GROUP SCHEMES *À LA MAZUR*

Contents

1. Finite flat group schemes

In this section we want to study the properties of finite flat group schemes G over a Dedekind base S. We will be mainly interested in the case in which $S = Spec(\mathbb{Z})$ or some affine open subschemes. Since finite morphism are affine, we will almost always restrict to the case $G = Spec(A)$.

Def 1. *Let X be a finite S-scheme. We say X is* flat *over S if and only if $\mathcal{O}_X$ is locally free of finite rank as an $\mathcal{O}_S$-mod. In particular, X is finite flat over S if and only if there exists a cover of S by affine U_i such that $f^{-1}(U_i) \to U_i$ is of the form*

$$Spec(A) \to Spec(R)$$

with A free of finite rank as an R-mod. If X and S are affine, this is equivalent to ask $\mathcal{O}_X(X)$ is flat as an $\mathcal{O}_S(S)$ module. The rank is a locally constant function on S and it is called the order *of X over S denoted by $[X : S]$.*

1.1. The étale case.

We recall a standard result for finite flat group schemes.

Prop. 1.1. *Let $G = Spec(A)$ a finite flat group scheme of order p over $S = Spec(R)$. If p is invertible in R then G is étale over S.*

Proof. See [EGA IV] 17.6.2. □

Recall that we have an important equivalence of categories for finite étale group schemes.

Theorem 1. *Let $S = Spec(R)$ be a connected affine scheme. Let $\overline{S} = Spec(\overline{R})$ an universal étale cover of S. Let $\pi = Gal(\overline{R}, R)$ be the absolute Galois group associated. We then have an equivalence of categories between finite étale commutative S-group schemes and the category of finite discrete π-modules. The functor is given by*

$$Y \mapsto Y(\overline{R}).$$

1.2. **Oort and Tate classification.** Let p be a prime, consider the ring Λ given by

$$\Lambda = \mathbb{Z}\left[\mu_{p-1}, \frac{1}{p(p-1)}\right] \cap \mathbb{Z}_p\,.$$

Hereafter some examples of Λ for various p's

(1) $p = 2, \quad \Lambda = \mathbb{Z}$,
(2) $p = 3, \quad \Lambda = \mathbb{Z}\left[\frac{1}{2}\right]$,
(3) $p = 5, \quad \Lambda = \mathbb{Z}\left[i, \frac{1}{2(2+i)}\right]$
(4) $p = 7, \quad \Lambda = \mathbb{Z}\left[\rho, \frac{1}{6(\rho-4)}\right]$

Let $S = Spec(R)$ a scheme over Λ and consider $G = Spec(A)$ a finite flat group scheme of order p over S. In this section, we want to classify all the possible R-algebra A. By a Theorem of Deligne, we know that G is annihilated by p, this means that A is a module over the group algebra $R[\mathbb{F}_p^\times]$. Let e_i the R-operators defined by

$$e_i = \frac{1}{p-1} \sum_{m \in \mathbb{F}_p^\times} \chi^{-i}(m)[m] \in R[\mathbb{F}_p^\times]$$

where χ is the usual Teichmuller character $\chi : \mathbb{F}_p^\times \to \mathbb{Z}_p$. This operators are orthogonal and idempotent on the augmentation ideal I of A, $I = \ker(A \to R)$. In particular we have a decomposition

$$I = \bigoplus_{i=1}^{p-1} I_i, \quad I_i = \{f \in A : [m]f = \chi^i(f)\}.$$

In particular, I_i are locally free of rank 1 and $I_1^i = I_i$ for every $1 \le i \le p-1$.

Consider the group $\mu_{p,\Lambda} = Spec(B)$ with $B = \Lambda[z]/(z^p - 1)$. The augmentation ideal is given by $I = B(z-1)$ that admits a basis over Λ given by $(1 - z^m)$. This induces the decomposition

$$I = \Lambda(1-z) + \Lambda(1-z^2) + \cdots + \Lambda(1-z^{p-1}).$$

For each i we define

$$y_i = (p-1)e_i(1-z) = \sum_{m \in \mathbb{F}_p^\times} \chi^{-i}(m)(1-z^m).$$

We then get the decomposition $I = \Lambda y_1 + \Lambda y_2 + \cdots \Lambda y_{p-1}$, where $I_i = y_i\Lambda$. From the definition of e_i we obtain that the $[m]y_i = \chi(m)^i y_i$. Since $I_1^i = I_i$ we define w_i to be

$$y_1^i = w_i y_i.$$

For the first primes we have the following list of w_i

(1) $p = 2$: $w_1 = 1, \quad w_2 = 2$,
(2) $p = 3$: $w_1 = 1, \quad w_2 = -1, \quad w_3 = -3$,
(3) $p = 5$: $w_1 = 1, \quad w_2 = -i(2+i), \quad w_3 = (2+i)^2, \quad w_4 = -(2+i)^2, \quad w_5 = -5(2+i)^2$.

The following proposition follows straightforwardly from the previous discussion

Prop. 1.2. *The elements w_i are invertible for every $1 \le i \le p-1$, $w_p = pw_{p-1}$. We have $B = \Lambda[y]/(y^p - w_p y)$ where $y = y_1$. Furthermore, y satisfies the following properties*

(i) $sy = y \otimes 1 + 1 \otimes y + \dfrac{1}{p-1} \displaystyle\sum_{i=1}^{p-1} \frac{1}{w_i w_{p-i}} y_i \otimes y_{p-i}$;
(ii) $[m]y = \chi(m)y$;
(iii) $z = 1 + \dfrac{1}{p-1}\left(y + \dfrac{y^2}{w_2} + \cdots + \dfrac{y^{p-1}}{w_{p-1}}\right)$.

Consider now again an S-group scheme $G = Spec(A)$ finite flat group of order p with $S = Spec(R)$ where R is a Λ-algebra. Then take the symmetric R-algebra generated by I_1

$$Sym_R(I_1) = R \oplus I_1 \oplus I_1^{\otimes 2} \oplus \cdots$$

by the previous discussion, we have a surjective morphism $Sym_R(I_1) \to A$ induced by the inclusion $I_1 \subset A$. The kernel is given by the ideal generated by $(a-1) \otimes I^{\otimes p}$ where $a \in I^{\otimes(1-p)} = Hom_R(I_1^{\otimes p}, I_1)$ is the element corresponding by the multiplication in A. Let $G' = Spec(A')$ the Cartier dual of G. We can define analogously I', I_1', a'. Since G is annihilated by p, we have that the Cartier pairing factors through $\mu_{p,s}$

$$G \times_S G' \to \mu_{p,S}.$$

Let $\varphi : R[y]/(y^p - w_p y) \to A \otimes_T A'$ the associated map on the algebras. We then have the following result.

Lemma 1.1. *The image $\varphi(y)$ of y is a generating section of $I_1 \otimes I_1'$. Identifying I_1' with $I_1^{\otimes(-1)} = Hom_R(I_1, R)$, we have $a \otimes a' = w_p$.*

From this characterisation we obtain the following equivalence result.

Theorem 2. *The map $G \mapsto (I_1', a, a')$ gives a bijection between isomorphism classes of S-group schemes of order p and isomorphism classes of triples (L, a, b) where*

(1) L is a locally free R-module of rank 1,
(2) $a \in L^{\otimes(p-1)}$ and,
(3) $b \in L^{\otimes(1-p)} = Hom_R(L^{\otimes(p-1)}, R)$

such that $a \otimes b = w_p$.

Proof. We will show only how to construct a group scheme from the triple (L, a, b). The problem is local on the base S, we can then restrict to $S = Spec(R)$ and $L = R$ free on S. We have in particular $a, b \in R$ such that $ab = w_p$. Let F the field of fractions of Λ, U an indeterminate. By the previous proposition, we have $\mu_{p,F(u)} = Spec(A)$ with

$$A = F(U)[y]/(y^p - w_p y),$$

with comultiplication given by

$$sy = y \otimes 1 + 1 \otimes y + \frac{1}{p-1} \sum_{i=1}^{p-1} \frac{1}{w_i w_{p-i}} y^i \otimes y^{p-i}.$$

Define $R_0 = \Lambda[X_1, X_2]/(X_1 X_2 - w_p)$ and $C = R_0[Y]/(Y^p - X_1 Y)$ under the change of variables $Y = U^{-1} y$ we observe that C injects in A. In particular, it can be checked that the comultiplication on A induces a comultiplication on C. Let $G_0 = Spec(C)$ the R_0-group scheme of order p then obtained. Consider the morphism $h : R_0 \to R$ induced by sending X_1 to a and X_2 to b. The group scheme obtained by base change is then

$$G = G_0 \times_{R_0} Spec(R) = Spec(R[Y]/(Y^p - aY)).$$

□

Example 1. *Consider the case of a Λ-algebra R that is complete noetherian local with residue field of characteristic p. In this case, every projective module of rank one is free. Given $a, c \in R$ such that $ac = p$, we denote $G^c_{a,R} = G^R_{a,cw_{p-1}}$*

$$G^c_{a,R} = Spec(R[Y]/(Y^p - aY)).$$

We will now focus to the case of K algebraic number field of finite degree over $\mathbb{Q}$ and R an integrally closed subring of K whose field of fractions is K (we then also allow $\mathbb{Z}[1/p]$ in $\mathbb{Q}$). Let M the set of non-trivial discrete valuations of R. For each $\nu \in M$ denote R_ν the completion and K_ν its fraction field. We want then to classify the R-group schemes G of order p. Let H the generic fiber of G, $H = G \times_R Spec(K)$ and $G_\nu = G \times_R Spec(R_\nu)$ its completion at every place ν. We then have that each generic fiber of G_ν coincide with the completion of H

$$G_\nu \times Spec(K_\nu) = H_\nu = H \times_R Spec(K_\nu).$$

Let E be the functor that associates to a ring X the set of isomorphism classes of group schemes over $Spec(X)$ of order p. Let $\mathbb{A}_K^\times$ be the idéle class of K and U_ν the group of units of R_ν for every $\nu \in M$. We then have the following characterisation for the set of étale group schemes.

Prop. 1.3. *We have the following canonical bijections*

$$E(K) \cong Hom_{cont}(\mathbb{A}_K^\times/K^\times, \mathbb{F}_p^\times),$$
$$E(K_\nu) \cong Hom_{cont}(K_\nu^\times, \mathbb{F}_p^\times),$$
$$E(R_\nu) \cong Hom_{cont}(K_\nu^\times/U_\nu, \mathbb{F}_p^\times) \quad \textit{for } \nu \nmid p.$$

Proof. First of all, observe that from Prop. 1.1 we have that all the group schemes for the rings mentioned are étale. By Theorem 1 we then have an equivalence of categories between finite étale group schemes and finite discrete π-modules. Since we are dealing with groups of order p, we only need to specify what is the continuous action of π on $\mathbb{Z}/p\mathbb{Z}$. This amounts to give a map from $\pi \to \mathbb{F}_p^\times$ that factors through a finite Galois extension. Using Class Field Theory we have the following commutative diagram

$$\begin{array}{ccc}
\mathbb{A}_K^\times/K^\times & \longrightarrow & \pi(K)^{ab} \\
\uparrow & & \uparrow \\
K_\nu^\times & \longrightarrow & \pi(K_\nu)^{ab} \\
\downarrow & & \downarrow \\
K_\nu^\times/U_\nu & \longrightarrow & \pi(R_\nu)^{ab}.
\end{array}$$

These horizontal maps becomes isomorphism when we pass to the completion with respect to open subgroups of finite index. They then induces an isomorphism when we consider the group of continuous characters with values in a finite group like $\mathbb{F}_p^\times$. □

In order to then give a final characterization to these group schemes, we need to specify the data at the places M_p corresponding to $\nu|p$. By Theorem 2 we have a characterisation of the finite group schemes of order p over a Λ-algebra. In particular, when we consider the completion at R_ν we have an explicit description provided in example 1. For every $\nu \in M_p$, there exists $a \in R_\nu$ such that

$$G_\nu = G \times_R Spec(R_\nu) \cong (G_a^{p/a})_{R_\nu}.$$

Let η_ν^G be the valuation of $a \in R_\nu$ attached to the completion of G. The value of η_ν completely determines the structure of G_ν. We can then state the classification result of Oort and Tate.

Theorem 3 (Oort - Tate)**.** *Let G be a finite flat group of order p over $Spec(R)$. The map $G \mapsto (\psi, (\eta_\nu^G)_{\nu\in M_p})$ gives a bijection between isomorphism classes of R-group schemes of order p and the system of continuous homomorphism $\psi : \mathbb{A}_K^\times/K^\times \to \mathbb{F}_p^\times$ together with a sequence of integers $(\eta_\nu)_{\nu\in M_p}$ such that $0 \le \eta_\nu \le \nu(p)$ satisfying the following properties*

(1) *for $\nu \in M - M_p$, ψ is unramified at ν, i.e. $\psi(U_\nu) = 1$;*
(2) *for $\nu \in M_p$, $\psi_\nu(u) = N_{k/\mathbb{F}_p}(\overline{u})^{-\eta_\nu}$, for all $u \in U_\nu$ where ψ_ν is the canonical restriction of ψ to K_ν, k is the residue field of R_ν and $\overline{u}$ is the reduction to the residue field.*

Corollary 3.1. *Let R ring of integers of a number field with class number coprime with $p-1$ such that p is inert. Then the only finite flat R-groups of order p are $(\mathbb{Z}/p\mathbb{Z})_R$ and $(\mu_p)_R$.*

2. Quasi-finite groups

First of all, recall the definition and basic properties of *quasi-finite* morphisms.

Def 2. *A morphism of schemes $f : X \to Y$ is called* quasi-finite *if it is of finite type and satisfies one of the following equivalent properties*

(i) every $x \in X$ is isolated in its fiber $f^{-1}(f(x))$;
(ii) for every $x \in X$, $f^{-1}(f(x)) = X \times_Y f^{-1}(f(x))$ is a finite $k(f(x))$ scheme;
(iii) for every $x \in X$, $\mathcal{O}_{X,x} \otimes k(f(x))$ is finitely generated over $k(f(x))$.

We have that closed immersions are quasi-finite, if f is unramified then f is quasi-finite and that quasi-finite morphisms are stable and base change and composition.

The main property of quasi-finite morphism is given by the following structure result.

Prop. 2.1 (Stacks 37.41.6)**.** *Let $f : X \to S$ be a quasi-finite morphism of schemes, separated and locally of finite type. Let $s \in S$ then there exists an elementary étale neighborhood $(U, u) \to (S, s)$ and a decomposition*

$$X \times_S U = X_f \coprod X_\nu$$

with

(1) $X_f \to U$ finite morphism,
(2) X_ν has empty fiber of s.

Let N, p be distinct prime numbers. We will mainly study quasi-finite schemes over $S = Spec\,\mathbb{Z}$ and $S' = Spec(\mathbb{Z}[1/N])$, $S'' = Spec(\mathbb{Z}[1/p])$. In particular, Mazur's theorem revolves around quasi-finite group schemes G over S of order a power of p with the following properties:

(1) $G_{|S'}$ is finite flat group scheme over S';
(2) $G_{|S''}$ is quasi-finite étale group scheme over S'';

in particular, $G_{|S' \cap S''}$ is a finite étale group scheme over $S' \cap S''$.

We want then to describe the quasi-finite étale morphism $X \to S''$ that are finite étale over $S' \cap S''$. A similar theorem gives us a classification in terms of the Galois structure where we specify the data at the special fiber over (N). To do this, the structure proposition for quasi-finite morphism plays a very important role

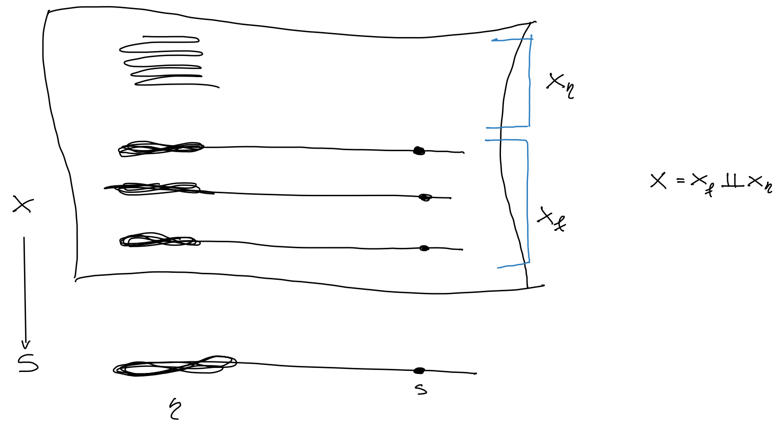
Lemma 2.1. *Let X a quasi-finite étale separated scheme over S''. Assume that X is finite étale over $(S' \cap S'')$. There is a canonical injection*

$$X(\overline{\mathbb{F}_N}) \hookrightarrow X(\overline{\mathbb{Q}})^{I_N},$$

in particular, this is a bijection with $\#X(\overline{\mathbb{F}_N}) = rank(X_{\mathbb{Q}})$ if and only if $X \to S''$ is finite.

Proof. The property of finiteness over an open neighborhood of (N) can be checked at $X_{|\mathcal{O}_{S'',(N)}} \to Spec(\mathcal{O}_{S'',(N)})$. Furthermore, we can check it after any $fppf$ base change, and in particular since the strict henselianization $\mathcal{O}^{sh}_{S'',(N)}$ is faithfully flat over $\mathcal{O}_{S'',(N)}$ we can restrict to the case $X \to S$ quasi-finite separated with S local and strictly henselian. In this case, the residue field becomes $\overline{\mathbb{F}}_N$ and the fraction field K is the fixed field of $\overline{\mathbb{Q}}$ under the inertia group I_N. By the structure result of quasi-finite schemes we have that over S, X decomposes as

$$X = X_f \coprod X_\eta$$



with X_f finite over S and X_η having empty closed fiber. In particular X_f is finite étale over S, this implies X_f is a finite disjoint union of copies of S. We then have a natural bijection

$$X_f(K) \to X_f(\overline{\mathbb{F}}_N) = X(\overline{\mathbb{F}}_N)$$

defined by reduction. We then obtain an injection

$$X(\overline{\mathbb{F}}_N) \hookrightarrow X(K) = X(\overline{\mathbb{Q}})^{I_N}.$$

This is bijective if and only if $X_f(K) = X(K)$. □

Theorem 4. *We have an equivalence of categories between quasi-finite separated étale S''-schemes that are finite over $(S'' \cap S')$ and the category whose objects are cuples*

$$(\Sigma, \Sigma_N)$$

with Σ as before a finite discrete $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$-sets that are unramified along $S' \cap S''$ and Σ_N a finite $Gal(\overline{\mathbb{F}_N}/\mathbb{F}_N)$-subsets of Σ^{I_N} fixed subset under the action of the inertia group I_N. The functor is given by

$$Y \mapsto (Y(\overline{\mathbb{Q}}), Y(\overline{\mathbb{F}_N}).$$

Corollary 4.1. *Let G be a finite étale $(S' \cap S'')$ group scheme. Then there exists quasi-finite separated S'' group schemes $G^\flat, G^\sharp$ with restriction G to $(S' \cap S'')$ such that for every quasi-finite G' S'' group scheme, G contains $G^\flat$ as an open subscheme and it is contained in $G^\sharp$ as an open subscheme. That is, $G^\flat$ and $G^\sharp$ are minimal and maximal quasi-finite separated S'' models for G. Moreover, $G^\sharp$ is finite over S'' if and only if $G(\overline{\mathbb{Q}})$ is unramified at N.*

Proof. To make the minimal and maximal model of G we can choose respectively $G^\flat(\overline{\mathbb{F}}_N)$ and $G^\sharp(\overline{\mathbb{F}}_N)$ to be the trivial and the full finite subgroup of $G(\overline{\mathbb{Q}})^{I_N}$. □

3. Admissible groups

3.1. Filtrations.

Def 3. *Let $G_{|S}$ a group scheme as above. Let $H(\overline{\mathbb{Q}})$ be any sub-$Gal(\overline{\mathbb{Q}}/\mathbb{Q})$-module of $G(\overline{\mathbb{Q}})$. We then define H to be the* subgroups scheme *associated to $H(\overline{\mathbb{Q}})$. To understand this group, we consider its restrictions to S' and S''.*

Over S' we consider the scheme-theoretic closure of $H(\overline{\mathbb{Q}})$ in the finite flat group scheme $G_{|S'}$.

Over S'' we consider the group scheme associated to the Galois structure $(H(\overline{\mathbb{Q}}), H(\overline{\mathbb{Q}}) \cap G(\overline{\mathbb{F}_N}))$.

Def 4. *An* admissible p-group *G over S is a separated, quasi-finite flat group scheme such that $G_{|S'}$ is finite flat of order a power of p, such that $G_{|S'}$ posses a filtration by finite flat subgroup schemes such that the successive quotients are S' isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or μ_p, called* admissible filtrations.

From the definition we obtain that closed subgroups and quotiens of admissible groups are again admissible. In particular, we then have the notion of short exact sequence of admissible groups

$$0 \to G_1 \to G_2 \to G_3 \to 0$$

with G_1 closed in G_2 and the morphism $G_2 \to G_3$ induces the isomorphism of $fppf$ sheaves $G_2/G_1 \cong G_3$.

Def 5. *Let G be an admissible p-group. We then define the following numerical invariants attached to G:*

(1) $l(G) = \log_p(order\ G_{|S'})$ called the length *of G;*
(2) $\delta(G) = \log_p(order\ G_{|S'}) - \log_p(order\ G_{|\mathbb{F}_N})$ called the defect *of G;*
(3) $\alpha(G)$ equals to the number of $(\mathbb{Z}/p\mathbb{Z})$'s occuring as successive quotients in the filtration of G;
(4) $h^i = \log_p(order\ H^i_{fppf}(S, G))$ order of the $fppf$ cohomology of G.

3.2. Elementary admissible groups.

Def 6. *We call an admissible group G* elementary *if it has length 1.*

Prop. 3.1. *Up to isomorphism, there are four elementary admissible p-groups over S:*

$$\mathbb{Z}/p\mathbb{Z}, \quad \mathbb{Z}/p\mathbb{Z}^\flat, \quad \mu_p, \quad \mu_p^\flat.$$

Proof. First of all, consider finite flat groups over S' of order p. By Reynauld's theorem we have that the only possibilities are $\mathbb{Z}/p\mathbb{Z}$ or μ_p. To extend this to S, we consider the restriction to $(S' \cap S'')$ and we apply Theorem 4. We then need to specify the structure at the fiber (N). Since $G(\overline{Q}) = \mathbb{Z}/p\mathbb{Z}$ we only have two possibilities, either we extend by 0 or we take the full group. In the first case we obtain $G^\flat$, in the latter we obtain the finite flat groups $\mathbb{Z}/p\mathbb{Z}$ or μ_p. ☐

The numerical invariants of the elementary admissible groups are given by the following table

	$\mathbf{Z/p}$	$\mathbf{Z/p}^\flat$	μ_p	$\mu_p^\flat$
δ	0	1	0	1
α	1	1	0	0
h^0	1	0	$0\ (p \neq 2)$ $1\ (p = 2)$	0
h^1	0	0	$0\ (p \neq 2)$ $1\ (p = 2)$	ε

where ε is given by

$$\varepsilon = \begin{cases} 0 & \text{if } N \not\equiv 1 \mod p \text{ for } p \text{ odd} \\ & \text{or } N \not\equiv 1 \mod 4 \text{ for } p = 2 \\ 1 & \text{otherwise.} \end{cases}$$

Prop. 3.2. *Let $G_{|S}$ be an admissible group, then*

$$h^1(G) - h^0(G) \leq \delta(G) - \alpha(G).$$

Proof. First of all, the right hand side is additive for short exact sequences of admissible groups. Indeed, consider

$$0 \to G_1 \to G_2 \to G_3 \to 0$$

short exact sequence of that type, then the order of G_2 over S' and over $\mathbb{F}_N$ is given by the sum of those of G_1 and G_3. Similar thing happens when we fix a filtration for G_2 and we consider the induced filtrations of G_1 and G_3, the number of $(\mathbb{Z}/p\mathbb{Z})$'s in the filtration of G_2 will correspond to the total number in G_1 and G_3. On the other hand, the difference of the orders of the cohomologies is subadditive. Considering the long exact sequence in the $fppf$ cohomology, will give us

$$h^1(G_2) - h^0(G_2) \leq (h^1(G_1) - h^0(G_1)) + h^1(G_3) - h^0(G_3).$$

We can then conclude by induction on the length, checking that the base case of length one holds by the numerical invariant provided in the table above. ☐

4. Criterion for rank 0

Let N, p be distinct prime numbers.

Theorem 5. *Let $A_{/\mathbb{Q}}$ be an abelian variety with good reduction outside of N and purely toric reduction at N. Let $\mathcal{A}$ be its Néron model and suppose $\mathcal{A}[p]$ is admissible. Then $\mathcal{A}_{/\mathbb{Q}}$ has rank 0.*

Proof. First of all, we replace A by $A \times A^\vee$. Showing that $(A \times A^\vee)(\mathbb{Q})$ has rank 0 will imply that A has rank 0. In this way, we can assume that $\mathcal{A}[p]_{|\mathbb{Z}[1/N]}$ is its own Cartier dual. Let $\mathcal{A}^0$ be the fiberwise identity component of the Néron model $\mathcal{A}$. $\mathcal{A}^0$ is obtained removing the non identity components of the bad fiber over (N). The purely toric reduction hypothesis implies that the multiplication-by-p map $[p] : \mathcal{A}^0 \to \mathcal{A}^0$ is surjective. We then have the following short exact sequence

$$0 \to \mathcal{A}^0[p] \to \mathcal{A}^0 \to \mathcal{A}^0 \to 0.$$

Consider the long exact sequence in the $fppf$ cohomology, obtaining

$$0 \to \mathcal{A}^0(\mathbb{Z})/p\mathcal{A}^0(\mathbb{Z}) \to H^1_{fppf}(\mathbb{Z}, \mathcal{A}^0[p]) \to H^1_{fppf}(\mathbb{Z}, \mathcal{A}^0)[p] \to 0.$$

As before, let $h^i = \log_p(\text{order } H^i_{fppf}(\mathbb{Z}, \mathcal{A}^0[p]))$ be the order of the cohomology group. Since $\mathcal{A}^0(\mathbb{Z})$ is of finite index in $\mathcal{A}(\mathbb{Z}) = \mathcal{A}(\mathbb{Q}) = \mathbb{Z}^\rho \oplus T$, with T torsion group, we deduce

$$\mathcal{A}^0(\mathbb{Z})/p\mathcal{A}^0(\mathbb{Z}) \cong (\mathbb{Z}/p\,\mathbb{Z})^{\rho+h^0}.$$

By the exact sequence in $fppf$ cohomology we then deduce $\rho + h^0 \le h^1$ and then $\rho \le h^1 - h^0$. Using Proposition 3.2 on admissible groups we have

$$\rho \le h^1 - h^0 \le \delta - \alpha.$$

Now $\mathcal{A}^0[p]$ is a torus by hypothesis, then we have $\mathcal{A}^0_{|\mathcal{F}_N}[p]$ has rank p^g with $g = \dim A$ and so $\delta = 2g - g = g$. Using the fact that $\mathcal{A}^0[p]_{|\mathbb{Z}[1/N]}$ is its own Cartier dual, we deduce that the number of $\mathbb{Z}/p\,\mathbb{Z}$'s is equal to the number of μ_p's, that means $\alpha = 2g/2 = g$. We conclude

$$\rho \le h^1 - h^0 \le \delta - \alpha = g - g = 0.$$

□

References

[Con04] Parson J. Conrad, B. Classification of quasi-finite étale separated schemes. https://math.stanford.edu/~conrad/vigregroup/vigre03/zmt.pdf, 2004.

[Gro67] Alexander Grothendieck. éléments de géométrie algébrique : IV. (EGA IV) étude locale des schémas et des morphismes de schémas, Quatrième partie. *Publications Mathématiques de l'IHÉS*, 32:5–361, 1967.

[Maz77] B. Mazur. Modular curves and the eisenstein ideal. *Publications mathématiques de l'IHÉS*, 47(1):33–186, December 1977.

[Par04] J. Parson. Mazur's Eisenstein Descent. https://math.stanford.edu/~conrad/vigregroup/vigre03/eisendescent.pdf, 2004.

[Ray74] M. Raynaud. Schémas en groupes de type $(p, \ldots, p)$. *Bulletin de la Société Mathématique de France*, 102:241–280, 1974.

[Sch00] R. Schoof. Introduction to finite group schemes. https://math.dartmouth.edu/~jvoight/notes/274-Schoof.pdf, 2000.

[Tat70] Oort F. Tate, J. Group schemes of prime order. *Annales scientifiques de l'École Normale Supérieure*, 3(1):1–21, 1970.

[Tat97] J. Tate. *Finite Flat Group Schemes*, pages 121–154. Springer New York, New York, NY, 1997.