INTEGRAL MODELS OF MODULAR CURVES AND THEIR REDUCTION MODULO p

Mémoire of Master 2, defended on June 20th, 2016

HUANG YU-LIANG [1]

[1] Email: mega.seraphus@gmail.com

Acknowledgements

I am grateful to my thesis supervisor Prof. MATTHIEU ROMAGNY (Université de Rennes 1) for introducing this very interesting subject to me, his guidance and innumerable helps. I would also like to thank Xavier CARUSO and Bernard LE STUM for being members of my thesis jury.

I would like to thank the organizers of *Lebesgue Master's Program* and *Fédération Recherche Mathématiques des Pays de Loire* for giving me such a great opportunity to study mathematics in the west of France.

Contents

1

Introduction: Historical Summary and Current State

Modular curves and their integral models have been intensively studied over the last few decades, not only for its applications in arithmetic questions, but also for its own geometric interests. In order to treat the Ramanujan conjecture for exceptional primes, Igusa studied in details about the moduli schemes of elliptic curves with level N structures over $\mathbb{Z}[\frac{1}{N}]$ in his a series of papers [12], [11], [13], [14], and he obtained most of the main results, but no essential progress in understanding the case at “bad” prime p, i.e., the case that $p|N$.

In Deligne and Rapoport’s paper [27], they use the language of algebraic stacks systematically in moduli problems of elliptic curves, and studied the compactification of the modular curves over $\mathbb{Z}[\frac{1}{N}]$, namely, the moduli spaces that parameterize the so called *generalized elliptic curves* with level structures, also with modular interpretation at the cusps, namely, they parameterizes the *Néron polygons* with level structures. At that time, the level structure was still in the naïve sense, which can hardly apply to the elliptic curves over bad primes.

In his paper [35], Drinfeld made the innovation, he introduced the general idea of level structure, which is the so called Drinfeld level structure. Though originally his theory is served for elliptic modules, the idea can apply to usual elliptic curves without any difficulties, and was known to many experts at that time. The advantage of Drinfeld level structure is that it uses subgroup schemes, instead of subgroups, which can be easily applied to the elliptic curves over bad primes. In 1985, Katz and Mazur concluded the results of modular curves over $\mathbb{Z}$ in their significant book [24], and analyzed the reduction modulo bad prime of the modular curves. Though Katz and Mazur studied the compactification of modular curves over $\mathbb{Z}$, their normalization process does not admit modular interpretations.

In order to fully understand the subject, one needs to not only construct proper flat models of modular curves, but also ensure the modular interpretation at the cusps. In an unpublished paper of Edixhoven [15], he treated the case for the level structures $\Gamma(N)$, $\Gamma_1(N)$ and $\Gamma_0(n)$ with square-free n, and some mixtures of then, in which he showed that the modular curves are all proper flat regular Deligne-Mumford stacks. In 2007, Conrad successfully eliminated the defects in his paper [6], he used a different approach, and constructed moduli stacks of generalized elliptic curves with Drinfeld level structures, which turn out to be proper Artin stakcs. Recently, in a preprint of Česnavičius [19], he constructed a refinement of the moduli stack $\mathscr{X}_0(n)$ with arbitrary n (not necessarily square-free) which admits modular interpretation, and also gave different proofs of the main results in Conrad's paper [6]. So far the subject is basically well-understood.

Organization of the thesis

In this article, we will only deal with open modular curves over $\mathbb{Z}$, following Katz-Mazur [24]. Moreover, we adopt the language of algebraic stacks, to discuss various moduli problems of elliptic curves.

- **Chapter 2**: In this chapter, we carefully develop the general theory of A-structures and A-generators, together with their representability results. In the last section, we turn to focus on the four basic Drinfeld level structures, which play the central roles in the later parts.
- **Chapter 3**: In this chapter, firstly we formulate the setting of moduli theory using the language of algebraic stacks. The main results are the representability theorem and regularity theorem for modular curves. We prove the regularity theorem for the modular curves $\mathscr{Y}(N)$, $\mathscr{Y}_1(N)$ and $\mathscr{Y}_1^{\mathrm{bal}}(N)$ in the current chapter. As for the case of $\mathscr{Y}_0(N)$, it requires deeper understanding about cyclic group schemes, which is the central topic of **Chapter 4**. In the last section, we study the relations and induced morphisms between modular curves.
- **Chapter 4**: We study in details about the theory of cyclic group schemes in this chapter, especially about the scheme of generators, and the structure of cyclic isogenies.
- **Chapter 5–6**: In the last two chapters, firstly we introduce the Igusa curve and exotic Igusa curves in **Chapter 5**, which form the "building blocks" of the reduction modulo p of modular curves. Combine the results that we developed in previous parts, we analyze the reduction modulo p of modular curves in details, and summarize the results in the last section.

What's next?

Elliptic curves can be generalized at least in two directions, namely,

(1) as abelian varieties of dimension $g = 1$, and

(2) as algebraic curves of genus $g = 1$.

For the first case, we shall deal with the moduli spaces of abelian varieties $\mathscr{A}_g(N)$ of dimension g with level N structures. And in the second case, we need to construct appropriate level N structures on the moduli spaces of curves $\mathscr{M}_g$ of genus g, and study their reduction modulo bad primes. Things are more complicated in both cases, and few works are available so far.

In the work of Abramovich and Romagny [8], they constructed a proper model of $\mathscr{M}_g(p)$, but there are still some properties that we need to prove, like flatness, regularity, etc., and furthermore, the study of its reduction modulo p. In general case, i.e., with level p^n for $n > 1$, it is still a problem to construct appropriate level structures.

2
Drinfeld Level Structure

Firstly we shall explain the motivation of Drinfeld level structure.

The modular group $SL_2(\mathbb{Z})$ and its congruence subgroups naturally act on the Poincaré half plane $\mathscr{H}$. The resulting quotient $\Gamma \setminus \mathscr{H}$ is a noncompact Riemann surface (denoted by $Y(\Gamma)$), and the term *modular curve* (over $\mathbb{C}$) is sometimes also used to refer to the compactification $X(\Gamma)$ of $Y(\Gamma)$, which is done by adding *cusps* of the congruence subgroup Γ.

Among all the congruence subgroups of $SL_2(\mathbb{Z})$, there are so called *full congruence subgroups*

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a \equiv d \equiv 1 \ (\mathrm{mod}\ N), \ c \equiv b \equiv 0 \ (\mathrm{mod}\ N) \right\}$$

where N is the level. There are also other interesting congruence subgroups

$$\begin{aligned} \Gamma_0(N) &:= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, c \equiv 0 \ (\mathrm{mod}\ N) \right\} \\ \Gamma_1(N) &:= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a \equiv d \equiv 1 \ (\mathrm{mod}\ N), \ c \equiv 0 \ (\mathrm{mod}\ N) \right\}, \end{aligned}$$

which play important roles in arithmetic geometry. The resulting modular curves of the above congruence subgroups have nice modular interpretations, i.e., they parameterize elliptic curves with some additional structures:

- The (open) modular curve $Y(N) := Y\big(\Gamma(N)\big)$ parameterizes elliptic curves with a *level N structure*, which is an isomorphism between $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ and N-torsion points.
- The (open) modular curve $Y_0(N) := Y\big(\Gamma_0(N)\big)$ parameterizes elliptic curves with a cyclic subgroup of order N.
- The (open) modular curve $Y_1(N) := Y\big(\Gamma_1(N)\big)$ parameterizes elliptic curves with a point of exact order N, or equivalently, an injective homomorphism to the subgroup of N-torsion points of an elliptic curve E

$$\mathbb{Z}/N\mathbb{Z} \longrightarrow E[N].$$

The situation over an algebraically closed field is well-behaved, but if we replace it by an arbitrary scheme, i.e., we consider the moduli problems of elliptic curves over general base with additional structures, then the notion such as a *cyclic subgroup of order N* is no longer worked out well.

For example, a supersingular elliptic curve over a field k of characteristic p has no non-trivial k-rational p^n-torsion points, hence such elliptic curves have no "naïve" level p^n structures. In general case, it is more reasonable to consider subgroup schemes rather than subgroups.

However, one cannot simply replace "a cyclic subgroup of order N" by "a subgroup scheme of rank N over the base" neither, because generally there are too many such subgroup schemes. The most important features that they should capture are "cyclicity" and "exact orders", i.e., we need to develop these concepts in the setting of finite locally free group schemes. This leads to the notion of Drinfeld level structure.

2.1 Points of "exact order N" and cyclic group schemes

Suppose C/S is a smooth curve over S together with a structure of commutative S-group scheme. A point $P \in C(S)$ has *"exact order N"* if the effective Cartier divisor

$$D := \sum_{i=1}^{N} [iP]$$

is a subgroup scheme of C/S, in which case we call D the *cyclic subgroup scheme* "generated" by P.

Definition 2.1.1. *A closed subgroup scheme $G \subset C$ which is finite locally free of rank N is called* ***cyclic****, if there exists some fppf morphism $T \to S$ and a point $P \in C(T)$ of exact order N such that P generates the subgroup scheme G_T/T, i.e., fppf-locally, G admits a "generator".*

Like in the theory of finite groups, we also have the "Lagrange theorem" for finite flat commutative group schemes.

Lemma 2.1.2. *If $P \in C(S)$ has exact order N, then $N \cdot P = 0$.*

The lemma is implied from the following theorem

Theorem 2.1.3 (Deligne)**.** *Any finite flat commutative S-group scheme of rank N is killed by N.*

Proof: The proof is according to [17], which is originally due to P. Deligne.

Let G be a finite locally free commutative S-group scheme of rank N. We need only to prove that for any section $u \in G(S)$, $u^N = 1$. Before the demonstration, we firstly define the *trace map* of a finite morphism $f : T \to S$, where T is a finite S-scheme with structure morphism f.

By our assumption, the structure morphism $G \to S$ is finite which is automatically affine, hence G has the form $\mathsf{Spec}\ (\mathscr{A})$, where $\mathscr{A}$ is a finite $\mathscr{O}_S$-algebra of rank N. Similarly, $T = \mathsf{Spec}\ (\mathscr{B})$ with $\mathscr{B}$ a finite $\mathscr{O}_S$-algebra, say with rank m. On the one hand, we have the following inclusion

$$G(S) = \mathsf{Hom}_{\mathfrak{Sch}_{/S}}(S, G) = \mathsf{Hom}_{\mathscr{O}_S\text{-}\mathfrak{Alg}}(\mathscr{A}, \mathscr{O}_S) \hookrightarrow \mathsf{Hom}_{\mathscr{O}_S}(\mathscr{A}, \mathscr{O}_S) = \mathscr{A}^\vee(S),$$

on the other hand, there is the norm map of commutative $\mathscr{A}^\vee$-algebras

$$N\colon\ \mathscr{B}(S)\otimes_{\mathscr{O}_S(S)}\mathscr{A}^\vee(S)\ \longrightarrow\ \mathscr{A}^\vee(S).$$

Now let us define the trace map Tr_f of f as the unique map such that the diagram

$$\begin{tikzcd}
G(T) \arrow[r, hook] \arrow[d, "\mathsf{Tr}_f"] & (\mathscr{O}_T\otimes_{\mathscr{O}_S}\mathscr{A}^\vee)(T) = (\mathscr{B}\otimes_{\mathscr{O}_S}\mathscr{A}^\vee)(S) \arrow[d, "N"] \\
G(S) \arrow[r, hook] & \mathscr{A}^\vee(S)
\end{tikzcd}$$

commutes. The uniqueness is obvious, since Tr_f is given by nothing but the restriction of the norm map N. From our definition, it is also clear that the trace map is a group homomorphism. Moreover, the norm map is invariant under composing with an $\mathscr{O}_S(S)$-automorphism, say ϕ, of $\mathscr{B}(S)$, since the left multiplication by some element $b\in\mathscr{B}(S)$ is conjugate with that by $\phi(b)$

$$\begin{tikzcd}
\mathscr{B}(S)\otimes_{\mathscr{O}_S(S)}\mathscr{A}^\vee(S) \arrow[r, "b\times"] \arrow[d, "\phi\otimes 1"'] & \mathscr{B}(S)\otimes_{\mathscr{O}_S(S)}\mathscr{A}^\vee(S) \arrow[d, "\phi\otimes 1"] \\
\mathscr{B}(S)\otimes_{\mathscr{O}_S(S)}\mathscr{A}^\vee(S) \arrow[r, "\phi(b)\times"] & \mathscr{B}(S)\otimes_{\mathscr{O}_S(S)}\mathscr{A}^\vee(S)
\end{tikzcd}$$

which shows that the norm map is independent with ϕ, since two conjugate matrices have the same determinant.

Back to the theorem. We denote r_u for the right multiplication by u

$$\begin{tikzcd}
G\times_S S \arrow[r, "(\mathsf{id}_G{,}\,u)"] & G\times_S G \arrow[d] \\
G \arrow[u, "\wr"] \arrow[r, "r_u"] & G
\end{tikzcd}$$

Consider the case that $T=G$, and now f is the structure morphism $G\to S$, the diagram becomes

$$\begin{tikzcd}
G(G) \arrow[r, hook] \arrow[d, "\mathsf{Tr}_f"] & (\mathscr{A}\otimes_{\mathscr{O}_S}\mathscr{A}^\vee)(S) \arrow[d, "N"] \\
G(S) \arrow[r, hook] & \mathscr{A}^\vee(S)
\end{tikzcd}$$

Consider $\mathsf{id}_G\in G(G)$. Notice that $\mathsf{Tr}_f(1_G)=\mathsf{Tr}_f(1_G\circ r_u)$, because r_u is a S-automorphism of G. Moreover we have

$$\mathsf{id}_G\circ r_u\ =\ \mathsf{id}_G\times f^*u,$$

where the "×" on the right side is the multiplication in the group $G(G)$, this can be easily deduced from the following commutative diagram

$$\begin{tikzcd}
 & G\times_S G \arrow[d, "(\mathsf{id}_G{,}\,f)"] \arrow[rd, "(\mathsf{id}_G{,}\,f^*u)"] & & \\
G \arrow[ru, "\Delta"] \arrow[r, "\sim"] & G\times_S S \arrow[r, "(\mathsf{id}_G{,}\,u)"] & G\times_S G \arrow[r, "m"] & G,
\end{tikzcd}$$

where the composition of the bottom line is the left side, and

$$G \xrightarrow{\Delta} G \times_S G \xrightarrow{(\mathrm{id}_G, f^* u)} G \times_S G \xrightarrow{m} G$$

is the right side. Thus

$$\begin{aligned} \mathrm{Tr}_f(\mathrm{id}_G) &= \mathrm{Tr}_f(\mathrm{id}_G \circ r_u) \\ &= \mathrm{Tr}_f(\mathrm{id}_G \times f^* u) \\ &= \mathrm{Tr}_f(\mathrm{id}_G) \times \mathrm{Tr}_f(f^* u) \\ &= \mathrm{Tr}_f(\mathrm{id}_G) \times u^N, \end{aligned}$$

which shows $u^N = 1$ after cancelling $\mathrm{Tr}_f(\mathrm{id}_G)$. □

Remark: Unlike abstract groups, a S-valued point of a finite locally free commutative S-group scheme can have many different exact orders. For example, let S be a $\mathbb{F}_p$-scheme, in the case which we have the relative Frobenius morphism $F_{C/S}$. Then the zero section $0 \in C(S)$ has exact order p^n for any integer $n \geqslant 1$, because the section 0 generates the S-subgroup scheme $\ker(F^n_{C/S})$.

Lemma 2.1.4. *Let G be a finite locally free commutative group scheme of rank N over a henselian local ring R, with maximal ideal $\mathfrak{m}$ and residue field k, where the characteristic of k is prime to N (including the case of zero characteristic). Then G is étale over R.*

Proof: See Tate [16] 3.7 (II).

Lemma 2.1.5. *Suppose S is a $\mathbb{Z}[\frac{1}{N}]$-scheme, and $P \in C(S)$ is a point satisfying $N \cdot P = 0$. Then the following conditions are equivalent:*

(1) P has exact order N in C/S;

(2) For every geometric point Spec $(k) \to S$, the point $P_k \in C(k)$ has exact order N in C_k/k;

(3) For every geometric point Spec $(k) \to S$, the point P_k has exact order N in the usual sense, equivalently, $\{aP_k\}_{a=1}^N$ is a subgroup (as an abstract group) of $C(k)$ with exactly N elements;

(4) The effective Cartier divisor $\sum_{a=1}^N [aP]$ in C/S is finite étale over S;

(5) The S-group morphism

$$\begin{array}{ccc} \mathbb{Z}/N\mathbb{Z} & \longrightarrow & C \\ 1 & \longmapsto & P \end{array}$$

is a closed S-immersion, and it identifies the constant S-group scheme $\mathbb{Z}/N\mathbb{Z}$ with the effective Cartier divisor $\sum_{a=1}^N [aP]$.

Proof: (1) $\Longrightarrow$ (2): Being a subgroup scheme is stable under base changes, i.e.

$$[P_k] + [2P_k] + ... + [NP_k]$$

is a closed k-subgroup scheme of C_k/k, hence P_k has exact order N as required.

(2) $\Longrightarrow$ (3): Thanks to the Lemma 2.1.4, since N is invertible on S, the k-subgroup scheme $D_k = \sum_{a=1}^{N}[aP_k]$ is étale over k. The number of geometric points on D_k is then equal to its rank N, which implies that $\{aP_k\}_{a=1}^{N}$ are all distinct.

(3) $\Longleftrightarrow$ (4): The condition (3) is equivalent to say that all geometric fiber D_k is étale over k. This is already an equivalent condition of $D = \sum_{a=1}^{N}[aP]$ being étale over S (cf. [5] EGA IV$_4$, Corollaire (17.6.2) (c")).

(3) $\Longleftrightarrow$ (5): We can certainly define the homomorphism between abstract groups

$$\begin{array}{ccc} \mathbb{Z}/N\mathbb{Z} & \longrightarrow & C(S) \\ 1 & \longmapsto & P \end{array}$$

and then induces the S-group homomorphism

$$\Psi : \mathbb{Z}/N\mathbb{Z} \longrightarrow C.$$

The image of Ψ is the effective Cartier divisor D, it suffices to prove is that Ψ is a closed immersion if and only if Ψ_k is a closed immersion over any geometric point $\mathsf{Spec}\,(k) \to S$. The latter assertion is equivalent to say that $\{aP_k\}_{a=1}^{N}$ are N distinct points in $C(k)$.

Closed immersion is preserved under base changes, hence (5) $\Longrightarrow$ (3). For the opposite direction, notice that being a closed immersion is a local property for the target, we may assume $S = \mathsf{Spec}\,(R)$ where R is a local ring, and then $D = \mathsf{Spec}\,(A)$ for some finite R-algebra A of rank N which is free as a R-module. The S-group homomorphism is then given by

$$\Psi^* : A \longrightarrow R^N$$

between R-algebras of rank N. Let us denote $d = \det(\Psi^*) \in R$ to be the determinant of the R-linear map Ψ^*. The condition (3) says that for any geometric point,

$$\Psi^* : A_k \longrightarrow k^N$$

is an isomorphism of R-algebras, i.e., d_k is a unit for any k. Indeed, d can't belong to the unique maximal ideal $\mathfrak{m}$ of R, otherwise over the geometric point given by

$$R \twoheadrightarrow R/\mathfrak{m} = \kappa \hookrightarrow \bar{\kappa},$$

$d_{\bar{\kappa}}$ would be 0. Thus $d \in R - \mathfrak{m}$ is a unit, which means Φ^* is an isomorphism, i.e., (3) $\Longrightarrow$ (5).

(5) $\Longrightarrow$ (1): This is trivial, since in the condition (5), D already has a structure of S-subgroup scheme. □

Remark: If we remove the condition that S being a $\mathbb{Z}[\frac{1}{N}]$-scheme, we will only have the following implications

$$(3) \Longleftrightarrow (4) \Longleftrightarrow (5) \Longrightarrow (1) \Longrightarrow (2),$$

since we used that condition only in the step (2) $\Longrightarrow$ (3). It also tells us that we cannot simply define the level N structure of an elliptic curve E/S as an isomorphism

$$\mathbb{Z}/N\mathbb{Z} \longrightarrow E[N],$$

because the isomorphism may not exist if N is not invertible on the base.

2.2 A-structures, A-generators and representability theorems

Now we are ready to define general “level structures”. Let C/S be a smooth curve over S with a structure of commutative S-group scheme, and A an abstract finite abelian group.

Definition 2.2.1. *An A-**structure** on C/S is a homomorphism*

$$\phi\colon A \longrightarrow C(S)$$

*of abstract abelian groups, such that the effective Cartier divisor $D = \sum_{a\in A}[\phi(a)]$ is a S-subgroup scheme of C/S. In this case, D is called an A-**subgroup** of C/S generated by ϕ, where ϕ is called an A-**generator** of the subgroup scheme D.*

Definition 2.2.2. *A closed S-subgroup scheme $G \subset C$ which is finite locally free over S of rank $\#(A)$ is called an A-**subgroup** if there exists a fppf morphism $T \to S$ and an A-structure*

$$\phi\colon A \longrightarrow C_T(T)$$

on C_T, such that ϕ generates the T-subgroup scheme G_T of C_T.

If we let $A = \mathbb{Z}/N\mathbb{Z}$, then given a point of exact order N in $C(S)$ is equivalent to give a $\mathbb{Z}/N\mathbb{Z}$-structure on C/S, with specifying the image of $1 \in \mathbb{Z}/N\mathbb{Z}$ as the point having exact order N. So we can restate the Lemma 2.1.5 as following

Lemma 2.2.3. *Suppose $\phi: A \to C(S)$ is a group homomorphism. Consider the following conditions:*

(1) ϕ is an A-structure on C/S;

(2) For every geometric point Spec $(k) \to S$, the induced group homomorphism

$$\phi_k\colon A \longrightarrow C(k)$$

is an A-structure on C_k/k;

(3) For every geometric point Spec $(k) \to S$, the induced group homomorphism

$$\phi_k\colon A \longrightarrow C(k)$$

is injective;

(4) The effective Cartier divisor $\sum_{a\in A}[\phi(a)]$ is finite étale over S;

(5) ϕ induces a closed S-immersion

$$A_S \hookrightarrow C$$

which identifies A_S with the effective Cartier divisor $\sum_{a\in A}[\phi(a)]$.

We have the following implications

$$(3) \Longleftrightarrow (4) \Longleftrightarrow (5) \Longrightarrow (1) \Longrightarrow (2).$$

Moreover, if $\#(A)$ is invertible on S, then all the conditions are equivalent.

Next we study the representability of A-structures and A-generators.

As a finite abelian group, we have an isomorphism

$$A \simeq \mathbb{Z}/N_1\mathbb{Z} \times \ldots \times \mathbb{Z}/N_r\mathbb{Z},$$

where $\{N_i\}_{i=1}^r$ are coprime, and each N_i is a power of some prime number. Consider the functor on the category $\mathfrak{Sch}_S$

$$\mathsf{Hom}_{S\text{-}\mathfrak{Grp}}(A,\, C) \colon\, T \longmapsto \mathsf{Hom}_{\mathfrak{Grp}}\big(A,\, C(T)\big),$$

we claim that the functor $\mathsf{Hom}_{S\text{-}\mathfrak{Grp}}(A, C)$ is represented by the S-scheme

$$C[N_1] \times_S \ldots \times_S C[N_r],$$

where S-subgroup scheme $C[N_i]$ is defined by

$$C[N](T) := \ker\left\{ \begin{array}{rcl} [N] : C(T) & \to & C(T) \\ P & \mapsto & N \cdot P \end{array} \right\}.$$

Indeed, for any S-scheme T

$$\begin{aligned} \mathsf{Hom}_{S\text{-}\mathfrak{Grp}}\big(A, C(T)\big) &\simeq \prod_{i=1}^r \mathsf{Hom}_{\mathfrak{Grp}}\big(\mathbb{Z}/N_i\mathbb{Z},\, C(T)\big) \\ &\simeq \prod_{i=1}^r C[N_i](T) \\ &= \bigoplus_{i=1}^r \mathsf{Hom}_{\mathfrak{Sch}_{/S}}\big(T,\, C[N_i]\big) \\ &\simeq \mathsf{Hom}_{\mathfrak{Sch}_{/S}}\big(T,\, C[N_1] \times_S \ldots \times_S C[N_r]\big) \end{aligned}$$

which shows our claim.

Proposition 2.2.4. *The functor A-Str(C/S) defined on the category $\mathfrak{Sch}_{/S}$*

$$T \longmapsto \{A\text{-structures on } C_T/T\}$$

is represented by a closed subscheme of $C[N_1] \times_S \ldots \times_S C[N_r]$, which is locally defined by $1 + \#(A) + \big(\#(A)\big)^2$ equations.

Proof: The functor A-$\mathsf{Str}(C/S)$ is a subfunctor of $\mathsf{Hom}_{S\text{-}\mathfrak{Grp}}(A, C)$, where a homomorphism $\phi \in \mathsf{Hom}_{S\text{-}\mathfrak{Grp}}(A, C(T))$ belongs to A-$\mathsf{Str}(C/S)(T)$ if and only if the subscheme $\sum_{a \in A}[\phi(a)]$ is a T-subgroup scheme of C_T.

Since the functor $\mathsf{Hom}_{S\text{-}\mathfrak{Grp}}(A, C)$ is representable, consider the universal homomorphism

$$\phi_{\text{univ}} \in \mathsf{Hom}_{\mathfrak{Grp}}\big(A,\, C(C[N_1] \times_S \ldots \times_S C[N_r])\big)$$

which is defined as the identity element in

$$\mathsf{Hom}_{\mathfrak{Sch}_S}\big(C[N_1] \times_S \ldots \times_S C[N_r],\, C[N_1] \times_S \ldots \times_S C[N_r]\big).$$

By the Corollary 7.4.9, there exists a unique closed subscheme Y of $C[N_1] \times_S \ldots \times_S C[N_r]$ which is universal for the relation

$$\text{“} \sum_{a \in A} [\phi_{\text{univ}}(a)] \text{ is a subgroup scheme”}$$

and it is defined by $1 + \#(A) + \big(\#(A)\big)^2$ equations. It is clear that the subscheme Y represents the functor A-$\mathsf{Str}(C/S)$. □

From now on, we do not distinguish the functor A-$\mathsf{Str}(C/S)$ and the S-scheme represents it.

Proposition 2.2.5. *Suppose that N is invertible on S, and $C[N]$ is finite over S. Then the S-scheme A-$Str(C/S)$ is finite étale over S.*

Proof: We claim that under the assumption, the morphism of multiplying by N

$$[N]:\ C \longrightarrow C$$

is étale. We use the characterization of étale morphisms which says that a morphism is étale if and only if it is formally étale and locally of finite presentation [1]. Since the structure morphism $C \to S$ is finitely presented

$$\begin{tikzcd}
C \arrow[rr, "{[N]}"] \arrow[dr] & & C \arrow[dl] \\
& S &
\end{tikzcd}$$

then $[N]$ being finitely presented is indicated from [22] Proposition 1.10.

For the formal étaleness, it is a little bit more complicated. We shall firstly prove that $C[N]$ is étale over S. Let $\mathsf{Spec}\ (B)$ be an affine scheme over S, and $J \subset B$ is an ideal such that $J^2 = 0$. Suppose we have the following commutative diagram

$$\begin{tikzcd}
\mathsf{Spec}\ (B/J) \arrow[r, "\bar{g}"] \arrow[dd, hook, "i"] & C[N] \arrow[d, hook] \\
& C \arrow[d] \\
\mathsf{Spec}\ (B) \arrow[r, "g"] \arrow[ur, dotted, "g_0"] & S
\end{tikzcd}$$

with given morphisms g and $\bar{g}$. Notice that we can always lift g to $C(B)$, because of the smoothness hence formal smoothness of C/S. Let us fix a lifting g_0 of g. Since $C \to S$ is not étale, the lifting is never unique. Let

$$V \ = \ \big\{g_1 \in C(B) \,\big|\, g_1 \circ i = \bar{g} \in C(B/J)\big\},$$

given any $g_1 \in V$, the difference $g_1 - g_0$ always belongs to

$$H \ := \ \ker \big\{C(B) \to C(B/J)\big\},$$

thus $V = g_0 + H$.

[1] cf. [5] EGA IV$_4$ 17.6.

Now we assume $S = \mathsf{Spec}\,(R)$, and $C \supset \mathsf{Spec}\,(A)$. Denote $\epsilon : S \to C$ and $\widetilde{\epsilon} : A \to R$ to be the unit and counit, and $I := \ker(\widetilde{\epsilon})$ is the augmentation ideal. It is clear that $A \simeq R \oplus I$. Take an element $h \in H$

$$\begin{tikzcd}
B/J & \\
 & A \arrow[dl, "h^{\#}"'] \\
B \arrow[uu, "i^{\#}"] & R \arrow[u] \arrow[l, "g^{\#}"]
\end{tikzcd}$$

it is by definition that

$$i^{\#} \circ h^{\#} = i^{\#} \circ g^{\#} \circ \widetilde{\epsilon},$$

or equivalently

$$h \circ i = \epsilon \circ g \circ i.$$

It is easy to see that $h^{\#}$ maps I to J, and consequently maps I^2 to $J^2 = 0$, hence it induces a R-homomorphism

$$h^{\#} : \; J/J^2 \longrightarrow I,$$

i.e., we have defined a map explicitly

$$\begin{array}{ccl} H & \longrightarrow & \mathsf{Hom}_R(J/J^2, I) = \mathsf{Der}_R(A, I) \\ h & \longmapsto & \big\{a \mapsto h^{\#}(a) - g^{\#}\big(\widetilde{\epsilon}(a)\big)\big\} \end{array}$$

it is actually bijective, we can construct its inverse explicitly

$$\begin{array}{rcl} \mathsf{Der}_R(A, I) & \longrightarrow & H \\ D & \longmapsto & \big(a \mapsto D(a) + g^{\#}(\widetilde{\epsilon}(a))\big)^{*} \end{array} \quad [2]$$

in fact these two mutually inverse maps are group homomorphisms, with natural group structures on H and $\mathsf{Der}_R(A, I)$.

Now we are trying to find a lifting $g_1 \in V$ of g, such that $g_1 \in C[N](C)$, and to prove the uniqueness. Such g_1 should satisfy $[N] \circ g_1 = 0 \in C(B)$, and vice versa. Hence equivalently, we want to find an $h \in H$ such that $[N] \circ (g_0 + h) = 0$ which ought to be unique. Using above identification of H and $\mathsf{Der}_R(A, I)$ as groups, composing h with $[N]$ is nothing but the multiplication by N in $\mathsf{Der}_R(A, I)$, and as we assumed that N is invertible in R, hence

$$h = N^{-1} \cdot \big(- [N] \circ g_0 \big), \text{[3]}$$

which is obviously unique. Thus it means that for every given morphisms g and $\bar{g}$,

$$\begin{tikzcd}
\mathsf{Spec}\,(B/J) \arrow[r, "\bar{g}"] \arrow[d] & C[N] \arrow[d] \\
\mathsf{Spec}\,(B) \arrow[r, "g"] \arrow[ur, dotted, "g_1"] & S
\end{tikzcd}$$

[2] Here the upper star means the morphism of affine schemes corresponding to the given homomorphism of rings of global sections.

[3] Note that we use "$\circ$" for composition of morphisms, and "$\cdot$" for the corresponding scalar multiplication in $\mathsf{Der}_R(A, I)$.

we can always find a unique lifting g_1, which shows $C[N] \to S$ is formally étale. Combining with finite presentation we already showed, $C[N]$ is then étale over S.

To prove $[N]$ is étale, we must show that given diagram

$$\begin{tikzcd}
\mathsf{Spec}\,(B/J) \arrow[r, "\bar{g}"] \arrow[d] & C \arrow[d, "{[N]}"] \\
\mathsf{Spec}\,(B) \arrow[r, "g"] \arrow[ur, dotted, "g'"] & C
\end{tikzcd}$$

with $J^2 = 0$, there is a unique lifting g' of $\bar{g}$. As a consequence of $C[N]$ being étale over S, we can certainly find a unique lifting for the zero section

$$\mathsf{Spec}\,(B) \xrightarrow{0} C$$

i.e., when $g \in C(B)$ is the zero element in the group. For general B-valued point g of C, we can simply imitate above process, aiming to the diagram

$$\begin{tikzcd}
\mathsf{Spec}\,(B/J) \arrow[r, "\bar{g}"] \arrow[dd] & {[N]^{-1}g} \arrow[d] & \\
& C_B \arrow[r] \arrow[d] & C \arrow[d] \\
\mathsf{Spec}\,(B) \arrow[r, "\mathsf{id}"] \arrow[ur, dotted] & \mathsf{Spec}\,(B) \arrow[r, "g"] & S
\end{tikzcd}$$

where the right side square is cartesian. The unique lifting is ensured by the invertibility of N on the base S in a similar way. Thus we have proved our claim.

Return to the proposition. It is clear that the S-scheme $C[N_1] \times_S \ldots \times_S C[N_r]$ is finite and finitely presented (as each $C[N_i]$ is so). As we showed in the Proposition 2.2.4, A-$\mathsf{Str}(C/S)$ is a closed subscheme of $C[N_1] \times_S \ldots \times_S C[N_r]$ locally defined by finitely many equations, hence it is finitely presented. In order to show that A-$\mathsf{Str}(C/S)$ is étale, we need only to verify the formal étaleness.

Suppose T is a S-scheme, and T_0 is a closed S-subscheme of T defined by some nilpotent ideal sheaf. Given any commutative diagram

$$\begin{tikzcd}
T_0 \arrow[r] \arrow[d] & A\text{-}\mathsf{Str}(C/S) \arrow[d] \\
T \arrow[r] \arrow[ur, dotted] & S
\end{tikzcd}$$

we want to lift $T_0 \to A$-$\mathsf{Str}(C/S)$ to $T \to A$-$\mathsf{Str}(C/S)$ which ought to be unique. That is to say, given any A-structure

$$\phi_0 \colon\ A \longrightarrow C(T_0)$$

on C_{T_0}, we want to show that it extends uniquely to an A-structure

$$\phi \colon\ A \longrightarrow C(T)$$

on C_T. Obviously, ϕ_0 and ϕ both factor through $C[N]$. Notice that ϕ_0, ϕ are determined by the images of finitely many generators of A, and for each image of ϕ_0, i.e., each T_0-valued point in $C[N]$, it extends uniquely to a T-valued point

$$\begin{tikzcd}
T_0 \arrow[r] \arrow[d] & C[N] \arrow[d] \\
T \arrow[r] \arrow[ur, dotted] & S
\end{tikzcd}$$

since we already know $C[N]$ is étale over S. Therefore $A\text{-}\mathsf{Str}(C/S)$ is formally étale, hence étale since it is also finitely presented. □

Proposition 2.2.6. *Suppose G is a closed S-subgroup scheme of C which is finite flat over S of rank $\#(A)$. Then the functor $A\text{-}\mathsf{Gen}(G/S)$ on $\mathfrak{Sch}_{/S}$*

$$T \longmapsto \{A\text{-generators of } G_T \text{ in } C_T\}$$

is represented by a finite and finitely presented S-subscheme of $\mathsf{Hom}_{S\text{-}\mathfrak{Grp}}(A,G)$, which is locally defined by $\#(A)$ equations.

Proof: The functor $A\text{-}\mathsf{Gen}(G/S)$ is indeed a subfunctor of $\mathsf{Hom}_{S\text{-}\mathfrak{Grp}}(A,G)$, and a homomorphism $\phi \in \mathsf{Hom}_{\mathfrak{Grp}}\big(A, G(T)\big)$ is an A-generator of G_T if and only if

$$G_T = \sum_{a\in A} [\phi(a)]$$

as effective Cartier divisors in C_T. Like what we did in the proof of Proposition 2.2.4, we consider the universal homomorphism ϕ_{univ}, and according to Corollary 7.4.9, there exists a unique closed subscheme of $\mathsf{Hom}_{S\text{-}\mathfrak{Grp}}(A,G)$ (i.e., $G[N_1] \times_S \ldots \times_S G[N_r]$) which is locally defined by $\#(A)$ equations, and it is universal for the relation

$$D_{\text{univ}} := \sum_{a\in A} [\phi_{\text{univ}}(a)] = G$$

as effective Cartier divisors. This closed subscheme of $\mathsf{Hom}_{S\text{-}\mathfrak{Grp}}(A,G)$ certainly represents the functor $A\text{-}\mathsf{Gen}(G/S)$. □

Similar to the Proposition 2.2.5, we have

Proposition 2.2.7. *If G is finite étale over S, then $A\text{-}\mathsf{Gen}(G/S)$ is also finite étale over S.*

The proof is not only similar but even easier, we skip it.

Another natural question to consider is, if we factorize A as $A_1 \times A_2$ with coprime orders, what is the relation between A-structures (resp. A-generators) and A_i-structures (resp. A_i-generators)? It turns out that they have the similar way of factorizations, which we call it the *principle of factorization.* It always allows us to reduce many questions concerning level N structures to the case that $N = p^n$ is a prime power.

Proposition 2.2.8. *Suppose $A \simeq A_1 \times A_2$, such that $N_1 := \#(A_1)$ and $N_2 := \#(A_2)$ are coprime. Then a group homomorphism*

$$\phi\colon A \longrightarrow C(S)$$

is an A-structure if and only if the two induced homomorphisms

$$\phi_i : A_i \longrightarrow C(S), \quad i = 1,2$$

are respectively A_i-structures on C/S. In this case, the groups G_1, G_2 and G generated by ϕ_1, ϕ_2 and ϕ respectively, satisfy $G = G_1 \times_S G_2$.

Proof: We have the canonical factorization of S-group scheme G generated by ϕ

$$G \simeq G[N_1] \times_S G[N_2],$$

this can be deduced from the factorization of abstract abelian groups [4]

$$\mathsf{Hom}_{\mathfrak{Sch}_{/S}}(S,G) \simeq \mathsf{Hom}_{\mathfrak{Sch}_{/S}}(S,G)[N_1] \times \mathsf{Hom}_{\mathfrak{Sch}_{/S}}(S,G)[N_2],$$

and notice that $\mathsf{Hom}_{\mathfrak{Sch}_{/S}}(S,G[N_i]) = \mathsf{Hom}_{\mathfrak{Sch}_{/S}}(S,G)[N_i]$, the latter are the N_i-torsions of $G(S)$. Hence

$$\mathsf{Hom}_{\mathfrak{Sch}_{/S}}(S,G) \simeq \mathsf{Hom}_{\mathfrak{Sch}_{/S}}(S,G[N_1]) \times \mathsf{Hom}_{\mathfrak{Sch}_{/S}}(S,G[N_2]),$$

and the factorization of G follows from it.

The S-subgroup schemes $G[N_i]$ are finite over S since G is. They are also finitely presented, since they are kernels of the morphisms

$$G \xrightarrow{[N_i]} G.$$

Moreover, locally speaking, the sheaf of $\mathscr{O}_S$-algebras defining $G[N_i]$ are summands of the sheaf of $\mathscr{O}_S$-algebras defining G, thanks to the factorization of G, hence $G[N_i]$ are both flat over S. Let us now determine the ranks of $G[N_i]$, which we need only to treat the case of geometric fibers. From the factorization, we have

$$\mathsf{rk}(G[N_1]) \cdot \mathsf{rk}(G[N_2]) = \mathsf{rk}(G) = N_1 \cdot N_2,$$

while $G[N_i]$ are killed by N_i. We then claim that

> If a finite flat commutative group scheme G over an algebraically closed field k is killed by N, then there is $k \geqslant 1$ such that $\mathsf{rk}(G) | N^k$.

Also, by factorization, it suffices to assume N is a power of a prime number p^n. When $\mathrm{char}(k) \neq p$, by Lemma 2.1.4, G is étale over k, the claim follows from elementary argument of abstract groups. Now assume $\mathrm{char}(k) = p$, then the claim follows from Waterhous [36] Theorem 14.4. Therefore, as the claim states, $\mathsf{rk}(G[N_i])$ divides some power of N_i, and since N_1, N_2 are coprime, it can only happen that $\mathsf{rk}(G[N_i]) = N_i$ $(i = 1,2)$.

To show ϕ_i are A_i-structure on C/S respectively, notice that N_1, N_2 are coprime, hence after localization on S, it is always possible to assume one of them is invertible on the base. So let us assume N_1 is invertible on S, and therefore $G[N_1]$ is étale over S. To show that ϕ_1 is an A_1-structure and generates the S-group scheme $G[N_1]$, it suffices to check the geometric fibers. For any geometric point $\mathsf{Spec}\,(k) \to S$, the geometric fiber

$$G_k = G[N_1]_k \times G[N_2]_k$$

[4] Note that according to Theorem 2.1.3, $G(S)$ is killed by N.

contains exactly N_1 points which are killed by N_1. On the other hand, since we have the equality of effective Cartier divisors

$$G \;=\; \sum_{a_1 \in A_1, a_2 \in A_2} [\phi(a_1) + \phi(a_2)],$$

the k-group scheme G_k is exhausted by (not necessarily all distinct)

$$\left\{\phi(a_1)_k + \phi(a_2)_k\right\}_{a_1 \in A_1, a_2 \in A_2},$$

where among these points, only $\{\phi(a_1)\}_{a_1 \in A_1}$ are killed by N_1, thus they must run out of N_1 distinct points, which indicates that they are all distinct. That is to say, the restriction homomorphism

$$\phi_1 : \; A_1 \;\longrightarrow\; G[N_1]$$

is isomorphic on each geometric fiber, which justifies (3) in Lemma 2.2.3, hence equivalent to that ϕ_1 is an A_1-structure, and generates $G_1 = G[N_1]$.

To show that ϕ_2 is an A_2-structure and generates the S-group scheme $G[N_2]$, we need to show the equality of effective Cartier divisors

$$D_2 \;:=\; \sum_{a_2 \in A_2} [\phi(a_2)] \;=\; G[N_2].$$

Observe that since $G[N_1] = \sum_{a_1 \in A_1} [\phi(a_1)]$ is étale over S, we can write G as [5]

$$G \;=\; \sum_{a_1 \in A_1} \phi(a_1)^*(D_2),$$

where pieces of D_2 are all disjoint, simply because $G[N_1]$ is isomorphic to a constant S-group scheme (cf. Lemma 2.2.3 (5)). Therefore

$$G \;\simeq\; \coprod_{a_1 \in A_1} \phi(a_1)^*(D_2).$$

Let T be any S-scheme, and $P \in G[N_2](T)$. Since $G(T) = \coprod_{a_1 \in A_1} \phi(a_1)^*(D_2(T))$, we know that

$$P - \phi(a_1) \in D_2(T)$$

for some $a_1 \in A_1$. For any geometric point $\mathsf{Spec}\,(k) \to T$, we have

$$P_k - \phi(a_1)_k \;=\; \phi(a_2)_k$$

for some $a_1 \in A_2$. But both P_k and $\phi(a_2)_k$ are killed by N_2, which implies $\phi(a_1)_k$ is also killed by N_2. This forces $\phi(a_1)_k = 0$ because $\phi(a_1)_k$ is also killed by N_1 which is coprime to N_2. Thus $P \in D_2(T)$, i.e., $G[N_2] \leqslant D_2$, and since both sides have the same rank, they are equal $G[N_2] = D_2$.

It remains to show the converse. Suppose given $\phi : A \to C(S)$ such that ϕ_1, ϕ_2 are A_1-, A_2-structures respectively on C/S, and they generate S-subgroup schemes G_1, G_2 respectively. As before, we may assume N_1 is invertible on S. The sum of G_1, G_2 defines a closed immersion [6]

$$G_1 \times_S G_2 \lhook\joinrel\longrightarrow C,$$

[5] Here each $\phi(a_1)$ is viewed as a translation by multiplication on G.

[6] Because their ranks are coprime.

with the image G in C. Since $G_1 \simeq A_1$, we can write G as disjoint unions

$$G = \coprod_{a_1 \in A_1} \phi(a_1)^*(D_2),$$

which is also the sum as effective Cartier divisors

$$\begin{aligned} G &= \sum_{a_1 \in A_1} \phi(a_1)^*(D_2) \\ &= \sum_{a_1 \in A_1} \phi(a_1)^* \Big(\sum_{a_2 \in A_2} [\phi(a_2)] \Big) \\ &= \sum_{a_1 \in A_1, a_2 \in A_2} [\phi(a_1) + \phi(a_2)] \ = \ \sum_{a \in A} [\phi(a)], \end{aligned}$$

which shows that ϕ is an A-structure on C/S and generates $G = G_1 \times_S G_2$. □

Corollary 2.2.9. *Suppose A is a finite abelian group of order $N = \prod_{i=1}^r p_i^{n_i}$, and*

$$A = A_1 \times \ldots \times A_r$$

is the corresponding factorization, i.e., each A_i has order $p_i^{n_i}$, where $\{p_i\}_{i=1}^r$ are primes. Then the factorization of A defines a canonical isomorphism

$$A\text{-}\mathit{Str}(C/S) \xrightarrow{\sim} A_1\text{-}\mathit{Str}(C/S) \times_S \ldots \times_S A_r\text{-}\mathit{Str}(C/S)$$

of S-schemes. Moreover, for any closed S-subscheme G of C/S which is finite flat over S of finite presentation and has rank N, let

$$G = G[p_1^{n_1}] \times_S \ldots \times_S G[p_r^{n_r}] =: G_1 \times_S \ldots \times_S G_r,$$

then there is a canonical isomorphism

$$A\text{-}\mathit{Gen}(G/S) \xrightarrow{\sim} A_1\text{-}\mathit{Gen}(G_1/S) \times_S \ldots \times_S A_r\text{-}\mathit{Gen}(G_r/S)$$

of S-schemes.

2.3 Intrinsic description of A-generators: full set of sections

In our previous discussion about A-generators, it seems depending on the ground group scheme C/S in the definition, while in the expression of the representable functor A-$\mathsf{Gen}(G/S)$, it makes no references on C/S. Instead of previous extrinsic description of A-generators, now we shall see that there is another approach to discuss them intrinsically, namely, using the concept of *full set of section.*

Suppose Z is a finite flat and finitely presented S-scheme of rank N.

Definition 2.3.1. *A set of N sections $P_1, \ldots, P_N \in Z(S)$ (not necessarily distinct) is called a* ***full set of sections*** *of Z/S if the following two equivalent conditions hold:*

1) *For any affine S-scheme Spec (R), and any $f \in \Gamma(Z_R, \mathscr{O}_{Z_R})$, we have*

$$det\,(T - f) = \prod_{i=1}^{N} \big(T - f(P_i)\big),$$

where the left side is the characteristic polynomial of f treated as a R-linear endomorphism of$\Gamma(Z_R, \mathscr{O}_{Z_R})$.

2) *For any affine S-scheme Spec (R), and any $f \in \Gamma(Z_R, \mathscr{O}_{Z_R})$, we have*

$$N(f) = \prod_{i=1}^{N} f(P_i),$$

where N is the norm map.

Remark: The equivalence is clear, since the map $\det(\cdot)$ is nothing but the norm map of the $R[T]$-algebra $\Gamma(Z_{R[T]}, \mathscr{O}_{Z_{R[T]}})$.

Lemma 2.3.2. *Suppose moreover Z is étale over S, then TFAE:*

(1) *$P_1, ..., P_N$ form a full set of sections of Z/S;*

(2) *For every geometric point Spec $(k) \to S$, the N points $(P_i)_k \in Z(k)$ are all distinct.*

(3) *The S-morphism*

$$\coprod_N S \longrightarrow Z$$

defined by $P_1, ..., P_N$ is an isomorphism;

Proof: (1) $\Longrightarrow$ (2): It suffices to consider the case $S = \text{Spec}\,(k)$ with $k = \bar{k}$. Then Z consists of N distinct reduced points, say $Q_1, ..., Q_N$. We might choose a function f on Z with distinct nonzero values on $Q_1, ..., Q_N$. On the one hand, by the definition of full set of sections

$$N(f) = \prod_{i=1}^{N} f(P_i).$$

On the other hand, $\Gamma(Z, \mathscr{O}_Z)$ is an étale k-algebra, hence isomorphic to k^N with the structure of product k-algebra. The k-linear endomorphism of multiplication by f can be represented as a diagonal matrix with diagonal entries $f(Q_1), ..., f(Q_N)$, thus

$$\prod_{i=1}^{N} f(Q_i) = N(f) = \prod_{i=1}^{N} f(P_i)$$

which indicates that $P_1, ..., P_N$ must be distinct.

(2) $\Longrightarrow$ (3): Only need to check the case $S = \text{Spec}(R)$. The morphism $\coprod_N S \to Z$ then corresponds to the homomorphism of two étale algebras of rank N, whose determinant is invertible over any geometric point, hence invertible in R, which deduces that it is an isomorphism.

(3) $\Longrightarrow$ (1): It is trivial. □

Remark: When we do not have the étale condition, we can still prove that the morphism defined by a full set of sections

$$\coprod_N S \longrightarrow Z$$

is surjective, while the converse is generally not true.

Example 2.3.3. *Let E/R be an elliptic curve over a $\mathbb{F}_p$-algebra R. The kernel of the relative Frobenius $F_{E/R}$ lies in the formal group $\widehat{E}$, it is visibly that*

$$\mathit{ker}\,(F_{E/S}) \simeq \alpha_{p,R} = \mathit{Spec}\left(R[X]/(X^p)\right).$$

We claim that the p zero sections form a full set of sections of $\mathit{ker}(F_{E/S})$. Take any function

$$f = \sum_{i=1}^{n} a_i X^i \ \ mod\, X^p \ in\, R[X]/(X^p),$$

we have

$$N(f) = a_0^p = \prod_{i=1}^{p} f(0),$$

which shows our claim.

Example 2.3.4. [7] *Let $S = \mathit{Spec}\left(k[\epsilon]/(\epsilon^2)\right)$, where k is a field, and $X = \mathit{Spec}\left(k[\epsilon,\epsilon']/(\epsilon^2,\epsilon'^2)\right)$. Consider two sections*

$$\begin{array}{rcl} \mathit{Spec}\left(k[\epsilon]/(\epsilon^2)\right) & \longrightarrow & \mathit{Spec}\left(k[\epsilon,\epsilon']/(\epsilon^2,\epsilon'^2)\right) \\ P_1 : \epsilon' & \longmapsto & 0 \\ P_2 : \epsilon' & \longmapsto & \epsilon \end{array}$$

the map

$$P_1 \coprod P_2 : S \coprod S \longrightarrow X$$

is certainly surjective. But

$$N(1+\epsilon') = 1 \neq 1+\epsilon = f(P_1)\cdot f(P_2),$$

therefore $\{P_1, P_2\}$ is not a full set of sections.

Lemma 2.3.5. *Suppose Z_1, Z_2 are finite flat and finitely presented S-schemes of rank N_1, N_2 respectively, and $P_1^{(i)}, \ldots, P_{N_i}^{(i)} \in Z_i(S)$ are sections ($i = 1,2$). Then the following two conditions are equivalent:*

(1) The set of sections $\left\{P_1^{(i)}, \ldots, P_{N_i}^{(i)}\right\}$ is a full set of sections of Z_i/S, $i = 1,2$;

(2) The set of sections $\left\{P_1^{(1)}, \ldots, P_{N_1}^{(1)}, P_1^{(2)}, \ldots, P_{N_2}^{(2)}\right\}$ is a full set of sections of $(Z_1 \coprod Z_2)/S$.

Moreover, if Z_1 is étale, then the above conditions are also equivalent to

(3) The set of sections $\left\{P_j^{(1)} \times P_k^{(2)}\right\}_{1\leqslant j\leqslant N_1, 1\leqslant k\leqslant N_2}$ is a full set of sections of $(Z_1 \times_S Z_2)/S$.

[7] This example is took from Saito's book [33].

Proof: Suppose $S = \mathsf{Spec}\ (R)$ and $Z_i = \mathsf{Spec}\ (B_i)$ $(i = 1,2)$, where B_i are finite R-algebras which are free as R-modules.

(1) $\Longleftrightarrow$ (2): Notice that $Z_1 \coprod Z_2 = \mathsf{Spec}\ (B_1 \oplus B_2)$, and for any element $f = f_1 \oplus f_2 \in B_1 \oplus B_2$,

$$N_{B_1 \oplus B_2 / R}(f) \ = \ N_{B_1/R}(f_1) \cdot N_{B_2/R}(f_2),$$

and the equivalence between (1), (2) now is obvious.

Moreover, if Z_1 is étale over R:

(1) $\Longrightarrow$ (3): According to Lemma 2.3.2, we have the isomorphism of S-schemes

$$\coprod_{N_1} S \xrightarrow{\sim} Z_1$$

which is defined by sections $P_1^{(1)}, ..., P_{N_1}^{(1)}$. This also induces the isomorphism

$$\coprod_{N_1} Z_2 \xrightarrow{\sim} Z_1 \times_S Z_2,$$

hence the implication follows from (1) $\Longleftrightarrow$ (2).

(3) $\Longrightarrow$ (1): Firstly we show that $\{P_1^{(1)}, ..., P_{N_1}^{(1)}\}$ is a full set of sections of Z_1/S. In order to do so, we can restrict us to the case $R = k$ with $k = \bar{k}$, thanks to Lemma 2.3.2. For any $f_1 \in B_1$, consider $f_1 \otimes 1 \in Z_1 \times_S Z_2$, from condition (3), it is known that

$$\mathsf{det}\ (T - f_1 \otimes 1) \ = \ \left(\prod_{i=1}^{N_1} (T - f_1(P_i^{(1)})) \right)^{N_2}.$$

On the other hand, indeed we have

$$\mathsf{det}\ (T - f_1 \otimes 1) \ = \ \Big(\mathsf{det}(T - f_1) \Big)^{N_2},$$

hence $\mathsf{det}(T - f_1) = \prod_{i=1}^{N_1} (T - f_1(P_i^{(1)}))$ since $k[T]$ is a UFD and these two polynomials are both monic, which shows the assertion.

So now we have the isomorphism of S-schemes

$$\coprod_{N_1} S \xrightarrow{\sim} Z_1$$

and consequently

$$\coprod_{N_1} Z_2 \xrightarrow{\sim} Z_1 \times_S Z_2,$$

the rest deduction follows from (1) $\Longleftrightarrow$ (2). □

Remark: Without étale condition, we only have (1) $\Longrightarrow$ (3).

We will see that being a full set of sections is a closed condition on the base.

Proposition 2.3.6. *Let Z/S be a finite flat S-group scheme of finite presentation. Suppose $\mathsf{rk}(Z) = N$, and $P_1, ..., P_N \in Z(S)$ is a set of sections which are not necessarily distinct. Then there exists a unique closed subscheme $W \subset S$ which is locally defined by finitely many equations on S, such that it is universal for that $\{P_1, ..., P_N\}$ being a full set of sections of Z/S.*

Proof: After localization, we may assume $S = \mathsf{Spec}(R)$ and $Z = \mathsf{Spec}(B)$, where B is a finite R-algebra, and is free of rank N as a R-module. Choose a R-basis $b_1,...,b_N$ of B. Consider the universal element

$$f = \sum_{i=1}^{N} T_i b_i \in B \otimes_R R[T_1,...,T_N],$$

the set of sections $\{P_1,...,P_N\}$ forms a full set of sections if and only if

$$N(f) = \prod_{i=1}^{N} f(P_i)$$

in $R[T_1,...,T_N]$. Observe that both sides are homogeneous polynomials of degree N in variables $T_1,...,T_N$. The subscheme $W \subset S$ defined by the ideal generated by the coefficients is certainly universal for the required relation. □

As an immediate corollary, when the base is reduced, it suffices to verify the equality on geometric fibers.

Corollary 2.3.7. *Suppose the base scheme S is reduced. The set of S-valued points $\{P_1,...,P_N\}$ forms a full set of sections of Z/S, if and only if that for any geometric point $Spec(k) \to S$, the set $\{(P_1)_k,...,(P_N)_k\}$ forms a full set of sections of Z_k/k.*

Now back to the case of smooth curves. We will see that the equality of effective Cartier divisors can be reinterpreted by using the concept of full set of sections.

Lemma 2.3.8. *Suppose R is a ring and $F(X) \in R[X]$ is a monic polynomial of degree $N \geqslant 1$, and $a_1,...,a_N \in R$. Denote $B = R[X]/(F(X))$. Then the following two conditions are equivalent:*

(1) $F(X) = \prod_{i=1}^{N}(X - a_i)$;

(2) For any $f \in B$,

$$det\,(T - f) = \prod_{i=1}^{N}(T - f(a_i)).$$

Proof: (1) $\Longrightarrow$ (2): Firstly it suffices to reduce to the universal case, i.e., let

$$R = \mathbb{Z}[A_1,...,A_N,B_0,...,B_{N-1}],$$
$$(a_1,...,a_N) = (A_1,...,A_N),$$
$$F(X) = \textstyle\prod_{i=1}^{N}(X - A_i),$$
$$f = \textstyle\sum_{i=0}^{N-1} B_i X^i,$$

where A_i, B_i are free variables. To verify (2), it suffices to verify it under any injective scalar extension $R \hookrightarrow R'$, in particular, we can choose R' to be the fraction field of R. By Chinese Remainder Theorem for PIDs,

$$R'[X]/\big(F(X)\big) \simeq \prod_{i=1}^{N} R'[X]/(X - a_i),$$

and $f \in R'[X]/\big(F(X)\big)$ corresponds to $\big(f(a_1),...,f(a_N)\big)$, therefore it is clear that

$$\mathsf{det}\,(T - f) = \mathsf{det}\begin{pmatrix} T - f(a_1) & & \\ & \ddots & \\ & & T - f(a_N) \end{pmatrix} = \prod_{i=1}^{N}(T - f(a_i)).$$

(2) $\Longrightarrow$ (1): We set $F(X) = X^N + \sum_{i=0}^{N-1} c_i X^i$. Then

$$\det(T-X) = \det\begin{pmatrix} T & -1 & & & \\ & T & -1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & -1 \\ a_0 & a_1 & \dots & a_{N-2} & T+a_{N-1} \end{pmatrix} = F(T),$$

by substituting f to X, we deduce (1). □

Theorem 2.3.9. *Let C/S be a smooth curve over the base S, $Z \subset C$ is a finite flat and finitely presented closed subscheme of rank N, and $\{P_1, ..., P_N\}$ is a set of points of $C(S)$ (not necessarily distinct). Then the following two conditions are equivalent:*

(1) $Z = \sum_{i=1}^{N}[P_i]$ as effective Cartier divisors in C/S;

(2) The set of points $\{P_1, ..., P_N\}$ forms a full set of sections of Z/S.

Proof: By a "standard reduction" argument (see [37] for details), it suffices to reduce to the case $S = \mathrm{Spec}\,(R)$ such that R is an artin local ring with maximal ideal $\mathfrak{m}$ and algebraically closed residue field k.

We have the decomposition of Z into disjoint union of connected components

$$Z = \coprod_{j=1}^{r} Z_j,$$

each Z_j is supported at a k-valued point $z_j \in Z(k)$. Since in either conditions, $P_1, ..., P_N$ are all lying in $Z(R)$, and the conditions (1) and (2) are equivalent if and only if they are equivalent on each connected component of Z, we may furthermore assume Z is connected, supported at $z \in Z(k) \subset C(k)$.

As C is a smooth curve, the complete local ring $\widehat{\mathscr{O}}_{C,z}$ at z is isomorphic to the formal power series in one variable, i.e., by choosing a uniformizing parameter X at z, we have the (non-canonical) isomorphism

$$\widehat{\mathscr{O}}_{C,z} \simeq R[\![X]\!].$$

According to the Weierstrass Preparation Theorem for complete local rings (cf. Lang [31] Chapter 5, Theorem 2.2), Z is defined in $\mathrm{Spec}\,(R[\![X]\!])$ by a unique monic polynomial $F(X)$ of degree N, which has the form

$$F(X) = X^N + \text{lower terms with coefficients in } \mathfrak{m}.$$

On the other hand, the effective Cartier divisor $\sum_{i=1}^{N}[P_i]$ is also supported at z, which is defined in $\mathrm{Spec}\,(R[\![X]\!])$ by the monic polynomial

$$G(X) = \prod_{i=1}^{N}(X - X(P_i))$$

of degree N. Notice that since $\sum_{i=1}^{N}[P_i]$ lies inside $Z(R)$, each $X(P_i)$ is a root of $F(X)$, which must belong to $\mathfrak{m}$.

Now the condition (1) is equivalent to that Z and $\sum_{i=1}^{N}[P_i]$ are equal inside $\mathsf{Spec}\,(R[\![X]\!])$, i.e.,

$$F(X) \;=\; G(X) \;=\; \prod_{i=1}^{N}(X - X(P_i)).$$

Let $a_i := X(P_i)$ for $i = 1,...,N$. The condition (2) is by definition

$$\mathsf{det}\,(T - f) \;=\; \prod_{i=1}^{N}(T - f(a_i))$$

for any $f \in R[\![X]\!]\big/\big(F(X)\big) \simeq R[X]\big/\big(F(X)\big)$. Thus the equivalence of (1) and (2) follows from Lemma 2.3.8. □

Corollary 2.3.10. *Let Z/S be a finite flat S-group scheme of finite presentation and of rank N, and $\{P_1,...,P_r\}$ is a set of S-valued points of Z. Suppose Z/S is embedded as a closed subscheme of a smooth curve C/S, then there exists at most one closed subscheme $W \subset Z$, such that the following two conditions hold:*

(1) W/S is locally free (over S) of rank r;

(2) $P_1,...,P_r$ lie in $W(S)$, and they form a full set of sections of W/S.

Moreover, the closed subscheme W exists, if and only if fppf-locally on S, $\{P_1,...,P_r\}$ can be completed to a full set of sections $\{P_1,...,P_r,P_{r+1},...,P_N\}$ of Z/S. And there exists a unique closed subscheme $S' \subset S$ locally defined by finitely many equation, which is universal for the existence of W.

Proof: The first assertion is fairly clear, since if such W exists, then it has to be the closed subscheme

$$W' \;=\; \sum_{i=1}^{r}[P_i] \;\subset\; C.$$

For the second assertion, the "if" part is obvious, by Theorem 2.3.9, that $W = W'$ in Z/S. As for the "only if" part, we firstly claim that:

For any effective Cartier divisor D in C/S, fppf-locally, it admits a full set of sections.

If $\mathsf{rk}(D) = 1$, it then comes from a section $S \to C$, which already forms a full set of sections. And if $\mathsf{rk}(D) > 1$, fppf-locally, we can always find a section $\sigma : S \to D$ of D, and then $D - \sigma$ is still an effective Cartier divisor. It is easy to show the claim by induction. Back to the case, if we know that W exists and $\{P_1,...,P_r\}$ is a full set of sections of W/S, then $W \leqslant Z$, and hence $D := Z - W$ is an effective Cartier divisor. Therefore fppf-locally, we can find a full set of sections $\{P_{r+1},...,P_N\}$ of D/S, and so that $\{P_1,...,P_N\}$ completes $\{P_1,...,P_r\}$ as a full set of sections of Z/S.

For the last assertion, the closed subscheme S' should exactly be the locus where the relation $W' \leqslant Z$ holds. It follows from 7.4.8. □

Remark: If the finite flat S-group scheme Z does not come from a closed subscheme of a smooth curve, then the uniqueness of W might be false. Let us see a counterexample. Suppose k is field of characteristic $p > 0$, recall that the finite flat k-group scheme α_p is defined by

$$\alpha_p \;:=\; \mathsf{Spec}\,\Big(k[T]/(T^p)\Big).$$

Consider the finite flat k-group scheme $\alpha_p \times \alpha_p$, it has a unique k-valued point $0 \in (\alpha_p \times \alpha_p)(k)$. Then the p points $\{0, ..., 0\}$ is a full set of sections of both $\alpha_p \times \mathsf{Spec}\,(k)$ and $\mathsf{Spec}\,(k) \times \alpha_p$.

Now we can give an intrinsic definition of A-generators.

Definition 2.3.11. *Suppose G/S is a finite flat S-group scheme of finite presentation, and has rank $N \geqslant 1$. Let A be an (abstract) abelian group of order N, a group homomorphism*

$$\phi\colon A \longrightarrow G(S)$$

*is called an A-**generator** of G/S, if $\{\phi(a)\}_{a\in A}$ is a full set of sections of G/S.*

As the consequence of our discussions so far, the two definitions of A-generators are equivalent:

Proposition 2.3.12. *Let C/S be a smooth curve with structure of commutative S-group scheme, and $G \subset C$ is a closed subscheme which is finite flat and of finite presentation over S, whose rank is N. Let A be an (abstract) abelian group of order N, and*

$$\phi\colon A \longrightarrow C(S)$$

is a group homomorphism. Then the following two conditions are equivalent:

(1) ϕ is an A-generator of G/S in the sense of Definition 2.2.1, 2.2.2;

(2) ϕ is an A-generator of G/S in the sense of Definition 2.3.11.

Corollary 2.3.13. *Let $C/S, C'/S$ be smooth curves with structure of commutative S-group scheme, and $N \geqslant 1$ is an integer. If we have an isomorphism*

$$C[N] \simeq C'[N]$$

of S-group schemes, then it induces an isomorphism

$$A\text{-}\mathsf{Str}(C/S) \simeq A\text{-}\mathsf{Str}(C'/S)$$

of S-schemes, for any abstract finite abelian group A of order N.

Corollary 2.3.14. *Let C/S be a smooth curve with structure of commutative S-group scheme, and A is an (abstract) abelian group of order $N \geqslant 1$. Suppose the N-torsion subgroup scheme $C[N]$ is finite flat over S, and*

$$\phi\colon A \longrightarrow C[N](S)$$

is a group homomorphism. Then

(1) If there exists a closed S-subgroup scheme $G \subset C[N]$, such that (G, ϕ) is an A-structure on $C[N]/S$, then it must be unique;

(2) There exists a unique closed subscheme of S, locally defined by finitely many equations, which is universal for the existence of G in (1).

Proof: This is immediately deduced from Corollary 2.3.10. □

2.4 Extension of an étale group scheme

We fix the base scheme S to be connected in this section.

Suppose H, G, E are finite flat and finitely presented commutative S-group schemes, which fit into a short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & H \arrow[r] & G \arrow[r] & E \arrow[r] & 0, \end{tikzcd}$$

here we mean precisely the short exact sequence of sheaves of abelian groups on the small site S_{fppf} [8]

$$\begin{tikzcd} 0 \arrow[r] & h_H \arrow[r] & h_G \arrow[r] & h_E \arrow[r] & 0, \end{tikzcd}$$

i.e., the morphism $h_G \to h_E$ is locally surjective, and h_H is the kernel sheaf of it.

Suppose moreover E is étale over S. Given any group homomorphism from an abstract abelian group A to $G(S)$

$$\phi\colon A \longrightarrow G(S),$$

it induces the morphism of étale S-schemes

$$A \longrightarrow E$$

from the composition $A \to G(S) \to E(S)$. Since S here is connected, the kernel as a S-subgroup scheme of the constant S-group scheme A_S should also be constant, which we denote it by K as an abstract subgroup of A. Therefore we obtain the following diagram

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r] \arrow[d, "\phi|_K"] & A \arrow[r] \arrow[d, "\phi"] & A/K \arrow[r] \arrow[d, hook, "\phi|_{A/K}"] & 0 \\ 0 \arrow[r] & H(S) \arrow[r] & G(S) \arrow[r] & E(S) & \end{tikzcd}$$

Proposition 2.4.1. *A group homomorphism $\phi: A \to G(S)$ is an A-generator if and only if*

(1) $\#(K) = rk(H)$, and $\phi|_K$ is a K-generator of H/S, and

(2) $\#(A/K) = rk(E)$, and $\phi|_{A/K}$ is an A/K-generator of E/S.

Proof: *The "only if" part*: By passing the base to any geometric point $\mathsf{Spec}\,(k) \to S$, we have the diagram

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r] \arrow[d] & A \arrow[r] \arrow[d] & A/K \arrow[r] \arrow[d, hook] & 0 \\ 0 \arrow[r] & H(k) \arrow[r] & G(k) \arrow[r] & E(k) \arrow[r] & 0 \end{tikzcd}$$

Since ϕ is an A-generator of G/S, $\phi_k : A \to G(k)$ must be surjective. Then it is easy to deduce from the diagram that $\phi_k|_{A/K}$ is also surjective, hence an isomorphism. This shows (2). To show (1), choose any set-theoretic section

$$\begin{tikzcd} 0 \arrow[r] & K \arrow[r] & A \arrow[r] & A/K \arrow[r] \arrow[l, bend right, "\sigma"'] & 0, \end{tikzcd}$$

[8] Representable functors are indeed sheaves under fppf topology, cf. [7] Theorem 2.55.

we claim that it induces a splitting (only in the sense of S-schemes) of the exact sequence of S-group schemes

$$G \simeq H \times_S E.$$

Explicitly, name the morphisms in the exact sequence by $i : H \to G$ and $j : G \to E$, observe that the diagram

$$\begin{tikzcd}
H \times_S E \arrow[rrd, bend left, "\mathrm{pr}_2"] \arrow[rd, "{(i,\sigma)}"] \arrow[rdd, bend right, "\mathrm{pr}_1"'] & & \\
& G \arrow[r, "j"] \arrow[d, "1-\sigma\circ j"'] & E \arrow[d] \\
& H \arrow[r] & S
\end{tikzcd}$$

commutes, then it is immediate to check that the compositions

$$H \times_S E \xrightarrow{(i,\sigma)} G \xrightarrow{(1-\sigma\circ j,\, j)} H \times_S E$$

$$G \xrightarrow{(1-\sigma\circ j,\, j)} H \times_S E \xrightarrow{(i,\sigma)} G$$

are identities. Therefore $G \simeq H \times_S E$.

Then by Lemma 2.3.5, that $\phi|_K$ being a K-generator of H/S is indicated from that ϕ and $\phi|_{A/K}$ being A-,A/K-generators of $G/S, E/S$ respectively.

The "if" part: Similarly, using the splitting trick, the assertion is implied by Lemma 2.3.5. □

If we drop the conditions that S being connected and E being étale, we still have some partial results.

Proposition 2.4.2. *Let S be any scheme, and G, G_1, G_2 are finite flat commutative S-group schemes of finite presentation with ranks N, N_1, N_2 respectively, which fit into a short exact sequence*

$$0 \longrightarrow G_1 \longrightarrow G \longrightarrow G_2 \longrightarrow 0.$$

Moreover, suppose A, A_1, A_2 are abstract finite abelian groups of order N, N_1, N_2, and we have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A_1 \arrow[r] \arrow[d, "\phi_1"] & A \arrow[r] \arrow[d, "\phi"] & A_2 \arrow[r] \arrow[d, "\phi_2"] & 0 \\
0 \arrow[r] & G_1(S) \arrow[r] & G(S) \arrow[r] & G_2(S) &
\end{tikzcd}$$

If ϕ_1, ϕ_2 are A_1- and A_2-generator of $G_1/S, G_2/S$ respectively, then ϕ is an A-generator of G/S.

Proof: Observe that the fiber of $G \to G_2$ over any S-valued point $\phi_2(a_2) \in G_2(S)$ for some $a_2 \in A_2$ is

$G_1 \to S$. Therefore for any function f on G,

$$\begin{aligned} N_{G/S}(f) &= N_{G_2/S}(N_{G/G_2}(f)) \\ &= \prod_{a_2\in A_2} N_{G/G_2}(f)\big(\phi_2(a_2)\big) \\ &= \prod_{a_2\in A_2}\left(\prod_{a\in A,\ a\mapsto a_2} f(\phi(a))\right) \\ &= \prod_{a\in A} f(\phi(a)). \end{aligned}$$

□

The opposite direction of Proposition 2.4.2 might be false. Even if ϕ is a generator, either ϕ_1 or ϕ_2 might not be a generator, or both of them.

Example 2.4.3. *Let $S = Spec(R)$ where R is a $\mathbb{F}_p$-algebra, p is a prime number. One has the short exact sequence for group schemes of roots of unity:*

$$0 \longrightarrow \mu_p \longrightarrow \mu_{p^2} \longrightarrow \mu_p \longrightarrow 0,$$

and an exact sequence for finite abelian groups:

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow 0,$$

they fit into the commutative diagram for any p-th root of unity $\zeta \in \mu_p(R)$:

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[d, "\phi_1"] & \mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[d, "\phi"] & \mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[d, "\phi_2"] & 0 \\ 0 \arrow[r] & \mu_p(R) \arrow[r] & \mu_{p^2}(R) \arrow[r, "(-)^p"] & \mu_p(R) & \end{tikzcd}$$

where

$$\begin{aligned} \phi_1(1) &= \zeta, \\ \phi(1,-) &= \zeta, \\ \phi_2(-) &= 1. \end{aligned}$$

Since $\mu_p = Spec\left(R[T]/(T^{p^2}-1)\right)$, and we have

$$T^{p^2}-1 = \prod_{k=0}^{p-1}(T-\zeta^k)^p = \prod_{(a,b)\in\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z}}(T-\phi(a,b)),$$

then it follows from Lemma 2.3.8 that ϕ is a $(\mathbb{Z}/p\mathbb{Z}\oplus\mathbb{Z}/p\mathbb{Z})$-generator of μ_{p^2}/R.

Moreover, ϕ_1 is a $\mathbb{Z}/p\mathbb{Z}$-generator of μ_p/R if and only if

$$T^p - 1 = \prod_{k=1}^{p-1}(T-\zeta^k).$$

This could be false, for example, take $R = \mathbb{F}_p[X]/(X^p-1)$, and $\zeta = X$. In such case, ϕ_1 is not a $\mathbb{Z}/p\mathbb{Z}$-generator of μ_p/R.

Example 2.4.4. *Still take R an $\mathbb{F}_p$-algebra, and $S = Spec(R)$. Consider the group scheme α_p, and fix a R-valued point $Y \in \alpha_p(R)$ such that $Y^{p-1} \neq 0$. We have the diagram*

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[d, "\phi_1"] & \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[d, "\phi"] & \mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[d, "\phi_2"] & 0 \\
0 \arrow[r] & \alpha_p(R) \arrow[r] & (\alpha_p \times \alpha_p)(R) \arrow[r, "(-)^p"] & \alpha_p(R) &
\end{tikzcd}$$

where

$$\begin{aligned}
\phi_1(-) &= 0, \\
\phi(-,1) &= (0, Y), \\
\phi_2(1) &= Y.
\end{aligned}$$

In this case, ϕ_1 and ϕ are $\mathbb{Z}/p\mathbb{Z}$-,$(\mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z})$-generators respectively. But since

$$T^p \neq \prod_{k=0}^{p-1} (T - kY),$$

ϕ_2 is not a $\mathbb{Z}/p\mathbb{Z}$-generator of α_p/R.

Example 2.4.5. *Take $R = \mathbb{Z}/p^2\mathbb{Z}$, consider the diagram*

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[d, "\phi_1"] & \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[d, "\phi"] & \mathbb{Z}/p\mathbb{Z} \arrow[r] \arrow[d, "\phi_2"] & 0 \\
0 \arrow[r] & \mu_p(R) \arrow[r] & (\mu_p \times \mu_p)(R) \arrow[r] & \mu_p(R) &
\end{tikzcd}$$

where we let $\phi = \phi_1 = \phi_2 \equiv 1$. Then immediately, since

$$T^p - 1 \neq (T-1)^p$$

in $R = \mathbb{Z}/p^2\mathbb{Z}$, ϕ_1, ϕ_2 are not $\mathbb{Z}/p\mathbb{Z}$-generators of μ_p/R.

To show that ϕ is a generator, we need to check for any $f(X,Y) \in R[X,Y]/(X^p - 1, Y^p - 1)$ that

$$N(f) \equiv f(1,1)^{p^2} \ mod\, p^2.$$

Using a property of norm map, we calculate it through the composition:

$$\begin{tikzcd}
R[X,Y]/(X^p-1, Y^p-1) \arrow[r, "N_X"] \arrow[dr, "N"'] & R[Y]/(Y^p-1) \arrow[d, "N_Y"] \\
& R
\end{tikzcd}$$

Observe that the zero map $\mathbb{Z}/p\mathbb{Z} \to \mu_p$ is always a $\mathbb{Z}/p\mathbb{Z}$-generator when the basis is a $\mathbb{F}_p$-algebra, so at least we have

$$N_X(f) \equiv f(1,Y)^p \ mod\, p,$$

i.e., $N_X(f) = f(1,Y)^p + pg(Y)$ for some $g \in R[Y]/(Y^p - 1)$. For any $F, G \in R[Y]/(Y^p - 1)$, the norm of $F + TG$ in $R[T][Y]/(Y^p - 1)$ has the form

$$N_Y(F+TG) \;=\; N_Y(F) + \sum_{i=1}^{p-1} T^i F_i(X,Y) + T^p N_Y(G),$$

and on the other hand,

$$N_Y(F+TG) \;\equiv\; (F(1)+TG(1))^p \;\equiv\; F(1)^p + T^p G(1)^p \;\; mod\, p,$$

so it can only be that $F_i(X,Y) \equiv 0$ mod p for all $1 \leqslant i \leqslant p-1$. Take $T = p$,

$$N_Y(F+pG) \;\equiv\; N_Y(F) \;\; mod\, p^2.$$

Then

$$\begin{aligned} N(f) &= N_Y(N_X(f)) \\ &= N_Y(f(1,Y)^p + pg(Y)) \\ &\equiv N_Y(f(1,Y)^p) \\ &\equiv \big(N_Y(f(1,Y))\big)^p \\ &\equiv f(1,1)^{p^2} \;\; (mod\, p^2) \end{aligned}$$

therefore ϕ is indeed a generator.

2.5 Roots of unity

Recall that the *group scheme (over any base S) of N-th roots of unity μ_N* is the kernel of the multiplication by N of the multiplicative group scheme $\mathbb{G}_m$, i.e., we have the exact sequence

$$0 \longrightarrow \mu_N \longrightarrow \mathbb{G}_m \xrightarrow{N} \mathbb{G}_m.$$

If the base scheme is affine $S = \mathsf{Spec}\,(R)$, then explicitly we have

$$\mu_N \;=\; \mathsf{Spec}\, R[T,T^{-1}]/(T^N - 1) \;=\; \mathsf{Spec}\, R[T]/(T^N - 1).$$

In particular, μ_N is a finite flat group scheme of finite presentation over S, and it has rank N.

Lemma 2.5.1. *The S-group scheme of N-th roots of unity μ_N is the unique closed S-subgroup scheme of $\mathbb{G}_m$ which is finite flat of finite presentation over S, and has rank N.*

Proof: Suppose G is a S-subgroup scheme of $\mathbb{G}_m$ with those properties. Then by Theorem 2.1.3, G is killed by N, hence

$$G \subset \mathbb{G}_m[N] \;=\; \mu_N.$$

Moreover, since G, μ_N have the same rank, they have to be equal. □

Corollary 2.5.2. *Let A be any finite (abstract) abelian group of order N, then*

$$A\text{-}\mathit{Str}(\mathbb{G}_m/\mathbb{Z}) \;=\; A\text{-}\mathit{Gen}(\mu_N/\mathbb{Z}).$$

Definition 2.5.3. *The scheme of **primitive N-th roots of unity** $\mu_N^\times$ (over $\mathbb{Z}$) is defined to be*

$$\mu_N^\times := \mathbb{Z}/N\mathbb{Z}\text{-}\mathsf{Str}(\mathbb{G}_m/\mathbb{Z}) = \mathbb{Z}/N\mathbb{Z}\text{-}\mathsf{Gen}(\mu_N/\mathbb{Z}).$$

Therefore for any ring R, the R-valued points of $\mu_N^\times$ are

$$\mu_N^\times(R) = \left\{ \zeta \in R \;\middle|\; T^N - 1 = \prod_{k=1}^{N}(T-\zeta^k) \text{ in } R[T] \right\}.$$

Remind that the R-valued points of $\mu_N^\times$ are exactly those who are $\mathbb{Z}/N\mathbb{Z}$-generators of $\mu_N^\times/R$.

Theorem 2.5.4. *The scheme $\mu_N^\times$ is regular of dimension 1, and finite flat over $\mathbb{Z}$ with rank $\varphi(N)$. Moreover, $\mu_N^\times \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{N}]$ is finite étale over $\mathbb{Z}[\frac{1}{N}]$.*

Proof: By Corollary 2.2.9, it suffices to assume $N = p^n$ is some power of a prime number. The last assertion is proved in Proposition 2.2.5. Moreover, to obtain the rank, we calculate it on the generic fiber $\mu_{p^n}^\times(\mathbb{Q})$. The rank of $\mu_{p^n}^\times$ (over $\mathbb{Z}[\frac{1}{N}]$) is the number of primitive p^n-th roots of unity in $\mathbb{Q}$, which is apparently $\varphi(p^n) = p^{n-1}(p-1)$.

We have shown in Proposition 2.2.6 that $\mu_{p^n}^\times$ is finite over $\mathbb{Z}$. The finiteness implies that the structural morphism

$$\mu_{p^n}^\times \longrightarrow \mathsf{Spec}\,(\mathbb{Z})$$

is surjective, since its image is closed and contains $\mathsf{Spec}\,(\mathbb{Z}[\frac{1}{p}])$. So in order to show that $\mu_{p^n}^\times$ is regular, it remains to check the dimension of the local rings of points over $\mathbb{F}_p$. And notice that $\mu_{p^n}^\times$ has a unique $\mathbb{F}_p$-valued closed point $\zeta_{(p)} = 1$. [9]

As $\mu_{p^n}^\times$ is finite over $\mathbb{Z}$, we have $\dim \mathscr{O}_{\mu_{p^n}^\times,\zeta_{(p)}} \geqslant 1$. In order to prove the equality, we show that $\mathfrak{m}_{\mu_{p^n}^\times,\zeta_{(p)}}$ is principal, so that

$$1 \leqslant \dim \mathscr{O}_{\mu_{p^n}^\times,\zeta_{(p)}} \leqslant \dim \left(\mathfrak{m}_{\mu_{p^n}^\times,\zeta_{(p)}} / \mathfrak{m}^2_{\mu_{p^n}^\times,\zeta_{(p)}} \right) \leqslant 1.$$

The affine coordinate ring of $\mu_{p^n}^\times$ is $\mathscr{O}_{\mu_{p^n}^\times} = \mathbb{Z}[\zeta]/\mathfrak{a}$, where $\mathfrak{a}$ is the ideal generated by the coefficients of the polynomial

$$T^{p^n} - 1 - \prod_{k=1}^{p^n}(T-\zeta^k).$$

We claim that the regular function $\zeta - 1$ generates the maximal ideal $\mathfrak{m}_{\mu_{p^n}^\times,\zeta_{(p)}}$. The quotient ring

$$\mathscr{O}_{\mu_{p^n}^\times}/(\zeta-1) = \mathbb{Z}/\mathfrak{a}',$$

where $\mathfrak{a}'$ is the the ideal generated by the coefficients of the polynomial

$$T^{p^n} - 1 - (T-1)^{p^n}.$$

Observe that the coefficient of $T^{p^{n-1}}$ is $\binom{p^n}{p^{n-1}}$, and

$$\mathsf{ord}_p \binom{p^n}{p^{n-1}} = \sum_{k=1}^{\infty} \left\lfloor \frac{p^n}{p^k} \right\rfloor - \left\lfloor \frac{p^{n-1}}{p^k} \right\rfloor - \left\lfloor \frac{p^n - p^{n-1}}{p^k} \right\rfloor = 1,$$

[9] The notation $\zeta_{(p)}$ is only to indicate that it is over $\mathbb{F}_p$.

hence $\mathbb{Z}/\mathfrak{a}'$ is a quotient of $\mathbb{F}_p$. Apparently $\zeta - 1$ is not invertible, so it forces

$$\mathscr{O}_{\mu^{\times}_{p^n}}/(\zeta-1) \;=\; \mathbb{Z}/\mathfrak{a}' \;=\; \mathbb{F}_p,$$

which shows that $\mathscr{O}_{\mu^{\times}_{p^n},\zeta(p)}/(\zeta-1) \simeq \mathbb{F}_p$ as well, hence $\zeta - 1$ generates the maximal ideal $\mathfrak{m}_{\mu^{\times}_{p^n},\zeta(p)}$. So far we have proved that $\mu^{\times}_{p^n}$ is regular of dimension 1.

To show that $\mu^{\times}_{p^n}$ is flat over $\mathbb{Z}$, using the fact that any finite morphism between regular schemes of the same dimension is flat (cf. [2] V, Corollary 3.6). Hence $\mu^{\times}_{p^n} \hookrightarrow \mu_{p^n}$ is flat, and since μ_{p^n} is flat over $\mathbb{Z}$, the flatness of $\mu^{\times}_{p^n}$ over $\mathbb{Z}$ follows. □

It is possible to clarify the affine coordinate ring of $\mu^{\times}_N$, namely, it is the ring of algebraic integers $\mathscr{O}_N$ in the *N-th cyclotomic field* $\mathbb{Q}(\zeta_N)$. Recall that the *N-th cyclotomic polynomial* is

$$\Phi_N(X) \;=\; \prod_{1\leq k\leq N,\ (k,N)=1} (X - e^{2\pi i \frac{k}{N}}),$$

whose coefficients belong to $\mathbb{Z}$, so that one can define the N-th cyclotomic field as

$$\mathbb{Q}(\zeta_N) \;=\; \mathbb{Q}[X]/\big(\Phi_N(X)\big),$$

and its ring of algebraic integers

$$\mathscr{O}_N \;=\; \mathbb{Z}[X]/\big(\Phi_N(X)\big).$$

Theorem 2.5.5. *There is an isomorphism between schemes (over $\mathbb{Z}$)*

$$\mathit{Spec}\,(\mathscr{O}_N) \xrightarrow{\ \sim\ } \mu^{\times}_N.$$

Proof: After embedding $\mathbb{Q}(\zeta_N) \hookrightarrow \mathbb{C}$, given by that

$$\mathscr{O}_N \;=\; \mathbb{Z}[X]/\big(\Phi_N(X)\big) \ni X \longmapsto e^{\frac{2\pi i}{N}} \in \mathbb{C},$$

it is obvious that $T^N - 1 = \prod_{k=1}^{N}(T - X^k)$. Hence X lies in $\mu^{\times}_N(\mathscr{O}_N)$, and it defines a morphism

$$\psi : \mathrm{Spec}\,(\mathscr{O}_N) \longrightarrow \mu^{\times}_N,$$

whose corresponding homomorphism of global sections is

$$\begin{array}{rcl} \psi^* : \mathbb{Z}[\zeta]/\mathfrak{a} & \longrightarrow & \mathbb{Z}[X]/\big(\Phi_N(X)\big) \\ \zeta & \longmapsto & X \end{array}$$

(recall the notation in the proof of Theorem 2.5.4).

In order to show that ψ is an isomorphism, we try to find its inverse. At first thought, we could define

$$\begin{array}{rcl} (\psi^*)^{-1} : \mathbb{Z}[X]/\big(\Phi_N(X)\big) & \longrightarrow & \mathbb{Z}[\zeta]/\mathfrak{a} \\ X & \longmapsto & \zeta \end{array}$$

but it is not clear whether if it is well-defined, we have to show that $\zeta \in \mathscr{O}_{\mu_N^\times}$ satisfies $\Phi_N(\zeta) = 0$ in $\mathscr{O}_{\mu_N^\times}$. By Theorem 2.5.4, $\mathscr{O}_{\mu_N^\times}$ is a flat $\mathbb{Z}$-module, and the natural inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}[\frac{1}{N}]$ induces

$$\mathscr{O}_{\mu_N^\times} \hookrightarrow \mathscr{O}_{\mu_N^\times} \otimes_{\mathbb{Z}} \mathbb{Z}\left[\frac{1}{N}\right]$$

Thus one only needs to verify the condition $\Phi_N(\zeta) = 0$ in $\mathscr{O}_{\mu_N^\times} \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{N}]$. We claim that the restriction morphism

$$\psi\Big|_{\mathbb{Z}[\frac{1}{N}]} : \mathsf{Spec}\left(\mathscr{O}_N \otimes_{\mathbb{Z}} \mathbb{Z}\left[\frac{1}{N}\right]\right) \longrightarrow \mu_N^\times \otimes_{\mathbb{Z}} \mathbb{Z}\left[\frac{1}{N}\right]$$

is an isomorphism. Indeed, in Theorem 2.5.4 we already proved that $\mu_N^\times \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{N}]$ is finite étale over $\mathbb{Z}[\frac{1}{N}]$. And for any algebraically closed field k with characteristic coprime to N, the N-th cyclotomic polynomial $\Phi_N(X)$ has no multiple roots, hence the finite k-algebra $k[X]/(\Phi_N(X))$ is étale, i.e., it is isomorphic to the product k-algebra $k^{\varphi(N)}$. This shows that $\mathsf{Spec}\left(\mathscr{O}_N \otimes_{\mathbb{Z}} \mathbb{Z}[\frac{1}{N}]\right)$ is finite étale over $\mathbb{Z}[\frac{1}{N}]$.

Now both sides of $\psi\Big|_{\mathbb{Z}[\frac{1}{N}]}$ are finite étale, it suffices to check on any geometric fiber over $\mathbb{Z}[\frac{1}{N}]$ that it is an isomorphism, in other words, to verify that the roots of $\Phi_N(X)$ in an algebraically closed field k with characteristic coprime to N are exactly all the primitive N-th roots of unity in k. Observe that in this case, the roots of $X^N - 1$ are all distinct, hence each root is simple. Suppose $\xi \in k$ is a root of $\Phi_N(X)$, use the property that

$$\Phi_N(X) \cdot \prod_{d|N,\ d\neq N} \Phi_d(X) \;=\; X^N - 1,$$

as a root of $X^N - 1$, ξ is simple, which deduces that $\Phi_d(\xi) \neq 0$ for any $d|N$ and $d \neq N$, i.e.,

$$\xi^d - 1 \;=\; \prod_{d'|d} \Phi_{d'}(X) \;\neq\; 0. \qquad \square$$

2.6 Four basic Drinfeld level structures

In this section, we study the four basic Drinfeld level structures on elliptic curves, and their representability, which will be the central objects in later chapters.

Let E/S be an elliptic curve, and $N \geqslant 1$ an integer.

Definition 2.6.1. *A $\Gamma(N)$-**structure** (**full level** N **structure**) on E/S is a $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$-generator of the finite flat S-group scheme $E[N]/S$:*

$$\phi\colon\ \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \longrightarrow E[N](S),$$

i.e., we have the equality of effective Cartier divisors

$$E[N] \;=\; \sum_{a,b \bmod N} [\phi(a,b)],$$

or intrinsically, the N^2 sections $\phi(a,b)$ form a full set of sections of $E[N]/S$. The two sections

$$P \;=\; \phi(1,0), \qquad Q \;=\; \phi(0,1)$$

*are called a **Drinfeld basis** of the $\Gamma(N)$-structure.*

Definition 2.6.2. *A $\Gamma_1(N)$-**structure** on E/S is a $\mathbb{Z}/N\mathbb{Z}$-structure on E/S:*

$$\phi\colon\ \mathbb{Z}/N\mathbb{Z}\ \longrightarrow\ E[N](S),$$

i.e., the effective Cartier divisors $\sum_{a \bmod N}[\phi(a)]$ is a S-subgroup scheme of E/S.

Definition 2.6.3. *A $\Gamma_1^{\boldsymbol{bal}}(N)$-**structure** (**balanced** $\Gamma_1(N)$-**structure**) on E/S is an exact sequence of S-group schemes*

$$0 \longrightarrow K \longrightarrow E[N] \longrightarrow K' \longrightarrow 0,$$

together with specified K-, K'-generators $P \in K(S)$, $P' \in K'(S)$. Here both K and K' are required to be locally free of rank N.

Definition 2.6.4. *A $\Gamma_0(N)$-**structure** on E/S is a cyclic S-subgroup scheme $K \subset E[N]$ of rank N.*

Remark:

- A $\Gamma_1(N)$-structure on E/S is equivalently given by a N-isogeny of elliptic curves over S:

$$\phi\colon\ E\ \longrightarrow\ E',$$

together with a specified generator $P \in \mathsf{ker}(\phi)(S)$, i.e., there is an equality of effective Cartier divisors:

$$\mathsf{ker}(\phi)\ =\ \sum_{a \bmod N}[aP].$$

- A $\Gamma_1^{\mathrm{bal}}(N)$-structure is equivalently given by a N-isogeny ϕ

$$\begin{tikzcd} E \arrow[r, shift left, "\phi"] & E', \arrow[l, shift left, "\phi^t"] \end{tikzcd}$$

together with specified generators of $\mathsf{ker}(\phi)$ and $\mathsf{ker}(\phi^t)$, where ϕ^t is the dual isogeny (cf. Definition 8.4.6) of ϕ.

- A $\Gamma_0(N)$-structure on E/S is equivalently given by a N-isogeny of elliptic curves $\phi: E \to E'$.

Fix an elliptic curve E/S, we denote the following contravariant functors

$$\begin{array}{ccl} \mathfrak{Sch}_{/S} & \longrightarrow & \mathfrak{Set} \\ T & \longmapsto & \left\{\begin{array}{l} \Gamma(N)\text{-structures on } E_T/T \\ \Gamma_1(N)\text{-structures on } E_T/T \\ \Gamma_1^{\mathrm{bal}}(N)\text{-structures on } E_T/T \\ \Gamma_0(N)\text{-structures on } E_T/T \end{array}\right. \end{array}$$

by $\Gamma(N)$-Str(E/S), $\Gamma_1(N)$-Str(E/S), $\Gamma_1^{\mathrm{bal}}(N)$-Str$(E/S)$ and $\Gamma_0(N)$-Str(E/S) respectively. By definition, we know that

$$\begin{aligned} \Gamma(N)\text{-}\mathsf{Str}(E/S) &= (\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z})\text{-}\mathsf{Gen}(E[N]/S) \\ \Gamma_1(N)\text{-}\mathsf{Str}(E/S) &= \mathbb{Z}/N\mathbb{Z}\text{-}\mathsf{Str}(E/S). \end{aligned}$$

Lemma 2.6.5. *Let E/S be an elliptic curve, and $N \geqslant 1$ is an integer. Suppose $N = N_1N_2$ with $(N_1, N_2) = 1$, then we have the functorial factorizations of S-schemes*

$$\begin{array}{rcl}
\Gamma(N)\text{-}\mathit{Str}(E/S) & \simeq & \Gamma(N_1)\text{-}\mathit{Str}(E/S)\times_S\Gamma(N_2)\text{-}\mathit{Str}(E/S)\\
\Gamma_1(N)\text{-}\mathit{Str}(E/S) & \simeq & \Gamma_1(N_1)\text{-}\mathit{Str}(E/S)\times_S\Gamma_1(N_2)\text{-}\mathit{Str}(E/S)\\
\Gamma_1^{bal}(N)\text{-}\mathit{Str}(E/S) & \simeq & \Gamma_1^{bal}(N_1)\text{-}\mathit{Str}(E/S)\times_S\Gamma_1^{bal}(N_2)\text{-}\mathit{Str}(E/S)\\
\Gamma_0(N)\text{-}\mathit{Str}(E/S) & \simeq & \Gamma_0(N_1)\text{-}\mathit{Str}(E/S)\times_S\Gamma_0(N_2)\text{-}\mathit{Str}(E/S).
\end{array}$$

Proof: The first two cases are implied by Corollary 2.2.9. The last case is by canonical factorization of cyclic group schemes, i.e., the isomorphism is given by

$$\begin{array}{rcl}
\Gamma_0(N)\text{-}\mathsf{Str}(E/S) & \simeq & \Gamma_0(N_1)\text{-}\mathsf{Str}(E/S)\times_S\Gamma_0(N_2)\text{-}\mathsf{Str}(E/S).\\
K & \longmapsto & K[N_1]\times K[N_2].
\end{array}$$

For the balanced structures, given a $\Gamma_1^{\mathrm{bal}}(N)$-structure on E/S

$$0 \longrightarrow K \longrightarrow E[N] \longrightarrow K' \longrightarrow 0,$$

it naturally induces a $\Gamma_1^{\mathrm{bal}}(N_i)$-structure

$$0 \longrightarrow K[N_i] \longrightarrow E[N_i] \longrightarrow K'[N_i] \longrightarrow 0.$$

Conversely, given a $\Gamma_1^{\mathrm{bal}}(N_1)$-structure and a $\Gamma_1^{\mathrm{bal}}(N_2)$-structure on E/S, one takes the product of two exact sequences, then it is a $\Gamma_1^{\mathrm{bal}}(N)$-structure. It is obvious that the two maps are mutually inverse. □

Next we study the representability of these functors, except for the $\Gamma_0[N]$-structures, which we leave to later section, after we further develop the theory of cyclic group schemes.

Theorem 2.6.6 (Relative Representability Theorem)**.** *The functors $\Gamma(N)$-$\mathit{Str}(E/S)$, $\Gamma_1(N)$-$\mathit{Str}(E/S)$ and $\Gamma_1^{bal}(N)$-$\mathit{Str}(E/S)$ are all represented by finite S-schemes.*

Proof: The first two cases have already been proved in Proposition 2.2.4 and Proposition 2.2.6. It remains to treat the balanced level structures. The finite S-scheme $\mathbb{Z}/N\mathbb{Z}$-Str$(E[N]/S)$ classifies all the cyclic subgroup scheme of $E[N]$ of rank N, with a specified generator. Let $\mathbf{K}_{\text{univ}}$ be the universal family, which is a closed subscheme of $\mathbb{Z}/N\mathbb{Z}$-Str$(E[N]/S)\times E[N]$:

$$\begin{tikzcd}
\mathbf{K}_{\text{univ}} \arrow[r, phantom, "\subset"] \arrow[d] & \mathbb{Z}/N\mathbb{Z}\text{-}\mathsf{Str}(E[N]/S)\times E[N] \arrow[dl, "p_1"'] \\
\mathbb{Z}/N\mathbb{Z}\text{-}\mathsf{Str}(E[N]/S) &
\end{tikzcd}$$

and let

$$\mathbf{K}'_{\text{univ}} = \mathbb{Z}/N\mathbb{Z}\text{-}\mathsf{Str}(E[N]/S)\times E[N]\big/\mathbf{K}_{\text{univ}}$$

be the universal quotient. Then it is straightforward that the functor $\Gamma_1^{\mathrm{bal}}(N)$-Str$(E/S)$ is represented by the $\big(\mathbb{Z}/N\mathbb{Z}\text{-}\mathsf{Str}(E[N]/S)\big)$-scheme:

$$\mathbb{Z}/N\mathbb{Z}\text{-}\mathsf{Gen}\big(\mathbf{K}'_{\text{univ}}/\mathbb{Z}/N\mathbb{Z}\text{-}\mathsf{Str}(E[N]/S)\big),$$

which is finite over $\mathbb{Z}/N\mathbb{Z}$-Str$(E[N]/S)$, and since $\mathbb{Z}/N\mathbb{Z}$-Str$(E[N]/S)$ is finite over S, the scheme $\Gamma_1^{\mathrm{bal}}(N)$-Str$(E/S)$ is therefore also finite over S. □

Theorem 2.6.7 (Relative Representability Theorem over $\mathbb{Z}[\frac{1}{N}]$)**.** *Assume that N is invertible on the base S, then the functors $\Gamma(N)$-Str(E/S), $\Gamma_1(N)$-Str(E/S), $\Gamma_1^{bal}(N)$-Str(E/S) and $\Gamma_0(N)$-Str(E/S) are all represented by finite étale S-schemes.*

Proof: The first two cases have already been proved in Proposition 2.2.5 and 2.2.7. The case for balanced level structures is a consequence of Proposition 2.2.5 and 2.2.7, since in the case that N is invertible on S, the scheme $\mathbb{Z}/N\mathbb{Z}\text{-Gen}\big(\mathbf{K}'_{\text{univ}}/\mathbb{Z}/N\mathbb{Z}\text{-Str}(E[N]/S)\big)$ is finite étale over $\mathbb{Z}/N\mathbb{Z}\text{-Str}(E[N]/S)$, and the scheme $\mathbb{Z}/N\mathbb{Z}\text{-Str}(E[N]/S)$ is finite étale over S.

It remains to treat the case of $\Gamma_0(N)$-structures. Firstly, observe that the functor $\Gamma_0(N)\text{-Str}(E/S)$ is a sheaf for the fppf topology. Indeed, by faithfully flat descent for affine morphisms (cf. Theorem 9.1.12), one can glue a finite locally free subgroup scheme from local data, [10] and the concept of cyclicity is already fppf-local. Thus, in order to show the representability of $\Gamma_0(N)\text{-Str}(E/S)$, it suffices to do so after a fppf base change. By Theorem 8.4.1, in the case that N is invertible, $E[N]$ is fppf-locally isomorphic to the constant group scheme $\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}$, so after some fppf base change, we assume $E[N]=\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}$. Let

$$\text{Cyc}_N(\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}) := \left\{ \begin{array}{l} \text{all cyclic } S\text{-subgroup schemes} \\ \text{of order } N \text{ in } E[N]. \end{array} \right\},$$

which is a finite set. We claim that for any connected S-scheme T, any cyclic T-subgroup scheme K of order N in $E_T[N]$ is constant. One can immediately reduce the case to where T is noetherian, since we have the condition of finite presentation. As a closed subgroup scheme of a finite étale group scheme $E_T[N]$ which is also flat over T, K is finite étale over T. Hence K is an étale covering of T. Choose any geometric point $t\in T$, let $\mathscr{C}$ be the category of étale coverings of T, recall that the functor

$$F_t : \mathscr{C} \longrightarrow \pi_1(T,t)\text{-}\mathfrak{FSet}$$

defines an equivalence between the category $\mathscr{C}$ and the category $\pi_1(T,t)$-$\mathfrak{FSet}$ of finite $\pi_1(T,t)$-sets. Since K is a subgroup scheme of $E_T[N]$, the finite $\pi_1(T,t)$-set $F(K)$ is naturally a $\pi_1(T,t)$-subset of $F(E_T[N])$. But the $\pi_1(T,t)$-action on $F(E_T[N])$ is trivial, hence so is $F(K)$, which deduces that K is also a trivial étale covering. Thus we proved the claim.

Now it is clear that the functor $\Gamma_0(N)\text{-Str}(E/S)$ is represented by the constant finite S-scheme $S\times\text{Cyc}_N(\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z})$. □

Étale-locally, all the four Drinfeld level structures are represented by constant schemes.

Corollary 2.6.8. *Assume that N is invertible on the base S, and $E[N]/S$ is isomorphic to the constant group scheme $\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}$. Then the functors $\Gamma(N)$-Str(E/S), $\Gamma_1(N)$-Str(E/S), $\Gamma_1^{bal}(N)$-Str(E/S) and $\Gamma_0(N)$-Str(E/S) are represented by constant S-schemes:*

- $S\times\{\textit{all Drinfeld basis of } \mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}\}$,
- $S\times\{\textit{all the points } P\in E[N](S) \textit{ of exact order } N\}$,
- $S\times\left\{\begin{array}{l}\textit{all triples } (K,P,P')\textit{, where } K \textit{ is a subgroup of } \mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}\textit{, and } P \textit{ is a} \\ \textit{generator of } K\textit{, } P' \textit{ is a generator of the quotient } (\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z})\big/K\end{array}\right\}$,
- $S\times Cyc_N(\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z})$

[10] We can ensure the group structure, since a group structure is given by a unit morphism, a multiplication morphism and an inverse morphism, satisfying some commutative diagrams, which all can be descended along a fppf covering.

respectively.

Remark: As an immediate consequence, the three representable moduli problems that we have discussed in Appendix II.3 are all étale over the base. Moreover, the elementary moduli schemes $\mathsf{Spec}\ (\mathbf{R}_2)$ and $\mathsf{Spec}\ (\mathbf{R}_3)$ are $GL(2,\mathbb{F}_2)\times\{\pm 1\}$-, $GL(2,\mathbb{F}_3)$-torsors respectively, in the sense that for any morphism $S\to\mathscr{M}_{1,1}$ from a scheme S to the stack $\mathscr{M}_{1,1}$, the morphism of schemes

$$S\times_{\mathscr{M}_{1,1}}\mathsf{Spec}\,\mathbf{R}_i\longrightarrow S\qquad(i=2,3)$$

is a $\big(GL(2,\mathbb{F}_2)\times\{\pm 1\}$-, $GL(2,\mathbb{F}_3)$-$\big)$ torsor.

3 Moduli Stacks of Elliptic Curves

In this chapter, we come to deal with various moduli problems of elliptic curves. The moduli stack of elliptic curves (without extra structures) is $\mathscr{M}_{1,1}$, which is a special case of moduli stack of n-pointed smooth genus g curves $\mathscr{M}_{g,n}$. In Katz-Mazur [24], they define a *moduli problem* $\mathscr{P}$ of elliptic curves as a functor

$$\mathscr{P}: \mathbf{Ell} \longrightarrow \mathfrak{Set}$$

where **Ell** is the category consists of objects as elliptic curves over schemes

$$\begin{tikzcd} E \arrow[d, "\pi"] \\ S \end{tikzcd}$$

and morphisms as Cartesian diagrams

$$\begin{tikzcd} E' \arrow[r, "\phi"] \arrow[d, "\pi'"'] & E \arrow[d, "\pi"] \\ S' \arrow[r, "f"] & S \end{tikzcd}$$

equivalently this means we have an isomorphism of S'-schemes

$$E' \xrightarrow[\sim]{(\phi,\pi')} E \times_S S'$$

An element of $\mathscr{P}(E/S)$ is called a *level $\mathscr{P}$ structure* on E/S.

Here the category **Ell** is exactly the moduli stack $\mathscr{M}_{1,1}$, and a moduli problem is given equivalently by a CFG [1] $\mathscr{P}$ over $\mathfrak{Sch}$

$$\begin{tikzcd}\mathscr{P} \arrow[d, "p"] \\ \mathfrak{Sch}\end{tikzcd}$$

whose fiber over a scheme S has objects $(E/S, a)$, where $a \in \mathscr{P}(E/S)$ is a level $\mathscr{P}$ structure, and morphisms are compatible with pull-back of respective level $\mathscr{P}$ structures. Moreover, there is a morphism of CFGs

$$F: \mathscr{P} \longrightarrow \mathscr{M}_{1,1}$$

given by forgetting the level $\mathscr{P}$ structures.

What we concern is when is $\mathscr{P}$ a stack, an algebraic stack, and further more, represented by a scheme. In the second case, we call the moduli problem $\mathscr{P}$ *algebraic*, and in the latter case it is called *representable*. If $\mathscr{P}$ is represented by a scheme $M(\mathscr{P})$, then the morphism $M(\mathscr{P}) \to \mathscr{M}_{1,1}$ provides (through Yoneda Lemma 9.2.6) the *universal family* of the moduli problem $\mathscr{P}$:

$$\begin{tikzcd}\mathbf{E} \arrow[d] \\ M(\mathscr{P})\end{tikzcd}$$

which is also the object representing the functor $\mathscr{P}: \mathscr{M}_{1,1} \to \mathfrak{Set}$, i.e.,

$$\mathscr{P}(-) \simeq \mathsf{Hom}_{\mathscr{M}_{1,1}}\big(-, \mathbf{E}/M(\mathscr{P})\big).$$

3.1 Representability of modular curves

From now on, we do not distinguish the moduli functor $\mathscr{P}$ and its associated CFG.

Any moduli problem $\mathscr{P}$ of elliptic curves gives a moduli functor on $\mathfrak{Sch}$:

$$\begin{aligned}\widetilde{\mathscr{P}}: \mathfrak{Sch} &\longrightarrow \mathfrak{Set}\\ S &\longmapsto \left\{(E/S, a) \,\middle|\, \begin{array}{l}E \text{ is an elliptic curve over}\\ S, \text{ and } a \in \mathscr{P}(E/S).\end{array}\right\} \Big/ \simeq\end{aligned}$$

If $\mathscr{P}$ is represented by a scheme $M(\mathscr{P})$, then $M(\mathscr{P})$ certainly represents the moduli functor $\widetilde{\mathscr{P}}$, and the image of the identity under the isomorphism

$$\begin{array}{ccc}\mathsf{Hom}_{\mathfrak{Sch}}(M(\mathscr{P}), M(\mathscr{P})) & \simeq & \widetilde{\mathscr{P}}(M(\mathscr{P}))\\ \uplus & & \uplus\\ \mathsf{id} & \longmapsto & a_{\text{univ}}\end{array}$$

is the *universal level $\mathscr{P}$ structure* on $\mathbf{E}/M(\mathscr{P})$. But conversely, even if the moduli functor $\widetilde{\mathscr{P}}$ is representable, $\mathscr{P}$ is not necessarily representable. One needs a condition of rigidity to ensure the converse.

[1] "CFG" stands for "categories fibered in groupoids", cf. 9.2

Definition 3.1.1. *The moduli problem $\mathscr{P}$ is called **rigid**, if any object of $\mathscr{P}$ has no non-trivial automorphisms.*

Remark:

- It is easy to see that any representable $\mathscr{P}$ has to be rigid. Conversely, if we only know that the moduli functor $\widetilde{\mathscr{P}}$ is representable, say by $(\mathbf{E}/M(\mathscr{P}), a_{\text{univ}})$, a priori we only have the natural transformation of functors
$$\Psi\colon \mathsf{Hom}_{\mathscr{M}_{1,1}}\big(-,\mathbf{E}/M(\mathscr{P})\big) \longrightarrow \mathscr{P}(-),$$
by representability of $\widetilde{\mathscr{P}}$, $\Psi(E/S)$ is surjective for any elliptic curve E/S. If moreover $\mathscr{P}$ is rigid, then $\Psi(E/S)$ is also injective, hence bijective, which shows the representability of $\mathscr{P}$.
- A moduli CFG $\mathscr{P}$ being rigid means exactly that it is a CFS [2] over $\mathscr{M}_{1,1}$, i.e., it comes from a functor, which is just $\widetilde{\mathscr{P}}$.

Definition 3.1.2. *The moduli problem $\mathscr{P}$ is called **relatively representable**, if the morphism of CFGs*
$$F\colon \mathscr{P} \longrightarrow \mathscr{M}_{1,1}$$
is representable.

Remark:

- Relative representability is also equivalent as following: the moduli problem $\mathscr{P}$ is relatively representable, if for any elliptic curve E/S, the functor
$$\begin{array}{rcl} \mathfrak{Sch}_{/S} & \longrightarrow & \mathfrak{Set} \\ T & \longmapsto & \mathscr{P}(E\times_S T/T) = \mathscr{P}(E_T/T) \end{array}$$
is represented by a S-scheme $\mathscr{P}_{E/S}$. Observe that $\mathscr{P}_{E/S}$ is nothing but the fiber product $\mathscr{P}\times_{\mathscr{M}_{1,1}} S$, since in the Cartesian diagram
$$\begin{tikzcd} \mathscr{P}\times_{\mathscr{M}_{1,1}} S \arrow[r] \arrow[d] & S \arrow[d] \\ \mathscr{P} \arrow[r] & \mathscr{M}_{1,1} \end{tikzcd}$$
the first row is a morphism of schemes, which is exactly the structure morphism of $\mathscr{P}_{E/S}$.
- Any representable moduli problem $\mathscr{P}$ is relatively representable, this is a consequence of that $\mathscr{M}_{1,1}$ has representable diagonal morphism, [3] by Lemma 9.3.3, any morphism from a scheme to $\mathscr{M}_{1,1}$ is representable, which implies that
$$\mathscr{P} \simeq M(\mathscr{P}) \longrightarrow \mathscr{M}_{1,1}$$
is representable.

[2] "CFS" stands for "categories fibered in sets".

[3] cf. Example 9.4.3.

- Another immediate consequence is that, if $\mathscr{P}$ is a relatively representable moduli problem, and $\mathscr{P}'$ is a representable moduli problem, then the *simultaneous moduli problem*

  $$E/S \longmapsto \mathscr{P}(E/S) \times \mathscr{P}'(E/S)$$

  is representable, and it is represented by the $M(\mathscr{P}')$-scheme

  $$\mathscr{P}_{\mathbf{E}'/M(\mathscr{P}')} \;=\; \mathscr{P} \times_{\mathscr{M}_{1,1},\mathbf{E}'} M(\mathscr{P}'),$$

  where $\mathbf{E}'/M(\mathscr{P}')$ is the universal family of $\mathscr{P}'$.

Proposition 3.1.3. *Any relatively representable moduli problem $\mathscr{P}$ of elliptic curves is a Deligne-Mumford stack.*

Proof: Firstly we show that any étale morphism is of effective descent for $\mathscr{P}$. Let $S' \to S$ be an étale morphism, and $((E'/S', \alpha), \theta)$ is a descent datum of an elliptic curve with a level $\mathscr{P}$ structure. By étale descent, we can descend E' to an elliptic curve E/S. To descend the level $\mathscr{P}$ structure, it amounts to prove that the following sequence is exact:

$$\mathscr{P}(E/S) \;\longrightarrow\; \mathscr{P}(E'/S') \;\rightrightarrows\; \mathscr{P}(E''/S'').$$

This is automatically satisfied by the relative representability of $\mathscr{P}$. To show that we can also glue morphisms, it suffices to prove the representability of the diagonal morphism. Let S be any scheme and $S \to \mathscr{P} \times \mathscr{P}$ be a morphism. From the cartesian diagram

$$\begin{tikzcd}
\mathscr{P} \times_{\mathscr{P}\times\mathscr{P}} S \arrow[r] \arrow[d] & S \arrow[d] \\
\mathscr{P} \arrow[r, "\Delta_{\mathscr{P}}"] \arrow[d] & \mathscr{P} \times \mathscr{P} \arrow[d] \\
\mathscr{M}_{1,1} \arrow[r, "\Delta_{\mathscr{M}_{1,1}}"] & \mathscr{M}_{1,1} \times \mathscr{M}_{1,1}
\end{tikzcd}$$

it is clear that $\mathscr{P} \times_{\mathscr{P}\times\mathscr{P}} S = \mathscr{M}_{1,1} \times_{\mathscr{M}_{1,1}\times\mathscr{M}_{1,1}} S$ is a scheme. Therefore $\mathscr{P}$ is a stack.

It remains to find an étale atlas for $\mathscr{P}$. Let $U \to \mathscr{M}_{1,1}$ be an étale atlas for $\mathscr{M}_{1,1}$, then obviously that

$$\mathscr{P} \times_{\mathscr{M}_{1,1}} U \;\longrightarrow\; \mathscr{P}$$

is an étale atlas for $\mathscr{P}$. □

Definition 3.1.4. *A relatively representable moduli problem $\mathscr{P}$ is said to have property*[4] *P if the representable morphism of Deligne-Mumford stacks*

$$F:\; \mathscr{P} \;\longrightarrow\; \mathscr{M}_{1,1}$$

has property P.

[4] Here P is some property for morphisms of schemes, which is preserved under any base change, e.g., affine, finite, étale... etc.

Our main result of this section is the following representability theorem:

Theorem 3.1.5. *Let $\mathscr{P}$ be a moduli problem of elliptic curves, which is relatively representable and affine. Then $\mathscr{P}$ is representable if and only if it is rigid.*

Proof: To make the proof clear, we divide it into three steps.

Step 1: Observe that we only need to prove the representability of $\mathscr{P}\otimes\mathbb{Z}[\frac{1}{2}]$ and $\mathscr{P}\otimes\mathbb{Z}[\frac{1}{3}]$. Because the surjective family

$$\mathsf{Spec}\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)\coprod\mathsf{Spec}\left(\mathbb{Z}\left[\frac{1}{3}\right]\right)\longrightarrow\mathsf{Spec}\,(\mathbb{Z})$$

is a morphism of effective descent, and by rigidity, the affine morphism

$$\mathscr{P}\otimes\mathbb{Z}\left[\frac{1}{2}\right]\coprod\mathscr{P}\otimes\mathbb{Z}\left[\frac{1}{3}\right]\longrightarrow\mathsf{Spec}\left(\mathbb{Z}\left[\frac{1}{2}\right]\right)\coprod\mathsf{Spec}\left(\mathbb{Z}\left[\frac{1}{3}\right]\right)$$

obviously satisfies the cocycle condition. Thus $\mathscr{P}$ is represented by the scheme which is descent from the above affine scheme over $\mathsf{Spec}\,(\mathbb{Z}[\frac{1}{2}])\coprod\mathsf{Spec}\,(\mathbb{Z}[\frac{1}{3}])$.

Step 2: *Descending the universal family.* Use the elementary moduli schemes $\mathsf{Spec}\,(\mathbf{R}_2)$, $\mathsf{Spec}\,(\mathbf{R}_3)$ as auxiliaries. We have the cartesian diagram for $i=2,3$

$$\begin{tikzcd}
\mathscr{P}\times_{\mathscr{M}_{1,1}}\mathsf{Spec}\,(\mathbf{R}_i) \arrow[r] \arrow[d] & \mathsf{Spec}\,(\mathbf{R}_i) \arrow[d] \\
\mathscr{P} \arrow[r] & \mathscr{M}_{1,1}
\end{tikzcd}$$

and $\mathsf{Spec}\,(\mathbf{R}_i)\to\mathscr{M}_{1,1}$ is a G_i-torsor, where

$$G_i=\begin{cases} GL(2,\mathbb{F}_2)\times\{\pm1\} & i=2\\ GL(2,\mathbb{F}_3) & i=3\end{cases}$$

We aim to show that

$$\mathscr{P}\;\simeq\;\left(\mathscr{P}\times_{\mathscr{M}_{1,1}}\mathsf{Spec}\,(\mathbf{R}_i)\right)/G_i, \tag{$*$}$$

and the simultaneous universal family of $\mathscr{P}\times_{\mathscr{M}_{1,1}}\mathsf{Spec}\,(\mathbf{R}_i)$ descends through the quotient by G_i. The right side of $(*)$ is a quotient of an affine scheme by finite group action, which is indeed an affine scheme. Let

$$\begin{tikzcd}
(\mathbf{E}_i,\alpha_{\text{univ}},\beta_{\text{univ}}) \arrow[d] \\
\mathscr{P}\times_{\mathscr{M}_{1,1}}\mathsf{Spec}\,(\mathbf{R}_i)
\end{tikzcd}$$

be the simultaneous universal family, where $\alpha_{\text{univ}},\beta_{\text{univ}}$ are the universal objects of respective factors. An element $g\in G_i$ acts on the universal object β_{univ}, the resulting family $(\mathbf{E}_i,\alpha_{\text{univ}},g\cdot\beta_{\text{univ}})$ corresponds to an isomorphism

$$\mathscr{P}\times_{\mathscr{M}_{1,1}}\mathsf{Spec}\,(\mathbf{R}_i)\xrightarrow[\sim]{g}\mathscr{P}\times_{\mathscr{M}_{1,1}}\mathsf{Spec}\,(\mathbf{R}_i),$$

which induces an isomorphism

$$g^*(\mathbf{E}_i,\alpha_{\text{univ}},\beta_{\text{univ}})\xrightarrow[\sim]{\theta(g)}(\mathbf{E}_i,\alpha_{\text{univ}},g\cdot\beta_{\text{univ}}),$$

take restriction on the first universal object, it gives an isomorphism

$$g^*(\mathbf{E}_i, \alpha_{\text{univ}}) \xrightarrow[\sim]{\theta(g)} (\mathbf{E}_i, \alpha_{\text{univ}}).$$

By rigidity of $\mathscr{P}$, $\theta(g)$ is the unique isomorphism between these two families, so it is necessarily compatible with the group structure of G, i.e., for any elements $g, g' \in G_i$, the diagram

$$\begin{tikzcd}
g'^* g^*(\mathbf{E}_i, \alpha_{\text{univ}}) \arrow[r, "g'^*\theta(g)"] \arrow[dr, "\theta(gg')"'] & g'^*(\mathbf{E}_i, \alpha_{\text{univ}}) \arrow[d, "\theta(g')"] \\
& (\mathbf{E}_i, \alpha_{\text{univ}})
\end{tikzcd}$$

commutes. Therefore $\big((\mathbf{E}_i, \alpha_{\text{univ}}), \theta\big)$ is a descent datum of the finite étale [5] morphism

$$\mathscr{P} \times_{\mathscr{M}_{1,1}} \mathsf{Spec}\,(\mathbf{R}_i) \longrightarrow \big(\mathscr{P} \times_{\mathscr{M}_{1,1}} \mathsf{Spec}\,(\mathbf{R}_i)\big)/G_i,$$

by faithfully flat descent, we obtain a family

$$\begin{tikzcd}
(\mathbf{E}'_i, \alpha'_{\text{univ}}) \arrow[d] \\
\big(\mathscr{P} \times_{\mathscr{M}_{1,1}} \mathsf{Spec}\,(\mathbf{R}_i)\big)/G_i.
\end{tikzcd}$$

Step 3: *Universality.* It remains to prove the universality of the family $(\mathbf{E}'_i, \alpha'_{\text{univ}})$ with respect to the moduli problem $\mathscr{P} \otimes \mathbb{Z}[\frac{1}{i}]$. Let S be a $\mathbb{Z}[\frac{1}{i}]$-scheme, and $(E/S, \alpha)$ is an elliptic curve over S with a level $\mathscr{P}$ structure α. Denote

$$\pi : \ S_i := S \times_{\mathscr{M}_{1,1}} \mathsf{Spec}\,(\mathbf{R}_i) \longrightarrow S,$$

which is a finite étale G_i-torsor. Base change E/S to $E_i/S_i := E \times_S S_i/S_i$, one obtains a family

$$\begin{tikzcd}
(E_i, \pi^*\alpha, \beta_E) \arrow[d] \\
S_i
\end{tikzcd}$$

where β_E is the universal object of E_i with respect to the moduli problem $\mathsf{Spec}\,(\mathbf{R}_i)$. This family corresponds to a G_i-equivariant morphism [6]

$$f : \ S_i = S \times_{\mathscr{M}_{1,1}} \mathsf{Spec}\,(\mathbf{R}_i) \longrightarrow \mathscr{P} \times_{\mathscr{M}_{1,1}} \mathsf{Spec}\,(\mathbf{R}_i)$$

taking the quotient by G_i, one has the cartesian diagram

$$\begin{tikzcd}
S_i \arrow[r, "f"] \arrow[d, "\pi"'] & \mathscr{P} \times_{\mathscr{M}_{1,1}} \mathsf{Spec}\,(\mathbf{R}_i) \arrow[d, "\pi_{\text{univ}}"] \\
S \arrow[r, "f_0"] & \big(\mathscr{P} \times_{\mathscr{M}_{1,1}} \mathsf{Spec}\,(\mathbf{R}_i)\big)/G_i
\end{tikzcd}$$

[5] By rigidity of $\mathscr{P}$, the action of G_i on $\mathscr{P} \times_{\mathscr{M}_{1,1}} \mathsf{Spec}\,(\mathbf{R}_i)$ is free, hence the quotient morphism is finite étale (cf. Demazure-Gabriel [22] III, 2.6.1).

[6] Indeed, G_i acts only on the second factor.

It is immediate to see that

$$\begin{aligned}\pi^*(E,\alpha) = (E_i,\pi^*\alpha) &= f^*(\mathbf{E}_i,\alpha_{\text{univ}})\\ &= f^*\pi^*_{\text{univ}}(\mathbf{E}'_i,\alpha'_{\text{univ}})\\ &= \pi^* f_0^*(\mathbf{E}'_i,\alpha'_{\text{univ}}),\end{aligned}$$

by finite étale descent, $(E,\alpha) \simeq f_0^*(\mathbf{E}'_i,\alpha'_{\text{univ}})$, i.e., the family $(E/S,\alpha)$ comes from the morphism f_0.

Finally we need to verify the uniqueness of such morphism f_0. Suppose

$$h_0\colon S \longrightarrow \big(\mathscr{P}\times_{\mathscr{M}_{1,1}}\mathsf{Spec}\,(\mathbf{R}_i)\big)/G_i$$

is another such morphism, i.e., $(E,\alpha)\simeq h_0^*(\mathbf{E}'_i,\alpha'_{\text{univ}})$. Let h be the lifting of h_0,

$$\begin{tikzcd}R \arrow[r, "h"] \arrow[d, "\pi'"'] & \mathscr{P}\times_{\mathscr{M}_{1,1}}\mathsf{Spec}\,(\mathbf{R}_i) \arrow[d, "\pi_{\text{univ}}"] \\ S \arrow[r, "h_0"] & \big(\mathscr{P}\times_{\mathscr{M}_{1,1}}\mathsf{Spec}\,(\mathbf{R}_i)\big)/G_i\end{tikzcd}$$

where R is the fiber product. Then E_R carries the level structure $h^*\beta_{\text{univ}}$, which corresponds to a G_i-equivariant morphism of G_i-torsors:

$$\begin{tikzcd}R \arrow[rr] \arrow[dr, "\pi'"'] & & S_i \arrow[dl, "\pi"] \\ & S & \end{tikzcd}$$

which is necessarily an isomorphism. Hence one has the cartesian diagram

$$\begin{tikzcd}S_i \arrow[r, "h"] \arrow[d, "\pi"'] & \mathscr{P}\times_{\mathscr{M}_{1,1}}\mathsf{Spec}\,(\mathbf{R}_i) \arrow[d, "\pi_{\text{univ}}"] \\ S \arrow[r, "h_0"] & \big(\mathscr{P}\times_{\mathscr{M}_{1,1}}\mathsf{Spec}\,(\mathbf{R}_i)\big)/G_i\end{tikzcd}$$

consequently $h^*(\mathbf{E}_i,\alpha_{\text{univ}}) = \pi^*(E,\alpha) = f^*(\mathbf{E}_i,\alpha_{\text{univ}})$, which forces $f = h$ by the universality of $\mathscr{P}\times_{\mathscr{M}_{1,1}}\mathsf{Spec}\,(\mathbf{R}_i)$. Therefore $h_0 = f_0$. □

Consider the moduli problems of $\Gamma(N)$-, $\Gamma_1(N)$-, $\Gamma_1^{\text{bal}}(N)$- and $\Gamma_0(N)$-structures on elliptic curves, let us denote their moduli stacks by $\mathscr{Y}(N)$, $\mathscr{Y}_1(N)$, $\mathscr{Y}_1^{\text{bal}}(N)$ and $\mathscr{Y}_0(N)$ respectively. Combine the previous theorem and the rigidity results (cf. Corollary 8.4.12, 8.4.13) of the four basic Drinfeld level structures, we immediately have the following representability results: [7]

Corollary 3.1.6 (Representability of modular curves). *(1) If $N \geqslant 3$, the modular curve $\mathscr{Y}(N)$ is represented by an affine curve $Y(N)$;*

(2) If $N \geqslant 4$, the modular curve $\mathscr{Y}_1(N)$ is represented by an affine curve $Y_1(N)$;

[7] We also call the Deligne-Mumford stacks $\mathscr{Y}(N)$, $\mathscr{Y}_1(N)$, $\mathscr{Y}_1^{\text{bal}}(N)$ and $\mathscr{Y}_0(N)$ as modular "curves", even though they are not always representable. Since we use different fonts, this won't cause any ambiguity.

(3) If $N \geqslant 4$, the modular curve $\mathscr{Y}_1^{bal}(N)$ is represented by an affine curve $Y_1^{bal}(N)$. Moreover, the affine curves $Y(N) \otimes \mathbb{Z}[\frac{1}{N}]$, $Y_1(N) \otimes \mathbb{Z}[\frac{1}{N}]$ and $Y_1^{bal}(N) \otimes \mathbb{Z}[\frac{1}{N}]$ are smooth over $\mathbb{Z}[\frac{1}{N}]$.

Proof: By Theorem 2.6.6, these three moduli problems are all relatively representable, and finite, hence affine. The first part of the corollary follows from Theorem 3.1.5.

For the last part, e.g., for the affine curve $Y(N)$, it suffices to prove that $Y(N) \times_{\mathscr{M}_{1,1}} \mathsf{Spec}\,(\mathbf{R}_i)$ for $i = 2, 3$ are smooth, then as a quotient of free action by a finite group G_i, $Y(N)$ is also smooth. To see that $Y(N) \times_{\mathscr{M}_{1,1}} \mathsf{Spec}\,(\mathbf{R}_i)$ is smooth, notice that we have the finite étale morphism

$$Y(N) \times_{\mathscr{M}_{1,1}} \mathsf{Spec}\,(\mathbf{R}_i) \longrightarrow \mathsf{Spec}\,(\mathbf{R}_i),$$

and combine that $\mathsf{Spec}\,(\mathbf{R}_i)$ is a smooth affine curve, the assertion follows. □

Remark: As for the modular curve $\mathscr{Y}_0(N)$, it is never representable. Indeed, for an elliptic curve E/S, the $[-1]$ morphism preserves any $\Gamma_0(N)$-structure.

3.2 Regularity

As we proved in Proposition 3.1.3, any relatively representable moduli problem $\mathscr{P}$ is Deligne-Mumford, hence admits an étale atlas. If P is a property of schemes which is local for the étale topology (e.g., regularity, normality...), we say that the moduli stack $\mathscr{P}$ has the property P, if for some étale atlas $U \to \mathscr{P}$, U has the property P. So it makes sense to talk about the regularity of a moduli stack.

In this subsection, the main result is:

Theorem 3.2.1 (Regularity Theorem)**.** *Let $\mathscr{Y}$ be either of four modular curves (i.e., $\mathscr{Y}(N)$, $\mathscr{Y}_1(N)$, $\mathscr{Y}_1^{bal}(N)$ or $\mathscr{Y}_0(N)$). Then $\mathscr{Y}$ is relatively representable, finite flat of constant rank $(\geqslant 1)$ over $\mathscr{M}_{1,1}$, and regular of dimension two. Moreover,*

$$\mathscr{Y} \otimes \mathbb{Z}\Big[\frac{1}{N}\Big] \longrightarrow \mathscr{M}_{1,1} \otimes \mathbb{Z}\Big[\frac{1}{N}\Big]$$

is finite étale.

Due to our previous discussions, we already proved the Regularity Theorem over $\mathbb{Z}[\frac{1}{N}]$ (i.e., the last part). For the first part, we focus on the case where N is a power of some prime p (due to the principle of factorization). The main idea of the proof is Deligne's *homogeneity principle*, we present the axiomatic form of it.

Lemma 3.2.2. *Let $k = \bar{\mathbb{F}}_p$, and $W(k)$ its ring of Witt vectors. Then for any scheme X of finite type over $\mathbb{Z}$, we have the following bijective correspondences:*

$$\left\{\begin{array}{l} \textit{closed points } \bar{x} \textit{ of } X \otimes W(t) \\ \textit{with residue field } k \end{array}\right\} \longleftrightarrow X(k) \longleftrightarrow \left\{\begin{array}{l} \textit{pairs } (x_0, i)\textit{, where } x_0 \textit{ is closed} \\ \textit{point of } X \textit{ with residue char. } p, \\ \textit{and } i : \mathbb{F}_p(x_0) \hookrightarrow k \textit{ is the inclusion} \\ \textit{of the finite field into } k. \end{array}\right\}$$

Moreover, under these correspondences, we have

$$\mathscr{O}_{X\otimes W(k),\bar{x}} = \mathscr{O}^{sh}_{X,x_0},$$

where $\bar{x}$ is the closed point of $X\otimes W(k)$ that corresponding to the pair (x_0, i).

Proof: Without loss of generality, we assume $X = \text{Spec }(A)$ is affine, where the ring A is of finite type over $\mathbb{Z}$. To show the first bijective correspondence, from the diagram

$$\begin{tikzcd}
\text{Spec }(k) \arrow[drr, bend left, "x"] \arrow[dr, dotted, "\bar{x}"] \arrow[ddr, bend right] & & \\
& X\otimes W(k) \arrow[r] \arrow[d] & X \arrow[d] \\
& \text{Spec }\big(W(k)\big) \arrow[r] & \text{Spec }(\mathbb{Z})
\end{tikzcd}$$

we know that a k-rational point x of X uniquely corresponds to a k-rational point $\bar{x}$ of $X\otimes W(k)$, it remains to show that $\bar{x}$ is indeed a closed point. Look at the diagram of global sections:

$$\begin{tikzcd}
k & & \\
& A\otimes_{\mathbb{Z}} W(k) \arrow[ul, "\bar{x}"'] & A \arrow[l] \arrow[ull, bend right, "x"'] \\
& W(k) \arrow[u] \arrow[uul, bend left] & \mathbb{Z} \arrow[l] \arrow[u]
\end{tikzcd}$$

suppose the prime ideal of x is $I\subset A$, then the prime ideal of the point $\bar{x}$ is $A\otimes(p)+I\otimes W(k)$, which is indeed a maximal ideal of $A\otimes W(k)$, and clearly that we have the isomorphism

$$A\otimes W(k)/\big(A\otimes(p)+I\otimes W(k)\big) \simeq k.$$

Therefore $\bar{x}$ is a closed point of $X\otimes W(k)$ with residue field k. Conversely, given a closed point of $X\otimes W(k)$, it gives a k-rational point by composing $X\otimes W(k)\to X$.

The second bijective correspondence is obvious. The residue field $\mathbb{F}_p(x_0)$ being finite is because that A is of finite type over $\mathbb{Z}$.

For the last assertion, recall the fact that the ring of Witt vectors $W(k)$ is isomorphic to the strict henselization of $\mathscr{O}_{\mathbb{Z},(p)} = \mathbb{Z}_{(p)}$, therefore the result follows from the cartesian diagram:

$$\begin{tikzcd}
\text{Spec }\big(\mathscr{O}_{X\otimes W(k),\bar{x}}\big) \arrow[r] \arrow[d] & \text{Spec }\big(\mathscr{O}_{X,x_0}\big) \arrow[d] \\
\text{Spec }\big(\mathscr{O}_{W(k),(p)}\big) \arrow[r] & \text{Spec }\big(\mathscr{O}_{\mathbb{Z},(p)}\big).
\end{tikzcd}$$

□

Theorem 3.2.3 (Axiomatic Regularity Theorem)**.** *Fix a prime number p. Any moduli stack $\mathscr{P}$ over $\mathscr{M}_{1,1}$ which satisfies following axioms*

***R1**: $\mathscr{P}$ is relatively representable and finite over $\mathscr{M}_{1,1}$;*

***R2**: $\mathscr{P} \otimes \mathbb{Z}[\frac{1}{p}]$ is finite étale over $\mathscr{M}_{1,1} \otimes \mathbb{Z}[\frac{1}{p}]$;*

***R3**: For any two elliptic curves $E, E' : S \rightrightarrows \mathscr{M}_{1,1}$ over S which have isomorphic p-divisible groups, then*

$$\mathscr{P} \times_{\mathscr{M}_{1,1},E} S \simeq \mathscr{P} \times_{\mathscr{M}_{1,1},E'} S,$$

i.e., the level $\mathscr{P}$ structures only depend on the underlying p-divisible groups;

***R4**: Let E_0/k be a supersingular elliptic curve over an algebraically closed field k of characteristic p, and $\mathbf{E}/W(k)[\![T]\!]$ its universal formal deformation, then:*

- ***R4-1**: The k-scheme $\mathscr{P} \times_{\mathscr{M}_{1,1},E_0} k$ consists of one point;*
- ***R4-2**: The $W(k)[\![T]\!]$-scheme $\mathscr{P} \times_{\mathscr{M}_{1,1},\mathbf{E}} W(k)[\![T]\!]$ is the spectrum of a 2-dimensional regular local ring.*

is finite flat over $\mathscr{M}_{1,1}$ of constant rank $(\geqslant 1)$, and regular of dimension two.

Proof: Consider the étale atlas of $\mathscr{M}_{1,1}$:

$$\mathsf{Spec}\,(\mathbf{R}_2) \coprod \mathsf{Spec}\,(\mathbf{R}_3) \longrightarrow \mathscr{M}_{1,1},$$

and the induced étale atlas of $\mathscr{P}$:

$$\big(\mathsf{Spec}\,(\mathbf{R}_2) \coprod \mathsf{Spec}\,(\mathbf{R}_3)\big) \times_{\mathscr{M}_{1,1}} \mathscr{P} \longrightarrow \mathscr{P}.$$

Denote $S_i = \mathsf{Spec}\,(\mathbf{R}_i)$ and $S_i' = S_i \times_{\mathscr{M}_{1,1}} \mathscr{P}$ for $i = 2, 3$, we must show that the morphism of schemes

$$f_i : S_i' \longrightarrow S_i$$

is finite flat, and S_i' is regular of dimension 2. Since f_i is already finite by conditions, and S_i is an affine smooth curve, in particular it is regular of dimension 2, hence we only need to show the regularity of S_i'.

Let

$$U_i := \left\{ y \in S_i \,\middle|\, \forall x \text{ that } f_i(x) = y,\, \mathscr{O}_{S_i',x} \text{ is regular, and flat over } \mathscr{O}_{S_i,y} \right\} \subset S_i.$$

This is an open subset of S_i. Indeed, since S_i is of finite type over $\mathbb{Z}$, both regular and flat loci are open in S_i' (cf. [1, Tag 07R2] and [1, Tag 0398]), hence as the image of irregular and non-flat loci under a finite morphism, $S_i \backslash U_i$ is closed in S_i. We aim to show that $U_i = S_i$, and since S_i is of finite type over $\mathbb{Z}$, it suffices to show that U_i contains every closed point of S_i. By **R2**, U_i already contains $S_i \otimes \mathbb{Z}[\frac{1}{p}]$, hence it remains to show that U_i contains every closed point with residue field of characteristic p, i.e., U_i contains $S_i \otimes \mathbb{F}_p$.

There are two kinds of points on $S_i \otimes \mathbb{F}_p$, namely, the *ordinary points*, which correspond to ordinary elliptic curves (with level structures), and the *supersingular points*, which correspond to supersingular elliptic curves (with level structures). The supersingular locus is finite (cf. Silverman [10]). We shall prove that U_i satisfies the following *homogeneity properties*:

- **H1**: If U_i contains one supersingular point of $S_i \otimes \mathbb{F}_p$, then it contains all the supersingular points;
- **H2**: If U_i contains one ordinary point of $S_i \otimes \mathbb{F}_p$, then it contains all the ordinary points.

If the homogeneity properties hold, one only needs to verify **H1** for the case, since then by the openness of U_i, it must contain some ordinary points, hence verifies **H2** as well.

Recall that both regularity and flatness are preserved by passing to the completion and strict henselization (cf. [1, Tag 06LN] for regularity), so we have to prove:

> For any closed point $y_0 \in S_i$, and any closed point $x_0 \in S_i'$ that lying over y_0, the complete noetherian local ring $\widehat{\mathscr{O}}^{\mathrm{sh}}_{S_i',x_0}$ is regular, and flat over $\widehat{\mathscr{O}}^{\mathrm{sh}}_{S_i,y_0}$.

According to Lemma 3.2.2, this is equivalent to

> For any closed point $\bar{y} \in S_i \otimes W(k)$, and any closed point $\bar{x} \in S_i' \otimes W(k)$ that lying over $\bar{y}$, the complete noetherian local ring $\widehat{\mathscr{O}}_{S_i'\otimes W(k),\bar{x}}$ is regular, and flat over $\widehat{\mathscr{O}}_{S_i\otimes W(k),\bar{y}}$.

Let E_0/k be the elliptic curve that corresponding to the closed point $y_0 \in S_i$. Since S_i is étale over $\mathscr{M}_{1,1}$, we have an isomorphism of complete noetherian local rings

$$\widehat{\mathscr{O}}_{S_i\otimes W(k),\bar{y}} \simeq W(k)[\![T]\!],$$

and by the universal property, the universal formal deformation $\mathbf{E}/W(k)[\![T]\!]$ of E_0/k exactly corresponds to the pull-back of the universal family of $S_i \otimes W(k)$ along

$$\mathsf{Spec}\left(\widehat{\mathscr{O}}_{S_i\otimes W(k),\bar{y}}\right) \longrightarrow S_i \otimes W(k).$$

Hence we have the identification

$$\mathscr{P} \times_{\mathscr{M}_{1,1},\mathbf{E}} W(k)[\![T]\!] = \mathscr{P}_{\mathbf{E}/W(k)[\![T]\!]} = \left(S_i' \otimes W(k)\right) \times_{S_i\otimes W(k)} \mathsf{Spec}\left(\widehat{\mathscr{O}}_{S_i\otimes W(k),\bar{y}}\right),$$

where the right side is exactly the spectrum of the product of complete noetherian local rings of those $\bar{x}$ which lies over $\bar{y}$, i.e.,

$$\left(S_i' \otimes W(k)\right) \times_{S_i\otimes W(k)} \mathsf{Spec}\left(\widehat{\mathscr{O}}_{S_i\otimes W(k),\bar{y}}\right) \simeq \mathsf{Spec}\left(\prod_{\bar{x}} \widehat{\mathscr{O}}_{S_i'\otimes W(k),\bar{x}}\right).$$

By the axiom **R3** and Serre-Tate Theorem 8.6.3, the isomorphism class of $\mathscr{P}_{\mathbf{E}/W(k)[\![T]\!]}$ only depends on whether E_0/k is ordinary or supersingular, and the regularity and flatness of $\mathscr{P}_{\mathbf{E}/W(k)[\![T]\!]}$ would imply the same for any $\widehat{\mathscr{O}}_{S_i'\otimes W(k),\bar{x}}$ (over $\widehat{\mathscr{O}}_{S_i\otimes W(k),\bar{y}}$). This proves the homogeneity properties.

Finally, the fact that U_i contains at least one (in fact, any) supersingular point is already implied by the axiom **R4-2**. □

Thanks to the Axiomatic Regularity Theorem, in order to prove Theorem 3.2.1, it suffices to verify the four axioms **R1**-**R4** for the modular curves $\mathscr{Y}(N)$, $\mathscr{Y}_1(N)$, $\mathscr{Y}_1^{\mathrm{bal}}(N)$ and $\mathscr{Y}_0(N)$. However, the case for $\mathscr{Y}_0(N)$ is more complicated than others, we shall prove the first three cases and leave the last one to the next chapter.

The first three axioms are immediate. It remains to verify **R4-1** and **R4-2**.

Lemma 3.2.4. *Let $\mathscr{Y}$ be either of three modular curves $\mathscr{Y}(p^n)$, $\mathscr{Y}_1(p^n)$ or $\mathscr{Y}_1^{bal}(p^n)$. Let k be a field of characteristic p, and E_0/k is a supersingular elliptic curve. Then the k-scheme $\mathscr{Y} \times_{\mathscr{M}_{1,1},E_0} k$ consists of one point.*

Proof: The p^n-torsion subgroup scheme $E_0[p^n]$ of a supersingular elliptic curve E_0/k is supported at the zero section, i.e., it has 0 as the unique k-rational point. The k-scheme $\mathscr{Y}(p^n)\times_{\mathscr{M}_{1,1},E_0} k$ is the moduli scheme of Drinfeld basis of $E_0[p^n]$, which only consists of one point, i.e., the Drinfeld basis $(0,0)$. The k-scheme $\mathscr{Y}_1(p^n)\times_{\mathscr{M}_{1,1},E_0} k$ is the moduli scheme of points of exact order p^n in $E_0[p^n]$, since 0 indeed has exact order p^n, it consists of one point. For the k-scheme $\mathscr{Y}_1^{\mathrm{bal}}(p^n)\times_{\mathscr{M}_{1,1},E_0} k$, it is the moduli scheme of triples (K,P,P'), where K is a cyclic subgroup scheme of $E_0[p^n]$ with rank p^n, and P,P' are generators of $K, E_0[p^n]/K$ respectively. Indeed, K is unique, which is generated by 0, and K' is also supported at the zero section, the choice of a generator is therefore unique, i.e., the zero section. □

Lemma 3.2.5. *Let R be a unital commutative ring, and C/R is a smooth 1-dimensional commutative R-group scheme. Suppose the zero section $0\in C(R)$ has exact order p^n, then $p=0$ in R, and $p^n[0]=\mathit{ker}\,(F^n_{C/S})$ as subgroup schemes.*

Proof: Choose a formal parameter X for the formal group of C/R, and let

$$F(X,Y) \;=\; X+Y+\,...\,\in R[\![X,Y]\!]$$

be the formal group law. By the condition, the effective Cartier divisor $p^n[0]$ is a R-subgroup scheme of C, which is visibly defined by $X^{p^n}=0$. Hence, for any R-algebra B, and any $x,y\in B$ with $x^{p^n}=y^{p^n}=0$ in B, we always have

$$\big(F(x,y)\big)^{p^n} \;=\; 0 \quad \text{in } B.$$

It suffices to check the universal case, namely, in the case $B=R[\![X,Y]\!]/(X^{p^n},Y^{p^n})$. Then

$$\big(F(X,Y)\big)^{p^n} \;\in\; \big(X^{p^n},Y^{p^n}\big),$$

and comparing the terms of degree p^n, we have

$$(X+Y)^{p^n} \;=\; X^{p^n}+Y^{p^n},$$

i.e.,

$$\begin{pmatrix} p^n \\ i \end{pmatrix} \;=\; 0, \qquad \text{for } i=1,...,p^n-1.$$

Because

$$\mathsf{ord}_p\begin{pmatrix} p^n \\ p^{n-1} \end{pmatrix} \;=\; 1,$$

hence $\binom{p^n}{1}=p^n=0$ and $\binom{p^n}{p^{n-1}}=0$ imply that $p=0$ in R.

Since $p^n[0]$ is defined by the equation $X^{p^n}=0$ in the formal group, which is also visibly $\mathsf{ker}(F^n_{C/S})$, hence they are equal. □

Lemma 3.2.6. *Let $\mathscr{Y}$ be either of three modular curves $\mathscr{Y}(p^n)$, $\mathscr{Y}_1(p^n)$ or $\mathscr{Y}_1^{bal}(p^n)$. Let E_0/k be a supersingular elliptic curve over an algebraically closed field k of characteristic p, and $\mathbf{E}/W(k)[\![T]\!]$ is its universal formal deformation. Then the scheme $\mathscr{Y}\times_{\mathscr{M}_{1,1},\mathbf{E}} W(k)[\![T]\!]$ is the spectrum of a regular local ring of dimension 2, and it is flat over $W(k)[\![T]\!]$.*

Proof: The scheme $\mathscr{Y} \times_{\mathscr{M}_{1,1},\mathbf{E}} W(k)[\![T]\!]$ is finite over $W(k)[\![T]\!]$, hence affine, say

$$\mathscr{Y} \times_{\mathscr{M}_{1,1},\mathbf{E}} W(k)[\![T]\!] \;=\; \mathsf{Spec}\,(A).$$

By Lemma 3.2.4, the special fiber has only one point, hence A is a local ring. Let $\mathfrak{m}_A$ be the maximal ideal of A. We need to prove that A is a regular of dimension 2, and then since $W(k)[\![T]\!]$ has the same dimension, the flatness of A over $W(k)[\![T]\!]$ automatically follows.

Observe that, since the morphism

$$\begin{tikzcd} \mathsf{Spec}\,(A) \arrow[d] \\ \mathsf{Spec}\,\big(W(k)[\![T]\!]\big) \end{tikzcd}$$

is finite, and the image contains $\mathsf{Spec}\,\big(W(k)[\![T]\!]\otimes\mathbb{Z}[\frac{1}{p}]\big)$, it must be surjective. Hence the dimension of A is at least 2. We will show that $\mathfrak{m}_A$ is generated by two elements, and then

$$2 \leqslant \dim A \leqslant \dim_k \mathfrak{m}_A/\mathfrak{m}_A^2 \leqslant 2$$

indicates the result.

Notice that the elliptic curve $\mathbf{E}_A = \mathbf{E}\otimes A$ carries a universal level structure α_{univ} with respect to the moduli problem $\mathscr{Y}$, i.e., the level structure corresponds to the identity morphism [8]

$$\mathsf{Spec}\,(A) \xrightarrow{\mathsf{id}_A} \mathsf{Spec}\,(A).$$

Consider the following moduli problem:

$$\begin{array}{ccc} \mathfrak{Art}(W(k);k) & \longrightarrow & \mathfrak{Set} \\ R & \longmapsto & \left\{ \begin{array}{l} \text{all triples } (E/R,\alpha,i)\text{, where } E/R \text{ is} \\ \text{an elliptic curve over } R,\ \alpha \text{ is a level} \\ \text{structure on } E/R\text{, and } i \text{ is an isom.} \\ \quad i:\ E\otimes_R k \xrightarrow{\sim} E_0 \\ \text{which pulls back the unique level} \\ \text{structure on } E_0/k \text{ to } \alpha\otimes k. \end{array} \right\} \end{array}$$

where $\mathfrak{Art}(W(k);k)$ is the category of artinian local $W(k)$-algebras with residue field k. This is the moduli problem of "deformation with level structures", it is straightforward that $(\mathbf{E}_A/A, \alpha_{\text{univ}})$ pro-represents the above moduli functor.

Now we are going to prove the lemma, dividing into three cases. From now on, we choose a formal parameter X for the formal group of $\mathbf{E}_A/A$.

$\boxed{\textbf{Case I: } \mathscr{Y}(N)}$ Let (P,Q) be the universal Drinfeld basis of $\mathbf{E}_A[p^n]/A$, which is just the universal level structure α_{univ} in our previous discussion. Since A is a complete local ring, and E_0/k has a unique Drinfeld basis, the points P,Q both lie in the formal group of $\mathbf{E}_A/A$. We claim that $X(P), X(Q) \in \mathfrak{m}_A$ generate $\mathfrak{m}_A$.

[8] Recall that the scheme $\mathsf{Spec}\,(A) = \mathscr{Y}\times_{\mathscr{M}_{1,1},\mathbf{E}} W(k)[\![T]\!]$ is the moduli scheme of level structures (w.r.p. $\mathscr{Y}$) on the elliptic curve $\mathbf{E}/W(k)[\![T]\!]$.

Let R be any artinian local $W(k)$-algebra with residue field k, and suppose $\phi : A \to R$ is a homomorphism who kills $X(P)$ and $X(Q)$. By the pro-representability of $(\mathbf{E}_A/A, (P, Q))$, the homomorphism ϕ corresponds to a triple $(E/R, (0,0), i)$, where $(0,0)$ is a Drinfeld basis of $E[p^n]/R$. And we have the equality of effective Cartier divisor

$$p^{2n}[0] = E[p^n],$$

in particular, the zero section 0 has exact order p^{2n}. Applying Lemma 3.2.5, we have $p = 0$ in R, which means that R is a $W(k)/(p) \simeq k$-algebra. Moreover we have

$$\ker (p^n) = p^{2n}[0] = \ker (F^{2n}_{E/R}).$$

In the following commutative diagram,

$$\begin{tikzcd}
0 \arrow[r] & \ker (p^n) \arrow[r] \arrow[d, "\mathrm{id}"] & E \arrow[r, "p^n"] \arrow[d, "\mathrm{id}_E"] & E \arrow[r] \arrow[d, dotted, "\wr"] & 0 \\
0 \arrow[r] & \ker (F^{2n}_{C/S}) \arrow[r] & E \arrow[r, "F^{2n}_{E/R}"] & E^{(p^{2n})} \arrow[r] & 0
\end{tikzcd}$$

it naturally induces an isomorphism

$$E \simeq E^{(p^{2n})},$$

and consequently

$$E \simeq E^{(p^{2n})} \simeq E^{(p^{4n})} \simeq \ldots \simeq E^{(p^{2kn})} \simeq \ldots$$

As k becomes sufficiently large, the elliptic curve $E^{(p^{2kn})}$ turns to "constant", in the sense that it is the pull back of E_0/k along the trivial homomorphism of k-alegbras

$$k \longrightarrow R,$$

because the maximal ideal of R is nilpotent. This means that any homomorphism $\phi : A \to R$ which kills $X(P), X(Q)$ is corresponding to the trivial triple $(E_0 \otimes_k R/R, \alpha \otimes R, i)$, in other words, $X(P), X(Q)$ generate $\mathfrak{m}_A$.

$\boxed{\textbf{Case II: } \mathscr{Y}_1(N)}$ Let $P \in \mathbf{E}_A(A)$ be the universal point of exact order p^n. As before, P lies in the formal group of $\mathbf{E}_A/A$. We claim that $\mathfrak{m}_A$ is generated by $X(P)$ and T. [9]

Let $\phi : A \to R$ be a homomorphism which kills $X(P)$ and T. In this case, the homomorphism ϕ corresponds to a triple $(E/R, 0, i)$, where 0 has exact order p^n in E/R. By Lemma 3.2.5, $p = 0$ in R, and hence R is a k-algebra. Consider the composition

$$\begin{tikzcd}
W(k)[\![T]\!] \arrow[r] \arrow[dr, "\widetilde{\phi}"'] & A \arrow[d, "\phi"] \\
& R
\end{tikzcd}$$

where the top homomorphism is local, which is the structure homomorphism of A as a finite $W(k)[\![T]\!]$-algebra. The homomorphism $\widetilde{\phi}$ kills both p and T, and because the image of (p, T) in A generates $\mathfrak{m}_A$, hence ϕ kills $\mathfrak{m}_A$. This shows our claim.

[9] The element T indeed lies in $\mathfrak{m}_A$, since it belongs to the maximal ideal of $W(k)[\![T]\!]$, and the homomorphism $W(k)[\![T]\!] \to A$ is local.

$\boxed{\textbf{Case III: } \mathscr{Y}_1^{\mathbf{bal}(N)}}$ Let $(\mathbf{K}, P, P')$ be the universal $\Gamma_1^{\mathrm{bal}}(p^n)$-structure on $\mathbf{E}_A/A$, where $\mathbf{K}$ is a cyclic subgroup scheme of $\mathbf{E}_A/A$ with rank p^n, and $P \in \mathbf{K}(A)$, $P' \in \mathbf{K}'(A) = \big(\mathbf{E}_A[p^n]/\mathbf{K}\big)(A)$ are generators. Choose a formal parameter X' for the formal group of the elliptic curve $\mathbf{E}'_A = \mathbf{E}_A/\mathbf{K}$. As before, the points P, P' lie in the formal groups of $\mathbf{E}_A, \mathbf{E}'_A$ respectively. We claim that A is generated by $X(P)$ and $X'(P')$.

Let $\phi : A \to R$ be a homomorphism which kills $X(P)$ and $X'(P')$. Like in the Case I, we aim to show that the triple corresponding to ϕ is trivial. The homomorphism ϕ corresponds to a triple $(E/R, (K, 0, 0'), i)$, or equivalently ($K = \mathsf{ker}(\phi)$)

$$\begin{tikzcd} E \arrow[r, shift left, "\phi"] & E' \arrow[l, shift left, "\phi^t"] \end{tikzcd},$$

where the zero sections 0, 0' generate the cyclic subgroup schemes $\mathsf{ker}(\phi)$, $\mathsf{ker}(\phi^t)$ respectively. The zero section 0 has exact order p^n in E/R, which implies $p = 0$ in R, hence R is a k-algebra. Moreover, we have

$$\mathsf{ker}\,(\phi) \;=\; \mathsf{ker}\,(F^n_{E/R}).$$

Similarly, the zero section 0' has exact order p^n in E'/R, and it implies that

$$\mathsf{ker}\,(\phi^t) \;=\; \mathsf{ker}\,(F^n_{E/R}).$$

Therefore

$$\mathsf{ker}\,(p^n) \;=\; \mathsf{ker}\,(F^{2n}_{E/R}),$$

and we only need to follow the arguments that we used in Case I. □

Proof of Theorem 3.2.1: Theorem 3.2.3 + Lemma 3.2.4 + Lemma 3.2.6. □

3.3 More properties of modular curves

In this section, we study more properties and relations among the three modular curves $\mathscr{Y}(N)$, $\mathscr{Y}_1(N)$ and $\mathscr{Y}_1^{\mathrm{bal}}(N)$.

Theorem 3.3.1. *Let E/S be an elliptic curve over an arbitrary scheme S, and let (P, Q) be a Drinfeld basis of $E[N]/S$ ($N > 1$). Then*

(1) The point P has exact order N;

(2) Let K be the cyclic S-subgroup scheme of E/S generated by P, and let E' be the quotient elliptic curve of E by K. Then the image Q' of Q has exact order N, and it generates $K' = E[N]/K$.

Proof: We claim that it suffices to assume the base S is affine and flat over $\mathbb{Z}$. Since having exact order is a fppf-local property, we may assume that some prime ℓ is invertible on S, and E/S equips with a naïve full level ℓ structure, i.e., an isomorphism of S-group schemes

$$\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \;\simeq\; E[\ell].$$

By passing to the universal case, we may assume that

$$S = \mathscr{Y}(N) \times_{\mathscr{M}_{1,1}} \left(\mathscr{Y}(\ell) \otimes \mathbb{Z}\left[\frac{1}{\ell}\right]\right),$$

and E is the corresponding universal elliptic curve, equipped with a universal full level ℓ structure and a universal Drinfeld basis $(P_{\text{univ}}, Q_{\text{univ}})$. Indeed, when $\ell \geqslant 3$, the moduli stack $\mathscr{Y}(\ell) \otimes \mathbb{Z}[\frac{1}{\ell}]$ is representable, and in the case $\ell = 2$, we may replace it by the Legendre moduli scheme $\mathsf{Spec}\ (\mathbf{R}_2)$. In any case, S is affine and flat over $\mathbb{Z}$, thus our claim follows. We denote $S = \mathsf{Spec}\ (A)$.

To prove the theorem, firstly observe that the theorem is clearly true over $\mathbb{Z}[\frac{1}{N}]$, by Corollary 2.6.8.

(1) By Proposition 2.2.4, the moduli of $\Gamma_1(N)$-structures on E/A is represented by a closed subscheme of the affine scheme

$$\mathsf{Hom}_{S\text{-}\mathfrak{Grp}}(\mathbb{Z}/N\mathbb{Z},\ E) \ = \ E[N],$$

let us assume that it is defined by functions $f_1, ..., f_r \in A$. We already know that for any $1 \leqslant i \leqslant r$

$$f_i(P) = 0 \ \text{ in } A\left[\frac{1}{N}\right]$$

By flatness of A, the homomorphism $A \to A[\frac{1}{N}]$ is injective. Therefore $f_i(P) = 0$ in A for any i.

(2) By Proposition 2.2.6, $\mathbb{Z}/N\mathbb{Z}$-$\mathsf{Gen}(K'/A)$ is represented by a closed subscheme of the affine scheme

$$\mathsf{Hom}_{S\text{-}\mathfrak{Grp}}(\mathbb{Z}/N\mathbb{Z},\ K') \ = \ K'.$$

Similarly, by flatness of K' over $\mathbb{Z}$, to check that P is a generator of K'/S, it suffices to check it on $\mathbb{Z}[\frac{1}{N}]$, which is already clear. □

Remark: By the theorem, fppf-locally, it is always possible to extend a $\Gamma_1(N)$-structure to a $\Gamma_1^{\text{bal}}(N)$-structure, by choosing a generator of K'/S. Moreover, we can also extend a $\Gamma_1^{\text{bal}}(N)$-structure to a $\Gamma(N)$-structure. Suppose Q' is a generator of K', and Q lies over Q' under the quotient by K. Applying Proposition 2.4.2 to the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/N\mathbb{Z} \arrow[r] \arrow[d, "P"] & \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z} \arrow[r] \arrow[d, "(P,Q)"] & \mathbb{Z}/N\mathbb{Z} \arrow[r] \arrow[d, "Q'"] & 0 \\
0 \arrow[r] & K(S) \arrow[r] & E[N](S) \arrow[r] & K'(S) &
\end{tikzcd}$$

thus (P,Q) is a Drinfeld basis extended by the $\Gamma_1^{\text{bal}}(N)$-structure.

Corollary 3.3.2. *There are natural morphisms of moduli stacks*

$$\begin{array}{ccccccc}
\mathscr{Y}(N) & \longrightarrow & \mathscr{Y}_1^{bal}(N) & \longrightarrow & \mathscr{Y}_1(N) & \longrightarrow & \mathscr{M}_{1,1} \\
(P,Q) & \longmapsto & (P,Q') & \longmapsto & P & &
\end{array}$$

which are all finite flat, of degree N, $\varphi(N)$ and $N^2 \cdot \prod_{d|N}(1-\frac{1}{d^2})$ respectively.

Proof: By the Regularity Theorem 3.2.1, all the moduli stacks are finite flat over $\mathscr{M}_{1,1}$. Moreover, since they are all regular with the same dimension, the morphisms are automatically flat. Finally, to count the degree, one only needs to restrict on $\mathbb{Z}[\frac{1}{N}]$. □

Theorem 3.3.3. *Let E/S be an elliptic curve over an arbitrary scheme S, and let (P,Q) be a pair of points in $E[N](S)$ $(N>1)$. Suppose d is any divisor of N, then:*

1. *(1) The pair (P,Q) is a Drinfeld N-basis if and only if (dP,dQ) is a Drinfeld N/d-basis;*
2. *(2) The point P has exact order N if and only if dP has exact order N/d.*

Proof: By the principle of factorization, we may assume $N=p^n$ and $d=p$. And since (2) can be deduced from (1) by Theorem 3.3.1, we shall concentrate on (1).

The "only if" part: Apply the same strategy as we did in the proof of Theorem 3.3.1, we reduce to the case that S is affine and flat over $\mathbb{Z}$. The moduli of $\Gamma(p^{n-1})$-structure on E/S is represented by a closed subscheme of the affine scheme $E[p^{n-1}]\times E[p^{n-1}]$, and the assertion is clear over $\mathbb{Z}[\frac{1}{p}]$. Hence by flatness, the conclusion extends to $\mathbb{Z}$.

The "if" part: As before, we assume that the base S is affine and flat over $\mathbb{Z}$. Observe that the fiber product $\mathscr{S}_{E/S}$

$$\begin{tikzcd}
\mathscr{S}_{E/S} \arrow[r, hook] \arrow[d] & E[p^n]\times E[p^n] \arrow[d, "{([p],[p])}"] \\
\mathscr{Y}(p^{n-1})\times_{\mathscr{M}_{1,1},E} S \arrow[r, hook] & E[p^{n-1}]\times E[p^{n-1}]
\end{tikzcd}$$

represents the following moduli problem:

$$\begin{array}{ccc}
\mathfrak{Sch}_{/S} & \longrightarrow & \mathfrak{Set} \\
T & \longmapsto & \left\{ \begin{array}{l} \text{all pairs } (P,Q) \text{ in } E[p^n](S) \text{ such that} \\ (pP,pQ) \text{ is a Drinfeld } p^{n-1}\text{-basis} \end{array} \right\}
\end{array}$$

The scheme $\mathscr{S}_{E/S}$ is the closed subscheme of the affine scheme $E[p^n]\times E[p^n]$ which is flat over $\mathbb{Z}$. Since the assertion is clear over $\mathbb{Z}[\frac{1}{p}]$, by flatness, it extends to $\mathbb{Z}$. □

Corollary 3.3.4. *Let $N>1$ be an integer and d a divisor of N. Then there is a commutative diagram of modular curves*

$$\begin{tikzcd}
\mathscr{Y}(N) \arrow[r, "d"] \arrow[d] & \mathscr{Y}(N/d) \arrow[d] \\
\mathscr{Y}_1(N) \arrow[r, "d"] & \mathscr{Y}_1(N/d),
\end{tikzcd}$$

where the vertical morphisms are from Corollary 3.3.2, and the horizontal morphisms are finite flat.

Proof: The horizontal morphisms are just by sending a Drinfeld N-basis (P,Q) (resp. a point P of exact order N) to the Drinfeld N/d-basis (dP,dQ) (resp. a point dP of exact order N/d). Let U be an étale atlas of $\mathscr{M}_{1,1}$, and E/U the elliptic curve inherits from the morphism $U\to\mathscr{M}_{1,1}$. Consider the cartesian diagrams:

$$\begin{tikzcd}
\mathscr{Y}(N)\times_{\mathscr{M}_{1,1}} U \arrow[r, hook] \arrow[d] & E[N]\times E[N] \arrow[d, "{([d],[d])}"] & \mathscr{Y}_1(N)\times_{\mathscr{M}_{1,1}} U \arrow[r, hook] \arrow[d] & E[N] \arrow[d, "{[d]}"] \\
\mathscr{Y}(N/d)\times_{\mathscr{M}_{1,1}} U \arrow[r, hook] & E[N/d]\times E[N/d] & \mathscr{Y}_1(N/d)\times_{\mathscr{M}_{1,1}} U \arrow[r, hook] & E[N/d]
\end{tikzcd}$$

it is known that the morphisms $[d]$ and $([d],[d])$ are finite flat, hence so are both the left side morphisms. This implies that the horizontal morphisms in the corollary are finite flat. The commutativity of the diagram is obvious. □

Theorem 3.3.5. *Let E/S be an elliptic curve over an arbitrary scheme S, and $N \geqslant 1$ is an integer.*

(1) Let (P,Q) be a Drinfeld N-basis of E/S, then $e_N(P,Q)$ is a primitive N-th root of unity;

(2) Let (ϕ, P, P') be a $\Gamma_1^{bal}(N)$-structure[10] *on E/S, then $< P, P' >_\phi$ is a primitive N-th root of unity.*

Proof: Use the intrinsic description of $\Gamma_1^{\mathrm{bal}}(N)$-structures, and the fact that we can complete a $\Gamma_1^{\mathrm{bal}}(N)$-structure to a $\Gamma(N)$-structure, it suffices to prove (1).

The assertion is obviously true over $\mathbb{Z}[\frac{1}{N}]$. Apply the same reduction, we may assume that the base $S = \mathrm{Spec}\,(A)$ is affine and flat over $\mathbb{Z}$. Let Φ_N be the cyclotomic polynomial. Since we already know that $\Phi_N(e_N(P,Q)) = 0$ in $A[\frac{1}{N}]$, by flatness of A, it is also zero in A, i.e., $e_N(P,Q)$ is primitive. □

Definition 3.3.6. *The primitive N-th root of unity $e_N(P,Q)$ is called the* ***determinant*** *of the Drinfeld basis (P,Q).*

Corollary 3.3.7. *The moduli stacks $\mathscr{Y}(N)$ and $\mathscr{Y}_1^{bal}(N)$ are naturally defined over $\mathbb{Z}[\zeta_N]$, in other words, their structure morphisms naturally factor through $\mathscr{M}_{1,1} \otimes \mathbb{Z}[\zeta_N]$:*

$$\begin{tikzcd}
\mathscr{Y}(N) \arrow[r] \arrow[dr] & \mathscr{M}_{1,1} & \mathscr{Y}_1^{bal}(N) \arrow[l] \arrow[dl] \\
 & \mathscr{M}_{1,1} \otimes \mathbb{Z}[\zeta_N] \arrow[u] &
\end{tikzcd}$$

Proof: It is straightforward, since by Theorem 3.3.5, in these cases, the primitive root ζ_N lies in the base S of an elliptic curve E/S with a $\Gamma(N)$- or a Γ_1^{bal}-structure. □

[10] Here ϕ is a N-isogeny $E \to E'$, and P, P' are generators of $\ker(\phi)$ and $\ker(\phi^t)$ respectively.

4

Theory of Cyclic Group Schemes: Revisited

In this chapter, we will study cyclic group schemes in details. In previous chapter, we have proved the Regularity Theorem 3.2.1 except for the modular curve $\mathscr{Y}_0(N)$, which we shall complete the case in current chapter.

4.1 The scheme of generators

Recall that by Proposition 2.2.6, the functor $\mathbb{Z}/N\mathbb{Z}$-Gen(G/S) of a finite flat commutative cyclic S-group scheme of rank N is represented by a closed subscheme of $\mathsf{Hom}_{S\text{-}\mathfrak{Grp}}(\mathbb{Z}/N\mathbb{Z},\ G) = G$, which locally on S is defined by finitely many equations. From now on, we call it the *scheme of generators* of G, and denote by $G^\times$. We know that the S-scheme $G^\times$ is finite and finitely presented over S, and its formation commutes with any base change, that is to say, for any base change $S' \to S$, we have

$$(G \times_S S')^\times \ = \ G^\times \times_S S'.$$

In this section, we will give a concrete characterization of $G^\times$. Remind that the generators of the finite abelian group $\mathbb{Z}/N\mathbb{Z}$ are exactly those numbers $1 \leqslant d \leqslant N$ such that $(d, N) = 1$. In the case that G is étale over S, the situation is obviously similar. In the étale case, let P be a (fppf-local) generator of G, then the scheme of generators is

$$G^\times \ = \sum_{(d,N)=1,\ d \bmod N} [dP],$$

in particular, it is locally free of rank $\varphi(N)$. In general case, this is still true, but not so obvious.

Theorem 4.1.1. *Let E/S be an elliptic curve over an arbitrary scheme S, and $G \subset E[N]$ $(N \geqslant 1)$ is a cyclic S-subgroup scheme of rank N over S which is generated by $P \in G(S)$. Then*

$$G^\times \ = \ D := \sum_{(d,N)=1,\ d\ mod\ N} [dP],$$

in particular, $G^\times$ is finite locally free of rank $\varphi(N)$ over S.

Proof: As we have seen, the situation is obvious if N is invertible on S. Firstly, we show that the effective Cartier divisor D lies inside $G^\times$. By passing to the universal case, we may assume that the base S is affine and flat over $\mathbb{Z}$. Consider the pull-back of G along the structure morphism of D:

$$\begin{tikzcd}
G \arrow[d] & G_G \arrow[l] \arrow[d, shift right] & G_D \arrow[l] \arrow[d, shift right] \\
S & G \arrow[l] \arrow[u, bend right, "\Delta_G"'] & D \arrow[l, hook'] \arrow[u, bend right, "\sigma"']
\end{tikzcd}$$

where Δ_G is the diagonal morphism of G, which is the *tautological section* of G_G/G, and σ is the pull-back of Δ_G to G_D. We claim that the relation $D \subset G^\times$ is equivalent to that the D-valued point σ generates the cyclic D-group scheme G_D. Indeed, the fact that section σ generates G_D means that

$$\sigma \in (G_D)^\times(D) = (G^\times \times_S D)(D),$$

which by the definition of σ, it means exactly that the image of $D \hookrightarrow G$ lies in $G^\times$.

Since the base S is affine and flat over $\mathbb{Z}$, the finite group scheme G/S is affine, say $G = \mathsf{Spec}\,(B)$. Let $\{f_i\}$ be the defining equations of the closed subscheme $G^\times$ in G, since we already know that

$$f_i(\sigma) = 0 \quad \text{in } \Gamma(D, \mathscr{O}_D) \otimes \mathbb{Z}\Big[\frac{1}{N}\Big],$$

by flatness, we have

$$f_i(\sigma) = 0 \quad \text{in } \Gamma(D, \mathscr{O}_D),$$

which shows that $D \subset G^\times$.

Now let us consider the following two moduli stacks over $\mathscr{M}_{1,1}$:

- $\mathscr{P}_1$: The objects are quadruples $(E/S, G/S, P, Q)$, where E/S is an elliptic curve over a scheme S, $G \subset E[N]$ is a cyclic S-subgroup scheme of rank N, $P \in G(S)$ is a generator of G/S, and $Q \in D(S)$. Morphisms are obvious cartesian diagrams, such that they are compatible with the quadruples.

- $\mathscr{P}_2$: The objects are quadruples $(E/S, G/S, P, Q)$, where E/S is an elliptic curve over a scheme S, $G \subset E[N]$ is a cyclic S-subgroup scheme of rank N, and $P, Q \in G(S)$ are generators of G/S. Morphisms are obvious cartesian diagrams, such that they are compatible with the quadruples.

As we already proved that $D \subset G^\times$, there is a natural morphism

$$\Phi : \mathscr{P}_1 \longrightarrow \mathscr{P}_2,$$

we need to prove that it is an isomorphism. In order to prove it, we apply a similar strategy as in the Axiomatic Regularity Theorem. By the principle of factorization, we may assume that N is a prime power p^n.

Theorem 4.1.2 (Axiomatic Isomorphism Theorem)**.** *Fix a prime number p. Let*

$$\Phi : \mathscr{P}_1 \longrightarrow \mathscr{P}_2$$

be a morphism of moduli stacks of elliptic curves. Suppose that Φ *satisfies the following axioms:*

I1 *$\mathscr{P}_1$, $\mathscr{P}_2$ satisfies **R1**, **R3** and **R4-1** (cf. Theorem 3.2.3);*

I2 *$\Phi \otimes \mathbb{Z}[\frac{1}{p}]$ is an isomorphism;*

I3 *Let E_0/k be a supersingular elliptic curve over an algebraically closed field k of characteristic p, and $\mathbf{E}/W(k)[\![T]\!]$ its universal formal deformation, then the morphism*

$$\Phi \times_{\mathbf{E}} W(k)[\![T]\!] : \mathscr{M}_{\mathscr{P}_1} \times_{\mathscr{M}_{1,1},\mathbf{E}} W(k)[\![T]\!] \longrightarrow \mathscr{M}_{\mathscr{P}_2} \times_{\mathscr{M}_{1,1},\mathbf{E}} W(k)[\![T]\!]$$

is an isomorphism.

Then Φ is an isomorphism.

Proof: The argument is essentially the same as in the proof of the Axiomatic Regularity Theorem 3.2.3, except for that the open subset $U_i \subset S_i$ now stands for the locus of the morphism $\Phi \times S_i$ being isomorphic, which is indeed open. □

It remains to verify these axioms for the morphism Φ. Observe that we have natural morphisms from $\mathscr{P}_i$ to $\mathscr{Y}_1(p^n)$, which are given by forgetting the point Q:

$$\begin{aligned} \mathscr{P}_i &\longrightarrow \mathscr{Y}_1(p^n) \\ (E/S, G/S, P, Q) &\longmapsto (E/S, G/S, P), \end{aligned}$$

and these morphisms are both representable and finite, concretely,

$$\begin{aligned} \mathscr{P}_1 \times_{\mathscr{Y}_1(N),E} S &= D \\ \mathscr{P}_2 \times_{\mathscr{Y}_1(N),E} S &= G^{\times} \end{aligned}$$

Therefore the compositions

$$\mathscr{P}_i \longrightarrow \mathscr{Y}_1(p^n) \longrightarrow \mathscr{M}_{1,1}$$

are also representable, and finite. This verifies the axiom **R1**. The axioms **R3** and **R4-1** are obvious.

Let A_i be the affine coordinate rings of $\mathscr{P}_i \times_{\mathscr{M}_{1,1},\mathbf{E}} W(k)[\![T]\!]$ respectively, and let A be the affine coordinate ring of $\mathscr{Y}_1(p^n) \times_{\mathscr{M}_{1,1},\mathbf{E}} W(k)[\![T]\!]$. We transform the diagram of morphisms of affine schemes into the diagram of homomorphisms of local rings:

$$\begin{tikzcd} A_1 & & A_2 \arrow[ll, "\Phi^*"'] \\ & A \arrow[ul] \arrow[ur] & \\ & W(k)[\![T]\!] \arrow[u] & \end{tikzcd}$$

we need to show that Φ^* is an isomorphism. In order to do so, we give concrete characterizations of these local rings. Choose a formal parameter X of the formal group $\widehat{\mathbf{E}}$ of $\mathbf{E}/W(k)[\![T]\!]$.

- Recall that A is regular of dimension 2, where T and the coordinate of P are parameters (cf. Lemma 3.2.6 Case II). The coordinate of P should satisfy the following condition: the closed subscheme defined by

$$\prod_{d=1}^{p^n} \big(X - [d](P)\big) = 0$$

is a subgroup scheme. Let $\mathfrak{a}$ be the ideal which expresses this condition. Then

$$A = W(k)[\![T,P]\!]/\mathfrak{a}.$$

- $A_1 = A[\![Q]\!]/\mathfrak{a}_1$, where $\mathfrak{a}_1$ is the principal ideal generated by

$$\prod_{(d,N)=1,\ d \bmod N} \big(Q - [d](P)\big).$$

- $A_2 = A[\![Q]\!]/\mathfrak{a}_2$, where $\mathfrak{a}_2$ is the ideal generated by the coefficients of the polynomial:

$$\prod_{d=1}^{p^n} \big(X - [d](Q)\big) \ - \ \prod_{d=1}^{p^n} \big(X - [d](P)\big) \ = \ 0.$$

By the fact that $D \subset G^\times$, we have $\mathfrak{a}_1 \supset \mathfrak{a}_2$, hence the homomorphism Φ^* is surjective. Therefore we have the short exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & \ker(\Phi^*) \arrow[r] & A_2 \arrow[r, "\Phi^*"] & A_1 \arrow[r] & 0, \end{tikzcd}$$

and we want to prove that $\ker(\Phi^*) = 0$. As a finitely generated $A[\![Q]\!]$-module, it suffices to show that $\ker(\Phi^*)/(Q) = 0$, by Nakayama's Lemma.

Consider the endomorphism of multiplying Q on the A-algebra A_1. We claim that it is injective. Since A is regular, therefore integral, we only need to show that the determinant of multiplying Q is not zero. The calculation is straightforward:

$$\det(Q) \ = \ \prod_{(d,N)=1,\ d \bmod N} [d](P),$$

it is indeed nonzero.

By the Snake Lemma, from the diagram

$$\begin{tikzcd} 0 \arrow[r] & \ker(\Phi^*) \arrow[r] \arrow[d, "\times Q"] & A_2 \arrow[r] \arrow[d, "\times Q"] & A_1 \arrow[r] \arrow[d, "\times Q"] & 0 \\ 0 \arrow[r] & \ker(\Phi^*) \arrow[r] & A_2 \arrow[r] & A_1 \arrow[r] & 0, \end{tikzcd}$$

we obtain a short exact sequence:

$$\begin{tikzcd} \ker\{Q : A_1 \to A_1\} = 0 \arrow[r] & \ker(\Phi^*)/(Q) \arrow[r] & A_2/(Q) \arrow[r, "\Phi^*/(Q)"] & A_1/(Q) \arrow[r] & 0. \end{tikzcd}$$

Therefore it remains to show that the homomorphism $\Phi^*/(Q)$ is an isomorphism.

It is clear that

- $A_1/(Q) = A/\mathfrak{a}_1'$, where $\mathfrak{a}_1'$ is the principal ideal generated by

$$\prod_{(d,N)=1,\ d \bmod N} [d](P).$$

- $A_2\big/(Q) = A\big/\mathfrak{a}_2'$, where $\mathfrak{a}_2'$ is the ideal generated by coefficients of the polynomial:

$$X^{p^n} - \prod_{d=1}^{p^n} \big(X - [d](P)\big) = 0.$$

and $\mathfrak{a}_1' \supset \mathfrak{a}_2'$, we need to show the inverse, i.e., $\mathfrak{a}_1' \subset \mathfrak{a}_2'$.

The coefficient of the degree $p^n - \varphi(p^n)$ term in the polynomial $X^{p^n} - \prod_{d=1}^{p^n} \big(X - [d](P)\big)$ is

$$\sum_{\{d_1,\dots,d_{\varphi(p^n)}\} \subset \{1,\dots,p^n\}} \left(\prod_{i=1}^{\varphi(p^n)} [d_i](P) \right). \tag{†}$$

Since we know that

$$[d](X) = dX + \text{higher terms},$$

in particular, when $(d,p) = 1$,

$$[d](X) = \text{unit} \cdot X,$$

and when $p|d$,

$$[d](X) \in \mathfrak{m}_A \cdot X.$$

Therefore the expression (†) is equal to

$$\text{unit} \cdot P^{\varphi(p^n)} = \text{unit} \cdot \prod_{(d,N)=1,\ d \bmod N} [d](P),$$

hence $\mathfrak{a}_1' \subset \mathfrak{a}_2'$. This completes our proof for Theorem 4.1.1. □

4.2 Regularity of $\mathscr{Y}_0(N)$

In this section, we will complete the proof of Regularity Theorem 3.2.1 for the case of $\mathscr{Y}_0(N)$.

We introduce an auxiliary moduli problem **Isog**(N), whose objects are pairs $(E/S, G)$, where E/S is an elliptic curve over S, and $G \subset E[N]$ is a finite flat commutative S-subgroup scheme of rank N.

Lemma 4.2.1. *The moduli problem* **Isog**(N) *is relatively representable, and finite over* $\mathscr{M}_{1,1}$.

Proof: The relative representability is a consequence of the representability of Quot schemes. [1] The finite flat group scheme $E[N]/S$ is the spectrum of an $\mathscr{O}_S$-algebra $\mathscr{E}$, and given a finite flat commutative S-subgroup scheme G of $E[N]$ is equivalent to give a quotient of $\mathscr{E}$, whose kernel is locally free of rank N. Hence **Isog**$(N) \times_{\mathscr{M}_{1,1},E} S$ is represented by a closed subscheme of $\mathsf{Quot}_{\mathscr{E}/S/\mathbb{Z}}$, in particular, it is projective over S. It remains to check that it is quasi-finite.

By the principle of factorization, we may assume $N = p^n$. Let E/k be any elliptic curve over an algebraically closed field k. If char$(k) \neq p$, it is clear. If char$(k) = p$, and E is supersingular, then the choice of G is unique. If E is ordinary, we have

$$E[N] \simeq \mu_{p^n} \times \mathbb{Z}/p^n\mathbb{Z}.$$

[1] For the definition and their representability, cf. Nitsure [7].

Since k is perfect, the connected-étale exact sequence splits, i.e., we have an isomorphism

$$G \simeq G^0 \times_S G^{\text{ét}}.$$

Therefore the only possible choices of G are of the form $\mu_{p^d} \times p^{n-d}\mathbb{Z}/p^n\mathbb{Z}$, which are indeed only finitely many. □

Lemma 4.2.2. *Let E/S be an elliptic curve over S, $N \geqslant 1$ an integer, and $G \subset E[N]$ a finite flat commutative S-subgroup scheme. Then there exists a closed subscheme $W \subset S$, which is locally on S defined by finitely many equations, and is universal for the condition of cyclicity of G.*

Proof: This is an immediate consequence of the *Flattening Stratification.*[2] We view $G^\times$ as an $\mathscr{O}_S$-algebra on S. Notice that any fiber of $G^\times$ has either rank $\varphi(N)$ or 0, and the required locus consists of points s such that $G_s^\times$ has rank $\varphi(N)$, by Flattening Stratification, this locus is a closed subscheme $W \subset S$. Since the formation of $G^\times$ commutes with any base change, W is indeed universal for cyclicity of G. □

Theorem 4.2.3. *The moduli stack $\mathscr{Y}_0(N)$ is relatively representable, finite flat over $\mathscr{M}_{1,1}$ of rank*

$$\frac{N^2}{\varphi(N)} \prod_{d|N} \Big(1 - \frac{1}{d^2}\Big),$$

and it is regular of dimension two.

Proof: Let E/S be any elliptic curve. By Lemma 4.2.2, $\mathscr{Y}_0(N) \times_{\mathscr{M}_{1,1},E} S$ is represented by a closed subscheme of $\mathbf{Isog}(N) \times_{\mathscr{M}_{1,1},E} S$. Therefore $\mathscr{Y}_0(N)$ is relatively representable and finite over $\mathscr{M}_{1,1}$.

There is a natural morphism

$$\mathscr{Y}_1(N) \longrightarrow \mathscr{Y}_0(N),$$

given by forgetting the generator. This morphism is representable, concretely, $\mathscr{Y}_1(N) \times_{\mathscr{Y}_0(N),E} S$ is the scheme of generators of the universal cyclic group scheme over $\mathscr{Y}_0(N)$. Moreover, in this case, $\mathscr{Y}_0(N)$ is also regular of dimension 2 (cf. Altman-Kleiman [2] VII, Theorem 4.8). In particular, as $\mathscr{Y}_0(N)$ and $\mathscr{M}_{1,1}$ having the same dimension, $\mathscr{Y}_0(N)$ is automatically flat over $\mathscr{M}_{1,1}$.

Finally, to compute the rank of $\mathscr{Y}_0(N)$ over $\mathscr{M}_{1,1}$, one only needs to consider any geometric fiber, i.e., the rank is equal to the number of cyclic subgroups of order N in $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. □

4.3 Standard factorization

In this section, we further investigate the structure theory of cyclic subgroup schemes and cyclic isogenies of elliptic curves.

Lemma 4.3.1. *Let E/S be an elliptic curve over S, and $G \subset E[N]$ a cyclic S-subgroup scheme of rank N. Then*

*(1) For any divisor d of N, there exists a **standard cyclic subgroup scheme** $G_d \subset G$ of rank d, such that fppf-locally, if P is a generator of G, then G_d is generated by $(N/d)P$.*

[2] cf. Nitsure [7] Theorem 5.13.

(2) *The quotient group scheme $G' = G/G_d$ is a cyclic subgroup scheme of $E' = E/G_d$ with rank N/d. And if P is a generator of G, then its image P' in G' is also a generator of G'.*

(3) *If $d|d'|N$, then G_d is the standard cyclic subgroup scheme of $G_{d'}$ with rank d, and the quotient group scheme $G_{d'}/G_d$ is the standard cyclic subgroup scheme of G/G_d with rank d'/d.*

Proof: (1) The question is fppf-local, we may assume that G admits a generator P. By Theorem 3.3.3 (2), the point $(N/d)P$ has exact order d, hence it generates a cyclic subgroup scheme $G_d \subset G$. To show that it is "standard", we need to show that G_d does not depend on the generator. Let P' be another generator of G, and it generates a cyclic subgroup scheme G'_d. In order to show that $G_d = G'_d$, by reducing to the universal case, we may assume that S is noetherian and flat over $\mathbb{Z}$.

The subgroup schemes G_d and G'_d are indeed contained in G. We claim that the locus of the condition $G_d = G'_d$ is closed.

Since G is affine over S, let $\mathscr{E}$ be the corresponding $\mathscr{O}_S$-algebra, and let $\mathscr{I}$, $\mathscr{J}$ be the ideal sheaves of G_d, G'_d respectively. Then the locus of the condition $G_d = G'_d$ is exactly the closed subscheme of S such that the homomorphisms

$$\mathscr{I} \longrightarrow \mathscr{E}/\mathscr{J}, \qquad \mathscr{J} \longrightarrow \mathscr{E}/\mathscr{I}$$

are zero homomorphisms. This shows the claim. Moreover, the locus obviously contains the dense (by flatness) open subset $S \otimes \mathbb{Z}[\frac{1}{N}]$, hence $G_d = G'_d$ holds on S.

(2) As before, by passing to the universal case, we assume that S is flat over $\mathbb{Z}$. By Lemma 4.2.2, the cyclicity is a closed condition. So the locus of G' being cyclic is closed on S, while the locus obviously contains $S \otimes \mathbb{Z}[\frac{1}{N}]$, it must be S itself. Therefore G' is a cyclic subgroup scheme of E'.

Similarly, for the latter assertion, the locus of P' being a generator of G' is expressed by the equality of effective Cartier divisors

$$G' = \sum_{d \bmod N/d} [dP],$$

which is indeed a closed condition. And the locus contains $S \otimes \mathbb{Z}[\frac{1}{N}]$, hence it must be S itself, i.e., P' generates G'.

(3) For the first assertion, it suffices to show that $G_d = (G_{d'})_d$ is a closed condition, we already proved it in (1). For the latter assertion, do the same for the condition $G_{d'}/G_d = (G/G_d)_{d'/d}$. □

Definition 4.3.2. *The* ***standard factorization*** *of a cyclic N-isogeny*

$$E \xrightarrow[ker = G]{\phi} E''$$

with respect to a divisor d of N, is the factorization of ϕ

$$E \xrightarrow[ker = G_d]{\phi_d} E' \xrightarrow[ker = G']{\phi'} E''$$

into a cyclic d-isogeny composed by a cyclic N/d-isogeny.

Definition 4.3.3. *A pair of composable isogenies (ϕ_1, ϕ_2)*

$$\begin{tikzcd} E \arrow[r, "\phi_1", "deg=d_1"'] & E' \arrow[r, "\phi_2", "deg=d_2"'] & E'' \end{tikzcd}$$

*is called **cyclic in standard order**, if $\phi_2 \circ \phi_1$ is a cyclic $d_1 d_2$-isogeny, and the above factorization is standard (w.r.t. the divisor d_1 of $d_1 d_2$).*

Example 4.3.4. *Let E/S be an ordinary[3] elliptic curve over a $\mathbb{F}_p$-scheme S. The morphism $[p]$ is cyclic (cf. Lemma 5.1.1), and its standard factorization is*

$$\begin{tikzcd} E \arrow[r, "F_{E/S}"] & E^{(p)} \arrow[r, "V_{E/S}"] & E, \end{tikzcd}$$

where $V_{E/S}$ is the Verschiebung, i.e., the dual isogeny of the relative Frobenius $F_{E/S}$. Whereas the factorization

$$\begin{tikzcd} E^{(p)} \arrow[r, "V_{E/S}"] & E \arrow[r, "F_{E/S}"] & E^{(p)}, \end{tikzcd}$$

is non-standard. For the reason, see the remark behind the Standard Order Criterion 4.3.9.

Proposition 4.3.5. *Consider a pair of composable isogenies (ϕ_1, ϕ_2)*

$$\begin{tikzcd} E \arrow[r, "\phi_1", "deg=d_1"'] & E' \arrow[r, "\phi_2", "deg=d_2"'] & E''. \end{tikzcd}$$

Suppose that $\phi = \phi_2 \circ \phi_1$ is a cyclic isogeny, and ϕ_2 is étale, then (ϕ_1, ϕ_2) is cyclic in standard order.

Proof: The question is fppf-local, we may assume that $G = \mathrm{ker}(\phi)$ admits a generator $P = \psi(1)$:

$$\psi : \mathbb{Z}/d\mathbb{Z} \longrightarrow G(S),$$

where $d = d_1 d_2$. The generator ψ induces the commutative diagram

$$\begin{tikzcd} 0 \arrow[r] & d_2\mathbb{Z}/d\mathbb{Z} \arrow[r] \arrow[d] & \mathbb{Z}/d\mathbb{Z} \arrow[r] \arrow[d, "\psi"] & \mathbb{Z}/d_2\mathbb{Z} \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & \mathrm{ker}\,(\phi_1) \arrow[r] & G \arrow[r] & \mathrm{ker}\,(\phi_2) \arrow[r] & 0, \end{tikzcd}$$

by Proposition 2.4.1, the left and right sides are generators, in particular, $d_2 P$ generates $\mathrm{ker}(\phi_1)$, hence $\mathrm{ker}(\phi_1) = G_{d_1}$, i.e., (ϕ_1, ϕ_2) is cyclic in standard order. □

Proposition 4.3.6. *Consider a pair of composable cyclic isogenies (ϕ_1, ϕ_2) of elliptic curves over S*

$$\begin{tikzcd} E \arrow[r, "\phi_1", "deg=d_1"'] & E' \arrow[r, "\phi_2", "deg=d_2"'] & E'', \end{tikzcd}$$

and their dual isogenies

$$\begin{tikzcd} E & E' \arrow[l, "\phi_1^t"', "deg=d_1"] & E''. \arrow[l, "\phi_2^t"', "deg=d_2"] \end{tikzcd}$$

Then (ϕ_1, ϕ_2) is cyclic in standard order if and only if (ϕ_2^t, ϕ_1^t) is cyclic in standard order.

[3] It means that any geometric fiber of E/S is an ordinary elliptic curve.

Proof: Clearly we only need to prove the "only if" part. Denote $\phi = \phi_2 \circ \phi_1$, and $d = d_1 d_2$. By passing to the universal case, we may assume that S is flat over $\mathbb{Z}$. It amounts to prove the relation $\mathsf{ker}(\phi_2^t) = \big(\mathsf{ker}(\phi^t)\big)_{d_2}$, which is a closed condition. Since the case is obviously true on $S \otimes \mathbb{Z}[\frac{1}{d}]$, hence by flatness of S, it is true on S. □

Proposition 4.3.7. *Consider a pair of composable isogenies* (ϕ_1, ϕ_2)

$$\begin{tikzcd} E \arrow[r, "\phi_1", "deg = d_1"'] & E' \arrow[r, "\phi_2", "deg = d_2"'] & E'', \end{tikzcd}$$

such that $(d_1, d_2) = 1$. *Then TFAE:*

(1) ϕ_1, ϕ_2 *are cyclic;*

(2) $\phi = \phi_2 \circ \phi_1$ *is cyclic;*

(3) (ϕ_1, ϕ_2) *is cyclic in standard order.*

Proof: Let $\phi = \phi_2 \circ \phi_1$, $G = \mathsf{ker}(\phi)$. By the condition $(d_1, d_2) = 1$, we have the canonical factorization

$$G \;=\; G_1 \times G_2 \;=\; G[d_1] \times G[d_2],$$

with $\mathsf{rk}(G_i) = d_i$.

(1) $\Longleftrightarrow$ (2): Indeed, G is cyclic if and only if G_1 and G_2 are both cyclic. We know that $\mathsf{ker}(\phi_1)$ is killed by d_1, hence $\mathsf{ker}(\phi_1) \subset G_1$, and because $\mathsf{ker}(\phi_1)$ and G_1 have the same rank, they must be equal. Moreover, $\mathsf{ker}(\phi_2) \simeq G/\mathsf{ker}(\phi_1) \simeq G_2$, hence ϕ is cyclic if and only if ϕ_1, ϕ_2 are cyclic.

(2) $\Longleftrightarrow$ (3): This is straightforward. Suppose that (fppf-locally) P is a generator of G, then $\mathsf{ker}(\phi_1) = G_1$ is generated by $d_2 P$, hence $\mathsf{ker}(\phi_1) = G_{d_1}$. □

Theorem 4.3.8 (Backing-Up Theorem)**.** *Let*

$$\begin{tikzcd} E \arrow[r, "\phi_d"] & E' \arrow[r, "\phi'"] & E'' \end{tikzcd}$$

be the standard factorization of the cyclic N*-isogeny* $\phi = \phi' \circ \phi_d$ *with respect to the divisor* d *of* N*. Then*

(1) If a point $P \in \mathit{ker}(\phi)(S)$ *generates* $G = \mathit{ker}(\phi)$*, then* $\phi_d(P)$ *generates* $G' = \mathit{ker}(\phi')$*;*

(2) If N *and* N/d *have the same prime factors, then the converse of (1) is also true.*

Proof: (1) As usual, we assume that S is flat over $\mathbb{Z}$. The condition that $\phi_d(P)$ generates G' is a closed condition, and its locus obviously contains $S \otimes \mathbb{Z}[\frac{1}{N}]$, therefore by flatness, the condition is true on S.

(2) Assume that S is flat over $\mathbb{Z}$. The case over $S \otimes \mathbb{Z}[\frac{1}{N}]$ claims that if G is a cyclic subgroup of $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ of order d, where N and N/d have the same prime factors, then the preimage of any generator of the cyclic group

$$G' \;=\; G/G_d$$

is a generator of G. By the principle of factorization, we may reduce to the case that $N = p^n$ and $d = p^k$ for $k < n$, whence the case is obvious. The question (2) amounts to prove that the diagram

$$\begin{tikzcd} G^\times \arrow[r, "\phi_d"] \arrow[d, hook] & (G')^\times \arrow[d, hook] \\ G \arrow[r, "\phi_d"] & G' \end{tikzcd}$$

is cartesian, i.e., to verify the relation

$$G^\times \;=\; G \times_{G'} (G')^\times$$

inside G. As we have shown in the proof of Lemma 4.3.1, this is a closed condition. Since the case is clear on $S \otimes \mathbb{Z}[\frac{1}{N}]$, by flatness, it is also true on S. □

Theorem 4.3.9 (Standard Order Criterion)**.** *Let (ϕ_1, ϕ_2) be a pair of composable cyclic isogenies*

$$E \xrightarrow[\mathit{deg} = d_1]{\phi_1} E' \xrightarrow[\mathit{deg} = d_2]{\phi_2} E''.$$

Suppose that d_1, d_2 have the same prime factors. Then (ϕ_1, ϕ_2) being cyclic in standard order is equivalent to one of the following equivalent conditions:

(1) For any generator $P' \in \ker(\phi_2)(S)$ of $\ker(\phi_2)$, and any $P \in E(S')$ for a fppf base change $S' \to S$ such that $\phi_1(P) = P'$, the point $d_2 P$ generates $\ker(\phi_1) \times_S S'/S'$;

(2) For some generator $P' \in \ker(\phi_2)(S)$ of $\ker(\phi_2)$, and some $P \in E(S')$ for a fppf base change $S' \to S$ such that $\phi_1(P) = P'$, the point $d_2 P$ generates $\ker(\phi_1) \times_S S'/S'$;

Proof: Numbering the assertion "(ϕ_1, ϕ_2) is cyclic in standard order" by (0).

(1) $\Longrightarrow$ (2): Trivial.

(2) $\Longrightarrow$ (0): Base change to S', we may assume that $P \in E(S)$.

Since $d_2 P$ generates $\ker(\phi_1)$, it has exact order d_1. By Theorem 3.3.3 (2), the point P has exact order $d = d_1 d_2$. Let G be the cyclic group scheme generated by P. The standard rank d_1 cyclic subgroup scheme of G is clearly $\ker(\phi_1)$, hence the standard quotient $G' = G/G_{d_1}$ is the cyclic subgroup scheme of E'/S generated by $P' = \phi_1(P)$, i.e., $G' = \ker(\phi_2)$. By Backing-Up Theorem 4.3.8, the point P generates $\ker(\phi)$, i.e., $G = \ker(\phi)$. This shows that (ϕ_1, ϕ_2) is cyclic in standard order.

(0) $\Longrightarrow$ (1): If (ϕ_1, ϕ_2) is cyclic in standard order, by the Backing-Up Theorem 4.3.8, the condition that $P' = \phi_1(P)$ generates $\ker(\phi_2)$ implies that P generates $\ker(\phi)$. Therefore by the definition of standard factorization, the point $d_2 P$ generates $\ker(\phi_1)$. □

Remark: In the Example 4.3.4, the factorization

$$E^{(p)} \xrightarrow{V_{E/S}} E \xrightarrow{F_{E/S}} E^{(p)}$$

of the p^2-isogeny $[p]$ is non-standard. Choose (fppf-locally) a generator $Q \in E(S)$ of $\ker(F_{E/S})$, and a point $P \in E^{(p)}(S)$ such that $V_{E/S}(P) = Q$. By Standard Order Criterion 4.3.9, if the above factorization is standard, then pP must generate $\ker(V_{E/S})$. But $pP = 0$, this cannot be the case.

Definition 4.3.10. *A sequence of composable cyclic isogenies*

$$E_0 \xrightarrow[deg=d_1]{\phi_1} E_1 \xrightarrow[deg=d_2]{\phi_2} \dots \xrightarrow[deg=d_n]{\phi_n} E_n$$

is called ***cyclic in standard order****, if $\phi = \phi_n \circ \dots \circ \phi_1$ is cyclic, and*

$$ker(\phi_i \circ \dots \circ \phi_1) = G_{d_1 \cdot \dots \cdot d_i} \quad \text{for any } 1 \leqslant i \leqslant n.$$

Theorem 4.3.11. *Let $(\phi_1, \dots, \phi_n)$ be a sequence of composable cyclic isogenies*

$$E_0 \xrightarrow[deg=d_1]{\phi_1} E_1 \xrightarrow[deg=d_2]{\phi_2} \dots \xrightarrow[deg=d_n]{\phi_n} E_n$$

such that $d_1, \dots, d_n$ have the same prime factors. Then $(\phi_1, \dots, \phi_n)$ is cyclic in standard order if and only if (ϕ_i, ϕ_{i+1}) is cyclic in standard order for any $1 \leqslant i \leqslant n-1$.

Proof: The "only if" part is clear from the definition and Lemma 4.3.1 (3).

Now we show the "if" part by induction on n. When $n = 2$, there is nothing to prove. Assume that any composable subsequence of $(\phi_1, \dots, \phi_n)$ with length less than n is cyclic in standard order. It amounts to show that the pair $(\phi_{n-1} \circ \dots \circ \phi_1, \phi_n)$

$$E_0 \xrightarrow{\phi_{n-1} \circ \dots \circ \phi_1} E_{n-1} \xrightarrow{\phi_n} E_n$$

is cyclic in standard order. The question is fppf-local, we may assume that $\mathsf{ker}(\phi_n)$ admits a generator $P_{n-1} \in E_{n-1}(S)$, and choose a sequence of points $(P_0, \dots, P_{n-1})$ such that

$$P_{i+1} = \phi_{i+1}(P_i) \quad \text{for any } 0 \leqslant i \leqslant n-2.$$

By Standard Order Criterion 4.3.9, it remains to show that the point $d_n P_0$ generates $\mathsf{ker}(\phi_{n-1} \circ \dots \circ \phi_1)$. Consider the pairs $(\phi_{n-2} \circ \dots \circ \phi_1, \phi_{n-1})$ and (ϕ_{n-1}, ϕ_n)

$$E_0 \xrightarrow{\phi_{n-2} \circ \dots \circ \phi_1} E_{n-2} \xrightarrow{\phi_{n-1}} E_{n-1} \xrightarrow{\phi_n} E_n,$$

by induction, these pairs are both cyclic in standard order. Since $P_{n-1} = \phi_{n-1}(P_{n-2})$ generates $\mathsf{ker}(\phi_n)$, by Standard Order Criterion 4.3.9, the point $d_n P_{n-2}$ generates $\mathsf{ker}(\phi_{n-1})$. And since

$$(\phi_{n-2} \circ \dots \circ \phi_1)(d_n P_0) = d_n P_{n-2},$$

by Backing-Up Theorem 4.3.8, the point $d_n P_0$ generates $\mathsf{ker}(\phi_{n-1} \circ \dots \circ \phi_1)$. □

5
Igusa Curves

In this chapter, we study a new moduli problem of elliptic curves, the *Igusa moduli problem*, which happens only in positive characteristic $p > 0$. The Igusa moduli problem plays an important role in the study of reduction mod p of modular curves, more precisely, the Igusa moduli stacks are the underlying reduced curves associated to the irreducible components of the reduction mod p of the four basic modular curves.

5.1 Some properties of relative Frobenius

Let E/S be an elliptic curve over a $\mathbb{F}_p$-scheme S. The relative Frobenius $F_{E/S}$ is a cyclic p-isogeny, since the zero section 0 is a generator of $\mathsf{ker}(F_{E/S})$. The *relative Verschiebung* $V_{E/S}$, as the dual isogeny of $F_{E/S}$, is also a cyclic p-isogeny.

The iterated relative Frobenius $F^n_{E/S}$ and Verschiebung $V^n_{E/S}$ are cyclic p^n-isogenies. The standard factorization of the iterated relative Frobenius $F^n_{E/S}$ is

$$E \xrightarrow{F_{E/S}} E^{(p)} \xrightarrow{F_{E/S}} E^{(p^2)} \xrightarrow{F_{E/S}} \dots \xrightarrow{F_{E/S}} E^{(p^n)},$$

and the standard factorization of $V^n_{E/S}$ is

$$E^{(p^n)} \xrightarrow{V_{E/S}} E^{(p^{n-1})} \xrightarrow{V_{E/S}} E^{(p^{n-2})} \xrightarrow{V_{E/S}} \dots \xrightarrow{V_{E/S}} E.$$

Lemma 5.1.1. *Let E/S be an elliptic curve over a $\mathbb{F}_p$-scheme S. Then the p^{2n}-isogeny $[p^n]$ is cyclic, and its standard factorization (w.r.t. the divisor p^n of p^{2n}) is*

$$E \xrightarrow{F^n_{E/S}} E^{(p^n)} \xrightarrow{V^n_{E/S}} E.$$

Proof: Choose (fppf-locally) a generator $Q \in E^{(p^n)}(S)$ of $\ker(V^n_{E/S})$, and $P \in E(S)$ such that $F^n_{E/S}(P) = Q$. Since $p^n P = 0$ generates $\ker(F^n_{E/S})$, by Standard Order Criterion 4.3.9, the pair $(F^n_{E/S}, V^n_{E/S})$ is cyclic in standard order. In particular, $[p^n]$ is cyclic. □

Corollary 5.1.2. *Let E/S be an elliptic curve over a $\mathbb{F}_p$-scheme S. Then S is a $\mathbb{F}_p$-scheme if and only if the p^{2n}-isogeny $[p]$ is cyclic.*

Proof: Choose (fppf-locally) a generator $P \in E(S)$ of $\ker([p])$, then $p^n P = 0$ has exact order p^n. By Lemma 3.2.5, $p = 0$ in S.

Proposition 5.1.3. *Let E/S be an elliptic curve over a $\mathbb{F}_p$-scheme S, and $P \in E[p^n](S)$ a p^n-torsion point. Then TFAE:*

(1) P is a generator of $E[p^n]$;

(2) $(0, P)$ is a Drinfeld basis of $E[p^n]/S$;

(3) There is an elliptic curve E_n/S with an isomorphism $E \simeq E_n^{(p^n)}$, and the image of P generates $\ker(V^n_{E_n/S})$.

Proof: (1) $\Longleftrightarrow$ (2): By Backing-Up Theorem 4.3.8, (1) is equivalent to the condition that $F^n_{E/S}(P)$ is a generator of $\ker(V^n_{E/S})$, which means that $\big(\ker(F^n_{E/S}), 0, F^n_{E/S}(P)\big)$ is a $\Gamma_1^{\text{bal}}(p^n)$-structure on E/S. This is equivalent to the condition (2). [1]

(2) $\Longrightarrow$ (3): Since $(0, P)$ is a Drinfeld basis, the point P has exact order p^n. Let K be the cyclic subgroup scheme of $E[p^n]$ generated by P, and let $E_n = E/K$ be the quotient elliptic curve. Let ϕ_n be the p^n-isogeny

$$\phi_n : E \longrightarrow E_n,$$

where $\ker(\phi_n) = K$. The point $\phi_n(0) = 0$ necessarily generates $\ker(\phi_n^t)$, while at the same time 0 generates the cyclic subgroup scheme $\ker(F^n_{E_n/S})$, which has the same rank p^n. Therefore $F^n_{E_n/S}$ is the dual isogeny of ϕ_n, and

$$E \simeq E_n^{(p^n)}.$$

Moreover, because $\phi_n = V^n_{E_n/S}$, the point P generates $\ker(V^n_{E_n/S})$.

(3) $\Longrightarrow$ (1): The standard factorization of $[p^n]$ on E is

$$E \simeq E_n^{(p^n)} \xrightarrow{F^n_{E/S}} E_n^{(p^{2n})} \xrightarrow{V^n_{E/S}} E_n^{(p^n)}.$$

On the one hand, $p^n P = 0$ obviously generates $\ker(F^n_{E/S})$. On the other hand, since P generates $\ker(V^n_{E_n/S})$, after the base change by the iterated absolute Frobenius F^n_{ab}:

$$\begin{tikzcd}
E_n^{(p^{2n})} \arrow[r, "V^n_{E/S}"] \arrow[d] & E_n^{(p^n)} \arrow[r] \arrow[d] & S \arrow[d, "F^n_{\text{ab}}"] \\
E_n^{(p^n)} \arrow[r, "V^n_{E_n/S}"] & E_n \arrow[r] & S
\end{tikzcd}$$

the point $F^n_{E/S}(P)$ generates $\ker(V^n_{E/S})$. By Standard Order Criterion 4.3.9, P generates $E[p^n]$. □

[1] See the remark behind Theorem 3.3.1.

Proposition 5.1.4. *Let E/S be an elliptic curve over a $\mathbb{F}_p$-scheme S. Then:*

(1) A point $P \in E(S)$ is a generator of $\mathrm{ker}([p^n])$ *if and only if $p^{n-1}P$ is a generator of* $\mathrm{ker}([p])$*;*

(2) A point $P \in E(S)$ is a generator of $\mathrm{ker}([p^n])$ *if and only if $p^{n-1}F_{E/S}(P)$ is a generator of* $\mathrm{ker}(V_{E/S})$*;*

(3) A point $Q \in E^{(p^n)}(S)$ is a generator of $\mathrm{ker}(V^n_{E/S})$ *if and only if $V^{n-1}_{E/S}(Q)$ is a generator of* $\mathrm{ker}(V_{E/S})$*.*

Proof: (1) By Proposition 5.1.3, $(0,P)$ is a Drinfeld basis of $E[p^n]$, hence by Theorem 3.3.3, $(0,p^{n-1}P)$ is a Drinfeld basis of $E[p]$. Therefore, again by Proposition 5.1.3, $p^{n-1}P$ is a generator of $\mathrm{ker}([p])$.

(2) Consider the standard factorization of $[p^n]$:

$$E \xrightarrow{p^{n-1}F_{E/S}} E^{(p)} \xrightarrow{V_{E/S}} E,$$

by Backing-Up Theorem 4.3.8, $P \in E(S)$ generates $\mathrm{ker}([p^n])$ if and only if $p^{n-1}F_{E/S}(P)$ generates $\mathrm{ker}(V_{E/S})$.

(3) Consider the standard factorization of $V^n_{E/S}$:

$$E^{(p^n)} \xrightarrow{V^{n-1}_{E/S}} E^{(p)} \xrightarrow{V_{E/S}} E,$$

again, apply Backing-Up Theorem 4.3.8. □

Now consider an elliptic curve E/k defined over an algebraically closed field of characteristic p. Let $P \in E^{(p)}(k)$ be a generator of $\mathrm{ker}(V_{E/k})$, then we have two possibilities:

1. $P=0$. In this case, by Proposition 5.1.4, the zero section 0 generates $\mathrm{ker}([p^n])$ and $\mathrm{ker}(V^n_{E/k})$ for any $n \geqslant 1$. In particular, $\mathrm{ker}([p^n]) = \mathrm{ker}(F^{2n}_{E/k})$ and $\mathrm{ker}(V^n_{E/k}) = \mathrm{ker}(F^n_{E/k})$.
2. $P \neq 0$. In this case, $\mathrm{ker}(V_{E/k})$ is étale over k, and the generator P defines an isomorphism:

$$P:\ \mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} \mathrm{ker}(V_{E/k}).$$

   Moreover, choose a series of points $P_i \in E^{(p^i)}(k)$ for $i \geqslant 1$, such that

$$P_1 = P, \qquad V_{E^{(p^i)}/k}(P_{i+1}) = P_i \qquad \text{for } i \geqslant 1.$$

   Then by Proposition 5.1.4 (3), P_i generates $\mathrm{ker}(V^i_{E/k})$ for any $i \geqslant 1$, and it defines an isomorphism

$$P_i:\ \mathbb{Z}/p^i\mathbb{Z} \xrightarrow{\sim} \mathrm{ker}(V^i_{E/k}).$$

The first (resp. second) case happens when E/k is supersingular (resp. ordinary). In the ordinary case, $\mathrm{ker}(V^n_{E/k})$ is isomorphic to the constant group scheme $\mathbb{Z}/p^n\mathbb{Z}$, and $\mathrm{ker}(F^n_{E/k})$ is its Cartier dual, which is isomorphic to μ_{p^n}. Thus we have the short exact sequence of k-group schemes:

$$0 \longrightarrow \mu_{p^n} \longrightarrow E[p^n] \longrightarrow \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0,$$

in particular, we have $E[p^n](k) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Passing to the direct limit, the short exact sequence gives

$$0 \longrightarrow \mu_{p^\infty} \longrightarrow E[p^\infty] \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow 0,$$

which is visibly splitting, i.e., we have the isomorphism

$$E[p^\infty] \simeq \mu_{p^\infty} \times \mathbb{Q}_p/\mathbb{Z}_p.$$

In particular, the p-divisible group $E[p^\infty]$ has infinitely many k-rational points:

$$E[p^\infty](k) \simeq \mathbb{Q}_p/\mathbb{Z}_p.$$

By passing to geometric fibers, the above discussion immediately gives the following result:

Proposition 5.1.5. *Let E/S be an elliptic curve over a $\mathbb{F}_p$-scheme S. Then TFAE:*

(1) E/S is ordinary;

(2) $V^n_{E/S}$ is étale for some $n \geqslant 1$;

(3) $V^n_{E/S}$ is étale for any $n \geqslant 1$;

(4) $Lie(V_{E/S}) : Lie(E/S)^{(p)} \to Lie(E/S)$ is an isomorphism;

(5) Any geometric fiber E_s contains infinitely many p-power order points.

Corollary 5.1.6. *Let $\phi : E \to E'$ be an isogeny of elliptic curves over a $\mathbb{F}_p$-scheme S. Then E/S is ordinary if and only if E'/S is ordinary.*

Proof: By passing to geometric fiber, we may assume that S is a geometric point $\mathsf{Spec}\ (k)$. The isogeny ϕ induces an isogeny of p-divisible groups:

$$\phi : E[p^\infty] \longrightarrow E'[p^\infty],$$

taking the k-rational points, it gives a homomorphism

$$\phi(k) : E[p^\infty](k) \longrightarrow E'[p^\infty](k)$$

with finite kernel. In particular, $E[p^\infty](k)$ and $E'[p^\infty](k)$ have the same cardinal. By Proposition 5.1.5 (5), this assertion is equivalent to say that E/S is ordinary if and only if E'/S is ordinary. □

5.2 Igusa moduli stack

Definition 5.2.1. *Let E/S be an elliptic curve over a $\mathbb{F}_p$-scheme S, $n \geqslant 1$ an integer. An **Igusa level p^n structure** on E/S is a generator $P \in E^{(p^n)}(S)$ of $\mathsf{ker}(V^n_{E/S})$. The corresponding **Igusa moduli stack** is denoted by $\mathbf{Ig}(p^n)$, which is naturally defined over $\mathscr{M}_{1,1} \otimes \mathbb{F}_p$.*

Remark: The moduli problem $\mathbf{Ig}(p^n)$ is indeed a Deligne-Mumford stack. To see this, it suffices to show that $\mathbf{Ig}(p^n)$ is relatively representable over $\mathscr{M}_{1,1}$, which is obvious:

$$\mathbf{Ig}(p^n) \times_{\mathscr{M}_{1,1}\otimes\mathbb{F}_p, E} S = \mathbb{Z}/p^n\mathbb{Z}\text{-}\mathsf{Gen}\big(\mathsf{ker}(V^n_{E/S})/S\big).$$

In particular, $\mathbf{Ig}(p^n)$ is finite and flat over $\mathscr{M}_{1,1} \otimes \mathbb{F}_p$, which has rank $\varphi(p^n)$.

Our main result about Igusa moduli stacks is

Theorem 5.2.2 (Igusa)**.** *The Igusa moduli stack* $\mathbf{Ig}(p^n)$ *is relatively representable, and finite flat of rank* $\varphi(p^n)$ *over* $\mathscr{M}_{1,1}\otimes\mathbb{F}_p$. *Moreover,* $\mathbf{Ig}(p^n)$ *is regular of dimension one.*

Proof: It is already clear that $\mathbf{Ig}(p^n)$ is relatively representable and finite flat of rank $\varphi(p^n)$ over $\mathscr{M}_{1,1}\otimes\mathbb{F}_p$. It remains to show that it is regular of dimension one. It suffices to check the supersingular points, since the ordinary part $\mathbf{Ig}^{\mathrm{ord}}(p^n)$ is obviously étale over $\mathscr{M}_{1,1}\otimes\mathbb{F}_p$.

Let E_0/k be a supersingular elliptic curve over an algebraically closed field k of characteristic p, and $\mathbf{E}_0/k[\![T]\!]$ its universal formal deformation to artinian local k-algebras with residue field k. We must show that the finite flat $k[\![T]\!]$-scheme

$$\mathbf{Ig}(p^n)\times_{\mathscr{M}_{1,1}\otimes\mathbb{F}_p,\mathbf{E}_0}k[\![T]\!]$$

is regular of dimension one. Let A be the affine coordinate ring of the above $k[\![T]\!]$-scheme. The ring A is indeed a local ring, since the only Igusa level p^n structure on E_0/k is the zero section. Let $\mathfrak{m}_A$ be the maximal ideal of A. We fix a formal parameter X of the formal group $\widehat{\mathbf{E}}_0$ of the elliptic curve $\mathbf{E}_0/k[\![T]\!]$, then we claim that the maximal ideal $\mathfrak{m}_A$ is generated by the X coordinate of the universal generator of $\mathsf{ker}\big(V^n_{\mathbf{E}_0/k[\![T]\!]}\big)$.

Like the proof of Regularity Theorem 3.2.1, we must show the following assertion:

> If E/R is an elliptic curve over an artinian local k-algebra, and 0 generates $\mathsf{ker}(V^n_{E/R})$, then E/R is a constant family.

In this case, we have $\mathsf{ker}(V^n_{E/R})=\mathsf{ker}\big(F^n_{E^{(p^n)}/R}\big)$, therefore we have the isomorphism

$$E\simeq E^{(p^{2n})},$$

and consequently

$$E\simeq E^{(p^{2n})}\simeq E^{(p^{4n})}\simeq\ldots\simeq E^{(p^{2kn})}\simeq\ldots$$

which implies that E/R is a constant family [2]. □

Next natural question is the representability of the Igusa moduli stack $\mathbf{Ig}(p^n)$. Unfortunately, the Igusa moduli problem is not globally rigid. However, when we restrict on the ordinary part, it turns out that the *ordinary Igusa moduli stack* $\mathbf{Ig}^{\mathrm{ord}}(p^n)$ has a nice result of representability.

Theorem 5.2.3. *If* $p^n\geqslant 3$, *the ordinary Igusa moduli stack* $\mathbf{Ig}^{ord}(p^n)$ *is represented by a smooth and geometrically connected curve over* $\mathbb{F}_p$.

Proof: We already know the relative representability and affineness of $\mathbf{Ig}^{\mathrm{ord}}(p^n)$, by Theorem 3.1.5, it remains to show that the ordinary Igusa moduli stack is rigid.

Let E/k be an ordinary elliptic curve over a field k of characteristic p, and P a generator of $\mathsf{ker}(V^n_{E/k})$. Then P defines an isomorphism

$$P:\ \mathbb{Z}/p^n\mathbb{Z}\xrightarrow{\ \sim\ }\mathsf{ker}\,(V^n_{E/k})\hookrightarrow E^{(p^n)}.$$

Let

$$\sigma:\ \mathrm{End}(E/k)\longrightarrow\mathbb{Z}/p^n\mathbb{Z}$$

[2] cf. "**Case I:** $\mathscr{Y}(N)$" of the proof of Regularity Theorem 3.2.1.

be the action of $\mathrm{End}(E/k)$ on $\ker(V^n_{E/k})$, it is a ring homomorphism. Let $\epsilon \in \mathrm{Aut}(E/k)$ be an automorphism of E/k, such that $\sigma(\epsilon) = 1$ in $\mathbb{Z}/p^n\mathbb{Z}$.

Since $p^n \geqslant 3$, the automorphism $\epsilon \neq \pm 1$. Then ϵ satisfies one of the following equations: [3]

- $\epsilon^2 + 1 = 0 \implies 2 \equiv 0 \bmod p^n$;
- $\epsilon^2 + \epsilon + 1 = 0 \implies 3 \equiv 0 \bmod p^n$;
- $\epsilon^2 - \epsilon + 1 = 0 \implies 1 \equiv 0 \bmod p^n$.

Obviously, the first and the third situations cannot happen. For the second case, this happens only if $p^n = 3$, i.e., $p = 3$. In this case, it is the elliptic curve with CM by $\mathbb{Q}(\zeta_3)$, which is the unique supersingular elliptic curve in characteristic 3, hence it is not in our consideration. Therefore the only possible case is $\epsilon = 1$, which shows the rigidity of the ordinary Igusa moduli stack $\mathbf{Ig}^{\mathrm{ord}}(p^n)$. □

5.3 Exotic Igusa moduli stacks

Let k be a perfect field of characteristic $p > 0$, and denote $\sigma : k \to k$ for the absolute Frobenius of k. For any k-scheme S, let us denote $S^{(\sigma^i)}$ for the pull-back along the iterated absolute Frobenius σ^i:

$$\begin{tikzcd}
S^{(\sigma^i)} \arrow[r] \arrow[d] & S \arrow[d] \\
\mathrm{Spec}\,(k) \arrow[r, "\sigma^i"] & \mathrm{Spec}\,(k).
\end{tikzcd}$$

Similarly, for any moduli problem $\mathscr{P}$ over $\mathscr{M}_{1,1} \otimes k$, we can define $\mathscr{P}^{(\sigma^i)}$ as the pull-back of $\mathscr{P}$ along σ^i:

$$\begin{tikzcd}
\mathscr{P}^{(\sigma^i)} \arrow[r] \arrow[d] & \mathscr{P} \arrow[d] \\
\mathscr{M}_{1,1} \otimes k \arrow[r] \arrow[d] & \mathscr{M}_{1,1} \otimes k \arrow[d] \\
\mathrm{Spec}\,(k) \arrow[r, "\sigma^i"] & \mathrm{Spec}\,(k)
\end{tikzcd}$$

Given any elliptic curve E/S over a k-scheme S, we have

$$\mathscr{P}(E/S) \;=\; \mathscr{P}^{(\sigma^i)}\big(E^{(\sigma^i)}/S^{(\sigma^i)}\big).$$

If $\mathscr{P}$ is relatively representable over $\mathscr{M}_{1,1} \otimes k$, then

$$\big(\mathscr{P}^{(\sigma^i)}\big)_{E^{(\sigma^i)}/S^{(\sigma^i)}} \;=\; (\mathscr{P}_{E/S})^{(\sigma^i)}.$$

In particular, if $\mathscr{P}$ is represented by a scheme $M(\mathscr{P})$, then $\mathscr{P}^{(\sigma^i)}$ is represented by the scheme $M\big(\mathscr{P}^{(\sigma^i)}\big) = M(\mathscr{P})^{(\sigma^i)}$. Notice that if the moduli problem $\mathscr{P}$ is defined over $\mathbb{F}_p$, then obviously $\mathscr{P}^{(\sigma^i)} = \mathscr{P}$, e.g.,

$$\big(\mathscr{Y}_1(N) \otimes \mathbb{F}_p\big)^{(\sigma^i)} \;=\; \mathscr{Y}_1(N) \otimes \mathbb{F}_p \quad \text{and} \quad \big(\mathscr{Y}_0(N) \otimes \mathbb{F}_p\big)^{(\sigma^i)} \;=\; \mathscr{Y}_0(N) \otimes \mathbb{F}_p.$$

[3] Since we work only on ordinary elliptic curves, the situations $\#\mathrm{Aut}(E/k) = 12$ or 24 cannot happen.

There is a natural map

$$\begin{array}{rcl} \mathscr{P}(E/S) & \longrightarrow & \mathscr{P}^{(\sigma^i)}(E^{(p^i)}/S) \\ \alpha & \longmapsto & \alpha^{(p^i)} \end{array}$$

which is given by the bijection $\mathscr{P}(E/S) = \mathscr{P}^{(\sigma^i)}(E^{(\sigma^i)}/S^{(\sigma^i)})$, and the pull-back along $F^i_{S/k}$:

$$\begin{tikzcd} E^{(p^i)} \arrow[r] \arrow[d] & E^{(\sigma^i)} \arrow[r] \arrow[d] & E \arrow[d] \\ S \arrow[r, "F^i_{S/k}"] \arrow[rr, bend right, "F_{\mathrm{ab}}"'] & S^{(\sigma^i)} \arrow[r] & S \end{tikzcd}$$

Example 5.3.1. *Let $\mathscr{P} = \mathscr{Y}_1(N)$, the above map is given by*

$$P \in E(S) \text{ of exact order } N \longmapsto F^i_{E/S}(P).$$

If N is prime to p, then there is an inverse map, given by

$$P \in E^{(p^i)}(S) \longmapsto \frac{1}{p^i} \cdot V^i_{E/S}(P).$$

Example 5.3.2. *Let $\mathscr{P} = \mathscr{Y}(N)$, the above map is given by*

$$(P, Q) \longmapsto \big(F^i_{E/S}(P), F^i_{E/S}(Q)\big).$$

Similarly, if N is prime to p, then there is an inverse map, given by

$$(P, Q) \longmapsto \left(\frac{1}{p^i} \cdot V^i_{E/S}(P), \frac{1}{p^i} \cdot V^i_{E/S}(Q)\right).$$

In fact, this map is always bijective when $\mathscr{P}$ is étale over $\mathscr{M}_{1,1} \otimes k$.

Let $\mathscr{P}$ be a representable moduli stack over $\mathscr{M}_{1,1} \otimes k$, then we have a natural morphism for any $i \geqslant 0$:

$$\begin{array}{rcl} p_i : \ M(\mathscr{P}) \times_{\mathscr{M}_{1,1} \otimes k} \mathbf{Ig}(p^n) & \longrightarrow & M\big(\mathscr{P}^{(\sigma^i)}\big) \\ (E/S, \alpha, P) & \longmapsto & \big(E^{(p^i)}/S, \alpha^{(p^i)}\big), \end{array}$$

where $\alpha \in \mathscr{P}(E/S)$ is a level $\mathscr{P}$ structure, and $P \in E^{(p^n)}(S)$ is a generator of $\ker(V^n_{E/S})$. Hence $M(\mathscr{P}) \times_{\mathscr{M}_{1,1} \otimes k} \mathbf{Ig}(p^n)$ can be viewed as a $M\big(\mathscr{P}^{(\sigma^i)}\big)$-scheme via p_i. Even more, $M(\mathscr{P}) \times_{\mathscr{M}_{1,1} \otimes k} \mathbf{Ig}(p^n)$ can be interpreted as a moduli $M\big(\mathscr{P}^{(\sigma^i)}\big)$-scheme.

Definition 5.3.3. *Let E/S be an elliptic curve over a $\mathbb{F}_p$-scheme S, and n, i be positive integers with $1 \leqslant i \leqslant n$. An **exotic Igusa level** (p^n, i) **structure** consists of two points $P \in E(S)$ and $Q \in E^{(p^{n-i})}(S)$, such that $(0, P)$ is a Drinfeld p^i-basis of E/S, and $V^{n-i}_{E/S}(Q) = P$. The corresponding **exotic Igusa moduli stack** over $\mathscr{M}_{1,1} \otimes \mathbb{F}_p$ is denoted by $\mathbf{ExIg}(p^n, i)$.*

Theorem 5.3.4. *For any $1 \leqslant i \leqslant n$, we have an isomorphism of moduli stacks over $\mathscr{M}_{1,1} \otimes \mathbb{F}_p$:*

$$\begin{array}{rcl} \Theta_i : \mathbf{Ig}(p^n) & \longrightarrow & \mathbf{ExIg}(p^n, i) \\ (E/S,\ P) & \longmapsto & \big(E^{(p^i)}/S,\ V^{n-i}_{E/S}(P),\ P\big). \end{array}$$

If $\mathscr{P}$ is a representable moduli stack over $\mathscr{M}_{1,1} \otimes k$, where k is a perfect field of characteristic p, then

$$\begin{array}{rcl} M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{Ig}(p^n) & \longrightarrow & M\big(\mathscr{P}^{(\sigma^i)}\big) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{ExIg}(p^n, i) \\ (E/S,\ \alpha\ ,P) & \longmapsto & \big(E^{(p^i)}/S,\ \alpha^{(p^i)},\ V^{n-i}_{E/S}(P),\ P\big) \end{array}$$

defines an isomorphism of $M\big(\mathscr{P}^{(\sigma^i)}\big)$-schemes, i.e., the diagram

$$\begin{tikzcd} M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{Ig}(p^n) \arrow[r, "\sim"] \arrow[rd, "p_i"'] & M\big(\mathscr{P}^{(\sigma^i)}\big) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{ExIg}(p^n, i) \arrow[d] \\ & M\big(\mathscr{P}^{(\sigma^i)}\big) \end{tikzcd}$$

commutes.

Proof: Firstly we show that the morphism Θ_i is well-defined, i.e., we need to show that if P is a generator of $\ker(V^n_{E/S})$, then $\big(0, V^{n-i}_{E/S}(P)\big)$ is a Drinfeld p^i-basis of $E^{(p^i)}/S$. From the standard factorization:

$$E^{(p^n)} \xrightarrow{V^{n-i}_{E/S}} E^{(p^i)} \xrightarrow{V^{i}_{E/S}} E,$$

by Backing-Up Theorem 4.3.8, the point $V^{n-i}_{E/S}(P)$ generates $\ker(V^i_{E/S})$, then applying Proposition 5.1.3, $\big(0, V^{n-i}_{E/S}(P)\big)$ is a Drinfeld p^i-basis of $E^{(p^i)}/S$.

That Θ_i being an isomorphism (equivalence of categories) is easily deduced from Proposition 5.1.3 (3). The last assertion is obvious. □

Corollary 5.3.5. *The exotic Igusa moduli stack $\mathbf{ExIg}(p^n, i)$ is relatively representable, and finite flat of rank $p^i \cdot \varphi(p^n)$ over $\mathscr{M}_{1,1} \otimes \mathbb{F}_p$. Moreover, it is regular of dimension 1.*

Proof: By Theorem 5.2.2 and Theorem 5.3.4, it is already clear that $\mathbf{ExIg}(p^n, i)$ is relatively representable and finite flat over $\mathscr{M}_{1,1} \otimes \mathbb{F}_p$, and regular of dimension 1. To compute its rank, we pick an auxiliary representable moduli stack $\mathscr{P}$ over $\mathscr{M}_{1,1} \otimes \mathbb{F}_p$ which is finite étale, and use the commutative diagram

$$\begin{tikzcd} M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes\mathbb{F}_p} \mathbf{Ig}(p^n) \arrow[r, "\sim"] \arrow[d, "\pi"] \arrow[rd, "p_i"] & M\big(\mathscr{P}^{(\sigma^i)}\big) \times_{\mathscr{M}_{1,1}\otimes\mathbb{F}_p} \mathbf{ExIg}(p^n, i) \arrow[d] \\ M(\mathscr{P}) \arrow[r, "F^i_{/k}"] & M\big(\mathscr{P}^{(\sigma^i)}\big) \end{tikzcd}$$

then it is visibly that the rank of $\mathbf{ExIg}(p^n, i)$ over $\mathscr{M}_{1,1} \otimes \mathbb{F}_p$ is equal to $p^i \cdot \varphi(p^n)$. □

6

Reduction Mod p of Modular Curves

6.1 Crossings at supersingular points

Let us consider the following situation:

Fix a field k. Let Y/k be a curve, and $\{y_0\}$ is a set of k-rational points of Y, which we call them "supersingular" points. Suppose that we are given the following morphisms of k-schemes:

$$\begin{tikzcd}
\coprod_{i\in I} Z_i \arrow[r, "\psi"] \arrow[dr, "\psi'"'] & X \arrow[d, "\phi"] \\
& Y
\end{tikzcd}$$

which satisfy the following conditions:

(a) Y is a smooth curve over k;

(b) ϕ is finite flat;

(c) For each supersingular point y_0 of Y, there exists a unique closed point x_0 of X which turns out to be k-rational and lying over y_0. Furthermore, the complete local ring of X at x_0 has the form
$$\widehat{\mathscr{O}}_{X,x_0} \simeq k[\![x,y]\!]/(f);$$

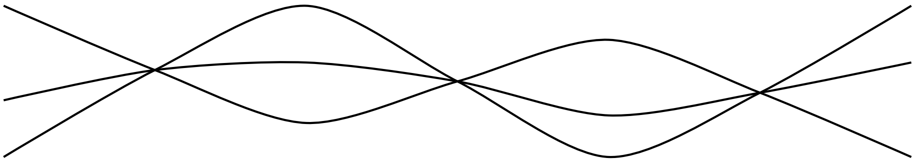
(d) Each $(Z_i)_{\mathrm{red}}$ is a smooth curve over k;

(e) Each $\psi'_i = \psi'|_{Z_i}$ is finite flat, and each $\psi_i = \psi|_{Z_i}$ is a closed immersion;

(f) For each supersingular point y_0 of Y, and each $i \in I$, there exists a unique closed point $z_{i,0}$ of Z_i which turns out to be k-rational and lying over y_0;

(g) The morphism $\psi|_{Y\setminus\{y_0\}}$ is an isomorphism.

A simple picture of X could be like the following:



In this situation, we call that X is the disjoint union of Z_i's with crossings at supersingular points. More precisely, we have the following theorem:

Theorem 6.1.1 (Crossings Theorem)**.** *Hypotheses and notations as above. Let y_0 be a supersingular point of Y, and x_0 is the unique k-rational point of X that lies over y_0. Then the complete local ring of X at x_0 has the form:*

$$\widehat{\mathcal{O}}_{X,x_0} \simeq k[\![x,y]\!]\Big/\Big(\prod_{i\in I} f_i^{e_i}\Big),$$

where f_i's are distinct[1] *irreducible elements in $k[\![x,y]\!]$, and*

$$\widehat{\mathcal{O}}_{Z_i,zi,0} \simeq k[\![x,y]\!]/\big(f_i^{e^i}\big) \quad \textit{for all } i \in I.$$

Moreover, if Y is connected (resp. geometrically connected), then so are Z_i's, and they are exactly all the irreducible components of X.

Proof: Since Y is smooth over k, we fix an isomorphism

$$\widehat{\mathcal{O}}_{Y,y_0} \simeq k[\![T]\!].$$

Then as a $k[\![T]\!]$-algebra, $k[\![x,y]\!]/(f)$ is finite and flat, say, of degree d over $k[\![T]\!]$. In particular, f is neither a unit nor 0. Factorize f into product of irreducible elements:

$$f = \prod_{j\in J} f_j^{e_j}.$$

Choose an element $T' \in k[\![x,y]\!]$, such that $T' \equiv T \bmod f$. Then the k-algebra

$$k[\![x,y]\!]\Big/\Big(\prod_{i\in I} f_i^{e_i}, T'\Big)$$

has dimension d. In particular, T' cannot be a unit nor 0. We factorize $T' = \prod g_k^{n_k}$ in $k[\![x,y]\!]$. Then the k-algebra $k[\![x,y]\!]/(f_j, g_k)$, as a quotient of a finite-dimensional k-algebra

$$k[\![x,y]\!]\Big/\Big(\prod_{i\in I} f_i^{e_i}, T'\Big) \longrightarrow k[\![x,y]\!]/(f_j, g_k),$$

is finite-dimensional. Therefore, any f_j and g_k are distinct irreducible elements.

Now consider the ring $k[\![x,y]\!][\frac{1}{T'}]$, it is regular of dimension 1, and a UFD. The elements f_i's are still irreducible in $k[\![x,y]\!][\frac{1}{T'}]$, since f_i's do not divide T'. By Chinese Remainder Theorem, we have the isomorphism

$$k[\![x,y]\!]\Big[\frac{1}{T'}\Big]/(f) \simeq \prod_{j\in J}\Big(k[\![x,y]\!]\Big[\frac{1}{T'}\Big]/(f_j^{e_j})\Big),$$

[1] When we work on the ring of formal power series, the distinction is always up to units.

in particular,

$$\widehat{\mathcal{O}}_{X,x_0} \otimes_{k\llbracket T\rrbracket} k(\!(T)\!) \;=\; \Big(k\llbracket x,y\rrbracket/(f)\Big) \otimes_{k\llbracket T\rrbracket} k(\!(T)\!) \;\simeq\; \prod_{j\in J}\Big(k\llbracket x,y\rrbracket/\big(f_j^{e_j}\big)\Big) \otimes_{k\llbracket T\rrbracket} k(\!(T)\!).$$

Thus we have the diagram

$$\begin{tikzcd}
\coprod_{j\in J} \operatorname{Spec}\Big(\Big(k\llbracket x,y\rrbracket/\big(f_j^{e_j}\big)\Big) \otimes_{k\llbracket T\rrbracket} k(\!(T)\!)\Big) \arrow[r, "\sim"] \arrow[dr] & \operatorname{Spec}\big(\widehat{\mathcal{O}}_{X,x_0} \otimes_{k\llbracket T\rrbracket} k(\!(T)\!)\big) \arrow[r, hook] \arrow[d] & X \arrow[d, "\phi"] \\
 & \operatorname{Spec}\big(\widehat{\mathcal{O}}_{Y,y_0} \otimes_{k\llbracket T\rrbracket} k(\!(T)\!)\big) \arrow[r, hook] & Y
\end{tikzcd}$$

By the condition (g), the morphism

$$\psi \times \operatorname{Spec}\big(k(\!(T)\!)\big) : \coprod_{i\in I} Z_i \times_Y \operatorname{Spec}\big(k(\!(T)\!)\big) \xrightarrow{\;\sim\;} X \times_Y \operatorname{Spec}\big(k(\!(T)\!)\big)$$

is an isomorphism. Thus we have

$$\begin{aligned}
\coprod_{j\in J} \operatorname{Spec}\Big(\Big(k\llbracket x,y\rrbracket/\big(f_j^{e_j}\big)\Big) \otimes_{k\llbracket T\rrbracket} k(\!(T)\!)\Big) \;&=\; X \times_Y \operatorname{Spec}\big(k(\!(T)\!)\big) \\
&\simeq\; \coprod_{i\in I} Z_i \times_Y \operatorname{Spec}\big(k(\!(T)\!)\big) \;=\; \coprod_{i\in I} \operatorname{Spec}\Big(\widehat{\mathcal{O}}_{Z_i,z_{i,0}} \otimes_{k\llbracket T\rrbracket} k(\!(T)\!)\Big)
\end{aligned}$$

where both sides are decompositions into connected components [2], therefore the index sets are in bijective correspondence, which we may just identify them. Now we have the isomorphisms

$$\widehat{\mathcal{O}}_{Z_i,z_{i,0}} \otimes_{k\llbracket T\rrbracket} k(\!(T)\!) \;\simeq\; \Big(k\llbracket x,y\rrbracket/\big(f_i^{e_i}\big)\Big) \otimes_{k\llbracket T\rrbracket} k(\!(T)\!) \tag{‡}$$

for all $i \in I$. It remains to extend these isomorphisms to $k\llbracket T\rrbracket$.

We want to show that the homomorphism

$$k\llbracket x,y\rrbracket/\big(\textstyle\prod_{i\in I} f_i^{e_i}\big) \;=\; \widehat{\mathcal{O}}_{X,x_0} \longrightarrow \widehat{\mathcal{O}}_{Z_i,z_{i,0}}$$

factors through the surjection

$$k\llbracket x,y\rrbracket/\big(\textstyle\prod_{i\in I} f_i^{e_i}\big) \twoheadrightarrow k\llbracket x,y\rrbracket/\big(f_i^{e_i}\big).$$

It is equivalent to show that the dashed arrow in the diagram vanishes:

$$\begin{tikzcd}
0 \arrow[r] & \ker(p) \arrow[r, hook] \arrow[dr, dotted] \arrow[ddr, "\text{vanishing}"'] & k\llbracket x,y\rrbracket/\big(\prod_{i\in I} f_i^{e_i}\big) \arrow[r, "p"] \arrow[d] & k\llbracket x,y\rrbracket/\big(f_i^{e_i}\big) \arrow[r] & 0 \\
 & & \widehat{\mathcal{O}}_{Z_i,z_{i,0}} \arrow[d, hook] & & \\
 & & \widehat{\mathcal{O}}_{Z_i,z_{i,0}} \otimes_{k\llbracket T\rrbracket} k(\!(T)\!). & &
\end{tikzcd}$$

[2] For the right side, by the condition that each $(Z_i)_{\text{red}}$ is a smooth curve over k.

This is clear, because of the isomorphism (‡), the homomorphism from $\mathrm{ker}(p)$ to $\widehat{\mathscr{O}}_{Z_i,z_{i,0}} \otimes_{k[\![T]\!]} k(\!(T)\!)$ vanishes, and by the flatness of $\widehat{\mathscr{O}}_{Z_i,z_{i,0}}$ over $k[\![T]\!]$, the bottom homomorphism is an inclusion. Thus we obtain a homomorphism

$$h\colon\ k[\![x,y]\!]/\big(f_i^{e_i}\big) \longrightarrow \widehat{\mathscr{O}}_{Z_i,z_{i,0}}.$$

Since $k[\![T]\!]$ is regular of dimension 1, $k[\![x,y]\!]/\big(f_i^{e_i}\big)$ is a Cohen-Macaulay $k[\![T]\!]$-module, hence $k[\![x,y]\!]/\big(f_i^{e_i}\big)$ is flat over $k[\![T]\!]$ [3], in particular, it is a free $k[\![T]\!]$-algebra. And we know that $h \otimes k(\!(T)\!)$ is an isomorphism, so h is injective. From the condition that each

$$\psi_i\colon\ Z_i \lhook\joinrel\longrightarrow X$$

is a closed immersion, and the diagram

$$\begin{tikzcd}
k[\![x,y]\!]/\big(\prod_{i\in I} f_i^{e_i}\big) \arrow[r, two heads] \arrow[dr, two heads] & k[\![x,y]\!]/\big(f_i^{e_i}\big) \arrow[d] \\
 & \widehat{\mathscr{O}}_{Z_i,z_{i,0}}
\end{tikzcd}$$

it is clear that h is also surjective, therefore it is an isomorphism.

The last assertion is straightforward, since each ψ'_i is finite flat, and for each supersingular point y_0 of Y, there is only one point $z_{i,0}$ lying over it. □

Theorem 6.1.2. *Let k be a perfect field of characteristic p, and $\mathscr{P}$ be a representable moduli problem over $\mathscr{M}_{1,1} \otimes k$ which is finite étale, such that all the supersingular points of $M(\mathscr{P})$ are k-rational. Denote $\mathscr{Y}$ for either of the four modular curves $\mathscr{Y}(p^n)$, $\mathscr{Y}_1(p^n)$, $\mathscr{Y}_1^{bal}(p^n)$ or $\mathscr{Y}_0(p^n)$. Then for any $n \geqslant 1$, the morphism*

$$\begin{tikzcd}
M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y} \arrow[d, "\pi"] \\
M(\mathscr{P})
\end{tikzcd}$$

satisfies the crossings conditions (a), (b) and (c).

Proof: The conditions (a) and (b) are contained in the Regularity Theorem 3.2.1. For the condition (c), we already proved that the complete local ring of $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}$ at a supersingular point x_0 (lying over a supersingular point $y_0 \in M(\mathscr{P})$) has the form

$$k[\![x,y]\!]/\mathfrak{a},$$

where $\mathfrak{a} \subset k[\![x,y]\!]$ is a proper ideal. Fix a formal parameter T of $M(\mathscr{P})$ at y_0, i.e., we have

$$\widehat{\mathscr{O}}_{M(\mathscr{P}),y_0} \simeq k[\![T]\!].$$

Then $k[\![x,y]\!]/\mathfrak{a}$ becomes a finite $k[\![T]\!]$-algebra which is noetherian and regular of dimension 1. Such a 1-dimensional noetherian regular local ring must have the form [4]

$$k[\![x,y]\!]/(f)$$

for some f contained in the maximal ideal $\mathfrak{m}$ of $k[\![x,y]\!]$ but not in $\mathfrak{m}^2$. This shows the condition (c). □

[3] cf. Altman-Kleiman [2] V. Proposition 3.5.

[4] cf. Liu [28] Chapter 4, Corollary 2.15.

6.2 Further discussion on p^n-isogenies

Recall that if E/S is an ordinary elliptic curve over a $\mathbb{F}_p$-scheme, then the relative Verschiebung $V_{E/S}$ is étale. The standard factorization of $[p^n]$ is

$$E \xrightarrow{F^n_{E/S}} E^{(p^n)} \xrightarrow{V^n_{E/S}} E.$$

The cyclic group scheme $\mathrm{ker}(V^n_{E/S})$ is finite étale on S, which is étale-locally isomorphic to the constant group scheme $\mathbb{Z}/p^n\mathbb{Z}$. Under the Cartier pairing [5], the cyclic group scheme $\mathrm{ker}(F^n_{E/S})$ is the Cartier dual of $\mathrm{ker}(V^n_{E/S})$, hence it is étale-locally isomorphic to μ_{p^n}.

Lemma 6.2.1. *Let $f : G \to H$ be a morphism of finite locally free commutative group schemes over an arbitrary scheme S. Suppose that H is étale over S, then there exists a finite étale locally free S-subgroup scheme $H' \subset H$, such that f factors through the inclusion*

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, dotted, two heads, "f'"'] & & H \\ & H' \arrow[ur, hook] & \end{tikzcd}$$

where f' is fppf surjective.

Proof: First of all, we make two claims:

(1) The condition "f is fppf surjective" is open and closed on S.

(2) The condition "$f = 0$" is open and closed on S.

Let $\mathscr{H}, \mathscr{G}$ be the $\mathscr{O}_S$-algebras corresponding to H, G. For the claim (1), we reduce to the case that S is noetherian. Now the condition is obviously open, which is given by the vanishing locus of the cokernel of the morphism:

$$\mathscr{H} \xrightarrow{f^*} \mathscr{G} \longrightarrow \mathrm{coker}\,(f^*) \longrightarrow 0.$$

For the closedness, we further reduce to the case that S is the spectrum of a complete noetherian local ring. In this case, we have the connected-étale exact sequence:

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

where G^0 is connected and $G^{\text{ét}}$ is étale. Since H is étale, the morphism f kills the connected component G^0, thus f is factorized as

$$f : G^{\text{ét}} \longrightarrow H.$$

Since then $G^{\text{ét}}$ and H are both étale-locally constant, the claim (1) follows from the same assertion for abstract abelian groups.

For the claim (2), the closedness is obvious, which is the zero set of all the entries of the matrix of the morphism f^*. For the openness, as in claim (1), we reduce to the case that S is the spectrum of

[5] cf. Definition 8.5.1.

a complete noetherian local ring, and the rest follows from the same assertion for abstract abelian groups.

Back to the lemma. The question is local, we may assume that H is constant. Moreover, we reduce to the case that S is noetherian and connected. Choose a geometric point $\mathsf{Spec}\ (\bar{k}) \to S$, and we consider the constant subgroup $H' \subset H$ such that $H'(\bar{k}) = \mathrm{im}(f(\bar{k}))$. Then the composition

$$\begin{tikzcd} G \arrow[r] & H \arrow[r] & H/H' \end{tikzcd}$$

is 0 at the chosen geometric point. By the claim (2), the above morphism is identically zero on S, which shows that f is factorized as

$$\begin{tikzcd} G \arrow[r, "f'"] & H' \arrow[r, hook] & H. \end{tikzcd}$$

And by the claim (1), f' is fppf surjective. □

Proposition 6.2.2. *Let E/S be an ordinary elliptic curve over a $\mathbb{F}_p$-scheme S, and $G \subset E$ be a finite locally free S-subgroup scheme of rank p^n. Then there exists a unique pair (a, b) of non-negative integers, with $a + b = n$, such that*

(1) $G \cap \mathit{ker}(F^n_{E/S}) = \mathit{ker}(F^a_{E/S})$;

(2) G mod $\mathit{ker}(F^a_{E/S})$ is a finite étale cyclic group scheme of order p^b.

Proof: By previous lemma, the morphism $F^n_{E/S}|_G$

$$\begin{tikzcd}
0 \arrow[r] & \mathsf{ker}\ (F^n_{E/S}) \arrow[r] & E[p^n] \arrow[r] & \mathsf{ker}\ (V^n_{E/S}) \arrow[r] & 0 \\
0 \arrow[r] & \mathsf{ker}\ (F^n_{E/S}|_G) \arrow[r] \arrow[u, hook] & G \arrow[u, hook] \arrow[ur, "F^n_{E/S}|_G"'] & &
\end{tikzcd}$$

maps G onto a finite étale S-subgroup scheme H' of $\mathsf{ker}(V^n_{E/S})$. Since the étale S-group scheme $\mathsf{ker}(V^n_{E/S})$ is étale-locally isomorphic to the constant group scheme $\mathbb{Z}/p^n\mathbb{Z}$, hence H' is also étale-locally isomorphic to $\mathbb{Z}/p^b\mathbb{Z}$ for some integer $b \geqslant 0$, which is nothing but

$$H' \ = \ \mathsf{ker}\left(V^b_{E^{(p^{n-b})}/S}\right).$$

In particular, the kernel of $F^n_{E/S}|_G$ is a finite locally free S-subgroup scheme of $\mathsf{ker}(F^n_{E/S})$. And étale-locally, $\mathsf{ker}(F^n_{E/S})$ is isomorphic to the group scheme μ_{p^n}, hence H' is also étale-locally isomorphic to μ_{p^a} for some integer $a \geqslant 0$, i.e.,

$$H' \ = \ G \cap \mathsf{ker}\ (F^n_{E/S}) \ = \ \mathsf{ker}\ (F^a_{E/S}).$$

By counting the ranks, we have $a + b = n$. □

Theorem 6.2.3. *Let $\phi : E \to E'$ be a p^n-isogeny of ordinary elliptic curves over a $\mathbb{F}_p$-scheme S. Then there exists a unique pair (a, b) of non-negative integers, such that we have the factorization of ϕ:*

$$\begin{tikzcd} E \arrow[r, "F^a_{E/S}"] & E^{(p^a)} \arrow[r, "\epsilon", "\sim"'] & E'^{(p^b)} \arrow[r, "V^b_{E'/S}"] & E', \end{tikzcd}$$

where the middle morphism ϵ is an isomorphism.

Proof: Let $G = \mathsf{ker}(\phi)$. By Proposition 6.2.2, there exists a unique pair (a,b) of non-negative integers, such that G contains $\mathsf{ker}(F^a_{E/S})$ as a subgroup scheme and the quotient is a twisted $\mathbb{Z}/p^b\mathbb{Z}$. The p^n-isogeny ϕ firstly is factorized as

$$\begin{tikzcd} E \arrow[r, "F^a_{E/S}"] & E^{(p^a)} \arrow[r, "\psi"] & E', \end{tikzcd}$$

where the kernel of the p^b-isogeny ψ is a twisted $\mathbb{Z}/p^b\mathbb{Z}$. By Cartier duality, the kernel of the dual isogeny ψ^t is a twisted μ_{p^b}, applying Proposition 6.2.2 to $\mathsf{ker}(\psi^t)$, we know that

$$\mathsf{ker}\,(\psi^t) = \mathsf{ker}\,(F^b_{E'/S}).$$

In particular, the p^b-isogenies ψ and $V^b_{E'/S}$ are differed by an isomorphism. □

Definition 6.2.4. *A p^n-isogeny $\phi : E \to E'$ of elliptic curves over a $\mathbb{F}_p$-scheme S is called a (a,b)-**isogeny**, if we have the following factorization*

$$\begin{tikzcd} E \arrow[r, "F^a_{E/S}"] & E^{(p^a)} \arrow[r, "\epsilon", "\sim"'] & E'^{(p^b)} \arrow[r, "V^b_{E'/S}"] & E'. \end{tikzcd}$$

Let X/S be any S-scheme, define $\mathsf{Inf}_d(\Delta_{X/S})$ to be the **d-th infinitesimal neighborhood of the diagonal**, which is the closed subscheme of $X \times_S X$ defined by the ideal sheaf $\mathscr{I}^d_{\Delta_{X/S}}$, where $\mathscr{I}_{\Delta_{X/S}}$ is the ideal sheaf of the diagonal $\Delta_{X/S}$.

Theorem 6.2.5. *Let k be a perfect field of characteristic p, and $\phi : E \to E'$ be a (a,b)-isogeny of elliptic curves over a k-scheme S. Let $\mathscr{P}$ be a representable moduli stack over $\mathscr{M}_{1,1} \otimes k$, which is finite étale, and represented by the k-scheme $M(\mathscr{P})$. And let α be a level $\mathscr{P}$ structure on E/S, denote*

$$\alpha_a = \alpha^{(p^a)} \in \mathscr{P}^{(\sigma^a)}\big(E^{(p^a)}/S\big).$$

There exists a unique level $\mathscr{P}^{(\sigma^{a-b})}$ level structure β on E'/S, such that

$$\beta^{(p^b)} = (\epsilon^{-1})^*(\alpha_a).$$

Let $x \in M(\mathscr{P})(S)$ and $y \in M\big(\mathscr{P}^{(\sigma^{a-b})}\big)(S)$ be the points that correspond to the isomorphism classes of $(E/S,\alpha)$ and $(E'/S,\beta)$ respectively. We denote by $F_k : M\big(\mathscr{P}^{(\sigma^i)}\big) \to M\big(\mathscr{P}^{(\sigma^{i+1})}\big)$ the Frobenius related to k. Then:

(1) $F^a_k(x) = F^b_k(y)$;

(2) Suppose $a,b > 0$. If $\big(F^{a-1}_k(x), F^{b-1}_k(y)\big)$ lies in $\mathsf{Inf}_{p-1}(\Delta_{X/S})$, then the (a,b)-isogeny ϕ is cyclic;

(3) Suppose $a,b > 0$. If E/S is ordinary, then $\big(F^{a-1}_k(x), F^{b-1}_k(y)\big)$ lies in $\mathsf{Inf}_{p-1}(\Delta_{X/S})$ if and only if the (a,b)-isogeny ϕ is cyclic;

(4) Suppose $a,b > 0$. If E/S is ordinary, and $j(E)(j(E)-1728)$ is invertible on S, then the (a,b)-isogeny ϕ is cyclic if and only if

$$\Big(j(E)^{p^{a-1}} - j(E')^{p^{b-1}}\Big)^{p-1} = 0.$$

Proof: (1) The point $F_k^a(x)$ represents the isomorphism class of $(E^{(p^a)}, \alpha_a)$, and the point $F_k^b(y)$ represents the isomorphism class of $(E'^{(p^b)}, \beta^{(p^b)})$, they are isomorphic by ϵ, hence $F_k^a(x) = F_k^b(y)$.

(2) We reduce to the universal case, i.e., the base scheme S is the pull-back of $\mathsf{Inf}_{p-1}(\Delta)$ along (F_k^{a-1}, F_k^{b-1}):

$$\begin{tikzcd}
S \arrow[r, "\text{finite flat}"] \arrow[d, hook] & \mathsf{Inf}_{p-1}(\Delta) \arrow[d, hook] \\
M(\mathscr{P}) \times_k M\big(\mathscr{P}^{(\sigma^{a-b})}\big) \arrow[r, "{(F_k^{a-1}, F_k^{b-1})}"] & M\big(\mathscr{P}^{(\sigma^{a-1})}\big) \times_k M\big(\mathscr{P}^{(\sigma^{a-1})}\big),
\end{tikzcd}$$

which is certainly finite flat over $\mathsf{Inf}_{p-1}(\Delta)$, hence finite flat over $M\big(\mathscr{P}^{(\sigma^{a-1})}\big)$. Thus the ordinary locus S^{ord} of S is open dense. By Lemma 4.2.2, the cyclicity is a closed condition, therefore (2) follows from (3).

(3) By Corollary 5.1.6, the elliptic curve E'/S is also ordinary. By Proposition 4.3.5, it is equivalent to show that the composable isogenies

$$E \xrightarrow{F^a_{E/S}} E^{(p^a)} \xrightarrow[\sim]{\epsilon} E'^{(p^b)} \xrightarrow{V^b_{E'/S}} E'$$

are cyclic in standard order. We further factorize it as the composition of $F_{E/S}$'s, ϵ and $V_{E'/S}$'s, by Theorem 4.3.11, it suffices to show the case for $a = b = 1$. Hence now what we need to prove is that, the $(1,1)$-isogeny ϕ is cyclic if and only if the point (x, y) lies in the $(p-1)$-th infinitesimal neighborhood $\mathsf{Inf}_{p-1}\big(\Delta_{M(\mathscr{P})}\big)$ of the diagonal.

Since we have $F_k(x) = F_k(y)$ from (1), the point (x, y) certainly lies in $\mathsf{Inf}_p\big(\Delta_{M(\mathscr{P})}\big)$. We reduce to the universal case, i.e., we assume that the base scheme S is $\mathsf{Inf}_p\big(\Delta_{M(\mathscr{P})}\big)$ itself. The assertion is equivalent to say that the closed subscheme $\mathsf{Inf}_{p-1}\big(\Delta_{M(\mathscr{P})}\big)$ is exactly the locus of cyclicity of ϕ. We know that the cyclicity is a closed condition on the base, hence the assertion amounts to verify an equality of two closed schemes of $\mathsf{Inf}_p\big(\Delta_{M(\mathscr{P})}\big)$, which by the standard reduction (cf. [37]), we can further reduce to the case that the base scheme S is the spectrum of an artinian local k-algebra R with maximal ideal $\mathfrak{m}_R$ and an algebraically closed residue field κ.

Over the residue field κ, we have an isomorphism $\epsilon \otimes \kappa$ between the two ordinary elliptic curves $E^{(p)} \otimes \kappa$ and $E'^{(p)} \otimes \kappa$. This implies

$$E \otimes \kappa \;\simeq\; E' \otimes \kappa,$$

since the isomorphism $\epsilon \otimes \kappa$ induces an isomorphism between $E[p](\kappa)$ and $E'[p](\kappa)$, which equal to $\ker(V_{E\otimes\kappa/\kappa})(\kappa)$ and $\ker(V_{E'\otimes\kappa/\kappa})(\kappa)$ respectively. By the uniqueness of β, the level structures α and β must be compatible over κ under the isomorphism between $E \otimes \kappa$ and $E' \otimes \kappa$. Thus $x = y$ over κ, we denote it by $(E_0/\kappa, \alpha_0)$.

We fix an isomorphism of p-divisible groups over κ:

$$E_0[p^\infty] \;\simeq\; \mu_{p^\infty} \times \mathbb{Q}_p/\mathbb{Z}_p.$$

Then there exist the Serre-Tate parameters (cf. 8.7)

$$q,\; q' \;\in\; 1 + \mathfrak{m}_R \;\subset\; R^\times$$

of E/R and E'/R respectively, i.e., we have isomorphisms of p-divisible groups over R:

$$\begin{aligned} E[p^\infty] &\simeq T[p^\infty]\otimes_{\mathbb{Z}[q,q^{-1}]}R \\ E'[p^\infty] &\simeq T[p^\infty]\otimes_{\mathbb{Z}[q',q'^{-1}]}R. \end{aligned}$$

The condition $F_k(x)=F_k(y)$ is saying $q^p=q'^p$, and what we need to prove is that $(q'-q)^{p-1}=0$ if and only if the $(1,1)$-isogeny ϕ is cyclic.

Let B be any R-algebra, such that $\mathsf{Spec}\,(B)$ is connected. Using the explicit expression of elements in $T[p^\infty]$ (cf. 8.7), the relative Frobenius on $E[p^\infty](B)$ is given by

$$\begin{aligned} F_{E/R}(B):\ E[p^\infty](B) &\longrightarrow E^{(p)}[p^\infty](B) \\ (X,\ a/p^n) &\longmapsto (X^p,\ a/p^n), \end{aligned}$$

and the relative Verschiebung is given by

$$\begin{aligned} V_{E'/R}(B):\ E'^{(p)}[p^\infty](B) &\longrightarrow E'[p^\infty](B) \\ (X,\ a/p^n) &\longmapsto (X,\ pa/p^n). \end{aligned}$$

Now let $B=R[Z]/(Z^p-q')$, it is a faithfully flat extension of R. The point $P=(Z,1/p)$ satisfies that $F_{E/S}(P)=(q',1/p)$ generates $\mathsf{ker}(V_{E'/R})$ over B. By the Standard Order Criterion 4.3.9, the isogeny ϕ is cyclic if and only if $pP=p(Z,1/p)=(q'/q,0)$ generates $\mathsf{ker}(F_{E/R})$ over B, i.e., q'/q generates $\mathsf{ker}(F_{E/S})\simeq\mu_p$. The latter condition is saying that q'/q is a primitive p-th root of unity, i.e.,

$$\Phi_p(q'/q)\ =\ \frac{(q'/q)^p-1}{q'/q-1}\ =\ (q'/q-1)^{p-1}\ =\ 0,$$

which is just $(q'-q)^{p-1}=0$.

(4) Similarly, we can reduce to the case $a=b=1$. In the case that $j(E)(j(E)-1728)$ is invertible on S, the following morphisms

$$\begin{tikzcd} M(\mathscr{P}) \arrow[r] \arrow[dr, "j"'] & \mathscr{M}_{1,1}\otimes k \arrow[d, "j"] \\ & \mathsf{Spec}\,(k[j]) \end{tikzcd}$$

are all étale (cf. Katz-Mazur [24] Corollary 8.4.5). Passing to the case that $S=\mathsf{Spec}\,(R)$, where R is an artinian local k-algebra with algebraically closed residue field. Then by (3), ϕ is cyclic if and only if (x,y) lies in $\mathsf{Inf}_{p-1}(\Delta_{M(\mathscr{P})})$, which is also equivalent to that the point $(j(x),j(y))$ lies in $\mathsf{Inf}_{p-1}(\Delta_{k[j]})$. The latter condition is exactly given by $(j(E)-j(E'))^{p-1}=0$. □

Let E/S be an elliptic curve over a $\mathbb{F}_p$-scheme S.

Definition 6.2.6. *A finite locally free S-subgroup scheme $G\subset E$ of rank p^n is called a (a,b)-**subgroup scheme**, where a,b are non-negative integers with $a+b=n$, if $\mathsf{ker}(F^a_{E/S})\subset G$, and in the following factorization*

$$E\xrightarrow{F^a_{E/S}}E^{(p^a)}\xrightarrow{\ \psi\ }E'=E/G$$

*we have $\mathsf{ker}(\psi^t)\simeq\mathsf{ker}(F^b_{E'/S})$. A (a,b)-subgroup scheme G is called (a,b)-**cyclic**, if either $ab=0$, or it satisfies the following condition:*

> *The two elliptic curves $E^{(p^{a-1})}$ and $E'^{(p^{b-1})}$ are infinitesimally near each other to order $p-1$, that is to say, there is a closed subscheme S' of S, which is defined by a nilpotent ideal sheaf $\mathscr{I}$ with $\mathscr{I}^{p-1}=0$, such that $E^{(p^{a-1})}$ and $E'^{(p^{b-1})}$ are isomorphic over S', and it induces the isomorphism between $E^{(p^a)}$ and $E'^{(p^b)}$ in the factorization.*

*In particular, a p^n-isogeny whose kernel is a (a,b)-subgroup scheme (resp. (a,b)-cyclic subgroup scheme) is called a (a,b)**-isogeny** (resp. (a,b)**-cyclic isogeny**).*

Remark: By Theorem 6.2.5, a (a,b)-subgroup scheme G being (a,b)-cyclic implies that the corresponding (a,b)-isogeny is cyclic. If E/S is ordinary, then the converse is also true. But in general they are not necessarily equivalent. [6]

6.3 Reduction mod p of $\mathscr{Y}_0(p^n)$

Let k be a perfect field of characteristic p, and E/S be an elliptic curve over a k-scheme S. Consider the moduli problem $\mathscr{Y}_0(a,b)$ over $\mathscr{M}_{1,1}\otimes k$ with $a,b\geqslant 0$, which is defined by

$$\mathscr{Y}_0(a,b)(E/S)=\big\{(a,b)\text{-subgroup schemes } G \text{ in } E/S\big\}.$$

There is a natural morphism from $\mathscr{Y}_0(a,b)$ to $\mathbf{Isog}(p^n)$ [7], which is given by forgetting (a,b).

Let $\mathscr{P}$ be a representable moduli stack over $\mathscr{M}_{1,1}\otimes k$, which is finite étale. It is obvious that we have the isomorphism

$$M(\mathscr{P})\times_{\mathscr{M}_{1,1}\otimes k}\mathscr{Y}_0(a,b)\ \simeq\ (F_k^a\times F_k^b)^{-1}\Big(\Delta_{M(\mathscr{P}^{(\sigma^a)})}\Big),$$

where $F_k^a\times F_k^b$ is the morphism

$$M(\mathscr{P})\times_k M\big(\mathscr{P}^{(\sigma^{a-b})}\big)\xrightarrow{F_k^a\times F_k^b}M\big(\mathscr{P}^{(\sigma^a)}\big)\times_k M\big(\mathscr{P}^{(\sigma^a)}\big).$$

Similarly, we define a moduli problem $\mathscr{Y}_0^{\mathrm{cyc}}(a,b)$ over $\mathscr{M}_{1,1}\otimes k$ as

$$\mathscr{Y}_0^{\mathrm{cyc}}(a,b)(E/S)=\left\{\begin{array}{l}(a,b)\text{-cyclic subgroup}\\ \text{schemes } G \text{ in } E/S\end{array}\right\}.$$

By Theorem 6.2.5, we have an isomorphism

$$M(\mathscr{P})\times_{\mathscr{M}_{1,1}}\mathscr{Y}_0^{\mathrm{cyc}}(a,b)\ \simeq\ \big(F_k^{a-1}\times F_k^{b-1}\big)^{-1}\Big(\mathsf{Inf}_{p-1}\Big(\Delta_{M(\mathscr{P}^{(\sigma^{a-1})})}\Big)\Big).$$

The morphism given by forgetting (a,b)

$$M(\mathscr{P})\times_{\mathscr{M}_{1,1}}\mathscr{Y}_0^{\mathrm{cyc}}(a,b)\ \longrightarrow\ M(\mathscr{P})\times_{\mathscr{M}_{1,1}}\mathscr{Y}_0(p^n)$$

is a closed immersion. Over any perfect k-algebra B, the morphism

$$M(\mathscr{P})\times_{\mathscr{M}_{1,1}}\mathscr{Y}_0^{\mathrm{cyc}}(a,b)\ \longrightarrow\ M(\mathscr{P})$$

is bijective on B-valued points.

[6] See the remark in the end of the next section.

[7] cf. Section 4.2.

Theorem 6.3.1. *Hypotheses and notations as above. The finite flat $M(\mathscr{P})$-scheme*

$$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_0(p^n)$$

is the disjoint union of the $n+1$ $M(\mathscr{P})$-schemes

$$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_0^{cyc}(a,b)$$

for $a+b=n$, with crossings at supersingular points. The complete local ring of each supersingular point of $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_0(p^n)$ is isomorphic to

$$k[\![x,y]\!] \Big/ (x-y^{p^n})(x^{p^n}-y)\Big(\prod_{a,b>0,a+b=n} (x^{p^{a-1}}-y^{p^{b-1}})^{p-1}\Big),$$

and in this complete local ring, each $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_0^{cyc}(a,b)$ is defined by the single equation

$$\begin{cases} (x^{p^{a-1}}-y^{p^{b-1}})^{p-1} & \text{if } a,b>0 \\ x^{p^a}=y^{p^b} & \text{if } (a,b)=(n,0) \text{ or } (0,n). \end{cases}$$

Proof: By Theorem 6.1.2, the crossings conditions (a), (b) and (c) are satisfied. And by our previous discussion, the conditions (d)-(g) also hold. Therefore the first assertion follows from the Crossings Theorem 6.1.1. The last assertion follows from Theorem 6.2.5. □

Remark: A cyclic p^n-isogeny which is also a (a,b)-isogeny does not imply that it is (a,b)-cyclic, in other words, the commutative diagram

$$\begin{tikzcd}
\mathscr{Y}_0^{\mathrm{cyc}}(a,b) \arrow[r, hook] \arrow[d, hook] & \mathscr{Y}_0(a,b) \arrow[d, hook] \\
\mathscr{Y}_0(p^n) \arrow[r, hook] & \mathbf{Isog}(p^n)
\end{tikzcd}$$

is not cartesian. In fact the diagram is not cartesian near the supersingular point, i.e., we may check it on the complete local rings at supersingular points. Consider the simplest case $a=b=1$. Pick any auxiliary representable moduli stack $\mathscr{P}$ which is finite étale over $\mathscr{M}_{1,1}\otimes k$. The complete local ring of $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_0^{\mathrm{cyc}}(1,1)$ is isomorphic to

$$k[\![x,y]\!]/(x-y)^{p-1},$$

and the complete local ring of the fiber product of $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_0(1,1)$ and $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_0(p^n)$ over $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{Isog}(p^n)$ is isomorphic to

$$k[\![x,y]\!] \Big/ \Big(x^p-y^p, (x-y^{p^2})(x^{p^2}-y)(x-y)^{p-1}\Big),$$

which is obviously not isomorphic to $k[\![x,y]\!]/(x-y)^{p-1}$.

6.4 Reduction mod p of $\mathscr{Y}_1(p^n)$

Proposition 6.4.1. *Let $\phi: E \to E'$ be a (a,b)-cyclic isogeny of elliptic curves over a $\mathbb{F}_p$-scheme S. Then the corresponding factorization*

$$E \xrightarrow{F^a_{E/S}} E^{(p^a)} \xrightarrow{\sim} E'^{(p^b)} \xrightarrow{V^b_{E'/S}} E'$$

is cyclic in standard order, with respect to the divisor p^a of p^n.

Proof: Pick an auxiliary representable moduli stack $\mathscr{P}$ which is finite étale over $\mathscr{M}_{1,1} \otimes \mathbb{F}_p$, e.g., $\mathscr{P} = \mathscr{Y}(\ell) \otimes \mathbb{F}_p$ for some prime $\ell \neq p$. Then we may reduce to the universal case, i.e., let

$$S \;=\; M(\mathscr{P}) \times_{\mathscr{M}_{1,1} \otimes \mathbb{F}_p} \mathscr{Y}_0^{\mathrm{cyc}}(a,b),$$

which is finite flat over $M(\mathscr{P})$. We need to compare the group scheme $\ker(F^a_{E/S})$ with the standard cyclic subgroup scheme of $\ker(\phi)$ of order p^a, which is a closed condition on the base. Over the ordinary locus $M(\mathscr{P})^{\mathrm{ord}}$, which is open dense in $M(\mathscr{P})$, the relative Verschiebung $V^b_{E'/S}$ is étale, hence by Proposition 4.3.5, the factorization is cyclic in standard order. Thus $\ker(F^a_{E/S})$ is equal to the standard cyclic subgroup scheme of $\ker(\phi)$ of order p^a over $M(\mathscr{P})^{\mathrm{ord}}$, which implies the equality over $M(\mathscr{P})$. □

Consider the moduli problem $\mathscr{Y}_1^{\mathrm{cyc}}(a,b)$, with $a+b=n$ and $a,b \geqslant 0$, which is defined by

$$\mathscr{Y}_1^{\mathrm{cyc}}(a,b)(E/S) \;=\; \left\{ \begin{array}{l} \text{all the points } P \text{ of exact order } p^n, \\ \text{which generates a } (a,b)\text{-cyclic} \\ \text{subgroup scheme of } E/S \end{array} \right\}.$$

These moduli problems are “components” of the reduction mod p of $\mathscr{Y}_1(p^n)$.

Let k be a perfect field of characteristic p, and we pick an auxiliary representable moduli stack $\mathscr{P}$ which is finite étale over $\mathscr{M}_{1,1} \otimes k$. We will see that the fiber product $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_1^{\mathrm{cyc}}(a,b)$ is represented by a finite flat $M(\mathscr{P})$-scheme. Let us divide it into three cases:

Case $(a,b) = (n,0)$:

It is represented by the finite flat $M(\mathscr{P})$-scheme $\left(\ker\left(F^n_{\mathbf{E}(\mathscr{P})/M(\mathscr{P})}\right)\right)^{\times}$, where $\mathbf{E}(\mathscr{P})$ is the universal elliptic curve over $M(\mathscr{P})$. It is exactly the $\varphi(p^n)$-th infinitesimal neighborhood of the zero section, i.e.,

$$\left(\ker\left(F^n_{\mathbf{E}(\mathscr{P})/M(\mathscr{P})}\right)\right)^{\times} \;=\; M(\mathscr{P}) \otimes_k \left(k[X]/\left(X^{\varphi(p^n)}\right)\right).$$

Case $(a,b) = (0,n)$:

It is represented by the finite flat $M(\mathscr{P})$-scheme

$$M\left(\mathscr{P}^{(\sigma^{-n})}\right) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{Ig}(p^n) \;\simeq\; M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{ExIg}(p^n, n).$$

Case $a,b \geqslant 1$:

Let $\mathbf{E}$ be the universal elliptic curve over the moduli scheme

$$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_0^{\mathrm{cyc}}(a,b),$$

and $\mathbf{G}$ be the universal (a,b)-cyclic subgroup scheme of $\mathbf{E}$. Then the fiber product $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_1^{\mathrm{cyc}}(a,b)$ is represented by $\mathbf{G}^{\times}$, which is finite flat over $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_0^{\mathrm{cyc}}(a,b)$. Since $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_0^{\mathrm{cyc}}(a,b)$ is finite flat over $M(\mathscr{P})$, hence $\mathbf{G}^{\times}$ is finite flat over $M(\mathscr{P})$.

Theorem 6.4.2. *Hypotheses and notations as above. The finite flat $M(\mathscr{P})$-scheme*

$$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_1(p^n)$$

is the disjoint union of the $n+1$ $M(\mathscr{P})$-schemes

$$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_1^{\mathrm{cyc}}(a,b)$$

for $a+b=n$, with crossings at supersingular points.

Proof: The crossings conditions (a), (b), (c) follows from Theorem 6.1.2, and the conditions (e), (f) and (g) are straightforward.

To show the condition (d), we analyze each case.

Case $(a,b)=(n,0)$:

In this case, $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_1^{\mathrm{cyc}}(n,0)$ is represented by the $M(\mathscr{P})$-scheme

$$M(\mathscr{P}) \otimes_k \left(k[X]/\left(X^{\varphi(p^n)}\right)\right),$$

whose associated reduced scheme is just $M(\mathscr{P})$ itself, hence a smooth curve.

Case $(a,b)=(0,n)$:

In this case, $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_1^{\mathrm{cyc}}(0,n)$ is represented by

$$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{ExIg}(p^n,n).$$

We know that the exotic Igusa moduli stack $\mathbf{ExIg}(p^n,n)$ is isomorphic to $\mathbf{Ig}(p^n)$, hence by Theorem 5.2.2, it is regular of dimension 1. This implies that $\mathbf{ExIg}(p^n,n)$ is smooth, since our ground field k is perfect. Therefore $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{ExIg}(p^n,n)$ is reduced, and it is a smooth curve.

Case $a,b \geqslant 1$:

In this case, $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_1^{\mathrm{cyc}}(a,b)$ is represented by $\mathbf{G}^\times$, the scheme of generators of the universal (a,b)-cyclic subgroup scheme of the universal elliptic curve $\mathbf{E}$ over $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_0^{\mathrm{cyc}}(a,b)$. Let $\mathbf{E}'$ be the universal quotient of $\mathbf{E}$ by $\mathbf{G}$. Observe that we have the following morphisms

$$\mathbf{G}^\times \xrightarrow[\mathsf{deg}=p^a]{F^a_{\mathbf{E}/(\ldots)}} \left(\mathsf{ker}\left(V^b_{\mathbf{E}'/(\ldots)}\right)\right)^\times \xrightarrow[\mathsf{deg}=\varphi(p^b)]{} M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_0^{\mathrm{cyc}}(a,b),$$

where $F^a_{\mathbf{E}/(\ldots)}$ is purely inseparable. Since $\left(\mathsf{ker}\left(V^b_{\mathbf{E}'/(\ldots)}\right)\right)^\times$ is nothing but

$$\mathbf{Ig}(p^b) \times_{\mathscr{M}_{1,1}\otimes k,\mathbf{E}} \left(M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_0^{\mathrm{cyc}}(a,b)\right),$$

and that the associated reduce scheme of $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_0^{\mathrm{cyc}}(a,b)$ is a smooth curve, hence the associated reduced scheme of $\left(\mathsf{ker}\left(V^b_{\mathbf{E}'/(\ldots)}\right)\right)^\times$ is a smooth curve.

Therefore, applying the Crossings Theorem 6.1.1, we obtain the result. □

6.5 Reduction mod p of $\mathscr{Y}^{\mathbf{can}}(p^n)$

Let k be a field of characteristic p, and E/S an elliptic curve over a k-scheme S. Recall that given a Drinfeld p^n-basis (P,Q) of E/S, by Theorem 3.3.5, the determinant $e_{p^n}(P,Q)$ is a primitive p^n-th root of unity.

We define a moduli substack $\mathscr{Y}^{\mathrm{can}}(N)$ of $\mathscr{Y}(N)$, who classifies all triples $(E/S,P,Q)$, where (P,Q) is a Drinfeld N-basis of E/S such that the determinant $e_N(P,Q)=\zeta_N$. Now let N be a prime power p^n. If the base scheme S of an object $(E/S,P,Q)$ of $\mathscr{Y}^{\mathrm{can}}(p^n)$ is naturally defined over a field k of characteristic p, then necessarily $e_{p^n}(P,Q)=1$.

Let k be a field of characteristic p. In fact, the moduli stack $\mathscr{Y}^{\mathrm{can}}(p^n)\otimes k$ is the associated reduced stack of $\mathscr{Y}(p^n)\otimes k$. Let S be a reduced k-scheme, and given a morphism $S\to\mathscr{Y}(p^n)\otimes k$, which is also an object $(E/S,P,Q)$ of $\mathscr{Y}(p^n)\otimes k$, then it factors through the closed immersion

$$\begin{tikzcd}
\mathscr{Y}^{\mathrm{can}}(p^n)\otimes k \arrow[r, hook] & \mathscr{Y}(p^n)\otimes k \\
S \arrow[u, dotted] \arrow[ur, "{(E/S,P,Q)}"']
\end{tikzcd}$$

simply because S is reduced, and we always have $e_{p^n}(P,Q)=1$. It remains to see that $\mathscr{Y}^{\mathrm{can}}(p^n)\otimes k$ is reduced. This will be clear after we analyze the reduction mod p of the moduli stack $\mathscr{Y}^{\mathrm{can}}(p^n)$.

Consider an ordinary elliptic curve E/S over a connected $\mathbb{F}_p$-scheme S, and let

$$\phi\colon\ (\mathbb{Z}/p^n\mathbb{Z})^2 \longrightarrow E[p^n]$$

be a $\Gamma(p^n)$-structure on E/S. It induces the diagram

$$\begin{tikzcd}
0 \arrow[r] & \ker(\Lambda) \arrow[r] \arrow[d, "\phi|_{\ker(\Lambda)}"] & (\mathbb{Z}/p^n\mathbb{Z})^2 \arrow[r] \arrow[d, "\phi"] \arrow[dr, "\Lambda"] & \operatorname{coker}(\Lambda) \arrow[r] \arrow[d, "\phi|_{\operatorname{coker}(\Lambda)}", "\wr"'] & 0 \\
0 \arrow[r] & \ker(F^n_{E/S}) \arrow[r] & E[p^n] \arrow[r, "F^n_{E/S}"] & \ker(V^n_{E/S}) \arrow[r] & 0
\end{tikzcd}$$

where $\Lambda=F^n_{E/S}\circ\phi$, and it is clear that both $\ker(\Lambda)$ and $\operatorname{coker}(\Lambda)$ are cyclic groups of order $\mathbb{Z}/p^n\mathbb{Z}$. Since in this case $\ker(V^n_{E/S})$ is étale, by Proposition 2.4.1, the left and right sides vertical morphisms are generators, and $\phi|_{\operatorname{coker}(\Lambda)}$ is an isomorphism of S-group schemes.

Lemma 6.5.1. *Hypotheses and notations as above. The $\Gamma(p^n)$-structure on E/S has determinant 1 if and only if $\phi|_{\ker(\Lambda)}=0$.*

Proof: Choose a basis (k_Λ,ℓ_Λ) of $(\mathbb{Z}/p^n\mathbb{Z})^2$, such that k_Λ is a $\mathbb{Z}/p^n\mathbb{Z}$-basis of $\ker(\Lambda)$, and ℓ_Λ projects to a $\mathbb{Z}/p^n\mathbb{Z}$-basis of $\operatorname{coker}(\Lambda)$. We know that $\Lambda(\ell_\Lambda)$ defines an isomorphism

$$\Lambda(\ell_\Lambda)\colon\ \mathbb{Z}/p^n\mathbb{Z}=\operatorname{coker}(\Lambda)\xrightarrow{\ \sim\ }\ker(V^n_{E/S}),$$

since $\ker(V^n_{E/S})$ is étale. The dual isomorphism is given by

$$\begin{array}{rcl}
\ker(F^n_{E/S}) & \longrightarrow & \mu_{p^n} \\
\zeta & \longmapsto & e_{p^n}\big(\zeta,\phi(\ell_\Lambda)\big).
\end{array}$$

Hence $\phi|_{\mathsf{ker}(\Lambda)} = 0$ if and only if $e_{p^n}\big(\phi(k_\Lambda), \phi(\ell_\Lambda)\big) = 1$, which is equivalent to $\det(\phi) = 1$. □

Once we choose a basis of $\mathsf{coker}(\Lambda)$, Λ defines an element in

$$\mathsf{Hom}^{\mathsf{surj}}\big((\mathbb{Z}/p^n\mathbb{Z})^2,\ \mathbb{Z}/p^n\mathbb{Z}\big),$$

i.e., all the surjective homomorphisms from $(\mathbb{Z}/p^n\mathbb{Z})^2$ to $\mathbb{Z}/p^n\mathbb{Z}$. Moreover, the class $[\Lambda]$ of Λ in

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \big\backslash \mathsf{Hom}^{\mathsf{surj}}\big((\mathbb{Z}/p^n\mathbb{Z})^2,\ \mathbb{Z}/p^n\mathbb{Z}\big)$$

is independent of the choice of a basis for $\mathsf{coker}(\Lambda)$, where $(\mathbb{Z}/p^n\mathbb{Z})^\times$ acts as the central subgroup of scalars of $GL(2, \mathbb{Z}/p^n\mathbb{Z})$.

Let $\mathscr{Y}^{[\Lambda]}(p^n)$ be the moduli stack who classifies all the pairs $(E/S, \ell_\Lambda)$, where ℓ_Λ is a basis for $\mathsf{coker}(\Lambda)$. We have seen that ℓ_Λ determines a Drinfeld p^n-basis $(0, \phi(\ell_\Lambda))$ on E/S, hence in other point of view, the moduli stack $\mathscr{Y}^{[\Lambda]}(p^n)$ also classifies all the pairs $(E/S, \phi)$, where ϕ is a $(\mathbb{Z}/p^n\mathbb{Z})^2$-structure on E/S such that $\phi|_{\mathsf{ker}(\Delta)} = 0$.

Lemma 6.5.2. *We have an isomorphism of moduli stacks*

$$\begin{array}{ccc} \mathscr{Y}^{[\Lambda]}(p^n) & \longrightarrow & \mathbf{ExIg}(p^n, n) \\ (E/S, \ell_\Lambda) & \longmapsto & (E/S, \phi(\ell_\Lambda)). \end{array}$$

Proof: It is straightforward. □

Theorem 6.5.3. *Let k be a perfect field of characteristic p, and $\mathscr{P}$ a representable moduli stack over $\mathscr{M}_{1,1} \otimes k$ which is finite étale. Then the finite flat $M(\mathscr{P})$-scheme*

$$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}^{can}(p^n)$$

is the disjoint union of the following $M(\mathscr{P})$-schemes:

$$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}^{[\Lambda]}(p^n)$$

for $[\Lambda] \in (\mathbb{Z}/p^n\mathbb{Z})^\times \backslash Hom^{surj}\big((\mathbb{Z}/p^n\mathbb{Z})^2,\ \mathbb{Z}/p^n\mathbb{Z}\big)$, with crossings at supersingular points.

Proof: The proof is straightforward, with help from Theorem 6.1.2. □

Remark: In particular, each component of $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}^{\mathrm{can}}(p^n)$

$$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}^{[\Lambda]}(p^n) \simeq M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{ExIg}(p^n, n)$$

is a reduced smooth curve, hence $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}^{\mathrm{can}}(p^n)$ is itself reduced. This ensures that $\mathscr{Y}^{\mathrm{can}}(p^n) \otimes k$ is the associated reduced stack of $\mathscr{Y}(p^n) \otimes k$.

Next let us compute the complete local ring of $\mathscr{Y}^{\mathrm{can}}(p^n)$ at supersingular points.

We choose a set of representatives of $(\mathbb{Z}/p^n\mathbb{Z})^\times \backslash \mathsf{Hom}^{\mathsf{surj}}\big((\mathbb{Z}/p^n\mathbb{Z})^2,\ \mathbb{Z}/p^n\mathbb{Z}\big)$:

$$\begin{cases} (1,\ -a) & a \in \mathbb{Z}/p^n\mathbb{Z} \\ (-pb,\ 1) & b \in \mathbb{Z}/p^{n-1}\mathbb{Z}. \end{cases}$$

Let $y_0 = (E_0/k, \alpha)$ be a supersingular point on $M(\mathscr{P})$, and x_0 the unique supersingular point on $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}^{\mathrm{can}}(p^n)$ that lies over y_0. The complete local ring of $M(\mathscr{P})$ at y_0 is isomorphic to $k[\![T]\!]$, let $\mathbf{E}_0/k[\![T]\!]$ be the universal formal deformation [8] of E_0/k. We choose a formal parameter X of $\widehat{\mathbf{E}}_0$, then the complete local ring of $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}^{\mathrm{can}}(p^n)$ at x_0 has the form (cf. Theorem 6.1.2)

$$k[\![x,y]\!]/(f),$$

where $x = X(P)$ and $y = X(Q)$ are coordinates of the universal Drinfeld p^n-basis (P,Q) with determinant 1 on $\mathbf{E}_0/k[\![T]\!]$.

The Drinfeld p^n-basis (P,Q) on $\mathbf{E}_0/k[\![T]\!]$ must satisfy the condition $\phi|_{\ker(\Lambda)} = 0$, where ϕ is the corresponding $(\mathbb{Z}/p^n\mathbb{Z})^2$-structure on $\mathbf{E}_0/k[\![T]\!]$, or equivalently:

$$\begin{cases} P = aQ & \text{if } \Lambda \sim (1,\ -a) \\ pbP = Q & \text{if } \Lambda \sim (-pb,\ 1). \end{cases}$$

In terms of the coordinates x, y of P, Q in formal group, let $\tilde{a}, \tilde{b}$ be representatives of a, b in $\mathbb{Z}_p$, then the conditions are read as

$$\begin{cases} x = [\tilde{a}](y) & \text{if } \Lambda \sim (1,\ -a) \\ y = [p\tilde{b}](x) & \text{if } \Lambda \sim (-pb,\ 1). \end{cases}$$

Theorem 6.5.4. *Hypotheses and notations as above. Let y_0 be a k-rational supersingular point on $M(\mathscr{P})$, and x_0 the unique k-rational supersingular point on $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}^{can}(p^n)$ that lies over y_0. Then the complete local ring of $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}^{can}(p^n)$ at x_0 is isomorphic to*

$$k[\![x,y]\!]\Big/\Big(\prod_{a\in\mathbb{Z}/p^n\mathbb{Z}} \big(x - [\tilde{a}](y)\big) \prod_{b\in\mathbb{Z}/p^{n-1}\mathbb{Z}} \big(y - [p\tilde{b}](x)\big)\Big),$$

and in this complete local ring, each $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}^{[\Lambda]}(p^n)$ is defined by the single equation

$$\begin{cases} x - [\tilde{a}](y) = 0 & \textit{if } \Lambda \sim (1,\ -a) \\ y - [p\tilde{b}](x) = 0 & \textit{if } \Lambda \sim (-pb,\ 1). \end{cases}$$

Proof: We already know that the complete local ring of $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}^{\mathrm{can}}(p^n)$ at x_0 has the form

$$k[\![x,y]\!]/(f).$$

As we discussed above, each $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}^{[\Lambda]}(p^n)$ in this complete local ring is defined by the single equation

$$\begin{cases} x - [\tilde{a}](y) = 0 & \text{if } \Lambda \sim (1,\ -a) \\ y - [p\tilde{b}](x) = 0 & \text{if } \Lambda \sim (-pb,\ 1) \end{cases}$$

hence their complete local rings are

$$\begin{cases} k[\![x,y]\!]/\big(f,\ x - [\tilde{a}](y)\big) & \text{if } \Lambda \sim (1,\ -a) \\ k[\![x,y]\!]/\big(f,\ y - [p\tilde{b}](x)\big) & \text{if } \Lambda \sim (-pb,\ 1) \end{cases}$$

But as the complete local ring of a smooth curve, we have the isomorphisms

$$\begin{cases} k[\![x,y]\!]/\big(f,\ x - [\tilde{a}](y)\big) \simeq k[\![y]\!] \\ k[\![x,y]\!]/\big(f,\ y - [p\tilde{b}](x)\big) \simeq k[\![x]\!] \end{cases}$$

[8] To artinian local k-algebras with residue field k.

therefore $f \in \big(x - [\widetilde{a}](y)\big)$ (resp. $f \in \big(y - [p\widetilde{b}](x)\big)$), i.e., the complete local ring of each $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}^{[\Lambda]}(p^n)$ at the supersingular point is isomorphic to

$$\begin{cases} k[\![x,y]\!]/\big(x - [\widetilde{a}](y)\big) & \text{if } \Lambda \sim (1,\ -a) \\ k[\![x,y]\!]/\big(y - [p\widetilde{b}](x)\big) & \text{if } \Lambda \sim (-pb,\ 1). \end{cases}$$

By the Crossings Theorem 6.1.1, the complete local ring of $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}^{\mathrm{can}}(p^n)$ at x_0 is

$$k[\![x,y]\!]\Big/\Big(\prod_{a\in\mathbb{Z}/p^n\mathbb{Z}} \big(x - [\widetilde{a}](y)\big) \prod_{b\in\mathbb{Z}/p^{n-1}\mathbb{Z}} \big(y - [p\widetilde{b}](x)\big)\Big). \qquad \square$$

6.6 Reduction mod p of $\mathscr{Y}_1^{\mathbf{bal,can}}(p^n)$

Similar as the situation of the modular curve $\mathscr{Y}(N)$, for the case of $\mathscr{Y}_1^{\mathrm{bal}}(N)$, we define the moduli substack $\mathscr{Y}_1^{\mathrm{bal,can}}(N)$, who classifies all the dual pairs of cyclic N-isogenies

$$\begin{tikzcd} E \arrow[r, "\phi"] & E' \arrow[r, "\phi^t"] & E \end{tikzcd}$$

with specified generators P, Q of $\ker(\phi)$ and $\ker(\phi^t)$ respectively, such that $< P, Q >_\phi = \zeta_N$.

Let N be a prime power p^n. When the elliptic curve is defined over a field of characteristic p, then the condition becomes $< P, Q >_\phi = 1$.

Theorem 6.6.1. *Let*

$$\begin{tikzcd} E \arrow[r, shift left, "\phi"] & E' \arrow[l, shift left, "\phi^t"] \end{tikzcd}$$

be a dual pair of cyclic p^n-isogenies of ordinary elliptic curves over a connected $\mathbb{F}_p$-scheme S, with specified generators P, Q of ker(ϕ) and ker(ϕ^t) respectively, such that $< P, Q >_\phi = 1$. Then

(1) There exists a pair (a, b) of non-negative integers with $a + b = n$, such that ϕ is (a, b)-cyclic and ϕ^t is (b, a)-cyclic;

(2) $p^b P = 0$, and $(0, P)$ is a Drinfeld p^b-basis for E/S. The point P generates a $\mathbb{Z}/p^b\mathbb{Z}$ in E, we denote the quotient by E_*. Then $E \simeq E_*^{(p^b)}$;

(3) $p^a Q = 0$, and $(0, Q)$ is a Drinfeld p^a-basis for E'/S. The point P generates a $\mathbb{Z}/p^a\mathbb{Z}$ in E', we denote the quotient by E_{**}. Then $E' \simeq E_{**}^{(p^a)}$;

(4) The standard factorization of ϕ with respect to the divisor p^a of p^n, is

$$\begin{tikzcd} E_*^{(p^b)} \arrow[r, shift left, "F^a"] & E_*^{(p^n)} \arrow[l, shift left, "V^a"] \arrow[r, shift left, "V^b"] & E_*^{(p^a)} \arrow[l, shift left, "F^b"] \end{tikzcd};$$

(5) We have a unique isomorphism $E_* \simeq E_{**}$, such that the diagram

$$\begin{tikzcd}
 & & E_* \simeq E_{**} \arrow[rrd, "F^a_{E_{**}/S}"] & & \\
E_*^{(p^b)} \arrow[rru, "V^b_{E_*/S}"] & E \arrow[l, "\sim"'] \arrow[rr, bend left, "\phi"] & & E' \arrow[r, "\sim"] \arrow[ll, bend left, "\phi^t"] & E_{**}^{(p^a)} \arrow[lld, "V^a_{E_{**}/S}"] \\
 & & E_* \simeq E_{**} \arrow[llu, "F^b_{E_*/S}"] & &
\end{tikzcd}$$

commutes.

(6) The point $P \in E_*^{(p^b)}(S)$ is an Igusa level p^b structure on E_*/S, and the point $Q \in E_*^{(p^a)}(S)$ is an Igusa level p^a structure on E_*/S;

(7) If $a \geqslant b$, then there exists a unique unit $u \in (\mathbb{Z}/p^b\mathbb{Z})^\times$ such that

$$V^{a-b}_{E_*/S}(Q) \;=\; u \cdot P \quad \text{in } E_*^{(p^b)}.$$

If $a < b$, then there exists a unique unit $u \in (\mathbb{Z}/p^a\mathbb{Z})^\times$ such that

$$Q \;=\; u \cdot V^{a-b}_{E_*/S}(P) \quad \text{in } E_*^{(p^a)}.$$

Proof: (1) This is by Theorem 6.2.3.

(2) Applying the Standard Order Criterion to the standard factorizations of the p^n-isogenies ϕ and ϕ^t:

$$\begin{tikzcd}
E \arrow[r, shift left, "F^a_{E/S}"] & E^{(p^a)} \arrow[l, shift left, "V^a_{E/S}"] \simeq E'^{(p^b)} \arrow[r, shift left, "V^b_{E'/S}"] & E', \arrow[l, shift left, "F^b_{E'/S}"]
\end{tikzcd}$$

we know that p^bP generates $\ker(F^a_{E/S})$, and $F^b_{E'/S}(Q)$ generates $\ker(V^a_{E'/S})$. Moreover, we have (cf. Lemma 8.5.3)

$$< p^bP,\, F^b_{E'/S}(Q) >_{F^a_{E/S}} \;=\; \big(< P,\, F^b_{E'/S}(Q) >_{F^a_{E/S}}\big)^{p^b} \;=\; \big(< P,\, Q >_\phi\big)^{p^b} \;=\; 1.$$

Since $\ker(V^a_{E'/S})$ is étale, the generator $F^b_{E'/S}(Q)$ defines an isomorphism

$$F^b_{E'/S}(Q) :\; \mathbb{Z}/p^a\mathbb{Z} \longrightarrow \ker(V^a_{E'/S}),$$

which induces the dual isomorphism

$$\begin{array}{ccc}
\ker\,(F^a_{E/S}) & \longrightarrow & \mu_{p^a} \\
\zeta & \longmapsto & <\zeta,\, F^b_{E'/S}(Q) >_{F^a_{E/S}}.
\end{array}$$

Hence $< p^bP,\, F^b_{E'/S}(Q) >_{F^a_{E/S}} = 1$ implies that $p^bP = 0$. Now the point P defines a homomorphism

$$P :\; \mathbb{Z}/p^b\mathbb{Z} \longrightarrow E,$$

we need to show that it is a closed immersion of S-group schemes, i.e., the point P has exact order p^b in the naïve sense. By the Backing-Up Theorem 4.3.8, we know that $F^a_{E/S}(P)$ generates the finite étale group scheme $\ker(V^b_{E'/S})$ of rank p^b, hence $F^a_{E/S}(P)$ has exact order p^b in the naïve sense, which implies that P also has exact order p^b in the naïve sense. This proves the closed immersion of $\mathbb{Z}/p^b\mathbb{Z}$ into E/S defined by P.

Next we show that $(0,P)$ is a Drinfeld p^b-basis of E/S. The closed immersion

$$P:\ \mathbb{Z}/p^b\mathbb{Z}\ \longrightarrow\ E[p^b]$$

provides a splitting of the exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \ker\,(F^b_{E/S}) \arrow[r] & E[p^b] \arrow[r, "F^b_{E/S}"] & \ker\,(V^b_{E/S}) \arrow[r] & 0 \\
& & \mathbb{Z}/p^b\mathbb{Z} \arrow[u, "P"] \arrow[ur, "\sim"'] & &
\end{tikzcd}$$

this is because the kernel of $F^b_{E/S}\circ P$ (which is étale) intersects with $\ker(F^b_{E/S})$ only at the zero section, so $F^b_{E/S}\circ P$ defines an isomorphism between $\mathbb{Z}/p^b\mathbb{Z}$ and $\ker(V^b_{E/S})$. Thus we have

$$E[p^b]\ \simeq\ \ker\,(F^b_{E/S})\oplus\mathbb{Z}/p^b\mathbb{Z},$$

and now it is clear that $(0,P)$ is a Drinfeld p^b-basis of E/S, since 0 generates $\ker(F^b_{E/S})$.

Let E_* be the quotient of E by the cyclic subgroup $\mathbb{Z}/p^b\mathbb{Z}$ generated by P. The splitting tells us that we have a (non-standard) factorization of $[p^b]$:

$$\begin{tikzcd}
E \arrow[r] & E_* \arrow[r, "F^b_{E/S}"] & E,
\end{tikzcd}$$

hence it is obvious that $E\simeq E_*^{(p^b)}$.

(3) This is the dual version of (2).

(4) It is obvious.

(5) Let us denote ψ for the isomorphism between $E^{(p^a)}$ and $E'^{(p^b)}$ composed with $V^b_{E'/S}$, i.e., we have the standard factorization of ϕ

$$\begin{tikzcd}
E \arrow[r, "F^a_{E/S}"] \arrow[rr, bend right, "\phi"'] & E^{(p^a)} \arrow[r, "\psi"] & E'.
\end{tikzcd}$$

Since P is a generator of $\ker(\phi)$, and it induces $F^a_{E/S}(P)$ as a generator of $\ker(\psi)$, hence we have the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}/p^a\mathbb{Z} \arrow[r] \arrow[d, "0"] & \mathbb{Z}/p^n\mathbb{Z} \arrow[r] \arrow[d, "P"] & \mathbb{Z}/p^b\mathbb{Z} \arrow[r] \arrow[d, "F^a_{E/S}(P)", "\wr"'] & 0 \\
0 \arrow[r] & \ker\,(F^a_{E/S}) \arrow[r] & \ker\,(\phi) \arrow[r, "F^a_{E/S}"] & \ker\,(\psi) \arrow[r] & 0
\end{tikzcd}$$

where the vertical morphisms are all generators, and the right side one is an isomorphism. From the diagram, we obtain a splitting

$$\ker\,(\phi)\ \simeq\ \ker\,(F^a_{E/S})\oplus\mathbb{Z}/p^b\mathbb{Z},$$

which induces a (non-standard) factorization of ϕ:

$$E \simeq E_*^{(p^b)} \xrightarrow{V^b_{E_*/S}} E_* \xrightarrow{F^a_{E_*/S}} E_*^{(p^a)}.$$

Thus we have $E' \simeq E_*^{(p^a)}$. On the other hand, in (3) we have proved that $E' \simeq E_{**}^{(p^a)}$, therefore

$$E_*^{(p^a)} \simeq E_{**}^{(p^a)}.$$

The kernel $\mathsf{ker}(V^a_{E_{**}/S})$ is exactly the $\mathbb{Z}/p^a\mathbb{Z}$ inside $E' \simeq E_{**}^{(p^a)}$ which is generated by Q. If we can prove that Q lies in $\mathsf{ker}(V^a_{E_*/S})$, then by the fact that Q has exact order p^a, we obtain the required isomorphism by taking the quotients:

$$E_* \simeq E_*^{(p^a)}\big/(\text{cyc. subgp generated by } Q) \longrightarrow E_{**}^{(p^a)}\big/(\text{cyc. subgp generated by } Q) \simeq E_{**}.$$

Thus our goal is to prove $V^a_{E_*/S}(Q) = 0$.

By passing to some fppf base change, we extend the $\Gamma_1^{\mathrm{bal}}(p^n)$-structure (P, Q) to a $\Gamma(p^n)$-structure $(P, \widetilde{Q})$, i.e., $(P, \widetilde{Q})$ is a Drinfeld p^n-basis of E/S, and $\phi(\widetilde{Q}) = Q$. By Theorem 6.5.4, we know that the condition for $(P, \widetilde{Q})$ is

$$\begin{cases} \widetilde{Q} = sP & s \in \mathbb{Z}/p^n\mathbb{Z} \\ P = pt\widetilde{Q} & t \in \mathbb{Z}/p^{n-1}\mathbb{Z} \end{cases}$$

In the first case, we have $Q = \phi(\widetilde{Q}) = \phi(sP) = 0$, which trivially implies $V^a_{E_*/S}(Q) = 0$. In the second case, after multiplying a unit in $\mathbb{Z}/p^n\mathbb{Z}$, we may assume that

$$P = p^\gamma \widetilde{Q}$$

for some $\gamma \geqslant 1$. Since $(p^\gamma\widetilde{Q}, \widetilde{Q})$ is a Drinfeld p^n-basis, hence so is $(0, \widetilde{Q})$, and $\widetilde{Q}$ has exact order p^n in the naïve sense (because E/S is ordinary). Therefore $P = p^\gamma\widetilde{Q}$ has exact order $p^{n-\gamma}$ in the naïve sense. But we already proved that P has exact order p^b in the naïve sense, so $\gamma = a$. Use the non-standard factorization of ϕ:

$$E \simeq E_*^{(p^b)} \xrightarrow{V^b_{E_*/S}} E_* \xrightarrow{F^a_{E_*/S}} E_*^{(p^a)} \simeq E',$$

we have

$$\begin{aligned} V^a_{E_*/S}(Q) &= V^a_{E_*/S}\big(\phi(\widetilde{Q})\big) \\ &= V^a_{E_*/S} \circ F^a_{E_*/S} \circ V^b_{E_*/S}(\widetilde{Q}) \\ &= V^b_{E_*/S}(p^a\widetilde{Q}) \\ &= V^b_{E_*/S}(P) = 0. \end{aligned}$$

(6) It is obvious, by construction.

(7) Both sides of points are generators of the finite étale group scheme $\mathsf{ker}\big(V^{\min(a,b)}_{E_*/S}\big)$, hence they are differed by a unique unit in $\mathbb{Z}/p^{\min(a,b)}\mathbb{Z}$. □

Theorem 6.6.2. *Let E/S be an elliptic curve over a $\mathbb{F}_p$-scheme, and (a,b) a pair of non-negative integers such that $a+b=n\geqslant 1$. We fix a unit u in $\mathbb{Z}/p^{min(a,b)}\mathbb{Z}$. Let $P\in E^{(p^b)}(S)$ and $Q\in E^{(p^a)}(S)$ be generators of $\mathrm{ker}(V^b_{E/S})$ and $\mathrm{ker}(V^a_{E/S})$ respectively, such that*

$$\begin{cases} V^{a-b}_{E/S}(Q)=u\cdot P & \text{if } a\geqslant b\\ Q=u\cdot V^{b-a}_{E/S}(P) & \text{if } a<b.\end{cases}$$

Then

(1) $\big(E^{(p^b)}/S,P,Q\big)$ is a $\Gamma_1^{bal}(p^n)$-structure for the dual pairs of isogenies

$$\begin{tikzcd} E^{(p^b)} \arrow[r, shift left, "F^a"] & E^{(p^n)} \arrow[l, shift left, "V^a"] \arrow[r, shift left, "V^b"] & E^{(p^a)} \arrow[l, shift left, "F^b"] \end{tikzcd}$$

with determinant 1.

(2) Let k be a perfect field of characteristic p, and $\mathscr{P}$ a representable moduli stack over $\mathscr{M}_{1,1}\otimes k$ which is finit étale. The construction defines a closed immersion

$$i^u_{(a,b)}:\ M(\mathscr{P})\times_{\mathscr{M}_{1,1}\otimes k}\mathbf{Ig}\big(p^{max(a,b)}\big)\hookrightarrow M\big(\mathscr{P}^{(\sigma^b)}\big)\times_{\mathscr{M}_{1,1}\otimes k}\mathscr{Y}_1^{bal,can}(p^n).$$

Proof: (1) Firstly, since P generates the kernel of the isogeny

$$V^b_{E/S}:\ E^{(p^b)}\longrightarrow E,$$

the point $F^a_{E/S}(P)=P^{(p^a)}$ must generate the kernel of

$$V^b_{E^{(p^a)}/S}:\ E^{(p^n)}\longrightarrow E^{(p^a)}.$$

Apply the Backing-Up Theorem 4.3.8 to the standard factorization:

$$E^{(p^b)}\xrightarrow{F^a}E^{(p^n)}\xrightarrow{V^b}E^{(p^a)},$$

we know that P generates the kernel of the isogeny $\phi=V^b\circ F^a$. Similarly, Q generates $\mathrm{ker}(\phi^t)$. So $\big(E^{(p^b)}/S,P,Q\big)$ is indeed a $\Gamma_1^{\mathrm{bal}}(p^n)$-structure of E/S. It remains to show that it has determinant 1.

Without loss of generality, we may assume $u=1$. By passing to some fppf base change, we assume that there exists $R\in E^{(p^n)}(S)$ such that

$$\begin{cases} V^a(R)=P & \text{if } a\leqslant b\\ V^b(R)=Q & \text{if } a>b\end{cases}$$

then automatically we have both $V^b(R)=Q$ and $V^a(R)=P$. Furthermore (also by some fppf base change) we assume that there exists $R'\in E^{(p^b)}(S)$ such that $F^a(R')=R$. Observe that

$$p^nR'\ =\ p^b\cdot V^a\circ F^a(R')\ =\ p^bP\ =\ F^b\circ V^b(P)\ =\ 0,$$

then use Corollary 8.5.5, we have

$$\begin{aligned} <P,\,Q>_\phi &= <V^a(R),\,V^b(R)>_{V^b\circ F^a}=<V^a(R),\,V^b\circ F^a(R')>_{V^b\circ F^a}\ =\ e_{p^n}(V^a(R),\,R')\\ &= e_{p^n}(R,\,F^a(R'))\ =\ e_{p^n}(R,\,R)\ =\ 1.\end{aligned}$$

(2) By (1) and Theorem 6.6.1, the morphism

$$i^u_{(a,b)} : M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{Ig}(p^{\max(a,b)}) \longrightarrow M\big(\mathscr{P}^{(\sigma^b)}\big) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_1^{\text{bal,can}}(p^n).$$

is well-defined. For example if $a \geqslant b$, given an object $(E/S, \alpha, Q)$ of $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{Ig}(p^a)$, where $\alpha \in \mathscr{P}(E/S)$ is a level $\mathscr{P}$ structure, it is mapped to

$$\big(E^{(p^b)}/S, \alpha^{(p^b)}, u^{-1}\cdot V^{a-b}(Q), Q\big) \in M\big(\mathscr{P}^{(\sigma^b)}\big) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_1^{\text{bal,can}}(p^n).$$

Since $i^u_{(a,b)}$ is a $M(\mathscr{P})$-morphism, both source and target are finite $M(\mathscr{P})$-schemes, hence it is proper. The injectivity of $i^u_{(a,b)}$ is clear, by passing to the exotic Igusa moduli stack: (again, suppose $a \geqslant b$)

$$\begin{tikzcd} M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{Ig}(p^a) \arrow[r, hook] \arrow[d, "\wr"] & M\big(\mathscr{P}^{(\sigma^b)}\big) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_1^{\text{bal,can}}(p^n) \\ M\big(\mathscr{P}^{(\sigma^b)}\big) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{ExIg}(p^a, b), & \end{tikzcd}$$

where the image of $(E/S, \alpha, Q)$ in $M\big(\mathscr{P}^{(\sigma^b)}\big) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{ExIg}(p^a, b)$ is just

$$\big(E^{(p^b)}/S, \alpha^{(p^b)}, u^{-1}\cdot V^{a-b}(Q), Q\big).$$ □

Theorem 6.6.3. *Let k be a perfect field of characteristic p, and $\mathscr{P}$ a representable moduli stack over $\mathscr{M}_{1,1}\otimes k$ which is finite étale. Then the $M(\mathscr{P})$-scheme*

$$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_1^{bal,can}(p^n)$$

is the disjoint union of the following $M(\mathscr{P})$-schemes:

$$\begin{tikzcd} M\big(\mathscr{P}^{(\sigma^{-b})}\big) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{Ig}(p^{max(a,b)}) \arrow[d, "p_b"] \\ M(\mathscr{P}) \end{tikzcd}$$

for each pair (a,b) of non-negative integers with $a+b=n$, and each unit $u \in (\mathbb{Z}/p^{min(a,b)}\mathbb{Z})^\times$, with crossings at suppersingular points.

Proof: It is straightforward. □

Remark: As we have seen, the moduli stack $\mathscr{Y}_1^{\text{bal,can}}(p^n)\otimes k$ is the associated reduced stack of $\mathscr{Y}_1^{\text{bal}}(p^n)\otimes k$, since each of its components is a reduced smooth curve.

6.7 Summary

In this section, we summarize the basic results of reduction mod p of four basic modular curves that we proved in previous sections. They all have the feature of "crossings at supersingular points", which we introduced in the first section of this chapter.

Let us fix a perfect field k of characteristic p, and an auxiliary representable moduli stack $\mathscr{P}$ over $\mathscr{M}_{1,1}\otimes k$, which is required to be finite étale over $\mathscr{M}_{1,1}\otimes k$.

$\boxed{\mathscr{Y}_0(p^n)}$

- **Components**: The components of $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_0(p^n)$ are
$$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_0^{\mathrm{cyc}}(a,b),$$
which are indexed by the pair (a,b) of non-negative integers with $a+b=n$. Hence there are totally $n+1$ components.
- **Underlying reduced curve of each component**: The $(n,0)$ component is reduced, which is isomorphic to $M(\mathscr{P})$ itself. The $(0,n)$ component is also reduced, which is isomorphic to $M(\mathscr{P})^{(\sigma^{-n})}$. In other cases, if $a \geqslant b$, the underlying reduced curve is isomorphic to $M(\mathscr{P})$; if $a<b$, the underlying reduced curve is isomorphic to $M(\mathscr{P})^{(\sigma^{a-b})}$.
- **Degree over** $M(\mathscr{P})$: The (a,b) component has rank p^b over $M(\mathscr{P})$.

$\boxed{\mathscr{Y}_1(p^n)}$

- **Components**: The components of $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_1(p^n)$ are
$$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_1^{\mathrm{cyc}}(a,b),$$
which are indexed by the pair (a,b) of non-negative integers with $a+b=n$. There are totally $n+1$ components.
- **Underlying reduced curve of each component**: The $(n,0)$ component is
$$M(\mathscr{P}) \otimes_k \Big(k[X]/\big(X^{\varphi(p^n)}\big)\Big),$$
its underlying reduced curve is $M(\mathscr{P})$. The $(0,n)$ component is
$$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{ExIg}(p^n,n),$$
which is already reduced. In other cases, the (a,b) component is not reduced, whose underlying reduced curve is
$$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{ExIg}(p^b,b).$$
- **Degree over** $M(\mathscr{P})$: The $(n,0)$ component has rank $\varphi(p^n)$ over $M(\mathscr{P})$. The $(0,n)$ component has rank $p^n\cdot\varphi(p^n)$ over $M(\mathscr{P})$. In other cases, the (a,b) component has rank $\varphi(p^n)\varphi(p^b)$ over $M(\mathscr{P})$.

$\boxed{\mathscr{Y}^{\mathrm{can}}(p^n)}$

- **Components**: The components of $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}^{\mathrm{can}}(p^n)$ are
$$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}^{[\Lambda]}(p^n),$$
which are indexed by elements in $(\mathbb{Z}/p^n\mathbb{Z})^\times \backslash \mathrm{Hom}^{\mathrm{surj}}\big((\mathbb{Z}/p^n\mathbb{Z})^2,\ \mathbb{Z}/p^n\mathbb{Z}\big)$. There are totally $\varphi(p^n)$ components.

- **Underlying reduced curve of each component**: Each component is isomorphic to

  $$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{ExIg}(p^n, n),$$

  which is already reduced.

- **Degree over** $M(\mathscr{P})$: The degree of each component over $M(\mathscr{P})$ is equal to the rank of the exotic Igusa moduli stack $\mathbf{ExIg}(p^n, n)$, which is $p^n \cdot \varphi(p^n)$.

$\boxed{\mathscr{Y}_1^{\mathrm{bal,can}}(p^n)}$

- **Components**: The components of $M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathscr{Y}_1^{\mathrm{bal,can}}(p^n)$ are

  $$M\big(\mathscr{P}^{(\sigma^{-b})}\big) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{Ig}\big(p^{\max(a,b)}\big),$$

  which are indexed by the pair (a,b) of non-negative integers with $a+b=n$, together with a unit $u \in \big(\mathbb{Z}/p^{\min(a,b)}\mathbb{Z}\big)^{\times}$. The number of components is

  $$p^{\lfloor \frac{n}{2} \rfloor} + p^{\lfloor \frac{n-1}{2} \rfloor} + 2.$$

- **Underlying reduced curve of each component**: The (a,b) component is isomorphic to

  $$M(\mathscr{P}) \times_{\mathscr{M}_{1,1}\otimes k} \mathbf{ExIg}\big(p^{\max(a,b)}, b\big),$$

  which is already reduced.

- **Degree over** $M(\mathscr{P})$: The degree of the (a,b)-component over $M(\mathscr{P})$ is equal to the rank of the exotic Igusa moduli stack $\mathbf{ExIg}\big(p^{\max(a,b)}, b\big)$, which is $p^b \cdot \varphi\big(p^{\max(a,b)}\big)$.

7

Appendix I: Review of relative Cartier divisors

For our very purpose, we shall only discuss effective divisors.

7.1 Effective Cartier divisors

Let S be a scheme, and X be a S-scheme.

Definition 7.1.1. *An* ***effective Cartier divisor*** *in X/S is a closed subscheme $D \subset X$, which is flat over S, and whose ideal sheaf $\mathscr{I}(D)$ is an invertible sheaf of $\mathscr{O}_X$-modules.*

We have another interpretation of effective Cartier divisors. We know that the effective Cartier divisor D on X/S is the zero locus of some section of $\mathscr{O}_X(D) = \mathscr{I}^{-1}(D)$. Explicitly, consider the tautological exact sequence of D

$$0 \longrightarrow \mathscr{I}(D) = \mathscr{O}_X(-D) \longrightarrow \mathscr{O}_X \longrightarrow i^*\mathscr{O}_D \longrightarrow 0,$$

where $i : D \hookrightarrow X$ is the closed immersion, tensoring $\mathscr{O}_X(D)$ to get

$$0 \longrightarrow \mathscr{O}_X \longrightarrow \mathscr{O}_X(D) \longrightarrow i^*\mathscr{O}_D \otimes_{\mathscr{O}_X} \mathscr{O}_X(D) \longrightarrow 0,$$

the image of the constant global section “1” in $\mathscr{O}_X(D)$ is what we expected, i.e., D is the zero locus of “1”. We claim that D is determined by the pair $(\mathscr{O}(D),$“1”$)$.

Suppose given a pair $(\mathscr{L}, \ell)$, where $\mathscr{L}$ is an invertible sheaf of $\mathscr{O}_X$-modules, and $\ell \in H^0(X, \mathscr{L})$ is a global section, such that in the following exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mathscr{O}_X \arrow[r, "\times \ell"] & \mathscr{L} \arrow[r] & \mathscr{L}/\mathscr{O}_X \arrow[r] & 0 \end{tikzcd}$$

$\mathscr{L}/\mathscr{O}_X$ is flat over S. Then the zero locus $V(\ell)$ is an effective Cartier divisor, and there is a unique isomorphism

$$(\mathscr{L},\ \ell) \simeq (\mathscr{I}^{-1}(V(\ell)),\ \text{“1”}).$$

Using such interpretation, the addition of twoeffective Cartier divisors can be defined as tensor product, i.e., given effective Cartier divisors $(\mathscr{L},\ell)$ and $(\mathscr{L}',\ell')$,

$$(\mathscr{L},\ \ell)\ +\ (\mathscr{L}',\ \ell')\ =\ (\mathscr{L}\otimes_{\mathscr{O}_X}\mathscr{L}',\ \ell\otimes\ell').$$

Locally speaking, the defining equation of $D+D'$ is given by product of defining equations of D and D'. If moreover we also consider non-effective Cartier divisors, then all relative Cartier divisors in X/S form an abelian group (the *Picard group*) under above addition, and $(\mathscr{O}_X,1)$ is the zero element.

Now suppose D, D' are effective Cartier divisors in X/S, we say that $D'\leqslant D$ if $D'\subset D$. Equivalently, this means:

(i) $\mathscr{I}(D)\subset\mathscr{I}(D')$, or

(ii) There exists an effective Cartier divisor D'' in X/S such that $D'+D''=D$.

If $D=(\mathscr{L},\ell)$ and $D'=(\mathscr{L}',\ell')$, then explicitly

$$D''\ =\ \Big(\mathscr{L}\otimes_{\mathscr{O}_X}(\mathscr{L}')^{-1},\ \frac{\ell}{\ell'}\Big).$$

7.2 Base changes and pull-backs

Let T be a S-scheme, and $X_T=X\times_S T$. Then $D_T=D\times_S T$ is an effective Cartier divisor in X_T/T. Indeed, D_T is a closed subscheme of X_T, and the flatness is preserved by base change. And if $D=(\mathscr{L},\ell)$, then $D_T=(\mathscr{L}_T,\ell_T)$.

Let Y be another S-scheme, and suppose we have a flat S-morphism

$$\begin{tikzcd} Y \arrow[rr, "f"] \arrow[dr] & & X \arrow[dl] \\ & S & \end{tikzcd}$$

then the closed subscheme $f^*(D)$ of Y

$$\begin{tikzcd} f^*(D) \arrow[r, hook, "i'"] \arrow[d] & Y \arrow[d, "f"] \\ D \arrow[r, hook, "i"] & X \end{tikzcd}$$

is an effective Cartier divisor in Y/S. Indeed, $f^*(D)$ is flat over D, and since D is flat over S, $f^*(D)$ is also flat over S. By flatness, the functor f^* on the category of quasi-coherent sheaves on X is exact, applying f^* to the tautological exact sequence

$$0\longrightarrow\mathscr{I}(D)\longrightarrow\mathscr{O}_X\longrightarrow i^*\mathscr{O}_D\longrightarrow 0,$$

we have

$$0\longrightarrow f^*\mathscr{I}(D)\longrightarrow\mathscr{O}_Y\longrightarrow i'^*\mathscr{O}_{f^*(D)}\longrightarrow 0,$$

insert it into the following diagram

$$\begin{tikzcd}
0 \arrow[r] & f^*\mathscr{I}(D) \arrow[r] \arrow[d] & \mathscr{O}_Y \arrow[r] \arrow[d, "\mathsf{id}"] & i'^*\mathscr{O}_{f^*(D)} \arrow[r] \arrow[d, "\mathsf{id}"] & 0 \\
0 \arrow[r] & \mathscr{I}(f^*(D)) \arrow[r] & \mathscr{O}_Y \arrow[r] & i'^*\mathscr{O}_{f^*(D)} \arrow[r] & 0
\end{tikzcd}$$

the first column is an isomorphism according to 5-lemma, therefore $\mathscr{I}(f^*(D)) = f^*\mathscr{I}(D)$ is an invertible sheaf.

7.3 A criterion for effective Cartier divisors

Proposition 7.3.1. *Suppose the base scheme S is locally noetherian, and X is flat of finite type. Then a closed subscheme $D \subset X$ which is flat over S is an effective Cartier divisor, if and only if any geometric fiber D_k ($k = \bar{k}$) is an effective Cartier divisor in X_k/k.*

Proof: *The "only if" part*: It is a consequence of our previous discussion on base change.

The "if" part: Firstly we need to verify the flatness of the ideal sheaf $\mathscr{I}(D)$ over X. Applying the fiber-wise criterion of flatness (cf. Altman-Kleiman [2] Proposition 3.4), one then only has to check the flatness over any fiber (not necessarily geometric). Although we only know the flatness over geometric fibers by condition, we will see how it can pass to arbitrary fibers.

Since flatness is local condition, it suffice to see the local picture. Let us say, R is a noetherian local ring with maximal ideal $\mathfrak{m}$, A is a flat local R-algebra (of finite type), and M is a finite A-module. Let $R' \to R$ be a flat extension of local rings, such that the residue field of R' is $\bar{k}$. Denote $M' = M \otimes_R R'$ and $A' = A \otimes_R R'$. Then $M' \otimes_{R'} \bar{k}$ is a flat $(A' \otimes_{R'} \bar{k})$-module by condition, which implies that M' is a flat A'-module according to the fiber-wise criterion of flatness. Since $A' \to A$ is also a flat extension of local rings, which is automatically faithfully flat, this implies M is flat over A.

Once we know that $\mathscr{I}(D)$ is flat over X, it is then locally free, in particular, with constant rank. While its geometric fiber has rank 1, $\mathscr{I}(D)$ indeed is an invertible sheaf, which shows that D is an effective Cartier divisor. □

7.4 Effective Cartier divisors in curves

Now we turn to study effective Cartier divisors in curves. Recall that a smooth curve C over S is a smooth morphism

$$\begin{tikzcd}
C \arrow[d] \\
S
\end{tikzcd}$$

of relative dimension 1, which is also separated and finitely presented.

Lemma 7.4.1. *Let D be a closed subscheme of C which is finite flat and finitely presented over S. Then D is an effective Cartier divisor in C/S, which is proper over S. Conversely, any proper effective Cartier divisor in C/S has this form.*

Proof: Since everything is of finite presentation here, it suffices to treat the case when $S = \mathsf{Spec}\,(R)$ is a noetherian affine scheme (cf. EGA IV$_3$, Proposition 8.9.1 et Corollaire 11.2.6.1), and furthermore by Proposition 7.3.1, reduces to the case $R = k$ (where $k = \bar{k}$). But then D is obviously an effective Cartier divisor in C_k/k which is proper, since it is finite over k.

Conversely, we need to show that any proper effective Cartier divisor D in C/S is finite and finitely presented over S (flatness is already in definition). Since D is locally defined by one equation on X, it is finitely presented over S. To show D is finite over S, it suffices to show that D is quasi-finite because we already know it is proper. Hence similarly, we are able to reduce to the case where S is a geometric point $\mathsf{Spec}\,(k)$ ($k = \bar{k}$), where the quasi-finiteness of D is obvious. □

Definition 7.4.2. *Suppose $D \subset C$ is a proper effective Cartier divisor in C/S. Define its degree to be the rank of D over S.*

Notice that any section $s \in C(S)$ defines a proper effective Cartier divisor $[s]$ in C/S of degree 1, it turns out that the converse is also true, i.e., any proper effective Cartier divisor of degree 1 in C/S comes from a section.

Lemma 7.4.3. *Let C/S be a smooth curve, and D is an effective Cartier divisor of degree n which is proper over S. Then fppf-locally, there exists a section $s \in C(S)$, such that $[s] \leqslant D$.*

Proof: Consider the cartesian diagrams

$$\begin{tikzcd}
D_D \arrow[r] \arrow[d, hook, "i_D"] & D \arrow[d, hook, "i"] \\
C_D \arrow[r] \arrow[d] & C \arrow[d] \\
D \arrow[r] & S
\end{tikzcd}$$

such a base change is fppf, since D is flat and finitely presented over S. The identity morphism of D induces a section $s \in C_D(D)$:

$$\begin{tikzcd}
D \arrow[drr, bend left, "\mathsf{id}_D"] \arrow[dr, "t"] \arrow[ddr, "s"'] \arrow[dddr, bend right, "\mathsf{id}_D"'] & & \\
& D_D \arrow[r] \arrow[d, hook, "i_D"] & D \arrow[d, hook, "i"] \\
& C_D \arrow[r] \arrow[d] & C \arrow[d] \\
& D \arrow[r] & S
\end{tikzcd}$$

Since D is proper over S, it is in particular separated. And notice that t is nothing but the relative diagonal morphism Δ of D/S, which is a closed immersion. This shows that t is a D-morphism, i.e., it is a section in $D_D(D)$. The composition $s = i_D \circ t$ shows that the section s lies in the effective Cartier divisor D. Such a section indeed defines an effective Cartier divisor $[s]$ in C_D, with the property $[s] \leqslant D_D$, which is exactly what we need. □

Lemma 7.4.4. *Let C/S be a smooth curve. Any section $s \in C(S)$ defines an effective Cartier divisor $[s]$ in C/S which is proper over S and of degree 1. Conversely, any proper effective Cartier divisor D of degree 1 comes from a unique section.*

Proof: The first assertion is straightforward. For the last assertion, by Lemma 7.4.3, fppf-locally on S, the degree 1 proper effective Cartier divisor D is given by a section, which shows that the structural morphism $D \to S$ is fppf-locally an isomorphism, hence an isomorphism. □

Lemma 7.4.5. *Let D_1, D_2 be effective Cartier divisors in C/S, then*

$$deg(D_1 + D_2) = deg(D_1) + deg(D_2).$$

Proof: Suppose $D_1 = (\mathscr{L}_1, \ell_1), D_2 = (\mathscr{L}_2, \ell_2)$. Consider the following commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & \mathscr{O}_X \arrow[r, "\times 1"] \arrow[d, "\times \ell_2"] & \mathscr{O}_X \arrow[r] \arrow[d, "\times \ell_1 \otimes \ell_2"] & 0 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathscr{L}_2 \arrow[r] \arrow[d] & \mathscr{L}_1 \otimes \mathscr{L}_2 \arrow[r] \arrow[d] & \mathscr{L}_1 \otimes \mathscr{L}_2 / \mathscr{L}_2 \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
0 \arrow[r] & \mathscr{L}_2 / \mathscr{O}_X \arrow[r] \arrow[d] & (\mathscr{L}_1 \otimes \mathscr{L}_2)/\mathscr{O}_X \arrow[r] \arrow[d] & (\mathscr{L}_1 \otimes \mathscr{L}_2)/\mathscr{L}_2 \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

all the columns as well as top two rows are trivially exact, according to the nine lemma, the bottom row is also exact. Equivalently, we have

$$0 \longrightarrow \mathscr{L}_2|_{D_2} \longrightarrow (\mathscr{L}_1 \otimes \mathscr{L}_2)|_{D_1+D_2} \longrightarrow (\mathscr{L}_1|_{D_1}) \otimes_{\mathscr{O}_{D_1}} (\mathscr{L}_2|_{D_1}) \longrightarrow 0,$$

notice that $\mathscr{L}_2|_{D_1}$ is an invertible sheaf on D_1, hence of rank 1. Thus locally speaking

$$\begin{aligned}
\mathrm{deg}(D_1 + D_2) &= H^0(\mathscr{L}_1 \otimes \mathscr{L}_2|_{D_1+D_2}) \\
&= H^0(\mathscr{L}_2|_{D_2}) + H^0(\mathscr{L}_1|_{D_1} \otimes \mathscr{L}_2|_{D_1}) \\
&= \mathrm{deg}(D_2) + \mathrm{deg}(D_1).
\end{aligned}$$

□

Lemma 7.4.6. *Let C be a smooth curve over S, and D a proper effective Cartier divisor in C/S. Suppose T is a S-scheme, then D_T is a proper effective Cartier divisor in C_T/T, and*

$$deg(D_T) = deg(D).$$

Lemma 7.4.7. *Let $f : C' \to C$ be a finite flat S-morphism between curves $C/S, C'/S$, and D is a proper effective Cartier divisor in C/S. Then $f^*(D)$ is a proper effective Cartier divisor in C'/S, and*

$$deg(f^*(D)) = deg(f) \cdot deg(D).$$

The following lemma is crucial for proving relative representability results.

Lemma 7.4.8. *Let C/S be a smooth curve, and D, D' are effective Cartier divisors in C/S, and D' is proper over S. Then there is a unique closed subscheme $Z \subset S$ which is universal for the relation $D' \leqslant D$, i.e., for any base change $T \to S$, $D'_T \leqslant D_T$ if and only if $T \to S$ factors through Z. Moreover, Z is locally defined by $d' = \mathsf{deg}(D')$ equations on S, and its formation commutes with any base change.*

Proof: We may assume $S = \mathsf{Spec}\,(R)$ is affine, since our question is local. Suppose $D = (\mathscr{L}, \ell)$ and $D' = (\mathscr{L}', \ell')$. Notice that the relation $D' \leqslant D$ holds if and only if $\ell|_{D'} = 0$ in $H^0(D', \mathscr{L}|_{D'})$. Since $\mathscr{L}|_{D'}$ is an invertible sheaf, hence locally free, without lose of generality we may assume $H^0(D', \mathscr{L}|_{D'})$ is a free R-module. The rank of $H^0(D', \mathscr{L}|_{D'})$ is d', choose a R-basis $\{e_1, ..., e_{d'}\}$ of $H^0(D', \mathscr{L}|_{D'})$, and express $\ell|_{D'}$ as

$$\ell|_{D'} = \sum_{i=1}^{d'} f_i \cdot e_i, \quad f_i \in R$$

Then the condition $\ell|_{D'} = 0$ is equivalent to d' equations $\{f_i = 0\}_{i=1}^{d'}$, this defines a closed subscheme $Z \subset S$. By the construction, it is obviously that Z satisfies the universal property.

And for any base change $T \to S$, Z_T is locally defined by equations $\{(f_i)_T = 0\}_{i=1}^{d'}$, which is also equivalent to $\ell_T|_{D'_T} = 0$, i.e., the relation $D'_T \leqslant D_T$. Therefore the formation of Z commutes with any base change. □

Corollary 7.4.9. *Let C/S be a smooth curve which has the structure of S-group scheme, D is a proper effective Cartier divisor in C/S. Then there is a unique closed subscheme $Z \subset S$ which is universal for the relation that D is a S-subgroup scheme. Moreover, Z is locally defined by $1 + \mathsf{deg}(D) + (\mathsf{deg}(D))^2$ equations, and its formation commutes with any base change.*

Proof: Let $0, \mathrm{inv}, m$ be the unit element, the inverse morphism and the multiplication morphism of C/S respectively. In order to be a S-subgroup scheme, the effective Cartier divisor D should satisfy following three conditions:

(i) $[0] \leqslant D$, where $[0]$ is the effective Cartier divisor given by the unit section 0;

(ii) $\mathrm{inv}^*(D) = D$;

(iii) Denote $W = D \times_S D$, and let $P_1, P_2 \in D_W(W)$ be the universal pair of points of D, i.e., they are given by

$$\begin{tikzcd}
W \arrow[rrd, bend left, "\mathsf{id}_W"] \arrow[rd, dotted, "P_1"] \arrow[rdd, bend right, "\mathrm{pr}_1"'] & & \\
& D_W \arrow[r] \arrow[d] & W \arrow[d] \\
& D \arrow[r] & S
\end{tikzcd}
\qquad
\begin{tikzcd}
W \arrow[rrd, bend left, "\mathsf{id}_W"] \arrow[rd, dotted, "P_2"] \arrow[rdd, bend right, "\mathrm{pr}_2"'] & & \\
& D_W \arrow[r] \arrow[d] & W \arrow[d] \\
& D \arrow[r] & S
\end{tikzcd}$$

in which we have the following diagram

$$\begin{tikzcd}
D_W \arrow[r, hook] & C_W \arrow[d] & D_W \arrow[l, hook'] \\
& W \arrow[lu, "P_1"] \arrow[ru, "P_2"'] &
\end{tikzcd}$$

Now the third condition is

$$[m(P_1,P_2)] \leqslant D_W.$$

The meanings of those three conditions are clear.

Condition (i) possesses one equation over S, because $\deg([0]) = 1$. Condition (ii) is equivalent to

$$\mathrm{inv}^*(D) \leqslant D,$$

since both sides have the same rank, this gives $\deg(D)$ equations over S. Condition (iii) possesses one equation over W, but since W is finite flat over S with rank $(\deg(D))^2$, therefore it gives $(\deg(D))^2$ equations over S. The closed subscheme Z locally defined by these equations obviously satisfies the universal property, and its formation commutes with any base change. □

8

Appendix II: Review of elliptic curves

The purpose of this appendix is to set up the foundations for elliptic curve over a base scheme, rather than a field. We mainly follow Katz-Mazur [24] and Deligne [25].

8.1 General formulation

Definition 8.1.1. *An* ***elliptic curve*** *E over a base scheme S is a proper smooth curve*

$$\begin{tikzcd} E \arrow[d, "f"] \\ S \arrow[u, bend left, "0"] \end{tikzcd}$$

with a "zero" section 0, such that any geometric fiber of f has genus 1.

Smoothness of relative dimension 1 implies that $\Omega^1_{E/S}$ is locally free of rank 1. It is not so obvious that E itself is a S-group scheme, although the existence of group structure on each geometric fiber is classic. But we can still use a similar approach to equip E with a group structure, i.e., by relating to the Jacobian.

Theorem 8.1.2 (Abel)**.** *Let E/S be an elliptic curve. Then there exists a unique commutative group-scheme structure, such that for any S-scheme T and any sections $P, Q, R \in E(T)$, we have*

$$P + Q = R$$

if and only if there is an invertible sheaf $\mathscr{L}_0$ on T and an isomorphism

$$\mathscr{O}_{E_T}(P) \otimes \mathscr{O}_{E_T}(Q) \otimes \mathscr{O}_{E_T}(-0) \simeq \mathscr{O}_{E_T}(R) \otimes f_T^* \mathscr{L}_0.$$

Proof: Recall the definition of *relative Picard functor* of E/S:

$$\mathsf{Pic}_{E/S}(T) := \mathsf{Pic}(E_T)/\mathsf{Pic}(T)$$

where the functor Pic is the *absolute Picard functor*, and the right side means precisely the set of isomorphism classes of invertible sheaves $\mathscr{L}$ on E_T modulo the equivalence relation

$$\mathscr{L} \sim \mathscr{L} \otimes f_T^*(\mathscr{L}_0).$$

Moreover, there are Picard functors with fixed degree (the connected components of $\mathsf{Pic}_{E/S}$), in particular, its neutral component (or the *Jacobian*) $\mathsf{Pic}^{(0)}_{E/S}$. In order to prove the theorem, it suffices to show that the morphism (between functors)

$$E/S \longrightarrow \mathsf{Pic}^{(0)}_{E/S}$$

which is defined by sending any S-valued point $P \in E(S)$ to the invertible sheaf $\mathscr{O}_E(P) \otimes \mathscr{O}_E(-0)$, is an isomorphism.

We claim that the problem is Zariski-local on S. This is a descent property (for affine Zariski coverings) for $\mathsf{Pic}^{(0)}_{E/S}$, which is obvious if we know the representability of $\mathsf{Pic}^{(0)}_{E/S}$. However, an elliptic curve $E \to S$ is always Zariski-locally projective [1], the representability of Jacobian $\mathsf{Pic}^{(0)}_{E/S}$ indeed holds [2].

Since S is finitely presented, we may reduce to the case that S is noetherian. Let $\mathscr{L}$ be an invertible sheaf on E which is fiber-wise of degree 0, and let $\widetilde{\mathscr{L}} = \mathscr{L} \otimes \mathscr{O}_E(0)$. By the Semicontinuity Theorem [3], the sheaf $f_*\widetilde{\mathscr{L}}$ is locally free over S, of rank 1. Zariski-locally on S, we choose an $\mathscr{O}_S$-basis ℓ of the invertible sheaf $\widetilde{\mathscr{L}}$. Then $(\widetilde{\mathscr{L}}, \ell)$ defines an effective Cartier divisor in E/S. Indeed, by the fiber-wise criterion for effective Cartier divisors, one only needs to ensure that $(\widetilde{\mathscr{L}}, \ell)$ defines an effective Cartier divisor on any geometric fiber of E/S, which is clear. Therefore it defines an effective Cartier divisor of degree 1 in E/S, which must come from a section in $E(S)$, i.e., this defines an inverse map

$$\begin{array}{rcl} \mathsf{Pic}^{(0)}_{E/S}(S) & \longrightarrow & E(S) \\ \mathscr{L} & \longmapsto & P = (\mathscr{L} \otimes \mathscr{O}(0), \ell) \end{array}$$

Moreover, the two morphisms we have defined

$$E/S \leftrightarrows \mathsf{Pic}^{(0)}_{E/S}$$

apparently are mutually inverse, this proves the theorem. □

Definition 8.1.3. *The sheaf $\omega_{E/S} = f_*\Omega^1_{E/S}$ on S is called the* ***sheaf of invariant differentials****.*

The function $h^0(s, \Omega^1_{E_s})$ is constant on S, with value 1, since each geometric fiber of E/S is of genus 1. By Semicontinuity Theorem, the sheaf of invariant differentials $\omega_{E/S}$ is an invertible sheaf on S. Hence Zariski-locally on S, it is possible to choose an $\mathscr{O}_S$-basis ω of $\omega_{E/S}$. As the name of $\omega_{E/S}$ implies, the basis ω turns out to be a differential on E which is invariant under translations. Indeed, the action of translations on ω defines a morphism of S-group schemes

$$E \longrightarrow \mathbb{G}_m,$$

[1] See the next section for the construction of generalized Weierstrass equations.

[2] cf. Kleiman [7] Theorem 9.4.8 and Theorem 9.5.20

[3] cf. Hartshorne [29] Theorem 12.8 and Corollary 12.9

which has to be constant, since E is proper over S. On the other hand, the pull-back invertible sheaf $0^*\Omega^1_{E/S}$ stands for those differentials on E which are given by translations of some fixed differential on the zero section $0 : S \to E$. So consequently, $\omega_{E/S}$ and $0^*\Omega^1_{E/S}$ must be isomorphic. We now give another proof.

Lemma 8.1.4. *There is an isomorphism*

$$\omega_{E/S} \longrightarrow 0^*\Omega^1_{E/S}.$$

Proof: Starting with the tautological exact sequence for the zero section

$$0 \longrightarrow \mathscr{O}_E(-0) \longrightarrow \mathscr{O}_E \longrightarrow 0^*\mathscr{O}_S \longrightarrow 0,$$

tensoring $\Omega_{E/S}$

$$0 \longrightarrow \Omega^1_{E/S}(-0) \longrightarrow \Omega^1_{E/S} \longrightarrow 0^*\mathscr{O}_S \otimes_{\mathscr{O}_E} \Omega^1_{E/S} = 0_*0^*\Omega^1_{E/S} \longrightarrow 0.$$

Applying the left exact functor f_*, one obtains the long exact sequence

$$0 \longrightarrow f_*\Omega^1_{E/S}(-0) \longrightarrow \omega_{E/S} \longrightarrow f_*0_*0^*\Omega^1_{E/S} = 0^*\Omega^1_{E/S}$$

$$\longrightarrow R^1f_*\Omega^1_{E/S}(-0) \longrightarrow R^1f_*\Omega^1_{E/S} \longrightarrow R^1f_*(\Omega^1_{E/S}|_S) \longrightarrow \ldots$$

where $R^1f_*(\Omega^1_{E/S}|_S) = 0$ for dimensional reason, and $f_*\Omega^1_{E/S}(-0) = 0$ by Riemann-Roch, hence the exact sequence becomes

$$0 \longrightarrow \omega_{E/S} \longrightarrow 0^*\Omega^1_{E/S} \longrightarrow R^1f_*\Omega^1_{E/S}(-0) \longrightarrow R^1f_*\Omega^1_{E/S} \longrightarrow 0.$$

By the Semicontinuity Theorem and Riemann-Roch, the last two sheaves are both invertible, so the surjective morphism between them must be an isomorphism. Now it follows that the morphism in above exact sequence

$$\omega_{E/S} \xrightarrow{\sim} 0^*\Omega^1_{E/S}$$

is an isomorphism. □

8.2 Generalized Weierstrass equations

Proposition 8.2.1. *Let E/S be an elliptic curve, with zero section $0 : S \to E$. Then $f_*\mathscr{O}_E(n\cdot 0)$ is locally free of rank n for any $n \geqslant 1$.*

Proof: Since by Riemann-Roch,

$$h^0(E_s, \mathscr{O}_{E_s}(n\cdot 0_s)) = h^1(E_s, \mathscr{O}_{E_s}(n\cdot 0_s)) + \deg(n\cdot 0_s) = h^0(E_s, \mathscr{O}_{E_s}(K_{E_s} - n\cdot 0_s)) + n = n$$

is constant on S, by Semicontinuity Theorem, the push-forward sheaf $f_*\mathscr{O}_E(n\cdot 0)$ is locally free of rank n. □

Lemma 8.2.2. *There is an isomorphism*

$$\omega_{E/S} \longrightarrow 0^*\mathscr{I}(0).$$

Proof: By the Second Exact Sequence of sheaves of differentials [4], we have a short exact sequence

$$0^*\mathscr{I}(0) \longrightarrow 0^*\Omega^1_{E/S} \longrightarrow \Omega^1_{S/S} = 0 \longrightarrow 0,$$

it shows that there is a surjective morphism

$$0^*\mathscr{I}(0) \longrightarrow\!\!\!\!\rightarrow 0^*\Omega^1_{E/S},$$

which must be an isomorphism, since both sheaves are invertible. □

Proposition 8.2.3. *Let E/S be an elliptic curve over S. Suppose that $\omega_{E/S}$ is free over S, then $f_*\mathscr{O}_E(n\cdot 0)$ is free for any $n \geqslant 1$.*

Proof: Tensoring $\mathscr{O}_E((n+1)0)$ with the tautological exact sequence for the zero section,

$$0 \longrightarrow \mathscr{O}_E(n\cdot 0) \longrightarrow \mathscr{O}_E((n+1)0) \longrightarrow 0_*0^*\mathscr{O}_E((n+1)0) \longrightarrow 0,$$

and applying f_*, we obtain

$$0 \longrightarrow f_*\mathscr{O}_E(n\cdot 0) \longrightarrow f_*\mathscr{O}_E((n+1)0) \longrightarrow 0^*\mathscr{O}_E((n+1)0) \longrightarrow 0,$$

because $R^1f_*\mathscr{O}_E(n\cdot 0) = 0$ for any $n \geqslant 1$. Using induction, suppose one knows that $f_*\mathscr{O}_E(n\cdot 0)$ is free. The condition $\omega_{E/S}$ being free implies that $0^*\mathscr{O}_E(-0)$ is free, by Lemma 8.2.2, hence so as $0^*\mathscr{O}_E((n+1)0)$. Thus above short exact sequence apparently splits, which shows that the middle one $f_*\mathscr{O}_E((n+1)0)$ is also free. □

Like in the theory of elliptic curves over fields, it is still possible to find *Weierstrass equation* for elliptic curves over a general base scheme, but only Zariski-locally on S. Assume $\omega_{E/S}$ is free on S, by Proposition 8.2.3, $f_*\mathscr{O}_E(n\cdot 0)$ is free for any $n \geqslant 1$.

Since E is smooth of relative dimension 1 over S, over an affine open subset $\mathsf{Spec}\,(R)$, its formal group $\widehat{E}$ is isomorphic to the formal spectrum of the formal power series in one variable:

$$\widehat{E} \simeq \mathsf{Spf}\,(R[\![T]\!]).$$

The choice of the formal parameter T is however not unique. We fix a formal parameter T, then there exists a unique invariant differential ω with the form

$$\omega = \big(1 + \text{ higher terms}\big)\cdot dT,$$

for such invariant differential, we call that ω is *adapted* to the formal parameter T. Conversely, if instead we fix an $\mathscr{O}_S$-basis ω of $\omega_{E/S}$, then there exists a formal parameter T which is unique up to some analytical isomorphism

$$T \longmapsto T + \text{ higher terms.}$$

[4] cf. Hartshorne [29] Proposition 8.12

By assumption, $f_*\mathscr{O}_E(2\cdot 0)$ is free of rank 2, let $\{1,x\}$ be its basis. With respect to the formal parameter T, we can normalize x so that it has the formal expansion

$$x = \frac{1}{T^2}\big(1 + \text{higher terms}\big),$$

then x is unique up to $x \mapsto x+c$ for some constant c. Similarly, let $\{1,x,y\}$ be a basis of $f_*\mathscr{O}_E(3\cdot 0)$, and normalize y so that it has the formal expansion

$$y = \frac{1}{T^3}\big(1 + \text{higher terms}\big),$$

and y is unique up to $y \mapsto y+ax+b$ for some constants a,b. We say those x,y are adapted to the formal parameter T, or to the invariant differential ω.

For $n=4,5$, we find basis for $f_*\mathscr{O}_E(n\cdot 0)$:

$$\begin{aligned} n=4: &\quad \{1,x,y,x^2\}, \\ n=5: &\quad \{1,x,y,x^2,xy\}, \end{aligned}$$

they are indeed linearly independent, since they have different orders at the zero section. As for $f_*\mathscr{O}_E(6\cdot 0)$, it has rank 6, so the following 7 elements of it must be linearly dependent:

$$1,\ x,\ y,\ x^2,\ xy,\ y^2,\ x^3$$

such relation is exactly the **generalized Weierstrass equation**:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1,\dots,a_6 \in H^0(S,\mathscr{O}_S)$. The affine coordinate ring of $E\backslash\{0\}$ over $\mathsf{Spec}(R)$ is

$$H^0(E\backslash\{0\},\mathscr{O}_{E\backslash\{0\}}) = \varinjlim H^0(E,\mathscr{O}_E(n\cdot 0)) = R[x,y]\Big/\big(y^2+a_1xy+a_3y-(x^3+a_2x^2+a_4x+a_6)\big).$$

If furthermore we assume $\mathscr{O}_E(0)$ is free over E, then so as the ideal sheaf $\mathscr{I}(0) = \mathscr{O}_E(-0)$. So we can choose a global function z which vanishes at the zero section with order 1, moreover, we can choose z so that the image of z in the formal completion along the zero section is nothing but the chosen formal parameter T. This allows us to homogenize the generalized Weierstrass equation as

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

i.e., E can be embedded into the projective plane $\mathbb{P}^2_R$ with above homogeneous generalized Weierstrass equation as the defining equation. In particular, we have proved:

Proposition 8.2.4. *Any elliptic curve E/S is projective.*

Remark: The projectivity is particularly important, e.g., it ensures the representability of the relative Picard functor $\mathsf{Pic}_{E/S}$ of E/S, and it also guarantees that the moduli space of elliptic curves $\mathscr{M}_{1,1}$ is a stack (cf. Appendix III 9).

8.3 Some universal elliptic curves

In this section, we study some universal elliptic curves, which serve as some elementary moduli problem.

Recall that for any elliptic curve E/S, Zariski-locally we can always find a generalized Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

which is unique adapted to a given invariant differential ω, up to

$$\begin{cases} x \mapsto x+c \\ y \mapsto y+ax+b \end{cases}$$

In the following discussions, we always assume the base scheme is affine $S = \mathsf{Spec}\,(R)$, and $\omega_{E/S}$ is trivial over S.

Case I. 6 is invertible

When 6 is invertible in R, choose a basis ω of $\omega_{E/S}$, and do some appropriate change of x, y, we obtain the generalized Weierstrass equation of the form

$$(2y)^2 = 4x^3 - g_2x - g_3,$$

and $\omega = -\frac{dx}{2y}$, where x, y are adapted to ω. The smoothness of E over R implies the discriminant

$$\Delta = g_2^3 - 27g_3^2$$

is an invertible element in R.

Consider the *universal Weierstrass family* $\mathbf{E}_{(\frac{1}{6})}$ defined over the ring $\mathbf{R}_0 = \mathbb{Z}[\frac{1}{6}, g_2, g_3][\frac{1}{\Delta}]$:

$$\mathbf{E}_{(\frac{1}{6})} = \mathsf{Proj}\,\mathbf{R}_0[x,y,z]\big/\big((2y)^2z - (4x^3 - g_2xz^2 - g_3z^3)\big),$$

with the chosen invariant differential $\Omega = -\frac{dx}{2y}$.

Proposition 8.3.1. *The pair $(\mathbf{E}_{(\frac{1}{6})}, \Omega)$ is universal in the sense that given any pair $(E/S, \omega)$, where S is a $\mathbb{Z}[\frac{1}{6}]$-scheme, there exists a unique cartesian diagram*

$$\begin{tikzcd} E \arrow[r] \arrow[d] & \mathbf{E}_{(\frac{1}{6})} \arrow[d] \\ S \arrow[r] & \mathsf{Spec}\,(\mathbf{R}_0) \end{tikzcd}$$

such that the pull-back of Ω is ω.

Proof: Given such a pair $(E/S, \omega)$, the existence of ω already indicates that $\omega_{E/S}$ is free over S, hence by Proposition 8.2.3, $f_*\mathscr{O}_E(n\cdot 0)$ is free for any $n \geqslant 1$. So we can find the generalized Weierstrass equation of the form

$$(2y)^2 = 4x^3 - g_2x - g_3,$$

with $\omega = -\frac{dx}{2y}$ under these coordinates. The specification of g_2, g_3 defines the morphism of base schemes

$$S \longrightarrow \mathsf{Spec}\,(\mathbf{R}_0),$$

it remains to check that the pull-back of the universal Weierstrass family $\mathbf{E}_{(\frac{1}{6})}$ is isomorphic to E, which suffices to check Zariski-locally on S. The isomorphism follows from our discussion of construction of generalized Weierstrass equation. Thus we have a cartesian diagram as required. The uniqueness also follows, from that once we fix the generalized Weierstrass equation and an invariant differential, then the coordinates x, y are unique. □

If we require furthermore that the discriminant $\Delta = 1$, then we obtain the *normalized universal Weierstrass family* $\mathbf{E}^1_{(\frac{1}{6})}$ defined over the ring $\mathbf{R}_1 = \mathbb{Z}[\frac{1}{6}, g_2, g_3]/(\Delta - 1)$:

$$\mathbf{E}^1_{(\frac{1}{6})} \;=\; \mathsf{Proj}\,\mathbf{R}_1[x,y,z]\big/\big((2y)^2z - (4x^3 - g_2xz^2 - g_3z^3)\big),$$

with the chosen invariant differential $\Omega_1 = -\frac{dx}{2y}$. Similarly, the pair $(\mathbf{E}^1_{(\frac{1}{6})}, \Omega_1)$ also satisfies the universal property.

Proposition 8.3.2. *The pair* $(\mathbf{E}^1_{(\frac{1}{6})}, \Omega_1)$ *is universal in the sense that given any pair* $(E/S, \omega)$ *with* $\Delta_E = 1$*, where S is a* $\mathbb{Z}[\frac{1}{6}]$*-scheme, there exists a unique cartesian diagram*

$$\begin{tikzcd}
E \arrow[r] \arrow[d] & \mathbf{E}^1_{(\frac{1}{6})} \arrow[d] \\
S \arrow[r] & \mathit{Spec}\,(\mathbf{R}_1)
\end{tikzcd}$$

such that the pull-back of Ω_1 *is* ω.

Case II. 2 is invertible

When 2 is invertible in R, the generalized Weierstrass equation of E/R can be made into the form

$$y^2 \;=\; x^3 \;+\; a_2x^2 \;+\; a_4x \;+\; a_6,$$

with the chosen $\omega = -\frac{dx}{2y}$, where y is uniquely adapted to ω, but x is up to $x \mapsto x + c$. In such form, the automorphism of E

$$P \longmapsto -P$$

is precisely given by $(x, y) \mapsto (x, -y)$. So the finite étale covering of R defined by

$$x^3 \;+\; a_2x^2 \;+\; a_4x \;+\; a_6 \;=\; 0$$

together with the zero section, gives the 2-torsion R-subgroup scheme $E[2]/S$. This group scheme is étale over R (cf. Proposition 2.2.5), there are exactly 4 R-valued 2-torsion points. Suppose these 2-torsion points (other than the zero section) are P_2, Q_2 and $P_2 + Q_2$.

There is a unique choice of x, such that $x(P_2) = 0$, i.e., the constant term in the generalized Weierstrass equation is killed

$$y^2 \;=\; x^3 \;+\; a_2x^2 \;+\; a_4x.$$

Furthermore, we normalize ω, in the way that after we make the following change

$$\begin{cases} x \mapsto c_1 \cdot x \\ y \mapsto c_2 \cdot y \end{cases}$$

for some scalars $c_1, c_2 \in R^\times$, so that $x(Q_2) = 1$, i.e.,

$$\omega \longmapsto \frac{c_1}{c_2}\omega.$$

So now the generalized Weierstrass equation of E/R has the form

$$y^2 = x(x-1)(x-\lambda),$$

with $\omega = -\frac{dx}{2y}$, where $\lambda = x(P_2 + Q_2)$. Such equation defines a smooth curve if and only if $\lambda \neq 0, 1$.

There is the *universal Legendre family* $\mathbf{E}_{(\frac{1}{2})}$ over the ring $\mathbf{R}_2 = \mathbb{Z}[\frac{1}{2}, \lambda][\frac{1}{\lambda(\lambda-1)}]$

$$\mathbf{E}_{(\frac{1}{2})} = \mathsf{Proj}\, \mathbf{R}_2[x,y,z]/\big(y^2z - x(x-z)(x-\lambda z)\big),$$

with the chosen $\Omega_2 = -\frac{dx}{2y}$, and two specified 2-torsion points $P_2^{\text{univ}}, Q_2^{\text{univ}}$ such that

$$x(P_2^{\text{univ}}) = 0, \quad x(Q_2^{\text{univ}}) = 1.$$

The quadruple $(\mathbf{E}_{(\frac{1}{2})}, \Omega_2, P_2^{\text{univ}}, Q_2^{\text{univ}})$ is universal.

Proposition 8.3.3. *The quadruple* $(\mathbf{E}_{(\frac{1}{2})}, \Omega_2, P_2^{univ}, Q_2^{univ})$ *is universal in the sense that given any quadruple* $(E/S, \omega, P_2, Q_2)$*, where* S *is a* $\mathbb{Z}[\frac{1}{2}]$*-scheme, there exists a unique cartesian diagram*

$$\begin{tikzcd} E \arrow[r] \arrow[d] & \mathbf{E}_{(\frac{1}{2})} \arrow[d] \\ S \arrow[r] & \mathsf{Spec}\,(\mathbf{R}_2) \end{tikzcd}$$

such that the pull-back of Ω *is* ω*, and the pull-backs of the effective Cartier divisors* P_2^{univ}, Q_2^{univ} *are* P_2, Q_2 *respectively.*

Case III. 3 is invertible

When 3 is invertible in R, after the change of x:

$$x \longmapsto x - \frac{a_2}{3},$$

the generalized Weierstrass equation of E/S can be made into the form

$$y^2 + a_1xy + a_3y = x^3 + a_4x + a_6,$$

with the chosen $\omega = -\frac{dx}{2y}$. In this case, x is specified, while y is up to $y \mapsto y + ax + b$. The 3-torsion R-subgroup scheme $E[3]/R$ is finite étale over R, of rank 9, which can be calculated from the geometric fibers. Let P_3, Q_3 be two 3-torsion R-valued points of $E(R)$, such that $Q_3 \neq \pm P_3$. Since 3-torsion points are inflection points, there exists a unique function which has a triple zero at P_3 and a triple pole at the zero section 0. By changing y, we can suppose y is such function, then the left side of the generalized Weierstrass equation

$$y^2 + a_1xy + a_3y$$

should be a perfect cube, more precisely,

$$y^2 + a_1xy + a_3y = (x - x(P_3))^3.$$

Hence after changing $x \mapsto x - x(P_3)$, the equation becomes

$$y^2 + a_1xy + a_3y = x^3,$$

in this case $P_3 = (0,0)$. Similarly, there exists a unique function with a triple zero at Q_3 and a triple pole at the zero section 0, which has the form $y - ax - b$. We claim that $a \in R$ is a unit. Otherwise there exists some geometric fiber of E/R such that a vanishes. Substitute $y = b$ into the generalized Weierstrass equation, one has

$$x^3 - a_1bx - (a_3b + b^2) = (x - x(Q_3))^3.$$

By comparing coefficients of x^2, since the characteristic of the base field is not 3, it forces that $x(Q_3) = 0$, which means $Q_3 = \pm P_3$, a contradiction. So after (unique) normalization of ω, we can make $a = 1$. Put $y = x + b$ into the generalized Weierstrass equation, and let $x(Q_3) = c$

$$x^3 - (a_1 + 1)x^2 - (2b + a_1b + a_3)x - (b^2 + a_3b) = (x - c)^3,$$

from this we can express a_1, a_3 in terms of b, c:

$$\begin{cases} a_1 = 3c - 1 \\ a_3 = -3c^2 - 3bc - b \end{cases}$$

and together with the relation of b, c:

$$c^3 + 3bc^2 + 3b^2c = 0.$$

The discriminant of E/R can also be interpreted in terms of b, c, and the smoothness of E/R is equivalent to that $\Delta(b,c) \in R^\times$.

There is the *universal family* $\mathbf{E}_{(\frac{1}{3})}$ *of naïve level 3*

$$\mathbf{E}_{(\frac{1}{3})} = \mathsf{Proj}\, \mathbf{R}_3[x,y,z] \big/ \big(y^2z + (3c-1)xyz - (3c^2 + 3bc + b)yz^2 - x^3\big),$$

defined over the ring $\mathbf{R}_3 = \mathbb{Z}[\frac{1}{3}, b, c][\frac{1}{\Delta(b,c)}]\big/(c^3 + 3bc^2 + 3b^2c)$, with the chosen $\Omega_3 = -\frac{dx}{2y}$ and the specifies 3-torsion points

$$P_3^{\text{univ}} = (0,0), \quad Q_3^{\text{univ}} = (c, b + c).$$

The quadruple $(\mathbf{E}_{(\frac{1}{3})}, \Omega_3, P_3^{\text{univ}}, Q_3^{\text{univ}})$ is universal.

Proposition 8.3.4. *The quadruple* $(\mathbf{E}_{(\frac{1}{3})}, \Omega_3, P_3^{univ}, Q_3^{univ})$ *is universal in the sense that given any quadruple* $(E/S, \omega, P_3, Q_3)$*, where* S *is a* $\mathbb{Z}[\frac{1}{3}]$*-scheme, there exists a unique cartesian diagram*

$$\begin{tikzcd} E \arrow[r] \arrow[d] & \mathbf{E}_{(\frac{1}{3})} \arrow[d] \\ S \arrow[r] & \mathsf{Spec}\,(\mathbf{R}_3) \end{tikzcd}$$

such that the pull-back of Ω_3 *is* ω*, and the pull-backs of the effective Cartier divisors* P_3^{univ}, Q_3^{univ} *are* P_3, Q_3 *respectively.*

8.4 Isogenies

Theorem 8.4.1. *Let E/S be an elliptic curve over an arbitrary scheme S. Then the S-morphism of multiplication by N*

$$[N]:\, E \longrightarrow E$$

is finite and locally free of rank N^2 over S. Moreover, if S is a $\mathbb{Z}[\frac{1}{N}]$-scheme, then the N-torsion S-subgroup scheme $E[N]$ is étale over S, and étale-locally it is isomorphic to the constant S-group scheme $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.

Proof: We have already proved the case where N is invertible on S. [5] And the rank $= N^2$ can be calculated on any geometric fiber, the result is classic.

In general case, Zariski-locally we can always find generalized Weierstrass equation for E, observe that it suffices to prove the theorem for the universal family $\mathbf{E}$

$$\mathbf{E} \;=\; \mathsf{Proj}\, \mathbf{R}[x,y,z]\big/\big(y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6)\big)$$

over the ring $\mathbf{R} = \mathbb{Z}[a_1, a_2, a_3, a_4, a_5, a_6][\frac{1}{\Delta}]$, and then the result follows from base change

$$\begin{tikzcd}
E \arrow[r] \arrow[d, "{[N]}"'] & \mathbf{E} \arrow[d, "{[N]}"] \\
E \arrow[r] & \mathbf{E}
\end{tikzcd}$$

since both finiteness and local freeness are preserved under base change.

The morphism $[N]$ is automatically proper, in order to prove the theorem, it suffices to prove that it is quasi-finite. Then being proper and quasi-finite implies that it is finite. And since $\mathbf{E}$ is smooth over a regular scheme Spec ($\mathbf{R}$), it is also regular. Finally, use the fact that any finite morphism between two regular schemes of the same dimension is automatically flat, and that under the noetherian condition, being finite flat implies being finite locally free, the theorem follows.

Thus it remains to prove the quasi-finiteness of $[N]$, or equivalently, over any geometric point,

$$[N]_k:\, E_k \longrightarrow E_k$$

is always non-zero, so that its kernel has to be finite. Let M be an integer which is coprime to $\mathrm{char}(k)$ and N. Then $E_k[M](k)$ consists of M^2 distinct points, and $[N]$ induces a bijection between these points since M, N are coprime. This already shows that $[N]$ cannot be 0 morphism.

Since any finite étale group scheme is étale-locally constant, by looking at the geometric fibers, it is indeed étale-locally isomorphic to the constant group scheme $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. □

Corollary 8.4.2. *Let E/S be an elliptic curve over an arbitrary scheme S, and $N \geqslant 1$ is an integer. Then $E[N]$ is finite étale over S if and only if N is invertible on S.*

Proof: The "if" part is in Theorem 8.4.1. For the "only if" part, suppose $E[N]$ is finite étale over S, as in the proof of Proposition 2.2.5, the morphism $[N]$ is finite étale. Hence it induces an isomorphism on Lie algebras

$$\mathrm{Lie}([N]):\, \mathrm{Lie}(E/S) \xrightarrow{\sim} \mathrm{Lie}(E/S),$$

[5] cf. Proposition 2.2.5 and Lemma 2.3.2.

which is just multiplication by the integer N. This shows that N must be invertible on S, otherwise we could find a geometric point such that $\mathrm{Lie}([N]) = 0$. □

Definition 8.4.3. *An* ***isogeny*** $\phi : E_1 \to E_2$ *of elliptic curves over an arbitrary scheme* S *is a* S*-morphism which is fppf-locally surjective and locally free of finite rank, such that* $\phi \circ 0_1 = 0_2$*, where* $0_1, 0_2$ *are zero sections of* E_1, E_2 *respectively.*

Obviously, the morphism $[N]$ of multiplication by N is an isogeny for any $N \geqslant 1$.

Lemma 8.4.4 (Drinfeld's Strictness Lemma)**.** *Let* $\phi : E_1 \to E_2$ *be a* S*-homomorphism of elliptic curves over a ring* R*, and* $I \subset R$ *is an ideal,* p *is a prime number. Suppose the ideal* (I, p) *is nilpotent, and* $f \equiv 0$ *mod* I*, then* $f = 0$*.*

Proof: Let

$$I^{(0)} = I, \quad I^{(1)} = (pI, I^2), \quad ..., \quad I^{(n+1)} = \left(pI^{(n)}, (I^n)^2\right), \quad ...$$

The descending sequence of ideals

$$I^{(0)} \supset I^{(1)} \supset ... \supset I^{(n)} \supset ...$$

is certainly stable, i.e., $I^{(n)} = 0$ for any sufficiently large n. If we can prove the lemma for any pair $\left(R/I^{(n+1)}, I^{(n)}/I^{(n+1)}\right)$ $(n \geqslant -1)$, where we let $I^{(-1)} = R$, then $\phi = 0$ in $R/I = R/I^{(0)}$ implies that $\phi = 0$ in $R/I = R/I^{(1)}$, and eventually $\phi = 0$ in $R/I^{(n)} = R$ for sufficiently large n. Therefore it suffices to prove the lemma with assumptions that $I^2 = pI = 0$ in R.

The morphism $[p] : E_1 \to E_1$ is fppf-locally surjective, it suffices to prove that $p\phi = 0$ if $\phi \equiv 0$ mod I. Let A be any R-algebra. Given any A-valued point $P \in E_1(A)$, its image $\phi(P)$ lies in the kernel

$$\ker\left\{E_2(A) \to E_2(A/IA)\right\},$$

in particular, it lies in the formal group $\widehat{E}_2(A)$. Choose a formal parameter X of $\widehat{E}_2$, i.e., fix an isomorphism

$$\widehat{E}_2 \simeq \mathrm{Spf}\,(R[\![X]\!]).$$

Then $X(f(P))$ belongs to IA. Recall that $[p](X)$ has the form [6]

$$[p](X) = pF(X) + G(X^p),$$

with $F(X), G(X) \in R[\![X]\!]$ and $F(0) = G(0) = 0$. Hence $X(p\phi(P)) \in (pI \cdot A, I^2 \cdot A) = 0$, i.e., $p\phi = 0$. □

Theorem 8.4.5 (Rigidity)**.** *Let* E_1, E_2 *be elliptic curves over an arbitrary scheme* S *with zero sections* $0_1, 0_2$*, and* $\phi : E_1 \to E_2$ *is a* S*-homomorphism. Then Zariski-locally on* S*, either* $\phi = 0$ *or* ϕ *is an isogeny.*

Proof: As indicated in the theorem, the question is Zariski-local, we assume $S = \mathrm{Spec}\,(R)$ is affine, such that E_1, E_2 are projective over R, in other words, there are generalized Weierstrass equations for E_1, E_2 with coefficients in R. Moreover, because E_1, E_2 are both finitely presented over R, we can assume R is of finite type over $\mathbb{Z}$.

[6] cf. Silverman [10] Corollary 4.4

To prove the theorem, we intend to show that the locus S_0 of $f = 0$ is both open and closed in S. Compare the two S-morphisms ϕ and 0:

$$\begin{tikzcd}
E_1 \arrow[rr, shift left, "\phi"] \arrow[rr, shift right, "0"'] \arrow[dr, "f_1"'] & & E_2 \arrow[dl, "f_2"] \\
& S &
\end{tikzcd}$$

the equalizer of ϕ and 0 is a closed subscheme of E_1:

$$\begin{tikzcd}
E_1 \times_{(\phi,0),\Delta_{E_2}} E_2 \arrow[r, hook] \arrow[d] & E_1 \arrow[d, "{(\phi,0)}"] \\
E_2 \arrow[r, hook, "\Delta_{E_2}"] & E_2 \times_S E_2
\end{tikzcd}$$

hence $S_0 = f_1(E_1 \times_{(\phi,0),\Delta_{E_2}} E_2)$ is closed in S, since f_1 is proper.

To show that S_0 is open in S, we adopt the assumption $S = \mathsf{Spec}\ (R)$. We have to show that if $x \in S_0$ is a closed point, then any of its generization y also lies in S_0. Let I_x be the maximal ideal corresponding to x, and

$$\widehat{\mathscr{O}}_x = \varprojlim R/I_x^n$$

is the complete local ring of S along x. Because $x \in S_0$, we know that $f \equiv 0 \bmod \widehat{I}_x$, what we need to prove is that $f = 0$ in $\widehat{\mathscr{O}}_x$. Observe that by passage to the inverse limit, we only need to treat the case that $f \equiv 0 \bmod I_x/I_x^n$ and to prove $f = 0$ in R/I_x^n.

Recall our assumption that R is of finite type over $\mathbb{Z}$, we claim that the artinian ring R/I_x^n has positive characteristic. Indeed, if the restriction of I_x on $\mathbb{Z}$ is the zero ideal, then the field R/I_x contains $\mathbb{Z}$ as a subring, hence has characteristic 0. But $\mathbb{Q}$ is obviously not of finite type over $\mathbb{Z}$, which leads to a contradiction. So $\mathbb{Z} \cap I_x$ is a maximal ideal of $\mathbb{Z}$, which shows that $\mathbb{Z} \cap I_x = (\ell)$ for some prime ℓ. Hence R/I_x^n is a finite $\mathbb{Z}/\ell\mathbb{Z}$-algebra, its characteristic is a power of ℓ, i.e., ℓ is nilpotent in R/I_x^n.

Now applying Drinfeld's Strictness Lemma 8.4.4, since the ideal $(I_x/I_x^n, \ell)$ is nilpotent in R/I_x^n. Therefore $S_0 \subset S$ is both open and closed, hence a union of connected components of S. On other components, f is fiber-wise flat, hence flat by the fiber-wise criterion of flatness. Plus that f is finite (quasi-finite and proper), over a noetherian base scheme S, f then is finite locally free, it is certainly an isogeny. □

Definition 8.4.6. *Let $\phi : E_1 \to E_2$ be an isogeny of elliptic curves over S. The **dual isogeny** ϕ^t of ϕ is defined as the composition*

$$\begin{tikzcd}
E_2 \arrow[r, "\sim"] \arrow[rrr, bend right, "\phi^t"'] & \mathsf{Pic}^{(0)}_{E_2/S} \arrow[r, "\phi^*"] & \mathsf{Pic}^{(0)}_{E_1/S} \arrow[r, "\sim"] & E_1.
\end{tikzcd}$$

Remark: The dual isogeny ϕ^t of an isogeny ϕ is indeed a S-homomorphism, by Theorem 8.4.5, it is Zariski-locally 0 or an isogeny. The fact that ϕ is an isogeny implies that locally it has positive constant rank, and after checking ϕ^t on any geometric fiber, it also has positive rank. Therefore ϕ^t is indeed an isogeny.

Proposition 8.4.7. *Let E/S be an elliptic curve over an arbitrary scheme S. The S-group scheme structure on E/S is unique, with the zero section 0 as the unit.*

Proof: Suppose we have a structure of S-group scheme $(E/S, m, i, e)$ on E, where m is the composition morphism, and i is the inverse morphism. We denote the structure of S-group scheme from Abel's Theorem 8.1.2 by $(E/S, +, -, e)$, and call it the "canonical" group structure. We have to show that the morphism ϕ_P defined by

$$\begin{array}{rcl} \phi_P(S): \ E(S) & \longrightarrow & E(S) \\ Q & \longmapsto & m(P,Q) - P \end{array}$$

is identity for any point $P \in E(S)$. Observe that ϕ_P is an isomorphism of the S-scheme E, since we have the inverse

$$\begin{array}{rcl} \phi_P^{-1}(S): \ E(S) & \longrightarrow & E(S) \\ Q & \longmapsto & m\big(P + Q, i(P)\big) \end{array}$$

Because ϕ_P fixes the zero section, the diagram

$$\begin{tikzcd} E(S) \arrow[r, "\phi_P(S)"] \arrow[d, "\wr"] & E(S) \arrow[d, "\wr"] \\ \mathsf{Pic}^{(0)}_{E/S}(S) \arrow[r, "(\phi_P^{-1})^*(S)"] & \mathsf{Pic}^{(0)}_{E/S}(S) \end{tikzcd}$$

commutes, which shows that ϕ_P is an isomorphism with respect to the "canonical" group structure. Consider the morphism

$$\begin{array}{rcl} \Phi(S): \ E_E(S) & \longrightarrow & E_E(S) \\ (P,\ Q) & \longmapsto & (P,\ \phi_P(Q)) \end{array}$$

which is an E-isomorphism of the elliptic curve E_E. The morphism $\Phi - \mathsf{id}$ is an E-homomorphism, hence by Theorem 8.4.5, it is locally either 0 or an isogeny. It is indeed 0 on the zero section of E_E, so $\Phi - \mathsf{id}$ is 0 in a Zariski open neighborhood of the zero section. But since the intersection of this neighborhood with each E (view as fibers of E_E over E) is a Zariski open neighborhood of 0 in E, which implies that $\Phi - \mathsf{id}$ is 0 on each fiber E of E_E, i.e., $\phi_P = \mathsf{id}$ for each $P \in E(S)$. □

Lemma 8.4.8. *Let $\phi: E_1 \to E_2$ be an isogeny of elliptic curves over an arbitrary scheme S, and ϕ^t is its dual isogeny. Then*

$$\phi^t \circ \phi \ = \ [deg(\phi)], \quad (\phi^t)^t \ = \ \phi,$$

and ϕ^t is the unique isogeny with these properties. In particular, $deg(\phi^t) = deg(\phi)$.

Proof: Denote $\deg(\phi) = N$. Let P be any S-valued point in $E_1(S)$. Then

$$\begin{array}{rcl} \phi^t(\phi(P)) & = & \phi^*\big(\mathscr{O}_{E_2}(\phi(P)) \otimes \mathscr{O}_{E_2}(-0_2)\big) \\ & = & \phi^*\big(\mathscr{O}_{E_2}(\phi(P))\big) \otimes \phi^*\big(\mathscr{O}_{E_2}(-0_2)\big) \\ & = & \mathscr{O}_{E_1}(P + \phi^*(0_2)) \otimes \mathscr{O}_{E_1}(-\phi^*(0_2)). \end{array}$$

By Lemma 7.4.3, fppf-locally on S, we can write the pull-back effective Cartier divisor $\phi^*(0_2)$ as

$$\phi^*(0_2) \ = \ [Q_1] + ... + [Q_N],$$

then [7]

$$\begin{aligned}\mathscr{O}_{E_1}(P+\phi^*(0_2)) &= \mathscr{O}_{E_1}([P+Q_1]+...+[P+Q_N]) \\ &= \mathscr{O}_{E_1}([P+Q_1])\otimes...\otimes\mathscr{O}_{E_1}([P+Q_N])\end{aligned}$$

and hence

$$\phi^t(\phi(P)) \;=\; \prod_{i=1}^{N}\mathscr{O}_{E_1}(P+Q_i)\otimes\mathscr{O}_{E_1}(-Q_i).$$

Notice that

$$\mathscr{O}_{E_1}(P+Q_i)\otimes\mathscr{O}_{E_1}(-Q_i) \;\simeq\; \mathscr{O}_{E_1}(P)\otimes\mathscr{O}_{E_1}(-0_1)$$

for any $1\leqslant i\leqslant N$, so they are equal in $\mathsf{Pic}^{(0)}_{E_1/S}$, which shows

$$\phi^t(\phi(P)) = \big(\mathscr{O}_{E_1}(P)\otimes\mathscr{O}_{E_1}(-0_1)\big)^{\otimes N} = [N](P),$$

i.e., $\phi^t\circ\phi=[N]$. If there is another isogeny ϕ' such that $\phi'\circ\phi=[N]$, it is clear that

$$(\phi^t-\phi')\circ\phi \;=\; [0].$$

By counting ranks, the rank of $\phi^t-\phi'$ must be 0 everywhere, hence it is itself 0, i.e., $\phi'=\phi^t$.

From the uniqueness, we can deduce some facts. According to Theorem 8.4.1, the degree of $[N]$ is N^2, and since

$$[N]\circ[N] \;=\; [N^2],$$

$[N]$ is self-dual, i.e., $[N]^t=[N]$. Also, the dual isogeny of a composition is

$$(\phi\circ\psi)^t \;=\; \psi^t\circ\phi^t.$$

Now it is immediate to show the second property:

$$\phi^t\circ\phi \;=\; [N] \;=\; [N]^t \;=\; (\phi^t\circ\phi)^t \;=\; \phi^t\circ(\phi^t)^t,$$

which implies $\deg\big(\phi-(\phi^t)^t\big)=0$, i.e., $(\phi^t)^t=\phi$. □

Proposition 8.4.9. *Any S-morphism $\phi: E_1\to E_2$ of elliptic curves $E_1/S, E_2/S$ with $\phi(0_1)=0_2$ is a S-homomorphism.*

Proof: It amounts to prove that for any S-scheme T, and any T-valued points $P,Q\in E(T)$,

$$\phi(P+Q) \;=\; \phi(P)+\phi(Q),$$

i.e., to show that

$$\begin{aligned}\Psi: E(T)\times E(T) &\longrightarrow E'(T)\\ (P,Q) &\longmapsto \phi(P+Q)-\phi(P)-\phi(Q)\end{aligned}$$

is zero morphism. The question is local on S, as usual, we assume $S=\mathsf{Spec}\,(R)$ with R of finite type over $\mathbb{Z}$. Through the faithfully flat morphism

$$\coprod_{x\,\in\,\mathrm{Specm}\,(R)}\mathsf{Spec}\,(\widehat{\mathscr{O}}_x) \longrightarrow \mathsf{Spec}\,(R),$$

[7] The notation here is a little bit awkward. The “+” in $P+Q_i$ is the addition of the group structure of E_1, while another “+” in $[P+Q_1]+...+[P+Q_N]$ means the addition of Cartier divisors.

where $\widehat{\mathscr{O}}_x$ is the complete local ring of S long the closed point x, the question is then reduced to the case where S is the spectrum of a complete local ring with finite residue field. We can furthermore reduce the question to the case of artinian local ring with finite residue field, by passage to the limit. So now we assume that R is an artinian local ring with finite residue field k of characteristic $p > 0$.

If $\phi_k : E_k \to E'_k$ is zero morphism, then for any R-algebra A and any A-valued point $P_A \in E(A)$, the image $\phi(P_A)$ must lie in the kernel

$$\ker\left\{E'(A) \longrightarrow E'(A/\mathfrak{m}A)\right\},$$

where $\mathfrak{m}$ is the maximal ideal of R. Applying the same argument we used in Lemma 8.4.4 and Theorem 8.4.5, there exists p^n for some integer $n \geqslant 1$ which is independent of A, such that p^n kills the kernel, i.e., $p^n\phi(P_A) = 0$. This means that the image of ϕ lies in the p^n-torsion subgroup scheme $E'[p^n]$. Since $E'[p^n]$ is finite over the affine base $\mathsf{Spec}\,(R)$, it is affine. While E is connected and proper (or even projective) over $\mathsf{Spec}\,(R)$, the morphism

$$\phi\colon\ E \ \longrightarrow\ E'[p^n]$$

has to be constant, therefore $\phi = 0$. In this case, ϕ is trivially a S-homomorphism.

If $\phi_k \neq 0$, as ϕ_k is a morphism between smooth curves over a field k, it is finite flat. It is immediate that ϕ is also flat, by the fiber-wise criterion of flatness. And ϕ is also finite, since it is quasi-finite and proper. So ϕ is an isogeny. Applying the dual isogeny ϕ^t to Ψ:

$$\phi^t \circ \Psi(P,Q) \ = \ \phi^t(\phi(P+Q) - \phi(P) - \phi(Q)) \ = \ [N](P+Q) - [N](P) - [N](Q) \ = \ 0,$$

i.e., Ψ takes values in $E'[\mathsf{deg}(\phi^t)]$, which is an affine scheme. Hence as we argued before, Ψ must be constant, which can only be $\Psi = 0$. □

Lemma 8.4.10. *Let $\phi, \phi' : E_1 \to E_2$ be S-homomorphisms of elliptic curves over S. Then*

$$(\phi + \phi')^t \ = \ \phi^t + \phi'^t.$$

Proof: Applying the base change $E_1 \to S$ to E_2, the two S-morphisms ϕ, ϕ' induce two E_1-valued points $\bar\phi, \bar\phi'$ of $(E_2)_{E_1}$:

$$\begin{tikzcd}
E_1 \arrow[drr, bend left, "\phi,\phi'"] \arrow[dr, dashed, "\bar\phi,\bar\phi'"] \arrow[ddr, bend right, "\mathsf{id}"'] & & \\
& E_2 \times_S E_1 \arrow[r, "\mathrm{pr}_1"] \arrow[d, "\mathrm{pr}_2"] & E_2 \arrow[d] \\
& E_1 \arrow[r] & S
\end{tikzcd}$$

The lemma amounts to show that for any point $Q \in E_2(S)$,

$$(\phi + \phi')^t(Q) \ = \ (\phi^t + \phi'^t)(Q),$$

i.e.,

$$\phi^*(\mathscr{L}) \otimes \phi'^*(\mathscr{L}) \ = \ (\phi + \phi')^*(\mathscr{L}) \otimes 0^*(\mathscr{L})$$

in $\mathsf{Pic}^{(0)}_{E_1/S}(S)$, for any invertible sheaf $\mathscr{L} \in \mathsf{Pic}^{(0)}_{E_2/S}(S)$ of fiber-wise degree 0. Thus lemma is reduced to the following question:

> Let $\pi : E \to S$ be an elliptic curve over S, and $P, Q \in E(S)$ are two points. Then for any invertible sheaf $\mathscr{L}$ on E which has fiber-wise degree 0, we have the isomorphism $P^*(\mathscr{L}) \otimes Q^*(\mathscr{L}) \simeq (P+Q)^*(\mathscr{L}) \otimes 0^*(\mathscr{L})$.

Clearly, the statement only depends on the equivalent class of $\mathscr{L}$, hence we may assume $\mathscr{L} = \mathscr{I}^{-1}(R) \otimes \mathscr{I}(0)$ for some point $R \in E(S)$. Let r_P be the transformation on $\mathscr{L}$ by P, then we have $P = r_P \circ 0$, and the isomorphism which we are trying to prove becomes

$$\mathscr{O}_S \simeq 0^*\big(r_P^*(\mathscr{L}) \otimes r_Q^*(\mathscr{L}) \otimes r_{P+Q}^*(\mathscr{L}^{-1}) \otimes \mathscr{L}^{-1}\big),$$

substitute $\mathscr{L} = \mathscr{I}^{-1}(R) \otimes \mathscr{I}(0)$ into it:

$$\begin{aligned} & r_P^*(\mathscr{L}) \otimes r_Q^*(\mathscr{L}) \otimes r_{P+Q}^*(\mathscr{L}^{-1}) \otimes \mathscr{L}^{-1} \\ = \ & \big(\mathscr{I}^{-1}(R-P) \otimes \mathscr{I}^{-1}(R-Q) \otimes \mathscr{I}(R-P-Q) \otimes \mathscr{I}(R)\big) \\ & \otimes \big(\mathscr{I}(-P) \otimes \mathscr{I}(-Q) \otimes \mathscr{I}^{-1}(-P-Q) \otimes \mathscr{I}^{-1}(0)\big) \\ = \ & \pi^*(\mathscr{L}_0) \otimes r_R^*(\pi^*(\mathscr{L}_0))^{-1} = \mathscr{O}_E, \end{aligned}$$

where $\mathscr{L}_0$ is some invertible sheaf on S. □

Consider a S-endomorphism $\phi : E \to E$ of an elliptic curve over a connected scheme S. By previous lemma,

$$[\deg(1+\phi)] = (1+\phi)^t \circ (1+\phi) = (1+\phi^t) \circ (1+\phi) = [1+\deg(\phi)] + (\phi + \phi^t),$$

hence $\phi + \phi^t = [\deg(1+\phi) - \deg(\phi) - 1] =: [m]$. We define this integer $\mathrm{tr}(\phi) := m$ to be the **trace** of the isogeny ϕ.

Theorem 8.4.11. *Let ϕ be an S-endomorphism of an elliptic curve E/S over a connected scheme S. Then*

(1) The isogeny ϕ is a root of

$$X^2 - tr(\phi)X + deg(\phi) = 0$$

in the endomorphism ring of E/S.

(2) $\big(tr(\phi)\big)^2 \leqslant 4deg(\phi)$.

Proof: (1) It is immediate to check that

$$\phi^2 - (\phi + \phi^t) \circ \phi + \phi^t \circ \phi = 0.$$

(2) Consider the S-endomorphism $[n] - [m] \circ \phi$, its degree is non-negative, hence

$$[\deg([n] - [m] \circ \phi)] = ([n] - \phi^t \circ [m]) \circ ([n] - [m] \circ \phi) = [n^2 - \mathrm{tr}(\phi) \cdot nm + \deg(\phi) \cdot m^2],$$

which indicates that

$$n^2 - \mathrm{tr}(\phi) \cdot nm + \deg(\phi) \cdot m^2 \geqslant 0$$

for any integers n, m. This is equivalent to the inequality $\big(\mathrm{tr}(\phi)\big)^2 \leqslant 4\deg(\phi)$. □

Using Theorem 8.4.11, we can prove some rigidity results of various level structures on an elliptic curve, which will be applied to prove the representability (i.e., the existence of fine moduli spaces) of various moduli stacks of elliptic curves.

Corollary 8.4.12 (Rigidity of $\Gamma(N)$-structures)**.** *Let ϕ be an S-automorphism of an elliptic curve E/S over a connected scheme S, and $N \geqslant 2$ is an integer. If ϕ induces the identity on the N-torsion S-subgroup scheme $E[N]$, then:*

(1) If $N \geqslant 3$, then $\phi = id$;

(2) If $N = 2$, then $\phi = \pm id$.

Proof: The N-torsion S-subgroup scheme $E[N]$ is contained in the kernel of the S-homomorphism $\phi - 1$, hence there exists a S-endomorphism ψ such that $\phi - 1 = \psi \cdot N$. Then we have

$$\begin{cases} \mathrm{tr}(\phi) = 2 + N \cdot \mathrm{tr}(\psi) \\ \deg(\phi) = 1 + N \cdot \mathrm{tr}(\psi) + N^2 \cdot \deg(\psi) \end{cases}$$

Using the inequality from Theorem 8.4.11, and that $\deg(\phi) = 1$, the second equality gives

$$N^2 \cdot (\deg(\psi))^2 \leqslant 4\deg(\psi),$$

hence if $N \geqslant 3$, then $\deg(\psi) = 0$, i.e., $\phi = 1 + \psi \cdot N = \mathrm{id}$.

If $N = 2$, then $\deg(\psi) \leqslant 1$, i.e., $\deg(\psi) = 0$ or 1. If $\deg(\psi) = 1$, substitute this into the first equality, we have $\mathrm{tr}(\psi) = -2$. Thus

$$\deg(\phi + 1) = 1 + \mathrm{tr}(\phi) + \deg(\phi) = 0,$$

i.e., $\phi = -\mathrm{id}$. □

Corollary 8.4.13 (Rigidity of $\Gamma_1(N)$-structures)**.** *Let ϕ be an S-automorphism of an elliptic curve E/S over a connected scheme S, $N \geqslant 4$ is an integer, and $G \subset E$ is a closed S-subgroup scheme which is finite locally free over S of rank N. If ϕ induces the identity on G, then:*

(1) If $N \geqslant 5$, then $\phi = id$;

(2) If $N = 4$, then $\phi = \pm id$. Moreover, if $\phi = -id$, then $G = E[2]$.

In particular, if G is a cyclic S-subgroup scheme, then $\phi = id$ for any $N \geqslant 4$.

Proof: The S-subgroup scheme G is contained in the kernel of the S-homomorphism $\phi - 1$, hence

$$\deg\,(\phi - 1) \equiv 0 \pmod N$$

and $\mathrm{tr}(\phi) \equiv 0 \bmod N$.

If $N \geqslant 5$, it forces $\mathrm{tr}(\phi) = 2$, so $\deg(\phi - 1) = 2 - \mathrm{tr}(\phi) = 0$, i.e., $\phi = \mathrm{id}$.

If $N = 4$, and $\mathrm{tr}(\phi) = -2$, we have $\deg(\phi + 1) = 2 + \mathrm{tr}(\phi) = 0$, hence $\phi = -\mathrm{id}$. And since $1 - \phi = 2$ kills G, which implies $G \subset E[2]$, but they have the same rank, so $G = E[2]$.

If G is cyclic, then the situation $G = E[2]$ cannot happen, so it can only be $\phi = \mathrm{id}$ for any $N \geqslant 4$. □

8.5 The Weil pairing

Let E/S be an elliptic curve over an arbitrary scheme S, name its structural morphism and the zero section as

$$\begin{tikzcd} E \arrow[d, "f"] \\ S \arrow[u, bend left, "0"] \end{tikzcd}$$

We now introduce the *normalized cocycles* in order to describe the relative Picard group $\mathrm{Pic}_{E/S}$, following Katz [23].

We claim that the relative Picard group $\mathrm{Pic}_{E/S}(S)$ can be viewed as a subgroup of the (absolute) Picard group $\mathrm{Pic}(E)$, as the kernel:

$$\ker\left\{0^* : \mathrm{Pic}(E) \longrightarrow \mathrm{Pic}(S)\right\}.$$

Explicitly, we can define a map

$$\begin{array}{rcl} \ker\left\{0^* : \mathrm{Pic}(E) \longrightarrow \mathrm{Pic}(S)\right\} & \longrightarrow & \mathrm{Pic}_{E/S}(S) \\ \mathscr{L} & \longmapsto & [\mathscr{L}] \end{array}$$

and it is straightforward to see that it has the inverse

$$\begin{array}{rcl} \mathrm{Pic}_{E/S}(S) & \longrightarrow & \ker\left\{0^* : \mathrm{Pic}(E) \longrightarrow \mathrm{Pic}(S)\right\} \\ [\mathscr{L}] & \longmapsto & \mathscr{L} \otimes f^*(0^*\mathscr{L}). \end{array}$$

Let $\mathscr{O}_E^\times$ be the sheaf of invertible functions. Define the subsheaf $K_E^\times \subset \mathscr{O}_E^\times$, consisting of functions which take the value 1 along the zero section 0. It fits into the short exact sequence:

$$0 \longrightarrow K_E^\times \longrightarrow \mathscr{O}_E^\times \longrightarrow 0_*\mathscr{O}_E^\times \longrightarrow 0,$$

and induces the long exact sequence of cohomology:

$$\dots \xrightarrow{0} H^1(E, K_E^\times) \longrightarrow \mathrm{Pic}(X) \xrightarrow{0^*} \mathrm{Pic}(S) \longrightarrow \dots$$

which indicates that

$$\mathrm{Pic}_{E/S}(S) \simeq H^1(E, K_E^\times).$$

Let $E/S, E'/S$ be elliptic curves over an arbitrary scheme S, and $\phi : E \to E'$ is an isogeny of rank N. Then we have the dual isogeny

$$\begin{tikzcd} (E,0) \arrow[r, shift left, "\phi"] & (E',0') \arrow[l, shift left, "\phi^t"] \end{tikzcd}$$

Then there exists a bilinear pairing:

$$\begin{array}{rcl} \ker(\phi) \times \ker(\phi^t) & \longrightarrow & \mu_N \subset \mathbb{G}_m \\ (P,\ P') & \longmapsto & <P,\ P'>_\phi \end{array}$$

which takes values in the group scheme of N-th roots of unity.

A S-valued point $P' \in \mathsf{ker}(\phi^t)(S)$ is given by an invertible sheaf $\mathscr{L} \in \mathsf{Pic}^{(0)}_{E'/S}(S)$ such that $\phi^*\mathscr{L} = 0$ in $\mathsf{Pic}^{(0)}_{E/S}(S)$. Choose an open covering $\{U_i\}$ of E', then $\mathscr{L}$ is represented by a normalized cocycle in $H^1(E', K^\times_{E'})$

$$f_{ij} \in K^\times_{E'}(U_i \cap U_j),$$

and $\phi^*\mathscr{L} = 0$ means that the normalized cocycle

$$f_{ij} \circ \phi \in K^\times_E\big(\phi^{-1}(U_i) \cap \phi^{-1}(U_j)\big)$$

is a coboundary, i.e., there are $h_i \in K^\times_E(\phi^{-1}(U_i))$ such that $f_{ij} \circ \phi = \frac{h_i}{h_j}$.

For a S-valued point $P \in \mathsf{ker}(\phi)(S)$, we view it as a morphism $P : S \to E$. Over each open subset $(\phi \circ P)^{-1}(U_i)$ of S, we have a function $h_i \circ P$. Since $\phi(P) = e'$, we have

$$\frac{h_i \circ P}{h_j \circ P} = f_{ij} \circ \phi \circ P = 1,$$

and hence all $h_i \circ P$ can be glued to a global function $h(P)$ on S, which lies in $\mathscr{O}^\times_S(S) = \mathbb{G}_m(S)$. This gives the pairing:

$$\begin{array}{rcl} \mathsf{ker}(\phi) \times \mathsf{ker}(\phi^t) & \longrightarrow & \mathbb{G}_m \\ (P,\ P') & \longmapsto & <P,\ P'>_\phi := h(P) \end{array}$$

moreover, the image must lie in μ_N because N kills $\mathsf{ker}(\phi)$.

Definition 8.5.1. *The pairing* $< \cdot, \cdot >_\phi$ *is called the* ***Cartier pairing*** *of the isogeny* ϕ.

Lemma 8.5.2. *The Cartier pairing is bilinear, alternating and non-degenerate.*

Proof: See Oda [32].

Lemma 8.5.3. *Let* ϕ, ϕ' *be isgenies of elliptic curves over S:*

$$\begin{tikzcd} E \arrow[r, shift left, "\phi"] & E' \arrow[l, shift left, "\phi^t"] \arrow[r, shift left, "\phi'"] & E'' \arrow[l, shift left, "\phi'^t"] \end{tikzcd}$$

Then for any points $P \in ker(\phi)(S)$, $P'' \in ker(\phi^t \circ \phi'^t)(S)$, *we have*

$$<P,\ P''>_{\phi^t \circ \phi'^t} = <P,\ \phi'^t(P'')>_\phi .$$

Proof: Suppose the point P'' is represented by the normalized cocycle $\{f_{ij}\}$ in $H^1(E'', K^\times_{E''})$ with respect to some covering of E'', such that the cocycle $\{f_{ij} \circ (\phi' \circ \phi)\}$ is a coboundary in $H^1(E, K^\times_E)$, i.e., there are h_i such that $f_{ij} \circ (\phi' \circ \phi) = \frac{h_i}{h_j}$. It is straightforward that the point $\phi'^t(P'')$ is given by the pull-back cocyle $\{f_{ij} \circ \phi'\}$, and $\{(f_{ij} \circ \phi') \circ \phi\}$ is also the coboundary of $\{h_i\}$, i.e., the gluing global function h is identified, therefore the two Cartier pairings give the same result $h(P)$. □

Definition 8.5.4. *The Cartier pairing $e_N :=< \cdot, \cdot >_{[N]}$ for the isogeny $[N] : E \to E$ is called the* ***Weil pairing****, which is an alternating and non-degenerate bilinear form on the N-torsion subgroup scheme $E[N]$.*

Corollary 8.5.5. *Let $\phi : E \to E'$ be an isogeny of elliptic curves over S, which has rank N. Let $P \in$ ker$(\phi)(S)$ and $Q \in E[N](S)$ be S-valued points, then*

$$e_N(P, Q) = < P, \phi(Q) >_\phi .$$

8.6 The Serre-Tate theorem

In this section, we present Drinfeld's short proof of Serre-Tate theorem. The proof is originated from Drinfeld's paper [34], and also exposed in Katz's article [23].

Through out this section, we fix a ring R, an integer $N \geqslant 1$ who kills R, and a nilpotent ideal $I \subset R$, i.e., $I^{k+1} = 0$ for some integer $k \geqslant 0$. And we denote $R_0 = R/I$.

For any functor G defined on the category of R-algebras R-$\mathfrak{Alg}$, we define a subfunctor G_I as

$$G_I(B) := \ker \left\{ G(B) \longrightarrow G(B/IB) \right\}$$

for any R-algebra B, and we define its *formal completion*:

$$\widehat{G}(B) := \ker \left\{ G(B) \longrightarrow G(B_{\text{red}}) \right\}$$

where B_{red} is the reduced R-algebra associated to B, i.e., $B_{\text{red}} = B/\text{nilrad}(B)$.

Lemma 8.6.1. *Let G be a fppf abelian sheaf over $S =$ Spec (R), such that its formal completion $\widehat{G}$ is locally represented by a commutative formal Lie group over R, then N^k kills G_I.*

Proof: Fix (locally) a set of parameters of $\widehat{G}$, i.e., fix a local isomorphism

$$\widehat{G} \simeq \mathsf{Spf}\left(R[\![X_1, ..., X_m]\!]\right),$$

then the morphism of multiplication by N has the form:

$$\left([N](X)\right)_i = N \cdot X_i + \text{higher terms}.$$

Suppose B is a R-algebra. Any point in $\widehat{G}_I(B)$ has coordinates in IB, and since N kills R, we have $[N](\widehat{G}_I) \subset \widehat{G}_{I^2}$, therefore

$$[N^k](\widehat{G}_I) \subset \widehat{G}_{I^{k+1}} = 0.$$

Finally, since G_I lies in the formal completion $\widehat{G}$, we have $G_I = \widehat{G}_I$, hence N^k kills G_I. □

Lemma 8.6.2. *Let G, H be fppf abelian sheaves over Spec (R), such that G is N-divisible, H is formally smooth, and $\widehat{H}$ is locally represented by a commutative formal Lie group. Denote $G_0 = G \otimes_R R_0$ and $H_0 = H \otimes_R R_0$. Then:*

(1) The homomorphism groups $\mathsf{Hom}_R(G,H), \mathsf{Hom}_{R_0}(G_0,H_0)$ *have no* N*-torsions;*

(2) The homomorphism by mod I

$$\mathsf{Hom}_R(G,\ H) \longrightarrow \mathsf{Hom}_{R_0}(G_0,\ H_0)$$

is injective;

(3) For any R_0*-homomorphism* $\phi_0 \in \mathsf{Hom}_{R_0}(G_0,H_0)$*, there exists a unique lifting of* $N^k \cdot \phi_0$ *in* $\mathsf{Hom}_R(G,H)$*;*

(4) A R_0*-homomorphism* $\phi_0 \in \mathsf{Hom}_{R_0}(G_0,H_0)$ *has a lifting in* $\mathsf{Hom}_R(G,H)$ *if and only if the (unique) lifting of* $N^k \cdot \phi_0$ *kills* $G[N^k]$*.*

Proof: (1) Since G (resp. G_0) is N-divisible, any N-torsion in $\mathsf{Hom}_R(G,H)$ (resp. $\mathsf{Hom}_{R_0}(G_0,H_0)$)is identically zero.

(2) The kernel of the mod I map is $\mathsf{Hom}_R(G,H_I)$. By Lemma 8.6.1, H_I is killed by N^k. Since G is N-divisible, the kernel must be zero.

(3) We construct a lifting of $N^k \cdot \phi_0$ explicitly. Observe that there is a well-defined R-homomorphism

$$H(B/IB) \xrightarrow{N^k} H(B)$$

for any R-algebra B, which is defined as following: Given an element $h_0 \in H(B/IB)$, pick any lifting $h \in H(B)$ of h_0 (this is possible by the formal smoothness condition), then the image of h_0 in $H(B)$ is $N^k \cdot h$. This is indeed well-defined, since N^k kills H_I. Now we can construct a lifting ϕ_{N^k} of $N^k \cdot \phi_0$, as the composition

$$\begin{tikzcd}
G(B/IB) \arrow[r, "\phi_0"] & H(B/IB) \arrow[d, "N^k"] \\
G(B) \arrow[u, "\text{mod } I"] \arrow[r, "\phi_{N^k}"] & H(B)
\end{tikzcd}$$

The uniqueness of the lifting is ensured by (2).

(4) *The "only if" part*: If ϕ_0 admits a lifting $\phi \in \mathsf{Hom}_R(G,H)$, by uniqueness, ϕ_{N^k} (the lifting of $N^k \cdot \phi_0$) must be coincide with $N^k \cdot \phi$, which certainly kills $G[N^k]$.

The "if" part: Since ϕ_{N^k} kills $G[N^k]$, through the short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & G[N^k] \arrow[r, hook] & G \arrow[r, "N^k"] \arrow[dr, "\phi_{N_k}"'] & G \arrow[r] \arrow[d, dotted, "\phi"] & 0 \\
& & & H &
\end{tikzcd}$$

we can construct a morphism $\phi : G \to H$ to make above diagram commutative, which is given by the quotient of ϕ_{N_k}

$$G \simeq G/G[N^k] \longrightarrow H.$$

Such a morphism ϕ is indeed a lifting of ϕ_0, since we know that

$$N^k \cdot (\phi \otimes R_0) = N^k \cdot \phi_0,$$

and there are no torsions in $\mathrm{Hom}_{R_0}(G_0, H_0)$ by (1), it must be $\phi \otimes R_0 = \phi_0$. □

Remark: Notice that in the proof of (3), we did not use the condition that G is N-divisible. So practically it works not only for p-divisible groups, but also for any abelian schemes.

From now on, we suppose $N = p^n$. Let $\mathscr{A}(R)$ be the category of abelian schemes over R. We define a category $\mathbf{Def}(R, R_0)$, whose objects are triples (A_0, G, ϵ), where A_0 is an abelian scheme over R_0, G is a p-divisible group over R, and ϵ is an isomorphism

$$\epsilon :\ G_0 \xrightarrow{\sim} A_0[p^\infty]$$

of p-divisible groups over R. A morphism in $\mathbf{Def}(R, R_0)$

$$(A_0, G, \epsilon) \xrightarrow{(\phi_0, \psi)} (A_0', G', \epsilon')$$

is given by a morphism $\phi_0 : A_0 \to A_0'$ of abelian schemes and a morphism $\psi : G \to G'$ of p-divisible groups, such that the diagram

$$\begin{tikzcd}
G_0 \arrow[r, "\epsilon"] \arrow[d, "\psi_0"'] & A_0[p^\infty] \arrow[d, "\phi_0[p^\infty]"] \\
G_0' \arrow[r, "\epsilon'"] & A_0'[p^\infty]
\end{tikzcd}$$

commutes.

Now we are ready to prove the Serre-Tate Theorem:

Theorem 8.6.3 (Serre-Tate)**.** *The functor*

$$\begin{array}{rcl} \mathscr{A}(R) & \longrightarrow & \mathbf{Def}(R, R_0) \\ A & \longmapsto & (A_0, A[p^\infty], id_{A_0[p^\infty]}) \end{array}$$

defines an equivalence of categories.

Proof: *"Full faithfulness"*: Suppose we are given abelian schemes A, B over R, and a morphism of triples

$$(\phi_0, \phi[p^\infty]) :\ (A_0, A[p^\infty], \mathrm{id}_{A_0[p^\infty]}) \longrightarrow (B_0, B[p^\infty], \mathrm{id}_{B_0[p^\infty]}),$$

we need to check that ϕ_0 and $\phi[p^\infty]$ are both induced by a unique R-morphism $\phi : A \to B$. By Lemma 8.6.2 (3), there is a unique lifting $\phi_{p^{nk}}$ of $p^{nk} \cdot \phi_0$. We must have

$$\phi_{p^{nk}}[p^\infty] = p^{nk} \cdot (\phi[p^\infty]),$$

since they are both liftings of $p^{nk} \cdot \phi_0[p^\infty]$. Thus $\phi_{p^{nk}}$ kills $A[p^{nk}]$, so by Lemma 8.6.2 (4), there exists a morphism $\phi : A \to B$ such that $\phi_{p^{nk}} = p^{nk} \cdot \phi$. The morphism ϕ is indeed a lifting of ϕ_0, and $\phi\big|_{A[p^\infty]} = \phi[p^\infty]$. The uniqueness is ensured by Lemma 8.6.2 (2).

"Essential surjectivity": It remains to prove that, given any triple (A_0, G, ϵ), there exists an abelian scheme A such that $A \otimes R_0 \simeq A_0$ and

$$(A_0, G, \epsilon) \simeq (A_0, A[p^\infty], \mathrm{id}_{A_0[p^\infty]}).$$

By Grothendieck's result (cf. Illusie [7] Theorem 8.5.23), there exists a lifting B of A_0 in $\mathscr{A}(R)$, with an isomorphism

$$\alpha_0 : B_0 \xrightarrow{\sim} A_0.$$

The isomorphism α_0 induces an isomorphism of p-divisible groups

$$\alpha_0[p^\infty] : B_0[p^\infty] \xrightarrow{\sim} A_0[p^\infty].$$

Consider the liftings for $p^{nk} \cdot \alpha_0[p^\infty]$ and $p^{nk} \cdot \alpha_0^{-1}[p^\infty]$:

$$B[p^\infty] \xrightarrow{F} G \xrightarrow{F^t} B[p^\infty],$$

where $F_0 = \epsilon^{-1} \circ p^{nk} \cdot \alpha_0[p^\infty]$, and $F_0^t = \epsilon^{-1} \circ p^{nk} \cdot \alpha_0^{-1}[p^\infty]$. Observe that, we can use the same argument in the proof of Proposition 8.4.9, to show that F (resp. F^t) is an isogeny of p-divisible groups. As $F \circ F^t = [p^{2nk}]$, F^t is indeed the dual isogeny of F. Let K be the kernel of F:

$$0 \longrightarrow K \longrightarrow B[p^\infty] \xrightarrow{F} G \longrightarrow 0,$$

i.e., the finite locally free closed subgroup scheme K is killed by F. Let $A = B/K$, we claim that A is the required lifting of A_0. Indeed, K is a lifting of $B_0[p^{nk}]$:

$$\begin{tikzcd}
0 \arrow[r] & K_0 \arrow[r] & B_0[p^\infty] \arrow[r, "p^{nk}\cdot\alpha_0{[p^\infty]}"] \arrow[dr, "{[p^{nk}]}"'] & A_0[p^\infty] \arrow[r] & 0 \\
& & & B_0[p^\infty] \arrow[u, "\alpha_0{[p^\infty]}"'] &
\end{tikzcd}$$

hence A lifts $B_0/K_0 \simeq B_0 \simeq A_0$, and $A_0[p^\infty] \simeq G_0$, as required. □

Now we consider the 1-dimensional case, i.e., elliptic curves over R. The category of elliptic curves over R is denoted by $\mathbf{Ell}(R)$, and we keep the same notation for the category $\mathbf{Def}(R, R_0)$ for the case of elliptic curves. Furthermore, we define another category $\mathbf{Def}_W(R, R_0)$, which is the category of "deformations with respect to the Weil pairings". The objects of $\mathbf{Def}_W(R, R_0)$ are quadruples $(E_0/R_0, G, \beta, \epsilon)$, where E_0 is an elliptic curve over R_0, G is a p-divisible group over R, $\beta = \{\beta_{p^n}\}$ is a family of alternating bilinear pairings on G, with β_{p^n} defined on each $G[p^n]$:

$$\beta_{p^n} : G[p^n] \times G[p^n] \longrightarrow \mu_{p^n} \subset \mathbb{G}_m,$$

such that

$$\beta_{p^{n-1}}\big([p](P),\ [p](Q)\big) \ = \ \big(\beta_{p^n}(P,\ Q)\big)^p$$

for any $P, Q \in G[p^n](R)$. And ϵ is an isomorphism of p-divisible groups over R

$$\epsilon : G_0 \xrightarrow{\sim} E_0[p^\infty]$$

which is compatible with the pairings β and the Weil pairings e_{p^n}, i.e.,

$$e_{p^n}(\epsilon(P),\ \epsilon(Q)) \ = \ \beta_{p^n}(P,\ Q)$$

for any $P, Q \in G[p^n](R)$. Morphisms in $\mathbf{Def}_W(R, R_0)$ are the same as in $\mathbf{Def}(R, R_0)$.

Theorem 8.6.4 (Serre-Tate)**.** *The functors*

$$\begin{array}{ccccc} \mathbf{Ell}(R) & \longrightarrow & \mathbf{Def}_W(R,R_0) & \longrightarrow & \mathbf{Def}(R,R_0) \\ E & \longmapsto & (E_0, E[p^\infty], id) & & \\ & & (E_0/R_0, G, \beta, \epsilon) & \longmapsto & (E_0/R_0, G, \epsilon) \end{array}$$

define equivalences of categories $\mathbf{Ell}(R)$, $\mathbf{Def}_W(R,R_0)$ *and* $\mathbf{Def}(R,R_0)$.

Proof: The second functor is obviously fully faithful. By Serre-Tate Theorem 8.6.3, the composition is an equivalence of categories, which implies the second functor is also essentially surjective. Therefore the second functor is also an equivalence of categories, which implies immediately that so as the first functor. □

8.7 Tate curves

The *Tate curve* $\mathbf{Tate}(q)$ is a particular curve defined over the ring of formal power series $\mathbb{Z}[\![q]\!]$, whose generic fiber is an elliptic curve over $\mathbb{Z}(\!(q)\!)$.

The motivation of the Tate curve is originated from analytic theory of elliptic curves over $\mathbb{C}$. We know that any elliptic curve $E/\mathbb{C}$ is isomorphic to $\mathbb{C}/\Lambda$ for some rank 2 lattice Λ. This characterization is very useful, because the group structure is pretty obvious, i.e., it is inherited from the additive structure of $\mathbb{C}$. In particular, the lattice Λ is isomorphic to $\mathbb{Z}\oplus\mathbb{Z}\tau$ for some $\Lambda_\tau := \tau \in \mathscr{H}$ in the upper-half plane. Observe that the map $\exp(2\pi i -)$ defines an isomorphism of Riemann surfaces:

$$\exp(2\pi i -) : \mathbb{C}/\Lambda_\tau \xrightarrow{\sim} \mathbb{C}^*/q^{\mathbb{Z}},$$

where $q = e^{2\pi i\tau}$, and $q^{\mathbb{Z}}$ is the free multiplicative subgroup in $\mathbb{C}^*$ generated by q. The complex number q satisfies $|q| < 1$.

Over the ring $\mathbb{Z}(\!(q)\!)$ of Laurent series, we have similar construction, due to J. Tate.

The group schemes $T[N]$ and T

Let $\mathbb{Z}[q,q^{-1}]$ be the ring of Laurent polynomials, and $N \geqslant 1$ an integer. Over $\mathbb{Z}[q,q^{-1}]$, we define a finite flat group scheme $T[N]$, which has rank N^2, and is killed by N. It is the disjoint union of the N schemes $T_i[N]$ for $0 \leqslant i \leqslant N-1$, which is the affine scheme:

$$T_i[N] := \mathrm{Spec}\left(\mathbb{Z}[q,q^{-1}][X]/(X^N - q^i)\right).$$

Hence the group scheme $T[N]$ is $\coprod_{i=0}^{N-1} T_i[N]$, as a $\mathbb{Z}[q,q^{-1}]$-scheme.

Let R be any $\mathbb{Z}[q,q^{-1}]$-algebra such that Spec (R) is connected, then the set of R-valued points $T[N](R)$ is characterized by

$$T[N](R) = \left\{(X, i/N) \,\middle|\, 0 \leqslant i \leqslant N-1,\ X \in R,\ X^N = q^i\right\},$$

and the group structure on it is

$$(X, i/N)\cdot(Y, j/N) = \begin{cases} (XY, i+j/N) & \text{if } i+j \leqslant N-1 \\ (XY/q, i+j-N/N) & \text{if } i+j \geqslant N \end{cases}$$

We have the natural inclusion of group schemes:

$$\begin{array}{rcl} a_N:\ \mu_N(R) & \hookrightarrow & T[N](R) \\ \xi & \longmapsto & (\xi, 0), \end{array}$$

which fits into the short exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \mu_N \arrow[r, "a_N"] & T[N] \arrow[r, "b_N"] & \mathbb{Z}/N\mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

where the morphism b_N is given by

$$b_N(X, i/N) \ = \ i \bmod N.$$

We call this exact sequence the **canonical extension structure** on $T[N]$. Moreover, if the $\mathbb{Z}[q,q^{-1}]$-algebra R contains $q^{\frac{1}{N}}$, then the sequence splits, and we have the explicit isomorphism $T[N](R) \simeq \mu_N(R) \times \mathbb{Z}/N\mathbb{Z}$ given by

$$(X, i/N) = (Xq^{-\frac{i}{N}}, 0) \times (q^{\frac{i}{N}}, i/N) \longmapsto (Xq^{-\frac{i}{N}},\ i \bmod N).$$

Hence over the ring $\mathbb{Z}[q,q^{-1}][q^{\frac{1}{N}}]$, we have the isomorphism of $\mathbb{Z}[q,q^{-1}][q^{\frac{1}{N}}]$-group schemes

$$T[N] \ \simeq \ \mu_N \times \mathbb{Z}/N\mathbb{Z}.$$

There is a unique alternating pairing, which we also call it the **Weil pairing**:

$$\begin{array}{rcl} e_N:\ T[N] \times T[N] & \longrightarrow & \mu_N \\ \big((X, i/N),\ (Y, j/N)\big) & \longmapsto & X^j/Y^i. \end{array}$$

It is compatible with the canonical extension structure on $T[N]$, i.e.,

$$e_N\big(a_N(\xi),\ P\big) \ = \ \xi^{b_N(P)}.$$

Next, we define a $\mathbb{Z}[q,q^{-1}]$-group scheme T, which is smooth of relative dimension 1 over $\mathbb{Z}[q,q^{-1}]$. Still let R be a $\mathbb{Z}[q,q^{-1}]$-algebra such that Spec (R) is connected. The set of R-valued points $T(R)$ is characterized by

$$T(R) \ = \ \big\{(X, \alpha) \bigm| X \in R^\times,\ \alpha \in \mathbb{Q} \cap [0,1)\big\},$$

and the group structure is given by

$$(X,\alpha)\cdot(Y,\beta) \ = \ \begin{cases} (XY, \alpha+\beta) & \text{if } \alpha+\beta < 1 \\ (XY/q, \alpha+\beta-1) & \text{if } \alpha+\beta \geqslant 1 \end{cases}$$

The group scheme T is the disjoint union of $T_\alpha = \mathbb{G}_m$:

$$T \ = \ \coprod_{\alpha \in \mathbb{Q}\cap[0,1)} T_\alpha,$$

and it has a canonical extension structure

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{G}_m \arrow[r] & T \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0. \end{tikzcd}$$

Consider the short exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{G}_m(R)\times\mathbb{Q} & \longrightarrow & T(R) & \longrightarrow & 0 \\ & & n & \longmapsto & (q^n, n) & & & & \\ & & & & (X, a) & \longmapsto & (X/q^{[a]}, \{a\}) & & \end{array}$$

where $[a]$ and $\{a\}$ are the integral and fractional parts respectively. This exact sequence provides a convenient way to calculate the morphism by multiplying N, namely, for any element (X, α) in $T(R)$, we have the formula

$$N\cdot(X, a) \;=\; (X^N/q^{[N\alpha]}, \{N\alpha\}).$$

Thus the group scheme $T[N]$ is naturally the N-torsion subgroup scheme of T.

Theorem 8.7.1. *There is a faithfully flat $\mathbb{Z}[q, q^{-1}]$-algebra R, an elliptic curve E/R and an isomorphism of ind-R-group schemes*

$$T_{tor}\otimes_{\mathbb{Z}[q,q^{-1}]} R \;\simeq\; E_{tor},$$

such that it induces the isomorphism for any $N \geqslant 1$

$$T[N]\otimes_{\mathbb{Z}[q,q^{-1}]} R \;\simeq\; E[N]$$

which is compatible with their Weil pairings.

The Tate curve

Theorem 8.7.2. *There exists an elliptic curve* **Tate**(q) *over $\mathbb{Z}(\!(q)\!)$, together with a canonical invariant 1-form ω_{can} which is nowhere vanishing, such that*

(1) *The Weierstrass equation of* **Tate**(q) *is*

$$y^2 + xy \;=\; x^3 + a_4(q)x + a_6(q),$$

where

$$\begin{cases} a_4(q) = -5\sum_{n=1}^{\infty}\frac{n^3q^n}{1-q^n} \\ a_6(q) = -\frac{1}{12}\sum_{n=1}^{\infty}\frac{(7n^5+5n^3)q^n}{1-q^n}. \end{cases}$$

and the canonical 1-form $\omega_{can} = \frac{dx}{2y+x}$. Moreover, it has the j-invariant

$$j\big(\mathbf{Tate}(q)\big) \;=\; \frac{1}{q} + 744 + 196884q + \ldots$$

and the discriminant

$$\Delta\big(\mathbf{Tate}(q), \omega_{can}\big) \;=\; q\cdot\prod_{n=1}^{\infty}(1-q^n)^{24}.$$

(2) *There exists a unique isomorphism of formal Lie groups*

$$\phi_{can}\colon \widehat{\mathbf{Tate}(q)} \xrightarrow{\sim} \widehat{\mathbb{G}}_m = \widehat{T},$$

such that

$$\phi_{can}^*\left(\frac{X}{dX}\right) \;=\; \omega_{can}.$$

(3) *There exists a canonical extension structure on* $\mathbf{Tate}(q)[N]$ *for each* $N \geqslant 1$*:*

$$0 \longrightarrow \mu_N \xrightarrow{a_N} \mathbf{Tate}(q)[N] \xrightarrow{b_N} \mathbb{Z}/N\mathbb{Z} \longrightarrow 0,$$

such that

- *for any* $\mathbb{Z}(\!(q)\!)$*-algebra* R *in which* N *is nilpotent, and any* $\xi \in \mu_N(R)$*, we have*

$$\phi_{can}\big(a_N(\xi)\big) = \xi.$$

- *the Weil pairing is compatible with the extension structure, i.e., for any* $\mathbb{Z}(\!(q)\!)$*-algebra* R*, any* $\xi \in \mu_N(R)$ *and* $X \in \mathbf{Tate}(q)[N](R)$*, we have*

$$e_N\big(a_N(\xi),\, X\big) = \xi^{b_N(X)}.$$

(4) *We have a unique isomorphism of ind-*$\mathbb{Z}(\!(q)\!)$*-group schemes*

$$T_{tor} \otimes_{\mathbb{Z}[q,q^{-1}]} \mathbb{Z}(\!(q)\!) \simeq \mathbf{Tate}(q)_{tor},$$

which is compatible with their extension structures, i.e., the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mu_\infty \arrow[r] \arrow[d, "id"] & T_{tor} \otimes \mathbb{Z}(\!(q)\!) \arrow[r] \arrow[d, "\wr"] & \mathbb{Q}/\mathbb{Z} \arrow[r] \arrow[d, "id"] & 0 \\
0 \arrow[r] & \mu_\infty \arrow[r] & \mathbf{Tate}(q)_{tor} \arrow[r] & \mathbb{Q}/\mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

commutes.

Serre-Tate parameter

Let k be an algebraically closed field of characteristic p, and R a complete noetherian local $W(k)$-algebra with residue field k. Consider an ordinary elliptic curve E over R, whose special fiber is denoted by E_0/k. We have an isomorphism

$$\phi_0 \colon \mu_\infty \times \mathbb{Q} \xrightarrow{\sim} (E_0)_{\text{can}},$$

which is compatible with the Weil pairings.

Let $q \in 1 + \mathfrak{m}_R \subset R^\times$ be a unit, in which we can view R as a $\mathbb{Z}[q, q^{-1}]$-algebra. By Serre-Tate Theorem 8.6.3, the isomorphism ϕ_0 can be lifted to an isomorphism

$$\phi \colon T_{\text{tor}} \otimes_{\mathbb{Z}[q,q^{-1}]} R \xrightarrow{\sim} E_{\text{can}},$$

which is compatible with their Weil pairings. We call such q a **Serre-Tate parameter** associated to the lifting isomorphism ϕ.

9
Appendix III: Algebraic stacks

In current appendix, we give an introductory exposé on algebraic stacks.

The theory of stacks was largely motivated from the attempt to deal with general moduli problems. In a moduli problem, the *fine moduli space* is the best solution, which captures all the information of the moduli functor. But indeed, such a nice thing does not always exist, e.g., the moduli spaces of curves with fixed genus, and moduli spaces of vector bundles on an algebraic curve.

From the classical point of view, the "best" replacement of the fine moduli space could be the *coarse moduli space*, whose "points" are still in bijective correspondence with the classes we are intended to classify. However the universal family is missing in this case, which means the coarse moduli space does not classify all families of those objects. A basic observation of the obstruction of existence of fine moduli space is the existence of nontrivial automorphisms of objects, i.e., non-rigidity. Briefly speaking, if we have an object X with nontrivial automorphisms, then it is often possible to construct an isotrivial family over some base space B, i.e., a family of objects whose fibers are all isomorphic to X, while the family is not trivial. So if the fine moduli space $\mathscr{M}$ existed, the morphism determined by this family could only be the constant morphism, which maps B to the point of $\mathscr{M}$ corresponding to the isomorphism class of X. But then the pull-back of the universal family is certainly trivial, which is against to our assumption.

Notice that classically our premise is to find moduli space inside the category $\mathfrak{Sch}$ (or $\mathfrak{Sch}_{/S}$), in order to reinterpret the moduli functor. So in order to find a possibly nicer reinterpretation of the moduli functor, it is natural to broaden our target category. Such target category should not be too general, for example if we seek moduli space in the dual category of $\mathfrak{Sch}$, then the case becomes completely trivial. It should capture features of schemes as many as possible.

For example, the *algebraic space* introduced by M. Artin [20], as an intermediate generalization of schemes (comparing to algebraic stacks), is natural and interesting. They behave like schemes, for example, a scheme is Zariski-locally affine, while an algebraic space is étale-locally affine. We give the precise definition:

Definition 9.0.3. *An **algebraic space** is an étale sheaf*

$$F\colon \mathfrak{Sch}^{op} \longrightarrow \mathfrak{Set}$$

which satisfies

(1) The diagonal morphism $\Delta_F : F \to F \times F$ is representable, quasi-compact and separated;

(2) There is an "atlas" of F, i.e., an étale surjective morphism $U \to F$ from a scheme U to F.

Algebraic spaces have some nicer properties than schemes, for example, algebraic spaces can be realized as étale equivalence relations and vice versa, and they behave better than schemes under quotients by group actions. Despite these interesting stories about algebraic spaces, we shall move forward to the theory of algebraic stacks for our very purpose.

9.1 Theory of descent

The theory of descent subjects to study the gluing of objects or morphisms from local to global. For a typical example, in the theory of fiber bundles over some topological space, an isomorphism class of fiber bundles is determined by a Čech 1-cocycle, which is specified by a covering of the base space, and some gluing maps on the intersections of the covering which satisfies the cocycle condition. This is a particular case of *effective descent*, namely, a surjective family of open immersions, which is a covering in the classical sense. The theory of descent is formulated essentially in the same way. When we move the stage to more general settings, namely, Grothendieck topologies and sites, one can talk about more general concept of "coverings", e.g., faithfully flat, fppf, fpqc, fpuo [1] morphisms, and their descent properties.

General framework

Let $\mathscr{C}$ be a category with fiber products. Assume for any $S \in \mathrm{Obj}(\mathscr{C})$, one has a category $\mathscr{C}_S$, and for any $\phi \in \mathrm{Hom}_{\mathscr{C}}(S', S)$, one has the "pull-back" functor $\phi^* : \mathscr{C}_S \to \mathscr{C}_{S'}$. Moreover, they satisfy following conditions:

(1) For any two morphisms

$$S'' \xrightarrow{\phi'} S' \xrightarrow{\phi} S,$$

one has the natural isomorphism of functors

$$c_{\phi,\phi'} : \phi'^* \circ \phi^* \xrightarrow{\sim} (\phi \circ \phi')^*;$$

(2) For any morphisms

$$S''' \xrightarrow{\phi_3} S'' \xrightarrow{\phi_2} S' \xrightarrow{\phi_1} S,$$

the diagram induced from (1)

$$\begin{tikzcd} \phi_3^* \circ \phi_2^* \circ \phi_1^* \arrow[r, "\sim"] \arrow[d, "\wr"'] & (\phi_2 \circ \phi_3)^* \circ \phi_1^* \arrow[d, "\wr"] \\ \phi_3^* \circ (\phi_1 \circ \phi_2)^* \arrow[r, "\sim"] & (\phi_1 \circ \phi_2 \circ \phi_3)^* \end{tikzcd}$$

commutes;

[1] In French: fidèlement plat de présentation finie, fidèlement plat et quasi-compact, fidèlement plat et universellement ouvert.

(3)

$$(\mathsf{id})^* = \mathsf{id};$$

(4)

$$(\mathsf{id})^* \circ \phi^* \xrightarrow{\mathsf{id}} (\phi \circ \mathsf{id})^* \qquad \phi^* \circ (\mathsf{id})^* \xrightarrow{\mathsf{id}} (\mathsf{id} \circ \phi)^*.$$

Given a morphism $\phi \in \mathsf{Hom}_{\mathscr{C}}(S', S)$, in the following Cartesian diagram

$$\begin{tikzcd} S' \times_S S' \arrow[r, "\mathrm{pr}_2"] \arrow[d, "\mathrm{pr}_1"'] & S' \arrow[d, "\phi"] \\ S' \arrow[r, "\phi"] & S \end{tikzcd}$$

we denote $\psi = \phi \circ \mathrm{pr}_1 = \phi \circ \mathrm{pr}_2$.

Now let us define a new category $\mathscr{C}_\phi$: its objects are pairs (ξ', θ), where $\xi' \in \mathsf{Obj}(\mathscr{C}_{S'})$, and

$$\theta : \mathrm{pr}_1^* \xi' \xrightarrow{\sim} \mathrm{pr}_2^* \xi'$$

is an isomorphism. A morphism

$$(\xi', \theta) \xrightarrow{u'} (\eta', \tau)$$

is given by $u' \in \mathsf{Hom}_{\mathscr{C}_{S'}}(\xi', \eta')$, such that the following diagram commutes

$$\begin{tikzcd} \mathrm{pr}_1^* \xi' \arrow[r, "\theta"] \arrow[d, "\mathrm{pr}_1^* u'"'] & \mathrm{pr}_2^* \xi' \arrow[d, "\mathrm{pr}_2^* u'"] \\ \mathrm{pr}_1^* \eta' \arrow[r, "\tau"] & \mathrm{pr}_2^* \eta' \end{tikzcd}$$

There is naturally a functor Φ defined as

$$\begin{aligned} \Phi : \mathscr{C}_S &\longrightarrow \mathscr{C}_\phi \\ \xi &\longmapsto (\phi^* \xi, \psi^* \mathsf{id}_\xi) \end{aligned}$$

Definition 9.1.1. *A morphism $\phi : S' \to S$ is called a* ***morphism of descent****, if the functor Φ is fully faithful.*

A morphism $\phi : S' \to S$ being a morphism of descent is equivalent to require the following sequence to be commutative:

$$\mathsf{Hom}_{\mathscr{C}_S}(\xi, \zeta) \to \mathsf{Hom}_{\mathscr{C}_{S'}}(\phi^* \xi, \phi^* \zeta) \rightrightarrows \mathsf{Hom}_{\mathscr{C}_{S' \times_S S'}}(\psi^* \xi, \psi^* \zeta),$$

where ξ, ζ are any objects in $\mathscr{C}_S$, and the last double arrows are given by pull-backs pr_1^* and pr_2^*.

Let $\Delta : S' \to S' \times_S S'$ be the diagonal morphism, and $\mathrm{pr}_{ij}^* : S' \times_S S' \times_S S' \to S' \times_S S'$ be the projection to the i-th and j-th factors. Suppose $\xi' \in \mathsf{Obj}(\mathscr{C}_{S'})$, if a morphism $\theta : \mathrm{pr}_1^* \xi' \to \mathrm{pr}_2^* \xi'$ satisfies the following conditions:

(1) θ is an isomorphism;

(2) $\Delta^* \circ \theta = \mathrm{id}$;

(3) Cocycle condition: $\mathrm{pr}_{23}^*(\theta) \circ \mathrm{pr}_{12}^*(\theta) = \mathrm{pr}_{13}^*(\theta)$,

then θ is called a **descent datum** of ξ'. We define a full subcategory $\mathscr{D}_\phi$ of $\mathscr{C}_\phi$, whose objects are pairs (ξ', θ), where θ is a descent datum of ξ'. The category $\mathscr{D}_\phi$ is called the **category of descent data** of ϕ. The functor Φ obviously factors through the inclusion $\mathscr{D}_\phi \hookrightarrow \mathscr{C}_\phi$

$$\Phi : \mathscr{C}_S \longrightarrow \mathscr{D}_\phi.$$

Definition 9.1.2. *A morphism $\phi : S' \to S$ is called an **morphism of effective descent**, if the functor Φ defines an equivalence of categories between $\mathscr{C}_S$ and $\mathscr{D}_\phi$.*

The full faithfulness of Φ means that we can glue morphisms (given by local data) of any two objects in the category $\mathscr{C}_S$ along the morphism ϕ, and the essential surjectivity means that we can glue objects (with descent data) along ϕ.

Faithfully flat descent in affine case

The descent theory for affine schemes and affine morphisms is essentially the descent theory for modules over a commutative ring. Let A, A' be commutative rings, given a homomorphism $f : A \to A'$, and set $A'' = A' \otimes_A A'$ with natural homomorphisms $p_1^*, p_2^* : A' \to A''$. Our main questions are

Q$_1$: Given A-modules M, N, and a homomorphism of A'-modules $h' : A' \otimes_A M \to A' \otimes_A N$ such that $h' \otimes_{A', p_1^*} A'' = h' \otimes_{A', p_2^*} A''$, does there exist a homomorphism of A-module $h : M \to N$ such that $h' = h \otimes A'$?

Q$_2$: Given an A'-module M' with a descent datum, does there exist an A-module M such that $M' \simeq A' \otimes_A M$?

In the viewpoint of general framework, the category $\mathscr{C}$ is the opposite category of commutative rings $\mathfrak{CRing}^{\mathrm{op}}$, and for any $A \in \mathrm{Obj}(\mathfrak{CRing}^{\mathrm{op}})$, the category $\mathscr{C}_A$ is A-$\mathfrak{Mod}^{\mathrm{op}}$. A homomorphism fulfilling **Q**$_1$ is exactly a morphism of descent, and if it also fulfills **Q**$_2$, then it is a morphism of effective descent. The situation is equivalent to the case of affine schemes, the questions are to ask whether we can glue quasi-coherent sheaves and their morphisms with given local data on an affine scheme.

Lemma 9.1.3. *Let $\delta^0 : A \to A'$ be a homomorphism of unital commutative rings, and define the **Amitsur complex** $(T^\bullet, \delta^\bullet)$ as following:*

- *$T^0 = A$, $T^n = A'^{\otimes n}$ for $n \geqslant 1$;*
- *δ^0 is as given, $\delta^n = \sum_{i=0}^n (-1)^i \epsilon_i$ for $n \geqslant 1$, where*

$$\begin{array}{rcl} \epsilon_i : T^n & \longrightarrow & T^{n+1} \\ x_1 \otimes \ldots \otimes x_n & \longmapsto & x_1 \otimes \ldots \otimes x_i \otimes 1 \otimes x_{i+1} \otimes \ldots \otimes x_n. \end{array}$$

For any A-module M, if δ^0 is faithfully flat, then the complex $T^\bullet \otimes_A M$ of A-modules is exact.

Proof: By faithful flatness of δ^0, it suffices to prove the exactness of the complex

$$A' \otimes_A T^\bullet \otimes_A M.$$

In order to show it, we construct a chain homotopy as following

$$\begin{array}{rcl} h^n : A'\otimes_A T^n \otimes_A M & \longrightarrow & A'\otimes_A T^{n-1}\otimes_A M \\ x\otimes x_1\otimes \ldots \otimes x_n \otimes m & \longmapsto & x\cdot x_1 \otimes \ldots \otimes x_n \otimes m. \end{array}$$

Then it remains to verify the following identity

$$h^{n+1}\circ\delta^n + \delta^{n-1}\circ h^n = \mathrm{id}_{A'\otimes_A T^n\otimes_A M}.$$

Combine [2]

$$\begin{array}{rl} & h^{n+1}\circ\delta^n(x\otimes x_1\otimes\ldots\otimes x_n\otimes m) \\ = & h^{n+1}\Big(\sum_{i=0}^{n}(-1)^i\ x\otimes x_1\otimes\ldots\otimes x_i\otimes 1\otimes x_{i+1}\otimes\ldots\otimes x_n\otimes m\Big) \\ = & x\otimes x_1\otimes\ldots\otimes x_n\otimes m+\sum_{i=1}^{n}(-1)^i\ x\cdot x_1\otimes\ldots\otimes x_i\otimes 1\otimes x_{i+1}\otimes\ldots\otimes x_n\otimes m \end{array}$$

and

$$\begin{array}{rl} & \delta^{n-1}\circ h^n(x\otimes x_1\otimes\ldots\otimes x_n\otimes m) \\ = & \delta^{n-1}(x\cdot x_1\otimes\ldots\otimes x_n\otimes m) \\ = & \sum_{i=0}^{n-1}(-1)^i\ x\cdot x_1\otimes\ldots\otimes x_{i+1}\otimes 1\otimes x_{i+2}\otimes\ldots\otimes x_n\otimes m \\ = & \sum_{i=1}^{n}(-1)^{i+1}\ x\cdot x_1\otimes\ldots\otimes x_i\otimes 1\otimes x_{i+1}\otimes\ldots\otimes x_n\otimes m \end{array}$$

we obtain the result. □

Corollary 9.1.4. *Let M be an A-module, and $A\to A'$ is faithfully flat. Then the sequence* [3]

$$M\to A'\otimes_A M \rightrightarrows A'\otimes_A A'\otimes_A M$$

is exact.

Corollary 9.1.5. *Let M, N be A-modules, and $A\to A'$ is faithfully flat. Then the sequence*

$$\mathit{Hom}_A(M,N)\to \mathit{Hom}_{A'}(A'\otimes_A M, A'\otimes_A N)\rightrightarrows \mathit{Hom}_{A'\otimes_A A'}(A'\otimes_A A'\otimes_A M, A'\otimes_A A'\otimes_A N)$$

is exact.

Proof: According to Corollary 9.1.4, we have the exact sequence

$$N\to A'\otimes_A N\rightrightarrows A'\otimes_A A'\otimes_A N,$$

applying the functor $\mathrm{Hom}_A(-,M)$, it remains exact

$$\mathrm{Hom}_A(M,N)\to\mathrm{Hom}_A(M,A'\otimes_A N)\rightrightarrows\mathrm{Hom}_A(M,A'\otimes_A A'\otimes_A N).$$

This is already what we want, since

$$\mathrm{Hom}_A(M,A'\otimes_A N)=\mathrm{Hom}_{A'}(A'\otimes_A M, A'\otimes_A N),$$

[2] Precisely here δ^n should be written as $A'\otimes\delta^n\otimes M$, but we did't bother to do so.

[3] The first map is by taking m to $1\otimes m$, and the second two maps are by taking $a'\otimes m$ to $1\otimes a'\otimes m$ and $a'\otimes 1\otimes m$ respectively.

$$\mathrm{Hom}_A(M, A' \otimes_A A' \otimes_A N) = \mathrm{Hom}_{A' \otimes_A A'}(A' \otimes_A A' \otimes_A M, A' \otimes_A A' \otimes_A N).$$

□

Let us fix some notations: let $A''' = A' \otimes_A A' \otimes_A A'$, and

$$p_i : \mathrm{Spec}\,(A'') \longrightarrow \mathrm{Spec}\,(A') \qquad p_{ij} : \mathrm{Spec}\,(A''') \longrightarrow \mathrm{Spec}\,(A'')$$

are projections to respective factors. Let $q_i = p_1 \circ p_{ij} = p_2 \circ p_{ki}$. Observe that given an A'-module M', we have the following isomorphisms of A''-modules:

$$\begin{array}{rcl} p_1^* M' = A'' \otimes_{p_1^*, A'} M' & \longrightarrow & M' \otimes_A A' \\ (a_1' \otimes a_2') \otimes m' & \longmapsto & a_1' m' \otimes a_2' \\ p_2^* M' = A'' \otimes_{p_2^*, A'} M' & \longrightarrow & A' \otimes_A M' \\ (a_1' \otimes a_2') \otimes m' & \longmapsto & a_1' \otimes a_2' m' \end{array}$$

similarly one can identify $q_1^* M', q_2^* M'$ and $q_3^* M'$ with $M' \otimes_A A' \otimes_A A', A' \otimes_A M' \otimes_A A'$ and $A' \otimes_A A' \otimes_A M'$ respectively. Hence, an isomorphism of A''-modules

$$\theta : M' \otimes_A A' \xrightarrow{\sim} A' \otimes_A M'$$

satisfying the cocycle condition, i.e., $p_{23}^*(\theta) \circ p_{12}^*(\theta) = p_{13}^*(\theta)$, is exactly a descent datum of the A'-module M'.

The following proposition gives affirmative answers to the questions $\mathbf{Q}_1, \mathbf{Q}_2$ for faithfully flat morphisms:

Proposition 9.1.6. *Any faithfully flat morphism ϕ : Spec $(A') \to$ Spec (A) is an effective descent morphism for quasi-coherent sheaves.*

Proof: We need to show that the functor Φ from the category of quasi-coherent sheaves on Spec (A) to the category of descent data $\mathscr{D}_\phi$ is an equivalence of categories.

"Full faithfulness": We need to show that for any A-modules M, N, the map

$$\mathrm{Hom}_A(M, N) \longrightarrow \mathrm{Hom}_{\mathscr{D}_\phi}\big((A' \otimes_A M, \psi^* \mathrm{id}_M), (A' \otimes_A N, \psi^* \mathrm{id}_N)\big)$$

is bijective. Recall that a morphism u' in the category $\mathscr{D}_\phi$ between $(A' \otimes_A M, \psi^* \mathrm{id}_M)$ and $(A' \otimes_A N, \psi^* \mathrm{id}_N)$ is given by

$$u' : \phi^* M \longrightarrow \phi^* N,$$

such that the following diagram commutes:

$$\begin{tikzcd} p_1^*(\phi^* M) \arrow[r, "\psi^* \mathrm{id}_M"] \arrow[d, "p_1^* u'"'] & p_2^*(\phi^* M) \arrow[d, "p_2^* u'"] \\ p_1^*(\phi^* N) \arrow[r, "\psi^* \mathrm{id}_N"] & p_2^*(\phi^* N) \end{tikzcd}$$

which is equivalently

$$\begin{tikzcd} A' \otimes_A M \otimes_A A' \arrow[r, "\psi^* \mathrm{id}_M"] \arrow[d, "u' \otimes A'"'] & A' \otimes_A A' \otimes_A M \arrow[d, "A' \otimes u'"] \\ A' \otimes_A N \otimes_A A' \arrow[r, "\psi^* \mathrm{id}_N"] & A' \otimes_A A' \otimes_A N \end{tikzcd}$$

i.e., u' lies in the equalizer of

$$\mathsf{Hom}_{A'}(A'\otimes_A M, A'\otimes_A N) \rightrightarrows \mathsf{Hom}_{A'\otimes_A A'}(A'\otimes_A A'\otimes_A M, A'\otimes_A A'\otimes_A N).$$

Therefore the assertion follows from Corollary 9.1.5.

"Essential surjectivity": We claim that given a descent datum (M',θ), the A-module

$$M := \{m' \in M' \mid \theta(m'\otimes 1) = 1\otimes m'\}$$

satisfies $A'\otimes_A M \simeq M'$, i.e., $(\phi^* M, \psi^*\mathsf{id}_M) \simeq (M',\theta)$. Define

$$\begin{array}{rcl} \tau : M' & \longrightarrow & A'\otimes_A M' \\ m' & \longmapsto & 1\otimes m' - \theta(m'\otimes 1) \end{array}$$

we have the short exact sequence of A-modules

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "i"] & M' \arrow[r, "\tau"] & A'\otimes_A M', \end{tikzcd}$$

it remains exact after tensoring A'

$$\begin{tikzcd} 0 \arrow[r] & M\otimes_A A' \arrow[r, "i"] & M'\otimes_A A' \arrow[r, "\tau"] & A'\otimes_A M'\otimes_A A', \end{tikzcd}$$

fit it into the diagram

$$\begin{tikzcd} 0 \arrow[r] & M\otimes_A A' \arrow[r, "i"] \arrow[d, "\lambda"] & M'\otimes_A A' \arrow[r, "\tau"] \arrow[d, "\theta"] & A'\otimes_A M'\otimes_A A' \arrow[d, "A'\otimes\theta"] \\ 0 \arrow[r] & M' \arrow[r, "\phi^*"] & A'\otimes_A M' \arrow[r, "p_1^* - p_2^*"] & A'\otimes_A A'\otimes_A M' \end{tikzcd} \qquad (\flat)$$

where λ is defined by

$$\begin{array}{rcl} \lambda : M\otimes_A A' & \longrightarrow & M' \\ m\otimes a' & \longmapsto & a'm \end{array}$$

we claim that the diagram $(\flat)$ is commutative. The commutativity of the first square in $(\flat)$ is immediate to check. For the second square, let $m'\otimes a' \in M'\otimes_A A'$, using cocycle condition

$$\begin{array}{rl} & (A'\otimes\theta)\circ(\tau\otimes A')(m'\otimes a') \\ = & (A'\otimes\theta)\big(1\otimes m'\otimes a' - \theta(m'\otimes 1)\otimes a'\big) \\ = & 1\otimes\theta(m'\otimes a') - p_{23}^*(\theta)\circ p_{12}^*(\theta)(m'\otimes 1\otimes a') \\ = & 1\otimes\theta(m'\otimes a') - p_{13}^*(\theta)(m'\otimes 1\otimes a') \\ = & (p_1^* - p_2^*)\circ\theta(m'\otimes a') \end{array}$$

we conclude the commutativity of $(\flat)$. Now since θ and $A'\otimes\theta$ are both isomorphisms, hence so as λ. Finally we need to check that λ indeed gives an isomorphism in the category $\mathscr{D}_\phi$, i.e., one needs to verify one more commutative diagram

$$\begin{tikzcd} A'\otimes_A M\otimes_A A' \arrow[r] \arrow[d, "p_1^*\lambda"'] & A'\otimes_A A'\otimes_A M \arrow[d, "p_2^*\lambda"] \\ M'\otimes_A A' \arrow[r, "\theta"] & A'\otimes_A M', \end{tikzcd}$$

where the map in the first row is given by $a_1' \otimes m \otimes a_2' \mapsto a_1' \otimes a_2' \otimes m$. This is straightforward:

$$\theta \circ p_1^* \lambda(a_1' \otimes m \otimes a_2') = \theta(a_1' m \otimes a_2') = a_1' \otimes a_2' m = p_2^* \lambda(a_1' \otimes a_2' \otimes m). \qquad \square$$

Descent of quasi-coherent sheaves

Move the stage to general schemes, i.e., in this case our category $\mathscr{C}$ is the category of schemes $\mathfrak{Sch}$, and for any $S \in \mathrm{Obj}(\mathfrak{Sch})$, the category $\mathscr{C}_S$ is the category of quasi-coherent sheaves $\mathfrak{QCoh}_{/S}$ on S, with the usual pull-back functors. Suppose $f : S' \to S$ is a morphism of schemes, and set $S'' = S' \times_S S'$ with natural projections $p_1, p_2 : S'' \to S'$. We consider the questions:

- $\mathbf{Q}_3$: Given quasi-coherent sheaves $\mathscr{F}, \mathscr{G}$ on S, and a morphism of $\mathscr{O}_{S'}$-modules

  $$h' : f^*\mathscr{F} \to f^*\mathscr{G}$$

  such that $p_1^* h' = p_2^* h'$, does there exist a morphism of $\mathscr{O}_S$-modules $h : \mathscr{F} \to \mathscr{G}$ such that $h' = f^* h$?
- $\mathbf{Q}_4$: Given a quasi-coherent $\mathscr{F}'$ on S' with a descent datum, does there exist a quasi-coherent sheaf $\mathscr{F}$ on S such that $\mathscr{F}' \simeq f^*\mathscr{F}$?

We have affirmative answers of $\mathbf{Q}_3, \mathbf{Q}_4$ for fpqc and fpuo [4] morphisms. The case of descent theory for quasi-coherent sheaves is essentially the same as the affine case, i.e., descent theory for modules, because of the quasi-coherence.

Lemma 9.1.7. *Let $g : R \to S$ and $f : S \to T$ be morphisms of schemes. Suppose g is a morphism of descent for quasi-coherent sheaves, and so as any base change of g. Then f is a morphism of descent if and only if $f \circ g$ is a morphism of descent.*

Proof: Consider the following commutative diagram:

$$\begin{tikzcd}
R \times_S R \arrow[rrr, "r_2"] \arrow[rd, "\ell"] \arrow[ddd, "r_1"'] & & & R \arrow[d, "\mathrm{id}"] \\
& R \times_T R \arrow[rr, "q_2"] \arrow[rd, "k"] \arrow[dd, "q_1"'] & & R \arrow[d, "g"] \\
& & S \times_T S \arrow[r, "p_2"] \arrow[d, "p_1"'] & S \arrow[d, "f"] \\
R \arrow[r, "\mathrm{id}"] & R \arrow[r, "g"] & S \arrow[r, "f"] & T
\end{tikzcd}$$

(♮)

which contains three cartesian diagrams:

$$\begin{tikzcd}
S \times_T S \arrow[r, "p_2"] \arrow[d, "p_1"'] \arrow[rd, "\psi"] & S \arrow[d, "f"] \\
S \arrow[r, "f"'] & T
\end{tikzcd}
\qquad
\begin{tikzcd}
R \times_T R \arrow[r, "q_2"] \arrow[d, "q_1"'] \arrow[rd, "\psi'"] & R \arrow[d, "f \circ g"] \\
R \arrow[r, "f \circ g"'] & T
\end{tikzcd}
\qquad
\begin{tikzcd}
R \times_S R \arrow[r, "r_2"] \arrow[d, "r_1"'] \arrow[rd, "\psi''"] & R \arrow[d, "g"] \\
R \arrow[r, "g"'] & S
\end{tikzcd}$$

[4] In particular, any fppf morphism is fpuo.

where we denote $\psi = f \circ p_i$, $\psi' = f \circ g \circ q_i$ and $\psi'' = g \circ r_i$. Let $\mathscr{F}, \mathscr{G}$ be any quasi-coherent sheaves on T.

The "only if" part: Assume f is a morphism of descent. Suppose given a morphism of $\mathscr{O}_R$-modules

$$h'' : (f \circ g)^* \mathscr{F} \longrightarrow (f \circ g)^* \mathscr{G}$$

satisfying

$$\psi'^* \mathrm{id}_{\mathscr{F}} \circ q_1^* h'' = q_2^* h'' \circ \psi'^* \mathrm{id}_{\mathscr{G}}.$$

Then immediately h'' also satisfies

$$\psi''^* \mathrm{id}_{f^* \mathscr{F}} \circ r_1^* h'' = \ell^* (\psi'^* \mathrm{id}_{\mathscr{F}} \circ q_1^* h'') = \ell^* (q_2^* h'' \circ \psi'^* \mathrm{id}_{\mathscr{G}}) = r_2^* h'' \circ \psi''^* \mathrm{id}_{f^* \mathscr{G}},$$

since g is a morphism of descent, there exists a unique morphism of $\mathscr{O}_S$-modules

$$h' : f^* \mathscr{F} \longrightarrow f^* \mathscr{G}$$

such that $h'' = g^* h'$. By the assumption that f is a morphism of descent, and that

$$k^* (\psi^* \mathrm{id}_{\mathscr{F}} \circ p_1^* h') = \psi'^* \mathrm{id}_{\mathscr{F}} \circ q_1^* h'' = q_2^* h'' \circ \psi'^* \mathrm{id}_{\mathscr{G}} = k^* (p_2^* h' \circ \psi^* \mathrm{id}_{\mathscr{G}}),$$

which implies $\psi^* \mathrm{id}_{\mathscr{F}} \circ p_1^* h' = p_2^* h' \circ \psi^* \mathrm{id}_{\mathscr{G}}$, since k is given by a base change of g. Thus there is a unique morphism of $\mathscr{O}_T$-modules

$$h : \mathscr{F} \longrightarrow \mathscr{G}$$

such that $h' = f^* h$, and therefore $h'' = (f \circ g)^* h$, i.e., $f \circ g$ is a morphism of descent for quasi-coherent sheaves.

The "if" part: Assume $f \circ g$ is a morphism of descent. Suppose given a morphism of $\mathscr{O}_S$-modules

$$h' : f^* \mathscr{F} \longrightarrow f^* \mathscr{G},$$

satisfying

$$\psi^* \mathrm{id}_{\mathscr{F}} \circ p_1^* h' = p_2^* h' \circ \psi^* \mathrm{id}_{\mathscr{G}}.$$

Consider the morphism $g^* h'$, it satisfies

$$\psi'^* \mathrm{id}_{\mathscr{F}} \circ q_1^* (g^* h') = k^* (\psi^* \mathrm{id}_{\mathscr{F}} \circ p_1^* h') = k^* (p_2^* h' \circ \mathrm{id}_{\mathscr{G}}) = q_2^* (g^* h') \circ \psi'^* \mathrm{id}_{\mathscr{G}}.$$

By the assumption that $f \circ g$ is a morphism of descent, there exists a unique morphism of $\mathscr{O}_T$-modules

$$h : \mathscr{F} \longrightarrow \mathscr{G}$$

such that $g^* h' = (f \circ g)^* h$, which implies $h' = f^* h$ since g is a morphism of descent. Therefore f is a morphism of descent for quasi-coherent sheaves. □

Lemma 9.1.8. *Let $g : R \to S$ and $f : S \to T$ be morphisms of schemes. Suppose g is a morphism of effective descent for quasi-coherent sheaves, and so as any base change of g. Then f is a morphism of effective descent if and only if $f \circ g$ is a morphism of effective descent.*

Proof: We keep the notations from the previous lemma. Moreover, let r_{ij}, q_{ij}, p_{ij} be the obvious projections from $R\times_S R\times_S R, R\times_T R\times_T R, S\times_T S\times_T S$ to respective factors.

The "only if" part: Suppose $(\mathscr{F}'',\theta')$ is a descent datum for $f\circ g$. We want to find a quasi-coherent sheaf $\mathscr{F}$ on T which ought to be unique, such that there is a unique isomorphism of descent data $(f\circ g)^*\mathscr{F}\simeq\mathscr{F}''$. Applying ℓ^* to θ', we obtain an isomorphism

$$\theta''=\ell^*\theta' : r_1^*\mathscr{F}''\longrightarrow r_2^*\mathscr{F}'',$$

and moreover, let ℓ' be the morphism given by the base change of ℓ as below

$$\begin{tikzcd}
R\times_S R\times_S R \arrow[r, "\ell'"] \arrow[d, "r_{ij}"'] & R\times_T R\times_T R \arrow[d, "q_{ij}"] \\
R\times_S R \arrow[r, "\ell"] & R\times_T R
\end{tikzcd}$$

then the cocycle condition for θ'' follows

$$r_{23}^*(\theta'')\circ r_{12}^*(\theta'')=\ell'^*\big(q_{23}^*(\theta')\circ q_{12}^*(\theta')\big)=(q_{13}\circ\ell')^*(\theta')=r_{13}^*(\theta''),$$

that is to say, $(\mathscr{F}'',\theta'')$ is a descent datum for g. Since g is a morphism of effective descent, there exists a unique quasi-coherent sheaf $\mathscr{F}'$ on S, with an isomorphism of descent data

$$\phi' : \mathscr{F}''\longrightarrow g^*\mathscr{F}'.$$

Let $\bar{\theta}'$ be the following composition

$$k^*p_1^*\mathscr{F}'=q_1^*g^*\mathscr{F}'\xrightarrow{q_1^*(\phi')^{-1}}q_1^*\mathscr{F}''\xrightarrow{\theta'}q_2^*\mathscr{F}''\xrightarrow{q_2^*\phi'}q_2^*g^*\mathscr{F}'=k^*p_2^*\mathscr{F}',$$

after checking that the pull-backs of $\bar{\theta}'$ to $(R\times_T R)\times_{S\times_T S}(R\times_T R)$ along two projections coincide (we omit the verification), the isomorphism $\bar{\theta}'$ is descent to an isomorphism

$$\theta : p_1^*\mathscr{F}'\longrightarrow p_2^*\mathscr{F}'$$

with $\bar{\theta}'=k^*\theta$. Then $(\mathscr{F}',\theta)$ is a descent datum for f, and the cocycle condition follows from

$$k'^*\big(p_{23}^*(\theta)\circ p_{12}^*(\theta)\big)=q_{23}^*(\bar{\theta}')\circ q_{12}^*(\bar{\theta}')=q_{13}^*(\bar{\theta}')=k'^*\big(p_{13}^*(\theta)\big),$$

where k' is given by base change of k:

$$\begin{tikzcd}
R\times_T R\times_T R \arrow[r, "k'"] \arrow[d, "q_{ij}"'] & S\times_T S\times_T S \arrow[d, "p_{ij}"] \\
R\times_T R \arrow[r, "k"] & S\times_T S
\end{tikzcd}$$

and that k' is a morphism of effective descent by condition. Thus there exists a unique quasi-coherent sheaf $\mathscr{F}$ on T, such that $\mathscr{F}'\simeq f^*\mathscr{F}$ as descent data, which implies $\mathscr{F}''\simeq(f\circ g)^*\mathscr{F}$ as descent data, i.e., $f\circ g$ is also a morphism of effective descent.

The "if" part: Suppose we have a descent datum $(\mathscr{F}',\theta)$ for f. Denote $\mathscr{F}''=g^*\mathscr{F}'$, then $(\mathscr{F}'',k^*\theta)$ is a descent datum for $f\circ g$. By effective descent of $f\circ g$, there is a unique quasi-coherent sheaf $\mathscr{F}$ on T, with an isomorphism of descent data

$$\phi' :\ g^*\mathscr{F}'=\mathscr{F}''\xrightarrow{\sim}(f\circ g)^*\mathscr{F}=g^*(f^*\mathscr{F}),$$

i.e., we have the commutative diagram

$$\begin{tikzcd}
q_1^*\mathscr{F}'' \arrow[r, "q_1^*\phi'"] \arrow[d, "k^*\theta"'] & q_1^*(f\circ g)^*\mathscr{F} \arrow[d, "\psi'^*\mathrm{id}_{\mathscr{F}}"] \\
q_2^*\mathscr{F}'' \arrow[r, "q_2^*\phi'"] & q_2^*(f\circ g)^*\mathscr{F}
\end{tikzcd} \tag{$\sharp$}$$

We need to check that ϕ' can be descent to an isomorphism of descent data $\phi:\mathscr{F}'\to f^*\mathscr{F}$. To show the existence, essentially we only need to verify the diagram [5]

$$\begin{tikzcd}
r_1^*\mathscr{F}'' \arrow[r, "r_1^*\phi'"] \arrow[d, "(k\circ\ell)^*\theta"'] & r_1^*(f\circ g)^*\mathscr{F} \arrow[d, "\psi''^*\mathrm{id}_{f^*\mathscr{F}}"] \\
r_2^*\mathscr{F}'' \arrow[r, "r_2^*\phi'"] & r_2^*(f\circ g)^*\mathscr{F}
\end{tikzcd}$$

is commutative, but this is straightforward by applying ℓ^* to the diagram ($\sharp$). Hence ϕ' is descent to ϕ. Finally we need to verify that ϕ is indeed an isomorphism of descent data, i.e., the following diagram commutes:

$$\begin{tikzcd}
p_1^*\mathscr{F}' \arrow[r, "p_1^*\phi"] \arrow[d, "\theta"'] & p_1^*f^*\mathscr{F} \arrow[d, "\psi^*\mathrm{id}_{\mathscr{F}}"] \\
p_2^*\mathscr{F}' \arrow[r, "p_2^*\phi"] & p_2^*f^*\mathscr{F}
\end{tikzcd}$$

Indeed, we have

$$k^*(\psi^*\mathrm{id}_{\mathscr{F}}\circ p_1^*\phi)=\psi'^*\mathrm{id}_{\mathscr{F}}\circ q_1^*\phi'=q_2^*\phi'\circ k^*\theta=k^*(p_2^*\phi\circ\theta),$$

since k is of effective descent, one obtains $\psi^*\mathrm{id}_{\mathscr{F}}\circ p_1^*\phi=p_2^*\phi\circ\theta$. □

Theorem 9.1.9. *Any fpqc or fpuo morphism $f:S'\to S$ is a morphism of effective descent for quasi-coherent sheaves.*

Proof: Let $\{S_i\}_i$ be an affine covering of S, and $\{S'_{ij}\}_j$ be an open affine covering of $f^{-1}(S_i)$.

Firstly we reduce the fpuo case to the fpqc case. Let $\{W_i\}$ be any open affine covering of S', the openness of f implies that $\{f(W_i)\}$ is an open covering of S. From the commutative diagram

$$\begin{tikzcd}
\coprod_i W_i \arrow[r, "\coprod_i f|_{W_i}"] \arrow[d] & \coprod_i f(W_i) \arrow[d] \\
S' \arrow[r, "f"] & S
\end{tikzcd}$$

[5] Here we use the condition that g is a morphism of descent.

it reduces [6] the question to each $f|_{W_i}$, since the effective descent holds for any surjective family of open immersions. Now each $f|_{W_i}$ is quasi-compact, hence we may assume the fpuo morphism f is also quasi-compact, i.e., fpqc.

Because f is quasi-compact, $\{S'_{ij}\}_j$ can be chosen to be finite. Let f_i be the restriction of f on $f^{-1}(S_i)$. From the commutative diagram

$$\begin{tikzcd}
\coprod_{i,j} S'_{ij} \arrow[r, "\coprod_i f_i"] \arrow[d, "\pi'"'] & \coprod_i S_i \arrow[d, "\pi"] \\
S' \arrow[r, "f"] & S
\end{tikzcd}$$

it reduces the question to each f_i. Since each f_i is a faithfully flat morphism between affine schemes, by Proposition 9.1.6, it is a morphism of effective descent. □

Remark: The finiteness conditions (i.e. quasi-compact or finitely presented) are crucial, there are examples of faithfully flat morphism which is not of effective descent. See e.g. [18] Appendix A and [30] 6.7.

Descent of schemes

When one comes to the case of gluing schemes rather than quasi-coherent sheaves, things are a bit different. This is simply because a morphism of schemes $T \to S$ is not locally (quasi-)coherent, i.e., over an affine open subscheme $\mathsf{Spec}\,(A)$ of S, the scheme T does not always come from an A-algebra. So in general, one cannot reduce the question to commutative algebra.

Let $f : S' \to S$ be a morphism of schemes, and S'' as usual, with projections p_1, p_2. Here we formulate our questions:

Q$_5$: Given S-schemes X, Y, and a morphism of S'-schemes

$$h' : \; X' = X \times_S S' \; \to \; Y' = Y \times_S S'$$

such that $p_1^* h' = p_2^* h'$, does there exist a morphism of S-schemes $h : X \to Y$ such that $h' = f^* h$?

Q$_6$: Given a S'-scheme X' on S' with a descent datum, does there exist a S-scheme X such that $X' \simeq X \times_S S'$?

Despite general cases, the case of affine morphisms is rather similar to the descent theory of modules.

Lemma 9.1.10. *Let $f : X \to Y$ be a fpqc morphism of schemes. Then a subset of Y is open (resp. closed) if and only if its preimage is open (resp. closed) in X, i.e., Y is a topological quotient of X by f.*

Proof: See EGA IV$_2$ [3] Corollaire 2.3.12.

[6] Notice that here we use Lemma 9.1.8 to reduce the case.

Lemma 9.1.11. *Let $f : S' \to S$ be a fpqc or fpuo morphism, and $g : S' \to X$ is a morphism satisfying $p_1^* g = p_2^* g$. Then there exists a unique morphism $h : S \to X$ such that $h \circ f = g$.*

Proof: To construct the morphism h, one needs to construct the map of underlying topological spaces, and the morphism of structure sheaves.

$$\begin{tikzcd}
S' \arrow[r, "f"] \arrow[d, "g"'] & S \arrow[dl, dotted, "h"] & & g_*\mathscr{O}_{S'} & h_*\mathscr{O}_S \arrow[l, "g_*f^\#"'] \\
X & & & \mathscr{O}_X \arrow[u, "g^\#"] \arrow[ur, dotted, "h^\#"'] &
\end{tikzcd}$$

Observe that for any points x, y in S' satisfying $f(x) = f(y)$, there must exist a point $z \in S''$ with $p_1(z) = x$ and $p_2(z) = y$, since we have the universal property of fiber products:

$$\begin{tikzcd}
\mathsf{Spec}\ (k) \arrow[drr, bend left, "x"] \arrow[dr, dotted] \arrow[ddr, bend right, "y"'] & & \\
& S'' \arrow[r, "p_2"] \arrow[d, "p_1"'] & S' \arrow[d, "f"] \\
& S' \arrow[r, "f"] & S
\end{tikzcd}$$

this means that we can construct h in a set-theoretic sense, as following: Let $s \in S$ be any point, and $s' \in S'$ is any preimage of s, define $h(s) := g(s')$. By previous observation, the definition of h is independent of choice of s', as g satisfies $p_1^* g = p_2^* g$. Moreover, since the topology of S is the quotient topology by f, the map h is continuous.

To construct $h^\#$, we firstly consider the exact sequence

$$\begin{tikzcd}
\mathscr{O}_S \arrow[r, "f^\#"] & f_*\mathscr{O}_{S'} \arrow[r, shift left] \arrow[r, shift right] & \psi_*\mathscr{O}_{S''}
\end{tikzcd}$$

where $\psi = f \circ p_i$. This is indeed exact, by Theorem 9.1.9. Applying the left exact functors h_* and $\mathsf{Hom}(\mathscr{O}_X, -)$, one obtains

$$\begin{tikzcd}
\mathsf{Hom}(\mathscr{O}_X,\ h_*\mathscr{O}_S) \arrow[r] & \mathsf{Hom}(\mathscr{O}_X,\ g_*\mathscr{O}_{S'}) \arrow[r, shift left] \arrow[r, shift right] & \mathsf{Hom}\big(\mathscr{O}_X,\ (h \circ \psi)_*\mathscr{O}_{S''}\big)
\end{tikzcd}$$

the condition $p_1^* g = p_2^* g$ indicates that $g^\#$ lies in the equalizer, hence it is induced by a morphism $h^\sharp \in \mathsf{Hom}(\mathscr{O}_X, h_*\mathscr{O}_S)$, which is exactly what we need to construct. □

Theorem 9.1.12. *Any fpqc or fpuo morphism $f : S' \to S$ is a morphism of effective descent for affine morphisms.*

Proof: Given an S'-scheme X' which is affine over S', it is equivalent to a quasi-coherent sheaf of $\mathscr{O}_{S'}$-algebras. Use the descent result for quasi-coherent sheaves, one can descend X' (as a sheaf) to a quasi-coherent sheaf of $\mathscr{O}_S$-module, and equip with a multiplication morphism by descending the multiplication morphism of the sheaf of $\mathscr{O}_{S'}$-algebras, which is then corresponding to a S-scheme which is affine over S.

Let X, Y be any S-schemes. It remains to show the exactness of the sequence

$$\mathsf{Hom}_S(X,\ Y) \longrightarrow \mathsf{Hom}_{S'}(X',\ Y') \rightrightarrows \mathsf{Hom}_{S''}(X'',\ Y'')$$

or equivalently,

$$\mathsf{Hom}_S(X,\ Y) \longrightarrow \mathsf{Hom}_S(X',\ Y) \rightrightarrows \mathsf{Hom}_S(X'',\ Y).$$

This is straightforwardly implied by Lemma 9.1.11. □

Observe that the affine condition is irrelevant in proving that one can glue morphisms of S-schemes along a fpqc or fpuo morphism $f : S' \to S$. Hence as a byproduct, we proved the following fact:

Corollary 9.1.13. *Any fpqc or fpuo morphism $f : S' \to S$ is a morphism of descent for any morphisms.*

Finally, we state the descent results for quasi-affine and quasi-projective morphism. For detailed proofs, one can find in [18].

Recall that a morphism $f : S' \to S$ is called *quasi-affine* if the preimage of any affine subscheme of S is quasi-affine.

Theorem 9.1.14. *Any fpqc or fpuo morphism $f : S' \to S$ is a morphism of effective descent for quasi-affine morphisms.*

To state the result for quasi-projective morphisms, we need to do one more thing, namely, to specify the relatively ample sheaf. Let $f : S' \to S$ be a fpqc or fpuo morphism, and S'', S''' as usual. Let $X' \to S'$ be a quasi-projective S'-scheme, with a relatively ample sheaf $\mathscr{L}'$. And we denote

$$\widetilde{p}_1 : X' \times_S S' \longrightarrow X', \qquad \widetilde{p}_2 : X' \times_S S' \simeq S' \times_S X' \longrightarrow X'$$

be projections.

Theorem 9.1.15. *Let $f : S' \to S$ be a fpqc or fpuo morphism. Suppose X' is a quasi-projective S'-scheme, with a relatively ample sheaf $\mathscr{L}'$. If we have a descent datum for X' (i.e., an isomorphism $\phi : X' \times_S S' \simeq S' \times_S X'$ satisfying the cocycle condition) and a descent datum for $\mathscr{L}'$ (i.e., an isomorphism $\omega : \widetilde{p}_1^*\mathscr{L}' \simeq \widetilde{p}_2^*\mathscr{L}'$ satisfying the cocycle condition), then there exists a unique quasi-projective S-scheme X with a relatively ample sheaf $\mathscr{L}$, such that $(f^*X, f^*\mathscr{L})$ is isomorphic to $(X', \mathscr{L}')$ as descent data.*

9.2 Categories fibered in groupoids

Although there is a more general theory on fibered categories (cf. Vistoli's lecture note in [7]), here we only consider the fibered categories whose fibers are groupoids, and always assume the base category is $\mathfrak{Sch}_{/S}$ for some base scheme S.

Definition 9.2.1. *A **category fibered in groupoids** (**CFG**) is a functor of categories $p_{\mathscr{X}}:\mathscr{X}\to\mathfrak{Sch}_{/S}$, such that for any arrow $f:T'\to T$ in $\mathfrak{Sch}_{/S}$, there is a "pull-back" functor $f^*:\mathscr{X}(T)\to\mathscr{X}(T')$, and for any composable arrows:*

$$T''\xrightarrow{g}T'\xrightarrow{f}T,$$

there is a canonical isomorphism of functors $c_{f,g}:g^*\circ f^*\simeq(f\circ g)^*$, such that the following diagram commutes:

$$\begin{tikzcd}
h^*g^*f^* \arrow[r] \arrow[d] & (gh)^*f^* \arrow[d] \\
h^*(fg)^* \arrow[r] & (fgh)^*
\end{tikzcd}$$

Here $\mathscr{X}(T)$ is the category whose objects are objects of $\mathscr{X}$ which are mapped to T by p, and whose arrows are arrows in $\mathscr{X}$ which are mapped to the identity morphism id_T in $\mathfrak{Sch}_{/S}$.

To specify the base category, we often call $\mathscr{X}$ a CFG over S. And we often call p as the structure morphism of the CFG $\mathscr{X}$.

From any functor $F:\mathfrak{Sch}_{/S}^{\mathrm{op}}\to\mathfrak{Set}$, we can construct a CFG $\mathscr{F}$ associated to F. The objects of $\mathscr{F}$ are pairs (T,ξ), where T is a S-scheme, and $\xi\in F(T)$. The projection p is by forgetting the element ξ in the pair. The pull-back functors are just given by F itself, i.e., for any arrow $f:T'\to T$, the pull-back functor is $f^*=F(f)$. The conditions for pull-back functors are naturally satisfied, hence $\mathscr{F}$ is indeed a CFG. The fibers of $\mathscr{F}$ is not only groupoids, but even sets. In fact, any *category fibered in sets* (*CFS*) comes from a functor. Let $\mathscr{F}$ be a CFS, define a functor $F:\mathfrak{Sch}_{/S}^{\mathrm{op}}\to\mathfrak{Set}$ as following: for any S-scheme T, let $F(T):=\mathscr{F}(T)$, and for any arrow $f:T'\to T$, let $F(f):=f^*$. These two processes are obviously mutually inverse. We shall call this kind of CFGs simply as functors.

Definition 9.2.2. *A morphism $\phi:\mathscr{X}\to\mathscr{Y}$ of CFGs over S is a functor compatible with structure morphisms. An isomorphism of CFGs is a morphism which is an equivalence of categories.*

Remark:

- We simply denote the morphisms from $\mathscr{X}$ to $\mathscr{Y}$ by $\mathsf{Hom}_S(\mathscr{X},\mathscr{Y})$, while it is worth to note that this is a groupoid, rather than a set. Thus the category of CFGs forms a 2-category.
- If a morphism $f:\mathscr{X}\to\mathscr{Y}$ of CFGs is an equivalence of categories, one can find an inverse functor $g:\mathscr{Y}\to\mathscr{X}$ which is compatible with structure morphisms, i.e., g is a morphism of CFGs.
- A morphism between CFSs is exactly a natural transformation of their functors.

Since the category of CFGs over S form a 2-category, there are naturally two kinds of commutativity of diagrams, namely, the *strict commutativity* and the *2-commutativity.* Conventionally, when we simply call a diagram of morphisms of CFGs commutes, we mean that it is 2-commutative.

Definition 9.2.3. *Let $f:\mathscr{X}\to\mathscr{Z}$ and $g:\mathscr{Y}\to\mathscr{Z}$ be morphisms of CFGs. The fiber product $\mathscr{X}\times_{\mathscr{Z}}\mathscr{Y}$ is a CFG defined as following: its objects are triples (ξ,ζ,α), where $\xi\in Obj(\mathscr{X})$, $\zeta\in Obj(\mathscr{Y})$, with $p_{\mathscr{X}}(\xi)=p_{\mathscr{Y}}(\zeta)$ in $\mathfrak{Sch}_{/S}$, and $\alpha:f(\xi)\to g(\zeta)$ is an arrow in $\mathscr{Z}$ such that $p_{\mathscr{Z}}(\alpha)=id$. A morphism*

$$(\xi,\zeta,\alpha)\xrightarrow{(\phi,\psi)}(\xi',\zeta',\beta)$$

is given by a pair (ϕ,ψ), where $\phi:\xi\to\xi'$ and $\psi:\zeta\to\zeta'$, with $p_{\mathscr{X}}(\phi)=p_{\mathscr{Y}}(\psi)$, such that the diagram

$$\begin{tikzcd}
f(\xi) \arrow[r, "\alpha"] \arrow[d, "f(\phi)"'] & g(\zeta) \arrow[d, "f(\psi)"] \\
f(\xi') \arrow[r, "\beta"] & g(\zeta')
\end{tikzcd}$$

commutes.

Notice that, the concept of CFGs already appears in the place of general framework of descent theory. So that once we equip some Grothendieck topology on $\mathfrak{Sch}_{/S}$, we can talk about descent data, and the effectiveness of a descent datum.

Definition 9.2.4. *A CFG $\mathscr{X}$ over S is a* ***stack****, if any arrow in the (big) étale site $\mathfrak{Sch}_{/S,ét}$ is a morphism of effective descent for the CFG $\mathscr{X}$.*

A morphism $\mathscr{X}\to\mathscr{Y}$ between stacks over S is a morphism of CFGs, and a fiber product of stacks is a fiber product of CFGs.

Lemma 9.2.5. *If a CFG $\mathscr{X}$ is a functor, then it is a stack if and only if it is a sheaf in the étale topology.*

Proof: It amounts to prove that it is always possible to glue morphisms and objects along coverings in the étale site $\mathfrak{Sch}_{/S,\text{ét}}$. The part for morphisms is trivial, since $\mathscr{X}$ is a CFS, hence only identity morphisms are allowed. For gluing objects, that is to say, for any covering $T'\to T$ in $\mathfrak{Sch}_{/S,\text{ét}}$, we need to verify the following sequence

$$\mathscr{X}(T)\longrightarrow\mathscr{X}(T')\rightrightarrows\mathscr{X}(T'\times_T T')$$

to be exact. This is exactly the sheaf axioms. □

Let T be a S-scheme, we have a natural functor $\mathfrak{Sch}_{/T}\to\mathfrak{Sch}_{/S}$, which makes $\mathfrak{Sch}_{/T}$ into a CFG over S. We simply denote this CFG by T itself. In fact the CFG T is a CFS, it comes from the functor $h_T=\mathsf{Hom}_S(-,T)$. By previous lemma, the CFG T is a stack. Thus we can embed the category of S-schemes into the category of stacks over S. This is a more general embedding comparing to the Yoneda embedding, since the category $(\mathfrak{Sch}_{/S})^\vee$ of functors forms a full subcategory consisting of CFSs:

$$\mathfrak{Sch}_{/S}\hookrightarrow(\mathfrak{Sch}_{/S})^\vee\hookrightarrow\text{2-category of }S\text{-stacks.}$$

We also have the stacky version of Yoneda Lemma:

Lemma 9.2.6 (Yoneda Lemma)**.** *Let $\mathscr{X}$ be a S-stack, and T is a S-scheme. The functor*

$$\begin{array}{rcl} u:\ \mathsf{Hom}_S(T,\mathscr{X}) & \longrightarrow & \mathscr{X}(T)\\ f & \longmapsto & f(id_T)\end{array}$$

is an equivalence of categories.

Proof: Define a functor

$$\begin{array}{rcl} v : \mathscr{X}(T) & \longrightarrow & \mathsf{Hom}_S(T, \mathscr{X}) \\ \xi & \longmapsto & \left\{ \{g : T' \to T\} \mapsto g^*\xi \right\} \end{array}$$

it is easy to check that v is an inverse of u. □

9.3 Algebraic stacks

Definition 9.3.1. *A morphism $f : \mathscr{X} \to \mathscr{Y}$ of S-stacks is called representable, if for any morphism $T \to \mathscr{Y}$ from a S-scheme T to $\mathscr{Y}$, the fiber product $\mathscr{X} \times_{\mathscr{Y}} T$ is a scheme.*

Let **P** be any property of morphisms of schemes which is stable under any base change. Given a representable morphism $f : \mathscr{X} \to \mathscr{Y}$ of stacks, we say that f has property P, if for any morphism $T \to \mathscr{Y}$ from a S-scheme T to $\mathscr{Y}$, the induced morphism $\mathscr{X} \times_{\mathscr{Y}} T \to T$ of schemes has property **P**.

Definition 9.3.2. *A S-stack $\mathscr{X}$ is an* ***algebraic stack****, if it satisfies:*

(1) The diagonal morphism $\Delta_{\mathscr{X}} : \mathscr{X} \to \mathscr{X} \times_S \mathscr{X}$ is representable, quasi-compact and separated;

(2) There is an "atlas" U of $\mathscr{X}$, i.e., an étale surjective morphism $U \to \mathscr{X}$ from a S-scheme U to $\mathscr{X}$.

Remark: An algebraic stack in above definition is often called a **Deligne-Mumford stack**, which is originated from Deligne and Mumford's paper [26] on moduli spaces of curves with fixed genus. If instead, we replace the étale atlas by a smooth atlas, then it is called an **Artin stack**, which is introduced in Artin's paper [21].

The assumption of representable diagonal is quite reasonable, since we have the lemma:

Lemma 9.3.3. *The diagonal morphism $\Delta_{\mathscr{X}}$ of a S-stack $\mathscr{X}$ is representable, if and only if any morphism from a scheme to $\mathscr{X}$ is representable.*

Proof: *The "only if" part*: Suppose the diagonal $\Delta_{\mathscr{X}}$ is representable, and let $f : T \to \mathscr{X}$ and $g : R \to \mathscr{X}$ be morphisms from S-schemes to $\mathscr{X}$. Observe that we have the diagram

$$\begin{tikzcd} T \times_{\mathscr{X}} R \arrow[r] \arrow[d] & \mathscr{X} \arrow[r, "\mathsf{id}_{\mathscr{X}}"] \arrow[d, "\Delta_{\mathscr{X}}"] & \mathscr{X} \arrow[d, "p_{\mathscr{X}}"] \\ T \times_S R \arrow[r, "f \times g"] & \mathscr{X} \times_S \mathscr{X} \arrow[r, "p_{\mathscr{X} \times_S \mathscr{X}}"] & S \end{tikzcd}$$

where the right square and the big squares are cartesian, hence so as the left square. By the representability of $\Delta_{\mathscr{X}}$, $T \times_{\mathscr{X}} R$ is a scheme.

The "if" part: Suppose that any morphism from a scheme to $\mathscr{X}$ is representable. Let $(f, g) : T \to \mathscr{X} \times_S \mathscr{X}$ be a morphism from a S-scheme T to the stack $\mathscr{X} \times_S \mathscr{X}$, which is given by morphisms $f, g : T \to \mathscr{X}$. As we have seen, the diagram

$$\begin{tikzcd} T \times_{\mathscr{X}} T \arrow[r] \arrow[d] & \mathscr{X} \arrow[d, "\Delta_{\mathscr{X}}"] \\ T \times_S T \arrow[r, "(f, g)"] & \mathscr{X} \times_S \mathscr{X} \end{tikzcd}$$

is cartesian. It fits into the diagram

$$\begin{tikzcd}
\mathscr{X} \times_{\mathscr{X}\times_S\mathscr{X}} T \arrow[r] \arrow[d] & T \times_{\mathscr{X}} T \arrow[r] \arrow[d] & \mathscr{X} \arrow[d, "\Delta_{\mathscr{X}}"] \\
T \arrow[r, "\Delta_T"] & T \times_S T \arrow[r, "{(f,g)}"] & \mathscr{X} \times_S \mathscr{X}
\end{tikzcd}$$

where all squares are cartesian. Notice that by assumption, $T \times_{\mathscr{X}} T$ is a scheme, therefore

$$\mathscr{X} \times_{\mathscr{X}\times_S\mathscr{X}} T \simeq (T \times_{\mathscr{X}} T) \times_{T\times_S T} T$$

is a scheme. □

Proposition 9.3.4. *The diagonal $\Delta_{\mathscr{X}}$ of a Deligne-Mumford stack $\mathscr{X}$ is unramified.*

Proof: Let $U \to \mathscr{X}$ be an étale atlas of $\mathscr{X}$, and let $T \to \mathscr{X} \times_S \mathscr{X}$ be a morphism from a S-scheme T to $\mathscr{X} \times_S \mathscr{X}$. Consider the following diagram

$$\begin{tikzcd}
(\mathscr{X} \times_{\mathscr{X}\times_S\mathscr{X}} T) \times_{\mathscr{X}} U \arrow[rrr] \arrow[dr] \arrow[ddd] & & & T \times_{\mathscr{X}\times_S\mathscr{X}} (U \times_S U) \arrow[dl] \arrow[ddd] \\
& U \arrow[r, "\Delta_U"] \arrow[d] & U \times_S U \arrow[d] & \\
& \mathscr{X} \arrow[r, "\Delta_{\mathscr{X}}"] & \mathscr{X} \times_S \mathscr{X} & \\
\mathscr{X} \times_{\mathscr{X}\times_S\mathscr{X}} T \arrow[ur] \arrow[rrr] & & & T \arrow[ul]
\end{tikzcd}$$

where the left, right and bottom squares are cartesian, hence so is the top square. The diagonal Δ_U is an immersion, hence the top arrow is also an immersion. The most left and the most right arrows are étale, therefore the bottom arrow is unramified, i.e., the diagonal $\Delta_{\mathscr{X}}$ is unramified. □

Remark: The main difference of an algebraic stack $\mathscr{X}$ and a scheme is that objects of $\mathscr{X}$ may have nontrivial automorphisms. This is certainly not the case for schemes, since they are CFSs, where the only automorphism allowed is the identity. Let $\xi \in \mathscr{X}(T)$ be an object over a S-scheme T, by the definition of stacks, the functor

$$\begin{array}{rcl}
\mathrm{Aut}_T(\xi) = \mathsf{Hom}_{\mathscr{X}(T)}(\xi,\xi):\ \mathfrak{Sch}_{/T} & \longrightarrow & \mathfrak{Set} \\
\{f: T' \to T\} & \longmapsto & \mathrm{Aut}_{T'}(f^*\xi)
\end{array}$$

is a sheaf (in étale topology). Moreover, by Yoneda Lemma, an object $\xi \in \mathscr{X}(T)$ determines a morphism of stacks

$$\xi:\ T \longrightarrow \mathscr{X}.$$

The functor $\mathrm{Aut}_T(\xi)$ is nothing but the fiber product:

$$\begin{tikzcd}
\mathrm{Aut}_T(\xi) \arrow[r] \arrow[d] & T \arrow[d, "{(\xi,\xi)}"] \\
\mathscr{X} \arrow[r, "\Delta_{\mathscr{X}}"] & \mathscr{X} \times_S \mathscr{X}
\end{tikzcd}$$

hence it is a T-group scheme, which is separated, quasi-compact, and unramified over T. In particular, if T is quasi-compact, then $\mathrm{Aut}_T(\xi)(T)$ has only finitely many points, that is to say, ξ has only finitely many automorphisms. The discussion already shows that the moduli space $\mathscr{M}_1$ of curves of genus 1 is not a Deligne-Mumford stack, since a smooth plane cubic over an algebraically closed field obviously has infinitely many non-trivial automorphisms.

9.4 Examples: Moduli of curves

In this last section, we discuss some examples of algebraic stacks. We principally concentrate on moduli spaces of curves. We fix a base category $\mathfrak{Sch}_{/S}$.

Example 9.4.1 (Schemes)**.** *Let T be a S-scheme. We have seen that T is a S-stack. It is obviously algebraic, since the diagonal is already a morphism of schemes, and we can choose the identity morphism to be the étale atlas.*

Example 9.4.2 (Moduli of n-pointed projective lines)**.** *Let $\mathscr{M}_{0,n}$ be a functor defined as*

$$\begin{array}{rcl} \mathscr{M}_{0,n}: \mathfrak{Sch}^{op} & \longrightarrow & \mathfrak{Set} \\ S & \longmapsto & \left\{ \begin{array}{l} \textit{isomorphism classes of smooth curves} \\ \textit{over } S \textit{ with genus 0 geometric fibers,} \\ \textit{and } n \textit{ pairwise distinct marked sections.} \end{array} \right\} \end{array}$$

It defines a CFG $\mathscr{M}_{0,n}$ over $\mathbb{Z}$. The CFG $\mathscr{M}_{0,n}$ has objects as $(n+1)$-tuples $(C/S, \sigma_1, ..., \sigma_n)$, where C/S is a smooth curve over S with genus 0 geometric fibers, and $\sigma_1, ..., \sigma_n$ are sections

$$\begin{tikzcd} C \arrow[d, "f"] \\ S \arrow[u, bend left, "\sigma_1,\dots,\sigma_n"] \end{tikzcd}$$

Morphisms are cartesian diagrams

$$\begin{tikzcd} C' \arrow[r] \arrow[d] & C \arrow[d] \\ S \arrow[r] & S \end{tikzcd}$$

which is compatible with respective n sections. However, it may not be a CFS, despite we define it as a moduli functor. The difference is that $\mathscr{M}_{0,n}(S)$ is a set of n-pointed genus 0 curves, but modulo isomorphisms, so objects of $\mathscr{M}_{0,n}$ may have non-trivial automorphisms. For example, when $0 \leqslant n \leqslant 2$, the CFG $\mathscr{M}_{0,n}$ is certainly not a CFS.

To check that $\mathscr{M}_{0,n}$ is a stack, we need to verify that any arrow in $\mathfrak{Sch}_{\acute{e}t}$ is a morphism of effective descent, i.e., we can glue both morphisms and objects in $\mathscr{M}_{0,n}$ along the arrow. The case for morphisms is automatically satisfied, according to Corollary 9.1.13.

Let $\phi: S' \to S$ be a surjective étale morphism, and $(C'/S', \sigma'_1, ..., \sigma'_n)$ is a n-pointed genus 0 smooth curve over S', with a descent datum $\theta: p_1^* C' \to p_2^* C'$, also together with gluing conditions for n

sections $\sigma'_1,...,\sigma'_n$. It amounts to glue the curve C' and n sections $\sigma'_1,...,\sigma'_n$. Observe that once we descend C' to a genus 0 smooth curve C over S, then gluing sections $\sigma'_1,...,\sigma'_n$ is just a matter of gluing morphisms $\sigma'_i : S' \to C'$, which is automatically satisfied by Corollary 9.1.13. In order to glue the curve C', we consider the invertible sheaf $\Omega^{-1}_{C'/S'}$, it is very ample over any fiber, hence it is relatively very ample[7]*. Therefore we can embed C' canonically into the projective bundle $\mathbb{P}(f_*\Omega^{-1}_{C'/S'})$, i.e., $C'_{S'}$ is projective. A descent data of C' naturally induces a descent data of the relatively very ample sheaf $\Omega^{-1}_{C'/S'}$, hence by Theorem 9.1.15, the smooth projective curve C'/S' descends to a curve C/S. Thus we have proved that $\mathscr{M}_{0,n}$ is a stack.*

Next natural question is if $\mathscr{M}_{0,n}$ is algebraic, i.e., Deligne-Mumford. By Lemma 9.3.3, the condition that the diagonal is representable, is equivalent to the following condition: let $C_1, C_2 \in \mathscr{M}_{0,n}(S)$ be two curves over S, then the functor $Hom_{\mathscr{M}_{0,n}(S)}(C_1, C_2)$ is representable. This is simply because we have the cartesian diagram:

$$\begin{tikzcd}
Hom_{\mathscr{M}_{0,n}(S)}(C_1,C_2) \arrow[r] \arrow[d] & S \arrow[d, "{(C_1,C_2)}"] \\
\mathscr{M}_{0,n} \arrow[r, "\Delta_{\mathscr{M}_{0,n}}"] & \mathscr{M}_{0,n} \times \mathscr{M}_{0,n}
\end{tikzcd}$$

Since C_1, C_2 are projective curves, the representability of $Hom_{\mathscr{M}_{0,n}(S)}(C_1, C_2)$ is a consequence of the representability of Hilbert schemes[8]*.*

It remains to show (or disprove) the existence of an étale atlas for the moduli stack $\mathscr{M}_{0,n}$. For $0 \leqslant n \leqslant 2$, the stack $\mathscr{M}_{0,n}$ is not Deligne-Mumford, since a projective line over an infinite field with at most two distinct marked points obviously has infinitely many non-trivial automorphisms. In fact, the rest of them are represented by schemes.

In the case $n = 3$, $\mathscr{M}_{0,3}$ is simply represented by $M_{0,3} = Spec\,(\mathbb{Z})$, with the universal family

$$\begin{tikzcd}
\mathbb{P}^1_{\mathbb{Z}} \arrow[d] \\
Spec\,(\mathbb{Z}) \arrow[u, bend left, "{0,1,\infty}"]
\end{tikzcd}$$

In the case $n = 4$, the moduli stack $\mathscr{M}_{0,4}$ is represented by the scheme:

$$M_{0,4} = \mathbb{P}^1_{\mathbb{Z}} \setminus \{0,1,\infty\},$$

with the universal family

$$\begin{tikzcd}
M_{0,4} \times \mathbb{P}^1_{\mathbb{Z}} \arrow[d] \\
M_{0,4} \arrow[u, bend left, "{\sigma_1^{univ},...,\sigma_4^{univ}}"]
\end{tikzcd}$$

where $\sigma_1^{univ}, \sigma_2^{univ}, \sigma_3^{univ}$ are constant sections $0, 1, \infty$, and σ_4^{univ} is the diagonal morphism $\Delta_{M_{0,4}}$.

In the case $n \geqslant 4$, the moduli stack $\mathscr{M}_{0,n}$ is represented by the scheme:

$$M_{0,n} = M_{0,4} \times ... \times M_{0,4} \setminus \{ \textit{ diagonals} \}, \qquad (n-3 \textit{ factors})$$

[7] cf. EGA IV$_3$ [4] Corollaire 9.6.4

[8] cf. Nitsure [7] Theorem 5.23

and the universal family is given by

$$\begin{tikzcd} M_{0,n}\times\mathbb{P}^1_{\mathbb{Z}} \arrow[d] \\ M_{0,n} \arrow[u, bend left, "\sigma_1^{univ},\dots,\sigma_n^{univ}"] \end{tikzcd}$$

where $\sigma_1^{univ},\sigma_2^{univ},\sigma_3^{univ}$ *are constant sections* $0,1,\infty$, *and* σ_k^{univ} *for* $4\leqslant k\leqslant n$ *is the diagonal morphism with respect to the* $(k-3)$*-th factor.*

Example 9.4.3 (Moduli of elliptic curves)**.** *Let* $\mathscr{M}_{1,1}$ *be a functor defined as*

$$\begin{array}{rcl} \mathscr{M}_{1,1}:\mathfrak{Sch}^{op} & \longrightarrow & \mathfrak{Set} \\ S & \longmapsto & \left\{ \begin{array}{l} \textit{isomorphism classes of} \\ \textit{elliptic curves over } S. \end{array} \right\} \end{array}$$

It defines a CFG $\mathscr{M}_{1,1}$ *over* $\mathbb{Z}$, *whose objects are elliptic curves over a base scheme, and morphisms are cartesian diagrams compatible with the zero section. As we proved, that for any elliptic curve* $f:E\to S$, *locally we can always find its generalized Weierstrass equation, so elliptic curves are projective. The relatively very ample sheaf is* $\mathscr{O}_E(3e)$, *and* E/S *can be canonically embedded into the projective bundle* $\mathbb{P}(f_*\mathscr{O}_E(3e))$. *So by almost the same argument as we showed in previous example, the CFG* $\mathscr{M}_{1,1}$ *is a stack.*

Recall that we defined some universal elliptic curves, namely, the universal Weierstrass families $\mathbf{E}_{(\frac{1}{6})}/\mathbf{R}_0,\mathbf{E}^1_{(\frac{1}{6})}/\mathbf{R}_1$, *the universal Legendre family* $\mathbf{E}_{(\frac{1}{2})}/\mathbf{R}_2$ *and the universal family* $\mathbf{E}_{(\frac{1}{3})}/\mathbf{R}_3$ *of naïve level 3. There are solutions for certain moduli problems. We claim that the universal Legendre family together with the universal family of naïve level 3, provide an étale atlas for* $\mathscr{M}_{1,1}$. *By Yoneda Lemma, these two families give two morphisms*

$$\mathsf{Spec}\,(\mathbf{R}_2)\longrightarrow\mathscr{M}_{1,1},\qquad \mathsf{Spec}\,(\mathbf{R}_3)\longrightarrow\mathscr{M}_{1,1},$$

where the induced morphisms

$$\mathsf{Spec}\,(\mathbf{R}_2)\longrightarrow\mathscr{M}_{1,1}\otimes\mathbb{Z}\left[\frac{1}{2}\right],\qquad \mathsf{Spec}\,(\mathbf{R}_3)\longrightarrow\mathscr{M}_{1,1}\otimes\mathbb{Z}\left[\frac{1}{3}\right]$$

are surjective. Hence

$$\mathsf{Spec}\,(\mathbf{R}_2)\coprod\mathsf{Spec}\,(\mathbf{R}_3)\longrightarrow\mathscr{M}_{1,1}$$

is surjective. Since both the Legendre moduli problem and the moduli problem of naïve level 3 are étale, this is indeed an étale atlas.

Example 9.4.4 (General case of moduli of curves)**.** *Let* $\mathscr{M}_{g,n}$ *be the moduli CFG of smooth curves of genus* g *with* n *distinct marked points, and suppose* $g\geqslant 2$. *Let* $f:C\to S$ *be a smooth curve with genus 2 geometric fibers. In this case, the invertible sheaf* $\Omega^{\otimes 3}_{C/S}$ *is relatively very ample* [9], *hence* C/S *is projective. Using the same argument,* $\mathscr{M}_{g,n}$ *is a stack over* $\mathfrak{Sch}$. *In fact they are all Deligne-Mumford, see Arbarello-Cornalba-Griffiths [9] Theorem 8.3.*

[9] cf. Delinge-Mumford [26] Theorem 1.2.

REFERENCES

[1] The Stacks Project Authors. *Stacks Project*. http://stacks.math.columbia.edu, 2016.

[2] A. ALTMAN, S. KLEIMAN. *Introduction to Grothendieck Duality Theory.* Berlin-Heidelberg-New York: Springer-Verlag, 1970.

[3] A. GROTHENDIECK. Éléments de géométrie algébrique. IV: Étude locale des schémas et des morphismes de schémas. (Séconde partie). *Publ. Math., Inst. Hautes Étud. Sci.*, 24:1–231, 1965.

[4] A. GROTHENDIECK. Éléments de géométrie algébrique. IV: Étude locale des schémas et des morphismes de schémas. (Troisième partie). Rédigé avec la colloboration de Jean Dieudonné. *Publ. Math., Inst. Hautes Étud. Sci.*, 28:1–255, 1966.

[5] A. GROTHENDIECK. Éléments de géométrie algébrique. IV: Étude locale des schémas et des morphismes de schémas (Quatrième partie). Rédigé avec la colloboration de Jean Dieudonné. *Publ. Math., Inst. Hautes Étud. Sci.*, 32:1–361, 1967.

[6] B. CONRAD. Arithmetic moduli of generalized elliptic curves. *J. Inst. Math. Jussieu*, 6(2):209–278, 2007.

[7] B. FANTECHI, L. GÖTTSCHE, L. ILLUSIE, S. L. KLEIMAN, N. NITSURE, A. VISTOLI. *Fundamental Algebraic Geometry: Grothendieck's FGA Explained.* Providence, RI: American Mathematical Society (AMS), 2005.

[8] D. ABRAMOVICH, M. ROMAGNY. Moduli of Galois p-covers in mixed characteristics. *Algebra Number Theory*, 6(4):757–780, 2012.

[9] E. ARBARELLO, M. CORNALBA, P. A. GRIFFITHS. *Geometry of Algebraic Curves. Volume II. With a contribution by Joseph Daniel Harris.* Berlin: Springer, 2011.

[10] J. H. SILVERMAN. *The Arithmetic of Elliptic Curves.* New York, NY: Springer, 2nd edition, 2009.

[11] J.-I. IGUSA. Fibre systems of Jacobian varieties. III: Fibre systems of elliptic curves. *Am. J. Math.*, 81:453–476, 1959.

[12] J.-I. IGUSA. Kroneckerian model of fields of elliptic modular functions. *Am. J. Math.*, 81:561–577, 1959.

[13] J.-I. IGUSA. On the transformation theory of elliptic functions. *Am. J. Math.*, 81:436–452, 1959.

[14] J.-I. IGUSA. On the algebraic theory of elliptic modular functions. *J. Math. Soc. Japan*, 20:96–106, 1968.

[15] J. S. EDIXHOVEN. Modular parameterizations at primes of bad reduction, 2001.

[16] J. TATE. Finite Flat Group Schemes. In *Modular Forms and Fermat's Last Theorem. Papers from a Conference, Boston, MA, USA, August 9–18, 1995*, pages 121–154. New York, NY: Springer, 1997.

[17] J. TATE, F. OORT. Group schemes of prime order. *Ann. Sci. Éc. Norm. Supér. (4)*, 3:1–21, 1970.

[18] K. BEHREND, B. CONRAD, D. EDIDIN, B. FANTECHI, W. FULTON, L. GÖTTSCHE, A. KRESCH. Algebraic stacks. link, 2007.

[19] K. ČESNAVIČIUS. A modular description of $\mathscr{X}_0(n)$. preprint 1511.07475.

[20] M. ARTIN. Algebraic Spaces. Yale Mathematical Monographs. 3. New Haven-London: Yale University Press. VII,39 p., 1971.

[21] M. ARTIN. Versal deformations and algebraic stacks. *Invent. Math.*, 27:165–189, 1974.

[22] M. DEMAZURE, P. GABRIEL. Groupes algébriques. Tome I: Géométrie algébrique. Généralités. Groupes commutatifs. Avec un appendice 'Corps de classes local' par Michiel Hazewinkel. Paris: Masson et Cie, Éditeur; Amsterdam: North-Holland Publishing Company. xxvi, 700 p., 1970.

[23] N. M. KATZ. Serre-Tate local moduli. Surfaces Algebriques, Séminaire de Géométrie Algébrique, Orsay 1976-78, Lect. Notes Math. 868, 138-202, 1981.

[24] N. M. KATZ, B. MAZUR. Arithmetic Moduli of Elliptic Curves. Annals of Mathematics Studies, 108. Princeton, New Jersey: Princeton University Press. XIV, 514 p., 1985.

[25] P. DELIGNE. Courbes elliptiques: formulaire d'après J. Tate. In *Modular Functions of One Variable. IV. Proceedings of the International Summer School, University of Antwerp, RUCA, July 17 - August 3, 1972*, pages 53–73. Berlin: Springer, 1975.

[26] P. DELIGNE, D. MUMFORD. The irreducibility of the space of curves of a given genus. *Publ. Math., Inst. Hautes Étud. Sci.*, 36:75–109, 1969.

[27] P. DELIGNE, M. RAPOPORT. Les schemas de modules de courbes elliptiques. Modular Functions of one Variable II, Proc. internat. Summer School, Univ. Antwerp 1972, Lect. Notes Math. 349, 143-316, 1973.

[28] Q. LIU. *Algebraic Geometry and Arithmetic Curves. Transl. by* REINIE ERNÉ. Oxford: Oxford University Press, 2006.

[29] R. HARTSHORNE. *Algebraic Geometry.* Graduate Texts in Mathematics, 52. New York-Heidelberg-Berlin: Springer-Verlag. XVI, 496 p., 1983.

[30] S. BOSCH, W. LÜTKEBOHMERT, M. RAYNAUD. *Néron Models.* Berlin etc.: Springer-Verlag, 1990.

[31] S. LANG. *Cyclotomic fields. I and II. With an appendix by Karl Rubin: The main conjecture.* New York etc.: Springer-Verlag, combined 2nd edition, 1990.

[32] T. ODA. The first De Rham cohomology group and Dieudonne modules. *Ann. Sci. Éc. Norm. Supér. (4)*, 2:63–135, 1969.

[33] T. SAITO. *Fermat's Last Theorem. The Proof. Translated from the Japanese by Masato Kuwata.* Providence, RI: American Mathematical Society (AMS), 2014.

[34] V. G. DRINFEL'D. Coverings of p-adic symmetric regions. *Funct. Anal. Appl.*, 10:107–115, 1976.

[35] V. G. DRINFEL'D. Elliptic modules. *Math. USSR, Sb.*, 23:561–592, 1976.

[36] W. C. WATERHOUSE. Introduction to Affine Group Schemes. Graduate Texts in Mathematics. 66. New York, Heidelberg, Berlin: Springer-Verlag. XI, 164 p., 1979.

[37] Y.-L. HUANG. A "standard reduction" argument. link, 2016.

Index