On the André-Oort conjecture for Hilbert modular surfaces. *

Bas Edixhoven†

April 5, 2000

1 Introduction.

In order to state the conjecture mentioned in the title, we need to recall some terminology and results on Shimura varieties; as a general reference for these, we use [19, Sections 1–2]. So let $\mathbb{S} := \mathrm{Res}_{\mathbb{C}/\mathbb{R}}\mathbb{G}_{\mathrm{m},\mathbb{C}}$ be the algebraic group over $\mathbb{R}$ obtained by restriction of scalars from $\mathbb{C}$ to $\mathbb{R}$ of the multiplicative group. For V an $\mathbb{R}$-vector space, it is then equivalent to give an $\mathbb{R}$-Hodge structure or an action by $\mathbb{S}$ on it. A Shimura datum is a pair (G, X), with G a connected reductive affine algebraic group over $\mathbb{Q}$, and X a $G(\mathbb{R})$-conjugacy class in the set of morphisms of algebraic groups $\mathrm{Hom}(\mathbb{S}, G_{\mathbb{R}})$, satisfying the three conditions of [19, Def. 1.4] (i.e., the usual conditions (2.1.1–3) of [13]). These conditions imply that X has a natural complex structure (in fact, the connected components are hermitian symmetric domains), such that every representation of G on a $\mathbb{Q}$-vector space defines a polarizable variation of Hodge structure on X. For (G, X) a Shimura datum, and K a compact open subgroup of $G(\mathbb{A}_{\mathrm{f}})$, we let $\mathrm{Sh}_K(G, X)(\mathbb{C})$ denote the complex analytic variety $G(\mathbb{Q})\backslash(X \times G(\mathbb{A}_{\mathrm{f}})/K)$, which has a natural structure of quasi-projective complex algebraic variety, denoted $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$; the projective limit $\mathrm{Sh}(G, X)_{\mathbb{C}}$ over all K of the $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ is a scheme on which $G(\mathbb{A}_{\mathrm{f}})$ acts continuously. (The action being continuous means that the scheme has a cover by open affines $U_i = \mathrm{Spec}(A_i)$ such that each U_i is stabilized by some open subgroup K_i of $G(\mathbb{A}_{\mathrm{f}})$ and each f in A_i has open stabilizer in K_i.) A

*A preprint version of this article together with an appendix that could be considered as the author's scratch paper while working on this subject can be downloaded from the author's home page. This appendix contains details that the author does not find interesting enough to publish, but that may be helpful for readers who got lost.

†partially supported by the Institut Universitaire de France, and by the European TMR Network Contract ERB FMRX 960006 "arithmetic algebraic geometry".

morphism of Shimura data from (G_1, X_1) to (G_2, X_2) is a morphism $f\colon G_1 \to G_2$ that maps X_1 to X_2; for K_1 and K_2 compact open subgroups of $G_1(\mathbb{A}_{\mathrm{f}})$ and $G_2(\mathbb{A}_{\mathrm{f}})$ with $f(K_1)$ contained in K_2, such an f induces a morphism $\mathrm{Sh}(f)$ from $\mathrm{Sh}_{K_1}(G_1, X_1)_{\mathbb{C}}$ to $\mathrm{Sh}_{K_2}(G_2, X_2)_{\mathbb{C}}$.

1.1 Definition. Let (G, X) be a Shimura datum, K an open compact subgroup of $G(\mathbb{A}_{\mathrm{f}})$, and Z an irreducible closed subvariety of $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$. Then Z is a *subvariety of Hodge type* if there is a Shimura datum (G', X'), a morphism of Shimura data $f\colon (G', X') \to (G, X)$, and an element g of $G(\mathbb{A}_{\mathrm{f}})$ such that Z is an irreducible component of the image of the map:

$$\mathrm{Sh}(G', X')_{\mathbb{C}} \xrightarrow{\mathrm{Sh}(f)} \mathrm{Sh}(G, X)_{\mathbb{C}} \xrightarrow{\cdot g} \mathrm{Sh}(G, X)_{\mathbb{C}} \longrightarrow \mathrm{Sh}_K(G, X)_{\mathbb{C}}.$$

This definition is equivalent to [19, 6.2], which uses only closed immersions $f\colon G' \to G$. In [20, Prop. 2.8] it is explained that the subvarieties of Hodge type are precisely the loci where certain given classes in certain variations of Hodge structures (obtained from representations of G) are Hodge classes; hence the terminology.

1.2 Definition. Let (G, X) be a Shimura datum. For h in X we let $\mathrm{MT}(h)$ be the Mumford-Tate group of h, i.e., the smallest algebraic subgroup H of G such that h factors through $H_{\mathbb{R}}$. A point h in X is called *special* if $\mathrm{MT}(h)$ is commutative (in which case it is a torus). For K a compact open subgroup of $G(\mathbb{A}_{\mathrm{f}})$, a point in $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ is special if its preimages in $\mathrm{Sh}(G, X)_{\mathbb{C}}$ are of the form (h, g) with h in X special. Equivalently, the special points in $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ are the zero dimensional subvarieties of Hodge type.

1.3 Conjecture. (André-Oort) *Let (G, X) be a Shimura datum. Let K be a compact open subgroup of $G(\mathbb{A}_{\mathrm{f}})$ and let S be a set of special points in $\mathrm{Sh}_K(G, X)(\mathbb{C})$. Then every irreducible component of the Zariski closure of S in $\mathrm{Sh}_K(G, X)_{\mathbb{C}}$ is a subvariety of Hodge type.*

Some remarks are in order at this point. André stated this conjecture as a problem for curves containing infinitely many special points in general Shimura varieties in [2, X.4]. Independently, Oort raised the question for general subvarieties of the moduli spaces of principally polarized abelian varieties in [25]. In [2, X.4] André mentions the similarity with the Manin-Mumford conjecture (proved by Raynaud, see [1]), and [4] contains a version generalizing both the conjecture above and the Manin-Mumford conjecture; see also [19, 6.7.2].

Let us now discuss the results on the conjecture above that have been obtained until now. All of them deal with moduli spaces of abelian varieties. Moonen proved in his thesis (see [21, §5], in particular the equivalence between Conjectures 5.1 and 5.3, and [18, IV]) that the conjecture is true for sets S for which there exists a prime number p at which all s in S have an ordinary reduction of which they are the canonical lift. Needless to say, his methods use reduction modulo a prime number p. This gives a quite general result, but it has the disadvantage that one neglects most of the Galois action on the special points, and that one has to work with one Frobenius element simultaneously for all s in S.

In [14], the conjecture was proved for the moduli space of pairs of elliptic curves, assuming the generalized Riemann hypothesis (GRH) for imaginary quadratic fields. In a few words, the proof exploits the Galois action on CM-points and considers intersections of the subvarieties in question with images of them under suitable Hecke operators. In this approach, we work with a different Frobenius element for each s in S; GRH comes in via the existence of small primes with suitable properties. The same case of Conjecture 1.3 was proved unconditionally by André in [5]. He uses the Galois action on the CM-points, and a Diophantine approximation result of Masser on the j-function.

More recently, Yafaev has generalized the result in [14] to the case of products of two Shimura curves that are associated to quaternion algebras over $\mathbb{Q}$, see [31], and B. Belhaj Dahman, a student of André, is working on the families of jacobians of the curves

$$y^n = x(x-1)(x-\lambda).$$

The question about these families of jacobians is whether or not the various isogeny factors coming from the decomposition for the action of $\mu_n(\mathbb{C})$ are simultaneously of CM type for infinitely many complex numbers λ.

Recently, Clozel and Ullmo have proved ([10]), for G among GSp_{2n} and GL_n, that sets of the form $T_p x$, with x in $G(\mathbb{Q})\backslash G(\mathbb{A})/K$ and T_p certain Hecke operators with p tending to infinity, are equidistributed. The idea behind this is that one would like to imitate and apply the equidistribution results for Galois orbits of strict sequences of points of small height in abelian varieties as in [1]. A sequence of closed points of an algebraic variety is called strict if every proper closed subset contains only finitely many elements of the sequence. Phrased in this terminology, the André-Oort conjecture says that a sequence of special points is strict if no proper subvariety of Hodge type contains an infinite subsequence. Of course, to prove the André-Oort conjecture in this way, one has to replace $T_p x$ by the Galois orbit of x, which seems to be a hard problem, and moreover, one has to deal with the fact that the heights of CM points tend to infinity and not to zero.

In this article, we prove the Conjecture 1.3, assuming GRH, for Hilbert modular surfaces. The method of proof is basically the same as in [14], but now we do use more advanced techniques. The two main results of the article are described in Section 2. The reason for which we state and prove Theorem 2.2 is that it has an interesting application to transcendence of special values of certain hypergeometric functions via work of Wolfart, Cohen and Wüstholz, see [11], *without* having to assume GRH.

Let us briefly describe the contents of this article. Section 2 introduces the Hilbert modular surfaces that we work with in terms of a Shimura datum, gives their interpretation as moduli spaces of abelian surfaces with multiplications by the ring of integers of a real quadratic field K, and states the main results.

Section 3, which is not so essential, discusses the difference between working with abelian surfaces with or without a given polarization. In group theoretical terms, the choice is between working with $\mathrm{GL}_2(K)$ or its subgroup $\mathrm{GL}_2(K)'$ consisting of the elements of $\mathrm{GL}_2(K)$ whose determinant is in $\mathbb{Q}^*$. The reason for considering both cases is that with a polarization (and a suitable level structure), the variation of Hodge structure provided by the lattices of the abelian surfaces comes from a representation of the group in the Shimura datum, which is not true without given polarizations. We need variations of Hodge structure in Section 4. On the other hand, the size of Galois orbits of special points, studied in Section 6, is simpler to understand in terms of class groups when working without polarizations. We could have chosen to work throughout the article with $\mathrm{GL}_2(K)'$, but we think that it is instructive to see the consequences of such a choice in the relatively easy case of Hilbert modular surfaces, before trying to treat general Shimura varieties completely in group theoretical terms.

In Section 4 we recall an important result of André, relating the generic Mumford-Tate group of a variation of Hodge structure to its algebraic monodromy group (i.e., the Zariski closure of the image of monodromy). We use it to prove that for a curve in a Hilbert modular surface that is not of Hodge type and that does contain a special point, the connected algebraic monodromy group is maximal, i.e., $\mathrm{SL}_{2,K}$.

Section 5 introduces the Hecke correspondence T_p associated to a prime number p. We use a very powerful result of Nori in order to prove that for C a curve with maximal algebraic monodromy group, T_pC is irreducible if C is large enough.

The main result of Section 6 says that the size of the Galois orbit of a special point x grows at least as a positive power of the discriminant $\mathrm{discr}(R_x)$ of the ring of endomorphisms (commuting with the real multiplications) of the corresponding abelian variety. This section is quite long, and contains some messy computations, depending on the structure of the Galois group of the normal closure of the CM field in question. The problem is that one has to give a lower bound for the image under the reflex type norm of one class group in another.

Section 7 gives an upper bound for the number of points in intersections of the form $Z_1 \cap T_g Z_2$, with Z_1 and Z_2 fixed subvarieties of a general Shimura variety, and with T_g a varying Hecke correspondence.

Finally, Section 8 combines all these preliminary results as follows. One supposes that C is a curve in a Hilbert modular surface S, containing infinitely many special points, and not of Hodge type. If p is large enough (depending only on C), then T_pC is irreducible by Section 5.

Since the T_p-orbits in S are dense, one cannot have $C = T_pC$. Hence the intersections $C \cap T_pC$ are finite, and hence bounded above (Section 7) by a constant times p^2. Let now x be a special point on C. If p is a prime that is split in R_x, then $C \cap T_pC$ contains the Galois orbit of x, hence $|C \cap T_pC|$ grows at least as a positive power of $|\mathrm{discr}(R_x)|$. But this lower bound for primes that are split in R_x contradicts the conditional effective Chebotarev theorem (this is where GRH comes in). Hence, assuming GRH, one has proved that if C does contain infinitely many special points, then C is of Hodge type. The reason that one can prove Thm. 2.2 unconditionally is that in that case the CM field $\mathbb{Q} \otimes R_x$ is independent of x, and hence Chebotarev's theorem itself is sufficient.

In April 1999, we have proved Conjecture 1.3, assuming GRH, for arbitrary products of modular curves, extending the methods of [14]. A detailed proof, which is quite elementary, will be written up in the near future. One can hope that combining the techniques used for these last two results will make it possible to treat more general higher dimensional cases of Conjecture 1.3. Of course, eventually everything should be expressed in terms of "(G, X)-language". In fact, in this article we could already have worked without mentioning abelian varieties.

Before we really start, let us first mention two obvious general principles. The first is that level structures don't matter in Conjecture 1.3: for (G, X) a Shimura datum, K and K' open compact in $G(\mathbb{A}_\mathrm{f})$ with $K \subset K'$, an irreducible subvariety Z of $\mathrm{Sh}_K(G, X)_\mathbb{C}$ is of Hodge type if and only if its image in $\mathrm{Sh}_{K'}(G, X)_\mathbb{C}$ is. The second principle says that the irreducible components of intersections of subvarieties of Hodge type are again of Hodge type (this is clear from the interpretation of subvarieties of Hodge type given right after Definition 1.1).

2 The main results.

Let K be a real quadratic extension of $\mathbb{Q}$, let O_K be its ring of integers, and let G be the $\mathbb{Z}$-group scheme $\mathrm{Res}_{O_K/\mathbb{Z}}(\mathrm{GL}_{2,O_K})$. After numbering the two embeddings of K in $\mathbb{R}$, we have $\mathbb{R} \otimes K = \mathbb{R}^2$, and hence $G(\mathbb{R}) = \mathrm{GL}_2(\mathbb{R})^2$. We will study the Shimura variety:

$$S(\mathbb{C}) := G(\mathbb{Q})\backslash(X \times G(\mathbb{A}_\mathrm{f})/G(\hat{\mathbb{Z}})),$$

where $X = (\mathbb{H}^\pm)^2$, and where $\mathbb{H}^\pm$ is the usual $\mathrm{GL}_2(\mathbb{R})$-conjugacy class of morphisms from $\mathbb{S}$ to $\mathrm{GL}_{2,\mathbb{R}}$, i.e., the class of $a + bi \mapsto \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$. The surface $S_\mathbb{C}$, called a Hilbert modular surface, is the coarse moduli space for pairs (A, α) with A an abelian surface and α a morphism from O_K to $\mathrm{End}(A)$ (see [30, Ch. X], and the end of Section 3 for the moduli interpretation for a closely related Shimura datum). This implies that the reflex field of (G, X) is $\mathbb{Q}$ and that the canonical model $S_\mathbb{Q}$ (see [19, Section 2] for this notion) is simply the coarse moduli space for pairs $(A/S/\mathbb{Q}, \alpha)$ with S a $\mathbb{Q}$-scheme, A/S an abelian scheme of relative dimension two, and α a morphism from O_K to $\mathrm{End}_S(A)$. The set of geometrically connected components of $S_{\mathbb{Q}}$ is $K^*\backslash\mathbb{A}_K^*/(\mathbb{R}\otimes K)^{*,+}O_K^{\wedge *} = \mathrm{Pic}(O_K)^+$, the group of isomorphism classes of invertible O_K-modules with orientations at the two infinite places, and has trivial action by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ([30, Ch. I, Cor. 7.3]). The main objective of this article is to prove the following two theorems.

2.1 Theorem. *Assume GRH. Let $C \subset S_{\mathbb{C}}$ be an irreducible closed curve containing infinitely many CM points. Then C is of Hodge type.*

2.2 Theorem. *Let $C \subset S_{\mathbb{C}}$ be an irreducible closed curve containing infinitely many CM points corresponding to abelian varieties that lie in one isogeny class (the isogenies are not required to be compatible with the multiplications by O_K). Then C is of Hodge type.*

Let us note immediately that these theorems apply in fact to all Hilbert modular surfaces, because the André-Oort conjecture is insensitive to level structure. Before proving the theorems we need to discuss some of the tools we will use in it.

3 Choosing a suitable Shimura variety.

For a variation of Hodge structure on a complex variety, one has the notions of generic Mumford-Tate group and that of monodromy. A relation between these two notions will be very useful for us. In order to get a suitable variation of Hodge structure on $S(\mathbb{C})$ as above, there is a little complication, and at least two options to get around it. The problem is that the tautological representation of $G_{\mathbb{Q}}$ on the $\mathbb{Q}$-vector space K^2 does not induce a variation of Hodge structure on $\mathrm{Sh}_H(G_{\mathbb{Q}}, X)(\mathbb{C})$, even if H is an arbitrary small open subgroup of $G(\mathbb{A}_{\mathrm{f}})$; just consider the action of O_K^* in $G(\mathbb{Q})$ on $X \times G(\mathbb{A}_{\mathrm{f}})/H$ (see [20, Section 2.3] for a general statement).

The first possible way out is to use an other representation, and have the monodromy take place in the image of G under this representation. For example, one can take the representation $\mathrm{Sym}^2(\rho_0) \otimes \det(\rho_0)^{-1}$, with ρ_0 the tautological representation on O_K^2. This representation induces a faithful representation ρ of the quotient $G^{\mathrm{ad}} = \mathrm{Res}_{O_K/\mathbb{Z}}\mathrm{PGL}_{2,O_K}$. The morphism $G \to G^{\mathrm{ad}}$ induces an isomorphism from X to a conjugacy class X^{ad} in $\mathrm{Hom}_{\mathbb{R}}(\mathbb{S}, G^{\mathrm{ad}}_{\mathbb{R}})$, and gives a morphism of Shimura data from (G, X) to $(G^{\mathrm{ad}}, X^{\mathrm{ad}})$. Let $S^{\mathrm{ad}}(\mathbb{C})$ be the Shimura variety $\mathrm{Sh}_{G^{\mathrm{ad}}(\hat{\mathbb{Z}})}(G^{\mathrm{ad}}, X^{\mathrm{ad}})(\mathbb{C})$. The natural morphism from $S_{\mathbb{C}}$ to $S^{\mathrm{ad}}_{\mathbb{C}}$ is finite and surjective (this follows directly from the definition); one can show that it is the quotient for a faithful action of $\mathrm{Pic}(O_K)$, but that will not be used. Conjecture 1.3 is then true for $S_{\mathbb{C}}$ if and only if it is true for $S^{\mathrm{ad}}_{\mathbb{C}}$, and ρ induces a variation of Hodge structure on $\mathrm{Sh}_H(G^{\mathrm{ad}}, X^{\mathrm{ad}})(\mathbb{C})$ for suitable H. The disadvantage of working with $S^{\mathrm{ad}}_{\mathbb{C}}$ is that it does not seem to have an interpretation as a moduli space of abelian varieties; this is not a real problem, but we prefer to work with Shimura varieties that are as simple as possible.

Another way out is to replace the group G by its subgroup G' given by the following Cartesian diagram:

$$\begin{array}{ccc} G' & \hookrightarrow & G \\ \downarrow & \square & \downarrow_{\det} \\ \mathbb{G}_{\mathrm{m},\mathbb{Z}} & \hookrightarrow & \mathrm{Res}_{O_K/\mathbb{Z}}\mathbb{G}_{\mathrm{m},O_K} \end{array}$$

Loosely speaking, G' is the subgroup of G consisting of those elements whose determinant is in $\mathbb{Q}$. As the morphism $\det$ in the diagram above is smooth, G' is smooth over $\mathbb{G}_{\mathrm{m},\mathbb{Z}}$, hence over $\mathbb{Z}$. It follows that G' is the scheme-theoretic closure in G of its generic fibre. We note that $G'(\mathbb{R})$ is the subgroup of (x,y) in $\mathrm{GL}_2(\mathbb{R})^2$ with $\det(x) = \det(y)$. All h in X factor through $G'_{\mathbb{R}}$, but X consists of two $G'(\mathbb{R})$-conjugacy classes. The conjugacy class X' we work with is the disjoint union of $(\mathbb{H}^+)^2$ and $(\mathbb{H}^-)^2$. This gives a morphism of Shimura data from (G', X') to (G, X), and a morphism of Shimura varieties $S'_{\mathbb{C}} \to S_{\mathbb{C}}$ with $S'_{\mathbb{C}} = \mathrm{Sh}_{G'(\hat{\mathbb{Z}})}(G', X')_{\mathbb{C}}$. One can prove that the Shimura variety $S'_{\mathbb{C}}$ is connected, and that the morphism to its image in $S_{\mathbb{C}}$ is the quotient by a faithful action of the finite group $O_K^{*,+}/O_K^{*,2}$, i.e., by the group of totally positive global units modulo squares of global units. We will only use that the morphism $S'_{\mathbb{C}} \to S_{\mathbb{C}}$ is finite and that its image is open and closed; these two facts follow directly from the definitions. It follows that Conjecture 1.3 is true for $S_{\mathbb{C}}$ if and only if it is for $S'_{\mathbb{C}}$, and similarly for the two theorems above that we want to prove. Moreover, the tautological representation of G' does induce a variation of Hodge structure on $\mathrm{Sh}_H(G', X')(\mathbb{C})$ for H sufficiently small.

The option we choose is the last. The variety $S'_{\mathbb{C}}$ is the (coarse) moduli space for triplets (A, α, λ) where:

$$\left\{ \begin{array}{l} A \text{ is a complex abelian surface,} \\ \alpha\colon O_K \to \mathrm{End}(A) \text{ a morphism of rings,} \\ \text{and } \lambda\colon A \to A^* \text{ a principal } O_K\text{-polarization,} \end{array} \right. \tag{3.1}$$

a notion that we will now explain. First of all, A^* is the dual of A in the category of abelian varieties with O_K-action: $A^* := \mathrm{Ext}^1(A, O_K \otimes \mathbb{G}_{\mathrm{m}})$. One verifies that $A^* = \delta \otimes_{O_K} A^t$, where δ is the different of the extension $\mathbb{Z} \to O_K$, and where $A^t = \mathrm{Ext}^1(A, \mathbb{G}_{\mathrm{m}})$, the dual of A in the usual sense. The inclusion $\delta \subset O_K$ induces a morphism $A^* \to A^t$, which is an isogeny. A principal O_K-polarization is then an isomorphism $\lambda\colon A \to A^*$ such that the induced morphism from A to A^t is a polarization. Interpreted in Hodge-theoretical terms, a triplet (A, α, λ) as in (3.1) corresponds to a triplet (V, h, ψ) with V a locally free O_K-module of rank two, $h\colon \mathbb{S} \to (\mathrm{GL}_{\mathbb{Z}}(V))_{\mathbb{R}}$ a Hodge structure of type $(-1,0), (0,-1)$, and $\psi\colon V \times V \to O_K$ a perfect antisymmetric O_K-bilinear form such that $\mathrm{tr} \circ \psi\colon V \times V \to \mathbb{Z}$ is a polarization. Note that for such a triplet (V, h, ψ), the pair (V, ψ) is isomorphic to the standard pair $(O_K \oplus O_K, (\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}))$. In order to prove that the set of isomorphism classes of (A, α, λ) as in (3.1) is $S'(\mathbb{C})$ one uses the following two facts: 1: $G'(\mathbb{A}_f)/G'(\hat{\mathbb{Z}})$ is the set of O_K-lattices in K^2 on which $\psi = (\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix})$ induces a perfect pairing of O_K-modules, up to a factor in $\mathbb{Q}^*$; and 2: X' is the set of Hodge structures of type $(-1, 0)$, $(0, -1)$ on the K-vector space K^2 such that, up to sign, $\mathrm{tr} \circ \psi$ is a polarization. The moduli space over $\mathbb{Q}$ of triplets $(A/S, \alpha, \lambda)$ with S a $\mathbb{Q}$-scheme, $\alpha \colon O_K \to \mathrm{End}_S(A)$ a morphism of rings, and λ a principal O_K-polarization, is then the canonical model $S'_{\mathbb{Q}}$ of $S'_{\mathbb{C}}$ (see also [27, 1.27] and [12, 4.11]).

For $n \geq 1$, let H_n be the kernel of the morphism $G'(\hat{\mathbb{Z}}) \to G'(\mathbb{Z}/n\mathbb{Z})$, and let $S'_{\mathbb{Q},n}$ denote the Shimura variety $\mathrm{Sh}_{H_n}(G', X')_{\mathbb{Q}}$. Then $S'_{\mathbb{Q},n}$ is the moduli space for 4tuples $(A/S, \alpha, \lambda, \phi)$, with S a $\mathbb{Q}$-scheme, $(A/S, \alpha, \lambda)$ an abelian scheme over S with multiplications by O_K and a principal O_K-polarization, and with ϕ an isomorphism of S-group schemes with O_K-action:

$$\phi \colon (O_K/nO_K)_S^2 \longrightarrow A[n],$$

such that there exists a (necessarily unique) isomorphism $\overline{\phi} \colon (\mathbb{Z}/n\mathbb{Z})_S \to \mu_{n,S}$ making the diagram:

$$\begin{array}{ccc} ((O_K/nO_K)_S^2)^2 & \xrightarrow{\phi} & A[n]^2 \\ \downarrow \psi_n & & \downarrow e_{\lambda,n} \\ O_K \otimes (\mathbb{Z}/n\mathbb{Z})_S & \xrightarrow{\mathrm{id}\otimes\overline{\phi}} & O_K \otimes \mu_{n,S} \end{array}$$

commutative. In this diagram, ψ_n is the pairing given by $(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix})$, and $e_{\lambda,n}$ is the perfect pairing on $A[n]$ induced by λ. For $n \geq 3$ the objects $((A/S, \alpha, \lambda))$ have no non-trivial automorphisms (see [22, IV, Thm. 5]), and $S'_{\mathbb{Q},n}$ is a fine moduli space. (Representability by an algebraic space can be found in [27, §1.23]. Quasi-projectiveness follows from [7].) In particular, for $n \geq 3$ we do have a polarized variation of $\mathbb{Z}$-Hodge structure on $S'_n(\mathbb{C})$, given by the first homology groups of the fibers of the universal family.

4 Monodromy and generic Mumford-Tate groups.

We recall some results that can be found in [20, Sections 1.1–1.3], with references to [9] and [3].

The Mumford-Tate group $\mathrm{MT}(V)$ of a $\mathbb{Q}$-Hodge structure V, given by $h \colon \mathbb{S} \to \mathrm{GL}(V)_{\mathbb{R}}$, is defined to be the smallest algebraic subgroup H of $\mathrm{GL}(V)_{\mathbb{Q}}$ such that h factors through $H_{\mathbb{R}}$. Equivalently, $\mathrm{MT}(V)$ is the intersection in $\mathrm{GL}(V)$ of all stabilizers of all lines generated by Hodge classes (i.e., of some type (p,p)) in all $\mathbb{Q}$-Hodge structures of the form $\oplus_i V^{\otimes n_i} \otimes (V^*)^{\otimes m_i}$.

For S a smooth complex algebraic variety with a polarizable variation of $\mathbb{Q}$-Hodge structure V on the associated analytic variety $S(\mathbb{C})$, there is a countable union Σ of proper algebraic subvarieties such that $s \mapsto \mathrm{MT}(V_s)$ is locally constant outside Σ (this makes sense because V is a locally constant sheaf on $S(\mathbb{C})$). The smallest such Σ is called the Hodge exceptional locus, and its complement the Hodge generic locus. For s in $S(\mathbb{C})$ and not in Σ, $\mathrm{MT}(V_s) \subset \mathrm{GL}(V_s)$ is called the generic Mumford-Tate group (at s).

Assume now that S is connected, and that we have an element s of $S(\mathbb{C})$. Then the locally constant sheaf V corresponds to a representation $\rho\colon \pi_1(S(\mathbb{C}), s) \to \mathrm{GL}(V_s)$, called the monodromy representation. The algebraic monodromy group is defined to be the smallest algebraic subgroup H of $\mathrm{GL}(V_s)$ such that ρ factors through H, i.e., it is the Zariski closure of the image of ρ; its connected component of identity is called the connected algebraic monodromy group, and denoted $\mathrm{AM}(V_s)$. With these hypotheses, we have the following theorem.

4.1 Theorem. (André) *Assume moreover that V admits a $\mathbb{Z}$-structure, that s in $S(\mathbb{C})$ is Hodge generic, and that there is a point t in $S(\mathbb{C})$ such that $\mathrm{MT}(V_t)$ is abelian (i.e., t is special). Then $\mathrm{AM}(V_s)$ is the derived subgroup $\mathrm{MT}(V_s)^{\mathrm{der}}$ of $\mathrm{MT}(V_s)$, i.e., the algebraic subgroup generated by commutators.*

Let us now consider what this theorem implies for the variation of Hodge structure that we have on $S'_n(\mathbb{C})$ ($n \geq 3$), and, more importantly, for its restrictions to subvarieties of $S'_n(\mathbb{C})$. The Hodge exceptional locus of $S'_n(\mathbb{C})$ is by construction the union of all lower dimensional subvarieties of Hodge type. The generic Mumford-Tate group on $S'_n(\mathbb{C})$ is G' (use that it contains a subgroup of finite index of $G'(\mathbb{Z})$, and that for all $h = (h_1, h_2)\colon \mathbb{C}^* \to \mathrm{GL}_2(\mathbb{R})^2$ in X' one has $\det(h_1(z)) = z\bar{z} = \det(h_2(z))$ for all z).

4.2 Proposition. *Let $n \geq 3$. Let C be an irreducible curve in $S'_{\mathbb{C},n}$ (i.e., an irreducible closed subvariety of dimension one); let C^{nor} denote its normalization and C^{sm} its smooth locus. Then C is of Hodge type if and only if the generic Mumford-Tate group on C^{sm} is strictly smaller than $G'_{\mathbb{Q}}$. If C is not of Hodge type and contains a special point, then the connected algebraic monodromy group on C^{nor} equals ${G'}_{\mathbb{Q}}^{\mathrm{der}} = \mathrm{Res}_{K/\mathbb{Q}}\mathrm{SL}_{2,K}$.*

Proof. Suppose that C is of Hodge type. Then some element in some tensor construction of the variation of Hodge structure on $S'_{\mathbb{C},n}$ is a Hodge class on C, but not on $S'_{\mathbb{C},n}$. The interpretation of the Mumford-Tate group as stabilizer of lines generated by Hodge classes shows that the generic Mumford-Tate group on C^{sm} is strictly smaller than $G'_{\mathbb{Q}}$. Now suppose that the generic Mumford-Tate group on C^{sm} is strictly smaller than $G'_{\mathbb{Q}}$. Then C does carry an extra Hodge class. The locus where this class is a Hodge class is necessarily of dimension one, hence, C, being an irreducible component of it, is of Hodge type. The second statement follows now from André's theorem above. $\square$

5 Irreducibility of images under Hecke correspondences.

For (G, X) a Shimura datum, K_1 and K_2 open subgroups of $G(\mathbb{A}_f)$, and g in $G(\mathbb{A}_f)$, one has the so-called Hecke correspondence T_g that is defined as follows. Consider the diagram:

$$\mathrm{Sh}_{K_1}(G,X)_{\mathbb{C}} \xleftarrow{\pi_1} \mathrm{Sh}(G,X)_{\mathbb{C}} \xrightarrow{\cdot g} \mathrm{Sh}(G,X)_{\mathbb{C}} \xrightarrow{\pi_2} \mathrm{Sh}_{K_2}(G,X)_{\mathbb{C}},$$

where π_1 and π_2 are the quotient maps for the actions by K_1 and K_2, respectively. The morphism $\pi_2 \circ \cdot g$ is the quotient for the action of gK_2g^{-1}, hence π_1 and $\pi_2 \circ \cdot g$ both factor through the quotient by $K := K_1 \cap gK_2g^{-1}$, and T_g is the correspondence:

$$\mathrm{Sh}_{K_1}(G,X)_{\mathbb{C}} \xleftarrow{\overline{\pi_1}} \mathrm{Sh}_{K}(G,X)_{\mathbb{C}} \xrightarrow{\overline{\pi_2 \circ \cdot g}} \mathrm{Sh}_{K_2}(G,X)_{\mathbb{C}}.$$

Of course, T_g exists already over the reflex field E of (G, X). In particular, for Z a closed subvariety of $\mathrm{Sh}_{K_1}(G,X)_E$, its image T_gZ is a closed subvariety of $\mathrm{Sh}_{K_2}(G,X)_E$.

We now specialize to our situation, i.e., to the Shimura datum (G', X') as above. For p a prime number, we let T_p be the Hecke correspondence on $S'_{\mathbb{Q}}$ given by the element $g(p)$ in $G'(\mathbb{A}_f)$ with $g(p)_p = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $g(p)_l = 1$ for l different from p. Note that $g(p)^{-1}$ gives the same correspondence as $g(p)$ does, because $g(p) = \left(\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)g(p)^{-1}\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. The modular interpretation of T_p is the following. Let $[(A, \lambda)]$ in $S'(\mathbb{C})$ denote the isomorphism class of a complex abelian surface A with multiplications by O_K and with a principal O_K-polarization λ. Then, as a cycle, the image of $[(A, \lambda)]$ is given by:

$$T_p[(A,\lambda)] = \sum_H [(A/H, \overline{p\lambda})],$$

where H ranges through the O_K/pO_K-submodules of $A[p](\mathbb{C})$ that are free of rank one, and where $\overline{p\lambda}$ is the principal O_K-polarization induced by $p\lambda$ on A/H. In order to see this, one uses, as in Section 3, that $G'(\mathbb{A}_f)/G'(\hat{\mathbb{Z}})$ is the set of O_K-lattices in K^2 on which $\psi = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ induces a perfect pairing of O_K-modules, up to a factor in $\mathbb{Q}^*$, and that the correspondence on it induced by $g(p)^{-1}$ sends such a lattice to the set of lattices containing it with quotient free of rank one over O_K/pO_K.

5.1 Proposition. *Let C be an irreducible curve in $S'_{\mathbb{C}}$. Suppose that C is not of Hodge type and that it contains a special point. Then, for all primes p large enough, T_pC is irreducible.*

Proof. Let $n \geq 3$ be some integer, and let C_n be an irreducible component of the inverse image of C in $S'_{\mathbb{C},n}$. Irreducibility of T_pC_n implies that of T_pC. Let V denote the polarized variation of $\mathbb{Z}$-Hodge structure on $S'_n(\mathbb{C})$ that we considered before, let s be in $C_n(\mathbb{C})$. We choose an isomorphism of O_K-modules from O_K^2 to V_s. Let $\rho\colon \pi_1(C_n(\mathbb{C}), s) \to \mathrm{SL}_2(O_K)$ be the monodromy representation. Proposition 4.2 implies that the Zariski closure in G' of $\rho(\pi_1(C_n^{\mathrm{nor}}(\mathbb{C}), s))$ is the subgroup $\mathrm{Res}_{O_K/\mathbb{Z}}\mathrm{SL}_{2,O_K}$. For p prime, the correspondence T_p on $S'_{\mathbb{C},n}$ is given by a diagram:

$$S'_{\mathbb{C},n} \xleftarrow{\pi_1} S'_{\mathbb{C},n,p} \xrightarrow{\pi_2} S'_{\mathbb{C},n}.$$

For $T_pC_n = \pi_2\pi_1^{-1}C_n$ to be irreducible, it suffices that $C_{n,p}$ be irreducible, with $C_{n,p}$ the covering of C_n^{nor} obtained from π_1. But this covering corresponds to the $\pi_1(C_n^{\mathrm{nor}}(\mathbb{C}), s)$-set $\mathbb{P}^1(O_K/pO_K)$ of O_K/pO_K-submodules of $(O_K/pO_K)^2$ that are free of rank one. Nori's Theorem [24, Thm. 5.1] (Theorem 5.2 below) implies that for p large enough, the reduction map from $\pi_1(C_n^{\mathrm{nor}}(\mathbb{C}), s)$ to $\mathrm{SL}_2(O_K/pO_K)$ is surjective. Since $\mathrm{SL}_2(O_K/pO_K)$ acts transitively on $\mathbb{P}^1(O_K/pO_K)$, irreducibility follows. □

5.2 Theorem. (Nori) *Let π be a finitely generated subgroup of $\mathrm{GL}_n(\mathbb{Z})$, let H be the Zariski closure of π, and for p prime, let $\pi(p)$ be the image of π in $\mathrm{GL}_n(\mathbb{F}_p)$. Then, for almost all p, $\pi(p)$ contains the subgroup of $H(\mathbb{F}_p)$ that is generated by the elements of order p.*

6 Galois action.

The aim of this section is to show that the Galois orbits of special points in $S'(\overline{\mathbb{Q}})$ are big, in a suitable sense. For A and B abelian surfaces (over some field) with O_K-action, we let $\mathrm{Hom}_{O_K}(A, B)$ be the O_K-module of morphisms from A to B that are compatible with the O_K-actions.

6.1 Lemma. *Let x in $S'(\overline{\mathbb{Q}})$ be a special point, corresponding to a triplet (A, α, λ) with A an abelian surface over $\overline{\mathbb{Q}}$, $\alpha\colon O_K \to \mathrm{End}(A)$ and λ a principal O_K-polarization. Then $\mathrm{End}_{O_K}(A)$ is an order, containing O_K, of a totally imaginary quadratic extension of K.*

Proof. Let R be the endomorphism algebra $\mathbb{Q} \otimes \mathrm{End}(A)$ of A. Then R is a semi-simple $\mathbb{Q}$-algebra containing a commutative semi-simple subalgebra of dimension 4. Suppose that A is simple. Then R is a division algebra. Since R acts faithfully on $\mathrm{H}_1(A(\mathbb{C}), \mathbb{Q})$, it has dimension dividing 4, hence R is a quadratic extension of K. Since $\mathbb{R} \otimes R$ has a complex structure commuting with the R-action, R is a totally imaginary. Suppose now that A is not simple. Then A is isogeneous to the product of two elliptic curves, B_1 and B_2, say. These elliptic curves are in fact isogeneous to each other, because otherwise K does not admit a morphism to the endomorphism algebra of $B_1 \times B_2$. So A is isogeneous to B^2, with B some elliptic curve. Since A is of CM-type, $\mathbb{Q} \otimes \mathrm{End}(B)$ is an imaginary quadratic field E, and $R = \mathrm{M}_2(E)$. In this case $\mathrm{End}_{O_K}(A)$ is an order in the totally imaginary extension $K \otimes E$ of K. □

6.2 Theorem. *There exist real numbers $\varepsilon > 0$ and $c > 0$ such that for (A, α, λ) corresponding to a special point x in $S'(\overline{\mathbb{Q}})$ one has:*

$$|\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}){\cdot}x| > c\,|\mathrm{discr}(R_x)|^{\varepsilon},$$

where $R_x = \mathrm{End}_{O_K}(A)$.

6.3 Remark. The proof will show that one can take ε to be any number less than $1/4$. (To get this, one also has to optimize Theorem 6.4, noting that we only apply Stark's result to fields L of degree at least 4.) Assuming the generalized Riemann hypothesis at this point does not improve this exponent (this is caused by the case where $\mathbb{Q} \otimes R_x$ is Galois over $\mathbb{Q}$ with group $(\mathbb{Z}/2\mathbb{Z})^2$).

Proof. Let $f\colon S'_{\mathbb{Q}} \to S_{\mathbb{Q}}$ be the morphism induced by the closed immersion of the Shimura data $(G'_{\mathbb{Q}}, X') \to (G_{\mathbb{Q}}, X)$. Since f is finite, and since the Hecke correspondences on $S_{\mathbb{Q}}$ permute the irreducible components transitively, the statement we want to prove is equivalent to its analog for $S_{\mathbb{Q}}$. So we will show in fact that there are positive ε and c such that for x special in $S(\overline{\mathbb{Q}})$ corresponding to (A, α), we have:

$$|\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}){\cdot}x| > c\,|\mathrm{discr}(R_x)|^{\varepsilon}.$$

For x special in $S(\overline{\mathbb{Q}})$, let L_x be $\mathbb{Q} \otimes R_x$, and let M_x be the Galois closure in $\overline{\mathbb{Q}}$ of L_x. Since M_x is of degree at most 8 over $\mathbb{Q}$, the statement we want to prove is equivalent to the existence of positive ε and c such that for all special x in $S(\overline{\mathbb{Q}})$:

$$|\mathrm{Gal}(\overline{\mathbb{Q}}/M_x){\cdot}x| > c\,|\mathrm{discr}(R_x)|^{\varepsilon}.$$

So let now x be special in $S(\overline{\mathbb{Q}})$, corresponding to some (A_x, α_x). To study the $\mathrm{Gal}(\overline{\mathbb{Q}}/M_x)$-orbit of x, we construct a zero-dimensional subvariety of Hodge type over M_x, containing x, and we use the theory of Shimura-Taniyama on complex multiplication, rephrased in the language of Shimura varieties (see [19, Section 2.2]). Let H_x be $\mathrm{H}_1(A(\mathbb{C}), \mathbb{Z})$; it is an R_x-module that is locally free of rank two as O_K-module. Let $f\colon K^2 \to \mathbb{Q} \otimes H_x$ be an isomorphism of K-vector spaces. The Hodge structure on H_x given by A_x gives an element h_x of X. The lattice $f^{-1}H_x$ in K^2 corresponds to an element $\overline{g_x}$ of $G(\mathbb{A}_{\mathrm{f}})/G(\hat{\mathbb{Z}})$. By construction, x is the image of (h_x, g_x). Let $T_x := \mathrm{Res}_{L_x/\mathbb{Q}}\mathbb{G}_{\mathrm{m},L_x}$. Then f gives a closed immersion $T_x \to G_{\mathbb{Q}}$. Since $\mathbb{Q} \otimes H_x$ is a one-dimensional L_x-vector space, T_x is its own centralizer in $G_{\mathbb{Q}}$. It follows that h_x factors through $T_{x,\mathbb{R}}$. Hence we have a closed immersion of Shimura data: $(T_x, \{h_x\}) \to (G_{\mathbb{Q}}, X)$. The reflex field of $(T_x, \{h_x\})$ is contained in M_x, hence we have a canonical model $\mathrm{Sh}(T_x, \{h_x\})_{M_x}$ over M_x. We put $U_x := T_x(\mathbb{A}_{\mathrm{f}}) \cap g_x G(\hat{\mathbb{Z}}) g_x^{-1}$. Then one easily verifies that we have an injective morphism of Shimura varieties $\mathrm{Sh}_{U_x}(T_x, \{h_x\})_{M_x} \to S_{M_x}$, which, on $\mathbb{C}$-valued points, is given by $\overline{t} \mapsto \overline{(h_x, tg_x)}$. By construction, U_x is the stabilizer in $T_x(\mathbb{A}_\mathrm{f})$ of the lattice $f^{-1}H_x$; it follows that $U_x = R_x^{\wedge,*}$, hence:

$$\mathrm{Sh}_{U_x}(T_x, \{h_x\})_{M_x}(\overline{\mathbb{Q}}) = L_x^* \backslash (\mathbb{A}_\mathrm{f} \otimes L_x)^* / R_x^{\wedge,*} = \mathrm{Pic}(R_x).$$

Our next objective is to describe in sufficient detail the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/M_x)$ on $\mathrm{Pic}(R_x)$ induced by the above bijections. Class field theory gives a continuous surjection from $M_x^* \backslash \mathbb{A}_{M_x,\mathrm{f}}^*$ to $\mathrm{Gal}(\overline{\mathbb{Q}}/M_x)^{\mathrm{ab}}$, characterized by the following property. In a representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/M_x)^{\mathrm{ab}}$ that is unramified at a finite place v of M_x, the arithmetic Frobenius element is the image of the class of an idèle that is trivial at all places other than v, and the inverse of a uniformizer at v. Let $\mu\colon \mathbb{G}_{\mathrm{m},\mathbb{C}} \to \mathbb{S}_\mathbb{C}$ be the cocharacter obtained by composing $\mathbb{C}^* \to \mathbb{C}^* \times \mathbb{C}^*$, $z \mapsto (z, 1)$ with the inverse of the isomorphism $\mathbb{S}(\mathbb{C}) = (\mathbb{C} \otimes_\mathbb{R} \mathbb{C})^* \to \mathbb{C}^* \times \mathbb{C}^*$, $x \otimes y \mapsto (xy, x\overline{y})$. Then $h_x \circ \mu$ is defined over M_x, and one defines:

$$r_x\colon T_x' := \mathrm{Res}_{M_x/\mathbb{Q}} \mathbb{G}_{\mathrm{m},M_x} \to T_x$$

to be the morphism $\mathrm{Res}_{M_x/\mathbb{Q}}(h_x \circ \mu)$ composed with the norm map from $\mathrm{Res}_{M_x/\mathbb{Q}} T_{x,M_x}$ to T_x. With these definitions, the quotient $\mathrm{Gal}(\overline{\mathbb{Q}}/M_x)^{\mathrm{ab}}$ of $T_x'(\mathbb{A}_\mathrm{f})$ acts on $\mathrm{Pic}(R_x)$ via the morphism r_x, where we view $\mathrm{Pic}(R_x)$ as $T_x(\mathbb{Q}) \backslash T_x(\mathbb{A}_\mathrm{f}) / R_x^{\wedge,*}$. It follows that:

$$|\mathrm{Gal}(\overline{\mathbb{Q}}/M_x) \cdot x| = |\text{image of } r_x(T_x'(\mathbb{A}_\mathrm{f})) \text{ in } \mathrm{Pic}(R_x)|.$$

We will need a more explicit description of r_x, in terms of the CM type associated to h_x. The morphism $h_x\colon \mathbb{C}^* \to (\mathbb{R} \otimes L_x)^*$ extends to a morphism of $\mathbb{R}$-algebras $h\colon \mathbb{C} \to \mathbb{R} \otimes L_x$. Extending scalars from $\mathbb{R}$ to $\mathbb{C}$ gives a morphism of $\mathbb{C}$-algebras $\mathrm{id} \otimes h\colon \mathbb{C} \otimes_\mathbb{R} \mathbb{C} \to \mathbb{C} \otimes L_x$. Via the isomorphisms:

$$\mathbb{C} \otimes_\mathbb{R} \mathbb{C} \to \mathbb{C} \times \mathbb{C}, \quad x \otimes y \mapsto (xy, x\overline{y}),$$

and

$$\mathbb{C} \otimes L_x \to \mathbb{C}^{\mathrm{Hom}(L_x, \mathbb{C})}, \quad x \otimes y \mapsto (\phi \mapsto x\phi(y)),$$

the idempotent $(1, 0)$ of $\mathbb{C} \times \mathbb{C}$ gives an idempotent in $\mathbb{C}^{\mathrm{Hom}(L_x, \mathbb{C})}$, i.e., a partition of $\mathrm{Hom}(L_x, \mathbb{C})$ into two sets Φ_x and $\iota\Phi_x$, where ι is the complex conjugation on $\mathbb{C}$. The set Φ_x is the CM type corresponding to h_x. Since M_x is the Galois closure of L_x in $\mathbb{C}$, $\mathrm{Hom}(L_x, M_x) = \mathrm{Hom}(L_x, \mathbb{C})$. With these notations, we have, for any $\mathbb{Q}$-algebra R:

$$r_x\colon (R \otimes M_x)^* \longrightarrow \prod_{\phi \in \Phi_x} (R \otimes L_x)^*, \quad u \longmapsto \prod_{\phi \in \Phi_x} \mathrm{Norm}_\phi(u),$$

where Norm_ϕ is the norm map of the extension $\phi\colon R \otimes L_x \to R \otimes M_x$. Finally, let ϕ_0 be in $\mathrm{Hom}(L_x, M_x)$, and define $\Sigma_{x,\phi_0} := \{g \in \mathrm{Gal}(M_x/\mathbb{Q}) \mid g\phi_0 \in \Phi_x\}$. Then we have:

$$\phi_0 \circ r_x\colon T_x' \longrightarrow T_x \hookrightarrow T_x', \quad u \mapsto \prod_{g \in \Sigma_{x,\phi_0}} g^{-1} u,$$

for all $\mathbb{Q}$-algebras R and all u in $(R \otimes M_x)^*$. This is the description of r_x that we work with.

Since M_x is generated over K by the extension L_x and its conjugate, M_x has degree 4 or 8 over $\mathbb{Q}$, and its Galois group $\mathrm{Gal}(M_x/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or D_4, the dihedral group of order 8. We define T to be $\mathrm{Res}_{K/\mathbb{Q}}\mathbb{G}_{\mathrm{m},K}$; note that T is a subtorus of T_x, equal to the center of $G_{\mathbb{Q}}$. We will see below that $r_x \circ \phi_0 \colon T_x \to T_x$ induces an endomorphism of T_x/T whose image, after passing to $\mathbb{A}_{\mathrm{f}}$-valued points, in $\mathrm{Pic}(R_x)/\mathrm{Pic}(O_K)$ is big enough for our purposes.

Suppose first that $\mathrm{Gal}(M_x/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$, say with generator σ. Then $M_x = L_x$, σ^2 is the complex conjugation and $K = L_x^{\langle\sigma^2\rangle}$. After changing ϕ_0, if necessary, one has that $\Sigma_{x,\phi} = \{1, \sigma\}$. The formula above for $\phi_0 \circ r_x$ shows that r_x is simply given by the element $1 + \sigma^{-1}$ of $\mathbb{Z}[\mathrm{Gal}(M_x/\mathbb{Q})]$. Since σ^2 acts as -1 on T_x/T, we have $r_x \circ (1 - \sigma^{-1}) = 2$ on T_x/T. It follows that:

$$|\mathrm{Gal}(\overline{\mathbb{Q}}/M_x)\cdot x| \geq |\text{image of } \cdot 2 \colon \mathrm{Pic}(R_x)/\mathrm{Pic}(O_K) \to \mathrm{Pic}(R_x)/\mathrm{Pic}(O_K)|.$$

Theorem 6.4 below finishes the proof in this case.

Suppose now that $\mathrm{Gal}(M_x/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. After changing ϕ_0, if necessary, one has $\Sigma_{x,\phi_0} = \{1, \sigma\}$, with σ of order two and $K_x := L_x^{\langle\sigma\rangle} \neq K$. Let R_x' be the order $O_{K_x} \cap R_x$ of K_x. Since r_x is given by $1 + \sigma$, the induced map $T_x'(\mathbb{A}_{\mathrm{f}}) \to \mathrm{Pic}(R_x)$ factors through $\mathrm{Pic}(R_x') \to \mathrm{Pic}(R_x)$ induced by the inclusion $R_x' \to R_x$. The fact that σ acts as 1 on $T_x'' := \mathrm{Res}_{K_x/\mathbb{Q}}\mathbb{G}_{\mathrm{m},K_x}$ and as -1 on T_x/T_x'' implies that the kernel of the map $\mathrm{Pic}(R_x') \to \mathrm{Pic}(R_x)$ is killed by multiplication by 2. Since $1 + \sigma$ acts as multiplication by 2 on T_x'', we get:

$$|\mathrm{Gal}(\overline{\mathbb{Q}}/M_x)\cdot x| \geq |\text{image of } \cdot 4 \colon \mathrm{Pic}(R_x') \to \mathrm{Pic}(R_x')|.$$

Since the order $O_K \otimes R_x'$ of L_x is contained in R_x, and has discriminant $\mathrm{discr}(R_x')^2\mathrm{discr}(O_K)^2$, we have:

$$|\mathrm{discr}(R_x')| \geq |\mathrm{discr}(O_K)|^{-1}|\mathrm{discr}(R_x)|^{1/2}.$$

The proof in this case is finished by Theorem 6.4.

Suppose that $\mathrm{Gal}(M_x/\mathbb{Q})$ is isomorphic to D_4. Let τ and σ be generators of $\mathrm{Gal}(M_x/\mathbb{Q})$, with $M_x^{\langle\tau\rangle} = L_x$, and with σ of order 4. Then σ^2 is the complex conjugation, and $\tau\sigma^{-1} = \sigma\tau$. After changing ϕ_0, if necessary, we have $\Sigma_{x,\phi_0} = \{1, \tau, \sigma, \sigma\tau\}$. It follows that $\phi_0 \circ r_x$ is given by the element $t := 1 + \tau + \sigma^3 + \sigma\tau$ of $\mathbb{Z}[\mathrm{Gal}(M_x/\mathbb{Q})]$. Using that $\mathrm{Norm}_{\phi_0} = 1 + \tau$, a simple computation gives:

$$\phi_0 \circ r_x \circ \phi_0 \circ \mathrm{Norm}_{\phi_0} = 2(1 + \tau) + \sigma\mathrm{Norm}_{M_x/K}.$$

It follows that $r_x \circ \phi_0$ acts as 2 on T_x/T. We conclude that:

$$|\mathrm{Gal}(\overline{\mathbb{Q}}/M_x)\cdot x| \geq |\text{image of } \cdot 2\colon \mathrm{Pic}(R_x)/\mathrm{Pic}(O_K) \to \mathrm{Pic}(R_x)/\mathrm{Pic}(O_K)|.$$

Theorem 6.4 finishes the proof in this last case. $\square$

6.4 Theorem. *Let K be a totally real number field. There exists $c > 0$ such that for all orders R, containing O_K, in totally complex quadratic extensions L of K, one has:*

$$|\textit{image of} \cdot 4 \textit{ on } \mathrm{Pic}(R)/\mathrm{Pic}(O_K)| \geq c\,|\mathrm{discr}(R)|^{1/8}.$$

If one assumes the generalized Riemann hypothesis, then one can replace the exponent $1/8$ by any number less than $1/2$.

Proof. We will use the following lower bound for class numbers:

> *let K be a totally real number field; there exists $c > 0$ such that for all totally complex quadratic extensions L of K, one has:*
>
> $$|\mathrm{Pic}(O_L)| \geq c\,|\mathrm{discr}(O_L)|^{1/6}.$$

In order to prove this, one distinguishes two cases: $K = \mathbb{Q}$ and $K \neq \mathbb{Q}$, and one notes that the regulator $\mathrm{Reg}(O_L)$ is at most $\mathrm{Reg}(O_K)$. In the case $K \neq \mathbb{Q}$ one uses the following consequence of Stark's Theorem 2 in [29]:

> *for K a totally real number field, there exists $c > 0$ such that for all totally complex quadratic extensions L of K, one has:*
>
> $$|\mathrm{Pic}(O_L)| \geq c\,|\mathrm{discr}(O_L)|^{1/2-1/[L:\mathbb{Q}]}.$$

In the case $K = \mathbb{Q}$ one applies the Brauer-Siegel theorem (see for example [17, Ch. XVI]):

> *for $N > 0$ and $\varepsilon > 0$, there exists $c > 0$ such that for all Galois extensions L of $\mathbb{Q}$ of degree at most N one has:*
>
> $$|\mathrm{Pic}(O_L)|\cdot\mathrm{Reg}(O_L) \geq c\,|\mathrm{discr}(O_L)|^{1/2-\varepsilon}.$$

Combining these two results, and using that $[L:\mathbb{Q}] \geq 3$ if $K \neq \mathbb{Q}$ gives the inequality we want. We could replace the exponent $1/6$ by $1/4$ if we would just use that $[L:\mathbb{Q}] \geq 4$ if $K \neq \mathbb{Q}$.

Let now K, R and L be as in the theorem. Then R is the inverse image of a subring $\overline{R}$ of some finite quotient $\overline{O_L}$ of O_L. We have an exact sequence:

$$0 \longrightarrow R^* \longrightarrow O_L^* \longrightarrow \overline{O_L}^*/\overline{R}^* \longrightarrow \mathrm{Pic}(R) \longrightarrow \mathrm{Pic}(O_L) \longrightarrow 0.$$

The torsion of O_L^* is bounded in terms of the degree of K, and by Dirichlet's theorem on units the quotient O_L^*/O_K^* is finite. The long exact cohomology sequence obtained by taking $\mathrm{Gal}(L/K)$-invariants of the short exact sequence:

$$0 \longrightarrow \mathrm{tors}(O_L^*) \longrightarrow O_L^* \longrightarrow O_L^*/\mathrm{tors}(O_L^*) \longrightarrow 0$$

gives an injection from $(O_L^*/\mathrm{tors}(O_L^*))/(O_K^*/\mathrm{tors}(O_K^*))$ into $\mathrm{H}^1(\mathrm{Gal}(L/K), \mathrm{tors}(O_L^*))$, showing that $(O_L^*/\mathrm{tors}(O_L^*))/(O_K^*/\mathrm{tors}(O_K^*))$ is of order at most two. We conclude that there exists $c > 0$, depending only on the degree of K, such that:

$$|\mathrm{Pic}(R)| \geq c \, \frac{|\overline{O_L}^*|}{|\overline{R}^*|} \, |\mathrm{Pic}(O_L)|.$$

On the other hand, we have:

$$\mathrm{discr}(R) = \left(\frac{|\overline{O_L}|}{|\overline{R}|}\right)^2 \mathrm{discr}(O_L).$$

We claim that for every $\varepsilon > 0$ there exists $c > 0$, depending only on the degree of K, such that:

$$\frac{|\overline{O_L}^*|}{|\overline{R}^*|} \geq c \left(\frac{|\overline{O_L}|}{|\overline{R}|}\right)^{1-\varepsilon}.$$

To prove this claim, one notes that:

$$\frac{|\overline{R}|}{|\overline{R}^*|} = \prod_{k \text{ res field of } \overline{R}} \frac{|k|}{|k^*|}, \quad \text{and} \quad \frac{|\overline{O_L}|}{|\overline{O_L}^*|} = \prod_{k \text{ res field of } \overline{O_L}} \frac{|k|}{|k^*|}.$$

A simple computation then shows:

$$\frac{|\overline{O_L}^*|}{|\overline{R}^*|} \geq n \prod_{p|n} \left(1 - \frac{1}{p}\right)^{[L:\mathbb{Q}]} \geq n \left(\frac{1}{5\log(n)}\right)^{[L:\mathbb{Q}]},$$

where $n = |\overline{O_L}|/|\overline{R}|$ is assumed to be at least 2. We conclude that there exists $c > 0$, depending only on K, such that:

$$|\mathrm{Pic}(R)| \geq c \, |\mathrm{discr}(R)|^{1/7}.$$

In order to finish the proof of the theorem, it suffices to prove that for every $\varepsilon > 0$ there exists $c > 0$, depending only on K, such that $|\mathrm{Pic}(R)[2]| \leq c\,|\mathrm{discr}(R)|^\varepsilon$. To do this, we proceed in the same way as we did in [14, Lemma 3.4]. As $\mathrm{Pic}(R)$ is a finite commutative group, the two $\mathbb{F}_2$-vector spaces $\mathrm{Pic}(R)[2]$ and $\mathbb{F}_2 \otimes \mathrm{Pic}(R)$ have the same dimension. The cover of $\mathrm{Spec}(R)$ by the disjoint union of $\mathrm{Spec}(\mathbb{Z}_2 \otimes R)$ and $\mathrm{Spec}(R[1/2])$ gives an exact sequence:

$$(\mathbb{Q}_2 \otimes L)^* \longrightarrow \mathrm{Pic}(R) \longrightarrow \mathrm{Pic}(R[1/2]) \longrightarrow 0.$$

It follows that $\dim_{\mathbb{F}_2} \mathbb{F}_2 \otimes \mathrm{Pic}(R)$ is bounded by $\dim_{\mathbb{F}_2} \mathbb{F}_2 \otimes \mathrm{Pic}(R[1/2])$ plus a number depending only on the degree of K. We put $S := \mathrm{Spec}(R[1/2])$ and $T := \mathrm{Spec}(O_K[1/2])$. The long exact sequence associated to the multiplication by two on the sheaf $\mathbb{G}_{\mathrm{m}}$ on the etale site S_{et} of S shows that $\dim_{\mathbb{F}_2} \mathbb{F}_2 \otimes \mathrm{Pic}(S)$ is at most $\dim_{\mathbb{F}_2} \mathrm{H}^1(S_{\mathrm{et}}, \mathbb{F}_2)$. Let $\pi\colon S \to T$ be the morphism induced by the inclusion of O_K in R. Then $\mathrm{H}^1(S_{\mathrm{et}}, \mathbb{F}_2)$ is the same as $\mathrm{H}^1(T_{\mathrm{et}}, \pi_*\mathbb{F}_2)$, and we have a short exact sequence:

$$0 \longrightarrow \mathbb{F}_{2,S_{\mathrm{et}}} \longrightarrow \pi_*\pi^*\mathbb{F}_{2,T} \longrightarrow j_!\mathbb{F}_{2,U} \longrightarrow 0,$$

where $j\colon U \to T$ is the maximal open immersion over which π is etale. Let $i\colon Z \to T$ be closed immersion giving the complement of U, with Z reduced. Then the long exact sequences of cohomology groups associated to the exact sequence above and to the exact sequence:

$$0 \longrightarrow j_!\mathbb{F}_{2,U_{\mathrm{et}}} \longrightarrow \mathbb{F}_{2,S_{\mathrm{et}}} \longrightarrow i_*\mathbb{F}_{2,Z_{\mathrm{et}}} \longrightarrow 0$$

show that there exists an integer c, depending only on K, such that:

$$\dim_{\mathbb{F}_2} \mathbb{F}_2 \otimes \mathrm{Pic}(R) \leq c + [K:\mathbb{Q}]\ \left|\{p \text{ prime dividing } \mathrm{discr}(R)\}\right|.$$

As $2^{|\{p|n\}|} = n^{o(1)}$, for $n \to \infty$, we have proved the first statement of the theorem. If one assumes GRH, then the Brauer-Siegel theorem as stated above is true without the condition that the extension $\mathbb{Q} \to L$ be Galois, see [17, XIII, §4]. $\square$

7 Intersection numbers.

The aim of this section is to give a bound on intersections of subvarieties of Shimura varieties, provided that they are finite. In particular, we need to study the intersection of a subvariety with its images under Hecke correspondences. As our arguments work for general Shimura varieties, we give such a result in the general case. The main tool used in proving the result is the Baily-Borel compactification, together with its given ample line bundles. We start by recalling some properties of these line bundles, that follow immediately from the results in [7] (see also [6]).

7.1 Theorem. *Let (G,X) be a Shimura datum. For $K \subset G(\mathbb{A}_{\mathrm{f}})$ a compact open subgroup, let $S_K := \mathrm{Sh}_K(G,X)_{\mathbb{C}}$ the corresponding complex Shimura variety, and $\overline{S}_K$ its Baily-Borel compactification. For every such K, and for every sufficiently divisible positive integer n, the nth power of the line bundle of holomorphic forms of maximal degree of X descends to S_K, and extends uniquely to a very ample line bundle $\mathcal{L}_{K,n}$ on $\overline{S}_K$, such that, at the generic points of the boundary components of codimension one, it is given by nth powers of forms with logarithmic poles. Let K_1 and K_2 be compact open subgroups of $G(\mathbb{A}_{\mathrm{f}})$, and g in $G(\mathbb{A}_{\mathrm{f}})$ such that $K_2 \subset gK_1g^{-1}$. Then the morphism from S_{K_2} to S_{K_1} induced by g extends to a morphism $f\colon \overline{S}_{K_2} \to \overline{S}_{K_1}$. If n is positive and sufficiently divisible so that $\mathcal{L}_{K_1,n}$ exists, then $\mathcal{L}_{K_2,n}$ exists, and is canonically isomorphic to $f^*\mathcal{L}_{K_1,n}$.*

Proof. Let us briefly recall how the compactification $\overline{S}_K$ is defined. Let X^+ be a connected component of X. Then each connected component of $S_K(\mathbb{C})$ is of the form $\Gamma_i\backslash X^+$, with Γ_i an arithmetic subgroup of $G^{\mathrm{ad}}(\mathbb{Q})$ (G^{ad} being the quotient of G by its center). The compactification $\overline{S}_K(\mathbb{C})$ is then defined as the disjoint union of the $\Gamma_i\backslash\overline{X^+}$, where $\overline{X^+}$ is the union of X^+ with its so-called rational boundary components, endowed with the Satake topology. It follows that we can write $\overline{S}_K(\mathbb{C})$ as $G(\mathbb{Q})\backslash(\overline{X} \times G(\mathbb{A}_{\mathrm{f}})/K)$, with $\overline{X}$ the disjoint union of the $\overline{X^+}$.

Let X^{ad} be the $G^{\mathrm{ad}}(\mathbb{R})$-conjugacy class of morphisms from $\mathbb{S}$ to $G^{\mathrm{ad}}_{\mathbb{R}}$ containing the image of X. Each connected component of X maps isomorphically to one of X^{ad} (see [19, 1.6.7]). We first prove the Theorem above for the Shimura datum $(G^{\mathrm{ad}}, X^{\mathrm{ad}})$. The group G^{ad} is a product of simple algebraic groups G_j over $\mathbb{Q}$, and X^{ad} decomposes as a product of X_j's. For compact open subgroups K, K_1 and K_2 that are products of compact open subgroups of the $G_j(\mathbb{A}_{\mathrm{f}})$, the corresponding Shimura varieties decompose as a product, so that it suffices to treat the G_j separately. If (G_j, X_j) gives compact Shimura varieties, Kodaira's theorem ([15, Section 1.4]) implies what we want, for compact open subgroups K_j that are sufficiently small; for arbitrary K_j one takes quotients by finite groups. Suppose now that (G_j, X_j) does give Shimura varieties that are not compact. If G_j is of dimension 3, then it is isomorphic to $\mathrm{PGL}_{2,\mathbb{Q}}$, and we are in the case of modular curves, where the Theorem we are proving is well known (the canonical line bundle with log poles at the cusps on the modular curve $X(n)$, $n \geq 3$, has degree > 0). Suppose now that G_j has dimension > 3. Then the boundary components are of codimension > 1, and the results we want are given in [7, Thm. 10.11].

The case of arbitrary open compact subgroups of $G^{\mathrm{ad}}(\mathbb{A}_{\mathrm{f}})$ follows by considering quotients by finite groups. The theorem for (G,X) itself follows from the fact that the connected components of the $S_K(\mathbb{C})$ are of the $\Gamma\backslash X^+$, with Γ an arithmetic subgroup of $G^{\mathrm{ad}}(\mathbb{Q})$. $\square$

7.2 Theorem. *Let (G,X) be a Shimura datum, let K_1 and K_2 be compact open subgroups of $G(\mathbb{A}_{\mathrm{f}})$, and let Z_1 and Z_2 be closed subvarieties of the Shimura varieties $S_1 := \mathrm{Sh}_{K_1}(G,X)_{\mathbb{C}}$*

and $S_2 := \mathrm{Sh}_{K_2}(G,X)_{\mathbb{C}}$, respectively. Suppose that Z_1 or Z_2 is of dimension at most one. Then there exists an integer c such that for all g in $G(\mathbb{A}_{\mathrm{f}})$ for which $T_gZ_1 \cap Z_2$ is finite, one has:

$$|T_gZ_1 \cap Z_2| \leq c \deg(\overline{\pi_1} \colon S_g \to S_1),$$

where $S_g = \mathrm{Sh}_{K_g}(G,X)_{\mathbb{C}}$ with $K_g = K_1 \cap gK_2g^{-1}$, and with T_g and $\overline{\pi_1}$ as in the beginning of Section 5.

Proof. We start with two reductions. First of all, writing Z_1 and Z_2 as the unions of their irreducible components, one sees that we may suppose that Z_1 and Z_2 are irreducible. Secondly, for g in $G(\mathbb{A}_{\mathrm{f}})$, let $p_{1,g}$ and $p_{2,g}$ be the morphisms from S_g to S_1 and S_2, respectively. Then one has:

$$T_gZ_1 \cap Z_2 = p_{2,g}\left(p_{1,g}^{-1}Z_1 \cap p_{2,g}^{-1}Z_2\right),$$

which shows that $T_gZ_1 \cap Z_2$ is finite if and only if $p_{1,g}^{-1}Z_1 \cap p_{2,g}^{-1}Z_2$ is, and that $|T_gZ_1 \cap Z_2|$ is at most $|p_{1,g}^{-1}Z_1 \cap p_{2,g}^{-1}Z_2|$. This also shows that we may replace K_1 and K_2 by smaller compact open subgroups. Hence we may suppose, by the previous theorem, that we have very ample line bundles $\mathcal{L}_1$ and $\mathcal{L}_2$ on the Baily-Borel compactifications $\overline{S_1}$ and $\overline{S_2}$ such that, for each g, $\overline{p_{1,g}}^*\mathcal{L}_1$ and $\overline{p_{2,g}}^*\mathcal{L}_2$ are isomorphic to the same line bundle $\mathcal{L}_g$ on $\overline{S_g}$.

We let $\overline{Z_1}$ and $\overline{Z_2}$ be the closures of Z_1 and Z_2 in $\overline{S_1}$ and $\overline{S_2}$, respectively. Let m denote the degree of $\overline{Z_2}$ with respect to $\mathcal{L}_2$. Let g be in $G(\mathbb{A}_{\mathrm{f}})$, such that $T_gZ_1 \cap Z_2$ is finite. If the intersection is empty, there is nothing to prove, so we suppose that the intersection is not empty. Then the codimension of Z_2 is at least the dimension d of Z_1, and we can choose $f_1, \ldots, f_d$ in $\mathrm{H}^0(\overline{S_2}, \mathcal{L}_2^{\otimes m})$ such that $\overline{Z_2}$ is contained in $V_{S_2}(f_1, \ldots, f_d)$, and $\overline{T_gZ_1} \cap V_{S_2}(f_1, \ldots, f_d)$ is finite (because of our assumption on the dimensions of Z_1 and Z_2, $\overline{Z_1} \cap \overline{Z_2}$ is finite). It then follows that $|\overline{p_{1,g}^{-1}Z_1} \cap \overline{p_{2,g}^{-1}Z_2}|$ is at most m^d times the degree of $\overline{p_{1,g}^{-1}Z_1}$ with respect to $\mathcal{L}_g$. But this degree is $\deg(p_{1,g})$ times the degree of $\overline{Z_1}$ with respect to $\mathcal{L}_1$, hence we have:

$$|T_gZ_1 \cap Z_2| \leq \deg(p_{1,g}) m^d \deg_{\mathcal{L}_1}(\overline{Z_1}).$$

$\square$

8 Proof of the main results.

We will now prove Theorems 2.1 and 2.2. We first deal with Thm. 2.1. As we have already noticed, we may as well replace $S_{\mathbb{C}}$ by $S'_{\mathbb{C}}$, so let C be an irreducible closed curve in $S'_{\mathbb{C}}$ that contains infinitely many CM points. We have to show that C is of Hodge type.

Since C has infinitely many points in $S'(\overline{\mathbb{Q}})$, it is, as a reduced closed subscheme of $S'_{\mathbb{C}}$, defined over $\overline{\mathbb{Q}}$. To be precise, there is a unique closed subscheme $C_{\overline{\mathbb{Q}}}$ of $S'_{\overline{\mathbb{Q}}}$ that gives C after base change from $\overline{\mathbb{Q}}$ to $\mathbb{C}$. But then $C_{\overline{\mathbb{Q}}}$ has only finitely many conjugates under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$; we let $C_{\mathbb{Q}}$ be the reduced closed subscheme of $S'_{\mathbb{Q}}$ that, after base change to $\overline{\mathbb{Q}}$, gives the union of these conjugates. In other words, we simply let $C_{\mathbb{Q}}$ be the image of C under the morphism of schemes $S'_{\mathbb{C}} \to S'_{\mathbb{Q}}$.

Let x in $C(\overline{\mathbb{Q}})$ be a CM point, corresponding to a pair (A, λ) with A an abelian variety over $\overline{\mathbb{Q}}$ with multiplications by O_K and with λ a principal O_K-polarization. As before, we let R_x denote $\mathrm{End}_{O_K}(A)$, $L_x := \mathbb{Q}\otimes R_x$ and M_x the Galois closure of L_x in $\mathbb{C}$. Let $\overline{x}$ be the image of x in $S(\overline{\mathbb{Q}})$. In the proof of Theorem 6.2 we have seen that the quotient $\mathrm{Gal}(\overline{\mathbb{Q}}/M_x)^{\mathrm{ab}}$ of $(\mathbb{A}_{\mathrm{f}} \otimes M_x)^*$ acts on the subset $\mathrm{Gal}(\overline{\mathbb{Q}}/M_x)\cdot\overline{x}$ of $L_x^*\backslash(\mathbb{A}_{\mathrm{f}} \otimes L_x)^*/R_x^{\wedge,*}$ via the morphism

$$r_x\colon (\mathbb{A}_{\mathrm{f}} \otimes M_x)^* \longrightarrow (\mathbb{A}_{\mathrm{f}} \otimes L_x)^*, \quad u \mapsto \prod_{\phi\in\Phi_x} \mathrm{Norm}_\phi(u),$$

where the subset Φ_x of $\mathrm{Hom}(L_x, M_x)$ is the CM type of x. Since Φ_x is a set of representatives for the action of $\mathrm{Gal}(L_x/K)$ on $\mathrm{Hom}(L_x, M_x)$, it follows that this map r_x factors through the subgroup of elements of $(\mathbb{A}_{\mathrm{f}} \otimes L_x)^*$ whose norm to $(\mathbb{A}_{\mathrm{f}} \otimes K)^*$ is in $\mathbb{A}_{\mathrm{f}}^*$. Hence, in the notation of the proof of Theorem 6.2, the morphism r_x factors through the intersection of the subtorus T_x of $G_{\mathbb{Q}}$ and $G'_{\mathbb{Q}}$. It follows that the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/M_x)$ on $\mathrm{Gal}(\overline{\mathbb{Q}}/M_x)\cdot x$ is given by the same morphism r_x, taking values in $G'(\mathbb{A}_{\mathrm{f}})$.

8.1 Lemma. *Suppose that p is a prime that is split in R_x, i.e., such that $\mathbb{F}_p \otimes R_x$ is isomorphic to a product of copies of $\mathbb{F}_p$. Then $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})x$ is contained in $C_{\mathbb{Q}}(\overline{\mathbb{Q}}) \cap (T_pC_{\mathbb{Q}})(\overline{\mathbb{Q}})$.*

Proof. The localization $\mathbb{Z}_{(p)} \otimes R_x$ of R_x is the same as that of O_K. Hence, if we let H_x denote $\mathrm{H}_1(A(\mathbb{C}), \mathbb{Z})$, then $\mathbb{Z}_{(p)} \otimes H_x$ is free of rank one over $\mathbb{Z}_{(p)} \otimes R_x$. It follows that we can choose the isomorphism $f\colon K^2 \to \mathbb{Q} \otimes H_x$ to preserve the integral structures on both sides at p, i.e., such that it induces an isomorphism from $(\mathbb{Z}_{(p)}\otimes R_x)^2$ to $\mathbb{Z}_{(p)}\otimes H_x$. We note that p is split in M_x (i.e., $\mathbb{F}_p \otimes O_{M_x}$ is a product of copies of $\mathbb{F}_p$), because M_x is the Galois closure of L_x. Consider now an element u of $(\mathbb{A}_{\mathrm{f}}\otimes M_x)^*$ that is equal to p at one place above p and equal to 1 at all other finite places of M_x. Then $r_x(u)$, viewed as an element of $(\mathbb{A}_{\mathrm{f}} \otimes L_x)^*$, is equal to p at exactly two places of L_x above p that are not in the same $\mathrm{Gal}(L_x/K)$-orbit, and equal to 1 at all other finite places of L_x. It follows that $r_x(u)$ is conjugated in $G'(\mathbb{A}_{\mathrm{f}})$, by some element in $G'(\hat{\mathbb{Z}})$, to the element $g(p)$ that induces T_p (use that $G'(\mathbb{Z}_p)$ acts transitively on the set of free rank one $\mathbb{Z}_p\otimes O_K$-submodules of $\mathbb{Z}_p\otimes O_K^2$). We conclude that $r_x(u)x$ is in T_px. But since x is in $C_{\mathbb{Q}}(\overline{\mathbb{Q}})$, $r_x(u)x$ is also in $C_{\mathbb{Q}}(\overline{\mathbb{Q}})$. It follows that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})x$ is contained in $C_{\mathbb{Q}}(\overline{\mathbb{Q}}) \cap (T_pC_{\mathbb{Q}})(\overline{\mathbb{Q}})$. $\square$

Theorem 6.2 gives a lower bound for $|\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})x|$, whereas Theorem 7.2 gives an upper bound for $|C_{\mathbb{Q}}(\overline{\mathbb{Q}}) \cap (T_pC_{\mathbb{Q}})(\overline{\mathbb{Q}})|$, assuming that the intersection is finite. What we want, of course, is to show that we can choose x and then p such that the lower bound exceeds the upper bound, and conclude that $C_{\mathbb{Q}}$ and $T_pC_{\mathbb{Q}}$ do not intersect properly. We note that if x varies over the infinite set of CM points of $C(\overline{\mathbb{Q}})$, then $|\mathrm{discr}(R_x)|$ tends to infinity because there are only finitely many orders of degree 2 over O_K with a given discriminant, and for each such order there are only finitely many x in $S(\overline{\mathbb{Q}})$ with R_x isomorphic to that order. Since our lower bound for $|\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})x|$ is a positive constant times a positive power of $|\mathrm{discr}(R_x)|$, and our upper bound for $|C_{\mathbb{Q}}(\overline{\mathbb{Q}}) \cap (T_pC_{\mathbb{Q}})(\overline{\mathbb{Q}})|$ is some fixed power of p, we get what we want if we can take, for $|\mathrm{discr}(R_x)|$ big, p of size something polynomial in $\log|\mathrm{discr}(R_x)|$. We note that $|\mathrm{discr}(O_{M_x})| \leq |\mathrm{discr}(R_x)|^4$ because M_x is the composite of the extension L_x of K and its conjugate. We also note that the number of primes dividing $\mathrm{discr}(R_x)$ is at most $\log_2(|\mathrm{discr}(R_x)|)$.

At this point we invoke the effective Chebotarev theorem of Lagarias, Montgomery and Odlyzko, assuming GRH, as stated in [28, Thm. 4] and the second remark following that theorem. A simple computation shows that this theorem implies the following result.

8.2 Proposition. *For M a finite Galois extension of $\mathbb{Q}$, let n_M denote its degree, d_M its absolute discriminant $|\mathrm{discr}(O_M)|$, and for x in $\mathbb{R}$, let $\pi_{M,1}(x)$ be the number of primes $p \leq x$ that are unramified in M and such that the Frobenius conjugacy class Frob_p contains just the identity element of $\mathrm{Gal}(M/\mathbb{Q})$. Then for M a finite Galois extension of $\mathbb{Q}$ and x sufficiently big (i.e., bigger than some absolute constant), and bigger than $2(\log(d_M)^2(\log(\log(d_M)))^2$, one has:*

$$\pi_{M,1}(x) \geq \frac{x}{3n_M\log(x)}.$$

This result shows that there exist infinitely many primes p such that $C_{\mathbb{Q}}$ and $T_pC_{\mathbb{Q}}$ do not intersect properly. Since $C_{\mathbb{Q}}$ is irreducible, it follows that, for such primes p, $C_{\mathbb{Q}}$ is contained in $T_pC_{\mathbb{Q}}$.

Assume now that C is not of Hodge type. Then Proposition 5.1 tells us that for all primes p large enough, T_pC is irreducible. Since the correspondence T_p is defined over $\mathbb{Q}$, i.e., is given by a correspondence on $S'_{\mathbb{Q}}$, it follows that $T_pC_{\mathbb{Q}}$ is irreducible for p large enough. But then we see that there exist infinitely many prime numbers p such that $C_{\mathbb{Q}}$ is equal to $T_pC_{\mathbb{Q}}$. But this is absurd, since by Lemma 8.3 below, for each x in $S'(\mathbb{C})$, the Hecke orbit $\cup_{n\geq 0}T_p^n x$ is dense in $S'(\mathbb{C})$ if p is unramified in K. This finishes the proof of Theorem 2.1.

8.3 Lemma. *Let x be in $S'(\mathbb{C})$ and let p be a prime number that is not ramified in K. Then the Hecke orbit $\cup_{n\geq 0}T_p^n x$ is dense in $S'(\mathbb{C})$ for the archimedean topology.*

Proof. By Lemma 8.4 below, $g_0 := \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $G'(\mathbb{Z}_p)$ generate $G'(\mathbb{Q}_p)$ (here we use that p is not ramified in K). Let now x be in $S'(\mathbb{C})$, and let (y, g) be a preimage of it in $X \times G'(\mathbb{A}_{\mathrm{f}})$

under the quotient map for the action by $G(\mathbb{Q}) \times G(\hat{\mathbb{Z}})$. The fact that T_p is then given by right multiplication on $G'(\mathbb{A}_{\mathrm{f}})$ by the element g_0 at the place p shows that the T_p-orbit of x is the image in $S'(\mathbb{C})$ of the $G'(\mathbb{Q}_p)$-orbit of (y, g). Let now Γ be the subgroup of $G'(\mathbb{Q})$ consisting of γ such that γg is in $gG'(\hat{\mathbb{Z}})G'(\mathbb{Q}_p)$. Then the T_p-orbit of x is the image in $S'(\mathbb{C})$ of the subset Γy of $X \times \{g\}$. Now one notes that Γ contains a congruence subgroup of $G'(\mathbb{Z}[1/p])$. It follows that the intersection of Γ with $\mathrm{SL}_2(O_K[1/p]) = G^{\mathrm{der}}(\mathbb{Z}[1/p])$ is dense in $G^{\mathrm{der}}(\mathbb{R})$ (for the archimedean topology) because G^{der} is generated by additive subgroups. Since $G^{\mathrm{der}}(\mathbb{R})$ acts transitively on $X^+ = (\mathbb{H}^+)^2$, the lemma is proved. □

8.4 Lemma. *Let p be a prime that is not ramified in K. Then $g_0 := \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $G'(\mathbb{Z}_p)$ generate $G'(\mathbb{Q}_p)$.*

Proof. In order to minimize notation, let $O_{K,p}$ denote $\mathbb{Z}_p \otimes O_K$, let K_p denote $\mathbb{Q}_p \otimes O_K$, and let H denote the subgroup of $G'(\mathbb{Q}_p)$ generated by $g_0 := \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $G'(\mathbb{Z}_p)$. Let Y be the set of $O_{K,p}$-lattices in K_p^2 on which the K_p-bilinear form ψ given by $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ is a perfect pairing of $O_{K,p}$-modules, up to a factor in $\mathbb{Q}_p^*$. The map $G'(\mathbb{Q}_p) \to Y$, $g \mapsto gO_{K,p}^2$ induces a bijection from $G'(\mathbb{Q}_p)/G'(\mathbb{Z}_p)$ to Y. Hence, in order to prove our claim, it suffices to show that H acts transitively on Y. So let L be in Y. We note that $O_{K,p}$ is either a product of two copies of $\mathbb{Z}_p$, or the ring of integers $\mathbb{Z}_{p^2}$ in the unramified quadratic extension $\mathbb{Q}_{p^2}$ of $\mathbb{Q}_p$; in both cases, $O_{K,p}$ is a product of discrete valuation rings with uniformizer p. The theory of finitely generated modules over a discrete valuation ring says that there exists r in $\mathbb{Z}$ and d_1 and d_2 in $O_{K,p}$ such that $p^r L$ is contained in $O_{K,p}^2$ and has an $O_{K,p}$-basis of the form $(d_1 e_1, d_2 e_2)$, with (e_1, e_2) the standard basis of $O_{K,p}^2$. We note that conjugating g_0 by suitable elements of $G'(\mathbb{Z}_p)$ shows that $\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right)$ are in H, and that, in the split case, $(\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right), \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right))$ is in H. Since the element $d_1 d_2$ of $O_{K,p}$ is the factor by which ψ differs from a perfect pairing on $p^r L$, it is actually in $\mathbb{Z}_p$. It follows that $\left(\begin{smallmatrix} d_1 & 0 \\ 0 & d_2 \end{smallmatrix}\right)$ is in H. This finishes the proof that H is $G'(\mathbb{Q}_p)$. □

Let us now prove Theorem 2.2. We keep the notations of the proof Theorem 2.1, and we assume again that C is not of Hodge type. So now we may suppose moreover that C contains infinitely many CM points that have the same CM type. In particular, we have infinitely many CM points x such that L_x and Φ_x are constant, say L and Φ. Of course, the orders R_x are such that $|\mathrm{discr}(R_x)|$ tends to infinity. The classical Chebotarev theorem (see for example [17, Ch. VIII, §4]) asserts that the set of primes p that are split in M has natural density $1/[M : \mathbb{Q}]$ (actually, Dirichlet density is good enough here). Also, recall that the number of primes dividing some $\mathrm{discr}(R_x)$ is at most $\log_2(|\mathrm{discr}(R_x)|)$. Hence there do exist x and p such that p is split in M, split in R_x, sufficiently large so that $T_p C_{\mathbb{Q}}$ is irreducible, and such that the lower bound for $|\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})x|$ of Theorem 6.2 exceeds the upper bound for the intersection $C_{\mathbb{Q}}(\overline{\mathbb{Q}}) \cap (T_p C_{\mathbb{Q}})(\overline{\mathbb{Q}})$, if it is finite. Then we have $C_{\mathbb{Q}} = T_p C_{\mathbb{Q}}$, hence a contradiction because of Lemma 8.3.

Acknowledgements.

It is a pleasure to thank Rutger Noot, for teaching a very useful course on Shimura varieties, for answering my questions concerning them, and for his useful comments on this manuscript. Without the influence of Johan de Jong, Ben Moonen and Frans Oort I would not even have started working on this subject. I thank Paula Cohen for sending me a preliminary version of [11], and for pointing out to me which version of the André-Oort conjecture was exactly needed in it. Peter Stevenhagen gave me the reference to Stark's results in [29]. I thank Andrei Yafaev for useful remarks on this manuscript; his numerous questions on the subject have caused me to learn a good deal about Shimura varieties. I thank the organizers of the Texel conference for their excellent work. The referee deserves much credit for pointing out a serious mistake in Section 7 of the preprint version, and for a long list of detailed comments. Last but not least I thank my wife Reinie Erné for her influence on this article via conversations both at work and at home, and for letting me sleep when I am too tired to fetch a bottle for Tom at five o'clock in the morning.

References

[1] A. Abbes. *Hauteurs et discrétude (d'après L. Szpiro, E. Ullmo et S. Zhang).* Séminaire Bourbaki, Vol. 1996/97. Astérisque No. **245**, (1997), Exp. No. 825, 4, 141–166.

[2] Y. André. *G-functions and geometry.* Aspects of mathematics, Vol. **E13**, Vieweg, Braunschweig, 1989.

[3] Y. André. *Mumford-Tate groups of mixed Hodge structures and the theorem of the fixed part.* Compositio Mathematica **82** (1992), pp. 1–24.

[4] Y. André. *Distribution des points CM sur les sous-variétés des variétés de modules de variétés abéliennes.* Manuscript, April 1997.

[5] Y. André. *Finitude de couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire.* J. Reine Angew. Math. **505** (1998), pp. 203–208.

[6] W.L. Baily and A. Borel. *On the compactification of arithmetically defined quotients of bounded symmetric domains.* Bull. Amer. Soc. **70** (1964), 588–593.

[7] W.L. Baily and A. Borel. *Compactification of arithmetic quotients of bounded symmetric domains.* Ann. Math. (2) **84** (1966), 442–528.

[8] J-L. Brylisnki and J-P. Labesse. *Cohomologie d'intersection et fonctions L de certaines variétés de Shimura.* Ann. Sci. E.N.S. 4ème série, **17** (1984), 361–412.

[9] E. Cattani, P. Deligne and A. Kaplan. *On the locus of Hodge classes.* J. Amer. Math. Soc. **8** (1995), pp. 483–506.

[10] L. Clozel and E. Ullmo. Talk at the Journées Arithmétiques, July 1999, Roma.

[11] P.B. Cohen and G. Wüstholz. *Application of the André-Oort conjecture to some questions in transcendence.* Preprint.

[12] P. Deligne. *Travaux de Shimura.* Séminaire Bourbaki, 23ème année (1970/71), Exp. No. **389**, pp. 123–165. Lecture Notes in Math., Vol. 244, Springer, Berlin, 1971.

[13] P. Deligne. *Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques*, in Automorphic forms, representations, and L-functions, Part 2, A. Borel and W. Casselman, eds., Proc. of Symp. in Pure Math., Vol. 33, American Mathematical Society, 1979, pp. 247–290.

[14] S.J. Edixhoven. *Special points on the product of two modular curves.* Compositio Mathematica **114**, 315–328, 1998.

[15] P. Griffiths and J. Harris. *Principles of algebraic geometry.* Pure and applied mathematics. A Wiley-Interscience publication, John Wiley and sons, New York, Chichester, Brisbane, Toronto, 1978.

[16] A. Grothendieck et. al. *Cohomologie locale des faisceaux cohérents et théorèmes de Lefschetz locaux et globaux*. North-Holland, Amsterdam (1968).

[17] S. Lang. *Algebraic number theory.* GTM 110, Springer-Verlag, second edition, 1994.

[18] B.J.J. Moonen. *Special points and linearity properties of Shimura varieties.* Thesis, Utrecht, September 1995.

[19] B.J.J. Moonen. *Models of Shimura varieties in mixed characteristic.* Pages 267–350 in "Galois representations in arithmetic algebraic geometry", edited by A.J. Scholl and R.L. Taylor. Cambridge University Press 1998.

[20] B.J.J. Moonen. *Linearity properties of Shimura varieties, I.* Journal of Algebraic Geometry **7** (1998), 539–567.

[21] B.J.J. Moonen. *Linearity properties of Shimura varieties, II.* Compositio Math. **114** (1998), no. 1, 3–35.

[22] D. Mumford. *Abelian varieties.* Oxford University Press, 1970.

[23] D. Mumford. *The topology of normal singularieties of an algebraic surface and a criterion for simplicity.* Publications Mathématiques de l'IHES **9** (1961), 5–22.

[24] M.V. Nori. *On subgroups of* $\mathrm{GL}_n(\mathbb{F}_p)$. Invent. math. **88** (1987), pp. 257–275.

[25] F. Oort. *Canonical lifts and dense sets of CM-points.* Arithmetic Geometry, Proc. Cortona symposium 1994, F. Catanese, ed., Symposia Math., Vol. XXXVII, Cambridge University Press, 1997, pp. 228–234.

[26] V.P. Platonov and S. Rapinchuk. *Algebraic groups and number theory.* Moscow, 1991 (in Russian). English translation: Academic Press, 1993.

[27] M. Rapoport. *Compactifications de l'espace de modules de Hilbert-Blumenthal.* Compositio Mathematica **36** (1978), 255–335.

[28] J-P. Serre. *Quelques applications du théorème de densité de Chebotarev.* Publications Mathématiques de l'IHES **54** (1981), 123–202.

[29] H.M. Stark. *Some effective cases of the Brauer-Siegel theorem.* Inventiones math. **23**, 135–152 (1974).

[30] G. van der Geer. *Hilbert modular surfaces.* Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band 16. Springer-Verlag, 1988.

[31] A. Yafaev. *Special points on products of two Shimura curves.* To appear in Manuscripta Mathematica.

Bas Edixhoven
IRMAR
Campus de Beaulieu
35042 Rennes cedex
France

A Abelian surfaces with real multiplication.

As above, K is a real quadratic field, and O_K is its ring of integers. Let us describe a bijection

$$S(\mathbb{C}) = G(\mathbb{Q})\backslash((\mathbb{H}^{\pm})^2 \times G(\mathbb{A}_{\mathrm{f}})/G(\hat{\mathbb{Z}})) \xrightarrow{\sim} \{(A, \alpha)\}/\cong,$$

where A is an abelian surface and $\alpha\colon O_K \to \mathrm{End}(A)$ a morphism of rings. By the way things have been set up, $(\mathbb{H}^{\pm})^2$ is the set of Hodge structures of type $\{(-1,0),(0,-1)\}$ on the K-vector space K^2, i.e., Hodge structures for which K acts by endomorphisms.

The set $G(\mathbb{A}_{\mathrm{f}})/G(\hat{\mathbb{Z}})$ is the set of O_K-lattices in K^2. (By an O_K-lattice in K^2 we mean a sub-O_K-module M of finite type that generates K^2 as a K-vector space). To see why the two sets are equal, we need an adelic description of the lattices. By an $O_K^\wedge$-lattices in $\mathbb{A}_{K,\mathrm{f}}^2$ we mean a sub-$O_K^\wedge$-module of $\mathbb{A}_{K,\mathrm{f}}^2$ that is free of rank two (and hence give the full $\mathbb{A}_{K,\mathrm{f}}^2$ after tensoring with $\mathbb{Q}$). (It is equivalent to consider sub-$O_K^\wedge$-modules of $\mathbb{A}_{K,\mathrm{f}}^2$ that are of finite type and that generate $\mathbb{A}_{K,\mathrm{f}}^2$ as K-vector space (or, equivalently, as $\mathbb{A}_{K,\mathrm{f}}$-module).) Now let $G(\mathbb{A}_{\mathrm{f}})$ act on the set of $O_K^\wedge$-lattices in $\mathbb{A}_{K,\mathrm{f}}^2$. This action is transitive (use that each such a lattice is free of rank two), and the stabilizer of the standard lattice $(O_K^\wedge)^2$ is precisely $G(\hat{\mathbb{Z}})$. This means that $G(\mathbb{A}_{\mathrm{f}})/G(\hat{\mathbb{Z}})$ is the set of $O_K^\wedge$-lattices in $\mathbb{A}_{K,\mathrm{f}}^2$.

Let us now see why the set of O_K-lattices in K^2 is the set of $O_K^\wedge$-lattices in $\mathbb{A}_{K,\mathrm{f}}^2$. This is always the same story, but let me just write it down in this case (the "classical case" as far as I'm concerned is for $\mathbb{Z}$). Let M be an O_K-lattice in K^2. To it, we associate the $O_K^\wedge$-lattice $\hat{\mathbb{Z}} \otimes M$ in $\mathbb{A}_{\mathrm{f}} \otimes M = \mathbb{A}_{K,\mathrm{f}}^2$. In the other direction, let N be a $O_K^\wedge$-lattice in $\mathbb{A}_{K,\mathrm{f}}^2$. To N, we simply associate $N \cap K^2$. These two maps are inverses of each other.

We can now show that $S(\mathbb{C})$ is the set of (A, α) up to isomorphism. Let (A, α) be given. Choose an isomorphism of K-vector spaces between K^2 and $\mathrm{H}_1(A, \mathbb{Q})$. Then we get a Hodge structure on K^2 and an O_K-lattice in K^2, hence an element of $(\mathbb{H}^{\pm})^2 \times G(\mathbb{A}_{\mathrm{f}})/G(\hat{\mathbb{Z}})$, defined up to the choice of isomorphism, i.e., up to $G(\mathbb{Q})$. Conversely, an element of $(\mathbb{H}^{\pm})^2 \times G(\mathbb{A}_{\mathrm{f}})/G(\hat{\mathbb{Z}})$ gives a pair (A, α), of which the isomorphism class depends only on the $G(\mathbb{Q})$-orbit. So, after all, one just has to view complex abelian varieties as given by a $\mathbb{Q}$-Hodge structure and a lattice, and use the usual stuff regarding lattices.

One can of course do something fancy now with the category of abelian varieties up to isogeny, and interpret $(\mathbb{H}^{\pm})^2 \times G(\mathbb{A}_{\mathrm{f}})$ as the set of isomorphism classes of $(A, \alpha, \beta, \gamma)$, with A an abelian surface up to isogeny, α an K-action on it, β an isomorphism of $\mathbb{A}_{K,\mathrm{f}}$-modules from $\mathbb{A}_{K,\mathrm{f}}^2$ to $\mathrm{H}_1(A, \mathbb{A}_{\mathrm{f}})$, and γ an isomorphism of K-vector spaces from K^2 to $\mathrm{H}_1(A, \mathbb{Q})$.

B Polarizations.

Why do we never have to discuss polarizability of our Hodge structures? Well, that's because they are in a sense only of dimension two, just as in the case of elliptic curves. So what is in fact true is that every complex torus of dimension two, with an action by O_K, is automatically an abelian variety. Of course, this is very standard, but I just write it down for myself, so that I understand it, and so that I have the argument available electronically.

Consider the standard symplectic form on the K-vector space K^2:

$$\psi_0 \colon K^2 \times K^2 \longrightarrow K, \quad (x,y) \mapsto x^t J y, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Then we compose this ψ_0 with an arbitrary non-zero $\mathbb{Q}$-linear map l from K to $\mathbb{Q}$ in order to get a $\mathbb{Q}$-bilinear anti-symmetric form:

$$\psi_l \colon K^2 \times K^2 \xrightarrow{\psi_0} K \xrightarrow{l} \mathbb{Q}.$$

In particular, one can take for l the trace map; in that case, we will denote ψ_l simply by ψ.

For all g in $\mathrm{GL}_2(K)$ and all x and y in K^2, one has $\psi_0(gx, gy) = \det(g)\psi_0(x,y)$. Hence if moreover $\det(g)$ is in $\mathbb{Q}$, one has: $\psi_l(gx, gy) = \det(g)\psi_l(x,y)$. This means that such a ψ_l is a Hodge class of weight two (or is it -2?) for all $h\colon \mathbb{S}_{\mathbb{R}} \to G_{\mathbb{R}}$ that are in $(\mathbb{H}^{\pm})^2$, since they factor through the subgroup of G of elements that have determinant in $\mathbb{G}_{\mathrm{m},\mathbb{Q}}$.

Let us now check that ψ is a polarization on $(\mathbb{H}^+)^2$. So the only condition left to check is that $x \mapsto \psi(x, h(i)x)$ should be positive definite on $\mathbb{R} \otimes K^2$. (One checks indeed that this makes sense, in the sense that $(x,y) \mapsto \psi(x, h(i)y)$ is symmetric.) The fact that $\mathbb{R} \otimes K = \mathbb{R}^2$ means that it suffices to check that $x \mapsto x^t h(i) x$ is positive definite on $\mathbb{R}^2$ for every h in $\mathbb{H}^+$. But now note that for all h in $\mathbb{H}^+$ and all non-zero x in $\mathbb{R}^2$, x and $h(i)x$ are $\mathbb{R}$-linearly independent (interpret h as giving a structure of complex vector space on $\mathbb{R}^2$). Hence either $x \mapsto x^t h(i) x$ is positive definite, or negative definite, for all h in $\mathbb{H}^+$ simultaneously. So let us check just what it is for the standard h, the one that sends $a+bi$ to $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$. In that case, one has $h(i) = -J$, hence $x^t J h(i) x = x^t x$, which is the standard inner product.

On $\mathbb{H}^-$, $x^t J h(i) x$ is negative definite, since the standard h there has $h(i) = J$. So we have seen that ψ is a polarization on $(\mathbb{H}^+)^2$, and $-\psi$ one on $(\mathbb{H}^-)^2$. On the other two components of $(\mathbb{H}^{\pm})^2$ one gets polarizations by varying the map l, for example by taking the composition of l with multiplication by a suitable element of K, i.e., an element with the right signs at the two infinite places.

C Some stuff on group (schemes).

Let G denote the group scheme GL_2 (over $\mathbb{Z}$, that is). Let V denote its standard representation. I use in the text that the kernel of G acting on $\mathrm{Sym}^2(V)\otimes\det^{-1}$ is precisely the scalar subgroup $\mathbb{G}_{\mathrm{m}}$ of G. This can be checked as follows. First of all, the pairing $V\times V\to\det(V)$, $(x,y)\to xy$, is perfect. Hence it gives us an isomorphism between $V\otimes\det^{-1}$ and V^*, the dual of V. Hence we may as well consider $\mathrm{End}(V)=V^*\otimes V$ as $V\otimes V\otimes\det^{-1}$. Under this isomorphism, the quotient $\mathrm{Sym}_2(V)\otimes\det^{-1}$ of $V\otimes V\otimes\det^{-1}$ corresponds to the quotient of $\mathrm{End}(V)$ by the submodule of scalar matrices. So we test the question there. One computes:

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} 1 & 0\\ 0 & 0\end{pmatrix}-\begin{pmatrix} 1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix} a & b\\ c & d\end{pmatrix}=\begin{pmatrix} 0 & -b\\ c & 0\end{pmatrix},$$
$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}\begin{pmatrix} 0 & 0\\ 1 & 0\end{pmatrix}-\begin{pmatrix} 0 & 0\\ 1 & 0\end{pmatrix}\begin{pmatrix} a & b\\ c & d\end{pmatrix}=\begin{pmatrix} b & 0\\ d-a & b\end{pmatrix}.$$

The condition that these two matrices are scalar give that $a=d$ and $b=c=0$.

D The Shimura datum for G^{ad}.

For $\pi\colon G\to G^{\mathrm{ad}}$ as above, we claim that π induces an isomorphism (of real algebraic varieties) from $(\mathbb{H}^{\pm})^2$ in $\mathrm{Hom}_{\mathbb{R}}(\mathbb{S},G_{\mathbb{R}})$ to a conjugacy class (that we will also denote by $(\mathbb{H}^{\pm})^2$) in $\mathrm{Hom}_{\mathbb{R}}(\mathbb{S},G^{\mathrm{ad}}_{\mathbb{R}})$. Let us denote the kernel of π by Z (it is the center of G). Let h_0 be our standard element in $(\mathbb{H}^{\pm})^2$. Let g be in $G(\mathbb{R})$, and suppose that $\pi\circ\mathrm{int}_g\circ h_0=\pi\circ h_0$. We have to show that $\mathrm{int}_g\circ h_0=h_0$. Here is how that goes. Define a map (i.e., morphism of real algebraic varieties) $z\colon\mathbb{S}\to Z_{\mathbb{R}}$ by: $z(s)=gh_0(s)g^{-1}{\cdot}h_0(s)^{-1}$. Then, because it goes to the center, z is actually a morphism of groups. All we have to show is that it is trivial. Well, it is trivial on the $\mathbb{G}_{\mathrm{m},\mathbb{R}}$ in $\mathbb{S}$, since that one is mapped centrally in $G_{\mathbb{R}}$. Now the argument is finished by noting that $Z_{\mathbb{R}}$ is a split torus, and $\mathbb{S}/\mathbb{G}_{\mathrm{m},\mathbb{R}}$ is not split.

E Comparing various groups.

It is not yet clear to me with which group I actually want to work. The possibilities are: $\mathrm{GL}_2(K)$, $\mathrm{PGL}_2(K)$ and $G'=\{g\in\mathrm{GL}_2(K)\mid\det(g)\in\mathbb{Q}\}$. Just to get some idea of what actually happens with these groups, and with the morphisms of Shimura data between them, I think it is a good idea to make some things explicit, such as the sets of connected components, and the finite maps between the various Shimura varieties.

So let us first think a bit about the π_0's. Let's first consider G as above. Then clearly we have:

$$\pi_0(S(\mathbb{C})) = \mathrm{GL}_2(K)^+\backslash \mathrm{GL}_2(\mathbb{A}_{K,\mathrm{f}})/\mathrm{GL}_2(O_K^\wedge).$$

But this set is the set of isomorphism classes of locally free rank 2 O_K-modules M with an orientation on $\det(M) = \Lambda^2_{O_K} M$ at the two infinite places. Now each locally free rank two module over O_K is isomorphic to one of the form $O_K \oplus L$ (show first that it is decomposable by choosing a one dimensional K-sub-vector space in $\mathbb{Q}\otimes M$; then show that M has a nowhere vanishing element). Of course, L is determined by M since one has $\det(M) = L$. It follows that:

$$\pi_0(S(\mathbb{C})) = \mathrm{Pic}(O_K)^+, \text{ the strict class group of } K.$$

Let us now consider $\pi_0(S^{\mathrm{ad}}(\mathbb{C}))$. We have:

$$\pi_0(S^{\mathrm{ad}}(\mathbb{C})) = \mathrm{PGL}_2(K)^+\backslash \mathrm{PGL}_2(\mathbb{A}_{K,\mathrm{f}})/\mathrm{PGL}_2(O_K^\wedge).$$

This we recognize as the set of isomorphism classes of $\mathbb{P}^1$-bundles on $S := \mathrm{Spec}(O_K)$, locally trivial in the Zariski topology, with an orientation at the two infinite places (it does not seem a complete tautology, the correspondence with the Zariski $\mathbb{P}^1$-bundles, namely, it says more directly something as: trivial over K, and over every completion). Anyway, let us show that each $\mathbb{P}^1$-bundle X on S comes from a locally free rank two bundle on S. Just note that each element of $X(K)$ extends to one in $X(S)$. An element in $X(S)$ gives an invertible $\mathcal{O}_X$-module $\mathcal{L}$ that has degree one on each fibre, hence with $p_*\mathcal{L}$ a rank two bundle on S. Then one checks that X is isomorphic, over S, to $\mathbb{P}(p_*\mathcal{L})$ (it is easy to see that X is the Grassmannian of locally free rank one quotients of $p_*\mathcal{L}$). This has an interpretation in the long exact sequence coming from the short exact sequence of Zariski sheaves on S:

$$1 \longrightarrow \mathbb{G}_{\mathrm{m},S} \longrightarrow \mathrm{GL}_{2,S} \longrightarrow \mathrm{PGL}_{2,S} \longrightarrow 1.$$

What is quite nice in this situation is that S is of dimension one, hence that $\mathrm{H}^2(S, \mathbb{G}_{\mathrm{m}}) = 0$, which explains the observation above. Now that we know that each element of $\pi_0(S^{\mathrm{ad}}(\mathbb{C}))$ comes from a locally free rank two O_K-module, we want to know when two such modules give isomorphic $\mathbb{P}^1$-bundles. Well, the Grassmannian interpretation says that that happens if and only if the two modules are isomorphic up to twist by an invertible O_K-module. Hence:

$$\mathbb{F}_2 \otimes \mathrm{Pic}(O_K) = \{\mathbb{P}^1\text{-bundles on } \mathrm{Spec}(O_K)\}_{/\cong}.$$

Let us now consider orientations. Note that $\mathrm{Aut}_{O_K}(O_K \oplus L)$ maps surjectively, under $\det$, to $\mathrm{Aut}_{O_K}(L) = O_K^*$, and that doubles in $\mathrm{Pic}(O_K)$ have a canonical orientation. It follows that:

$$\pi_0(S^{\mathrm{ad}}(\mathbb{C})) = \mathrm{Pic}(O_K)^+/2\mathrm{Pic}(O_K),$$

and that:

$$\#\pi_0(S^{\mathrm{ad}}(\mathbb{C})) = \begin{cases} \#\mathbb{F}_2 \otimes \mathrm{Pic}(O_K) & \text{if } N(O_K^*) = \{1, -1\}, \\ 2\#\mathbb{F}_2 \otimes \mathrm{Pic}(O_K) & \text{if } N(O_K^*) = \{1\}. \end{cases}$$

Let us now say something about the map $S(\mathbb{C}) \to S^{\mathrm{ad}}(\mathbb{C})$. This makes it necessary to know things about the morphism of group schemes $\mathrm{GL}_{2,O_K} \to \mathrm{PGL}_{2,O_K}$. We would like to know that this morphism is surjective for the Zariski topology. For this, it suffices to show that on a scheme S, an S-automorphism of $\mathbb{P}^1_S$ is induced, locally on S, by an element of $\mathrm{GL}_2(S)$. Now use that for any scheme T, to give an element of $\mathbb{P}^1(T)$ is to give an invertible O_T-module with two sections that generate it. Let g be an S-automorphism of $\mathbb{P}^1_S$. Then $g^*\mathcal{O}(1)$ is of the form $p^*\mathcal{L} \otimes \mathcal{O}(1)$ for some invertible $\mathcal{O}_S$-module $\mathcal{L}$. Since $\mathcal{L}$ is locally trivial, we get what we want.

Hence: the morphism $\mathrm{GL}_2(O_K^\wedge) \to \mathrm{PGL}_2(O_K^\wedge)$ is surjective (use that $O_K^\wedge$ is the product of the completions at all finite places and that one has the surjectivity for each such completion). And: $\mathrm{GL}_2(\mathbb{A}_{K,\mathrm{f}}) \to \mathrm{PGL}_2(\mathbb{A}_{K,\mathrm{f}})$ is surjective (just use what elements of $\mathbb{A}_{K,\mathrm{f}}$ look like, or use that to give a point of a scheme with values in $\mathbb{A}_\mathrm{f}$ is to give, for each p, a point with values in $\mathbb{Q}_p$, such that for almost all p the point comes from a point with values in $\mathbb{Z}_p$). The more difficult thing that remains now is the question of surjectivity of the morphism $\mathrm{GL}_2(O_K) \to \mathrm{PGL}_2(O_K)$.

It follows that $S(\mathbb{C}) \to S^{\mathrm{ad}}(\mathbb{C})$ is surjective. The stabilizer of $(\mathbb{H}^+)^2 \times \{1\}$ in $\mathrm{GL}_2(K)$ and $\mathrm{PGL}_2(K)$ are $\mathrm{GL}_2(O_K)^+$ and $\mathrm{PGL}_2(O_K)^+$, respectively. So let us find out what the cokernel of $\mathrm{GL}_2(O_K)^+ \to \mathrm{PGL}_2(O_K)^+$ is.

An automorphism of $\mathbb{P} := \mathbb{P}^1_S$ is given by an invertible $\mathcal{O}_\mathbb{P}$-module of degree one together with two generating sections. Such a module is of the form $p^*\mathcal{L} \otimes \mathcal{O}(1)$. But then we have the condition that $p_*p^*\mathcal{L} \otimes \mathcal{O}(1) = \mathcal{L} \oplus \mathcal{L}$ is generated by two global sections. This can be done if and only if $\mathcal{L} \oplus \mathcal{L} \cong \mathcal{O} \oplus \mathcal{O}$, i.e., if and only if $\mathcal{L}^{\otimes 2} \cong \mathcal{O}$. This explains that we have an exact sequence:

$$1 \longrightarrow O_K^* \longrightarrow \mathrm{GL}_2(O_K) \longrightarrow \mathrm{PGL}_2(O_K) \longrightarrow \mathrm{Pic}(O_K)[2] \longrightarrow 0$$

Likewise, one gets:

$$1 \longrightarrow O_K^* \longrightarrow \mathrm{GL}_2(O_K)^+ \longrightarrow \mathrm{PGL}_2(O_K)^+ \longrightarrow \mathrm{Pic}(O_K)[2] \longrightarrow 0.$$

We conclude that $S(\mathbb{C})^0 \to S^{\mathrm{ad}}(\mathbb{C})^0$ is the quotient for a faithful action by the group $\mathrm{Pic}(O_K)[2]$, where $S(\mathbb{C})^0$ and $S^{\mathrm{ad}}(\mathbb{C})^0$ are the standard irreducible components of $S(\mathbb{C})$ and $S^{\mathrm{ad}}(\mathbb{C})$. One computes directly that the map $S(\mathbb{C}) \to S^{\mathrm{ad}}(\mathbb{C})$ is the quotient for a faithful action by the group $K^*\backslash\mathbb{A}_K^*/O_K^{\wedge,*}$, i.e., by $\mathrm{Pic}(O_K)$.

Let us now do some comparing between S and S', with S' coming from the Shimura datum with the group G'. We first remark that $G'(\mathbb{R})$ is the set of (g_1, g_2) in $\mathrm{GL}_2(\mathbb{R})^2$ such that

$\det(g_1) = \det(g_2)$. This means that the $G'(\mathbb{R})$ conjugacy class of morphisms from $\mathbb{S}$ to $G'_{\mathbb{R}}$ that we deal with is:

$$X' := (\mathbb{H}^+)^2 \coprod (\mathbb{H}^-)^2 = (\mathbb{H}^2)^{\pm}.$$

Hence we have:

$$S'(\mathbb{C}) = G'(\mathbb{Q})\backslash(X' \times G'(\mathbb{A}_{\mathrm{f}})/G'(\hat{\mathbb{Z}})), \quad \pi_0(S'(\mathbb{C})) = G'(\mathbb{Q})^+\backslash G'(\mathbb{A}_{\mathrm{f}})/G'(\hat{\mathbb{Z}}).$$

This last set is the set of isomorphism classes of triplets (M, ϕ, α) with M a locally free O_K-module of rank two, $\phi\colon O_K \to \det(M)$ an isomorphism, and α an orientation on $\mathbb{R} \otimes_{\mathbb{Z}} \det(M)$ that induces plus or minus the standard orientation on $\mathbb{R} \otimes O_K = \mathbb{R} \times \mathbb{R}$ via ϕ. Since every such triplet is isomorphic to $(O_K^2, \mathrm{id}, (+,+))$, we see:

$$S'(\mathbb{C}) \text{ is connected.}$$

What about the map $S'(\mathbb{C}) \to S(\mathbb{C})$? It suffices to look at what happens on $(\mathbb{H}^2)^+ \times \{1\}$. The stabilizer of this in $G'(\mathbb{Q})$ is simply $\mathrm{SL}_2(O_K)$, and the stabilizer in $G(\mathbb{Q})$ is $\mathrm{GL}_2(O_K)^+$. Hence the map $S'(\mathbb{C}) \to S(\mathbb{C})^+$ is the quotient for the faithful action by the group $O_K^{*,+}/O_K^{*,2}$, i.e., totally positive global units modulo squares of global units.

F Some stuff on bilinear forms and field extensions.

Let $k \to K$ be a finite field extension, say of degree d. Let V be a finite dimensional K-vector space, say of dimension n. Let X denote the k-vector space of k-bilinear forms $b\colon V \times V \to k$ such that $b(ax, y) = b(x, ay)$ for all x and y in V and all a in K. (I.e., the maps $x \mapsto ax$ are required to be self-adjoint.) We want to relate X to the set Y of K-bilinear forms on V.

Let $l\colon K \to k$ be a surjective k-linear map (for example, one can take the trace map if $k \to K$ is separable). Then we have a map:

$$L\colon Y \longrightarrow X, \quad b \mapsto l \circ b.$$

Indeed, for b in Y we have: $(l \circ b)(ax, y) = l(b(x, ay)) = (l \circ b)(x, ay)$. The map L is injective, since, for b a K-bilinear form, the image of b is either 0 or K.

Let us now assume that $k \to K$ is separable. Then one computes that both X and Y are of dimension n^2d over k (of course, for Y this is clearly true without the separability assumption; for X, one uses this assumption in order to reduce to the case $K = k^d$ via base change from k to some algebraic closure for example). Hence we conclude that the map L above is bijective. (I did not bother to check if this is still true without the separability.) So we have the following result.

F.1 Proposition. *Let k be a field, and K a finite separable k-algebra. Let $l\colon K \to k$ be a surjective k-linear map (for example the trace map). Let V be a finitely generated projective K-module. Then for every k-bilinear form $b\colon V \times V \to k$ such that $b(ax, y) = b(x, ay)$ for all x and y in V and all a in K there exists a unique K-bilinear $b'\colon V \times V \to K$ such that $b = l \circ b'$. With this notation, b is symmetric (antisymmetric) if and only if b' is so.*

Proof. It only remains to prove that b is symmetric (antisymmetric) if and only if b' is so. For b as above, let b^t denote its adjoint, i.e., $b^t(x, y) = b(y, x)$; we will use the same notation for elements of Y. Then one has $(b^t)' = (b')^t$. Now b is symmetric if and only if $b^t = b$, and b is antisymmetric if and only if $b^t = -b$. Hence the result. □

The next result gives a construction of the inverse of L, if one takes l to be the trace map.

F.2 Proposition. *Let k be a field, and K a finite separable k-algebra. Let V be a finitely generated projective K-module, and $b\colon V \times V \to k$ a k-bilinear map such that $b(ax, y) = b(x, ay)$ for all x and y in V and all a in K. Because of the separability, we have a natural isomorphism of K-algebras: $K \otimes_k K = K \times K'$, where we view $K \otimes_k K$ as a K-algebra via the first factor. This decomposition gives a decomposition of K-modules: $K \otimes_k V = K \otimes_k K \otimes_K V = V \oplus V'$ with $V' = K' \otimes_K V$. Let b_K denote the K-bilinear form on $K \otimes_k V$ obtained by extension of scalars. Then the decomposition of $K \otimes_k V$ in V and V' is orthogonal for b_K, and b' is the restriction to V of B_K. In particular, one has $b = \mathrm{tr} \circ b'$.*

Let us now note the special case where V is of dimension two. In that case, the K-vector space Y of antisymmetric K-bilinear forms is of dimension one, hence one gets the following corollary, which is of interest for Hilbert modular varieties.

F.3 Corollary. *Let k be a field, and $k \to K$ a finite separable k-algebra. Let V be a free K-module of rank two. Let $\psi_0\colon V \times V \to K$ be a non-degenerate alternating K-bilinear form. Then for every alternating k-bilinear form $\psi\colon V \times V \to k$ such that $\psi(ax, y) = \psi(x, ay)$ for all x and y in V and all a in K, there exists a unique b in K such that $\psi(x, y) = \mathrm{tr}(b\psi_0(x, y))$ for all x and y in V.*

G Moduli interpretation for the symplectic group.

For details, see [12, Sections 1, 4]. Just in this section, let G denote the group of symplectic similitudes of rank $2n$. More precisely, let $n \geq 0$ be an integer, and let G denote the group of automorphisms of the $\mathbb{Z}$-module $\mathbb{Z}^{2n}$ that preserve, up to scalar multiple, the standard symplectic form, i.e., the form given by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Let $X := \mathbb{H}_n^{\pm}$ the set of $h\colon \mathbb{S} \to G_{\mathbb{R}}$ that are Hodge structures of weight -1 such that ψ is a polarization up to a sign. Then this X is one $G(\mathbb{R})$-conjugacy class and it is called the Siegel double space. Let us consider:

$$A_n(\mathbb{C}) := G(\mathbb{Q})\backslash(X \times G(\mathbb{A}_{\mathrm{f}})/G(\hat{\mathbb{Z}})).$$

What we want to show is that $A_n(\mathbb{C})$ is the set of isomorphisms classes of pairs (A, λ) of principally polarized abelian varieties of dimension n. We already know what the interpretation of X is: it is the set of Hodge structures of weight -1 such that ψ is a polarization up to a sign. Let us now interpret $G(\mathbb{A}_{\mathrm{f}})/G(\hat{\mathbb{Z}})$. Consider the action of $G(\mathbb{A}_{\mathrm{f}})$ on the set of lattices in $\mathbb{A}_{\mathrm{f}}^2$. The stabilizer of the standard lattice $\hat{\mathbb{Z}}^2$ is $G(\hat{\mathbb{Z}})$. Hence $G(\mathbb{A}_{\mathrm{f}})/G(\hat{\mathbb{Z}})$ is the set of lattices of the form $x\hat{\mathbb{Z}}^2$, with x in $G(\mathbb{A}_{\mathrm{f}})$. We claim that this is the set of lattices L on which a suitable multiple of ψ induces a perfect pairing. For x in $G(\mathbb{A}_{\mathrm{f}})$ we have: $\psi(xu, xv) = \mu(x)\psi(u, v)$, which proves that $\mu(x)^{-1}\psi$ is a perfect pairing on $x\hat{\mathbb{Z}}^2$. On the other hand, let L be a lattice and a in $\mathbb{A}_{\mathrm{f}}^*$ be such that $a\psi$ is a perfect pairing on L. Then take a $\hat{\mathbb{Z}}$-basis $l_1, \ldots, l_{2n}$ of L such that $a\psi$ is in standard form, i.e., given by the matrix $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. Then the element x of $\mathrm{GL}_{2n}(\mathbb{A}_{\mathrm{f}})$ with $xe_i = l_i$ is in $G(\mathbb{A}_{\mathrm{f}})$. This finishes the proof of the fact that $G(\mathbb{A}_{\mathrm{f}})/G(\hat{\mathbb{Z}})$ is the set of lattices on which a multiple of ψ is perfect.

Let us now describe the constructions that give $A_n(\mathbb{C})$ the interpretation as the set of isomorphism classes of abelian varieties of dimension n, with a principal polarization.

Suppose (A, λ) is given. Then choose an isomorphism $f\colon \mathbb{Q}^{2n} \to \mathrm{H}_1(A, \mathbb{Q})$ such that ψ corresponds to a multiple of λ (such an f is unique up to an element of $G(\mathbb{Q})$). Let x be the element of X that is given by the Hodge structure on $\mathbb{Q}^{2n}$ induced from A via f. Let L in $G(\mathbb{A}_{\mathrm{f}})/G(\hat{\mathbb{Z}})$ be the lattice corresponding to $\mathbb{Z}^{2n}$ via f. The class of (x, L) modulo $G(\mathbb{Q})$ depends only on the isomorphism class of (A, λ).

Suppose now that we have (x, L) in $X \times G(\mathbb{A}_{\mathrm{f}})/G(\hat{\mathbb{Z}})$. Then let A be $(\mathbb{R} \otimes L)/L$ with the complex structure given by the Hodge structure corresponding to x. Let a be the element of $\mathbb{Q}^*$ such that $a\psi$ is perfect on L (this fixes a up to sign) and is a polarization λ on A (this fixes the sign). For g in $G(\mathbb{Q})$, multiplication by g gives an isomorphism from (A, λ) to the (A', λ') obtained from (gx, gL).

Let us end with a remark which is just a reminder to myself.

G.1 Remark. Let V be a free finitely generated $\mathbb{Z}$-module, with $h\colon \mathbb{S} \to \mathrm{GL}(V)_{\mathbb{R}}$ a Hodge structure of type $(-1, 0), (0, -1)$. Let $A := (\mathbb{R} \otimes V)/V$ be the associated complex torus. Then the dual complex torus corresponds to the Hodge structure $t \mapsto (h(t)^\vee)^{-1}N(t) = h(\bar{v})^\vee$ on $V^\vee$. In other words, the dual of A is $(\mathbb{R}\otimes V^\vee)/V^\vee$, with the complex structure on $\mathbb{R}\otimes V^\vee = (\mathbb{R}\otimes V)^{\vee_{\mathbb{R}}}$ such that z in $\mathbb{C}$ acts as $\bar{z}^\vee$. In order to prove this, one notes that the tangent space of A^t is

$\mathrm{H}^1(A, \mathcal{O}_A)$, which is naturally $\mathbb{C}$-anti-linearly isomorphic to $\mathrm{H}^0(A, \Omega^1_A)$, which is the dual of the tangent space of A at zero.

H Moduli interpretation of $S'(\mathbb{C})$.

Let us recall:

$$S'(\mathbb{C}) = G'(\mathbb{Q})\backslash(X' \times G'(\mathbb{A}_\mathrm{f})/G'(\hat{\mathbb{Z}})).$$

H.1 Proposition. *The Shimura variety $S'_\mathbb{Q}$ is the moduli space of triplets (A, α, λ) with A an abelian surface, $\alpha\colon O_K \to \mathrm{End}(A)$ a ring morphism, and $\lambda\colon A \to A^*$ a principal O_K-polarization.*

First of all, we have to explain what A^* is, and what we call a principal O_K-polarization. Let us begin with A^*: it is the dual of A in the category of abelian varieties with O_K-action. More precisely, since for A an abelian variety the dual is defined to be $A^t := \mathrm{Ext}^1(A, \mathbb{G}_\mathrm{m})$, we put:

$$A^* := \mathrm{Ext}^1_{O_K}(A, O_K \otimes \mathbb{G}_\mathrm{m}) = \delta \otimes_{O_K} \mathrm{Ext}^1(A, \mathbb{G}_\mathrm{m}) = \delta \otimes_{O_K} A^t,$$

with

$$\delta := \mathrm{Hom}_{O_K}(\mathrm{Hom}_\mathbb{Z}(O_K, \mathbb{Z}), O_K)$$

the different of the extension $\mathbb{Z} \to O_K$. In order to prove the above equalities, it is useful to note that for $A \to B$ a morphism of rings, for M a B-module and N and A-module, one has the adjunction:

$$\mathrm{Hom}_B(M, \mathrm{Hom}_A(B, N)) = \mathrm{Hom}_A({}_AM, N),$$

where ${}_AM$ denotes the A-module given by M. Then one uses that for B locally free of finite rank as A-module one has $\mathrm{Hom}_A(B, N) = B^{\vee_A} \otimes_A N$, with $B^{\vee_A} = \mathrm{Hom}_A(B, A)$ the A-dual of B. And then one uses that for P a finitely generated locally free B-module one has:

$$\mathrm{Hom}_B(M, P \otimes_A N) = P \otimes_B \mathrm{Hom}_B(M, B \otimes_A N).$$

This establishes:

$$\mathrm{Hom}_B(M, B \otimes_A N) = \delta \otimes_B \mathrm{Hom}_A(M, N),$$

with $\delta = (B^{\vee_A})^{\vee_B}$. Deriving with respect to N then gives:

$$\mathrm{Ext}^i_B(M, B \otimes_A N) = \delta \otimes_B \mathrm{Ext}^i_A(M, N).$$

This explains the reason that A^* occurs in this context. In our context, $A = \mathbb{Z}$ and $B = O_K$, so that δ is an ideal in O_K, since the trace map $\mathrm{tr}\colon O_K \to \mathbb{Z}$ gives an injective morphism

$O_K \to (O_K)^{\vee_{\mathbb{Z}}}$ (in fact, the trace map from B to A always gives a morphism $\delta \to B$, but it might be zero). This gives an isogeny:

$$A^* = \delta \otimes_{O_K} A^t \longrightarrow A^t.$$

We define an O_K-polarization to be an O_K-morphism $\lambda\colon A \to A^*$ such that the induced morphism from A to A^t is a polarization; λ is called principal if it is an isomorphism (note that this means that the induced morphism $A \to A^t$ is not an isomorphism, since O_K is ramified over $\mathbb{Z}$ (we do suppose that K is a field, after all).

Let us now turn to the proof of the proposition above that gives the moduli interpretation of $S'_{\mathbb{Q}}$. So we want to show that $S'(\mathbb{C})$ is the set of isomorphism classes of triplets (A, α, λ) over $\mathbb{C}$. In Hodge theoretical terms, such triplets are given by triplets (V, h, ψ) with V a locally free O_K-module of rank two, $h\colon \mathbb{S} \to (\mathrm{GL}_{\mathbb{Z}}(V))_{\mathbb{R}}$ a Hodge structure of type $(-1, 0), (0, -1)$, and $\psi\colon V \times V \to O_K$ a perfect antisymmetric O_K-bilinear form such that $\mathrm{tr} \circ \psi\colon V \times V \to \mathbb{Z}$ is a polarization. Note that for such a triplet (V, h, ψ), the pair (V, ψ) is isomorphic to the standard pair $(O_K \oplus O_K, \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right))$. The proof of the proposition can now be easily described. As in the last section, one shows that $G'(\mathbb{A}_{\mathrm{f}})/G'(\hat{\mathbb{Z}})$ is the O_K-lattices in K^2 on which $\psi = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ induces a perfect pairing of O_K-modules, up to a factor in $\mathbb{Q}^*$. The space X' is the set of Hodge structures. As in the last section, one shows that $G'(\mathbb{A}_{\mathrm{f}})/G'(\hat{\mathbb{Z}})$ is the O_K-lattices in K^2 on which $\psi = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ induces a perfect pairing of O_K-modules, up to a factor in $\mathbb{A}_{\mathrm{f}}^*$. The space X' is the set of Hodge structures of type $(-1, 0), (0, -1)$ on the K-vector space K^2 such that, up to sign, $\mathrm{tr} \circ \psi$ is a polarization. f type $(-1, 0), (0, -1)$ on the K-vector space K^2 such that, up to sign, $\mathrm{tr} \circ \psi$ is a polarization. After these remarks one simply follows the lines of the proof above of the modular interpretation for the symplectic group. Anyway, for details, one can consult [12, 4.11].

Let us end by stating that the multiplier character $\mu\colon G' \to \mathbb{G}_{\mathrm{m}}$ is the determinant (view G' as a subgroup of $\mathrm{Res}_{O_K/\mathbb{Z}}\mathrm{GL}_{2,O_K}$ and $\mathbb{G}_{\mathrm{m}}$ as a subgroup of $\mathrm{Res}_{O_K/\mathbb{Z}}\mathbb{G}_{\mathrm{m},O_K}$. More precisely, for all g in $G'(\mathbb{Q})$ and all x and y in K^2 we have $(\mathrm{tr} \circ \psi)(gx, gy) = \det(g)(\mathrm{tr} \circ \psi)(x, y)$.

I A remark on Mumford-Tate groups.

What I want to say is that to an isomorphism class of $\mathbb{Q}$-Hodge structures one can associate its Mumford-Tate group. Namely, if V and V' are isomorphic $\mathbb{Q}$-Hodge structures, and if f and f' are isomorphisms from V to V', then $f' = fg$ with g an automorphism of V. But then g centralizes the Mumford-Tate group in $\mathrm{GL}(V)$. Hence f and f' induce the same isomorphism from $\mathrm{MT}(V)$ to $\mathrm{MT}(V')$. For example, the functor $V \mapsto \mathrm{Aut}(V)$ does not have this property.

The same argument shows that a point P on a Shimura variety $\mathrm{Sh}_K(G,X)(\mathbb{C})$ defines an algebraic group $\mathrm{MT}(P)$, with a given $G(\mathbb{Q})$-conjugacy class of embeddings in G.

J On computing the generic Mumford-Tate group on $S'(\mathbb{C})$.

First note that for all $h = (h_1, h_2)\colon \mathbb{C}^* \to \mathrm{GL}_2(\mathbb{R})^2$ in X' one has $\det(h_1(z)) = \det(h_2(z))$ for all z. This shows that MT is contained in $G'_{\mathbb{Q}}$. The locally constant sheaf V becomes constant on X'. Hence $\mathrm{MT}_{\mathbb{R}}$ contains all $h(\mathbb{C}^*) \subset \mathrm{GL}_2(\mathbb{R})^2$ for the h in X'. In particular, it contains all conjugates under $G'(\mathbb{R})$ of those images. but then it contains all (x,x), all (yxy^{-1}, x), hence all $(xyx^{-1}y^{-1}, 1)$, etc. It follows that $\mathrm{MT} = G'_{\mathbb{Q}}$.

K Other remarks on Mumford-Tate groups.

We have defined the Mumford-Tate group $\mathrm{MT}(V)$ of a $\mathbb{Q}$-Hodge structure V given by a morphism $h\colon \mathbb{S} \to \mathrm{GL}(V)_{\mathbb{R}}$ to be the smallest algebraic subgroup H of $\mathrm{GL}(V)$ such that h factors through $H_{\mathbb{R}}$. This is not the usual definition, perhaps. The usual definition is to take $\mathrm{MT}'(V)$, the smallest subgroup H of $\mathrm{GL}(V) \times \mathbb{G}_{\mathrm{m}}$ such that $h'\colon \mathbb{S} \to \mathrm{GL}(V)_{\mathbb{R}} \times \mathbb{G}_{\mathrm{m},\mathbb{R}}$ factors through $H_{\mathbb{R}}$, where $\mathbb{S} \to \mathbb{G}_{\mathrm{m},\mathbb{R}}$ corresponds to $\mathbb{Q}(1)$. The difference between the two choices is that $\mathrm{MT}'(V)$ keeps track of weights, whereas $\mathrm{MT}(V)$ doesn't. The Tannakian interpretation of $\mathrm{MT}(V)$ is that it is the automorphism functor of the fibre functor "forget Hodge structure" on the tensor category generated by V. For $\mathrm{MT}'(V)$, one considers the tensor category generated by V and $\mathbb{Q}(1)$. Yet another (of course related) characterization is that $\mathrm{MT}'(V)$ seems to be the biggest subgroup of $\mathrm{GL}(V) \times \mathbb{G}_{\mathrm{m}}$ that fixes all elements of type $(0,0)$ in $\mathbb{Q}$-Hodge structures of the form $V^{\otimes n} \otimes (V^*)^{\otimes m} \otimes \mathbb{Q}(p)$. For this, see Deligne-Milne-Ogus-Shih. In the same way, $\mathrm{MT}(V)$ is characterized by the fact that it stabilizes all lines generated by Hodge classes (i.e., classes of some type (p,p)) in $\mathbb{Q}$-Hodge structures of the form $\oplus_i V^{\otimes n_i} \otimes (V^*)^{\otimes m_i}$.

Since I did not find this explicitly written (but I haven't looked very much, I should say), let me write a proof. So let H be the intersection of the stabilizers of such lines. Let us first prove that $\mathrm{MT}(V) \subset H$. So let t in some $T = \oplus_i V^{\otimes n_i} \otimes (V^*)^{\otimes m_i}$ be of some type (p,p). Then $\mathbb{R}t \subset T_{\mathbb{R}}$ is fixed by $\mathbb{S}$, hence by $\mathrm{MT}(V)$. This proves that $\mathrm{MT}(V) \subset H$. Let's now prove that $H \subset \mathrm{MT}(V)$. Now we use Chevalley's result: every subgroup of $\mathrm{GL}(V)$ is the stabilizer of a line in some finite dimensional representation of $\mathrm{GL}(V)$, plus the fact that each finite dimensional representation of $\mathrm{GL}(V)$ is contained in a representation of the form $\oplus_i V^{\otimes n_i} \otimes (V^*)^{\otimes m_i}$ (I will even give proofs for these two facts below, since I do not like the proof given in DMOS). Anyway, let t in some T be such that $\mathrm{MT}(V)$ is the stabilizer of $\mathbb{Q}t$. Then $\mathbb{R}t$ is fixed by $\mathbb{S}$, hence t is of some type (p,p).

(Use for example that the norm $\mathbb{S} \to \mathbb{G}_{\mathrm{m},\mathbb{R}}$ generates $\mathrm{Hom}(\mathbb{S}, \mathbb{G}_{\mathrm{m},\mathbb{R}})$.)

As I said, I do not like the proof of parts (a) and (b) of Proposition 3.1 in Chapter I of DMOS. So I give one.

K.1 Theorem. *Let G be an affine algebraic group over a field $k \supset \mathbb{Q}$. Let H be an algebraic subgroup of G, and V a finite dimensional faithful representation of G. Then there exists a line L in some representation of G of the form $\oplus_i V^{\otimes n_i} \otimes (V^*)^{\otimes m_i}$, such that H is the stabilizer of L.*

Proof. First of all, we may and do suppose that $G = \mathrm{GL}(V)$. The idea is now the following: let G act on itself by right translation; then G acts on $k[G]$, and H is the stabilizer of the ideal I_H; then use that I_H is finitely generated, and that $k[G]$ is locally finite. Let us first write down what $k[G]$ is, as a G-module via right translation on G. Well,

$$k[G] = k[\mathrm{End}(V)][1/\det] = \mathrm{Sym}_k(\mathrm{End}(V)^*)[1/\det] = \mathrm{Sym}_k(V^d)[1/\det],$$

where the last equality comes from the fact that $\mathrm{End}(V)^*$, as G-module given by right translation on $\mathrm{End}(V)$, is simply V^d, where d is of course the dimension of V (note that the G-action on $\mathrm{End}(V)^*$ extends to an $\mathrm{End}(V)$-action). Also, note that $\det$ is in $\mathrm{Sym}^d(\mathrm{End}(V)^*)$, and that we have $g \cdot \det = \det(g) \det$. The scalar subgroup $\mathbb{G}_\mathrm{m}$ of G induces a $\mathbb{Z}$-grading on $k[G]$. We have:

$$k[G]_i = \bigcup_j k[\mathrm{End}(V)]_{i+dj} \det^{-j},$$

and:

$$\begin{aligned}
&k[\mathrm{End}(V)]_i = \mathrm{Sym}^i(\mathrm{End}(V)^*) = \mathrm{Sym}^i(V^d) \subset (V^d)^{\otimes i} = (V^{\otimes i})^{d^i},\\
&k \cdot \det = \Lambda^d V \subset V^{\otimes d},\\
&k \cdot \det^{-1} = (\Lambda^d V)^* \subset (V^*)^{\otimes d}.
\end{aligned}$$

This describes $k[G]$ as G-module. Let $f_1, \ldots, f_r$ be a finite set of generators of the ideal I_H of $k[G]$. Let $W \subset k[G]$ be a finite dimensional sub-G-module containing the f_i. Then H is the stabilizer of the subspace $I_H \cap W$ of W, hence of the line $\Lambda^n(I_H \cap W) \subset \Lambda^n(W)$, with $n = \dim(I_H \cap W)$. Now note that W is a subrepresentation of a representation of the form $\oplus_i V^{\otimes n_i} \otimes (V^*)^{\otimes m_i}$. $\square$

K.2 Remark. If we allow subquotients of the $\oplus_i V^{\otimes n_i} \otimes (V^*)^{\otimes m_i}$, then we can drop the hypothesis that k is of characteristic zero.

K.3 Remark. If H contains the scalars in $G = \mathrm{GL}(V)$, then one can take L to be in some representation of the form $(V^{\otimes n})^m$. To prove this, consider the Zariski closure $\overline{H}$ of H in $\mathrm{End}(V)$, and use that it is a cone.

Just for fun, let us look at some examples in $G := \mathrm{GL}_2$. The Borel subgroup $B := \{(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix})\}$ is the stabilizer of the line generated by $(1,0)$ in $V := k^2$. The subgroup $\{(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix})\}$ is the stabilizer of $k(1,(1,0))$ in $k \oplus V$. The subgroup $\{(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix})\}$ is the stabilizer of $k(1,(0,1)^*)$ in $k \oplus V^*$. The subgroup $\{(\begin{smallmatrix} t & 0 \\ 0 & t \end{smallmatrix})\}$ is the stabilizer of $k((1,0),(0,1))$ in $V \oplus V$. The subgroup $\{(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix})\}$ is the stabilizer of the two-dimensional subspace of the $((x,0),(0,y))$ in $V \oplus V$; note that the proof above gives the same result. Finally, the trivial subgroup $\{(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix})\}$ is the stabilizer of $(1,(1,0),(0,1))$ in $k \oplus V \oplus V$.

L Modular interpretation of T_p.

Let A be a complex abelian surface with multiplication by O_K and with a principal O_K-polarization $\lambda\colon A \to A^*$. Let H be an O_K-submodule of $A[p](\mathbb{C})$ that is free of rank one. Then we claim that $p\lambda$ induces a principal O_K-polarization on A/H. So how does this work? Write $p\lambda = \pi_2\pi_1$, with $\pi_1\colon A \to B$ the quotient by H. Then $(A/H)^*$ is the quotient of A by $\ker(\pi_2^*)$. So we have to see that $\ker(\pi_2^*) = \ker(\pi_1)$. Since both have the same number of elements, it suffices to see that one is contained in the other. Since $\ker(\pi_1)$ is maximal isotropic for the pairing $e_{\lambda,p}$ that λ induces on $A[p]$, it suffices to see that $\ker(\pi_2^*)$ and $\ker(\pi_1)$ are orthogonal for that pairing. That results from standard things about such pairings coming from expressions like $A^* = \mathrm{Ext}^1(A, O_K \otimes \mathbb{G}_{\mathrm{m}})$.

The general statement is this: let $f\colon A \to B$ and $g\colon B \to C$ be isogenies of abelian varieties with multiplications by O_K. Let $h := gf$. Then we have a short exact sequence:

$$0 \longrightarrow \ker(f) \longrightarrow \ker(h) \longrightarrow \ker(g) \longrightarrow 0.$$

Applying $\mathrm{Hom}(\cdot, O_K \otimes \mathbb{G}_{\mathrm{m}})$ gives an isomorphism of short exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(g^*) & \longrightarrow & \ker(h^*) & \longrightarrow & \ker(f^*) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \ker(g)^* & \longrightarrow & \ker(h)^* & \longrightarrow & \ker(f)^* & \longrightarrow & 0. \end{array}$$

The fact that the map from $\ker(g^*)$ to $\ker(f)^*$ is zero means that $\ker(f)$ and $\ker(g^*)$ are orthogonal for the paring induced by h between $\ker(h)$ and $\ker(h^*)$.

M Some stuff on orders in finite separable $\mathbb{Q}$-algebras.

I need lower bounds for orders of Picard groups of certain orders in certain CM fields. Therefore, some general theory should be quite useful.

Let $\mathbb{Q} \to K$ be a finite separable $\mathbb{Q}$-algebra. Then K is a finite product of number fields, say $K = K_1 \times \cdots \times K_m$, and the integral closure of $\mathbb{Z}$ in K is then the product of the maximal orders of the K_i. Let $R \subset K$ be an order in K, i.e., a subring of K with $\mathbb{Q} \otimes R = K$ and which is finitely generated as a $\mathbb{Z}$-module. Then R is contained in O_K since the elements of R are integral over $\mathbb{Z}$, and O_K/R is a finite additive group, since R and O_K are free $\mathbb{Z}$-modules of the same finite rank. Consider ideals of R that are also O_K-ideals. Clearly a lot of such ideals do exist: for every n in $\mathbb{Z}$ that annihilates O_K/R, we have the example nO_K. The sum of a family of such ideals is again one such, hence there exists a unique maximal such ideal, called the conductor of R (relative to O_K). I don't think that we will use this conductor so much, since we want estimates in terms of the discriminant of R.

Let $I \subset R$ be a non-zero ideal that is also an O_K-ideal. Then R is the inverse image in O_K of the subring R/I of the quotient O_K/I of O_K). Actually, the diagram:

$$\begin{array}{ccc} R & \longrightarrow & R/I \\ \downarrow & & \downarrow \\ O_K & \longrightarrow & O_K/I \end{array}$$

is both Cartesian and co-Cartesian. For us, the most important is that every order of K is obtained as follows: take the inverse image in O_K of a subring of a finite quotient of O_K.

M.1 Discriminants.

Recall that $\mathrm{discr}(O_K)$ is the discriminant of the trace form on O_K. To be precise: for M a free $\mathbb{Z}$-module of finite rank and b a bilinear form on M, let $\mathrm{discr}(M, b)$ be the integer defined by: let m be a basis of M, then $\mathrm{discr}(M, b)$ is the determinant of the matrix of b relative to m. In more intrinsic terms, one can use that b induces a bilinear form on the maximal exterior power of M, and use the integer coming from there. The whole thing does not depend on the basis because changing the basis changes it by the square of a unit. Over more general rings, and for projective modules, one obtains an ideal, locally principal, with some extra structure due to the squares of units that intervene. In fact, one sees that if the local generators of the ideal are non zero divisors, then the ideal is, as invertible module, the square of ΛM. In our case, we use the bilinear form $(x, y) \mapsto \mathrm{tr}(xy)$. The separability of $\mathbb{Q} \to K$ shows that $\mathrm{discr}(O_K) \neq 0$. Choosing a basis of O_K adapted to R shows that:

$$\mathrm{discr}(R) = \mathrm{discr}(O_K)\, |O_K/R|^2.$$

M.2 Theorem. *Let ζ_R denote the zeta function of the order R, i.e., the zeta function of* $\mathrm{Spec}(R)$

in the usual sense. Then:

$$\mathrm{Res}_1(\zeta_R) := \lim_{s\to 1}(s-1)^m\zeta_R(s) = \frac{2^{r_1}(2\pi)^{r_2}|\mathrm{Pic}(R)|\,\mathrm{Reg}(R)}{|\mathrm{tors}(R^*)|\,|\mathrm{discr}(R)|^{1/2}},$$

with $\mathbb{R}\otimes K \cong \mathbb{R}^{r_1}\times\mathbb{C}^{r_2}$ and $\mathrm{Reg}(R)$ the regulator of R (see in the proof for the definition). (Recall that K is the product of m number fields.)

Proof. For O_K, see for example Lang's "Algebraic number theory", 2nd edition, VIII, §2. In fact, Lang gives the proof when K is a field, but for O_K in a product of number fields everything decomposes into products. Let us digress a little bit on the regulator. I find that the regulator $\mathrm{Reg}'(R)$ should be defined as follows: one considers

$$O_K^* \longrightarrow (\mathbb{R}\otimes O_K)^* \stackrel{\log\|\|}{\longrightarrow} \mathbb{R}^{r_1+r_2},$$

and puts:

$$\mathrm{Reg}'(R) := \mathrm{Vol}(\mathbb{R}^{r_1+r_2,+=0}/\text{image of } O_K^*),$$

with the volume measured with respect to the volume form coming from the standard inner product on $\mathbb{R}^{r_1+r_2}$, and where $\log\|\,\|$ is taking log of absolute value at every factor of $\mathbb{R}\otimes O_K$, with $\|x\|$ being the factor by which the Haar measures change ($|x|$ for a real place, $|x|^2$ for a complex one). But this does not give the usual definition, as given in Lang. There one omits any one of the infinite places in order to get a square matrix of which one takes absolute value of the determinant. One easily proves that $\mathrm{Reg}'(R) = 2^{-r_2}(r_1+2r_2)(r_1+r_2)^{-1/2}\mathrm{Reg}(R)$, which actually makes my definition a bit ugly.

Anyway, let's proceed. Since we know the theorem for O_K, all we have to do is to compare our R to O_K. Let $X := \mathrm{Spec}(O_K)$, $Y := \mathrm{Spec}(R)$, and $N\colon X\to Y$ the morphism induced by the inclusion of R in O_K. Then we have a short exact sequence of sheaves on X:

$$0\longrightarrow \mathcal{O}_Y^* \longrightarrow N_*\mathcal{O}_X^* \longrightarrow Q \longrightarrow 0,$$

with Q a skyscraper sheaf given by $\overline{O_K}^*/\overline{R}^*$ in case R is given by the subring $\overline{R}$ of the finite quotient $\overline{O_K}$ of O_K. This gives a long exact sequence:

$$0\longrightarrow R^*\longrightarrow O_K^*\longrightarrow \overline{O_K}^*/\overline{R}^*\longrightarrow \mathrm{Pic}(R)\longrightarrow \mathrm{Pic}(O_K)\longrightarrow 0.$$

Let A be the cokernel of $R^*\to O_K^*$, and B the kernel of $\mathrm{Pic}(R)\to\mathrm{Pic}(O_K)$. Then one gets:

$$|\mathrm{Pic}(R)| = |B|\,|\mathrm{Pic}(O_K)|,\quad |\overline{O_K}^*/\overline{R}^*| = |A|\,|B|,\quad |A| = \frac{|\mathrm{tors}(O_K^*)|}{|\mathrm{tors}(R^*)|}\left|\frac{O_K^*/\mathrm{tors}}{R^*/\mathrm{tors}}\right|$$
$$\mathrm{Reg}(R) = \left|\frac{O_K^*/\mathrm{tors}}{R^*/\mathrm{tors}}\right|\mathrm{Reg}(O_K),\quad |\mathrm{discr}(R)|^{1/2} = \frac{|\overline{O_K}|}{|\overline{R}|}|\mathrm{discr}(O_K)|^{1/2}.$$

Putting this all together shows that the right hand side of the equality we want to prove changes by the factor $|\overline{O_K}^*|\,|\overline{R}^*|^{-1}\,|\overline{R}|\,|\overline{O_K}|^{-1}$ when going from O_K to R. So all that we have to do now is to show that the left hand side changes by the same factor. But then note:

$$\frac{|\overline{R}|}{|\overline{R}^*|} = \prod_{k \text{ res field of } \overline{R}} \frac{|k|}{|k^*|} = \prod_k \frac{1}{1-|k|^{-1}},$$

which is clearly the contribution to $\mathrm{Res}_1(\zeta_R)$ of those residue fields. $\square$

M.3 Theorem. *Let $N > 0$. Then there exists a real number $c > 0$ such that for every order R in a separable $\mathbb{Q}$-algebra K of degree at most N, one has:*

$$|\mathrm{Pic}(R)|\,\mathrm{Reg}(R) \geq c\,|\mathrm{discr}(R)|^{1/7}.$$

M.4 Remark. As the proof will show, we can actually get $1/6-\varepsilon$ as exponent, instead of $1/7$, with a c depending on ε, for every $\varepsilon > 0$. If one assumes the generalized Riemann hypothesis, then one can get $1/2-\varepsilon$ as exponent, for every $\varepsilon > 0$, with again c depending on ε. In that case, one uses Siegel's theorem that one finds in [17, Ch. XIII, §4].

Proof. We will first prove this for maximal orders in number fields of bounded degree, then for maximal orders in finite separable $\mathbb{Q}$-algebras of bounded degree, and then for arbitrary orders of bounded degree.

In the case of a maximal order of a number field of bounded degree, we just apply two theorems. The first one is the Brauer-Siegel theorem (see for example [17, Ch. XVI]), that states that:

> *for $N > 0$ and $\varepsilon > 0$, there exists $c > 0$ such that:*
>
> $$|\mathrm{Pic}(O_K)|\,\mathrm{Reg}(O_K) \geq c\,|\mathrm{discr}(O_K)|^{1/2-\varepsilon}$$
>
> *for all Galois extensions K of $\mathbb{Q}$ of degree at most N.*

The second theorem is one of Stark ([29, Thm. 1]):

> *let $N > 0$. There exists $c > 0$ such that for all number fields K of degree at most N over $\mathbb{Q}$, one has:* $|\mathrm{Pic}(O_K)|\,\mathrm{Reg}(O_K) \geq c\,|\mathrm{discr}(O_K)|^{1/2-1/[K:\mathbb{Q}]}$.

Together, these two results show:

> *let $N > 0$. There exists $c > 0$ such that for every number field K of degree at most N over $\mathbb{Q}$ one has:* $|\mathrm{Pic}(O_K)|\,\mathrm{Reg}(O_K) \geq c\,|\mathrm{discr}(O_K)|^{1/6}$.

This settles the case where the $\mathbb{Q}$-algebra K is a field. The case for a maximal order in a finite separable $\mathbb{Q}$-algebra of degree at most N then follows, because everything decomposes into a product of at most N factors, for which one has the result already.

So let now K be a finite separable $\mathbb{Q}$-algebra of degree at most N, and let R be an order in it, given by the subring $\overline{R}$ of some finite quotient $\overline{O_K}$ of O_K. We have already seen that:

$$|\mathrm{Pic}(R)|\,\mathrm{Reg}(R) = \frac{|\overline{O_K}^*|}{|\overline{R}^*|}|\mathrm{Pic}(O_K)|\,\mathrm{Reg}(O_K)\frac{|\mathrm{tors}(R^*)|}{|\mathrm{tors}(O_K^*)|},$$
$$|\mathrm{discr}(R)| = \left(\frac{|\overline{O_K}|}{|\overline{R}|}\right)^2 |\mathrm{discr}(O_K)|.$$

We note that the quotient $|\mathrm{tors}(R^*)|\,|\mathrm{tors}(O_K^*)|^{-1}$ and its inverse are bounded in terms of N only. Hence the theorem follows from the following claim:

for $N > 0$ and $\varepsilon > 0$ there exists $c > 0$ such that for R an order in a finite separable $\mathbb{Q}$-algebra K of degree at most N, one has:

$$\frac{|\overline{O_K}^*|}{|\overline{R}^*|} \geq c\left(\frac{|\overline{O_K}|}{|\overline{R}|}\right)^{1-\varepsilon},$$

where R is the inverse image of the subring $\overline{R}$ of the finite quotient $\overline{O_K}$ of O_K.

We now prove this claim. Let n denote $|\overline{O_K}/\overline{R}|$. We may and do assume that $n > 1$. Localizing at the maximal ideals of $\overline{R}$, followed by a simple computation, shows that:

$$\frac{|\overline{O_K}^*|}{|\overline{R}^*|} \geq n\prod_{p|n}\left(1-\frac{1}{p}\right)^N \geq n\left(\frac{1}{5\log(n)}\right)^N.$$

Since $\log(n) = n^{o(1)}$, this shows our claim, and hence finishes the proof of the theorem. □

N On effective Chebotarev.

As usual, let $\mathrm{Li}(x) := \int_2^x dt/\log(t)$. If one assumes GRH, then the effective Chebotarev theorem of Lagarias, Montgomery and Odlyzko, stated as in [28, Thm. 4] and the second remark following that theorem, says:

for M a finite Galois extension of $\mathbb{Q}$, let n_M denote its degree, d_M its absolute discriminant $|\mathrm{discr}(O_M)|$, and for x in $\mathbb{R}$, let $\pi_{M,1}(x)$ be the number of primes $p \leq x$ that are unramified in M and such that the Frobenius conjugacy class Frob_p contains *just the identity element of* $\mathrm{Gal}(M/\mathbb{Q})$*. Then one has, for all sufficiently large* x *and all finite Galois extensions* M *of* $\mathbb{Q}$*:*

$$\left|\pi_{M,1}(x) - \frac{1}{n_M}\mathrm{Li}(x)\right| \leq \frac{1}{3n_M}x^{1/2}\left(\log(d_M) + n_M \log(x)\right).$$

This result shows that for all x sufficiently large, and all finite Galois extensions M of $\mathbb{Q}$, one has:

$$\pi_{M,1}(x) \geq \frac{x}{n_M \log(x)}\left(\mathrm{Li}(x)\frac{\log(x)}{x} - \frac{\log(x)}{3x^{1/2}}\left(\log(d_M) + n_M \log(x)\right)\right).$$

If x tends to infinity, $\mathrm{Li}(x)\log(x)/x$ tends to 1 and $\log(x)^2/x^{1/2}$ tends to 0. Some computation (that we will do below) shows that if x is sufficiently big (i.e., bigger than some absolute constant), and bigger than $2(\log(d_M)^2(\log(\log(d_M)))^2$, then $\log(x)\log(d_M)/3x^{1/2} < 1/2$, and hence:

$$\pi_{M,1}(x) \geq \frac{x}{3n_M \log(x)}.$$

Here is the computation that I promised. Put $a := \log(d_M)/3$. We want to find a lower bound for x that implies that $a\log(x)/\sqrt{x} < 1/2$. We put $x := y^2$ (with $y > 0$, of course). Then what we want is a lower bound for y such that $b\log(y) < y$, with $b = 4a$. we put $y = zb$. Then what we want is a lower bound for z such that $z - \log(z) > c$, with $c = \log(b)$. Now write $z = (1+u)c$. Then what we want is: $uc - \log(1+u) - \log(c) > 0$. Since $\log(1+u) \leq u$, it suffices that $uc - u - \log(c) > 0$, i.e., that $u > \log(c)/(c-1)$ (by the way, since we are willing to let x be sufficiently large, we may take care of small d_M by that, and suppose that c is sufficiently large). For c sufficiently large, for any $\varepsilon > 0$, $u > \varepsilon$ is good enough. Translating this back to x and $\log(d_M)$, one gets that $x > (1+\varepsilon)^2(4a\log(4a))^2$ is good. Then one uses that $2 > 16/9$.

O Real approximation.

It is known that for G an affine algebraic group over $\mathbb{Q}$ one has $G(\mathbb{Q})$ dense in $G(\mathbb{R})$. This is what Deligne calls real approximation. To prove it, one reduces to the case of tori. But even that case is not so trivial to me. Of course, tori are unirational (they are images of tori that are products of multiplicative groups of number fields), but that is not enough: that only gives that the rational points of G are dense in the connected components of $G(\mathbb{R})$ that do contain a rational point. Anyway, for a detailed proof I would refer to the book [26] of Platonov and Rapinchuk.