{2,2})$, x defines a nonzero morphism $\pi(\psi,\chi) \to V$, which is then surjective, and V comes from principal series by Section B.1. □

Definition B.2.2 A representation V of G is *cuspidal* if $V^U = \{0\}$. Therefore, there are exactly $\frac{p(p-1)}{2}$ isomorphism classes of irreducible cuspidal representations of G.

Lemma B.2.3 *If V a cuspidal representation of G, then* $\dim V \geq p-1$.

Proof. – Let $u \in \mathcal{L}(V)$ be the endomorphism induced by U. Then u^p is the identity, but 1 is not an eigenvalue of u. Thus the set S of eigenvalues of u is made with primitive p-th roots of unity. For any $a \in \mathbb{F}_p^\times$, U and U^a are conjugate in G, so u^a is conjugate to u in $GL(V)$, thus $S^a \subset S$. Thus, S contains all the primitive p-th roots of unity, hence $\dim V \geq |S| \geq p-1$. □

Corollary B.2.4 *Every irreducible cuspidal representation of G has dimension $p-1$; a representation of G is cuspidal if and only if every one of its irreducible factors is cuspidal.*

Proof. – There are exactly $\frac{p(p-1)}{2}$ isomorphism classes of cuspidal representations, all of them have dimension at least $p-1$, and the sum of the squares of their dimensions is $\frac{p(p-1)^3}{2}$. □

Corollary B.2.5 *If V is an irreducible cuspidal representation of G, then U acts with trace -1, and any matrix $\Delta_{a,b}$ with $a \neq b$ acts with trace* 0.

Proof. – By the proof of Lemma B.2.3, the eigenvalues of the endomorphism u of U contain all the primitive p-th roots of unity. Since $\dim V = p-1$, the eigenvalues of u are exactly the primitive p-th roots of unity and they are all simple. Thus $\mathrm{Tr}(u) = \sum_{\omega^p=1, \omega \neq 1} \omega = -1$. Now, $\Delta_{a,b} U^{b/a} = U \Delta_{a,b}$, so that the endomorphism δ of V induced by $\Delta_{a,b}$ preserves the $p-1$ eigenspaces of u, and maps the ω-eigenspace to the $\omega^{b/a}$-eigenspace. In particular, δ permutes the eigenspaces of u without any fixed point, so $\mathrm{Tr}(\delta) = 0$. □

Proposition B.2.6 *Let $C \leq G$ be a nonsplit Cartan subgroup. To any irreducible cuspidal representation V of* $\mathrm{GL}_2(\mathbb{F}_p)$ *we may attach a pair $\{\chi, \chi^p\}$ of characters of C that do not factor through* det *such that:*

- *the pair $\{\chi, \chi^p\}$ characterizes the isomorphism class of V,*
- *every such pair is attached to some irreducible cuspidal representation,*
- *for any $a \in \mathbb{F}_p^\times$, aI_2 acts on C by $\chi(a)$,*
- *the character of V is that of the virtual representation $\mathrm{Ind}_{\mathbb{F}_p^\times \langle U \rangle}^G \left[aU^b \longmapsto \chi(a)\psi(b)\right] - \mathrm{Ind}_C^G \chi$, for any nontrivial $\psi : \mathbb{F}_p \to R^\times$,*
- *for any $g \in C \backslash \mathbb{F}_p^\times I_2$, the trace of g acting on V is $-\chi(g) - \chi^p(g)$.*

Proof. – This is a direct consequence of the construction of [21, (6.4) Theorem], as long as the character computation holds (and the action of $\mathbb{F}_p^\times I_2$ is correctly described). For the action of $\mathbb{F}_p^\times I_2$, it follows from the fact that these matrices are central. So all that remains is the character computation at $g \in C \backslash \mathbb{F}_p^\times I_2$. Since g is not similar to any aU^b, by [142, §7.2 Proposition 20],

$$\begin{aligned} &\mathrm{Tr}\left(g \mid \mathrm{Ind}_{\mathbb{F}_p^\times \langle U \rangle}^G \left[aU^b \longmapsto \chi(a)\psi(b)\right] - \mathrm{Ind}_C^G \chi\right) \\ &= -\mathrm{Tr}\left(g \mid \mathrm{Ind}_C^G \chi\right) = - \sum_{h \in G/C, h^{-1}gh \in C} \chi(h^{-1}gh) = -\chi(g) - \chi(g^p), \end{aligned}$$

since the only matrix in C conjugate to g is g^p, and the centralizer of g is exactly C. □

Remark Given any nonsplit Cartan subgroup $C \leq G$, there are two isomorphisms $C \to \mathbb{F}_{p^2}^\times$ preserving the trace and the determinant: if ι denotes one of them, the other one is ι^p. Thus, we will often identify, when discussing cuspidal representations, characters of C and characters of $\mathbb{F}_{p^2}^\times$. If C' is another nonsplit Cartan subgroup identified with $\mathbb{F}_{p^2}^\times$, then the composition isomorphism $C \to C'$ preserves the trace and the determinant, and is thus given by conjugation by some matrix $M \in G$, so this is harmless.

Corollary B.2.8 *Let $C \leq G$ be a nonsplit Cartan subgroup and V an irreducible cuspidal representation of* $\mathrm{GL}_2(\mathbb{F}_p)$ *attached to some character ϕ of C. For any Dirichlet character $\psi : \mathbb{F}_p^\times \to \mathbb{C}^\times$, $V \otimes \psi(\det)$ is an irreducible cuspidal representation of* $\mathrm{GL}_2(\mathbb{F}_p)$ *attached to the character $\phi \cdot \psi(\det)$.*

Proof. – The representation $V \otimes \psi(\det)$ is irreducible, and, since $\det U = 1$, it is cuspidal. The character $\phi \cdot \psi(\det) : C \to \mathbb{C}^\times$ does not factor through det, and it is a direct computation using Proposition B.2.6 and Corollary B.2.5 that $V \otimes \psi(\det)$ has the same character as the cuspidal representation attached to $\phi \cdot \psi(\det)$. □

Corollary B.2.9 *If V is an irreducible cuspidal representation of G, then $V^{\circ *} \simeq V^*$; if V is attached to the pair $\{\chi, \chi^p\}$, V^* is attached to the pair $\{\overline{\chi}, \overline{\chi}^p\}$.*

Lemma B.2.10 *Let V be a cuspidal representation of G. Then* $\det V = \left(\frac{\det}{p}\right)$.

Proof. – Let χ be a character of some nonsplit Cartan subgroup attached to V. Then $\det V$ is an abelian representation of G of dimension one, so it is of the form $\psi(\det)$ for some $\psi : \mathbb{F}_p^\times \to R^\times$. For any $a \in \mathbb{F}_p^\times$, $\psi(a^2) = \det(aI_2 \mid V) = \chi(aI_2)^{p-1} = \chi((aI_2)^{p-1}) = 1$, so ψ is quadratic.

Let $g \in \mathbb{F}_p^\times$ be a generator and $A \in \mathcal{M}_{p-1}(\mathbb{C})$ be the matrix of its action on V. Since $g^{p-1} = 1$, one has $A^{p-1} = I_{p-1}$ so A is diagonalizable. Moreover, we proved that if $1 \leq k < p-1$, $\mathrm{Tr}(A^k) = 0$. Thus, if $\lambda_1, \ldots, \lambda_{p-1}$ denote the eigenvalues of A (all of them $(p-1)$-th roots of unity), for any polynomial $P \in \mathbb{C}[X]$ with degree less than $p-1$, one has

$$\sum_{i=1}^{p-1} P(\lambda_i) = \mathrm{Tr}(P(A)) = (p-1)P(0).$$

If the λ_i are not exactly the $(p-1)$-th roots of unity, we can choose P such that the λ_i are exactly the roots of P. Then we get $(p-1)P(0) = \sum_{i=1}^{p-1} 0 = 0$, whence a contradiction. □

Proposition B.2.11 *Let V be an irreducible cuspidal representation of G with trivial central character. It is attached to a pair $\{\phi, \phi^p\}$, for some character $\phi : \mathbb{F}_{p^2}^\times / \mathbb{F}_p^\times \to R^\times$. Then V can be realized over $\mathbb{Q}(i, \phi)^+$, where $\mathbb{Q}(i, \phi)^+$ is the maximal real subextension of $R/\mathbb{Q}$ contained in the subfield of R generated by i and the values of ϕ. In particular, V is realizable over $\mathbb{R}$, and in fact over $\mathbb{Q}$ if ϕ has order* 4.

Proof. – Let C be a nonsplit Cartan subgroup of G, we identify ϕ with a character of $C/\mathbb{F}_p^\times I_2$. Since ϕ does not factor through the determinant, ϕ has order at least 3. Fix a nontrivial character $\psi : \mathbb{F}_p \to R^\times$. By Proposition B.2.6 and [142, §12.1 Proposition 33], it is enough to check that the representations $\mathrm{Ind}_{\mathbb{F}_p^\times U^{\mathbb{Z}}}^B \left[aU^b \longmapsto \psi(b)\right]$ and $\mathrm{Ind}_C^G \phi$ can be realized over $\mathbb{Q}(i, \phi)^+$.

We show that $\mathrm{Ind}_{\mathbb{F}_p^\times U^{\mathbb{Z}}}^B \left[aU^b \longmapsto \psi(b)\right]$ can be realized over $\mathbb{Q}$. Indeed, let $M = \mathbb{Q}(\mu_p)$, and we consider the following action of $B/\mathbb{F}_p^\times I_2$ on M: a matrix $aU^b\Delta_{c,1}$ (for $a, c \in \mathbb{F}_p^\times$ and $b \in \mathbb{F}_p$) acts by $\psi(b)\underline{c}$, where $\underline{c} \in \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ is the element whose cyclotomic character modulo p is c. One directly checks that this action is well-defined, and that there is a natural map $\lambda : \mathrm{Ind}_{\mathbb{F}_p^\times U^{\mathbb{Z}}}^B \left[aU^b \longmapsto \psi(b)\right] \to M$ mapping a generator of the one-dimensional representation with character $aU^b \longmapsto \psi(b)$ to 1. Since 1 generates M over $\mathbb{Q}[B]$, λ is onto; since it is between $\mathbb{Q}$-vector spaces of same dimension, λ is a $\mathbb{Q}[B]$-isomorphism.

Next, let N be the normalizer of C: $C \leq N$ is a subgroup of index two, and (for instance by computing an explicit example), there exists some $d \in N \backslash C$ with order two. Since N/C acts by taking the p-th power, it exchanges ϕ and ϕ^p; since $\phi(\mathbb{F}_p^\times) = 1$ by assumption, $\phi^p = \phi^{-1}$. We can then directly check that

$$g \in D \longmapsto \begin{pmatrix} \Re\phi(g) & -\Im\phi(g) \\ \Im\phi(g) & \Re\phi(g) \end{pmatrix} \in \mathcal{M}_2(\mathbb{R}),\ t \longmapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

is a realization over $\mathbb{Q}(i, \phi)^+$ of $\mathrm{Ind}_C^N \phi$, so that $\mathrm{Ind}_C^G \phi$ is also realizable over $\mathbb{Q}(i, \phi)^+$. □

B.3 Restriction of representations to smaller subgroups

In this section, we take $R = \mathbb{C}$ for the sake of simplicity, but the results apply to any algebraically closed field on which $p(p^2-1)$ is invertible. The letter D denotes the subgroup of B made with diagonal matrices.

The letter C always denotes a nonsplit Cartan subgroup with normalizer N. The character $N \to N/C \simeq \{\pm 1\}$ is noted ϵ. Given a character $\psi : C \to \mathbb{C}^\times$, ι_ψ denotes the representation $\mathrm{Ind}_C^N \psi$, so that $\iota_\psi = \iota_{\psi^p}$. It is reducible if and only if ψ factors through $\det : C \to \mathbb{F}_p^\times$, or in other words if $\psi^p = \psi$.

Lemma B.3.1 *$\mathrm{St}^U = \mathrm{St}^B$ is a line, and the eigenvalues of the endomorphism of* St *induced by U are exactly the p-th roots of unity.*

Proof. – By Proposition B.1.2, one has

$$\dim \pi(1,1)^B = \dim \mathrm{Hom}_B(\mathbf{1}, \pi(1,1)) = \dim \mathrm{Hom}_{\mathrm{GL}_2(\mathbb{F}_p)}(\pi(1,1), \pi(1,1)) = 2,$$

so, since $\pi(1,1) \simeq \mathrm{St} \oplus \mathbf{1}$, it is enough to show that $\dim \pi(1,1)^U = 2$. Let u be the endomorphism of St induced by U. Since $\pi(1,1) \simeq \mathbb{C}[G/B]$, $\mathrm{Tr}(u) = |(G/B)^U| - 1 = 0$. Since $U^p = I_2$ and U is similar to any U^a (for $a \in \mathbb{F}_p^\times$), u^p is the identity and $\mathrm{Tr}(u^a) = 0$ for any $a \in \mathbb{F}_p^\times$. Our goal is to show that the eigenvalues of u are exactly the p-th roots of unity, each with multiplicity one. If this is not the case, then there is a p-th root of unity which is not an eigenvalue of u. Therefore, there is a polynomial P of degree less than p, whose roots are p-th roots of unity, and such that $P(u) = 0$. Then $0 = \mathrm{Tr}(P(u)) = pP(0)$, so $P(0) = 0$, a contradiction. □

Lemma B.3.2 *Let $g \in C$ be a generator and $x \in \mathrm{St}^B$ be a nonzero vector. Let $P \in \mathbb{C}[x]$; then $P(g) \cdot x = 0$ if and only $P(g) \cdot \mathrm{St} = 0$ if and only if $X^{p+1} - 1 \mid (X-1)P(X)$.*

Proof. – Let γ be the endomorphism of the space of St induced by g. By Proposition B.1.11, for any $1 \leq k \leq p$, $\mathrm{Tr}(\gamma^k) = -1$ and $\gamma^{p+1} = \mathrm{id}$. Thus, the characteristic polynomial of γ is $P_0(X) = \frac{X^{p+1}-1}{X-1} \in \mathbb{C}[X]$, whose (simple) roots are the nontrivial $(p+1)$-th roots of unity. Since St is irreducible, there is an exact sequence of $\mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)]$-modules

$$0 \to \mathbb{C} \xrightarrow{u} \mathbb{C}[\mathrm{GL}_2(\mathbb{F}_p)/B] \xrightarrow{v} \mathrm{St} \to 0, \quad u(1) = \sum_{h \in \mathrm{GL}_2(\mathbb{F}_p)/B} [h], \quad v(I_2) = x.$$

The natural function $C/\mathbb{F}_p^\times \to \mathrm{GL}_2(\mathbb{F}_p)/B$ is between sets of cardinality $p+1$; it is injective, because $C \cap B = \mathbb{F}_p^\times I_2$, so is bijective. Hence, if $P \in \mathbb{C}[X]$ is such that $P(g) \cdot x = 0$, then $P(g) \cdot I_2 \in \mathbb{C} \cdot \sum_{h \in \mathrm{GL}_2(\mathbb{F}_p)/B} [h]$, thus $\deg P \geq p$ or $P = 0$. In particular, if P_1 denotes the remainder in the Euclidean division of P by P_0, then $P_1 = 0$, that is, $P_0 \mid P$. The conclusion follows. □

Lemma B.3.3 *Let $q : \Delta_{a,b} \in D \longmapsto \frac{a}{b} \in \mathbb{F}_p^\times$. Then*

$$\mathrm{St}_{|D} \simeq \mathbf{1} \oplus \bigoplus_{\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times} \chi(q).$$

Proof. – Since both of these representations have the same dimension and factor through $D/\mathbb{F}_p^\times$, it is enough to show that for each $g \in \mathbb{F}_p^\times \backslash \{1\}$, the trace of the action of $\Delta_{g,1}$ on both representations is the same. Clearly, the trace of the action of $\Delta_{g,1}$ on the right-hand side is $1 + \sum_{\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times} \chi(g) = 1$. By Proposition B.1.11, the trace of the action of $\Delta_{g,1}$ on St is $1 + 1 - 1 = 1$, whence the conclusion. □

Lemma B.3.4 *Let $C \leq \mathrm{GL}_2(\mathbb{F}_p)$ be a nonsplit Cartan subgroup with normalizer N. Then*

$$\mathrm{St}_{|N} \simeq \alpha \oplus \bigoplus_{\psi} \iota_\psi,$$

where:

- *α is the character $\left(\frac{\det(\cdot)}{p}\right)\epsilon^{\mathbf{1}(-1\notin\mathbb{F}_p^{\times 2})}$*
- *ψ runs through the characters $C/\mathbb{F}_p^\times I_2 \to \mathbb{C}^\times$ such that $\psi^2 \neq 1$, and always counting exactly one character in any pair $\{\psi, \psi^{-1}\}$.*

Proof. – It is a character computation. First, both representations have the same dimension and factor through $N/\mathbb{F}_p^\times I_2$.

Next, for any $g \in C\backslash\{I_2\}$, the trace of the action of g on the right hand side is exactly $\alpha(g) - 1 - \left(\frac{\det g}{p}\right) + \sum_\psi \psi(g)$, where ψ runs through characters $C/\mathbb{F}_p^\times \to \mathbb{C}^\times$, so the trace is exactly $\alpha(g) - 1 - \frac{\det g}{p} = -1$ since $\epsilon(g) = 1$. The trace of $\mathrm{St}(g)$ is -1 by Proposition B.1.11, so the characters agree.

For any $g \in N\backslash C$, g acts with trace 0 on any ι_ψ, so the action of g on the right-hand side has trace $\alpha(g) = \left(\frac{-\det g}{p}\right)$. The action of g on the left-hand side is, by Proposition B.1.11, 1 if g is not diagonalizable over $\mathbb{F}_p$, and -1 otherwise. Since $g \in N\backslash C$, $\mathrm{Tr}(g) = 0$, so $g^2 = -\det g I_2$. So g is diagonalizable over $\mathbb{F}_p$ if and only if $g^{p-1} = I_2$, if and only if $(-\det g)^{(p-1)/2} = 1$, if and only if $\left(\frac{-\det g}{p}\right)$: in other words, the action of g on St also has trace $\left(\frac{-\det g}{p}\right)$, whence the conclusion. □

Lemma B.3.5 *Let $C \leq \mathrm{GL}_2(\mathbb{F}_p)$ be a nonsplit Cartan subgroup with normalizer N, and $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ be a character. Then*

$$\pi(1,\chi)_{|N} \simeq A \oplus \bigoplus_{\psi} \iota_\psi,$$

where:

- *A is the sum of the characters $\alpha(\det)\epsilon^{\mathbf{1}(\alpha(-1)=-1}$ over all $\alpha : \mathbb{F}_p^\times \to \mathbb{C}^\times$ with $\alpha^2 = \chi$ (so A has dimension two if χ is even and is zero if χ is odd).*
- *ψ runs through the characters $C \to \mathbb{C}^\times$ such that $\psi(tI_2) = \chi(t)$ for every $t \in \mathbb{F}_p^\times$, such that $\psi^{p-1} \neq 1$, and always counting exactly one character in any pair $\{\psi, \psi^p\}$.*

Proof. – It is a character computation. Note that any aI_2 (for $a \in \mathbb{F}_p^\times$) acts by $\chi(a)$ on either side.

Moreover, the trace of the action of any matrix in $C\backslash\mathbb{F}_p^\times I_2$ is zero by Proposition B.1.11, and the trace of the action of any $\Delta_{a,b}$ with $a \neq b$ is $\chi(a) + \chi(b)$. For any $g \in N\backslash C$, $\mathrm{Tr}(g) = 0$, so $g^2 = -\det g I_2$, so that g is diagonalizable with eigenvalues in $\mathbb{F}_p$ if and only if $-\det g \in \mathbb{F}_p^{\times 2}$. In this case, the two eigenvalues of g are $\pm\sqrt{-\det g}$. Thus the character of the left-hand side is the following:

$$\begin{array}{ll} aI_2 : \chi(a)(p+1), & g \in C : 0, \\ g \in N\backslash C, -\det g \notin \mathbb{F}_p^{\times 2} : 0, & g \in N\backslash C, -\det g \in \mathbb{F}_p^{\times 2} : \chi(\sqrt{-\det g}) + \chi(-\sqrt{-\det g}). \end{array}$$

Assume that $\chi(-1) = -1$. Then A is zero by definition and the set of $p+1$ characters $\psi : C \to \mathbb{C}^\times$ extending χ does not contain any character with order $p-1$ (such a character factors through the determinant $C \to \mathbb{F}_p^\times$, therefore vanishes at $-I_2$, contradicting the fact that

$\chi(-1) = 1$), so that $\psi \longmapsto \psi^p$ is an involution of this set of characters, and the right-hand side has dimension $p+1$ like the left-hand side.

The character of the right-hand side at some $g \in C\backslash\mathbb{F}_p^\times I_2$ is $\sum_{\psi_{|\mathbb{F}_p^\times}=\chi} \psi(g) = 0$ (because these ψ are cosets of the subgroup of characters $C/\mathbb{F}_p^\times \to \mathbb{C}^\times$, and the characters in this subgroup do not all vanish at g). The character of the right-hand side is also zero on $N\backslash C$, which then matches the character of the left-hand side.

Now, assume that $\chi(-1) = 1$, so that $\chi = \alpha^2$ for some character $\alpha : \mathbb{F}_p^\times \to \mathbb{C}^\times$. Let $\lambda : \mathbb{F}_p^\times \to \{\pm 1\}$ be the unique nontrivial quadratic character. Then $\alpha(\det), (\alpha\lambda)(\det) : C \to \mathbb{C}^\times$ are two distinct characters whose restriction to $\mathbb{F}_p^\times$ is χ. The characters $C \to \mathbb{C}^\times$ agreeing with χ on $\mathbb{F}_p^\times$ are exactly of the form $\alpha(\det)\psi$ for some $\psi : C/\mathbb{F}_p^\times \to \mathbb{C}^\times$, and such a character has order dividing $p-1$ if and only if $\psi^{p-1} = 1$, if and only if $\psi^2 = 1$; there are at most two such characters, so, for any character $\psi : C \to \mathbb{C}^\times$ agreeing with χ on $\mathbb{F}_p^\times$, $\psi^{p-1} = 1$ if and only if $\psi \in \{\alpha(\det), (\alpha\lambda)(\det)\}$. It follows that the right-hand side has dimension $2\frac{p-1}{2} + 2 = p+1$.

For any $g \in C\backslash\mathbb{F}_p^\times I_2$, the trace of its action on the right-hand side is

$$\mathrm{Tr}(g \mid A) + \sum_{\psi} (\psi + \psi^p)(g) = \alpha(\det g) - (\alpha\lambda)(\det g) - \alpha(\det g) - (\alpha\lambda)(\det g) = 0.$$

Any $g \in N\backslash C$ acts on the right-hand side with trace

$$\begin{aligned}\mathrm{Tr}(g \mid A) + 0 &= \alpha(\det g)(-1)^{\mathbf{1}(\alpha(-1)=-1)} + (\alpha\lambda)(\det g)(-1)^{\mathbf{1}((\alpha\lambda)(-1)=-1)} \\ &= \alpha(-\det g)(1 + \lambda(-\det g)).\end{aligned}$$

Hence this trace is zero if $-\det g \notin \mathbb{F}_p^{\times 2}$, and $2\alpha(-\det g) = \chi(\sqrt{-\det g}) + \chi(-\sqrt{-\det g})$.

Thus the right-hand side and the left-hand side have the same characters. □

Proposition B.3.6 *Write $(\alpha, \beta) : \Delta_{u,v} \in D \longmapsto (u, v) \in \mathbb{F}_p^\times \times \mathbb{F}_p^\times$. Let V be a cuspidal representation of G attached to the character ϕ of $\mathbb{F}_{p^2}^\times$. Then*

$$V_{|D} \simeq \phi(\alpha) \otimes \bigoplus_{\psi:\mathbb{F}_p^\times \to \mathbb{C}^\times} \psi\left(\frac{\alpha}{\beta}\right).$$

Proof. – The two sides have dimension $p-1$, and, by Proposition B.2.6, any $aI_2 \in \mathbb{F}_p^\times$ acts by multiplication by the scalar $\phi(a)$ on either side, so the two characters agree at aI_2. If $a, b \in \mathbb{F}_p^\times$ are distinct, then $\Delta_{a,b}$ acts with trace zero on V, and the trace of the action of $\Delta_{a,b}$ on the right-hand side is $\phi(a)\sum_\psi \psi(ab^{-1}) = 0$. □

Proposition B.3.7 *Let V be an irreducible cuspidal representation of G, attached to an even character ϕ of $\mathbb{F}_{p^2}^\times$. Let $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ be a character such that $\chi^2 = \phi_{|\mathbb{F}_p^\times}$. Let $U' \triangleleft B$ denote the abelian subgroup $\mathbb{F}_p^\times U^{\mathbb{Z}}$. Then V is an irreducible representation of B and*

$$V_{|B} \simeq \chi(\det) \otimes \mathrm{Ind}_{U'}^B\left[aU^b \longmapsto e^{2i\pi b/p}\right] \simeq \mathrm{Ind}_{U'}^B\left[aU^b \longmapsto \phi(a)e^{2i\pi b/p}\right].$$

Proof. – Since $\dim V = p-1$, $V_{|U'}$ is a sum of $p-1$ characters of U'. Since aI_2 acts on V by multiplication by $\phi(a)$, all of these characters are of the form $\gamma_\phi : aU^b \in U' \longmapsto \phi(a)\gamma(b)$, for some character $\gamma : \mathbb{F}_p \to \mathbb{C}^\times$. Since V^U is null, id_ϕ does not contribute to this sum; that is, every character appearing in $V_{|U'}$ is of the form γ_ϕ for some nontrivial character $\gamma : \mathbb{F}_p \to \mathbb{C}^\times$. Since B-conjugacy acts transitively on the set of such γ_ϕ, $V_{|B}$ is irreducible and $V_{|U'}$ is the sum of the γ_ϕ over all nontrivial $\gamma : \mathbb{F}_p \to \mathbb{C}^\times$.

By the reasoning of [142, §8.1 Proposition 24], $V_{|B}$ is induced from the stabilizer of any

isotypic component of $V_{|U'}$. Since B/U' has cardinality $p-1$, the same as the number of isotypic components of B/U' (on which it acts transitively), B/U' acts freely on these isotypic components, so $V_{|B}$ is induced of any one of the isotypic components of $V_{|U'}$ from U' to B. □

Proposition B.3.8 *Let V be an irreducible cuspidal representation of G attached to a character ϕ of C. Then*

$$V_{|N} \simeq W \oplus \bigoplus_{\psi} \iota_\psi,$$

where:

- *W is a sum of two characters if ϕ is even and zero otherwise,*
- *If $\phi(-I_2) = 1$, W is the sum of the two characters $\chi(\det)\epsilon^r$, where $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ is a character such that $\phi(uI_2) = \chi(u^2)$ for each $u \in \mathbb{F}_p^\times$ (there are exactly two such χ), and $r \in \{0,1\}$ is such that $(-1)^r\chi(-1) = -1$ if $\phi(uI_2) = \chi(u^2)$ for each $u \in \sqrt{\mathbb{F}_p^\times}$, and $(-1)^r\chi(-1) = 1$ otherwise (so that for either χ, exactly one value of r works).*
- *ψ runs through the morphisms $C \to \mathbb{C}^\times$ such that $\psi \notin \{\phi, \phi^p\}$, $\psi^{p-1} \neq 1$, $\psi(tI_2) = \phi(tI_2)$ for every $t \in \mathbb{F}_p^\times$, and we only count one character in every pair $\{\psi, \psi^p\}$.*

Proof. – For any $a \in \mathbb{F}_p^\times$, aI_2 acts on both sides by multiplication by $\phi(aI_2)$. Next, we show that the representations on both sides have dimension $p-1$. The left-hand side clearly has dimension $p-1$, so we discuss the right-hand side. This amounts to showing that if $\phi(-I_2) = -1$ (resp. $\phi(-I_2) = 1$), there are exactly $p-1$ (resp. $p-3$) characters $\psi : C \to \mathbb{C}^\times$ agreeing with ϕ on $\mathbb{F}_p^\times$ and such that $\psi \notin \{\phi, \phi^p\}$ as well as $\psi^{p-1} = 1$.

Since C is cyclic with order p^2-1, there are $p+1$ characters $C \to \mathbb{C}^\times$ agreeing with ϕ on $\mathbb{F}_p^\times I_2$, and ϕ, ϕ^p are two of them. So we need to show that if $\phi(-1) = -1$ (resp. $\phi(-1) = 1$), no character $\psi : C \to \mathbb{C}^\times$ agreeing with ϕ on $\mathbb{F}_p^\times I_2$ verifies $\psi^{p-1} = 1$ (resp. exactly two such characters satisfy the condition). Let $g \in C$ be a generator, then a character $\psi : C \to \mathbb{C}^\times$ agreeing with ϕ on $\mathbb{F}_p^\times I_2$ is uniquely defined by the value of $\psi(g) \in \phi(g)\mu_{p+1}$. Given $\omega \in \mu_{p+1}$, the number of $\omega \in \mu_{p+1}$ such that $(\phi(g)\omega)^{p-1} = 1$ is the number of $\omega \in \mu_{p+1}$ such that $\omega^2 = \phi(g)^{p-1}$. There are either two such ω or zero, depending on whether $\phi(g)^{(p-1)(p+1)/2} = 1$. The correct dimension count follows since $\phi(g)^{(p^2-1)/2} = \phi(-I_2)$.

If $\phi(-I_2) = 1$, the two characters of C agreeing with ϕ on $\mathbb{F}_p^\times I_2$ and with order dividing $p-1$ are the two possible $\chi(\det)$.

Now, we need to show that the characters agree at every $g \in C\backslash\mathbb{F}_p^\times I_2$ and at every $g \in N\backslash C$.

When $g \in C\backslash\mathbb{F}_p^\times I_2$, by the remark above, the character of the right-hand side is $\sum_\psi \psi(g)$, where ψ runs through all the characters $\psi : C \to \mathbb{C}^\times$ agreeing with ϕ on $\mathbb{F}_p^\times I_2$ with $\psi \notin \{\phi, \phi^p\}$. So the character of the right-hand side is $-\phi(g) - \phi^p(g)$, which is also the value at g of the character of the left-hand side by Proposition B.2.6.

Let $g \in N\backslash C$. Then g has trace zero, hence $g^2 = -\det g I_2$, and the character of the right-hand side is 0 if $\phi(-I_2) = -1$, and $\sum_\chi (-1)^{r_\chi}\chi(\det g)$ over $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ such that $\chi(t^2) = \phi(tI_2)$ for each $t \in \mathbb{F}_p^\times$, where r_χ is the r attached to χ in the statement.

Suppose that $-\det g = u^2$ for some $u \in \mathbb{F}_p^\times$: then g is similar over $\mathbb{F}_p$ to $\Delta_{u,-u}$, hence the character of the left-hand side vanishes at g, while the character of the right-hand side is $\phi(u)\sum_\chi (-1)^{r_\chi}\chi(-1) = 0$, because the two characters χ over which we sum are distinct, so that the $(-1)^{r_\chi}\chi(-1)$ are distinct signs.

Suppose now that $-\det g$ is not a square. Then g is similar to some $g' \in C\backslash\mathbb{F}_p^\times$, the pair $\{g', (g')^p\}$ being uniquely defined (and $(g')^2$ is scalar). Then $(g')^{2(p-1)} = I_2$ while $(g')^{p-1} \neq I_2$, hence $(g')^{p-1} = -I_2$. By the same arguments as previously, the characters of both sides of the equality agree at g if $\phi(-I_2) = -1$ (they are equal to $-\phi(g') - \phi(g')^p$), so we may assume that $\phi(I_2) = 1$. In this case, the character of the left-hand side is $-\phi(g') - \phi(g')^p = -2\phi(g')$, while the character of the right-hand side is $\sum_\chi (-1)^{r_\chi}\chi(\det g)$, where $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$ is one of the two

characters such that $\chi(t^2) = \phi(tI_2)$ for each $t \in \mathbb{F}_p^\times$. By checking both possible, we see that $(-1)^{r_\chi}\chi(-1) = -\frac{\phi(g')}{\chi(-\det g')}$, so $(-1)^{r_\chi}\chi(\det g') = -\phi(g')$, whence the claimed equality. □

B.4 Splitting of a certain cuspidal representation restricted to $\mathrm{SL}_2(\mathbb{F}_p)$

We now assume that $p \equiv 3 \pmod 4$, and write $\phi_2 : \mathbb{F}_{p^2}^\times \to \mathbb{C}^\times$ (resp. $\phi_4 : \mathbb{F}_{p^2}^\times \to \mathbb{C}^\times$) as the unique character of order 2 (resp. one of the two characters of order 4). Thus ϕ_4 and $\phi_4^3 = \phi_4^p = \phi_4^{-1}$ are distinct characters $\mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times \to \mathbb{C}^\times$ which do not factor through the norm. We denote by V_4 the cuspidal representation (with coefficients in $\mathbb{Q}$, by Proposition B.2.11) of G attached to the pair of characters $\{\phi_4, \phi_4^{-1}\}$.

Finally, let $G_2 \triangleleft G$ denote the subgroup $\mathbb{F}_p^\times \mathrm{SL}_2(\mathbb{F}_p)$, and $C \leq G$ a nonsplit Cartan subgroup with normalizer N.

Proposition B.4.1 *There exist two irreducible representations V^+, V^- of G_2 with dimension $\frac{p-1}{2}$ satisfying the following properties:*

- *V^+ and V^- are contragredients of each other and conjugates of each other under G/G_2,*
- *$(V_4)_{|G_2} \simeq V^+ \oplus V^-$,*
- *$V_4 \simeq \mathrm{Ind}_{G_2}^G V^+ \simeq \mathrm{Ind}_{G_2}^G V^-$,*
- *V^+ and V^- factor through $\mathrm{PSL}_2(\mathbb{F}_p) \simeq G_2/\mathbb{F}_p^\times I_2$,*
- *the restrictions of V^+ and V^- to any subgroup with order prime to p are isomorphic,*
- *V^+, V^- can be realized over $\mathbb{Q}(\sqrt{-p})$.*

Proof. – If $g \in G_2$, the trace of the action of g on V_4 is, by Proposition B.2.6:

(a) $p-1$ if g is scalar,
(b) -1 if g is not scalar but its minimal polynomial is not separable,
(c) 0 if g has two distinct eigenvalues in $\mathbb{F}_p^\times$,
(d) ± 2 if g has two distinct eigenvalues in $\mathbb{F}_{p^2}\backslash\mathbb{F}_p^\times$.

There are $p-1$ G-conjugacy classes in G_2 of the first type, and all of them have cardinality one. There are $p-1$ G-conjugacy classes in G_2 of the second type, and all of them have cardinality p^2-1. There are, finally, $\frac{1}{2}\left(\frac{p^2-1}{2} - (p-1)\right) = \frac{(p-1)^2}{4}$ G-conjugacy classes in G_2 of the last type. Therefore,

$$\begin{aligned}\frac{2}{p(p-1)^2(p+1)} \sum_{g\in G_2} |\mathrm{Tr}(g \mid V_4)|^2 &= \frac{2((p-1)\cdot(p-1)^2 + (p-1)\cdot(p^2-1) + (p-1)^2\cdot p(p-1)}{p(p-1)^2(p+1)} \\ &= \frac{2(p-1)^2(p-1+p+1+p(p-1))}{p(p-1)^2(p+1)} = 2,\end{aligned}$$

therefore $(V_4)_{|G_2}$ is the sum of two non-isomorphic irreducible representations of G_2, which we denote by V^+, V^-. Since $\mathbb{F}_p^\times I_2$ acts trivially on V_4, it also acts trivially on $V^\pm$.

Let $\tau^\pm$ be the trace of the action of U on $V^\pm$. The $\tau^\pm$ are algebraic integers and their sum is the trace of the action of U on V_4, that is, $\tau^+ + \tau^- = -1$. Hence $\tau^+ \neq \tau^-$ and V^+, V^- are not isomorphic. Since V_4 is irreducible, G/G_2 acts transitively on $\{V^+, V^-\}$, so V^+ is conjuagte to V^- under G/G_2.

If $M \in G_2$ has order prime to p, then M is contained (up to G-conjugacy) in a group of diagonal matrices or in a nonsplit Cartan subgroup. In particular, the centralizer of M in G has full determinant. Therefore, M is G_2-similar to any of its G-conjugates, and the characters of V^+ and V^- agree at M.

Since U^{-1} is G-conjugate to U but not G_2-conjugate to U, τ^+ and τ^- are complex conjugates of each other, so $\tau^+ \notin \mathbb{R}$. Therefore, neither V^+ not V^- is self-dual. Since $(V_4)_{|G_2} \simeq V^+ \oplus V^-$ is self-dual by Corollary B.2.9, V^+ and V^- are duals of each other. In particular, they both have dimension $\frac{p-1}{2}$.

Let $\epsilon \in \{\pm 1\}$, then there is a natural map $\mathrm{Ind}_{G_2}^G V^\epsilon \to V_4$. It is nonzero and G-equivariant by construction. Since V_4 is irreducible, it is surjective and between representations of the same dimension, hence is an isomorphism.

All we need to do is check that $V^\pm$ can be defined over $\mathbb{Q}(\sqrt{-p})$.

Since the eigenvalues of the action of U on V_4 are exactly the primitive p-th roots of unity, there exists a partition of the primitive p-th roots of unity into two subsets $E^\pm$, where E^ϵ is the set of eigenvalues of the action of U on V^ϵ. For any $t \in \mathbb{F}_p^\times$, $U^{t^2} = \Delta_{t,1/t} U \Delta_{1/t,t}$, so each $E^\pm$ is stable after taking t^2-th powers for any $t \in \mathbb{F}_p^\times$. As a consequence,

$$\{E^\epsilon \mid \epsilon \in \{\pm 1\}\} = \{\{e^{2i\pi\epsilon t^2/p, t \in \mathbb{F}_p^\times}\} \mid \epsilon \in \{\pm 1\}\}.$$

Therefore, there exists a sign a such that, on any complex realization of V^ϵ,

$$\sum_{t \in \mathbb{F}_p^\times} \left(\frac{t}{p}\right) U^t = a\epsilon \sum_{t \in \mathbb{F}_p^\times} \left(\frac{t}{p}\right) e^{2i\pi t/p} := a\epsilon \mathfrak{g}_p.$$

Let V be a realization of the cuspidal representation V_4 over $\mathbb{Q}$, and γ be the $\mathbb{Q}$-endomorphism $\sum_{t \in \mathbb{F}_p^\times} \left(\frac{t}{p}\right) U^t$. Since $V \otimes_{\mathbb{Q}} \mathbb{C}$ is the sum of one copy of V^+ and one copy of V^- (as $\mathbb{C}[G_2]$-modules), γ acts on the copy of V^ϵ by multiplication by $a\epsilon\mathfrak{g}_p$. In particular, $\gamma \otimes \mathbb{C}$ is a G_2-automorphism of $V \otimes_{\mathbb{Q}} \mathbb{C}$ with square $\mathfrak{g}_p^2 = -p$ by Proposition C.1.3, hence γ is a $\mathbb{Q}[G_2]$-automorphism of V with square $-p$. We can thus view V as a representation V' of G_2 with coefficients in $\mathbb{Q}[\gamma] \simeq \mathbb{Q}(\sqrt{-p})$. By construction, $V' \otimes_{\mathbb{Q}[\gamma]} \mathbb{C}$ is exactly a complex realization of V^b for the sign b such that $v\epsilon\mathfrak{g}_p$ is the image of γ in $\mathbb{C}$. □

Corollary B.4.2 *With the notations of Proposition B.4.1, for any $M \in G_2$ with order prime to p inducing endomorphisms g^+, g^- of the spaces of the representations V^+, V^-, g^+ and g^- have the same trace. It is equal to $\frac{p-1}{2}$ if M is scalar, 0 if M has two distinct eigenvalues in $\mathbb{F}_p$, -1 if M is G-similar to some element in $4C\backslash\mathbb{F}_p^\times$, 1 if M is G-similar to some $M' \in 2C\backslash 4C$. Moreover, after possibly exchanging V^+, V^-, the eigenvalues of U acting on V^ϵ are exactly the $e^{2i\pi\epsilon t/p}$ for $t \in \mathbb{F}_p^{\times 2}$.*

Proof. – The first and last parts of the statement are consequences of the proof of Proposition B.4.1. The common trace of g^+ and g^- is one half the character of V at g. Now, if $M \in 2C\backslash 4C$, then $\phi_4(M) = \phi_4^3(M) = -1$, while, if $M \in 4C\backslash\mathbb{F}_p^\times I_2$, $\phi_4(M) = \phi_4(M)^{-1} = 1$, so the claims follow from Proposition B.2.6. □

In the rest of this section, we break the symmetry between V^+ and V^- by stating that V^+ is the representation (over $\mathbb{C}$) such that the complex eigenvalues of U acting on V^+ are exactly the $e^{2i\pi t/p}$ for $t \in \mathbb{F}_p^{\times 2}$.

Proposition B.4.3 *Let $B_2 = B \cap G_2$ and $\epsilon = \pm$ be a sign. Then $C^\epsilon_{|B_2}$ is irreducible and*

$$C^\epsilon_{|B_2} \simeq \mathrm{Ind}_{\mathbb{F}_p^\times U^{\mathbb{Z}}}^{B_2} \left[aU^b \longmapsto e^{2i\pi b\epsilon/p}\right].$$

Proof. – $(V_4)_{|B} = \mathrm{Ind}_{B_2}^B C^\epsilon$ is irreducible, so $C^\epsilon_{|B_2}$ is irreducible. Since $C^-_{|B_2}$ is the conjugate of $C^+_{|B_2}$ under B/B_2, we may assume $\epsilon = +$. Both sides have the same dimension, and that any aI_2 for $a \in \mathbb{F}_p^\times$ acts trivially on either side. The trace of the action of any $g \in B_2\backslash\mathbb{F}_p^\times U^{\mathbb{Z}}$ on the left-hand side vanishes; since such a g is not conjugate to $\mathbb{F}_p^\times U^{\mathbb{Z}}$, the trace of the action of g on the right-hand side also vanishes by [142, §7.2 Proposition 20].

So it is enough to check that the restrictions of the two representations are isomorphic as $\mathbb{C}[U]$-modules. The eigenvalues of U acting on the left-hand side are exactly the $e^{2i\pi t/p}$ for $t \in \mathbb{F}_p^{\times 2}$, while the eigenvalues of U acting on the right-hand side are the conjugates of the characters $U^b \longmapsto e^{2i\pi b/p}$ by $B_2/\mathbb{F}_p^\times U$. The conjugates of these characters are exactly the $e^{2i\pi bt/p}$ for $t \in \mathbb{F}_p^{\times 2}$. □

Proposition B.4.4 *Let $D_2 \leq G_2$ be the subgroup of diagonal matrices, and $\alpha, \beta : D_2 \to \mathbb{F}_p^\times$ denote the first and second coefficients on the diagonal. Then*

$$C^\pm_{|D_2} \simeq \bigoplus_{\chi:\mathbb{F}_p^{\times 2}\to\mathbb{C}^\times} \chi\left(\frac{\alpha}{\beta}\right).$$

Proof. – We can check that the characters coincide: for any non-scalar $d \in D_2$, d acts with trace zero on either side. For any $a \in \mathbb{F}_p^\times$, aI_2 acts trivially on either side, and both sides are representations of D_2 of dimension $\frac{p-1}{2}$. □

Proposition B.4.5 *Let $C_2 = G_2 \cap C$ and $N_2 = G_2 \cap N$. Let $\eta : N_2 \to N_2/C_2 \to \{\pm 1\}$ be the character which is trivial if and only if $p \equiv 3 \pmod 8$. Then one has*

$$V^\pm_{|N_2} \simeq \eta \oplus {\bigoplus_{\chi:C_2\to\mathbb{C}^\times}}' \mathrm{Ind}_{N_2}^{D_2}\chi,$$

where the sum is over characters $\chi : C_2/\mathbb{F}_p^\times \to \mathbb{C}^\times$ with order at least 3 and such that we count exactly one character in any pair $\{\chi, \chi^p\}$.

Proof. – The group $C_2/\mathbb{F}_p^\times$ is cyclic with even order $\frac{p+1}{2}$, so the right-hand side has dimension $1 + \left(\frac{p+1}{2} - 2\right) = \frac{p-1}{2}$, like the left-hand side. Any scalar matrix acts trivially on either side.

If $g \in N_2\backslash C_2$, then the trace of the action of g on the right-hand side is 1 if $p \equiv 3 \pmod 8$ and -1 otherwise. Since $\mathrm{Tr}(g) = 0$, one has $g^2 = -\det g I_2$. Since $p \equiv 3 \pmod 4$ and $\det g \in \mathbb{F}_p^{\times 2}$, g has a G-conjugate $g' \in C_2$, so that $(g')^2 = -\det g' I_2 \in \mathbb{F}_p^\times I_2 \backslash \mathbb{F}_p^{\times 2} I_2$. Since $\frac{p-1}{2}$ is odd, the 2-adic valuation of the order of g' is exactly 4, so that g' is not scalar, a square in C, and it is a fourth power in C if and only if $p \equiv -1 \pmod 8$. Now, the trace of the action of g' (hence of g) on $V^\pm$ is 1 if g' is not a fourth power, and -1 otherwise.

Let $g \in C_2\backslash \mathbb{F}_p^\times I_2$. The trace of the action of g on the right-hand side is $1 + \sum_\chi \chi(g)$, where χ runs over characters $C_2/\mathbb{F}_p^\times \to \mathbb{C}^\times$ that have order at least 3. Thus said trace is exactly $-\chi_2(g)$, where χ_2 is the unique character of $C_2/\mathbb{F}_p^\times$ with order two. Since χ_2 agrees with ϕ_4 (after identifying C to $\mathbb{F}_{p^2}^\times$), this matches the trace of the left-hand side. □

B.5 Representations of G in characteristic p

In this section, the ring of coefficients of our representations will always be specified and is a $\mathbb{F}_p$-algebra.

The tautological representation of G (acting on $\mathbb{F}_p^2$, whose elements are identified with column matrices) is denoted by R, and we write $x = (1, 0), y = (0, 1)$. Let $X : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ be the tautological character.

For any $k \geq 0$, $R^{\otimes k}$ is a $\mathbb{F}_p[\mathfrak{S}_k \times G]$-module (where G acts simultaneously on each factor and $\mathfrak{S}_k$ permutes these factors). We let $\mathrm{Sym}^k R$ (resp. $\mathrm{TSym}^k R$) be the co-invariants (resp. its invariants) under the action of $\mathfrak{S}_k$. Note that the natural map $R^{\otimes k} \to \mathrm{Sym}^k R$ has a section whenever $k < p$.

The following well-known result is nonetheless important.

Proposition B.5.1 *Let V be a nonzero representation of G on any extension k of $\mathbb{F}_p$. Then V^U is nonzero.*

Proof. – Since $U^p = I_2$, the endomorphism u of V induced by U also satisfies $u^p = \mathrm{id}$. Thus $(u - \mathrm{id})^p = 0$, hence $u - \mathrm{id}$ is not injective. □

Corollary B.5.2 *Let V be a representation of G over some extension k of $\mathbb{F}_p$. Then, if $\dim_k V^U = 1$ and the sub-$k[G]$-module generated by V^U is V, then V is absolutely irreducible.*

Proof. – If k'/k is any field extension, then $V \otimes_{k'}$ (as a representation of G over k') satisfies the assumptions, so it is enough to show that V is irreducible. So let $W \subset V$ be a nonzero irreducible subrepresentation. So $\{0\} \neq W^U \subset V^U$: since V^U is a line, $W^U = V^U$ and V is generated over G by W^U, hence $V \subset W$ thus $V = W$. □

Corollary B.5.3 *Let $0 \leq k < p$ and $r \in \mathbb{Z}/(p-1)\mathbb{Z}$. Then $S_{k,r} := \det^r \otimes \mathrm{Sym}^k R$ is an absolutely irreducible representation of G over any field extension F of $\mathbb{F}_p$. Moreover, the $S_{k,r}$ are pairwise non isomorphic.*

Proof. – Let $F \supset \mathbb{F}_p$ be any field. It is enough to show that the $S_{k,r}$ are irreducible and pairwise non-isomorphic over F. For irreducibility, we may assume that $r = 0$. Since $Ux = x, Uy = x + y$, for any $0 \leq a, b \leq k$ with $a + b = k$, $U \cdot (x^a y^b) \in x^a y^b + b x^{a+1} y^{b-1} + \sum_{k \geq a' > a+1} F \cdot x^{a'} y^{k-a'}$. Thus, the matrix of the action of $U - 1$ on $\mathrm{Sym}^k R$, in the basis $(x^k, x^{k-1}y, x^{k-2}y^2, \ldots, xy^{k-1}, y^k)$ is upper triangular, its diagonal is zero and every coefficient just above the main diagonal is one. Thus the kernel of the action of $U - 1$ on $S_{k,0}$ is Fx^k.

If $k = a + b$ with $b > 0$, one can directly compute that

$$x^a y^b = -\binom{k}{b}^{-1} \sum_{i \in \mathbb{F}_p^\times} i^{p-1-b} (x + iy)^k = -\binom{k}{b}^{-1} \sum_{i \in \mathbb{F}_p^\times} i^{p-1-b} (T^i \cdot x^k),$$

so the sub-G-module generated by Fx^k is $S_{k,0}$, whence the irreducibility.

The isomorphism class of $\det^r \otimes \mathrm{Sym}^k R$ obviously determines k (using its dimension). Thus it is enough to show that if $0 \leq r < p - 1$ and $0 \leq k < p$, $\mathrm{Sym}^k R$ is not isomorphic to any of its twists by $\det^r$.

By the above argument, the action of $\Delta_{u,1}$ on $\ker(U - 1 \mid S_{k,r}) = Fx^k$ is the multiplication by u^{k+r}. In particular, the isomorphism class of $S_{k,r}$ over F determines k and $k + r \pmod{p-1}$, hence determines k and $r \pmod{p-1}$, whence the conclusion. □

Lemma B.5.4 *Let $0 \leq k < p$ and $r \in \mathbb{Z}/(p-1)\mathbb{Z}$. There is a perfect G-bilinear pairing $S_{k,r} \times S_{-k,-k-r} \to \mathbb{F}_p$ (where the representations are defined over $\mathbb{F}_p$) mapping (x^k, y^k) to 1. In particular, $S_{k,r}^* \simeq S_{k,-k-r}$.*

Proof. – We may obviously assume that $k > 0$ and $r = 0$. The following linear map

$$(u_1 \otimes \ldots \otimes u_k) \otimes (v_1 \otimes \ldots \otimes v_k) \in R^{\otimes k} \otimes R^{\otimes k} \longmapsto \prod_{i=1}^{k} \det(u_i, v_i) \in \mathbb{F}_p$$

is clearly invariant under the action of $\mathfrak{S}_k$, so factors as a map $\mu : S_{k,0} \otimes S_{k,0} \to \mathbb{F}_p$. By construction, $\mu(x^k, y^k) = 1$. For $g \in G$, $\mu(g\alpha, g\beta) = \det g^k \mu(\alpha, \beta)$, so that, if we let G act on $\mathbb{F}_p$ as the character $S_{0,k}$, μ is a G-bilinear pairing $S_{k,0} \otimes S_{k,0} \to S_{0,k}$, ie μ defines a G-bilinear pairing $S_{k,0} \times S_{k,-k} \to S_{0,0} = \mathbb{F}_p$. This pairing is then perfect because $S_{k,0}, S_{k,-k}$ are both irreducible and $\mu(x^k, y^k) = 1$. □

Proposition B.5.5 *Let $0 \leq a \leq p - 1$. There is a natural surjection of $\mathbb{F}_p[G]$-modules $\pi'_a : \pi(1, X^a) \to S_{p-1-a,a}$ mapping $\mathbb{F}_p(1, X^a)$ to $\mathbb{F}_p x^{p-1-a}$.*

Proof. – For any $M = \begin{pmatrix} b & * \\ 0 & d \end{pmatrix} \in B$, one has $Mx = bx$. Therefore, one has

$$M \cdot x^{p-1-a} = (bd)^a b^{p-1-a} x^{p-1-a} = d^a x^{p-1-a}.$$

Thus, if g is a generator for $R(1, X^a)$, $g \longmapsto x^{p-1-a} \in S_{p-1-a,a}$ is a morphism of $\mathbb{F}_p[B]$-modules, so it induces a morphism $\pi(1, X^a) \to S_{p-1-a,a}$. The morphism is onto because it is nonzero and $S_{p-1-a,a}$ is irreducible. □

Proposition B.5.6 *In Proposition B.5.5,* $\ker \pi'_a$ *is isomorphic to* $S_{a,0}$. *If* $a \notin \{0, p-1\}$, *then the exact sequence* $0 \to S_{a,0} \to \pi(1, X^a) \to S_{p-1-a,a} \to 0$ *of* $\mathbb{F}_p[G]$*-modules does not split.*

Proof. – First, we show that $\ker \pi'_a$ is isomorphic to $S_{a,0}$. By Proposition B.5.5, there is a surjective map $f : \pi(1, X^{p-1-a}) \to S_{a,-a}$ of $\mathbb{F}_p[G]$-modules. By Lemma B.1.9 and Lemma B.5.4, the contragredient of f is an injective map $f' : S_{a,0} \to \pi(1, X^a)$. Since $S_{a,0}$ and $S_{p-1-a,a}$ are irreducible and pairwise non-isomorphic, $\pi'_a \circ f' : S_{a,0} \to S_{p-1-a,a}$ is the zero map and $\operatorname{im} f' \subset \ker \pi'_a$. Since $\dim \ker \pi'_a = p + 1 - (p - 1 - a + 1) = a + 1 = \dim S_{a,0} = \dim \operatorname{im} f'$, $\ker \pi'_a$ is exactly the image of f', which is isomorphic to $S_{a,0}$.

When $a \notin \{0, p-1\}$, then, by Proposition B.1.3, the exact sequence cannot split since $\mathrm{End}_{\mathbb{F}_p[G]}(\pi(1, X^a))$ is a line. □

Remark The kernel of the map $\pi(1,1) \to S_{p-1,0}$ is isomorphic to $S_{0,0}$, so it is the unique line of $\pi(1,1)$ fixed by G. By Proposition B.1.1, the exact sequence of the previous definition is exactly $0 \to \mathbb{F}_p \to \pi(1,1) \to \mathrm{St} \to 0$; in particular, over $\mathbb{F}_p$, St is isomorphic to $\mathrm{Sym}^{p-1} R$.

Corollary B.5.8 *Let* $0 \leq a \leq b \leq p-1$, *there are exact sequences*

$$0 \to S_{b-a,a} \to \pi(X^a, X^b) \to S_{p-1-(b-a),b} \to 0,$$
$$0 \to S_{p-1-(b-a),b} \to \pi(X^b, X^a) \to S_{b-a,a} \to 0,$$

which split if and only if $(a, b) = (0, p-1)$ *or* $a = b$.

Proposition B.5.9 *Let* F *be any field extension of* $\mathbb{F}_p$ *and* V *be an irreducible representation of* G *over* F. *Then* V *is isomorphic to some* $S_{k,r}$.

Proof. – The F-vector space V^U is endowed with an action of the abelian group $B/U \simeq \mathbb{F}_p^{\times 2}$. It has exponent $p-1$ prime to p and the polynomial $X^{p-1} - 1$ splits in F with simple roots. So V^U is the direct sum of characters of B/U. Let $x \in V^U \backslash \{0\}$, $\alpha, \beta : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$ be such that for any $M = \begin{pmatrix} u & * \\ 0 & v \end{pmatrix} \in B$, $Mx = \alpha(u)\beta(v)x$. Write $\alpha = X^a, \beta = X^b$, then mapping $F(X^a, X^b)$ to Fx defines a nonzero morphism $\pi(X^a, X^b) \to V$. Since V is irreducible, this morphism is onto.

We know that there is an exact sequence $0 \to S_{q,r} \to \pi(X^a, X^b) \to S_{s,t} \to 0$. Since $S_{q,r} \to \pi(X^a, X^b) \to V$ is a morphism between two irreducible representations of G over F, it is either an isomorphism or zero. If it is an isomorphism, we are done; otherwise, the map $\pi(X^a, X^b) \to V$ factors as a map $\pi(X^a, X^b) \to S_{s,t} \to V$, so that $S_{s,t} \to V$ is surjective between irreducible representations, thus is an isomorphism. □

Appendix C

Modular forms and local constants

The goal of this appendix is to recall various classical results about local constants for Galois representations and modular forms. These results are mostly contained in [104], [103] for twists of modular forms and their local constants, as well as [21] and [160] for more general results about local constants. The point is to be able to reuse these results more systematically, thus more conveniently.

C.1 Gauss sums

We recall here a few classical results on Gauss sums that we will end up needing.

Definition C.1.1 Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character. Then its *Gauss sum* is

$$\mathfrak{g}(\chi) = \sum_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(x) e^{2i\pi x/N}.$$

We will usually assume that N is the conductor of χ, but this need not be always the case.

Lemma C.1.2 *Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a primitive Dirichlet character. Then*

$$|\mathfrak{g}(\chi)|^2 = \mathfrak{g}(\chi)\mathfrak{g}(\overline{\chi})\chi(-1) = N.$$

Proof. – The first equality is a direct computation, and the second equality is well-known, see for instance [123, Proposition VII.2.6]. □

The following result is well-known and due to Gauss, and a proof is given in [77, §6.4].

Proposition C.1.3 *Let p be an odd prime and $\lambda : \mathbb{F}_p^\times \to \{\pm 1\}$ be the unique nontrivial quadratic character. Then $\mathfrak{g}(\lambda) = u\sqrt{p}$, where $u = 1$ if $p \equiv 1 \pmod 4$ and $u = 3$ if $p \equiv 3 \pmod 4$.*

Lemma C.1.4 *Let q be a prime number, $Q \geq q^2$ be a power of q and $\alpha : (\mathbb{Z}/Q\mathbb{Z})^\times \to \mathbb{C}^\times$ be a primitive Dirichlet character. Then, there exists $z \in (\mathbb{Z}/Q\mathbb{Z})^\times$ such that for any Dirichlet character $\chi : (\mathbb{Z}/Q\mathbb{Z})^\times \to \mathbb{C}^\times$ with conductor $C \leq \sqrt{Q}$, $\mathfrak{g}(\alpha\chi) = \chi(z)\mathfrak{g}(\alpha)$.*

Proof. – This can be seen as a consequence of, say, [21, §23.6 Proposition], but let us give an explicit proof. In the situation of the statement, $C \mid Q$, so C is a power of q and $C^2 \mid Q$.

Write $Q = AB$ with $qB \geq A \geq B \geq q$ (if $Q = q^{2n+1}$, then $A = qB = q^{n+1}$, otherwise $A = B\sqrt{Q}$). Then the function $n \in \mathbb{Z}/B\mathbb{Z} \longmapsto \alpha(1 + An) \in \mathbb{C}^\times$ is well-defined and is a group homomorphism, so it is of the form $n \longmapsto e^{2i\pi tn/B}$ for some $t \in \mathbb{Z}/B\mathbb{Z}$.

Let $\chi : (\mathbb{Z}/Q\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character with conductor at most (hence dividing) B. Then

$$\mathfrak{g}(\alpha\chi) = \sum_{\substack{1\le k\le A\\(k,q)=1}} \sum_{0\le l<B} (\alpha\chi)(k(1+Al))e^{2i\pi k(1+Al)/Q} = \sum_{\substack{1\le k\le A\\(k,q)=1}} \alpha(k)\chi(k)e^{2i\pi k/Q} \sum_{0\le l<B} e^{2i\pi(kl+tl)/B}$$
$$= B \sum_{\substack{1\le k\le A\\k\equiv -t \pmod B}} \alpha(k)\chi(k)e^{2i\pi k/Q} = B\chi(-t) \sum_{\substack{1\le k\le A\\k\equiv -t \pmod B}} \alpha(k)e^{2i\pi k/Q},$$

so $z = -t$ satisfies the conditions. □

Lemma C.1.5 *Let p be an odd prime and $\psi : \mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times \to \mathbb{C}^\times$ be a nontrivial character. Let $a \in \mathbb{F}_p^\times \backslash \mathbb{F}_p^{\times 2}$, then $\psi(\sqrt{a}) \in \{\pm 1\}$ is well-defined and does not depend on the choice of a. Moreover, if $\tau : \mathbb{F}_{p^2} \to \mathbb{F}_p$ is the trace, one has*

$$\sum_{x\in\mathbb{F}_{p^2}^\times} \psi(x)e^{2i\pi\tau(x)/p} = p\psi(\sqrt{a}).$$

Proof. – The first part of the claim is clear, since $\sqrt{a}$ is defined (allowing for different a) up to multiplication by $\mathbb{F}_p^\times$, and $\psi(\sqrt{a})^2 = \psi(a) = 1$. Write $k = \mathbb{F}_{p^2}$ for short. Since ψ is a nontrivial character of $k^\times/\mathbb{F}_p^\times$, the sum of its values vanishes. Since τ is $\mathbb{F}_p$-linear and onto, its kernel is a $\mathbb{F}_p$-line. It is clear that $\sqrt{a} \in \ker\tau$, so $\ker\tau = \mathbb{F}_p\sqrt{a}$.

$$\sum_{x\in k^\times} \psi(x)e^{2i\pi\tau(x)/p} = \sum_{x\in k^\times/\mathbb{F}_p^\times} \psi(x) \sum_{t\in\mathbb{F}_p^\times} e^{2i\pi t\tau(x)/p} = \sum_{x\in k^\times/\mathbb{F}_p^\times} \psi(x)(p\mathbf{1}_{\tau(x)=0} - 1)$$
$$= p \sum_{\substack{x\in k^\times/\mathbb{F}_p^\times\\ \tau(x)=0}} \psi(x) = p\psi(\sqrt{a}).$$

□

C.2 Twists and local L-factors of newforms

Proposition C.2.1 *Let $k, N \ge 1$, $f \in \mathcal{S}_k(\Gamma_1(N))$ a normalized newform with primitive character χ of conductor M. Let $q \mid N$ be a prime, $Q = q^{v_q(N)}$ and $N' = N/Q$. Then*

- *If $q = Q$ is coprime to M, then $a_q(f)^2 = \chi(q)q^{k-2}$.*
- *If N/M is coprime to q, then $|a_q(f)|^2 = q^{(k-1)/2}$.*
- *Otherwise, $a_q(f) = 0$.*

Proof. – This is well-known, see for instance [121, Theorem 4.6.17]. □

Proposition C.2.2 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a normalized newform with primitive character χ of conductor C. Let $\psi : (\mathbb{Z}/D\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character of conductor $M \mid D$. There exists a unique normalized newform $f \otimes \psi \in \mathcal{S}_k(\Gamma_1(L))$ such that, for any prime $p \nmid ND$, $a_p(f \otimes \psi) = a_p(f)\psi(p)$. Moreover,*

(a) The newform $f \otimes \psi$ only depends on the primitive character attached to ψ.
(b) The primitive character of $f \otimes \psi$ is the primitive character attached to $\chi\psi^2$.
(c) L divides the least common multiple P of N, CM, M^2.
(d) For any prime number $q \nmid M$, $v_q(L) = v_q(N)$.
(e) Let q be a prime number, and write $\psi = \psi_q\psi'$, where ψ' has conductor prime to q and the conductor of ψ_q is a power of q. Then $v_q(L)$ only depends on f and ψ_q.

(f) Let $q \mid M$ be a prime such that $v_q(P) = v_q(N)$. If moreover $v_q(L) < v_q(N)$, then $\max(v_q(CM), v_q(M^2)) = v_q(N)$.

Proof. – The existence of $f \otimes \psi$ and (a) (b), (c) are a consequence of [104, Proposition 3.1] and the strong multiplicity one theorem [121, Theorem 4.6.19].

If $q \nmid M$ is a prime. By (c), one has $v_q(L) \leq v_q(N)$. On the other hand, since $f = (f \otimes \psi) \otimes \overline{\psi}$ by strong multiplicity one, N divides the least common multiple of $L, C'M, M^2$, where C' is the conductor of the character of $f \otimes \psi$. Since $v_q(C') \leq v_q(N)$ and $v_q(M) = 0$, $v_q(L) \leq v_q(N)$, so (d) holds, and (e) follows.

Let $q \mid M$ be a prime such that $v_q(CM)$ and $v_q(M^2)$ are both lower than $v_q(N)$, so that $v_q(P) = v_q(N)$. Let C' be the conductor of $\chi\psi^2$. Since $f = (f \otimes \psi) \otimes \overline{\psi}$, one has $v_q(N) \leq \max(v_q(L), v_q(C'M), v_q(M^2))$ by (c). Since one has $v_q(C') \leq \max(v_q(C), v_q(M))$, the assumptions imply that $v_q(N) \leq v_q(L)$. This proves the contrapositive of (f). □

Remark (c), (d) and (f) may look like [104, Theorem 3.1], but they are not exactly the same: *loc.cit.* discusses the modular form $\sum_{n\geq 1} a_n(f)\psi(n)q^n$, which need not be a newform.

C.3 Local constants and twists of newforms

Most of the statements of this section come from [104].

Let $k, N \geq 1$. Let $Q \mid N$ be a positive number, prime to $N' := N/Q$. Let $x, y, z, w \in \mathbb{Z}$ be such that $Q^2xw - Nyz = Q$, $y \equiv 1 \pmod{Q}, x \equiv 1 \pmod{N'}$. Then the map

$$W_Q : f \in \mathcal{S}_k(\Gamma_1(N)) \longmapsto f \mid_k \begin{pmatrix} Qx & y \\ Nz & Qw \end{pmatrix} \in \mathcal{S}_k(\Gamma_1(N)),$$

does not depend on the choice of x, y, z, w by [104, Proposition 1.1].

Proposition C.3.1 *Let k, N, Q, N' be as above. Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a normalized newform with primitive character χ, and write $\chi = \chi_Q\chi'_Q$, where the conductor of χ_Q (resp. χ'_Q) divides Q (resp. N'). Then there exists a constant $\lambda_Q(f) \in \mathbb{C}^\times$ and a normalized newform $g \in \mathcal{S}_k(\Gamma_1(N))$ such that:*

- *$W_Q(f) = \lambda_Q(f)g$,*
- *$\lambda_Q(f)$ is an algebraic number of complex modulus one.*
- *g is $f \otimes \overline{\chi'_Q}$.*

Moreover, one has $\lambda_Q(f)\lambda_Q(g) = \chi_Q(-1)\overline{\chi'_Q}(Q)$.

Proof. – This is proved in [104, §1]. □

Proposition C.3.2 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a normalized newform. The associated L-series $L(f,s) = \sum_{n\geq 1} \frac{a_n(f)}{n^s}$ converges absolutely when $\mathrm{Re}(s) > k/2+1$, and $s \longmapsto L(f,s)$ extends to an entire function (also denotes $L(f,s)$). The completed L-function $\Lambda(f,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(f,s)$ is entire and the following functional equation holds: $\Lambda(f,s) = (-i)^k\lambda_N(f)\Lambda(\overline{f}, k-s)$.*

Proof. – This is a classical computation, see for instance [41, Section 5.10] (but note that $\lambda_N(f)\overline{f}$ is $f \mid \begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix}$ rather than $f \mid \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$). □

The main case of interest is the situation where Q is a power of a prime $q \mid N$. In this case, we write W_q and λ_q for W_Q and λ_Q respectively.

Proposition C.3.3 *In the situation of Proposition C.3.1, assume furthermore that Q is the power of some prime $q \mid N$ such that $a_q(f) \neq 0$. Then $\lambda_Q(f) = Q^{k/2-1}\frac{\mathfrak{g}(\chi_q)}{a_Q(f)}$, where χ_q is viewed as a Dirichlet character modulo its conductor if it is not trivial, and modulo q otherwise.*

Proof. – This is [104, Theorem 2.1]. □

Proposition C.3.4 *Let k, N, Q, N', f, χ as in Proposition C.3.1. Let ψ be a primitive Dirichlet character of conductor M prime to Q. Then $\lambda_Q(f \otimes \psi) = \overline{\psi}(Q)\lambda_Q(f)$.*

Proof. – This can be deduced from [104] as follows. If D is an integer prime to Q, the automorphism W_Q of $\mathcal{S}_k(\Gamma_1(ND))$ extends the automorphism W_Q of $\mathcal{S}_k(\Gamma_1(N))$ (for the inclusion $\mathcal{S}_k(\Gamma_1(N)) \subset \mathcal{S}_k(\Gamma_1(ND))$).

Let C be the conductor of χ and P be the least common multiple of N, CM, M^2, so that P/N is prime to Q, By [104, Proposition 3.1], there exists a twisting operator

$$S_\psi : \sum_{n\geq 1} a_n q^n \in \mathcal{S}_k(\Gamma_1(N), \chi) \longmapsto \sum_{n\geq 1} a_n \psi(n) q^n \in \mathcal{S}_k(\Gamma_1(P), \chi\psi^2).$$

By [104, Proposition 3.4], one has $\overline{\psi}(Q) S_\psi W_Q = W_Q S_\psi$. Moreover, by [104, Proposition 3.2], we can write $(S_\psi f)(\tau) = g(\tau) + \sum_{t>1} \alpha_t g(t\tau)$, where $g = f \otimes \psi$ has conductor $L \mid P$, t runs through divisors of P/L and the α_t are complex numbers. By Theorem C.2.2, Q is coprime to P/L, so, by [104, Proposition 1.5], $W_Q g = W_Q(S_\psi f) - \sum_t \alpha'_t (W_Q g)(t\tau)$, and therefore

$$\begin{aligned}\lambda_Q(f \otimes \psi) = \lambda_Q(g) = a_1(W_Q g) = a_1(W_Q S_\psi f) = \overline{\psi}(Q) a_1(S_\psi W_Q f) \\ = \overline{\psi}(Q) a_1(W_Q(f)) = \overline{\psi}(Q)\lambda_Q(f).\end{aligned}$$

□

Corollary C.3.5 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a normalized newform with character χ. For each prime $q \mid N$, write $N = N_q N'_q$ with $N_q = q^{v_q(N)}$, and $\chi = \chi_q \chi'_q$, where χ_q, χ'_q are characters modulo N_q and N'_q respectively. Then $\lambda_N(f) = \prod_{q|N} \lambda_q(f)\chi'_q(N_q)$.*

Proof. – Let $Q_1, Q_2 \geq 1$ be coprime divisors of N such that Q_i is prime to N/Q_i. Then, by [104, Proposition 1.4], one has

$$\overline{\chi_{Q_2}}(Q_1)\lambda_{Q_1Q_2}(f) = a_1(W_{Q_2}(W_{Q_1} f)) = \lambda_{Q_1}(f)\lambda_{Q_2}(f \otimes \overline{\chi_{Q_1}}) = \chi_{Q_1}(Q_2)\lambda_{Q_1}(f)\lambda_{Q_2}(f),$$

so $\lambda_{Q_1Q_2}(f) = \lambda_{Q_1}(f)\lambda_{Q_2}(f)\chi_{Q_1}(Q_2)\chi_{Q_2}(Q_1)$.

One deduces by induction that for any $Q \geq 1$ dividing N and coprime to N/Q,

$$\lambda_Q(f) = \prod_{p,q|Q, q\neq r} \lambda_q(f)\chi_p(N_q),$$

and the conclusion follows after taking $Q = N$. □

Definition C.3.6 Given a normalized newform $f \in \mathcal{S}_k(\Gamma_1(N))$ with primitive character χ and a prime number $p \mid N$, write $\chi = \chi_p \chi'_p$, where the conductor of χ_p (resp. χ'_p) is a power of p (resp. prime to p). We denote $\varepsilon_p(f) = \lambda_p(f)\chi'_p(p^{v_p(N)})$. Thus, $\lambda_N(f) = \prod_{p|N} \varepsilon_p(f)$. If $p \nmid N$, we define $\varepsilon_p(f)$ as equal to 1.

Lemma C.3.7 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a normalized newform with character χ. Let ψ be a primitive Dirichlet character of conductor P, where $P \nmid N$ is a power of some prime p. Write $N = N_p N'$ with $N_p = p^{v_p(N)} < P$, $\chi = \chi_p \chi'_p$, where χ_p (resp. χ'_p) has conductor dividing N_p (resp. dividing N'). Then*

- *The exact level of the modular form $g = \sum_{n\geq 1} a_n(f)\psi(n)e^{2i\pi n\tau}$ is $N'P^2$.*
- *If $N_p = 1$, then $W_{NP^2}(g) = \lambda_N(f)\psi(-N)\chi(P)\frac{\mathfrak{g}(\psi)}{\mathfrak{g}(\overline{\psi})}\overline{g}$.*

Proof. – The first part is [104, Theorem 3.1 ii)], so we assume that $N_p = 1$. Then W_{NP^2} is the action of the matrix $\begin{pmatrix} 0 & 1 \\ -NP^2 & 0 \end{pmatrix}$. Let $1 \leq u, v \leq P$ be coprime to p and such that $Nuv \equiv -1$

(mod P). Then there exists some matrix $A_u \in \Gamma_0(N)$ such that $[A]_{1,1} \equiv P \pmod N$ and

$$\begin{pmatrix} 1 & u/P \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -NP^2 & 0 \end{pmatrix} = P \begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix} A \begin{pmatrix} 1 & v/P \\ 0 & 1 \end{pmatrix}.$$

For each $1 \leq u \leq P$ prime to p, there is a unique $1 \leq v \leq P$ prime to p such that $Nuv \equiv -1 \pmod P$, and every v comes from a unique u. Therefore,

$$\begin{aligned} W_{NP^2}(\mathfrak{g}(\overline{\psi})g) &= \sum_{1\leq u\leq P,(u,P)=1} \overline{\psi}(u) f \mid \begin{pmatrix} 1 & u/P \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -NP^2 & 0 \end{pmatrix} \\ &= \sum_{1\leq v\leq P,(v,p)=1} \psi(-Nv)(\langle P\rangle^{-1}(f \mid W_N)) \mid \begin{pmatrix} 1 & v/P \\ 0 & 1 \end{pmatrix} \\ &= \psi(-N) \sum_{1\leq v\leq P,(v,p)=1} \psi(v)\lambda_N(f)\chi(P)\overline{f} \mid \begin{pmatrix} 1 & v/P \\ 0 & 1 \end{pmatrix} \\ &= \psi(N)\lambda_N(f)\chi(P) \overline{\sum_{1\leq v\leq P,(v,p)=1} \overline{\psi}(v) f \mid \begin{pmatrix} 1 & v/P \\ 0 & 1 \end{pmatrix}} \\ &= \psi(N)\lambda_N(f)\chi(P)\overline{\mathfrak{g}(\overline{\psi})}\overline{g} = \psi(-N)\lambda_N(f)\chi(P)\mathfrak{g}(\psi)\overline{g}. \end{aligned}$$

□

Corollary C.3.8 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a normalized newform with character χ. Let $M > 1$ be an integer coprime to N and ψ a primitive Dirichlet character of conductor M. Then*

$$f \otimes \psi = \sum_{n\geq 1} a_n(f)\psi(n)e^{2i\pi n\tau} \in \mathcal{S}_k(\Gamma_1(NM^2))$$

is a newform of conductor NM^2 and

$$\lambda_{NM^2}(g) = \lambda_N(f)\psi(-N)\chi(M)\frac{\mathfrak{g}(\psi)}{\mathfrak{g}(\overline{\psi})}.$$

Proof. – When M is a power of a prime number m, by Lemma C.3.7, it is enough to show that the modular form $g(\tau) = \sum_{n\geq 1} a_n(f)\psi(n)e^{2i\pi n\tau} \in \mathcal{S}_k(\Gamma_1(NM^2))$ is a newform (of conductor NM^2): by strong multiplicity one, this implies that $g = f \otimes \psi$. This then follows from the definition of g and [102, Theorem 9].

For a general M, it is enough to proceed by induction after we check that for any primitive Dirichlet characters ψ_1, ψ_2 with coprime conductors M_1, M_2, then

$$\mathfrak{g}(\psi_1\psi_2) = \psi_1(M_2)\psi_2(M_1)\mathfrak{g}(\psi_1)\mathfrak{g}(\psi_2).$$

This equality is true because $(a, b) \in (\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times \longmapsto aM_2 + bM_1 \in (\mathbb{Z}/M_1M_2\mathbb{Z})^\times$ is a bijection. □

Proposition C.3.9 *Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be a normalized newform with character χ and q a prime number (possibly not dividing N). Let $Q = q^{v_q(N)}, N' = N/Q$, and write $\chi = \chi_q\chi'_q$ as in the previous statements. Let ψ be a primitive Dirichlet character whose conductor is some power $Q_1 > 1$ of q with $Q \mid Q_1$. Assume that $\psi\chi_q$ and ψ have the same conductor (which is automatic if $Q_1 > Q$). Then*

$$f \otimes \psi = \sum_{n\geq 1} a_n(f)\psi(n)e^{2i\pi n\tau}$$

has conductor $N'Q_1^2$, and

$$\lambda_q(f\otimes\psi)=\overline{\chi'_q}(Q_1)\psi(-1)\frac{\mathfrak{g}(\chi_q\psi)}{\mathfrak{g}(\overline{\psi})}.$$

Proof. – If $q\nmid N$, the first part follows from Corollary C.3.8. To prove the second part, one has:

$$\begin{aligned}
\lambda_{NQ_1^2}(f\otimes\psi)&=\lambda_N(f)\psi(-N)\chi(M)\frac{\mathfrak{g}(\psi)}{\mathfrak{g}(\overline{\psi})},\\
\lambda_{NQ_1^2}(f\otimes\psi)&=\lambda_q(f\otimes\psi)\chi(Q_1^2)\prod_{p|N}\lambda_p(f\otimes\psi)(\chi'_p\psi^2)(N_p)\\
&=\lambda_q(f\otimes\psi)\chi(Q_1)^2\prod_{p|N}\lambda_p(f)\chi'_p(N_p)\psi(N_p)\\
&=\lambda_q(f\otimes\psi)\chi(Q_1)^2\psi(N)\prod_{p|N}\lambda_p(f)\chi'_p(N_p)\\
&=\lambda_q(f\otimes\psi)\chi(Q_1)^2\psi(N)\lambda_N(f),
\end{aligned}$$

whence the conclusion.

So we may assume that $q\mid N$, and then the statement follows from [104, Theorem 4.1]. □

Corollary C.3.10 *Let $f\in\mathcal{S}_k(\Gamma_1(N))$ be a newform with conductor χ, $M>1$ and ψ a primitive Dirichlet character of conductor M. Let L be the conductor of $f\otimes\psi$, and $q\mid M$ be a prime number such that $v_q(M)\geq v_q(N)$, and such that $\psi_q\chi_q$ has the same conductor as ψ_q (where $\chi=\chi_q\chi'_q$, the conductor of χ_q is a power of q, that of χ'_q is coprime to q). Then $v_q(L)=2v_q(M)$.*

Proof. – Since $v_q(L)$ only depends on ψ_q, we may assume $\psi=\psi_q$, and this is a consequence of Proposition C.3.9. □

Bibliography

[1] N. Adžaga, V. Arul, L. Beneish, M. Chen, S. Chidambaram, T. Keller, and B. Wen, *Quadratic Chabauty for Atkin-Lehner quotients of modular curves of prime level and genus 4, 5, 6*, Acta Arith. **208** (2023), no. 1, 15–49.

[2] S. Anantharaman, *Schémas en groupes, espaces homogènes et espaces algébriques sur une base de dimension* 1, Sur les groupes algébriques, no. 33, Soc. Math. France, 1973, pp. 5–79.

[3] S. Arias-de-Reyna and L. Dieulefait, *Automorphy of* $\mathrm{GL}_2 \otimes \mathrm{GL}_n$ *in the self-dual case*, 2022, arXiv preprint 1611.06918v3.

[4] The Stacks Project Authors, *Stacks project*.

[5] A. Bajolet, Y. Bilu, and B. Matschke, *Computing integral points on* $X_{ns}^+(p)$, Algebra Number Theory **15** (2021), no. 3, 569–608.

[6] M. H. Baker, *Torsion points on modular curves*, Invent. Math. **140** (2000), no. 3, 487–509.

[7] Benjamin Bakker and Jacob Tsimerman, *p-torsion monodromy representations of elliptic curves over geometric function fields*, Ann. of Math. (2) **184** (2016), no. 3, 709–744.

[8] S. Balakrishnan, N. Dogra, S. Müller, J. Tuitman, and J. Vonk, *Explicit Chabauty–Kim for the split Cartan modular curve of level* 13, Ann. of Math. (2) **189** (2019), no. 3, 885–944.

[9] ———, *Quadratic Chabauty for modular curves: algorithms and examples*, Compos. Math. **159** (2023), no. 6, 1111–1152.

[10] F. Bars, A. Kontogeorgis, and X. Xarles, *Bielliptic and hyperelliptic modular curves* $X(N)$ *and the group* $Aut(X(N))$, Acta Arith. **161** (2013), no. 3, 283–299.

[11] L. Berger and S. Rozensztajn, *Modular representations of* $GL_2(\mathbb{F}_p)$, Found online.

[12] Y. Bilu and P. Parent, *Serre's uniformity problem in the split Cartan case*, Ann. of Math. **173** (2011), no. 1, 569–584.

[13] Y. Bilu, P. Parent, and M. Rebolledo, *Rational points on* $X_0^+(p^r)$, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984.

[14] S. Bloch and K. Kato, *L-Functions and Tamagawa Numbers of Motives*, The Grothendieck Festschrift: A Collection of Articles Written in Honor of the 60th Birthday of Alexander Grothendieck (P. Cartier, L. Illusie, N. M. Katz, G. Laumon, Y. I. Manin, and K. A. Ribet, eds.), Birkhäuser Boston, Boston, MA, 2007, pp. 333–400.

[15] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Ergeb. Math. Grenzgeb. (3), Springer-Verlag, 1990.

[16] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR MR1484478

[17] G. Boxer, F. Calegari, T. Gee, and V. Pilloni, *Abelian surfaces over totally real fields are potentially modular*, Publ. Math. Inst. Hautes Études Sci. **134** (2021), no. 1, 153–501.

[18] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the Modularity of Elliptic Curves Over* $\mathbf{Q}$*: Wild 3-Adic Exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.

[19] F. Brumley, Private communication.

[20] D. Bump, *Automorphic forms and representations*, Cambridge Stud. Adv. Math., Cambridge Univ. Press, 1997.

[21] C. J. Bushnell and G. Henniart, *The Local Langlands Conjecture for GL(2)*, 1st ed. 2006. ed., Grundlehren Math. Wiss., no. 335, Springer, 2006.

[22] L. Caporaso, J. Harris, and B. Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. **10** (1997), no. 1, 1–35.

[23] H. Carayol, *Sur les représentations l-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. Éc. Norm. Supér. 4 **19** (1986), no. 3, 409–468.

[24] ———, *Preuve de la conjecture de Langlands locale pour* GL_n *: travaux de Harris-Taylor et Henniart*, Séminaire Bourbaki : volume 1998/99, exposés 850-864, Astérisque, no. 266, Soc. Math. France, 2000, Exposé 857.

[25] I. Chen, *On Relations between Jacobians of Certain Modular Curves*, J. Algebra **231** (2000), no. 1, 414–448.

[26] L. Clozel, *Motives and automorphic representations*, Autour des motifs—École d'été Franco-Asiatique de Géométrie Algébrique et de Théorie des Nombres / Asian-French Summer School on Algebraic Geometry and Number Theory. Vol. III (J.-B. Bost and J.-M. Fontaine, eds.), Panor. Synthèses, vol. 49, Soc. Math. France, 2016, pp. 29–60.

[27] J. W. Cogdell, *Lectures on L-Functions, Converse Theorems, and Functoriality for* $GL(n)$.

[28] R. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765 – 770.

[29] ———, *Torsion points on curves and p-adic abelian integrals*, Ann. of Math. **121** (1985), no. 1, 111–168.

[30] B. Conrad, *Finite Group Schemes over Bases with Low Ramification*, Compos. Math. **119** (1999), no. 3, 239–326.

[31] ———, *Grothendieck duality and base change*, Lecture Notes in Math., vol. 1750, Springer, 2000.

[32] B. Conrad, F. Diamond, and R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), no. 2, 521–567.

[33] J. Cremona and N. Freitas, *Global methods for the symplectic type of congruences between elliptic curves*, Rev. Mat. Iberoam. **38** (2022), no. 1, 1–32.

[34] H. Deconinck, *The generalized Fermat equation over totally real number fields*, Unpublished, online at `https://wrap.warwick.ac.uk/id/eprint/81893/1/WRAP_Theses_Deconinck_2016.pdf`, last accessed Oct 25th 2024, July 2016.

[35] P. Deligne, *Les Constantes des Equations Fonctionnelles des Fonctions L*, Modular Functions of One Variable II (Berlin, Heidelberg) (P. Deligne and W. Kuijk, eds.), Springer Berlin Heidelberg, 1973, pp. 501–597.

[36] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular Functions of One Variable II (Berlin, Heidelberg) (P. Deligne and W. Kuijk, eds.), Springer Berlin Heidelberg, 1973, pp. 143–316.

[37] P. Deligne and J.-P. Serre, *Formes modulaires de poids* 1, Ann. Sci. Éc. Norm. Supér. 4 **7** (1974), no. 4, 507–530.

[38] M. Demazure and A. Grothendieck, *Schémas en groupes. Tome I, Propriétés générales des schémas en groupes : Séminaire de géométrie algébrique du Bois Marie, 1962-64, SGA 3*, Lecture Notes in Math., vol. 151, Springer, 1962–64.

[39] F. Diamond, Private communication.

[40] ———, *On deformation rings and Hecke rings*, Ann. of Math. **144** (1996), no. 1, 137–166.

[41] Fred Diamond and Jerry Shurman, *A First Course in Modular Forms*, Grad. Texts in Math., vol. 228, Springer, 2005.

[42] L. Dieulefait, *Langlands base change for $GL(2)$*, Ann. of Math. (2) **176** (2012), no. 2, 1015–1038.

[43] ———, *Automorphy of* $\mathrm{Symm}^5(GL(2))$ *and base change*, J. Math. Pures Appl. (9) **104** (2015), no. 4, 619–656.

[44] N. Dogra and S. Le Fourn, *Quadratic Chabauty for modular curves and modular forms of rank one*, Math. Ann. **380** (2021), no. 1, 393–448.

[45] G. Faltings, *Finiteness Theorems for Abelian Varieties over Number Fields*, Arithmetic Geometry (G. Cornell and J. H. Silverman, eds.), Springer New York, New York, NY, 1986, pp. 9–27.

[46] T. Fisher, *The Hessian of a genus one curve*, Proc. Lond. Math. Soc. (3) **104** (2012), no. 3, 613–648.

[47] ———, *On families of 7- and 11-congruent elliptic curves*, LMS J. Comput. Math. **17** (2014), no. 1, 536–564.

[48] ———, *On families of 13-congruent elliptic curves*, 2019, arXiv preprint 1912.10777.

[49] ———, *On pairs of 17-congruent elliptic curves*, 2021, arXiv preprint 2106.02033.

[50] J.-M. Fontaine, *Il n'y a pas de variété abélienne sur* $\mathbb{Z}$., Invent. Math. **81** (1985), 515–538.

[51] O. Forster, *Lectures on Riemann surfaces*, Grad. Texts in Math., vol. 81, Springer-Verlag, New York Heidelberg Berlin, 1981.

[52] N. Freitas, *On the Fermat-type equation $x^3 + y^3 = z^p$*, Comment. Math. Helv. **91** (2016), 295–304.

[53] N. Freitas and A. Kraus, *On the symplectic type of isomorphisms of the p-torsion of elliptic curves*, Mem. Amer. Math. Soc. **277** (2022), no. 1361, v+105.

[54] N. Freitas, B. Naskręcki, and M. Stoll, *The generalized Fermat equation with exponents 2, 3, n*, Compos. Math. **156** (2020), no. 1, 77–113.

[55] G. Frey, *Links between stable elliptic curves and certain diophantine equations*, Ann. Univ. Sarav. Ser. Math. **1** (1986), no. 1, iv+40.

[56] ———, *On Ternary Equations of Fermat Type and Relations with Elliptic Curves*, Modular forms and Fermat's Last Theorem (G. Cornell, J. H. Silverman, and G. Stevens, eds.), Springer-Verlag NY, 1997, pp. 527–548.

[57] A. Fröhlich and J. Queyrut, *On the functional equation of the Artin L-function for characters of real representations*, Invent. Math. **20** (1973), no. 2, 125–138.

[58] L. Furio and D. Lombardo, *Serre's uniformity question and proper subgroups of* $C_{ns}^{+}(p)$, 2023, arXiv preprint 2305.17780.

[59] T. Gee, *Modularity lifting theorems*, Essential Number Theory **1** (2022), no. 1, 73–126.

[60] S. S. Gelbart, *Automorphic forms on Adele groups*, Ann. of Math. Stud., vol. 83, Princeton Univ. Press, 1975.

[61] ———, *Three lectures on the modularity of* $\overline{\rho}_{E,3}$ *and the Langlands Reciprocity Conjecture*, Modular forms and Fermat's Last Theorem (G. Cornell, J. H. Silverman, and G. Stevens, eds.), Springer-Verlag NY, 1997, pp. 155–207.

[62] J. R. Getz and H. Hahn, *An Introduction to Automorphic Representations. With a view toward trace formulae*, Grad. Texts in Math., vol. 300, Springer International Publishing, 2024.

[63] E. Ghate, E. González-Jiménez, and J. Quer, *On the Brauer class of modular endomorphism algebras*, Int. Math. Res. Not. IMRN **2005** (2005), no. 12, 701–723.

[64] B. H. Gross and M. Reeder, *Arithmetic invariants of discrete Langlands parameters*, Duke Math. J. **154** (2010), no. 3, 431–508.

[65] A. Grothendieck, *Techniques de construction et théorèmes d'existence en géométrie algébrique III : préschémas quotients*, Séminaire Bourbaki: années 1960/61, exposés 205–222, Séminaire Bourbaki, no. 6, Soc. Math. France, 1961, pp. 99–118.

[66] A. Grothendieck and J. Dieudonné, *Éléments de géométrie algébrique : III. Étude cohomologique des faisceaux cohérents, Seconde partie*, Publ. Math. Inst. Hautes Études Sci. **17** (1963), 5–91 (fr). MR 163911

[67] ———, *Éléments de géométrie algébrique : IV. Étude locale des schémas et des morphismes de schémas, Quatrième partie*, Publ. Math. Inst. Hautes Études Sci. **32** (1967), 5–361 (fr).

[68] A. Grothendieck and M. Raynaud, *Revêtements étales et groupe fondamental : Séminaire de géométrie algébrique du Bois Marie, 1960-61, SGA 1*, Lecture Notes in Math., vol. 224, Springer, 1960–61.

[69] A. J. Hahn and O. T. O'Meara, *The Classical Groups and K-Theory*, Grundlehren Math. Wiss., no. 291, Springer-Verlag, 1989.

[70] E. Halberstadt, *Calculs explicites sur les courbes modulaires*, Feb 2021.

[71] E. Halberstadt and A. Kraus, *Courbes de Fermat: résultats et problèmes*, J. reine angew. Math. **548** (2002), 167–234.

[72] ———, *Sur la courbe modulaire* $X_E(7)$, Exp. Math. **12** (2003), no. 1, 27–40.

[73] D. Harari, *Galois Cohomology and Class Field Theory*, Universitext., Springer, 2020.

[74] Y. Hellegouarch, *Étude des points d'ordre fini des variétés abéliennes de dimension un définies sur un anneau principal*, J. Reine Angew. Math. **244** (1970), 20–36.

[75] ———, *Courbes elliptiques et équation de Fermat*, 1972, Thèse.

[76] H. Hida, *Elementary Theory of L-functions and Eisenstein Series*, London Math. Soc. Stud. Texts, Cambridge Univ. Press, 1993.

[77] K. F. Ireland and M. I. Rosen, *A classical introduction to modern number theory*, Grad. Texts in Math., vol. 84, Springer International Publishing, 1990.

[78] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc. Colloq. Publ, AMS, Providence (R.I.), 2004.

[79] H. Jacquet, *Automorphic forms on $GL(2)$ Part II*, Lecture Notes in Math., vol. 278, Springer Berlin Heidelberg, 1972.

[80] H. Jacquet and R. Langlands, *Automorphic forms on $GL(2)$*, Lecture Notes in Math., no. 114, Springer-Verlag, 1970.

[81] A. Jorza, *Complex representations of $GL_2(\mathbb{F}_q)$*, Found online.

[82] E. J. Kani and O. G. Rizzo, *Mazur's question on mod 11 representations of elliptic curves*, preprint.

[83] E. J. Kani and W. Schanz, *Modular diagonal quotient surfaces*, Math. Z. **227** (1998), no. 2, 337–366.

[84] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Cohomologies p-adiques et applications arithmétiques (III) (P. Berthelot, J.-M. Fontaine, L. Illusie, K. Kato, and M. Rapoport, eds.), Astérisque, no. 295, Soc. Math. France, 2004. MR 2104361

[85] N. Katz, *p-adic properties of modular schemes and modular forms*, Modular Functions of One Variable III (Berlin, Heidelberg) (W. Kuijk and J.-P. Serre, eds.), Springer Berlin Heidelberg, 1973, pp. 69–190.

[86] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, no. 108, Princeton University Press, 1985.

[87] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (I)*, Invent. Math. **178** (2009), no. 3, 485–504.

[88] ———, *Serre's modularity conjecture (II)*, Invent. Math. **178** (2009), no. 3, 505–586.

[89] M. Kim, *The motivic fundamental group of $\mathbb{P}^1\backslash\{0,1,\infty\}$ and the theorem of Siegel.*, Invent. math. **161** (2005), 629–656.

[90] ———, *The unipotent Albanese map and Selmer varieties for curves*, Publ. Res. Inst. Math. Sci. **45** (2009), 89–133.

[91] M. Kim and A. Tamagawa, *The l-component of the unipotent Albanese map*, Math. Ann. **340** (2008), 223 – 235.

[92] G. Kings, D. Loeffler, and S. Zerbes, *Rankin-Eisenstein classes and explicit reciprocity laws*, Camb. J. Math. **5** (2017), no. 1, 1–122.

[93] S. L. Kleiman, *Relative duality for quasi-coherent sheaves*, Compos. Math. **41** (1980), no. 1, 39–60.

[94] V. A. Kolyvagin and D. Y. Logachëv, *Finiteness of the Shafarevich-Tate group and the group of points for some modular abelian varieties*, Algebra i Analiz **1** (1989), no. 5, 171–196.

[95] A. Kraus, *Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique*, Dissertationes Math. (Rozprawy Mat.) **364** (1997), 39.

[96] ———, *Sur l'équation* $\{a^3 + b^3 = c^p\}$, Exp. Math. **7** (1998), no. 1, 1 – 13.

[97] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur.*, Math. Ann. **293** (1992), no. 2, 259–276.

[98] A. Kumar, *Hilbert modular surfaces for square discriminants and elliptic subfields of genus 2 function fields*, Res. Math. Sci. **2** (2015), Art. 24, 46 p.

[99] S. Lang, *Algebraic number theory*, 2nd edition ed., Grad. Texts in Math., vol. 110, Springer, 1994.

[100] ———, *Complex Analysis*, 4th ed., Grad. Texts in Math., vol. 103, Springer, New York, 1999.

[101] S. Le Fourn and P. Lemos, *Residual Galois representations of elliptic curves with image contained in the normaliser of a nonsplit Cartan*, Algebra Number Theory **15** (2021), no. 3, 747–771.

[102] W.-C. W. Li, *Newforms and Functional Equations*, Math. Ann. **212** (1975), no. 4, 285–315.

[103] ———, *L-series of Rankin type and their functional equations*, Math. Ann. **244** (1979), no. 2, 135–166.

[104] W.-C. W. Li and A.O.L. Atkin, *Twists of Newforms and Pseudo-Eigenvalues of W-Operators*, Invent. Math. **48** (1978), 221–244.

[105] Q. Liu, D. Lorenzini, and M. Raynaud, *Néron models, Lie algebras, and reduction of curves of genus one*, Invent. math. **157** (2004), no. 3, 455–518.

[106] Q. Liu and E. Reinie, *Algebraic geometry and arithmetic curves*, Oxf. Grad. Texts Math., Oxford University Press, 2002.

[107] The LMFDB Collaboration, *The L-functions and modular forms database*, `https://www.lmfdb.org`, 2023, [Online; accessed 12 June 2023].

[108] D. Loeffler, *Images of adelic Galois representations for modular forms*, Glasg. Math. J. **59** (2017), no. 1, 11—25.

[109] D. Loeffler and J. Weinstein, *On the computation of local components of a newform*, Math. Comp. **81** (2012), 1179–1200.

[110] D. Masser and G. Wüstholz, *Isogeny estimates for abelian varieties, and finiteness theorems*, Ann. of Math. (2) **137** (1993), no. 3, 459–472.

[111] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. Inst. Hautes Études Sci. **47** (1977), 33–186.

[112] ———, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), no. 2, 129–162, With an appendix by D. Goldfeld.

[113] ———, *Open problems regarding rational points on curves and varieties*, Galois Representations in Arithmetic Algebraic Geometry (A. J. Scholl and R. L. Taylor, eds.), London Math. Soc. Lecture Note Ser., Cambridge Univ. Press, 1998, pp. 239–266.

[114] B. Mazur and K. Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc., Amer. Math. Soc., Providence (R.I.), 2004.

[115] W. McCallum and B. Poonen, *The Method of Chabauty and Coleman*, Explicit methods in number theory, Panor. Synthèses, vol. 36, Soc. Math. France, 2012, pp. 99–117.

[116] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1, 437–449.

[117] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), no. 3, 177–190.

[118] ———, *Abelian varieties*, Arithmetic Geometry (G. Cornell and J. H. Silverman, eds.), Springer-Verlag, 1985, pp. 102–150.

[119] ———, *Jacobian varieties*, Arithmetic Geometry (G. Cornell and J. H. Silverman, eds.), Springer-Verlag, 1985, pp. 167–212.

[120] ———, *Arithmetic duality theorems*, 2nd edition ed., BookSurge, 2006.

[121] T. Miyake, *Modular forms*, Springer Monogr. Math., Springer, 1989.

[122] F. Momose, *On the ℓ-adic representations attached to modular forms*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 1, 89–109. MR 617867

[123] J. Neukirch, *Algebraic number theory*, Grundlehren Math. Wiss., Springer, cop. 1999, transl. from German by N. Schappacher.

[124] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Grundlehren Math. Wiss., vol. 323, Springer, 2008, Second edition.

[125] J. Newton and J. Thorne, *Symmetric power functoriality for holomorphic modular forms*, Publ. Math. Inst. Hautes Études Sci. **134** (2021), no. 1, 1–116.

[126] ———, *Symmetric power functoriality for holomorphic modular forms, II*, Publ. Math. Inst. Hautes Études Sci. **134** (2021), no. 1, 117–152.

[127] J. Newton and J. A. Thorne, *Symmetric power functoriality for Hilbert modular forms*, 2022, arXiv preprint 2212.03595.

[128] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. **506** (1999), 85–116.

[129] F. Pellarin, *Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques*, Acta Arith. **100** (2001), no. 3, 203–243.

[130] B. Poonen, E. Schaefer, and M. Stoll, *Twists of $X(7)$ and primitive solutions to $x^2+y^3 = z^7$*, Duke Math. J. **137** (2007), no. 1, 103 – 158.

[131] D. Prasad, *Notes on modular representations of p-adic groups, and the Langlands Correspondence*, Found online.

[132] K. A. Ribet, *Galois representations attached to eigenforms with nebentypus*, Modular Functions of one Variable V (Berlin, Heidelberg) (J.-P. Serre and D. Zagier, eds.), Springer Berlin Heidelberg, 1977, pp. 18–52.

[133] ———, *On ℓ-adic representations attached to modular forms. II*, Glasgow Math. J. **27** (1985), 185–194. MR 819838

[134] ———, *On modular representations of* $(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 1, 431–476.

[135] ———, *Report on mod l representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Part 2, Amer. Math. Soc., Providence, RI, 1994, pp. 639–676.

[136] K. A. Ribet and W. A. Stein, *Lectures on Serre's conjectures*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, With appendices by B. Conrad and K. Buzzard., pp. 143–232.

[137] K. Rubin, *Euler systems*, Ann. of Math. Stud., Princeton Univ. Press, 2000.

[138] K. Rubin and A. Silverberg, *Families of elliptic curves with constant mod p representations*, Elliptic curves, modular forms, and Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, vol. I, Int. Press, Cambridge, MA, 1995, pp. 148–161.

[139] J.-P. Serre, *Local Class Field Theory*, Algebraic Number Theory: Proceedings of an Instructional Conference (J.W.S. Cassels and A. Frölich, eds.), Academic Press Inc. (London) Ltd, 1967.

[140] ———, *Abelian ell-adic representations and elliptic curves : McGill University lecture notes*, W. A. Benjamin, Inc., New York Amsterdam, 1968.

[141] ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1971), no. 4, 259–331.

[142] ———, *Linear representations of finite groups*, 1st ed. 1977. ed., Grad. Texts in Math., vol. 42, Springer New York, 1977.

[143] ———, *Local fields*, Grad. Texts in Math., no. 67, Springer, 1979, translated from French by Marvin J. Greenberg.

[144] ———, *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. Inst. Hautes Études Sci. **54** (1981), 123–201.

[145] ———, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.

[146] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517.

[147] S. Shatz, *Group Schemes, Formal Groups, and p-Divisible Groups*, Arithmetic Geometry (G. Cornell and J. H. Silverman, eds.), Springer-Verlag, 1985, pp. 102–150.

[148] G. Shimura, *The special values of the zeta functions associated with cusp forms*, Comm. Pure Appl. Math. **29** (1976), no. 6, 783–804.

[149] ———, *On the periods of modular forms*, Math. Ann. **229** (1977), no. 3, 211 – 221.

[150] ———, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, 1994.

[151] S. Siksek, *The Modular Approach to Diophantine Equations*, Explicit methods in number theory, Panor. Synthèses, vol. 36, Soc. Math. France, 2012, pp. 151–179.

[152] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math., vol. 151, Springer-Verlag, 1994, Second printing.

[153] ———, *The arithmetic of elliptic curves*, 2nd ed. 2009. ed., Grad. Texts in Math., no. 106, Springer New York, 2009.

[154] W. A. Stein, *Modular forms, a computational approach*, vol. 79, Am. Math. Soc., 2007.

[155] E. Studnia, *On obstructions to the Euler system method for Rankin-Selberg convolutions*, 2024, arXiv preprint 2401.17769.

[156] T. Szamuely, *Galois groups and fundamental groups*, Cambridge Stud. Adv. Math., Cambridge Univ. Press, 2009.

[157] R. Takloo-Bighash, *Spinor L-functions, theta correspondence, and Bessel coefficients*, Forum Math. **19** (2007), no. 3, 487–554, With an appendix by P. Michel.

[158] J. Tate, *Fourier analysis in number fields and Hecke's zeta-functions*, Algebraic Number Theory: Proceedings of an Instructional Conference (J.W.S. Cassels and A. Frölich, eds.), Academic Press Inc. (London) Ltd, 1967.

[159] ———, *p-Divisible Groups*, Proceedings of a Conference on Local Fields (Berlin, Heidelberg) (T. A. Springer, ed.), Springer Berlin Heidelberg, 1967, pp. 158–183.

[160] ———, *Number theoretic background*, Automorphic forms, representations and *L*-functions, Part 2, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979, pp. 3–26.

[161] The PARI Group, Univ. Bordeaux, *PARI/GP version `2.13.3`*, 2023, available from `http://pari.math.u-bordeaux.fr/`.

[162] V. Vatsal, *Special Value Formulae for Rankin L-Functions*, Heegner Points and Rankin L-Series (H. Darmon and S.-W. Zhang, eds.), Math. Sci. Res. Inst. Publ., Cambridge Univ. Press, 2004, pp. 165—-190.

[163] C. Virdol, *Zeta functions of twisted modular curves*, J. Aust. Math. Soc. **80** (2006), no. 1, 89–103.

[164] L. Washington, *Galois cohomology*, Modular forms and Fermat's Last Theorem (G. Cornell, J. H. Silverman, and G. Stevens, eds.), Springer-Verlag NY, 1997, pp. 101–120.

[165] G. Wiese, *Galois representations*, Online, last accessed May 13th 2024.

[166] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. **141** (1995), no. 3, 443–551.

[167] D. Zywina, *On the possible images of the mod ell representations associated to elliptic curves over* $\mathbb{Q}$, 2015, arXiv preprint 1508.07660.

[168] ———, *On the surjectivity of mod ℓ representations associated to elliptic curves*, Bull. Lond. Math. Soc. **54** (2022), no. 6, 2404–2417.

Elie STUDNIA — Université Paris Cité, Sorbonne Université, CNRS, IMJ-PRG, F-75013 Paris, France