There is no abelian scheme over $\mathbb{Z}$

Contents

Introduction

In his 1962 ICM talk [Sh], Shafarevich suggested several conjectures regarding the finiteness of isomorphism classes of arithmetic objects having good reduction almost everywhere. Such problems can find their origins from basic finiteness theorems in algebraic number theory, especially the **Hermite-Minkowski theorem**: *for any integer $N > 0$ and a number field K, there are only finitely many number fields L such that the discriminant of L/K is at most N.* A more geometric re-statement of the theorem is as follows.

Theorem (Hermite-Minkowski)**.** *For any number field K, a finite set of primes S of K and an integer $N > 0$, there are only finitely many isomorphism classes of zero-dimensional varieties of degree at most N over K which possess a smooth model over $\mathrm{Spec}(\mathcal{O}_{K,S})$, where $\mathcal{O}_{K,S}$ is the ring of S-integers in K.*

In this regard, we can state the Shafarevich conjectures in the following form.

Conjecture (Shafarevich)**.** *Let K be a number field and S be a finite set of primes of K. Let $g \geq 2$ be an integer.*

(a) (Shafarevich conjecture for curves) *There are only finitely many isomorphism classes of smooth curves over $\mathcal{O}_{K,S}$ of genus g. Equivalently, there are only finitely many isomorphism classes of curves over K of genus g having good reduction outside S.*

(b) (Shafarevich conjecture for abelian varieties) *There are only finitely many isomorphism classes of abelian schemes over $\mathcal{O}_{K,S}$ of dimension g. Equivalently, there are only finitely many isomorphism classes of abelian varieties over K of dimension g having good reduction outside S.*

In particular, Faltings [Fa] proved the Shafarevich conjectures in conjunction with various other finiteness results, including the finiteness of isogeny classes and the Mordell's conjecture.

On the other hand, there are some special cases where one can suspect whether the set of isomorphism classes of arithmetic object is actually *empty*. This can be motivated from the classic theorem of Minkowski that *there is no nontrivial unramified extension of* $\mathbb{Q}$. We can as well geometrically re-interpret the statement as follows.

Theorem (Minkowski)**.** *The only connected zero-dimensional variety over $\mathbb{Q}$ admitting a smooth model over $\mathrm{Spec}(\mathbb{Z})$ is $\mathrm{Spec}(\mathbb{Q})$.*

From this theorem, Shafarevich further conjectured that the sets of isomorphism classes considered in the Shafarevich conjectures are *empty* if $K = \mathbb{Q}$ and $S = \emptyset$. In other words,

Conjecture (Shafarevich)**.** *There is no nontrivial abelian scheme over $\mathbb{Z}$. Equivalently, there is no nontrivial abelian variety over $\mathbb{Q}$ with everywhere good reduction.*

This conjecture is established independently by Fontaine [Fo1] and Abrashkin [Ab1], and this is the direction we will mostly focus on amongst many Shafarevich conjectures.

The basic strategy behind the first proofs is to study ramification of *finite flat group schemes* and *p-divisible groups*. Specifically, if there is an abelian scheme A over $\mathbb{Z}$, then for a prime p, the collection of p^n-torsions $\{A[p^n]\}_{n\geq 1}$ forms an object called a *p-divisible group* over $\mathbb{Z}$. By studying the ramification bounds on such objects, just like the proof of Minkowski's theorem, the proofs show that, for a small prime p, a p-divisible group over $\mathbb{Z}$ is of very simple form, so simple that it cannot arise as a p-divisible group from p-power torsions of an abelian variety.

Somehow in a different flavor, Fontaine [Fo2] and Abrashkin [Ab2] later revisited the nonexistence of abelian scheme over $\mathbb{Z}$. Instead of analyzing the ramification behavior of p-divisible groups and torsion subgroups, which are objects only available to group schemes, they instead analyzed the ramification of p-adic étale cohomology as a Galois representation. This strategy became possible via the development of p-adic Hodge theory and its integral counterpart. This strategy enabled them to generalize the nonexistence results to certain smooth proper schemes with no group structure. In particular, they proved the following.

Theorem (Fontaine, [Fo2, Théorème 1], [Ab2, 7.6])**.** *Let X be a smooth proper variety over $\mathbb{Q}$ with everywhere good reduction. Then, $H^i(X, \Omega^j_X) = 0$ for $i \neq j$, $i + j \leq 3$.*

In particular, this implies the nonexistence of abelian scheme over $\mathbb{Z}$ as corollary.

In this essay, we review the both approaches towards the proof of nonexistence of abelian variety over $\mathbb{Q}$ with everywhere good reduction. The first chapter will focus on the analysis of finite flat group schemes and p-divisible groups. In the chapter, we will go through the details of Fontaine's original proof. In the chapter, we will also review some extensions of the result using the same kind of technique, most notably the one by Schoof [Sc1]; it gives the nonexistence of abelian varieties over a small number field with semi-stable reduction at one small prime and good reduction at everywhere else. We briefly examine the results due to Brumer-Kramer [BK], who used a different approach more in conjunction with the Shafarevich conjecture (or, Faltings' Finiteness Theorem).

The second chapter will be aiming for p-adic Hodge theoretic proofs of nonexistence of abelian schemes over $\mathbb{Z}$. In particular, we will observe various classes of p-adic Galois representations, and examine how to classify those representations in a different way. In particular, we will see p-adic Galois representations and their integral sublattices can be classified by modules with various (semi)linear structures attached. Such modules then will have a similar kind of discriminant bound as p-divisible groups and finite flat group schemes have. In particular, using integral p-adic Hodge theoretic constructions, including Fontaine-Laffaille modules, Breuil-Kisin modules and $(\varphi, \widehat{G})$-modules, we give discriminant bounds for torsion crystalline and semi-stable representations. This generalization to semi-stable representations can yield some other nonexistence results, and we in particular will review the result of Abrashkin [Ab4] on the nonexistence of a smooth projective variety over $\mathbb{Q}$ with semi-stable reduction at 3 and good reduction at everywhere else.

In the course, we will introduce the relevant preliminaries, including the theory of finite flat group schemes, p-divisible groups, abelian varieties and their reduction types, étale cohomology theory, p-adic Hodge theory and integral p-adic Hodge theory. A reader is assumed to have good familiarity with homological algebra as in [La] (including spectral sequences), algebraic geometry as in [Har] or [EGA] and algebraic number theory/class field theory as in [Se] and [CF].

Notations. G_K will mean the absolute Galois group of K. $\overline{K}$, K_s and K^{nr} will mean the algebraic closure, the separable closure and the maximal unramified extension of K, respectively. $\mathcal{O}_K$, I_K and k_K will mean the ring of integers, the inertia group and the residue field, respectively. For a p-adic field K, K_0 will mean the maximal unramified (over $\mathbb{Q}_p$) sub-extension of K, i.e. $K_0 = W(k_K)[1/p]$. The letters $\mathfrak{D}$ and Δ will be reserved for different and discriminant ideals, respectively. χ will be the cyclotomic character, and both φ and σ will be used for the Frobenius. ζ_n is the n-th root of unity. $\operatorname{Frac} R$ is the field of fractions of R. A subscript attached to a scheme usually means the base change to the subscript scheme. Γ usually means the section functor. $[n]$ is the multiplication-by-n map.

Chapter 1

Nonexistence of Certain Abelian Varieties

1.1 Overview

The following theorem can be regarded as the main theorem of Fontaine's first proof in [Fo1].

Theorem 1.1.1 [Fo1, Théorème 1]. *Let K be a finite extension of $\mathbb{Q}_p$, and let $e = v_K(p)$ be the absolute ramification index. For an integer $n \geq 1$, suppose Γ is a finite flat commutative group scheme over $\mathcal{O}_K$ killed by p^n. Let $L = K(\Gamma(\overline{K}))$, and $G = \mathrm{Gal}(L/K)$. Then, $G^{(u)} = 1$ for $u > e\left(n + \frac{1}{p-1}\right)$, and $v(\mathfrak{D}_{L/K}) < e\left(n + \frac{1}{p-1}\right)$, where $\mathfrak{D}_{L/K}$ is the different of L/K.*

In particular, if G is the restriction of some finite flat group scheme $\Gamma/\mathcal{O}_K$ for a number field K, then it turns out that $K(\Gamma(\overline{K}))$ is unramified at primes outside p and is very mildly ramified at p by the above theorem; this is the heart of nonexistence results in this vein. Combining with the discriminant bounds of Odlyzko [Mar], one can then give an upper bound of $[L : K]$. Case analysis for L/K will give a severe restriction on the structure of Γ as a finite flat group scheme. In particular, the cases we will examine will only have a finite flat commutative group scheme of p-power order as being an extension of a *constant group scheme* by a *diagonalizable group scheme*. An abelian variety, however, cannot yield such group scheme, as such group scheme has "too many points," as we will see. The main nonexistence results are as follows.

Theorem 1.1.2 [Fo1, Corollaire 2]. *For $E = \mathbb{Q}, \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{5})$, there is no nontrivial abelian variety over E with everywhere good reduction.*

Theorem 1.1.3 [Sc1, Theorem 1.1]. *For the primes $\ell = 2, 3, 5, 7, 13$, there is no nontrivial abelian variety over $\mathbb{Q}$ with good reduction outside ℓ and semi-stable reduction at ℓ.*

1.2 Preliminaries

1.2.1 Finite Flat Group Schemes

1.2.1.1 Affine Group Schemes

Let S be a base 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; namely, the associativity, identity, inverse axioms are satisfied. One can define the same notion more cleanly via the functor of points approach; a group scheme over S is a representable contravariant functor $(\mathbf{Sch}/S) \to \mathbf{Grp}$

from the category of S-schemes to the category of groups. In other words, an S-scheme G is a group scheme when you can give compatible group structures on $G(T)$'s, for all S-schemes T. In particular, one does not have to construct multiplication, inverse and identity by hand because, for example, the multiplication $m : G \times G \to G$ can be recovered as the addition of two natural projections $\mathrm{pr}_1, \mathrm{pr}_2 : G \times G \to G$ using the group structure we have on $G(G \times G)$. Also, a functor of points is determined by its restriction to affine schemes[1], so we only need to construct compatible group structures of $G(T)$'s for affine T's.

From now on, we will mostly focus on the case of affine base scheme $S = \operatorname{Spec} R$ and affine S-group scheme $G = \operatorname{Spec} A$. Then, induced from multiplication, identity and inverse morphisms of G, the R-algebra A will have corresponding R-algebra maps with everything dualized, namely $\widetilde{m} : A \to A \otimes_R A$, $\widetilde{e} : A \to R$ and $\widetilde{i} : A \to A$, called *comultiplication, counit and coinverse*, respectively. An R-algebra with such extra structures is called a *Hopf algebra*.

Example 1.2.1. Let R be a ring.

1. **The additive group** $\mathbb{G}_a$. Let $\mathbb{G}_a = \operatorname{Spec}(R[t])$. For an R-algebra T,
$$\mathbb{G}_a(T) = \operatorname{Hom}_{R-\mathrm{alg}}(R[t], T) = T,$$
and the additive group structure of T given on $\mathbb{G}_a(T)$ makes $\mathbb{G}_a$ a group scheme.

2. **The multiplicative group** $\mathbb{G}_m$. Let $\mathbb{G}_m = \operatorname{Spec}(R[t, t^{-1}])$. For an R-algebra T,
$$\mathbb{G}_m(T) = \operatorname{Hom}_{R-\mathrm{alg}}(R[t, t^{-1}], T) = T^\times,$$
so the multiplicative group structure of $T^\times$ given on $\mathbb{G}_m(T)$ makes $\mathbb{G}_m$ a group scheme.

3. **Roots of unity**. For an integer $n \geq 2$, let $\mu_n = \operatorname{Spec} R[t]/(t^n - 1)$. Then, for an R-algebra T,
$$\mu_n(T) = \operatorname{Hom}_{R-\mathrm{alg}}(R[t]/(t^n - 1), T) = \{n-\text{th roots of unity in } T\}.$$
So the multiplicative group structures make μ_n a group scheme.

4. **Constant group schemes**. For a finite group Γ, let R^Γ be a direct product of $|\Gamma|$ copies of R. We call $\operatorname{Spec} R^\Gamma$ the *constant group scheme* associated with Γ, denoted also as Γ (or Γ_R). For an R-algebra T, $\operatorname{Spec} T$ is divided into connected components, so $T = \prod_i T_i$ where the only idempotents in T_i are 0 and 1. So,
$$\operatorname{Hom}_{R-\mathrm{alg}}(R^\Gamma, T) = \prod_i \operatorname{Hom}_{R-\mathrm{alg}}(R^\Gamma, T_i),$$
and for each i, an R-algebra homomorphism $R^\Gamma \to T_i$ is completely determined by choosing which direct factor R embeds into T; if one is chosen, the other factors should collapse in T. Thus, $\operatorname{Hom}_{R-\mathrm{alg}}(R^\Gamma, T_i) = \Gamma$. The natural group structure on $\operatorname{Hom}_{R-\mathrm{alg}}(R^\Gamma, T) = \prod_i \operatorname{Hom}_{R-\mathrm{alg}}(R^\Gamma, T_i) = \prod_i \Gamma$ is that induced from Γ.

5. **Diagonalizable group schemes**. For an abelian group Γ, let $R[\Gamma] = \oplus_{\gamma \in \Gamma} R\gamma$ be the group algebra of Γ over R. We call $\operatorname{Spec} R[\Gamma]$ the *diagonalizable group scheme* associated with Γ, denoted as $D(\Gamma)$. Note that, for an R-algebra T,
$$\operatorname{Hom}_{R-\mathrm{alg}}(R[\Gamma], T) = \operatorname{Hom}(\Gamma, T^\times),$$
the set of group homomorphisms from Γ to $T^\times$. The multiplicative group structure of $T^\times$ thus gives a natural group structure on $(\operatorname{Spec} R[\Gamma])(T)$. Note that $\operatorname{Spec} R[\mathbb{Z}] = \mathbb{G}_m$, whereas $\operatorname{Spec} R[\mathbb{Z}/n\mathbb{Z}] = \mu_n$.

[1] This is just another way of saying that every scheme is built up from affine schemes, e.g. [EH, Proposition VI-2].

The notions of *a subgroup scheme and a group scheme homomorphism* can be defined neatly in the same way by using the functor of points approach. Moreover, given a homomorphism $\varphi : G \to G'$ of S-group schemes, the functor $H : T \mapsto \ker(G(T) \xrightarrow{\varphi(T)} G'(T))$ is representable, as it can be also thought as a fiber product of $\varphi : G \to G'$ and the identity section $e_{G'} : S \to G'$. This defines the *kernel* of a homomorphism of group schemes. On the other hand, given a homomorphism $\varphi : G \to G'$ of S-group schemes, the functor $T \mapsto \mathrm{coker}(\varphi(T)) = G'(T)/\varphi(G(T))$ is in general not representable. The formation of quotient in certain cases will be discussed later.

1.2.1.2 Finite Flat Group Schemes

Over a locally noetherian base scheme S, an S-scheme G is *finite and flat* over S if and only if $\mathcal{O}_X$ is locally free of finite rank as $\mathcal{O}_S$-module. For an affine noetherian base $S = \operatorname{Spec} R$, a finite flat R-scheme G is an affine scheme $\operatorname{Spec} A$ where A is locally free of finite rank as R-module. A finite flat scheme is *of rank n (or order n)* if A is locally free of rank n as R-module. For a general base, this can be also defined as the rank of $\mathcal{O}_G$ as $\mathcal{O}_S$-module.

Remark 1.2.1. For a general base S, the category of finite flat group schemes over S is just a *pre-abelian category* (i.e. an additive category with kernels and cokernels), not necessarily an abelian category. This kind of problem is inherent in all kinds of categories of *schemes*; recall that in a general category of schemes, there are no "quotient schemes." On the other hand, the whole yoga of *topos* says that you need to think an object as a representable sheaf on a site. Thus, the "right way" to think of finite flat S-group schemes is to regard it as a *representable object in the category of sheaves over the (big) fppf (=finitely presented and faithfully flat, "fidèlement plate de présentation finie") site of S*. Such category of sheaves is an abelian category with enough injectives, so we can perform homological algebra in this larger category. One way to go back to the category of finite flat S-group schemes is via *faithful flat descent*, which basically says that *a sheaf is representable if and only if it is locally representable.* The meaning of this remark will be a bit clearer as we will introduce the notion of sites in the preliminaries section of the second chapter.

For a finite flat *commutative* group scheme $G = \operatorname{Spec} A$ over $S = \operatorname{Spec} R$, let $A^D = \operatorname{Hom}_R(A, R)$. This is also an R-module. Then, by dualizing everything, A^D becomes an R-Hopf algebra, which is also finite and flat over R. The finite flat group scheme $G^D = \operatorname{Spec} A^D$ is called the *(Cartier) dual group scheme.* It is the dual of G in the sense that, for any R-algebra T,

$$G^D(T) = \operatorname{Hom}_T(G_T, \mathbb{G}_{m,T}),$$

where G_T is the base change of G to T, and $\mathbb{G}_{m,T}$ is defined over T. This is called *the Cartier duality* (cf. [Tat1, (3.8)]). The most basic examples are the duality between constant group schemes and diagonalizable group schemes; if Γ is a commutative group, the Cartier dual of Γ_S is $D(\Gamma)_S$, and vice versa.

The Cartier duality is crucial in proving that, for a finite flat commutative group scheme, the order kills the group.

Theorem 1.2.1 (Deligne)**.** *If $G = \operatorname{Spec} A$ is a finite flat commutative group scheme over R of rank n, then repeating the group law n times gives a zero map, i.e. the multiplication by n map*[2] *$[n] : G \to G$ factors through the identity map* $\operatorname{Spec} R \to G$.

[2] This is a group homomorphism as G is commutative. This map, especially its kernel, plays a crucial role.

Proof. As A is flat over R, we can verify the annihilation over the localizations of R. Thus, we can assume that R is local, so that A becomes free over R.

We can identify the subgroup $G(R) = \mathrm{Hom}_{R-\mathrm{alg}}(A, R) \subset \mathrm{Hom}_{R-\mathrm{mod}}(A, R) = A^D$ as the group of *group-like elements* of A^D, that is, the group of elements $\lambda \in (A^D)^\times$ such that the comultiplication of A^D (which is the dual of the multiplicative structure of A) sends λ to $\lambda \otimes \lambda$. Namely, an element $\lambda \in A^D$ is group-like if and only if it is invertible in A^D and the corresponding map $\lambda : A \to R$ is multiplicative. Note that the formation of dual Hopf algebra and the identifiaction of group-like elements are compatible with base change. Thus it is sufficient to show that $\lambda^n = 1$ for all $\lambda \in G(R) \subset A^D$.

Let $\tau_\lambda : A \to A$ be the transpose of right multiplication by λ, which is an R-automorphism of A. Let $\tau = \mathrm{id}_{A^D} \otimes \tau_\lambda : A^D \otimes_R A \to A^D \otimes_R A$ be an A-automorphism of $A^D \otimes_R A$. As $A^D \otimes A$ is a free A-module, for an A-automorphism of $A^D \otimes_R A$, we can think of the determinant $\det : \mathrm{Aut}_A(A^D \otimes_R A) \to A$. As τ_λ is originally an R-automorphism of A, τ does not change the determinant. Thus, $\det(\mathrm{id}_A) = \det(\tau(\mathrm{id}_A))$. However, as $\tau(\mathrm{id}_A) = \lambda\,\mathrm{id}_A$, we have $\det(\mathrm{id}_A) = \det(\lambda)\det(\mathrm{id}_A) = \lambda^n \det(\mathrm{id}_A)$. As $\det(\mathrm{id}_A)$ is invertible, $\lambda^n = 1$, as desired. □

1.2.1.3 Kähler Differentials on Affine Group Schemes

For an affine R-group scheme $G = \mathrm{Spec}\, A$, the kernel of the counit $\widetilde{e} : A \to R$ is called the *augmentation ideal*. As the canonical map $R \to A$ splits the counit, we have $A = R \oplus I$ as an R-module. Therefore, for $f \in I$, $\widetilde{m}(f) - f \otimes 1 - 1 \otimes f \in I \otimes I$.

In terms of the augmentation ideal, we can describe the module of *Kähler differentials* and a universal derivation. Recall that, for an A-module M, a *derivation* is an R-linear map $D : A \to M$ such that it satisfies the Leibniz rule, i.e. $D(ab) = aD(b) + bD(a)$. The set of all derivations $A \to M$ is denoted as $\mathrm{Der}_R(A, M)$. Then, there exists a univeral object $\Omega^1_{A/R}$, *the module of Kähler differentials*, such that $\mathrm{Der}_R(A, M) \cong \mathrm{Hom}_A(\Omega^1_{A/R}, M)$ for all A-modules M [Mat, §26]. A *universal derivation* is a derivation $A \to \Omega^1_{A/R}$ corresponding to the identity map of $\Omega^1_{A/R}$. Note that, as $A = R \oplus I$, we have a map $A \to I/I^2$ which first kills $R \subset A$ and then mods out by I^2.

Proposition 1.2.1 [Tat1, (2.11)]. *Let M be an A-module, and $\psi : M \otimes_R A \to M$ be the map giving the action of A on M. The map $\lambda \mapsto \psi \circ ((\lambda \circ \pi) \otimes \mathrm{id}_A) \circ \widetilde{m}$ is an isomorphisim from $\mathrm{Hom}_{R-\mathrm{mod}}(I/I^2, M)$ to $\mathrm{Der}_R(A, M)$. In particular, $\Omega^1_{A/R} \cong (I/I^2) \otimes_R A$, and $(\pi \circ \mathrm{id}_A) \circ \widetilde{m} : A \to (I/I^2) \otimes_R A$ is a universal R-linear derivation for A.*

Proof. We will only prove the case when A is finitely generated. However, the same proof can be justified to work for general A. Note that, if we denote $J = \ker(m : A \otimes_R A \to A)$, the kernel of multiplication, then $A \otimes_R (I/I^2) \cong J/J^2$ as A-modules. So it is sufficient to prove that $\Omega^1_{A/R} \cong J/J^2$ as A-modules. Suppose $A = R[x_1, \cdots, x_n]/\langle f_i(x)\rangle_i$. Then, the multiplication map can be seen as $R[x_1, \cdots, x_n, y_1, \cdots, y_n]/\langle f_i(x), f_i(y)\rangle_i \to R[t_1, \cdots, t_n]/\langle f_i(t)\rangle_i$, sending $x_i, y_i \mapsto t_i$. Thus, $\ker m$ is generated by $\epsilon_i := y_i - x_i$'s. Then $A \otimes_R A = k[x_1, \cdots, x_n, \epsilon_1, \cdots, \epsilon_n]/\langle f_i(x), f_i(x+\epsilon)\rangle_i$, so $J/J^2 = \oplus_i A\epsilon_i/\langle \sum_k \frac{\partial f_j}{\partial x_k}\epsilon_k\rangle_j$, which is isomorphic to $\Omega^1_{A/R}$. □

1.2.1.4 Finite Étale Group Schemes

A finite flat S-group scheme G is *étale* if the structure map $G \to S$ is étale. There are several equivalent ways of defining étaleness for a finite flat S-group scheme G.

- G is étale if $\Omega^1_{G/S} = 0$.

- G is étale if for each point $s \in S$, the fiber G_s is the spectrum of a finite product of separable extensions of the residue field $\kappa(s)$.
- G is étale if for each point $s \in S$, the fiber G_s is geometrically reduced.

It turns out that, at least over a connected noetherian affine base $S = \operatorname{Spec} R$, the category of finite étale R-group schemes is an *abelian full subcategory* of the category of finite flat R-group schemes. This is achieved via the equivalence of categories

$$\{\text{finite étale } R\text{-group schemes}\} \xrightarrow{\sim} \{\text{finite groups with continuous } \pi_{1,\text{ét}}(S,s)\text{-action}\}$$

([SGA1, Exposé V], [Dem, II.2]), where $\pi_{1,\text{ét}}(S,s)$ is the *étale fundamental group* of S for a choice of a geometric point $s \in S$. Note that the category of finite flat R-group schemes is not in general abelian as quotients may fail to exist.

Example 1.2.2.

1. Over a field k, a finite étale k-algebra is a finite product of finite separable extensions of k.
2. Over a characteristic zero complete discrete valuation ring R with residue field k, it turns out that the reduction to the special fiber $X \to X_k$ is an equivalence of categories from the category of finite étale R-schemes to the category of finite étale k-schemes. A quasi-inverse is constructed via Witt vectors.

It is worth noting that étaleness comes free over a field of characteristic zero:

Theorem 1.2.2 (Cartier)**.** *If G is a finite (flat) group scheme over a field k of characteristic zero, then G is étale.*

Proof. Let $G = \operatorname{Spec} A$, and I be the augmentation ideal of A. Let $x_1, \cdots, x_n$ be a k-basis for I/I^2. Let $J = \cap_n I^n$. As a field is Artinian, $A = \prod_i A_i$ for local algebras A_i's, and maximal ideals $\mathfrak{m}_i$'s are nilpotent. Thus, taking high powers of an ideal in each component will either vanish or remain to be the unit ideal. Thus, J is a direct factor of A as an k-algebra, which means that A/J is a direct factor of A, implying that $\Omega^1_{(A/J)/k}$ is a direct factor of $\Omega^1_{A/k}$. As $\Omega^1_{A/k} \cong A \otimes_k I/I^2 \cong \oplus A dx_i$, it follows that $\Omega^1_{(A/J)/k} \cong \oplus (A/J) dx_i$, as A/J is a direct factor of A. Note however that we have $A/J \cong k[x_1, \cdots, x_n]/(f_1, \cdots, f_m)$, as $A/J = \varprojlim A/I^n$. Thus, $\Omega^1_{(A/J)/k} \cong \oplus (A/J) dx_i / (\sum_j (\partial f_1/\partial x_j) dx_j, \cdots, \sum_j (\partial f_m/\partial x_j) dx_j)$. This means that $\frac{\partial f_i}{\partial x_j} = 0$ for all i, j. As $\operatorname{char} k = 0$, this implies that f_i's are zero. Thus, $A/J \cong k[x_1, \cdots, x_n]$. As A/J is finite over k, it follows that $n = 0$, or $I/I^2 = 0$. This implies that $\Omega^1_{A/k} = 0$, or that A is étale. □

1.2.1.5 Quotients, Cokernels and Exact Sequences

A *right group action* of an S-group scheme G on an S-scheme X is a morphism $a : X \times_S G \to X$ which, as a functor of points, defines a group action of $G(T)$ on $X(T)$ for every S-scheme T. With a right G-action on X, an S-morphism $f : X \to Y$ is called to be *constant on orbits* if $f \circ a = f \circ \mathrm{pr}_1$, i.e. $f(xg) = f(x)$ for all $x \in X(T), g \in G(T)$ for all S-schemes T. We define the *quotient of X by G* to be the initial object (if exists) of the category of S-morphisms $X \to Z$ which are constant on orbits. We denote the quotient as $u : X \to X/H$, if exists.

A group action is *strictly free* if the morphism

$$(\mathrm{id}, a) : X \times_S G \to X \times_S X$$

is a closed immersion.

Theorem 1.2.3 (Grothendieck, [Tat1, Theorem 3.4])**.** *Suppose that S is a locally noetherian base scheme, G is a finite flat group scheme over S and X is a finite type S-scheme with a strictly free G-action. Suppose further that every G-orbit of a closed point is contained in an affine open set. Then the quotient $u : X \to X/G$ exists, and has the following properties.*

(i) $u : X \to X/G$ is finite flat, and its degree is the order of G.

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

(iii) If $S = \operatorname{Spec} R, G = \operatorname{Spec} A, X = \operatorname{Spec} B$ are affine, then $X/G = \operatorname{Spec} B_0$, where B_0 is the equalizer of the two homomorphisms $\widetilde{\mathrm{pr}_1}, \widetilde{a} : B \to B \otimes_R A$.

Remark 1.2.2. The condition that every G-orbit is contained in an affine open set is satisfied if, for example, $S = \operatorname{Spec} k$ is the spectrum of an infinite field and X is a quasiprojective variety. This is because, for any finite set of closed points in $\mathbb{P}^n_k$, there is a hyperplane that does not pass through any of them. This will later apply to the case when X is an abelian variety over a local/global field k.

Remark 1.2.3. It is not the group action but rather the *equivalence relation* $\mathcal{R} \subset X \times_R X$ that makes the quotient work. An equivalence relation is a subscheme of $X \times_R X$ which satisfies the reflexivity, symmetry and transitivity conditions. A *finite flat equivalence relation* is an equivalence relation $\mathcal{R} \subset X \times_R X$ such that the projection maps $\mathrm{pr}_i : \mathcal{R} \to X$ are finite flat. Then, what is rather proved in [SGA3-1, Exposé V] is that, for a noetherian ring R and an affine finite type R-scheme X, *if $\mathcal{R}$ is a finite flat equivalence relation, then the sheafification of the presheaf $T \mapsto (X(T) \times X(T))/\mathcal{R}(T)$ on the* fppf topology *of R is representable.* The heart of the proof is the faithfully flat descent.

Now consider the case when $S = \operatorname{Spec} R$ is noetherian, G is an affine R-group scheme and H is a finite flat closed normal R-subgroup scheme of G. Then, Theorem 1.2.3 tells us that G/H *exists as an affine R-group scheme, and $G \to G/H$ is finite and faithfully flat; if G is finite (resp. finite flat) over R, then G/H is finite (resp. finite flat) over R*[3]. In particular, using the Cartier duality, we obtain the following.

Theorem 1.2.4 [Dem, II.6]**.** *The category of finite flat commutative group schemes over a field k is an abelian category.*

Proof. Let $\varphi : G \to H$ be a group homomorphism of finite flat commutative group schemes over k. As every k-module is flat, a closed subgroup of a finite flat group scheme over k is automatically finite flat. Thus we know that kernels and cokernels of φ exist. Also, the natural map $\mathrm{coim}(\varphi) \to \mathrm{im}(\varphi)$ is injective and surjective. Thus, it is sufficient to show that a bijective homomorphism of finite flat commutative k-group schemes $\phi : \operatorname{Spec} A \to \operatorname{Spec} B$ is an isomorphism. As the order of $\operatorname{Spec} B$ is equal to the order of $\phi(\operatorname{Spec} A)$, we have $\dim_k B = \dim_k \phi^* B$. Thus $\phi^* : B \to A$ is injective. This means that the Cartier dual $\phi^D : \operatorname{Spec} B^D \to \operatorname{Spec} A^D$ is a closed immersion with a cokernel Q. Applying the Cartier duality again, the composition $Q^D \to \operatorname{Spec} A \to \operatorname{Spec} B$ is zero. Thus, $Q^D \to \operatorname{Spec} A$, thereby $\operatorname{Spec} A^D \to Q$, is zero. Thus, $Q = 1$, which means that $\phi^{D*} : A^D \to B^D$ is injective. Thus, ϕ is a bijective k-algebra homomorphism, thus an isomorphism. $\square$

Now that we have defined cokernels, we would like to define what it means to be an exact sequence of group schemes. We define a complex of group schemes over a base to be exact if *it is exact as a complex of sheaves on the fppf topology of the base.* Over a noetherian ring R, a sequence $1 \to G' \xrightarrow{i} G \xrightarrow{\pi} G'' \to 1$ of affine R-group schemes is exact if and only if π is *faithfully*

[3]A morphism is faithfully flat if it is flat and surjective.

flat and $i : G' \to G$ is the kernel of π. It is also equivalent to that i is a closed immersion with $i(G')$ a normal subgroup of G, and $\pi : G \to G''$ is identified with the cokernel of $i : G' \to G$.

We end this discussion with the following proposition.

Proposition 1.2.2. *Over a noetherian ring R, the Cartier dual of a short exact sequence of finite flat commutative group schemes is again exact.*

Proof. Let $1 \to G' \xrightarrow{i} G \xrightarrow{\pi} G'' \to 1$ be the short exact sequence of finite flat commutative R-group schemes. Note that the short exact sequence remains exact after an arbitrary base change. Thus, for each R-algebra T, the natural map

$$\ker(G^D \to G'^D)(T) = \ker(\mathrm{Hom}(G_T, \mathbb{G}_m) \xrightarrow{i^*} \mathrm{Hom}(G'_T, \mathbb{G}_m)) \xrightarrow{\pi^D} (G''_T, \mathbb{G}_m) = G''^D(T)$$

is an isomorphism because of the universal property of quotient. Therefore, the Cartier dual of a cokernel is a kernel.

It is thus sufficient to show that $i^D : G^D \to G'^D$ is the cokernel of $\pi^D : G''^D \to G^D$. A priori we know that there is a finite flat cokernel G^D/G''^D, and the universal property of quotient gives a map $G^D/G''^D \to G'^D$. We have already observed that the Cartier dual of a cokernel is a kernel. Thus, the map $G^D/G''^D \to G'^D$ is the Cartier dual of the map $G' \to \ker(G \to G'')$, which is an isomorphism. Thus, $G^D/G''^D \to G'^D$ is an isomorphism, so i^D is the cokernel of π^D, as desired. □

1.2.1.6 Classification of Finite Flat Group Schemes

For a group scheme G, we define G^0 be the open and closed subscheme of G corresponding to the connected component of G containing the unit section. This in general may not be a subgroup scheme of G. However, over a *henselian local ring*, i.e. a ring that satisfies Hensel's lemma, G^0 is indeed a subgroup scheme, and, even more, the quotient also has a nice description.

Proposition 1.2.3 [Tat1, (3.7)]**.** *Let $(R, \mathfrak{m})$ be a henselian local ring (e.g. a field or a complete discrete valuation ring). Let G be a finite flat R-group scheme. Then the following are true.*

(i) G^0 is the spectrum of a henselian local R-algebra with the same residue field as R, and is a flat closed normal subgroup scheme of G.

(ii) The quotient $G^{\text{ét}} := G/G^0$ is a finite étale R-group scheme. The exact sequence

$$0 \to G^0 \to G \to G^{\text{ét}} \to 0,$$

called the connected-étale sequence for G, *is characterized by that every group homomorphism $\varphi : G \to H$ to a finite étale R-group scheme H factors uniquely through $G \to G^{\text{ét}}$.*

(iii) The functors $G \mapsto G^0, G \mapsto G^{\text{ét}}$ on the category of finite flat R-group schemes are exact.

(iv) If R is a perfect field, the composition $G_{\text{red}} \hookrightarrow G \to G^{\text{ét}}$ is an isomorphism, so the connected-étale sequence splits canonically.

Proof. Note that, if $G = \operatorname{Spec} A$, then as R is henselian, $A = \prod_{i=1} A_i$ with each A_i a local henselian ring, and each $\operatorname{Spec} A_i$ corresponds to a connected component of G. Without loss of generality, suppose $G^0 = \operatorname{Spec} A_1$. As it contains the image of the unit section, the residue field of A_1 must be $k = R/\mathfrak{m}$. Thus $G^0 \times_R \operatorname{Spec} A_i$ is connected. This implies that the multiplication and the inverse morphisms send G^0 to G^0. Also, each A_i is flat over R, so this implies (i).

As G is finite flat, the quotient $G^{\text{ét}}$ is automatically finite flat. Also, the image of the identity section is $\operatorname{Spec} R = G^0/G^0$, and this is open as $G^0 \subset G$ is open. Let $G^{\text{ét}} = \operatorname{Spec} A^{\text{ét}}$, and let $I^{\text{ét}}$ be the augmentation ideal of $A^{\text{ét}}$. Then, this means that the complement of $\operatorname{Spec}(A^{\text{ét}}/I^{\text{ét}})$ is closed, which implies that I is a direct factor of A, or $I^{\text{ét}} = (I^{\text{ét}})^2$, so $G^{\text{ét}}$ is étale. As the identity component of an étale R-group scheme is just $\operatorname{Spec} R$, any homomorphism from a connected R-group scheme to an étale R-group scheme is trivial. This finishes (ii).

For (iii), note that, given an exact sequence $1 \to G' \xrightarrow{i} G \xrightarrow{\pi} G'' \to 1$, the restriction $\pi|_{G^0} : G^0 \to G''^0$ is faithfully flat, as it is the pullback of faithfully flat π by $G''^0 \to G''$. Also, it is evident that $\ker(\pi|_{G^0}) = G'^0$, as it is connected. Thus, $G \mapsto G^0$ is an exact functor. Fron this, abstract nonsense gives the exactness of $G \mapsto G^{\text{ét}}$.

For (iv), as the residue fields are perfect, taking the reduced subscheme is compatible with products. Note also that a scheme over a field is étale iff it is geometrically reduced. Thus, $G_{\text{red}} \to G^{\text{ét}}$ is an isomorphism after a base change to $\overline{k}$, which implies that $G_{\text{red}} \to G^{\text{ét}}$ is an isomorphism, via faithfully flat descent. □

Recall that a characteristic $p > 0$ scheme G has the *relative Frobenius* $F : G \to G^{(p)}$, where $G^{(p)}$ is the pullback of G by the absolute Frobenius of the base scheme. Using Frobenius, we can classify finite flat group schemes over a perfect field of characteristic p.

Theorem 1.2.5 (e.g. [Sc2]). *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*

$$A \cong k[x_1, \cdots, x_r]/(x_1^{p^{e_1}}, \cdots, x_r^{p^{e_r}}),$$

for some $r \in \mathbb{N}$ and $e_1, \cdots, e_r \in \mathbb{N}$. These are well-defined invariants of G up to permutation of e_i's.

Proof sketch. Note that G has a finite *Frobenius height*, which means that the composition $G \to G^{(p)} \to G^{(p^2)} \to \cdots \to G^{(p^n)}$ of relative Forbenii is zero for some finite $n > 0$. We can then use an induction on Frobenius heights. The base case $n = 1$ and the induction step both proceed as the proof of Cartier's theorem, with a bit more careful look at coefficients of formal derivatives. □

This has a number of consequences.

Proposition 1.2.4. *(i) The order of a connected finite flat group scheme over a field of characteristic p is a power of p.*

(ii) A finite flat group scheme of order invertible in the base is étale.

(iii) Let $(R, \mathfrak{m})$ be a complete discrete valuation ring with a perfect residue field k of characteristic p. Then a finite flat connected group scheme $G = \operatorname{Spec} A$ over R satisfies

$$A \cong R[[x_1, \cdots, x_n]]/(f_1, \cdots, f_n),$$

so that for each $1 \le i \le n$, there exists $e_i \in \mathbb{N}$ such that $f_i - x_i^{p^{e_i}} \in \mathfrak{m}R[x_1, \cdots, x_n]$ is a polynomial of degree $< p^{e_i}$ with respect to x_i.

Proof. (i) A connected group scheme over a field is geometrically connected via faithfully flat descent, so it follows from Theorem 1.2.5.

(ii) As we can check étaleness fiber by fiber, we can assume that the base is a field. Cartier's theorem (Theorem 1.2.2) deals with the case when the base is of characteristic 0. If the base is of characteristic $p > 0$, by (i), the order being invertible implies that the connected component is actually trivial. By the connected-étale exact sequence, the group is étale.

(iii) As A is a complete local finite flat R-algebra, by Theorem 1.2.5,

$$A \otimes_R k = k[x_1, \cdots, x_n]/(x_1^{p^{e_1}}, \cdots, x_n^{p^{e_n}}).$$

By Nakayama, the lifts of x_i's will generate A as an R-algebra. Thus, $A \cong R[[x_1, \cdots, x_n]]/J$ for some ideal J. As A is R-free, we know that J is a direct factor of $R[[x_1, \cdots, x_n]]$. Thus, $J \otimes_R k = (x_1^{p^{e_1}}, \cdots, x_n^{p^{e_n}})$ is a direct factor of $k[[x_1, \cdots, x_n]]$. We can therefore lift $x_i^{p^{e_i}}$'s to J to get generators f_i's of J. As the monomials $\{x_1^{a_1} \cdots x_n^{a_n}\}_{0 \le a_i < p^{e_i}}$ generate A as an R-module, so we can pick f_i's so that $f_i - x_i^{p^{e_i}}$'s are polynomials of x_i-degree less than p^{e_i}. □

We record some results about classifying finite flat group schemes over a Dedekind domain, which is our main case of interest. In particular, these imply that we can see things locally.

Proposition 1.2.5. *For a finite flat group scheme G over a Dedekind domain R, the correspondence $H \mapsto H_K$ is a one-to-one correspondence between the set of closed flat R-subgroup schemes of G and the set of closed flat K-subgroup schemes of G_K.*

Proof. Let $G = \operatorname{Spec} A$. The inverse is given as follows. Suppose we are given a closed flat K-subgroup scheme of $G_K = \operatorname{Spec} A_K$, which just corresponds to a flat Hopf ideal $J \subset A_K$, i.e. $c(J) \subset A_K \otimes J + J \otimes A_K$, where c is the comultiplication. Then the inverse of this correspondence is given by $\operatorname{Spec} A_K/J \mapsto \operatorname{Spec} A/(J \cap A)$, using that $A \hookrightarrow A_K$. This is a flat ideal as flatness over R is the same as being torsion-free over R. □

Theorem 1.2.6 [Sc2, §5]**.** *Let R be a noetherian domain, and $p \in R$. Let $\widehat{R}$ be the completion of R with respect to the p-adic topology. Then, a finite flat R-group scheme G is completely determined by $G_{\widehat{R}}$, $G_{R[1/p]}$ and the isomorphism of these after base change to $\widehat{R}[1/p]$. To be more precise, the functor*

$$G \mapsto (G_{\widehat{R}}, G_{R[1/p]}, \mathrm{id}_{G_{\widehat{R}[1/p]}})$$

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 $\widehat{R}, R[1/p]$, respectively, and $\phi : (G_1)_{\widehat{R}[1/p]} \xrightarrow{\sim} (G_2)_{\widehat{R}[1/p]}$.

Proof sketch. It follows from the fact that $\widehat{R}$ and $R[1/p]$ are faithfully flat over R, and the functor

$$M \mapsto (M \otimes_R \widehat{R}, M \otimes_R R[1/p], \mathrm{id}_{M \otimes \widehat{R}[1/p]})$$

is an equivalence of categories from the category of finitely genreated R-modules to the category of triples (M_1, M_2, ϕ), where M_1, M_2 are finitely generated $\widehat{R}, R[1/p]$-module, respectively, and $\phi : M_1 \otimes_{\widehat{R}} \widehat{R}[1/p] \cong M_2 \otimes_{R[1/p]} \widehat{R}[1/p]$, which is an easy algebra. □

We now know quite well what finite étale group schemes and finite flat connected group schemes look like. We thus record some results about extensions of some finite flat group scheme by another finite flat group scheme. This will be useful since, given a finite flat group scheme, we proceed by first figuring out what simple objects in the given category are, and see how Jordan-Hölder composition series comes up with to form the full group via repeated group extensionos.

Proposition 1.2.6. *Let R be a henselian local ring.*

(i) An extension of a connected *finite flat R-group scheme by a* connected *finite flat R-group scheme is connected.*

(ii) An extension of a finite étale *R-group scheme by a finite* étale *R-group scheme is étale.*

(iii) An extension of a connected *finite flat R-group scheme by a finite* étale *R-group scheme is a trivial extension, i.e. the extension is a product of the two groups.*

Proof. (i) is immediate by taking an exact functor $G \mapsto G^{\text{ét}}$ to the connected-étale sequence to observe that the étale component is trivial, so the given group is connected. (ii) is also immediate by using $G \mapsto G^0$ instead. By the same reason, if G is an extension of a connected H by an étale H', then $H = G^0, H' = G^{\text{ét}}$. Thus a splitting and a retraction are given by the connected-étale sequence of G. □

It will be very nice if we can classify extensions via an analogue of Ext functor in homological algebra. Even though the category of finite flat group schemes is not very nice, we know that it embeds into a very nice abelian category, *the category of fppf sheaves*. On that category, we can certainly define the $\mathrm{Ext}^i(\cdot,\cdot)_{\mathrm{fppf}}$ functor, but we do not know yet if the functor Ext^1 really parametrizes extensions as *finite flat group schemes*, not as fppf sheaves.

Proposition 1.2.7. *In the category of fppf sheaves over a base scheme S, an extension of a representable sheaf by a representable sheaf is representable.*

Proof. We only need to show that the extension is locally representable [SGA1, Exposé VI]; it is another way of describing faithfully flat descent. However, an extension is split locally, so locally the extension is a product of the two representable sheaves, which is obviously representable. □

Thus, $\mathrm{Ext}^1_S(G,H)_{\mathrm{fppf}}$ for finite flat S-group schemes G, H really parametrizes extensions as finite flat S-group schemes. We can use the usual long exact sequences for Ext. We also have a local-global compatibility exact sequence, which is an analogue of Mayer-Vietoris exact sequence. From now on we drop the subscript fppf.

Theorem 1.2.7 (Mayer-Vietoris Exact Sequence, [Sc2, §5])**.** *Let G, H be p-power order finite flat group schemes over a noetherian ring R. Then,*

$$\begin{aligned} 0 \quad &\to \quad \mathrm{Hom}_R(G,H) \to \mathrm{Hom}_{\widehat{R}}(G,H) \times \mathrm{Hom}_{R[1/p]}(G,H) \to \mathrm{Hom}_{\widehat{R}[1/p]}(G,H) \\ &\xrightarrow{\delta} \quad \mathrm{Ext}^1_R(G,H) \to \mathrm{Ext}^1_{\widehat{R}}(G,H) \times \mathrm{Ext}^1_{R[1/p]}(G,H) \to \mathrm{Ext}_{\widehat{R}[1/p]}(G,H) \end{aligned}$$

is exact, where δ is defined by

$$\delta\alpha = ((G \times H)_{\widehat{R}}, (G \times H)_{R[1/p]}, \mathrm{id}_H \, \mathrm{id}_G + \alpha)$$

for $\alpha \in \mathrm{Hom}_{\widehat{R}[1/p]}(G,H)$.

1.2.1.7 Prolongations of Commutative p-Group Schemes

We are interested in how much the generic fiber of a finite flat group scheme determines the original group. The results of Raynaud ([R], [Tat1, §4], [Fo1, 3.1]) give us some control when the base ring is mildly ramified. Throughout this section, let R be a discrete valuation ring of mixed characteristic, K be its fraction field, π a uniformizer, k the residue field, p the residue characteristic, v the normalized valuation (so that $v(\pi) = 1$), and $e = v(p)$ the absolute ramification index.

Let $G_0 = \mathrm{Spec}(A_0)$ be a finite (flat) commutative K-group scheme. A finite flat R-group scheme G whose generic fiber G_K is isomorphic to G_0 is called *a prolongation of* G_0. In terms of R-algebras, a prolongation $G = \mathrm{Spec}\, A$ comes from a finite R-subalgebra A of A_0, which contains R and spans A_0 over K, such that the comultiplication $c : A_0 \to A_0 \otimes A_0$ sends $c(A) \subset A \otimes_R A$. By taking the Cartier dual, this is equivalent to that $A^D \supset A^D A^D$.

For two prolongations $G = \mathrm{Spec}\, A$ and $G' = \mathrm{Spec}\, A'$ of G_0, we write $G \geq G'$ if $A \supset A'$. Even though this is a partial order, any two prolongation has *a least upper bound and a greatest* *lower bound* [Tat1, Proposition 4.1.1]. This is because, for two prolongations $G = \operatorname{Spec} A$ and $G' = \operatorname{Spec} A'$, $\operatorname{Spec} AA'$ is also a prolongation, which is obviously a least upper bound, and a greatest lower bound is achieved via Cartier duality. This means that, if G_0 has a prolongation, *it has a maximal prolongation G^+ and a minimal prolongation G^-.*

The maximal and minimal prolongations G^+, G^- are somewhat more understandable than a general prolongation G. In particular, for certain cases, both will become *Raynaud F-module schemes*, which can be completely classified. Recall that, given a finite field F, a *Raynaud F-module scheme* is a finite flat F-module R-scheme[4]of the same order as F. We then specifically have the following.

Proposition 1.2.8 [Tat1, Proposition 4.3.2]**.** *Suppose that G_0 is a simple commutative K-group scheme of p-power order which admits a prolongation. Suppose further that R is strictly henselian (i.e. a henselian ring with separably closed residue field). Then,* $\operatorname{End}(G_0) = \operatorname{End}(G^+) = \operatorname{End}(G^-) =:$ *F is a finite field, and G_0, G^+, G^- are Raynaud F-module schemes.*

Proof sketch. As $\operatorname{Gal}(\overline{K}/K)$ acts on $G_0(\overline{K})$ through an abelian quotient group [Tat1, Lemma 4.3.1], $G_0(\overline{K})$ is a 1-dimensional vector space over the residue field of $\mathbb{Z}[\operatorname{Gal}(\overline{K}/K)]$, which we call F. This F has the same number of elements as $G_0(\overline{K})$, so it is necessarily finite, and $F = \operatorname{End}(G_0(\overline{K})) = \operatorname{End}(G_0)$. Thus G_0 is a Raynaud F-module scheme. Note also that an automorphism of G_0 extends to G^+ and G^- as they are unique up to isomorphism. As we can also construct the inverse by taking the generic fiber, we deduce that $\operatorname{End}(G_0) = \operatorname{End}(G^+) = \operatorname{End}(G^-)$. Thus, G^+ and G^- are F-module schemes over R. As the R-orders of G^+ and G^- are equal to the K-order of G_0, it follows that G^+, G^- are also Raynaud F-module schemes. □

If R has enough roots of unity, we can completely classify Raynaud F-module schemes over R, see for example [Tat1, Theorem 4.4.1]. Using this, we can partially answer the question we originally asked.

Theorem 1.2.8 ([R, 3.3], [Fo1, Théorème 2])**.** *Let R be a discrete valuation ring of mixed characteristic $(0, p)$, and let K be its fraction field. Suppose that $e < p - 1$.*

(i) A finite flat commutative K-group scheme killed by a power of p admits at most one finite flat prolongation over R. In other words, for a finite flat commutative R-group scheme G killed by a power of p, G is the unique prolongation of G_K.

(ii) The generic fiber functor from the category of finite flat commutative R-groups killed by a p-power to the category of finite flat commutative K-groups killed by a p-power is fully faithful, and its image is stable under taking sub-objects and quotients.

For a proof, a reader is advised to consult with [Tat1, §4] and [R, Paragraphe 3].

1.2.2 p-divisible Groups

1.2.2.1 Basic Definitions and Properties

Motivated from the construction of Tate modules of abelian varieties, we define the notion of p-divisible groups.

Definition 1.2.1 (p-divisible Group)**.** *For a prime p, an integer $h \geq 0$ and a scheme S, a* p-divisible group *of height h over S is a directed system $G = \{G_n\}$ of finite flat commutative group schemes over S such that each G_n is p^n-torsion of order p^{nh}, and each transition map $i_n : G_n \to G_{n+1}$ is the kernel of $[p^n] : G_{n+1} \to G_{n+1}$, for all $n \geq 1$.*

[4] F-module R-schemes are similarly defined as group schemes, via functor of points approach, i.e. R-schemes with compatible F-actions on functors of points.

A homomorphism $f : G \to H$ of p-divisible groups is a compatible collection of S-group scheme homomorphisms $f_n : G_n \to H_n$.

Example 1.2.3. 1. The simplest example is the *constant group* $\mathbb{Q}_p/\mathbb{Z}_p = (\mathbb{Z}/p^n\mathbb{Z})_n$ with standard inclusions.

2. The next simplest example is the *diagonalizable group* $\mu_{p^\infty} = (\mu_{p^n})_n$ with standard inclusions. This can also be constructed by taking p^n-torsions of the group scheme $\mathbb{G}_m$; it is therefore sometimes denoted as $\mathbb{G}_m(p)$.

3. A basic yet rich and important example is $(A[p^n])_{n\geq 1}$ for an abelian scheme A over S. This is denoted as $A(p)$. We will study this construction in detail with applications towards the theory of abelian varieties/schemes in Section 1.2.3.7.

Even though many applications of theory of p-divisible groups are geared towards to the theory of abelian varieties, we will only focus on algebraic preliminaries in this section. In particular, some are immediate from the theory of finite flat group schemes.

- In particular, for a p-divisible group $G = (G_n, i_n)$, the sequence

$$0 \to G_n \to G_{n+m} \xrightarrow{[p^n]} G_{n+m}$$

  is exact. This factors through the p^m-torsion of G_{n+m}, which is G_m. Therefore, we have a short exact sequence

$$0 \to G_n \to G_{n+m} \xrightarrow{[p^n]} G_m \to 0.$$

- **Connected-Étale Sequence**. Let R be a henselian local ring. Then the connected-étale sequence of finite flat group scheme over R extends to p-divisible groups. Namely, if $G = (G_n, i_n)$ is a p-divisible group over R, then $G^0 := (G_n^0, i_n)$ as well as $G^{\text{ét}} := (G_n^{\text{ét}}, i_n)$ forms a p-divisible group over R so that we have an exact sequence

$$0 \to G^0 \to G \to G^{\text{ét}} \to 0.$$

  This is true as the functors $G_n \mapsto G_n^{\text{ét}}$ and $G_n \mapsto G_n^0$ are exact. Using this notation, we say a p-divisible group G is *connected* (*étale*, resp.) if $G = G^0$ ($G = G^{\text{ét}}$, resp.).

- **Cartier Duality**. For a p-divisible group $G = (G_n, i_n)$ over a noetherian ring R, we can define the *Cartier dual* $G^D = (G_n^D, [p]^D)$. It is indeed a p-divisible group as

$$0 \to G_n^D \xrightarrow{[p]^D} G_{n+1}^D \xrightarrow{[p^n]^D} G_{n+1}^D$$

  is a dual of an exact sequence

$$G_{n+1} \xrightarrow{[p^n]} G_{n+1} \xrightarrow{[p]} G_n \to 0.$$

- **Relative Frobenius**. As for the scheme case, given a p-divisible group G, there is a relative Frobenius $F : G \to G^{(p)}$ with a p-divisible group $G^{(p)}$. Note that $[p] : G \to G$ factors through F via $G \xrightarrow{F} G^{(p)} \xrightarrow{V} G$, and $V : G^{(p)} \to G$ is called the *Verschiebung*.

- **Tate module**. Inspired from the theory of abelian varieties, we can try to define the *Tate module* of a p-divisible group over a field. Let G be a p-divisible group over a field K of characteristic different from p. Fix an algebraic closure $\overline{K}$ of K. The *Tate module* of G, $T(G)$, is a $\mathrm{Gal}(\overline{K}/K)$-module defined as

$$T(G) = \varprojlim_n G_n(\overline{K}),$$

where the limit is taken with respect to transition maps $[p] : G_{n+1} \to G_n$. As $(G_n)_K$ is étale by Proposition 1.2.4(ii), $T(G)$ is a $\mathbb{Z}_p$-module isomorphic to $\mathbb{Z}_p^h$, where h is the height of G.

More generally, over a connected base scheme S, with a choice of geometric point $\overline{s} \in S$, for a p-divisible group G over S, we can define the Tate module $T(G)$ as

$$T(G) = \varprojlim_n \mathcal{O}_{G_n, \overline{s}},$$

where the sheaves are over the étale topology of S. The Tate module is a continuous $\pi_{1,\text{ét}}(S, \overline{s})$-module, and its definition agrees with the above one when $S = \operatorname{Spec} K$. Moreover, if G is finite étale over S, then by the same reason $T(G)$ is a finite free $\mathbb{Z}_p$-module, with the rank equal to the height of G.

1.2.2.2 Formal Lie Groups

Let R be a complete noetherian local ring with residue field k of characteristic $p > 0$. We can classify connected p-divisible groups over R in terms of *formal Lie groups*.

Definition 1.2.2 (Formal Lie Group)**.** *An n-dimensional* formal Lie group Γ *over* R *is a homomorphism* $m : \mathscr{A} \to \mathscr{A} \widehat{\otimes}_R \mathscr{A}$, *where* $\mathscr{A} = R[[x_1, \cdots, x_n]]$ *and* $\widehat{\otimes}$ *is the completed tensor product with respect to the obvious adic topology, making* $\mathscr{A}$ *a Hopf algebra. More concretely,* f *satisfies the following axioms, for* $x, y, z \in \mathscr{A}$.
(i) $x = f(x, 0) = f(0, x)$.
(ii) $f(x, f(y, z)) = f(f(x, y), z)$.
(iii) $f(x, y) = f(y, x)$.

We denote $x * y$ for $f(x, y)$, and $[p](x) = x * \cdots * x$, x multiplied with itself p times. A formal Lie group Γ is said to be *divisible* if $[p] : \mathscr{A} \to \mathscr{A}$ is finite free.

For a divisible formal Lie group Γ, we can obtain a p-divisible group $\Gamma(p) = (\Gamma[p^m])_m$ where $\Gamma[p^m]$ is the *kernel* of $[p^m] : \Gamma \to \Gamma$; more concretely,

$$\Gamma[p^m] = \operatorname{Spec} A_m := \operatorname{Spec} \mathscr{A}/([p^m]x_1, \cdots, [p^m]x_n),$$

and the transition maps are natural inclusions. Note that, as A_m is local, $\Gamma(p)$ is a *connected* p-divisible group.

It turns out that this functor is an equivalence of categories.

Theorem 1.2.9 [Tat2, Proposition 1]**.** *Let* R *be a complete noetherian local ring with perfect residue field of characteristic* $p > 0$. *Then* $\Gamma \mapsto \Gamma(p)$ *is an equivalence of categories from the category of divisible formal Lie groups over* R *to the category of connected* p*-divisible groups over* R.

Proof. Let $\mathfrak{m}_R$ be the maximal ideal of R, and let $I = (x_1, \cdots, x_n)$ be the augmentation ideal of $\mathscr{A} = R[[x_1, \cdots, x_n]]$. Then the maximal ideal of $\mathscr{A}$ is $M = \mathfrak{m}_R\mathscr{A} + I$. Let $[p]$ also denote the corresponding R-algebra map $\mathscr{A} \to \mathscr{A}$. Note that, as $[p](x_i) = px_i (\operatorname{mod} I^2)$, it follows that $[p](I) \subset pI + I^2 \subset MI$, or $[p^n](I) \subset M^n I$. As each ideal $\mathfrak{m}_R^n\mathscr{A} + [p]^n(I)$ is open, it follows that they form a fundamental system of neighborhoods of 0 in the M-adic topology of $\mathscr{A}$. As $\mathscr{A}$ is M-adically complete, $\mathscr{A} = \varprojlim \mathscr{A}/[p^n](I)$. Thus, a formal Lie group Γ can be recovered from $\Gamma(p)$, which means that the functor is fully faithful.

Let k be the residue field of R. Let $\Gamma = (\Gamma_n = \mathrm{Spec}(A_n))$ be our connected p-divisible group. As A_n's form a projective system, letting $A = \varprojlim A_n$, the group laws of A_n's induce a group law on A, i.e. a homomorphisim $A \to A\widehat{\otimes}_R A$. Thus, it remains to show that A is isomorphic to $R[[x_1, \cdots, x_n]]$. We will show that the general case will follow from the case of $R = k$. Assuming the case $R = k$, we have a topological isomorphism $\overline{A} = \varprojlim \overline{A_n} \cong k[[x_1, \cdots, x_m]]$. Choose liftings $R[[x_1, \cdots, x_m]] \to A_n$ of the quotients $k[[x_1, \cdots, x_m]] \twoheadrightarrow \overline{A_n}$ so that they are compatible to each other. This is possible because A_n's are finite free R-modules and transition maps are surjective. Nakayama's lemma implies that the maps $R[[x_1, \cdots, x_m]] \to A_n$ is surjective. Thus, the natural map $R[[x_1, \cdots, x_m]] \xrightarrow{f} A$ is surjective as well. This is also split as A_n's are finite free R-modules with surjective transition maps, A is also a free R-module. Thus, $\ker(f) \otimes k = \ker(f \otimes k) = 0$, which by Nakayama again implies that $\ker(f) = 0$. Therefore, A is isomorphic to $R[[x_1, \cdots, x_m]]$.

Now it remains to prove the case $R = k$. Using the same notation as the above paragraph, we have $H_n = \ker(\Gamma \xrightarrow{F^n} \Gamma^{(p^n)}) = \mathrm{Spec}\, B_n$, the kernel of n-th repeated applications of (relative) Frobenius. It is a finite flat commutative group scheme over k with p-power torsion. Thus, $H_n \subset \Gamma_n$, and $\Gamma_n \subset H_{\log_p |\Gamma_n|}$ by Deligne's theorem, Theorem 1.2.1. Therefore, $A = \varprojlim A_n = \varprojlim B_n$, and its maximal ideal is $I = \varprojlim I_n$, where $I_n \subset B_n$ is the maximal ideal.

Let $x_1, \cdots, x_m$ be elements of I whose images form a k-basis of I_1/I_1^2. Note that as $H_1 = \ker(F : H_n \to H_n^{(p)})$, we have $I_n/I_n^2 \cong I_1/I_1^2$. Thus, $x_1, \cdots, x_m$ will also form a k-basis of I_n/I_n^2 for all $n \geq 1$. Consider the map

$$u_n : k[x_1, \cdots, x_m] \to B_n,$$

sending x_i to x_i. This is surjective by Nakayama, and the kernel contains $(x_1^{p^n}, \cdots, x_m^{p^n})$, as F^n kills $H_n = \mathrm{Spec}\, B_n$. Thus, we get a surjective homomorphism

$$u_n : k[x_1, \cdots, x_m]/(x_1^{p^n}, \cdots, x_m^{p^n}) \to B_n.$$

On the other hand, from the exact sequence

$$0 \to H_1 \to H_{n+1} \to H_n \to 0,$$

by induction, it follows that $|H_n| = |H_1|^n$, where $|H_n|$ denotes the order of H_n over k. The upshot is that H_1 is a connected finite flat k-group scheme over a perfect field of characteristic $p > 0$, with *Frobenius height 1.* Therefore, by Theorem 1.2.5, it follows that

$$B_1 \cong k[x_1, \cdots, x_m]/(x_1^p, \cdots, x_m^p).$$

Therefore, by considering the k-dimensions, we deduce that u_n's are isomorphisms. Passing to the limit, we get an isomorphism $k[[x_1, \cdots, x_m]] \to A$, as desired. □

With this equivalence in hand, we can define the *dimension* of a p-divisible group G over a complete noetherian local ring to be the dimension of the formal Lie group corresponding to G^0.

Proposition 1.2.9 [Tat2, Proposition 3]**.** *Let G be a p-divisible group over a complete noetherian local ring of height h. Then $h = \dim G + \dim G^D$.*

Proof. As $[p] = V \circ F$, we have a short exact sequence

$$0 \to \ker F \to \ker[p] \xrightarrow{F} \ker V \to 0.$$

Note that $\ker F \subset G^0$, so $\ker F$ coincides with the analogous map on a smooth formal group, which is a map $k[[x_1, \cdots, x_{\dim G}]] \to k[[x_1, \cdots, x_{\dim G}]]$ sending $x_i \mapsto x_i^p$. Thus, $|\ker F| = p^{\dim G}$. By Cartier duality, $|\ker V| = p^{\dim G^D}$. Finally, we know $|\ker[p]| = p^h$. Thus, $h = \dim G + \dim G^D$. □

1.2.2.3 Passage to Special Fibers, Generic Fibers and Tate Modules

Recall that the most important examples of p-divisible groups are those coming from abelian varieties. Thus, one is naturally interested in a classification and deformation of p-divisible groups. By the equivalence of categories we have seen in Section 1.2.1.4, we first note that étale p-divisible groups are classified by their Tate modules.

Proposition 1.2.10. *Over a connected scheme S, the functor $G \mapsto T(G)$ is an equivalence of categories from the category of étale p-divisible groups over S to the category of finite free $\mathbb{Z}_p$-modules with a continuous $\mathbb{Z}_p$-linear Galois action of $\pi_{1,\text{ét}}(S, \overline{s})$, where $\overline{s}$ is a fixed geometric point of S. In particular, if p is invertible on S, then $G \mapsto T(G)$ is an equivalence of categories from the category of p-divisible groups.*

Proof. All finite flat group schemes with p-power torsion over a field of characteristic $\neq p$ are étale by Proposition 1.2.4(ii), and étaleness is checked fiberwise, so the second assertion follows from the first assertion. The first statement is immediate via the equivalence of categories between the category of étale K-group schemes and the category of finite continuous $\pi_{1,\text{ét}}(S, \overline{s})$-modules (Section 1.2.1.4). □

This gives a nice connection to abelian varieties in terms of their p-divisible groups, which are purely algebraic. They are crucial in the deformation theory of abelian varieties and p-divisible groups. For example, a theorem of Serre-Tate [I, Corollaire A.1.3] says that liftings of abelian schemes over a nilpotent thickening are completely classified by the liftings of the corresponding p-divisible groups.

Also, this itself is a very useful tool in studying p-divisible groups algebraically, which is often complemented with the connected-étale sequence and the classification of connected p-divisible groups in terms of formal Lie groups. For example, as with the abelian schemes, we have the following property.

Proposition 1.2.11. *For a local noetherian ring $(R, \mathfrak{m})$ with residue field k of characteristic $p > 0$, the special fiber functor $G \mapsto G_k$ from the category of p-divisible groups over R to the category of p-divisible groups over k is faithful. Moreover, if R is henselian and k is a perfect field, then this functor is an equivalence of categories.*

Proof. We first deduce the second statement from the first statement. As we only need to show the essential surjectivity of the special fiber functor $G \mapsto G_k$, it is enough to show that, given a p-divisible group G_0 over k, there is a lift G over R. As k is perfect, by Proposition 1.2.3(iv), the connected-étale sequence is split, so that $G_0 = G_0^0 \times G_0^{\text{ét}}$. Recall that, for a henselian local ring R with residue field k, the functor $X \mapsto X \otimes_R k$ is an equivalence of categories from the category of finite étale R-schemes to the category of finite étale k-schemes. Thus, $G_0^{\text{ét}}$ has a (unique) lift to R, which is an étale p-divisible group over R. Thus, we can assume that G_0 is connected. On the other hand, by Theorem 1.2.9, we know that G_0 comes from a formal

Lie group Γ_0 over k. As R is henselian, one can lift the group law of the formal Lie group Γ_0 coefficient-wise to a formal Lie group Γ over R. Thus, $G_0 = \Gamma_0(p) = (\Gamma(p))_k$, as desired.

We now prove the first statement. Suppose G, H are p-divisible groups over R, and $f : G \to H$ is a morphism where $f_k : G_k \to H_k$ is a zero map. By the equivalence of categories for étale and connected p-divisible groups, Proposition 1.2.10 and Theorem 1.2.9, the proposition follows when G, H are both étale or when they are both connected. Thus, we only need to prove the two cases, when G is étale and H is connected, and when G is connected and H is étale. As there is only a trivial map from a connected finite flat group scheme to a finite étale group scheme, we can therefore assume that G is étale and H is connected.

We will inductively prove that $f \otimes_R R/\mathfrak{m}^k = 0$ for all $k \geq 1$. We already know $f \otimes_R R/\mathfrak{m} = 0$. For the induction step, it is sufficient to prove the following: *for an artin local ring* $(R, \mathfrak{m})$ *with an ideal* $I \subset R$ *with* $\mathfrak{m}I = 0$*, if* $f \otimes_R R/I = 0$*, then* $f = 0$. As the property of a map being zero can be checked over the strict henselization of R, we can assume that R is strictly henselian, so that G, an étale R-scheme, is constant. Thus, we can assume that $G = \mathbb{Q}_p/\mathbb{Z}_p$. Then, a map f corresponds to a sequence of p-power compatible elements in $\ker(H_n(R) \to H_n(R/I))$. Let $H_n = \operatorname{Spec} B_n$. As H is connected, we can think of B_n as the quotient of the formal power series ring $B = \varprojlim B_n$. As $I\mathfrak{m} = 0$, it follows that the kernel of each map $H_n(R) \to H_n(R/I)$ is killed by $[p]$. Thus, $f \circ [p] = 0$. As $[p]$ is an isogeny, it follows that $f = 0$. □

As the problem of integral models of abelian varieties is of great interest, we can also think of the analogous problem for p-divisible groups. The Tate's theorem in [Tat2] states that the generic fiber functor is fully faithful.

Theorem 1.2.10 (Tate, [Tat2, Theorem 4])**.** *Let R be a noetherian normal domain whose field of fractions K is of characteristic 0. Then, the generic fiber functor $G \mapsto G_K$ from the category of p-divisible groups over R to the category of p-divisible groups over K is fully faithful. In other words, for p-divisible groups G, H over R, the map*

$$\operatorname{Hom}_R(G, H) \to \operatorname{Hom}_K(G \otimes_R K, H \otimes_R K)$$

is bijective.

Proof sketch. One first proves that, given a p-divisible group Γ over R, any $\mathbb{Z}_p$-direct summand of $T(\Gamma)$ arises from a p-divisible subgroup of Γ. Then, given $f \in \operatorname{Hom}_K(G_K, H_K) = \operatorname{Hom}_{\operatorname{Gal}(\overline{K}/K)}(T(G), T(H))$, we construct the extension in $\operatorname{Hom}_R(G, H)$ via considering the graph of f in $T(G) \times T(H)$. The corresponding p-divisible group in $G \times H$ then in fact is the graph of an R-morphism $G \to H$. □

It is regarded as a starting point of p-adic Hodge theory; for example, one can deduce a Hodge-Tate decomposition for p-divisible groups [Tat2, Theorem 3] from this. The Hodge-Tate decomposition, and more generally p-adic Hodge theory, will be discussed in detail in the later sections.

We state the de Jong's generalization of the Tate's theorem over any base.

Theorem 1.2.11 (de Jong, [dJ, Corollary 1.2])**.** *Let R be a discrete valuation ring, and G, H be p-divisible groups over R. Let $K = \operatorname{Frac}(R)$. Then,*

$$\operatorname{Hom}_R(G, H) \to \operatorname{Hom}_K(G \otimes_R K, H \otimes_R K)$$

is bijective.

1.2.2.4 Deformation of p-divisible Groups

Grothendieck developed a theory of deformations of (truncated) p-divisible groups, which involves with the obstruction and classification of infinitesimal liftings of (truncated) p-divisible groups.

Remark 1.2.4. In a discussion of this kind of flavor, p-divisible groups are more often called *Barsotti-Tate groups*, following Grothendieck's terminology.

Definition 1.2.3 (n-Truncated p-divisible Group)**.** *An* n-truncated p-divisible group *(or n-truncated Barsotti-Tate groups) G over a base scheme S is an abelian sheaf on S_{fppf} which satisfies the following.*

1. *G is annihilated by p^n.*
2. *G is flat over the constant sheaf $\mathbb{Z}/p^n\mathbb{Z}$.*
3. *$G(1) := \ker[p]_G$ is finite locally free over S.*
4. *If $n = 1$, then $\ker V_{G_0} = \operatorname{im} F_{G_0}$, where V, F are the Verschiebung and the Frobenius morphisms respectively, and G_0 is the reduction of G modulo p (i.e. the closed subscheme defined by $p\mathcal{O}_G$).*

The deformation theory of finite flat group schemes of n-torsion is particularly nice.[5] Using it, Grothendieck gives the following result on infinitesimal lifting of (truncated) p-divisible groups.

Theorem 1.2.12 (Grothendieck, [I, Théorème 4.4])**.** *Let $n \geq 1$, p be a prime number and $i : S \to S'$ be a closed immersion defined by a nilpotent ideal. Suppose that S' is affine.*

(i) If G is an n-truncated p-divisible group over S, then there exists an n-truncated p-divisible group G' over S' extending G.

(ii) If H is a p-divisible group over S, then there exists a p-divisible group H' over S' extending G.

(iii) Let H be a p-divisible group over S, then every n-truncated p-divisible group G' over S' extending H_n comes from a p-divisible group H' over S' extending H, i.e. $G' = H'_n$. This lift is unique if $p^N\mathcal{O}_S = 0$ for some $N \geq 1$ and $S \subset S'$ is defined by a nilpotent ideal of level $\leq \frac{n}{N}$.

(iv) If S is the spectrum of a complete noetherian ring with perfect residue field, then for any n-truncated p-divisible group G over S, there exists a p-divisible group H over S such that $G = H_n$.

1.2.2.5 Classification of p-divisible Groups

We have observed that p-divisible groups are more or less classified by their Tate modules, over a base on which p is invertible. We will look at several cases where there is a very good alternative, which all started from the case when the base is $\operatorname{Spec} k$ for a perfect field k of characteristic p. This is due to Dieudonné, so the theory is sometimes called the *Dieudonné theory*. This line of thought is continued in Fontaine's study of filtered (ϕ, N)-modules and their relations to crystalline and semi-stable representations, which will be discussed in the next chapter.

For this section, we let k be a perfect field of characteristic $p > 0$, and let $W(k)$ be the ring of Witt vectors over k (see for example [Se, II.6] for the definition). Let $\varphi : W(k) \to W(k)$ be the absolute Frobenius, i.e. the automorphism lifting the p-power map on k.

[5] For a general statement on the obstruction of infinitesimal lifting of finite flat group schemes, see [I, Proposition 3.1].

Definition 1.2.4 (Dieudonné Ring). *The* Dieudonné ring *of k is the associative ring $\mathscr{D}_k = W(k)[F, V]$ subject to the relations $FV = VF = p$, $Fc = \varphi(c)F$ for $c \in W(k)$ and $cV = V\varphi(c)$ for $c \in W(k)$.*

Obvious from the definitions, F and V are defined to be analogous to the Frobenius and the Verschiebung maps, respectively. Note that a *left $\mathscr{D}_k$-module* is just a $W(k)$-module D with a φ-semilinear map $F : D \to D$ and a φ^{-1}-semilinear map $V : D \to D$ such that $FV = VF = [p]_D$. A left $\mathscr{D}_k$-module is called a *Dieudonné module*. It is the Dieudonné module that replaces the role of the Tate module. The main result in this case, applied for both finite flat commutative group schemes of p-power order and p-divisible groups, is summarized as follows.

Theorem 1.2.13 [BC, Theorem 7.2.4]. *There is an additive anti-equivalence of categories $G \mapsto \mathbf{D}(G)$ from the category of finite flat commutative k-group schemes of p-power order to the category of Dieudonné modules of finite $W(k)$-length, with the following properties.*

1. *The order of G is $p^{\ell_{W(k)}(\mathbf{D}(G))}$, where $\ell_{W(k)}(\mathbf{D}(G))$ is the $W(k)$-length of $\mathbf{D}(G)$.*
2. *If k'/k is an extension of perfect fields , then $W(k') \otimes_{W(k)} \mathbf{D}(G) \cong \mathbf{D}(G_{k'})$ naturally as left $\mathscr{D}_{k'}$-modules. In particular, for the absolute Frobenius map $\varphi : k \to k$, $\varphi^*(\mathbf{D}(G)) \cong \mathbf{D}(G^{(p)})$ as $W(k)$-modules.*
3. *The action of F on $\mathbf{D}(G)$ is described by the $W(k)$-linear map*
$$\varphi^*(\mathbf{D}(G)) \cong \mathbf{D}(G^{(p)}) \xrightarrow{\mathbf{D}(F_{G/k})} \mathbf{D}(G),$$
wherer $F_{G/k} : G \to G^{(p)}$ is the relative Frobenius. Moreover, G is connected if and only if F is nilpotent on $\mathbf{D}(G)$.
4. *The k-vector space $\mathbf{D}(G)/F\,\mathbf{D}(G)$ is canonically identified with the k-linear dual $t_G^\vee := \mathrm{Hom}_k(t_G, k)$ of the tangent space $t_G := \ker(G(k[\epsilon]/(\epsilon^2)) \to G(k))$. In particular, G is étale if and only if F is bijective on $\mathbf{D}(G)$.*

Theorem 1.2.14 [BC, Proposition 7.2.6]. *The functor $G \mapsto \mathbf{D}(G) := \varprojlim \mathbf{D}(G_n)$ is an anti-equivalence of categories from the category of p-divisible groups over k and the category of finite free $W(k)$-modules D equipped with a φ-semilinear map $F : D \to D$ such that $pD \subset F(D)$, with the following properties.*

1. *The height of G is the $W(k)$-rank of $\mathbf{D}(G)$.*
2. *The equivalence is compatible with any extension k'/k of perfect fields, in the sense of Theorem 1.2.13.*
3. *For $n \geq 1$, $\mathbf{D}(G_n) \cong \mathbf{D}(G)/(p^n)$, and this isomorphism is compatible with change in n.*

Similarly, on $W(k)$, a p-divisible group is classified by its Dieudonné module of the special fiber, plus some lifting data.

Definition 1.2.5 (Honda System). *A* Honda system *over $W(k)$ is a pair (M, L) of a finite free $W(k)$-module M and a $W(k)$-submodule L equipped with a φ-semilinear map $F : M \to M$ satisfying that $pM \subset F(M)$ and that $L/pL \to M/F(M)$ is an isomorphism. If F is topologically nilpotent, the Honda system is called* connected.

A finite Honda system *over $W(k)$ is a pair (M, L) consisting of a Dieudonné module M of finite $W(k)$-length and a $W(k)$-submodule L such that $V|_L : L \to M$ is injective and $L/pL \to M/F(M)$ is an isomorphism. If F is nilpotent, the finite Honda system is called* connected.

It turns out that it is the category of Honda systems that classifies the p-divisible groups over $W(k)$, which is due to Fontaine.

Theorem 1.2.15 [BC, Theorem 7.2.10]**.** *Let $p > 2$.*

(i) There is a natural anti-equivalence of categories $G \mapsto (\mathbf{D}(G_k), L(G))$ from the category of p-divisible groups over $W(k)$ to the category of Honda systems.

(ii) There is a natural anti-equivalence of categories $H \mapsto (\mathbf{D}(H_k), L(H))$ from the category of finite flat commutative group schemes of p-power order over $W(k)$ to the category of finite Honda systems.

(iii) The two anti-equivalences are compatible with a perfect residue field extension. Also, the two anti-equivalences are compatible to each other, in the sense that if G is a p-divisible group over $W(k)$, then $(\mathbf{D}((G_n)_k), L(G_n))$ is naturally identified with $(\mathbf{D}(G_k)/(p^n), L(G)/(p^n))$.

Moreover, the above results are true for $p = 2$ when we restrict ourselves to connected objects on both sides.

This can be subsequently generalized to the case of a perfect discrete valuation ring; in that case, p-divisible groups are classified by the *crystalline Dieudonné functor* (cf. [BBM, 3.3]). We will be subsequently observing that other p-adic Hodge theoretic objects (e.g. crystalline/semi-stable representations) can also be classified by (semi-)linear algebraic data. The development of crystalline Dieudonné theory in [BBM] relies crucially on the following beautiful theorem by Raynaud; we record it here as we will need the theorem for other purpose. The meaning of the theorem should be clear after we define the notion of abelian schemes.

Theorem 1.2.16 (Raynaud, [BBM, Théorème 3.1.1])**.** *Let G be a finite flat commutative group scheme over any base S. For every $x \in S$, there is a (Zariski) open neighborhood $U \subset S$ such that there is a closed U-immersion of G_U into some abelian scheme A_U over U.*

1.2.3 Abelian Varieties and Abelian Schemes

1.2.3.1 Rigidity and Commutativity

Over a base scheme S, an *abelian scheme* over S is an S-group scheme $A \to S$ which is smooth[6], proper with (geometrically) connected fibers[7]. If the base scheme $S = \operatorname{Spec} k$ is the spectrum of a field, we instead use the term *abelian variety*. Namely, we define an abelian variety over a field k to be a *smooth, connected, proper k-group scheme*, which is the usual definition of an abelian variety.

There are many basic results for abelian varieties that follow from only the definition of abelian varieties, including rigidity, commutativity, existence of the dual. We postpone the discussion of the dual abelian variety to the next section, as we will need to invoke some general facts about existence of Picard schemes.

Proposition 1.2.12 (Rigidity Lemma)**.** *Let X, Y be geometrically integral schemes of finite type over a field k, and Z be a separated k-scheme. Suppose that X is proper. Let $f : X \times_k Y \to Z$ be a k-morphism such that f evaluated at some geometric point $y_0 \in Y(\overline{k})$ is a constant morphism. Then, f is independent of X, i.e. there is a unique k-morphism $g : Y \to Z$ such that $f = g \circ \mathrm{pr}_2$, where $\mathrm{pr}_2 : X \times_k Y$ is the projection.*

Proof. Uniqueness is immediate, as $X \times_k Y \to Y$ is surjective and Y is reduced. By Galois descent, we can pass the problem to the separable closure k_s, or assume that $k = k_s$. An

[6] We differ the notion of smoothness from formal smoothness, i.e. we require a smooth morphism to be locally of finite presentation.

[7] There is a parenthesis since a geometrically connected group scheme over a field is automatically connected.

advantage here is that X is guaranteed to have a k-rational point, since, for example, X has a dense open (in particular, nonempty) smooth locus, a locally finite type scheme over a field has a very dense subset of closed points, and a smooth point over a field has a finite separable residue field extension (cf. [Stacks, Tag 04QM]). Pick $x_0 \in X(k)$, and let $g(y) = f(x_0, y)$. It is sufficient to show that $f = g \circ \mathrm{pr}_2$. By faithfully flat descent, we can extend the base field to $\overline{k}$. Suppose that $f(X \times \{y_0\}) = \{z_0\}$, which was the assumption. Pick an affine open $U \subset Z$ of z_0, then $W := X \times_k Y - f^{-1}(U)$ is closed. As X is proper, $\mathrm{pr}_2(W)$ is closed in Y, which does not contain y_0. Thus, $V = Y - \mathrm{pr}_2(W)$ is a nonempty open neighborhood of y_0. We know that f maps $X \times_k V$ into U. Since X is proper and U is affine, for any point $v_0 \in V$, $X \times_k \{v_0\}$ is a point, which means that $f|_{X \times_k V} = g \circ \mathrm{pr}_2|_{X \times_k V}$, namely they are identified on a dense open subset. As these two are maps from a reduced scheme to a separated scheme, $f = g \circ \mathrm{pr}_2$. □

Corollary 1.2.1. *Let A, A' be abelian varieties over a field k.*

(i) Any morphism of pointed k-varieties $f : (A, e) \to (A', e')$ is a homomorphism, where e, e' are the identity sections of A, A', respectively.

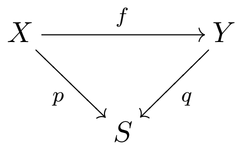
(ii) A is commutative.

Proof. (i) Consider the map $h : A \times_k A \to A'$ defined by $(a_1, a_2) \mapsto f(a_1, a_2) f(a_2)^{-1} f(a_1)^{-1}$. By Proposition 1.2.12, this is a constant map to e'.

(ii) Apply (i) to the inverse map of A. □

As we are also interested in the problem of reduction of abelian varieties, we will recall those basic properties in a more general setting of abelian schemes.

Proposition 1.2.13 (Rigidity Lemma, [MFK, Proposition 6.1])**.** *Given an S-morphism $f : X \to Y$, i.e. a commutative diagram*



suppose S is connected, p is flat, proper and $H^0(X_s, \mathcal{O}_{X_s}) = \kappa(s)$ for all $s \in S$. For a point $s \in S$, if $f(X_s)$ is consisted of one point, then there is a section $\eta : S \to Y$ of q such that $f = \eta \circ p$.

Proof sketch. As p is faithfully flat, we can extend the base to X and use the faithfully flat descent. On this base, $X \to S$ has a section, so we proceed like the proof of rigidity lemma over a field. □

Corollary 1.2.2. *Let A be an abelian scheme over a base scheme S.*

(i) For any S-group scheme G, an S-morphism $f : A \to G$ taking the identity to the identity is a homomorphism.

(ii) A is commutative.

Proof. (i) Apply the Rigidity Lemma, Proposition 1.2.13, to

$$(f \circ m_A, \mathrm{pr}_2) \cdot (f \circ m_A \circ (\mathrm{id}_A, e_A \circ p), \mathrm{id}_A)^{-1} : A \times_S A \to G \times_S A,$$

where $m_A : A \times_S A \to A$, $e_A : S \to A$ and $p : A \to S$ are the multiplication map, the identity section and the structure map of A, respectively, and $(-) \cdot (-), (-)^{-1}$ are from the group structure of the A-group scheme $G \times_S A$.

(ii) Apply (i) to the inverse map of A. □

1.2.3.2 Picard Schemes and Existence of Dual Abelian Schemes

Recall that the *Picard group* $\operatorname{Pic}(X)$ of a scheme X is the group of isomorphism classes of invertible sheaves on X. Its rigidified variant is often representable by a scheme or an algebraic space, and it is called the *Picard scheme*.

Definition 1.2.6 (Relative Picard Functor)**.** *For a separated finitely presented morphism $f : X \to S$, the* relative Picard functor $\operatorname{Pic}_{X/S}$, *from the category of locally Noetherian S-schemes to the category of abelian groups, is defined by*

$$\operatorname{Pic}_{X/S}(T) := \operatorname{Pic}(X_T)/\operatorname{Pic}(T).$$

The open subfunctor $\operatorname{Pic}^0_{X/S}$ of $\operatorname{Pic}_{X/S}$ is the subgroup of invertible sheaves having degree 0 on all geometric fibers. Equivalently, it is the subset of fiberwise algebraically trivial[8] *invertible sheaves.*

This is the rigidified variant of the Picard group by the following.

Lemma 1.2.1 [FGA, Lemma 9.2.9]**.** *Suppose that $f : X \to S$ has a section g. For an S-scheme T,*

$$\left\{\begin{matrix}\textit{isomorphism classes of } (\mathcal{L}, u) \textit{ where } \mathcal{L} \textit{ is an} \\ \textit{invertible sheaf on } X_T \textit{ and } u : \mathcal{O}_T \xrightarrow{\sim} g_T^*\mathcal{L} \textit{ is an isomorphism}\end{matrix}\right\} \to \operatorname{Pic}_{X/S}(T), \qquad (\mathcal{L}, u) \mapsto \mathcal{L}$$

is an isomorphism. Along this isomorphism, $\operatorname{Pic}^0_{X/S}$ corresponds to the pairs $(\mathcal{L}, u)$ with $\mathcal{L}$ having degree 0 on all (geometric) fibers.

It is shown that, if $f : X \to S$ is proper and flat, $\operatorname{Pic}_{X/S}$ is representable.

Theorem 1.2.17. *Let $f : X \to S$ be a flat, proper and finitely presented map.*

(i) (Grothendieck/Oort-Murre, [FGA, Corollary 9.4.18.3]) *If $S = \operatorname{Spec} k$ is the spectrum of a field k, and X is geometrically reduced, geometrically connected and $X(k) \neq \emptyset$, then $\operatorname{Pic}_{X/k}$ is represented by a locally finite type k-scheme, which is a disjoint union of quasiprojective open S-subschemes.*

(ii) (Artin, [FGA, Theorem 9.4.18.6]) *Assume that the formation of $f_*\mathcal{O}_X$ commutes with changing S; namely, for every $S' \to S$, we have $f'_*\mathcal{O}_{X'} = \mathcal{O}_{S'} \otimes_{\mathcal{O}_S} f_*\mathcal{O}_X$, where $X' = X \times_S S'$ and $f' : X' \to S'$ is the pullback of f. Then $\operatorname{Pic}_{X/S}$ is represented by an algebraic space locally of finite presentation over S.*

(iii) [BLR, Theorem 8.4.3] *If the formation of $f_*\mathcal{O}_X$ commutes with changing S and f has integral geometric fibers, then $\operatorname{Pic}_{X/S}$ is separated over S.*

We will not recall the precise definition of an algebraic space. Rather, we will just regard it as some kind of a generalized scheme. We define an *abelian algebraic space* over a base scheme S to be a *smooth, proper algebraic space over S with geometrically connected fibers.* Even though we don't really know what an algebraic space is, we can make this definition rigorous by using the functor of points approach, given that we already know that an algebraic space is locally of finite presentation. Namely, an algebraic space, locally of finite presentation over S, representing the functor $F : (\mathbf{Sch}/S) \to \mathbf{Sets}$ is an abelian algebraic space if,

[8] Two line bundles $\mathcal{L}_1, \mathcal{L}_2$ on a scheme X are *algebraically equivalent* if there exists a connected scheme T, two closed points $t_1, t_2 \in T$ and a line bundle $\mathcal{L}$ on $X \times T$ such that $\mathcal{L}_{X \times \{t_i\}} \cong \mathcal{L}_i$ for $i = 1, 2$. An invertible sheaf is *algebraically trivial* if it is algebraically equivalent to the structure sheaf.

- F is a group algebraic space, in the sense that F comes from a functor $F' : (\mathbf{Sch}/S) \to \mathbf{Grp}$ by composing a forgetful functor $\mathbf{Grp} \to \mathbf{Sets}$.
- F is proper, by using the valuative criterion of properness. Namely, for any affine S-scheme $Y = \operatorname{Spec} A$ with A being a (discrete) valuation ring, if we let $K = \operatorname{Frac}(A)$, then the natural map $F(Y) \to F(\operatorname{Spec} K)$ induced from the inclusion $A \hookrightarrow K$ is bijective.
- F is formally smooth, by using the infinitesimal lifting criterion for smoothness. Namely, for $s \in S$, A an artin local ring which is a finite $\mathcal{O}_{S,s}$-algebra, $I \subset A$ an ideal such that $\mathfrak{m}_A I = 0$, $F(\operatorname{Spec} A) \to F(\operatorname{Spec} A/I)$ is bijective.
- F has geometrically connected fibers, by using the following fact, proven by Artin [Ar, Lemma 4.2]: *a group algebraic space which is locally of finite type over a field is a group scheme.*

For an abelian scheme A over S, the conditions of Theorem 1.2.17(ii) are satisfied. Thus, $\operatorname{Pic}_{A/S}$ always exists as an algebraic space, locally of finite presentation over S. Also, both $\operatorname{Pic}_{A/S}$ and $\operatorname{Pic}^0_{A/S}$ are naturally group objects in the category of algebraic spaces. If $\operatorname{Pic}^0_{A/S}$ is represented by an abelian scheme, we will call it *the dual abelian scheme* of A, often denoted as $\widehat{A}$. Our objective is to show that *the dual abelian scheme always exists.* We want to deduce this by using the following theorem of Raynaud and Deligne.

Theorem 1.2.18 (Raynaud-Deligne, [FC, Theorem 1.9])**.** *Let S be a scheme, and A be an abelian algebraic space over S. Then A is a scheme, hence an abelian scheme over S.*

Note that we already know that $\operatorname{Pic}^0_{A/S}$ is locally of finite presentation over S. By the above discussion, we now know how to prove that $\operatorname{Pic}^0_{A/S}$ is an abelian algebraic space, by only using the functorial description of $\operatorname{Pic}^0_{A/S}$.

By Theorem 1.2.17(i), if $S = \operatorname{Spec} k$ is the spectrum of a field, $\operatorname{Pic}_{A/k}$ (and therefore $\operatorname{Pic}^0_{A/k}$) is a locally finite type k-group scheme. Note that a group scheme G over a field k is automatically separated, as the diagonal $\Delta_G : G \to G \times_k G$ is a base change of the identity section $e : \operatorname{Spec} k \to G$ via the map $G \times_k G \xrightarrow{(x,y)\mapsto xy^{-1}} G$, which is a closed immersion. We can thus apply the Rigidity Lemma with $\operatorname{Pic}_{X/k}$ as a target, whenever it exists as a scheme, and prove the following important theorem.

Theorem 1.2.19 (Theorem of the Cube)**.** *Let Z be a separated finite type scheme over a field k, and X, Y be proper k-schemes. Suppose that X, Z are geometrically integral and Y is geometrically reduced and geometrically connected. Let $x_0 \in X(k), y_0 \in Y(k), z_0 \in Z(k)$. Suppose $\mathcal{L}$ is a line bundle on $X \times_k Y \times_k Z$ such that $\mathcal{L}_{x_0} := \mathcal{L}|_{\{x_0\}\times_k Y \times_k Z} \cong \mathcal{O}_{Y\times_k Z}$ and similarly $\mathcal{L}_{y_0}, \mathcal{L}_{z_0}$ are trivial. Then $\mathcal{L} \cong \mathcal{O}_{X\times_k Y \times_k Z}$.*

Proof. As $\mathcal{L}_{y_0}$ is trivial, $\mathcal{L} \in \operatorname{Pic}_{Y/k}(X \times_k Z)$. We want to show that $\mathcal{L} = 0$ inside $\operatorname{Pic}_{Y/k}(X \times_k Z)$. Note that as Y is proper, geometrically reduced, geometrically connected and $Y(k) \neq \emptyset$, $\operatorname{Pic}_{Y/k}$ exists as a separated k-scheme, by Theorem 1.2.17(i) and the above discussion. Now we can apply the Rigidity Lemma, Proposition 1.2.12, to the corresponding map $X \times_k Z \to \operatorname{Pic}_{Y/k}$, since $\mathcal{L}_{z_0} \cong \mathcal{O}_{X\times_k Y}$ implies that $X \times_k \{z_0\} \to 0$. As $\mathcal{L}_{x_0}$ is trivial on $Y \times_k Z$, this means that the morphism $X \times_k Z \to \operatorname{Pic}_{Y/k}$ is identically zero. □

Theorem 1.2.20 (Cubical Structure Theorem)**.** *Let A/S be an abelian scheme, and $\mathcal{L}$ be an invertible sheaf on A. For an S-scheme T and $a_1, a_2, a_3 \in A(T)$, the line bundle on S,*

$$(a_1 + a_2 + a_3)^*\mathcal{L} \otimes (a_1 + a_2)^*\mathcal{L}^{-1} \otimes (a_1 + a_3)^*\mathcal{L}^{-1} \otimes (a_2 + a_3)^*\mathcal{L}^{-1}$$
$$\otimes a_1^*\mathcal{L} \otimes a_2^*\mathcal{L} \otimes a_3^*\mathcal{L} \otimes (e^*\mathcal{L})_T^{-1},$$

is canoncially trivial, where $e \in A(S)$ is the identity section.

Proof. It is sufficient to do the universal case, $T = A \times_S A \times_S A$ and $a_i = \mathrm{pr}_i : T \to A$. By the Theorem of the Cube, Theorem 1.2.19, and by symmetry, we only need to show that the line bundle is trivial on $\{0\} \times_S A \times_S A$. As one can check, the eight factors formally cancel out. □

Using the Cubical Structure Theorem, one can prove the following.

Proposition 1.2.14 [MFK, Proposition 6.7]**.** *For an abelian scheme A/S, $\mathrm{Pic}^0_{A/S}$ is formally smooth over S.*

Proof. Let $s \in S$, R be an artin local ring, finite over $\mathcal{O}_{S,s}$, $I \subset R$ be an ideal of R satisfying $\mathfrak{m}_R I = 0$. Let $\mathcal{L}$ be an element of $\mathrm{Pic}^0_{A/S}(R/I)$, which is an invertible sheaf on $A \times_S \mathrm{Spec}(R/I)$. The obstruction on extending this to an invertible sheaf on $A \times_S \mathrm{Spec}\, R$ is an element of $H^2(A_k, \mathcal{O}_{A_k}) \otimes_k I/\mathfrak{m}_R I$, where $k = R/\mathfrak{m}_R$ and $A_k = A \otimes_S \mathrm{Spec}(R/\mathfrak{m}_R)$. Note that by the Cubical Structure Theorem, Theorem 1.2.20, if $m : A \times_S A \to A$ is the multiplication map, we have that $m^*\mathcal{L} \otimes \mathrm{pr}_1^* \mathcal{L}^{-1} \otimes \mathrm{pr}_2^* \mathcal{L}^{-1}$ is trivial, as it comes from a degree zero line bundle over $\mathrm{Spec}\, R/I$, which is trivial as $\mathrm{Spec}\, R/I$ is a point scheme. On the other hand, by Künneth formula,

$$H^2(X_k, \mathcal{O}_{X_k}) \otimes_k I \xrightarrow{m^* - \mathrm{pr}_1^* - \mathrm{pr}_2^*} H^2(X_k \times X_k, \mathcal{O}_{X_k \times X_k}),$$

is injective. As the obstruction of extending $(m^* - \mathrm{pr}_1^* - \mathrm{pr}_2^*)\mathcal{L}$ to $A \times_S A \times_S \mathrm{Spec}\, R$ is trivial, the obstruction of extending $\mathcal{L}$ to $A \times_S \mathrm{Spec}\, R$ is trivial, as well. This shows the formal smoothness of $\mathrm{Pic}^0_{A/S}$. □

Proposition 1.2.15. *For an abelian variety A over a field k, A is projective.*

Proof. We first reduce the problem to the case of $k = \overline{k}$. Suppose $A_{\overline{k}}$ is projective. Then, there is a very ample divisor D on $A_{\overline{k}}$, which is meant to be defined over a finite extension k'/k. Let k'' be the separable closure of k in k'. As k'/k'' is purely inseparable, $k''^{p^m} \subset k'$ for some large enough m. Then, $p^m D$ arises from a divisor on $A_{k''}$, and is very ample. Thus we can assume that k'/k is finite separable. Extending to the Galois closure of k', we can assume that k'/k is finite Galois. Then, $D' = \sum_{\sigma \in \mathrm{Gal}(k'/k)} \sigma D$ arises from a divisor over k. As it is a sum of ample divisors, it is ample. Therefore, D' defines an ample divisor on A, which makes A projective.

Suppose $k = \overline{k}$. As $\overline{k}$ is infinite, it is quite clear that we can choose finite set of codimension 1 integral subschemes $\{Z_1, \cdots, Z_n\}$ such that $\cap_{i=1}^n Z_i = \{e\}$ and, for any $t \in T_e A$, there exists $1 \le i \le n$ such that $t \notin T_e Z_i$; we first add Z_i's to reduce the dimension of $\cap_i T_e Z_i$, and after making it zero, we add Z_i's to reduce the dimension of $\cap_i Z_i$. Let $D = \sum_i Z_i$. We will show that $3D$ is very ample, which will suffice to show that A is projective. To show that $3D$ is very ample, it is sufficient to show that the linear system $|3D|$ separates points and tangent vectors. Note that for any choice of closed points $a_i, b_i \in A(k)$ for $1 \le i \le n$, $\sum_i (t^*_{a_i} Z_i + t^*_{b_i} Z_i + t^*_{-a_i - b_i} Z_i) \sim 3D$. Now, for any distinct points $a, b \in A(k)$, there is j such that Z_j does not contain $b - a$. Choose $a_j = -a$, then $t^*_{a_j} Z_j$ passes through a but not b. Now we can choose all other a_i, b_i's so that all other $t^*_{a_i} Z_i, t^*_{b_i}, t^*_{-a_i - b_i} Z_i$ miss b. Then this shows that $|3D|$ separates points. The same proof shows that $|3D|$ separates tangent vectors, as desired. □

We now prove the existence of dual abelian schemes, with no other assumptions.

Theorem 1.2.21. *For an abelian scheme A over S, there exists the dual abelian scheme $\widehat{A}$ of A. In other words, $\widehat{A} := \mathrm{Pic}^0_{A/S}$ is represented by an abelian scheme over S.*

Proof. We first prove the case when $S = \operatorname{Spec} k$ is the spectrum of a field, namely when A/k is an abelian variety. We already know $\operatorname{Pic}^0_{A/k}$ is a smooth k-group scheme, by Proposition 1.2.14. As every k-scheme is faithfully flat, the valuative criterion for properness clearly holds, so $\operatorname{Pic}^0_{A/k}$ is proper. We thus only need to show that it is connected. By passage to the algebraic closure, we can assume that $k = \overline{k}$. Let $\operatorname{Pic}^{0c}_{A/k}$ be the connected component of the identity section of $\operatorname{Pic}_{A/k}$. Then, a line bundle corresponding to a point in $\operatorname{Pic}^{0c}_{A/k}$ is algebraically trivial via the universal line bundle $\mathcal{P} \in \operatorname{Pic}_{A/k}(\operatorname{Pic}^{0c}_{A/k})$ on $A \times_k \operatorname{Pic}^{0c}_{A/k}$. On the other hand, for a connected k-scheme T, closed points $t_1, t_2 \in T(k)$ and a line bundle $\mathcal{L}$ on $X \times_k T$, both $\mathcal{L}_{X \times \{t_1\}}$ and $\mathcal{L}_{X \times \{t_2\}}$ lie inside the image of the corresponding map $T \to \operatorname{Pic}_{X/k}$. As T is connected, both line bundles lie in the same connected component. This means that any algebraically trivial line bundle should lie in $\operatorname{Pic}^{0c}_{A/k}$. Thus, $\operatorname{Pic}^{0c}_{A/k} = \operatorname{Pic}^0_{A/k}$, which is connected. Thus, we deduced that $\operatorname{Pic}^0_{A/k}$ is an abelian variety.

Suppose now that A/S is an abelian scheme. By the discussion around Theorem 1.2.18, it is sufficient to show that the algebraic space $\operatorname{Pic}^0_{A/S}$ is proper, formally smooth and has geometrically connected fibers. By Proposition 1.2.14, we again know $\operatorname{Pic}^0_{A/S}$ is formally smooth. As geometric fibers of $\operatorname{Pic}^0_{A/S}$ are $\operatorname{Pic}^0_{A_s/\kappa(s)}$ for geometric points s of S, we know it is connected. We also know $\operatorname{Pic}^0_{A/S}$ is separated, by Theorem 1.2.17(iii). Note that the proof of [EGA, IV-3, Corollaire 15.7.11] can be verbatim adapted to algebraic spaces to deduce the following: *let X be an algebraic space, separated and of finite presentation over S, with a section $S \to X$; suppose that, for any point $s \in S$, X_s is geometrically connected and proper over $\kappa(s)$; then, X is proper over S.* If we know that $\operatorname{Pic}^0_{A/S}$ is of finite presentation over S, or, that it is quasicompact over S, we can use this and we are done. On the other hand, by [SGA6, Exposé XIII, Théorème 4.7], we know that, if S is quasicompact, $\operatorname{Pic}^0_{X/S} \hookrightarrow \operatorname{Pic}_{X/S}$ is representable and quasicompact. This in particular implies that $\operatorname{Pic}^0_{X/S}$ is quasicompact over S whenever S is affine. Thus, for any base scheme S and an affine open $U \subset S$, $\operatorname{Pic}^0_{X/S} \times_S U = \operatorname{Pic}^0_{X_U/U}$ is quasicompact over U. Therefore, $\operatorname{Pic}^0_{X/S}$ is quasicompact over S. This finishes the proof of the theorem. □

For an abelian variety A over k, we often refer to the restriction of the universal line bundle to $A \times \operatorname{Pic}^0_{A/k}$ as the *Poincaré bundle* $\mathcal{P}_A$. In particular, it gives rise to a canonical isomorphism of an abelian variety to its double dual.

1.2.3.3 Isogenies and Polarizations

Let S be a base scheme. A homomorphism $f : G \to G'$ of S-group schemes is called an *isogeny* if f is surjective and its kernel $\ker(f)$ is a flat finite group scheme over S; recall that the kernel always exists as a group scheme, unlike cokernels. Note that the quotient by a finite flat group scheme is an isogeny, if exists. Conversely, as an isogeny $f : G \to G'$ is flat, so f is identified with the quotient $G \to G/\ker f$.

Over a connected base scheme S, an isogeny f is *of degree n* if $\ker f$ is a finite flat group scheme of order n. Over a general base, the degree is a locally constant function over S. This degree is the same as the degree as a finite map.

Perhaps the most important isogeny for abelian schemes is the multiplication by n map.

Proposition 1.2.16. *Let A be an abelian scheme over S, and let $n \neq 0$ be an integer. Then the multiplication by n map, $[n] : A \to A$, is an isogeny of degree n^{2g}, where g is the relative dimension of A over S.*

Proof. From the definition of isogeny, it is clear that we can check isogeny fiberwise. Thus, we can assume that $S = \operatorname{Spec} k$ is the spectrum of a field, and A is an abelian variety over k. By induction and the Cubical Structure Theorem, Theorem 1.2.20, we can show that, for any line bundle $\mathcal{L}$ over A, $[n]^*\mathcal{L} \cong \mathcal{L}^{\otimes \frac{n^2+n}{2}} \otimes ([-1]^*\mathcal{L})^{\otimes \frac{n^2-n}{2}}$. Let $\mathcal{L}$ be an ample line bundle over A, which is possible as we know A is projective over k, and consider the restriction to $A[n] = \ker[n]$. We have

$$\mathcal{O}_{A[n]} \cong \mathcal{L}_{A[n]}^{\otimes \frac{n^2+n}{2}} \otimes ([-1]^*\mathcal{L})_{A[n]}^{\otimes \frac{n^2-n}{2}},$$

where both $\mathcal{L}_{A[n]}$ and $([-1]^*\mathcal{L})_{A[n]} = [-1]^*(\mathcal{L}_{A[n]})$ are ample on $A[n]$. As $n \neq 0$, at least one of the powers are positive, so it implies that $\mathcal{O}_{A[n]}$ is ample. As $A[n]$ is projective over k, by using Serre's vanishing, every coherent sheaf over $A[n]$ has vanishing higher cohomology after twisting sufficiently high power of $\mathcal{O}_{A[n]}$, which does nothing. Thus, by Serre's criterion of affineness, $A[n]$ is affine over k. An affine proper scheme over k must be finite, so $A[n]$ is a finite flat k-group scheme. Now notice that as $[n]$ is a morphism between smooth proper irreducible schemes of the same dimension with 0-dimensional kernel, so it has a closed dense image, or it is surjective. Thus $[n]$ is an isogeny.

Replacing $\mathcal{L}$ with $\mathcal{L} \otimes [-1]^*\mathcal{L}$, we have an ample line bundle $\mathcal{L}$ which satisfies $[n]^*\mathcal{L} \cong \mathcal{L}^{n^2}$. Note that $\deg \mathcal{L} \neq 0$, and $\deg([n]^*\mathcal{L}) = \deg[n] \cdot \deg \mathcal{L}$ whereas $\deg \mathcal{L}^{n^2} = n^{2g} \deg \mathcal{L}$. Thus $\deg[n] = n^{2g}$. □

Proposition 1.2.17. *Let A, A' be abelian schemes of dimension g over S. Let $f : A \to A'$ be an isogeny of constant degree n. Then, there exists an isogeny $f' : A' \to A$ of constant degree n such that $f \circ f' = [n^{2g}]_{A'}$ and $f' \circ f = [n^{2g}]_A$.*

Proof. By Deligne's theorem, Theorem 1.2.1, $\ker f$ is killed by $[n^{2g}]_A$. Then the proposition is immediate from the universal property of quotients. □

This is important, as this shows that an isogeny is in fact an *equivalence relation.* We can thus safely call two abelian schemes A, A' over S *isogenous* if there exists an isogeny $f : A \to A'$.

Another important example of isogeny is an isogeny between an abelian variety and its dual. Given an invertible sheaf $\mathcal{L}$ on A, define $\lambda(\mathcal{L}) : A \to \widehat{A}$ to be a morphism corresponding to the line bundle

$$m^*\mathcal{L} \otimes \mathrm{pr}_1^* \mathcal{L}^{-1} \otimes \mathrm{pr}_2^* \mathcal{L}^{-1} \otimes (e^*\mathcal{L})_{A \times_S A},$$

on $A \times_S A$.

Proposition 1.2.18. *If $\mathcal{L}$ is relatively ample over S, then $\lambda(\mathcal{L}) : A \to \widehat{A}$ is an isogeny.*

Proof. For each $s \in S$, $\lambda(\mathcal{L})_s = \lambda(\mathcal{L}_s)$, so we can assume that $S = \operatorname{Spec} k$ is the spectrum of a field. Let $A' = \ker(\lambda(\mathcal{L}))^0$. Note that $m^*\mathcal{L}|_{A'} \otimes \mathrm{pr}_1^*(\mathcal{L}|_{A'})^{-1} \otimes \mathrm{pr}_2^*(\mathcal{L}|_{A'})^{-1} \otimes (e^*\mathcal{L}|_{A'})_{A' \times_k A'}$ is trivial on $A' \times_k A'$. The pullback of this sheaf by the map $A' \xrightarrow{a \mapsto (a,-a)} A' \times_k A'$ is $\mathcal{L}|_{A'} \otimes [-1]^*(\mathcal{L}|_{A'})$, which is again ample and trivial. Thus, $\dim A' = 0$, or $\lambda(\mathcal{L})$ is finite.

To show the surjectivity, it is sufficient to show that $\dim A = \dim \widehat{A}$. Note that $T_e\widehat{A} = \ker(\mathrm{Pic}_{A/k}(k[\varepsilon]/\varepsilon^2) \to \mathrm{Pic}_{A/k}(k)) = H^1(A, \mathcal{O}_A)$. It is $\dim A$-dimensional, as $\dim_k H^p(A, \mathcal{O}_A) = \binom{\dim A}{p}$, e.g. [Mum, 13, Corollary 2]. □

This kind of isogeny is called a *polarization.*

Definition 1.2.7 (Polarization)**.** *Let A be an abelian scheme over S. A* polarization *of A is a homomorphism $\lambda : A \to \widehat{A}$ such that, for each geometric point $\overline{s}$ of S, $\lambda_{\overline{s}} = \lambda(\mathcal{L}_{\overline{s}})$ for some ample invertible sheaf $\mathcal{L}_{\overline{s}}$ on $A_{\overline{s}}$. A polarization is* principal *if it is an isomorphism, i.e. when is of degree* 1*.*

The construction $\lambda(\mathcal{L})$ has nice properties, and is often a better object to study that the line bundle $\mathcal{L}$ itself.

Proposition 1.2.19. *Let $\lambda : A \to \widehat{A}$ be a polarization of an abelian scheme A over S.*
(i) Through the canonical isomorphism $i : A \xrightarrow{\sim} A^{\wedge\wedge}$, $\widehat{\lambda} \circ i = \lambda$.
(ii) For $\mathcal{L} \in \mathrm{Pic}^0_{A/S}(S)$, $\lambda(\mathcal{L}) = 0$.
(iii) $\lambda(\mathcal{L}^{-1}) = \lambda(\mathcal{L}) \circ [-1]_A$.
(iv) $\lambda(\mathcal{L}_1 \otimes \mathcal{L}_2) = \lambda(\mathcal{L}_1) + \lambda(\mathcal{L}_2)$.
(v) For $x \in A(S)$, $\lambda(t_x^*\mathcal{L}) = \lambda(\mathcal{L})$.
(vi) If $S = \mathrm{Spec}\, k$ is the spectrum of a field, $\lambda(\mathcal{L}) = 0$ implies that $\mathcal{L} \in \mathrm{Pic}^0_{A/k}(k)$.

Proof. All except (vi) follow from the Cubical Structure Theorem, Theorem 1.2.20, and identification of maps into $\widehat{A}$ via their pullback of the Poincaré bundle. For (vi), we use the fact that $\deg \lambda(\mathcal{L}) = \chi(L)^2$ (cf. [Mum, 16]), where $\chi(L)$ is the Euler characteristic of L. □

Define the *isogeny category* of abelian varieties over a field k to be the localization of the category of abelian varieties over a field k where k-isogenies are considered as isomorphisms. The isogeny category is very nice, in fact is semi-simple.

Theorem 1.2.22 (Poincaré Complete Reducibility Theorem)**.** *Let A be an abelian variety over a field k. For $A' \hookrightarrow A$ an abelian subvariety over k, there is an abelian subvariety $A'' \hookrightarrow A$ over k such that $A' \times_k A'' \to A$ is an isogeny.*

Proof. Choose an ample line bundle $\mathcal{L}$ on A. Then we have a commutative diagram

$$\begin{array}{ccc} A' & \xrightarrow{\ i\ } & A \\ {\scriptstyle \lambda(i^*\mathcal{L})}\downarrow & & \downarrow{\scriptstyle \lambda(\mathcal{L})} \\ \widehat{A'} & \xleftarrow[\ \widehat{i}\ ]{} & \widehat{A} \end{array}$$

Let $A'' = \ker(\widehat{i} \circ \lambda(\mathcal{L}))^0_{\mathrm{red}}$. It is a projective smooth connected k-group scheme, so it is an abelian subvariety of A over k. Note that $A'' \cap A' \subset \ker \lambda(i^*\mathcal{L})$, so it is finite. Therefore, to show that $A' \times A'' \to A$ is an isogeny, we only need to show that the dimensions are right, i.e. $\dim A'' = \dim A - \dim A'$. One way is easy, the other way we have $\dim A'' = \dim \ker \widehat{i}$ as $\lambda(\mathcal{L})$ is finite surjective, so $\dim A'' = \dim \ker \widehat{i} \geq \dim \widehat{A} - \dim \widehat{A'} = \dim A - \dim A'$. □

The isogeny category is "the category of abelian varieties modulo torsion."

Proposition 1.2.20. *Let A, B be abelian varieties over a field K. Then,* $\mathrm{Hom}^0_K(A, B) := \mathrm{Hom}_{K\text{-isogeny}}(A, B) = \mathrm{Hom}_K(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$*. In other words, the group of homomorphisms from the isogeny class of A to the isogeny class to B is naturally identified with* $\mathrm{Hom}_K(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Proof. Obviously $\mathrm{Hom}_K(A, B) \subset \mathrm{Hom}_{K\text{-isogeny}}(A, B)$, and as $[n]$ maps are isogeny, we can compose it and its "inverse" inside the isogeny category, so that we have a natural inclusion $\mathrm{Hom}_K(A, B) \otimes_{\mathbb{Z}} \mathbb{Q} \subset \mathrm{Hom}_{K\text{-isogeny}}(A, B)$. On the other hand, an element of $\mathrm{Hom}_{K\text{-isogeny}}(A, B)$ is of form

$$A = A_0 \leftarrow A_1 \to A_2 \leftarrow \cdots \to A_{j-1} \leftarrow A_j \to B_k \leftarrow B_{k-1} \to \cdots \leftarrow B_2 \to B_1 \leftarrow B_0 = B,$$

where the arrows between A_i's and the arrows between B_i's are isogenies. On the other hand, given an isogeny $i : A' \leftarrow A''$, there is $n \in \mathbb{Z}\backslash\{0\}$ and an isogeny $i' : A' \to A''$, so that $i \circ j = [n]$. Thus, the "inverse" $i^{-1} \in \mathrm{Hom}_{K\text{-isogeny}}(A', A'')$ is identified as "$j \circ [n]^{-1}$," which up to torsion the same as j. Thus, an element of $\mathrm{Hom}_{K\text{-isogeny}}(A, B)$ is in $\mathrm{Hom}_K(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$ in this sense. □

1.2.3.4 Duality and the Weil Pairing

Given a map of abelian schemes $f : A \to B$, the pullback of invertible sheaves induces the *dual map* $\widehat{f} : \widehat{B} \to \widehat{A}$.

Proposition 1.2.21. *Let A, B be abelian schemes over S.*

(i) If $f, g : A \rightrightarrows B$ be two morphisms of abelian schemes. Then $(f+g)^\wedge = \widehat{f} + \widehat{g}$. In particular, $\widehat{[n]_A} = [n]_{\widehat{A}}$.

(ii) The dual of an isogeny is an isogeny.

Proof. (i) We would like to show that, for any S-scheme T and $\mathcal{L} \in \mathrm{Pic}^0_{B/S}(T)$, $(f_T + g_T)^*\mathcal{L} = (f_T)^*\mathcal{L} \otimes (g_T)^*\mathcal{L}$. We can check whether a given line bundle is trivial fiberwise, so we can assume $S = \operatorname{Spec} k$ is the spectrum of a field. Checking if two morphisms are equal can be done after a faithfully flat base change, so we can assume $k = \overline{k}$. Then as $\mathcal{L} \in \mathrm{Pic}^0_{B/k}(k)$, $\lambda(\mathcal{L}) = 0$, so the Cubical Structure Theorem, Theorem 1.2.20, gives us the identity.

(ii) It follows from (i) and the fact that an isogeny factors through $[n]$ for some nonzero integer n. □

Let A be an abelian scheme over S of dimension g. As we know $[n] : A \to A$ is an isogeny, it follows that $A[n] = \ker[n]$ is a finite flat commutative group scheme over S of order n^{2g}. As forseen before, it is then immediate that, for any prime p, $A(p) := (A[p^n])$ forms a p-divisible group over S of height $2g$. A natural question to ask is that, what is the relation between $A[n]$ and $\widehat{A}[n]$?

Proposition 1.2.22. *For abelian schemes A, B over S and $f : A \to B$ an isogeny, naturally* $\ker \widehat{f} \cong (\ker f)^D$. *To be more precise, for any S-scheme T,*

$$(\ker \widehat{f})(T) \cong \mathrm{Hom}_{T-\mathbf{Grp}}((\ker f)_T, \mathbb{G}_{m,T}).$$

The pairing $(\ker f) \times_S (\ker \widehat{f}) \to \mathbb{G}_{m,S}$ induced from this is called the *Weil pairing*.

Proof. As our setup is compatible with base change, we can just treat the case $S = T$. Note that $\ker \widehat{f}(S) = \ker(\mathrm{Pic}(B) \xrightarrow{f^*} \mathrm{Pic}(A))$, and by descent theory, it is equal to the group of isomorphisms $\mathrm{pr}_1^* \mathcal{O}_A \cong \mathrm{pr}_2^* \mathcal{O}_A$ satisfying cocycle condition as $\mathcal{O}_{A\times_B A}$-modules. As $f : A \to B$ is the quotient of A by $\ker f$, the action map $(\ker f) \times_S A \xrightarrow{(g,a)\mapsto(ga,a)} A \times_B A$ is an isomorphism. Along this isomorphism, the data of $\mathrm{pr}_1^* \mathcal{O}_A \cong \mathrm{pr}_2^* \mathcal{O}_A$ becomes $m^*\mathcal{O}_A \cong \mathrm{pr}_2^* \mathcal{O}_A$ on $(\ker f) \times_S A$. This is the same as the data of a unit u in $\Gamma((\ker f) \times_S A, \mathcal{O}_{(\ker f)\times_S A})^\times$. It is the collection of $u(g) \in \Gamma(A, \mathcal{O}_A)^\times$ for $g \in (\ker f)(S)$. The cocycle condition is exactly demanding $g \mapsto u(g)$, as a morphism $\ker f \to \mathbb{G}_{m,S}$, to be a homomorphism. On the other hand, coboundaries vanish because $p_*\mathcal{O}_A = \mathcal{O}_S$, where $p : A \to S$ is the structure morphism, and its formation is compatible with base change. □

Remark 1.2.5. In particular, the Weil pairing shows that *the dual isogeny is of the same degree as the original isogeny.*

1.2.3.5 Néron Models and Reductions

We now define what it means for an abelian variety over a field to have a good or semi-stable reduction. It need a procedure to pass to an integral model, and it is the integral model that decides the reduction. On the other hand, it is questionable about how canonical is the passage to integral model. For example, is there always an integral model which is an abelian scheme? This cannot be the case, as there is an abelian variety over $\mathbb{Q}$ but no nontrivial abelian scheme over $\mathbb{Z}$ as we will see shortly. However, there is some kind of a "canonical" integral model which is not necessarily proper, which is called a *Néron model*.

Definition 1.2.8 (Néron Model)**.** *Let R be a Dedekind domain and $K = \mathrm{Frac}(R)$. 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 $Y_K \cong X$ and it satisfies the following* Néron mapping property*.*

For each smooth R-sheme Y' and each K-morphisms $u_K : Y'_K \to Y_K = X$, there is a unique R-morphism extending u_K.

The Néron mapping property is a kind of universal property to make sure that a Néron model, if exists, is a canonical object. It is easy to see the following.

Proposition 1.2.23 [BLR, 1.2]**.** *(i) A Néron model is uniquely determined by its generic fiber, up to canonical isomorphism.*

(ii) The formation of Néron models commutes with étale base change.

(iii) A Néron model can be computed locally on the base.

(iv) 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.

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

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

A nontrivial theorem is that an abelian variety admits a Néron model.

Theorem 1.2.23 [BLR, Corollary 1.3.2, Theorem 1.4.2]**.** *Let R be either a Dedekind domain or a discrete valuation ring. Let $K = \mathrm{Frac}(R)$. For an abelian variety A over K, A admits a Néron model over R, which is quasi-projective over R.*

The remaining problem is whether this Néron model is an abelian scheme over R or not. In fact, it is not necessarily an abelian scheme, due to the lack of properness. We thus say an abelian variety has a *good reduction* if its Néron model is an abelian scheme.

Definition 1.2.9 (Reduction Types)**.** *Let K be either a global field or a local field of mixed characteristic. Let A be an abelian variety over K.*

(i) If K is a local field, A is called to have a good reduction *if its Néron model over $\mathcal{O}_K$ is an abelian scheme.*

(ii) If K is a global field, A is called to have a good reduction at a prime $\mathfrak{p} \subset \mathcal{O}_K$ *if its Néron model over $(\mathcal{O}_K)_\mathfrak{p}$ is an abelian scheme.*

If an abelian variety does not have good reduction (at a closed point), then it is called to have a *bad reduction* (at the point). We now can easily see the equivalence of different formulations of Shafarevich conjecture. Namely, for a number field K and a finite set of primes S of K, an abelian scheme over $\mathcal{O}_{K,S}$ really is the same thing as an abelian variety over K with good reduction outside S.

There are multiple ways of seeing good reduction, all in a similar vein.

Proposition 1.2.24. *Let A be an abelian variety over a field K.*

(i) If K is a global field, A has good reduction at a prime $\mathfrak{p} \subset \mathcal{O}_K$ if and only if $A_{K_\mathfrak{p}}$ has good reduction.

(ii) Let R be either a Dedekind domain or a discrete valuation ring such that $K = \mathrm{Frac}(R)$. For a closed point $s \in \operatorname{Spec} R$, A has good reduction at s if and only if $A_s = A \otimes_R \kappa(s)$ is an abelian variety over $\kappa(s)$.

Proof. (i) is immediate. For (ii), one direction is also immediate, as properness is preserved by base change. The really nontrivial result we need to use here is that, for a Néron model $\mathcal{A}$ over $\mathcal{O}_{\operatorname{Spec} R,s}$, that its reduction $\mathcal{A}_s$ is $\kappa(s)$-proper implies that $\mathcal{A}$ is $\mathcal{O}_{\operatorname{Spec} R,s}$. This follows from the following fact [EGA, IV-3, Corollaire 15.7.10]: *for a separated, finite type, faithfully flat morhpsim $f : X \to Y$, if Y is locally noetherian and each fiber X_y for $y \in Y$ is geometrically connected and proper over $\kappa(y)$, then f is proper.* □

We now know that the property of having good reduction at a prime is solely dependent on the reduction modulo the prime. We know that the reduction is a smooth finite type commutative group scheme over the residue field. As we are only interested in the cases of number fields or local fields of mixed characteristic, the residue field is a finite field. In this case, we can apply the Chevalley Structure Theorem to analyze the structure of the reduction.

Theorem 1.2.24 (Chevalley Structure Theorem, cf. [BLR, Theorem 9.2.1])**.** *Let G be a smooth connected group scheme over a perfect field k. Then, there is a unique exact sequence*

$$1 \to H \to G \to B \to 1$$

where H is a connected smooth affine k-group scheme and B is an abelian variety over k. If furthermore G is commutative, H uniquely splits as $H = T \times_k U$, where T is a k-torus (i.e. $T_{\overline{k}} \cong \mathbb{G}_{m,\overline{k}}^N$ for some N) and U is a smooth connected unipotent k-group (i.e. has a filtration over $\overline{k}$ with successive subquotients isomorphic to $\mathbb{G}_a$).

Borrowed from the terminology of describing group schemes in terms of the Chevalley Structure Theorem, we define the following mildly bad reductions.

Definition 1.2.10 (Reduction Types)**.** *Let G be a smooth connected group scheme of finite type over a Dedekind scheme S. Let $s \in S$ be a closed point.*

(i) We say G has abelian reduction *at s if G_s^0 is an abelian variety, i.e. the corresponding H in the Chevalley Structure Theorem is trivial.*

(ii) We say G has semi-abelian reduction (or semi-stable reduction) *at s if G_s^0 is an extension of an abelian variety by an affine torus ("semi-abelian variety"), i.e. the corresponding U in the Chevalley Structure Theorem is trivial.*

(iii) We say G has potentially good (abelian, semi-abelian/semi-stable, respectively) reduction *if there is a finite Galois extension L of $K = K(S)$ such that, over the normalization S' of S in L, $G_{S'}$ has good (abelian, semi-abelian/semi-stable, respectively) reduction at every point lying over s.*

Note that, for abelian varieties and schemes, an abelian reduction is just a good reduction. These reduction types are reluctant to isogeny.

Proposition 1.2.25. *(i) An abelian variety isogenous to an abelian variety with semi-stable (good, respectively) reduction has semi-stable (good, respectively) reduction.*

(ii) A semi-abelian integral model of an abelian variety is identified with an open subscheme of the Néron model via the morphism from the Néron mapping property.

Proof. (i) By the Néron mapping property, it is sufficient to show the following: if $f : A \to A'$ is an isogeny of abelian varieties over K, and if A has semi-stable reduction (at a prime), then f extends to an isogeny of Néron models. Note that, on a semi-abelian group scheme, the multiplication by n map is finite and flat, as they are on both abelian varieties and torii, for any $n \neq 0$. Thus, we can lift multiplication by n maps to an isogeny of Néron models. Then the general case follows as f factors through $[\deg f]$.

(ii) Suppose that the semi-abelian integral model is connected. We can pass to the strict henselization, as the formation of Néron models is compatible with the passage to strict henselization. Let n be a positive integer not divisible by the characteristic of residue field k. Then, for a semi-abelian integral model G over R and Néron model A over R, both extending A_K over $K = \mathrm{Frac}(R)$, we have $G[n](K) \cong A[n](K)$, as both are extending A_K. As $A[n](K) \cong A[n](R)$ by Néron mapping property and $G[n](R) \subset G[n](K)$ by valuative criterion for separatedness, we deduce that $G[n](R) \subset A[n](R)$. Reducing to k, we have $G[n](k) \subset A[n](k)$. As $k = k^s$, the points of finite order not divisible by $\mathrm{char}\, k$ form a dense subset of $G_k(k)$, so it follows that $G_k \to A_k^0$ has finite kernel. It is surjective as the dimensions match. By Zariski's Main Theorem, it is an isomorphism. □

Proposition 1.2.26 (cf. [BLR, 7.4, 7.5])**.** *Let R be either a Dedekind domain or a discrete valuation ring of mixed characteristic, and $K = \mathrm{Frac}(R)$. If R is Dedekind, choose a prime $\mathfrak{p}$ in $\mathcal{O}_K$. Let k be the residue field (at $\mathfrak{p}$).*

Suppose that we are given an exact sequence $0 \to A' \to A \to A'' \to 0$ of abelian varieties over K, and consider the corresponding complex of Néron models over R, $0 \to X' \to X \to X'' \to 0$. Using the Poincaré Complete Reducibility Theorem, Theorem 1.2.22, we can find an abelian K-subvariety $B \subset A$ such that $A \to A''$ induces an isogeny $u : B \to A''$. Let $n = \deg u$.

(i) A has semi-stable reduction (at $\mathfrak{p}$) if and only if A', A'' have semi-stable reductions (at $\mathfrak{p}$).

(ii) If $\mathrm{char}\, k$ does not divide n, then $X' \to X$ is a closed immersion, $X \to X''$ is smooth with kernel X', and the cokernel of $A_k \to A''_k$ is killed by multiplication with n. If furthermore A has good reduction (at $\mathfrak{p}$), then $0 \to X' \to X \to X'' \to 0$ is exact.

(iii) If A has semi-stable reduction (at $\mathfrak{p}$), then $0 \to X' \to X \to X'' \to 0$ is exact up to isogeny.

(iv) Suppose R is a discrete valuation ring with $e < p-1$, where e is the absolute ramification index. Then the following assertions hold.

(a) If A' has semi-stable reduction, $X' \to X$ is a closed immersion.

(b) If A has semi-stable reduction, $0 \to X' \to X \to X''$ is exact.

(c) If A has good reduction, A, A'' also have good reductions, and $0 \to X' \to X \to X'' \to 0$ is exact.

Proof. (i) It is an immediate consequence that A is isogenous to $A' \times A''$.

(ii) In the proof of Proposition 1.2.25(i), it is also clear that, if m is not divisible by $\mathrm{char}\, k$, $[m]$ is an étale isogeny on the level of Néron models. Thus, the isogeny $A' \times B \to A$ induced from $u : B \to A''$ lifts to an étale isogeny, factoring through $[n]$. The statements follow easily from this observation.

(iii) From the proof of Proposition 1.2.25(i), we know we can lift u and $A' \times B \to A$ to isogenies. This gives a split exact sequence isogenous to $0 \to X' \to X \to X'' \to 0$.

(iv) See the proof of [BLR, Theorem 7.5.4]. The condition $e < p - 1$ is required precisely because the proof utilizes Raynaud's theorem on prolongations, Theorem 1.2.8. □

1.2.3.6 Jacobians of Relative Curves

In this section, we will discuss about *the Shafarevich conjecture for curves* mentioned in the introduction. First of all, we define a *curve over a field* to be a *proper, geometrically connected 1-dimensional scheme*, and a *(relative) curve over a base scheme S* to be a *proper flat S-scheme whose fibers are curves*. For a smooth curve C over a number field K, we define C to have *good reduction at a prime* $\mathfrak{p}$ if there is a smooth proper curve $\mathcal{C}$ over $(\mathcal{O}_K)_{\mathfrak{p}}$ extending C. It is equivalent to saying that the reduction $\overline{\mathcal{C}}$ over $\kappa(\mathfrak{p})$ is a smooth proper curve; smoothness is a local condition, and properness can be checked at the special fiber by the lemma [EGA, IV-3, Corollaire 15.7.10] we used.

The first thing to ask is the following: *why does C having good reduction outside a finite set of primes S in K admit a smooth proper curve $\mathcal{C}$ over $\mathcal{O}_{K,S}$ extending C?* We cannot directly use the argument we used for abelian varieties, since the theory of Néron models is not very nice in this case. On the other hand, a viewpoint from birational geometry gives us a different kind of model for curves.

Definition 1.2.11 (Regular Proper R-model)**.** *Let R be a Dedekind domain, $K = \mathrm{Frac}(R)$, and C be a smooth K-curve. A* regular proper R-model *of C is a regular (proper) R-curve whose generic fiber is isomorphic to C. A* minimal regular proper R-model *of C is a regular proper R-model $\mathcal{C}$ such that any dominant morphism $\mathcal{C} \to \mathcal{C}'$ of another regular proper R-model of C is an isomorphism.*

Theorem 1.2.25 (Minimal Models Theorem, [Li, Q, Theorem 9.3.21])**.** *For a smooth K-curve C of positive genus, there exists a unique minimal regular proper R-model C^{reg}.*

Now the situation is clear; if a smooth K-curve has good reduction outside a finite set of primes S, then the minimal regular proper $\mathcal{O}_{K,S}$-model C^{reg} is necessarily smooth, as it is fiberwise smooth.

Now we will see how *the Shafarevich conjecture for curves follows from the Shafarevich conjecture for abelian varieties*. Given a smooth curve C over a Dedekind domain R, consider $\mathrm{Pic}^0_{C/R}$. It turns out that this is also representable by a scheme.

Proposition 1.2.27 [BLR, Proposition 9.4.4]**.** *Let $f : X \to S$ be a proper smooth morphism of schemes whose geometric fibers are connected curves. Then, $\mathrm{Pic}^0_{X/S}$ is an abelian S-scheme, and there is a canonical S-ample rigidified line bundle $\mathcal{L}(X/S)$ on $\mathrm{Pic}^0_{X/S}$.*

We call $J(C) := \mathrm{Pic}^0_{C/R}$ *the Jacobian* of C. As the formation of Picard scheme is compatible with completion, it follows that the generic fiber of $J(C)$ is just $J(C_K)$. Therefore, for a number field K and a finite set of primes S, a K-curve having good reduction outside S is associated with a *principally polarized*[9] abelian variety over K having good reduction outside S. Thus, the Shafarevich conjecture for curves is deduced from the Shafarevich conjecture for abelian varieties if we show that the functor $C \mapsto J(C)$ is a finite-to-one map. This is established by the following theorems.

Theorem 1.2.26 (Torelli's Theorem, [CS, VII, Corollary 12.2])**.** *Over a perfect field K, let C, C' be smooth K-curves of genus $g \geq 2$. If $(J(C), \lambda(\mathcal{L}(C/K))) \cong (J(C'), \lambda(\mathcal{L}(C'/K)))$ as principally polarized abelian varieties, then $C \cong C'$ as smooth K-curves.*

Theorem 1.2.27 [NN, Theorem 1.1]**.** *An abelian variety admits only finitely many principal polarizations.*

Now it is clear that the Shafarevich conjecture for curves follows from the Shafarevich conjecture for abelian varieties; the Jacobian of a curve over K with good reduction outside S is an abelian variety over K with good reduction outside S, and this correspondence is finite-to-one (up to isomorphism).

[9]Recall that an ample line bundle $\mathcal{L}$ gives a polarization $\lambda(\mathcal{L})$. As the construction of $\mathcal{L}(X/S)$ is canonical, it turns out that the associated polarization is principal in this case, cf. [CS, VII, 6.11].

1.2.3.7 Reduction Types Via p-divisible Groups

We now describe how a p-divisible group can describe the reduction behavior of an abelian variety. Recall that we have a famous Néron-Ogg-Shafarevich criterion, treated in many basic courses on, say, elliptic curves.

Theorem 1.2.28 (Néron-Ogg-Shafarevich Criterion, [BLR, Theorem 7.4.5]). *Let A be an abelian variety over a local field K with residue characteristic p. Let $\ell \neq p$ be a prime. Then A has good reduction if and only if the ℓ-adic Tate module $T_\ell(A) := \varprojlim A[\ell^n](\overline{K})$ is unramified as a Galois representation of the absolute Galois group G_K of K.*

That we need $\ell \neq p$ is reasonable, as generally p-adic Tate modules are badly behaved. We know that ℓ-adic Tate modules secretly come from ℓ-divisible groups (Proposition 1.2.10), and it turns out that, if one instead consider ℓ-divisible groups, one does not need the condition $\ell \neq p$. This philosophy is extensively explored in [SGA7-1, Exposé IX], with one extra condition that the base field K is of characteristic 0. This condition could not be removed precisely because the Tate's theorem, Theorem 1.2.10, is only valid over characteristic 0. Therefore, de Jong's results, in particular Theorem 1.2.11, can remove this extra hypothesis and prove the results in full generality.

Theorem 1.2.29 ([SGA7-1, Exposé IX, Corollaire 5.10], [dJ, 2.5]). *Let R be a henselian discrete valuation ring with fraction field K. Let ℓ be any prime. Let A be an abelian variety over K. Then, A has good reduction if and only if "$A(\ell)$ has good reduction," i.e. $A(\ell)$ extends to an ℓ-divisible group over R.*

The Néron-Ogg-Shafarevich criterion is immediate from this. Note that, if $\ell \neq p$, an ℓ-divisible group over R is always étale, so by Theorem 1.2.10 A has good reduction if and only if $T(A(\ell)) = T_\ell(A)$, a $\pi_{1,\text{ét}}(K,\alpha)$-module, factors through a $\pi_{1,\text{ét}}(R,\alpha)$-module, where α is a geometric point of $\operatorname{Spec} K$. Now the Néron-Ogg-Shafarevich Criterion follows as $\pi_{1,\text{ét}}(K,\alpha) = G_K$, whereas $\pi_{1,\text{ét}}(R,\alpha) = I_K$, the inertia group.

One can also distinguish semi-stable reduction in terms of p-divisible groups.

Theorem 1.2.30 ([SGA7-1, Exposé IX, Proposition 5.13], [dJ, 2.5]). *Let R be a henselian discrete valuation ring with fraction field K. Let ℓ be any prime. Let A be an abelian variety over K. Then, the following are equivalent.*

1. *A has semi-stable reduction.*
2. *For all $g \in I_K$ in the inertia group, $(g-1)^2$ acts trivially on $A(\ell)$. In other words, the inertia group acts* "unipotently of echelon two"*.*
3. *For all $g \in I_K$ in the inertia group, g acts unipotently on $A(\ell)$.*
4. *There is a filtration[10] of ℓ-divisible groups $A(\ell)^t \subset A(\ell)^f \subset A(\ell)$ such that both $A(\ell)^t$ and $A(\ell)^f/A(\ell)^t$ extend to ℓ-divisible groups F_1, F_2 over R (i.e. good reduction) such that F_2 and F_1^D are étale ℓ-divisible groups over R.*

There is also another criterion for semi-stable reduction, called the Raynaud's Criterion.

Theorem 1.2.31 (Raynaud's Criterion for Semi-stable Reduction, [SGA7-1, Exposé IX, Théorème 4.7]). *Let R be a henselian discrete valuation ring with fraction field K. Let n be a positive integer not divisible by the residue characteristic of R. Suppose that an abelian variety A over*

[10] t stands for "toric part", and f stands for "finite part."

K satisfies that $K(A[n](\overline{K}))$ is unramified over K (i.e. the inertia group I_K acts trivially on $A[n](\overline{K})$).

(i) If $n > 2$, then A has semi-stable reduction.

(ii) If $n = 2$, then A acquires semi-stable reduction after a finite Galois extension K'/K where $\mathrm{Gal}(K'/K)$ is of form $(\mathbb{Z}/2\mathbb{Z})^r$.

These results give the celebrated *Semi-stable Reduction Theorem.*

Theorem 1.2.32 (Semi-stable Reduction Theorem, [SGA7-1, Exposé IX, Théorème 3.6])**.** *Let S be a noetherian regular connnected scheme of dimension 1. Let $K = K(S)$. For an abelian variety A over K, there is a finite Galois extension K'/K such that $A_{K'}$ has semi-stable reduction over $S' = S \times_K K'$. In other words, every abelian variety over K has potentially semi-stable reduction.*

The extension K' can be explicitly given by the splitting field of $A[\ell]$, where ℓ can be any odd prime different from the residue characteristic. Alternatively, one can choose the splitting field of $A[4]$ instead.

Note that these results can be easily globalized.

Theorem 1.2.33. *Let A be an abelian variety over a number field F. Let S be a finite set of primes in F, and ℓ be any (rational) prime.*

(i) A has good reduction outside primes in S if and only if $A(\ell)$ extends to an ℓ-divisible group over $\mathcal{O}_{F,S}$.

(ii) A has semi-stable reduction at primes in S if and only if the inertia groups of primes in S acts unipotently of echelon two on $A(\ell)$.

Proof. There is nothing new on the statement of (ii). For (i), we need to construct a global extension of $A(\ell)$ over $\mathcal{O}_{F,S}$. Even thought we do not yet know if such thing exists, we know what it should be. Namely, let $\mathcal{A}$ be a Néron model over $\mathcal{O}_{F,S}$. Then, $\mathcal{A}(\ell) := (\mathcal{A}[\ell^n])$ may not be an ℓ-divisible group, but it is not precisely because it may not be finite (or rather more precisely, proper). We already observed that properness of such thing can be checked fiberwise by the lemma [EGA, IV-3, Corollaire 15.7.10], and each fiber is proper as $A(\ell)_s$ extends to an ℓ-divisible group, which is nothing but $\mathcal{A}(\ell)_s$. □

We end this section by recording similar results on seeing semi-stable reduction based on Galois actions on torsion subgroups and ℓ-adic cohomology groups for later purposes.

Proposition 1.2.28 [SZ, §4]**.** *Let R be a henselian discrete valuation ring, $K = \mathrm{Frac}(R)$, and A an abelian variety of dimension g over K. Let p be the residue characteristic of R, and let I_K be the inertia group.*

(i) Let n be an integer not divisible by p. If A has semi-stable reduction, then the inertia group I_K acts unipotently of echelon two on $A[n]$. If $n \geq 5$, the converse is true.

(ii) Let k be an integer between $0 < k < 2g$, and $\ell \neq p$ be a prime number. If A has semi-stable reduction, then the inertia group I_K acts unipotently of echelon $(k+1)$ on the ℓ-adic cohomology $H^k_{\text{ét}}(X_{\overline{F}}, \mathbb{Z}_\ell)$. If k is odd, the converse is true.

1.2.3.8 Tate Modules and Faltings' Finiteness Theorems

As with p-divisible groups, we would like to see how much ℓ-adic Tate modules can tell about abelian varieties. Recall that, given an abelian variety A over a field K, the ℓ-adic Tate module is $T_\ell(A) := \varprojlim_n A[\ell^n](\overline{K})$. One then define $V_\ell(A) := T_\ell(A)[1/\ell]$ to make a representation. It is a free $\mathbb{Z}_\ell$-module, and in particular, if $\ell \neq \mathrm{char}\, K$, $A[\ell^n]$'s are étale over K, so $T_\ell(A) \cong \mathbb{Z}_\ell^{2g}$

as $\mathbb{Z}_\ell$-modules. How much information does the functor $A \mapsto T_\ell(A)$ preserve? Certainly, for abelian varieties A, B over K, we have a map

$$\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathrm{Hom}_K(A, B) \to \mathrm{Hom}_{\mathbb{Z}_\ell[G_K]}(T_\ell(A), T_\ell(B)).$$

Theorem 1.2.34 [CS, Theorem V.12.5]**.** *The above map is injective, for $\ell \neq \mathrm{char}\, K$.*

Proof sketch. As $\mathrm{End}_K(A \times_K B) = \mathrm{End}_K(A) \oplus \mathrm{Hom}_K(A, B) \oplus \mathrm{Hom}_K(B, A) \oplus \mathrm{End}_K(B)$, it is suffficient to show when $A = B$. Also, as $\mathrm{End}_K(A) \hookrightarrow \mathrm{End}^0_K(A) := \mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, one only needs to work on the isogeny category to show that $\mathrm{End}^0_K(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \to \mathrm{End}_{\mathbb{Q}_\ell[G_K]}(V_\ell(A))$ is injective. By Poincaré Complete Reducibility Theorem, Theorem 1.2.22, one can assume that A is simple. Then one shows that a degree function $\deg : \mathrm{End}_K A \to \mathbb{Z}$ extends uniquely to $\deg : \mathrm{End}^0_K(A) \to \mathbb{Q}$, and it becomes a "polynomial function," i.e. a polynomial function whenever restricted to a finite dimensional subspace. One shows by using this fact that $\mathrm{End}_K(A)$ is $\mathbb{Z}$-finite. Then one can explicitly show that an element in the kernel of $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} \mathrm{End}_K(A) \to \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell A)$ is zero by using finite generation of $\mathrm{End}_K(A)$. □

In particular, using the fact that the degree function is a polynomial, we can define a *characteristic polynomial* of an element $\varphi \in \mathrm{End}_K(A)$ as the polynomial $n \mapsto \deg(\varphi - n)$. It is a monic polynomial of degree $2 \dim A$ with integer coefficients. If K is a finite field, G_K is topologically generated by the Frobenius map $x \mapsto x^q$, and one can think of the characteristic polynomial f_A of the Frobenius endomorphism on $V_\ell(A)$. It turns out that f_A, a monic polynomial with integer coefficients, classifies the isogeny class of A.

It is a very nontrivial theorem of Tate, Zahrin and Faltings that this map is an isomorphism for many cases of K, and this is an important piece in Faltings' proof of Mordell Conjecture. That it is an isomorphism is called the *Isogeny Theorem*.

Theorem 1.2.35 (Isogeny Theorems)**.** *For abelian varieties A, B over a field K and $\ell \neq \mathrm{char}\, K$, the map $\mathrm{Hom}_K(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{End}_{\mathbb{Z}_\ell[G_K]}(T_\ell(A), T_\ell(B))$ is an isomorphism, when*
(i) (Tate, [CS, I.§6]) if K is a finite field,
(ii) (Zahrin, [CS, I.§7]) if K is a global function field, or
(iii) (Faltings, [CS, Theorem II.5.4]) if K is a number field.

This is accompanied with the following another nontrivial theorems, usually referred as the *Semi-simplicity Theorem.*

Theorem 1.2.36 (Semi-simplicity Theorems)**.** *For an abelian variety A over a field K and $\ell \neq \mathrm{char}\, K$, the rational ℓ-adic Tate module is a semisimple G_K-representation, when*
(i) (Tate, [CS, I.§6]) if K is a finite field, or
(ii) (Falting, [CS, Theorem II.5.3]) if K is a number field.

These are very strong results. For example, one deduces the following criterion on determining isogenous abelian varieties.

Theorem 1.2.37. *Let k be a finite field. For abelian varieties A, B over k, the following are equivalent.*
(i) A and B are k-isogenous.
(ii) $V_\ell(A)$ and $V_\ell(B)$ are isomorphic as ℓ-adic representations of G_k, for some $\ell \neq \mathrm{char}\, k$.
(iii) $f_A = f_B$.
(iv) For each finite extension k'/k, $\#A(k') = \#B(k')$.

Proof. That (i) implies (ii) implies (iii) is obvious. (iii) implies (ii) as semisimple G_k-representations are determined by eigenvalues of Frobenius. To show that (ii) implies (i), suppose $\mathrm{Hom}^0_k(A,B)\otimes_{\mathbb{Q}}\mathbb{Q}_\ell = \mathrm{Hom}_{\mathbb{Q}_\ell[G_k]}(V_\ell A, V_\ell B)$ contains an isomorphism. We can approximate the isomorphism by elements of $\mathrm{Hom}^0_k(A,B)$. As being an isogeny is determined by degree, any homomorphism sufficiently close to an isomorphism is an isomorphism. Therefore, there is an isomorphism in $\mathrm{Hom}^0_k(A,B)$, which means that A, B are isogenous to each other.

Note also that, if k'/k is of degree h, then as $\#A(k')$ is the number of fixed points of the map $x \mapsto x^{\#k'}$, $\#A(k') = \prod(1-\alpha_i^h)$, where α_i's are eigenvalues of the Frobenius. Thus, (iv) holds if and only if the eigenvalues of the Frobenius are the same if and only if (iii) holds. □

The Isogeny and Semi-simplicity Theorems eventually enable us to prove various finiteness results.

Theorem 1.2.38 (Faltings' Finiteness Theorems, [CS, II.§6])**.** *Over a number field K, the following are true.*

(i) The Shafarevich conjecture for curves is true.

(ii) The Shafarevich conjecture for abelian varieties is true.

(iii) Given an abelian variety A over K, there are only finitely many K-abelian varieties, up to isomorphism, isogenous to A.

(iv) The Mordell conjecture is true; namely, a K-curve of genus ≥ 2 has only finitely many K-rational points.

1.3 Nonexistence of Abelian Scheme over $\mathbb{Z}$

We are ready to prove the nonexistence of abelian variety over $\mathbb{Q}$ with everywhere good reduction. Although the spirit of the proof comes from [Fo1], there are several ways to proceed from the main ramification bound (Theorem 1.1.1). In particular, we will give several different results that p-divisible groups and finite flat commutative p-group over the ring of integer of a small number field are of certain simple forms. These results will imply the nonexistence of abelian variety over a small number field with everywhere good reduction. The following proofs are originated from [Fo1] and [Sc2].

1.3.1 Fontaine's Ramification Bound

Our objective of this section is to prove the aforementioned following theorem about the ramification number of field of definition of a finite flat group scheme.

Theorem 1.1.1. *Let K be a finite extension of $\mathbb{Q}_p$, and let $e = v_K(p)$ be the absolute ramification index. For an integer $n \geq 1$, suppose Γ is a finite flat commutative group scheme over $\mathcal{O}_K$ killed by p^n. Let $L = K(\Gamma(\overline{K}))$, and $G = \mathrm{Gal}(L/K)$. Then, $G^{(u)} = 1$ for $u > e\left(n + \frac{1}{p-1}\right)$, and $v(\mathfrak{D}_{L/K}) < e\left(n+\frac{1}{p-1}\right)$, where $\mathfrak{D}_{L/K}$ is the different of L/K.*

First, we fix the notations. Let K be a complete discrete valuation ring with mixed characteristic $(0,p)$ and L/K be a finite extension. Let $\pi_L \in \mathcal{O}_K$ be a uniformizer, v_K a valuation normalized such that $v_K(\pi_K) = 1$. Choose π_L to be a uniformizer of $\mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. Let v_L be the extended valuation of v_K such that $v_L(\pi_L) = 1/e_{L/K}$, where $e_{L/K}$ is the ramification index of L/K. For $\sigma \in G = \mathrm{Gal}(L/K)$, we define $i_{L/K}(\sigma) = v_L(\sigma(\pi_L) - \pi_L)$. We can then define a piecewise linear continuous increasing function $\phi_{L/K} : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ by $\phi_{L/K}(i) = \sum_{\sigma\in G}\min(i, i_{L/K}(\sigma))$. Let $\psi_{L/K}$ be the inverse function of $\phi_{L/K}$. Define

$u_{L/K}(\sigma) = \phi_{L/K}(i_{L/K}(\sigma))$. Let $i_{L/K} = \sup_{\sigma\neq 1} i_{L/K}(\sigma)$, $u_{L/K} = \sup_{\sigma\neq 1} u_{L/K}(\sigma)$. Finally, we define the *lower/upper ramification groups* as follows.

$$G_{(i)} = \{\sigma \in G \mid i_{L/K}(\sigma) \geq i\}, G^{(u)} = \{\sigma \in G \mid u_{L/K}(\sigma) \geq u\}.$$

This upper/lower numbering of ramification groups is slightly different from the usual convention, e.g. [Se, Chapter IV]. If G_i, G^u are the usual notations in [Se, Chapter IV], then our notations are related as

$$G_{(i)} = G_{e_{L/K}i-1}, G^{(u)} = G^{u-1}.$$

1.3.1.1 Ramification of Complete Intersection Algebra

Using the basic ramification theory, we will prove the following.

Proposition 1.3.1 [Fo1, Proposition 1.7]**.** *Let A be a finite flat $\mathcal{O}_K$-algebra of form $A = \mathcal{O}_K[[x_1, \cdots, x_m]]/\langle f_1, \cdots, f_m\rangle$. Suppose there exists an element $0 \neq a \in \mathcal{O}_K$ annihilating $\Omega^1_{A/\mathcal{O}_K}$, so that $\Omega^1_{A/\mathcal{O}_K}$ is a flat A/aA-module.*

(i) Suppose S is a finite flat $\mathcal{O}_K$-algebra and I is a topologically nilpotent divided power ideal. Then,

$$\mathrm{Hom}_{\mathcal{O}_K}(A, S) = \mathrm{im}(\mathrm{Hom}_{\mathcal{O}_K}(A, S/aI) \to \mathrm{Hom}_{\mathcal{O}_K}(A, S/I)).$$

(ii) If L is the field over K generated by the $\overline{K}$-points of $Y = \operatorname{Spec} A$ (notationally $L = K(Y(\overline{K}))$), then $u_{L/K} \leq v_K(a) + \frac{e_K}{p-1}$.

Before proving the theorem, we define some terms. For a finite flat $\mathcal{O}_K$-scheme $X = \operatorname{Spec} B$, $K(X(\overline{K}))$, the field generated by $\overline{K}$-valued points of X, is defined as follows: as $B_K = B \otimes_{\mathcal{O}_K} K$ is finite over K and $\Omega^1_{B_K/K} = \Omega^1_{B/\mathcal{O}_K} \otimes_{\mathcal{O}_K} K = 0$, B_K is a finite étale algebra over K; thus, B_K is a finite product of finite separable extensions $L_1, \cdots, L_m$ of K. We can then define $K(X(\overline{K}))$ to be the compositum of L_i's in a fixed algebraic closure $\overline{K}$.

For a finite flat $\mathcal{O}_K$-algebra S, an ideal $I \subset S$ is a *divided power ideal* if, for all $x \in I$ and $n \in \mathbb{N}$, the element $\gamma_n(x) = x^n/n!$ is also an element of I. We define $I^{[m]}$ 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 *topologically nilpotent* if $\cap_{m=1}^{\infty} I^{[m]} = 0$.

Proof of Proposition 1.3.1(i). (i) Let $\mathfrak{m}_A$ be the maximal ideal of A (A is local!) and $J = \langle f_1, \cdots, f_m\rangle \subset \mathcal{O}_K[[x_1, \cdots, x_m]]$. As $\Omega^1_{A/\mathcal{O}_K}$ is a free A/aA-module (A is local!), we have $\frac{\partial f_i}{\partial x_j} = ap_{ij}$ for some $p_{ij} \in A$. Also, as $a \cdot dx_i$ should be expressed as a linear combination of df_j's, the coefficient matrices will form an inverse matrix of the matrix (p_{ij}). In particular, the matrix (p_{ij}) is invertible.

The statement of (i) will follow if, given an $\mathcal{O}_K$-homomorphism $\phi : A \to S/aI$, we can *uniquely* lift ϕ to an $\mathcal{O}_K$-homomorphism $\phi : A \to S$. Note that $I^{[1]} = I$ and $\cap I^{[n]} = 0$. We will inductively lift $\phi : A \to S/aI^{[n]}$ to $\phi : A \to S/aI^{[n+1]}$. To be more precise, given $u_1, \cdots, u_m \in S$ such that $f_i(u_1, \cdots, u_m) \in aI^{[n]}$, we want to find $\epsilon_i \in I^{[n]}$, unique modulo $I^{[n+1]}$, such that $f(u_1 + \epsilon_1, \cdots, u_m + \epsilon_m) \in aI^{[n+1]}$. The *unique* lifting will then follow and the proof of (i) will be finished.

Using the Taylor expansion, we have

$$\begin{aligned} f_i(u_1 + \epsilon_1, \cdots, u_m + \epsilon_m) &= f_i(u_1, \cdots, u_m) + \sum_{j=1}^{m} \frac{\partial f_i}{\partial x_j}(u_1, \cdots, u_m)\epsilon_j \\ &\quad + \sum_{|r|\geq 2} \frac{\partial^r f_i}{\partial x_r}(u_1, \cdots, u_m)\frac{\epsilon^r}{r!}, \end{aligned}$$

where $\epsilon^r = \prod_k \epsilon_k^{r_k}$. The series converges as I is a topologically nilpotent divided power ideal. Lift p_{ij}'s to A, and we have $\frac{\partial f_i}{\partial x_j} = ap_{ij} + r_{ij}$ where $r_{ij} \in J$. As $f_i(u_1, \cdots, u_m) \in aI^{[n]}$, we have

$$\frac{\partial f_i}{\partial x_j}(u_1, \cdots, u_m)\epsilon_j = ap_{ij}(u_1, \cdots, u_m)\epsilon_j + r_{ij}(u_1, \cdots, u_m)\epsilon_j.$$

Note that, as $r_{ij} \in J$, $r_{ij}(u_1, \cdots, u_m)\epsilon_j \in aI^{[n]}I^{[n]} \subset aI^{[n+1]}$. Similarly, for $r_1 + \cdots + r_m \geq 2$, the higher derivatives $\frac{\partial^{r_1+\cdots+r_m} f_i}{\partial x_1^{r_1}\cdots\partial x_m^{r_m}}$ are a sum of a polynomial in J and a multiple of a. Therefore, $\frac{\partial^{r_1+\cdots+r_m} f_i}{\partial x_1^{r_1}\cdots\partial x_m^{r_m}}(u_1, \cdots, u_m)$ is a multiple of a. An important point is the following.

Claim. For $|r| \geq 2$, $\frac{\epsilon^r}{r!}$ *is in* $I^{[n+1]}$, i.e. $(I^{[n]})^{[2]} \subset I^{[n+1]}$.

To show this, it is sufficient to show that $x \in I^{[n]}$ implies $x^2/2 \in I^{[n+1]}$. We can further assume that $x = \frac{x_1^{a_1}\cdots x_t^{a_t}}{a_1!\cdots a_t!}$ for $a_1 + \cdots + a_t \geq n$, $x_1, \cdots, x_t \in I$. Note however that

$$\begin{aligned} \frac{x^2}{2} &= \frac{x_1^{2a_1}\cdots x_t^{2a_t}}{2a_1!^2\cdots a_t!^2} \\ &= \frac{x_1^{2a_1}\cdots x_t^{2a_t}}{(2a_1)!\cdots(2a_t)!}\cdot\frac{1}{2}\binom{2a_1}{a_1}\cdots\binom{2a_t}{a_t} \\ &= \frac{x_1^{2a_1}\cdots x_t^{2a_t}}{(2a_1)!\cdots(2a_t)!}\cdot\binom{2a_1-1}{a_1-1}\binom{2a_2}{a_2}\cdots\binom{2a_t}{a_t} \in I^{[2n]} \subset I^{[n+1]}. \end{aligned}$$

Appplying this to the Taylor expansion, we have

$$f_i(u_1+\epsilon_1, \cdots, u_m+\epsilon_m) \equiv f_i(u_1, \cdots, u_m) + a\sum_j p_{ij}(u_1, \cdots, u_m)\epsilon_j \pmod{aI^{[n+1]}}.$$

Thus it is sufficient to show that there are unique $\epsilon_1, \cdots, \epsilon_m \in I^{[n]}$ such that

$$\sum_j p_{ij}(u_1, \cdots, u_m)\epsilon_j \equiv -f_i(u_1, \cdots, u_m) \pmod{I^{[n+1]}}.$$

As $(p_{ij}) \in \mathrm{GL}_m(A)$, $(p_{ij}(u_1, \cdots, u_m)) \in \mathrm{GL}_m(S)$, which means that the solution is unique. Finally, the unique solution is in $I^{[n]}$, as $-f_i(u_1, \cdots, u_m) \in I^{[n]}$. □

1.3.1.2 Converse to Krasner's Lemma

To prove Proposition 1.3.1(ii), we first need a lemma.

Lemma 1.3.1 [Fo1, Proposition 1.5]**.** *For any finite Galois extension E/K and a positive real number t, denote $\mathfrak{m}_E^t = \{x \in \mathcal{O}_E \mid v(x) \geq t\}$, where v is the unique extended valuation of v_K.*

(i) If $t > u_{L/K}$, then for any finite Galois extension E/K, every $\mathcal{O}_K$-algebra homomorphism $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}_E^t$ lifts to an $\mathcal{O}_K$-algebra homomorphism $\mathcal{O}_L \to \mathcal{O}_E$.

(ii) Given a finite Galois extension E/K and a positive real number t, if every $\mathcal{O}_K$-algebra homomorphism $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}_E^t$ lifts to an $\mathcal{O}_K$-algebra homomorphism $\mathcal{O}_L \to \mathcal{O}_E$, then $t > u_{L/K} - \frac{1}{e_{L/K}}$.

Proof. (i) Let $f(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of π_L. An $\mathcal{O}_K$-algebra homomorphism $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}_E^t$ is determined by its image $\beta \in \mathcal{O}_E$ of π_L, where β must satisfy $v(f(\beta)) \geq t > u_{L/K}$. On the other hand, we claim that $v(f(\beta)) = \phi_{L/K}(\sup_{g\in G} v(\beta - g\pi_L))$, where v is the unique valuation of an algebraic closure containing both L and E. Suppose $g_0 \in G$ achieves the maximum of $v(\beta - g\pi_L)$. For all $g \in G$, $v_K(\beta - g\pi_L) = \min\{v_K(\beta - g_0\pi_L), v_K(g_0(\pi_L - g_0^{-1}g\pi_L))\} = \min\{v_K(\beta - g_0\pi_L), i_{L/K}(g_0^{-1}g)\}$. As $f(\beta) = \prod_{g\in G}(\beta - g\pi_L)$, the claim follows.

By the claim, we get $v(\beta - g_0\pi_L) = \sup_{g\in G} v(\beta - g\pi_L) > i_{L/K} = \sup_{1\neq g\in G} v(g\pi_L - \pi_L)$, for some $g_0 \in G$. By Krasner's lemma, $K(g_0\pi_L) = L \subset K(\beta) \subset E$, which induces a lift $\mathcal{O}_L \to \mathcal{O}_E$.

(ii) It is sufficient to prove that, for $t = u_{L/K} - \frac{1}{e_{L/K}}$, there is an $\mathcal{O}_K$-algebra map $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}_E^t$ which does not lift to an $\mathcal{O}_K$-algebra map $\mathcal{O}_L \to \mathcal{O}_E$. Let $L/K'/K$ be the maximal unramified extension. As a base change of an étale morphism is étale, $E \otimes_K K' = \prod E_i$ is unramified over E, where E_i/E's are finite unramified extensions of E. Taking any E_i, any $\mathcal{O}_K$-algebra map $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}_E^t$ extends to an $\mathcal{O}_{K'}$-algebra map $\mathcal{O}_L \to \mathcal{O}_{E_i}/\mathfrak{m}_{E_i}^t$. As $u_{L/K} = u_{L/K'}$ and $e_{L/K} = e_{L/K'}$, we can therefore assume that L/K is totally ramified. Also, we can assume that $L \neq K$.

Suppose L/K is tamely ramified, then $v_L(g\pi_L - \pi_L) > \frac{1}{e_{L/K}}$ implies $g = 1$. Thus, $i_{L/K}(g) = \frac{1}{e_{L/K}}$ for all $1 \neq g \in G$, so $i_{L/K} = \frac{1}{e_{L/K}}$. Therefore, $u_{L/K} = 1$, and $t = 1 - \frac{1}{e_{L/K}}$. Take E/K be any totally ramified extension of degree $d < e_{L/K}$. There is no $\mathcal{O}_K$-algebra map $\mathcal{O}_L \to \mathcal{O}_E$, as they have different ramification indices. On the other hand, define $f : \mathcal{O}_L \to \mathcal{O}_E/\pi_K^t\mathcal{O}_E$ as sending π_L to a uniformizer π_E of E. As $v_L(\prod_{g\in G}(g\pi_L - \pi_E)) = \frac{[L:K]}{e_{L/K}} = 1$, this is a well-defined map. This proves the case when L/K is tamely ramified.

If L/K is wildly ramified, then for all $g \in G$ with $g \neq 1$, $e_{L/K}i_{L/K}(g) \geq 1$, and as $p \mid [L : K]$, $p - 1$ of $g \in G - \{1\}$ satisfies $e_{L/K}i_{L/K}(g) \geq 2$. Therefore, $t > 1$. As $e_{L/K}t$ is an integer, let $e_{L/K} = e_{L/K}r + s$ where $r, s \in \mathbb{N}$ with $s < e_{L/K}$. Let $f[x] \in \mathcal{O}_K[x]$ be the minimal polynomial of π_L, and let $g(x) = f(x) - \pi_K^r x^s$. As $e_{L/K} > s$, this polynomial is monic, and $r \geq 1$, so π_K divides all coefficients of g other than the top coefficient. As f is Eisenstein, if $s > 0$, g is automatically Eisenstein; if $s = 0$, $r \geq 2$, so again g is Eisenstein. Let β be a root of $g(x)$, and let $E = K(\beta)$. As g is Eisenstein, E/K is totally ramified. We claim that the map $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}_E^t$ sending π_L to β is a well-defined $\mathcal{O}_K$-algebra map. This is because $v(\beta) = \frac{1}{e_{L/K}}$, and $f(\beta) = \pi_K^r\beta^s$, so $v(f(\beta)) = v(\pi_K^r\beta^s) = t$.

Now it remains to show that there is no $\mathcal{O}_K$-algebra map $\mathcal{O}_L \to \mathcal{O}_E$. If not, this implies $L \subset E$. As both extensions L/K and E/K have the same degree, $L = E$. Thus, $v(g\pi_L - \beta) \in \frac{1}{e_{L/K}}\mathbb{Z}$ for all $g \in G$. On the other hand, $v_K(\prod_{g\in G}(g\pi_L - \beta)) = v_K(f(\beta)) = v_K(\pi_K^r\beta^s) = t$. Thus,

$$e_{L/K} \sup_{g\in G} v(g\pi_L - \beta) = e_{L/K}\phi_{L/K}^{-1}(v_K(f(\beta))) = e_{L/K}\phi_{L/K}^{-1}(t)$$

is an integer. Let d be the slope of the left segment of $\phi_{L/K}$ at $i_{L/K}$. This is precisely the cardinality of $G_{(i_{L/K})}$. Then, $e_{L/K}\phi_{L/K}^{-1}(t) = e_{L/K}(i_{L/K} - \frac{1}{e_{L/K}d}) = e_{L/K}i_{L/K} - \frac{1}{d}$. This implies that $d = 1$. However, as $G_{(i_{L/K})} \neq 1$, this is a contradiction. □

This is certainly not a difficult conclusion. In particular, one can kill the error term $e_{L/K}^{-1}$ by taking an arbitrarily large tamely ramified base change. We record this for later use.

Theorem 1.3.1 [Y, Proposition 3.3]**.** *With the same notation as Lemma 1.3.1, one can improve (ii) by $t \geq u_{L/K}$ instead of $t > u_{L/K} - \frac{1}{e_{L/K}}$.*

1.3.1.3 Ramification Bound

Now we can finish the proof of Proposition 1.3.1.

Proof of Proposition 1.3.1(ii). If L/K is tamely ramified, then $u_{L/K} \leq 1 \leq v_K(a) \leq v_K(a) + \frac{e}{p-1}$, so we can assume that L/K is wildly ramified. Here we use Lemma 1.3.1. Specifically, we will show the following.

Claim. For $t > v_K(a) + \frac{e_K}{p-1}$ and a finite Galois extension E/K, any $\mathcal{O}_K$-algebra homomorphism $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}_E^t$ lifts to an $\mathcal{O}_K$-algebra homomorphism $\mathcal{O}_L \to \mathcal{O}_E$.

If this is true, then $v_K(a) + \frac{e_K}{p-1} \geq u_{L/K} - \frac{1}{e_{L/K}}$, so $u_{L/K} \leq v_K(a) + \frac{e_K}{p-1} + \frac{1}{e_{L/K}}$. As $e_{L/K}i_{L/K}(g)$ is an integer for all $g \in G - \{1\}$ and $|G_{(i)}|$ is divisible by p for all $i \leq i_{L/K}$, it follows that $e_{L/K}u_{L/K}$ is an integer divisible by p. On the other hand, by the claim,

$$e_{L/K}(p-1)u_{L/K} \leq e_{L/K}(p-1)v_K(a) + e_{L/K}e_K + p - 1.$$

As $e_{L/K}$ is divisible by p, $e_{L/K}(p-1)v_K(a) + e_{L/K}e_K$ is divisible by p. As $e_{L/K}(p-1)u_{L/K}$ is divisible by p, It turns out that

$$e_{L/K}(p-1)u_{L/K} \leq e_{L/K}(p-1)v_K(a) + e_{L/K}e_K,$$

or $u_{L/K} \leq v_K(a) + \frac{e_K}{p-1}$, as desired.

Thus, it remains to prove the claim. As $Y(\mathcal{O}_L)$ realizes all geometric points of Y as L-rational points (by the definition of L), for any finite Galois E/K, $\#Y(\mathcal{O}_E) \leq \#Y(\overline{K}) = \#Y(\mathcal{O}_L)$ with equality if and only if $L \subset E$ if and only if there is an $\mathcal{O}_K$-algebra map $\mathcal{O}_L \to \mathcal{O}_E$.

Note that $\mathfrak{m}_E^t = a\mathfrak{m}_E^{t-v(a)}$. As $t - v(a) > \frac{e_K}{p-1}$, $\mathfrak{m}_E^{t-v(a)}$ is a divided power ideal[11]. Also, it is obviously topologically nilpotent. Given a map $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}_E^t$, the kernel of the composition $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}_E^t \to \mathcal{O}_E/\mathfrak{m}_E^{t-v(a)}$, which is just $\mathfrak{m}_L^{t-v(a)}$, is also a topologically nilpotent divided power ideal by the same reason. We apply (i) of Proposition 1.3.1 to get

$$\mathrm{Hom}_{\mathcal{O}_K}(A, \mathcal{O}_E) = \mathrm{im}(\mathrm{Hom}_{\mathcal{O}_K}(A, \mathcal{O}_E/a\mathfrak{m}_E^{t-v(a)}) \to \mathrm{Hom}_{\mathcal{O}_K}(A, \mathcal{O}_E/\mathfrak{m}_E^{t-v(a)}))$$

and

$$\mathrm{Hom}_{\mathcal{O}_K}(A, \mathcal{O}_L) = \mathrm{im}(\mathrm{Hom}_{\mathcal{O}_K}(A, \mathcal{O}_L/a\mathfrak{m}_L^{t-v(a)}) \to \mathrm{Hom}_{\mathcal{O}_K}(A, \mathcal{O}_L/\mathfrak{m}_L^{t-v(a)})).$$

As we are given a map $\mathcal{O}_L \to \mathcal{O}_E/\mathfrak{m}_E^t$, composing this map with an element in $Y(\mathcal{O}_L) = \mathrm{Hom}_{\mathcal{O}_K}(A, \mathcal{O}_L)$, which is an element in $\mathrm{Hom}_{\mathcal{O}_K}(A, \mathcal{O}_L/\mathfrak{m}_L^t)$. gives an element in $Y(\mathcal{O}_E) = \mathrm{Hom}_{\mathcal{O}_K}(A, \mathcal{O}_E)$, which is an element in $\mathrm{Hom}_{\mathcal{O}_K}(A, \mathcal{O}_E/\mathfrak{m}_E^t)$. This is necessarily injective by the definition of L being the field of definition of $Y = \mathrm{Spec}\, A$. Thus, $\#Y(\mathcal{O}_E) = \#Y(\mathcal{O}_L)$, so $L \subset E$, and the claim follows. □

Proposition 1.3.1 proves the main ramification bound, Theorem 1.1.1.

Theorem 1.1.1. *Let K be a finite extension of $\mathbb{Q}_p$, and let $e = v_K(p)$ be the absolute ramification index. For an integer $n \geq 1$, suppose Γ is a finite flat commutative group scheme over $\mathcal{O}_K$ killed by p^n. Let $L = K(\Gamma(\overline{K}))$, and $G = \mathrm{Gal}(L/K)$. Then, $G^{(u)} = 1$ for $u > e\left(n + \frac{1}{p-1}\right)$, and $v(\mathfrak{D}_{L/K}) < e\left(n + \frac{1}{p-1}\right)$, where $\mathfrak{D}_{L/K}$ is the different of L/K.*

Proof. We just need to prove that $u_{L/K} \leq e\left(n + \frac{1}{p-1}\right)$; the statement about the valuation of different follows from the general fact that $v(\mathfrak{D}_{L/K}) = u_{L/K} - i_{L/K}$. This is because $v(\mathfrak{D}_{L/K}) = v(\prod_{1\neq g\in G}(g\pi_L - \pi_L))$. As $u_{L/K} = \phi_{L/K}(i_{L/K})$, we have

$$\begin{aligned} u_{L/K} &= \sum_{g\in G} \min(i_{L/K}, i_{L/K}(g)) \\ &= i_{L/K} + \sum_{1\neq g\in G} i_{L/K}(g) \\ &= i_{L/K} + v(\prod_{1\neq g\in G}(g\pi_L - \pi_L)) \\ &= i_{L/K} + v(\mathfrak{D}_{L/K}), \end{aligned}$$

[11] This follows by looking at the valuations of factorials.

which implies that $v(\mathfrak{D}_{L/K}) < u_{L/K} \le e\left(n + \frac{1}{p-1}\right)$.

Let $\Gamma = \operatorname{Spec} A$. Suppose first that $\Omega^1_{A/\mathcal{O}_K}$ is a free A/p^nA-module. As k is perfect, by Proposition 1.2.3(iv), $\Gamma_k = \operatorname{Spec} A \otimes_{\mathcal{O}_K} k$ is a direct product $\Gamma_k^{\text{ét}} \times \Gamma_k^0$. By the classification result, Theorem 1.2.5, in particular we deduce that $A \otimes_{\mathcal{O}_K} k$, thus A, is locally of complete intersection. Thus, $A = \prod_i A_i$ with each A_i of form $A_i = \mathcal{O}_{K_i}[[x_1, \cdots, x_m]]/(f_{i1}, \cdots, f_{im})$ for some unramified extensions K_i/K. This enables us to apply Proposition 1.3.1(ii).

Now it only remains to reduce the problem to the case when $\Omega^1_{A/\mathcal{O}_K}$ is a free A/p^nA-module. For a general case, note that, by Theorem 1.2.16, we can embed Γ into an abelian scheme X over $\mathcal{O}_K$, as $\mathcal{O}_K$ is local. As $X[p^n](\overline{K})$ contains $\Gamma(\overline{K})$, it is sufficient to prove the theorem for $X[p^n]$. On the other hand, the exact sequence of étale group schemes

$$0 \to X[p^n] \to X \xrightarrow{[p^n]} X \to 0$$

gives us

$$0 \to \Omega^1_{X/\mathcal{O}_K} \xrightarrow{[p^n]} \Omega^1_{X/\mathcal{O}_K} \to \Omega^1_{X[p^n]/\mathcal{O}_K} \to 0.$$

As $\Omega^1_{X/\mathcal{O}_K}$ is a (locally) free $\mathcal{O}_K$-module, $\Omega^1_{X[p^n]/\mathcal{O}_K}$ is a free $\mathcal{O}_K/p^n\mathcal{O}_K$-module and we can use the argument discussed in the previous paragraph. □

Remark 1.3.1. In [Fo1], Fontaine conjectured that a similar ramification bound holds for étale cohomologies of a proper smooth scheme over a ring of Witt vectors. It is indeed a generalization of Theorem 1.1.1, as what we are really analyzing is the first étale cohomology group of an abelian variety. It is proved in [Ab3], which will be discussed in the next chapter.

We record the global consequences, which we will be really using in proving nonexistence results.

Theorem 1.3.2 [Fo1, Théorème 3, Corollaire 3.3.2]**.** *Let E be a number field, and fix an algebraic clousre $\overline{E}$. Let Γ be a finite flat commutative $\mathcal{O}_E$-group scheme killed by p^n, and let $F = E(\Gamma(\overline{E}))$. For all prime ideal $\mathfrak{p} \subset \mathcal{O}_E$, 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 $\Delta_{F/E}$. Then we have the following.*

(i) If $\mathfrak{p}$ does not divide p, $r_{\mathfrak{p}} = 0$. In other words, F/E is unramified outside p.

(ii) If $\mathfrak{p}$ divides p,

$$r_{\mathfrak{p}} < [F : E]e_{\mathfrak{p}}\left(n + \frac{1}{p-1}\right).$$

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

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

Proof. (i) Let $\Gamma = \operatorname{Spec} A$. As A is killed by p^n, it annihilates I/I^2, where I is the augmentation ideal of A. Thus, p^n annihilates $\Omega^1_{\Gamma/\mathcal{O}_E} = A \otimes_{\mathcal{O}_E} I/I^2$. As p^n is a unit in $\kappa(\mathfrak{p})$, $\Omega^1_{\Gamma_{\kappa(\mathfrak{p})}/\kappa(\mathfrak{p})}$, killed by p^n, is zero. Thus, $\Gamma_{\kappa(\mathfrak{p})}$ is étale. By Proposition 1.2.11, $\Gamma_{\mathcal{O}_{E_{\mathfrak{p}}}}$ is étale. Thus, $A \otimes_{\mathcal{O}_E} \mathcal{O}_{E_{\mathfrak{p}}}$ is the product of unramified extensions $\mathcal{O}_{E'} \supset \mathcal{O}_{E_{\mathfrak{p}}}$. Thus $A \otimes_{\mathcal{O}_E} E_{\mathfrak{p}}$ is the product of unramified extensions of $E_{\mathfrak{p}}$, which implies that any direct factor of $A \otimes_{\mathcal{O}_E} E$ is a field extension of E unramified at $\mathfrak{p}$. Thus, F/E, which is the compositum of those direct factors, is unramified at $\mathfrak{p}$.

(ii) Let $\mathfrak{P}_1, \cdots, \mathfrak{P}_g$ be prime ideals of F dividing $\mathfrak{p}$. Let $m = v(\mathfrak{D}_{F_{\mathfrak{P}_1}/E_{\mathfrak{p}}})$. By Theorem 1.1.1, we know that $m < ee_{\mathfrak{p}}\left(n + \frac{1}{p-1}\right)$. As F/E is Galois, we know that $\mathfrak{P}_i$'s are Galois conjugate to each other. Thus, the contribution of $\mathfrak{p}$ in $\Delta_{F/E}$ is $N_{F/E}((\mathfrak{P}_1\cdots\mathfrak{P}_g)^m) = \mathfrak{p}^{mfg}$, where f is the degree of the residue field extension of $F_{\mathfrak{P}_1}/E_{\mathfrak{p}}$. Thus,

$$r_{\mathfrak{p}} = mfg = efge_{\mathfrak{p}}\left(n+\frac{1}{p-1}\right) = [F:E]e_{\mathfrak{p}}\left(n+\frac{1}{p-1}\right).$$

(iii) Let the prime factorization of (p) in E be denoted as $(p)=\prod_{i=1}^h \mathfrak{p}_i^{e_i}$. By (i) and (ii), $\Delta_{F/E}=\prod_{i=1}^h \mathfrak{p}_i^{r_i}$, where $r_i < [F:E]e_i\left(n+\frac{1}{p-1}\right)$. Recall that

$$\Delta_{F/\mathbb{Q}} = \Delta_{E/\mathbb{Q}}^{[F:E]} N_{E/\mathbb{Q}}(\Delta_{F/E}).$$

Let f_i be the degree of the residue field extension of $E_{\mathfrak{p}_i}/\mathbb{Q}_p$. Then, $N_{E/\mathbb{Q}}(\Delta_{F/E}) = (p^r)$, where $r=\sum_{i=1}^h f_ir_i$. Therefore, taking the $[F:\mathbb{Q}]$-th roots on both sides, we now know that

$$|d_F|^{\frac{1}{[F:\mathbb{Q}]}} = |d_E|^{\frac{1}{[E:\mathbb{Q}]}} p^{\frac{r}{[F:\mathbb{Q}]}}.$$

Then, the following proves the statement.

$$\frac{r}{[F:\mathbb{Q}]} = \sum_{i=1}^h \frac{f_ir_i}{[F:\mathbb{Q}]} < \left(n+\frac{1}{p-1}\right)\sum_{i=1}^h \frac{f_ie_i[F:E]}{[F:\mathbb{Q}]} = \left(n+\frac{1}{p-1}\right)\frac{[E:\mathbb{Q}]}{[E:\mathbb{Q}]} = n+\frac{1}{p-1}.$$

□

1.3.2 Constraints on p-groups and p-divisible Groups

1.3.2.1 Results of Fontaine

The ramification bounds we proved in the previous section give severe restrictions on the field F generated by geometric points of a p-group over the ring of integers of a small number field. In particular, it gives an upper bound on the absolute discriminant d_F. Combined with the Odlyzko discriminant bound [Mar], we can bound the degree $[F:\mathbb{Q}]$, and this reduces us to consider only finitely many cases. The low-degree cases have very simple structures, thanks to the following.

Proposition 1.3.2 [Fo1, Proposition 3.2.1]**.** *Let k be an algebraically closed field of characteristic p, which is an odd prime, $W=W(k)$, $K=\operatorname{Frac}W$, and $\overline{K}$ an algebraic closure of K. Let Γ be a finite flat commutative W-group scheme killed by p, and let $L=K(\Gamma(\overline{K}))$. 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 exists integers r,s such that $\Gamma\cong(\mathbb{Z}/p\mathbb{Z})^r\otimes\mu_p^s$.*
2. *$[L:K]=p(p-1)$, and there exists integers r,s and a short non-split exact sequence $0\to\mu_p^s\to\Gamma\to(\mathbb{Z}/p\mathbb{Z})^r\to 0$.*
3. *L/K is cyclic of degree p^2-1.*
4. *$[L:K]\geq p^2(p-1)$.*

Proof. Note that as $e=1<p-1$, so we can use the results of Section 1.2.1.7. In particular, by embedding the category of finite flat commutative W-group schemes of p-power order inside the category of finite flat commutative K-group schemes of p-power order, we see that the category of finite flat commuatitve W-group schemes of p-power order is an abelian category. In particular, any such group scheme has a Jordan-Hölder composition series. Note also that, by Cartier's

theorem, Theorem 1.2.2, and the equivalence of categories in Section 1.2.1.4, $G \mapsto G(\overline{K})$ is an equivalence of categories from the category of finite flat commutative K-group schemes killed by p to the category of finite $\mathbb{F}_p[G_K]$-modules, where α is a geometric point in $\operatorname{Spec} W$. The classification of Raynaud F-schemes in [R] can be translated into the language of $\mathbb{F}_p[G_K]$-modules in this case as follows.

- A simple $\mathbb{F}_p[G_K]$-module M of dimension h is a 1-dimensional $\mathbb{F}_{p^h}$-vector space, with the G_K-action given by $\chi_h^{i_0+pi_1+\cdots+p^{h-1}i_{h-1}}$ for integers $0 \le i_0, \cdots, i_{h-1} \le p-1$, not all equal to $p-1$, where $\chi_h : G_K \to \mathbb{F}_{p^h}^\times$ is a character sending $g \mapsto g\pi_h/\pi_h$ and $\pi_h \in \overline{K}$ is a (p^h-1)-st root of p.
- $\operatorname{End}_{\mathbb{F}_p[G_K]}(M) = \mathbb{F}_{p^h}$, and a conjugation by an element in $\operatorname{End}_{\mathbb{F}_p[G_K]}(M)$ shifts $(i_0, \cdots, i_{h-1})$ circularly, so that M being simple implies that $(i_0, \cdots, i_{h-1})$, as a function from $\mathbb{Z}/h\mathbb{Z}$ to $\mathbb{Z}$, has period exactly h.

Let $\Gamma_1, \cdots, \Gamma_t$ be Jordan-Hölder factors of Γ, and let $h_m = \dim_{\mathbb{F}_p} \Gamma_m(\overline{K})$. Let $i^m : \mathbb{Z}/h_m\mathbb{Z} \to \mathbb{Z}$ be the map of period exactly h_m corresponding to $\Gamma_m(\overline{K})$. By [R, Corollaire 3.4.4], we can suppose that $i^m(j) \le e = 1$ for all j. Let L_m be the compositum of $K(\zeta_p)$ and $K(\Gamma_m(\overline{K}))$. It is clear that L_m/K is tamely ramified, thus cyclic. Let $d_m = [L_m : K]$. If there is $h_m \ge 3$, then we are automatically directed to the fourth case by the following claim.

Claim. If $h_m \ge 3$, then $d_m > p^2(p-1)$.

Note that d_m is the smallest multiple of $p-1$ such that $p^{h_m}-1$ divides $d_m(i^m(0)+pi^m(1)+\cdots+p^{h_m-1}i^m(h_m-1))$. If there are consecutive $j, j+1$ (modulo h_m) such that $i^m(j) = i^m(j+1) = 0$, then we can shift so that we can assume $i^m(h_m-2) = i^m(h_m-1) = 0$. Then $d_m \ge \frac{p^{h_m}-1}{\frac{p^{h_m-2}-1}{p-1}} > p^2(p-1)$. If not, as $h_m \ge 3$ and $(i^m(0), \cdots, i^m(h_m-1))$ is of period h_m, there exist consecutive $j, j+1$ (modulo h_m) such that $i^m(j) = i^m(j+1) = 0$. We can shift so that we can assume $i^m(h_m-2) = i^m(h_m-1) = 0$. By considering that $d_m((1-i^m(0)) + p(1-i^m(1)) + \cdots + p^{h_m-1}(1-i^m(h_m-1)))$ is divisible by $p^{h_m}-1$ as well, we get the same bound, namely $d_m \ge \frac{p^{h_m}-1}{\frac{p^{h_m-2}-1}{p-1}} > p^2(p-1)$.

Now we can assume that $h_m \le 2$ for all m. If $h_m = 1$ (2, respectively), then $d_m = p-1$ (p^2-1, respectively), because of the simplicity assumption on Jordan-Hölder factors. If Γ is semi-simple (i.e. a direct sum of Jordan-Hölder factors), then we can conclude that L is cyclic of degree either $p-1$ or p^2-1. If it is not semisimple, then $[L : K]$ cannot be tamely ramified (as it cannot be cyclic), so p divides $[L : K]$. Therefore, if there exists some $h_m = 2$, then p^2-1 divides $[L : K]$, so that $[L : K] \ge p(p^2-1)$ and it is in the fourth case.

Therefore, we are left with the case of non-semi-simple Γ with $h_m = 1$ for all $1 \le m \le t$. Over K, any extension of μ_p by μ_p or $\mathbb{Z}/p\mathbb{Z}$ is trivial, and the same is for an extension of $\mathbb{Z}/p\mathbb{Z}$ by $\mathbb{Z}/p\mathbb{Z}$. Thus, the only way Γ_K can be non-semi-simple (which is true by the full faithfulness of generic fiber functor) is that Γ_K is an extension of $(\mathbb{Z}/p\mathbb{Z})^r$ by μ_p^s, for some $r, s \ge 0$. In that case, $[L : K] = p^u(p-1)$ for some $u \ge 1$; if $u = 1$, we are in the second case, and if $u \ge 2$, we are in the fourth case. So we have checked that all are divided into the four cases, when p is odd. □

Combined with the above proposition, it can be shown that the field generated by geometric points of a p-group is of certain form. The following is an example of the consequence of this philosophy, which is proved in [Fo1].

Lemma 1.3.2 [Fo1, 3.4.2]. *Let E be a number field and Γ be a finite flat commutative $\mathcal{O}_E$-group scheme. Suppose that Γ is killed by p and $F = E(\Gamma(\overline{E}))$. Then we have the following.*

(i) If $E = \mathbb{Q}$ (resp. $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$) and $p \in \{3,5,7,11,13,17\}$ (resp. $p \in \{3,5,7\}$, $p \in \{5,7\}$), then $F \subset E(\zeta_p)$.

(ii) If $E = \mathbb{Q}(\sqrt{5})$ and $p = 3$, $F \subset E(\zeta_3, \sqrt[3]{\eta})$, where η is a fundamental unit of E.

Proof. By taking $\Gamma \times \mu_p$ instead of Γ, we can assume that there is a closed subscheme of Γ isomorphic to μ_p. Let $F_0 = E(\zeta_p)$, so that $F_0 \subset F$. If $E \neq \mathbb{Q}$, let $i : E \to E$ be the nontrivial element of $\mathrm{Gal}(E/\mathbb{Q})$. The, replacing Γ with $\Gamma \oplus i(\Gamma)$, we can also assume that $F/\mathbb{Q}$ is Galois.

Let $n = [F : \mathbb{Q}]$, $n_0 = [F : E]$, $n_0' = [F : F_0]$, $a = [E : \mathbb{Q}]$. Then, we have $n = an_0$ and $n_0 = (p-1)n_0'$. Let d_E and d_F be the absolute discriminant of E and F. By Theorem 1.3.2(iii), we have $|d_F|^{1/n} < |d_E|^{1/a} \cdot p^{p/(p-1)}$. Thus, for each E, we have a bound on d_F. By using the Odlyzko discriminant bound [Mar], for each case, we deduce bounds on $n = [F : \mathbb{Q}]$, thereby n_0'.

- For $E = \mathbb{Q}$, if $p = 3,5,7,11,13,17$, then $n \leq 6,12,18,50,88,574$, so that $n_0' \leq 3,3,3,5,7,35$.
- For $E = \mathbb{Q}(\sqrt{-1})$, if $p = 3,5,7$, then $n \leq 22,64,316$, so that $n_0' \leq 5,8,26$.
- For $E = \mathbb{Q}(\sqrt{-3})$, if $p = 5,7$, then $n \leq 38,108$, so that $n_0' \leq 4,9$.
- For $E = \mathbb{Q}(\sqrt{5})$, if $p = 3$, then $n \leq 28$, so that $n_0' \leq 7$.

To show that $F = F_0$, note that we know from Theorem 1.3.2 that F/F_0 is unramified outside p. Also, we can check from [Mas] that F_0 has class number 1 in all cases we are considering. Thus, the Hilbert class field of F_0 is F_0 itself. Therefore, to show that $F = F_0$, we only need to show that F/F_0 is unramified at primes over p.

Let e be the absolute ramification index of a place of F over p, which is independent of the choice of place as F is Galois over $\mathbb{Q}$. As the absolute ramification index of F_0 at a place over p is $p-1$, $e = (p-1)e'$. What we want to show for all cases except $E = \mathbb{Q}(\sqrt{5})$ and $p = 3$ is that $e' = 1$. For all cases we are considering, $E/\mathbb{Q}$ is unramified at p. Thus, e divides n_0, and e' divides n_0'. By Proposition 1.3.2, it follows that either $e' \in \{1, p, p+1\}$ or $e' \geq p^2$. For all cases we are considering, $n_0' < p^2$. Therefore, if $e' \neq 1$, then either $e' = p$ or $p+1$. This is even impossible if $n_0' < p$. Thus, we are left to deal with cases

$$(E,p) = (\mathbb{Q},3), (\mathbb{Q},17), (\mathbb{Q}(\sqrt{-1}),3), (\mathbb{Q}(\sqrt{-1}),5), (\mathbb{Q}(\sqrt{-1}),7), (\mathbb{Q}(\sqrt{-3}),7), (\mathbb{Q}(\sqrt{5}),3).$$

The case $e' = p+1$ is when $e = p^2 - 1$, so F/E is tamely ramified. In that case, we observed in the proof of Theorem 1.1.1 that $v(\mathfrak{D}_{F/E}) < u_{F/E} = 1$, so that actually a sharper bound $|d_F|^{1/n} < |d_E|^{1/a} p$ holds. After recalculation, we get $n \leq 2,116,8,20,50,32,78$ so that $n_0' \leq 1,7,2,2,4,2,6$, respectively, which is $< p+1$ for all cases. Thus, $e' = p+1$ is impossible.

For the case $e' = p$, let's first show that $n_0' = p$. If $p < n_0' < p^2$, then by Sylow theorems, there is only one Sylow p-group of $\mathrm{Gal}(F/F_0)$, which is of order n_0' (as the number of Sylow p-groups is 1 modulo p). Therefore, for a prime $\mathfrak{P}$ of F lying over p, the inertia group I_β is the unique Sylow p-group of $\mathrm{Gal}(F/F_0)$. Then F^{I_β} is an everywhere unramified extension of F_0, which is a contradiction as F_0 has class number 1. Note however that $n_0' < p^2$ for all cases we have. Therefore, necessarily we have $n_0' = e' = p$, and $n_0 = e = p(p-1)$.

Let $\mathfrak{p}$ be a prime of E over p. Let k be the residue field of $\mathcal{O}_{F_\mathfrak{p}}$, and let $W = W(\overline{k})$; it is an extension of $\mathcal{O}_{E_\mathfrak{p}}$ as E is unramified at p. By Proposition 1.3.2, Γ_W is a nontrivial extension of $(\mathbb{Z}/p\mathbb{Z})^r$ by μ_p^s, for some nonnegative integers r, s. We will eventually show that Γ itself is a nontrivial extension of $(\mathbb{Z}/p\mathbb{Z})^r$ by μ_p^s. First we show $\Gamma_{\mathcal{O}_{E_\mathfrak{p}}}$ is so. As both $\mathrm{Frac}\, W$ and $E_\mathfrak{p}$ have absolute ramification index $e = 1 < p-1$, the generic fiber functor on the category of finite flat commutative group schemes over W ($\mathcal{O}_{E_\mathfrak{p}}$, respectively) killed by p-power is fully faithful respecting sub-objects and quotients, by Theorem 1.2.8. As every finite flat group scheme over $E_\mathfrak{p}$ or $\operatorname{Frac} W$ is étale, we can think of finite flat group schemes over those fields as Galois modules, and here we can finally use Galois descent. Therefore, that Γ_W is a nontrivial extension of $(\mathbb{Z}/p\mathbb{Z})^r$ by μ_p^s is also true for $\Gamma_{\mathcal{O}_{E_\mathfrak{p}}}$. Here we went through the process

$$\Gamma_W \xrightarrow{\text{generic fiber}} \Gamma_{\operatorname{Frac} W} \xrightarrow{\text{Galois descent}} \Gamma_{E_p} \xleftarrow{\text{generic fiber}} \Gamma_{\mathcal{O}_{E_\mathfrak{p}}}.$$

Now we proceed to Γ. By Theorem 1.2.6, we can think of Γ as a triple $(\prod_{\mathfrak{p}|p} \Gamma_{\mathcal{O}_{E_\mathfrak{p}}}, \Gamma_{\mathcal{O}_E[1/p]}, \mathrm{id}_{\Gamma_{E_p}})$. First, the extensions $\Gamma_{\mathcal{O}_{E_\mathfrak{p}}}$ are compatible with Galois conjugates, as the extension exact sequences are just connected-étale sequences in this case. As Γ is of p-power order, $\Gamma_{\mathcal{O}_E[1/p]}$ is étale by Proposition 1.2.4(ii). What is more is that we know F/E is unramified outside p. Thus, $\Gamma_{\mathcal{O}_E[1/p]}$ is an étale group scheme with a trivial $\pi_{1,\text{ét}}$-action, so it is a constant group scheme. Thus, we can identify μ_p^s inside Γ as a triple

$$\left(\prod_{\mathfrak{p}|p} (\mu_p^s)_{\mathcal{O}_{E_\mathfrak{p}}}, G, \left(\mathrm{id}_{\prod_{\mathfrak{p}|p} \Gamma_{E_\mathfrak{p}}}\right)|_{\prod_{\mathfrak{p}|p} (\mu_p^s)_{E_\mathfrak{p}}}\right),$$

where G is the collection of points in $\Gamma_{\mathcal{O}_E[1/p]}$ which lifts to a point in $\prod_{\mathfrak{p}|p} (\mu_p^s)_{E_\mathfrak{p}} \subset \prod_{\mathfrak{p}|p} \Gamma_{E_\mathfrak{p}}$; this is the only choice we can make as $\Gamma_{\mathcal{O}_E[1/p]}$ is a constant group scheme. Thus, μ_p^s exists as a closed $\mathcal{O}_E$-subgroup scheme of Γ, and its quotient is an étale $\mathcal{O}_E$-group scheme whose base change to $\mathcal{O}_{E_p}$ is $(\mathbb{Z}/p\mathbb{Z})^r$. As it has trivial Galois action outside p, again by Theorem 1.2.6, it is a constant group scheme as a $\mathcal{O}_E$-group scheme, and it is thus necessarily $(\mathbb{Z}/p\mathbb{Z})^r$.

Now F/F_0 is generated by $\sqrt[p]{u_1}, \cdots, \sqrt[p]{u_r}$ upon the choice of elements $u_1, \cdots, u_r \in E$, corresponding to generators of $(\mathbb{Z}/p\mathbb{Z})^r$. However, as we know $[F : F_0] = p$, only one unit will be sufficient to generate F. Thus, $F = E(\zeta_p, \sqrt[p]{u})$ for some $u \in E$ which is not a p-th power. By rescaling, we can suppose that u is an algebraic number not divisible by a p-th power of a prime. To show that u is a unit, it is sufficient to prove so for an extension of $\mathbb{Z}/p\mathbb{Z}$ by μ_p, as the field generated by geometric points of such extension is certainly contained in F, which should be just equal to F by degree reasons. Note however that as $\mathcal{O}_E$ is a PID, we can completely classify such extensions.

Claim. Over $\mathcal{O}_E$, if a finite flat commutative $\mathcal{O}_E$-group scheme satisfies $0 \to \mu_p \to G \to \mathbb{Z}/p\mathbb{Z} \to 0$, then G is a *Katz-Mazur group scheme*; namely, there exists $\eta \in \mathcal{O}_E^\times$ such that, for an $\mathcal{O}_E$-algebra S,

$$G(S) = \{(x, i) \mid x \in S^\times, x^p = \eta^i \text{ for all } 0 \leq i < n\}.$$

Equivalently, $G = \operatorname{Spec} \prod_{i=0}^{p-1} \mathcal{O}_E[x]/(x^p - \eta^i)$.

If the claim is true, then $F = E(\zeta_p, \sqrt[p]{\eta})$, as desired. On the other hand, except $E = \mathbb{Q}(\sqrt{5})$, there is no nontrivial fundamental unit of $\mathcal{O}_E$. Therefore, proving the claim will finish the proof. We actually prove the claim by calculating the order of $\operatorname{Ext}^1_{\mathcal{O}_E}(\mathbb{Z}/p\mathbb{Z}, \mu_p)$, which will be a finite group in this case. First of all, there are $|\mathcal{O}_E^\times / \mathcal{O}_E^{\times p}|$ many different Katz-Mazur groups, as E does not contain a primitive p-th root of unity (recall that $p \neq 2$), you have to first choose a unit η, and any other η' off by a p-th power will give the same group. On the other hand, we have exact sequences

$$0 \to \mu_{p,\mathcal{O}_E} \to \mathbb{G}_{m,\mathcal{O}_E} \xrightarrow{p} \mathbb{G}_{m,\mathcal{O}_E} \to 0$$

and

$$0 \to (\mathbb{Z})_{\mathcal{O}_E} \xrightarrow{p} (\mathbb{Z})_{\mathcal{O}_E} \to (\mathbb{Z}/p\mathbb{Z})_{\mathcal{O}_E} \to 0.$$

Therefore, the following are also exact, as they are long exact sequences of Ext functor.

$$\begin{aligned} &\mathrm{Hom}_{\mathcal{O}_E}((\mathbb{Z})_{\mathcal{O}_E}, \mathbb{G}_{m,\mathcal{O}_E}) \xrightarrow{x\mapsto x^p} \mathrm{Hom}_{\mathcal{O}_E}((\mathbb{Z})_{\mathcal{O}_E}, \mathbb{G}_{m,\mathcal{O}_E}) \\ \to\ &\mathrm{Ext}^1_{\mathcal{O}_E}((\mathbb{Z})_{\mathcal{O}_E}, \mu_{p,\mathcal{O}_E}) \to \mathrm{Ext}^1_{\mathcal{O}_E}((\mathbb{Z})_{\mathcal{O}_E}, \mathbb{G}_{m,\mathcal{O}_E}), \end{aligned}$$

$$\begin{aligned} &\mathrm{Hom}_{\mathcal{O}_E}((\mathbb{Z})_{\mathcal{O}_E}, \mu_{p,\mathcal{O}_E}) \xrightarrow{x\mapsto x^p} \mathrm{Hom}_{\mathcal{O}_E}((\mathbb{Z})_{\mathcal{O}_E}, \mu_{p,\mathcal{O}_E}) \to \mathrm{Ext}^1_{\mathcal{O}_E}((\mathbb{Z}/p\mathbb{Z})_{\mathcal{O}_E}, \mu_{p,\mathcal{O}_E}) \\ \to\ &\mathrm{Ext}^1_{\mathcal{O}_E}((\mathbb{Z})_{\mathcal{O}_E}, \mu_{p,\mathcal{O}_E}) \xrightarrow{x\mapsto x^p} \mathrm{Ext}^1_{\mathcal{O}_E}((\mathbb{Z})_{\mathcal{O}_E}, \mu_{p,\mathcal{O}_E}). \end{aligned}$$

Now we know some of these entries. First of all, the functor $\mathrm{Hom}_{\mathcal{O}_E}((\mathbb{Z})_{\mathcal{O}_E}, -)$ is just the global section functor. Therefore, for any fppf sheaf $\mathscr{F}$, $\mathrm{Ext}^i_{\mathcal{O}_E}((\mathbb{Z})_{\mathcal{O}_E}, \mathscr{F}) = H^i((\operatorname{Spec} R)_{\mathrm{fppf}}, \mathscr{F})$. Thus, $\mathrm{Hom}_{\mathcal{O}_E}((\mathbb{Z})_{\mathcal{O}_E}, \mathbb{G}_{m,\mathcal{O}_E}) = \mathcal{O}_E^\times$, and $\mathrm{Ext}^1_{\mathcal{O}_E}((\mathbb{Z})_{\mathcal{O}_E}, \mathbb{G}_{m,\mathcal{O}_E}) = H^1_{\mathrm{fppf}}(\operatorname{Spec} \mathcal{O}_E, \mathbb{G}_{m,\mathcal{O}_E})$. Note however that, by faithfully flat descent, an invertible sheaf on fppf topology is the same as just an invertible sheaf on Zariski topology, so it is just $\mathrm{Pic}(\mathcal{O}_E)$ (cf. [Stacks, Tag 03P8]). As $\mathcal{O}_E$ is a PID, the Picard group vanishes. Thus, the first exact sequence gives us

$$\mathrm{Ext}^1_{\mathcal{O}_E}((\mathbb{Z})_{\mathcal{O}_E}, \mu_{p,\mathcal{O}_E}) = \mathcal{O}_E^\times / \mathcal{O}_E^{\times p}.$$

On the other hand, the second exact sequence gives us

$$\mathrm{Ext}^1_{\mathcal{O}_E}((\mathbb{Z}/p\mathbb{Z})_{\mathcal{O}_E}, \mu_{p,\mathcal{O}_E}) = \mathrm{Ext}^1_{\mathcal{O}_E}((\mathbb{Z})_{\mathcal{O}_E}, \mu_{p,\mathcal{O}_E}) = \mathcal{O}_E^\times / \mathcal{O}_E^{\times p}.$$

Thus, the orders match, and the claim is proved. □

Finally, now we can prove the structural restrictions on finite flat commutative group schemes over the ring of integer of a small number field.

Theorem 1.3.3 [Fo1, Théorème 4]**.** *Let E be a number field, and Γ be a finite flat commutative group scheme over $\mathcal{O}_E$ of p-power order.*

(i) If $E = \mathbb{Q}$ (resp. $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$) and $p \in \{3, 5, 7, 11, 13, 17\}$ (resp. $p \in \{3, 5, 7\}$, $p \in \{5, 7\}$), then Γ is a direct sum of a constant group and a diagonalizable group.

(ii) If $E = \mathbb{Q}(\sqrt{5})$ and $p = 3$, Γ is an extension of a constant group by a diagonalizable group.

Proof. Let $F = E(\Gamma(\overline{E}))$. As F/E is unramified outside p, by Theorem 1.2.6, the category of finite flat commutative $\mathcal{O}_E$-group schemes of p-power order can be fully faithfully embedded in the category of finite flat commutative $\mathcal{O}_{E_\mathfrak{p}}$-group schemes of p-power order, for a prime $\mathfrak{p}|p$ in E. By Proposition 1.2.6, any extension of $\mathbb{Z}/p\mathbb{Z}$ (μ_p, μ_p, respectively) by $\mathbb{Z}/p\mathbb{Z}$ ($\mathbb{Z}/p\mathbb{Z}$, μ_p, respectively) is étale (trivial, connected, respectively). Also, except the case of $E = \mathbb{Q}(\sqrt{5})$ and $p = 3$, any extension of μ_p by $\mathbb{Z}/p\mathbb{Z}$ is trivial, by the proof of Lemma 1.3.2. Also as in the proof of Lemma 1.3.2, using that $E/\mathbb{Q}$ is unramified at p, we can use, via Theorem 1.2.8, Raynaud's classification utilized in the proof of Proposition 1.3.2 to see that the only simple objects of the category of finite flat commutative $\mathcal{O}_E$-group schemes of p-power order are μ_p and $\mathbb{Z}/p\mathbb{Z}$, and the category is abelian.

We now show that, using Jordan-Hölder composition series, for all cases, Γ is an extension of a constant group by a diagonalizable group. Let $0 = \Gamma_0 \subset \Gamma_1 \subset \cdots \subset \Gamma_{m-1} \subset \Gamma_m = \Gamma$ be a composition series. Suppose that there is some $0 < i < m$ such that Γ_i/Γ_{i-1} is μ_p whereas Γ_{i+1}/Γ_i is $\mathbb{Z}/p\mathbb{Z}$. As the extension

$$0 \to \mu_p \to \Gamma_{i+1}/\Gamma_{i-1} \to \mathbb{Z}/p\mathbb{Z} \to 0$$

is trivial by the remark in the above paragraph, we can in particular find a subgroup $\Gamma_i' \subset \Gamma_{i+1}$ such that $\Gamma_i'/\Gamma_{i-1} \cong \mu_p$ and $\Gamma_{i+1}/\Gamma_i' \cong \mathbb{Z}/p\mathbb{Z}$. We then replace Γ_i with Γ_i' in the composition.

After repeating this process finitely many times, we get a composition series where there is some $0 < j < m$ such that for all $0 < i \leq j$, $\Gamma_i/\Gamma_{i-1} = \mu_p$, whereas for all $j < i \leq m$, $\Gamma_i/\Gamma_{i-1} = \mathbb{Z}/p\mathbb{Z}$. The discussion in the above paragraph says that, an extension of a constant (diagonalizable, respectively) group by a constant (diagonalizable, respectively) group is constant (diagonalizable, respectively). Thus, we deduce that Γ/Γ_j is constant whereas Γ_j is diagonalizable. This implies that, in all cases, Γ is an extension of a connected group by a diagonalizable group. This proves (ii).

To show (i), we need to show that the extension is split. To show this, we just need to show that $\mathrm{Ext}^1_{\mathcal{O}_E}(G_c, G_d) = 0$ for any constant group G_c and diagonalizable G_d of p-power order. We prove this via strong induction on $|G_c||G_d|$. Note that $\mathrm{Ext}^1_{\mathcal{O}_E}(\mathbb{Z}/p\mathbb{Z}, \mu_p) = 0$ in the cases of (i) by the remark we made in the first paragraph of the proof. Thus, the case $|G_c| = |G_d| = p$ is done. Now in a general case, suppose $|G_c| > p$. Then, we can find a subgroup $G'_c \subset G_c$ such that $G'_c \cong \mathbb{Z}/p\mathbb{Z}$ and $G_c/G'_c \neq 1$. Note also that any morphism from an étale group scheme to a connected group scheme is trivial, as it factors through the reduction of the connected group, which is trivial. Thus, a part of the long exact sequence for Ext in this case is

$$0 \to \mathrm{Ext}^1_{\mathcal{O}_E}(G_c/G'_c, G_d) \to \mathrm{Ext}^1_{\mathcal{O}_E}(G_c, G_d) \to \mathrm{Ext}^1_{\mathcal{O}_E}(G'_c, G_d).$$

By strong induction, $\mathrm{Ext}^1_{\mathcal{O}_E}(G_c, G_d) = 0$. The same argument applies to the case when $|G_d| > p$, as in this case we can find $G'_d \subset G_d$ such that $G'_d \cong \mu_p$. This finishes the proof. □

This easily gives the nonexistence result we were looking at.

Theorem 1.1.2 [Fo1, Corollaire 2]. *For $E = \mathbb{Q}, \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{5})$, there is no nontrivial abelian variety over E with everywhere good reduction.*

Proof. Suppose the contrary, and let A be an abelian variety of dimension $g \geq 1$ over E with everywhere good reduction. Let p be any prime corresponding to E as in Theorem 1.3.3. Then, the p-divisible group $A(p)$ is, by Theorem 1.3.3, an extension of a constant p-divisible group by a diagonalizable p-divisible group. Note that a constant p-divisible group is necessarily of form $(\mathbb{Q}_p/\mathbb{Z}_p)^r$, as it is clear by passage to Tate module, and a diagonalizable p-divisible group is necessarily off form $(\mu_{p^\infty})^s$ by Cartier duality. Thus, $A(p)^0 = (\mu_{p^\infty})^s$ and $A(p)^{\text{ét}} = (\mathbb{Q}_p/\mathbb{Z}_p)^r$. As $A(p)$ is of dimension g (cf. [Tat2, 2.3]), $A(p)^0$ is of dimenson g, and $A(p)^{\text{ét}} = (\widehat{A}(p)^0)^D$ is so by Cartier duality and existence of dual abelian varieties. Thus, $A(p)$ sits inside a short exact sequence

$$0 \to (\mu_{p^\infty})^g \to A(p) \to (\mathbb{Q}_p/\mathbb{Z}_p)^g \to 0.$$

In particular, if $E = \mathbb{Q}, \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, we have $A(p) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^g \oplus (\mu_{p^\infty})^g$. Thus, for any $n > 0$, there is an E-rational primitive p^n-torsion point of A, where primitivity here means that the point is not of p^{n-1}-torsion. Let $\mathcal{A}$ be a Néron model of A over $\mathcal{O}_E$, then this E-rational point in $\mathcal{A}$ factors through $\mathcal{O}_E$, so there is a $\mathcal{O}_E$-rational primitive p^n-torsion point of $\mathcal{A}$. For a prime $\mathfrak{p}$ of E over p, after the reduction modulo $\mathfrak{p}$, the $\mathcal{O}_E$-rational primitive p^n-torsion point of $\mathcal{A}$ becomes a k-rational primitive p^n-torsion point of A_k, where $k = \kappa(\mathfrak{p})$. This means that $A_k(k)$ has at least p^n elements. As this is a finite set, choosing a large enough n gives us a contradiction.

For $E = \mathbb{Q}(\sqrt{5})$, for any $n > 0$, still we have a subgroup $\Gamma_n \subset A$ such that $\Gamma_n \cong (\mu_{p^n})^g$. The quotient A/Γ_n, which exists by Theorem 1.2.3, is an abelian variety as it is proper and connected, and $A[p^n]/\Gamma_n = (A/\Gamma_n)[p^n]$ is a constant group scheme of order p^{ng}. By the same process of passage to Néron model and its reduction, it follows that $p^{ng} \leq \#(A/\Gamma_n)_k(k)$. On the other hand, an abelian variety over a finite field k has a bounded number of k-rational points, namely $\#(A/\Gamma_n)_k(k) \leq (\sqrt{\#k} + 1)^{2g}$, which is a consequence of Riemann Hypothesis over a finite field, Proposition 2.2.9. Thus, $p^{ng} \leq (\sqrt{\#k}+1)^{2g}$, which is a contradiction if we take n large enough.

One can alternatively prove this corollary just with finite flat group schemes, without appealing to p-divisible groups. Namely, for any $n \geq 1$, we have the exact sequence

$$0 \to D_n \to A[p^n] \to C_n \to 0,$$

where D_n and C_n are diagonalizable and constant, respectively. By using the same argument as above, we can bound $|C_n| \leq (\sqrt{\#k}+1)^{2g}$. We can take the Cartier dual of this sequence, and get the exact sequence

$$0 \to C_n^D \to \widehat{A}[p^n] \to D_n^D \to 0,$$

as $\widehat{A}[p^n] = A[p^n]^D$ by the Weil pairing, Proposition 1.2.22. Thus we can similarly bound $|D_n| = |D_n^D| \leq (\sqrt{\#k}+1)^{2g}$. Thus, $p^{2ng} = |A[p^n]| \leq (\sqrt{\#k}+1)^{4g}$, which is a contradiction by taking a large enough n.

Without appealing to the Riemann Hypothesis over finite field, one can argue alternatively as follows. As A/D_n and A are isogenous, $(A/D_n)_k$ and A_k are isogenous abelian varieties over k. As they have the same number of k-rational points by Theorem 1.2.37, $\#A_k(k) \geq |C_n|$. By taking dual, $\#\widehat{A}_k(k) \geq |D_n^D| = |D_n|$. As $\widehat{A}$ and A are also isogenous, we have $\#A_k(k)^2 = \#A_k(k) \cdot \#\widehat{A}_k(k) \geq |C_n| \cdot |D_n| = |A[p^n]| = p^{2ng}$. Taking large enough n, one gets a contradiction. □

1.3.2.2 Restrictions on 2-Groups

Although we have proved the nonexistence of abelian variety over $\mathbb{Q}$ with everywhere good reduction, it will be beneficial to review the whole argument in general terms so that we can see what is needed in generalizing the argument to other situations. In particular, we prove that a finite flat commutative $\mathbb{Z}$-group scheme of 2-power order is also an extension of a constant group scheme by a diagonalizable group scheme, a case excluded in the previous section.

There are several arguments that work for all cases, regardless of the choice of E or p.

- Given a finite flat commutative $\mathcal{O}_E$-group scheme G of p-power order, $F = E(G(\overline{E}))$ will still be unramified outside p and moderately ramified at p, by Theorem 1.3.2.

- The Jordan-Hölder composition series will exist. Even though we cannot appeal to Raynaud's theory on prolongations, we can use Proposition 1.2.5 so that we can find a filtration by finding a corresponding filtration for the generic fiber. Also, even though we do not know if the category of finite flat commutative $\mathcal{O}_E$-group schemes is abelian, we know quotients exist by Theorem 1.2.3; it is the behavior of general cokernel that we do not know well, but we will not need it in this situation. The quotients will be simple objects as, if not, there will be some object strictly in between consecutive entries of the filtration, which will translate into an object in between consecutive entries of the filtration of the generic fiber, and this is impossible as, over the generic fiber, we know the category is abelian.

- If we know that the only simple objects are constant and diagonalizable groups, then we can rearrange the given composition series so that any finite flat commutative $\mathcal{O}_E$-group scheme of p-power order is an extension of a constant group by a diagonalizable group. This is always possible because Theorem 1.2.6 and Proposition 1.2.6 are all we need for this argument.

On the other hand, what was special about the cases we considered in the previous section is esssentially *the classification of simple objects*. Namely, to conclude that the only simple objects in the category of finite flat commutative $\mathcal{O}_E$-group schemes of p-power order are μ_p and $\mathbb{Z}/p\mathbb{Z}$, one needs a very special condition so that one can use something like Lemma 1.3.2 or Raynaud's results on full faithfulness of generic fiber functor. For example, we can see that even if $E = \mathbb{Q}$ and $p = 2$, the only simple objects are μ_2 and $\mathbb{Z}/2\mathbb{Z}$, and it is because "2 is small so that we can consider all cases."

Proposition 1.3.3 [Sc2, §5]**.** *The simple objects of the category of finite flat commutative $\mathbb{Z}$-group schemes of 2-power order are μ_2 and $\mathbb{Z}/2\mathbb{Z}$.*

Proof. Let G be a finite flat commutative $\mathbb{Z}$-group scheme killed by 2. Let $L = \mathbb{Q}(G(\overline{\mathbb{Q}}))$. Note that the Katz-Mazur group scheme G_{-1} with the choice $\eta = -1$ has $\mathbb{Q}(G_{-1}(\overline{\mathbb{Q}})) = \mathbb{Q}(\sqrt{-1})$; recall that $G_{-1} = \operatorname{Spec} \prod_{i=0}^{1} \mathbb{Z}[x]/(x^2-(-1)^i)$. As G_{-1} is killed by 2, we can define $G' := G \times G_{-1}$ and instead consider $F = \mathbb{Q}(G'(\overline{\mathbb{Q}})) \supset \mathbb{Q}(\sqrt{-1})$. By Theorem 1.3.2, $|d_F|^{\frac{1}{[F:\mathbb{Q}]}} < 2^{1+\frac{1}{2-1}} = 4$, so by Odlyzko's discriminant bound [Mar], $[F : \mathbb{Q}] \leq 4$. Thus, either $F = \mathbb{Q}(\sqrt{-1})$ or $[F : \mathbb{Q}(\sqrt{-1})] = 2$. In any case, L, as a subfield of F, is also a Galois 2-extension of $\mathbb{Q}$.

Now, let H be a finite flat commutative $\mathbb{Z}$-group scheme of 2-power order, which is also simple in that category. As $0 \neq H[2] \subset H$, it follows that H is killed by 2, so $K = \mathbb{Q}(H(\overline{\mathbb{Q}}))$ is of degree 1, 2 or 4 over $\mathbb{Q}$. As $\mathrm{Gal}(K/\mathbb{Q})$, a 2-group, acts on $H_{\mathbb{Q}}(\overline{\mathbb{Q}})$, which is a finite set of 2-power order, by basic conjugacy class counting technique from group theory, we know that the subgroup of $H_{\mathbb{Q}}(\overline{\mathbb{Q}})$ fixed by $\mathrm{Gal}(K/\mathbb{Q})$ is nontrivial and is of order divisible by p. Therefore, one can take a Galois submodule of $H_{\mathbb{Q}}(\overline{\mathbb{Q}})$ of order p. As $H_{\mathbb{Q}}$ is étale over $\mathbb{Q}$, it follows that there is a order 2 closed $\mathbb{Q}$-subgroup scheme S of $H_{\mathbb{Q}}$. By Proposition 1.2.5, there is a corresponding order 2 subgroup scheme S' of H. As H is simple, it follows that $H = S'$, or that H is of order 2. By [Tat1, 3.2], it is of form $G_{a,b}$ where, $a, b \in \mathbb{Z}$ with $ab = -2$, such that $G_{a,b}$ is characterized as, for a commutative ring S, $G_{a,b}(S) = \{y \in S \mid y^2 = ay\}$ with group structure as $y * z = y + z + byz$. Pairs off by a unit give the same group scheme, and $G_{-2,1} = \mu_2$ whereas $G_{1,-2} = (\mathbb{Z}/2\mathbb{Z})$. This is the desired conclusion. □

Thus, the discussion we had earlier in this section proves the following theorem.

Theorem 1.3.4. *A finite flat commutative $\mathbb{Z}$-group scheme of 2-power order is an extension of a constant group by a diagonalizable group.*

This alone also implies the nonexistence of abelian scheme over $\mathbb{Z}$.

1.4 Nonexistence of Certain Semi-stable Abelian Varieties over $\mathbb{Q}$

Fontaine's first nonexistence proof in the previous section is really a structure theorem of finite flat group schemes and p-divisible groups "having everywhere good reduction," i.e. those extending to the ring of integers. Philosophically, one can prove a structure theorem of "low degree objects" in a certain category if

1. the given category is pre-abelian, i.e. has kernels and cokernels,
2. one identifies all the simple objects in the category,
3. and one identifies all the possible extensions of a simple object by another simple object in the category.

What the proofs we have seen in the previous section did was to associate the given category, *the category of abelian varieties over a number field with everywhere good reduction*, to a pre-abelian subcategory of an abelian category. Examples are p^n-torsion subgroups in a category of finite flat group schemes in a category of fppf sheaves, p-divisible groups in a category of p-divisible groups in a category of fppf sheaves, and Tate modules in a category of $\mathbb{F}_p$ or $\mathbb{Z}_p$-modules with a group action. This *dévissage-like argument* is the heart of all proofs of similar nonexistence problems. In particular, the proofs in the next chapter will use certain (pre-)abelian categories coming up in (integral) p-adic Hodge theory.

Residing in the category of finite flat group schemes/p-divisible groups for now, one might ask if a similar proof applies to a certain type of abelian variety which can be characterized by its torsion subgroups or p-divisible groups. We have observed that *semi-stable reduction* can also be determined purely by p-divisible groups and/or torsion subgroups, thanks to Theorem 1.2.30 and its related theorems in the Section 1.2.3.7. We would like to indulge in this idea to prove the following result.

Theorem 1.1.3 [Sc1, Theorem 1.1]**.** *For the primes $\ell = 2, 3, 5, 7, 13$, there is no nontrivial abelian variety over $\mathbb{Q}$ with good reduction outside ℓ and semi-stable reduction at ℓ.*

Alternatively, one can try to control the ramification of ℓ-adic Tate modules, where ℓ is different from the place of bad reduction. This, although gives no stronger result than Theorem 1.1.3, is in some sense more related to the more general approach we will take in the second chapter. Finite flat group schemes and p-divisible groups are, in some sense, more rigid, as there always is representability issue. On the other hand, we can quite freely handle purely algebraic objects such as Galois representations, Dieudonné modules and Tate modules, although it is more difficult to find meaning in the real world. A miracle of p-adic Hodge theory is that such linear algebraic data can encode so much information.

1.4.1 Results of Schoof

1.4.1.1 The category $\mathcal{D}_\ell^p$

Let ℓ be a prime. An abelian variety A over $\mathbb{Q}$ with good reduction everywhere outside ℓ will give an abelian scheme $\mathcal{A}$ over $\mathbb{Z}[1/\ell]$. We will consider p^n-torsion subgroups $\mathcal{A}[p^n]$, for $p \neq \ell$ another prime. Note that $\mathcal{A}[p^n]$ obviously lies inside the category of *finite flat commutative $\mathbb{Z}[1/\ell]$-group schemes of p-power order*, which we denote as $\mathcal{C}_\ell^p$. By Theorem 1.2.30, $\mathcal{A}[p^n]$ actually lies inside the full subcategory of $\mathcal{C}_\ell^p$ of *finite flat commutative $\mathbb{Z}[1/\ell]$-group schemes G for which $(g-1)^2$ acts trivially on $G(\overline{\mathbb{Q}})$ for all g in the inertia groups of primes lying over ℓ*. We denote this subcategory as $\mathcal{D}_\ell^p$. The following properties of $\mathcal{D}_\ell^p$ are clear from the very definition of $\mathcal{D}_\ell^p$.

- If $G \in \mathcal{D}_\ell^p$, then $G^D \in \mathcal{D}_\ell^p$.
- If $G_1, G_2 \in \mathcal{D}_\ell^p$, then $G_1 \times_{\mathbb{Z}[1/\ell]} G_2 \in \mathcal{D}_\ell^p$.
- $\mathcal{D}_\ell^p$ is a pre-abelian category. More generally, for an object in $\mathcal{D}_\ell^p$, any quotient or subobject of it inside $\mathcal{C}_\ell^p$ is in $\mathcal{D}_\ell^p$.
- Any $G \in \mathcal{C}_\ell^p$ for which the inertia groups of primes over ℓ act trivially on $G(\overline{\mathbb{Q}})$ is also in $\mathcal{D}_\ell^p$. We denote the category of such objects in $\mathcal{C}_\ell^p$ as $\mathcal{G}_\ell^p$.[12] Examples are $\mu_p, \mathbb{Z}/p\mathbb{Z}$.

[12]Note that objects in $\mathcal{G}_\ell^p$ do *not necessarily come from a $\mathbb{Z}$-group scheme*. Being a p-divisible group is quite a restriction so that unramified Galois action implies good reduction, but a lot more freedom is given in formation of finite flat group schemes.

- Given $G \in \mathcal{D}_\ell^p$, any *twist*, unramified outside ℓ and semi-stable at ℓ, of G is also in $\mathcal{D}_\ell^p$. To be more precise, let ρ be a finite-dimensional representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ over $\mathbb{F}_p$. It can be regarded as an $\mathbb{F}_p[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module, denoted as $V(\rho)$. If ρ is unramified outside $\ell\infty$, and if $(\rho(g)^2 - \mathrm{id})^2 = 0$ for every g in an inertia group of any prime over ℓ, then this Galois module, as an étale group scheme over $\mathbb{Q}$, extends to an object in $\mathcal{D}_\ell^p$, as $\mathcal{O}_L[1/\ell]/\mathbb{Z}[1/\ell]$ is unramified. An example we will primarily use is $\rho_{p;\ell} : \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}) \to \mathrm{GL}(\mathbb{F}_p^2)$, where, under the identification $\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}) \cong (\mathbb{Z}/\ell\mathbb{Z})^\times \cong \mathbb{Z}/(\ell-1)\mathbb{Z}$,
$$x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},$$
which makes sense if $p|(\ell-1)$.
- Note that an extension of $G_1 \in \mathcal{D}_\ell^p$ by $G_2 \in \mathcal{D}_\ell^p$ is not necessarily an object in $\mathcal{D}_\ell^p$, because even though we know that an intertia group over ℓ acts unipotently, the rank of unipotence may increase. Thus, $\mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(G_1, G_2)$ does not necessarily parametrize extensions of G_1 by G_2 in $\mathcal{D}_\ell^p$. On the other hand, if $G_1, G_2 \in \mathcal{G}_\ell^p$, the inertia group action on an extension of G_1 by G_2 is at worst tamely ramified; as the extension is a p-group, this shows that the group action is actually unramified, so that the extension is also in $\mathcal{G}_\ell^p$, so is in $\mathcal{D}_\ell^p$. Thus, in that case we know that $\mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(G_1, G_2)$ parametrizes extensions of G_1 by G_2 in $\mathcal{D}_\ell^p$.

1.4.1.2 Criterion for Appropriate Choice of Primes $\ell \neq p$

We now try to adapt the general strategy to $\mathcal{D}_\ell^p$. According to the general strategy, we expect the following.

Proposition 1.4.1 [Sc1, Proposition 3.1]. *Let ℓ be a prime, and suppose there is a prime $p \neq \ell$ satisfying the following two conditions.*

1. *The only simple objects in $\mathcal{D}_\ell^p$ are $\mathbb{Z}/p\mathbb{Z}$ and μ_p.*
2. $\mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) = 0$ *(which is equal to $\mathrm{Ext}^1_{\mathcal{D}_\ell^p}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ by the remark in the previous section).*

Then, there is no nontrivial abelian vareity over $\mathbb{Q}$ having good reduction outside ℓ and semi-stable reduction at ℓ.

Proof. As $\mathcal{D}_\ell^p$ is a pre-abelian category, any object has a Jordan-Hölder composition series. By 1, all successive subquotients are either μ_p or $\mathbb{Z}/p\mathbb{Z}$. By 2, you can push all $\mathbb{Z}/p\mathbb{Z}$'s to the right. So, for any object $G \in \mathcal{D}_\ell^p$, there is an exact sequence $0 \to D \to G \to C \to 0$, where D (C, respectively) is obtained by successive extensions by μ_p's ($\mathbb{Z}/p\mathbb{Z}$'s, respectively). In particular, C is étale, and as the order of C is a power of p, $\pi_{1,\text{ét}}(\mathbb{Z}[1/\ell]) = \mathrm{Gal}(K/\mathbb{Q})$, where K is the maximal p-extension unramified outside $\ell\infty$, acts through a finite p-group P. Its abelianization is cyclic, as every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension. Thus, it follows that P itself is cyclic; one can see this by for example noticing that the *Frattini quotient* of P is cyclic [G, Section 5.1, Theorem 1.2]. Specifically, $\pi_{1,\text{ét}}(\mathbb{Z}[1/\ell])$ acts through $\mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$. Thus, the Jordan-Hölder filtration of C by $\mathbb{Z}/p\mathbb{Z}$'s becomes *split* after the base change to $\mathbb{Z}[1/\ell, \zeta_\ell]$, which means that C is constant over the ring. By Cartier duality, D becomes diagonalizable over the same ring.

Now suppose that there is a nontrivial abelian variety A over $\mathbb{Q}$ having good reduction outside ℓ and semi-stable reduction at ℓ. If we let its Néron model over $\mathbb{Z}[1/\ell]$ as $\mathcal{A}$, then for any $n \geq 1$, $\mathcal{A}[p^n] \in \mathcal{D}_\ell^p$ by Theorem 1.2.30. Thus, it fits into an exact sequence of finite flat $\mathbb{Z}[1/\ell]$-group schemes

$$0 \to D_n \to \mathcal{A}[p^n] \to C_n \to 0,$$

where C_n and D_n become constant and diagonalizable, respectively, over $\mathbb{Z}[1/\ell, \zeta_\ell]$. Pick any prime $\mathfrak{p}$ of $\mathbb{Z}[1/\ell, \zeta_\ell]$ and let k be the residue field. As $\mathcal{A}/D_n$ is also an abelian scheme over $\mathbb{Z}[1/\ell, \zeta_\ell]$, its reduction mod $\mathfrak{p}$, $(\mathcal{A}/D_n)_k$, is an abelian variety over k. As in the last part of the proof of Theorem 1.1.2, one can use either the Riemann Hypothesis over finite field or Theorem 1.2.37 to deduce that $\mathcal{A}$ has too many rational points, leading to a contradiction. □

For convenience, we will call a pair (ℓ, p) of primes *appropriate* if it satisfies the conditions of Proposition 1.4.1.

1.4.1.3 Calculation of $\mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(\mu_p, \mathbb{Z}/p\mathbb{Z})$

We will first calculate $\mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(\mu_p, \mathbb{Z}/p\mathbb{Z})$, which really has nothing specific to this problem.

Theorem 1.4.1 [Sc1, Corollary 4.2]**.** *For $\ell \neq p$ distinct primes, $\mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ is naturally an $\mathbb{F}_p$-vector space, and*

$$\dim_{\mathbb{F}_p} \mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) = \begin{cases} 1 & \text{if } \frac{\ell^2-1}{24} \equiv 0 (\operatorname{mod} p) \\ 0 & \text{otherwise} \end{cases}.$$

Proof. We use the Mayer-Vietoris sequence, Theorem 1.2.7. Note that Hom's all vanish. Also, $\mathrm{Ext}^1_{\mathbb{Z}_p}(\mu_p, \mathbb{Z}/p\mathbb{Z}) = 0$, as we can utilize the connected-étale sequence in this case, so that the exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to G \to \mu_p \to 0$$

becomes, after taking the connected component functor,

$$0 \to 0 \to G^0 \to \mu_p \to 0,$$

which means that the extension is split by identifying the connected component with μ_p. Therefore, the Mayer-Vietoris sequence becomes

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}[1/p\ell]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Q}_p}(\mu_p, \mathbb{Z}/p\mathbb{Z}).$$

What is $\mathrm{Ext}^1_{\mathbb{Q}_p}(\mu_p, \mathbb{Z}/p\mathbb{Z})$? Note that the two group schemes $\mu_p, \mathbb{Z}/p\mathbb{Z}$ are étale, so we can think everything in terms of Galois modules. As $\mu_p \cong \mathbb{Z}/p\mathbb{Z}$ over $\mathbb{Q}_p(\zeta_p)$, $\mathrm{Ext}^1_{\mathbb{Q}_p(\zeta_p)}(\mu_p, \mathbb{Z}/p\mathbb{Z}) \cong \mathrm{Ext}^1_{\mathbb{Q}_p(\zeta_p)}(\mathbb{Z}/p\mathbb{Z}, \mu_p)$. On the other hand, the $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$-invariants of $\mathrm{Ext}^1_{\mathbb{Q}_p(\zeta_p)}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ are precisely $\mathrm{Ext}^1_{\mathbb{Q}_p}(\mu_p, \mathbb{Z}/p\mathbb{Z})$, as an obstruction of Galois descent is in H^2 of Galois cohomology of $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ acting on a p-group, and as $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ is of order coprime to p, the Galois cohomology should vanish. On the other hand, if we denote $\chi : \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p) \to \mathbb{F}_p^\times$ to be the cyclotomic character, then as $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$ acts on μ_p as χ whereas acts trivially on $\mathbb{Z}/p\mathbb{Z}$, the $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$-invariant subspace of $\mathrm{Ext}^1_{\mathbb{Q}_p}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ is identified with the χ^2-eigenspace of $\mathrm{Ext}^1_{\mathbb{Q}_p(\zeta_p)}(\mathbb{Z}/p\mathbb{Z}, \mu_p)$.

The exactly same argument applies to $\mathbb{Z}[1/p\ell]$ via the extension $\mathbb{Z}[1/p\ell, \zeta_p]/\mathbb{Z}[1/p\ell]$; for a number field E, the étale fundamental group of $\mathcal{O}_E[\frac{1}{N}]$ is the Galois group $\mathrm{Gal}(E_N/E)$, where E_N is maximal among extensions of E unramified outside N, so the Galois group of $\mathbb{Z}[1/p\ell, \zeta_p]/\mathbb{Z}[1/p\ell]$ is also $\mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)$, a group of order coprime to p. Thus, our Mayer-Vietoris sequence becomes

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Ext}^1_{\mathbb{Z}[1/p\ell, \zeta_p]}(\mathbb{Z}/p\mathbb{Z}, \mu_p)_{\chi^2} \to \mathrm{Ext}^1_{\mathbb{Q}_p(\zeta_p)}(\mathbb{Z}/p\mathbb{Z}, \mu_p)_{\chi^2}.$$

The Ext long exact sequence of functor $\mathrm{Hom}_{\mathbb{Q}_p(\zeta_p)}(\cdot, \mu_p)$ and $\mathrm{Hom}_{\mathbb{Z}[1/p\ell,\zeta_p]}(\cdot, \mu_p)$ to the exact sequence $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$ gives

$$0 \to \mu_p \to \mathrm{Ext}^1_{\mathbb{Z}[1/p\ell,\zeta_p]}(\mathbb{Z}/p\mathbb{Z}, \mu_p) \to H^1(\pi_{1,\text{ét}}(\mathbb{Z}[1/p\ell, \zeta_p]), \mu_p) \to 0,$$

and

$$0 \to \mu_p \to \mathrm{Ext}^1_{\mathbb{Q}_p(\zeta_p)}(\mathbb{Z}/p\mathbb{Z}, \mu_p) \to H^1(\pi_{1,\text{ét}}(\mathbb{Q}_p(\zeta_p)), \mu_p) \to 0,$$

where H^1 here is a group cohomology. Taking χ^2-eigenspaces, as $(\mu_p)_{\chi^2} = 0$, we have

$$\mathrm{Ext}^1_{\mathbb{Z}[1/p\ell,\zeta_p]}(\mathbb{Z}/p\mathbb{Z}, \mu_p)_{\chi^2} \xrightarrow{\sim} H^1(\pi_{1,\text{ét}}(\mathbb{Z}[1/p\ell, \zeta_p]), \mu_p)_{\chi^2},$$

and

$$\mathrm{Ext}^1_{\mathbb{Q}_p(\zeta_p)}(\mathbb{Z}/p\mathbb{Z}, \mu_p)_{\chi^2} \xrightarrow{\sim} H^1(\pi_{1,\text{ét}}(\mathbb{Q}_p(\zeta_p)), \mu_p)_{\chi^2}.$$

Thus, the Mayer-Vietoris sequence now becomes

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) \to H^1(\pi_{1,\text{ét}}(\mathbb{Z}[1/p\ell, \zeta_p]), \mu_p)_{\chi^2} \to H^1(\pi_{1,\text{ét}}(\mathbb{Q}_p(\zeta_p)), \mu_p)_{\chi^2}.$$

Now we fit this into the long exact sequence of group cohomology applied to the Kummer sequence $0 \to \mu_p \to \mathbb{G}_m \xrightarrow{x \mapsto x^p} \mathbb{G}_m \to 0$. Then, we get the following diagram with vertical complexes being exact (written in this way due to the lack of space).

$$\begin{array}{ccc}
\mathbb{Z}[1/p\ell, \zeta_p]^\times & \longrightarrow & \mathbb{Q}_p(\zeta_p)^\times \\
\downarrow{\scriptstyle x\mapsto x^p} & & \downarrow{\scriptstyle x\mapsto x^p} \\
\mathbb{Z}[1/p\ell, \zeta_p]^\times & \longrightarrow & \mathbb{Q}_p(\zeta_p)^\times \\
\downarrow & & \downarrow \\
H^1(\pi_{1,\text{ét}}(\mathbb{Z}[1/p\ell, \zeta_p]), \mu_p) & \longrightarrow & H^1(\pi_{1,\text{ét}}(\mathbb{Q}_p(\zeta_p)), \mu_p) \\
\downarrow & & \downarrow \\
H^1(\pi_{1,\text{ét}}(\mathbb{Z}[1/p\ell, \zeta_p]), \mathbb{G}_m) & \longrightarrow & H^1(\pi_{1,\text{ét}}(\mathbb{Q}_p(\zeta_p)), \mathbb{G}_m) \\
\downarrow{\scriptstyle x\mapsto x^p} & & \downarrow{\scriptstyle x\mapsto x^p} \\
H^1(\pi_{1,\text{ét}}(\mathbb{Z}[1/p\ell, \zeta_p]), \mathbb{G}_m) & \longrightarrow & H^1(\pi_{1,\text{ét}}(\mathbb{Q}_p(\zeta_p)), \mathbb{G}_m)
\end{array}$$

Note that $H^1(\pi_{1,\text{ét}}(R), \mathbb{G}_m) = \mathrm{Pic}(R)$. Thus, the above diagram simplifies into

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}[1/p\ell, \zeta_p]^\times/\mathbb{Z}[1/p\ell, \zeta_p]^{\times p} & \longrightarrow & H^1(\pi_{1,\text{ét}}(\mathbb{Z}[1/p\ell, \zeta_p]), \mu_p) & \longrightarrow & \mathrm{Pic}(\mathbb{Z}[1/p\ell, \zeta_p])[p] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Q}_p(\zeta_p)^\times/\mathbb{Q}_p(\zeta_p)^{\times p} & \xrightarrow{\sim} & H^1(\pi_{1,\text{ét}}(\mathbb{Q}_p(\zeta_p)), \mu_p) & \longrightarrow & \mathrm{Pic}(\mathbb{Q}_p(\zeta_p))[p] = 0 & &
\end{array}$$

Note that $\mathrm{Pic}(\mathbb{Z}[1/p\ell, \zeta_p])$ is the ideal class group of $\mathbb{Z}[\zeta_p]$ modulo the ideal classes supported in the primes lying over ℓ. Thus, $\mathrm{Pic}(\mathbb{Z}[1/p\ell, \zeta_p])[p]_{\chi^2}$ is a quotient of $\mathrm{Pic}(\mathbb{Z}[\zeta_p])[p]_{\chi^2}$. Note however that $\mathrm{Pic}(\mathbb{Z}[\zeta_p])[p]_\chi = 0$ by [W, Proposition 6.16] and this implies $\mathrm{Pic}(\mathbb{Z}[\zeta_p])[p]_{\chi^2} = 0$ by the proof of [W, Theorem 5.34]. This implies that $\mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ fits into an exact sequence with very computable entries, namely

$$0 \to \mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) \to (\mathbb{Z}[1/p\ell, \zeta_p]^\times/\mathbb{Z}[1/p\ell, \zeta_p]^{\times p})_{\chi^2} \to (\mathbb{Q}_p(\zeta_p)^\times/\mathbb{Q}_p(\zeta_p)^{\times p})_{\chi^2}.$$

We know quite well about fundamental units of cyclotomic fields thanks to [W, §8], so the computation will not be so bad. We now divide into cases.

1. $p = 2$. As the only fundamental units of $\mathbb{Q}(\zeta_2)$ are ± 1, and as $\pm 5^a$ generates the whole $(\mathbb{Z}/2^m\mathbb{Z})^\times$, the group $\mathbb{Z}[1/2\ell]^\times/\mathbb{Z}[1/2\ell]^{\times 2}$ is generated by $2, -1, \ell$ whereas the group $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ is generated by $2, -1, 5$. So the kernel is nonzero if and only if $\pm\ell$ is a 2-adic square, i.e. $\ell \equiv \pm 1 (\bmod 8)$.

2. $p = 3$. Note that $\chi^2 = 1$. As the fundamental unit of $\mathbb{Z}$ is ± 1, the group

$$(\mathbb{Z}[1/3\ell, \zeta_3]^\times/\mathbb{Z}[1/3\ell, \zeta_3]^{\times 3})_{\mathrm{id}}$$

is 2-dimensional, generated by 3 and ℓ. Also 2-dimensional is $(\mathbb{Q}_3(\zeta_3)^\times/\mathbb{Q}_3(\zeta_3)^{\times 3})_1$, which is generated by 3 and some other integer n. Thus the kernel is nonzero if and only if ℓ is a 3-adic cube, i.e. when $\ell \equiv \pm 1 (\bmod 9)$.

3. $p \geq 5$. As $2 < p - 1$, $(\mathbb{Q}_p(\zeta_p)^\times/\mathbb{Q}_p(\zeta_p)^{\times p})_{\chi^2}$ is 1-dimensional. The theorem [W, Theorem 8.25] implies that the exact sequence is surjective on the right, so $\mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ is 0-dimensional if and only if $(\mathbb{Z}[1/p\ell, \zeta_p]^\times/\mathbb{Z}[1/p\ell, \zeta_p]^{\times p})_{\chi^2}$ is 1-dimensional. As $\mathbb{Z}[1/p\ell, \zeta_p]$ is obtained by inverting ℓ from $\mathbb{Z}[1/p, \zeta_p]$, there is a natrual exact sequence

$$0 \to \mathbb{Z}[1/p, \zeta_p]^\times \to \mathbb{Z}[1/p\ell, \zeta_p]^\times \to \bigoplus_{\mathfrak{l}|\ell} \mathbb{Z} \to \mathrm{Pic}(\mathbb{Z}[1/p, \zeta_p]) \xrightarrow{p} \mathrm{Pic}(\mathbb{Z}[1/p\ell, \zeta_p]) \to 0.$$

Note that we already have seen that $\mathrm{Cl}(\mathbb{Z}[1/p, \zeta_p])[p]_{\chi^2} = 0$. Thus, after tensoring with $\mathbb{Z}_p$, we can take χ^2-eigenspace, so that we get an exact sequence

$$0 \to (\mathbb{Z}_p[1/p, \zeta_p]^\times)_{\chi^2} \to (\mathbb{Z}[1/p\ell, \zeta_p]^\times)_{\chi^2} \to \left(\bigoplus_{\mathfrak{l}|\ell} \mathbb{Z}_p\right)_{\chi^2} \to 0.$$

This is split as the third entry is $\mathbb{Z}_p$-free. Thus we can take quotient on each entry by p-th power and still remain to get an exact sequence. Thus, we have an exact sequence

$$0 \to (\mathbb{Z}[1/p, \zeta_p]^\times/\mathbb{Z}[1/p, \zeta_p]^{\times p})_{\chi^2} \to (\mathbb{Z}[1/p\ell, \zeta_p]^\times/\mathbb{Z}[1/p\ell, \zeta_p]^{\times p})_{\chi^2} \to \left(\bigoplus_{\mathfrak{l}|\ell} \mathbb{F}_p\right)_{\chi^2} \to 0.$$

Note that [W, Proposition 8.13] says that, as $\mathbb{F}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})]$-modules,

$$\mathbb{Z}[1/p, \zeta_p]^\times/\mathbb{Z}[1/p, \zeta_p]^{\times p} \cong \mu_p \times \mathbb{F}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p + \zeta_p^{-1})/\mathbb{Q})],$$

which has one-dimensional χ^2-eigenspace. Thus, $\mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ is 0-dimensional if and only if $\left(\bigoplus_{\mathfrak{l}|\ell} \mathbb{F}_p\right)_{\chi^2}$ is 0-dimensional. Note that $\left(\bigoplus_{\mathfrak{l}|\ell} \mathbb{F}_p\right)$, as an $\mathbb{F}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})]$-module, is isomorphic to $\mathbb{F}_p[\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})/(\ell)]$, so the χ^2-eigenspace is nontrivial if and only if it is one-dimensional and $\chi^2(\ell) = 1$, which is equivalent to $\ell \equiv \pm 1 (\bmod p)$.

Thus we have computed all cases, so that

$$\dim_{\mathbb{F}_p} \mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) = \begin{cases} & \text{if } p = 2 \text{ and } \ell \equiv \pm 1 (\bmod 8), \\ 1 & p = 3 \text{ and } \ell \equiv \pm 1 (\bmod 9), \\ & \text{or } p \geq 5, \ell \equiv \pm 1 (\bmod p) \\ 0 & \text{otherwise.} \end{cases}$$

A compact way of writing the long condition above is that $\frac{\ell^2 - 1}{24} \equiv 0 (\bmod p)$, so we are done. □

1.4.1.4 Simple Objects of $\mathcal{D}_\ell^p$

To use Proposition 1.4.1, the simple objects of $\mathcal{D}_\ell^p$ should be μ_p and $\mathbb{Z}/p\mathbb{Z}$. Recall that, in the first nonexistence proofs, we deduced this via arguing first that, a simple object must be of order p, andn that there are not many choices for order p groups. Along the lines of Proposition 1.3.3, we have the following.

Theorem 1.4.2 [TO, §3, Corollary]**.** *If R is a localization of the ring of integers of a field K whose class number is coprime to $p-1$ and (p) stays inert to be a prime ideal in R, then, up to a twist by everywhere unramified character, the only finite flat commutative R-group schemes of order p are μ_p and $\mathbb{Z}/p\mathbb{Z}$.*

In particular, this theorem can be applied to $R = \mathbb{Z}[1/\ell]$. So what we need to prove is that, for an appropriate choice of $p \neq \ell$, simple objects of $\mathcal{D}_\ell^p$ are of order p.

Proposition 1.4.2. *Let $\ell \neq p$ be distinct primes. Suppose that every $G \in \mathcal{D}_\ell^p$, killed by p and containing μ_p as a closed subgroup scheme, has a field of definition $L = \mathbb{Q}(G(\overline{\mathbb{Q}}))$ a p-extension of $\mathbb{Q}(\zeta_p)$. Then the only simple objects of $\mathcal{D}_\ell^p$ are μ_p and $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Let G be a simple object in $\mathcal{D}_\ell^p$. The field L' generated by geometric points of $G \times \mu_p$ has $[L' : \mathbb{Q}(\zeta_p)]$ a power of p. As $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_p)) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $G(\overline{\mathbb{Q}})$ via the finite p-group $\mathrm{Gal}(L/\mathbb{Q}(\zeta_p))$, and as $G(\mathbb{Q})$ is a simple Galois module of p-power order, the fixed part of $G(\overline{\mathbb{Q}})$ being nontrivial implies that the whole $G(\overline{\mathbb{Q}})$ is fixed by $\mathrm{Gal}(L/\mathbb{Q}(\zeta_p))$. Thus, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $G(\overline{\mathbb{Q}})$ via $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. As $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ is a cyclic group of order $p-1$, and as the $(p-1)$-st roots of unity are all in $\mathbb{F}_p$, the eigenspace decomposition of $G(\overline{\mathbb{Q}})$ implies that the whole $G(\overline{\mathbb{Q}})$ is equal to one of the eigenspaces, and is therefore 1-dimensional over $\mathbb{F}_p$. Therefore, G is of order p, so by Theorem 1.4.2, G is $\mathbb{Z}/p\mathbb{Z}$ or μ_p twisted by a character ψ unramified outside $\ell\infty$. As G is an order p group, such a character necessarily has order dividing $p-1$. On the other hand, as $G \in \mathcal{D}_\ell^p$, the ramification index at ℓ of the field generated by geometric points of ψ should be a power of p. Thus, ψ is ramified only at ∞, or ψ is trivial. This finishes the proof. □

Thus, we can alleviate our condition to embed a group scheme in $\mathcal{D}_\ell^p$ killed by p to a known group scheme whose field of definition is of degree a power of p over $\mathbb{Q}(\zeta_p)$.

Lemma 1.4.1 [Sc1, Proposition 5.1]**.** *Let ℓ, p be distinct primes and $G \in \mathcal{D}_\ell^p$ be killed by p. Then, one can find another $G' \in \mathcal{D}_\ell^p$, containing G and killed by p, such that the field of definition $L = \mathbb{Q}(G'(\overline{Q}))$ satisfies the following properties.*

- *Let*
$$F = \begin{cases} \mathbb{Q}(\zeta_\ell) & \text{if } p|(\ell-1) \\ \mathbb{Q} & \text{otherwise.} \end{cases}$$
Then, $F(\zeta_{2p}, \sqrt[p]{\ell}) \subset L$, and this extension is unramified at all primes outside p.
- *Let d_L be the absolute discriminant of L. Then, $v_p(d_L^{\frac{1}{[L:\mathbb{Q}]}}) < 1 + \frac{1}{p-1}$.*

Proof. Let $G' \in \mathcal{D}_\ell^p$ be defined as follows.

$$G' = \begin{cases} \mu_p \times G \times G_\ell \times G_{-1} & \text{if } p = 2 \\ \mu_p \times G \times G_\ell \times \rho_{p;\ell} & \text{if } p > 2, p|(\ell-1) \\ \mu_p \times G \times G_\ell & \text{otherwise.} \end{cases}$$

Here G_ϵ is the Katz-Mazur group scheme, and $\rho_{p;\ell}$ is the 2-dimensional $\mathbb{F}_p$-representation of $G_{\mathbb{Q}}$ defined at the beginning of the section. It is obvious that $L = \mathbb{Q}(G'(\overline{Q}))$ contains $F(\zeta_{2p}, \sqrt[p]{\ell})$. As $G' \in \mathcal{D}_\ell^p$, we know that the inertia group of any prime $\mathfrak{l}$ in L over ℓ acts tamely. Also, as G' is killed by p, for any g in the inertia group of $\mathfrak{l}$, $g^p = \mathrm{id}$. Since tame ramification groups are cyclic, this implies that the ramification index of $\mathfrak{l}$ divide p. On the other hand, we know that any prime over ℓ in $F(\zeta_{2p}, \sqrt[p]{\ell})$ has ramification index exactly p, so $L/F(\zeta_{2p}, \sqrt[p]{\ell})$ is unramified over ℓ. By Theorem 1.3.2, we a priori knew this extension is unramified outside p and ℓ. Thus, this extension is unramified outside p. The upper bound on the p-adic valuation of discriminant is the Fontaine's ramification bound in Theorem 1.3.2 as well. □

Now we completely translated our problem into a Galois theory problem. *Given a prime ℓ, is there a prime $p \neq \ell$ such that $\frac{\ell^2-1}{24} \not\equiv 0 (\mathrm{mod}\, p)$ and a Galois extension satisfying the conditions of Lemma 1.4.1 has degree a power of p*? If so, (ℓ, p) will be appropriate, and we can deduce the nonexistence of semi-stable abelian varieties over $\mathbb{Z}[1/\ell]$.

Theorem 1.1.3 [Sc1, §6]**.** *For the primes $\ell = 2, 3, 5, 7, 13$, there is no nontrivial abelian variety over $\mathbb{Q}$ with good reduction outside ℓ and semi-stable reduction at ℓ.*

Proof. We will show that the pairs of primes $(\ell, p) = (2, 3), (3, 2), (5, 2), (7, 3), (13, 2)$ are appropriate. Indeed, those primes satisfy $\frac{\ell^2-1}{24} \not\equiv 0 (\mathrm{mod}\, p)$. Thus, we need to check that, for a pair of prime in the above, a field extension L satisfying the conditions of Lemma 1.4.1 has a degree over $\mathbb{Q}$ a power of p. The Odlyzko discriminant bounds [Mar] with a discriminant bound from Lemma 1.4.1 imply that,

$$[L:\mathbb{Q}] < \begin{cases} 24 & \text{if } (\ell,p) = (2,3) \\ 32 & \text{if } (\ell,p) = (3,2) \\ 480 & \text{if } (\ell,p) = (5,2) \\ 270 & \text{if } (\ell,p) = (7,3) \\ 60 & \text{if } (\ell,p) = (13,2). \end{cases}$$

Let $F(\zeta_{2p}, \sqrt[p]{\ell})$ as in the conditions of Lemma 1.4.1 be denoted as K. Then, it follows that

$$[L:K] \leq \begin{cases} 3 & \text{if } (\ell,p) = (2,3) \\ 7 & \text{if } (\ell,p) = (3,2) \\ 59 & \text{if } (\ell,p) = (5,2) \\ 14 & \text{if } (\ell,p) = (7,3) \\ 14 & \text{if } (\ell,p) = (13,2). \end{cases}$$

In particular, the Galois group $\mathrm{Gal}(L/K)$ is of order < 60 for all cases, so it is *solvable*. As $\mathrm{Gal}(K/\mathbb{Q})$ is also solvable in all cases, $G = \mathrm{Gal}(L/\mathbb{Q})$ is solvable as well.

Then the proof proceeds by calculating various cases using class field theory to show that successive subquotients of the derived series of $[G:G]$ is a p-group, and the fixed field of $[G:G]$, the maximal abelian extension of $\mathbb{Q}$ in L, is a p-extension of $\mathbb{Q}(\zeta_p)$; one can check the calculations in [Sc1, §6]. In particular, this implies that $[G:G]$ as well as $\mathrm{Gal}(L/\mathbb{Q}(\zeta_p))/[G:G]$ is a p-group. Thus, $\mathrm{Gal}(L/\mathbb{Q}(\zeta_p))$ is a p-group. We can then use Lemma 1.4.1 and Proposition 1.4.2 to deduce that the only simple objects of $\mathcal{D}_\ell^p$ are μ_p and $\mathbb{Z}/p\mathbb{Z}$. Therefore, the pairs of primes we stated in the beginning of the proof are appropriate, as desired. □

1.4.2 Results of Brumer-Kramer

Despite of yielding strictly weaker results, the work of Brumer-Kramer in [BK] should be mentioned, as it uses a different application of Fontaine's discriminant bounds. The proof is quite different in spirit, since it proceeds by making a contradiction, not by analyzing restrictions on p-divisible groups, but by *constructing infinitely many non-isomorphic isogenous abelian varieties, contradicting with the Faltings' Finiteness Theorem*, Theorem 1.2.38(iii). We will in particular use ℓ-adic Tate modules, for $\ell \neq p$.

1.4.2.1 Increasing Effective Stage of Inertia

Let A be an abelian variety over $\mathbb{Q}_p$ of dimension $d > 0$ with semi-stable bad reduction. We want to keep track of *how ramified $A(\ell)$ is* via the following definition.

Definition 1.4.1. *The* effective stage of inertia *acting on $T_\ell(A)$, written $i(A, \ell, p)$, is the minimal integer $n \geq 1$ such that $\mathbb{Q}_p(A[\ell^n])$ is ramified at p.*

This definition is in particular well-defined because of the Néron-Ogg-Shafarevich Criterion, Theorem 1.2.28. We would like to construct a new non-isomorphic yet isogenous abelian variety from A via taking the quotient of it by an appropriate finite subgroup so that the effective stage of inertia increases.

Recall that, by Theorem 1.2.30, the ℓ-adic Tate module $T_\ell(A)$ has a "finite part" $\mathcal{M}_\ell^f(A) = T_\ell(A)^{I_p}$, where I_p is the inertia group, and a "toric part" $\mathcal{M}_\ell^t(A) \subset \mathcal{M}_\ell^f(A)$ which corresponds to $\mathcal{M}_\ell^f(\widehat{A})$ via the Weil pairing. From this information, we know how to quotient A to increase the effective stage of inertia.

Theorem 1.4.3 [BK, Lemma3]**.** *Let $\overline{\mathcal{M}}_f(A)$ and $\overline{\mathcal{M}}_t(A)$ denote the projections of $\mathcal{M}_\ell^f(A)$ and $\mathcal{M}_\ell^t(A)$ to $A[\ell]$. For any $G_{\mathbb{Q}_p}$-submodule κ of $\overline{\mathcal{M}}_f(A)$ containing $\overline{\mathcal{M}}_t(A)$, $i'(A/\kappa, \ell, p) = i(A, \ell, p) + 1$.*

Proof sketch. Let $A' = A/\kappa$. As $\kappa \subset A[\ell]$, the isogeny $\varphi : A \to A'$ is of degree ℓ, so we can construct a $\mathbb{Q}_p$-isogeny $\varphi' : A' \to A$ so that $\varphi \circ \varphi' = [\ell]_{A'}$, $\varphi' \circ \varphi = [\ell]_A$. Note that the effect of φ on ℓ-adic Tate modules is that it is injective, it factors through $T_\ell(A')/\ell T_\ell(A') = A'[\ell]$, and the cokernel is isomorphic to an ℓ-Sylow subgroup of κ. In particular, $T_\ell(\varphi)(\mathcal{M}_\ell^f(A)) \subset \mathcal{M}_\ell^f(A')$ and $T_\ell(\varphi)(\mathcal{M}_\ell^t(A)) \subset \mathcal{M}_\ell^t(A')$. So we have a commutative diagram

$$\begin{array}{ccc} T_\ell(A)/\mathcal{M}_\ell^f(A) & \xrightarrow{\varphi} & T_\ell(A')/\mathcal{M}_\ell^f(A') \\ \Big\downarrow{\scriptstyle \times\ell} & & \Big\downarrow \\ \mathcal{M}_\ell^t(A) & \xleftarrow{\varphi'} & \mathcal{M}_\ell^t(A') \end{array}$$

The condition $\overline{\mathcal{M}}_t(A) \subset \kappa \subset \overline{\mathcal{M}}_f(A)$ implies that the horizontal arrows are isomorphisms, and the conclusion follows. □

To apply this to our situation, consider an abelian variety A over $\mathbb{Q}$ with semi-stable bad reduction at p and good reduction outside p. It is sufficient to show that, for some $\ell \neq p$, $\overline{\mathcal{M}}_\ell^f(A_{\mathbb{Q}_p})$ and/or $\overline{\mathcal{M}}_\ell^t(A_{\mathbb{Q}_p})$, a priori $G_{\mathbb{Q}_p}$-submodules of $T_\ell(A)$, are actually $G_{\mathbb{Q}}$-submodules of $T_\ell(A)$. This is possible with a restriction on the ℓ-division field $\mathbb{Q}(A[\ell])$.

Proposition 1.4.3 [BK, Proposition 4]**.** *Let $A/\mathbb{Q}$ be an abelian variety with semi-stable bad reduction at p and good reduction at ℓ. Suppose that the ℓ-division field $L = \mathbb{Q}(A[\ell])$ satisfies the following condition:* there is only one prime over p. *Then, there is a $\mathbb{Q}$-isogeny $\varphi : A \to A'$ such that $i(A', \ell, p) = i(A, \ell, p) + 1$.*

Proof. As noted above, it is sufficient to show that $\overline{\mathcal{M}}_\ell^f(A_{\mathbb{Q}_p})$ is a $G_{\mathbb{Q}}$-submodule of $T_\ell(A)$. As the inertia group I_p is normal in the decomposition group D_p, it follows that $\mathcal{M}_\ell^f(A_{\mathbb{Q}_p})$ is a D_p-module. As there is only one prime in L over p, it follows that D_p maps onto $\mathrm{Gal}(L/\mathbb{Q})$ by restriction. This implies that $\mathcal{M}_\ell^f(A_{\mathbb{Q}_p})$ is a $\mathrm{Gal}(L/\mathbb{Q})$-module. As L is the field of definition of $A[\ell]$, it follows that $\mathcal{M}_\ell^f(A_{\mathbb{Q}_p})$ is a $G_{\mathbb{Q}}$-submodule of $A[\ell]$. □

Thus, as done in the proof of Fontaine, we have reduced the problem about the field of definition of a torsion subgroup. We have seen a fair amount of problems like this, so we list what we know about $L = \mathbb{Q}(A[\ell])$.

- The extension $L/\mathbb{Q}$ is Galois, and is unramified outside ℓ and p.
- The ramification degree of L at p divides ℓ, as $A[\ell]$ is killed by ℓ.
- The higher ramification groups $G_\ell^{(u)}$ vanishes for $u > 1 + \frac{1}{\ell-1}$, where G_ℓ is a decomposition group at a prime over ℓ.
- It actually turns out that L *always contains* $\mathbb{Q}(\zeta_\ell)$. This is due to the following lemma.

Lemma 1.4.2 [BK, Lemma 1]**.** *If A is an abelian variety defined over a field K of characteristic 0, then $K(\zeta_{\ell^n}) \subset K(A[\ell^n])$.*

Proof. Consider a polarization $\lambda : A \to \widehat{A}$ over K of minimal degree. If $A[\ell] \subset \ker\lambda$, then there exists another polarization $\gamma : A \to \widehat{A}$ over K such that $\gamma \circ [\ell]_A = \lambda$, which gives a contradiction on the minimality of degree. Thus, $A[\ell]$ is not contained in $\ker\lambda$. We can then choose a point $p_1 \in A[\ell] - \ker\lambda$ and lift it to $p_n \in A[\ell^n]$ such that its ℓ^{n-1}-th power is p_1. That $p_1 \in A[\ell]$ but not in $\ker\lambda$ implies that $\lambda(p_n)$ is of order exactly ℓ^n. As $\mathrm{char}\, K = 0$, the Weil pairing $e_{\ell^n} : A[\ell^n] \times \widehat{A}[\ell^n] \to \mu_{\ell^n}$ is perfect, we can find a point $q_n \in A[\ell^n]$ such that $e_{\ell^n}(q_n, \lambda(p_n)) = \zeta_n$. Observe that $\mathrm{Gal}(K(A[\ell^n])/K)$ fixes $p_n, q_n \in A[\ell^n]$, so it fixes ζ_n. Thus, $K(\zeta_n) \subset K(A[\ell^n])$. □

1.4.2.2 Finishing the Proof

We have succeeded in translating the whole problem to a class field theoretic problem. The following result is the main down-to-earth calculation of [BK].

Theorem 1.4.4. *For pairs of primes $(\ell, p) = (2,3), (2,7), (3,2), (3,6), (5,2), (5,3)$, a Galois extension $L/\mathbb{Q}(\zeta_\ell)$ satisfying the following conditions have only one prime over p.*

1. *The ramification degree of $L/\mathbb{Q}$ at p divides ℓ.*
2. *The higher ramification groups $G_\ell^{(u)}$ vanishes for $u > 1 + \frac{1}{\ell-1}$, where G_ℓ is a decomposition group at a prime over ℓ.*

This will induce the following main result of [BK].

Theorem 1.4.5 [BK, Theorem 1]**.** *There is no semi-stable abelian variety of positive dimension defined over $\mathbb{Q}$ with good reduction everywhere outside one prime $p \leq 7$.*

Proof sketch of Theorem 1.4.4. Consider the following subfield of L,

$$F = \begin{cases} \mathbb{Q}(\zeta_\ell) & \text{if } \ell \text{ is odd} \\ \mathbb{Q}(\zeta_4) & \text{if } \ell = 2 \end{cases}$$

Here, if $\ell = 2$, one may need to extend L to contain ζ_4, which is harmless in proving the theorem. Let E be the maximal abelian subextension of F in L and $H = \mathrm{Gal}(L/F)$. Note that we now face a case where $L/\mathbb{Q}$ may be ramified even outside ℓ. However, note that the valuation of the different $\mathfrak{D}_{\mathbb{Q}_p(A[\ell^n])/\mathbb{Q}_p}$ is $\ell^{n-i(A,\ell,p)+1}-1$ for $n \geq i(A,\ell,p)$; this is because the inertia group I_p acts via the maximal pro-ℓ quotient, which is (topologically) generated by one element. Thus, we have a discriminant bound

$$|d_L|^{\frac{1}{[L:\mathbb{Q}]}} < \ell^{1+\frac{1}{\ell-1}} p^{1-\frac{1}{\ell}}.$$

The Odlyzko discriminant bound [Mar] tells us that

$$[L:\mathbb{Q}] \leq \begin{cases} 10 & \text{if } (\ell,p)=(2,3) \\ 22 & \text{if } (\ell,p)=(2,7) \\ 14 & \text{if } (\ell,p)=(3,2) \\ 68 & \text{if } (\ell,p)=(3,5) \\ 40 & \text{if } (\ell,p)=(5,2) \\ 168 & \text{if } (\ell,p)=(5,3) \end{cases}$$

Thus,

$$[L:F] \leq \begin{cases} 5 & \text{if } (\ell,p)=(2,3) \\ 11 & \text{if } (\ell,p)=(2,7) \\ 7 & \text{if } (\ell,p)=(3,2) \\ 34 & \text{if } (\ell,p)=(3,5) \\ 10 & \text{if } (\ell,p)=(5,2) \\ 42 & \text{if } (\ell,p)=(5,3) \end{cases} < 60,$$

which implies that H is solvable.

For ℓ odd, p is inert in F, so E is necessarily $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{p})$. We use class field theory to compute successive subquotients of derived series of H to conclude that H is an ℓ-group. As the ramification degree at p divides ℓ, $|H|=\ell$, so $E=L$, and indeed there is only one prime in E over p.

On the other hand, if $\ell=2$, E is a subfield of $\mathbb{Q}(\zeta_4,\sqrt{p})$, and as there is only one prime in $\mathbb{Q}(\zeta_4,\sqrt{p})$ over p, one can assume that L/E is nontrivial. Let E' be the maximal abelian subextension of E in L. A basic Galois theory shows that E'/E is nontrivial of odd degree, unramified outside 2 and at worst tamely ramified for primes over 2. However, such field does not exist via class field theory. □

Chapter 2

Nonexistence of Certain Proper Schemes

2.1 Overview

Thanks to the development of p-adic Hodge theory, algebraic objects can be associated to a vastly wider class of varieties and schemes, and it starts by looking at the *p-adic étale cohomology groups* of the schemes. If a given scheme is nice enough, which is a condition especially has to do with reduction behavior, the p-adic étale cohomology, as a p-adic Galois representation, is known to fall into some very nice class of p-adic Galois representations. Such classes of p-adic Galois representations have corresponding *Dieudonné modules*, which are just consisted of Galois modules with linear algebraic data. By proving ramification bounds for such algebraic objects, one can lay severe structural restrictions on the p-adic Galois representation coming from geometry.

More specifically, for a smooth proper scheme X over a number field K having everywhere good reduction, it is known that the p-adic étale cohomology group $H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ as a p-adic G_K-representation is unramified outside p and *crystalline* at p. The relevant discriminant bound we will be proving for this situation is the following.

Theorem 2.1.1 (Fontaine, [Fo2, Théorème 2])**.** *Let k be a perfect field of characteristic $p > 0$, $W = W(k)$, $K = \operatorname{Frac} W$ and $G = G_K$. Let X be a proper smooth scheme over O. Let $0 \le m < p - 1$ be an integer. Then, the ramification subgroups $G^{(v)} \subset G$ acts trivially on any subfactor in $H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ which is annihilated by p if $v > 1 + \frac{m}{p-1}$.*

On the other hand, if X has a *semi-stable reduction* at p and good reduction everywhere else, then the p-adic étale cohomology group $H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ as a p-adic G_K-representation is unramified outside p and *semi-stable* at p. The relevant discriminant bound in this situation is the following.

Theorem 2.1.2 (Caruso-Liu, [CL, Theorem 1.1])**.** *Let $p > 2$ be a prime number and k be a perfect field of characteristic p. Let $W = W(k)$, and K be a totally ramified extension of $W[1/p]$ of degree e. Let $G = G_K$, and v_K be the discrete valuation on K noramlized by $v_K(K^\times) = \mathbb{Z}$.*

Consider a positive integer r and V a semi-stable representation of G with Hodge-Tate weights in $[-r, 0]$. Let T be the quotient of two G-stable $\mathbb{Z}_p$-lattices in V, which is again a representation of G annihilated by p^n for some integer n. Denote by $\rho : G \to \operatorname{Aut}_{\mathbb{Z}_p}(T)$ the associated group homomorphism and by L the finite extension of K defined by $\ker \rho$. If we write $\frac{nr}{p-1} = p^\alpha \beta$ with $\alpha \in \mathbb{N}$ and $\frac{1}{p} < \beta \le 1$, then

1. *if $\mu > 1 + e(n + \alpha) + \max(e\beta - \frac{1}{p^{n+\alpha}}, \frac{e}{p-1})$, then $G^{(\mu)}$ acts trivially on T;*

2. $v_K(\mathfrak{D}_{L/K}) < 1 + e(n+\alpha+\beta) - \frac{1}{p^{n+\alpha}}$,

where $\mathfrak{D}_{L/K}$ *is the different of* L/K*.*

Using these two discriminant bounds, we will prove the following two nonexistence results.

Theorem 2.1.3 (Fontaine, [Fo2, Théorème 1], [Ab2, 7.6])**.** *Let* X *be a smooth proper variety over* $\mathbb{Q}$ *with everywhere good reduction. Then,* $H^i(X, \Omega_X^j) = 0$ *for* $i \neq j$, $i + j \leq 3$.

Theorem 2.1.4 (Abrashkin, [Ab4, Theorem 0.1])**.** *If* Y *is a smooth projective variety over* $\mathbb{Q}$ *having semi-stable reduction at 3 and good reduction outside 3, then* $h^2(Y_{\mathbb{C}}) = h^{1,1}(Y_{\mathbb{C}})$.

In this chapter, we develop the necessary preliminaries to understandn the above results. The preliminaries include étale cohomology theory, p-adic Hodge theory, p-adic comparison theorems and various integral p-adic Hodge theory including the theory of Fontaine-Laffaille, Breuil-Kisin and Liu.

2.2 Preliminaries

We assume the reader is familiar with class field theory, algebraic geometry and homological algebra, including spectral sequences.

2.2.1 Étale Cohomology and the Weil Conjectures

2.2.1.1 Sites and Topoi

The first motivation for development of étale cohomology is to develop a cohomology theory of schemes that is analogous to singular cohomology of topological spaces. To achieve the objective, one needs a cohomology theory that is defined over some topology which is finer than the Zariski topology.

In retrospect, sheaf cohomology as well as singular cohomology can be neatly defined as *a right derived functor of a left-exact section functor*. In this sense, one realizes that what is really needed to define a cohomology theory is not the underlying topology, but the *category of sheaves on the topology*, known as *a topos*. Recall that a sheaf on a scheme is determined by its restriction on affine open subschemes. In this regard, we can in particular massage the restriction of having an actual topology to instead have information on a certain kind of open sets and how such open sets cover other open sets. This is the notion of site, which we will define now.

Definition 2.2.1 (Site)**.** *A* site *is consisted of a pair* $(T, \mathrm{Cov}(T))$ *of a category* T *and a collection* $\mathrm{Cov}(T)$ *of* coverings*, i.e. families* $\{\varphi_i : U_i \to U\}_{i\in I}$ *of morphisms in* T*, satisfying the following properties.*

1. *For* $\{\varphi_i : U_i \to U\}_{i\in I} \in \mathrm{Cov}(T)$ *and a morphism* $V \to U$ *in* T*, the fiber products* $U_i \times_U V$ *exist for all* $i \in I$*, and* $\{\varphi_{i,V} : U_i \times_U V \to V\}_{i\in I} \in \mathrm{Cov}(T)$*.*
2. *Given* $\{\varphi_i : U_i \to U\}_{i\in I} \in \mathrm{Cov}(T)$ *and* $\{\psi_{ij} : V_{ij} \to U_i\}_{j\in J_i} \in \mathrm{Cov}(T)$ *for all* $i \in I$*, the family* $\{\varphi_i \circ \psi_{ij} : V_{ij} \to U\}_{i\in I, j\in J_i}$ *is also a covering.*
3. *If* $\varphi : U' \to U$ *is an isomorphism in* T*, then* $\{\varphi : U' \to U\}$ *is a covering.*

We often denote the site itself as T *too.*

Example 2.2.1. Obviously, any topology on a topological space X gives a site $(O_X, \mathrm{Cov}(O_X))$, where O_X is the category of open subsets of X, and coverings are just topological coverings. This is why categorical-minded people sometimes use the word *topology* instead of site.

A slightly more interesting example is the *canonical topology.* Given a category $\mathcal{C}$ with fiber products, one can always define a site, the canonical topology, by requiring a covering to be *a family of universal effective epimorphisms.* Namely, a family $\{U_i \to V\}$ of morphisms in $\mathcal{C}$ is *a family of effective epimorphisms* if the equalizer sequence

$$\mathrm{Hom}(V, Z) \to \prod_i \mathrm{Hom}(U_i, Z) \rightrightarrows \prod_{i,j} \mathrm{Hom}(U_i \times_V U_j, Z)$$

is exact for each $Z \in \mathcal{C}$. A family of morphisms is *a family of universal effective epimorphisms* if any pullback of the family is a family of effective epimorphisms. It is easy to check that this is indeed a site, and it is also meant to be the finest site on $\mathcal{C}$ that each representable presheaf, $U \mapsto \mathrm{Hom}(U, Z)$ for a fixed $Z \in \mathrm{Obj}\,\mathcal{C}$, is a sheaf.

As the assignment of data in the definition of sites is functorial, we can define a morphism of sites and, more importantly, the notion of presheaves and sheaves on a site.

Definition 2.2.2 (Morphism of Sites)**.** *Given sites T, T', a* morphism of sites *is a functor $f : T \to T'$ of the underlying categories satisfying the following.*

1. *Given a covering $\{\varphi_i : U_i \to U\}_{i\in I} \in \mathrm{Cov}(T)$, we have a covering $\{f(\varphi_i) : f(U_i) \to f(U)\}_{i\in I}\,\mathrm{Cov}(T')$.*
2. *Given a covering $\{\varphi_i : U_i \to U\}_{i\in I} \in \mathrm{Cov}(T)$ and a morphism $g : V \to U$ in T, the canonical morphism*
$$f(U_i \times_U V) \to f(U_i) \times_{f(U)} f(V),$$
coming from the universal property of fiber products, is an isomorphism.

Definition 2.2.3 (Sheaves on Sites)**.** *Let T be a site, and $\mathcal{C}$ be a category with products, for example* **AbGrp** *or* **Sets***. Then a* presheaf on T with values in $\mathcal{C}$ *is a contravariant functor $F : T \to \mathcal{C}$. A* morphism of presheaves *is a natural transformation between contravariant functors.*

A presheaf F on T is a sheaf *if, for every $\{U_i \to U\}_{i\in I} \in \mathrm{Cov}(T)$, the equalizer sequence*

$$F(U) \to \prod_{i\in I} F(U_i) \rightrightarrows \prod_{i,j\in I} F(U_i \times_U U_j)$$

is exact in $\mathcal{C}$. A morphism of sheaves *is a morphism as a morphism of presheaves. In particular, (pre)sheaves on T with values in* **AbGrp** *are called* abelian (pre)sheaves*.*

We would like to introduce general facts about sites and categories of abelian sheaves on sites. The proofs will be omitted, but they are fairly straightforward abstract nonsense. In this section, we will let T be a site, and $\mathcal{P}$ ($\mathcal{S}$, respectively) be the category of abelian presheaves (abelian sheaves, respectively) on T.

Theorem 2.2.1 ([Tam, (I.2.1.2), (I.3.2.2)])**.** *The categories $\mathcal{P}, \mathcal{S}$ are abelian categories with sufficiently many injectives.*

For $U \in \mathrm{Obj}(T)$, $\Gamma_U : \mathcal{P} \to$ **AbGrp** be the section functor, i.e. $F \mapsto F(U)$. We will use the same notation for the section functor on the category of abelian sheaves as well.

Proposition 2.2.1 [Tam, (I.2.1.1), (I.3.2.1), (I.3.1.1)]**.** *Let* $U \in \mathrm{Obj}(T)$*.*

(i) The section functor $\Gamma_U : \mathcal{P} \to$ **AbGrp** *on* $\mathcal{P}$ *is exact. More generally, a sequence* $F' \to F \to F''$ *in* $\mathcal{P}$ *is exact if and only if* $F'(U) \to F(U) \to F''(U)$ *is exact in* **AbGrp** *for all* $U \in \mathrm{Obj}(T)$*.*

(ii) The natural inclusion functor $\iota : \mathcal{S} \to \mathcal{P}$ *is left exact. Therefore, the section functor* $\Gamma_U : \mathcal{S} \to$ **AbGrp** *on* $\mathcal{S}$ *is left exact.*

(iii) The inclusion $\iota : \mathcal{S} \to \mathcal{P}$ *has the left adjoint functor, the* sheafification functor $\# : \mathcal{P} \to \mathcal{S}$*. The sheafification functor is exact.*

Definition 2.2.4 (Direct and Inverse Images)**.** *Let* T, T' *be sites, and* $\mathcal{P}, \mathcal{P}'$ *be the categories of abelian presheaves on* T, T'*, respectievly. Given a morphism* $f : T \to T'$ *of topologies, we define the* (presheaf) inverse image functor $f^p : \mathcal{P}' \to \mathcal{P}$ *by* $f^p F'(U) = F'(f(U))$*. The functor* f^p *has a left adjoint* $f_p : \mathcal{P} \to \mathcal{P}'$*, called the* (presheaf) direct image functor*.*

Similarly, let $\mathcal{S}, \mathcal{S}'$ *be the categories of abelian sheaves on* T, T'*. Then, there are the* (sheaf) inverse image functor $f^s := \#_T \circ f^p \circ \iota_{T'}$ *and the* (sheaf) direct image functor $f_s := \#_{T'} \circ f_p \circ \iota_T$*, which is left adjoint to* f^s*.*

Proposition 2.2.2. *Let* $f : T \to T'$ *be a morphism of topologies.*

(i) f^p *is exact and commutes with direct limits.*

(ii) f_p *is right exact and commutes with direct limits.*

(iii) f^s *is left exact.*

(iv) f_s *is right exact and commutes with direct limits.*

Therefore, given an abelian sheaf F on T, we can define the *cohomology of* $U \in \mathrm{Obj}(T)$ *with values in* F via

$$H^q(U, F) = R^q\Gamma_U(F),$$

where the right derived functor is taken on $\mathcal{S}$. If T has a final object e, one sometimes writes $H^q(T, F)$ instead of $H^q(e, F)$. More generally, there is a right dervide functor $R^q f^q : \mathcal{S}' \to \mathcal{S}$, which is called the *higher direct image sheaves*.

Even though a definition by derived functor is almost uncomputable, we can adapt an idea from classical cases to define the Čech cohomology. Consider a covering $\{U_i \to U\} \in \mathrm{Cov}(T)$. Then, as it is not necessarily a sheaf, the functor

$$H^0(\{U_i \to U\}, \cdot) : \mathcal{P} \to \mathbf{AbGrp},$$

defined as

$$H^0(\{U_i \to U\}, F) = \ker(\prod_i F(U_i) \rightrightarrows \prod_{i,j} F(U_i \times_U U_j)),$$

is not necessarily the same as $F(U)$, and is instead *left exact*. Thus, with respect to the covering $\{U_i \to U\}$, we can define the *q-th Čech cohomology group* as the q-th right derived functor $H^q(\{U_i \to U\}, \cdot) := R^q H^0(\{U_i \to U\}, \cdot)$. As usual, we call an abelian sheaf F *flasque (or flabby)* if $H^q(\{U_i \to U\}, F) = 0$ for all $q > 0$ and all coverings $\{U_i \to U\}$. By general abstract nonsense, the following are standard.

Proposition 2.2.3 [Tam, §3.5]**.** *Let* F *be a flasque abelian sheaf on a site* T*.*

(i) $H^q(U, F) = 0$ *for all* $q > 0$ *and* $U \in T$*.*

(ii) Injective abelian sheaves are flasque.

(iii) Flasque resolutions in $\mathcal{S}$ *can be used to compute* $H^q(U, \cdot)$*.*

The Čech cohomology is computable by the following sense.

Proposition 2.2.4 [Tam, I.2.2.3]. *For an abelian presheaf F on T, the group $H^q(\{U_i \to U\}, F)$ is the q-th cohomology group of the* Čech complex $\mathcal{C}^\bullet(\{U_i \to U\}, F)$*, defined as*

$$\mathcal{C}^q(\{U_i \to U\}, F) = \prod_{(i_0,\cdots,i_q)\in I^{q+1}} F(U_{i_0} \times_U \cdots \times_U U_{i_q}),$$

with the coboundary $d^q : C^q(\{U_i \to U\}, F) \to C^{q+1}(\{U_i \to U\}, F)$ defined as

$$(d^q s)_{i_0,\cdots,i_{q+1}} = \sum_{j=0}^{q+1} (-1)^j F(\mathrm{pr})(s_{i_0,\cdots,\widehat{i_j},\cdots,i_{q+1}}),$$

where $\widehat{i_j}$ means i_j is deleted and pr *is the appropriate projection.*

One can define the notion of Čech cohomology without referring to a specific covering as follows. We define $\{U'_j \to U\}_{j\in J} \in \mathrm{Cov}(T)$ is a *refinement* of $\{U_i \to U\}_{i\in I}$ if there is a map $\varepsilon : J \to I$ of index sets and a family of U-morphisms $f_j : U'_j \to U_{\varepsilon(j)}$. Then there is a natural homomorphism

$$H^0(F, f) : H^0(\{U_i \to U\}, F) \to H^0(\{U'_j \to U\}, F).$$

Taking the direct limit over the category of coverings of U, we get

$$\check{H}^q(U, F) := \varinjlim_{\{U_i\to U\}\in\mathrm{Cov}(T)} H^q(\{U_i \to U\}, F),$$

the q-th Čech cohomology group of U with values in F.

Proposition 2.2.5 [Tam, I.2.2.6]. *The functor $F \mapsto \check{H}^0(U, F)$ from $\mathcal{P}$ to* **AbGrp** *is left exact, and the right derived functors of this functor are the q-th Čech cohomology groups.*

Now one remains to compare these various right derived functors. The most fundamental theorem is *Grothendieck's Composition of Functors Spectral Sequence.*

Theorem 2.2.2 (Grothendieck's Composition of Functors Spectral Sequence, [Tam, 0.2.3.5]). *Let $\mathcal{C}, \mathcal{C}'$ be abelian categories with sufficiently many injectives, and $\mathcal{C}''$ be another abelian category. Let $F : \mathcal{C} \to \mathcal{C}'$ and $G : \mathcal{C}' \to \mathcal{C}''$ be left exact additive covariant functors. Suppose that the functor F maps injectives in $\mathcal{C}$ to G-*acyclic objects*, i.e. those with vanishing R^qG's for $q > 0$. Then, for $A \in \mathrm{Obj}\,\mathcal{C}$, there is a cohomological spectral sequence*

$$E_2^{p,q}(A) \Rightarrow E^{p+q}(A),$$

given by

$$E_2^{p,q}(A) = R^pG(R^qF(A)),$$
$$E^n(A) = R^n(G \circ F)(A).$$

We wonder if we can use this to Γ_U on $\mathcal{S}$, as $\Gamma_U = \check{H}^0(U, \cdot) \circ \iota$. We define $\mathcal{H}^q := R^q\iota$.

Proposition 2.2.6 [Tam, (I.3.4.2, I.3.4.3)]. *Let F be an abelian sheaf, and $U \in \mathrm{Obj}(T)$.*
(i) There is a canonical isomorphism $\mathcal{H}^q(F)(U) \cong H^q(U, F)$.
(ii) For $q > 0$, $\check{H}^0(U, \mathcal{H}^q(F)) = 0$.

Thus, we have the following spectral sequences.

Theorem 2.2.3 (Čech-to-Derived Spectral Sequence, [Tam, I.3.4.4]). *Let F be an abelian sheaf, $U \in \mathrm{Obj}(T)$.*

(i) For a covering $\{U_i \to U\} \in \mathrm{Cov}(T)$, there is a cohomological spectral sequence

$$E_2^{p,q} = H^p(\{U_i \to U\}, \mathcal{H}^q(F)) \Rightarrow E^{p+q} = H^{p+q}(U, F),$$

functorial in F.

(ii) There is a cohomological spectral sequence

$$E_2^{p,q} = \check{H}^p(U, \mathcal{H}^q(F)) \Rightarrow E^{p+q} = H^{p+q}(U, F),$$

functorial in F.

Theorem 2.2.4 (Leray Spectral Sequence, [Tam, I.3.7.5]). *Let $T'' \xrightarrow{g} T \xrightarrow{f} T'$ be morphisms of sites. Let F' be an abelian sheaf on T'. Then, there is a cohomological spectral sequence*

$$E_2^{p,q} = R^p g^s(R^q f^s(F')) \Rightarrow E^{p+q} = R^{p+q}(f \circ g)^s(F'),$$

functorial in F'. In particular, if g is the restriction of the site T to $U \in \mathrm{Obj}(T)$, then the spectral sequence is

$$E_2^{p,q} = H^p(U, R^q f^s(F')) \Rightarrow E^{p+q} = H^{p+q}(f(U), F'),$$

functorial in F'.

In particular, using the low-term exact sequence coming from a cohomological spectral sequence, one gets the following useful corollary.

Corollary 2.2.1 [Tam, I.3.4.7]. *For an abelian sheaf F, $\check{H}^p(U, F) \to H^p(U, F)$ is bijective for $p = 0, 1$ and injective for $p = 2$.*

We end this section by noticing how to compute cohomology by restricting sites. Firstly, given an object $U \in \mathrm{Obj}(T)$, one can think of the category T/U consisted of U-objects. It has a site, also denoted as T/U, whose coverings are coverings in T. For the natural morphism $i : T/U \to Y$ of sites, i^s is exact ([Tam, I.3.8.1]). This implies that $H^p(U, F) \cong H^p(\{U \xrightarrow{\mathrm{id}} U\}, i^s F)$, where the right cohomology is evaluated over T/U.

More generally, we have the following *Comparison Lemma.*

Theorem 2.2.5 (Comparison Lemma, [Tam, I.3.9.1]). *Let $i : T' \to T$ be a morphism of sites with the following properties.*

1. *As a functor, i is fully faithful.*
2. *A covering $\{U_i \to U\} \in \mathrm{Cov}(T)$, with U_i's and U objects coming from T', is a covering in T'.*
3. *Each object $U \in \mathrm{Obj}(T)$ has a covering $\{U_i \to U\}$ with objects U_i's coming from T'.*

Then, the functors i^s and i_s are quasi-inverse equivalences of categories between the category of abelian sheaves on T and the category of abelian sheaves on T'. In particular, one can evaluate cohomology over any of the two sites.

This in particular enables us to compare various cohomology theories over different sites.

2.2.1.2 Étale Site, Étale Sheaves and Étale Cohomology

Now that we have the whole general framework of cohomology defined over a site, we can just define what the étale site is and let the étale cohomology to be defined as *the cohomology over the étale site.*

Definition 2.2.5 (Étale Site)**.** *Let X be a scheme. Consider the category* $\mathbf{\acute{E}t}/X$ *whose objects are the étale morphisms $U \to X$ and whose morphisms are the X-morphisms between X-étale schemes (which are necessarily étale). We can define* the étale site $X_{\text{ét}}$ *on* $\mathbf{\acute{E}t}/X$ *by defining a covering to be a family $\{U_i \to U\}$ of X-morphisms whose union of images cover the whole U.*

The generalities on sites immediately provide us the inverse image and direct image functors, and more importantly the cohomology group for sheaves on the étale site, called the *étale cohomology.* A sheaf on the étale site is called *an étale sheaf.* Also, we have the notion of sheaf pullback and pushforward, coming from the generalities of sites. We will denote from now on with asterisks on superscripts and subscripts. In particular, given a morphism $f : X \to Y$,

$$f_*F(Y') = F(Y' \times_Y X),$$

for an étale sheaf F on X and an étale Y-scheme Y', whereas

$$f^*G(X') = \lim_{(Y',g)} G(Y'),$$

for an étale sheaf G on Y and an étale X-scheme X', where the limit runs over pairs (Y', g) with étale Y-scheme Y' and an Y-morphism $g : X' \to Y'$.

We first examine various examples of étale sheaves.

Example 2.2.2. Let X be a scheme.

1. **The structure sheaf**. We define the *structure sheaf* $\mathcal{O}_{X_{\text{ét}}}$ (or $\mathcal{O}_X$, if there is no confusion) to take values $\mathcal{O}_{X_{\text{ét}}}(U) = \Gamma(U, \mathcal{O}_U)$. That it is a sheaf is basically a faithfully flat descent.

2. **Representable sheaves**. Given an X-scheme, we can define a functor $\underline{Z} : \mathbf{\acute{E}t}/X \to \mathbf{Sets}$ by $\underline{Z}(U) = \mathrm{Hom}_X(U, Z)$. That this is a sheaf is also seen by faithfully flat descent. This sheaf is called to *be representable by Z*. We drop underline in the notation if there is no confusion.

   If we started with an X-group scheme, we end up with a sheaf of groups. Most commonly used representable étale sheaves are as follows.

   - The structure sheaf, which is just $\underline{\mathbb{G}_a}$.
   - $\mathcal{O}_X^\times = \underline{\mathbb{G}_m}$, where the sheaf is defined by $U \mapsto \Gamma(U, \mathcal{O}_U)^\times$.
   - $\underline{\mu_n}$, where the sheaf is defined by $U \mapsto \{x \in \Gamma(U, \mathcal{O}_U) \mid x^n = 1\}$.
   - $\underline{\mathrm{GL}_{n,X}}$, where the sheaf is defined by $U \mapsto \mathrm{GL}_n(\Gamma(U, \mathcal{O}_U))$.

3. **Constant sheaves**. Given a set (or an abelian group) F, one can define the *constant sheaf* $\underline{F}(U) = F^{\pi_0(U)}$, where $\pi_0(U)$ is the number of connected components of U. This is the sheafification of the presheaf $U \mapsto F$.

4. **Quasicoherent $\mathcal{O}_X$-modules**. Given a quasicoherent $\mathcal{O}_X$-module $\mathcal{F}$, the functor $(f : U \to X) \mapsto \Gamma(U, f^*\mathcal{F})$ defines an étale sheaf $\mathcal{F}_{\text{ét}}$. A convenient fact is that $H^i_{\text{ét}}(X, \mathcal{F}_{\text{ét}}) = H^i(X, \mathcal{F})$, where the right side is the usual sheaf cohomology. We can use the Leray

spectral sequence for the inclusion $i : X_{\mathrm{Zar}} \to X_{\text{ét}}$ of Zariski topology to étale topology gives a cohomological spectral sequence

$$E_2^{p,q} = H^p(X, R^q i^s(F)) \Rightarrow E^{p+q} = H^{p+q}_{\text{ét}}(X, F),$$

for an abelian étale sheaf F. If $F = \mathcal{F}_{\text{ét}}$ for some quasicoherent $\mathcal{O}_X$-module, then $R^q i^s \mathcal{F}_{\text{ét}} = 0$ for $q > 0$ whereas $i^s \mathcal{F}_{\text{ét}} = F$, so we get $H^i_{\text{ét}}(X, \mathcal{F}_{\text{ét}}) = H^i(X, \mathcal{F})$.

5. **Skyscraper sheaves**. Let $\overline{x}$ be a geometric point of X, and F be a set (or a group). The *skyscraper sheaf* $F^{\overline{x}}$ is defined by $F^{\overline{x}}(U) = \oplus_{\mathrm{Hom}_X(\overline{x},U)} F$. For an abelian étale sheaf $\mathcal{F}$, there is a natural isomorphism $\mathrm{Hom}(\mathcal{F}, F^{\overline{x}}) = \mathrm{Hom}(\mathcal{F}_{\overline{x}}, F)$; this will be clear when we define a stalk of an abelian étale sheaf.

We now examine the most basic case—when $X = \operatorname{Spec} k$ is the spectrum of a field k. Note that an étale k-scheme is necessarily of form $\operatorname{Spec} \prod_i k_i$, where k_i/k is a finite separable extension. Thus, $X' \to X'(k_s)$ is an equivalence of sites between $(\operatorname{Spec} k)_{\text{ét}}$ and the canonical topology on the category of sets with continuous left $\mathrm{Gal}(k_s/k)$-actions. From this equivalence of sites, one gets the following consequences on abelian sheaves.

Corollary 2.2.2 [Tam, II.2.2]. *The functor $F \mapsto \varinjlim_{k'/k \text{ finite separable}} F(\operatorname{Spec} k')$ is an equivalence of categories from the category of abelian sheaves on $(\operatorname{Spec} k)_{\text{ét}}$ and the category of continuous $\mathrm{Gal}(k_s/k)$-sets. Thus, for any abelian étale sheaf F on $\operatorname{Spec} k$,*

$$H^q_{\text{ét}}(\operatorname{Spec} k, F) \cong H^q(\mathrm{Gal}(k_s/k), \varinjlim_{k'/k \text{ finite separable}} F(\operatorname{Spec} k')),$$

where the right hand side is Galois cohomoology.

Thus, even over a point scheme, an abelian étale sheaf can be quite complex, except for example when the field is separably closed. Thus, it will be more appropriate to evaluate *stalk* of an étale sheaf at a *geometric point.*

Definition 2.2.6. *Given a geometric point $\overline{x} : \operatorname{Spec} \Omega \to X$ (so that Ω is separably closed) and an abelian étale sheaf F on X, the* stalk $F_{\overline{x}}$ of F at $\overline{x}$ *is defined by the abelian group $\overline{x}^* F(\operatorname{Spec} \Omega)$. Equivalently,*

$$F_{\overline{x}} = \varinjlim_{U} F(U),$$

where U runs over étale neighborhoods of $\overline{x}$. Alternatively, one can only evaluate the limit in the full subcategory of connected affine étale neighborhoods of $\overline{x}$, as it is initial.

The following are easy formal consequences which are not specific to étale topology, except that the stalk of the étale structure sheaf is the *strict henselization* of the stalk of the scheme structure sheaf; it is however just a re-statement of how a strict henselization is constructed.

Proposition 2.2.7 [Tam, II.5, II.6]. *Let $\overline{x} : \operatorname{Spec} \Omega \to X$ be a geometric point, and F be an abelian étale sheaf.*

(i) The functor $F \mapsto F_P$ is exact and commutes with direct limits.

(ii) If $f : X \to Y$ is a morphism of schemes, then for any abelian sheaf G on $Y_{\text{ét}}$, $(f^*G)_{\overline{x}} \cong G_{f \circ \overline{x}}$.

(iii) The stalk $\mathcal{O}_{X,\overline{x}}$ is the strict henselization of the usual scheme-stalk $\mathcal{O}_{X,x}$.

(iv) The property of being an isomorphism, a monomorphism, an epimorphism, a zero étale sheaf, an exact sequence of étale sheaves can all be checked at the level of (étale) stalks.

(v) Sheafification does not change stalks.

However, the stalks is "not compatible with pushforwards." For example, for an *open immersion* $j : U \hookrightarrow X$ and an étale sheaf F on $U_{\text{ét}}$, the stalks of j_*F need not be zero outside U. On the other hand, there is another functor $j_!$, the *extension by zero* functor, defined by the sheafification of the presheaf defined by

$$\varphi : V \to X \text{ étale} \mapsto \begin{cases} F(V) & \text{if } \varphi(V) \subset U \\ 0 & \text{otherwise.} \end{cases}$$

This functor sends a sheaf to a sheaf which indeed has a zero stalk outside U, as the sheafification does not change stalks. Also, $j_!$ is an exact functor, and is a left adjoint to j^*. Note that this construction is bound to that j is an *open immersion*; a pushforward through a closed immersion has a zero stalk outside the closed set. In particular, if we let $Z = X - U$ be the complement closed set and let $i : Z \hookrightarrow X$ denote a closed immersion, adjointness gives us a canonical map $j_!j^*F \to F$ and $F \to i_*i^*F$, and they fit into an exact sequence

$$0 \to j_!j^*F \to F \to i_*i^*F \to 0,$$

as this can be checked at stalks. More generally, data over U and Z is sufficient to characterize the original sheaf by the following.

Proposition 2.2.8 [Mil1, Proposition 8.17]**.** *Let $i : Z \to X$ be a closed immersion, and let $j : X - Z = U \to X$ be an open immersion. The functor*

$$F \mapsto (i^*F, j^*F, i^*F \to i^*j_*(j^*F))$$

is an equivalence of categories from the category of abelian sheaves over $X_{\text{ét}}$ to the category of triples (F_1, F_2, ϕ) where F_1, F_2 are abelian sheaves on $Z_{\text{ét}}, U_{\text{ét}}$, respectively, and $\phi : F_1 \to i^*j_*F_2$ is a morphism.

The existence of shriek functors is bound to the fact that the pullback f^* is not only left exact but *exact*, as $j_!$ makes a previously left adjoint j^* to be also a right adjoint of some functor. More concretely, $G_{f(x)} \xrightarrow{\sim} (f^*G)_x$ is canonically isomorphic, for $f : X \to Y$ and G an étale sheaf on Y. Finally, we remark that étale site is a *topological invariant*, so that a *pullback and pushforward by a universal homeomorphism induces equivalences of étale sites* (cf. [FK, Proposition I.3.16]).

2.2.1.3 $\mathbb{G}_a$, $\mathbb{G}_m$, μ_n and $\mathbb{Z}/n\mathbb{Z}$

We now want to compute very basic étale cohomology groups. Note that we already know $H^p(X, \mathcal{F}) \cong H^p_{\text{ét}}(X, \mathcal{F}_{\text{ét}})$, so that $H^p_{\text{ét}}(X, \mathcal{O}_X) = H^p(X, \mathcal{O}_X)$. But there is more: recall the notion of exact sequences of finite flat group schemes. The sequence of Zariski sheaves induced by the given exact sequence is not necessarily exact. For example, the sequence

$$0 \to \mu_n \to \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \to 0,$$

even though n is invertible at each point in X, need not be surjective on the right, as $\mathcal{O}_{X,x}$ simply may not have all n-th roots. However, this sequence is *exact as étale sheaves*, precisely because *stalks are strictly henselian.* Thus, we can use of long exact sequence for étale cohomology of this exact sequence. This sequence is called *the Kummer sequence.* Moreover, $H^1_{\text{ét}}(X, \mathcal{O}^\times_{X,\text{ét}})$ has a special meaning; we know by Corollary 2.2.1 that it is $\check{H}^1_{\text{ét}}(X, \mathcal{O}^\times_{X,\text{ét}})$, and, as we have seen in Section 1.3.2.1, any étale invertible sheaf descends to a Zariski invertible sheaf, so that $\check{H}^1_{\text{ét}}(X, \mathcal{O}^\times_{X,\text{ét}}) = H^1(X, \mathcal{O}^\times_X) = \text{Pic}(X)$. Thus, for example, from the long exact sequence we get

$$0 \to H^0_{\text{ét}}(X, \mathcal{O}^\times_{X,\text{ét}})/(H^0_{\text{ét}}(X, \mathcal{O}^\times_{X,\text{ét}}))^n \to H^1_{\text{ét}}(X, (\mu_n)_X) \to \text{Pic}(X)[n] \to 0.$$

Another basic exact sequence is called *the Artin-Schreier sequence*, which applies for the base scheme of characteristic $p > 0$. Note that in that case, $\mathcal{O}_{X,\text{ét}} \xrightarrow{x \mapsto x^p - x} \mathcal{O}_{X,\text{ét}}$ is also surjective (which is *not surjective* as Zariski sheaves), and the kernel is the constant sheaf $(\mathbb{Z}/p\mathbb{Z})_X$. Thus, we get the Artin-Schreier sequence

$$0 \to (\mathbb{Z}/p\mathbb{Z})_X \to \mathcal{O}_{X,\text{ét}} \xrightarrow{x \mapsto x^p - x} \mathcal{O}_{X,\text{ét}} \to 0.$$

On the other hand, for an irreducible regular scheme X, there is the *Weil divisor exact sequence* ([Mil1, Proposition 13.4])

$$0 \to \mathbb{G}_m \to g_*\mathbb{G}_{m,K} \to \bigoplus_{\text{codim}(z)=1} i_{z*}\mathbb{Z} \to 0,$$

where $g : \eta \to X$ is the inclusion of the generic point, K is the function field, and $i_z : z \to X$ is the inclusion of the point. This really is just a divisor exact sequence in the usual scheme theory. This exact sequence can be used to prove the cohomology of μ_n over curves.

Theorem 2.2.6 (cf. [Mil1, §14], [FK, I.5.1])**.** *Let X be a connected, smooth, projective curve over an algebraically closed field k. Then, if n is not divisible by the characteristic of k,*

$$H^i_{\text{ét}}(X, \mu_n) = \begin{cases} \mu_n(k) & i = 0 \\ \text{Pic}(X)[n] & i = 1 \\ \mathbb{Z}/n\mathbb{Z} & i = 2 \\ 0 & i \geq 3 \end{cases}$$

If $\operatorname{char} k = p > 0$*, then*

$$H^i_{\text{ét}}(X, \mathbb{Z}/p\mathbb{Z}) = \begin{cases} \mathbb{Z}/p\mathbb{Z} & i = 0 \\ \textit{a finite abelian group} & i = 1 \\ 0 & i \geq 2 \end{cases}$$

2.2.1.4 Finiteness Conditions on Sheaves

We start with noticing how finite morphisms behave very nicely with étale cohomology. Let $f : X \to Y$ be a finite morphism, then, first of all, *all the higher direct images $R^q f_*$ vanish* [FK, I.3.4]. Thus, for arbitary morphism $g : Z \to Y$, the natural *base change morphism* $g^*(R^q f_* G) \to R^v f'_*(g'^* G)$ is canonically isomorphic, where f', g' are pullbacks of f, g by g, f, respectively. This is a special case of the Proper Base Change Theorem, but nevertheless philosophically this case should be the prime case.

Another reason why finiteness works well with étale cohomology can be seen in the *Representability Lemma.*

Theorem 2.2.7 (Representability Lemma, [FK, I.3.15])**.** *An étale sheaf F of sets on a scheme X is representable if and only if the following conditions are satisfied.*

1. *The stalks of F are finite sets.*
2. *For each étale scheme $U \to X$ over X and every two sections $\alpha, \beta \in F(U)$, the set of poitns $x_0 \in U$ for which germs $\alpha_{x_0}, \beta_{x_0}$ are different is an open set.*

This Lemma can be seen in the following context. Note that any étale sheaf F on X has a surjection $\amalg \underline{X_\alpha} \to F$ from disjoint union of representable sheaves, e.g. you can just take the collection of stalks. The finiteness conditions are laying finiteness condition on this family so that F can actually be thought as being "represented by a quotient space." In this regard, we can develop a very important notion of *contructible sheaves.*

Definition 2.2.7 (Locally Constant Sheaves, Constructible Sheaves). *An étale sheaf F on a noetherian scheme X is* locally constant *if there is an étale cover $\{U_i \to X\}$ such that $F|_{U_i}$ is constant. If in addition each $F|_{U_i}$ is represented by a finite set, we say F is* locally constant constructible *(or,* finite locally constant *as in [FK]). Finally, F is* constructible *if X admits a* finite stratification *over which F is locally constant constructible. Here, a* finite stratification *is a finite set $\{X_i\}$ of pairwise-disjoint non-empty locally closed subschemes of X.*

This definition of constructibility is to ensure that F is a quotient of a finite disjoint union of representable sheaves. Thus, F is always at least represented by an *algebraic space*, which we have had a glimpse on in Section 1.2.3.2. Note also that we need noetherianness for X to apply noetherian induction. This is not a restriction, as all the scheme we will be interested in will be noetherian.

We list basic properties of constructible sheaves. Let X be a noetherian scheme, and F be an étale sheaf over X.

- *Locally constant constructible sheaves are representable.* This is just a faithfully flat descent. In particular, the category of locally constructible sheaves over X is equivalent to the category of finite étale X-schemes via $Y \mapsto \underline{Y}$.
- A sheaf represented by an étale scheme is constructible.
- A sheaf is constructible if and only if, for every nonempty closed irreducible subscheme $Y \subset X$, there is an étale scheme V over Y such that $F|_V$ is constructible [FK, I.4.3"].
- *Constructibility is étale-local.* More precisely, if there is an étale cover $\{U_i\}$ such that $F|_{U_i}$ is constructible for all i, then F is constructible [C, Theorem 1.1.7.5].
- If F is constructible, then given a family of sheaves $\{F_i \to F\}$ whose union $\amalg_i F_i \to F$ is surjective, there is a finite subfamily $F_{i_1}, \cdots, F_{i_n}$ such that $\amalg_{j=1}^n F_{i_j} \to F$ is surjective [FK, I.4.5].
- F is constructible if and only if there is an étale scheme Y over X such that F has a surjection from $\underline{Y}$, i.e. there exists a surjective map $\underline{Y} \to X$. From this condition, it is immediate that *a subsheaf of a constructible sheaf is constructible.* By Representability Lemma, Theorem 2.2.7, we can deduce that *a subsheaf of a representable sheaf is representable.*
- Constructibility is preserved by many functors, for example pullback, image, finite limit. This can be easily seen by noetherian induction: by noetherian induction, we can reduce to the case when the given étale sheaf F is locally constant constructible, and locality of constructibility reduces the problem to the case when F is finite constant. On the other hand, it is not in general true that a pushforward of a constructible sheaf is constructible, unless there is another finiteness condition on the morphism we are pushing forward. In contrast, extension of a constructible sheaf by zero is constructible [C, Example 1.1.7.8].

Note that stalks of constructible sheaves are finite groups, so they are torsion groups. We will call a sheaf with torsion stalk groups *a torsion sheaf.* The relation between the category of constructible sheaves and the category of torsion sheaves is this.

Theorem 2.2.8 [FK, I.4.8-9]. *The category of constructible sheaves is an abelian subcategory of the category of torsion sheaves. Conversely, the category of torsion sheaves is generated by the category of constructible sheaves via filtered direct limit. In other words, every torsion sheaf is the filtered direct limit of its constructible subsheaves.*

An abelian étale torsion sheaf satisfies the ascending chain condition, then it is constructible.

In particular, if F is a constructible sheaf killed by $n \neq 0$, then F is a subsheaf of a direct sum of $\underline{\mathbb{Z}/n\mathbb{Z}}$!

2.2.1.5 Base Change Theorems

Recall that we have a natural *base change homomorphism* for a cartesian diagram. Namely, given a cartesian square

$$\begin{array}{ccc} X_T & \xrightarrow{f'} & T \\ {\scriptstyle g'}\big\downarrow & & \big\downarrow{\scriptstyle g} \\ X & \xrightarrow{f} & S \end{array}$$

using adjunction, there is a natural map

$$g^*(R^i f_* F) \to R^i f'_*(g'^* F),$$

for every abelian étale sheaf F on X. We call this map *the base change homomorphism.* This morphism, even though not isomorphic in all cases, is indeed isomorphic for certain important cases. One is the *Proper Base Change Theorem*; we fix the above notation throughout this section.

Theorem 2.2.9 (Proper Base Change Theorem, [FK, I.6.1])**.** *If $f : X \to S$ is proper and F is a torsion sheaf on X, then the base change homomorphism is an isomorphism.*

It is done via various reduction techniques. As cohomology and filtered direct limit of sheaves commute [C, Theorem 1.3.2.1], we can assume F is constructible $\mathbb{Z}/n\mathbb{Z}$-module for some integer $n > 1$. By Noetherian induction [C, Theorem 1.3.2.2], since an isomorphism can be checked stalkwise, we can reduce the problem to the case when $S = \operatorname{Spec} R$ is the spectrum of a strictly henselian local noetherian ring R and $g : S' \to S$ is the inclusion of the closed point. Using Chow's lemma, one can also assume that f is projective. Embedding X into $\mathbb{P}^n_S$ and subsequently covering it by $\mathbb{P}^1_S \times \cdots \times \mathbb{P}^1_S$, it is sufficient to prove when $X = \mathbb{P}^1_S$. Then one is reduced to the problem of cohomology of curves. The detailed proof can be found in [C, 1.3.4] and [FK, I.6.1].

The Proper Base Change Theorem has some immediate corollaries as follows.

Corollary 2.2.3. *Let $f : X \to Y$ be a proper morphism, and F be an abelian torsion sheaf on X.*

(i) For every geometric point $\overline{y} \in Y$, $(R^q f_*(F))_{\overline{y}} \cong H^q(X_{\overline{y}}, F_{\overline{y}})$ for $q \geq 0$.

(ii) If f is of relative dimension $\leq n$, $R^q f_* F = 0$ for $q > 2n$.

(iii) If X is a proper k-scheme and k'/k is an extension of separably closed fields, then $H^q(X, F) \cong H^q(X_{k'}, F_{k'})$ for all $q \geq 0$.

Another instance where the base change homomorphism is an isomorphism is when base-changing through a *smooth morphism.*

Theorem 2.2.10 (Smooth Base Change Theorem, [C, Theorem 1.3.5.2], [FK, I.7.3])**.** *If $g : T \to S$ is an inverse limit of smooth S-schemes*[1] *with affine transition maps, and if the torsion orders of sections of F are invertible on S, then the base change homomorphism is an isomorphism.*

[1] The requirement that T is an *inverse limit of smooth S-schemes* is convenient in considering non-finite type base change. For example, we can see that étale cohomology of a torsion sheaf of invertible order stays the same through a *purely transcendental* field extension.

This is proven by again using various reduction techniques; the details are in [FK, I.7] and [C, 1.3.5]. In particular, this is equivalent to the *Acyclicity Theorem.*

Theorem 2.2.11 (Acyclicity Theorem, [FK, I.7.4])**.** *Let $g : \operatorname{Spec} B \to \operatorname{Spec} A$ be a smooth homomorphism of strictly henselian rings. Then, for any torsion sheaf F on $\operatorname{Spec} A$ of invertible order, $F \to g_* g^* F$ is an isomorphism, and $R^i g_*(g^*F) = 0$ for $i > 0$.*

2.2.1.6 Cohomology with Proper Support and Finiteness Theorems

We will eventually reach theorems inspired from algebraic topology, for example Poincaré duality. Thus, it is viable to expect that we will at some point need the notion of *cohomology with compact support*. Its existence was somehow forseen in the case of extension-by-zero functor. We can generalize this functor to a wider class of morphisms.

Definition 2.2.8 (Higher Direct Images with Proper Support, [C, Definition 1.3.6.1])**.** *Let $f : X \to S$ be a separated finite type morphism with S quasicompact quasiseparated. By Nagata compactification theorem, there exists an open immersion $j : X \to \overline{X}$ to a proper S-scheme $\overline{f} : \overline{X} \to S$. The* higher direct images with proper support for torsion sheaves *are $R^q f_! := (R^q \overline{f}_*) \circ j_!$.*

In this setting, the cohomology with proper support *is defined as*

$$H^q_{c,\text{ét}}(X, F) := H^q_{\text{ét}}(\overline{X}, j_! F).$$

We list some basic properties. Let $f : X \to S$ be separated finite type with S quasicompact quasiseparated.

- Indeed, the definition $R^q f_!$ is well-defined, so that it does not depend on the choice of compactification. In particular, $f_! = f_*$ if f is already proper.
- The functor $f_!$ is left adjoint to f^*.
- The formation of the functor $R^q f_!$ is compatible with base change [FK, I.8.7(1)].
- If $h = g \circ f$, then in the derived category $\mathrm{R}\, h_! \cong \mathrm{R}\, g_! \circ \mathrm{R}\, f_!$. More concretely, this means that we can apply Grothendieck's Composition of Functors Spectral Sequence, Theorem 2.2.2, so that there is a cohomological spectral sequence

  $$E_2^{p,q} = R^p g_!(R^q f_!(F)) \Rightarrow E^{p+q} = R^{p+q} h_!(F),$$

  for any torsion sheaf F [FK, I.8.7(2)].
- We knew that $j_!$ is exact for an open embedding j. This means that $R^q j_! = 0$ for $q > 0$.
- **Excision**. If $Z \hookrightarrow X$ is a closed subscheme with open complement U, then there is a long exact *excision sequence*

  $$\cdots \to R^i(f|_U)_!(F|_U) \to R^i f_! F \to R^i(f|_Z)_!(F|_Z) \to \cdots$$

  for torsion sheaves F on X [FK, I.8.7(3)].

The cohomology with proper support is somehow the "right object" to satisfy finiteness; the finiteness of (ordinary) étale cohomology is a consequence of finiteness of cohomology with proper support. We record various finiteness theorems with references, since the proofs are technical and long-winding as others are.

Theorem 2.2.12 [C, Theorem 1.3.6.3]**.** *Let $f : X \to S$ be a finite type separated map to a scheme S, and let F be a torsion abelian sheaf on $X_{\text{ét}}$. Then $R^i f_!(F)$ vanishes for $i > 2\sup_{s\in S} \dim X_s$. If S is noetherian and F is constructible, $R^i f_!(F)$ is constructible as well. In particular, if $S = \operatorname{Spec} k$ for a separably closed field k, $H^i_{c,\text{ét}}(X, F)$ is a finite group and it vanishes for $i > 2\dim X$.*

Theorem 2.2.13 [C, Theorem 1.3.6.4]**.** *Let $f : X \to S$ be a finite type separated map between schemes of finite type over a regular base of dimension ≤ 1 (e.g. the spectrum of a field or a Dedekind domain). Let F be a constructible abelian sheaf on X whose torsion-orders are invertible on S. Then, the sheaves $R^i f_* F$ are constructible, and they vanish for $i > \dim S + 2\dim X$.*

Theorem 2.2.14 [C, Theorem 1.3.7.1]**.** *Let $f : X \to S$ be smooth and proper. Let F be a locally constant constructible abelian sheaf on X, whose torsion-orders are invertible on S. Then, $R^i f_* F$ is locally constant constructible on S and its formation commutes with arbitrary base change.*

2.2.1.7 Künneth Formula, Poincaré Duality

As promised, we have Künneth formula and Poincaré duality for étale cohomology. In this section, we briefly explain how to construct the natural map for those formulas and state theorems on when those maps are isomorphic (or fit inside a short exact sequence).

We first start with Künneth formula. The setting is as follows. Fix a commutative ring Λ that is killed by a nonzero integer. Let $f : X \to S$, $f' : X' \to S$ be separated finite type maps. Given étale sheaves of Λ-modules F, F' on X, X', respectively, we would likt to relate the cohomology of $\pi^* F \otimes_\Lambda \pi'^* F'$ where $\pi : X \times_S X' \to X$, $\pi' : X \times_S X' \to X'$ are projections. We cannot define pullback along π or π' as they might not be proper.

First, assume that S is quasicompact and quasiseparated. We can then choose $j : X \hookrightarrow \overline{X}$ and $j' : X' \hookrightarrow \overline{X'}$ into proper S-schemes $\overline{f} : \overline{X} \to S$, $\overline{f'} : \overline{X'} \to S$. Then, $\overline{X} \times_S \overline{X'}$ is also a compactification of $X \times_S X'$. Along the projections of this product we can pullback, which gives us a map

$$\begin{array}{ccc} R^p\overline{f}_*(j_!F) \otimes_\Lambda R^q\overline{f'}_*(j'_!F') & \longrightarrow & R^{p+q}(\overline{f} \times \overline{f'})_*(\overline{\pi}^*(j_!F) \otimes_\Lambda \overline{\pi'}^*(j'_!F')) \\ \| & & \| \\ R^p f_!(F) \otimes_\Lambda R^q f'_!(F') & & R^{p+q}(\overline{f} \times \overline{f}')_*(j \times j')_!(\pi^*F \otimes_\Lambda \pi'^*F') \\ & \searrow & \| \\ & & R^{p+q}(f \times f')_!(\pi^*F \otimes_\Lambda \pi'^*F'). \end{array}$$

This map is independent of compactification, so this construction globalizes to give the *Künneth morphism*

$$\bigoplus_{p+q=n} R^p f_!(F) \otimes_\Lambda R^q f'_!(F') \to R^n(f \times f')_!(\pi^*F \otimes_\Lambda \pi'^*F').$$

As there is an extra torsion term in the Künneth formula from algebraic topology, we also need torsion terms to correctly characterize $R^{r+s}(f \times f')_!(\pi^*F \otimes_\Lambda \pi'^*F')$. This is because what we really get is an isomorphism of complexes in the derived category. For example, if F or F' has Λ-flat stalks, then the Künneth morphism is the edge map of a cohomological spectral sequence

$$\bigoplus_{a+a'=s} \operatorname{Tor}^r_{\underline{\Lambda}}(R^a f_! F, R^{a'} f'_! F') \Rightarrow R^{r+s}(f \times f')_!(\pi^*F \otimes_\Lambda \pi'^*F'),$$

where the Tor is evaluated in the category of étale sheaves [C, Theorem 1.3.9.2]. From this, we know that the Künneth morphism is an isomorphism when, for example, either F or F' has flat direct images with proper support.

For the Poincaré duality, one starts with a globalized *trace map.* For a $\mathbb{Z}[1/n]$-scheme S and any smooth separated finite type map $f : Y \to S$ with pure relative dimension d, there is a unique theory of trace map $\mathrm{tr}_f : R^{2d} f_!(\mu_n^{\otimes d}) \to \mathbb{Z}/n\mathbb{Z}$ satisfying axioms, including compatibility with base change, reduction modulo a divisor of n, transitivity in f (via spectral sequence) and match with originally existing trace maps in low dimensions [C, 1.3.8.5]. Then, the Poincaré duality is really about the existence of cup product pairing. For any $\mathbb{Z}/\ell^n\mathbb{Z}$-sheaf G, we define $G(d) := G \otimes_{\mathbb{Z}/\ell^n\mathbb{Z}} \mu_{\ell^n}^{\otimes d}$.

Theorem 2.2.15 (Poincaré duality, [C, Theorem 1.3.8.1])**.** *Let ℓ be a prime, and $f : X \to S$ be a smooth separated map between noetherian $\mathbb{Z}[1/\ell]$-schemes. Let $(\Lambda, \mathfrak{m})$ be a complete discrete valuation ring with finite residue field of characterristic ℓ and fraction field of charcateristic zero. Let F, G be constructible sheaves on X of $\Lambda/\mathfrak{m}^{n+1}$-modules on X and S, respectively. Then, there is a canonical isomorphism*

$$\mathrm{Ext}^i_X(F, f^*G(d)) \cong \mathrm{Hom}_S(R^{2d-i} f_!(F), G),$$

that is compatible with base change and étale localization on X.

When $S = \mathrm{Spec}\, k$ is a geometric point and F is locally constant constructible with $\Lambda/\mathfrak{m}^{n+1}$-flat stalks, then the isomorphism in the special case $G = \Lambda/\mathfrak{m}^{n+1}$ is induced by the perfect cup product pairing

$$H^i_{\text{ét}}(X, F^\vee(d)) \otimes H^{2d-i}_{c,\text{ét}}(X, F) \to H^{2d}_{c,\text{ét}}(X, (\Lambda/\mathfrak{m}^{n+1})(d)) \xrightarrow{\mathrm{tr}} \Lambda/\mathfrak{m}^{n+1}.$$

2.2.1.8 ℓ-adic Cohomology

Even though the étale cohomology of a non-torsion sheaf is not saying much, we can instead exploit the fact that *projective limit does not commute with étale cohomology.* Let ℓ be a prime.

Definition 2.2.9 (ℓ-adic Sheaves)**.** *A projective system $(F_n)_{n\in\mathbb{N}}$ of constructible sheaves on a scheme X is called an* ℓ-adic sheaf *if $\ell^{n+1}F_n = 0$ for all $n \geq 0$ and*

$$F_{n+1} \otimes_{\mathbb{Z}/\ell^{n+2}\mathbb{Z}} \mathbb{Z}/\ell^{n+1}\mathbb{Z} \xrightarrow{\sim} F_n.$$

An ℓ-adic sheaf $F = (F_n)$ is locally constant *(*constructible*, respectively) if all F_n's are locally constant (constructible, respectively).*

Example 2.2.3.

1. If a constructible sheaf F is killed by ℓ^m, then $F_n = F/\ell^{n+1}F$ for $n \geq 0$ forms an ℓ-adic sheaf. In particular, the category of constructible ℓ-power torsion sheaves embeds as a full subcategory inside the category of ℓ-adic sheaves.
2. Given a finitely generated $\mathbb{Z}/\ell\mathbb{Z}$-module M, $M_X = ((M/\ell^{n+1}M)_X)$ is an ℓ-adic sheaf.
3. The constant sheaf $\mathbb{Z}_\ell = ((\underline{\mathbb{Z}/\ell^{n+1}\mathbb{Z}})_X)$ is an ℓ-adic sheaf.
4. The *Tate twist* $\mathbb{Z}_\ell(1) = (\mu_{\ell^{n+1},X})$ is an ℓ-adic sheaf. Thus, $\mathbb{Z}_\ell(m)$ for any $m \in \mathbb{Z}$ is an ℓ-adic sheaf.

Given an ℓ-adic sheaf, we define the ℓ-adic cohomology to be the projective limit of étale cohomologies of component torsion sheaves.

Definition 2.2.10 (ℓ-adic Cohomology). *For $F = (F_n)$ an ℓ-adic sheaf on X, we define the ℓ-adic cohomology (with proper support)*

$$H^r_{\text{ét}}(X, F) = \varprojlim_n H^r_{\text{ét}}(X, F_n), H^r_{\text{ét},c}(X, F) = \varprojlim_n H^r_{\text{ét},c}(X, F_n).$$

To show that this is a well-behaving concept, one puts this concept inside the *Artin-Rees category of $\mathbb{Z}/\ell\mathbb{Z}$-sheaves*, which is a better category to study algebraically. In the end, the ℓ-adic sheaves behave like how we expect.

Theorem 2.2.16 [Mil2, Lemma V.1.11]. *Let $F = (F_n)$ be an ℓ-adic sheaf on $X_{\text{ét}}$ such that F_n is flat as a sheaf of $\mathbb{Z}/\ell^n\mathbb{Z}$-modules, and $H^r_{\text{ét}}(X, F_n)$ is finite for all r and n. Then, $H^r(X, F)$ is finitely generated as a $\mathbb{Z}_\ell$-module, and there are exact sequences*

$$0 \to H^r_{\text{ét}}(X, F)/\ell^n H^r_{\text{ét}}(X, F) \to H^r_{\text{ét}}(X, F_n) \to H^{r+1}(X_{\text{ét}}, F)[\ell^n] \to 0.$$

One can define the *rational ℓ-adic cohomology* by inverting ℓ's in the cohomology group, and get similar results.

2.2.1.9 Weil Conjectures and the Hard Lefschetz Theorem

The Weil conjectures are about number of points of a nonsingular variety over a finite field. Suppose X is a nonsingular projective (or proper) variety of dimension n over $\mathbb{F}_q$. For each m, let N_m be the number of points in $X(\mathbb{F}_{q^m})$. We define the *zeta function* of X to be

$$Z(X, t) = \exp\left(\sum_{m \geq 1} N_m \frac{t^m}{m}\right).$$

The Weil conjectures are the four assertions about $Z(X, t)$.

1. **Rationality**. $Z(X, t)$ is a rational function of t, so that it can be written as a finite alternating product of polynomials

$$Z(X, t) = \frac{P_1(t) \cdots P_{2n-1}(t)}{P_0(t) \cdots P_{2n}(t)},$$

where each $P_i(t)$ is an integral polynomial. Furthermore, $P_0(t) = 1 - t$, $P_{2n}(t) = 1 - q^n t$, and $P_i(t) = \prod_j (1 - \alpha_{i,j} t)$ for some numbers $\alpha_{i,j} \in \mathbb{C}$.

2. **Functional Equation**. $Z(X, t)$ satisfies

$$Z(X, \frac{1}{q^n t}) = \pm q^{n\chi/2} t^\chi Z(X, t),$$

where χ is the Euler characteristic of X.

3. **Riemann Hypothesis**. For all $1 \leq i \leq 2n - 1$ and all j, $|\alpha_{i,j}| = q^{i/2}$.

4. **Betti Numbers**. If X is a reduction of a nonsingular projective variety Y over a number field, then the degree of P_i is the i-th Betti number of Y.

Its first full proof was done by Deligne by using Lefschetz pencils. We will only record some remarks and consequences regarding the conjecture and its proof.

Let ℓ be a prime different from the characteristic of $\mathbb{F}_q$. Note first that the Frobenius φ of $\mathbb{F}_q$ acts on $X_{\overline{\mathbb{F}_q}}$, and in turn acts on the ℓ-adic cohomology $H^m_{\text{ét}}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell) = H^m_{\text{ét}}(X_{\overline{\mathbb{F}_q}}, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. By the Finiteness Theorems, the ℓ-adic cohomology groups are finite-dimensional. The Lefschetz Fixed Point Formula then implies that

$$N_m = \sum_r (-1)^r \operatorname{Tr}(\varphi^m \mid_{H^r_{\text{ét}}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)}).$$

Noticing this, we record what Deligne proved.

Theorem 2.2.17 (Deligne, [FK, IV.1.2])**.** *Let X be a smooth projective variety over a finite field κ with $q = p^m$ elements. Let $\ell \neq p$.*

(1) The polynomials

$$P_i(t) = \det(1 - t\varphi|_{H^i_{\text{ét}}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)})$$

in $\mathbb{Q}_\ell[t]$ have rational integer coefficients independent of ℓ.

(2) All eigenvalues λ of $\varphi|_{H^i_{\text{ét}}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)}$ have the complex absolute value $|\lambda| = q^{i/2}$.

(3) We have $Z(X,t) = \prod_i P_i(t)^{(-1)^{i+1}}$, and the functional equation

$$Z(X, 1/q^n t) = \varepsilon q^{\frac{1}{2}n\chi(X)} t^{\chi(X)} Z_X(t),$$

where $n = \dim_{\mathbb{F}_q} X$, $\chi(X) = \sum_i (-1)^i \dim_{\mathbb{Q}_\ell} H^i(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)$, and $\varepsilon = (-1)^N$ where N is the multiplicity of the eigenvalue $q^{\lfloor n/2 \rfloor}$ of $\varphi|_{H^n(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)}$.

An immediate consequence is this.

Proposition 2.2.9. *Let X be a smooth, projective variety over $\mathbb{F}_q$ of pure dimension d, and let $N_n = \#X(\mathbb{F}_{q^n})$. Then, $N_n = 1 + q^{nd} + r_n$ where $|r_n| \leq \sum_{0<i<2d} q^{ni/2} \dim_{\mathbb{Q}_\ell} H^i_{\text{ét}}(X_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)$. In particular, if X is an abelian variety, then $N_n \leq (1 + \sqrt{q})^{2n}$.*

Along with the Riemann Hypothesis (that eigenvalues are of modulus $q^{i/2}$), the following *Hard Lefschetz Theorem*, which was proved also by Deligne in his generalization of Weil Conjectures, is frequently used.

Theorem 2.2.18 (Hard Lefschetz Theorem, [FK, IV.5.5])**.** *Let X be a smooth irreducible projective scheme over an algebraically closed field K, and let $\ell \neq \operatorname{char} K$. Then, there is a cohomology class $\eta \in H^2(X, \mathbb{Q}_\ell(1))$ such that, for $0 < i \leq n = \dim X$,*

$$\eta^i : H^{n-i}(X, \mathbb{Q}_\ell) \xrightarrow{a \mapsto \eta^i \cup a} H^{n+i}(X, \mathbb{Q}_\ell(i))$$

is an isomorphism.

2.2.2 p-adic Hodge Theory

2.2.2.1 Ax-Sen-Tate Theorem and Galois Cohomology of $\mathbb{C}_p$

The p-adic Hodge theory is about classifying p-adic Galois representations of p-adic local fields. Recall that a ground of mental composure in algebraic geometry came from the world over algebraically closed fields; over an algebraically closed field, everything is as expected in the classical algebraic geometry, and one can work with closed points, etc. A similar ground in the theory of p-adic Galois representations is the field $\mathbb{C}_p$, which is defined as the p-adic completion of the algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$. It is complete with respect to p-adic topology as well as algebraically closed by standard approximation argument.

Let K be a *p-adic field*, i.e. a field of characteristic 0, complete with respect to a discrete valuation having a perfect residue field of characteristic $p > 0$. Note that $\mathbb{C}_K := \widehat{\overline{K}}$ is also isomorphic to $\mathbb{C}_p$. As the Galois action G_K on $\overline{K}$ is continuous, G_K also continuously acts on $\mathbb{C}_K$. What Tate observed in his article [Tat2] is that the p-adic étale cohomology of a p-divisible group (especially an abelian variety) over a p-adic field K becomes very nice when *the p-adic representation is base-changed to* $\mathbb{C}_K$. More precisely, the Galois representation coming from the étale cohomology is *Hodge-Tate*. It turns out that, among abundance of badly behaving p-adic representations of $G_K = \mathrm{Gal}(\overline{K}/K)$, Hodge-Tate representations are all what we "really care"; in particular, *p-adic Galois representations coming from geometric objects are Hodge-Tate.* We will see that Hodge-Tate representations over $\mathbb{C}_K$ are split as a sum of $\mathbb{C}_K[G_K]$-modules one-dimensional over $\mathbb{C}_K$, known as *Tate twists.* Thus, among all others, it is crucial to first understand the Galois cohomology of $\mathbb{C}_K$ and its Tate twists.

We now explain what the Tate twists are. Recall that for any representation of a group can be "twisted by a character." To be more precise, given a topological group G and a topological ring R with a continuous G-action, an R-representation of G is a finite free R-module M with a G-semilinear action, i.e. an action of $g \in G$ on M is $g(\alpha m) = g(\alpha)g(m)$ for $\alpha \in R, m \in M$. Then, given a continuous homomorphism $\eta : G \to R^\times$ (a "character"), $M(\eta)$ is another R-representation of G with the same underlying module with G-action defined by $g(\alpha m) = g(\alpha)\eta(g)m$ for $g \in G, \alpha \in R, m \in M$. In particular, for a $\mathbb{Z}_p$-representation of G_K, we have a very well-known character, *the cyclotomic character* $\chi : G_K \to \mathbb{Z}_p^\times$, defined by $g(\zeta_{p^n}) = \zeta_{p^n}^{\chi(g)}$ for arbitrary $n \geq 0$. Given a $\mathbb{Z}_p$-representation V of G_K, the *m-th Tate twist* $V(m)$ is just $V(\chi^m)$.

We would like to understand the Galois cohomology $H^0(G_K, \mathbb{C}_K(n))$ and $H^1(G_K, \mathbb{C}_K(n))$. The main method is to approximate $\mathbb{C}_K$ via $\overline{K}$. The first result in this kind is the *Ax-Sen-Tate Theorem.*

Theorem 2.2.19 (Ax-Sen-Tate Theorem, [BC, Proposition 2.1.2])**.** *Let L/K be an algebraic extension. Then, $\mathbb{C}_K^{G_L} = \widehat{L}$. In particular, if L/K is finite, $\mathbb{C}_K^{G_L} = L$.*

Proof. Given $x \in \mathbb{C}_K^{G_L} \subset \mathbb{C}_K$, we choose a sequence $\alpha_n \in \overline{K}$ to approximate x. Using Krasner's lemma, one can find $\beta_n \in L$ such that $v(\alpha_n - \beta_n) \geq \min_{g \in G_K} v(g(\alpha_n) - \alpha_n) - \frac{v(p)}{(p-1)^2}$, where v is a p-adic valuation. Then $v(x - \beta_n)$ goes to infinity as n goes to infinity. □

To compute the Galois cohomology $H^i(G_K, \mathbb{C}_K(n))$, one exploits an intermediate field $K(\zeta_{p^\infty})$, which we denote[2] as K_∞, as $\ker \chi = G_{K_\infty}$. Denote $K_n = K(\zeta_{p^n})$, $H_K = G_{K_\infty}$ and $\Gamma_K = \mathrm{Gal}(K_\infty/K)$. Then, after n gets large enough, say $n \geq n_K$, the ramification behavior of $\mathrm{Gal}(K_n/F_n)$ becomes the same as $\mathrm{Gal}(K_\infty/F_\infty)$. For $n \geq n_K$, we can then define the normalized trace $\mathrm{pr} : K_\infty \to K$ by $\mathrm{pr}(x) = \frac{1}{p^n}\mathrm{Tr}_{K_n/K}(x)$ for n satisfying $x \in K_n$; this is independent of n. The normalized trace map is a continuous map from K_∞ to K, and does not deviate too much from the identity map, so that $\alpha = \lim_{n\to\infty} \mathrm{pr}_n(\alpha)$ (cf. [BC, Lemma 14.1.4]). Extending this map to $\widehat{K_\infty}$, we have a decomposition $L \cong K \oplus \ker \mathrm{pr}$. Using this decomposition, one computes that, for $i = 0, 1$,

$$H^i(\Gamma_K, \widehat{K_\infty}(n)) = \begin{cases} K & \text{if } n = 0 \\ 0 & \text{otherwise} \end{cases}$$

(cf. [BC, Lemma 14.1.19]) A similar approximation argument shows that $H^i(H, \mathbb{C}_K(n)) = 0$ for $i \geq 1$ and any n (cf. [BC, Proposition 14.3.2]). Using the Ax-Sen-Tate for $i = 0$ and the inflation-restriction sequence for higher degrees, we can finally get the Galois cohomology of $\mathbb{C}_K(n)$ by G_K.

[2]This might be a confusing notation, but we do it only in this section for notational convenience.

Proposition 2.2.10. *For $i = 0, 1$,*

$$H^i(G_K, \mathbb{C}_K(n)) = \begin{cases} K & \text{if } n = 0 \\ 0 & \text{otherwise} \end{cases}$$

It turns out that all $\mathbb{C}_K$-representations of G_K come from K_∞. Thus, the above strategy of analyzing problems over K_∞ is actually a natural first thing to do. This is called the *Sen theory.*

Theorem 2.2.20 [BC, Theorem 15.1.2]**.** *Given $V \in \mathrm{Rep}_{\mathbb{C}_K}(G_K)$ a $\mathbb{C}_K$-representation of G_K, there uniquely exists a Γ_K-stable K_∞-submodule $\mathbf{D}_{\mathrm{Sen}}(V)$ of V such that $\widehat{K_\infty} \otimes_{K_\infty} \mathbf{D}_{\mathrm{Sen}}(V) \cong V^{H_K}$.*

2.2.2.2 Hodge-Tate Representations

A $\mathbb{C}_p$-representation $V \in \mathrm{Rep}_{\mathbb{C}_p}(G_K)$ of the absolute Galois group of a p-adic field K is *Hodge-Tate* if it splits as a sum of Tate twists $\mathbb{C}_p(m)$. It is a perfectly good definition, but we would like to have a more canonical way of checking if a representation if Hodge-Tate, since choosing a basis of $\mathbb{C}_p(1) \cong \mathbb{C}_p$ and describing an action of the cyclotomic character χ involves with a choice of compatible system $(\zeta_{p^n})_{n\geq 1}$ of p-power roots of unity.

Note that the χ^n-eigenspace of V can be identified more canonically via $V\{q\} := V(q)^{G_K}$; this is canonically a K-subspace of $V(q)$, but not canonically in V. Upon choosing a basis, this is isomorphic as a K-vector space to $\{v \in V \mid g(v) = \chi(g)^{-q}v \text{ for all } v \in G_K\}$. We then have a natural G_K-equivariant K-linear map

$$K(-q) \otimes_K V\{q\} \hookrightarrow K(-q) \otimes_K V(q) \cong V,$$

where the last isomorphism is canonical. Extending scalars and adding all twists together, we have the following natural map

$$\xi_V : \bigoplus_q (\mathbb{C}_K(-q) \otimes_K V\{q\}) \to V.$$

Lemma 2.2.1. *The map ξ_V is injective. In particular, $V\{q\} = 0$ for all but finitely many q, and $\dim_K V\{q\} < \infty$ for all q, with $\sum_q \dim_K V\{q\} \leq \dim_{\mathbb{C}_K} V$. The equality holds if and only if ξ_V is an isomorphism.*

We will see that this statement is a formal consequence of the formalism of admissible representation; the proof therefore can be found therein. Regarding this lemma, we can now define a representation $V \in \mathrm{Rep}_{\mathbb{C}_K}(G_K)$ to be *Hodge-Tate* if the comparison map ξ_V is an isomorphism. We define the *Hodge-Tate weights* of a Hodge-Tate representation V to be *the integers n such that $V\{n\} \neq 0$.*

Remark 2.2.1. Note that this convention makes $\mathbb{C}_K(1)$, the cyclotomic character, to have the Hodge-Tate weight -1, not 1. There is another convention with all the signs flipped, making $\mathbb{C}_K(1)$ to have the Hodge-Tate weight 1; this is preferred in the realm of integral p-adic Hodge theory.

We can similarly define $V \in \mathrm{Rep}_{\mathbb{Q}_p}(C_K)$ to be Hodge-Tate if $\mathbb{C}_K \otimes_{\mathbb{Q}_p} V \in \mathrm{Rep}_{\mathbb{C}_K}(G_K)$ is Hodge-Tate. The *Hodge-Tate Decomposition*, which is proven in full generality by Faltings, says that, for a smooth proper K-scheme X, the étale cohomology $H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ is Hodge-Tate!

Theorem 2.2.21 (Hodge-Tate Decomposition, cf. [BC, Theorem 2.2.3]). *Let K be a p-adic field, and X be a smooth proper K-scheme. Then, there is a canonical isomorphism*

$$\mathbb{C}_K \otimes_{\mathbb{Q}_p} H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) \cong \bigoplus_q (\mathbb{C}_K(-q) \otimes_K H^{n-q}(X, \Omega^q_{X/K}))$$

in $\mathrm{Rep}_{\mathbb{C}_K}(G_K)$, where the cohomology on the right side is a sheaf cohomology, and the action of $g \in G_K$ on both sides are $g \otimes g$ on the left and $g \otimes 1$ on the right.

This is the starting point of *comparison theorems*, where all sorts of cohomology theories are canonically identified after tensoring with some rings, *p-adic period rings.* In this section, we try to make the characterization of Hodge-Tate representation as formal as possible. Notice that the subcategory of Hodge-Tate representations is closed under direct sum, dual and tensor product. In this regard, we can give the Hodge-Tate decomposition a $\mathbb{Z}$-grading, so that $V\{q\}$ is of degree $q \in \mathbb{Z}$. We define the covariant functor $\mathbf{D}_{\mathrm{HT}} : \mathrm{Rep}_{\mathbb{C}_K}(G_K) \to \mathrm{Gr}_K$ as

$$\mathbf{D}_{\mathrm{HT}}(V) = \oplus_q V\{q\} = \bigoplus_q (\mathbb{C}_K(q) \otimes_{\mathbb{C}_K} W)^{G_K},$$

where Gr_K is the category of $\mathbb{Z}$-graded vector spaces over K. Here, $\mathbf{D}$ stands for Dieudonné, and we will in general call this kind of functor a *Dieudonné functor.* This is a direct sum of invariants, so the functor is obviously left-exact. This definition can be once more simplified if we *define the Hodge-Tate period ring* $B_{\mathrm{HT}} := \bigoplus_q \mathbb{C}_K(q)$; then $\mathbf{D}_{\mathrm{HT}}(V) = (B_{\mathrm{HT}} \otimes_{\mathbb{C}_K} V)^{G_K}$.

How do we compactify the left hand side of ξ_V? Notice that $\bigoplus_q \mathbb{C}_K(-q) \otimes_K V\{q\} = \bigoplus_q (B_{\mathrm{HT}})_{-q} \otimes_K (\mathbf{D}_{\mathrm{HT}}(V))_q = (B_{\mathrm{HT}} \otimes_K \mathbf{D}_{\mathrm{HT}}(V))_0$, where the subscript means the degree in the grading. Thus, we can define a functor $\mathbf{V}_{\mathrm{HT}} : \mathrm{Gr}_K \to \mathrm{Rep}_{\mathbb{C}_K}(G_K)$ as

$$\mathbf{V}_{\mathrm{HT}}(W) = (B_{\mathrm{HT}} \otimes_K W)_0 = \mathrm{gr}^0(B_{\mathrm{HT}} \otimes_K W),$$

where gr^0 comes from the filtration $\mathrm{Fil}^i B_{\mathrm{HT}} = \oplus_{q \le i} \mathbb{C}_K(q)$, and then the map ξ_W is just the 0-th grade part of the *comparison morphism* α_W, where

$$\alpha_W : B_{\mathrm{HT}} \otimes_K \mathbf{D}_{\mathrm{HT}}(W) \hookrightarrow B_{\mathrm{HT}} \otimes_K (B_{\mathrm{HT}} \otimes_{\mathbb{C}_K} W) \to B_{\mathrm{HT}} \otimes_{\mathbb{C}_K} W,$$

defined using the grading-respecting multiplication $B_{\mathrm{HT}} \otimes_K B_{\mathrm{HT}} \to B_{\mathrm{HT}}$. Note that on the other hand $\alpha_W = \oplus_q \xi_W(q)$, the sum of Tate-twisted ξ_W's. Therefore, we deduce that *α_W is always injective, and $W \in \mathrm{Rep}_{\mathbb{C}_K}(G_K)$ is Hodge-Tate if and only if α_W is an isomorphism.* Notice that we can recover the complete information of $\mathbf{D}_{\mathrm{HT}}(W)$ from α_W, as $B_{\mathrm{HT}}^{G_K} = K$. Taking G_K-invariants, for Hodge-Tate W, we have $\mathbf{D}_{\mathrm{HT}}(W) \cong (B_{\mathrm{HT}} \otimes_K W)^{G_K}$. This in particular implies that, for any finite-dimensional $D \in \mathrm{Gr}_K$, $\mathbf{D}_{\mathrm{HT}}(\mathbf{V}_{\mathrm{HT}}(D)) \cong D$, as $\mathbf{V}_{\mathrm{HT}}(D)$ is always Hodge-Tate in that case.

Definition 2.2.11 (Hodge-Tate Representations). *Let $\mathrm{Rep}_{\mathrm{HT}}(G_K)$ be the full subcategory of $\mathrm{Rep}_{\mathbb{Q}_p}(G_K)$ consisted of Hodge-Tate objects (i.e. $V \in \mathrm{Rep}_{\mathrm{HT}}(G_K)$ if $V \otimes_{\mathbb{Q}_p} \mathbb{C}_K$ is Hodge-Tate). Define the functor $\mathbf{D}_{\mathrm{HT}} : \mathrm{Rep}_{\mathbb{Q}_p}(G_K) \to \mathrm{Gr}_K$ by $\mathbf{D}_{\mathrm{HT}}(V) = \mathbf{D}_{\mathrm{HT}}(\mathbb{C}_K \otimes_{\mathbb{Q}_p} V)$.*

The Hodge-Tate Decomposition Theorem can be written in a more appealing form.

Theorem 2.2.21 (Hodge-Tate Decomposition). *Let K be a p-adic field, and X be a smooth proper K-scheme. Then, for $n \ge 0$, $V := H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ is in $\mathrm{Rep}_{\mathrm{HT}}(G_K)$, with $\mathbf{D}_{\mathrm{HT}} \cong H^n_{\mathrm{Hodge}}(X/K) := \oplus_q H^{n-q}(X, \Omega^q_{X/K})$.*

This is an archetype of comparison theorems, which can be called as the main objective of p-adic Hodge theory. Namely, comparison theorems are mostly about asserting the following.

- For certain types of schemes, the p-adic étale cohomology groups as Galois representations are of some type (e.g. de Rham, crystalline, semi-stable).
- There is an analogue of Dieudonné functor, $\mathbf{D}$, such that $\mathbf{D}$ applied to the p-adic cohomology group is some other kind of cohomology group of the scheme (e.g. de Rham, crystalline, log-crystalline).

The program is by now mostly settled by the help of many mathematicians. We will be surveying comparison theorems in a later section.

2.2.2.3 Admissible Representations

We will define an abstract formalism, developed by Fontaine, that mimics the situation of Hodge-Tate representations. Let F be a field and G be a group. Let B be an F-algebra domain (which will be our *period ring*), equipped with a G-action as an F-algebra. Assume that $E = B^G$ is a field. Our goal is to *use B to construct an interesting functor from $\mathrm{Rep}_F(G)$, the category of finite-dimensional F-representations of G, to Vect_E, the category of finite-dimensional E-vector spaces.*

Definition 2.2.12 ((F,G)-regular Ring)**.** *The algebra B is* (F,G)-regular *if the following conditions are satisfied.*

1. $(\mathrm{Frac}\, B)^G = E (:= B^G)$.
2. *If $b \in B$ is nonzero and the F-linear span Fb is G-stable, then b is a unit in B.*

Obviously, we want to make sure that we are going into a correct direction.

Proposition 2.2.11. *The ring B_{HT} is $(\mathbb{Q}_p, G_K)$-regular.*

Proof. By Ax-Sen-Tate, we know $B_{\mathrm{HT}}^{G_K} = K$ is a field. To show that $(\mathrm{Frac}\, B_{\mathrm{HT}})^{G_K} = K$, notice that, after a choice of basis, $B_{\mathrm{HT}} \cong \mathbb{C}_K[T, T^{-1}]$, where G_K acts on T via $g(T) = \chi(g)T$. Then, $\mathrm{Frac}\, B_{\mathrm{HT}}$ can be G_K-equivariantly embedded into the ring $\mathbb{C}_K((T))$ of formal Laurent series. Thus, it is sufficient to show that $\mathbb{C}_K((T))^{G_K} = K$. On the other hand, if $f(T) = \sum_{n \ge n_0} a_n T^n$ is G_K-invariant, then $a_n \in \mathbb{C}_K(n)^{G_K}$ so that $f(T) = a_0 \in \mathbb{C}_K^{G_K} = K$.

For the second condition, suppose that a nonzero $\sum_{n=0}^{\infty} a_n T^n = f(T) \in \mathbb{C}_K[T] = B_{\mathrm{HT}}$ gives a G_K-stable line $f(T)\mathbb{Q}_p$. This means that G_K acts via a character $\eta : G_K \to \mathbb{Q}_p^{\times}$. Thus, $g\left(\sum_{n=0}^{\infty} a_n T^n\right) = \sum_{n=0}^{\infty} \eta(g) a_n T^n$, which gives $a_n \in (\mathbb{C}_K(\chi^n \eta^{-1}))^{G_K}$. The argument we used in calculating the Galois cohomologies of $\mathbb{C}_K(n)$ can be used in the same way to calculate the Galois cohomologies of $\mathbb{C}_K(\psi)$ for any character ψ; in particular, $H^0(G_K, \mathbb{C}_K(\psi))$ is nonzero if and only if ψ has a finite image (cf. [BC, Theorem 2.2.7]). This implies that there can only be one $n \ge 0$ with nonzero a_n, so that $f(T) = a_n T^n$ is indeed a unit in $B_{\mathrm{HT}} \cong \mathbb{C}_K[T, T^{-1}]$. $\square$

Aside from B_{HT}, we have one another easy example of (F,G)-regular ring: *when B is a field.* Although it may seem very silly (and it is indeed), we will actually use a case where the period ring is a field, e.g. B_{dR}.

Now we define the Dieudonné functor.

Definition 2.2.13 (Dieudonné Functors and Admissible Representations)**.** *Suppose that B is a (F,G)-regular ring. For $V \in \mathrm{Rep}_F(G)$, we define*

$$\mathbf{D}_B(V) = (B \otimes_F V)^G,$$

to be the associated Dieudonné module. This is an E-vector space equipped with a canonical map, the comparison morphism,

$$\alpha_V : B \otimes_E \mathbf{D}_B(V) \to B \otimes_E (B \otimes_F V) = (B \otimes_E B) \otimes_F V \to B \otimes_F V.$$

We call $V \in \mathrm{Rep}_F(G)$ *a* B-admissible representation *if* α_V *is an isomorphism. We let* $\mathrm{Rep}_F^B(G) \subset \mathrm{Rep}_F(G)$ *be the full subcategory of* B*-admissible representations.*

Example 2.2.4.

1. Hodge-Tate representations are precisely B_{HT}-admissible representations.

2. In general, it is obvious that $V = F$ with trivial G-action is B-admissible, with $\mathbf{D}_B(F) = E$.

As we have promised, the analogues of Lemma 2.2.1 hold true in general under this formalism.

Theorem 2.2.22 [BC, Theorem 5.2.1]. *For* $V \in \mathrm{Rep}_F(G)$*, the following are true.*

(i) The map α_V *is always injective, and* $\mathbf{D}_B(V)$ *is always finite-dimensional with* $\dim_E \mathbf{D}_B(V) \leq \dim_F V$*. The equality holds if and only if* V *is* B*-admissible.*

(ii) The covariant functor $\mathbf{D}_B : \mathrm{Rep}_F^B(G) \to \mathrm{Vect}_E$ *is faithful and exact.*

(iii) Any subrepresentation or quotient of a B*-admissible representation is* B*-admissible.*

(iv) If $V_1, V_2 \in \mathrm{Rep}_F^B(G)$*, then there is a natural isomorphism*

$$\mathbf{D}_B(V_1) \otimes_E \mathbf{D}_B(V_2) \cong \mathbf{D}_B(V_1 \otimes_F V_2),$$

so that $V_1 \otimes_F V_2 \in \mathrm{Rep}_F^B(G)$*.*

(v) If $V \in \mathrm{Rep}_F^B(G)$*, then the* F*-dual* $V^\vee$ *is* B*-admissible, and* $\mathbf{D}_B(V) \otimes_E \mathbf{D}_B(V^\vee) \to \mathbf{D}_B(F) = E$ *is a perfect duality.*

(vi) B*-admissibility is preserved under the formation of exterior and symmetric powers, and* $\mathbf{D}_B$ *naturally commutes with both such constructions.*

Proof. (i) Suppose not. Let $d_1, \cdots, d_n$ be linearly independent elements in $\mathbf{D}_B(V)$ such that there exist $b_i \neq 0$ with $\alpha_V(\sum b_i \otimes_E d_i) = \sum b_i d_i = 0$. We can choose them so that n is minimal among such sets. As d_i's are G-invariant, for all $g \in G$, we have $\sum g(b_i) d_i = 0$. By the minimality of n, we have $\frac{b_i}{b_1} \in (\mathrm{Frac}\, B)^G = B^G = E$. Then $d_1 + \sum_{i=2}^n \frac{b_i}{b_1} d_i = 0$ is a linear dependence relation over E, which is a contradiction.

This actually shows that $\alpha_V \otimes_B \mathrm{Frac}\, B$ is injective, so that $\dim_E \mathbf{D}_B(V) \leq \dim_F V$. Suppose that the equality holds. Let e_i be an E-basis of $\mathbf{D}_B(V)$ and v_j be an F-basis of V and let $\alpha_V(e) = Av$, where A is a matrix with $\det A \in (\mathrm{Frac}\, B)^\times$. As e_i's are G-invariant, $\det \alpha_V(e_1 \wedge \cdots \wedge e_d) = \det A v_1 \wedge \cdots \wedge v_d$ is also G-invariant. As $v_1 \wedge \cdots \wedge v_d \neq 0$, it follows that the F-line $F \cdot \det A$ is G-stable. By regularity, $\det A \in B^\times$, and this implies that α_V is an isomorphism.

(ii) Exactness follows from the fact that $\mathbf{D}_B$ is already left-exact and that we know the dimensions behave well with $\mathbf{D}_B$ for B-admissible representations by (i). The same argument shows that $\mathbf{D}_B$ is faithful.

(iii) If $0 \to V' \to V \to V'' \to 0$ is an exact sequence in $\mathrm{Rep}_F(G)$ with $V \in \mathrm{Rep}_F^B(G)$, the left-exactness of $\mathbf{D}_B$ implies that $\dim_E \mathbf{D}_B(V) \leq \dim_E \mathbf{D}_B(V') + \dim_E \mathbf{D}_B(V'')$. But the left hand side is as large as possible, so V' and V'' are B-admissible.

(iv) The image of $\mathbf{D}_B(V) \otimes_E \mathbf{D}_B(V') \to (B \otimes_F V) \otimes_E (B \otimes_E V') \to B \otimes_F (V \otimes_F V')$ is G-invariantn, so it factors through $\mathbf{D}_B(V \otimes_F V')$. As $\dim_E(\mathbf{D}_B(V) \otimes_E \mathbf{D}_B(V')) = \dim_F V \dim_F V'$ whereas $\dim_E \mathbf{D}_B(V \otimes_F V') \leq \dim_F V \dim_F V'$ by (i), it is enough to show that the map

$\mathbf{D}_B(V) \otimes_E \mathbf{D}_B(V') \to \mathbf{D}_B(V \otimes_F V')$ we induced above is injective. On the other hand, after tensoring this with B, it becomes an isomorphism. By dimensionality reason, it is thus injective.

(vi) This is immediate by realizing that symmetric powers and exterior powers are sub-objects of tensor products.

(v) The pairing arises from utilizing a natural isomorphism $\det(V^\vee) \otimes_F \wedge^{\dim_F V - 1} V \cong V^\vee$. The perfectness of one-dimensional cases is trivial, and the perfectness of general cases follows from the perfectness of one-dimensional cases via taking determinants. □

2.2.2.4 De Rham Representations

The theory of Hodge-Tate representations are nice, but they are nice only because we are working over $\mathbb{C}_p$, over which many subtle Galois-theoretic informations are ignored and therefore many things become nicer. Thus, we need a finer theory. We would like to construct a period ring whose Dieudonné functor yields *algebraic de Rham cohomology*, which we will not discuss for now. The *de Rham period ring* B_{dR}, if exists, should be a refinement of B_{HT}, so that it is $(\mathbb{Q}_p, G_K)$-regular, $B_{\text{dR}}^{G_K} = K$ and it has a descreasing filtration $\text{Fil}^i(B_{\text{dR}})$ (which comes from the Hodge filtration of algebraic de Rham cohomology) such that $\text{gr}^\bullet(B_{\text{dR}}) = B_{\text{HT}}$. This motivation will be justified more detailedly in the later section on p-adic comparison theorems.

We briefly recall the construction called the *ring of Witt vectors*, which can be found for example in [Se, II.§6]. Let R be a perfect ring of characteristic $p > 0$, which means that the Frobenius $x \mapsto x^p$ is bijective. Then there exists a unique *strict p-ring* $W(R)$, called the *ring of Witt vectors over R*, with residue ring R. Recall that a *p-ring* is a ring A complete and separated with respect to a filtration of ideals $A \supset I_1 \supset I_2 \cdots$ such that $A/I_1 = R$, *the residue ring*, is of characteristic p, and $I_n \cdot I_m \subset I_{n+m}$. A p-ring is *strict* if p is not nilpotent. The ring of Witt vectors comes with the *Teichmüller lift* $[\cdot] : R \to W(R)$, which is a ring homomorphiism and also a section of the reduction map $W(R) \to R$.

To construct B_{dR}, the *de Rham period ring*, we want to start with an object that looks like "$W(\mathcal{O}_{\mathbb{C}_K}/(p))$," for a p-adic field K. However, the ring $\mathcal{O}_{\mathbb{C}_K}/(p)$ is not perfect. Therefore, we instead use the *perfection* $R(\mathcal{O}_{\mathbb{C}_K}/(p))$. Recall that for an $\mathbb{F}_p$-algebra A, the perfection $R(A)$ is defined by $R(A) = \varprojlim_{x \mapsto x^p} A$. These are some ring-theoretic properties of $R(\mathcal{O}_{\mathbb{C}_K}/(p))$, which are very easy to be verified.

Proposition 2.2.12 [BC, 4.3]**.** *Let $R = R(\mathcal{O}_{\mathbb{C}_K}/(p))$, for a p-adic field K.*

(i) The ring R can be described as $\{(x_0, x_1, \cdots) \mid x_i \in \mathcal{O}_{\mathbb{C}_K}, x_{i+1}^p = x_i\}$. It is therefore an integral domain.

(ii) Let $v_R((x^{(0)}, \cdots)) = v_p(x^{(0)})$, where v_p is the normalized p-adic valuation on $\mathbb{C}_K$ (i.e. $v_p(p) = 1$). Then, v_R is a valuation on R. With respect to v_R, R is complete and separated.

(iii) If $x, y \in R$ satisfies $v_R(x) \geq v_R(y)$, then there exists $z \in R$ such that $x = yz$.

(iv) The action of G_K on R is defined via $g((x_0, x_1, \cdots,)) = (g(x_0), g(x_1), \cdots)$, and the Frobenius map φ on R is defined via $\varphi((x_0, x_1, \cdots)) = (x_0^p, x_0, x_1, \cdots)$. Then, $R^{\varphi^r = 1} = \mathbb{F}_{p^r}$, and $R^{G_K} = k_K$, the residue field of K.

A deeper fact is the following.

Theorem 2.2.23 [BC, Theorem 4.3.5]**.** *The field* $\text{Frac}\, R$ *is an algebraically closed field of characteristic p.*

Proof. We know that $\text{Frac}\, R = \{(x_0, x_1, \cdots) \mid x_i \in \mathbb{C}_K, x_{i+1}^p = x_i\}$. Suppose we are given a monic polynomial $P(x) \in R[x]$, $P(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0$. Each $a_k \in R$ has a representative $a_k = (a_{k,0}, a_{k,1}, \cdots)$ where $a_{k,n} \in \mathcal{O}_{\mathbb{C}_K}/(p)$. Let $P_n(x) = x^d + a_{d-1,n}x^{d-1} + \cdots + a_{0,n} \in$

$(\mathcal{O}_{\mathbb{C}_K}/(p))[x]$ satisfies $P_n(x)^p = P_n(x^p)$. Choose lifts $\widetilde{P_n}(x) \in \mathcal{O}_{\mathbb{C}_K}[x]$, and let $\alpha_{n,1}, \cdots, \alpha_{n,d}$ be roots of $\widetilde{P_n}(x)$. Then, we know $\widetilde{P_{n-1}}(\alpha_{n,i}^p) \equiv 0 (\bmod p)$ for all i. Thus,

$$\prod_{j=1}^{d} (\alpha_{n,i}^p - \alpha_{n-1,j}) \in (p).$$

Thus, for each i, there exists at least one j such that $v_p(\alpha_{n,i}^p - \alpha_{n-1,j}) \geq \frac{1}{d}$. Then, by the binomial formula, it follows that, for all $k \geq 1$, $v_p(\alpha_{n,i}^{p^k} - \alpha_{n-1,j}^{p^{k-1}}) \geq \frac{k}{d}$. This implies that $(\alpha_{n,i}^{p^{d-1}})^p \equiv \alpha_{n-1,j}^{p^{d-1}} (\bmod p)$. Thus this correspondence $i \mapsto j$ is actually a one-to-one correspondence from $\{1, \cdots, d\}$ to itself, so that after reording the roots, $\varprojlim_n a_{n,i}^{p^{d-1}} (\bmod p) \in \operatorname{Frac} R$ for all $1 \leq i \leq d$. This implies that $\operatorname{Frac} R$ is algebraically closed. □

As R is a perfect ring of characteristic p, we can construct $W(R)$. It inherits the Galois action and the Frobenius so that $g \in G_K$ acts via $g(\sum p^n [c_n]) = \sum p^n [g(c_n)]$ and $\varphi(\sum p^n [c_n]) = \sum p^k [\varphi(c_n)]$, for $c_n \in R$. In particular, by our characterization of R, there is a G_K-equivariant surjective ring homomorphism $\theta : W(R) \to \mathcal{O}_{\mathbb{C}_K}$ such that

$$\theta(\sum p^n [c_n]) = \sum (c_n)_0 p^n,$$

for $c_n \in R$ ([BC, Lemma 4.4.1]). This in turn induces a G_K-equivariant surjective ring homomorphism

$$\theta_{\mathbb{Q}} : W(R)[1/p] \to \mathcal{O}_{\mathbb{C}_K}[1/p] = \mathbb{C}_K.$$

We are now almost there, but there is one remaining problem, that $W(R)[1/p]$ is not a complete discrete valuation ring. Thus, we shall replace $W(R)[1/p]$ with its $\ker \theta_{\mathbb{Q}}$-adic completion.

Definition 2.2.14 (B_{dR}^+ and B_{dR})**.** *The ring B_{dR}^+ is defined as $\varprojlim_{n\to\infty} W(R)[1/p]/(\ker \theta_{\mathbb{Q}})^n$. The* de Rham period ring *B_{dR} is defined by $B_{\mathrm{dR}} = \operatorname{Frac} B_{\mathrm{dR}}^+$.*

We are yet to be done, as we have not verified some of the most important properties of $W(R)$.

Proposition 2.2.13. *The ideal $\ker \theta \subset W(R)$ is a principal ideal, and any $\alpha \in \ker \theta$ with $v_R(\overline{\alpha}) = 1$ generates $\ker \theta$.*

Proof. As $\mathbb{C}_K$ is torsion-free, $\ker \theta \cap p^n W(R) = p^n \ker \theta$. If $\theta(x) = 0$, then $\overline{x}_0 \in (p)$ due to the definition of θ. Therefore, $v_R(\overline{x}) = v_p(\overline{x}_0) \geq v_R(\overline{\alpha}) = 1$, which implies that there is $\overline{y} \in R$ such that $\overline{x} = \overline{\alpha y}$. Thus $x \equiv \alpha y (\bmod p)$ for some $y \in W(R)$. We can successively lift modulo p^n so that x is actually a multiple of α. □

Example 2.2.5. There are two major examples we will use for a generator of $\ker \theta$.

- Let $\alpha = [\widetilde{p}] - p$, where $\widetilde{p} = (p, p^{1/p}, p^{1/p^2}, \cdots) \in R$. Obviously $\theta([\widetilde{p}]) = p$ and $\theta(p) = p$, so $\theta([\widetilde{p}] - p) = 0$. Also, the image of $[\widetilde{p}] - p$ in R is $\widetilde{p}$, which has v_R-valuation 1. We usually denote this element as ξ.
- Let $\alpha = \frac{[\varepsilon]-1}{[\varepsilon^{1/p}]-1}$, where $\varepsilon = (1, \zeta_p, \zeta_{p^2}, \cdots) \in R$. Note that $v_R(\varepsilon - 1) = \lim_{n\to\infty} p^n v_p(\zeta_{p^n} + (-1)^p) = \lim_{n\to\infty} \frac{p^n}{p^{n-1}(p-1)} = \frac{p}{p-1}$, and $v_R(\varepsilon^{1/p} - 1) = \lim_{n\to\infty} p^n v_p(\zeta_{p^{n+1}} + (-1)^p) = \lim_{n\to\infty} \frac{p^n}{p^n(p-1)} = \frac{1}{p-1}$. Thus, $v_R(\alpha) = 1$, and $\theta([\varepsilon] - 1) = 0$ whereas $\theta([\varepsilon^{1/p}] - 1) = \zeta_p - 1 \neq 0$, so α generates $\ker \theta$. We usually denote this element as ω.

From this, it is clear that B_{dR}^+ is a complete discrete valuation ring.

Proposition 2.2.14. *The ring B_{dR}^+ is a complete discrete valuation ring with maximal ideal $\ker\theta$, residue field $\mathbb{C}_p$ and uniformizer any choice of generator of the principal ideal $\ker\theta$.*

Proof. It is a formal consequence from that $W(R)[1/p]$ is separated with respect to $\ker\theta_{\mathbb{Q}}$-adic topology. Suppose $x \in \cap_{n\geq 0}(\ker\theta_{\mathbb{Q}})^n \subset W(R)[1/p]$. For some k, we have $p^k x \in W(R)$. Note that $\theta_{\mathbb{Q}}|_{W(R)} = \theta$, so this implies that $p^k x \in \cap_{n\geq 0}(\ker\theta)^n$. Thus, it is enough to show that $\cap_{n\geq 0}(\ker\theta)^n = 0$. Any element $x \in \cap_{n\geq 0}(\ker\theta)^n$ is divisible by arbitrary powers of $[\widetilde{p}] - p$. So, $\overline{x} \in R$ is divisible by arbitrary powers of $\widetilde{p}$. As R is v_R-complete, $\overline{x} = 0$. This implies that $x = px'$ for some $x' \in W(R)$. On the other hand, $x = ([\widetilde{p}] - p)^n y$ for some $y \in W(R)$, and as $\overline{x} = 0$, $\overline{y} = 0$, and y is divisible by p. Cancelling p's out, we have $x' = ([\widetilde{p}] - p)^n y'$ for some $y' \in W(R)$, or $x' \in (\ker\theta)^n$. Thus it follows that $x' \in \cap(\ker\theta)^n$. Thus x is divisible by arbitrary powers of p, so is 0. □

From this, we can define the *filtration of* B_{dR} *to be* $\mathrm{Fil}^n B_{\mathrm{dR}} = \mathfrak{m}^n_{B^+_{\mathrm{dR}}}$*, which is* G_K*-stable.* To show that B_{dR} is a good refinement of B_{HT}, we want to prove that the graded algebra $\mathrm{gr}^\bullet(B_{\mathrm{dR}})$ is, G_K-equivariantly, B_{HT}. This amounts to proving that $\mathfrak{m}_{B^+_{\mathrm{dR}}}/\mathfrak{m}^2_{B^+_{\mathrm{dR}}}$ has a canonical copy of $\mathbb{Z}_p(1)$. The situation here is much more explicit, that we can identify a uniformizer t of B^+_{dR} in a very explicit way, which should be canonical up to $\mathbb{Z}_p^\times$-multiple, so that G_K acts by the cyclotomic character. A uniformizer t is defined by

$$t = \log([\varepsilon]) = \sum_{n\geq 1}(-1)^{n+1}\frac{([\varepsilon]-1)^n}{n} \in B^+_{\mathrm{dR}}.$$

Proposition 2.2.15. *Let t be defined as above.*

(i) The series defining t converges in the max-adic topolog on B^+_{dR} to a uniformizer, which we will call as t.

(ii) The Galois group G_K acts by the cyclotomic character.

(iii) There is a canonical G_K-equivarian isomorphism $\mathrm{gr}^\bullet B_{\mathrm{dR}} \cong B_{\mathrm{HT}}$.

Proof. (i) That it converges is obvious. To see that it is a uniformizer, note that $\frac{t}{1-[\varepsilon]} \in (B^+_{\mathrm{dR}})^\times$ by definition. Also, we already know that $\frac{1-[\varepsilon]}{1-[\varepsilon^{1/p}]}$ is a uniformizer and $1-[\varepsilon^{1/p}]$ is a unit. Thus, t is a uniformizer.

(ii) One can construct another topology on B^+_{dR} so that the formal power series $\log((1+x)^a) = \log(1+((1+x)^a-1))$ converges and is equal to $a\log(1+x)$ (cf. [BC, Exercise 4.5.3]). Given the topology, we immediately get the conclusion, as

$$g(t) = g(\log[\varepsilon]) = \log(g([\varepsilon])) = \log[g(\varepsilon)] = \log[\varepsilon^{\chi(g)}] = \log([\varepsilon]^{\chi(g)}) = \chi(g)t.$$

(iii) The discussion right before the statement of the proposition shows that (i) and (ii) will show (iii). □

Before studying de Rham representations, we study cohomology of B^+_{dR}.

Lemma 2.2.2. *Let $i \in \mathbb{Z}$. Then,*

$$H^0(G_K, t^i B^+_{\mathrm{dR}}) = \begin{cases} K & \text{if } i \leq 0 \\ 0 & \text{otherwise,} \end{cases}$$

and

$$H^1(G_K, t^k B^+_{\mathrm{dR}}) = 0,$$

for $k \geq 1$.

Proof. We start with a G_K-equivariant exact sequence

$$0 \to t^{i+1}B_{\mathrm{dR}}^+ \to t^iB_{\mathrm{dR}}^+ \to \mathbb{C}_p(i) \to 0,$$

for $i \in \mathbb{Z}$. The cohomology long exact sequence gives

$$\begin{aligned} 0 &\to H^0(G_K, t^{i+1}B_{\mathrm{dR}}^+) \to H^0(G_K, t^iB_{\mathrm{dR}}^+) \to H^0(G_K, \mathbb{C}_p(i)) \\ &\to H^1(G_K, t^{i+1}B_{\mathrm{dR}}^+) \to H^1(G_K, t^iB_{\mathrm{dR}}^+) \to H^1(G_K, \mathbb{C}_p(i)). \end{aligned}$$

An immediate consequence is that $H^j(G_K, t^{i+1}B_{\mathrm{dR}}^+) = H^j(G_K, t^iB_{\mathrm{dR}}^+)$ for $i \neq 0$. Thus, we only need to calculate the Galois cohomology for $i = 0, 1$. Moreover, $H^0(G_K, tB_{\mathrm{dR}}^+) = (tB_{\mathrm{dR}})^{G_K} = (t^iB_{\mathrm{dR}})^{G_K}$ for any $i \geq 1$, so in particular $(tB_{\mathrm{dR}})^{G_K} \subset \cap_{i\geq 1}t^iB_{\mathrm{dR}}^+ = 0$.

Next we calculate $H^1(G_K, tB_{\mathrm{dR}}^+)$. Let $M \in H^1(G_K, tB_{\mathrm{dR}}^+)$, we recursively get $M_i \in H^1(G_K, t^iB_{\mathrm{dR}}^+)$ such that $M_1 = M$ and $M_{i+1}(g) = M_i(g) + g(y_i) - y_i$ for some $y_i \in t^iB_{\mathrm{dR}}^+$; this is possible by the cohomology long exact sequence. Letting $y = \sum y_i$, it converges in B_{dR}^+, and we get $M(g) = M_1(g) + g(y) - y$ is in $H^1(G_K, t^iB_{\mathrm{dR}}^+)$ for all $i \geq 0$. As B_{dR}^+ is separated, $M = 0$, so $M_1 = 0$. Now $(B_{\mathrm{dR}}^+)^{G_K} = K$ also follows from the long exact sequence. □

Now we briefly study *de Rham representations*, which should be obviously defined as B_{dR}-admissible representations. First of all, this makes sense as B_{dR} is a field, which is automatically $(\mathbb{Q}_p, G_K)$-regular. We already linear algebraic properties of Dieudonné functor $\mathbf{D}_{\mathrm{dR}} : \mathrm{Rep}_{\mathrm{dR}}(G_K) \to \mathrm{Vect}_K$ by Theorem 2.2.22. However, our general philosophy is the following: *if the period ring has some structure, then Dieudonné modules also have similar structures, so that the comparison isomorphism $\alpha_V : B \otimes_E \mathbf{D}_B(V) \to B \otimes_F V$ respects all structures on both sides.* In our case, we have the filtration $\mathrm{Fil}^i B_{\mathrm{dR}}$, and we would like to give a natural filtration to $\mathbf{D}_{\mathrm{dR}}(V)$ for $V \in \mathrm{Rep}_{\mathrm{dR}}(G_K)$.

Definition 2.2.15. *Given $V \in \mathrm{Rep}_{\mathrm{dR}}(G_K)$, let $\mathrm{Fil}^i D_{\mathrm{dR}}(V) = (t^iB_{\mathrm{dR}}^+ \otimes_{\mathbb{Q}_p} V)^{G_K}$. This makes $\mathbf{D}_{\mathrm{dR}}$ a functor into $\mathrm{FilVect}_K$, the category of K-filtered vector spaces.*

Remark 2.2.2. There is a subtle point lurking behind: the category $\mathrm{FilVect}_K$ is in general *not an abelian category.* Nevertheless we can do all basic linear-algebraic constructions, including the notion of exact sequences. In particular, it is pre-abelian (i.e. has kernels and cokernels).

In particular, we can now make the statement that B_{dR} *is a refinement of* B_{HT}.

Proposition 2.2.16. *For $V \in \mathrm{Rep}_{\mathrm{dR}}(V)$, then $\mathrm{gr}^\bullet \mathbf{D}_{\mathrm{dR}}(V) \cong \mathbf{D}_{\mathrm{HT}}(V)$. In particular, de Rham implies Hodge-Tate.*

Proof. As the de Rham filtrations are Galois stable, we have $\mathrm{Fil}^i \mathbf{D}_{\mathrm{dR}}(V)/\mathrm{Fil}^{i+1} \mathbf{D}_{\mathrm{dR}}(V) \cong (\mathrm{gr}^i B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V)^{G_K} = \mathrm{gr}^i \mathbf{D}_{\mathrm{HT}}(V)$. □

It is a tedious yet very straightforward process to check that the additional structure, filtration, behaves well with all other linear-algebraic constructions.

Proposition 2.2.17 [BC, §6.3]. *Let $V \in \mathrm{Rep}_{\mathrm{dR}}(G_K)$.*

(i) The functor $\mathbf{D}_{\mathrm{dR}} : \mathrm{Rep}_{\mathrm{dR}}(G_K) \to \mathrm{FilVect}_K$ is faithful, carries short exact sequences to short exact sequences, and is compatible with the formation of tensor products and duals.

(ii) The comparison isomorphism $\alpha_V : B_{\mathrm{dR}} \otimes_K \mathbf{D}_{\mathrm{dR}}(V) \cong B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} V$ is G_K-equivariant and respects the filtrations.

(iii) If L/K is complete and discretely valued field extension in $\mathbb{C}_p$, then the natural map $L \otimes_K \mathbf{D}_{\mathrm{dR},K}(V) \to \mathbf{D}_{\mathrm{dR},L}(V)$ is a filtration-respecting isomorphism. In particular, this holds for L/K finite or $L = \widehat{K^{\mathrm{nr}}}$.

Example 2.2.6. It is automatic that $\mathbb{Q}_p(n)$ is de Rham for $n \in \mathbb{Z}$ as $\mathbf{D}_{\mathrm{dR}}(\mathbb{Q}_p(n)) = Kt^{-n}$, with its unique filtration jump in degree $-n$. Thus, $V \in \mathrm{Rep}_{\mathbb{Q}_p}(G_K)$ is de Rham if and only if $V(n)$ is de Rham. More generally, a continuous character $\eta : G_K \to \mathbb{Z}_p^\times$ gives a de Rham twist $\mathbb{Q}_p(\eta)$ if and only if there exists $n \in \mathbb{Z}$ such that $\chi^n\eta$ is potentially unramified.

2.2.2.5 Crystalline and Semi-stable Period Rings

Recall that B_{dR} was constructed as a refinement of B_{HT} so that de Rham representations had filtrations coming from the natural filtration structure of $W(R)[1/p]$. On the other hand, we still have lost some information: *Frobenius.* As the Frobenius automorphism of $W(R)[1/p]$ does not preserve $\ker\theta_{\mathbb{Q}}$, there is no natural Frobenius endomorphism on B_{dR}. To remedy this, we will introduce a subring $A^0_{\mathrm{cris}} \subset W(R)[1/p]$ that is Frobenius-stable. Explicitly, A^0_{cris} is defined as the G_K-stable $W(R)$-subalgebra of $W(R)[1/p]$ generated by *divided powers*,

$$A^0_{\mathrm{cris}} = W(R)[\frac{\alpha^m}{m!}]_{m\geq 1, \alpha\in\ker\theta}.$$

It is clear that A^0_{cris} is $\mathbb{Z}$-flat. We define A_{cris} to be the p-adic completion of A^0_{cris}; it is p-adically separated and complete, and is $\mathbb{Z}_p$-flat. It is also stable under φ, as

$$\varphi(\omega) = \varphi(\sum_{i=0}^{p-1}[\varepsilon^{i/p}]) = p + \sum_{i=0}^{p-1}([\varepsilon^i]-1) = p + \omega a,$$

for some $a \in W(R)$, which implies that

$$\varphi(\frac{\omega^m}{m!}) = \frac{(p+\omega a)^m}{m!} = \sum_{k=0}^{m}\frac{p^{m-i}a^i}{(m-i)!}\frac{\omega^i}{i!},$$

which is in A^0_{cris} as $n!|p^n$ in $\mathbb{Z}_p$.

The ring A^0_{cris} is quite painful to analyze, so not many properties of A_{cris} are immediate. Nevertheless, one can prove that (cf. [BC, Exercise 9.4.1]) there is a unique continuous map $j : A_{\mathrm{cris}} \to B^+_{\mathrm{dR}}$ lifting $A^0_{\mathrm{cris}} \hookrightarrow W(R)[1/p]$ which is bound to be G_K-equivariant and injective. This gives a concrete description of A_{cris}:

$$A_{\mathrm{cris}} = \left\{\sum_{n\geq 0} a_n\frac{\xi^n}{n!} \mid a_n \in W(R), a_n \to 0 \text{ with respect to the } p\text{-adic topology}\right\},$$

where $\xi = [\widetilde{p}] - p$ as before (or any generator of $\ker\theta$). Moreover, the p-adic topology on A_{cris} is generated by sets of form $\{\sum_{n\geq 0} a_n\xi^n/n! \mid |a_n| < \epsilon, a_n \to 0\}$. Although the divided power series expansion is *not unique*, nonetheless this implies that the composite map $A_{\mathrm{cris}} \hookrightarrow B^+_{\mathrm{dR}} \to \mathbb{C}_K$ is a surjective map onto $\mathcal{O}_{\mathbb{C}_K}$. By an alternative G_K-equivariant description of A_{cris}, one can show that its G_K-action is p-adically continuous (cf. [BC, Proposition 9.1.2]). We then define $B^+_{\mathrm{cris}} = A_{\mathrm{cris}}[1/p] \subset B^+_{\mathrm{dR}}$, and hope to define B_{cris} from B^+_{cris}. Note that $B_{\mathrm{dR}} = B^+_{\mathrm{dR}}[1/t]$, so first attempt is to define $B_{\mathrm{cris}} = B^+_{\mathrm{cris}}[1/t]$. This is indeed the right definition, modulo that we do not know yet if $t \in B^+_{\mathrm{cris}}$. On the other hand, as we can use any generator of $\ker\theta$ instead of ξ for the concrete description of A_{cris},

$$t = \sum_{n\geq 1}(-1)^{n-1}\frac{([\varepsilon]-1)^n}{n} = \sum_{n\geq 1}(-1)^{n-1}(n-1)!([\varepsilon^{1/p}]-1)^n\frac{\omega^n}{n!},$$

and the coefficients converge to 0 with respect to p-adic topology, as $n! \to 0$. Thus, $t \in A_{\mathrm{cris}} \subset B^+_{\mathrm{cris}}$, and we can *now define* $B_{\mathrm{cris}} = B^+_{\mathrm{cris}}[1/t]$. Also, we give the filtration on B_{cris} as the subspace filtration of B_{dR}, i.e. $\operatorname{Fil}^i B_{\mathrm{cris}} = \operatorname{Fil}^i B_{\mathrm{dR}} \cap B_{\mathrm{cris}}$. Also, as we know A^0_{cris} is φ-stable, we can just let the Frobenius φ on B^+_{cris} be *the map induced from* $\varphi|_{A^0_{\mathrm{cris}}}$. To check that it extends to B_{cris}, we need to check that $\varphi(t)$ goes to a unit in B_{cris}. Indeed,

$$\varphi(t) = \sum_{n\geq 1} (-1)^{n-1} \frac{([\varepsilon^p]-1)^n}{n} = \log[\varepsilon^p] = pt,$$

so φ extends to B_{cris}. A fundamental fact is that $\phi : A_{\mathrm{cris}} \to A_{\mathrm{cris}}$ is injective ([BC, Theorem 9.1.8]).

A must-to-check is the following.

Proposition 2.2.18 [BC, Proposition 9.1.6]**.** *The domain* B_{cris} *is* $(\mathbb{Q}_p, G_K)$*-regular.*

Proof. Notice first that $K_0 \subset B^{G_K}_{\mathrm{cris}} \subset (\operatorname{Frac} B_{\mathrm{cris}})^{G_K}$. As the natural map $K \otimes_{K_0} B_{\mathrm{cris}} \to B_{\mathrm{dR}}$ is an injection ([BC, Theorem 9.1.5]), we deduce that $K \otimes_{K_0} \operatorname{Frac} B_{\mathrm{cris}} \hookrightarrow B_{\mathrm{dR}}$ is also an injection. Thus, $(K \otimes_{K_0} \operatorname{Frac} B_{\mathrm{cris}})^{G_K} = K \otimes_{K_0} (\operatorname{Frac} B_{\mathrm{cris}})^{G_K} \hookrightarrow (B_{\mathrm{dR}})^{G_K} = K$, which implies that $(\operatorname{Frac} B_{\mathrm{cris}})^{G_K} = B^{G_K}_{\mathrm{cris}} = K_0$.

Suppose that $0 \neq b \in B_{\mathrm{cris}}$ such that $\mathbb{Q}_p b$ is G_K-stable. As $\mathbb{Q}_p t$ is G_K-stable, we can multiply or invert t so that we can assume $b \in B^+_{\mathrm{dR}} - tB^+_{\mathrm{dR}}$. Let $\bar{b}$ be the reduction in $B^+_{\mathrm{dR}}/tB^+_{\mathrm{dR}} = \mathbb{C}_K$. Let $\eta : G_K \to \mathbb{Q}_p^\times$ be the character acting on $\mathbb{Q}_p b$. Then η is continuous and should be $\mathbb{Z}_p^\times$-valued, so that $\mathbb{C}_K(\eta^{-1})^{G_K} = 0$. This implies that η has finite image, i.e. potentially unramified. On the other hand, as the formation of B_{cris} is compatible with a base-change to $\widehat{K^{\mathrm{nr}}}$ (Proposition 2.2.17(iii)), we deduce that $\bar{b}$ is algebraic over $\widehat{K^{\mathrm{nr}}}$. Such element uniquely lifts to $\beta \in B^+_{\mathrm{dR}}$ by Hensel's lemma, so in particular $b - \beta \in \operatorname{Fil}^1(B^+_{\mathrm{dR}})$. As β is a unique lift, G_K acts on β by η. Thus, $b - \beta$ spans a G_K-stable $\mathbb{Q}_p$-line in $\operatorname{Fil}^1(B^+_{\mathrm{dR}})$. If this line is nonzero, then any nonzero element will give an element in $\mathbb{C}_K(\chi^r \eta)^{G_K}$ for some $r \geq 1$, which is impossible. Therefore, $b = \beta$ is algebraic over $\widehat{K^{\mathrm{nr}}}$.

This implies that $L = \widehat{K_0^{\mathrm{nr}}}(b) \subset B_{\mathrm{cris}}$ is a finite extension of $\widehat{K_0^{\mathrm{nr}}}$. Let L_0 be a maximal unramified subfield, which must be $\widehat{K_0^{\mathrm{nr}}}$. As $L \otimes_{L_0} B_{\mathrm{cris}} \to B_{\mathrm{dR}}$ is injective, $L = L_0$, or $b \in L_0^\times \subset B^\times_{\mathrm{cris}}$, as desired. ☐

There is a mild relation between filtration and Frobenius.

Theorem 2.2.24 (Fundamental Exact Sequence, [Fo3, Théorème 5.3.7])**.** *The natural map* $B^{\varphi=1}_{\mathrm{cris}} \to B_{\mathrm{dR}}/B^+_{\mathrm{dR}}$ *is surjective, and its kernel is identified with* $\mathbb{Q}_p$*. Moreover,*

$$0 \to \mathbb{Q}_p(r) \to \operatorname{Fil}^r B^+_{\mathrm{cris}} \xrightarrow{p^{-r}\varphi - 1} B^+_{\mathrm{cris}} \to 0$$

is exact for all $r \geq 0$ *and*

$$0 \to \mathbb{Q}_p(r) \to \operatorname{Fil}^r B_{\mathrm{cris}} \xrightarrow{p^{-r}\varphi - 1} B_{\mathrm{cris}} \to 0$$

is exact for all $r \in \mathbb{Z}$*.*

Now we can define *crystalline representations* to be B_{cris}-admissible representations. This is meant to capture good reduction of smooth proper K-schemes. To capture semi-stable reduction, we would want to extend the period ring B_{cris} by allowing additional freedom to contain singularities coming from semi-stable reduction. Motivated from the bad reduction by the Tate curve, B_{st} should be generated over B_{cris} by the hypothetical element "$\log([\widetilde{p}])$." Canonically we can define B_{st} as follows: let $\lambda : R^\times \to B^+_{\mathrm{cris}}$ be the G_K-equivariant logarithm, requiring it to be trivial on $\overline{k}^\times$ and to be $x \mapsto \log([x])$ on $x \in \mathfrak{m}_R$, which is well-defined as the formal series converges. This induces a canonical G_K-equivariant $\mathbb{Q}$-algebra map $\operatorname{Sym}_{\mathbb{Q}}(R^\times) \to B^+_{\mathrm{cris}}$. With a choice of variable, $\operatorname{Sym}_{\mathbb{Q}}(\operatorname{Frac}(R)^\times)$ is a 1-variable polynomial ring over $\operatorname{Sym}_{\mathbb{Q}}(R^\times)$.

Definition 2.2.16 (Semi-stable Period Ring)**.** *Let $B_{\mathrm{st}}^+ := \mathrm{Sym}_{\mathbb{Q}}(\mathrm{Frac}(R)^\times) \otimes_{\mathrm{Sym}_{\mathbb{Q}}(R^\times)} B_{\mathrm{cris}}^+$ with the induced G_K-action. Let $\lambda_{\mathrm{st}}^+ : \mathrm{Frac}(R)^\times \to B_{\mathrm{st}}^+$ be the canonical G_K-equivariant homomorphism $h \mapsto h \otimes 1$. We define φ on B_{st}^+ to extend φ on B_{cris}^+ and $\varphi(\lambda_{\mathrm{st}}^+(x)) = p\lambda_{\mathrm{st}}^+(x)$. Define $B_{\mathrm{st}} = B_{\mathrm{st}}^+[1/t]$ with its evident G_K-action and Frobenius.*

As mentioned above, $B_{\mathrm{st}}^+ = B_{\mathrm{cris}}^+[X]$ and $B_{\mathrm{st}} = B_{\mathrm{cris}}[X]$ non-canonically, upon choosing $y \in \mathrm{Frac}(R)^\times - R^\times$ and setting $X = \lambda_{\mathrm{st}}^+(y)$. In this form, the Frobenius is

$$\varphi(\sum a_n X^n) = \sum \varphi(a_n) p^n X^n,$$

and the Galois action is

$$g(\sum a_n X^n) = \sum g(a_n)(X + c(g)t)^n,$$

where $c(g)$ is defined by $g(\widetilde{p}) = \widetilde{p}\varepsilon^{c(g)}$.

Note that we can also define the *monodromy operator* $N = -\frac{d}{dX}$ as in the non-canonical form. This in fact does not depend on the choice of X. Note that $N\phi = p\phi N$, and that N on B_{st} is G_K-equivariant.

Now it will be also nice if we can construct a filtration. Unfortunately, there is *no canonical filtration on* B_{st}, and the crucial reason behind this is that *there is no canonical embedding of* B_{st} *into* B_{dR}, unlike B_{cris}. This embedding depends upon the choice of G_K-equivariant logarithm $\log_{\overline{K}} : \overline{K}^\times \to \overline{K}$. It is well-defined on $1 + \mathfrak{m}_{\overline{K}}$ as well as Teichmüller lifts of $\overline{k}^\times$, but one can choose *any* $c \in K$ *so that* $\log_{\overline{K}}(p) = c$.

Given a logarithm, we construct a G_K-equivariant B_{cris}^+-algebra map $B_{\mathrm{st}}^+ \to B_{\mathrm{dR}}^+$ as follows. We need to construct a G_K-equivariant homomorphism $\mathrm{Frac}(R)^\times \to B_{\mathrm{dR}}^+$ whose restriction to $R^\times$ is the G_K-equivariant homomorphism $\lambda_{\mathrm{cris}} : x \mapsto \log_{\mathrm{cris}}([x]) \in A_{\mathrm{cris}}$, which is defined as usual to be zero for Teichmüller representatives of $\overline{K}^\times$ and the converging value of the formal series on $1 + \mathfrak{m}_R$. As every coset $\mathrm{Frac}(R)^\times / R^\times$ has a representative in $\overline{K}^\times$, for every $y \in \mathrm{Frac}(R)^\times$, one can find $y^{(0)} \in \overline{K}^\times$ such that $y/y^{(0)} \in R^\times$. Let $[y] \in (B_{\mathrm{dR}}^+)^\times$ be the Teichmüller representative of y. Then, using the canonical embedding $\overline{K} \hookrightarrow B_{\mathrm{dR}}^+$, $[y]/y^{(0)} \in B_{\mathrm{dR}}^+$, and it has a canonical value for logarithm. Thus, we define $\lambda : \mathrm{Frac}(R)^\times \to B_{\mathrm{dR}}^+$ to be

$$\lambda(y) = \log([y]/y^{(0)}) + \log_{\overline{K}}(y^{(0)}).$$

As $B_{\mathrm{st}}^+ = \mathrm{Sym}_{\mathbb{Q}}(\mathrm{Frac}(R)^\times) \otimes_{\mathrm{Sym}_{\mathbb{Q}}(R^\times)} B_{\mathrm{cris}}^+$, choice of λ gives a G_K-equivariant $B_{\mathrm{st}}^+ \to B_{\mathrm{dR}}^+$. It turns out that $K \otimes_{K_0} B_{\mathrm{st}}^+ \to B_{\mathrm{dR}}^+$ is *injective* regardless of choice of $\log_{\overline{K}}(p)$ ([BC, Theorem 9.2.10]), and thus we can give a non-canonical filtration on B_{st} as $\mathrm{Fil}^i B_{\mathrm{st}} = B_{\mathrm{st}} \cap \mathrm{Fil}^i B_{\mathrm{dR}}$ and similarly for B_{st}^+. It is conventional to use $\log_{\overline{K}}(p) = 0$.

Another must-check:

Proposition 2.2.19. *The ring B_{st} is $(\mathbb{Q}_p, G_K)$-regular.*

Proof. As we are given a G_K-equivariant injection $K \otimes_{K_0} B_{\mathrm{st}} \to B_{\mathrm{dR}}$, the inclusion $K_0 \subset B_{\mathrm{st}}^{G_K}$ is an equality.

To check the second condition, let $0 \neq b \in B_{\mathrm{st}}$ such that $\mathbb{Q}_p b$ is G_K-stable. We use the non-canonical expression of B_{st}. Write $b = b_0 + b_1 X + \cdots + b_r X^r$ with $b_r \neq 0$. Let $\eta : G_K \to \mathbb{Q}_p^\times$ be the character through which G_K acts on $\mathbb{Q}_p b$. Then,

$$g(b) = \eta(g) \sum_{i=0} b_i X^i = \sum_{i=0}^{r} g(b_i)(X + c(g)t)^i.$$

As $\eta(g)b_r = g(b_r)$, ψ is continuous. Also, $\mathbb{Q}_p b_r \subset B_{\mathrm{cris}}$ is G_K-stable, so $\psi = \chi^n\psi'$ for some unramified ψ'. Replacing b by bt^{-n}, we can assume that ψ is unramified. This implies that $b_r \in B_{\mathrm{cris}}^{I_K} = \widehat{K_0^{\mathrm{nr}}}$. Comparing coefficients of X^{r-1}, we have

$$\eta(g)b_{r-1} = g(b_{r-1}) + rg(b_r)c(g)t.$$

If $g \in I_K$, this becomes

$$b_{r-1} = g(b_{r-1}) + rb_rc(g)t,$$

or

$$\frac{b_{r-1}}{rb_r} - g\left(\frac{b_{r-1}}{rb_r}\right) = c(g)t.$$

Note that $g(X) - X = c(g)t$. Thus, this means that $X + \frac{b_{r-1}}{rb_r} \in B_{\mathrm{st}}^{I_K} = B_{\mathrm{cris}}^{I_K} \subset B_{\mathrm{cris}}$. But note that $X \notin B_{\mathrm{cris}}$ yet $\frac{b_{r-1}}{rb_r} \in B_{\mathrm{cris}}$, so unless $r = 0$, we have a contradiction. This means $b = b_0 \in B_{\mathrm{cris}}$. As B_{cris} is $(\mathbb{Q}_p, G_K)$-regular, b is invertible, as desired. □

We then define *semi-stable representations* to be B_{st}*-admissible representations.*

2.2.2.6 Filtered (φ, N)-modules

We now want to see the extra structures on the Dieudonné modules for crystalline and semi-stable representations. We throw a plenty of definitions, motivated from the concept of crystals, which will sum up to give us an algebraic description of the target category of $\mathbf{D}_{\mathrm{cris}}$ and $\mathbf{D}_{\mathrm{st}}$.

Definition 2.2.17 (Isocrystals)**.** *An* isocrystal *over K_0 is a finite-dimensional K_0-vector space D, equipped with a bijective Frobenius-semilinear endomorphism $\varphi_D : D \to D$ (*“Frobenius”*). Let the category of isocrystals be denoted as* $\mathrm{Mod}_{K_0}^{\varphi}$.

An important example of an isocrystal is the following.

Example 2.2.7. For any integers r, s with $r > 0$, we can define the isocrystal

$$D_{r,s} := \mathscr{D}_k[1/p]/\mathscr{D}_k[1/p](F^r - p^s),$$

where $\mathscr{D}_k$ is the Dieudonné ring (see Definition 1.2.4). A less tantalizing version is as a quotient of a polynomial ring,

$$D_{r,s} = K_0[\phi]/K_0[\phi](\phi^r - p^s),$$

where $\phi c = \varphi(c)\phi$ for $c \in K_0$.

We have a total classification of isocrystals over $\widehat{\mathbb{Q}_p^{\mathrm{nr}}}$.

Theorem 2.2.25 (Dieudonné-Manin Classification, [BC, Theorem 8.1.4])**.** *The category* $\mathrm{Mod}_{\widehat{\mathbb{Q}_p^{\mathrm{nr}}}}^{\varphi}$ *is semisimple, and the simple objects are $D_{\widehat{\mathbb{Q}_p^{\mathrm{nr}}},r,s}$ for $(r, s) = 1$.*

We will denote $D_{\widehat{\mathbb{Q}_p^{\mathrm{nr}}},r,s}$ by $\Delta_{\frac{s}{r}}$, as the *slope* $\frac{s}{r}$ is the most important invariant. An isocrystal is called *isoclinic* if it has only one slope, and let the *multiplicity* of an isoclinic object $D(\alpha)$ be the number of Δ_α's inside when base changed to $\widehat{\mathbb{Q}_p^{\mathrm{nr}}}$. In general, the Dieudonné-Manin classification gives us the *slope decomposition* $D = \oplus_{\alpha\in\mathbb{Q}} D(\alpha)$ of an isocrystal over K_0, where $D(\alpha)$ is isoclinic of slope α [BC]8.1.1. This can be seen via Galois descent; if $\widehat{D}$ is the base change of D to $\widehat{\mathbb{Q}_p^{\mathrm{nr}}}$, then the slope decomposition $\widehat{D} = \oplus \widehat{D}(\alpha)$ descends as $(\widehat{D}(\alpha))^{G_K/I_K} \otimes_{K_0} \widehat{\mathbb{Q}_p^{\mathrm{nr}}} \cong \widehat{D}(\alpha)$.

Given an isocrystal D, we can draw a *Newton polygon* as follows. Let $D = D(\alpha_0) \oplus \cdots \oplus D(\alpha_n)$ be the slope decomposition with $\alpha_0 < \alpha_1 < \cdots < \alpha_n$ with multiplicities $\mu_0, \cdots, \mu_n$. The Newton polygon $P_N(D)$ of D is the convex polygon starting at $(0, 0)$ and that the i-th segment has horizontal length μ_i and slope α_i. Let $t_N(D)$ be the *y-coordinate of the rightmost endpoint of* $P_N(D)$. As we know what Δ_α explicitly is, direct calculations give the following.

Proposition 2.2.20 [BC, §8.1]. *Let D, D' be isocrystals over K_0.*

(i) $t_N(D)$ is an integer.

(ii) If D and D' are isoclinic of slopes α, β, respectively, then $D \otimes_{K_0} D'$ is isoclinic of slope $\alpha + \beta$.

(iiii) $t_N(D \otimes_{K_0} D') = \dim_{K_0} D \cdot t_N(D') + t_N(D) \cdot \dim_{K_0} D'$.

(iv) $t_N(D) = t_N(\det D)$.

(v) $t_N(D^\vee) = -t_N(D)$.

(vi) If $0 \to D' \to D \to D'' \to 0$ is an exact sequence in $\mathrm{Mod}^{\varphi}_{K_0}$, then $t_N(D) = t_N(D') + t_N(D'')$.

Somewhat differently, we can associate a polygon to an object in $\mathrm{FilVect}_K$, the category of K-filtered vector spaces.

Definition 2.2.18 (Hodge Polygon). *Given $(D, \mathrm{Fil}^i D) \in \mathrm{FilVect}_K$, let $i_0 < i_1 < \cdots < i_n$ be the integers such that $\mathrm{gr}^i D \neq 0$. The* Hodge polygon *$P_H(D)$ of $(D, \mathrm{Fil}^i D)$ is the convex polygon starting from $(0, 0)$ and whose k-th segment has horizontal length $\dim_K \mathrm{gr}^{i_k} D$ and slope i_k. We denote $t_H(D)$ the y-coordinate of the rightmost endpoint of $P_H(D)$.*

A similar property holds for $P_H(D)$, and the verification is even easier.

Proposition 2.2.21. *Let $D, D' \in \mathrm{FilVect}_K$.*

(i) $t_H(D \otimes_K D') = \dim_K D \cdot t_H(D') + t_H(D) \cdot \dim_K D'$.

(ii) $t_H(D) = t_H(\det D)$.

(iii) $t_H(D^\vee) = -t_H(D)$.

(iv) If $0 \to D' \to D \to D'' \to 0$ is an exact sequence in $\mathrm{FilVect}_K$, then $t_H(D) = t_H(D') + t_H(D')$.

(v) If $D' \subset D$, then $P_H(D')$ completely lies above $P_H(D)$.

(vi) If $f : D' \to D$ is a morphism in $\mathrm{FilVect}_K$ which is an isomorphism as a morphism of K-vector spaces, then $t_H(D') \leq t_H(D)$. The equality holds if and only if f is an isomorphism in $\mathrm{FilVect}_K$.

Now we can define a target category of D_{cris} and D_{st}.

Definition 2.2.19 (Filtered φ-modules). *The category MF^{φ}_K of* filtered φ-modules *consists of triples $(D, \varphi_D, \mathrm{Fil}^i D_K)$ such that $(D, \varphi_D) \in \mathrm{Mod}^{\varphi}_{K_0}$ and $(D_K, \mathrm{Fil}^i D_K) \in \mathrm{FilVect}_K$. Morphiisms in the category are morphisms in the category $\mathrm{Mod}^{\varphi}_{K_0}$ such that the base change to K gives a morphism in $\mathrm{FilVect}_K$.*

Definition 2.2.20 (Filtered (φ, N)-modules). *The category $\mathrm{MF}^{\varphi,N}_K$ of* filtered (φ, N)-modules *consists of tuples $(D, \varphi_D, \mathrm{Fil}^i D_K, N_D)$ where $(D, \varphi_D, \mathrm{Fil}^i D_K) \in \mathrm{MF}^{\varphi}_K$, and $N_D : D \to D$ (*"monodromy"*) is a K_0-linear morphism such that $N_D\varphi_D = p\varphi_D N_D$. Morphisms in the category are morphisms in the category MF^{φ}_K which commute with N_D.*

The first thing to notice is that MF^{φ}_K can be embedded into $\mathrm{MF}^{\varphi,N}_K$, as $(D, \varphi, \mathrm{Fil}^i D_K) \in \mathrm{MF}^{\varphi}_K$ implies that $(D, \varphi, \mathrm{Fil}^i D_K, N_D = 0) \in \mathrm{MF}^{\varphi,N}_K$. Thus, most things we will prove for filtered (φ, N)-modules will be automatically true for filtered φ-modules. Also, even though MF^{φ}_K and $\mathrm{MF}^{\varphi,N}_K$ are not abelian categories, they are *pre-abelian categories*, as $\mathrm{Mod}^{\varphi}_{K_0}$ is an abelian category. In other words, one can think of kernels, cokernels, image, coimage, short exact sequences, tensor product and duals. Note that $N_{D\otimes D'} = N_D \otimes 1 + 1 \otimes N_D$ and $N_{D^\vee} = -N_D^\vee$.

The relation $N\varphi = p\varphi N$ gives us the slope filtration as follows.

Proposition 2.2.22. *Let $(D, \varphi_D, \mathrm{Fil}^i D_K, N_D) \in \mathrm{MF}^{\varphi,N}_K$. Let $D = \oplus D(\alpha)$ be the slope decomposition. Then, $\oplus_{\alpha \leq \alpha_0} D(\alpha)$ is N-stable for any $\alpha \in \mathbb{Q}$. Also, N_D is nilpotent.*

Proof. Note that $N(\Delta_{\frac{r}{s}}) \subset \Delta_{\frac{r}{s}-1}$, since by relation $N\phi = p\phi N$,

$$\phi^r Nv = p^{-r} N\phi^r v = p^{s-r} Nv.$$

Thus, $\oplus_{\alpha \leq \alpha_0} D(\alpha)$ is N-stable as well as N is nilpotent. □

We need a lemma to explain the essential image of $D_{\text{cris}}, D_{\text{st}}$.

Lemma 2.2.3. *Let $D \in \mathrm{MF}_K^{\varphi,N}$. Then, the following two statements are equivalent.*

(i) For all subobjects $D' \subset D$ in $\mathrm{MF}_K^{\varphi,N}$, the Netwon polygon $P_N(D')$ lies completely over the Hodge polygon $P_H(D')$.

(ii) For all subobjects $D' \subset D$ in $\mathrm{MF}_K^{\varphi,N}$, we have $t_N(D') \geq t_H(D')$.

The same is true for MF_K^{φ}.

Proof. As $\mathrm{MF}_K^{\varphi} \hookrightarrow \mathrm{MF}_K^{\varphi,N}$ by setting $N = 0$, we only need to prove for filtered (φ, N)-modules. Also, the first statement obviously implies the second. Thus, we now assume that the second statement is true and try to prove the first statement.

Suppose that there is some subobject $D' \subset D$ such that $P_N(D')$ does not sit above $P_H(D')$. As $t_N(D') \geq t_H(D')$, there is some vertex $(x, P_N(D')(x))$ of $P_N(D')$ that lies below $P_H(D')$. Let α_0 be the slope of the segment to the left of this vertex. Let $D'' = \oplus_{\alpha \leq \alpha_0} D'(\alpha)$. This is a subobject of D, so $t_N(D'') \geq t_H(D'')$. Thus,

$$t_H(D'') = P_H(D'')(x) \geq P_H(D')(x) > P_N(D')(x) = t_N(D''),$$

which is a contradiction. □

Definition 2.2.21 (Weakly Admissible Modules)**.** *An object in $D \in \mathrm{MF}_K^{\varphi,N}$ (MF_K^{φ}, respectively) is* weakly admissible *if for all subobjects $D' \subset D$ in $\mathrm{MF}_K^{\varphi,N}$ (MF_K^{φ}, respectively), we have $t_N(D') \geq t_H(D')$, and the equality holds if and only if $D = D'$. Let the full subcategory of weakly admissible objects of $\mathrm{MF}_K^{\varphi,N}$ (MF_K^{φ}, respectively) be denoted as $\mathrm{MF}_K^{\varphi,N,\mathrm{wa}}$ ($\mathrm{MF}_K^{\varphi,\mathrm{wa}}$, respectively).*

By checking that all linear algebraic constructions behave well with weak admissibility condition, we can see that $\mathrm{MF}_K^{\varphi,N,\mathrm{wa}}$ and $\mathrm{MF}_K^{\varphi,\mathrm{wa}}$ are abelian categories [BC, Theorem 8.2.11].

As promised, these categories are the essential images of $\mathbf{D}_{\text{cris}}$ and $\mathbf{D}_{\text{st}}$.

Theorem 2.2.26 (Colmez-Fontaine, [BC, Theorem 9.2.14, Theorem 9.3.4])**.** *The functors $\mathbf{D}_{\text{cris}} : \mathrm{Rep}_{\text{cris}}(G_K) \to \mathrm{MF}_K^{\varphi}$ and $\mathbf{D}_{\text{st}} : \mathrm{Rep}_{\text{st}}(G_K) \to \mathrm{MF}_K^{\varphi,N}$ are fully faithful, and they have essential image $\mathrm{MF}_K^{\varphi,\mathrm{wa}}$ and $\mathrm{MF}_K^{\varphi,N,\mathrm{wa}}$, respectively. In other words, those functors are equivalence of categories between $\mathrm{Rep}_{\text{cris}}(G_K)$ and $\mathrm{MF}_K^{\varphi,\mathrm{wa}}$, and between $\mathrm{Rep}_{\text{st}}(G_K)$ and $\mathrm{MF}_K^{\varphi,N,\mathrm{wa}}$. The quasi-inverses are given as*

$$\mathbf{V}_{\text{cris}}(D) := \mathrm{Fil}^0(B_{\text{cris}} \otimes_{K_0} D)^{\varphi=1}, \quad \mathbf{V}_{\text{st}}(D) := \mathrm{Fil}^0(B_{\text{st}} \otimes_{K_0} D)^{\varphi=1,N=0}.$$

2.2.2.7 Étale φ-modules

We so far have examined problems over a local field of mixed characteristic. On the other hand, there is a very similar story for equal characteristic fields. The analogy between those two cases is one of the central themes in number theory. As there are ways to translate a result in one case to another, it is worthwile to briefly cover the problem of classifying p-adic representations of G_E for a field of charcateristic $p > 0$. In this section, we let E be a field of characteristic $p > 0$, although the theory is geared towards the case when E is an equal characteristic local field.

As one case motivates another, in this equal characteristic case, we can expect to classify representations in terms of a similar period ring formalism. It turns out that the "period ring" for the analogue of Hodge-Tate represenatations is E_s, the separable closure of E.

Definition 2.2.22 (Étale φ-modules over E)**.** *A* φ-module over E *is a pair* (M_0, φ_{M_0}) *where* M_0 *is a finite-dimensional* E*-vector space and* $\varphi_{M_0} : M_0 \to M_0$ *is a* φ_E*-semilinear endomorphism. It is an* étale φ-module *if the* E*-linearization* $E \otimes_{\varphi,E} M_0 \xrightarrow{c\otimes m\mapsto c\varphi_{M_0}(m)} M_0$ *is an isomorphism. This is equivalent to that* $\varphi_{M_0}(M_0)$ *spans* M_0 *over* E*. The category of étale* φ*-modules over* E*, denoted as* $\Phi M_E^{\text{ét}}$*, where the morphisms are* E*-linear morphisms respecting Frobenius structures.*

Lemma 2.2.4 [BC, Lemma 3.1.3]**.** *The category* $\Phi M_E^{\text{ét}}$ *is abelian.*

Proof. Given a morphism $h : M \to M'$ in $\Phi M_E^{\text{ét}}$, then we have a commutative diagram

$$\begin{array}{ccc} \varphi_E^*(M') & \xrightarrow{\varphi_E^*(h)} & \varphi_E^*(M) \\ \cong\downarrow & & \downarrow\cong \\ M' & \xrightarrow[h]{} & M \end{array}$$

and this induces the corresponding isomorphisms between kernels, cokernels, images and coimages, and as such formations coommute with ground field extension, by taking a base change to $\varphi_E : E \to E$, we get the étaleness of kernels, cokernels, images and coimages. Images and coimages coincide as they do in the category of E-vector spaces. □

Remember that the "period ring" in this case is E_s. Thus it is natural to define a Dieudonné functor as follows.

Definition 2.2.23. *For* $V_0 \in \mathrm{Rep}_{\mathbb{F}_p}(G_E)$*, a mod* p *representation of* G_E*, define* $\mathbf{D}_E(V_0) = (E_s \otimes_{\mathbb{F}_p} V_0)^{G_E}$ *as an* E*-vector space, equipped with the* φ_E*-semilinear endomorphism* $\varphi_{\mathbf{D}_E(V_0)} = \varphi_{E_s} \otimes 1$*.*

Conversely, for any $M_0 \in \Phi M_E^{\text{ét}}$*, we define* $\mathbf{V}_E(M_0) = (E_s \otimes_E M_0)^{\varphi=1}$*, where* $\varphi = \varphi_{E_s} \otimes \varphi_{M_0}$*.*

It is just a linear algebra to check the following.

Proposition 2.2.23 [BC, Theorem 3.1.8]**.** *The functors* $\mathbf{D}_E : \mathrm{Rep}_{\mathbb{F}_p}(G_E) \to \Phi M_E^{\text{ét}}$ *and* $\mathbf{V}_E : \Phi M_E^{\text{ét}} \to \mathrm{Rep}_{\mathbb{F}_p}(G_E)$ *are rank-preserving quasi-inverse equivalences of categories, compatible with tensor products and duality.*

To improve this to $\mathrm{Rep}_{\mathbb{Z}_p}(G_E)$, the category of continuous G_E-representations on finitely generated $\mathbb{Z}_p$-modules, we would like to lift E-coefficients to some characteristic zero ring with Frobenius, so we would hope to have something like "$W(E)$", which is again not a good idea as E is imperfect. Thus, from now on, we assume that we are already *given a complete discrete valuation ring* $\mathcal{O}_{\mathcal{E}}$ *of charcateristic* 0*, uniformizer* p*, residue field* E*, and a Frobenius* $\varphi : \mathcal{O}_{\mathcal{E}} \to \mathcal{O}_{\mathcal{E}}$. We let $\mathcal{E} = \mathcal{O}_{\mathcal{E}}[1/p]$.

Example 2.2.8. For example, in our main case $E = k((u))$, $\mathcal{O}_{\mathcal{E}}$ can be set to be the p-adic completion of the Laurent series ring $W(k)((u))$ over $W(k)$.

Since $\mathcal{O}_{\mathcal{E}}$ is a complete discrete valuation ring, the ring of integers $\mathcal{O}_{\mathcal{E}^{\text{nr}}}$ of the maximal unramified extension $\mathcal{E}^{\text{nr}}$ of $\mathcal{E}$ is unique up to unique isomorphism[3]. In particular, given a local map $f : \mathcal{O}_{\mathcal{E}} \to \mathcal{O}_{\mathcal{E}}$ with a specified lifting $\overline{f'} : E_s \to E_s$ of a reduction $\overline{f} : E \to E$, we get a

[3]More concise way to see this is that $\mathcal{O}_{\mathcal{E}^{\text{nr}}}$ is a strict henselization of $\mathcal{O}_{\mathcal{E}}$.

unique local map $f' : \mathcal{O}_{\mathcal{E}^{\mathrm{nr}}} \to \mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}$. Applying this to $f = \varphi$ and $\overline{f'} = \varphi_{E_s}$, we get a unique local endomorphiism of $\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}$, which will also be denoted by φ. As the formation of this lift is unique up to unique isomorphism, we get an induced action of G_E on $\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}$. Thus, we can define the same notion of *étale φ-modules over $\mathcal{O}_{\mathcal{E}}$.*

Definition 2.2.24 (Étale φ-modules over $\mathcal{O}_{\mathcal{E}}$)**.** *The category $\Phi M^{\text{ét}}_{\mathcal{O}_{\mathcal{E}}}$ of étale φ-modules over $\mathcal{O}_{\mathcal{E}}$ consists of pairs $(\mathscr{M}, \varphi_{\mathscr{M}})$ where $\mathscr{M}$ is a finitely generated $\mathcal{O}_{\mathcal{E}}$-module and $\varphi_{\mathscr{M}}$ is a φ-semilinear endomorphism of $\mathscr{M}$ whose $\mathcal{O}_{\mathcal{E}}$-linearization $\varphi^*(\mathscr{M}) \to \mathscr{M}$ is an isomorphism.*

Proposition 2.2.24 [BC, Lemma 3.2.3]**.** *The category $\Phi M^{\text{ét}}_{\mathcal{O}_{\mathcal{E}}}$ is abelian.*

Clearly, $\Phi M^{\text{ét}}_{E}$ is the full subcategory of p-torsion objects in $\Phi M^{\text{ét}}_{\mathcal{O}_{\mathcal{E}}}$. In this integral case, the period ring should be "$\widehat{\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}}$, the p-adic completion of $\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}$; similarly, for $\mathbb{Q}_p$-representations of G_E, the period ring should be "$\widehat{\mathcal{E}^{\mathrm{nr}}}$." Indeed, as with other period rings, these rings satisfy the following basic structures.

- $\widehat{\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}}^{G_E} \cong \mathcal{O}_{\mathcal{E}}$.
- $(\widehat{\mathcal{E}^{\mathrm{nr}}})^{G_E} \cong \mathcal{E}$.
- $(\widehat{\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}})^{\varphi=1} = \mathbb{Z}_p$.
- $(\widehat{\mathcal{E}^{\mathrm{nr}}})^{\varphi=1} = \mathbb{Q}_p$.

Theorem 2.2.27 [BC, Theorem 3.2.5, Theorem 3.3.4]**.** *There is an equivalence of categories between $\mathrm{Rep}_{\mathbb{Z}_p}(G_E)$ ($\mathrm{Rep}_{\mathbb{Q}_p}(G_E)$, respectively) and $\Phi M^{\text{ét}}_{\mathcal{O}_{\mathcal{E}}}$ ($\Phi M^{\text{ét}}_{\mathcal{E}}$, respectively) via period rings $\widehat{\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}}$ ($\widehat{\mathcal{E}^{\mathrm{nr}}}$, respectively). To be more precise, there are covariant naturally quasi-inverse equivalences of abelian categories*

$$\mathbf{D}_{\mathcal{O}_{\mathcal{E}}} : \mathrm{Rep}_{\mathbb{Z}_p}(G_E) \to \Phi M^{\text{ét}}_{\mathcal{O}_{\mathcal{E}}}, \mathbf{V}_{\mathcal{O}_{\mathcal{E}}} : \Phi M^{\text{ét}}_{\mathcal{O}_{\mathcal{E}}} \to \mathrm{Rep}_{\mathbb{Z}_p}(G_E),$$

$$\mathbf{D}_{\mathcal{E}} : \mathrm{Rep}_{\mathbb{Q}_p}(G_E) \to \Phi M^{\text{ét}}_{\mathcal{E}}, \mathbf{V}_{\mathcal{E}} : \Phi M^{\text{ét}}_{\mathcal{E}} \to \mathrm{Rep}_{\mathbb{Q}_p}(G_E),$$

defined by

$$\mathbf{D}_{\mathcal{O}_{\mathcal{E}}}(V) = \left(\widehat{\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}} \otimes_{\mathbb{Z}_p} V\right)^{G_E}, \mathbf{V}_{\mathcal{O}_{\mathcal{E}}}(M) = \left(\widehat{\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}} \otimes_{\mathcal{O}_{\mathcal{E}}} M\right)^{\varphi=1},$$

$$\mathbf{D}_{\mathcal{E}}(V) = \left(\widehat{\mathcal{E}^{\mathrm{nr}}} \otimes_{\mathbb{Q}_p} V\right)^{G_E}, \mathbf{V}_{\mathcal{E}}(M) = \left(\widehat{\mathcal{E}^{\mathrm{nr}}} \otimes_{\mathcal{E}} M\right)^{\varphi=1}.$$

These functors preserve rank and invariant fanctors, and are compatible with tensor products and duality.

Although we will not use this theory directly, the étale φ-modules for G_E is highly motivating for the analogous development in integral p-adic Hodge theory, e.g. see Section 2.2.3.3.

2.2.2.8 Comparison Theorems I: Generalities, de Rham Cohomology

Recall the statement of the Hodge-Tate decomposition.

Theorem 2.2.21 (Hodge-Tate Decomposition, cf. [BC, Theorem 2.2.3])**.** *Let K be a p-adic field, and X be a smooth proper K-scheme. Then, there is a canonical isomorphism*

$$\mathbb{C}_K \otimes_{\mathbb{Q}_p} H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) \cong \bigoplus_q (\mathbb{C}_K(-q) \otimes_K H^{n-q}(X, \Omega^q_{X/K}))$$

in $\mathrm{Rep}_{\mathbb{C}_K}(G_K)$, where the cohomology on the right side is a sheaf cohomology, and the action of $g \in G_K$ on both sides are $g \otimes g$ on the left and $g \otimes 1$ on the right.

A more concise way to say this is that $H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ is Hodge-Tate, and that $\mathbf{D}_{\text{HT}}(H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)) = H^n_{\text{Hodge}}(X/K) := \oplus_{p+q=n} H^p(X, \Omega^q_{X/K})$. The general philosophy of *comparison theorems* is the following.

- Let K be a p-adic field. For each period ring B, there is a class of smooth proper[4] varieties over K whose p-adic étale cohomology $H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ is B-admissible.
- There is some appropriate cohomology theory H_B applicable to those varieties, so that $\mathbf{D}_B(H^n_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p))$ is canonically isomorphic to "$H^n_B(X)$." The cohomology $H^n_B(X)$ has all structures that the Dieudonné modules of B-admissible representation should have (e.g. Frobenius, filtration, monodromy).

As we are in an advanced world, we already know all of the answers.

- B_{dR}. *All smooth proper varieties* have de Rham p-adic étale cohomology. The Dieudonné module is the *algebraic de Rham cohomology*, which has a natural filtration.
- B_{cris}. *Smooth proper varieties with a smooth proper model over* $\mathcal{O}_K$ have crystalline p-adic étale cohomology. The Dieudonné module is the *crystalline cohomology*, which has a natural filtration and Frobenius.
- B_{st}. *Smooth proper varieties with a proper semi-stable model over* $\mathcal{O}_K$ have semi-stable p-adic étale cohomology. The Dieudonné module is the *log-crystalline cohomology*, which has a filtration, Frobenius and monodromy operator.
- All proper smooth varieties have potentially semi-stable p-adic étale cohomology. This is because de Rham representations are potentially semi-stable, by Berger-André-Kedlaya-Mebkhout [Be, Théorème 0.7].

As they were all originally conjectures, we will call those comparison theorems as C_{HT}, C_{dR}, C_{cris}, C_{st}. We will shortly see that C_{st} implies C_{cris} implies C_{dR} implies C_{HT}. For our applications, we will not explicitly use neither crystalline cohomology nor log-crystalline cohomology. Thus, those cohomologies will only be reviewed very briefly.

As C_{dR} is the next thing to study, we will review the construction of (algebraic) de Rham cohomology. Let X be a variety over a field k. Note that we have a complex of sheaves

$$0 \to \mathcal{O}_X \xrightarrow{d} \Omega^1_{X/k} \xrightarrow{d} \Omega^2_{X/k} \xrightarrow{d} \cdots,$$

and this is indeed a complex as formally $d^2 = 0$. We define the *algebraic de Rham cohomology*

$$H^i_{\text{dR}}(X/k) = \mathbb{H}^i(\Omega^\bullet_{X/k}),$$

the *hypercohomology* of $\Omega^\bullet_{X/k}$. Recall that the hypercohomology can be computed by embedding the complex into an *injective resolution of the complex*, i.e. there exist injective sheaves $\mathcal{I}^{i,j}$ for

[4]We require this to make sure that the étale cohomologies are finite-dimensional, see Section 2.2.1.6.

$i \geq 0, j \geq 1$ such that they fit into a commutative diagram

$$\begin{array}{ccccccc}
\cdots & & \cdots & & \cdots & & \\
\uparrow & & \uparrow & & \uparrow & & \\
\mathcal{I}^{0,1} & \longrightarrow & \mathcal{I}^{1,1} & \longrightarrow & \mathcal{I}^{2,1} & \longrightarrow & \cdots \\
\uparrow & & \uparrow & & \uparrow & & \\
\mathcal{I}^{0,0} & \longrightarrow & \mathcal{I}^{1,0} & \longrightarrow & \mathcal{I}^{2,0} & \longrightarrow & \cdots \\
\uparrow & & \uparrow & & \uparrow & & \\
\mathcal{O}_X & \longrightarrow & \Omega^1_{X/k} & \longrightarrow & \Omega^2_{X/k} & \longrightarrow & \cdots \\
\uparrow & & \uparrow & & \uparrow & & \\
0 & & 0 & & 0 & &
\end{array}$$

where the vertical complexes are exact. Then the hypercohomology can be computed as the cohomology of the total complex of the above double complex minus the bottom row, the row containing the original complex. It is a pure algebra (cf. [McC, Theorem 2.15])that, given a cohomological double complex $C^{i,j}$, there is a convergent spectral sequence whose E_1-page is

$$\begin{array}{ccccccc}
\cdots & & \cdots & & \cdots & & \\
h^2(C^{0,\bullet}) & \longrightarrow & h^2(C^{1,\bullet}) & \longrightarrow & h^2(C^{2,\bullet}) & \longrightarrow & \cdots \\
h^1(C^{0,\bullet}) & \longrightarrow & h^1(C^{1,\bullet}) & \longrightarrow & h^1(C^{2,\bullet}) & \longrightarrow & \cdots \\
h^0(C^{0,\bullet}) & \longrightarrow & h^0(C^{1,\bullet}) & \longrightarrow & h^0(C^{2,\bullet}) & \longrightarrow & \cdots
\end{array}$$

Applying this, we have a spectral sequence converging to $E^n_\infty = H^n_{\mathrm{dR}}(X/k)$ whose E_1-page is

$$\begin{array}{ccccccc}
\cdots & & \cdots & & \cdots & & \cdots \\
H^2(X, \mathcal{O}_X) & \longrightarrow & H^2(X, \Omega^1_{X/k}) & \longrightarrow & H^2(X, \Omega^2_{X/k}) & \longrightarrow & \cdots \\
H^1(X, \mathcal{O}_X) & \longrightarrow & H^1(X, \Omega^1_{X/k}) & \longrightarrow & H^1(X, \Omega^2_{X/k}) & \longrightarrow & \cdots \\
H^0(X, \mathcal{O}_X) & \longrightarrow & H^0(X, \Omega^1_{X/k}) & \longrightarrow & H^0(X, \Omega^2_{X/k}) & \longrightarrow & \cdots
\end{array}$$

which means that we have the *Hodge-de Rham spectral sequence*

$$E_1^{p,q} = H^p(X, \Omega^q_{X/k}) \Rightarrow E_\infty^{p+q} = H^{p+q}_{\mathrm{dR}}(X/k).$$

Theorem 2.2.28 (Deligne, [Del, Théor'eme 5.5])**.** *If* $\operatorname{char} k = 0$ *and* X *is proper, then the Hodge-de Rham spectral sequence degenerates at* E^1*.*

This implies that the de Rham cohomology has a *Hodge filtration* $\mathrm{Fil}^i H^n_{\mathrm{dR}}(X/k)$ such that

$$\mathrm{Fil}^{i+1} H^n_{\mathrm{dR}}(X/k)/\mathrm{Fil}^i H^n_{\mathrm{dR}}(X/k) = H^i(X, \Omega^{n-i}_{X/k}).$$

We can now formulate the de Rham comparison theorem by Faltings.

Theorem 2.2.29 (C_{dR})**.** *Let K be a p-adic field, and let X be a smooth proper variety over K. Then, $H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ is, as a p-adic G_K-representation, de Rham, and $\mathbf{D}_{\mathrm{dR}}(H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p))$ is canonically isomorphic to $H^m_{\mathrm{dR}}(X/K)$ which respects Galois action and filtrations. In other words, we have a canonical isomorphism*

$$B_{\mathrm{dR}} \otimes_{\mathbb{Q}_p} H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) \cong B_{\mathrm{dR}} \otimes_K H^m_{\mathrm{dR}}(X/K),$$

which respects Galois action and filtrations.

- *A Galois element $g \in G_K$ acts by $g \otimes g$ on the left hand side and by $g \otimes 1$ on the right hand side.*
- *The filtration on the left hand side is $\mathrm{Fil}^i \otimes H^m_{\text{ét}}$ whereas the filtration on the right hand side is $\mathrm{Fil}^i = \sum_{i=j+k} \mathrm{Fil}^j \otimes \mathrm{Fil}^k$.*

If we take the graded quotient of the de Rham comparison isomorphism, we get Galois-equivariant isomorphism

$$\mathbb{C}_K(n) \otimes_{\mathbb{Q}_p} H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) \cong \oplus_{n=a+b} \mathbb{C}_K(a) \otimes H^b(X, \Omega^{m-a}_{X/K}),$$

or after Tate twist

$$\mathbb{C}_K \otimes_{\mathbb{Q}_p} H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) \cong \oplus_b \mathbb{C}_K(-b) \otimes H^b(X, \Omega^{m-a}_{X/K}),$$

which is C_{HT}.

2.2.2.9 Comparison Theorems II: Crystalline and Semi-stable Conjectures

We now very briefly describe how to construct the crystalline cohomology.

Definition 2.2.25 (PD structure)**.** *For an ideal $I \subset A$, a* PD structure *over I is a collection of maps $\gamma_n : I \to A$ for $n \geq 0$ such that $\gamma_n(x)$ "behaves like $\frac{x^n}{n!}$," i.e. it satisfies the following axioms.*

- $\gamma_0(x) = 1$, $\gamma_1(x) = x$ *for every* $x \in I$.
- $\gamma_n(x) \in I$ *if* $n \geq 1$.
- $\gamma_n(x + y) = \sum_{i+j=n} \gamma_i(x)\gamma_j(y)$.
- $\gamma_n(\lambda x) = \lambda^n \gamma_n(x)$ *for* $\lambda \in A$.
- $\gamma_n(x)\gamma_m(x) = \binom{n+m}{n}\gamma_{m+n}(x)$.
- $\gamma_m(\gamma_n(x)) = \frac{(mn)!}{m!(n!)^m}\gamma_{mn}(x)$.

Example 2.2.9. For a perfect field k of characteristic $p > 0$, the ideal $(p) \subset W(k)$ has a PD structure, simply because $\frac{p^n}{n!}$ always has p-adic valuation ≥ 0.

Definition 2.2.26 (Crystalline Site, Crystalline Cohomology). *Let k be a perfect field of characteristic $p > 0$, and X be a k-scheme. Let $W_n = W_n(k) = W(k)/p^n$ be the ring of n-truncated Witt vectors. We define the* crystalline site $(X/W_n)_{\text{cris}}$ *as follows.*

- *The objects of the underlying category are commutative diagrams*

$$\begin{array}{ccc} U & \overset{i}{\hookrightarrow} & V \\ \downarrow & & \downarrow \\ \operatorname{Spec} k & \longrightarrow & \operatorname{Spec} W_n \end{array}$$

  where $U \subset X$ is a Zariski open subsets and i is a closed immersion of W_n-schemes such that the ideal $\ker(\mathcal{O}_V \to \mathcal{O}_U)$ *is endowed with a* PD structure δ*, compatible with the* canonical PD structure on $pW_n \subset W_n$*. We denote an object by (U, V, δ).*

- *The morphisms of the underlying category are $(U, V, \delta) \to (U', V', \delta')$ such that $U' \hookrightarrow U'$ is an open immersion and $V \to V'$ is a morphism compatible with PD structures.*

- *The coverings are families of morphisms $\{(U_i, V_i, \delta_i) \to (U, V, \delta)\}$ such that $\{V_i \to V\}$ is a topological covering consisted of open immersions.*

The structure sheaf $\mathcal{O}_{X/W_n}$ *is given by*

$$(U, V, \delta) \mapsto \mathcal{O}_V.$$

The crystalline cohomology $H^i_{\text{cris}}(X/W)$ *is defined by*

$$H^i_{\text{cris}}(X/W_n) := H^i((X/W_n)_{\text{cris}}, \mathcal{O}_{X/W_n}),$$

and

$$H^i_{\text{cris}}(X/W) := \varprojlim_n H^i_{\text{cris}}(X/W_n).$$

Note that it has an obvious Frobenius structure as well as Galois action, since $H^m_{\text{cris}}(X/W)$ is functorial in X. The filtration comes from the *Berthelot-Ogus isomorphism.*

Theorem 2.2.30 (Berthelot-Ogus, [BO, Corollary 2.5]). *If Y is a smooth proper W-scheme and $K = \operatorname{Frac} W$, then there is a canonical isomorphism*

$$H^m_{\text{dR}}(Y_K/K) \cong K \otimes_W H^m_{\text{cris}}(Y/W).$$

Now we state the C_{cris} developed by many people including Fontaine-Messing, Kato, Tsuji.

Theorem 2.2.31 (C_{cris}). *Let K be a p-adic field, and X be a proper smooth variety over K such that it admits a proper smooth model $\mathcal{X}$ over $\mathcal{O}_K$, i.e. $(\mathcal{O}_X)_K = X$. Let k be the residue field, $W = W(k)$ and $K_0 = \operatorname{Frac} W$. Then, $H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ is, as a p-adic G_K-representation, crystalline, and $\mathbf{D}_{\text{cris}}(H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p))$ is canonically isomorphic to $H^m_{\text{cris}}(\mathcal{X}_k/W)$, respecting Galois action, filtrations and Frobenius. In other words, there is a canonical isomorphism*

$$B_{\text{cris}} \otimes_{\mathbb{Q}_p} H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) \cong B_{\text{cris}} \otimes_W H^m_{\text{cris}}(\mathcal{X}_k/W),$$

respecting Galois action, Frobenius and filtrations.

- *A Galois element $g \in G_K$ acts by $g \otimes g$ on the left hand side and by $g \otimes 1$ on the right hand side.*

- *The Frobenius endomorphism acts by* $\varphi \otimes 1$ *on the left hand side and by* $\varphi \otimes \varphi$ *on the right hand side.*

- *The filtration is given by* $\mathrm{Fil}^i = \mathrm{Fil}^i \otimes H^m_{\text{ét}}$ *on the left hand side and by* $\mathrm{Fil}^i = \sum_{i=j+k} \mathrm{Fil}^j \otimes \mathrm{Fil}^k$ *on the right hand side.*

By taking $B_{\mathrm{dR}} \otimes_{B_{\mathrm{cris}}} (\cdot)$ on the comparison isomorphism, we get B_{dR}. Also, in this case you can recover the whole p-adic étale cohomology from the crystalline and de Rham cohomology. Namely, taking G_K-invariants of the crystalline comparison isomorphism, we get

$$(B_{\mathrm{cris}} \otimes_{\mathbb{Q}_p} H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p))^{G_K} \cong K_0 \otimes_W H^m_{\mathrm{cris}}(\mathcal{X}_k/W).$$

By taking $\mathrm{Fil}^0(B_{\mathrm{dR}} \otimes_{B_{\mathrm{cris}}} (\cdot)) \cap (\cdot)^{\varphi=1}$, we get

$$H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) \cong \mathrm{Fil}^0(B_{\mathrm{dR}} \otimes_K H^m_{\mathrm{dR}}(X/K)) \cap (B_{\mathrm{cris}} \otimes_W H^m_{\mathrm{cris}}(\mathcal{X}_k/W))^{\varphi=1},$$

which is the *mysterious functor* conjectured by Grothendieck.

One can also define a *log-crystalline cohomology*, which we will not review. We will just state the semi-stable conjecture, C_{st}, which was settled through the help of many mathematicians, most notably Fontaine-Jannsen, Hyodo-Kato, Tsuji.

Theorem 2.2.32 (C_{st})**.** *Let K be a p-adic field, X be a proper smooth variety over K, admitting a proper semi-stable model $\mathcal{X}$ over $\mathcal{O}_K$, i.e. $\mathcal{X}_K = X$. In other words, $\mathcal{X}$ is regular, proper and flat over $\mathcal{O}_K$, and its special fiber $\mathcal{X}_k$ is a normal crossing divisor. Let $M_{\mathcal{X}_k}$ be the natural log-structure on $\mathcal{X}_k$. Then, $H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ is, as a p-adic G_K-representation, semi-stable, and $\mathbf{D}_{\mathrm{st}}(H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p))$ is canonically isomorphic to $H^m_{\text{log-cris}}((\mathcal{X}_k, M_{\mathcal{X}_k})/(W, \mathcal{O}_W^\times))$, respecting Galois action, Frobenius endomorphism and monodromy operator. Upon the choice of uniformizer, it is also compatible with filtrations, where the filtration on $H^m_{\text{log-cris}}((\mathcal{X}_k, M_{\mathcal{X}_k})/(W, \mathcal{O}_W^\times))$ is given by the Hyodo-Kato isomorphism*

$$K \otimes_W H^m_{\text{log-cris}}((\mathcal{X}_k, M_{\mathcal{X}_k})/(W, \mathcal{O}_W^\times)) \cong H^m_{\mathrm{dR}}(X/K),$$

which is also dependent on the choice of uniformizer.

In other words, there is a canonical isomorphism

$$B_{\mathrm{st}} \otimes_{\mathbb{Q}_p} H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p) \cong B_{\mathrm{st}} \otimes_W H^m_{\text{log-cris}}((\mathcal{X}_k, M_{\mathcal{X}_k})/(W, \mathcal{O}_W^\times)),$$

which is compattible with filtrations, Galois action, Frobenius endomorphism and monodromy operator.

- *A Galois element* $g \in G_K$ *acts by* $g \otimes g$ *on the left hand side and by* $g \otimes 1$ *on the right hand side.*

- *The Frobenius endomorphism acts by* $\varphi \otimes 1$ *on the left hand side, and by* $\varphi \otimes \varphi$ *on the right hand side.*

- *The monodromy operator acts by* $N \otimes 1$ *on the left hand side, and by* $N \otimes 1 + 1 \otimes N$ *on the right hand side.*

- *The filtrations are endowed by* $\mathrm{Fil}^i = \mathrm{Fil}^i \otimes H^m_{\text{ét}}$ *on the left hand side and by* $\mathrm{Fil}^i = \sum_{i=j+k} \mathrm{Fil}^j \otimes \mathrm{Fil}^k$ *on the right hand side.*

Note that we get C_{cris} from C_{st} by taking $(\cdot)^{N=0}$. Also, by taking G_K-invariant and then $\mathrm{Fil}^0(B_{\mathrm{dR}} \otimes_{B_{\mathrm{st}}} (\cdot)) \cap (\cdot)^{\varphi=1, N=0}$, we get a complete recovery of p-adic étale cohomology from de Rham and log-crystalline cohomology.

2.2.3 Integral p-adic Hodge Theory

2.2.3.1 Fontaine-Laffaille Theory

The theory of filtered (φ, N)-modules provides us an alternative of seeing crystalline and semi-stable representations using only semi-linear algebraic data. On the other hand, there are many reasons that one wants to develop such theory for *integral Galois representations*; one reason might be that the p-adic étale cohomology is constructed from an integral representation, not the other way around.

Let V be a crystalline G_{K_0}-representation; recall that $K_0 = W(k_K)[1/p]$. Let $D = \mathbf{D}_{\mathrm{cris}}(V)$, with a decreasing filtration $\mathrm{Fil}^i D$ and a φ-semilinear $\varphi : D \to D$. We would like to classify G_{K_0}-stable $\mathbb{Z}_p$-lattices of V, which morally should correspond to $W = W(k_K)$-lattices of D. Fontaine-Laffaile theory succeeds in solving this problem in a restricted setting by using ideas coming from crystalline cohomology. As the theory uses the idea of divided powers, it is quite inevitable that we need to restrict ourselves to those with nonpositive Hodge-Tate weights in $[-r, 0]$, where $er \leq p-1$; in particular, if one is interested in G_{K_0}-representations, the condition becomes $r \leq p-1$. Therefore, we lay an extra assumption on V that it is of Hodge-Tate weights in $[-(p-1), 0]$. Also, the integral versions of admissibility conditions for φ, D^i and M can be motivated from crystalline cohomology as well. Based on this discussion, we define the Fontaine-Laffaille modules as follows.

Definition 2.2.27 (Fontaine-Laffaille Modules)**.** *Let the notations be the same as above. A* Fontaine-Laffaille module *over W is a W-module M with an exhaustive and separating decreasing filtration* $\mathrm{Fil}^i M$ *(i.e. $\cup_i M^i = M$ and $\cap_i M^i = 0$) and a family of φ-semilinear maps*[5] *$\{\varphi^i_M : M^i \to M\}_{i\in\mathbb{Z}}$ which satisfies $p\varphi^{i+1}(x) = \varphi^i(x)$ for $x \in \mathrm{Fil}^i M$. A morphism of Fontaine-Laffaille modules are W-linear maps respecting filtrations and φ^i's. A sequence of Fontaine-Laffaille modules is exact if the underlying W-module sequence is exact and the sequence of the i-th filtrations is exact for all $i \in \mathbb{Z}$. We denote this category as MF_W.*

For any integers $a \leq b$, we denote by $\mathrm{MF}^{[a,b]}_W$ the full subcategory of MF_W consisting of M with $\mathrm{Fil}^a M = M$, $\mathrm{Fil}^{b+1} M = 0$. Another full subcategory $\mathrm{MF}_{W,tf}$ ($\mathrm{MF}^{[a,b]}_{W,tf}$, respectively) of MF_W is consisted of a W-module M (with $M \in \mathrm{MF}^{[a,b]}_W$, respectively) of finite length, with $\sum_{i\in\mathbb{Z}} \varphi^i(M^i) = M$.

It is very surprising that the category $\mathrm{MF}^{[a,b]}_{W,tf}$ is very nice.

Proposition 2.2.25 [BM, Proposition 3.1.1.1]**.** *Let $f : M \to N$ be a morphism in $\mathrm{MF}^{[a,b]}_{W,tf}$. Then, f is strict with respect to the filtration, i.e. for all i, $f(\mathrm{Fil}^i M) = \mathrm{Fil}^i N \cap f(M)$.*

Proof. For any $M \in \mathrm{MF}^{[a,b]}_W$, we define an injective map $\theta_M : \bigoplus_{j=a+1}^b \mathrm{Fil}^j M \to \bigoplus_{j=a}^b \mathrm{Fil}^j M$ by

$$(x_{a+1}, x_{a+2}, \cdots, x_b) \mapsto (x_{a+1}, -px_{a+1} + x_{a+2}, \cdots, -px_{b-1} + x_b, -px_b).$$

Let $\overline{M}$ be the cokernel of this map. Then, the map $\sum \varphi^j : \bigoplus_{j=a}^b \mathrm{Fil}^j M \to M$ induces a W-linear map $\psi_M : \overline{M} \to M$. This construction is functorial in M, and it is easity to check that $M \mapsto \overline{M}$ is exact and, if $\mathrm{lg}_W(M) < \infty$, we have $\mathrm{lg}_W(M) = \mathrm{lg}_W(\overline{M})$, where lg_W denotes the W-length. Such M is contained in $\mathrm{MF}^{[a,b]}_{W,tf}$ if and only if ψ_M is surjective, and by the length equality, if and only if ψ_M is injective or bijective.

Now we go back to the setting of the proposition. We first assume that f is injective, so that M is identified with a submodule of N. As ψ_M, ψ_N are isomorphisms, $\overline{M} \to \overline{N}$ is also

[5] Morally $\varphi^i =$"$\frac{\varphi}{p^i}$".

injective. Suppose that there is $x \in (\mathrm{Fil}^i N \cap M)\setminus \mathrm{Fil}^i M$. Take $j < i$ such that $x \in \mathrm{Fil}^j$ but $x \notin \mathrm{Fil}^{j+1} M$. As M, a finite length W-module, is of p-power torsion, we have $p^s x \notin M^{j+1}$ and $p^{s+1}x \in M^{j+1}$ for some integer $s \geq 0$. Replacing x by $p^s x$, we may assume $px \in M^{j+1}$. Now let $y = (0, \cdots, 0, x, -px, 0, \cdots, 0) \in \bigoplus_{k=a}^{b} \mathrm{Fil}^k M$, where x is at the j-th entry. Then $y \notin \mathrm{im}(\theta_M)$ whereas $y \in \mathrm{im}(\theta_N)$. Thus, the image of y in $\overline{M}$ is nonzero, whereas it is zero in $\overline{N}$. This contradicts with the injectivity of $\overline{M} \to \overline{N}$.

For a general f, we let $L = f(M)$ with $\mathrm{Fil}^i L := f(\mathrm{Fil}^i M)$. As $\ker(\mathrm{Fil}^i M \to \mathrm{Fil}^i L) = \ker f \cap \mathrm{Fil}^i M$ and f commutes with φ^i's, we get an induced map $\varphi^i_L : \mathrm{Fil}^i L \to L$ for every i. Note that L is automatically of finite W-length, and the commutative diagram

$$\begin{array}{ccc} \overline{M} & \longrightarrow & \overline{L} \\ \sim\big\downarrow & & \big\downarrow \psi_L \\ M & \twoheadrightarrow & L \end{array}$$

makes $\psi_L : \overline{L} \to L$ surjective. This eventually makes $L \in \mathrm{MF}^{[a,b]}_{W,tf}$. As $L \to N$ is an injection, we already know that it respects with filtrations, giving us $f(\mathrm{Fil}^i M) = f(M) \cap \mathrm{Fil}^i N$. □

This proof makes $\mathrm{MF}^{[a,b]}_{W,tf}$ an *abelian category*. More specifically, if $f : M \to N$ is a morphism in $\mathrm{MF}^{[a,b]}_{W,tf}$, the kernel is given by

$$(\ker f, (\ker f) \cap \mathrm{Fil}^i M, \varphi^i|_{(\ker f)\cap \mathrm{Fil}^i M}),$$

whereas the cokernel is given by

$$(\mathrm{coker}(f), \mathrm{Fil}^i N / f(\mathrm{Fil}^i M), \overline{\varphi^i_N}).$$

That $f(M) \cap \mathrm{Fil}^i N = f(\mathrm{Fil}^i M)$ is exactly encoding the fact that the coimage is equal to the image.

A hope is that $\mathrm{MF}^{[a,b]}_{W,tf}$ corresponds to *torsion crystalline representations*, i.e. subquotients of Galois-stable integral lattices inside a crystalline representation. To make this precise, we need a concept in the Dieudonné module side that corresponds to Galois-stable integral lattices, so that every object in $\mathrm{MF}^{[a,b]}_{W,tf}$ is a quotient of those objects.

Definition 2.2.28 (Strongly Divisible Module)**.** *A* strongly divisible module *is a free W-module M of finite type, equipped with a decreasing filtration of sub-W-modules* $(\mathrm{Fil}^i M)_{i\in\mathbb{Z}}$ *and a σ-semilinear map $\varphi : M \to M$, such that* $\mathrm{Fil}^{\ll 0} M = M$, $\mathrm{Fil}^{\gg 0} M = 0$, *$M/\mathrm{Fil}^i M$ has no p-torsion for all i, and $\varphi(\mathrm{Fil}^i M) \subset p^i M$ and $\sum_{i\in\mathbb{Z}} \frac{\varphi}{p^i}(\mathrm{Fil}^i M) = M$. Such module is of weights in $[a, b]$ if* $\mathrm{Fil}^a M = M$ *and* $\mathrm{Fil}^{b+1} M = 0$.

It is obvious that, if M is a strongly divisible module of weights in $[a, b]$, then $M/p^n M \in \mathrm{MF}^{[a,b]}_{W,tf}$ for any n by defining $\varphi_i = \frac{\varphi}{p^i}|_{\mathrm{Fil}^i}$.

The main theorem of the Fontaine-Laffaille theory is the following.

Theorem 2.2.33 [BM, Theorem 3.1.3.2]**.** *Let M be a strongly divisible module of rank d of weights in $[0, p-1]$. Then,* $\mathrm{Hom}(M, A_{\mathrm{cris}})$*, the group of W-linear maps respecting filtrations and φ's, is a $\mathbb{Z}_p$-lattice in a d-dimensional crystalline representation of G_{K_0} with Hodge-Tate weights in $[-(p-1), 0]$. Moreover, all such $\mathbb{Z}_p$-lattices arise in this way.*

By taking quotients, we get the following analogous result for torsion crystalline representations; note that we lose $r = p - 1$ case as we are literally requiring φ_i's to be divided powers.

Theorem 2.2.34 [BM, Theorem 3.1.3.3]. *Let $0 \le r \le p-2$. Define the functor $T^*_{\mathrm{cris}} : \mathrm{MF}^{[0,r]}_{W,tf} \to \mathrm{Rep}_{\mathrm{cris}}(G_K)$ as*

$$T^*_{\mathrm{cris}}(M) = \mathrm{Hom}(M, A_{\mathrm{cris}}/p^n A_{\mathrm{cris}}),$$

where n is chosen[6] *so that $p^n M = 0$, and the homomorphisms are W-linear maps respecting filtrations and φ's. Then, this functor is an anti-equivalence of categories between $\mathrm{MF}^{[0,r]}_{W,tf}$ and the category of torsion crystalline representations of G_{K_0} of Hodge-Tate weights in $[-r,0]$, i.e. finite representations of G_{K_0} which are subquotients of two integral G_{K_0}-stable lattices in crystalline representations of G_{K_0} with Hodge-Tate weights in $[-r,0]$.*

2.2.3.2 Breuil Modules

An immediate generalization of the theory of Fontaine-Laffaille modules is to generalize it to semi-stable representations; indeed, in terms of (φ, N)-modules, the only difference in classifying semi-stable representations is that there is an extra *monodromy operator*. Therefore, we can try to mimic the construction of (φ, N)-modules here, so that one is led to introduct a monodromy operator N on $\mathrm{MF}^{[0,r]}_{W,tf}$. The compatibility $N\varphi = p\varphi N$ from the (φ, N)-modules should translate into $N\varphi_i = \varphi_{i-1}N$, as φ_i's should be $\frac{\varphi}{p^i}$'s. On the other hand, this is applicable only when $N(\mathrm{Fil}^i) \subset \mathrm{Fil}^{i-1}$, which is called the *Griffiths transversality condition*. However, this is not really always the case, as there is no direct relation of N and filtration other than weak admissibility condition.

A way to resolve this, by Breuil in [Br1], is to work on a "PD-completed" ring instead of W so that we can actually obtain the Griffiths transversality. For simplicity, we work mostly for K_0. Define S to be the p-adic completion of

$$W\langle u\rangle = W[\frac{u^i}{i!}]_{i\in\mathbb{N}},$$

where u is an indeterminate. Choose a uniformizer π of W, and define $\mathrm{Fil}^i S, \varphi, N$ on S to be

$$\mathrm{Fil}^i S = \langle\{\frac{(u-\pi)^j}{j!}\}_{j\ge i}\rangle^\wedge,$$

$$\varphi(\sum_i w_i \frac{u^i}{i!}) = \sum \varphi(w_i)\frac{u^{p^i}}{i!},$$

$$N(\sum_i w_i \frac{u^i}{i!}) = \sum (-1)^i i w_i \frac{u^i}{i!},$$

where the completion is the p-adic completion, and $w_i \in W$. Note that we are really just requiring φ and N to satisfy $N(u) = -u$ and $\varphi(u) = u^p$, and that $\mathrm{Fil}^i S$ is the natural divided power filtration of S, which in particular does not depend on the choice of π. One checks that $N\varphi = p\varphi N$, $\varphi(\mathrm{Fil}^i S) \subset p^i S$, and most notably $N(\mathrm{Fil}^{i+1} S) \subset \mathrm{Fil}^i S$. We let $S_{K_0} = K_0 \otimes_W S$ to have the same kind of structures inherited from S. Surprisingly, it turns out that the functor $D \mapsto D \otimes_{K_0} S_{K_0}$ gives *an equivalence of categories from the category of positively filtered (φ, N)-modules in the usual sense to the category of positively filtered (φ, N)-modules over S_{K_0}*, which is the notion we will define now.

Definition 2.2.29. *Let $\mathcal{MF}^{\varphi,N,+}_{K_0}$ be the category of finitely generated free S_{K_0}-modules $\mathcal{D}$ equipped with $\mathrm{Fil}^i \mathcal{D}, \varphi, N$ such that the following hold.*

[6] It is clear that the definition of T^*_{cris} does not depend on the choice of n.

1. $\mathrm{Fil}^i D$ *is a descreasing filtration by sub-*S_{K_0}*-modules with* $\mathrm{Fil}^i \mathcal{D} = \mathcal{D}$, $\mathrm{Fil}^j S_{K_0} \cdot \mathrm{Fil}^i \mathcal{D} \subset \mathrm{Fil}^{j+i} \mathcal{D}$ *and, for* $i \gg 0$, $\mathrm{Fil}^i \mathcal{D} = \mathrm{Fil}^1 S_{K_0} \cdot \mathrm{Fil}^{i-1} \mathcal{D} + \mathrm{Fil}^i S_{K_0} \cdot \mathcal{D}$.
2. $\varphi : \mathcal{D} \to \mathcal{D}$ *is a* S_{K_0}*-semilinear map such that* $\det(\varphi) \in S_{K_0}^{\times}$.
3. $N : \mathcal{D} \to \mathcal{D}$ *is a* K_0*-linear map such that* $N(sx) = N(s)x + sN(x)$ *for* $s \in S_{K_0}, x \in \mathcal{D}$, $N\varphi = p\varphi N$ *and* $N(\mathrm{Fil}^i \mathcal{D}) \subset \mathrm{Fil}^{i-1} \mathcal{D}$.

The morphisms in this category are the S_{K_0}*-linear maps respecting the structures.*

Let $\mathrm{MF}_{K_0}^{\varphi,N}$ be the subcategory of filtered (φ, N) modules D with $\mathrm{Fil}^0 D = D$ ("positively filtered (φ, N)-modules"). Then, $D \mapsto D \otimes_{K_0} S_{K_0}$ is an *equivalence of categories* $\mathcal{MF}_{K_0}^{\varphi,N,+} \to \mathrm{MF}_{K_0}^{\varphi,N,+}$ in the following precise sense.

Theorem 2.2.35 [BM, Theorem 4.2.1]**.** *Let* π *be a uniformizer of* W*. Let* $f_\pi : S_{K_0} \to K_0$ *be defined by* $f_\pi(\sum_i w_i \frac{u^i}{i!}) = \sum_i w_i \frac{\pi^i}{i!}$*. Given a positively filtered* (φ, N)*-module* $D \in \mathrm{MF}_{K_0}^{\varphi,N,+}$*, we can endow a structure of* (φ, N)*-module on* $\mathcal{D} := D \otimes_{K_0} S_{K_0}$ *by the following.*

1. $\varphi_{\mathcal{D}} = \varphi_D \otimes_{K_0} \varphi_{S_{K_0}}$.
2. $N_{\mathcal{D}} = N_D \otimes_{K_0} \mathrm{id} + \mathrm{id} \otimes N_{S_{K_0}}$.
3. $\mathrm{Fil}^0 \mathcal{D}$*, and inductively* $\mathrm{Fil}^i \mathcal{D} = \{x \in \mathcal{D} \mid N(x) \in \mathrm{Fil}^{i-1} \mathcal{D}, f_\pi(x) \in \mathrm{Fil}^i D\}$.

Then, the above functor $D \mapsto D \otimes_{K_0} S_{K_0}$ *is an equivalence of categories* $\mathrm{MF}_{K_0}^{\varphi,N,+} \to \mathcal{MF}_{K_0}^{\varphi,N,+}$.

Thanks to this equivalence of categories, we can try to find integral structures inside $\mathcal{MF}_{K_0}^{\varphi,N,+}$, in which we also have the Griffiths transversality. In particular, we can try to define an analogue of $\mathrm{MF}_{W,tf}^{[0,r]}$ here, so that the new subcategory is also *abelian*. On the other hand, in this case we have a problem in lifting elements ([BM, Example 4.3.1]), so that we only keep track of the "last filtration" Fil^r. In view of this, we can define the analogue of $\mathrm{MF}_{W,tf}^{[0,r]}$ for $\mathcal{MF}_{K_0}^{\varphi,N,+}$.

Definition 2.2.30. *Let* $0 \leq r \leq p-2$*, and* π *be a uniformizer of* W*. The category* $\mathcal{MF}_{\pi}^{[0,r]}$ *is consisted of an* S*-module* $\mathcal{M}$ *abstractly isomorphic to* $\oplus_{i\in I}(S/p^i S)^{d_i}$*, where* I *is a finite set of integers and* $d_i \in \mathbb{N}$*. The extra data we keep track of are as follows.*

- *A sub-*S*-module* $\mathrm{Fil}^r \mathcal{M}$ *containing* $\mathrm{Fil}^r S \cdot \mathcal{M}$.
- *A* σ*-semilinear map* $\varphi_r : \mathrm{Fil}^r \mathcal{M} \to \mathcal{M}$ *such that* $\varphi_1(u-\pi)^r \varphi_r(sm) = \varphi_r(s)\varphi_r((u-\pi)^r m)$ *for* $s \in \mathrm{Fil}^r S$ *and* $x \in \mathcal{M}$*. Also,* $\varphi_r(\mathrm{Fil}^r \mathcal{M})$ *generates* $\mathcal{M}$ *over* S.
- *A map* $N : \mathcal{M} \to \mathcal{M}$ *such that* $N(sm) = N(s)m + sN(m)$ *for* $s \in S, m \in \mathcal{M}$.

The morphisms are S*-linear maps respecting these structures.*

We will see shortly that this definition does not depend on the choice of π. A similar dévissage argument as in the proof of Proposition 2.2.25 gives us the following analogous statements.

Proposition 2.2.26 [BM, Theorem 5.1.1.1]**.** *For a morphism* $f : \mathcal{M} \to \mathcal{N}$ *in* $\mathcal{MF}_{\pi}^{[0,r]}$, $f(\mathrm{Fil}^r \mathcal{M}) = \mathrm{Fil}^r \mathcal{N} \cap f(\mathcal{M})$*. In particular,* $\mathcal{MF}_{\pi}^{[0,r]}$ *is an abelian category.*

Note that our definition of $\mathcal{MF}_{\pi}^{[0,r]}$ does not make it to be a subcategory of $\mathcal{MF}_{K_0}^{\varphi,N,+}$, as we gave up tracking the whole filtration. We thus separately define a functor relating $\mathcal{MF}_{\pi}^{[0,r]}$ and $\mathrm{MF}_{W,tf}^{[0,r]}$.

Proposition 2.2.27 [BM, Proposition 5.1.1.3]. *Let $\mathcal{F}^r_\pi : \mathrm{MF}^{[0,r]}_{W,tf} \to \mathcal{MF}^{[0,r]}_\pi$ be functor sending $(M, \mathrm{Fil}^i M, \varphi_i)$ to the object $\mathcal{F}^r(M) = S \otimes_W M$ with the structure*

$$\mathrm{Fil}^r \mathcal{F}^r(M) = \sum_{j=0}^{r} \mathrm{Fil}^{r-j} S \otimes_W \mathrm{Fil}^j M,$$

$$\varphi_r = \sum_{j=0}^{r} \varphi_{r-j} \otimes \varphi_j,$$

$$N = N \otimes \mathrm{id}.$$

It is a fully faithful and exact functor which gives a one-to-one correspondence between the simple objects of $\mathrm{MF}^{[0,r]}_{W,tf}$ and $\mathcal{MF}^{[0,r]}_\pi$.

We can now see that $\mathcal{MF}^{[0,r]}_\pi$ does not depend on π.

Proposition 2.2.28 [BM, Proposition 5.1.1.5]. *For each choice $w \in W^*$, there is a canonical equivalence of categories $\mathcal{MF}^{[0,r]}_\pi \xrightarrow{\sim} \mathcal{MF}^{[0,r]}_{\pi w}$, such that via this equivalence $\mathcal{F}^r_\pi$ is identified with $\mathcal{F}^r_{\pi w}$.*

To get a similar equivalence of torsion semi-stable representations and $\mathcal{MF}^{[0,r]}_\pi$, we need an analogue of A_{cris} for this setting.

Definition 2.2.31. *The ring $\widehat{A_{\mathrm{st}}}$ is an S-algebra defined as the p-adic completion of $A_{\mathrm{cris}}\langle u\rangle = A_{\mathrm{cris}}[\{\frac{u^i}{i!}\}_{i\in\mathbb{N}}]$, with a Galois action, Frobenius φ, filtration $\mathrm{Fil}^i \widehat{A_{\mathrm{st}}}$ and monodromy N defined as follows.*

1. *The Galois action extends that of A_{cris}, and $g \in G_{K_0}$ acts on u via $g(u) = [\chi(g)]u + [\chi(g)] - 1$, where χ is the cyclotomic character and $[\chi(g)]$ is the corresponding Teichmüller element in A_{cris}.*
2. *φ extends that of A_{cris} and $\varphi(u) = (1+u)^p - 1$.*
3. *N extends that of A_{cris} and a continuous A_{cris}-derivation such that $N(u) = 1 + u$.*
4. *The filtration is defined as*

$$\mathrm{Fil}^i \widehat{A_{\mathrm{st}}} = \{\sum_{j=0}^{\infty} a_j \frac{u^j}{j!} \mid a_j \in \mathrm{Fil}^{i-j} A_{\mathrm{cris}}, a_j \to 0\}.$$

As with A_{cris}, we have $\varphi(\mathrm{Fil}^i \widehat{A_{\mathrm{st}}}) \subset p^i \widehat{A_{\mathrm{st}}}$ for $0 \le i \le p-1$, and we can define $\varphi_i = \frac{\varphi}{p^i}|_{\mathrm{Fil}^i}$ for such i.

All these structures extend obviously to $\widehat{A_{\mathrm{st}}}/p^n\widehat{A_{\mathrm{st}}}$ for all $n \ge 0$. Thus, we define a functor $T^*_{\mathrm{st}} : \mathcal{MF}^{[0,r]}_\pi \to \mathrm{Rep}(G_{K_0})$ as

$$T^*_{\mathrm{st}}(\mathcal{M}) = \mathrm{Hom}(\mathcal{M}, \widehat{A_{\mathrm{st}}}/p^n\widehat{A_{\mathrm{st}}}),$$

for $n \in \mathbb{N}$ with $p^n\mathcal{M} = 0$. The analogous main result is that this functor is fully faithful.

Theorem 2.2.36 [BM, Theorem 5.2.2.1]. *For $0 \le r \le p-2$, the functor T^*_{st} is exact and fully faithful. Its essential image contains the category of torsion semi-stable representations of G_{K_0} with Hodge-Tate weights in $[-r, 0]$.*

This is proven via first establishing an equivialence of integral structures with strongly divisible modules. Note that in this case we do not know the essential image of this functor. For our application, however, we just need torsion semi-stable representations can be recast in another form, so this will suffice.

2.2.3.3 Kisin Modules

The limitation $r < p-1$ for the Fontaine-Laffaille theory and the Breuil's theory is inevitable, as we were developing a theory using a divided power envelope. Another breakthrough on integral p-adic Hodge theory also started from Breuil by using a classification over $W[[u]]$, not $W\langle u\rangle$. This was subsequently extended by Kisin in [K], and in particular was able to *completely classify G_{K_∞}-stable $\mathbb{Z}_p$-lattices in semi-stable G_K-representations*, where $K_\infty = K(\pi^{1/p^\infty})$ for a K-uniformizer π. As we will observe, this theory is parallel to the theory of étale φ-modules via Fontaine-Wintenberger's theorem.

Let k be a perfect field of characteristic $p > 2$, $K_0 = W(k)[1/p]$, K/K_0 a finite totally ramified extension, $e = e(K/K_0)$ the absolute ramification index, $\pi \in K$ a uniformizer and $E(u)$ the corresponding Eisenstein polynomial over K_0. Define $\mathfrak{S} = W(k)[[u]]$, with Frobenius $\varphi : u \mapsto u^p$. A φ-module over $\mathfrak{S}$ is an $\mathfrak{S}$-module $\mathfrak{M}$ equipped with a φ-semilinear map $\varphi : \mathfrak{M} \to \mathfrak{M}$.

Definition 2.2.32 (Kisin Modules)**.** *The category* $\mathrm{Mod}^{\varphi}_{/\mathfrak{S}}$ *(*$\mathrm{Mod}^{\varphi,r}_{/\mathfrak{S}}$*, respectively), called the* category of φ-modules (of $E(u)$-height r, respectively)*, is a φ-module $\mathfrak{M}$ which is finite free over $\mathfrak{S}$ and the cokernel of $\varphi^* = 1 \otimes \varphi : \mathfrak{S} \otimes_{\varphi,\mathfrak{S}} \mathfrak{M} \to \mathfrak{M}$ is killed by some power of $E(u)$ ($E(u)^r$, respectively). An object in* $\mathrm{Mod}^{\varphi}_{/\mathfrak{S}}$ *(*$\mathrm{Mod}^{\varphi,r}_{/\mathfrak{S}}$*, respectively) is also called a* Kisin module (of height $\leq r$, respectively)*.*

This so far is very much the same as the theory of étale φ-modules. The new idea is that we can recast the whole picture inside $W(\operatorname{Frac} R)$, where $R = R(\mathcal{O}_{\mathbb{C}_K}/(p))$ as in the construction of B_{dR}.

Choose a compatible system of p^n-th roots of unity $\pi_n \in \overline{K}$, and let $[(\pi_n)] \in W(R)$ be the Teichmuller representative, corresponding to the choice of p^n-th roots of π. We can then embed $\mathfrak{S}$ into $W(R)$ so that $u \mapsto [(\pi_n)]$. It is easy to see that this embedding respects Frobenius structures, and is also G_{K_∞}-invariant, as G_{K_∞} is the isotropy subgroup of (π_n) in G_K. As $[(\pi_n)] \in \operatorname{Frac} R$ is nonzero, we can extend this embedding to $\mathfrak{S}[1/u] \hookrightarrow W(\operatorname{Frac} R)$. Let $\mathcal{O}_{\mathcal{E}}$ be the p-adic completion of $\mathfrak{S}[1/u]$. It is a discrete valuation ring with residue field $k((u))$. As p is a uniformizer of $W(\operatorname{Frac} R)$, we still maintain an embedding $\mathcal{O}_{\mathcal{E}} \hookrightarrow W(\operatorname{Frac} R)$ whose residue field homomorphism is $k((u)) \to \operatorname{Frac} R$ sending u to $[(\pi_n)]$. The embedding is still compatible with Frobenius structures, where $\varphi_{\mathcal{O}_{\mathcal{E}}}$ is induced by $\varphi_{\mathfrak{S}}$.

Let $\mathcal{E} = \operatorname{Frac}(\mathcal{O}_{\mathcal{E}})$, so that it embeds into $\mathcal{E} \hookrightarrow W(\operatorname{Frac} R)[1/p]$. Let $\mathcal{E}^{\mathrm{nr}}$ be the maximal unramified extension of $\mathcal{E}$ inside $W(\operatorname{Frac} R)[1/p]$. As $\operatorname{Frac} R$ is algebraically closed, Theorem 2.2.23, the residue field $\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}/p\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}$ of $\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}$ is the separable closure of $k((u))$. Let $\widehat{\mathcal{E}^{\mathrm{nr}}}$ be the closure of $\mathcal{E}^{\mathrm{nr}}$ in $W(\operatorname{Frac} R)[1/p]$, which is just the p-adic completion. The connection to the theory of étale φ-modules starts from the following, which uses the theory of field of norms.

Theorem 2.2.37 [BC, Theorem 11.1.2]**.** *The natural action of G_{K_∞} on $\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}$ via the inclusion $\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}} \hookrightarrow W(\operatorname{Frac} R)$ induces an isomorphism of topological groups $G_{K_\infty} \xrightarrow{\sim} G_{k((u))}$.*

In particular, we can see that the theory of étale φ-modules gives a classification of $\mathcal{O}_{\mathcal{E}}$-modules. Our objective is to adapt this theory to instead study $\mathfrak{S}$-modules. In place of $\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}$, let $\widehat{\mathfrak{S}^{\mathrm{nr}}} = \mathcal{O}_{\widehat{\mathcal{E}^{\mathrm{nr}}}} \cap W(R)$ and $\mathfrak{S}^{\mathrm{nr}} = \mathcal{O}_{\mathcal{E}^{\mathrm{nr}}} \cap W(R)$. Our constructions have been G_{K_∞}-equivariant, and in particular, the embeddings $\mathcal{O}_{\mathfrak{E}^{\mathrm{nr}}} \hookrightarrow W(\operatorname{Frac} R)$ and $\mathfrak{S}^{\mathrm{nr}} \hookrightarrow W(\operatorname{Frac} R)$ are G_{K_∞}-equivariant. Now we can state the equivalence of categories for integral lattices.

Theorem 2.2.38 ([BC, §11.2], [Li, T3, Theorem 2.1.1])**.** *For $\mathfrak{M} \in \mathrm{Mod}^{\varphi}_{/\mathfrak{S}}$, define*

$$\mathbf{V}^*_{\mathfrak{S}}(\mathfrak{M}) = \operatorname{Hom}_{\mathfrak{S}}(\mathfrak{M}, \widehat{\mathfrak{S}^{\mathrm{nr}}}),$$

the collection of $\mathfrak{S}$-linear maps respecting Frobenius structures. Then $\mathbf{V}^*_{\mathfrak{S}}(\mathfrak{M})$ is a continuous linear G_{K_∞}-representation on a finite free $\mathbb{Z}_p$-module. As a functor, $\mathbf{V}^*_{\mathfrak{S}} : \mathrm{Mod}^{\varphi}_{/\mathfrak{S}} \to \mathrm{Rep}^{\mathrm{free}}_{\mathbb{Z}_p}(G_{K_\infty})$ is fully faithful. Furthermore, it classifies G_{K_∞}-stable $\mathbb{Z}_p$-lattices of a p-adic G_{K_∞}-representation in the following sense: given $\mathfrak{M} \in \mathrm{Mod}^{\varphi}_{/\mathfrak{S}}$, let $V = \mathbf{V}^*_{\mathfrak{S}}(\mathfrak{M}) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ be a d-dimensional p-adic G_{K_∞}-representation. Then, the functor $\mathbf{V}^*_{\mathfrak{S}}$ restricts to a bijection between rank d objects $\mathfrak{N} \subset \mathfrak{M} \otimes_{\mathfrak{S}} \mathcal{E}$ and G_{K_∞}-stable $\mathbb{Z}_p$-lattices $L \subset V$ of rank d.

This basically comes from the fact that we already have a theory of étale φ-modules and that $\mathbf{V}^*_{\mathfrak{S}}$ can be fit into the picture.

Theorem 2.2.39 [BC, §11.2]**.** *Let $\Phi M^{\text{ét,tor}}_{\mathcal{O}_{\mathcal{E}}}$ and $\Phi M^{\text{ét,free}}_{\mathcal{O}_{\mathcal{E}}}$ be the categories of étale φ-modules over $\mathcal{O}_{\mathcal{E}}$ whose underlying $\mathcal{O}_{\mathcal{E}}$-modules are finite free and torsion, respectively. Define the contravariant functors*

$$\mathbf{V}^*_{\mathcal{O}_{\mathcal{E}}} : \Phi M^{\text{ét}}_{\mathcal{O}_{\mathcal{E}}} \to \mathrm{Rep}^{\mathrm{free}}_{\mathbb{Z}_p}(G_{K_\infty}), \quad M \mapsto \mathrm{Hom}_{\mathcal{O}_{\mathcal{E}}}(M, \widehat{\mathcal{O}^{\mathrm{nr}}_{\mathcal{E}}}),$$

$$\mathbf{D}^*_{\mathcal{O}_{\mathcal{E}}} : \mathrm{Rep}^{\mathrm{free}}_{\mathbb{Z}_p}(G_{K_\infty}) \to \Phi M^{\text{ét}}_{\mathcal{O}_{\mathcal{E}}}, \quad V \mapsto \mathrm{Hom}_{\mathbb{Z}_p[G_{K_\infty}]}(V, \widehat{\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}}),$$

$$\mathbf{V}^{\mathrm{tor}\,*}_{\mathcal{O}_{\mathcal{E}}} : \Phi M^{\text{ét,tor}}_{\mathcal{O}_{\mathcal{E}}} \to \mathrm{Rep}^{\mathrm{tor}}_{\mathbb{Z}_p}(G_{K_\infty}), \quad M \mapsto \mathrm{Hom}_{\mathcal{O}_{\mathcal{E}}}(M, \mathcal{E}^{\mathrm{nr}}/\mathcal{O}^{\mathrm{nr}}_{\mathcal{E}}),$$

$$\mathbf{D}^{\mathrm{tor}\,*}_{\mathcal{O}_{\mathcal{E}}} : \mathrm{Rep}^{\mathrm{tor}}_{\mathbb{Z}_p}(G_{K_\infty}) \to \Phi M^{\text{ét,tor}}_{\mathcal{O}_{\mathcal{E}}}, \quad V \mapsto \mathrm{Hom}_{\mathbb{Z}_p[G_{K_\infty}]}(V, \mathcal{E}^{\mathrm{nr}}/\mathcal{O}_{\mathcal{E}^{\mathrm{nr}}}),$$

which are duals of the originally defined Dieudonné functors for étale φ-modules over $\mathcal{O}_{\mathcal{E}}$. Then, these are quasi-inverse equivalences between the categories of finite free objects as well as between the categories of torsion objects.

Moreover, for any $\mathfrak{M}$ in $\mathrm{Mod}^{\varphi}_{/\mathfrak{S}}$, the extension of scalars map $\mathbf{V}^*_{\mathfrak{S}}(\mathfrak{M}) \to \mathbf{V}^*_{\mathcal{O}_{\mathcal{E}}}(\mathfrak{M} \otimes_{\mathfrak{S}} \mathcal{O}_{\mathcal{E}})$ is an isomorphism.

One consequence is that the notion of a *G_{K_∞}-representation having a $E(u)$-height $\le r$* is well-defined. This is the analogue of Hodge-Tate weights in this case.

Theorem 2.2.40 [Li, T3, Theorem 2.1.1]**.** *A semi-stable representation with Hodge-Tate weights in $[-r, 0]$ is of finite $E(u)$-height $\le r$.*

2.2.3.4 $(\varphi, \widehat{G})$-modules

The remaining problem for classifying G_K-lattices is that K_∞/K is not Galois. To remedy this, Liu developed a theory of $(\varphi, \widehat{G})$-modules, where it additionally keeps track of the action of $\widehat{G} = \mathrm{Gal}(K_\infty(\zeta_{p^\infty})/K)$. This gives an *anti-equivalence of a category of $(\varphi, \widehat{G})$-modules and the category of G_K-stable $\mathbb{Z}_p$-lattices in semi-stable G_K-respresentations.* We review this theory from now on.

We continue to use the notation as in the previous section on Kisin modules. Let S be as defined in the theory of Breuil modules, the p-adic completion of the divided power envelope of $W(k)[u]$. Here, we have no assumption like $K = K_0$, so the correct definition of S would be the p-adic completion of $W[\frac{E(u)^i}{i!}]_{i\in\mathbb{N}}$. Define a continuous K_0-linear derivation $N : S \to S$ such that $N(u) = -u$. We denote $S[1/p]$ by S_{K_0}.

Recall that via $u \mapsto [(\pi_n)]$, we could embed $W(k)[u]$ into $W(R)$. As A_{cris} is the p-adic completion of the divided power envelope of $W(R)$ with respect to $\ker\theta$, the embedding $W(k)[u] \hookrightarrow W(R)$ extends to an embedding $S \hookrightarrow A_{\mathrm{cris}}$, where $\theta|_S$ sends u to π. Note that this embedding is compatible with Frobenius endomorphisms.

The key idea is that $K_{\infty,p^\infty} = \cup_{n=1}^\infty K(\pi_n, \zeta_{p^n})$ is Galois over K. Let $K_{p^\infty} := \cup_{n=1}^\infty K(\zeta_{p^n})$, and

$$G_0 := \mathrm{Gal}(K_{\infty,p^\infty}/K_{p^\infty}),$$

$$H_K := \mathrm{Gal}(K_{\infty,p^\infty}/K_\infty),$$
$$\widehat{G} := \mathrm{Gal}(K_{\infty,p^\infty}/K).$$

For completeness, we define $K_n = K(\pi_n)$ and $F_{p^m} = F(\zeta_{p^m})$ for any field F.

We get some results on these groups via class field theory.

Lemma 2.2.5 [Li, T2, Lemma 5.1.2]**.** *The following hold.*

(i) $K_{p^\infty} \cap K_\infty = K$*.*

(ii) $\mathrm{Gal}(K_{p^\infty}/K) \cong H_K$ *and* $G_0 \cong \mathbb{Z}_p(1)$*.*

(iii) $\widehat{G} = G_0 \rtimes H_K$*, and* H_K *acts on* $\mathbb{Z}_p(1) \cong G_0$ *via the cyclotomic character.*

Proof. (ii) and (iii) is immediate from (i), once one realizes that (i) also implies $G_0 \cong \mathrm{Gal}(K_\infty/K)$. Thus, we only need to prove (i). Let $F_n = K(\pi_n) \cap K_{p^\infty}$ and $K_n = K(\pi_n)$. We prove that $F_n = K$ by an induction on n. The base case is trivial. Suppose $F_n = K$ and $F_{n+1} \neq K$. We first show that $\zeta_p \in K$. Note that as $[K_{n+1} : K_n] = p$, $F_{n+1} \neq K$ implies that $[F_{n+1} \cdot K_n : K_n] = p$, or $F_{n+1} \cdot K_n = K_{n+1}$. As F_{n+1}/K is abelian and $F_{n+1} \cap K_n = K$, it follows that K_{n+1}/K_n is Galois and $\mathrm{Gal}(K_{n+1}/K_n) \cong \mathrm{Gal}(F_{n+1}/K)$. Let $\sigma \in \mathrm{Gal}(K_{n+1}/K_n)$ be a nontrivial element. Then, $\sigma(\pi_{n+1})/\pi_{n+1} \in K_{n+1}$ is a nontrivial p-th root of unity, hence $\zeta_p \in K_{n+1}$. As K_{n+1}/K_n is of degree p, there is no intermediate extension in between, and as $[K_n(\zeta_p) : K_n] \leq p-1$, it follows that $K_n(\zeta_p) = K_n$. As $F_n = K$, we have $\zeta_p \in K$.

As $\zeta_p \in K$, $\mathrm{Gal}(K_{p^\infty}/K)$ is a closed subgroup of $\mathrm{Gal}(\mathbb{Q}_{p,p^\infty}/\mathbb{Q}_p(\zeta_p)) \cong 1 + p\mathbb{Z}_p$, whose closed subgroups are of form $1 + p^n\mathbb{Z}_p$ (here we use $p > 2$). As $[F_{n+1} : k] = p$, there exists m such that

$$\mathrm{Gal}(K_{p^\infty}/K) \cong 1 + p^m\mathbb{Z}_p = \mathrm{Gal}(\mathbb{Q}_{p,p^\infty}/\mathbb{Q}_p(\zeta_{p^m}))$$

whereas

$$\mathrm{Gal}(K_{p^\infty}/F_{n+1}) \cong 1 + p^{m+1}\mathbb{Z}_p = \mathrm{Gal}(\mathbb{Q}_{p,p^\infty}/\mathbb{Q}_p(\zeta_{p^{m+1}})).$$

This implies that $\zeta_{p^m} \in K$ whereas $\zeta_{p^{m+1}} \notin K$. Thus, $F_{n+1} = K(\zeta_{p^{m+1}})$. In particular, $\mathrm{Gal}(K_{n+1}/K_n) = \mathbb{Z}/p\mathbb{Z}$. Choose $\sigma \in \mathrm{Gal}(K_{n+1}/K_n)$ such that $\sigma(\zeta_{p^{m+1}}) = \zeta_p\zeta_{p^{m+1}}$. Then, $\sigma(\pi_{n+1}) = \zeta_p^b\pi_{n+1}$ for some $b \not\equiv 0 (\mathrm{mod}\, p)$. As $\zeta_{p^{m+1}} \in K(\pi_{n+1})$, we can write $\zeta_{p^{m+1}} = \sum_{i=0}^{p-1} a_i\pi_{n+1}^i$ for some $a_i \in \mathcal{O}_{K_n}$. Then,

$$\zeta_p\zeta_{p^{m+1}} = \sigma(\zeta_{p^{m+1}}) = \sum_{i=0}^{p-1} a_i\zeta_p^{bi}\pi_{n+1}^i,$$

which means that $a_0 = \zeta_p a_0$ and $a_0 = 0$. This means that $\zeta_{p^{m+1}}$ is not a unit in $\mathcal{O}_{K_n}$, which is a contradiction. □

Let $\varepsilon : G_K \to A_{\mathrm{cris}}^\times$ be defined as $\varepsilon(g) = g([(\pi_n)])/[(\pi_n)]$. This is a cocycle; thus, fixing a topological generator τ of G_0, $\varepsilon(\tau) = [(\varepsilon_i)_{i\geq 0}] \in W(R)$ with ε a primitive p^i-th root of unity. Thus, $t_{\pi,\tau} := -\log(\varepsilon(\tau)) \in A_{\mathrm{cris}}$ is well-defined; the Galois group G_K acts on t as $g(t) = \chi(g)t$.

Let $\gamma_i(x) = x^i/i!$, and let

$$t^{\{n\}} = t^{r(n)}\gamma_{\widetilde{q}(n)}\left(\frac{t^{p-1}}{p}\right),$$

where $n = (p-1)\widetilde{q}(n) + r(n)$ with $0 \leq r(n) < p-1$. We then define a subring $\mathcal{R}_{K_0} \subset B_{\mathrm{cris}}^+$ as

$$\mathcal{R}_{K_0} = \left\{ x = \sum_{i=0}^{\infty} f_i t^{\{i\}} \mid f_i \in S_{K_0}, f_i \to 0 \right\},$$

and $\widehat{\mathcal{R}} := \mathcal{R}_{K_0} \cap W(R)$. By [Li, T3, Lemma 2.2.1], $\widehat{\mathcal{R}}$ *is a* $\mathfrak{S}$*-subalgebra of* $W(R)$ *which is both* φ*-stable and* G*-stable.* Furthermore, the G-action on $\widehat{\mathcal{R}}$ factors through $\widehat{G}$.

Now we can define the notion of $(\varphi, \widehat{G})$*-modules.*

Definition 2.2.33 ($(\varphi, \widehat{G})$-modules)**.** *A* $(\varphi, \widehat{G})$-module *(of height $\leq r$) is a triple* $(\mathfrak{M}, \varphi, \widehat{G})$ *where*

(i) $(\mathfrak{M}, \varphi)$ *is a Kisin module (of height $\leq r$),*

(ii) there is a $\widehat{\mathcal{R}}$-semilinear $\widehat{G}$-action on $\widehat{\mathfrak{M}} := \widehat{\mathcal{R}} \otimes_{\varphi,\mathfrak{S}} \mathfrak{M}$ which commutes with $\varphi_{\widehat{\mathfrak{M}}} := \varphi_{\widehat{\mathcal{R}}} \otimes \varphi_{\mathfrak{M}}$, and

(iii) $\mathfrak{M} \subset \widehat{\mathfrak{M}}^{H_K}$, when $\mathfrak{M}$ is regarded as a $\varphi(\mathfrak{S})$-submodule.

Given a $(\varphi, \widehat{G})$-module $\widehat{\mathfrak{M}} = (\mathfrak{M}, \varphi, \widehat{G})$, we can associate a $\mathbb{Z}_p[G_K]$-module

$$\widehat{\mathbf{V}}^*(\widehat{\mathfrak{M}}) := \mathrm{Hom}_{\widehat{\mathcal{R}},\varphi}(\widehat{\mathcal{R}} \otimes_{\varphi,\mathfrak{S}} \mathfrak{M}, W(R)),$$

where $g \in G$ acts via $g(f)(x) = g(f(g^{-1}(x)))$. It turns out that this is an equivalence of categories classifying integral lattices in semi-stable representations:

Theorem 2.2.41 [Li, T3, Theorem 2.3.1]**.** *Let $\widehat{\mathfrak{M}} = (\mathfrak{M}, \varphi, \widehat{G})$ be a $(\varphi, \widehat{G})$-module. Then, as a $\mathbb{Z}_p[G_\infty]$-module, $\widehat{\mathbf{V}}^*(\widehat{\mathfrak{M}})$ coincides with $\mathbf{V}^*_{\mathfrak{S}}(\mathfrak{M})$ as a Kisin module. Moreover, the functor $\widehat{\mathbf{V}}^*$ induces an anti-equivalence from the category of $(\varphi, \widehat{G})$-modules of height $\leq r$ to the category of G_K-stable $\mathbb{Z}_p$-lattices in semi-stable representations with Hodge-Tate weights in $[-r, 0]$.*

2.2.3.5 Torsion Kisin Modules and Torsion $(\varphi, \widehat{G})$-modules

We use the same notation as the previous section. As the ramification bounds will be proved for torsion representations, we will need the torsion analogue of Kisin modules and $(\varphi, \widehat{G})$-modules. We define a Kisin module to be *torsion* if it is killed by a power of p. Hereby we define some categories using this definition.

- $\mathrm{Mod}^{\varphi,r}_{/\mathfrak{S}_\infty}$ is the category of all torsion Kisin modules of height $\leq r$.
- $\mathrm{Mod}^{\varphi,r}_{/\mathfrak{S}_n}$ is the category of Kisin modules of height $\leq r$ killed by p^n.
- $\mathrm{Free}^{\varphi,r}_{/\mathfrak{S}_n}$ is the category of Kisin modules of height $\leq r$ killed by p^n and finite free over $\mathfrak{S}_n = \mathfrak{S}/p^n\mathfrak{S}$.

We briefly remark the properties of torsion Kisin modules. First of all, a torsion Kisin module is always a quotient of two free Kisin modules of the same rank [Li, T1, .] Similar to the functor $\mathbf{V}^*_{\mathfrak{S}}$, one can also define a functor $\mathbf{V}^*_{\mathfrak{S}_n} : \mathrm{Mod}^{\varphi,r}_{/\mathfrak{S}_n} \to \mathrm{Rep}^{\mathrm{tor}}_{\mathbb{Z}_p}(G_\infty)$ for torsion Kisin modules by

$$\mathbf{V}^*_{\mathfrak{S}_n}(\mathfrak{M}) := \mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, \mathfrak{S}^{\mathrm{nr}}_n),$$

where the homomorphisms are $\mathfrak{S}$-linear and respects Frobenius structures. It is notable that one can use $W_n(R)$ instead of $\mathfrak{S}^{\mathrm{nr}}_n$ via the embedding $\mathfrak{S}^{\mathrm{nr}}_n \hookrightarrow W_n(R)$ [CL, Lemma 2.2.1].

Inspired by the Fontaine's converse to Krasner's lemma, one defines the following: we define $\mathfrak{a}^{>c}_R = \{x \in R \mid v_R(x) > c\}$ and $[\mathfrak{a}^{>c}_R]$ to be the ideal of $W_n(R)$ generated by all $[x]$ with $x \in \mathfrak{a}^{>c}_R$, and similarly we define $\mathfrak{a}^{\geq c}_R$ and $[\mathfrak{a}^{\geq c}_R]$. As $[\mathfrak{a}^{>c}_R]$ is stable under φ and Galois action, the quotient $W_n(R)/[\mathfrak{a}^{>c}_R]$ inherits a Frobenius action. Thus, we can now define

$$J_{n,c}(\mathfrak{M}) := \mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, W_n(R)/[\mathfrak{a}^{>c}_R]),$$

which has a natural G_∞ action. For convenience, we define $J_{n,\infty} = \mathbf{V}^*_{\mathfrak{S}_n}(\mathfrak{M}) = \mathrm{Hom}_{\mathfrak{S},\varphi}(\mathfrak{M}, W_n(R))$. Then, for $c \leq c'$, we get a natrual G_∞-equivariant morphism $\rho_{c',c} : J_{n,c'}(\mathfrak{M}) \to J_{n,c}(\mathfrak{M})$. From now on, let N be a positive integer such that $u^N = 0$ in $W_n[u]/E(u)^r$; it is always true that $u^{ern} = 0$ in $W[u]/E(u)^r$ ([CL, Lemma 2.3.2]), so we can for example let $N = ern$. Also, for the rest of the section, $b = \frac{N}{p-1}$ and $a = \frac{pN}{p-1}$.

Proposition 2.2.29 [CL, Proposition 2.3.3]. *The morphism* $\rho_{\infty,b} : \mathbf{V}^*_{\mathfrak{S}_n}(\mathfrak{M}) \to J_{n,b}(\mathfrak{M})$ *is injective, and its image is* $\rho_{a,b}(J_{n,a}(\mathfrak{M}))$.

Proof. Injectivity can be seen by just checking valuations. To see that the image is $\rho_{a,b}(J_{n,a}(\mathfrak{M}))$, note that certainly the image is contained inside $\rho_{a,b}(J_{n,a}(\mathfrak{M}))$. To see the converse, what we need to prove is that, given $f : \mathfrak{M} \to W_n(R)/[\mathfrak{a}_R^{>a}]$ a φ-morphism, there is a φ-morphism $g : \mathfrak{M} \to W_n(R)$ such that $g \equiv f(\mathrm{mod}[\mathfrak{a}_R^{>b}])$. This can be seen first for $\mathfrak{M} \in \mathrm{Free}^{\varphi,r}_{/\mathfrak{S}_n}$ by successive lifting and then for general object in $\mathrm{Mod}^{\varphi,r}_{/\mathfrak{S}_n}$ by using the fact that any such object is a quotient of two finite free torsion Kisin modules. □

To get an information on $J_{n,c}(\mathfrak{M})$, we first need to analyze the structures of $W_n(R)/[\mathfrak{a}_R^{>c}]$. Here we summarize some facts regarding those quotients; the proofs are all done by checking valuations, and are very straightforward. Define $\theta_s : R \to \mathcal{O}_{\overline{K}}/(p)$ by $(x_0, x_1, \cdots) \mapsto x_s$.

- For $c > 0$ a real number and $s > \log_p(c/e)$ an integer, the map θ_s induces a Galois equivariant isomorphism of k-algebras
$$R/\mathfrak{a}_R^{>c} \to k \otimes_{k,\varphi^s} \mathcal{O}_{\overline{K}}/\mathfrak{a}_{\overline{K}}^{>c/p^s}.$$
- For $c > 0$ a real number and $s > n-1+\log_p(c/e)$ an integer, θ_s induces a Galois equivariant isomorphism of $W_n(k)$-algebras
$$W_n(R)/[\mathfrak{a}_R^{>c}] \to W_n(k) \otimes_{W_n(k),\varphi^s} W_n(\mathcal{O}_{\overline{K}}/(p))/[\mathfrak{a}_{\overline{K}}^{>c/p^s}].$$
- Define $s_0(c) = n - 1 + \log_p(c/e)$ and $s_1 = n - 1 + \log_p(c(p-1)/ep) = s_0(c) + \log_p(1 - \frac{1}{p})$, and $s_{\min} = s_1(a) = n - 1 + \log_p(N/e)$. Let $\mathfrak{M} \in \mathrm{Mod}^{\varphi,r}_{/\mathfrak{S}_n}$. Then, for any nonnegative integer $s > s_1(c)$, the natrual action of G_s on $W_n(R)$ makes $J_{n,c}(\mathfrak{M})$ a $\mathbb{Z}_p[G_s]$-module. This action is compatible with $\rho_{c',c}$'s.
- In particular, for any integer $s > s_{\min}$, $\mathbf{V}^*_{\mathfrak{S}_n}(\mathfrak{M})$ is canonically endowed with a G_s-action.

The proofs are found in [CL, §2].

We would like to extend the above theory of torsion Kisin modules to the theory of $(\varphi, \widehat{G})$-modules to define $\widehat{J}_{n,c}(\widehat{\mathfrak{M}})$. Firstly, for a $(\varphi, \widehat{G})$-module $(\mathfrak{M}, \varphi, \widehat{G})$ which is of p^n-torsion, we define
$$\widehat{\mathbf{V}_n}^*(\widehat{\mathfrak{M}}) := \mathrm{Hom}_{\widehat{R},\varphi}(\widehat{\mathfrak{M}}, W_n(R)).$$
In particular, if we let $\theta : \mathbf{V}^*_{\mathfrak{S}}(\mathfrak{M}) \to \widehat{\mathbf{V}}^*(\widehat{\mathfrak{M}})$ and $\theta_n : \mathbf{V}^*_{\mathfrak{S}_n}(\mathfrak{M}) \to \widehat{\mathbf{V}_n}^*(\widehat{\mathfrak{M}})$ be
$$\theta(f)(a \otimes x) = a\varphi(f(x)) \text{ for } a \in \widehat{\mathcal{R}}, x \in \mathfrak{M},$$
$$\theta_n(f)(a \otimes x) = a\varphi(f(x)) \text{ for } a \in \widehat{\mathcal{R}}, x \in \mathfrak{M},$$
then it gives a natural isomorphism of $\mathbb{Z}_p[G_\infty]$-modules. As G_K-stable $\mathbb{Z}_p$-lattice of semi-stable representations are classified by $(\varphi, \widehat{G})$-modules (Theorem 2.2.41), it follows that any torsion semi-stable G_K-module is in the essential image of $\widehat{\mathbf{V}_n}^*$ ([CL, Theorem 3.1.3]).

Thus, we may know the ramification behavior on a torsion representation from the ramification behavior on lattices. Given a lattice $\widehat{\mathfrak{L}}$, if we let $s_2(c) = s_1(c) + 1$, then for any $s > s_2(c)$, $g \in G_s$ and $x \in \mathfrak{L}$, $g(x) - x$ is in $\left(\left[\mathfrak{a}_R^{>pc}\right] + p^n W(R)\right) \otimes_{\widehat{\mathcal{R}}} \widehat{\mathfrak{L}}$ ([CL, Lemma 3.2.1]).

Using this, we can now analyze the relation between $J_{n,c}(\mathfrak{M})$ and
$$\widehat{J}_{n,c}(\widehat{M}) := \mathrm{Hom}_{\widehat{\mathcal{R}}_n,\varphi}(\widehat{\mathfrak{M}}, W_n(R)/[\mathfrak{a}_R^{>pc}]),$$
and $\widehat{J}_{n,\infty}(\widehat{\mathfrak{M}}) := \widehat{\mathbf{V}_n}^*(\widehat{\mathfrak{M}})$.

Theorem 2.2.42 [CL, Proposition 3.3.2]. *For any nonnegative integer $s > s_2(c)$, $\theta_{n,c} : J_{n,c}(\mathfrak{M}) \to \widehat{J}_{n,c}(\widehat{\mathfrak{M}})$ is an isomorphism of $\mathbb{Z}_p[G_s]$-modules.*

Thanks to this theorem, the results from the Kisin modules case direcly translates as follows.

Corollary 2.2.4 [CL, 3.3]. *The morphism $\widehat{\rho}_{\infty,b} : \widehat{\mathbf{V}}^*_n(\widehat{\mathfrak{M}}) \to \widehat{J}_{n,b}(\widehat{\mathfrak{M}})$ is injective and its image is $\widehat{\rho}_{a,b}(\widehat{J}_{n,a}(\widehat{\mathfrak{M}}))$. Also, $\theta_n : \mathbf{V}^*_{\mathfrak{S}_n}(\mathfrak{M}) \xrightarrow{\sim} \widehat{\mathbf{V}}^*_n(\widehat{\mathfrak{M}})$ is an isomorphism of $\mathbb{Z}_p[G_s]$-modules for all integers $s > s_{\min}$.*

2.3 Vanishing of Low-Degree Hodge Cohomologies: Good Reduction Case

2.3.1 Results of Fontaine

We now explain the general strategy on how to deduce vanishing of Hodge cohomologies from discriminant bound on torsion crystalline. This will also apply to the semi-stable representation case in the later chapter as well. What one eventually proves from the discriminant bound is the following kind of result: for an appropriate choice of p and r, *if V is p-adic $G_{\mathbb{Q}}$-representation which is unramified outside p and crystalline (or semi-stable) at p of Hodge-Tate weights in $[-r, 0]$, there is a $\mathbb{Q}_p[G_{\mathbb{Q}}]$-filtration of V by*

$$V = V_0 \supset V_1 \supset \cdots \supset V_N \supset V_{N+1} = 0,$$

such that for all $0 \le i \le N$, $V_i/V_{i+1} \cong \mathbb{Q}_p(i)^{s_i}$ for $s_i \ge 0$.

Proposition 2.3.1 [Ab5, Proposition 5.3]. *If such thing is true, for any smooth proper variety X over $\mathbb{Q}$ with good reduction everywhere (semi-stable reduction at p and good reduction everywhere else, if the result is about semi-stable representation), $H^i(X, \Omega^j_{X/\mathbb{Q}}) = 0$ if $i \neq j$ and $i + j \le r$.*

Proof. We put $V = H^{i+j}_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)^\vee$. We can apply the above result to V by various comparison theorems, asserting that V is crystalline (or semi-stable) at p, and has Hodge-Tate weights in $[-r, 0]$ because nontrivial Hodge-Tate weight can only occur when the de Rham cohomology jumps, by C_{dR}. Choose $\ell \neq p$, then X has good reduction modulo ℓ, which means that

$$H^{i+j}_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p) \cong H^{i+j}_{\text{ét}}(X_{\overline{\mathbb{F}_\ell}}, \mathbb{Q}_p),$$

as $G_{\mathbb{Q}_\ell}$-represetations (which really uses some kind of base change theorem, e.g. our version of Smooth Base Change Theorem will suffice, Theorem 2.2.10). By the Riemann Hypothesis, Theorem 2.2.17, the Frobenius φ_ℓ acts on V with eigenvalues of modulus $\ell^{-(i+j)/2}$. On the other hand, φ_ℓ acts on $\mathbb{Q}_p(k)$ via the multiplication by ℓ^{-k}. Therefore, the subquotients of the filtration should be zero except possibly at one place. Thus, we have

$$H^{i+j}_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p) = \begin{cases} \mathbb{Q}_p(-\frac{i+j}{2})^s & \text{if } i+j \equiv 0 (\operatorname{mod} 2) \\ 0 & \text{otherwise} \end{cases}$$

By C_{dR}, we have

$$\left(H^{i+j}_{\text{ét}}(X_{\mathbb{Q}}, \mathbb{Q}_p) \otimes_{\mathbb{Q}_p} B_{\text{dR}}\right)^{G_{\mathbb{Q}_p}} \cong H^{i+j}_{\text{dR}}(X_{\mathbb{Q}_p}/\mathbb{Q}_p).$$

Taking filtration subquotient, we have

$$H^i(X_{\mathbb{Q}_p}, \Omega^j_{X_{\mathbb{Q}_p}/\mathbb{Q}_p}) = (\mathbb{Q}_p(\frac{i-j}{2})^s)^{G_K},$$

which is necessarily zero if $i \neq j$. As $H^i(X_{\mathbb{Q}_p}, \Omega^j_{X_{\mathbb{Q}_p}/\mathbb{Q}_p}) = H^i(X, \Omega^j_{X/\mathbb{Q}}) \otimes_{\mathbb{Q}} \mathbb{Q}_p$, we get the desired result. □

Recall that what we want to prove is the following.

Theorem 2.1.3 (Fontaine, [Fo2, Théorème 1], [Ab2, 7.6]). *Let X be a smooth proper variety over $\mathbb{Q}$ with everywhere good reduction. Then, $H^i(X, \Omega_X^j) = 0$ for $i \neq j$, $i + j \leq 3$.*

Specifically, we choose $p = 7, r = 3$. Thus, we would like to prove the following.

Theorem 2.3.1 [Fo2, Proposition 2]. *Let V be a 7-adic $G_{\mathbb{Q}}$-representation coming from geometry, crystalline at 7 and unramified outside 7, with Hodge-Tate weights in $[-3, 0]$. Then, there is a filtration $V = V_0 \supset V_1 \supset V_2 \supset V_3 \supset V_4 = 0$ such that, for all $0 \leq i \leq 3$, $V_i/V_{i+1} \cong \mathbb{Q}_7(i)^{s_i}$ for some $s_i \geq 0$.*

On the other hand, ramification bounds we will get are about torsion crystalline (or semi-stable) representations. Thus, we need a way to relate this result from torsion crystalline representations. However, note that p-adic étale cohomology groups are defined as

$$H^m_{\text{ét}}(X, \mathbb{Q}_p) = \varprojlim_n H^m_{\text{ét}}(X, \mathbb{Z}/p^n\mathbb{Z}).$$

In particular, if $W = H^m_{\text{ét}}(X, \mathbb{Q}_p)$, then there are $\mathbb{Z}_p$-lattices $W = W(p^0) \supset W(p^1) \supset \cdots$ such that $W(p^i)/W(p^{i+1})$ is a torsion representation killed by p. Note also that the above theorem can be rewritten in the following form.

Theorem 2.3.1 [Fo2, Proposition 2]. *Let V be a 7-adic $G_{\mathbb{Q}}$-representation coming from geometry, crystalline at 7 and unramified outside 7, with Hodge-Tate weights in $[-3, 0]$. Suppose $V_4 = 0$, and inductively $V_i = \{v \in V \mid gv - \chi^i(g)v \in V_{i+1} \text{ for all } g \in G_{\mathbb{Q}}\}$. Then, $V_0 = V$.*

Thus, we can show that the torsion crystalline version will imply the above version as follows: V_0 is consisted of $v \in V$ where

$$(g_3 - \chi^3(g_3))(g_2 - \chi^2(g_2))(g_1 - \chi^1(g_1))(g_0 - \chi^0(g_0))v = 0$$

for all $g_0, g_1, g_2, g_3 \in G_{\mathbb{Q}}$. On the other hand, the torsion crystalline version to $V(p^0)/V(p^1)$ implies that

$$(g_3 - \chi^3(g_3))(g_2 - \chi^2(g_2))(g_1 - \chi^1(g_1))(g_0 - \chi^0(g_0))v \in V(p^1).$$

The torsion crystalline version to $V(p^1)/V(p^2)$ implies that

$$(g_3 - \chi^3(g_3))(g_2 - \chi^2(g_2))(g_1 - \chi^1(g_1))(g_0 - \chi^0(g_0))v \in V(p^2).$$

Subsequently, the element in the left hand side lies in $\cap_n V(p^n) = 0$, which implies that $V_0 = V$.

Thus, what we really will show is the following.

Theorem 2.3.2 [Fo2, Proposition 1']. *Let V be a 7-adic $\mathbb{F}_7[G_{\mathbb{Q}}]$-module, crystalline at 7 and unramified outside 7, with Hodge-Tate weights in $[-3, 0]$. Then, there is a filtration $V = V_0 \supset V_1 \supset V_2 \supset V_3 \supset V_4 = 0$ such that, for all $0 \leq i \leq 3$, $V_i/V_{i+1} \cong \mathbb{F}_7(i)^{s_i}$ for some $s_i \geq 0$.*

We prove this by proving series of lemmas. Let $C_{\text{cris}}^{[-3,0]}$ be the category of torsion 7-adic representations of $G_{\mathbb{Q}}$, crystalline at 7 and unramified elsewhere, with Hodge-Tate weights in $[-3, 0]$ and killed by 7.

Lemma 2.3.1 [Fo2, Lemme 1]. *If $0 \to U' \to U \to U'' \to 0$ is an exact sequence in $C_{\text{cris}}^{[-3,0]}$ such that $G_{\mathbb{Q}}$ acts trivially on U' and U'', then G acts trivially on U.*

Proof. This is clear. For example, by sending this exact sequence to Fontaine-Laffaille modules, we have $0 \to M' \to M \to M'' \to 0$ of Fontaine-Laffaille modules where $\mathrm{Fil}^1 M' = \mathrm{Fil}^1 M'' = 0$, as U', U'' had the only Hodge-Tate weight 0. This implies that $\mathrm{Fil}^1 M = 0$, or $G_{\mathbb{Q}}$ acts trivially on U. □

Lemma 2.3.2 [Fo2, Lemme 2]**.** *In the category $C_{\mathrm{cris}}^{[-3,0]}$, $\mathbb{F}_7(i)$ for $i = 0, 1, 2, 3$ are the only simple objects, up to isomorphism.*

Proof. Let U be a simple object, and let E be the field of definition (i.e. the field generated by the kernel of the representation over $\mathbb{Q}$). Let $F = E(\zeta_7)$, and $n = [F : \mathbb{Q}]$. It is a multiple of 6 as $n/6 = [F : \mathbb{Q}(\zeta_7) =: n'$. Note that F is the field of definition of $U \oplus \mathbb{F}_7(1)$. By the discriminant bound, Theorem 2.1.1, we have a discriminant bound

$$|d_F|^{1/n} < 7^{1+\frac{3}{6}} < 18.52026,$$

which means that, by the Odlyzko discriminant bound [Mar], $n \le 208$. If $F/\mathbb{Q}$ is wildly ramified, then $n' = 7n''$, so $n'' \le 7$. Therefore, the 7-Sylow group of $\mathrm{Gal}(F/\mathbb{Q}(\zeta_7))$ is unique and a normal subgroup; let F' be the field fixed by the 7-Sylow sbugroup. Then, $F'/\mathbb{Q}$ is tamely ramified at 7 and unramified outside 7. Thus, the discriminant bound becomes sharper, $|d'_F|^{1/[F':\mathbb{Q}]} < 7$, as $u_{L/K} = 1$. Thus, the Odlyzko discriminant bound implies that $6n'' = [F' : \mathbb{Q}] \le 10$, or $n'' = 1$. But a conjugacy class counting implies that a group of order 42 cannot simply act on a $\mathbb{F}_7$-vector space.

Thus, $F/\mathbb{Q}$ must be tamely ramified, and we get the same degree bound $[F : \mathbb{Q}] \le 10$. Thus, $n' = 1$ and $F = \mathbb{Q}(\zeta_7)$. This implies that U is a 1-dimensional vector space, and $U = \mathbb{F}_7(i)$ for $0 \le i \le 6$. As $U \in C_{\mathrm{cris}}^{[-3,0]}$, we get the desired result. □

Lemma 2.3.3 [Fo2, Lemme 3]**.** *In $C_{\mathrm{cris}}^{[-3,0]}$, all extension, annihilated by 7, of $\mathbb{F}_7(i)$ by $\mathbb{F}_7(j)$ is split, except when $i = 0, j = 3$.*

Proof. If $i = j$, then after Tate-twisting by $\mathbb{F}_7(-i)$, we get $i = j = 0$ and this is Lemma 2.3.1. Suppose $i > j$. Then, after passing to the Fontaine-Laffaille modules, we have an extension $0 \to M' \to M \to M'' \to 0$ such that $T^*_{\mathrm{cris}}(M') = \mathbb{F}_7(-j)$, $T^*_{\mathrm{cris}}(M'') = \mathbb{F}_7(-i)$. Note however that the filtration jump happens only at i for M'' and j for M', respectively. Thus, $\mathrm{Fil}^j M = \mathrm{Fil}^j M''$, and in particular, one can find a section $M'' \hookrightarrow M$. This means that the original sequence splits, if seen as $G_{\mathbb{Q}_7}$-representations. As there is no cyclic everywhere unramified extension of $\mathbb{Q}(\zeta_7)$ of degree 7, this implies that the original splits as $G_{\mathbb{Q}}$-representations.

If $i < j$, then after Tate-twisting by $\mathbb{F}_7(-i)$ we can suppose that $i = 0$. Then the extension is a Galois representation in $\mathrm{GL}_2(\mathbb{F}_7)$ of type

$$\begin{pmatrix} \chi^j & * \\ 0 & 1 \end{pmatrix}.$$

Let E be the field of definition, and $F = E(\zeta_7)$. If this extension is not split, then $F/\mathbb{Q}(\zeta_7)$ must be cyclic of degree 7 by the above form. It is unramified outside 7. As there is no everywhere unramified extension of $\mathbb{Q}(\zeta_7)$ of degree 7, it follows that $F/\mathbb{Q}(\zeta_7)$ is totally ramified, with ramification number j. Thus, $|d_F| = 7^{(42-7)+6(j+1)} = 7^{41+6j}$. If $j \le 2$, then $|d_F| \le 7^{53}$, so $|d_F|^{1/[F:\mathbb{Q}]} \le 7^{53/42} < 11.66$, which means that $[F : \mathbb{Q}] \le 28$. As we already have $[F : \mathbb{Q}] = 6[F : \mathbb{Q}(\zeta_7)] = 42$, this is a contradiction. □

Lemma 2.3.4 [Fo2, Lemme 4]. *If U is an object in $C_{\mathrm{cris}}^{[-3,0]}$ with no quotient isomorphic to $\mathbb{F}_7$, then $U = \oplus_{i=0}^3 g_i U$, where*

$$g_i U = \{u \in U \mid gu = \chi^i(g)u \text{ for all } g \in G\}.$$

Proof. The problem is clear as $C_{\text{cris}}^{[-3,0]}$ is a pre-abelian category. By forming the Jordan-Hölder composition series, thanks to Lemma 2.3.2 and Lemma 2.3.3, it is immediate that U is an extension of $\mathbb{F}_7^s$ by $\mathbb{F}_7(1)^{s_1} \oplus \mathbb{F}_7(2)^{s_2} \oplus \mathbb{F}_7(3)^{s_3}$ for some $s, s_1, s_2, s_3 \geq 0$. However, as U does not have a quotient isomorphic to $\mathbb{F}_7$, we are done. $\square$

Now we can finish the proof.

Proof of Proposition 2.3.2. We proceed by an induction on the order of U. By Lemma 2.3.4, we are supposed to deal with the case when U has a quotient isomorphic to $\mathbb{F}_7$. So, U is fit into the exact sequence

$$0 \to U' \to U \to \mathbb{F}_7 \to 0.$$

By the induction hypothesis, $U' = U'_0$, using the notation of Proposition 2.3.2. Let $\overline{U} = U/U'_1$. As it fits into the exact sequence

$$0 \to U'/U'_1 \to \overline{U} \to \mathbb{F}_7 \to 0,$$

it followws that, by Lemma 2.3.3, $\overline{U} = \mathbb{F}_7^s$ for some $s \geq 1$. Thus, $U_0 = U$, as desired. $\square$

2.3.2 Ramification Bounds for Crystalline Representations

In this section, we will prove the following discriminant bound for torsion crystalline representations.

Theorem 2.1.1 (Fontaine, [Fo2, Théorème 2])**.** *Let k be a perfect field of characteristic $p > 0$, $W = W(k)$, $K = \operatorname{Frac} W$ and $G = G_K$. Let X be a proper smooth scheme over O. Let $0 \leq m < p-1$ be an integer. Then, the ramification subgroups $G^{(v)} \subset G$ acts trivially on any subfactor in $H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$ which is annihilated by p if $v > 1 + \frac{m}{p-1}$.*

Note that, as $r < p-1$, this falls into the realm of Fontaine-Laffaille theory by taking the dual of the étale cohomology group. Let $M \in \mathrm{MF}_{W,tf}^{[0,m]}$ be the Fontaine-Laffaille module corresponding to the dual of the étale cohomology $H^m_{\text{ét}}(X_{\overline{K}}, \mathbb{Q}_p)$. Let L be the field of definition, i.e. the field generated by the kernel of the representation over K. As the theorem only concerns about the action of the inertia group on $T^*_{\text{cris}}(M)$, we may take the maximal unramified extension and assuume the residue field k is algebraically closed. We would like to use the Converse to Krasner's Lemma, Theorem 1.3.1. Thus, let $m > 1 + \frac{r}{p-1}$, and let $\eta : \mathcal{O}_L \to \mathcal{O}_E/\mathfrak{a}^m_{E/K}$ a W-algebra homomorphism, for any algebraic extension E/K. We would like to show that this is liftable to $L \to E$.

Before proceeding, we need to simplify the functor T^*_{cris}. Namely, $A_{\text{cris}}/pA_{\text{cris}}$ is isomorphic to $(\mathcal{O}_{\overline{K}}/p\mathcal{O}_{\overline{K}})[Y_1, \cdots]/(Y_1^p, \cdots)$ via sending Y_k to $\delta^k([\tilde{p}])$, where $\delta(x) = (p-1)!\gamma_p(x)$ ([Hat, Lemma 4.1]). One can then subsequently cut down the divided power ring to obtain that

$$T^*_{\text{cris}}(M) \xrightarrow{\sim} \operatorname{Hom}(M, \mathcal{O}_K/\mathfrak{b}_K),$$

where $\mathfrak{b}_K = \{x \in \mathcal{O}_K \mid v_p(x) > \frac{r}{p-1}\}$ with the obvious divided power structures, and the filtration is given by $(\mathcal{O}_K/\mathfrak{b}_K)^i = \{x \in \mathcal{O}_K \mid v_p(x) \geq \frac{i}{p}\}/\mathfrak{b}_K$ ([Hat, Lemma 4.5]).

Now let $P(X)$ be the minimal polynomial over W of a uniformizer π_L of L, which is written as

$$P(X) = X^{e_{L/K}} + \sum_{s=0}^{e_{L/K}-1} pc_s X^s,$$

with some $c_s \in W$ such that $c_0 \in W^\times$. Let $\widehat{x}$ be a lift of $\eta(\pi_L)$ in $\mathcal{O}_E$. As $P(\eta(\pi_L)) = 0$ in $\mathcal{O}_E/\mathfrak{a}^m_{E/K}$, we have $P(\widehat{x}) + \delta = 0$ for some $\delta \in \mathcal{O}_E$ satisfying $v_p(\delta) > 1 + \frac{r}{p-1}$. From the

Newton polygon of the polynomial $P(X)+\delta$, it follows that $v_p(\widehat{x}) = \frac{1}{e_{L/K}} = v_p(\pi_L)$. Thus, η induces an injection $\eta : \mathcal{O}_L/\mathfrak{b}_L \to \mathcal{O}_E/\mathfrak{b}_E$. As the filtration is determined by valution at v_p, this also respects filtrations. If we show that this respects divided power structures, then by Fontaine-Laffaile theory, we get an injection $T^*_{\mathrm{cris},L}(M) \to T^*_{\mathrm{cris},E}(M)$, and since the action is trivial for $T^*_{\mathrm{cris},L}(M)$, the same holds for E, or, G_E acts trivially on $T^*_{\mathrm{cris}}(M)$; this implies that $G_E \subset G_L$ or $L \subset E$, and we are done.

Therefore, it only remains to prove that the injection $\eta : \mathcal{O}_L/\mathfrak{b}_L \to \mathcal{O}_E/\mathfrak{b}_E$ respects divided powers. For each j, let $pj = e_{L/K_0}i + l$ be the division by e_{L/K_0} so that $0 \le l < e_{L/K_0}$. Then,

$$\varphi^i(\pi_L^j) = \frac{\pi_L^{pj}}{p^i} \bmod \mathfrak{b}_L = \pi_L^l \left(\sum_{s=0}^{e_{L/K_0}-1} c_s \pi_L^s \right)^i \bmod \mathfrak{b}_L,$$

whereas

$$\varphi^i(\eta(\pi_L^j)) = \varphi^i(\widehat{x}^j) = \frac{\widehat{x}^{pj}}{p^i} \bmod \mathfrak{b}_E = \widehat{x}^l \left(\sum_{s=0}^{e_{L/K_0}-1} c_s \widehat{x}^s + \frac{\delta}{p} \right)^i \bmod \mathfrak{b}_E.$$

As $v_p(\delta) > 1 + \frac{r}{p-1}$ implies $\frac{\delta}{p} \in \mathfrak{b}_E$, this proves that $\eta(\varphi^i(\pi_L^j)) = \varphi^i(\eta(\pi_L^j))$, as desired. This proves the discriminant bound, Theorem 2.1.1.

Remark 2.3.1. Note that a similar bound holds for torsion crystalline representations annihilated by p^n; see [Ab3].

2.4 Vanishing of Low-Degree Hodge Cohomologies: Semi-stable Reduction Case

2.4.1 Ramification Bounds for Semi-stable Representations

We will prove the following discriminant bound.

Theorem 2.1.2 (Caruso-Liu, [CL, Theorem 1.1])**.** *Let $p > 2$ be a prime number and k be a perfect field of characteristic p. Let $W = W(k)$, and K be a totally ramified extension of $W[1/p]$ of degree e. Let $G = G_K$, and v_K be the discrete valuation on K noramlized by $v_K(K^\times) = \mathbb{Z}$.*

Consider a positive integer r and V a semi-stable representation of G with Hodge-Tate weights in $[-r, 0]$. Let T be the quotient of two G-stable $\mathbb{Z}_p$-lattices in V, which is again a representation of G annihilated by p^n for some integer n. Denote by $\rho : G \to \mathrm{Aut}_{\mathbb{Z}_p}(T)$ the associated group homomorphism and by L the finite extension of K defined by $\ker\rho$*. If we write $\frac{nr}{p-1} = p^\alpha \beta$ with $\alpha \in \mathbb{N}$ and $\frac{1}{p} < \beta \le 1$, then*

1. *if $\mu > 1 + e(n+\alpha) + \max(e\beta - \frac{1}{p^{n+\alpha}}, \frac{e}{p-1})$, then $G^{(\mu)}$ acts trivially on T;*
2. *$v_K(\mathfrak{D}_{L/K}) < 1 + e(n+\alpha+\beta) - \frac{1}{p^{n+\alpha}}$,*

where $\mathfrak{D}_{L/K}$ is the different of L/K.

We will just prove the bound for the valuation of the different, as it is standard to go back and forth from the valuation of different and the upper ramification number, as seen in Fontaine's first proof. The idea is as follows. For any integer $s \ge 0$, we have $v_K(\mathfrak{D}_{L_s/K}) = 1 + es - \frac{1}{p^s} + v_K(\mathfrak{D}_{L_s/K_s})$. If we take s high enough, we can use compatibilities of $J_{n,c}(\mathfrak{M})$

and $\widehat{J}_{n,c}(\widehat{\mathfrak{M}})$ with G_s-action. Specifically, we take $s > s_0(a)$. Then, $s > s_{\min}$, and for all $c \in [0, ep^{s-n+1}[$, we have a G_s-equivariant isomorphism

$$J_{n,c}(\mathfrak{M}) = \mathrm{Hom}_{\mathfrak{S},\varphi}\left(\mathfrak{M}, W_n(k) \otimes_{W_n(k),\varphi^s} \frac{W_n(\mathcal{O}_{\overline{K}}/(p))}{[\mathfrak{a}_{\overline{K}}^{>c/p^s}]}\right),$$

where $W_n(\mathcal{O}_{\overline{K}}/(p))$ is a $\mathfrak{S}$-module via $u \mapsto 1 \otimes \pi_s$.

Now we start with a proof. Let T be a torsion semi-stable representation annihilated by p^n, so that $T = \Lambda/\Lambda'$ be a quotient of two lattices in a semi-stable representation. Since $\Lambda/p^n\Lambda \to T$ is surjective, it is sufficient to bound ramification for $\Lambda/p^n\Lambda$. Thus, we can assume that T is free over $\mathbb{Z}/p^n\mathbb{Z}$. We know from Section 2.2.3.5 that T should come from a $(\varphi, \widehat{G})$-module $(\mathfrak{M}, \varphi, \widehat{G})$ so that $\mathfrak{M} \in \mathrm{Free}_{\mathfrak{S}_n}^{\varphi,r}$ by our assumption. By Corollary 2.2.4, we have $T|_{G_s} \cong \mathrm{im}\,\rho_{a,b}$ where

$$\rho_{a,b} : J_{n,a}(\mathfrak{M}) \to J_{n,b}(\mathfrak{M}),$$

is the usual morphism. Let L be the field of definition of T, i.e. the field fixed by the kernel of the representation, and let $L_n = K_n L$.

By Theorem 1.3.1, we need to prove the following: for some small given m, given an algebraic extension E/K_s and an $\mathcal{O}_{K_s}$-algebra homomorphism $f : \mathcal{O}_{L_s} \to \mathcal{O}_E/\mathfrak{a}_E^{\geq m}$, f extends to an inclusion $L_s \subset E$. To establish this, we need a final ingredient about analyzing how $J_{n,c}(\mathfrak{M})$ changes via base field extensions. Let E be an algebraic extension of K_s inside $\overline{K}$. For $c \in [0, ep^{s-n+1}[$, we define

$$J_{n,c}^{(s),E}(\mathfrak{M}) := \mathrm{Hom}_{\mathfrak{S},\varphi}\left(\mathfrak{M}, W_n(k) \otimes_{W_n(k),\varphi^s} \frac{W_n(\mathcal{O}_E/(p))}{[\mathfrak{a}_E^{>c/p^s}]}\right).$$

If E/K is Galois, then they are endowed with an action of G_s. Also, if $0 \leq c \leq c' \leq ep^{s-n+1}$, we have a natural morphism $\rho_{c,c'}^{(s),E} : J_{n,c'}^{(s),E}(\mathfrak{M}) \to J_{n,c}^{(s),E}(\mathfrak{M})$. Also, $J_{n,c}^{(s),E}(\mathfrak{M}) \hookrightarrow J_{n,c}^{(s),\overline{K}}(\mathfrak{M}) = J_{n,c}(\mathfrak{M})$. It turns out that this compatibility can capture the containment of field.

Theorem 2.4.1 [CL, Theorem 4.1.1]. *The natural injection $\rho_{a,b}^{(s),E}(J_{n,a}^{(s),E}(\mathfrak{M})) \hookrightarrow \rho_{a,b}(J_{n,a}(\mathfrak{M}))$ is bijective if and only if $L_s \subset E$.*

Proof of Theorem 2.1.2. We will use the Fontaine's converse to Krasner's lemma for $m = ap^{n-1-s}$. Suppose we are given an $\mathcal{O}_{K_s}$-algebra homomorphism $f : \mathcal{O}_{L_s} \to \mathcal{O}_E/\mathfrak{a}_E^{\geq m}$. For any real number $c \in [0, m]$, f induces a map $f_c : \mathcal{O}_{L_s}/\mathfrak{a}_{L_s}^{>c} \to \mathcal{O}_E/\mathfrak{a}_E^{>c}$. This map is injective, by the same reason we have seen in the proof of Proposition 1.3.1; we can characterize kernel. On the other hand, if $c \leq a$, one easily sees that the natural maps $\mathcal{O}_{L_s}/(p) \to \mathcal{O}_{L_s}/\mathfrak{a}_{L_s}^{>cp^{n-1-s}}$ and $\mathcal{O}_E/(p) \to \mathcal{O}_E/\mathfrak{a}_E^{>cp^{n-1-s}}$ induces isomorphisms

$$W_n(\mathcal{O}_{L_s}/(p))/\left[\mathfrak{a}_{L_s}^{>c/p^s}\right] \cong W_n(\mathcal{O}_{L_s}/\mathfrak{a}_{L_s}^{>cp^{n-1-s}})/\left[\mathfrak{a}_{L_s}^{c/p^s}\right],$$

$$W_n(\mathcal{O}_E/(p))/\left[\mathfrak{a}_E^{>c/p^s}\right] \cong W_n(\mathcal{O}_E/\mathfrak{a}_E^{>cp^{n-1-s}})/\left[\mathfrak{a}_E^{c/p^s}\right],$$

by evaluating valuations. Thus, as $f_{cp^{n-1-s}}$ is an injection, we also get an injection

$$W_n(\mathcal{O}_{L_s}/\mathfrak{a}_{L_s}^{>cp^{n-1-s}})/\left[\mathfrak{a}_{L_s}^{>c/p^s}\right] \to W_n(\mathcal{O}_E/\mathfrak{a}_E^{>cp^{n-1-s}})/\left[\mathfrak{a}_E^{>c/p^s}\right].$$

Applying this injection to the construction of $J_{n,c}^{(s),E}(\mathfrak{M})$, we get a successive composition of injections

$$T \cong \rho_{a,b}^{(s),L_s}(J_{n,a}^{(s),L_s}(\mathfrak{M})) \hookrightarrow \rho_{a,b}^{(s),E}(J_{n,a}^{(s),E}(\mathfrak{M})) \hookrightarrow \rho_{a,b}(J_{n,a}(\mathfrak{M})) \cong T.$$

As T is a finite set, this is an isomorphism. Thus, $\rho_{a,b}^{(s),E}(J_{n,a}^{(s),E}(\mathfrak{M})) \hookrightarrow \rho_{a,b}(J_{n,a}(\mathfrak{M}))$ is bijective, which means that $L_s \subset E$. Thus, we can now apply the converse to Krasner's lemma, Theorem 1.3.1, and deduce that $v_K(\mathfrak{D}_{L_s/K_s}) < ap^{n-1-s}$. Now, we pick $\alpha' \in \mathbb{N}$, $\frac{1}{p} < \beta' \leq 1$ such that $\frac{N}{e(p-1)} = p^{\alpha}\beta$. Then, we have

$$\begin{aligned} v_K(\mathfrak{D}_{L_s/K}) &= 1 + es - \frac{1}{p^s} + v_K(\mathfrak{D}_{L_s/K_s}) < 1 + es - \frac{p^s}{+} ap^{n-1-s} \\ &= 1 + es - \frac{1}{p^s} + ep^{\alpha'+n-s}\beta' = 1 + e(n + \alpha' + \beta') - \frac{1}{p^{n+\alpha''}}. \end{aligned}$$

As $v_K(\mathfrak{D}_{L/K}) \leq v_K(\mathfrak{D}_{L_s/K})$, taking $N = ern$, we get the desired bound. □

2.4.2 Results of Abrashkin

Now, we briefly review the following result by Abrashkin.

Theorem 2.1.4 (Abrashkin, [Ab4, Theorem 0.1])**.** *If Y is a smooth projective variety over $\mathbb{Q}$ having semi-stable reduction at 3 and good reduction outside 3, then $h^2(Y_{\mathbb{C}}) = h^{1,1}(Y_{\mathbb{C}})$.*

Proof. We will in particular use the ramification bound, Theorem 2.1.2 for $p = 3$, $r = p - 1$, $e = 1$, $\alpha = 0$, $\beta = 1$, which gives the bound $v(\mathfrak{D}_{L/K}) < 3 - \frac{1}{3}$. The main upshot is the following — given a torsion semi-stable representation V of $G_{\mathbb{Q}}$ killed by 3 and having Hodge-Tate weights in $[-2, 0]$, the field of definition L is *totally ramified over* $\mathbb{Q}$ *at* p. This is via the discriminant bound, Theorem 2.1.2, and the Odlyzko discriminant bound, [Mar], the $[L : \mathbb{Q}] < 230$. As $\mathbb{F}_3(1)$ as well as the semi-stable singularity from a Tate curve contributes enlarging the field of definition, we can assume that K contains $K_1 = \mathbb{Q}(\sqrt[3]{3}, \zeta_9)$. Note that, for $K_0 = \mathbb{Q}(\zeta_9)$, K_1/K_0 as well as $K_0/\mathbb{Q}$ are abelian. Thus, $\mathrm{Gal}(L/\mathbb{Q})$ is solvable. Now Abrashkin [Ab4] proceeds by extensively using SAGE, a computing program for number theory, to deduce that $L \subset \mathbb{Q}(\sqrt[3]{3}, \zeta_9)$. Therefore, $L/\mathbb{Q}$ is totally ramified at 3. Then, $\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(L\mathbb{Q}_3/\mathbb{Q}_3)$. Thus, one only needs to deduce structural restrictions locally at 3.

Now observe that the $i \geq j$ case of Lemma 2.3.3 verbatim translates to this case, as for Breuil modules (the theory of Breuil modules is applicable to this problem) Hodge-Tate weights are also reflected on filtrations. As the category of torsion semi-stable representations of $G_{\mathbb{Q}_3}$ killed by 3 is pre-abelian, the same consideration of Jordan-Hölder composition series gives us the desired result, modulo that there are *no other simple objects*. However, there is another simple object, based on the fact that order 6 group can act simply transitively on one-dimesional $\mathbb{F}_3$-vector space. It is denoted as $\mathcal{L}(1/2, 1/2)$ in [Ab4], and its definition is very explicit, so that one can calcalate Ext values of the object [Ab4, Proposition 5.4]. This in particular shows that the subquotient corresponding to the Hodge-Tate weight -1 is a direct sum of $\mathbb{F}_3(1)$ and the object $\mathcal{L}(1/2, 1/2)$. This may rise to a 3-adic (rational) semi-stable representation of $G_{\mathbb{Q}_3}$, but such representation does not exist by explicit consideration of 2-dimensional non-crystalline semi-stable representations in [Br2, 6.1]. Thus, we get the usual structure theorem, and by the same argument as usual, the theorem is proved. □

References

[Ab1] V. A. Abrashkin, *Galois modules of group schemes of period p over the ring of Witt vectors*. Math. USSR-Izv. **31**-1 (1998), 1-46.

[Ab2] V. A. Abrashkin, *Modular representations of the Galois group of a local field and a generalization of a conjecture of Shafarevich*. Math. USSR-Izv. **35**-3 (1990), 469-518.

[Ab3] V. A. Abrashkin, *Ramification in étale cohomology*. Invent. Math. **101** (1990), 631-640.

[Ab4] V. A. Abrashkin, *Projective Varieties with Bad Semi-stable Reduction at 3 Only*. Documenta Math. **18** (2013), 547-619.

[Ab5] V. A. Abrashkin, *A semi-stable case of the Shafarevich conjecture*, in F. Diamond, P. L. Kassaei, M. Kim, *Automorphic forms and Galois representations, Vol. 1*. London Math. Soc. Lect. Note Series **414**, Cambridge Univ. Press, 2014.

[Ar] M. Artin, *Algebraization of formal moduli. I*, in D. C. Spencer, S. Iyanaga, *Global Analysis (Papers in Honor of K. Kodaira)*. Univ. Tokyo Press, 1969.

[BBM] P. Berthelot, L. Breen, W. Messing, *Théorie de Dieudonné Cristalline II*. Lect. Notes in Math. **930**, Springer, 1982.

[BC] O. Brinon, B. Conrad, *CMI Summer School Notes on p-adic Hodge Theory*. Preprint, Clay Mathematics Institute, 2009.

[Be] L. Berger, *Représentations p-adiques et équations différentielles*. Invent. Math. **148** (2002), 219-284.

[BK] A. Brumer, K. Kramer, *Non-existence of certain semistable abelian varieties*. Manuscripta Math. **106**, 291-304.

[BLR] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models*. Ergebnisse der Mathematik und ihrer Grenzgebiete **21**, Springer-Verlag, 1990.

[BM] C. Breuil, W. Messing, *Torsion étale and crystalline cohomologies*, in *Cohomologies p-adiques et applications arithmétiques II*, Astérisque **279**, Soc. Math. de France, 2002.

[BO] P. Bertholot, A. Ogus, *F-Isocrystals and De Rham Cohomology I*. Invent. Math. **72** (1983), 159-199.

[Br1] C. Breuil, *Représentations p-adiques semi-stables et transversalité de Griffiths*, Math. Ann. **307** (1997), 191-224.

[Br2] C. Breuil, *Construction de représentations p-adiques semi-stables.* Ann. Sci. École Norm. Sup. **31** (1998), 281-327.

[C] B. Conrad, *Étale cohomology.* Preprint, available at `http://math.stanford.edu/~conrad/`.

[CF] J. W. S. Cassels, A. Fröhlich, *Algebraic Number Theory.* Academic Press, 1967.

[CL] X. Caruso, T. Lui, *Some bounds for ramification of p^n-torsion semi-stable representations.* Journal of Algebra **325** (2011), 70-96.

[CS] G. Cornell, J. H. Silverman, *Arithmetic Geometry.* Springer-Verlag, 1986.

[Del] P. Deligne, *Théorème de Lefschetz et critères de dégénérescence de suites spectrales.* Publ. Math. de IHÉS **35** (1968), 107-126.

[Dem] M. Demazure, *Lectures on p-divisible groups.* Springer Lect. Notes **302**, Springer, 1972.

[dJ] A.J. de Jong, *Homomorphisms of Barsotti-Tate groups and crystals in positive characteristic.* Invent. Math. **134** (1998), 301-333.

[EGA] J. Dieudonné, A. Grothendieck, *Éléments de géométrie algébrique.* IHÉS Publ. Math. **4, 8, 11, 17, 20, 24, 28, 32**, IHÉS, 1961-1967.

[EH] D. Eisenbud, J. Harris, *The Geometry of Schemes.* Graduate Texts in Math. **197**, Springer, 1999.

[Fa] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. **73** (1983), 349-366.

[FC] G. Faltings, C.-L. Chai, *Degeneration of Abelian Varieties.* Ergebnisse der Mathematik und ihrer Grenzgebiete **22**, Springer-Verlag, 1990.

[FGA] B. Fantechi et al., *Fundamental Algebraic Geometry: Grothendieck's FGA Explained.* Math. Surveys and Monographs **123**, Amer. Math. Soc., 2005.

[FK] E. Freitag, R. Kiehl, *Étale Cohomology and the Weil Conjecture.* Ergebnisse der Mathematik und ihrer Grenzgebiete **13**, Springer-Verlag, 1988.

[FM] J.-M. Fontaine, W. Messing, *p-adic periods and p-adic étale cohomology.* Contemp. Math. **67** (1987), 179-207.

[Fo1] J.-M. Fontaine, *Il n'y a pas de variété abelienne sur $\mathbb{Z}$.* Compos. Math. **54**-2 (1985), 121-171.

[Fo2] J.-M. Fontaine, *Schémas propres et lisses sur $\mathbb{Z}$*, in S. Ramanan, A. Beauville, *Proceedings of the Indo-French Conference on Geometry (Bombay 1989).* National Board for Higher Mathematics, Hindustan Book Agency, 1993.

[Fo3] J.-M. Fontaine, *Le corps des périodes p-adiques*, in *Périodes p-adiques.* Astérisque **223**, Soc. Math. de France, 1994.

[G] D. Gorenstein, *Finite Groups.* AMS Chelsea Publishing, 19800.

[Har] R. Hartshorne, *Algebraic Geometry.* Graudate Texts in Math. **52**, Springer, 1977.

[Hat] S. Hattori, *Ramification of crystalline representations*. Preprint, 2014.

[I] L. Illusie, *Déformations de groupes de Barsotti-Tate, d'après A. Grothendieck*, in L. Szpiro, *Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell*. Astérisque **127**, Soc. Math. de France, 1985.

[K] M. Kisin, *Crystalline representations and F-crystals*, in V. Ginzburg, *Algebraic Geometry and Number Theory: In Honor of Vladimir Drinfeld's 50th Birthday*. Prog. in Math. **253**, Birkhäuser, 2006.

[La] S. Lang, *Algebra*. Graduate Texts in Math. **211**, Springer, 2002.

[Li, Q] Q. Liu, *Algebraic Geometry and Arithmetic Curves*. Oxford Grad. Texts in Math. *6*, Oxford Univ. Press, 2002.

[Li, T1] T. Liu, *Torsion p-adic Galois representation and a conjecture of Fontaine*. Ann. Sci. École Norm. Sup. **40** (2007), 633-674.

[Li, T2] T. Liu, *On lattices in semi-stable representations: a proof of a conjecture of Breuil*. Compositio Math. **144** (2008), 61-68.

[Li, T3] T. Liu, *A Note on Lattices in Semi-stable Representations*. Math. Ann. **346** (2010), 117-138.

[Mar] J. Martinet, *Petits discriminants des corps de nombres*, in *Number theory days (Exeter, 1980)*. London Math. Soc. Lect. Note Series **56**, Cambridge Univ. Press, 1982.

[Mas] J. M. Masley, *Where are number fields with small class number?*, in *Number theory (Carbondale, 1979)*. Lect. Notes in Math. **751**, Springer, 1979.

[Mat] H. Matsumura, *Commutative algebra*. W.A. Benjamin, 1970.

[McC] J. McCleary, *A User's Guide to Spectral Sequences*. Cambridge Univ. Press, 2001.

[MFK] D. Mumford, J. Fogarty, F. Kirwan, *Geometric Invariant Theory*. Ergebnisse der Mathematik und ihrer Grenzgebiete **34**, Springer-Verlag, 1994.

[Mil1] J. Milne, *Lectures on Étale Cohomology*. Available at `www.jmilne.org/math/`, 2013.

[Mil2] J. Milne, *Étale Cohomology*. Princeton Univ. Press, 1980.

[Mum] D. Mumford, *Abelian Varieties*. Hindustan Book Agency, 2014.

[NN] M. S. Narasimhan, M. V. Nori, *Polarisations on an abelian variety*. Proc. Indian Acad. Sci. (Math. Sci.) **90**-2 (1981), 125-128.

[R] M. Raynaud, *Schémas en groupes de type* $(p, \cdots, p)$. Bull. Soc. Math. France **102** (1974), 241-280.

[Sc1] R. Schoof, *Abelian varieties over $\mathbb{Q}$ with bad reduction in one prime only*. Compositio Math. **141** (2005), 847-868.

[Sc2] R. Schoof, *Introduction to Finite Group Schemes*. Seminars held at UC Berkeley in Fall 2000. Notes taken by John Voight. `https://math.dartmouth.edu/~jvoight/notes/274-Schoof.pdf`.

[Se] J.-P. Serre, *Local Fields*. Graduate Texts in Math. **67**, Springer, 1979.

[SGA1] A. Grothendieck et al., *Revêtements étales et groupes fondamental (SGA 1)*. Lect. Notes in Math. **224**, Springer, 1971.

[SGA3-1] A. Grothendieck et al., *Schémas en groupes I (SGA 3-1)*. Lect. Notes in Math. **151**, Springer, 1970.

[SGA6] A. Grothendieck et al., *Théorie des Intersections et Théorème de Riemann-Roch (SGA 6)*. Lect. Notes in Math. **225**, Springer, 1971.

[SGA7-1] A. Grothendieck et al., *Groupes de Monodromie en Géometrie Algébrique I (SGA 7-1)*. Lect. Notes in Math. **288**, Springer, 1972.

[Sh] I. R. Shafarevich, *Algebraic number fields*, in *Proceedings of the International Congress of Mathematics (Stockholm, 1962)*. Institut Mittag-Leffler, 1963; English translation in Amer. Math. Soc. Transl. (**2**) **31** (1963).

[Stacks] *The Stacks Project*, `http://stacks.math.columbia.edu/`.

[SZ] A. Silverberg, Y. G. Zarhin, *Reduction of Abelian Varieties*, in B. Gordon et al., *The Arithmetic and Geometry of Algebraic Cycles*. NATO Sci. Series **548**, Springer, 2000.

[Tam] G. Tamme, *Introduction to Étale Cohomology*. Springer-Verlag, 1994.

[Tat1] J. Tate, *Finite flat group schemes*, in G. Cornell, J. H. Silverman and G. Stevens, *Modular Forms and Fermat's Last Theorem (Boston, 1995)*. Springer, 1997.

[Tat2] J. Tate, *p-divisible groups*, in T. A. Springer, *Proceedings of a Conference on Local Fields (Driebergen, Netherlands, 1966)*. Springer, 1967.

[TO] J. Tate, F. Oort, *Group schemes of prime order*. Ann. Sci. École Norm. Sup. (4) **3** (1970), 1-21.

[W] L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer, 1982.

[Y] M. Yoshida, *Ramification of local fields and Fontaine's property* (P_m). J. Math. Sci. Univ. Tokyo 17 (2010), 247-265.