On the Nonexistence of Abelian Varieties over $\mathbb{Z}$

Hang Chen

May 30, 2024

Abstract

In this paper, we review the proof of Fontaine's fascinating theorem indicating the nonexistence of abelian schemes over $\mathbb{Z}$ in his paper [4]. The main approach of the proof is to first develop a ramification bound for finite flat p-groups, and then classify all the finite p-groups over $\mathbb{Z}$.

Contents

1 Introduction

The main purpose of this paper is to review Fontaine's proof of the following theorem:

Theorem 1.1 (Fontaine, [4], 3.4.6)**.** *There is no nontrivial abelian scheme over $\mathbb{Z}$. Equivalently, there is no nontrivial abelian variety over $\mathbb{Q}$ with everywhere good reduction.*

This theorem is related in spirit to the classical Minkowski's theorem which states that the only number field that is everywhere unramified is $\mathbb{Q}$. In the context of algebraic geometry, this theorem shows that the only connected 0-dimensional variety over $\mathbb{Q}$ admitting a smooth $\mathbb{Z}$-model is $\operatorname{Spec}\mathbb{Q}$. Then Theorem 1.1 can be viewed as a higher dimensional generalization of this basic nonexistence theorem.

This theorem is an application of Fontaine's theorem as follows.

Theorem 1.2 (Fontaine, [4], 2.1)**.** *Let n be a positive integer, and let Γ be a commutative finite flat group scheme over O_K killed by p^n. Let $G = \mathrm{Ker}(Gal(\bar{K}/K) \to \mathrm{Aut}(\Gamma(\bar{K})))$ and $L = \bar{K}^G$. Then, $u_{L/K} \leq e(n + 1/(p-1))$.*

This theorem develops a ramification bound for finite flat p-group schemes over $\mathbb{Z}_p$, and we can obtain a global version of the ramification bound for finite flat p-group schemes over $\mathbb{Z}$ immediately. With the help of Raynaud's theory and Odlyzko discriminant bound, we can classify the finite flat p-groups over $\mathbb{Z}$ with low ramification. We can apply the classification results to the p-divisible group associated to an abelian scheme over $\mathbb{Z}$ and show the nonexistence of nontrivial abelian scheme over $\mathbb{Z}$. The ramification bound in Theorem 1.2 is sharp. For example, for Katz-Mazur groups, the equality $u_{L/K} = e(n + 1/(p-1))$ holds.

This idea behind considering the bound for the ramification of p-divisible groups over $\mathbb{Q}_p$ is related to Fontaine's theory in p-adic Hodge theory. Later, using the comparison theorem between crystalline cohomology and p-adic étale cohomology, Fontaine applies this method to develop a ramification bound for the crystalline representation $H^m_{\text{ét}}(X_{\bar{\mathbb{Q}}_P}, \mathbb{Q}_p)$ for a proper smooth scheme X over $\mathbb{Z}_p$ and proves the following generalization of Theorem 1.1.

Theorem 1.3 (Fontaine, [5], Theorem 1)**.** *If X is a smooth proper variety over $\mathbb{Q}$ with everywhere good reduction, then $H^i(X, \Omega^j_X) = 0$ for $i \neq j, i + j \leq 3$.*

One thing worth mentioning is that both nonexistence results in Theorem 1.1 and Minkowski's theorem will fail if one replaces $\mathbb{Q}$ with a general number field K since they rely on the fact that the class group of $\mathbb{Q}$ is trivial. In the more general setting where $\mathbb{Q}$ is replaced by any number field K and the existence of good reduction everywhere is weakened to the existence of good reduction outside a set of finite places S, there are finiteness results instead. Also, we can view a basic finiteness theorem in algebraic number theory, the Hermite-Minkowski theorem, as a prototype. It says that given an integer N and a number field K, there are only finitely many number fields L/K such that the discriminant of L/K is smaller than N. Geometrically, this means for a finite set S of primes in K, there are only finitely many isomorphism classes of zero-dimensional varieties of degree at most N over K which have a smooth model over $Spec(O_{K,S})$. In the 1962 ICM conference, Shafarevich suggested several conjectures based on this. Especially, there is one concerning abelian varieties.

Conjecture 1.1. *If K and S are as above and g is a positive integer, then there are only finitely many isomorphism classes of abelian schemes over $O_{K,S}$ of dimension g.*

This conjecture was proven by Faltings when he proved the Mordell conjecture and some other finiteness theorems.

In the next two Chapters, we provide the necessary preliminaries about finite flat group schemes and abelian varieties. In Chapter 4, the proof of Theorem 1.1 is demonstrated.

2 Finite Flat Group Schemes

The details of the first three sections of this chapter can be found in [11].

2.1 Definitions and Examples

Definition 2.1. Let S be a scheme. A group scheme over S is an S-scheme G equipped with S-morphisms $m : G \times_S G \to G$ (multiplication), $e : S \to G$ (identity), and $i : G \to G$ (inverse) such that the usual compatibility relations of groups are satisfied.

From the view of functor of points, the group schemes can be interpreted as the representable contravariant functors $(\mathbf{Sch}/S) \to \mathbf{Grp}$ from the category of schemes over

S to the category of groups. The homomorphisms of group schemes can also be interpreted via this approach.

Definition 2.2. A homomorphism (a group morphism between group schemes) $f : G \to G'$ of S-group schemes is called an isogeny if f is surjective and its kernel $\mathrm{Ker}(f)$ is a flat finite group scheme over S.

Example 2.1.

1. **The additive group** $\mathbb{G}_a$. Let $\mathbb{G}_a = \mathrm{Spec}\, R[t]$. Then, for an R-algebra T, $\mathbb{G}_a(T) = \mathrm{Hom}_{R-alg}(R[t], T) = T$, and the group structure of $\mathbb{G}_a$ is defined by the additive group structure of $\mathbb{G}_a(T) = T$.

2. **The multiplicative group** $\mathbb{G}_m$. Let $\mathbb{G}_m = \mathrm{Spec}\, R[t, t^{-1}]$. Then, for an R-algebra T, $\mathbb{G}_m(T) = \mathrm{Hom}_{R-alg}(R[t, t^{-1}], T) = T^\times$, and the group structure of $\mathbb{G}_m$ is defined by the multiplicative group structure of $\mathbb{G}_m(T) = T^\times$.

3. **Roots of unity**. For an integer $n \geq 2$, let $\mu_n = \mathrm{Spec}\, R[t]/(t^n - 1)$. Then, for an R-algebra T, $\mu_n(T) = \{x \in T^\times \mid x^n = 1\}$, and the group structure of μ_n is defined by the multiplicative group structure of $\mu_n(T)$.

4. **Constant group schemes**. For a finite group Γ, define a finite R-group scheme $\Gamma = \mathrm{Spec} \prod_{i\in\Gamma} R_i$ where R_i is a copy of R. Let e_i be the unit in R_i. The group structure is given by $m^*(e_i) = \sum_{jk=i} e_j \otimes e_k$, $i^*(e_i) = e_{i^{-1}}$, and e^* being the natural projection $\prod_{i\in\Gamma} R_i \to R_1 \simeq R$ where 1 is the unit of Γ.

5. **Diagonalizable group schemes**. For a finite group Γ, define a finite R-group scheme $D(\Gamma) = \mathrm{Spec}\, R[\Gamma]$. Then, for an R-algebra T, $D(\Gamma)(T) = \mathrm{Hom}(\Gamma, T^\times)$. The group structure on the set of group homomorphism $\mathrm{Hom}(\Gamma, T^\times)$ provides the group structure of $D(\Gamma)$. Then $\mu_n = D(\mathbb{Z}/n\mathbb{Z})$.

6. Let G be a group scheme and $[n] : G \to G$ be the map of multiplication by n. Then $[n]$ is an isogeny when $G = \mathbb{G}_m$ (resp. $\mathbb{G}_a$), and $\mathrm{Ker}[n] = \mu_n$ (resp. $\mathbb{Z}/n\mathbb{Z}$).

For the rest of the section, we focus on the properties of finite flat group schemes over an affine base scheme. Let $S = \mathrm{Spec}\, R$ and G be a finite flat S-group scheme. Then, G is an affine scheme $\mathrm{Spec}\, A$, and A is locally free of finite rank as an R-module. An R-algebra A such that $G = \mathrm{Spec}\, A$ is a group scheme is called a Hopf algebra. Of course, one can define the notion of Hopf algebra with total algebra language.

Definition 2.3. The order of G is defined as the rank of A as a R-module and is denoted by $[G : S]$.

Proposition 2.1. *Let $S = \operatorname{Spec} R$ and G be a finite S-group scheme. Let $A^D = \operatorname{Hom}_R(A, R)$ and $G^D = \operatorname{Spec} A^D$. Then the sheaf $G^D : T \mapsto \operatorname{Hom}(G_T, \mathbb{G}_{m,T})$, which is the sheaf associated to the presheaf of characters $T \mapsto \operatorname{Hom}(G(T), O_T^\times)$, is representable by G^D. Thus, G^D is called the Cartier dual of G and A^D is called the dual Hopf algebra of A.*

Actually, the structure of the Hopf algebra of A^D can be defined explicitly with the structure of the Hopf algebra of A, and one can prove the above proposition by checking $G^D(T) = \operatorname{Hom}(G(T), T^\times)$ for any R-algebra T. By the definition of Cartier dual, there is a pairing $G \times G^D \to \mathbb{G}_m$ and a canonical isomorphism $(G^D)^D \simeq G$. The Cartier dual of constant group scheme Γ is the diagonalizable group scheme $D(\Gamma)$. In particular, $(\mathbb{Z}/n\mathbb{Z})^D = \mu_n$.

2.2 Finite Étale Group Schemes

Let G be a finite étale group scheme over a field k. Then A is a finite étale k-algebra. An étale k-algebra is of the form $A = \prod_{i=1}^n k_i$ where k_i is a finite separable extension of k. Thus, A is determined by the action of $\operatorname{Gal}(\bar{k}/k)$ on $G(\bar{k}) = \operatorname{Hom}_{k-alg}(A, \bar{k})$. The inverse map is also clear. This roughly states that the functor {finite étale group schemes over k}$\to$ {finite groups with continuous $\operatorname{Gal}(\bar{k}/k)$-action}: $G \mapsto G(\bar{k})$ defines an equivalence of categories. Moreover, it can be shown that this is an equivalence of categories and that it can also be generalized to the following theorem.

Theorem 2.1. *There is an equivalence of categories: {finite étale R-group schemes} $\xrightarrow{\sim}$ {finite groups with continuous $\pi_{1,\acute{e}t}(S, s)$-action}*

The above equivalence indicates that the category of finite étale R-group schemes is an abelian full subcategory of the category of finite flat R-group schemes.

2.3 Finite Flat Group Schemes

The category of commutative finite flat R-group schemes is generally a pre-abelian category (which is an additive category with kernels and cokernels). A view is that it is a subcategory of the category of sheaves of abelian groups over the fppf (faithfully flat finite presentation) site of $S = \operatorname{Spec} R$. The kernel of a morphism $f : G \to H$ is just the pull-back of G by $e : S \to H$. The existence of cokernel is due to the following theorem of Grothendieck.

Theorem 2.2. *Let H be an S-group scheme and X be a scheme over S. Let $a : X \times_S H \to X$ be a right action of H on S. Suppose H, which is finite flat over S and locally noetherian, acts strictly freely on X, which is of finite type over S, in such a way that every orbit is contained in an affine open set. Then the category of morphisms $X \to Z$ which are constant on orbits has an initial object. In other words, there exists an S-scheme Y and a morphism $u : X \to Y$ which is constant on orbits such that for every morphism $v : X \to Z$ which is constant on orbits, there is a unique morphism $f : Y \to Z$ such that $v = f \circ u$. The morphism $u : X \to Y = X/H$ has the following further properties:*

(1) X is finite flat over X/H and $[X : (X/H)] = [H : S]$.

(2) For every S-scheme T, the map $X(T)/H(T) \to (X/H)(T)$ is injective.

(3) If $S = \operatorname{Spec} R$, $H = \operatorname{Spec} B$ and $X = \operatorname{Spec} A$ are affine, then $X/H = \operatorname{Spec} A_0$, where A_0 is the subring of A where the two homomorphisms $pr_1^*, a^* : A \to A \otimes_R B$ coincide.

Given a closed subgroup scheme H of finite flat S-group scheme G, we have the corresponding free right action $\alpha : G \times_S H \xrightarrow{id \times f} G \times_S G \xrightarrow{m} G$. Then we can apply this theorem, and get a quotient group scheme G/H that is of the desired order $[G : S]/[H : S]$.

A sequence of $0 \to G' \xrightarrow{i} G \xrightarrow{j} G'' \to 1$ of finite R-groups is called exact if i is a closed immersion which identifies G' with the kernel of j and j is faithfully flat. Given the existence of cokernel, this is equivalent to that i is a closed immersion and j is the cokernel of i. The Carier dual of an short exact sequence is still a short exact sequence.

A more ideal picture is that G/H represents the quotient fppf sheaf G/H. If this is true, then the category of commutative finite flat group schemes over S becomes an abelian subcategory of the category of sheaves of abelian groups over the fppf site of S. In general, this is not true. It holds if $\dim R \leq 1$ and R is noetherian ([1]). In particular, we have the following result.

Theorem 2.3. *The category of commutative finite flat group schemes over a field k is an abelian category.*

Now we suppose (R, m) is a henselian local ring (e.g. a field or a complete discrete valuation ring). Let K be the fractional field of R. Let $G = \operatorname{Spec} A$ be a finite flat R-group scheme. There is a canonical exact sequence $0 \to G^0 \to G \to G^{\text{ét}} \to 0$, called the connected-étale sequence for G, where connected G^0 and étale $G^{\text{ét}}$ is defined as follows.

Let $A = \prod A_i$ where A_i is a local ring such that the identity map $e : A \to R$ factors through the projection $A \to A_0$. Let $G^0 = \operatorname{Spec} A_0$. Then it is the connected component of G containing the identity section. Under the condition that R is a henselian local ring, G^0 is also a subgroup of G, and then it is the maximal connected subgroup.

Let $G^{\text{ét}} = G/G^0$. Then $G^{\text{ét}} = \operatorname{Spec} A^{\text{ét}}$ is a finite étale R-group scheme where $A^{\text{ét}}$ is the maximal étale subalgebra of A. $G^{\text{ét}}$ is characterized by the universal property that every group homomorphism $\phi : G \to H$ to a finite étale R-group scheme H factors uniquely through $G \to G^{\text{ét}}$.

The functors $G \mapsto G^0$, $G \mapsto G^{\text{ét}}$ on the category of finite flat R-group schemes are exact. If R is a perfect field, the composition $G^{red} \to G \to G^{\text{ét}}$ is an isomorphism, so the connected-étale sequence splits canonically.

The étale group schemes are discussed in the last section. Now we turn to deal with the finite connected group schemes over a field K.

Theorem 2.4. *Let K be a field of characteristic 0. Then the only connected finite group scheme is the trivial one.*

Proof. Assume $G = \operatorname{Spec} A$ is a connected finite K-group scheme. Let $I = \operatorname{Ker}(A \xrightarrow{e} K)$ be the augmentation ideal. Then $A = K \oplus I$. Let $p : A \to I/I^2$ be the natural projection. If I is nonzero, take $x_1, \cdots, x_n$ as a basis of K-vector space I/I^2 and $f_1, \cdots, f_n$ as the dual basis of the dual space of I/I^2. The invariant differential operator D_i is defined to be the composition $A \xrightarrow{m^*} A \otimes_K A \xrightarrow{id \otimes p} A \otimes_K I/I^2 \xrightarrow{id \otimes f_i} A$. Let ϕ be a map $K[X_1, \cdots, X_n] \to \operatorname{Gr}_I(A) = \oplus_{i=0}^{\infty} I^n/I^{n+1}$ which takes X_i to x_i. Because $\phi \circ \partial/\partial x_i = D_i \circ \phi$, we know the kernel of ϕ is invarient under $\partial/\partial x_i$ and has to be 0. So ϕ is injective which contradicts our assumption that A is a finite K-algebra. □

When k is a field of positive characteristic p, there do exist connected group schemes over k. For example, $\alpha_p = \operatorname{Spec} k[x]/(x^p)$ and $\mu_p = \operatorname{Spec} k[x]/(x^p - 1)$ are connected finite group schemes over k. As k-schemes, α_p and μ_p are isomorphic. But one can see their group structures are different in various ways. One way is to look at the Cartier dual. One can check that $\alpha_p^D = \alpha_p$ is connected and $\mu_p^D = \mathbb{Z}/p\mathbb{Z}$ is étale, so the two are different as group schemes. Another way is to consider the invariant derivations of α_p and μ_p. We view α_p and μ_p are two group structures put on $k[x]/(x^p)$. The invariant derivations of each is a one-dimensional k-vector space generated by a D such that $D(x) = 1 \mod (x)$. But $D^p = 0$ for α_p and $D^p = D$ for μ_p, distinguishing the difference of two group strucatures. Actually, one can prove a height one connected group scheme G over k is uniquely determined by the pair $(\operatorname{Lie} G, \phi)$ where $\operatorname{Lie} G$ is a k-vector space consisting of invariant derivations of G and $\phi : \operatorname{Lie} G \to \operatorname{Lie} G$ is the map $D \mapsto D^p$.

It can also be shown the k-scheme structure of all connected finite K-group schemes are of a similar form when k is perfect. Let $G = \operatorname{Spec} A$ be a connected finite flat group scheme over a perfect field k. Let $G^{(p)} = G \times_{K,\mathrm{Frob}} K$. Then there is a relative Frobenius map $F : G \to G^{(p)}$. Explicitly, if $A = k \oplus I$ where I is the augmentation ideal and $\{x_1, \cdots, x_r\}$ is a lift a basis of I/I^2, then F^* sends x_i to x_i^p, and the kernel of F^* is $A/(x_1^p, \cdots, x_r^p)$. Then $\operatorname{Ker} F$ is a height one group scheme, which means $x^p = 0$ for any $x \in I$. Actually, every height one group scheme is of the form $k[x_1, \cdots, x_r]/(x_1^p, \cdots, x_r^p)$. Let D_i be the invariance differential we defined in the proof of Theorem 2.4. Because of the existence of D_i such that $D_i(x_j) = \delta_{ij} \mod I$, we can easily show that $\prod_i x_i^{\alpha_i}$, $i \leq \alpha_i < p$ have no linear relationship. Because $G/\operatorname{Ker} F$ is of order $[G : S]/p$, we can proceed by induction to show that the order of G is a power of p. Thus, if a finite group scheme G over k of order prime to p, it has to be étale. Furthermore, we have the following classification.

Theorem 2.5. *If k is a perfect field of characteristic $p > 0$, and if $G = \operatorname{Spec} A$ is a connected finite flat k-group scheme, then*

$$A \simeq k[x_1, \cdots, x_r]/(x_1^{p^{e1}}, \cdots, x_r^{p^{e_r}}),$$

for some r, $e_1, \cdots, e_r \in \mathbb{Z}_+$. Also, these are well-defined invariants of G up to permutation of e_i's.

Since étaleness can be checked fiberwise, we conclude with the following theorem.

Theorem 2.6. *If G is a finite flat group scheme over S and the order of G is invertible on S, then G is étale.*

We list some useful properties of finite finite group schemes.

Theorem 2.7. *Let R be a noetherian domain and $p \in R$. Let $\hat{R}$ be the completion of R with respect to the p-adic topology. Then, the functor $G \mapsto (G_{\hat{R}}, G_{R[1/p]}, id_{\hat{R}[1/p]})$ is an equivalence of categories from the category of finite flat group schemes over R to the category of triples (G_1, G_2, ϕ), where G_1, G_2 are finite flat group schemes over $\hat{R}$, $R[1/p]$ respectively, and ϕ is an isomorphism $(G_1)_{\hat{R}[1/p]} \simeq (G_2)_{\hat{R}[1/p]}$.*

Proposition 2.2. *In the category of fppf sheaves over a base scheme S, an extension of a representable sheaf by a representable sheaf is representable.*

Thus, $Ext^1_S(G,H)_{fppf}$ for two finite flat S-group schemes G and H really parametrizes extensions of G by H as finite flat S-group schemes.

We now introduce Raynaud's theorem and a sketchy proof of it, and talk about some results that can be deduced from it. Raynaud's theorem tells that if $K/\mathbb{Q}_p$ is a finite field extension of a small ramification index, then every commutative finite flat p-group over O_K is determined by its general fibre. In other words, a commutative finite flat O_K-group scheme is determined by the Galois action associated to its generic fibre in this case. This offers us a very powerful tool to classify commutative finite flat O_K-group schemes, which plays an essential role in the proof of Theorem 1.1. The reference of the details is Raynaud's paper [9].

Theorem 2.8 (Raynaud, [9], 3.3.3)**.** *Let R be a discrete valuation ring of mixed characteristic $(0,p)$, and let F be its field of fractions. Let $\pi \in R$ be a uniformizer and k be the residue field of R. Let V be the normalized valuation on R such that $v(\pi) = 1$, and let $e = v(p)$ be the absolute ramification index.*

A prolongation of a finite group scheme Γ_0/K is a finite flat group scheme Γ/R equipped with an isomorphism $\Gamma_K \to \Gamma_0$. Suppose $e \leq p-1$. Let Γ_0 be a commutative finite flat group scheme over K of p-power order. Then any two prolongations of Γ_0 to R are isomorphic.

Proof. (Sketchy) The proof of Raynaud's theorem is split into three steps.

Step 1: to show that we only have to prove that the result holds for simple group scheme Γ_0 over K^{un}. Because of the faithfully flat descent, we can verify the desired properties by taking a base change to K^{un}. Thus, we suppose $K = K^{un}$ in the rest of the proof.

We need to show that if there is a short exact sequence $1 \to \Gamma_0' \to \Gamma_0 \to \Gamma_0'' \to 1$ and Γ_0' and Γ_0'' have at most one prolongation, then Γ_0 has at most one prolongation. Assume that Γ_0 admits a prolongation Γ. We denote the closure of Γ_0' in Γ by Γ', and then it is a prolongation of Γ_0'. We denote the quotient scheme Γ/Γ' by Γ''. One essential observation is that Γ_0 has maximal and minimal prolongations. If $\Gamma_1 \subset \Gamma_2$ are two prolongations of Γ_0, then by assumption that Γ_0' and Γ_0'' have at most one prolongation, we get $\Gamma_1' = \Gamma_2'$ and $\Gamma_1'' = \Gamma_2''$. So it is clear $\Gamma_1 = \Gamma_2$ and therefore Γ_0 has at most one prolongation.

Step 2: Suppose $K = K^{un}$. We classify all the prolongation of a simple commutative finite flat group scheme over K killed by (a power of) p (without restrictions on e).

First, we show all simple K-group schemes killed by (a power of) p are so-called Raynaud $\mathbb{F}$-module schemes.

Definition 2.4. Let $\mathbb{F}$ be a finite field of characteristic p. An $\mathbb{F}$-module scheme (over R or K) is a commutative group scheme Γ equipped with a ring homomorphism $\mathbb{F} \to \mathrm{End}(\Gamma)$. If $\Gamma = \operatorname{Spec} A$, we write $[t] : A \to A$ for the corresponding $\mathbb{F}$-action on A.

A Raynaud $\mathbb{F}$-module scheme is a finite flat $\mathbb{F}$-module scheme of the same order as $\mathbb{F}$.

Let Γ_0 be a simple K-group scheme killed by a power of p. Let $G_K = \mathrm{Gal}(\bar{K}/K)$. Because Γ_0 is simple, Γ_0 is killed by p and $V = \Gamma_0(\bar{K})$ is a simple $\mathbb{F}_p[G_K]$-module. Let $\mathbb{F}$ be the centralizer of G_K in $\mathrm{End}(V)$. Then $\mathbb{F}$ is a finite extension of $\mathbb{F}_p$, and V is an irreducible $\mathbb{F}$-linear representation of G_K. We now show V is 1-dimensional $\mathbb{F}$-vector space. Because $K = K^{ur}$, G_K is an extension of tame part I^t by wild part I^w. Since I^w is a normal pro-p subgroup of G_K, the fixed subspace V^{I^w} is not zero-dimensional and is invariant under G_K-action, which has to be V itself as V is an irreducible representation of G_K. In other words, I^w acts trivially on V. Then V is an irreducible representation of abelian group I^t, so it has to be 1-dimensional. Hence, we have shown G_0 is canonically a Raynaud $\mathbb{F}$-module scheme for a finite field extension $\mathbb{F}/\mathbb{F}_p$.

We now explain the approach to classifying all the Raynaud $\mathbb{F}$-module schemes admitting a prolongation. Let $\#\mathbb{F} = q = p^r$. Assume a Raynaud $\mathbb{F}$-module scheme $\Gamma_0 = \operatorname{Spec} A_0$ adimits a prolongation $\Gamma = \operatorname{Spec} A$. Because $\Gamma_0(\bar{K})$ is identified with $\mathbb{F}$ on which $\mathbb{F}^\times$ acts by scalar multiplication, $(A_0)_{\bar{K}}$ is isomorphic to the algebra of functions $\mathbb{F} \to \bar{K}$. One can also write down the structure of Hopf algebra of $(A_0)_{\bar{K}}$ and the action of $\mathbb{F}^\times$ on $(A_0)_{\bar{K}}$

explicitly. The augmentation ideal $(I_0)_{\bar{K}}$ is identified with $\{f : \mathbb{F} \to \bar{K} \mid f(0) = 0\}$. If $\chi : \mathbb{F}^\times \to \bar{K}^\times$ is a character, we define a function $\epsilon_\chi : \mathbb{F} \to K$ such that $\epsilon_\chi(0) = 0$ and $\epsilon_\chi|_{\mathbb{F}^\times} = \chi$. Then all the ϵ_χ form a $\mathbb{F}$-basis of $I_{\bar{K}}$ on which the $\mathbb{F}^\times$-action is $[t]\epsilon_\chi = \chi(t)\epsilon_\chi$.

We view A as a R-lattice in $(A_0)_{\bar{K}} = A \otimes_R \bar{K}$ with the structure of Hopf algebra inherited from A_0. Because $R^\times$ contains μ_{q-1}, the group of $(q-1)$st roots of unity, the image of any character χ is contained in $R^\times$ and χ factors through $\chi : \mathbb{F}^\times \to R^\times$. Thus, $I = \bigoplus_\chi I_\chi$ where $I_\chi = \epsilon_\chi \cdot \bar{K} \supset I$ being the subspace of I where $\mathbb{F}^\times$ acts via the character χ.

Choose a character $\chi_0 : \mathbb{F}^\times \to R^\times$ such that the composition $\chi_0 : \mathbb{F}^\times \to R^\times \to k^\times$ can extend to a field homomorphism. Such a character is called a fundamental character by Raynaud. Other fundamental characters are $\chi_i = \chi_0^{p^i}$, $i = 0, \cdots, r-1$, and all characters can expressed as $\prod_i \chi_i^{j_i}, j_i = 0, \cdots, p-1$. Take a R-generator $X_i = c_i \epsilon_{\chi_i}$ in each I_{χ_i}. Let $\delta_i \in R$ such that $X_i^p = \delta_i X_{i+1}$. Then $\delta_i = c_i^p / c_{i+1}$.

Considering the structure of Hopf algebra the Cartier dual of Γ, it can be shown that A is generated by X_i as an R-algebra and $0 \leq v(\delta_i) \leq e$. Clearly, (δ_i) decides Γ because one can solve (c_i) up to roots of unity, and (δ_i) also provides Γ with a unique structure of Raynaud $\mathbb{F}$-module scheme. We conclude the following theorem.

Theorem 2.9 ([9], 1.5.1)**.** *If $\Gamma = \operatorname{Spec} A$ is a prolongation of Γ_0, then A is isomorphic to the quotient of $R[X_1, \cdots, X_n]$ by equations $X_i^p = \delta_i X_{i+1}$, where δ_i is an element of R of valuation at most e. Conversely, if A is of this form, then there is a unique structure of a Raynaud F-module scheme on $\Gamma = \operatorname{Spec}(A)$ such that $[t]X_i = \chi_i(t)X_i$ for all $t \in \mathbb{F}^\times$.*

Step 3: to check that a simple group scheme $\Gamma_0 = \operatorname{Spec} A_0$ over K^{ur} adimitting at most one prolongation when $e < p-1$. As shown in step 1, we only have to show that if $\Gamma_1 \supset \Gamma_2$ are two prolongations of Γ, then $\Gamma_1 = \Gamma_2$. Suppose that $\Gamma_1 \supset \Gamma_2$ are two prolongations of Γ. Let $\Gamma_1 = \operatorname{Spec} A_1$ and $\Gamma_2 = \operatorname{Spec} A_2$. Then $A_1 \subset A_2$ as two R-lattices in A_0. As in step 2, we choose $X_0, \cdots, X_{r-1} \in A_1$ and $Y_0, \cdots, Y_{r-1} \in A_2$. Let $X_i^p = \delta_i X_{i+1}$, $Y_i^p = \lambda_i Y_{i+1}$, and $Y_i = \alpha_i X_i$. Then we derive by these relationship that $\lambda_i = \alpha_i^p \delta_i \alpha_{i+1}^{-1}$ for all i. If there exists a α_i such that $v(\alpha_i) > 0$, we choose i_0 such that $v(\alpha_{i_0})$ is maximal, and then it is easy to see $v(\lambda_{i_0}) \geq (p-1)v(\alpha_{i_0}) \geq p-1$. But we have $v(\lambda_{i_0}) \leq e < p-1$. which leads to a contradiction. Thus, $v(\alpha_i) = 0$ for all i and then $A_1 = A_2$. □

Remark 2.1 ([9], 3.4)**.** Let Γ be a simple Raynaud $\mathbb{F}$-module scheme over R, where R is a strictly henselian ring. Let K, π, v be the same as in the proof. It is shown that all information of Γ can be derived from (δ_i) and we make it clear in this remark.

It is natural to ask how to tell the Galois action on $\Gamma(\bar{K})$ from (δ_i). Also, according to Raynaud's theorem, it is expected that, when $e < p-1$, we can tell whether a prolongation exists directly from the Galois action and write down (δ_i) if the prolongation does exist.

In the following, we identify $\Gamma(\bar{K})$ with $\mathbb{F}$. Let $\psi_i : \mu_{q-1}(K) \to \mathbb{F}^\times$ be the inverse of χ_i. Let $L = K(\pi^{1/(q-1)})$. By Kummer theory, any group homomorphism $G_K \to \mathbb{F}^\times$ factors through a natural projection $j_q : I^t \to \mathrm{Gal}(L/K) \simeq \mu_{q-1}(K)$. Assume the Galois action on $\Gamma(\bar{K}) = \mathbb{F}$ is given by $\psi \circ j_q$, where $\psi : \mu_{q-1}(K) \to \mathbb{F}^\times$ is a homomorphism. We can deduce from $X_i^p = \sigma_i X_{i+1}$ for all i that, $X_0^q = a_0 X_0$ where $a_0 = \delta_0^{p^{r-1}} \delta_1^{p^{r-2}} \cdots \delta_{r-1}$. Thus, for any $x \in \mathbb{F}$, $X_0(x)^q = a_0 X_0(x)$. Then we get $\sigma(X_0(x)) = j_q(\sigma)^{v(a_0)} X_0(x)$ for any $\sigma \in G_K$. Since $\sigma(X_0(x)) = X_0(\sigma x) = X_0(\psi \circ j_q(\sigma)(x)) = [\psi \circ j_q(\sigma)] X_0(x) = \chi_0(\psi \circ j_q(\sigma)) X_0(x)$, we obtain $j_q(\sigma)^{v(a_0)} = \chi_0(\psi \circ j_q(\sigma))$. Thus, $\psi = \psi_0^{v(a_0)} = \psi_0^{p^{r-1}v(\delta_0)+p^{r-2}v(\delta_1)+\cdots+v(\delta_{r-1})}$. Because ψ_i is the inverse of χ_i, we get $\psi^p = \psi_{i_1}$. Therefore, $\psi = \psi_1^{v(\delta_0)} \psi_2^{v(\delta_1)} \cdots \psi_0^{v(\delta_{r-1})}$.

Moreover, it is easy show that a $\mathbb{F}$-module scheme over K has a prolongation if and only if the Galois group G_K acts on $\Gamma(\bar{K})$ by $\psi \circ j_q$ where $\psi = \prod_{i=0}^{r-1} \psi_i^{n_i}$ with $0 \leq n_i \leq e$. To ensure Γ is simple, $(n_0, \cdots, n_{r-1})$ as a function from $\mathbb{Z}/r\mathbb{Z} \to \mathbb{Z}$ should has period exactly r.

Remark 2.2 ([9], 3.3.6)**.** Let K be a finite extension of $\mathbb{Q}_p$ such that the absolute ramification $e = 1$. One can also deduce from this theorem that any object in the category admits a well-defined Jordan-Holder composition series.

We claim that Raynaud's theorem implies that $\Gamma \mapsto \Gamma_K$ is a fully faithful functor. In fact, $H \mapsto H_K$ induces a bijection between the set of closed subgroup schemes of Γ and the set of closed subgroup schemes of Γ_K. It is injective because of Raynaud's theorem. The inverse map is given by taking the schematic closure in Γ. Using Cartier duality, we get that $H \mapsto H_K$ induces a bijection between the set of quotient group schemes of Γ and the set of quotient group schemes of Γ_K. Thus, we can show that if Γ_1 and Γ_2 are two group schemes, every $u : \Gamma_{1,K} \to \Gamma_{2,K}$ can extend uniquely to $\Gamma_1 \to \Gamma_2$. Especially, for a $u : \Gamma_1 \to \Gamma_2$, $\mathrm{Coker}(\mathrm{Ker}(u)) \to \mathrm{Ker}(\mathrm{Coker}(u))$ is an isomorphism, and then the category of finite flat group schemes over R is an abelian category.

From the discussion above, we see a Jordan-Holder composition series for Γ_K induces a Jordan-Holder composition series for Γ.

Corollary 2.1 ([4], 3.2.1)**.** *Let Γ be a commutative finite flat $W = W(\bar{k})$-group scheme killed by p, and let $K = W[1/p]$, $L = K(\Gamma(\bar{K}))$. Suppose that Γ contains a subgroup isomorphic to μ_p. Then L satisfies one of the following:*

(1) L/K is cyclic of degree $p-1$, and there exist integers r, s such that $\Gamma \cong (\mathbb{Z}/p\mathbb{Z})^r \oplus \mu_p^s$.

(2) $[L : K] = p(p-1)$, and there exist integers r, s such that $0 \to \mu_p^s \to \Gamma \to (\mathbb{Z}/p\mathbb{Z})^r \to 0$ is a nontrivial extension.

(3) L/K is cyclic of degree $p^2 - 1$.

(4) $[L : K] \geq p^2(p-1)$.

Proof. Assume first that Γ is a simple commutative finite flat group scheme over W. Then from the proof of Theorem 2.8, G is a Raynaud $\mathbb{F}$-module scheme for a finite extension $\mathbb{F}/\mathbb{F}_p$. Let G_K, p_j, ψ_i be as in Remark 2.1.

We know from Remark 2.1 that G_K-action on $\Gamma(\bar{K}) = \mathbb{F}$ is given by $\psi \circ j_q$ where $\psi = \prod_{i=0}^{r-1} \psi_i^{n_i}$ such that $n_i \in \{0, 1\}$ and $\mathbb{Z}/r\mathbb{Z} \to \mathbb{Z} : i \mapsto (n_i)$ is of period exact r. Let $L = K(\Gamma(\bar{K}))$ and $L' = LK(\zeta_p)$. Then $[L : K] = d$ which is the order of ψ and also the minimal number such that $p^r - 1 | d(\sum_{i=0}^{r-1} p^i n_i)$. Thus, $[L' : K] = d'$ which is the minimal multiple of $p-1$ such that $p^r - 1 | d(\sum_{i=0}^{r-1} p^i n_i)$. By definition, $d, d' | p^r - 1$. Also note that, since $\operatorname{Ker} j_q$ is cyclic and $\bar{K}^{\operatorname{Ker} j_q} = K(\pi^{1/(q-1)})$ is linear indepent to $K(\zeta_p)$, L and L' is decided by d, d' respectively. The whole reason to introduce L' is that d' is easier to estimate for some technical cause we will see soon, which is also why we assume Γ contains a subgroup μ_p in the statement of the corollary.

We claim that, if $r > 2$, then $d' > p^2(p-1)$. In fact, because $i \mapsto n_i$ is of period exact r, there is consecutive $i, i+1$ such that $n_i = n_{i+1}$. We may assume $i = r-2$. If $n_{r-2} = n_{i-1} = 0$, $p^r - 1 \leq d'(\sum_{i=0}^{r-1} p^i n_i) = d'(\sum_{i=0}^{r-3} p^i n_i) \leq d'(p^{r-2} - 1)/(p-1)$, Then $d' \geq (p^r - 1)(p-1)/(p^{r-2} - 1) > p^2(p-1)$. If $n_{r-2} = n_{i-1} = 1$, $d'(\sum_{i=0}^{r-1} p^i(1 - n_i)) = d'(p^r - 1)/(p-1) - d'(\sum_{i=0}^{r-1} p^i n_i)$ is still a multiple of $p^r - 1$ since $p - 1 | d'$. Thus, we can also obtain $d' > p^2(p-1)$.

In general, we consider a Jordan-Holder composition series of Γ and let $\Gamma_1, \cdots, \Gamma_m$ be the Jordan-Holder factors. Let $L_i = K(\Gamma_i(\bar{K}))$, $L_i' = L_i K(\zeta_p)$, $a_i = [L_i' : K]$, and r_i be the r for Γ_i. The discussion above shows that if $[L : K] < p^2(p-1)$, then $r_i \leq 2$ and $p-1 \mid a_i \mid p^2-1$. So, $a_i = p-1$ or p^2-1. Also, L_i' has a unique option of a cyclic extension of K for every possibility of a_i. Thus, If Γ is semi-simple (which means it is a direct sum of Jordan-Holder factors), we have already proved that L/K is cyclic of degree $p-1$ or p^2-1.

If $[L : K] = p-1$, then every r_i must be 0 or 1. Based on the classification result in the proof of Theorem 2.8, r_i uniquely decides Γ_i when $i \leq 2$. We have $\Gamma_i = \mathbb{Z}/p\mathbb{Z}$ if $r_i = 0$ and $\Gamma_i = \mu_p$ if $r_i = 1$. Therefore, Γ is a direct sum of $(\mathbb{Z}/p\mathbb{Z})^r$ and $(\mu_p)^s$ for some r, s.

If Γ is not semi-simple, M is not a semi-simple $\mathbb{F}_p[G_K]$-module, and then $[L : K]$ can not be tamely ramified. Thus, $p|[L : K]$. If we moreover ask $[L : K] \leq p^2(p-1)$, then every r_i must be 0 or 1. Because any extension of μ_p (resp. μ_p, $\mathbb{Z}/p\mathbb{Z}$) by $\mathbb{Z}/p\mathbb{Z}$ (resp. $\mathbb{Z}/p\mathbb{Z}$, μ_p) killed by p is trivial, Γ must be an extension of $(\mathbb{Z}/p\mathbb{Z})^r$ by $(\mu_p)^s$. Then $[L : K] = p^u(p-1)$ by calculation and it is only possible to be $p(p-1)$, which finishes our proof. □

There is another theorem of Raynaud we need for our proof of Theorem 1.1, and we cite it here:

Theorem 2.10 (Raynaud, [2], 3.1.1)**.** *Let G be a commutative finite flat group scheme over any base S. For every $x \in S$, there is an open neighborhood $U \subset S$ such that there is a closed U-immersion of G_U into some abelian scheme A_U over U.*

2.4 p-divisible Groups

p-divisible groups show up naturally in the study of abelian varieties and are involved in the proof of Theorem 1.1. We introduce the definition and some basic properties of p-divisible groups in this section. For more details, one can see [10].

Definition 2.5. Let p be a prime number, and h be a non-negative integer. A p-divisible group G over R of height h is an inductive system $(G_n; i_n : G_n \to G_{n+1})_{n \in \mathbb{Z}_{\geq 0}}$ such that

(1) G_n is a finite group scheme over R of order p^{nh},

(2) for every n, $0 \to G_n \xrightarrow{i_n} G_{n+1} \xrightarrow{[p^n]} G_{n+1}$ (i.e. i_n identifies G_n with $G_n[p^n]$).

Remark 2.3. In the mind, a p-divisible group G can be thought as $G = \varinjlim G_i$ with respect to the inductive system. In contrast, the Tate module associated to a p-divisible group G over k is the projective limit $T(G) = \varprojlim G_(\bar{k})$ with respect to the map $[p] : G_{n+1} \to G_n$. When G is a system of étale group schemes over k, it is decided by $T(G)$.

Example 2.2. (1) The constant group is $\mathbb{Q}_p/\mathbb{Z}_p = (\mathbb{Z}/p^n\mathbb{Z})_n$.

(2) The diagonalizable group is $\mu_{p^\infty} = (\mu_{p^n})_n$.

(3) Let A be an abelian scheme over S of dimension g. Then $A(p) := (A[p^n])_n$ is a p-divisible group of height $2g$, which is both a rich example of p-divisible groups and an important tool to study abelian varieties.

If $G = (G_n, i_n)$ is a p-divisible group over R, then $G^0 := (G_n^0, i_n)$ and $G^{\text{ét}} := (G_n^{\text{ét}}, i_n)$ still form p-divisible groups over R. Also, $G \mapsto G^{\text{ét}}$ and $G \mapsto G^0$ are exact, and we have a connected-étale sequence $0 \to G^0 \to G \to G^{\text{ét}} \to 0$ for a p-divisible group G. The Cartier dual G^D of G can also defined as $G^D = (G_n^D)_n$.

Definition 2.6. Let R be a complete noetherian local ring with residue field k of Characteristic $p > 0$. An n-dimensional commutative formal Lie group Γ over R is a homomorphism $m : A \to A \widehat{\otimes}_R A$, where $A = R[[x_1, \cdots, x_n]]$ and $\widehat{\otimes}$ is the completed tensor product with respect to the obvious adic topology, which is the ring of formal power series in $2n$ variables Y_i, Z_j. Then the homomorphism m can be described by $f(Y, Z) = (f_i(Y, Z))$ where f_i is the image of X_i.

The following axioms are satisfied:

1. $X = f(X, 0) = f(0, X)$.

2. $f(X, f(Y, Z)) = f(f(X, Y), Z)$.

3. $f(X, Y) = f(Y, X)$.

We write $X * Y = f(X, Y)$. Let $\psi : A \to A$ defined by $\psi(X) = X * \cdots * X$ (p times) corresponding to the multiplication by p in Γ. Γ is said to be divisible if $p : \Gamma \to \Gamma$ is an isogeny, which means ψ makes A a finite free module over itself. In this case, as in

Example 2.2, we can construct a p-divisible group $\Gamma(p) = (\Gamma_{p^n})$ of height h over R, where p^h is the degree of the isogeny $p : \Gamma \to \Gamma$.

Proposition 2.3. *Let R be a complete noetherian local ring with residue field k of Characteristic $p > 0$. Then $\Gamma \to \Gamma(p)$ is an equivalence between the category of divisible commutative formal Lie groups over R and the category of connected p-divisible groups over R.*

Let $G = (G_n)$ be a p-divisible group over R, and let $G_n = \operatorname{Spec} A_n$. Then the associated formal group is $A = \varprojlim A_n$. It can be shown that A is a isomorphic to $R[[X_1, \cdots, X_r]]$. The group law $m : A \to A \widehat{\otimes} A$ is given by the group laws of A_n. The dimension of G is defined as r.

Proposition 2.4. *Let n and n' be the dimension of a p-divisible group G and its dual G'. Then $n + n' = h$, the height of G and G'*

Thus, if an abelian scheme A over R has a dual abelian $\hat{A}$. Then $A(p)^D = \hat{A}(p)$. Because A and $\hat{A}$ are isogenous, both $A(p)$ and $\hat{A}$ have height $2n$ and dimension n.

Theorem 2.11 (Mordell-Weil)**.** *If A is an abelian variety over a number field K, $A(K)$ is a finitely generated group.*

3 Abelian Schemes

3.1 Definitions

Definition 3.1. An abelian variety A over a field k is a complete algebraic variety over k which is a group scheme.

It can be proven that an abelian variety is projective, everywhere non-singular, and commutative as a group scheme. (See [7], §4).

Similarly, we have the definition of abelian scheme.

Definition 3.2. An abelian scheme over a scheme S is a smooth proper group scheme with connected geometric fibers.

But unlike the case of abelian varieties, an abelian scheme over S does not need to be projective.

Proposition 3.1. *([8], XI.1.4.) Let A be an abelian scheme over S. Then A is projective over S if S is normal.*

Proposition 3.2. *Let A be an abelian scheme over S of relative dimension g. Let $[n]$ denote the multiplication by n, then $\deg[n] = n^{2g}$.*

Therefore, the kernel of $[N]$, denoted by $A[N]$, is a finite group scheme over S of degree N^2. If N is invertible on S, then $A[N]$ is an étale group scheme over S. Moreover, if $S = \operatorname{Spec} \bar{k}$ where k is a field such that char k is coprime to N, $A[N]$ is a constant group variety of degree N^{2g}. In this case, varying N, it is easy to see $A[N] \simeq (\mathbb{Z}/N\mathbb{Z})^{2g}$.

If N is not invertible on S, $A[N]$ is far away from an étale scheme over S. However, we can still apply our theory of commutative finite flat group schemes to $A[N]$. If we take $N = p^n$ and vary n, then we get a p-divisible group $A(p) = (A[p^n])$ called the associated p-divisible group of the abelian variety A, the height of which is $2g$.

3.2 Dual Abelian Schemes

Let X be a scheme over S. The relative Picard functor $\mathrm{Pic}_{X/S} : \mathbf{Sch}/S \to \mathbf{Grp}$ is defined to be the fppf sheaf associated to $P_{X/S}(T) = \mathrm{Pic}(X \times_S T)$. Assume that $f : X \to S$ is quasi-compact and quasi-separated and f satisfies $f_*(O_X) = O_S$, then $\mathrm{Pic}_{X/S}(T) = Pic(X \times_S T)/Pic(T)$ ([3], 8.4). If further $f : X \to S$ has a section e, then

$$\mathrm{Pic}_{X/S}(T) = \{(L, \alpha) \mid L \in \mathrm{Pic}(X_T), \alpha : e^*L \simeq O_T\}.$$

Let $\mathrm{Pic}^0_{X/S}$ be the identity component of $\mathrm{Pic}_{X/S}$.

Theorem 3.1 ([3], 8.5)**.** *Let A be a projective abelian S-scheme.*

(1) Then $\mathrm{Pic}^0_{X/S}$ is representable by a projective abelian S-scheme. It is denoted by $\hat{A}$ and is called the dual abelian scheme of A, and the universal line bundle on $A \times_S \hat{A}$ called the Poincare bundle.

(2) The Poincare bundle on $A \times_S \hat{A}$ gives rise to a canonical isomorphism $A \simeq \hat{\hat{A}}$ where $\hat{\hat{A}}$ is the dual abelian scheme of $\hat{A}$.

Clearly, a morphism $f : X \to Y$ between two abelian schemes over S induces a morphism $f^* : \mathrm{Pic}^0_{Y/S} \to \mathrm{Pic}^0_{X/S}$ by pulling back line bundles along f. If f is an isogeny, then $Y = X/K$ where $K = \operatorname{Ker} f$. Let K' be the kernel of f^*. By definition,

$$\begin{aligned} K'(T) &= \operatorname{Ker}\{(\text{line bundles on } T \times_S Y) \to (\text{line bundles on } T \times_S X)\} \\ &= \{\text{liftings of the action of } K \text{ on } T \times_S X \text{ to actions on } T \times_S X \times \mathbb{A}^1\} \\ &= \operatorname{Hom}_T(K, \mathbb{G}_m) = K^D(T). \end{aligned}$$

Thus, K' is canonically isomorphism to the Cartier dual of K. One can prove that $[n]_A^* = [n]_{\hat{A}}$. Therefore, there is a natural isomorphism $\hat{X}[n] \simeq X[n]^D$.

3.3 Néron Models

Definition 3.3. Let A be an abelian variety over K where K is either a global field or a local field of mixed characteristic.

(1) If K is a local field or a global field, A is called to have a good reduction if there exists an abelian scheme X over O_K such that $X_K = A$.

(2) If K is a global field, A is called to have a good reduction at a prime $\mathfrak{p} \subset O_K$ if there exists an abelian scheme X over $O_{K,\mathfrak{p}}$ such that $X_K = A$.

Definition 3.4. Let R be a Dedekind domain and $K = \operatorname{Frac}(R)$. For a smooth separated finite type K-scheme X, a Néron model of X is a smooth separated finite type R-scheme Y such that $Y_K = X$ and satisfies the Néron mapping property: for each smooth R-scheme Z and each K-morphisms $u_K : Z_K \to Y_K = X$, there is a unique R-morphism $u : Z \to Y$ extending u_K.

Proposition 3.3 ([3], 1.2)**.** *Let R be a Dedekind domain and $K = \operatorname{Frac}(R)$. Let Y be a smooth separated finite type K-scheme. The following are some properties of Néron Models.*

(1) A Néron model can be checked at closed points. Namely, an R-scheme X is a Néron model of its generic fiber if, for all closed points $s \in \operatorname{Spec} R$, an R_s-scheme X_s is a Néron model of its generic fiber.

(2) If the generic fiber has a group structure, it extends uniquely to a group structure of a Néron model.

(3) An abelian scheme is a Néron model of its generic fiber.

A nontrivial theorem indicates that every abelian variety over K admits a Néron model.

Theorem 3.2. *Let R be a Dedekind domain and $K = \mathrm{Frac}(R)$. For an abelian variety A over K, A admits a Néron model over R, which is quasi-projective over R.*

Thus, an abelian variety has a good reduction if its Néron model is an abelian scheme. We also know from the theory of Néron model that the two statements in Theorem 1.1 are really equivalent.

4 The Proof of Theorem 1.1

4.1 Notations and Fontaine's Property (Pm)

We fix the following notation in this section. Let p be a prime number, and let K be a finite extension of $\mathbb{Q}_p$. Choose π_K to be a uniformizer of K. The valuation v on K is normalised such that $v(\pi_K) = 1$. It can extend uniquely to each finite extension of K. Let k be the residue field of O_K and e be the absolute ramification index of K. If L/K is a finite extension, let $e_{L/K}$ be the ramification index of L/K and let $D_{L/K}$ be the different of L/K.

Choose x to be an O_K-generator of O_L. For $\sigma \in G = \mathrm{Gal}(L/K)$, we define $i_{L/K}(\sigma) = v(\sigma(x) - x)$. The piecewise linear continuous increasing function $\phi_{L/K} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is defined by $\phi_{L/K}(i) = \sum_{\sigma \in G} \min(i, i_{L/K})$. Define $u_{L/K}(\sigma) = \phi_{L/K}(i_{L/K}(\sigma))$. Let

$$i_{L/K} = \sup_{\sigma \in G \setminus \{1\}} i_{L/K}(\sigma), \quad u_{L/K} = \sup_{\sigma \in G \setminus \{1\}} u_{L/K}(\sigma).$$

Proposition 4.1. $v(D_{L/K}) = u_{L/K} - i_{L/K}$.

Proof. Let $f \in O_K[x]$ be the minimal polynomial of x over K. Then $f(t) = \prod_{\sigma \in G}(t - \sigma x)$ and $f'(x) = \prod_{\sigma \in G \setminus \{1\}}(x - \sigma x)$. Thus,

$$\begin{aligned} v(D_{L/K}) =& v(f'(x)) = \sum_{\sigma \in G \setminus \{1\}} v(x - \sigma x) = \sum_{\sigma \in G \setminus \{1\}} i_{L/K}(\sigma) \\ &= \sum_{\sigma \in G} \min\{i_{L/K}, i_{L/K}(g)\} - i_{L/K} = \phi_{L/K}(i_{L/K}) - i_{L/K} = u_{L/K} - i_{L/K} \end{aligned}$$

□

Proposition 4.2. *Let x, f be as above, and let y be an element of L. Let $i = \sup_{\sigma\in G} v(y-\sigma x)$ and $u = v(f(y))$. Then $u = \phi_{L/K}(i)$.*

Proof. Replace x with a conjugate such that $v(y-x) = i$. Then we have

$$v(y-\sigma x) = v((y-x)+(x-\sigma)) = \min\{v(y-x), v(x-\sigma x)\} = \min\{i, i_{L/K}(\sigma)\}$$

for a $\sigma \in G$. Thus,

$$u = v(f(y)) = v(\prod(y-\sigma x)) = \sum v(y-\sigma x) = \sum \min\{i, i_{L/K}(\sigma)\} = \phi_{L/K}(i).$$

□

The following proposition serves as a main method to bound the ramification in Fontaine's proof of Theorem 1.1, 1.3. We present a refined version proved in [12] here, which will simplify some of the proof of Theorem 1.2.

Proposition 4.3 (Converse to Krasner's Lemma, [4], 1.5, [12], 3.4)**.** *For any finite Galois extension E/K and a positive real number t, denote $m_E^t = \{x \in O_E \mid v(x) \geq t\}$. Consider the property (P_m): For all finite extension E/K, if there exists an O_K-algebra homomorphism from O_L to O_E/m_E^m, then there exists K-algebra homomorphism from L to E.*

Define $m_{L/K} = \inf\{m \mid P_n$ holds for all $n \geq m\}$. Then, $m_{L/K} = u_{L/K}$.

Note that the definition of m_E^n is different from our usual definition. Actually, m_E^t is the usual $m_E^{[te_{E/K}]}$.

Proof. (1) First we prove $m_{L/K} \leq u_{L/K}$. Let n be any real number larger that $u_{L/K}$. Choose an O_K-generator x of O_L and let f be its minimal polynomial. Choose a lift $y \in O_E$ of $\bar{y} = s(x) \in O_E/m_E^n$. We embed E and L in $\bar{K}$. We have $u = v(f(y)) \geq n \geq u_{L/K}$. By Proposition 4.1, $i = \sup_{\sigma\in G} v(y-\sigma x) = \phi_{L/K}^{-1}(u) \geq \phi_{L/K}^{-1}(u_{L/K}) = i_{L/K}$. Assume $v(y-x) = i$. Then, $v(y-x) > v(\sigma x - x)$ for any $\sigma \in G$. Thus, due to Krasner's lemma, $L = K(x) \subset K(y) \subset E$. Hence, (P_n) holds, and then $m_{L/K} \leq u_{L/K}$.

(2)We now prove $m_{L/K} \geq u_{L/K}$. Notice that if K_1 is the maximal intermediate extension of L/K such that K_1/K is unramified, it is clear (P_n) holds for L/K_1 if (P_n) holds for L/K. Then we can assume L/K is totally ramified and $L \neq K$.

It will suffice to prove (P_n) fails for any $n \geq u_{L/K} - \epsilon$ and $\epsilon > 0$. To show (P_n) does not hold for L/K, we shall construct an E such that $\mathrm{Hom}_{O_K}(O_L, O_E/m_E^n) \neq \emptyset$ and $\mathrm{Hom}_K(L, E) = \emptyset$.

If L/K is tamely ramified, then $u_{L/K} = 1$. Take $E = K$ and $n = 1$. We have the reduction map $L \to O_L/m_L = O_K/m_K$ but there is no embedding of L in K. So, $m_{L/K} \geq u_{L/K} = 1$, and then we deduce $m_{L/K} = u_{L/K} = 1$ in this case.

Suppose L/K is wildly ramified (i.e. $p \mid [L : K]$). By definition, $e_{L/K} i_{L/K}(\sigma)$ is a positive integer for any σ. In this case, there are at least $p - 1$ of $\sigma \in G \backslash \{1\}$ such that $e_{L/K} i_{L/K}(\sigma) \geq 2$. Therefore, it is clear that $\phi_{L/K}$ is linear of slope larger than 1 on $[i_{L/K} - 1/e_{L/K}, i_{L/K}]$ and $u_{L/K} > 1 + (p-1)/e_{L/K}$.

Take $n = u_{L/K} - 1/e_{L/K}$. Choose a uniformizer π_L of L and let r be its minimal polynomial over O_K. Then r is an Eisenstein polynomial. Let $s(t) = r(t) - \pi_K^{u_{L/K}-1} t^{e_{L/K}-1}$. Then s is also an Eisenstein polynomial. Let $E = K[t]/(s(t))$ and $\alpha \in E$ be a root of s. Then $v(\alpha) = 1/e_{L/K}$. Define an O_K homomorphism $f : O_L \to O_E/m_E^n$ such that $f(\pi_L) = \alpha$. It is well-defined because $r(\alpha) = \pi_K^{u_{L/K}-1} \alpha^{e_{L/K}-1} \in (\alpha^{e_{L/K}(u_{L/K}-1)+e_{L/K}-1}) = m_E^n$. If (P_n) holds, then L can be embedded in E, which means r splits in E and π_L can be viewed as an element in E. By proposition 4.1, $\phi_{L/K}(\sup_{\sigma \in G} v(\alpha - \sigma\pi_L)) = v(r(\alpha)) = n = u_{L/K} - 1/e_{L/K}$. Because $\phi_{L/K}$ is linear of slope larger than 1 on $(i_{L/K}, i_{L/K} - 1/e_{L/K})$, we deduce $\sup_{\sigma \in G} v(\alpha - \sigma\pi_L) \in (i_{L/K} - 1/e_{L/K}, i_{L/K})$, which is impossible because $v(\alpha - \sigma\pi_L) \in 1/e_{L/K}\mathbb{Z}$. Therefore, (P_n) must fail for L/K and

$$m_{L/K} \geq u_{L/K} - 1/e_{L/K}. \tag{1}$$

Suppose L_1 and L_2 be two finite extensions of K and $L = L_1 L_2$. Suppose (P_n) holds for L_1/K and L_2/K. If E/L is a finite extension and there is an O_K-algebra homomorphism $f : O_L \to O_E/m_E^n$, it restricts to O_{L_1} and O_{L_2} respectively and we obtain two O_K-algebra homomorphism from O_{L_1} and O_{L_2} respectively to O_E/m_E^n. Because (P_n) holds for L_1/K and L_2/K, L_1 and L_2 can both be embedded in E. Thus, $L = L_1 L_2$ can be embedded in E and (P_n) holds for L/K. We obtain that

$$m_{L/K} \leq \max\{n_{L_1/K}, n_{L_2/K}\}. \tag{2}$$

Suppose L/K is wildly ramified. Choose an L' tamely ramified over K of degree of arbitrarily large l such that it is linear independent of L over K. Then $L_0 = LL'$ is wildly ramified over K of ramification index $le_{L/K}$. Combining Equation 1 and Equation 2, we get $\max\{m_{L/K}, n_{L'/K}\} \geq n_{L_0/K} \geq u_{L_0/K} - 1/le_{L/K} \geq u_{L/K} - 1/le_{L/K}$. Because $n_{L'/K} = 1 < u_{L/K} - 1/le_{L/K}$, we get $m_{L/K} \geq u_{L/K} - 1/le_{L/K}$. As one can take l as arbitrarily large real number, $m_{L/K} \geq u_{L/K}$.

Combining (1) and (2), we have shown $m_{L/K} = u_{L/K}$.

□

4.2 Ramification Bound for p-Groups

In this section, we will prove Theorem 4.1 which provides the main ramification bound used in the proof of Theorem 1.1. We start with the following local version of ramification bound for commutative finite flat p-groups.

Theorem 1.2 (Fontaine, [4], 2.1)**.** *Let n be a positive integer, and let Γ be a commutative finite flat group scheme over O_K killed by p^n. Let $G = \mathrm{Ker}(Gal(\bar{K}/K) \to \mathrm{Aut}(\Gamma(\bar{K})))$ and $L = \bar{K}^G$. Then, $u_{L/K} \leq e(n + 1/(p-1))$.*

Actually L is a field extension of K by adding all the points of Γ. So we can also write $L = K(\Gamma(\bar{K}))$. We will reduce Theorem 1.2 to the case of the following proposition.

Proposition 4.4 ([4], 1.7)**.** *Let B be a finite and flat O_K-algebra of locally complete intersection. Suppose there exists an $a \in O_K$ such that $a\Omega^1_{B/O_K} = 0$ and that Ω^1_{B/O_K} is a flat B/a module. Then the following hold.*

(1) If S is a finite flat O_K-algebra and I is a topologically nilpotent ideal of S, then:

(a) for all $u \in \mathrm{Hom}_{O_K}(B, S/aI)$, there exists a unique homomorphism $u' : B \to S$ such that the following diagram commutes:

$$\begin{tikzcd}
B \arrow[r, "u"] \arrow[d, "u'"] & S/aI \arrow[d, "proj."] \\
S \arrow[r, "proj."] & S/I
\end{tikzcd}$$

(b) The map $\mathrm{Hom}_{O_K}(B, S) \to \mathrm{Hom}_{O_K}(B, S/I)$ is injective.

(2) Let G be the kernel of the action of $Gal(\bar{K}/K)$ on $Hom_K(B, \bar{K})$, and let $L = \bar{K}^G$. Then, $u_{L/K} \leq v(a) + e/(p-1)$.

An ideal $I \subset S$ is a divided power ideal if, for all $x \in I$ and $n \in \mathbb{Z}_+$, the element $\gamma_n(x) = x^n/n! \in I$. The ideal $I^{[m]}$ is defined to be the ideal of S generated by the products $\gamma_{n_1}(x_1)\cdots\gamma_{n_r}(x_r)$ for all $x_1, \cdots, x_r \in I$ and $\sum n_i \geq m$. A divided power ideal I is called topologically nilpotent if $\bigcap_{m=1}^{\infty} I^{[m]} = 0$. An example of a topologically nilpotent divided power ideal is $m_E^{e/(p-1)} \subset O_E$. One can check this easily by calculating the p-adic valuation.

Proof. In order to see why we need the technical result (1), we start with proving (2) by assuming (1). According to Proposition 4.1, we have to show $m_{L/K} \leq v(a) + e/(p-1)$, equivalently, to show for any $h > v(a) + e/(p-1)$, (P_h) holds for L/K. Assume $h > v(a) + e/(p-1)$ and $v : O_L \to O_E/m_E^h$ is an O_K-homomorphism. Let $X = \operatorname{Spec} B$. We want to show L can be embedded in E, which is the same as to show $\#X(E) \geq \#X(L)$ because L is the field of definition of X. If $u_0 \in X(O_L) = \operatorname{Hom}_{O_K}(B, O_L)$, composite with v, we obtain $u = v \circ u_0 \in \operatorname{Hom}_{O_K}(B, O_E/m_E^h)$. Let $I = (a)^{-1}m_E^h$. Then, $I \in m_E^{e/(p-1)}$, and I is a topologically nilpotent divided power ideal. Assuming (1), we get a $u' \in \operatorname{Hom}_{O_K}(B, O_E) = X(O_E)$.

Our next step is to show the map $X(O_L) \to X(O_E) : u_0 \mapsto u'$ is injective. Let v' be the composition $O_L \xrightarrow{v} O_E/m_E^h \to O_E/I$. Then the kernel I' of v' is $m_L^{h-v(a)} \in m_L^{e/(p-1)}$ is a topologically nilpotent divided power ideal. Thus, we have the following composition of injective maps $\operatorname{Hom}_{O_K}(B, O_L) \to \operatorname{Hom}_{O_K}(B, O_L/I') \to \operatorname{Hom}_{O_K}(B, O_E/I)$ sends u_0 to the image of u' under the injective map $\operatorname{Hom}_{O_K}(B, O_E) \to \operatorname{Hom}_{O_K}(B, O_E/I)$. Therefore, we have constructed an injection $X(O_L) \to X(O_E) : u_0 \mapsto u'$. Because X is finite flat over O_K, every L-point (resp. E-point) of X extends to a unique O_L-point (resp. O_E-point) of X. Thus, $\#X(E) = \#X(O_E) \geq \#X(O_L) = \#X(L)$. Therefore, L can be embedded in E and we attain that (P_h) holds for L/K. By Proposition 4.1, $u_{L/K} = m_{L/K} \leq v(a) + e/(p-1)$.

We now prove (1)(a). Clearly, we can assume B is a local ring. Let m_B be its maximal ideal and k be the residue field.

Take $x_1, \cdots, x_n$ be a basis of the k-vector space $m_B/(m_B^2 + m_K B)$. Then $dx_1, \cdots, dx_n$ is a basis of $\Omega^1_{B/O_K} \otimes_{O_K} k$. As Ω^1_{B/O_K} is a free B/a-module, $dx_1, \cdots, dx_n$ is a basis of Ω^1_{B/O_K} as a free B/a-module by Nakayama lemma. Define a map $f : O_K[[X_1, \cdots, X_n]] \to B$ such that $f(X_i) = x_i$ for $i = 1, \cdots, n$. Because B is of locally complete intersection and

$dx_1, \cdots, dx_n$ is a basis of Ω^1_{B/O_K}, the kernel of f is generated by n elements $P_1, \cdots, P_n$. Then the kernel of $Bdx_1 + \cdots + Bdx_n \to \Omega^1_{B/O_K}$ is generated by $\sum_{j=1}^n f(\frac{\partial P_i}{\partial X_j})dx_j$, $i = 1, \cdots, n$. Since $adx_1, \cdots, adx_n$ is a B-basis of this kernel and B is a local ring, we deduce $f(\frac{\partial P_i}{\partial X_i}) = ap_{ij}$ and $(p_{ij})_{1\leq i,j\leq n} \in \mathrm{Mat}_{n\times n}(B)$ is invertible.

Because I is topologically nilpotent, it will suffice to show that for each m and an O_K-homomorphism $u : B \to S/aI^{[m]}$, there exists a $u' : B \to S/aI^{[m+1]}$ such that the compositions $B \xrightarrow{u} S/aI^{[m]} \to S/I^{[m]}$ and $B \xrightarrow{u'} S/aI^{[m+1]} \to S/I^{[m]}$ coincide and that the composition $B \xrightarrow{u'} S/aI^{[m+1]} \to S/I^{[m+1]}$ is unique. Let $u : B \to S/aI^{[m]}$ be an O_K-homomorphism and $a_1, \cdots, a_n \in S$ be a choice of lift of the image of $x_1, \cdots, x_n$ under the map of u. Then $P_i(a_1, \cdots, a_n) \in aI^{[m]}$ for $i = 1, \cdots, n$. Let $P_i(a_1, \cdots, a_n) = aq_i$ for some $q_i \in I^{[m]}$. We have to find $b_1, \cdots, b_n \in I^{[m]}$ such that $P_i(a_1 + b_1, \cdots, a_n + b_n) \in aI^{[m+1]}$. For a $r = (r_1, \cdots, r_n) \in \mathbb{Z}_+^n$ and $P \in O_K[[X_1, \cdots, X_n]]$, we introduce the following multi-index notation:

$$|r| = \sum r_i, \quad \frac{\partial^r P}{\partial X^r} = \frac{\partial^{|r|} P}{\partial X_1^{r_1} \cdots \partial X_n^{r_n}}, \quad \gamma_r(b) = \gamma_{r_1}(b_1) \cdots \gamma_{r_n}(b_n).$$

Consider the Taylor's expansion,

$$\begin{aligned} P_i(a_1 + b_1, \cdots, a_n + b_n) =& P_i(a_1, \cdots, a_n) + \sum_{j=1}^n \frac{\partial P_i}{\partial X_j}(a_1, \cdots, a_n)b_j + \sum_{|r|\geq 2} \frac{\partial^r P}{\partial X^r}(a_1, \cdots, a_n)\gamma_r(b) \\ =& aq_i + \sum_j af(p_{ij})b_j + \sum_{|r|\geq 2} \frac{\partial^r P}{\partial X^r}(a_1, \cdots, a_n)\gamma_r(b). \end{aligned} \tag{3}$$

Because $\frac{\partial P_i}{\partial X_j}(x_1, \cdots, x_n) \in aB$, we get $\frac{\partial^r P}{\partial X^r}(a_1, \cdots, a_n) \in aS$ by some calculation. When $|r| \geq 2$, $\gamma_r(b) \in (I^{[m]})^{[2]} \subset I^{[m+1]}$. Then we deduce

$$P_i(a_1 + b_1, \cdots, a_n + b_n) = aq_i + \sum_j af(p_{ij})b_j \mod aI^{[m+1]}.$$

As (p_{ij}) is an invertible B-matrix, $f(p_{ij})$ is an invertible S-matrix. Therefore, there is unique $b_1, \cdots, b_n \mod I^{[m+1]}$ such that $P_i(a_1 + b_1, \cdots, a_n + b_n) = 0 \mod aI^{[m+1]}$. We have proved the claim.

Now we prove (1)(b). If $u : B \to S/I$ admits a lift to $u : B \to S$, it can first be lifted to $u : B \to S/aI$. According to the claim, the lift is unique. Therefore, this shows that $\mathrm{Hom}_{O_K}(B, S) \to \mathrm{Hom}_{O_K}(B, S/I)$ is injective. □

The proof of Theorem 1.2. Suppose that $\Gamma = \operatorname{Spec} B$ where B is locally of complete intersection and that Ω^1_{B/O_K} is annihilated by p^n and is a free B/p^nB-module. Then the desired result is concluded from Proposition 4.4 because $v(D_{L/K}) = u_{L/K} - i_{L/K} \leq u_{L/K} \leq v(p^n) + e/(p-1) = e(n + 1/(p-1))$, where the first equality is from Proposition 4.1.

In general, the condition that B is locally of complete intersection comes for free, because $B \otimes_{O_K} k$ is locally of complete intersection as shown in Theorem 2.5 and thus B is also locally of complete intersection. It is clear that, if we can find an O_K-group scheme $\Gamma' \supset \Gamma$ such that the desired result holds for Γ', then the result holds for Γ. Theorem 2.10 shows that there is a closed embedding $i : \Gamma \to A$ where A is an abelian scheme over O_K. Because Γ is killed by p^n, the image of i is contained in $A[p^n]$, and then Γ can be seen as a closed subgroup scheme of $A[p^n]$. Apparently, for $\Gamma' = A[p^n] = \operatorname{Spec} B$, Ω_{Γ'/O_K} is killed by p^n and is a free B/p^n-module. Thus, $\Gamma' = A[p^n]$ satisfies the special case we discussed in the last paragraph, and the result holds for $A[p^n]$ and also for Γ.

□

We can reach a global consequence immediately from this local result.

Corollary 4.1 ([4], 3.3.2)**.** *Let E be a number field, and fix an algebraic closure E. Let Γ be a commutative finite flat O_E-group scheme killed by p^n , and let $F = E(\Gamma(\bar{E}))$. For a prime ideal $\mathfrak{p} \subset O_E$, let $e_\mathfrak{p}$ be the absolute ramification index of $\mathfrak{p}$ and $r_\mathfrak{p}$ be the exponent of $\mathfrak{p}$ inside the discriminant $D_{F/E}$. Then we have the following.*

(1) If $\mathfrak{p}$ does not divide p, $r_\mathfrak{p} = 0$.

(2) If $\mathfrak{p}$ divides p, $r_\mathfrak{p} < [F : E]e_\mathfrak{p}(n + 1/(p-1))$.

(3) If d_E, d_F are the absolute discriminants of E, F, respectively, then

$$|d_F|^{\frac{1}{[F:\mathbb{Q}]}} < |d_E|^{\frac{1}{[E:\mathbb{Q}]}} p^{n+1/(p-1)}.$$

It is directly from Theorem 1.2 and Theorem 2.6, using the formulas $D_{F/\mathbb{Q}} = D_{E/\mathbb{Q}}^{[F:E]} N_{E/\mathbb{Q}}(D_{F/E})$ and $D_{F/E} = \prod_w (D_{F_w/E_v} \cap O_F)$ where w runs through the places of F and v is the restriction of w on E.

4.3 Calculations and Applications

We are going to classify the commutative finite flat p-groups over $\mathbb{Z}$. The simple idea is to combine the golbal ramification bound developed in Theorem 4.1 with the local classification result of low ramification cases in Corollory 2.1. It turns out that the ramification bound is very effective in our attempt to classify all the p-groups over $\mathbb{Z}_p$ or $\mathbb{Z}$.

Theorem 4.1 (Fontaine, [4], 3.4.1)**.** *Let Γ be a commutative finite flat group scheme over $\mathbb{Z}$ of p-power order. Then Γ is a direct sum of a constant group and a diagonalizable group.*

Lemma 4.1 ([4], 3.4.2)**.** *Let Γ be a commutative finite flat group scheme over $\mathbb{Z}$ killed by p, and let $E = \mathbb{Q}(\Gamma(\bar{\mathbb{Q}}))$. Suppose that Γ has a closed subgroup scheme μ_p. If $p \in \{3, 5, 7, 11, 13, 17\}$, then $E = \mathbb{Q}(\mu_p)$, $\Gamma = (\mathbb{Z}/p\mathbb{Z})^r \oplus \mu_p^s$.*

Proof. Let $n = [E : \mathbb{Q}]$. By theorem 4.1, we get $|d_F|^{1/n} < p^{p/(p-1)}$ and E is unramified outside p. By using the Odlyzko discriminant bound [6], we deduce, in each case, n has an upper bound as follows: if $p = 3, 5, 7, 11, 13, 17$, then $n \leq 6, 12, 18, 50, 88, 574$.

Let e be the absolute ramification index of a place $\mathfrak{p}$ of E over p. If $E_p/\mathbb{Q}_p$ is not totally ramified, since $E/\mathbb{Q}$ is unramified outside p, we can find an intermediate field $F \neq \mathbb{Q}$ such that $F/\mathbb{Q}$ is totally unramified, which is impossible because $\mathbb{Q}$ has class number 1. Thus, $E_p/\mathbb{Q}_p$ is totally ramified. In each case listed above, $n < p^2(p-1)$. Thus, by Corollary 2.1, $e = p-1, p(p-1), p^2-1$.

If $e = p-1$, then E is totally unramified over $\mathbb{Q}(\mu_p)$. We can check that, for all p in the statement, $\mathbb{Q}(\mu_p)$ has class number 1. Thus, $E = \mathbb{Q}(\mu_p)$.

If $e = p^2-1$, then $n \geq p^2-1$ and p has to be $3, 17$ according to the above calculation results. In this case, $E_\mathfrak{p}/\mathbb{Q}_p$ is tamely ramified and we get a sharper bound. In fact, by Proposition 4.1, $v(D_{E_\mathfrak{p}/\mathbb{Q}_p}) \leq u_{E_\mathfrak{p}/\mathbb{Q}_p} = 1$. Because $E/\mathbb{Q}$ is unramified outside p, we obtain $v(d_E) < p$. After recalculation using the Odlyzko discriminant bound, we get for $p = 3, 17$, $n \leq 2, 116$. In both cases, $n < p^2-1$. So it is impossible to have $e = p^2-1$.

If $e = p(p-1)$, we are going to show $n = e = p(p-1)$.Because $n/(p-1) < p^2$, then by Sylow theorem, $\mathrm{Gal}(E/\mathbb{Q}(\mu_p))$ contains only one Sylow p-group, which is a normal subgroup. Let $\mathfrak{p}'$ be the prime ideal of $\mathbb{Q}(\mu_p)$ over p. Since $\#\mathrm{Gal}(E_\mathfrak{p}/\mathbb{Q}_p(\mu_p)) = p$, then the decomposition group $D_{\mathfrak{p}/\mathfrak{p}'}$ is the Sylow p-group. Because $E^{D_{\mathfrak{p}/\mathfrak{p}'}}$ is an everywhere unramified Galois extension of $\mathbb{Q}(\mu_p)$ and the class number of $\mathbb{Q}(\mu_p)$ is 1, we get $E^{D_{\mathfrak{p}/\mathfrak{p}'}} = \mathbb{Q}(\mu_p)$. Thus, $[E : \mathbb{Q}(\mu_p)] = \# D_{\mathfrak{p}/\mathfrak{p}'} = [E_{\mathfrak{p}} : \mathbb{Q}_p(\mu_p)] = p$. Therefore, $n = [E : \mathbb{Q}] = p(p-1)$.

Let $W = W(\bar{\mathbb{F}}_p)$ and $K = \mathrm{Frac}W$. Because $e = p-1$ or $p(p-1)$ and Γ contains μ_p as a closed subgroup. We know from Corollary 2.1 that $\Gamma_W = \Gamma \times_{\mathbb{Z}} W$ is an extension of $(\mathbb{Z}/p\mathbb{Z})^r$ by μ_p^s for two non-negative integers r, s. We claim that Γ is also an extension of $(\mathbb{Z}/p\mathbb{Z})^r$ by μ_p^s. First, we can show Γ is determined by its generic fibre, or equivalently, by the associated Galois action. Since $G_{\mathbb{Q}}$ decides $\Gamma_{\mathbb{Z}_p}$ by Raynaud's theorem and also decides the étale $\Gamma_{\mathbb{Z}[1/p]}$, it decides Γ by Theorem 2.7. In our case, $[E : \mathbb{Q}] = [E_{\mathfrak{p}} : \mathbb{Q}_p]$ and $E_{\mathfrak{p}}/\mathbb{Q}_p$ is totally ramified. Thus, we obtain the natural isomorphisms $\mathrm{Gal}(E : \mathbb{Q}) \simeq \mathrm{Gal}(E_{\mathfrak{p}} : \mathbb{Q}_p) \simeq \mathrm{Gal}(KE_{\mathfrak{p}} : K)$. Therefore, one can tell the Galois action associated to Γ from the one associated to Γ_W. Hence, $\Gamma_{\mathbb{Q}}$ is an extension of $(\mathbb{Z}/p\mathbb{Z})^r$ by μ_p^s. As explained in Remark 2.2, there is a natural bijection between the closed subgroup (resp. quotient group) schemes of Γ and $\Gamma_{\mathbb{Q}}$. Then Γ is also an extension of $(\mathbb{Z}/p\mathbb{Z})^r$ by μ_p^s.

We now show that any extension of $(\mathbb{Z}/p\mathbb{Z})^r$ by μ_p^s over $\mathbb{Z}$ has to be trivial. Then we only have to show the triviality of every extension of $\mathbb{Z}/p\mathbb{Z}$ by μ_p over $\mathbb{Z}$. By Proposition 2.2, it is now reduced to the calculation of $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}, \mu_p)$. Consider the following two exact sequences:

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{G}_m) \xrightarrow{x \mapsto x^p} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{G}_m) \to \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}, \mu_p) \to \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}, \mathbb{G}_m), \tag{4}$$

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mu_p) \xrightarrow{x \mapsto x^p} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mu_p) \to \mathrm{Ext}^1_{\mathbb{Z}}((\mathbb{Z}/p\mathbb{Z})_{\mathbb{Z}}, \mu_p) \to \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}, \mu_p) \xrightarrow{x \mapsto x^p} \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}, \mu_p). \tag{5}$$

In exact sequence (4), because $\mathbb{Z}^\times = 1$, $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{G}_m) = 1$. Then $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}, \mu_p) \to \mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}, \mathbb{G}_m) = \mathrm{Pic}(\mathbb{Z}) = 1$. Now we look at the exact sequence (5). Because $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}, \mu_p) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mu_p) = 1$, we get $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}, \mu_p) = 1$. Thus, we have already showed that any extension of $(\mathbb{Z}/p\mathbb{Z})^r$ by μ_p^s over $\mathbb{Z}$ is trivial. Therefore, $\Gamma = (\mathbb{Z}/p\mathbb{Z})^r \oplus \mu_p^s$. □

Proof of Theorem 4.1. By Remark 2.2, we have a Jordan-Holder composition series of G. We obtain from Lamma 4.1 that all simple p-groups over $\mathbb{Z}$ are $\mathbb{Z}/p\mathbb{Z}$ and μ_p. It is easy to see an extension of a constant group scheme by a constant group scheme is a constant group scheme. Using Cartier duality, we get an extension of a diagonalizable group scheme by a diagonalizable group scheme is a diagonalizable group scheme. Also, an extension of a diagonalizable group scheme by a constant group scheme is always trivial, which is ensured by the connected-étale sequence. Therefore, Γ is an extension of a constant group scheme Γ_c by a diagonalizable group scheme Γ_d. The only thing left is to show the extension is trivial.

We introduce the following notion. If Γ is a commutative finite p-group over $\mathbb{Z}$, let $V_0 = \{x \in \Gamma(\bar{\mathbb{Q}}) \mid \sigma x = x$, for all $\sigma \in G(\bar{\mathbb{Q}}/\mathbb{Q})$, and $V_1 = \{x \in \Gamma(\bar{\mathbb{Q}}) \mid \sigma x = \chi(\sigma)x$, for all $\sigma \in G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ where χ is the p-adic cyclotomic character. Γ is called admissible if $\Gamma(\bar{\mathbb{Q}}) = V_0 \oplus V_1$. Then our goal, translated into the language of Galois representation, is to prove every commutative finite flat p-group over $\mathbb{Z}$ is admissible. The category of admissible p-groups is stable under subquotients and finite sums.

When the order of Γ is p, it is admissible by Lemma 4.1. We proceed by induction. Suppose there exists a commutative finite flat p-group over $\mathbb{Z}$ is not admissible. Choose a Γ which is not admissible and of the minimal order. Take a subgroup Γ' of Γ such that Γ/Γ' is a simple group. Then by Lemma 4.1, Γ/Γ' is isomorphic to μ_p or $\mathbb{Z}/p\mathbb{Z}$. Because the order of Γ' is smaller than Γ, $\Gamma' = \Gamma_0 \oplus \Gamma_1$ where Γ_0 is constant and Γ_1 is diagonalizable.

If $\Gamma_0 \neq 0$ and $\Gamma_1 \neq 0$, then Γ/Γ_0 and Γ/Γ_1 are both admissible. Since $\Gamma \to \Gamma/\Gamma_0 \oplus \Gamma/\Gamma_1$ is an injection, Γ is admissible.

If $\Gamma_0 = 0$ and $\Gamma_1 \neq 0$, then Γ' is diagonalizable. If $\Gamma/\Gamma' \simeq \mu_p$, Γ is still diagonalizable and also admissible. If $\Gamma/\Gamma' \simeq \mathbb{Z}/p\mathbb{Z}$, consider the exact sequence $0 \to \Gamma'(\bar{\mathbb{Q}}) \to \Gamma(\bar{\mathbb{Q}}) \to \mathbb{Z}/p\mathbb{Z} \to 0$. Let u be an element in $\Gamma(\bar{\mathbb{Q}})$ whose image in $\mathbb{Z}/p\mathbb{Z}$ is $\bar{1}$. We have $pu = v \in \Gamma'(\bar{\mathbb{Q}})$. Let $w_\sigma = \sigma u - u$ for $\sigma \in G_{\mathbb{Q}}$. Because $v \in \Gamma'(\bar{\mathbb{Q}})$, $\chi(\sigma)v = \sigma v = \sigma(pu) = p\sigma u = pu + pw_\sigma$. Then, $(\chi(\sigma) - 1)v = pw_\sigma$. Choose σ such that $\chi(\sigma) - 1$ is a p-adic unit. We deduce that $v \in p\Gamma'(\bar{\mathbb{Q}})$. Let $v = pv_1$, $v_1 \in \Gamma'(\bar{\mathbb{Q}})$. Therefore, we can replace u with $u - v_1$, and we get $pu = 0$. Therefore, we obtain that $0 \to \Gamma'[p](\bar{\mathbb{Q}}) \to \Gamma[p](\bar{\mathbb{Q}}) \to \mathbb{Z}/p\mathbb{Z} \to 0$ is also exact. By Lemma 4.1, this sequence splits. Hence, $\Gamma[p]$ has a subgroup isomorphic to $\mathbb{Z}/p\mathbb{Z}$, so does Γ. Therefore, $0 \to \Gamma' \to \Gamma \to \mathbb{Z}/p\mathbb{Z} \to 0$ splits, and Γ is admissible.

If $\Gamma_0 \neq 0$ and $\Gamma_1 = 0$, then Γ' is constant. If $\Gamma/\Gamma' \simeq \mathbb{Z}/p\mathbb{Z}$, Γ is still constant. If $\Gamma/\Gamma' \simeq \mu_p$, the short exact sequence $0 \to \Gamma' \to \Gamma \to \mu_p \to 0$ splits because Γ' is constant.

Thus, Γ is admissible in all cases, contradicting our assumption. Then, all commutative finite flat p-groups over $\mathbb{Z}$ are a direct sum of a constant group and a diagonalizable group. □

Theorem 1.1 (Fontaine, [4], 3.4.6)**.** *There is no nontrivial abelian scheme over $\mathbb{Z}$. Equivalently, there is no nontrivial abelian variety over $\mathbb{Q}$ with everywhere good reduction.*

Proof of Theorem 1.1. We first assume that there is a nontrivial abelian variety A over $\mathbb{Z}$ of dimension $g > 1$, and then we deduce some contradiction. Let $(A[p^n])$ be the p-divisible group associated to A. Then by Theorem 4.1, it a direct sum of $(\mathbb{Q}_p/\mathbb{Z}_p)^r$ and $(\mu_{p^\infty})^s$ $(r + s = 2g)$. Because $(A[p^n])$ is of dimension g, $(\mathbb{Q}_p/\mathbb{Z}_p)$ is of dimension 0, (μ_{p^∞}) is of dimension 1, $r = s = g$. Thus $A(\mathbb{Q})$ has infinite p-torsion points, in contradiction to the Mordell-Weil theorem. □

References

[1] Sivaramakrishna Anantharaman. Schémas en groupes, espaces homogènes et espaces algébriques sur une base de dimension 1. In *Sur les groupes algébriques*, pages 5–79. Société mathématique de France, 1973.

[2] Pierre Berthelot, Lawrence Breen, and William Messing. *Théorie de Dieudonné cristalline II*. Lecture notes in mathematics: 930. Berlin: Springer, 1982.

[3] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron Models*. A Series of Modern Surveys in Mathematics. Springer Berlin, Heidelberg, 1990.

[4] Jean Marc Fontaine. Il n'y a pas de variété abélienne sur $\mathbb{Z}$. *Inventiones mathematicae*, 81:515–538, 1985.

[5] Jean-Marc Fontaine. Schemes which are proper and smooth over $\mathbb{Z}$. In *Proceedings of the Indo-French conference on geometry held in Bombay, India, 1989*, pages 43–56. Delhi: Hindustan Book Agency, 1993.

[6] Jacques Martinet. *Petits discriminants des corps de nombres*, page 151–193. London Mathematical Society Lecture Note Series. Cambridge University Press, 1982.

[7] D. Mumford, C.P. Ramanujam, and I.U.I. Manin. *Abelian Varieties*. Studies in mathematics. Hindustan Book Agency, 2008.

[8] Michel Raynaud. *Faisceaux amples sur les schemas en groupes et les espaces homogenes.* Lecture Notes in Mathematics. Springer Berlin, Heidelberg, 1973.

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

[10] J. T. Tate. p-divisible groups. In T. A. Springer, editor, *Proceedings of a Conference on Local Fields*, pages 158–183, Berlin, Heidelberg, 1967. Springer Berlin Heidelberg.

[11] John Tate. Finite flat group schemes. In *Modular Forms and Fermat's Last Theorem*, pages 121–154. Springer New York, 1997.

[12] Manabu Yoshida. Ramification of local fields and fontaine's property (pm). *J. Math. Sci. Univ. Tokyo*, 17:247–265, 2010.