UNIVERSITÀ DEGLI STUDI DI PADOVA

FACOLTÀ DI SCIENZE MM. FF. NN.
CORSO DI LAUREA IN MATEMATICA

ELABORATO FINALE

MOD P^N MONODROMY OF THE J-LINE

RELATORE: PROF. M. GARUTI

DIPARTIMENTO DI MATEMATICA PURA E APPLICATA

LAUREANDO: M. E. ARASTEH RAD

ANNO ACCADEMICO 2006/2007

Contents

Introduction

In this thesis we work over a field of char. p. As it is well known elliptic curves are characterized by their j-invariant up to isomorphism and the j-line is a coarse moduli space for elliptic curves. We consider the extension problems for group schemes associated with an p^n kernel $E[p^n]$, of an elliptic curve over j-line for every n. Let U be the ordinary locus of the j-line. The étale quotient of $E[p^n]$ gives rise to representation $\chi : \pi_1(U) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ of algebraic fundamental group. We will show that χ extends over ∞. We also show that the representation χ is surjective, this is obtained by studying the action of inertia at the supersingular points.

The restriction of $E[p^n]$ to U is an extension of an étale group scheme $G = E[p^n]^{et}$ by a local group scheme $E[p^n]^0$, these two are Cartier duals to each other. The fact that χ extends to infinity is equivalent to the fact that G (and by duality G^D) extends to infinity. It is natural to ask whether $E[p^n]$ extends. We show that this is not the case. We reduce the problem to computation of the extension classes in flat cohomology and finally we give a solution by Kummer theory.

In first chapter we collect some material back-ground that are necessary to approach to the main problems of this thesis: étale covers, the algebraic fundamental group, finite group schemes over henselian local ring, Frobenius and Verschiebung, and the Tate curve. In the 5th section of this chapter we shall briefly describe how the algebraic fundamental group makes it possible to generalize Galois descent over general base schemes. Together with the Tate uniformization theorem, this will be our main tools in the next chapter to deal with the monodromy of an étale (resp. local) group scheme G (resp. G^D) over the j-line.
In chapter §2 we will show that the representation $\chi : \pi_1(U) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ extends over ∞. Using some properties of the formal group of an elliptic curve, we will also prove that χ is surjective
The third chapter gives cohomological tools for handling the last problem.
Finally in last chapter we show that the extension of G by G^D can be parameterized by the cocycles in $H^1(R, \boldsymbol{\mu}_{p^n})$, i.e. $H^1(R, \boldsymbol{\mu}_{p^n}) \cong Ext^1_R(G'', G')$. Afterward we reduce the problem to the case of extending a group scheme over field K to a group scheme over a henselian ring R. Ultimately by computing the extension class $[E[p^n]]$ explicitly, we prove that there is no extension of $E[p^n]$ over ∞.

Acknowledgments: I am very grateful to Prof.Edixhoven, indeed without the materials that I learned from him during my first year ALGANT program, it would have been impossible for me to work on this subject. I would like to thank Valentina Di Proietto who arranged this thesis systematically and also for her mathematical helps and comments. I would like to

thank Giovanni Di Matteo for his patience in editing the drafts of this thesis. Finally and most importantly I gratefully acknowledge my advisor Prof.M.Garuti, who did manage this master thesis step by step.

Chapter 1

Preliminaries

1.1 Étale Coverings

In this section we recall some basic definitions and properties of étale coverings.

Let X be a connected locally noetherian scheme. We would like to define the notion of algebraic covering. If X is of finite type over $\mathbb{C}$, it admits an analytic structure. Thus we like that the étale map $Y \to X$ induces an étale analytic morphism, which is local analytic isomorphism. Thus, we require that our covering satisfy the hypotheses of the implicit function theorem, motivating the following general definition.

Definition 1.1.1 *A morphism of of finite type $f : Y \to X$ is said to be* étale *if for every $y \in Y$, there exist open affine neighborhoods $V = \operatorname{Spec} B$ of y and $U = \operatorname{Spec} A$ of $x = f(y)$ such that $f(U) \subseteq V$ and $B = A[x_1, ..., x_n]/(P_1, ..., P_n)$, with $\det(\partial P_i/\partial x_j)$ invertible in $\mathcal{O}_{X,x}$.*

Remark 1.1.2 *Some authors prefer to define the étale morphism to be an unramified and flat morphism. [1]. Note that these two definitions are equivalent, (c.f. [6], chapter I, corollary 3.16.)*

Proposition 1.1.3 *Let $f : Y \to X$ be a morphism of finite type of locally noetherian schemes. Then f is unramified if and only if $\Omega^1_{Y/X} = 0$.*

Proof. c.f. [5], corollary 6.2.3.

Proposition 1.1.4 *The following properties hold:*

[1] (f is said to be *unramified* at x if the homomorphism $\mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ verifies $\mathcal{O}_{X,x}/\mathfrak{m}_y\mathcal{O}_{X,x} = k(x)$, and if the finite extension of residue fields $k(y) \to k(x)$ is separable, moreover f is called *unramifed* if it is unramified at every point of X)

a) Any open immersion is étale.

b) Étale morphisms are stable under base change, composition, and fibered products.

Proof. c.f. [5], proposition 4.3.22. or [6], chapter I, proposition 3.3.

1.2 Algebraic Fundamental Group

Let X be a topological space which is connected and locally contractible with a fixed base point $x_0 \in X$. The topological fundamental group can be defined as the group of homotopy classes of paths $\gamma : [0,1] \to X$ with $\gamma(0) = \gamma(1) = x_0$. We would like to define an analog of the fundamental group of a scheme X. Working with the usual definition does not give a reasonable answer, because the above topological approach does not have an algebraic analogue. Fortunately there is a more intrinsic description of $\pi_1(X, x_0)$ that works well, that is to define the algebraic fundamental group as the automorphism group of the universal covering. Notice that, since X is a locally contractible space, the universal covering $\widetilde{X}$ exists. But in general such a cover does not exist in the algebraic situation. This problem can be solved by passing to the projective limit of all étale covers.

Definition 1.2.1 *Let X be a scheme, Ω an algebraic closed field and $x_0 \in X(\Omega)$ a geometric point of X. Let FEt_X be the category of finite étale covers $Y \to X$ of X. Notice that the morphisms in FEt_X are automatically finite étale morphisms ([6], chap.I, Corollary 3.6.). We define a functor $F_{x_0} : \mathrm{FEt}_X \to \mathrm{Sets}$, by setting $F_{x_0}(Y) = \mathrm{Hom}_X(x_0, Y)$.*

Thus to give an element of $F_{x_0}(Y)$ is to give a point $y \in Y$ that lies over x and a $k(x)$-homomorphism $k(y) \to k(x_0)$.

Definition 1.2.2 *Let X be a connected locally noetherian scheme. The fundamental group $\pi_1(x_0, X)$ of X at the geometric point x_0 is the group of automorphisms of the functor F_{x_0}.*

Let X be a variety over $\mathbb{C}$ and choose a point $x_0 \in X(\mathbb{C})$. Let us denote the topological fundamental group of $X(\mathbb{C})$ by $\pi_1^{top}(X, x_0)$. The étale covering $Y \to X$ induces a finite analytic covering $Y(\mathbb{C}) \to X(\mathbb{C})$. Since $\pi_1^{top}(X, x_0)$ acts naturally on the fiber of $Y(\mathbb{C})$, we get a homomorphism $\pi_1^{top}(X, x_0) \to \pi_1(X, x_0)$. It can be proven that this map induces an isomorphism

$$\widehat{\pi_1^{top}(X, x_0)} \xrightarrow{\sim} \pi_1(X, x_0)$$

where the left hand side is the pro-finite completion of $\pi_1^t(X, x_0)$.

It can be shown that there exist a projective system $(X_i, \varphi_{ij})_{i,j \in I}$ of Galois objects of FEt_X and a pro-étale integral scheme $\widetilde{X} = projlim_{i \in I} X_i$ such that $\pi_1(x_0, X) \cong Aut(\widetilde{X}/X)$. Moreover, up to isomorphism, the algebraic fundamental group of the connected scheme X does not depend on the choice of a base point (for more details we refer to [1], Exp. V.

Theorem 1.2.3 *Let X be locally noetherian and connected, and let x_0 be a geometric point of X. Then F_{x_o} induces an equivalence of categories between FEt_X and (finite $\pi_1(x_0, X)$-sets), where the second category is the category of finite sets with a continuous action of $\pi_1(x_0, X)$.*

Proof. [1], Exp. V.

For any X-scheme Y, we write $Aut_X(Y)$ for the group of X-automorphisms of Y. For any $Y \in \mathrm{FEt}_X$, $Aut_X(Y)$ acts on $F_{x_0}(Y)$. If $Aut_X(Y)$ acts faithfully and transitively on $F_{x_0}(Y)$ (that is if for any $P \in F_{x_0}(Y)$ $Aut_X(Y) \to F_{x_0}$, $\alpha \mapsto \alpha(P)$ is bijective) then Y is said to be Galois. Notice that for connected Y, this action is automatically faithful (see for instance [6], chap.I, corollary 3.13.).

Let us now compute the algebraic fundamental group for the simplest cases,

a) Let $X = \operatorname{Spec} k$ be the spectrum of a field. The geometric point of X corresponds to the embedding $\sigma : k \to \bar{k}$. It would be enough that we consider the connected coverings of X, that are of the form $\operatorname{Spec} L$, where L/k is finite separable extension. For such a covering $f : Y = \operatorname{Spec} L \to X$, we have:

$$F_{x_0}(Y) = \{\varphi : L \hookrightarrow \bar{k} : \varphi|_k = \sigma\}$$

in other words, $F_{x_0}(Y)$ consists of the embeddings $\varphi : L \hookrightarrow \bar{k}$ making the diagram

$$\begin{array}{ccc} k & \xrightarrow{x_0} & \bar{k} \\ {\scriptstyle f}\downarrow & & \| \\ L & \xrightarrow{\varphi} & \bar{k} \end{array}$$

commutative.

Clearly every element of $Gal(k^{sep}/k)$ gives an automorphism of F_{x_0}. Conversely, take $\alpha \in k^{sep}$ and let $\gamma \in \pi(X, x_0)$ and set $\varphi : L = k(\alpha) \to \bar{k}$. γ gives an automorphism of L, let's call it γ_φ . Sending α to $\gamma_\varphi(\alpha)$ giving an element of $Gal(k^{sep}/k)$. One can verify easily that these two constructions are inverse to each other, so we have that

$$\pi(X, x_0) \cong Gal(k^{sep}/k)$$

b) Let $X = \mathbb{P}^1_k$ with k separably closed. If $k = \mathbb{C}$, then X is topologically a sphere, and therefore $\pi_1(X, x_o) = \{1\}$. Let us verify this in general case. Consider the differential dt on $\mathbb{P}^1$, having double pole at infinity and no other zeros or poles. Let $f : Y \to X$ be an étale cover of degree n. Then $f^*(dt)$ has $2n$ poles and no zero, while the Riemann-Hurwitz formula shows $-2n = 2g - 2$, so we deduce that $n = 1$ and f is an isomorphism.

Remark 1.2.4 *(Theorem of the purity of branch locus) For a regular scheme X, and an open subscheme U with complement of codimension greater than 1, we have $\pi(X, x_0) \cong \pi(U, x_0)$, where x_0 is a geometric point of U. [1], Exp. X, Theorem 3.1.*

c) Let $X = E$, where E is an elliptic curve over an algebraic closed field k.Let $f : Y \to X$ be an étale covering of E of degree d. Again by Riemann-Hurwitz we get $g(Y) = 1$. Thus Y is an elliptic curve too. Hence $f : (Y, y) \to (X, f(y))$ is an isogeny, so $Aut(Y/E) = \ker f$. Now let g be the dual isogeny of f, then $f \circ g = [d]$, hence $[d]$ dominates f and

$$\pi(X, x_0) \cong projlim_n X[n](k^{sep})$$

The right hand side is the product of Tate modules $T_l(E)$, l ranges over all prime integers.

Remark 1.2.5 *Using Lang-Serre theorem one can prove that the above isomorphism also holds more generally for any abelian variety over field k, see for example [3], corollary (10.37).*

1.3 Finite Group Schemes and Cartier Duality

A group functor over S is a cofunctor, $\mathcal{F}$, from the category of schemes over S to the category of groups. Let us give a few famous ones. For each scheme X over S, we put

a) $\mathbb{G}_a(X)$ is the additive group of $\Gamma(X, \mathcal{O}_X)$,

b) $\mathbb{GL}_n(X)$, the set of invertible $n \times n$ matrices with entries in $\Gamma(X, \mathcal{O}_X)$. $\mathbb{GL}_1$ is denoted by the special symbol $\mathbb{G}_{\mathrm{m}}$.

c) The n-th roots of unity, $\boldsymbol{\mu}_n(X) = \{x \in \mathbb{G}_{\mathrm{m}}(X) : x^n = 1\}$,

d) For S a scheme of characteristic $p > 0$, $\alpha_{p^n} = \{x \in \mathbb{G}_a(X) : x^{p^n} = 0\}$.

Let us assume that $\mathcal{F}$ is a representable functor, and let G be a group scheme that represents $\mathcal{F}$. Yoneda's lemma tells us that the group axioms can be translated into the following commutative diagrams.

1. (Associativity Law) There exists an S-morphism $m : G \times_S G \to G$ such that

$$\begin{array}{ccc} G \times_S G \times_S G & \xrightarrow{id \times m} & G \times_S G \\ {\scriptstyle m \times id}\downarrow & & \downarrow{\scriptstyle m} \\ G \times_S G & \xrightarrow{m} & G \end{array}$$

commutes, where m is the group multiplication.

2. (Identity Element)There exist a section of the structure morphism $G \to S$, such that

$$\begin{array}{ccc} S \times_S G & \xrightarrow{id} & G \\ {\scriptstyle id\times\varepsilon}\downarrow & & \downarrow{\scriptstyle id} \\ G \times_S G & \xrightarrow{m} & G \end{array}$$

and

$$\begin{array}{ccc} G \times_S S & \xrightarrow{id} & G \\ {\scriptstyle \varepsilon\times id}\downarrow & & \downarrow{\scriptstyle id} \\ G \times_S G & \xrightarrow{m} & G \end{array}$$

commute.

3. (The inverse element) Let $\Delta : G \to G \times_S G$ be the diagonal morphism, there exist an S-morphism $i : G \to G$, so that the diagrams

$$\begin{array}{ccc} G & \xrightarrow{(id\times i)\circ\Delta} & G \times_S G \\ \downarrow & & \downarrow{\scriptstyle m} \\ S & \xrightarrow{\varepsilon} & G \end{array}$$

and

$$\begin{array}{ccc} G & \xrightarrow{(id\times i)\circ\Delta} & G \times_S G \\ \downarrow & & \downarrow \\ S & \xrightarrow{\varepsilon} & G \end{array}$$

commute.

The homomorphism of group schemes are trivial to formulate. Let us now restrict ourselves to the category of affine group schemes. As is well known the assignment $R \mapsto \operatorname{Spec} R$ is an anti-equivalence of categories. So let G be a group functor from the category of schemes over $S = \operatorname{Spec} R$ to the category of groups, and suppose that G can be represented by A. The morphisms associated with the group scheme G correspond to the following homomorphisms of R-modules:

$m^\sharp : A \to A \otimes_R A$

$\varepsilon^\sharp : A \to R$

$i^\sharp : A \to A$

and those morphisms which carry out the algebraic structure:

$e : R \to A$ (giving the R-algebra structure)

$\Delta^\sharp : A \otimes A \to A$ (giving the ring multiplication)

If no confusion is possible we omit the symbol $\sharp$. The axioms for a commutative group scheme translate to the certain axioms for the above morphisms. A together with these maps satisfying these axioms is called a *Hopf algebra*.
Now assume $G = \operatorname{Spec} R$ is commutative, finite and flat over R. Let $A^D = \operatorname{Hom}(A, R)$. Identifying $R \simeq R^D$ and $(A \otimes_R A)^D \simeq A^D \otimes_R A^D$, we get the following collection of morphisms:

$\Delta^D : A^D \to A^D \otimes A^D$

$e^D : A^D \to R$

$i^D : A^D \to A^D$

and those morphisms which carry out the algebraic structure:

$m^D : A^D \otimes_R A^D \to A^D$

$\varepsilon^D : R \to A^D$

One easily verifies that A^D and the above morphisms constitute a Hopf algebra over R. $G^D = \operatorname{Spec} A^D$ is then a finite flat group scheme over $\operatorname{Spec} R$ which is called the *Cartier dual* of G. Note that the canonical evaluation isomorphism induces the group scheme isomorphism $(G^D)^D \simeq G$.

We finish this section by giving some explicit examples.
Let Γ be a finite abelian group. The finite constant group scheme associated to Γ over $\operatorname{Spec} R$ is the group scheme $\underline{\Gamma}_R$ (or simply $\underline{\Gamma}$ if no confusion is possible), whose underlying scheme is $\coprod_{\gamma\in\Gamma} \operatorname{Spec} R$, and mapping the component $\operatorname{Spec} R$ of $\underline{\Gamma} \times \underline{\Gamma}$ indexed by (γ, γ') identically to the component $\operatorname{Spec} R$ of $\underline{\Gamma}$ indexed by $\gamma + \gamma'$, gives the multiplication. Let us mention that the associated ring of regular functions on $\underline{\Gamma}$ is $R^{\underline{\Gamma}}$. The comultiplication map $m : R^\Gamma \to R^{\Gamma\times\Gamma}$, is defined by $m(f)(\gamma, \gamma') = f(\gamma, \gamma')$, and the co-inverse map $i : R^\Gamma \to R^\Gamma$ by $i(f)(\gamma) = f(-\gamma)$ and finally $\varepsilon : R^\Gamma \to R^\Gamma$ takes $f \mapsto f(1)$. If $\{e_\gamma\}_{\gamma\in\gamma}$ is the canonical basis of R^Γ, then $\{\hat{e}_\gamma\}_{\gamma\in\gamma}$ is the basis of $(R^\Gamma)^D$. The dual maps are then given by the following formulas:

$\Delta^D(\hat{e}_\gamma) = \hat{e}_\gamma \otimes \hat{e}_\gamma$

$e^D(\hat{e}_\gamma) = 1$

$i^D(\hat{e}_\gamma) = \hat{e}_{-\gamma}$

and those morphisms which carry out the algebraic structure are

$m^D(\hat{e}_\gamma \otimes \hat{e}_\gamma) = e_{\gamma+\gamma'}$

$\varepsilon^D(1) = \hat{e}_0$

The last two morphism show that $(R^\Gamma)^D \cong R[\Gamma]$. For example set $\Gamma = \mathbb{Z}/n\mathbb{Z}$, then $(R^\Gamma)^D \cong R[\mathbb{Z}/n\mathbb{Z}] \cong R[x]/(x^n - 1)$, where $x = \hat{e}_1$, and multiplication is given by $\Delta^D(x) = x \otimes x$. Therefore $(\underline{\mathbb{Z}/n\mathbb{Z}}_R)^D \cong \boldsymbol{\mu}_{n,R}$. Similarly for R with prime characteristic p one could verify that $\alpha_{p,R} \cong (\alpha_{p,R})^D$.

1.4 The local-étale exact sequence over a Henselian local ring.

Let S be a locally noetherian base scheme. We say that X is finite flat over S iff $\mathcal{O}_X$ is locally free of finite rank as an $\mathcal{O}_S$-module. This rank is a locally constant function that we call the *order* of X over S and denoted by $Ord(X/S)$. Let us first state the following theorem

Theorem 1.4.1 *Let H be a finite flat S-group scheme over S and let X be a scheme of finite type over S. Suppose H acts on X via $\phi : H \times_S X \to X$. Moreover suppose this action is free; i.e. $id \times \phi : X \times H \to X \times X$ is a closed immersion and every orbit is contained in an affine open set. Then there exists an S-group scheme Y and a morphism $\pi : X \to Y$ constant on orbits such that every morphism $X \to Y$ which is constant on orbits factors uniquely through π. We denote it by $\pi : X \to X/H$. The morphism π has the following properties:*

i) X is finite flat over X/H and $Ord(X/(X/H)) = Ord(H/S)$

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

Proof. This is a special case of results of Grothendieck ([2], I, Exp.V).

Let us mention that in the affine case $S = \mathrm{Spec}\,(R)$, $H = \mathrm{Spec}\,(B)$ and $X = \mathrm{Spec}\,(A)$, $X/H = \mathrm{Spec}\,(A^H)$ where $A^H = \{a \in A : \phi^\sharp(a) = a \otimes 1\}$.

As is well known every finite group scheme over a perfect field k is an extension of étale group scheme with local group scheme ([10] Theorem 6.8). But we will need this in a more general context, namely over henselian rings.

Theorem 1.4.2 *Let G be a flat S-group scheme where $S = Spec(R)$ is the spectrum of a local henselian ring R. Let $\mathfrak{m}$ be the maximal ideal of R, $k = R/\mathfrak{m}$ the residue field. Let G^0 be the connected component of the identity in G, then G^0 is a flat closed subgroup scheme of G such that the quotient $G^{et} := G/G^0$ is étale.*

Proof. Let $G = \mathrm{Spec}\,(A)$ with A a finite R-algebra. Since R is a henselian ring we have a decomposition $A = \prod_0^n A_i$ with each A_i a local henselian ring. So we see that $G = \coprod_0^n G_i$ where each G_i is the spectrum of the local henselian ring A_i, so they are connected components of G. For each i, let t_i be the closed point of G_i. Let G^0 be the connected component which contains the image of $\varepsilon : S \to G$. Then S is a closed subscheme of G_0 therefore $k(t_0) = k$. Notice that $G_s = ((G_s)_{\bar{k}})^\pi$ where $\pi = Gal(k^{sep}/k)$. So we see that $G_i \times G^0$ is connected, indeed since $\bar{k}$ valued point of G_s are

$$G_s(\bar{k}) = \mathrm{Hom}(A \otimes k(s), \bar{k}) = \coprod_0^n \mathrm{Hom}_k(k(t_i), \bar{k}) = \coprod_0^n (G_i)_s(\bar{k})$$

we have in particular $\sharp(G_i)_s(\bar{k}) = deg_{sep}(k(t_i)/k)$. Now precisely $(G_i)_s(\bar{k})$ are the orbits for the action of π, thus $G_i \times_S G_j$ is connected if and only if π acts transitively on $(G_i)_s(\bar{k}) \times_S (G_j)_s(\bar{k})$ if and only if $(G_i)_s(\bar{k})$ or $(G_j)_s(\bar{k})$ contains just one element if and only if either $k(t_i)$ or $k(t_j)$ is purely inseparable over k.

From the discussion above we may conclude that $G_i \times_S G^0$ is connected and therefore its image G_iG^0 via $m : G \times_G G \to G$ and since that contains G_i we have $G_iG^0 = G_i$ and in particular $G^0G^0 = G^0$. The following diagram shows that the inverse morphism $i : G \to G$ preserves G^0.

$$\begin{array}{ccc} S & \xrightarrow{\varepsilon} & G \\ \| & & \downarrow i \\ S & \xrightarrow{\varepsilon} & G \end{array}$$

Hence G^0 is a subgroup of G. Note that G^0 is normal, since for every i the image of $G_i \times G^0$ under the morphism $m \circ (m \times i \circ \pi_1)$ contains S and moreover that is connected, so that is contained in G^0. Since $Ord(G^0/S) = m$ is a positive constant therefore by part (i) of Theorem 1.4.1 $Ord(G/G^0) = m$ is constant thus $G \to G/G^0$ is faithfully flat. Hence the fact that G is flat implies that G/G^0 is flat. Up to now we have deduced that G^0 is a flat normal subgroup scheme of G. According to Theorem 1.4.1 we can form the quotient S-group scheme G/G^0. The fact that G^0 is open in G implies that $G^0/G^0 = S$ is open in G/G^0, i.e. Spec $(\mathcal{O}_{G/G^0}/I)$ is open in G/G^0, where I is the related augmentation ideal. Therefore $I = I^2$ and hence G/G^0 is étale.□

We call the the exact sequence

$$0 \longrightarrow G^0 \longrightarrow G \longrightarrow G^{et} \longrightarrow 0$$

the local- étale sequence for G. Notice that it can be characterized by the fact that every homomorphism from G to an étale S-group scheme factors through $G \to G^{et}$, and G^0 is the kernel of that homomorphism.

1.5 Étale group schemes

Let S be a base scheme. Let us first restrict to the case $S = \operatorname{Spec} K$, where K is a field and let L/K be a finite Galois extension of fields with Galois group $Gal(L/K)$. It can be shown that the base change functor $X \mapsto X \times_K L$ induces an equivalence from the category of affine schemes over K to the category of affine schemes over L together with covering action by $Gal(L/K)$. This is called Galois descent. Notice that passing to the limit over finite Galois extensions we see that the above statement also holds for any infinite Galois extension with a continuous action of pro-finite Galois group. Using this result and the well known fact that a finite group scheme G over a field K is étale if and only if $G_{K^{sep}} \cong \underline{G(K^{sep})}$ is constant group scheme, one can prove that the functor $G \mapsto G_{K^{sep}}$ defines an equivalence from the category of finite étale group schemes over K to the category of continues finite $\mathbb{Z}[Gal(K^{sep/K})]$-modules. In this section we shall briefly describe the situation over general base scheme.

Proposition 1.5.1 *Let X be a scheme over a field k and G/X a commutative étale group scheme. Then there exists an étale covering $Y \to X$ such that $G \times_X Y \cong \underline{\Gamma} \times_k Y$, where $\underline{\Gamma}$ is a constant group scheme.*

Proof. Easily follows from Theorem 1.2.3.

Let us take an étale group scheme G over X, then the above theorem shows that there exists an étale covering $Y \to X$ of X, such that G becomes a constant group scheme over Y, meaning that $G \times_X Y \cong \underline{\Gamma}$, for some abstract group Γ. Let $H = Aut(Y/X)$ and suppose $G = \operatorname{Spec} \mathcal{A}$. It gives an action of H on $\underline{\Gamma}_Y$, in other words, we have a morphism $H \to Aut(\Gamma)$. Indeed, $G \times_X Y \cong \operatorname{Spec} \mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{O}_Y \cong \operatorname{Spec} (A \otimes_k \mathcal{O}_Y)$, where A is the ring of functions of Γ. H acts on $(\mathcal{A} \otimes_{\mathcal{O}} \mathcal{O}_X)\mathcal{O}_Y$, we get an action of H on $A \otimes_k \mathcal{O}_Y$, which gives the desired action $H \to Aut(\Gamma)$. So we get an action $\pi(X, x_0) \to Aut(\Gamma)$.
Conversely let H be a quotient of $\pi(X, x_0)$ that acts on Γ, then $(A \otimes_k \mathcal{O}_Y)^H$ is a Hopf algebra on X and defines a group scheme on X. We summarize this discussion in the following Corollary.

Corollary 1.5.2 *Let X be a k-scheme. Let $Y \to X$ be a Galois cover of of X with $H = Aut(Y/X)$ There is an equivalence between:*

1. *Actions of H on the abstract group Γ.*
2. *Group schemes on X that become isomorphic to $\underline{\Gamma}$ over Y.*

1.6 Frobenius and Veschiebung

Let S be a scheme of characteristic $p > 0$. We denote by $F_S : S \to S$ the *absolute* Frobenius morphism (which is the identity on the topological space while $F_S^\sharp : \mathcal{O}_S \to \mathcal{O}_S$ is $F_S^\sharp(a) = a^p$). If X is an S-scheme, denote by $X^{(p/S)}$ (or simply $X^{(p)}$ if no confusion is possible) the fibred product:

$$\begin{array}{ccc} X^{(p)} & \longrightarrow & X \\ \downarrow & & \downarrow \\ S & \xrightarrow{F_S} & S \end{array}$$

The universal property of the fibre product gives a factorization of the map F_X:

$$X \xrightarrow{F_{X/S}} X^{(p)} \longrightarrow X$$

where $F_{X/S}$ is a morphism of S-schemes, called the *relative* Frobenius morphism. See [5], section 3.2.4 for more details.

Proposition 1.6.1 *Let X be an S-scheme of finite type.*

a) If $F_{X/S}$ is an isomorphism then X is unramified over S.

b) If X is étale over S then $F_{X/S}$ is an isomorphism.

Proof. (a)Let us first show that $F^*_{X/S}\Omega^1_{X^{(p)}/S} \to \Omega^1_{X/S}$ is the zero map. Clearly it suffices to prove in the affine case, so let $X = SpecB$ and $S = SpecA$ then the morphism $F_X : X \to X^{(p)}$ corresponds to the A-algebra homomorphism:

$$B^{(p)} = \frac{A[T_1,...,T_n]}{I^{(p)}} \longrightarrow B = \frac{A[U_1,...,U_n]}{I},$$

which takes $T_i \mapsto U_i^p$. Thus $F^*_X\Omega^1_{B^{(p)}/A} \to \Omega^1_{B/A}$ takes $b \otimes dT_i$ to $b.dU_i^p = 0$ Now consider the exact sequence:

$$F^*_{X/S}\Omega_{X^{(p)}/S} \xrightarrow{\alpha} \Omega_{X/S} \xrightarrow{\beta} \Omega_{X/X^{(p)}} \to 0$$

As we have just seen $im(\alpha) = 0$ and since $F_{X/S}$ is an isomorphism $\Omega_{X/X^{(p)}} = 0$ hence $\Omega^1_{X/S} = 0$ so by Proposition 1.1.3, X is unramified over S.

(b) Since étale morphisms are stable under base change, $X^{(p)}$ is also étale over S. Therefore $F_{X/S} : X \to X^{(p)}$ because the morphism between étale scheme is étale (see forward [6], chapter1, corollary 3.6). Notice that also F_X is finite, because in affine charts $\{U_1^{a_1}, ..., U_n^{a_n}\}_{0\le a_i\le p-1}$ generate B over $B^{(p)}$. Using Theorem 1.2.3 we could conclude that F_X is an isomorphism. Notice that F_X is a homeomorphism.

Corollary 1.6.2 *If X is a flat S-scheme of finite type then X is étale over S if and only if $F_{X/S}$ is an isomorphism.*

Proof. Obviously follows from the above theorem.

Notice that $F_{X/S}$ is functorial and commutes with products of S-schemes. Therefore, if G is an S-group scheme, $F_{G/S} : G \to G^{(p)}$ is a group morphism.

Let G be a finite, commutative, S-group scheme. Assume that it is locally free i.e. $\mathcal{O}_G$ is a locally free as a sheaf of $\mathcal{O}_S$-modules. As we mention in the section 1.3. the Cartier dual G^D of G is the group scheme whose Hopf algebra is $\mathcal{H}om_{\mathcal{O}_S}(\mathcal{O}_G, \mathcal{O}_S)$. Notice that G^D represents the group scheme $Hom(G, \mathbb{G}_{\mathrm{m}})$. Let us take an affine cover for S. For an affine chart $U \subseteq S$, G_U is an affine group scheme because G is finite over S. So we may assume that $G = SpecB$ and $S = SpecR$ where B is a free R-module. We have the following isomorphisms: $(B \otimes_{F_S} R)^D \cong B^D \otimes_{F_S} R^D \cong B^D \otimes_{F_S} R$. Indeed we could define the morphisms $\varphi : B^D \otimes_{F_S} R \to (B \otimes_{F_S} R)^D$ which takes ι to $\iota \otimes 1$ and $\psi : (B \otimes_{F_S} R)^D \to B^D \otimes_{F_S} R$ that takes $\gamma \otimes r$ to $\overline{\gamma \otimes r} : m \otimes 1 \mapsto r^p \cdot \gamma(m)$. Clearly we see that these morphisms are mutually inverse. Notice that multiplication in $(G^{(p)})^D$ is given by $(\Delta^{(p)})^D$ where $\Delta^\sharp$ is the ring multiplication of B. The commutativity of the diagram

$$\begin{array}{ccc} B \otimes_{F_S} R & \xrightarrow{(\Delta^\sharp{}^{(p)})^D} & (B \otimes_R B \otimes_{F_S} R)^D \\ \downarrow & & \downarrow \\ B^D \otimes_{F_S} R & \xrightarrow{(\Delta^\sharp{}^D)^{(p)}} & B^D \otimes_R B^D \otimes_{F_S} R \end{array}$$

shows that it is an isomorphism of group schemes. Note that the vertical arrows are the isomorphisms described above. Now dualizing the morphism $F_{G^D/S} : G^D \to (G^D)^{(p)}$ gives $V_{G/S} : ((G^D)^{(p)}))^D \to G$, where the former is isomorphic to $G^{(p)}$, so indeed we have $V_{G/S} : (G^{(p)} \to G$, this morphism is called the Verschiebung morphism.

Theorem 1.6.3 *Let G be a finite commutative group scheme,*

a) $V_{G/S} \circ F_{G/S} = p \cdot id_G$

b) $F_{G/S} \circ V_{G/S} = p \cdot id_{G^{(p)}}$.

Proof. Let us mention that for schemes X and Y, the Frobenius $F_{X/S}$ is functorial, i.e. for every morphism $\rho : X \to Y$, the diagram

$$\begin{array}{ccc} X & \xrightarrow{F_X} & X^{(p)} \\ {\scriptstyle\rho}\downarrow & & \downarrow{\scriptstyle\rho\otimes id} \\ Y & \xrightarrow{F_Y} & Y^{(p)} \end{array}$$

commutes.
Put $\rho = V_G$, we get the following commutative diagram :

$$\begin{array}{ccc} G^{(p)} & \xrightarrow{F_{G^{(p)}/S}} & G^{(p^2)} \\ {\scriptstyle V_G}\downarrow & & \downarrow{\scriptstyle V_{G/S}\otimes id} \\ G & \xrightarrow{F_G} & G^{(p)} \end{array}$$

Since the Frobenius morphism is compatible with base change, its dual Verschiebung i.e. $V_{G/S} \otimes id \cong V_{G^{(p)}/S}$ hence $F_{G/S} \circ V_{G/S} = F_{G^{(p)}/S} \circ V_{G^{(p)}/S} = p \cdot id_{G^{(p)}}$. So it would be enough that we prove (a). Notice also that we may reduce to the affine case. So we may take $S = \operatorname{Spec} A$ affine and $G = \operatorname{Spec} B$ with B free A-module.

We now consider the morphism $\Delta^{\sharp\otimes p} : B^{\otimes p} \to B$ induced by ring multiplication, which is stable under switching. Hence this morphism factors through $Sym^p B$, thus we get a morphism $Sym^p(B) \twoheadrightarrow B$. We also define the morphism $B \otimes_{F_R} R \to Sym^p B$, induced by $a \otimes x \mapsto xa \otimes a \ldots \otimes a$. Clearly the composition of these morphisms is the relative Frobenius. Note that the last morphism is R-linear:

$$x(a+b) \otimes \ldots \otimes (a+b) = x \cdot \sum_r a_{p,r} \cdot a^{\otimes p-r} \otimes b^{\otimes r}$$

where $a_{p,r}$ are the coefficients of the expansion of $(a+b)^p$. Since all of these coefficients are divisible by p except for $r=1$ and $r=p$, the expression simplifies to

$$x(a+b)\otimes\ldots\otimes(a+b) = (x\cdot a\otimes a\otimes\ldots)+(x\cdot b\otimes b\ldots\otimes b)$$

Thus we have:

$$F_B : B\otimes_{F_R} R \rightarrowtail Sym^p(B) \twoheadrightarrow B$$

Now since B is an R-module of finite rank, we may take the above diagram for B^D and dualize to get:

$$V_B : B \xrightarrow{\overline{\mu}^\sharp} TS^p(B) \xrightarrow{\upsilon_B} B^{(p)}$$

where $\overline{\mu}^\sharp$ is the morphism induced by the comultiplication $\mu^\sharp$. By definition of υ_B, we have the following commutative diagram:

$$\begin{array}{ccc} TS^p(B) & \xrightarrow{\nu_B} & B^{(p)} \\ \downarrow & & \downarrow{\scriptstyle F_A} \\ B^{\otimes p} & \xrightarrow{\Delta^{\sharp\otimes p}} & B \end{array}$$

Composing with the morphism $\overline{\mu}^\sharp$, we get the following commutative diagram of group schemes:

$$\begin{array}{ccc} G & \xrightarrow{\Delta} & G^{\times p} \\ {\scriptstyle F_G}\downarrow & & \downarrow{\scriptstyle \mu} \\ G^{(p)} & \xrightarrow{V_{G/S}} & G \end{array}$$

which shows $V_{G/S}\circ F_{G/S} = p\cdot id_G$.□

1.7 The Tate Curve

In this section we describe a particular scheme **Tate**(q) over $\mathbb{Z}[[q]]$, called the *Tate Curve*. The motivation of constructing this curve comes from analytic theory of elliptic curves, where an elementary result says that every complex elliptic curve is isomorphic to $\mathbb{C}/\Lambda$ for a lattice Λ, moreover Λ can be chosen to be of the normalized form $\Lambda = \mathbb{Z}+\mathbb{Z}\tau$, for some number τ in the complex upper half plane. Conversely, any such a lattice Λ determines an elliptic curve. This is a very useful characterization, indeed because the group law in $\mathbb{C}/\Lambda$ is very simple. Now suppose we replace $\mathbb{C}$ with some p-adic field K and endeavor to parameterize elliptic curves over K by groups of the form K/Λ. This approach immediately fails, since such a field can have no non-trivial discrete subgroup. For example if $K=\mathbb{Q}_p$ and $\Lambda\subset\mathbb{Q}_p$ is a nonzero subgroup, then for any nonzero $t\in\Lambda$, $\lim_{n\to\infty} p^n t = 0$, therefore 0 is an accumulation point of Λ.
Tate's idea is based on alternative description of the normalization. That is, the exponential map $e : z\mapsto e^{2\pi iz}$ induces an isomorphism

$$\mathbb{C}/\Lambda \xrightarrow{e} \mathbb{C}^*/q^{\mathbb{Z}}$$

where $q^{\mathbb{Z}}$ denotes the free multiplicative group generated by $q = e(\tau)$. Then from the above correspondence we see that a complex elliptic curve is isomorphic to $\mathbb{C}^*/q^{\mathbb{Z}}$ for some nonzero complex number q with $|q| < 1$, and every such q gives an elliptic curve. Thus we get a family of elliptic curves

$$\mathcal{E} \to D^*$$

over the punctured unit disk, the fiber over q is $\mathbb{C}^*/q^{\mathbb{Z}}$. We can construct an embedding of $\mathcal{E}$ in the projective space in a way that the fiber above q is the elliptic curve given by the Weierstrass equation, whose coefficients depend holomorphically on the parameter q. Then we can expand the associative values j, Δ, as Laurent series in the parameter q. For example this gives the well known expansion:

$$j(q) = \frac{1}{q} + 744 + 196884q + \ldots = \frac{1}{q}(1 + 744q + 196884q^2 + \ldots)$$

and it can be shown that the Weierestrass equation can be written as

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q).$$

Tate regarded the coeficients $a_4(q)$ and $a_6(q)$ just as formal series in q, he observed that this is not just an elliptic curve in $\mathbb{P}^2_{\mathbb{C}[[q]]}$, but in fact lies in $\mathbb{P}^2_{\mathbb{Z}[[q]]}$. Tate's construction perform the same trick over local fields, requiring only $|q| < 1$ for convergence. Here we state "Tate's Uniformization Theorem".

Theorem 1.7.1 *Let K be a local field with absolute value $|\cdot|$, let $q \in K^*$ such that $|q| < 1$, and let*

$$s_k(q) = \sum_{n \geq 1} \frac{n^k.q^n}{1 - q^n}.$$

Set $a_4(q) = -s_3(q)$ and $a_6(q) = -\frac{5s_3(q)+7s_5(q)}{12}$. Then

a) The series $a_4(q)$ and $a_6(q)$ converge in K.

b) The discriminant and j-invariant of the Tate curve E_q are as follows:

$$\Delta = q\prod_{n \geq 1}(1 - q^n)^{24}$$

and

$$j(q) = \frac{1}{q} + 744 + 196884q + ... = \frac{1}{q}(1 + 744q + 196884q^2 + ...).$$

c) Let L be an algebraic extension of K. The series

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} - 2s_1(q),$$

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{(q^n u)^2}{(1-q^n u)^3} + s_1(q),$$

converge for all $u \in L \setminus q^{\mathbb{Z}}$. They define the surjective homomorphism

$$\phi : L^* \longrightarrow E_q(L)$$

which takes $u \mapsto (X(u,q), Y(u,q))$ if $u \in L \setminus q^{\mathbb{Z}}$ and $u \mapsto 0$ otherwise, with kernel $q^{\mathbb{Z}}$.

For the proof we refer to [8] ,chapter V, theorem 3.1.

Remark 1.7.2 *For further applications we also give the following alternative expressions for $X(u,q)$ and $Y(u,q)$:*

$$X(u,q) = \frac{u}{(1-u)^2} + \sum_{n\geq 1}\left(\frac{q^n u}{(1-q^n u)^2} + \frac{q^n u^{-1}}{(1-q^n u^{-1})^2} - 2\frac{q^n}{(1-q^n)^2}\right)$$

$$Y(u,q) = \frac{u^2}{(1-u)^3} + \sum_{n\geq 1}\left(\frac{(q^n u)^2}{(1-q^n u)^3} - \frac{q^n u^{-1}}{(1-q^n u^{-1})^3} + \frac{q^n}{(1-q^n)^2}\right).$$

These expressions also can be found in [8], page 425.

Chapter 2

p-Adic Monodromy

From now on, we will work over a perfect field k of characteristic $p > 0$. Let $\mathcal{S}$ be the set of supersingular values of $j \in k$ and put $U = \mathbb{A}^1 - \mathcal{S}$ and $\overline{U} = \mathbb{P}^1 - \mathcal{S}$. Let $E \to U$ be the restriction of the elliptic curve over the j-line, $F : E \to E^{(p)}$ and $V : E^{(p)} \to E$ the Frobenius and Verschiebung morphisms. Using Theorem 1.6.3, for every n we get the following diagram, whose first row is exact:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker F^n & \longrightarrow & E[p^n] & \longrightarrow & \ker V^n & \longrightarrow & 0 \\ & & \| & & \downarrow & & \downarrow & & \downarrow \\ & & \ker F^n & \longrightarrow & E & \xrightarrow{F^n} & E^{(p^n)} & \xrightarrow{V^n} & E. \end{array} \tag{2.1}$$

So for every n we have the exact sequence:

$$0 \longrightarrow \ker F^n \longrightarrow E[p^n] \longrightarrow \ker V^n \longrightarrow 0 \tag{2.2}$$

Notice that $\ker V^n$ (resp. $\ker F^n$) is an étale (resp. a local) group scheme over U. Indeed we only need to consider the fibers. So now we assume that we are working with an ordinary elliptic curve E over the field k. A finite commutative group scheme over a perfect field can be decomposed as a product of connected group scheme and étale group scheme. Let us consider the case $n = 1$, general case is similar. Since E is ordinary, we have that $E[p](k^{sep})$ consists of p points. As $E[p]$ is a finite group scheme of order p^2 over k we have that the connected part and étale part of $E[p]$ are both of order p. By proposition 1.6.1 F is an isomorphism on the étale part of $E[p]$ and it also vanishes on the local part(for example see [10], Theorem 14.4) so we see that the $\ker F$ has to be the local part of $E[p]$ hence the $\ker V$ is the étale part of $E[p]$. The étale group scheme $\ker V^n$ defines a character

$$\chi : \pi_1(U) \to (\mathbb{Z}/p^n\mathbb{Z})^\times . \tag{2.3}$$

Theorem 2.0.1 *χ extends to a character $\pi_1(\overline{U}) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$.*

Proof. Let us take $n = 1$, in general one easily sees that the same arguments hold for an arbitrary n. Let $K = k(j)$ be the fraction field of U.

Assume that the action of $\pi_1(U)$ factors through the automorphism of étale covering $\overline{im\chi}$: $W \to U$. Set $L = Frac(W)$ and $\Gamma = (\mathbb{Z}/p\mathbb{Z})$. Since the character χ factors through the action of the automorphism group of the étale covering W of U, so $\ker V^n \times_U W \cong \underline{\Gamma} \times_k W$. So we have the following commutative diagram:

$$\begin{array}{ccc} \underline{\Gamma} \times_k W & \longrightarrow & KerV^n \\ \downarrow & & \downarrow \\ W & \longrightarrow & U \end{array}$$

Taking the generic fiber, we have:

$$\begin{array}{ccc} \underline{\Gamma} \times_k L & \longrightarrow & (KerV^n)_K \\ \downarrow & & \downarrow \\ \operatorname{Spec} L & \longrightarrow & \operatorname{Spec} K \end{array}$$

which clearly gives the character $\chi : Gal(K^{sep}/K) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$.

Let $\overline{W}$ be the normalization of W inside L. Now considering the following diagram

$$\begin{array}{ccc} W & \longrightarrow & \overline{W} \\ \downarrow & & \downarrow \\ U & \longrightarrow & \overline{U} \end{array}$$

we see that it suffices to prove L/K is unramified at ∞, which is equivalent to saying that for the prime ideals of L above infinity the inertia group is trivial.

Let $\hat{K} = k((j))$ be the completion of K at ∞. Write $\hat{K} = k((q))$, where $j = \frac{1}{q} + 744 + 196884q + \cdots$, hence the pullback of E to $\hat{K}$ is isomorphic to the Tate curve

$$E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$$

Since we are working over a field of characteristic p we see that raising the partial sums of $a_4(q)$ or $a_6(q)$ to the power p is the same as rising q to the p in $a_4(q)$ or $a_6(q)$. So the same holds for the limit. Therefore $E_q^{(p)} = E_{q^p}$. Now since V is the dual of F, we have $V(Q) = [degF] \cdot P$ where $Q = F(P)$. Now, Tate uniformization gives us the following diagram :

$$\begin{array}{ccc} K^*/q^Z & \xrightarrow{\simeq} & E_q(K^{sep}) \\ {\scriptstyle \hat{F}}\downarrow & & \downarrow{\scriptstyle F} \\ K^*/(q^p)^Z & \xrightarrow{\simeq} & E_{q^p}(K^{sep}) \\ {\scriptstyle \hat{V}}\downarrow & & \downarrow{\scriptstyle V} \\ K^*/q^Z & \xrightarrow{\simeq} & E_q(K^{sep}) \end{array}$$

Note that $\hat{F} : K^*/q^Z \to K^*/(q^p)^Z$ takes $u \mapsto u^p$ and therefore $\hat{V} : K^*/(q^p)^Z \to K^*/q^Z$ takes $t \mapsto \bar{t}$. We see that $\ker \hat{V}$ is generated by $\overline{q}$, this in particular shows that $\ker V$ consists of p distinct points (similarly $\ker V^n$ consists of p^n points). Moreover, as we have just seen, the points lying in $\ker V$ are rational, so the decomposition group acts trivially on this set and therefore the inertia group acts trivially.□

Corollary 2.0.2 *The group scheme* $\ker V^n$ *(resp.* $\ker F^n$*) extends to an étale (resp. local) group scheme over* $\overline{U}$*.*

Proof. We apply Corollary 1.5.2 for $X = \overline{U}$ to get the desired scheme over $\overline{U}$ lets call it $\overline{G}$. Indeed $\overline{\chi} : \pi_1(\overline{U}) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ factors through the automorphism group of some étale cover $\overline{W}$ of $\overline{U}$, so we get:

$$\begin{array}{ccc} \underline{\Gamma} \times_k \overline{W} & \longrightarrow & \overline{G} \\ \downarrow & & \downarrow \\ \overline{W} & \longrightarrow & \overline{U} \end{array}$$

Notice that in fact $\overline{G} \cong (\underline{\Gamma} \times_k \overline{W})^{\overline{H}}$ where $\overline{H} = Aut(\overline{W}/\overline{U})$, and it is then clear that if we restrict to U we get:

$$\begin{array}{ccc} \underline{\Gamma} \times_k W & \longrightarrow & (\ker V^n) \\ \downarrow & & \downarrow \\ W & \longrightarrow & U \end{array}$$

Hence we may conclude that $\overline{G}$ is the extension of $\ker V^n$.

Theorem 2.0.3 χ *is surjective.*

Proof. Let $s \in S$ be a supersingular point and z a local coordinate at s. Then E defines an elliptic curve over $R = k[[z]]$ with ordinary generic fibre and good supersingular reduction.

It is sufficient to show that the image of a subgroup of the fundamental group maps surjectively. As in the proof of the above theorem we can replace U by the generic point of U and even by the spectrum of the completion K_s of $K = k(j)$ at some point s outside U, then E defines an elliptic curve over $R = k[[z]]$ (where z is a local coordinate at s), with ordinary generic fibre and good supersingular reduction. In which case the fundamental group becomes the Galois group $Gal(K_s^{sep}/K_s)$. This action factors through the Galois group of L, where L is the cyclic extension of $k((z))$ obtained by adjoining the points of $\ker V^n$. Let I be the inertia subgroup at s it is enough to prove that χ maps $I = Gal(K_s^{sep}/K_s^{unr})$ surjectively, and therefore it is enough to show that $Gal(LK_s^{unr}/K_s^{unr}) \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ is surjective. This would mean that the cyclic, totally ramified extension L/K_s^{unr} has degree $\Phi(p^n) = p^{n-1}(p-1)$.
Now consider the n-th iterates of Verschiebung, that is the composite homomorphism

$$E^{(p^n)} \xrightarrow{V_{E^{(p^{n-1})}}} E^{(p^{n-1})} \longrightarrow \ldots E^{(p^2)} \xrightarrow{V_{E^{(p)}}} E^{(p)} \xrightarrow{V_E} E$$

Let $P_1 \in E^{(p)}$ be a point which maps to 0 via V_E. We now take an inductive series of points $\{P_i\}$ where $P_i \in E^{(p^i)}(K_s^{sep})$ and such that $V_{E^{(p^{i+1})}}(P_{i+1}) = P_i = (x_i, y_i)$. We claim that $\nu(x_i) = \frac{1}{p^{i-1}(p-1)}$, where ν is the valuation of K_s extended to a valuation of K_s^{sep}. Note that as we mentioned above, then this claim implies theorem. We are going to prove it inductively. The formal power series corresponds to the multiplication by p, is given by $[p](T) = g(T^p) = \alpha' T^p + \beta T^{p^2} + \ldots$. The fact that s is a supersingular point implies that the reduction of $\hat{E}$ modulo z has height 2 (c.f. [8], chapter V, Theorem 3.1), thus:

$$[p](T) = \alpha z T^p + \beta T^{p^2} + \ldots$$

with α,$\beta \in k[[z]]^\times$. Since $V \circ F = [p]$ and the formal power series associated to the Frobenius morphism is $F(T) = T^p$, we realize that

$$\hat{V} = \alpha z T + \beta T^p + \ldots$$

with α and β in $k[[z]]^\times$. Raising the coefficients of the equation of $E : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$ to p^i, we see that the coefficients of formal group scheme associated to E (c.f [8], chapter.IV, §1)

$$F(z_1, z_2) = i(z_3(z_1, z_2)) = z_1 + z_2 - a_1 z_1 Z_2 - a_2(z_1^2 z_2 + z_1 z_2^3) - \ldots$$

raise to p^i and thus the coefficients of p-th iterate $[p](T) = F(...(F(F(0,T),T),T))...)$, hence

$$\hat{V}_{E^{(p^i)}} = \alpha^{p^i} z^{p^i} T + \beta^{p^i} T^p + \ldots$$

Let $i = 1$, we have

$$0 = \hat{V}_{(E^{(p)})}(x_1) = \alpha z x_1 + \beta x_1^p + \ldots$$

canceling factor x_1 we get $0 = \alpha z + \beta x_1^{p-1} + \ldots$. Clearly $\nu(x_1)$ can not be bigger than $1/(p-1)$, because then every term with higher order has a valuation bigger than $1/(p-1)$, therefore they can not cancel the first term αz. So we have $\nu(x_1) \leq \frac{1}{p-1}$. Suppose $\nu(x_1) < \frac{1}{p-1}$, then the term βx_1^{p-1} has the lowest valuation among all terms, and the value of all other terms are strictly bigger than that, it then can not cancel. This contradiction shows $\nu(x_1) = \frac{1}{p-1}$. Assume now that it is true for $i-1$, so we have $\nu(x_{i-1}) = \frac{1}{p^{i-2}(p-1)}$.

$$x_{i-1} = \hat{V}_{(E^{(p^i)})}(x_i) = \alpha^{p^i} z^{p^i} x_i + \beta^{p^i} {x_i}^p + \ldots$$

Now if $\nu(x_i) > \frac{1}{p^{i-1}(p-1)}$ then value of x_{i-1} is strictly less than every value of every term in right hand side, and if $\nu(x_i) < \frac{1}{p^{i-1}(p-1)}$ then the value of $\beta^{p^i} {x_i}^p$ is strictly smaller than the values of other terms in both sides of the above equation. We may deduce that $\nu(x_i) = \frac{1}{p^{i-1}(p-1)}$. So in particular $\nu(x_n) = \frac{1}{p^{n-1}(p-1)}$. $\square$

Chapter 3

Extensions and Flat Cohomology

3.1 Twisted Forms and Cohomology

Let $\mathcal{F}$ be an abelian group functor and $R \to S$ a flat morphism of rings. Let $d^i : \bigotimes^n S \to \bigotimes^{n+1} S$ insert a 1 in i-th place. Let's define $d : \mathcal{F}(\bigotimes^n S) \to \mathcal{F}(\bigotimes^{n+1} S)$ by $d = \sum(-1)^k d^k$. One can verify easily that $d \circ d = 0$, so that the groups $H^m(S/R, \mathcal{F})$ can be defined as a kernel modulo image at m-th stage. From sheaf point of view this cohomology is Cech cohomology for the covering $\operatorname{Spec} S \to \operatorname{Spec} R$.
$H^m(R, \mathcal{F})$ is defined to be $\varinjlim H^m(S/R, \mathcal{F})$ where the limit is taken over all over all flat coverings $R \to S$.

Suppose $M$is given R-module, possibly with some additional algebraic structure(for example a bilinear multiplication or whole Hopf algebra structure). An S/R-form of M, or twist form splits by S, is another R-module with the same type of structure becomes isomorphic to M after tensoring with S.

Let us consider the functor $\mathbf{Aut}(M)$, that takes any R-algebra S to the automorphism of $M \otimes_R S$ preserving the given structure. If M is a Hopf algebra representing a finite group scheme G, then we also denote this functor by $\mathbf{Aut}(G)$.

Theorem 3.1.1 *There is a one to one correspondence between the isomorphism class of S/R-forms of M and $H^1(S/R, \mathbf{Aut}(M))$*

Proof. c.f [10], Theorem 17.6.

3.2 Kummer Theory

Let S be a base scheme. Let $\boldsymbol{\mu}_n$ be the subsheaf of G_m defined by the group scheme $\operatorname{Spec} \mathbb{Z}[T]/(T^n - 1)$. Let $n : \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}$ be the map $\mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}$ which takes $u \mapsto u^n$. The sequence

$$0 \to \boldsymbol{\mu}_n \to \mathbb{G}_{\mathrm{m}} \xrightarrow{n} \mathbb{G}_{\mathrm{m}}$$

is clearly exact. However the morphism $n : \mathbb{G}_{\mathrm{m}} \to \mathbb{G}_{\mathrm{m}}$ need not to an be epimorphism in general, because $\Gamma(U, \mathcal{O}_U)^*$ might have an element which is not n-th power locally. But the flat topology is fine enough that

$$0 \to \boldsymbol{\mu}_n \longrightarrow \mathbb{G}_{\mathrm{m}} \xrightarrow{n} \mathbb{G}_{\mathrm{m}} \to 0$$

becomes exact. To prove this, let $U \to S$ be a flat morphism of schemes, and let $a \in \Gamma(U, \mathcal{O}_U)^*$. We may assume that U is affine. Let $V = \operatorname{Spec}(A[T]/(T^n - a))$. Then clearly $V \to U$ is a flat covering of U, and the restriction of a to V is in the image of $n : \mathbb{G}_{\mathrm{m}}(V) \to \mathbb{G}_{\mathrm{m}}(V)$.

The following result paves the road for computing $H^1(X, \boldsymbol{\mu}_n)$.

Theorem 3.2.1 *Let $U = \operatorname{Spec} R$, where R is a local ring, then $H^1(U, \mathbb{GL}_n)$ is trivial.*

Proof. Take $\alpha \in H^1(U, \mathbb{GL}_n)$ then there is a faithfully flat affine U-scheme $V = \operatorname{Spec} B$ of finite type such that $\alpha \in H^1(V/U, \mathbb{GL}_n)$. Let M be the R-module B^n with no other structure. Thus, we have $\mathbb{GL}_n = \mathbf{Aut}(M)$. A twist form of M is some other R-module M' with $M \otimes_R B \cong M' \otimes_R B$. Since $M \otimes_R B$ is flat and finitely generated as a B-module and B is a faithfully flat over R, M' is flat and finitely generate over R. Now since R is local, M' should be free of rank n. Thus the isomorphism class of B/R-forms is trivial, so α is a coboundary. □

Remark 3.2.2 *The above theorem shows in particular that for the local affine scheme X, $H^1(X, \mathbb{G}_{\mathrm{m}})$ is trivial. This is the special case of more general statement namely Hilbert's Theorem 90, that is the canonical map $Pic(X) = H^1(X_{zar}, \mathcal{O}_X^*) \to H^1(X_{fl}, \mathbb{G}_{\mathrm{m}})$ is an isomorphism. The proof involves some techniques in spectral sequences, see for example [6], chapter III, Proposition 4.9.*

Corollary 3.2.3 *Let X be a local affine scheme. Then $H^1(X, \boldsymbol{\mu}_n) \cong \Gamma(X, \mathcal{O}_X)^*/(\Gamma(X, \mathcal{O}_X)^*)^n$.*

Proof. As we have seen above, $H^1(X, \mathbb{G}_{\mathrm{m}})$ is trivial for every local affine scheme X, therefore the exact sequence

$$0 \to \boldsymbol{\mu}_n \longrightarrow \mathbb{G}_{\mathrm{m}} \xrightarrow{n} \mathbb{G}_{\mathrm{m}} \to 0$$

gives rise to the cohomological sequence

$$0 \to \boldsymbol{\mu}_n(X) \to \Gamma(X, \mathcal{O}_X)^* \xrightarrow{n} \Gamma(X, \mathcal{O}_X)^* \to H^1(X, \boldsymbol{\mu}_n) \to 0.$$

and so $H^1(X, \boldsymbol{\mu}_n) \cong \Gamma(X, \mathcal{O}_X)^*/(\Gamma(X, \mathcal{O}_X)^*)^n$.□

Chapter 4

There is No Extension of $E[p^n]$ to $\bar{U}$

If G' and G'' are finite locally free group schemes over $\operatorname{Spec} R$, we consider the group functor $\mathbf{Hom}(G'', G')$ defined for any R-algebra S by

$$\mathbf{Hom}(G'', G')(S) = \operatorname{Hom}_S(G''_S, G'_S) \qquad \text{(group scheme homomorphisms)}.$$

We shall say that a group scheme G is an *extension of G'' by G'* if G sits in a short exact sequence

$$1 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 1. \tag{4.1}$$

An extension is *trivial* if it admits a splitting $G'' \to G$. A morphism between two extensions G and $\tilde{G}$ of G'' by G' is a homomorphism $\alpha : G \to \tilde{G}$ such that

$$\begin{array}{ccccccccc} 1 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G'' & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \alpha} & & \| & & \\ 1 & \longrightarrow & G' & \longrightarrow & \tilde{G} & \longrightarrow & G'' & \longrightarrow & 1. \end{array}$$

Notice that a morphism of extensions is always an isomorphism. We show the set of isomorphism classes of extensions of G' by G'' with $\operatorname{Ext}^1(G'', G')$.

Theorem 4.1 *There is a morphism $H^1(R, \mathbf{Hom}(G'', G')) \to \operatorname{Ext}^1(G'', G')$. Moreover if R has characteristic $p > 0$, G' is an infinitesimal group scheme, and G' is a finite étale group scheme, then this morphism is a bijection.*

Proof. Let S be a faithfully flat R-algebra. Set $H = G''_{S\times S} \times G'_{S\times S}$, by the universal property of fiber product morphisms $G''_{S\times S} \to G'_{S\times S}$ and $id_{G''}$ give a section $\varphi' : G''_{S\times S} \to H$. This morphism and the section $\sigma : G'_{S\times S} \to H$, which is identity on the second factor, give a morphism $H \to H \times_{S\times S} H$. Composing with the multiplication of H, we get an automorphism of H. One can easily see that for any R-algebra B, this morphism can be described as follows:

$$\psi(\varphi)(B) : G''_{S\times S}(B) \times G'_{S\times S}(B) \to G'_{S\times S}(B) \times G'_{S\times S}(B)$$

taking $(g,x) \mapsto (g, \varphi(g).x)$.
So we get a morphism of group functors $\psi : \mathbf{Hom}(G'', G') \to \mathbf{Aut}(G'' \times G')$, but we need to verify that this morphism takes cocycles to cocycles and cohomologus elements to cohomologus ones.

Assume that φ is a cocycle, i.e. φ satisfies $d^1\varphi = d^0\varphi d^2\varphi$. Let us write $\rho = \psi(\varphi)$ then clearly $d^1\rho(g,x) = (g, x \cdot d^1\varphi) = (g, x \cdot d^0(\varphi)d^2(\varphi)(g)) = d^0\rho d^2\rho$, notice that $d^i\rho = \psi(d^i\varphi)$. Now suppose that $\widetilde{\varphi}$ is cohomologous to φ, so there is a $\lambda \in \mathbf{Hom}(G'', G')(S)$ such that $\widetilde{\varphi} = d^0\lambda\varphi(d^1\lambda)^{-1}$ and therefore $\psi(\widetilde{\varphi}) = \psi(d^0\lambda\varphi(d^1\lambda)^{-1})$, hence $\psi(\widetilde{\varphi})(g,x) = (g, d^0\lambda\varphi(d^1\lambda)^{-1})$. Thus we have $\psi(\widetilde{\varphi}) = d^0\psi(\lambda)(\psi(\varphi))(d^1\psi(\lambda))^{-1}$, so we may deduce that $\psi(\widetilde{\varphi}) \sim \psi(\varphi)$. Finally we deduce that for a cocycle $\varphi \in H^1(S/R, \mathbf{Hom}(G'', G'))$, $\psi(\varphi)$ is a cocycle in $H^1(S/R, \mathbf{Aut}(G'' \times G'))$. Hence by Theorem 3.1.1 we can conclude that $\psi(\varphi)$ represents a twisted form G_φ of $G'' \times G'$ which is an extension of G'' by G'. We now define $H^1(S/R, \mathbf{Hom}(G'', G')) \to \mathrm{Ext}^1(G'', G')$ by mapping φ to the class $[G_\varphi]$.

Set $G'' = \operatorname{Spec} A''$ and $G' = \operatorname{Spec} A'$. Let $G = \operatorname{Spec} A$ be an extension of G'' by G'. Write M'', M' and M for the respective augmentation ideals. Consider the following exact sequence:

$$0 \longrightarrow M' \longrightarrow A' \xrightarrow{\varepsilon} R \longrightarrow 0$$

which admits a splitting $e : R \to A'$, therefore we have $A' \cong R \oplus M'$ as R-modules. Since M' is direct summand of A' which is locally free, M is locally projective which is the same as locally free. Similarly we see that M'' is locally free. The exact sequence:

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

shows that M is also projective. Now consider the decomposition $A = R \oplus M$, restricting the morphism F_A^m to M gives us a morphism $F^m : M \otimes R \to M$. Then composing with σ^m-linear morphism $M \to M \otimes_{\sigma^m} R$ which takes $m \mapsto m \otimes 1$. Conversely having such a morphism $M \to M \otimes_{\sigma^m} R$ we get a factorization through $M \otimes_{\sigma^m} R$. Hence the data of $F^m_{G/R} : G \to G^{(p^m)}$ is equivalent to the data of an additive map $\psi : M \to M$ which is σ^m-linear. Clearly we have the similar arguments for $M'$and M''. Note that $F^m_{A''}$ is an isomorphim because G'' is étale and note also that G' is a finite infinitesimal group scheme so we may take m enough big such that the induced morphism $F^m_{A'}$ vanishes. So we deduce:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & M'' & \xrightarrow{i} & M & \xrightarrow{h} & M' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle 0} & & \\
0 & \longrightarrow & M'' & \xrightarrow{i} & M & \xrightarrow{h} & M' & \longrightarrow & 0
\end{array}$$

Lemma 4.2 *The extension (4.1) splits if and only if the canonical map of R-modules $\ker\psi \to M'$ is surjective.*

Proof. Suppose that the extension (4.1) splits, so we have a morphism $\tau : M' \to M$ such that $h \circ \tau = id_{M'}$. Take $m' \in M'$ then $\psi \circ \tau(m') = 0$, thus $\psi \circ \tau(m') \in Im(i)$, let $\psi \circ \tau(m') = i(m'')$. Set $m = \tau(m' - i(m''))$ then clearly $h(m) = m'$ and $\psi(m) = 0$ so $\ker\psi \to M'$ is surjective.

Conversely suppose $\ker\psi \to M'$ is surjective. Take $m' \in M'$ and assume that there are two elements m_1 and m_2 in $\ker\psi$ such that $\psi(m_1) = \psi(m_2) = m'$, therefore $m_1 - m_2$ maps to zero

via h and ψ, so it comes from $z \in M''$ which should map to zero by f. But f is an isomorphism because G'' is étale therefore z is zero itself, and thus $m_1 = m_2$. Hence $\ker\psi \to M'$ is an isomorphism and therefore (4.1) splits.$\square$

Using Corollary 1.5.2 we see that there is a finite R-algebra R' such that G' becomes constant group scheme over R'. Then M'' is isomorphic to R'^n for some $n > 0$, and clearly ψ takes the canonical basis of R'^n to itself.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M'' = \bigoplus_1^n Rz_i & \xrightarrow{i} & M & \xrightarrow{h} & M' = \bigoplus_1^m Re_i & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle \psi} & & \downarrow{\scriptstyle 0} & & \\ 0 & \longrightarrow & M'' = \bigoplus_1^n Rz_i & \xrightarrow{i} & M & \xrightarrow{h} & M' = \bigoplus_1^m Re_i & \longrightarrow & 0 \end{array}$$

Let $M' = \bigoplus_1^m Re_i$ and $M'' = \bigoplus_1^n Rz_i$. Put $l = p^m$. Take $\{x_j\}$ such that $\psi(x_j) = e_i$. Since $h \circ \psi(x_j) = 0$, $\psi(x_j) = g(\Sigma_1^s r_i z_i)$ for some r_i's in R. Set $S = R[x_1, ..., x_s]/(x_1^l - r_1, ..., x_s^l - r_s)$ and let us write $1 \otimes x_i = r_i^{(1/l)}$. Hence $\psi(x_j) = g(\Sigma_1^s r_i z_i) = g(f(\Sigma r_i^{(1/l)} z_i)) = \psi \circ g(\Sigma r_i^{(1/l)} z_i)$. Note that $\psi(x_j) - \Sigma r_i^{(1/l)} g(z_i) = 0$ and $h((x_j) - \Sigma r_i^{(1/l)} \cdot g(z_i)) = e_i$. Therefore the restriction of h to $\ker\psi$ is surjective and therefore (4.1) splits by the above lemma. Hence the class $[G]$ of G in $\mathrm{Ext}^1(G'', G')$ is determined by a cocycle $\varphi \in H^1\left(S/R, \mathbf{Hom}(G'', G')\right)$.$\square$

Let us return to the case in which we considered the extension of $G'' = \ker V^n$ by its dual $G' = \ker F^n$). As an application of Proposition 1.5.1 we saw that we can base change in way that the étale group scheme G'' becomes isomorphic to the constant group scheme$\underline{(\mathbb{Z}/p^n\mathbb{Z})}$ and therefore its dual G' becomes isomorphic to $\boldsymbol{\mu}_{p^n}$. So the above theorem tells us that these extensions correspond to cocycles in $H^1\left(S/R, \mathbf{Hom}(G'', G')\right) = H^1\left(S/R, \mathbf{Hom}(\underline{(\mathbb{Z}/p^n\mathbb{Z})}, \boldsymbol{\mu}_{p^n})\right) = H^1\left(S/R, \boldsymbol{\mu}_{p^n}\right)$. Recall that in section §2 we have shown that in exact sequence:

$$1 \longrightarrow \ker F^n \longrightarrow E[p^n] \longrightarrow \ker V^n \longrightarrow 1$$

the étale (resp.local) group scheme $\ker V^n$(resp. $\ker F^n$) over U can be extend to the étale (resp. local) group scheme $\overline{\ker V^n}$ (resp. $\overline{\ker F^n}$) over $\bar{U}$. One might naturally ask that whether $E[p^n]$ does extend too? I.e. whether $E[p^n]$ extend to the group scheme $\overline{E[p^n]}$ sitting in short exact sequence

$$1 \longrightarrow \overline{\ker F^n} \longrightarrow \overline{E[p^n]} \longrightarrow \overline{\ker V^n} \longrightarrow 1$$

Theorem 4.3 *There is no extension for $E[p^n]$ over $\overline{U} = \mathbb{P}^1 - \mathcal{S}$, where $\mathcal{S}$ is the set of supersingular values of $j \in k$.*

Proof. We keep the notation of Theorem 4.1. Meanwhile, we essentially follow the procedure involved in the last part of Theorem 4.1 to determine the class $[E[p^n]] \in H^1\left(S/K, \boldsymbol{\mu}_{p^n}\right)$ explicitly, where $K = k((j))$. So $B^{(p^n)} = K[x, y]/(f_q^{(p^n)})$ and therefore $B^{(p^n)} = K[x, y]/(f_q^{(p^n)})$, where f_q is the equation of Tate curve E_q. As we have seen in §2, $\ker V^n$ corresponds to $\{q^i\}_{0,...,p^n-1} \subset K^*/(q^{p^n})^{\mathbb{Z}} \cong E_q^{(p^n)}$. Let $q_i = (x_i, y_i) = (X(q^i, q^{(p^n)}), Y(q^i, q^{(p^n)}))$. One can verify

easily that y_i's are distinct. The morphism of algebras corresponding to the closed immersion $ker(V^n) \to E^{(p^n)}$ can be described as follows:
It is the map $B^{(p^n)} \to \bigoplus K(q_i)$, which takes $a \mapsto (a(q_i))$, where $a(q_i)$ is the evaluation of a at q_i.

Let us take elements $b_i \in B^{(p^n)}$ lifting the canonical basis $\{z_i\}$ of $\bigoplus K(q_i)$ by setting $b_i = \frac{\prod_{j\neq i}(y-y_j)}{\prod_{j\neq i}(y_i-y_j)}$. Clearly we have $b_i(q_j) = \delta_{ij}$. Note that $F_B^n : B^{(p^n)} \to B$ takes $b_i \mapsto c_i = \frac{\prod_{j\neq i}(y^{(p^n)}-y_j)}{\prod_{j\neq i}(y_i-y_j)}$, so the induced morphism $\tilde{F}^n : E[p^n] \to kerV^n$ gives the algebra morphism:

$$\bigoplus K(q_i) \longrightarrow B \otimes_{V\circ F} K(e),$$

$$z_i \mapsto \bar{c_i} = c_i \otimes 1$$

Notice that we have $\bar{c_i} \cdot \bar{c_j} = \delta_{ij}$. Let e' be the zero element of $E^{(p^n)}$. One also easily verifies that the morphism $B^{(P^n)} \otimes K(e') \to K[y]/(y^{p^n} - 1)$ sending $y \otimes 1$ to y is an isomorphism. So we have the following diagram of algebras analogous to the diagram (2.1).

$$\begin{array}{ccccc}
B^{(p^n)} & \longrightarrow & B & \longrightarrow & B \otimes K(e') \\
\downarrow & & \downarrow & & \| \\
B^{(p^n)} \otimes K(e) & \longrightarrow & B \otimes K(e) & \longrightarrow & B \otimes K(e') \\
\downarrow \cong & & \| & & \cong \downarrow \\
\bigoplus K(q_i) & \longrightarrow & B \otimes K(e) & \longrightarrow & K[y]/(y^{p^n} - 1)
\end{array}$$

Clearly y comes from $y \otimes 1$ via h and we have $y^{p^n} = \sum_i y_i \cdot c_i \otimes 1$. This gives us the system of equations $\{T^{p^n} = y_i\}$. Similarly for y^2 we have

$$(y^2)^{p^n} \otimes 1 = (\sum_i y_i \cdot c_i)^2 \otimes 1 = \sum_i y_i^2 \cdot c_i \otimes 1$$

so we get the equations $\{T^{p^n} = y_i^2\}$ so we may reduce to the previous case $\{T^{p^n} = y_i\}$ where $y_i = Y(q^i, q^{p^n})$. As we mentioned in Remark 1.7.2 there is an alternative expression of $Y(u, q)$:

$$Y(u,q) = \frac{u^2}{(1-u)^3} + \sum_{n\geq 1}\left(\frac{(q^n u)^2}{(1-q^n u)^3} - \frac{q^n u^{-1}}{(1-q^n u^{-1})^3} + \frac{q^n}{(1-q^n)^2}\right)$$

we realize that we only need to add the p^n-th root of q. Therefore we may reduce to the equation $T^{p^n} = q$.

Suppose now that there exist a finite flat group scheme G, extending $E[p^n]$ over $\overline{U}$. Changing the base to $Y = \operatorname{Spec} k[[q]]$, we get a group scheme over Y, meanwhile we denote it again by G, extending $E[p^n]/K$, where $K = k((q))$. As remarked at the end of section 1.3, such a G over henselian base scheme is an extension of a local group scheme by an étale group scheme and it then gives an extension of $\overline{\ker V^n}$ by $\overline{\ker F^n}$. Theorem 4.1 and the discussion before the proposition imply that it would be enough to show that there does not exist a class $[G] \in H^1(S/R, \boldsymbol{\mu}_{p^n})$ for every S/R that mapping to $[E[p^n]]$ via the canonical morphism

$$H^1(S/R, \boldsymbol{\mu}_{p^n}) \longrightarrow H^1(S \otimes K/K, \boldsymbol{\mu}_{p^n})$$

As it did turn out from the above computations, the class $[E[p^n]]$ is represented by the equation $T^{p^n} = q$, but this is not a $\boldsymbol{\mu}_{p^n}$-torsor over R, since q is not invertible. Note that if there is an $f \in R^*$ which represents the same class, then Corollary 3.2.3 asserts that there is an element $g \in K^*$ such that $q = g^{p^n} \cdot f$, meaning $q \in R^*$, which is a contradiction. Hence we may conclude that there is not such a class that lifts $[E[p^n]]$ and therefore there is no extension for $E[p^n]$ over $\overline{U}$.$\square$

Bibliography

[1] A. Grothendieck, *Séminaire de Géométrie Algébrique, Revetments étales et groupe fondamental (1960-61)*. Lecture Notes in Math. vol. 224, Springer, 1971.

[2] A. Grothendieck, *Séminaire de Géométrie Algébrique, Schemes en Groupes (1960-61)*. Lecture Notes in Math. vol. 151, Springer, 1971.

[3] G. van der Geer and B. Moonen, *Abelian Varieties*, in preparation (http://staff.science.uva.nl/ bmoonen/boek/BookAV.html)

[4] Jean-Benoît Bost, *Courbes semi-stables et groupe fondamental en géométrie algébrique*, Birkhäuser Verlag, 1998.

[5] Q. Liu, *Algebraic Geometry and Arithmetic Curves*, Oxford University Press, 2002.

[6] J.S. Milne, *Étale Cohomology*, Princeton University Press, 1980.

[7] G. Cornell, *Modular Forms and Fermat's Last Theorem*, Springer, 1997.

[8] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1985.

[9] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, 1994.

[10] W.C. Waterhouse, *Introduction to Affine Group Scheme*, Springer, 1979.