Cohomology of certain Artin stacks

Dissertation

Zur Erlangung des Doktorgrades
der Mathematisch-Naturwissenschaftlichen Fakultät
der Heinrich-Heine-Universität Düsseldorf

vorgelegt von

Thuong Tuan Dang

aus Thua Thien-Hue

Düsseldorf, March 2022

Aus dem Mathematischen Institut
der Heinrich-Heine-Universität Düsseldorf

Gedruckt mit der Genehmigung der
der Mathematisch-Naturwissenschaftlichen Fakultät
der Heinrich-Heine-Universität Düsseldorf

Referent: Prof. Dr. Stefan Schröer
Koreferent: Prof. Dr. Jens Hornbostel

Tag der mündlichen Prüfung: 20.04.2022

Summary

Artin stacks are important objects in algebraic geometry. They usually arise in the context of moduli problems. Roughly speaking, they are a generalization of schemes and allow objects to have extra automorphisms. The main goal of the thesis is to compute cohomology of certain Artin stacks.

Mumford [M64] computed the Picard group of the moduli stack of elliptic curves (denoted $\mathcal{M}_{1,1}$) over a field k whose characteristic $p > 3$. Later, Fulton and Olsson [FO10] computed the Picard group of $\mathcal{M}_{1,1}$ over a general base scheme S, where S is either reduced or 2 is invertible on S.

Using the close relations between elliptic curves and genus one curves over general base schemes and the results above, we computed the Picard group of the moduli stack of genus one curves over any base field, and give a geometric description of the stack of genus one curves.

Furthermore, by using the machinery of cohomological descent and spectral sequences, we compute certain cohomology groups of some classifying stacks.

Contents

Chapter 1

Introduction

One of the fundamental quesitons in algebraic geometry is when a functor from the category of schemes to the category of sets is representable. A functor can parametrize important information of schemes, for example, its Picard group or its closed subschemes. Most of the cases, the given functor is not representable, but in some cases, it is. An example is that the functor that parametrizes elliptic curves or curves of genus one, due to the existence of automorphisms is not representable.

To cope with this, we use the language of stacks. In [SGA I], Grothendieck gave basic ingredients of stacks, namely descent theory. Stacks are natural generalizations of sheaves of sets. And roughly speaking, they are objects that we can glue local data to obtain global information. In the famous paper [DM69], Deligne-Mumford proved that the moduli space of curves of genus at least 2 is irreducible. Later, Artin [A74] introduced algebraic stacks. And similar to the case of schemes, we can define the notions of sheaves and cohomology groups on algebraic stacks.

Mumford [M64] showed that, when the characteristic of the base field is not 2 or 3, the Picard group of the moduli stack of elliptic curves, denoted $\mathcal{M}_{1,1}$ is $\mathbb{Z}/12\mathbb{Z}$. Later, Fulton-Olsson [FO10] showed that when the base scheme S is either reduced or 2 is invertible on S, then $\mathrm{Pic}(\mathcal{M}_{1,1}) \cong \mathbb{Z}/12\mathbb{Z} \times \mathrm{Pic}(\mathbb{A}^1_S)$. Shin [S19] computed a certain cohomology of algebraic stacks, including classifying stack of an elliptic curve, classifying stack of diagonalizable group schemes, the Brauer group of the moduli stack of an elliptic curves, and some $\mathbb{G}_m$-gerbes.

Motivated by these computations, in this thesis, we compute cohomology group of certain algebraic stacks. Our main results are

Theorem 1.0.1. *Over any base field k, the Picard group of the moduli stack of genus one curve $\mathcal{M}_{1,0}$ is $\mathbb{Z}/12\mathbb{Z}$.*

Moreover, we also prove that $\mathcal{M}_{1,0}$ is a classifying stack over $\mathcal{M}_{1,1}$.

Theorem 1.0.2. *The moduli stack stack of genus one curve $\mathcal{M}_{1,0}$ is an algebraic stack, and it is isomorphic to the stack $B_{\mathcal{M}_{1,1}}\mathcal{E}$, where $\mathcal{E}$ is the universal elliptic curve over $\mathcal{M}_{1,1}$.*

Later, by using the techniques of cohomological descent, we prove a generalization of a result in [S19]

Theorem 1.0.3. *Let A be an abelian variety, and BA the classifying stack of A-torsors, then $H^2(BA, \mathbb{G}_m) \cong Br(k) \oplus \mathrm{Pic}^0(A)$, where $\mathrm{Pic}^0(A) \subset \mathrm{Pic}(A)$ is the group of numerically trivial invertible sheaf on A.*

The thesis is organized as follows. In the second chapter, we will review important notions, namely sheaves on sites, algebraic spaces, descent and stacks. At the end of the chapter, we will introduce Artin stacks and Deligne-Muford stacks, and as an important example, we prove classifying stacks are Artin stacks.

The third chapter is the main core of the thesis, there we recall about elliptic curves, curves of genus one over fields, and their properties in families. We shall prove that the moduli stack of elliptic curves $\mathcal{M}_{1,1}$ is a Deligne-Mumford stack. Using this result, we prove that $\mathcal{M}_{1,0}$ is an Artin stack. And also in this chapter, we compute the Picard group of $\mathcal{M}_{1,0}$ over any base field, and prove that it is isomorphic to the classifying stack $B_{\mathcal{M}_{1,0}}\mathcal{E}$, where $\mathcal{E}$ is the universal elliptic curve over $\mathcal{M}_{1,1}$.

In the fourth chapter, we will introduce the notion of cohomological descent and present how it is related to classical theory of cohomology of groups. And at the end of the chapter, we will use the machinery to compute cohomology of certain Artin stacks, including classifying stack of constant group schemes, classifying stack of the additive group scheme, and the classifying stack of an abelian variety.

Acknowledgement. I would like to thank many people who have helped me a lot during the time I was working on the thesis. First and foremost, I would like to send my

deepest gratitude to Prof. Dr. Stefan Schröer, my advisor, for his constant support, his generosity to share his ideas, his time and effort to help me finish the thesis. I also wish to thank Prof. Dr. Jens Hornbostel, my co-advisor, for helpful discussions and numerous of suggestions he made for my thesis.

I would also like to thank the Algebraic Geometry group in Heinrich-Heine-University Düsseldorf for the knowledge they shared. In particular, I would like to thank Saša Novaković and Jakob Bergqvist for their helpful discussions and they are always available to discuss mathematical ideas with me. I would like to thank the Algebraic Geometry group in the Institute of Mathematics, Hanoi, Vietnam for their helpful seminars.

Last but not least, I would like to send my special thanks to my family and friends for too many reasons to mention.

This research was conducted in the framework of the research training group GRK 2240: Algebro-Geometric Methods in Algebra, Arithmetic and Topology, funded by the DFG.

Chapter 2

Background

In this chapter, we will review the theory of descent and stacks. We will also introduce the notions of Artin and Deligne-Mumford stacks. And in the last section, we will discuss about classifying stack, an important class of Artin stacks.

2.1 Sites and sheaves on sites

During the section, we will recall the definition of Grothendieck topology and examples. We will fix a category $\mathcal{C}$, whose fiber products exist, and a base scheme S.

Definition 2.1.1. A *Grothendieck topology* on $\mathcal{C}$ is a set T of families of morphisms $\{U_i \to U\}_i$ in $\mathcal{C}$ such that

- Any isomorphism of $\mathcal{C}$ is in T.
- Assume that $\{U_i \to U\}_i$ and $\{U_{ji} \to U_i\}_j$ are in T for all i, then $\{U_{ij} \to U\}_{i,j}$ is in T.
- Let $V \to U$ be any morphism in $\mathcal{C}$ and $\{U_i \to U\}_i$ is in T, then $\{U_i \times_U V \to V\}$ is in T.

Such family $\{U_i \to U\}_i$ in T is called a *covering*. And $\mathcal{C}$ with a Grothendieck topology T defined above is called a *site*.

This defintion is mainly motivated for the theory of sheaves on the category of schemes with different Grothendieck topology. There are some important examples of Grothendieck topology we can look at.

Example 2.1.2. Let X be a topological space. Let X_{Zar} be a category consists of open subsets of X and morphisms are inclusions. A family of morphisms $\{U_i \to U\}$ in X_{Zar} is a covering if $\bigcup_i U_i = U$. We note that in this case the fiber product $U_i \times_U U_j$ is just the intersection $U_i \cap U_j$. And it is a routine to check X_{Zar} is indeed a site, which is called the Zariski site.

Example 2.1.3. We will define the *Zariski site* on $(\mathrm{Sch}\,/S)$ as follows. A family of morphisms $\{U_i \xrightarrow{\phi_i} X\}$ in $(\mathrm{Sch}\,/S)$ is a covering if each ϕ_i is an open immersion of schemes, and $\coprod_i U_i \to X$ is surjective. Because an isomorphism is an open immersion, and open immersion is stable under base change and composition, we obtain the Zariski site on $(\mathrm{Sch}\,/S)$.

Example 2.1.4. We will define the *etale site* on the category $(\mathrm{Sch}\,/S)$. A family of morphisms $\{U_i \xrightarrow{\phi_i} X\}_i$ in $(\mathrm{Sch}\,/S)$ is a covering if for all i, ϕ_i is etale, and $\coprod_i U_i \to X$ is surjective. The axioms of Grothendieck topology is easy to check because isomorphism of schemes is etale, and etale morphism is stable under base change and composition.

Example 2.1.5. We recall that a morphism of schemes $f : Y \to X$ is said to be *fppf* if f is surjective, flat and locally of finite presentation. We can define the *fppf site* on $(\mathrm{Sch}\,/S)$ as follows. A family of morphisms $\{U_i \xrightarrow{\phi_i} X\}_i$ is a covering if for all i, ϕ_i is fppf and $\coprod_i U_i \to X$ is surjective.

Remark 2.1.6. Because an open immersion is etale and an etale morphism is flat and locally of finite presentation, we can see that the fppf topology is finer than the etale topology, which is finer than Zariski topology. It means that for fppf or etale topology, we can have more "open" sets.

We will next define our main notion of this chapter.

Definition 2.1.7. Let $\mathcal{C}$ be a site, a *sheaf of sets* on $\mathcal{C}$ is a (contravariant) functor $F : \mathcal{C} \to (\mathrm{Sets})$, such that for any covering $\{U_i \to U\}_i$ the following diagram

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

is exact.

Say another words, F is a sheaf if and only if for any tuple $u_i \in F(U_i)$ such that the restriction of u_i and u_j on $F(U_i \times_U U_j)$ are the same for all i, j, then there exists a unique $u \in F(U)$ such that u_i is the restriction of u on U_i. As we will see, the definition above is a generalization of sheaves on topological spaces.

Example 2.1.8. Let X be a topological space and X_{Zar} the Zariski site. A functor $F : X_{Zar} \to (\mathrm{Sets})$ is a sheaf if and only if for any open covering $\{U_i \to U\}_i$ on X_{Zar} and any $u_i \in F(U_i)$ such that $u_i|_{U_i \cap U_j} = u_j|_{U_i \cap U_j}$ then there exists a unique $u \in F(U)$ such that $u|_{U_i} = u_i$.

Example 2.1.9. In this example, we will prove that the moduli functor of elliptic curves is not a sheaf in general. An *elliptic curve* over S is a scheme E together with a structure morphism $f : E \to S$ such that f is flat, proper of finite presentation, together with a section $s : S \to E$ and fibers over geometric points of S are elliptic curves. For now, we assume that $S = \operatorname{Spec} k$ is a spectrum of a field. Let us consider the following functor $M_{1,1} : (\mathrm{Sch}\,/k) \to (\mathrm{Sets})$ sending a k-scheme X to isomorphism classes of elliptic curves over X. Let us fix two elliptic curves E_1, E_2 over k such that they are not isomorphic over k, but isomorphic over k^{sep}. Actually, there is an finite, seperable extension of l of k such that $E_{1,l} \cong E_{2,l}$. We can see $\operatorname{Spec} l \to \operatorname{Spec} k$ is an fppf covering, but $M_{1,1}(k)$ to $M_{1,1}(l)$ is not injective, because E_1, E_2 are different in $M_{1,1}(k)$ but they have the same image in $M_{1,1}(l)$. This implies that $M_{1,1}$ is not a sheaf.

Among functors from $\mathcal{C}$ to (Sets), there is an important class consisting of representable functors. Let X be an object in $\mathcal{C}$, we denote $h_X : \mathcal{C} \to (\mathrm{Sets})$ the functor sending any object Y in $\mathcal{C}$ to the set $\mathrm{Hom}_{\mathcal{C}}(Y, X)$. In the next example, we will see that representable functors are sheaves on Zariski topology over $\mathrm{Sch}\,/S$.

Example 2.1.10. Let $(\mathrm{Sch}\,/S)_{Zar}$ be the Zariski site on $\mathrm{Sch}\,/S$, and X be an object. Consider the functor $h_X : (\mathrm{Sch}\,/S) \to (\mathrm{Sets})$ defined by $Y \mapsto \mathrm{Hom}_{\mathrm{Sch}\,/S}(Y, X)$. We shall prove that h_X is a sheaf on $(\mathrm{Sch}\,/S)_{Zar}$. Let U be a scheme and $(U_i)_i$ an open covering of U. Let $f : U \to X$ be a morphism, we can see that f is uniquely determined by the restrictions $f|_{U_i} : U_i \to X$. Moreover, if for each i, there is a morphism $f_i : U_i \to X$ such that $f_i|_{U_i \cap U_j} = f_j|_{U_i \cap U_j}$ for each i, then we can glue f_i to obtain a morphism $f : U \to X$

such that $f|_{U_i} = f_i$. And this yields representable functors are sheaves with respect to the Zariski topology.

An important result of Grothendieck (see e.g. [FGAE, Theorem 2.55]) is

Theorem 2.1.11. *Representable functors are sheaves with respect to the fppf topology on* Sch/S.

2.2 Algebraic spaces

The theory of algebraic spaces was developed by Artin in order to form quotients by group actions. Quotients by group actions do not always exists as schemes. One possible solution for this is to enlarge the category of schemes. In this section, we will recall basic notions of algebraic spaces. As usual, we will fix a category $\mathcal{C}$ with fiber product.

Definition 2.2.1. Let F, G, H be contravariant functors from $\mathcal{C}$ to Sets, and $f : F \to H$, $g : G \to H$ be natural transformations. The *fiber product* $F \times_H G$ is defined to be

$$(F \times_H G)(U) \stackrel{\text{def}}{=} \{(a, b) \in F(U) \times G(U) | f_U(a) = g_U(b)\}$$

for all object U of $\mathcal{C}$.

It can be checked that $F \times_H G$ is indeed a functor from $\mathcal{C}$ to Sets, and it is the fiber product in the category of functors from $\mathcal{C}$ to Sets with morphisms are natural transformations.

Definition 2.2.2. Let F, G be two functors from $\mathcal{C}$ to Sets, and $f : F \to G$ a natural transformation. We say that f is *relative representable* if for all object T in $\mathcal{C}$ and all natural transformation $g : h_T \to G$, the fiber product $h_T \times_G F$ is representable by an object in $\mathcal{C}$.

Example 2.2.3. Let T, U, V be objects in $\mathcal{C}$ and $f : h_T \to h_V, g : h_U \to h_V$ be natural transformations. Then by Yoneda's lemma, there are corresponding morphisms $f : T \to V, g : U \to V$ (by abusing of notations) in $\mathcal{C}$, and it can be seen that $h_T \times_{h_V} h_U$ is representable by $T \times_V U$.

Definition 2.2.4. Let $\mathcal{P}$ be a property of morphisms in $\mathcal{C}$ such that isomorphism in $\mathcal{C}$ verfies $\mathcal{P}$, and $\mathcal{P}$ is stable under base changes and compositions. Let $f : F \to G$ be a representable natural transformation between two functors F, G. We say that *f verifies $\mathcal{P}$* if for all object T in $\mathcal{C}$ and all natural transformation $g : h_T \to G$, the induced morphism from X to T verifies $\mathcal{P}$, where X is object of $\mathcal{C}$ representing $h_T \times_G F$.

We note that by Yoneda's lemma, X is unique up to a unique isomorphism and isomorphisms in $\mathcal{C}$ verify $\mathcal{P}$, so the definition above is well-defined.

Example 2.2.5. Let us consider the category (Sch/S). Let $f : X \to Y$ be an fppf (etale, open immersion,...) morphism. Because fppf morphism is stable under base change, we can see that the corresponding natural transformation $h_X \to h_Y$ is fppf (etale, open immersion,...).

Lemma 2.2.6. *Let $F : \mathcal{C} \to (\mathrm{Sets})$ be a functor such that the diagonal natural transformation $\Delta : F \to F \times F$ is representable, then for any object T in $\mathcal{C}$, any morphism $f : h_T \to F$ is representable.*

Proof. The statement is equivalent to say that for any object V in $\mathcal{C}$ and any natural transformation $g : h_V \to F$, $h_T \times_F h_V$ is representable. The pair (f, g) induces a natural transformation $f \times g : h_{T\times V} \cong h_T \times h_V \to F \times F$.

By assumption, the fiber product $h_{T\times V} \times_{F\times F} F$ is representable. And by definition, for all object U in $\mathcal{C}$, we have

$$(h_{T\times V} \times_{F\times F} F)(U) = \{(a, b, c) \in h_T(U) \times h_V(U) \times F(U) | f_U(a) = g_U(b) = c\}$$

And the latter is exactly $(h_T \times_F h_V)(U)$. Hence, $h_T \times_F h_V$ is representable. □

With the notation as the lemma above, and by Definition 2.2.4, it is clear in the context what we mean by properties of the morphism $T \to F$.

Definition 2.2.7. An *algebraic space* over a scheme S is an etale sheaf $F : (\mathrm{Sch}/S) \to (\mathrm{Sets})$ such that

- The diagonal $\Delta : F \to F \times F$ is representable.
- There is a scheme U and a surjective, etale morphism $U \to F$.

Example 2.2.8. Let U be a scheme, then by Grothendieck's theorem that every scheme is an fppf sheaf (Theorem 2.1.11), h_U is an etale sheaf. Moreover, because U and $U \times U$ are schemes, the diagonal morphism is clearly representable. The identity morphism $\mathrm{id} : U \to U$ gives a surjective etale map to U from a scheme. Hence, a scheme is an algebraic space.

2.3 Etale equivalence relations and a non-trivial example of algebraic spaces

In this section, we will give an equivalent definition for algebraic spaces. This will help us construct a non-trivial example of algebraic spaces. Throughout the section, we will fix a base scheme S. Let A be a set, we recall that an *equivalence relation* on A is a subset $R \subseteq A \times A$ such that

(i) For all $a \in A$, $(a, a) \in R$.

(ii) For all $a, b, c \in A$ such that $(a, b) \in R, (b, c) \in R$ then $(a, c) \in R$.

(iii) For all $a, b \in A$ such that $(a, b) \in R$ then $(b, a) \in R$.

Definition 2.3.1. Let R, U be schemes. A *pre-relation defined by R on U* is a morphism $j : R \to U \times_S U$ of schemes. A pre-relation j is said to be

(i) a *relation* if j is a monomorphism.

(ii) a *pre-equivalence relation* if for any S-scheme T, the image of $j_T : R(T) \to U(T) \times U(T)$ is an equivalence relation.

(iii) j an *equivalence relation* if j is a relation, and a pre-equivalence relation.

Let j be an equivalence relation difined by R on U. For any S-scheme T, we define $\sim_T$ the equivalence relation on $U(T)$ induced by $R(T)$, i.e. $a \sim_T b$ if and only if $(a, b) \in R(T)$ for all $a, b \in U(T)$. Let U/R be the etale sheaf associated to the presheaf $(\mathrm{Sch/S})^{\mathrm{op}} \to$ Sets by sending any S-scheme T to the set $U(T)/\sim_T$. It follows directly from the definion that

Lemma 2.3.2. *With the assumption as above, we have*

1. *As functors,* $U \times_{U/R} U \cong R$.

2. $R \rightrightarrows U \longrightarrow U/R$ *is a coequalizer diagram.*

The second statement of the lemma above is a special case of the following observation, whose proof can be found in [SP, Sites and sheaves, Lemma 11.3].

Lemma 2.3.3. *Let* F, G *be two sheaves from* $(\mathrm{Sch}/S) \to \mathrm{Sets}$ *and* $\alpha : F \to G$ *a surjective sheaf map, then there is a coequalizer diagram* $F \times_G F \rightrightarrows F \longrightarrow G$.

We are now ready to see the connections between algebraic spaces and equivalence relations.

Proposition 2.3.4. *Let* F *be an algebraic space, and* $U \xrightarrow{f} F$ *a surjective, etale covering from an* S*-scheme* U*, and* $R \overset{\mathrm{def}}{=} U \times_F U$*, then*

(i) The map $R \to U \times_S U$ *defines an equivalence relation.*

(ii) The induced maps $R \xrightarrow{s,t} U$ *are etale.*

(iii) The diagram $R \rightrightarrows U \longrightarrow F$ *is coequalizer.*

Proof. Because F is an algebraic space, R is a scheme, and $R(T) = (U \times_F U)(T) = \{(a, b) | a, b \in U(T), f \circ a = f \circ b\}$. Moreover, the canonical morphism $R \to U \times_F U$ is monomorphism, and it can be seen that R defines an equivalence relation on U. For the second statement, because $U \to F$ is etale, the base change $U \times_F U \to U$ is etale as well. Finally, the coequalizer in (iii) follows directly from the previous lemma. □

Definition 2.3.5. Let F be an algebraic space over S, and $U \to F$ an etale covering, R an equivalence relation on U, then R is said to be an *etale equivalence relation* if the induced maps $s, t : R \to U$ are etale. We say that U is a *presentation* of F if there is an etale equivalence relation R on U and $F \cong U/R$.

According to Lemma 2.3.3 and Proposition 2.3.4, we obtain

Proposition 2.3.6. *Let* F *be an algebraic space over* S*,* $U \to F$ *an etale covering, and* R *an equivalence relation on* U*, then* (U, R) *is a presentation of* F *if and only if* $R \cong U \times_F U$.

Proof. Assume that (U, R) is a presentation of F, i.e. $F \cong U/R$. By (1) of Lemma 2.3.2, we obtain $U \times_F U \cong R$. Conversely, assume that $R \cong U \times_F U$, then according to Proposition 2.3.4, $R \rightrightarrows U \longrightarrow F$ is a coequalizer diagram, and by (2) of Lemma 2.3.2, $R \rightrightarrows U \longrightarrow U/R$ is also a coequalizer diagram, and this yields $F \cong U/R$. □

The next theorem is the main ingredient to construct algebraic spaces. A proof can be found in [SP, Algebraic Spaces, Theorem 10.5].

Theorem 2.3.7. *Let U be a scheme over S, and R an etale equivalence relation, then U/R is an algebraic space, and (U, R) is a presentation of $F \overset{\text{def}}{=} U/R$.*

Let G be an abstract group acting freely on a scheme U, with an action is a morphism from $R = \coprod_{\sigma \in G} U$ to $U \times_S U$ given by sending (σ, x) to $(\sigma x, x)$, for all $g \in G$. We will prove that R defines an etale equivalence relation on U.

Proposition 2.3.8. *The quotient $G\backslash U \overset{\text{def}}{=} U/R$ is an algebraic space.*

Proof. By the theorem above, it is sufficient to prove that R defines an etale equivalence relation on U. We will first prove R defines an equivalence relation by showing that it is a relation and a pre-equivalence relation. By definition of free group actions, the morphism $\coprod_{\sigma \in G} U \to U \times U$ is a monomorphism, and this implies R is a relation on U. Furthermore, the condition of pre-equivalence relation is easy to check. And we obtain that R is an equivalence relation on U. Moreover, the two maps $s, t : R = \coprod_{\sigma \in G} U \to U$ are clearly etale, where s sends (σ, x) to σx and t sends (σ, x) to x, because R is disjoint union of U. And the statement now follows from the theorem above. □

Example 2.3.9. Let k be a field of characteristic 0. For any $n \in \mathbb{Z}$, we can define an automorphism $+_n$ of $k(x)$ by sending $x \mapsto x + n$. This defines an injective map $\mathbb{Z} \to \operatorname{Aut} k(x)$. And it follows that the action of $\mathbb{Z}$ to $\operatorname{Spec} k(x)$ is free, and we can form an algebraic space $F := \mathbb{Z}\backslash \operatorname{Spec} k(x)$, due to Proposition 2.3.8. Assume F is a scheme, consider an etale surjective covering $\operatorname{Spec} k(x) \to F$ (Theorem 2.3.7). Looking at the fiber product $\operatorname{Spec} k(x) \times_F \operatorname{Spec} k(x) = \coprod_{n \in \mathbb{Z}} \operatorname{Spec} k(x)$, which is not quasi-compact. Assume that F is affine, then the fiber product above would be affine, but as we pointed out, it is not quasi-compact, and hence, F cannot be affine. Topologically, F is just

a one-point space. Take the point in F, because F is a scheme, there exists an open affine neighborhood $\operatorname{Spec} R$ of this point, pulling this neighborhood back through the quotient map $\operatorname{Spec} k(x) \to F$, we obtain the fiber product would be affine, which is a contradiction. Hence, there is no affine neighborhood of the point of F, and F is not a scheme.

Example 2.3.10. We can construct geometric examples of algebraic spaces as follows. We can start with a scheme X and two closed points x, y on X such that they have the same residue field and they do not have a common affine neighborhood. And we glue x and y by defining an etale equivalence relation. Then the quotient defined by that gluing is an algebraic space, and it is not a scheme. We refer to [S21] for more details.

2.4 Descent data and stacks

As we saw earlier, sheaves on sites are generalizations of schemes. But there are important functors that fail to be a sheaf. Usually, there are two ways to cope with that. The first one is to sheafify these functors, but it sometimes is difficult to capture useful information after sheafification. Also, because our sheaves are valued in sets, which means we have to kill possible automorphisms. The second solution is the notion of stacks, where we allow the existence of automorphisms, and in many cases, we can just keep our naive functors, as in the case of moduli functor of curves. To define what a stack is, we need to review the notion of descent datum. Throughout the section, we will fix a category $\mathcal{C}$. We will first recall about fibered categories and the equivalence of the definition of a fibered cateogry and a pseudo functor.

Definition 2.4.1. A *category over* $\mathcal{C}$ is a pair $(\mathcal{F}, p)$, where $\mathcal{F}$ is a category and $p : \mathcal{F} \to \mathcal{C}$ is a functor.

Definition 2.4.2. Let $(\mathcal{F}, p)$ be a category over $\mathcal{C}$, an arrow $\phi : \psi \to \eta$ in $\mathcal{F}$ is said to be *cartesian* if for any arrow $\alpha : \zeta \to \eta$ in $\mathcal{F}$, and any $h : p(\zeta) \to p(\psi)$ in $\mathcal{C}$ such that $p(\phi) \circ h = p(\alpha)$, then there exists only one $\theta : \zeta \to \psi$ such that $h = p(\theta)$, and $\phi \circ \theta = \alpha$.

Definition 2.4.3. Let $(\mathcal{F}, p)$ be a category over $\mathcal{C}$, we say that $\mathcal{F}$ *is a fibered category over* $\mathcal{C}$ if for any arrow $f : U \to V$ in $\mathcal{C}$ and any η in $\mathcal{F}$ such that $p(\eta) = V$, there exists ψ in $\mathcal{F}$

and $\phi : \psi \to \eta$ a catersian arrow such that $p(\phi) = f$.

Definition 2.4.4. Let $(\mathcal{F}, p)$ be a fibered category over $\mathcal{C}$, for any U in $\mathcal{C}$, we can define *the fiber over* U, denoted $\mathcal{F}(U)$, which consist of objects in F such that they map to U via p, and morphisms in $\mathcal{F}(U)$ are morphisms in $\mathcal{F}$ that maps to id_U in $\mathcal{C}$ via p.

The definition of fibered categories is equivalent to the definition of pseudo functor below [FGAE, Section 3.1.3].

Definition 2.4.5. A *pseudo functor* on $\mathcal{C}$ consists of the following data

- For each object U of C, there is a category ΦU.
- For each arrow $f : U \to V$ in $\mathcal{C}$, there is a functor $f^* : \Phi V \to \Phi U$.
- For each object U in $\mathcal{C}$, there is an isomorphism of functors $\epsilon_U : \mathrm{id}_U^* \cong \mathrm{id}_{\Phi U}$.
- For each pair of arrows $U \xrightarrow{f} V \xrightarrow{g} W$, there is an isomorphism of functors $\alpha_{f,g} : f^*g^* \cong (gf)^*$ from ΦW to ΦU.

And these data are required to satisfied these conditions

- For an arrow $U \xrightarrow{f} V$ in $\mathcal{C}$ and η is an object in ΦV, we have $\alpha_{\mathrm{id}_U,f} = \epsilon_U(f^*\eta)$ and $\alpha_{f,\mathrm{id}_U} = f^*\epsilon_V\eta$.
- Whenever we have arrows $U \xrightarrow{f} V \xrightarrow{g} W \xrightarrow{h} T$, and an object θ in ΦT, we have

$$\alpha_{gf,h}(\theta) \circ \alpha_{f,g}(h^*\theta) = \alpha_{f,gh}(\theta) \circ f^*\alpha_{g,h}(\theta)$$

  from $f^*g^*h^*\theta$ to $(hgf)^*\theta$.

Example 2.4.6. We associate each scheme X the category $\mathrm{QCoh}(X)$ of quasi-coherent sheaves on X. And for each morphism of scheme $X \xrightarrow{f} Y$, we associate the pullback functor of sheaves $f^* : \mathrm{QCoh}(Y) \to \mathrm{QCoh}(Y)$. This defines a pseudo functor QCoh over (Sch). And this defines a category QCoh fibered over (Sch).

From now on we will fix a site $\mathcal{C}$ with fiber products and a category $\mathcal{F}$ together with a functor $p : \mathcal{F} \to \mathcal{C}$.

Definition 2.4.7. For any covering $\{U_i \to U\}_i$ in $\mathcal{C}$, we define the *category of descent datum* $\mathcal{F}(\{U_i \to U\}_i)$ consisting of objects of the form $(\xi_i, \phi_{ij})_{i,j}$ where $\xi_i \in \mathcal{F}(U_i)$ and ϕ_{ij} is an isomorphism from $\mathrm{pr}_1^*\xi_i$ to $\mathrm{pr}_2^*\xi_j$ in $\mathcal{F}(U_i \times_U U_j)$ such that $\mathrm{pr}_{13}^*\phi_{ik} \cong \mathrm{pr}_{23}^*\phi_{jk} \circ \mathrm{pr}_{12}^*\phi_{ij}$ in $\mathcal{F}(U_i \times_U U_j \times_U U_k)$. Let (ψ_i, ϕ_{ij}) and (η_i, φ_{ij}) be two descent datum, we define a morphism between them is a family of morphism $\alpha_i : \xi_i \to \eta_i$ such that for all i, j, we have $\varphi_{ij} \circ \mathrm{pr}_1^*\alpha_i \cong \mathrm{pr}_2^*\alpha_j \circ \phi_{ij}$. Say another words, those α_i make the following diagram commute

$$\begin{array}{ccc} \mathrm{pr}_1^*\xi_i & \xrightarrow{pr_1^*\alpha_i} & \mathrm{pr}_1^*\eta_i \\ {\scriptstyle \phi_{ij}}\downarrow & & \downarrow{\scriptstyle \varphi_{ij}} \\ \mathrm{pr}_2^*\xi_j & \xrightarrow[pr_2^*\alpha_j]{} & \mathrm{pr}_2^*\eta_j. \end{array}$$

For any covering $\{U_i \to U\}_i$ in $\mathcal{C}$, there is a canonical functor $\mathcal{F}(U) \to \mathcal{F}(\{U_i \to U\}_i)$ by sending any object ξ to $(\xi|_{U_i}, \mathrm{id})$, where id is the identity morphism of $\xi|_{U_i \times_U U_j}$.

Definition 2.4.8. We say that $\mathcal{F}$ is a *stack* over $\mathcal{C}$ if for any covering $\{U_i \to U\}$ in $\mathcal{C}$, the canonical functor above is an equivalence of categories.

There are important examples of stacks we will consider.

Proposition 2.4.9. *Let F be a sheaf of sets on $\mathcal{C}$, then F can be seen as a stack over $\mathcal{C}$.*

Proof. We can view F as a category fibred over $\mathcal{C}$ with the identification between $\mathcal{F}(U)$ and $F(U)$ for all object U in $\mathcal{C}$, and all arrows are identity morphisms. Let $\{U_i \to U\}_i$ be a covering in $\mathcal{C}$ then $\mathcal{F}(\{U_i \to U\}_i)$ consists of $(\xi_i, \phi_{ij})_{i,j}$ where $\xi_i \in \mathcal{F}(U_i)$ and ϕ_{ij} is the identification between $\mathrm{pr}_1^*\xi_i$ and $\mathrm{pr}_2^*\xi_j$ since arrows in sets are just identities. Now, because F is a sheaf, we have the following exact sequence

$$0 \to \mathcal{F}(U) \to \prod_i \mathcal{F}(U_i) \rightrightarrows \prod_{i,j} \mathcal{F}(U_i \times_U U_j).$$

And this yields the canonical functor $\mathcal{F}(U) \to \mathcal{F}(\{U_i \to U\}_i)$ is a bijection of sets. This implies $\mathcal{F}$ is a stack. □

Corollary 2.4.10. *Schemes are stacks in the fppf topology. Algebraic spaces are also stacks.*

Proof. By Theorem 2.1.11, schemes are sheaves with respect to the fppf topology. This yields by the previous proposition that schemes are stacks. For algebraic spaces, by defintion, they are sheaves. The conclusion follows directly from the previous proposition. □

Example 2.4.11. (Stack of quasi-coherent sheaves in the Zariski topology) Let us denote QCoh the category over (Sch) whose fiber over a scheme X is the category of quasi-coherent sheaves on X. Let $\{U_i \to X\}_i$ be an open covering of X. By gluing properties of sheaves, given a quasi-coherent sheaf F on X is equivalent to give a family $(F_i, \phi_{ij})_{ij}$ where F_i is a sheaf on U_i and ϕ_{ij} is an isomorphism between $F_i|_{U_i \cap U_j}$ and $F_j|_{U_i \cap U_j}$ such that for all i, j, k, we have $\phi_{ik} = \phi_{jk} \circ \phi_{ij}$ on $U_i \cap U_j \cap U_k$. And this is clear that $\mathrm{QCoh}(\{U_i \to X\}_i)$ consists of these (F_i, ϕ_{ij}). This implies that QCoh is stack over $(\mathrm{Sch})_{Zar}$.

Remark 2.4.12. It is proved by Grothendieck, for a proof, see e.g. [FGAE, Theorem 4.23] that QCoh is also a stack over $(\mathrm{Sch})_{fppf}$.

2.5 Hom sheaves and an equivalent defintion of stacks

In this section, we will give an equivalent definition of stacks. That is very useful to prove if fibered category over (Sch/S) is a stack. For example, we will see its applications in the next chapter when we prove that the moduli problem of elliptic curves are a Deligne-Mumford stack and the moduli of genus one curves are Artin stacks. As usual, we will fix a site $\mathcal{C}$ and a category $\mathcal{F}$ over $\mathcal{C}$.

Definition 2.5.1. We say that $\mathcal{F}$ is a *prestack* over $\mathcal{C}$ if for any covering $\{U_i \to U\}_i$ in $\mathcal{C}$, the canonical morphism $\mathcal{F}(U)$ to $\mathcal{F}(\{U_i \to U\}_i)$ is fully faithful.

Lemma 2.5.2. *$\mathcal{F}$ is a prestack over $\mathcal{C}$ if and only if for all covering $\{U_i \xrightarrow{f_i} U\}_i$, and all ψ, η in $\mathcal{F}(U)$ together with a morphism $\alpha_i : f_i^*\xi \to f_i^*\eta$, such that $pr_1^*\alpha_i = pr_2^*\alpha_j$ on $\mathcal{F}(U_i \times_U U_j)$, then there exists a unique morphism $\alpha : \xi \to \eta$ in $\mathcal{F}(U)$ such that $\alpha_i = f_i^*\alpha$.*

Proof. The family of morphisms $(\alpha_i)_i$ defines a morphism of two descent datum $(f_i^*\xi, \mathrm{id})$ and $(f_i^*\eta, \mathrm{id})$. Because the functor is fully faithful, there exists a unique morphism $\alpha : \xi \to \eta$ such that $\alpha_i = f_i^*\alpha$. □

Let U be an object of $\mathcal{C}$, we denote $\mathcal{C}/U$ the category whose objects are morphisms $V \xrightarrow{f} U$ in $\mathcal{C}$. A morphism between $V \xrightarrow{f} U$ and $W \xrightarrow{g} U$ is a morphism $h : V \to W$ in $\mathcal{C}$

such that $f = g \circ h$. For an object U in $\mathcal{C}$, and two objects ξ, η in $\mathcal{F}(U)$. We define the following functor

$$\mathrm{Hom}(\xi, \eta) : \mathcal{C}/U \to (\mathrm{Sets})$$

sending $\mathrm{Hom}(\xi, \eta)(V \xrightarrow{f} U)$ to $\mathrm{Hom}_{\mathcal{F}(V)}(f^*\xi, f^*\eta)$.

Proposition 2.5.3. *$\mathcal{F}$ is a prestack over $\mathcal{C}$ if for any object U in $\mathcal{C}$ and any ξ, η in $\mathcal{F}(U)$, the functor $\mathrm{Hom}(\xi, \eta)$ defined above is a sheaf.*

Proof. Assume that for all object U in $\mathcal{C}$ and all objects ξ, η in $\mathcal{F}(U)$, $\mathrm{Hom}(\xi, \eta)$ is a sheaf, then in particular, for an arrow $U \xrightarrow{\mathrm{id}} U$ in $\mathcal{C}/U$, we have an exact sequence for any covering $\{U_i \to U\}_i$ in $\mathcal{C}$

$$0 \to \mathrm{Hom}_{\mathcal{F}(U)}(\xi, \eta) \to \prod_i \mathrm{Hom}_{\mathcal{F}(U_i)}(f_i^*\xi, f_i^*\eta) \rightrightarrows \prod_{i,j} \mathrm{Hom}_{\mathcal{F}(U_i \times_U U_j)}(f_{ij}^*\xi, f_{ij}^*\eta)$$

where $f_{ij} : U_i \times_U U_j \to U$ is the composition of $f_i \circ \mathrm{pr}_1 = f_j \circ \mathrm{pr}_2$. And the fact that this sequence is exact is exactly the condition of the lemma above, and this yields $\mathcal{F}$ is a prestack over $\mathcal{C}$. The converse is basically the same by the lemma above again. □

Definition 2.5.4. A descent datum $(\xi_i, \phi_{ij})_{i,j}$ of $\mathcal{F}(\{U_i \to U\}_i)$ is said to be *effective* if it is an image of an object from $\mathcal{F}(U)$ via the canonical functor from $\mathcal{F}(U)$ to $\mathcal{F}(\{U_i \to U\}_i)$.

Using the proposition above, we obtain the following equivalent defintion of a stack.

Proposition 2.5.5. *Let $\mathcal{F}$ be a category over $\mathcal{C}$, then $\mathcal{F}$ is a stack over $\mathcal{C}$ if and only if*

- *For all object U in $\mathcal{C}$ and all objects ξ, η of $\mathcal{F}(U)$, $\mathrm{Hom}(\eta, \xi)$ is a sheaf.*
- *All descent datum is effective.*

Proof. It is just a consequence of the proposition above. □

2.6 Deligne-Mumford stacks and Artin stacks

In this section, we will define the notions of Artin stacks and Deligne-Mumford stacks.

Definition 2.6.1. An **Artin stack** $\mathcal{X}$ over S is a category $\mathcal{X}$ over (Sch/S) with the following properties

- $\mathcal{X}$ is a stack over (Sch/S) fibred in groupoids.
- The diagonal morphism $\Delta : \mathcal{X} \to \mathcal{X} \times \mathcal{X}$ is representable by algebraic spaces.
- There exists a smooth surjection $U \to \mathcal{X}$ from a scheme.

We note that the second condition is equivalent to say that for any algebraic spaces U, V over $\mathcal{X}$, the fiber product $U \times_{\mathcal{X}} V$ is algebraic space. And this makes sense the third condition, i.e. we require that there exists there exists a scheme U over $\mathcal{X}$ such that for any algebraic space V over X, the morphism $U \times_{\mathcal{X}} V \to V$ is smooth, surjective.

Example 2.6.2. In the next chapter, we will see that the stack $\mathcal{M}_{1,0}$ of curves of genus one is an Artin stack.

Example 2.6.3. Let G be a smooth group scheme over S, in the next section, we will see that the classifying stack BG is an Artin stack over S.

Definition 2.6.4. A **Deligne-Mumford stack** $\mathcal{X}$ over S is a category $\mathcal{X}$ over Sch/S with the following properties

- $\mathcal{X}$ is a stack over (Sch/S) fibred in groupoids.
- The diagonal morphism $\Delta : \mathcal{X} \to \mathcal{X} \times \mathcal{X}$ is representable by algebraic spaces.
- There exists a etale surjection $U \to \mathcal{X}$ from a scheme.

Example 2.6.5. In the next chapter, we will prove that the stack $\mathcal{M}_{1,1}$ of elliptic curves is a Deligne-Mumford stack.

2.7 Torsors and principal bundles

Throughout the section, we will fix a base scheme S and a topology $\tau \in \{\text{Zariski, etale, fppf}\}$ in (Sch/S). We will introduce the notions of torsors and and principal bundles. We refer to [O, Section 4.5] for further details.

Definition 2.7.1. Let G be a group scheme, a *principal G-bundle over B* (or a *principal homogeneous space over B*) is a pair $(X, \pi : X \to B)$ where X is a scheme with an action

from G, and the morphism $\pi : X \to B$ is a covering and G-invariant, i.e. $\pi(\sigma x) = \pi(x)$ on points, such that the morphism

$$G \times_B X \longrightarrow X \times_B X \quad (\sigma, x) \longmapsto (x, \sigma x)$$

is an isomorphism.

Definition 2.7.2. Let $\mathcal{G}$ be a sheaf of groups on $(\mathrm{Sch}/S)_\tau$, a *torsor over* $\mathcal{G}$ is a sheaf $\mathcal{F}$ together with an action $\mu : \mathcal{G} \times \mathcal{F} \to \mathcal{F}$ such that

(i) For all scheme U, there exists a covering $\{U_i \to U\}$ of U such that $\mathcal{F}(U_i) \neq \emptyset$ for all i.

(ii) The morphism of sheaves

$$\mathcal{G} \times \mathcal{F} \longrightarrow \mathcal{F} \times \mathcal{F} \quad (\sigma, f) \longmapsto (f, \sigma f)$$

is an isomorphism.

From the defintion, it is clear that the second condition is equivalent to the action of $\mathcal{G}$ on $\mathcal{F}$ is simply transitive.

Lemma 2.7.3. *Let G be a group scheme, and $(X, \pi : X \to B)$ is a principal G-bundle over B, then X is a G-torsor over B.*

Proof. It is sufficient to check the first condition of the definition of torsors. Because $X \to B$ is a covering, for any scheme U over B, $\{U_X \to U\}$ is a covering, and there is a canonical projection $pr_2 : U_X \to U$ making $X(U_X) \neq \emptyset$. □

Definition 2.7.4. Let $(X_1, \pi_1 : X_1 \to B), (X_2, \pi_2 : X_2 \to B)$ be principal G-bundles over B, a morphism between them is a G-equivariant map between B-schemes. Similarly, a morphism between $\mathcal{G}$-torsors is a G-equivariant morphism of sheaves.

From the definition and the lemma, we obtain the following faithful functor between two categories

$$\{\text{Principal } G\text{-bundles over } B\} \longrightarrow \{G\text{-torsors over } B\} \quad (X, \pi : X \to B) \longmapsto X$$

This proposition tells us that when G is a smooth group scheme, the two categories are equivalent with respect to the etale topology [O, Remark 4.5.7].

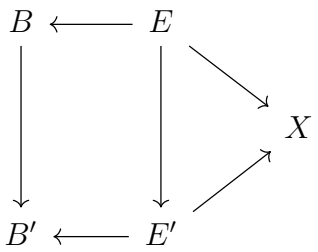
Proposition 2.7.5. *The functor above is an equivalent of categories if G is a smooth group scheme over S, and τ is the etale topology on (Sch/S).*

2.8 Quotient stacks and classifying stacks

As usual, throughout the section, we will fix a base scheme S, a smooth group scheme G over S and an S-scheme X with an action from G.

We denote $[X/G]$ a category fibered over $(\mathrm{Sch}/S)_{et}$ whose objects over a scheme B are of the form $(B \leftarrow E \rightarrow X)$, where $E \rightarrow B$ is a principal G-bundle, and $E \rightarrow X$ is G-equivariant morphism.

A morphism between $(B \leftarrow E \rightarrow X)$ and $(B' \leftarrow E' \rightarrow X)$ are morphisms $B \rightarrow B'$ and $E \rightarrow E'$ making the following digram



commute, where the left square is cartesian.

Proposition 2.8.1. *The category $[X/G]$ over $(\mathrm{Sch}/S)_{et}$ is an algebraic stack.*

Proof. It is clear from the definition that $[X/G]$ is fibered in groupoid. We will check that

(i) The Isom sheaf is representable (cf. Proposition 2.5.5).

(ii) All descent datum is effective.

(iii) There is a smooth covering of $[X/G]$ from a scheme.

For the first statement, let B be an S-scheme, and ξ, η two objects of $[X/G](B)$, where $\xi = (B \leftarrow E \xrightarrow{f} X)$ and $\eta = (B \leftarrow E' \xrightarrow{f'} X)$. Then $\mathrm{Isom}_B(\xi, \eta) \neq \emptyset$ if and only if $E = E'$ and $f = f'$. And in this case, $\mathrm{Isom}_B(\xi, \eta)$ is completely determined by morphism $\pi : E \rightarrow E$ such that $\pi = f \circ \pi$.

Now, $G(E)$ acts on $X(E)$ and over E, G and E are isomorphic. And hence, such a morphism π is exactly an element in $G(E)$ that fixes f. Hence, $\mathrm{Isom}_B(\xi, \eta)$ is representable by the stabilizer of f, which is a scheme. And this proves the first statement.

For the second statement, let B be an S-scheme and $\{B_i \rightarrow B\}$ an etale covering and $E_i \rightarrow B_i$ are principal G-bundles such that the cocycle condition holds. In particular, E_i

are G-torsors, and we can glue E_i as sheaves to get a sheaf E over B such that E is a B-torsor. Because G is smooth over S, and we are in etale site, such a G-torsor is indeed a principal G-bundle over B.

Finally, for the third statement, there is a morphism $X \to [X/G]$ that sends any X-scheme U to the trivial principal G-bundle $(U, G\times U, X)$ where the morphism $G\times U \to X$ sends (σ, u) to $\sigma f(u)$ on points. It is G-equivariant with the left translation action of G on itself. We will show that this morphism is smooth.

Let $B \to [X/G]$ be a morphism given by $(B \leftarrow E \to X)$, then $(X \times_{[X/G]} B)(B')$ is characterized by $\phi : E_{B'} \cong G_{B'}$, and such an isomorphism ϕ is determined by a section $B' \to E_{B'}$ (because the principal bundle $E_{B'}$ is trivial if and only if it has a section). Hence, the fiber product above is just $\mathrm{Hom}_{B'}(B', E_{B'})$, and this yields $X \times_{[X/G]} B$ is representable by E, which is smooth over B, since G is smooth over S. Therefore, $[X/G]$ is an algebraic stack over $(\mathrm{Sch}\,/S)_{et}$. □

Definition 2.8.2. When $X = S$ and the action of G on S is trivial, then $[S/G]$ is called the *classifying stack*, denoted $B_S G$. When the context is clear, we denote BG the classifying stack of G.

Chapter 3

Moduli of elliptic and genus one curves

In this chapter, we will review the theory of elliptic curves and curves of genus one in absolute and relative settings. Furthermore, we also define the category of family of genus one curves and prove it is an algebraic stack.

3.1 Elliptic curves

Elliptic curves are important objects in algebraic geometry and number theory. An elliptic curve is an abelian variety of dimension 1, which can be described by an explicit equation. Throughout the section, we will fix a base field k.

Definition 3.1.1. An elliptic curve E over k is a smooth, proper, geometrically integral scheme of dimension one over k with a k-rational point such that $H^1(E, \mathcal{O}_E) = 1$.

We note that it is not immediate from the definition that an elliptic curve E over k is a group scheme. We will prove this later in our third section. By Riemann-Roch's theorem, there is a bijection between $E(k)$ and $\mathrm{Pic}^0(E)$, where $\mathrm{Pic}^0(E)$ is the abelian group of linearly equivalent classes of degree zero divisors on E. If we denote O the k-rational point of E, then the bijection above can be defined as follows

$$E(k) \longrightarrow \mathrm{Pic}^0(E), \quad P \longmapsto [P] - [O]$$

And this bijection defines the group law on $E(k)$. Again, by Riemann-Roch theorem, the divisor $3[O]$ is very ample on E, and we can define an embedding of E into $\mathbb{P}^2_k$.

This embdding will give us the explicit equation defining E. More presecily, when $2, 3$ is invertible in k, any elliptic curve E over k is of the homogeneous form

$$y^2z = x^3 + axz^2 + bz^3$$

for some a, b in k such that $\Delta = 4a^3 + 27b^2 \neq 0$, with a k-rationl point $O = (0, 1, 0)$. We note that the condition on Δ is equivalent to say the equation $x^3 + ax + b = 0$ does not have double roots in k, otherwise the curve will be singular. Over $\mathbb{C}$, an elliptic curve can be defined as the quotient of $\mathbb{C}$ by a lattice of rank 2 over $\mathbb{Z}$. We will next prove that the automorphism group of an elliptic curve is finite.

Proposition 3.1.2. *Assume that $2, 3$ is invertible in k, where k is algebraically closed, then for any elliptic curve over k, $\mathrm{Aut}(E)$ is either $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z}$.*

Proof. Assume that our elliptic curve E is given by $y^2 = x^3 + ax + b$. Any automorphism of E induces an automorphism of $H^0(E, \mathcal{O}_E(nO))$, where $n = 1, 2, 3$; and hence, is of the form $(x, y) \mapsto (cx + d, ex + fy + g)$, which also satisfies the equation of E. By comparing coefficients, we obtain $d = e = g = 0$, and $c^3 = f^2$. Denote u the square root of e in k, then $c = u^2, f = u^3$, then any automorphism of E is of the form $x' = u^2x, \quad y' = u^3y$. And this yields $u^4a = a$ and $u^6b = b$. If both $a, b \neq 0$, then $u^2 = 1$, and in this case $\mathrm{Aut}(E) \cong \mathbb{Z}/2\mathbb{Z}$. If $a = 0$, then $b \neq 0$ (because of the condition on Δ), and in this case, $u^6 = 1$, and $\mathrm{Aut}(E) \cong \mathbb{Z}/6\mathbb{Z}$. Finally, if $b = 0$, then $u^4 = 1$, and $\mathrm{Aut}(E) \cong \mathbb{Z}/4\mathbb{Z}$. □

When the characteristic of k is 2 or 3, the computation is more complicated, but it is still true that $\mathrm{Aut}(E)$ is finite. We refer to [Silverman, Apendix A] for the proof.

Example 3.1.3. Over $\mathbb{C}$, the automorphism of the curve $y^2 = x^3 + 1$ is cyclic of order 6, generated by $(x, y) \mapsto (\zeta^2 x, \zeta^3 y)$, where ζ is the 6th primitive root of unity in $\mathbb{C}$.

Example 3.1.4. Let p be a prime such that $p \equiv 1 \mod 4$. By Euler's criterion [IR, Theorem 1, Chapter 5], -1 is a square in $\mathbb{F}_p$. Denote ω the 4th-primitive root of 1 in $\mathbb{F}_p$. Consider the curve $(E) : y^2 = x^3 + x$ over $\mathbb{F}_p$. The automorphism group of E is isomorphic to $\mathbb{Z}/4\mathbb{Z}$, and generated by $(x, y) \mapsto (-x, -\omega y)$. This automorphism is defined over $\mathbb{F}_p$.

Next, we will discuss about twists and torsors over elliptic curves and their relations to Galois cohomology. One hopes to obtain the similar correspondence in the relative setting, by replacing the absolute Galois group by etale fundamental group, but this does not hold true. More details for relative settings will be discussed later.

3.2 Recollections on relative effective Cartier divisors

In this section, we will review the theory of relative Cartier divisor, which is needed to study sections of family of curves. Throughout the section, we will fix a base scheme S, and an S-scheme X.

Definition 3.2.1. Let $D \subset X$ be a closed subscheme, we say that D is a *relative Cartier divisor* if D is flat over S, and the ideal sheaf $\mathcal{O}_X(-D)$ is an invertible $\mathcal{O}_X$-module.

Locally, when $S = \operatorname{Spec} R$, $X = \operatorname{Spec} A$, any such Cartier divisor D is the zero locus of of some $f \in A$, such that f is non-zero divisor in A, and A/fA is flat over R.

Let D be a relative Cartier divisor, we have the following exact sequence of $\mathcal{O}_X$ modules

$$0 \to \mathcal{O}_X(-D) \to \mathcal{O}_X \to \mathcal{O}_D \to 0$$

Tensoring with $\mathcal{O}_X(D)$ we obtain

$$0 \to \mathcal{O}_X \to \mathcal{O}_X(D) \to \mathcal{O}_D \otimes_{\mathcal{O}_X} \mathcal{O}_X(D) \to 0$$

And there is a canonical section l of $\mathcal{O}_X(D)$, which is the image of the section 1 of $\mathcal{O}_X$, and we can recover D as the zero locus of l.

Conversely, let $(\mathcal{L}, l)$ be a pair, where $\mathcal{L}$ is an invertible sheaf on X, and l is a section of $\mathcal{L}$, such that we have the following exact sequence of $\mathcal{O}_X$ modules

$$0 \to \mathcal{O}_X \xrightarrow{\times l} \mathcal{L} \to \mathcal{L}/\mathcal{O}_X \to 0$$

and $\mathcal{L}/\mathcal{O}_X$ is flat over S. Then we can obtain an effective Cariter disvisor as the zero locus of l and $\mathcal{L} = \mathcal{O}_X(D)$. And this yields

Proposition 3.2.2. *Given a relative effective Cartier disisor on X is the same as to be given a pair $(\mathcal{L}, l)$ where $\mathcal{L}$ is an invertible sheaf on X, and l is a section of $\mathcal{L}$, such that*

$$0 \to \mathcal{O}_X \xrightarrow{\times l} \to \mathcal{L} \to \mathcal{L}/\mathcal{O}_X \to 0$$

is exact and $\mathcal{L}/\mathcal{O}_X$ is flat over S.

There are some useful properties of effective Cartier divisors.

Proposition 3.2.3. *The following statements holds:*

(i) Let D_1, D_2 be relative effective Cartier divisors on X, then so is $D_1 + D_2$.

(ii) Let T be any scheme with a structure morphism $f : T \to S$, and D is an effective Cartier divisor on X, then $f_T^* D$ is an effective Cartier divisor on X_T over T.

Proof. For (i), we note that locally, if D_1 (respectively D_2) is given by $f_1 \in A$ (resp. $f_2 \in A$), then $D_1 + D_2$ is the zero locus of $f_1 f_2$. For (ii), we can use the presentation of D by the pair $(\mathcal{L}, l)$, then $f_T^* D$ is characterized by the pair $(\mathcal{L} \otimes_{\mathcal{O}_S} \mathcal{O}_T, l \otimes 1)$. □

To check if a closed subscheme of X is an effective Cartier divisor, we can reduce to the absolute case.

Lemma 3.2.4. *Assume that S is locally Noetherian and X is flat of finite presentation over S. Let $\mathcal{F}$ be a coherent sheaf on X, flat over S, then $\mathcal{F}$ is flat over X if and only if for all geometric point $\operatorname{Spec}\Omega \to S$, $\mathcal{F}_\Omega$ is flat over X_Ω.*

Proof. It is the fiber by fiber criterion of flatness, and we refer to [SP, Lemma 37.16.4] for the proof. □

We now come to the main result of this section.

Proposition 3.2.5. *Assume that S is locally Noetherian, X is flat of finite presentation over X. Let D be a closed subscheme of X flat over S, then D is a relative effective Cartier divisor if and only if for all geometric points $\operatorname{Spec}\Omega \to S$, D_Ω is a effective Cartier divisor on X_Ω over $\operatorname{Spec}\Omega$.*

Proof. The only if part follows from the previous proposition that relative effective Cartier divisors behave well under pull back.

We will now prove the if part. From the exact sequence

$$0 \to \mathcal{O}_X(-D) \to \mathcal{O}_X \to \mathcal{O}_D \to 0$$

where $\mathcal{O}_D$ and $\mathcal{O}_X$ is S-flat. By [SP, Lemma 17.8], $\mathcal{O}_X(-D)$ is also flat over S. Because $\mathcal{O}_D$ is flat over $\mathcal{O}_S$, we obtain

$$0 \to \mathcal{O}_X(-D) \otimes_{\mathcal{O}_S} \Omega \to \mathcal{O}_X \otimes_{\mathcal{O}_S} \Omega \to \mathcal{O}_D \otimes_{\mathcal{O}_S} \Omega \to 0$$

is also exact. And there is also an exact sequence

$$0 \to \mathcal{O}_X(-D_\Omega) \to \mathcal{O}_{X_\Omega} \to \mathcal{O}_D|_{\operatorname{Spec}\Omega} \to 0$$

Comparing the first terms, we obtain $\mathcal{O}_X(-D) \otimes_{\mathcal{O}_S} \Omega \cong \mathcal{O}_X(-D_\Omega)$, which is invertible $\mathcal{O}_{X_\Omega}$-module. By the previous lemma, $\mathcal{O}_X(-D)$ is a flat $\mathcal{O}_X$-module.

We will next prove that $\mathcal{O}_X(-D)$ is coherent. For this, it is sufficient to reduce to the affine settings, where $S = \operatorname{Spec} R$, with R is Noetherian, and $X = \operatorname{Spec} A$, where $A \cong R[x_1, ..., x_n]/(f_1, ..., f_m)$ and $D = \operatorname{Spec} R'$. The surjection R onto R' implies R' is of finite presentation over R.

The diagram $R \to A \to R'$ has $R \to R'$ is of finite presentation and $R \to A$ is of finite type. This yields, by [SP, Lemma 10.6.2] that $A \to R'$ is of finite presentation, and this immediately implies that the ideal sheaf defining R' is finitely generated as A-module. And this yields $\mathcal{O}_X(-D)$ is a coherent $\mathcal{O}_X$-module.

Now, because $\mathcal{O}_X(-D)$ is both flat and coherent, it is a locally free $\mathcal{O}_X$-module, and the hypothesis on geometric fibers implies that $\mathcal{O}_X(-D)$ is an invertible $\mathcal{O}_X$-module. From the definition, D is a relative effective Cartier divisor. □

3.3 Families of curves

In this section, we will define families of curves over a base scheme. Furthermore, we will give some characterizations of relative effective Cartier divisors in this setting. Throughout the section, we will fix a base scheme S.

Definition 3.3.1. A *family of curves* over S is a pair (C, f), where C is a scheme over S, $f : C \to S$ is flat, proper, of finite presentation, and all geometric fibers of f are smooth curves.

From the definition, because C is of relative dimension one over S, and f is proper, any section of f defines a closed immersion of S into C.

Proposition 3.3.2. *Let (C, f) be a family of curves, then any section $\sigma : S \to C$ of f defines a relative effective Cartier divisor, denoted $[\sigma]$.*

Proof. Because $f : C \to S$ is proper, and in particular, separated, and $\mathrm{id}_S = f \circ \sigma$ is a closed immersion, σ is a closed immersion. And this yields $[\sigma]$ is closed in C and flat over S.

Because f is of finite presentation, we can reduce to the case $S = \operatorname{Spec} R$ is Noetherian [EGA IV, 8.9.1 and 11.2.6.1]. Applying Proposition 3.2.5 for geometric points of S will give us the statement. □

Proposition 3.3.3. *Let (C, f) be a family of curves, then any relative effective Cartier divisor on C is finite, flat, of finite presentation over S. Conversely, any closed subscheme of X that is finite, flat, of finite presentation over S defines a relative effective Cartier divisor on C.*

Proof. Let $D \subset C$ be a relative effective Cartier divisor, then D is flat over S by definition. Moreover, reducing to the case $S = \operatorname{Spec} R$ is Notherian, gives us D is of finite presentation. Finally, for finiteness, because $D \to S$ is proper, it is sufficient to show that the map is quasi-finite, but it is clear when we reduce to the case $S = \operatorname{Spec} k$: any effective Cartier divisor of C/k is given by a finite sum of closed points.

For the converse, by Proposition 3.2.5, we can reduce to the case $S = \operatorname{Spec} \Omega$, where Ω is an algebraically closed field. And in this case, any effective divisor on C is defined by a finite sum of closed points, which are clearly flat, finite, of finite presentation over Ω. □

By this proposition, Zarisky local on S, say $S = \operatorname{Spec} R$, then $\Gamma(D, \mathcal{O}_D)$ is a locally free R-module of finite rank. This rank is defined to be the *degree of D*. There is an easy characterization of a relative effective Cartier divisor of degree one.

Proposition 3.3.4. *Any section σ of f defines an relative effective Cartier divisor of degree one. Conversely, any relative effective Cartier divisor of degree one give a section of f.*

Proof. The first assertion is clear because such σ defines a closed immersion from S to C. For the converse, if D is a relative effective Cartier divisor of C, the composition $D \to X \to C$ is an isomorphism, and the inverse map defines a section of f. □

3.4 Families of elliptic curves

Family of elliptic curves is a generaliztion of elliptic curves over fields. We will prove in this section, such a family gives us a group scheme over the base scheme, and will give examples for family of elliptic curves. As usual, we will fix a base scheme S.

Definition 3.4.1. A *family of elliptic curves* over S is a triple $(E, f, 0)$, where E is a scheme over S, $f : E \to S$ is proper, flat of finite presentation, with all geometric fibers of f are smooth curves of genus one, and 0 is a section of f.

We will now prove the main result of this section.

Theorem 3.4.2. *Let (E, f, σ) be a family of elliptic curves, then E is a group scheme over S. Moreover, there exists a unique group structure on E such that for any scheme T, and any T-points P, Q, R in $E_T(T)$, we have $P + Q = R$ if and only if there exists an invertible sheaf $\mathcal{L}_0$ on T and an isomorphism of invertible sheaf on E_T*

$$\mathcal{O}_X(P) \otimes \mathcal{O}_X(Q) \otimes \mathcal{O}_X(-0) \cong \mathcal{O}_X(-R) \otimes f_T^*\mathcal{L}_0.$$

Proof. We denote $\mathrm{Pic}^1_{E/S}(T)$ the set of isomorphism classes of invertible sheaf $\mathcal{L}$ on X_T such that fiber by fiber, $\mathcal{L}$ is of degree one, modulo the equivalent relation $\mathcal{L} \sim \mathcal{L} \otimes f_T^*\mathcal{L}_0$, where $\mathcal{L}_0$ is an invertible sheaf on T.

The core idea is to prove the bijection between $\mathrm{Pic}^1_{E/S}(T)$ and $E_T(T)$, defined by

$$E_T(T) \longmapsto \mathrm{Pic}^1_{E/S}(T), \quad P \longmapsto \mathcal{O}_X(P)$$

If such bijection exsists, then for any point P, Q in $E_T(T)$, the invertible sheaf $\mathcal{O}_X(P) \otimes \mathcal{O}_X(Q) \otimes \mathcal{O}_X(-0)$ is fiberwise of degree one invertible sheaf. And there exists a unique R in $E_T(T)$, such that

$$\mathcal{O}_X(P) \otimes \mathcal{O}_X(Q) \otimes \mathcal{O}_X(-0) \cong \mathcal{O}_X(-R) \otimes f_T^*\mathcal{L}_0.$$

Denote $\mathrm{Pic}^0_{E/S}(T)$ the group of isomorphism classes of invertible sheaf $\mathcal{L}$ on X_T such that fiber by fiber, $\mathcal{L}$ is of degree 0, modulo the subgroup of the form $f_T^*\mathcal{L}_0$, where $\mathcal{L}_0$ is an invertible sheaf on T. Then there is a bijection between $\mathrm{Pic}^1_{E/S}(T)$ and $\mathrm{Pic}^0_{E/S}(T)$ defined by

$$\mathrm{Pic}^1_{E/S}(T) \longrightarrow \mathrm{Pic}^0_{E/S}(T), \quad \mathcal{L} \longmapsto \mathcal{L} \otimes \mathcal{O}_X(-0)$$

And this gives us the bijection between $E_T(T)$ and $\mathrm{Pic}^0_{E/S}(T)$, and the induced group structure is exactly what we described in the statement.

In short, it is sufficient for us to prove that the map

$$E_T(T) \longmapsto \mathrm{Pic}^1_{E/S}(T), \quad P \longmapsto \mathcal{O}_X(P)$$

is bijective. Because we can replace T by S, and E_T by E, it is enough to prove there is a bijection between $E(S)$ and Pic^1, where Pic^1 denotes $\mathrm{Pic}^1_{E/S}(S)$.

Now, take any invertible sheaf $\mathcal{L}$ on E in Pic^1, we want to construct a section of $E(S)$, i.e. the inverse of the map above. By Proposition 13, it is sufficient to construct a relative effective Cartier divisor of degree 1 corresponding to $\mathcal{L}$.

Because E is of finite presentation over S, we can again reduce to the case $S = \mathrm{Spec}\, R$ is Noetherian. The sheaf $R^1 f_* \mathcal{L}$ vanishes. In fact, at geometric points $\mathrm{Spec}\, \Omega \to S$, $R^1 f_* \mathcal{L}|_{\mathrm{Spec}\,\Omega} = (R^1 f_* \mathcal{L})_\Omega = H^1(E_\Omega, \mathcal{L}) = 0$ because $\deg \mathcal{L} = 1 > 2g_{E_\Omega} - 2 = 0$. And by [M74, Corollary 3, p. 53], $f_*\mathcal{L}$ is locally free of rank one, because over geometric points, it is of rank one. Hence, Zarisky locally, we can choose $l \in \Gamma(S, f_*\mathcal{L})$ such that it is an $\mathcal{O}_S$ basis of $\mathcal{L}$. Note that we also have $\Gamma(E, \mathcal{L}) = \Gamma(S, f_*\mathcal{L})$. Consider the morphism of sheaves $\mathcal{O}_X \xrightarrow{\times l} \mathcal{L}$, we will prove that it is injective and the quotient $\mathcal{L}/\mathcal{O}$ is flat over S. We now need to use a result in [EGA IV, Part 3, Proposition 11.3.7], that stated

Lemma 3.4.3. *Let $i : A \to B$ be a ring homomorphism of finite presentation, $u : M \to N$ is a morphism between B-modules, then the following are equivalent:*

(i) u is injective and $\mathrm{coker}(u)$ is flat over A.

(ii) For all $q \in \mathrm{Spec}\, B$, $p = i^{-1}(q)$, the induced morphism $\mathrm{id} \otimes u : k(p) \otimes_A M \to k(p) \otimes_A N$ is injective.

By using this, we can reduce to the case $S = \mathrm{Spec}\, k$, E is an elliptic curve over k, $H^0(E, \mathcal{O}_E) = k$ and l is now a k-basis, and in particular, non-zero. This yields, by the lemma above that $\mathcal{O}_E \xrightarrow{\otimes l} \mathcal{L}$ is injective, and $\mathcal{L}/\mathcal{O}$ is flat over S. Hence, by

characterization of relative effective Cartier divisor (Proposition 3.2.2), the pair $(\mathcal{L}, l)$ defines a relative effective Cartier divisor. Moreover, it is of degree one because of the hypothesis on fibers. By Proposition 3.3.4, it defines a section of f.

It is clear from the construction that the maps $E(S) \to \mathrm{Pic}^1$ and $\mathrm{Pic}^1 \to S$ are inverse of each other. And we now obtain a bijection between them. □

3.5 $\Gamma_1(N)$-structure on family of elliptic curves and its representability

In this section, we will introduce an important moduli problem, which is called $\mathbb{Z}/N\mathbb{Z}$ level structure on families of elliptic curves. As we will see, it will be a finite, flat cover of $\mathcal{M}_{1,1}$. When N is invertible over the base scheme, this cover is etale. The full generalities for level structures can be found in [KM]. Here we will only discuss what we need for our applications. Throughout the section, as usual, we will fix a base scheme S and E/S a family of elliptic curves.

Proposition 3.5.1. *Let $[N] : E \to E$ be the multiplication by N morphism on E. Then $[N]$ is finite, flat of degree N^2. The kernel $E[N]$ of $[N]$ represents the following functor*

$$T \mapsto \mathrm{Hom}_{Grp}(\mathbb{Z}/N\mathbb{Z}, E_T(T))$$

Moreover, if N is invertible on S, then $[N]$ is etale.

Proof. Because E is proper over S, the morphism $[N]$ is automatically proper. For the rest, it is sufficient to reduce to the case $S = \mathrm{Spec}\, k$. The theory of elliptic curves over fields yields $[N] : E \to E$ is flat of degree N^2 and the fiber at 0 has at most N^2 points. The equality occurs if and only if N is invertible on k, and this is equivalent to say $[N]$ is etale.

For the representability of $E[N]$, take any $\phi \in \mathrm{Hom}_{\mathrm{Grp}}(\mathbb{Z}/N\mathbb{Z}, E_T(T))$, then $\phi(1) \in E[N](T)$, and for the inverse map, for any $\sigma \in E[N](T)$, we can define a homomorphism of group $1 \mapsto \sigma$ from $\mathbb{Z}/N\mathbb{Z}$ to $E_T(T)$. It is clear that they are funtorial and inverse of each other. □

We will next define the notion of points of exact order N.

Definition 3.5.2. A section $P \in E(S)$ is said to be a *point of exact order* N if $D = \sum_{i=0}^{N-1}[iP]$ is of degree N and D is a subgroup scheme of E.

Example 3.5.3. Take $S = \operatorname{Spec} k$, and P is a point of order N on $E(k)$. The divisor $D = [0] + [P] + ...[(N-1)P]$ can be seen as the abelian group generated by P. It is of degree N, and a subgroup scheme of E. This follows that P is a point of exact order N by the definition. Conversely, if P is a point of exact order N, then D is killed by N. It then follows that P itself is killed by N, and because D is of degree N, the order of P is exactly N in E.

Proposition 3.5.4. *Assume N is invertible on S, and P is a point of $E(S)$ then the following are equivalent*

(1) P is of exact order N.

(2) For every geometric point $\operatorname{Spec}\Omega$ of S, P_Ω is a point of exact order N in E_Ω.

(3) For every geometric point $\operatorname{Spec}\Omega$ of S, P_Ω is a point of order N in $E(\Omega)$ (c.f. example above).

(4) The effective Cartier divisor $D = \sum_{i=0}^{N-1}[iP]$ is finite etale over S.

(5) The map $\mathbb{Z}/N\mathbb{Z} \to E(S)$ sending $1 \mapsto P$ defines a closed embeding of the constant group scheme $\mathbb{Z}/N\mathbb{Z} \to E$, which identifies $\mathbb{Z}/N\mathbb{Z}$ with the closed subscheme $\sum_{i=0}^{N-1}[iP]$.

Proof. (1) implies (2) is clear, since the degree of $D = \sum_{i=0}^{N-1}[iP]$ is stable under base change, and moreover D is a subgroup scheme of E implies that D_Ω is a subgroup scheme of E_Ω. Next, (2) and (3) are equivalent from Example 3.5.3. Assume (3) holds, then over any geometric point $\operatorname{Spec}\Omega \to S$, D_Ω is finite etale over $\operatorname{Spec}\Omega$. It then follows that D is also finite etale over S. And thus, (3) implies (4).

The morphism $(\mathbb{Z}/N\mathbb{Z})_S \to E$ sending 1 to P always factor through D. And this yields a morphism $(\mathbb{Z}/N\mathbb{Z})_S \to D$. To check if it is an isomorphism, we can reduce to a geometric point $\operatorname{Spec}\Omega \to S$. Over there, $(\mathbb{Z}/N\mathbb{Z})_\Omega \to D_\Omega$ is an isomorphism if and only if all points in D_Ω are distinct, i.e. D_Ω is finite etale over Ω. This is also equivalent to say D is finite etale over S. Hence, we obtain the equivalence between (4) and (5).

Finally, (5) implies (1) is clear, since $(\mathbb{Z}/N\mathbb{Z})_S$ is of degree N over S and it is a closed subgroup scheme of E by the assumptions of (5). □

By the proposition above, we obtain the following equivalent definition for points of exact order N.

Definition 3.5.5. A homomorphism $\phi : \mathbb{Z}/N\mathbb{Z} \to E(S)$ is said to be a $\mathbb{Z}/N\mathbb{Z}$*-structure* if $D = \sum_{i=0}^{N-1}[\phi(i)]$ is a relative effective Cartier divisor of degree N and D is a subgroup scheme of E.

Lemma 3.5.6. *Assume that $\phi : \mathbb{Z}/N\mathbb{Z} \to E(S)$ is a $\mathbb{Z}/N\mathbb{Z}$-structure, then $\phi(1)$ is a point of exact order N. Conversely, if P is a point of exact order N in $E(S)$, then there is a $\mathbb{Z}/N\mathbb{Z}$-structure ϕ defined by $\phi(1) = P$.*

Proof. It is clear from the definitions. □

Equivalently, we also have the following criterion for $\mathbb{Z}/N\mathbb{Z}$ structure on E.

Proposition 3.5.7. *Let $\phi : \mathbb{Z}/N\mathbb{Z} \to E(S)$ be a group homomorphism, then the following are equivalent*

(1) ϕ is $\mathbb{Z}/N\mathbb{Z}$-structure.

(2) For every geometric point $\operatorname{Spec}\Omega$ of S, $\phi_\Omega : \mathbb{Z}/N\mathbb{Z} \to E(\Omega)$ is $\mathbb{Z}/N\mathbb{Z}$ structure on E_Ω.

(3) For every geometric point $\operatorname{Spec}\Omega$ of S, the induced homomorphism $\phi_\Omega : \mathbb{Z}/N\mathbb{Z} \to E(\Omega)$ is injective.

(4) The effective Cartier divisor $D = \sum_{i=1}^{N-1}[\phi(i)]$ is finite etale over S.

(5) ϕ defines a closed immersion of the constant group scheme $\mathbb{Z}/N\mathbb{Z}$ to E which identifies $\mathbb{Z}/N\mathbb{Z}$ with the divisor $\sum_{i=0}^{N-1}[\phi(i)]$.

Consider the functor $\Gamma_1(E/S, N)$ defined by

$$T \longmapsto \{\mathbb{Z}/N\mathbb{Z} - \text{structures on } E_T/T\}$$

We will prove that $\Gamma_1(E/S, N)$ is representable by a closed subscheme of $E[N]$. To do this, we need the following

Lemma 3.5.8. *Let D be an effective Cartier divisors on E/S. Then there exists a closed subscheme $Z \subset S$ such that for any scheme T, D_T is a subgroup scheme of E_T if and only if the structure morphism $T \to S$ factors through Z. And the formation of Z commutes with arbitrary base change $S' \to S$.*

Proof. We will first prove the following claim.

Claim. *Let D, D' be two effective Cartier divisors on E/S, then there exists a unique closed subscheme Z of S, such that Z is universal for the relation $D' \leq D$ in the following sense: for any S-scheme T, $D'_T \leq D_T$ if and only if the structure morphism $T \to S$ factors through Z. Moreover, the formation of Z is compatible with base change.*

Proof of the claim. Assume D is represented by the pair $(\mathcal{L}, \ell)$, then $\mathcal{L}_{D'}$ is an invertible sheaf on D'. Because of Proposition 3.3.3, D' is finite, flat of finite presentation over S. Locally on S, say $S = \operatorname{Spec} R$, the rank of D' over S, say n, is exactly the rank of $H^0(\mathcal{O}_{D'}, \mathcal{L}_{D'})$ as R-module. Let $(e_1, ..., e_n)$ be a basis of this module.

Now, the condition $D' \leq D$ is equivalent to say that D' also vanishes on ℓ. Because ℓ can be uniquely expressed $\ell = f_1 e_1 + ... + f_n e_n$, for $f_i \in R$. Therefore, the condition $\ell = 0$ can be read as $f_1 = f_2 = ... = f_n = 0$, which defines a closed subscheme of $\operatorname{Spec} R$. And we have done the proof of the claim.

We now come back to the proof of the lemma. We first recall that D is a closed subgroup scheme of E if

1. The zero section factors through D, i.e. $[0] \leq D$.
2. D is stable under inversion i defined on points as $P \mapsto -P$, i.e. $i(D) = D$,
3. For all S-scheme T, and for all $f_1, f_2 \in D(T)$, $m(f_1, f_2)$ is also in $D(T)$.

For the first two conditions, by the claim above, they are universal on a closed subscheme of S, and it is sufficient to prove the last condition is also universal on a closed subscheme of S.

Let $W = D \times_S D$ with canonical projections p_1, p_2 to D. We will first show that last condition is satisfied if and only if $m(p_1, p_2) \in D(W)$. The only if part is clear. Now, assume that $m(p_1, p_2) \in D(W)$. For any S-scheme T, and any f_1, f_2 in $D(T)$, there exists a unique morphism $\theta : T \to D$ making the following diagram commute

$$\begin{array}{ccccc} D & \xleftarrow{f_1} & T & \xrightarrow{f_2} & D \\ & \nwarrow^{p_1} & \downarrow{\scriptstyle \theta} & \nearrow_{p_2} & \\ & & W & & \end{array}$$

And $m(f_1, f_2) = m(p_1 \circ \theta, p_2 \circ \theta) = m(p_1, p_2) \circ \theta$, where the last identity follows from the functorial property of group schemes: for any group scheme G and any morphism

of schemes $\theta : T \to T'$, the induced map $G(T') \to G(T)$ sending $f \to f \circ \theta$ is a group homomorphism, i.e. $m(f_1 \circ \theta, f_2 \circ \theta) = m(f_1, f_2) \circ \theta$ for all f_1, f_2 in $G(T')$. Now, since $m(p_1, p_2) \in D(W)$, it follows that $m(f_1, f_2)$ is in $D(T)$.

Next, we note that a morphism $f : T \to E$ from an S-scheme T factor through D if and only if $[f_T] \leq D_T$. Therefore, $m(p_1, p_2) \in D(W)$ if and only if $[m(p_1, p_2)_W] \leq D_W$. Now, we apply the claim, and conclude that the last condition is also universal on a closed subscheme of S.

□

Using this, we can prove

Proposition 3.5.9. *Assume that N is invertible in S, then $\Gamma_1(E/S, N)$ is representable by a scheme, which is finite and etale over S.*

Proof. Denote $S' = E[N]$, we will prove that $\Gamma_1(E/S, N)$ is representable by a closed subscheme of S'. From the definition, we can see that $\Gamma_1(E/S, N)$ is a subfunctor of S'. Moreover, since S' represents the functor $\mathrm{Hom}_{Grp}(\mathbb{Z}/N\mathbb{Z}, E(-))$, there is a universal homomorphism $\phi_{univ} : \mathbb{Z}/N\mathbb{Z} \to E(S')$ corresponding to $\mathrm{id} : S' \to S'$. By the proposition above, ϕ_{univ} defines a $\mathbb{Z}/N\mathbb{Z}$-structure on S' because over geometric points, ϕ_{univ} is an embedding of groups $\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Let $D = \sum_{i=0}^{n-1} [\phi_{univ}(i)]$ be the corresponding Cartier divisor on $E_{S'}$. It is a finite, etale subgroup scheme of S' of order n. It then follows by the previous lemma that there exists a closed subscheme Z of S' such that for any S'-scheme T, D_T is a subgroup scheme of E_T if and only if the structure $T \to S'$ factors through Z. It is now clear that Z represents $\Gamma_1(E/S, N)$.

Because $S' = E[N]$ is finite of finite presentation over S, Z is also finite of finite presentation over S. Hence, for etaleness, it is sufficient to prove Z is formally etale over S. Let T be any scheme, and T_0 its closed subscheme such that the ideal sheaf defined T_0 is nilpotent. Let $\phi_0 : \mathbb{Z}/N\mathbb{Z} \to E(T_0)$ be a $\mathbb{Z}/N\mathbb{Z}$-structure on E_{T_0}/T_0, we have to prove that ϕ_0 extends uniquely to $\phi : \mathbb{Z}/N\mathbb{Z} \to E(T)$ such that ϕ defines a $\mathbb{Z}/N\mathbb{Z}$-structure on E_T/T.

By the hypothesis, ϕ_0 defines a homomorphism from $\mathbb{Z}/N\mathbb{Z} \to E[N](T_0)$. And because $E[N]$ is etale, this extends uniquely to $\phi : \mathbb{Z}/N\mathbb{Z} \to E[N](T)$. To show that ϕ defines a $\mathbb{Z}/N\mathbb{Z}$-structure, it is sufficient to reduce to the case E is an elliptic curve over an

algebraically closed field Ω. But over there, ϕ and ϕ_0 are the same, because a field has (0) as the only ideal. And this follows that Z is formally etale over S, and hence, etale. □

3.6 Rigidity

Let E, E' be two elliptic curves over a *connected* base scheme S. Let $f : E \to E'$ be an isogeny. f induces a homomorphism $f^* : \mathrm{Pic}^0_{E'/S} \to \mathrm{Pic}^0_{E/S}$ sending $\mathcal{L} \mapsto f^*\mathcal{L}$. Because there is an isomorphism from E/S is to $\mathrm{Pic}^0_{E/S}$, which is compatible with group structures, $f^t = f^*$ defines a homomorphism in the other direction $E' \to E$.

Proposition 3.6.1. *Let $N = \deg f$, then the following hold:*

(1) $\deg f^t = N$,

(2) $f \circ f^t = [N]_{E'}$ *and* $f^t \circ f = [N]_E$.

(3) Let $g : E \to E'$ be another isogeny, then $(f+g)^t = f^t + g^t$

Moreover, if $E' = E$, then the following holds:

(3) There exists an integer, called the trace of f, denoted $tr(f)$, such that $f + f^t = [tr(f)]$.

(4) Inside the endomorphism ring of E, f is a root of the polynomial $X^2 - tr(f)X + \deg f = 0$.

(5) We have an inequality $tr(f)^2 \leq 4 \deg f$.

Proof. By Drinfeld's rigidity results [KM, Theorem II.2.4.1 and II.2.4.2], we can reduce the theorem to the case of elliptic curves over a field. The reduction in details can be found in [KM, Theorem 2.5.1]. When $S = \mathrm{Spec}\, k$, we refer to [Sil, Chapter III].

□

The next corollary will tell us that, indeed, the moduli problem $\Gamma_1(E/S, N)$ is rigid, for $N \geq 5$.

Corollary 3.6.2. *Let $\epsilon : E \to E$ be an automorphism of family of elliptic curves, and G a subgroup scheme of E of degree N over S. When $N \geq 5$, then ϵ induces the identity on G if and only if* $\epsilon = \mathrm{id}$.

Proof. Assume that ϵ induces the identity on G, we obtain $\epsilon - 1$ kills G. If $\epsilon \neq \mathrm{id}$, $\epsilon - 1$ is an isogeny of E, and its kernel contains G. We then obtain $\deg(\epsilon - 1) \equiv 0 \mod N$. By the proposition above, we have

$$\deg(\epsilon - 1) = (\epsilon^t - 1)(\epsilon - 1) = 1 - tr(\epsilon) + 1 \equiv 0 \mod N$$

And this yields $tr(\epsilon) \equiv 2 \mod N$. Because $tr(\epsilon)^2 \leq 4, \deg \epsilon = 4$, and $N \geq 5$, this shows $tr(\epsilon) = 2$, and ϵ satisfies $(\epsilon - 1)^2 = 0$. Because $\epsilon \neq \mathrm{id}$, $(\epsilon - 1)^2$ is an isogeny and hence, non-zero, a contradiction. This show $\epsilon = \mathrm{id}$. □

3.7 $\mathcal{M}_{1,1}$ is a Deligne-Mumford stack

In this section, we will define the category of elliptic curves and prove it is a Deligne-Mumford stack. Throughout the section, we will fix a base scheme S and an integer $N \geq 5$, which is invertible on S.

We denote (Aff/S) the category of affine schemes over S, and $\mathcal{M}_{1,1}$ a category over (Aff/S). Objects of $\mathcal{M}_{1,1}$ are of the form $(E, f, T, 0)$, where T is an affine scheme, and $(E, f, 0)$ is a family of elliptic curves over T. Given two objects $(E, f, T, 0)$ and $(E', f', T', 0)$, a morphism between is a pair (g, h) where $g : E \to E'$ and $h : T \to T'$ are morphisms of algebraic spaces such that the diagram

$$\begin{array}{ccc} E & \xrightarrow{g} & E' \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f'} \\ T & \xrightarrow{h} & T' \end{array}$$

is Catersian, and $E \xrightarrow{(g,f)} E' \times'_T T$ is an isomorphism of family of elliptic curves over T'. This is a category with a functor $\mathcal{M}_{1,1} \to (\mathrm{Aff}/S)$ sending $(E, f, T, 0)$ to T.

Definition 3.7.1. A *moduli problem for elliptic curves* is a contravariant functor $\mathcal{P} : \mathcal{M}_{1,1} \to \mathrm{Sets}$. $\mathcal{P}$ is said to be *relatively representable* if for all family of elliptic curves $(E, f, T', 0)$, the functor $T \mapsto \mathcal{P}(E_T, f_T, T, 0)$ is representable, denoted $\mathcal{P}_{E/T'}$. $\mathcal{P}$ is said to be *rigid* if the group $\mathrm{Aut}(E/T)$ acts freely on $\mathcal{P}(E/T)$ for all family of elliptic curves E over T. $\mathcal{P}$ is said to be *representable* if there exists a family of elliptic curves $(E_{\mathcal{P}}, f, \mathcal{M}(\mathcal{P}), 0)$ such that for all family of elliptic curves E over T, there is functorial isomorphism $\mathcal{P}(E/S) \cong \mathrm{Hom}_{\mathcal{M}_{1,1}}(E/S, E_{\mathcal{P}}/\mathcal{M}(\mathcal{P}))$.

Example 3.7.2. The functor $\Gamma_1(N)$ sends $(E, f, S, 0) \mapsto \{\mathbb{Z}/N\mathbb{Z} - \text{structures on } E/S\}$ is a moduli problem for elliptic curves. It is rigid and relatively rerepsentable by a scheme Z, where Z is a closed subgroup scheme of $E[N]$ and is finite, etale over S.

Definition 3.7.3. Let $\mathcal{P}$ be a relatively representable moduli problem of elliptic curves, $\mathbb{P}$ a property of morphism of schemes, we say that $\mathcal{P}$ *is* $\mathbb{P}$ *over* $\mathcal{M}_{1,1}$ if $\mathcal{P}_{E/T}$ is $\mathbb{P}$ over T for all family of elliptic curves E/T.

From the definition, we can see that $\Gamma_1(N)$ is finite, etale over $\mathcal{M}_{1,1}$. The following theorem will tell us $\Gamma_1(N)$ is representable.

Theorem 3.7.4. *Let $\mathcal{P}$ be a relatively representable moduli problem for elliptic curves, which is affine over $\mathcal{M}_{1,1}$. Then $\mathcal{P}$ is representable if and only if it is rigid.*

Proof. We will describe the main ideas for the proof of this theorem. Details can be found in [KM, Theorem IV.4.7.0]. Because our moduli problem is rigid, it is sufficient to prove the representable results on $\mathbb{Z}[1/2]$ and $\mathbb{Z}[1/3]$ and then glue them over $\mathbb{Z}[1/6]$. We first need the following

Claim. *Let $\mathcal{P}, \mathcal{P}'$ be moduli problems of elliptic curves such that $\mathcal{P}$ is representable and $\mathcal{P}'$ is relative representable then the product $\mathcal{P} \times \mathcal{P}'$ is representable.*

Proof of the claim. Assume that $\mathcal{P}$ is represented by $(E_{\mathcal{P}}, \mathcal{M}(\mathcal{P}))$. Then for all object (E, T) in $\mathcal{M}_{1,1}$, $(\mathcal{P} \times \mathcal{P}')(E/T)$ consits of all pairs (ϕ, ϕ') where $\phi : E/T \to E_{\mathcal{P}}/\mathcal{M}(\mathcal{P})$ is a morphism in $\mathcal{M}_{1,1}$ and $\phi' : E/T \to \mathcal{P}'$ is a morphism of functor. Because $\mathcal{P}'$ is relative representable, we have $\mathcal{P}'(E/T) = \mathcal{P}'_{E_{\mathcal{P}}/\mathcal{M}(\mathcal{P})}(T)$. If we denote $\mathcal{P}'' = \mathcal{P}'_{E_{\mathcal{P}}/\mathcal{M}(\mathcal{P})}$, then ϕ' defines a morphism $T \to \mathcal{P}''$ of functors. Denote $E'' = E_{\mathcal{P}} \times_{\mathcal{M}(\mathcal{P})} \mathcal{P}''$, we then obtain the following commutative diagram

$$\begin{array}{ccccc} E'' \times_{\mathcal{P}''} T & \longrightarrow & E'' & \longrightarrow & E_{\mathcal{P}} \\ \downarrow & & \downarrow & & \downarrow \\ T & \longrightarrow & \mathcal{P}'' & \longrightarrow & \mathcal{M}(\mathcal{P}). \end{array}$$

Because all three squares are cartesian, we obtain $E'' \times_{\mathcal{P}''} T$ is exactly E. We thus obtain a morphism from E/T to $E''/\mathcal{P}''$ in $\mathcal{M}_{1,1}$. Conversely, any morphism from E/T to $E''/\mathcal{P}''$ in $\mathcal{M}_{1,1}$ will give us a morphism from E/T to $E_{\mathcal{P}}/\mathcal{M}(\mathcal{P})$, and also a morphism from E/T to $\mathcal{P}'$ by the diagram above. We can thus conclude that the product $\mathcal{P} \times \mathcal{P}'$ is representable by $E''/\mathcal{P}''$.

We now come back to the proof of the theorem. Assume that our original moduli problem is $\mathcal{P}'$, we need to find a moduli functor $\mathcal{P}$ with the following conditions:

1. $\mathcal{P}$ is representable, finite and affine over $\mathcal{M}_{1,1}$.

2. There is a finite group G, such that for every family of elliptic curves E/T, the scheme $\mathcal{P}_{E/T}$ is a finite etale principal homogeneous space over G.

Then $\mathcal{P}'$ is represented by $(\mathcal{P} \times \mathcal{P}')/G$, and the family of elliptic curve over this base is the descent of E'' (notations as in the proof of the previous claim).

Now, over $\mathbb{Z}[1/2]$, we choose $\mathcal{P}$ as the Legendre family, $G = \mathrm{GL}_2(\mathbb{F}_2) \times \{\pm 1\}$ [KM, II.2.2.9], and over $\mathbb{Z}[1/3]$, we choose $\mathcal{P}$ as the naive level three structure, $G = \mathrm{GL}_2(\mathbb{F}_3)$ [KM, II.2.2.10].

□

So, in particular, for $N \geq 5$, $\Gamma_1(N)$ is representable. We will use this to prove that $\mathcal{M}_{1,1}$ is a Deligne-Mumford stack.

Theorem 3.7.5. *The category $\mathcal{M}_{1,1}$ is a Deligne-Mumford stack over $(\mathrm{Aff}\,/S)_{fppf}$.*

Proof. The fact that $\mathcal{M}_{1,1}$ is a stack follows from a statement: descent of elliptic curves is effective [R, XI.3.1]. To prove the stack $\mathcal{M}_{1,1}$ is Deligne-Mumford, we will prove that

- The diagonal morphism $\Delta : \mathcal{M}_{1,1} \to \mathcal{M}_{1,1} \times_S \mathcal{M}_{1,1}$ is representable by an algebraic space.
- There is an etale surjective morphism $U \to \mathcal{M}_{1,1}$, where U is a scheme.

To prove the first fact, take any T in $(\mathrm{Aff}\,/S)$, any morphism from T to $\mathcal{M}_{1,1} \times \mathcal{M}_{1,1}$ is given by a pair $(E_1, T, f_1, 0)$, $(E_2, T, f_2, 0)$, where $f_1 : E_1 \to T$ and $f_2 : E_2 \to T$ are family of elliptic curves. The fiber product $(\mathcal{M}_{1,1} \times_{\mathcal{M}_{1,1} \times \mathcal{M}_{1,1}} T)$ over some affine scheme B is exacly

$$\left\{ \big((E, B, f, 0), g : B \to T\big), (E, B, f, 0) \cong g^*(E_1, T, f_1, 0) \cong g^*(E_2, T, f_2, 0) \right\}$$

And this is $\mathrm{Isom}(X_1, X_2)(B)$. By [SP, Proposition 98.4.3], the Isom sheaf is representable by an algebraic space. And it follows that the diagonal is representable.

For the second fact, let $(E_N, f, Z, 0)$ be the elliptic curve represents the functor $(E, f, s, 0) \mapsto \{\mathbb{Z}/N\mathbb{Z} - \text{structures on } E/S\}$. Consider the morphism $Z \to \mathcal{M}_{1,1}$ defined by E_N. For any affine scheme B and any morphism $B \to \mathcal{M}_{1,1}$ defined by a family

of elliptic curves E over B, the fiber product $Z \times_{\mathcal{M}_{1,1}} B$ over a scheme T is exactly $\mathrm{Hom}_{\mathcal{M}_{1,1}}(E_T, (E_N)_T) = \{\mathbb{Z}/N\mathbb{Z} - \text{structures on } E_T/T\}$. By Proposition 3.5.9, $Z \times_{\mathcal{M}_{1,1}} B$ is finite, etale over B. Hence, Z is an etale covering of $\mathcal{M}_{1,1}$. □

3.8 Curves of genus one

In this section, we will review the theory of genus one curves. Roughly speaking, a genus one curve is an elliptic curve without a chosen rational point. Throughout the section, we will fix a base field k.

Definition 3.8.1. A *curve of genus one* C over k is a smooth, proper, geometrically integral scheme of dimension one over k such that $H^1(C, \mathcal{O}_C) = 1$.

Due to Riemann-Roch's theorem, a curve of genus one can also be characterized in term of its trivial dualizing sheaf. For a curve of genus zero or at least two, we can easily deduce it is projective by its dualizing sheaf, which is non-trivial. More presicely, if $g_C = 0$, ω_C is of degree -1 and $\omega_C^{\otimes -1}$ defines a very ample invertible sheaf, and if $g_C \geq 2$, $\omega_C^{\otimes 3}$ is very ample. For the case of an elliptic curve with a rational point O, the invertible sheaf $\mathcal{O}_X(3[O])$ is very ample.

Proposition 3.8.2. *Let C be a curve of genus one over k, then C is projective over k.*

Proof. Because C is quasi-compact, there exists a closed point $P \in C$. This closed point defines a Weil divisor of C and it corresponds to an effective Cartier divisor, because C is smooth. The associated invertible sheaf $\mathcal{O}_C(P)$ is of positive degree, and hence, ample. By Riemann-Roch's theorem, for sufficiently large n, $\mathcal{O}_C(P)^{\otimes n}$ is very ample, and it follows that C is projective. □

There is more general result, that stated any proper (not necessarily smooth) curve is projective. We refer to [SP, Lemma 33.42.4]. Examples of genus one curve are mainly from cubic curve: by the genus-degree formula, any smooth, projective curve of degree d in $\mathbb{P}^2_k$ has genus $\frac{(d-1)(d-2)}{2}$.

Example 3.8.3. Let $K = k(x_0, x_1, x_2)$ be the field of rational functions over k of characteristic not 3 in 3 variables. Consider a projective curve $(C) : x_0X^3 + x_1Y^3 + x_2Z^3 = 0$

over K. Due to partial derivatives, the curve is non-singular. Furthermore, it does not have K-rational point, because if it does, then x_0, x_1, x_2 are algebraically dependent over k.

The example above gives us a cubic curve that has no rational points. Constructing such a curve over $\mathbb{Q}$ is difficult. Over a finite field $\mathbb{F}_q$, we will show that a genus one curve C always have $\mathbb{F}_q$-points. Recall the Hasse-Weil's bound [Sil, V.1.1]

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}.$$

If $\#C(\mathbb{F}_q)$ is empty, then $q + 1 \leq 2\sqrt{q}$, which never happens because $q \geq 2$. Hence, a curve of genus one always have rational points over finite field. Next, we will see how to construct a curve of genus one on $\mathbb{P}^3$.

Example 3.8.4. Let $H \subset \mathbb{P}^n$ be a hypersurface of degree d, then the adjunction formula yields

$$\omega_H = (\omega_{\mathbb{P}^n} \otimes \mathcal{O}_{\mathbb{P}^n}(H))|_H = \mathcal{O}_H(-n-1+d)$$

Let $X = H_1 \cap ... \cap H_r \subset \mathbb{P}^n$ be a complete intersection of hypersurface $H_1, ..., H_r$ of degree $d_1, ..., d_r$. Using the adjunction formula inductively, we obtain

$$\omega_X = \mathcal{O}_X(-n-1+d_1+...+d_r)$$

If we want X to be a curve of genus one, we first choose $r = n-1$, and because a genus one curve is characterized by its trivial dualizing sheaf, we can choose $d_1, ..., d_{n-1}$ such that $d_1 + ... + d_{n-1} = n+1$. When $n = 3$, a cubic curve in $\mathbb{P}^3$ can be constructed by the complete intersection of two hypersurface of degree 2. For $n \geq 4$, because $d_i \geq 1$ for all i, there exists exactly two indices i, j such that $d_i = d_j = 2$, and the rest are 1. And hence, we can always reduce to the case of complete intersection of two quadratic surfaces in $\mathbb{P}^3_k$.

Example 3.8.5. We can also construct a curve of genus one as a curve of type (2,2) of $\mathbb{P}^1 \times \mathbb{P}^1$. More precisely, denote $X = \mathbb{P}^1 \times \mathbb{P}^1$ with canonical projections $p_1, p_2 : X \to \mathbb{P}^1$. We denote $\mathcal{O}_X(2,2) = p_1^*\mathcal{O}_{\mathbb{P}^1}(2) \times p_2^*\mathcal{O}_{\mathbb{P}^1}(2)$, and Z the corresponding closed subscheme of X with the canonical embedding $i : Z \to X$.

There is an exact sequence of sheaves on X

$$0 \to \mathcal{O}_X(-Z) \to \mathcal{O}_X \to i_*\mathcal{O}_Z \to 0$$

The long exact sequence yields

$$\begin{array}{l} 0 \longrightarrow H^0(X, \mathcal{O}_X(-Z)) \longrightarrow H^0(X, \mathcal{O}_X) \longrightarrow H^0(X, i_*\mathcal{O}_Z) \xrightarrow{\alpha^0} \\ H^1(X, \mathcal{O}_X(-Z)) \longrightarrow H^1(X, \mathcal{O}_X) \longrightarrow H^1(X, i_*\mathcal{O}_Z) \xrightarrow{\alpha^1} \\ H^2(X, \mathcal{O}_X(-Z)) \longrightarrow H^2(X, \mathcal{O}_X) \longrightarrow H^2(X, i_*\mathcal{O}_Z) \longrightarrow 0 \end{array}$$

Because a closed embedding is an affine morphism, we have $R^q f_*\mathcal{O}_Z = 0$ for all $q > 0$ [H, Exercise 4.1, Chapter III]. And by Lerray's spectral sequence, there exists a spectral sequence E such that $E^2_{p,q} = H^p(X, R^q f_*\mathcal{O}_Z)$ converges to $H^{p+q}(Z, \mathcal{O}_Z)$, we have $H^p(X, f_*\mathcal{O}_Z) \cong H^p(Z, \mathcal{O}_Z)$ for all p. Because X is integral, we have $H^0(X, \mathcal{O}_X) = k$. For any quasi-coherent sheaves $\mathcal{F}, \mathcal{G}$ on $\mathbb{P}^1$, the Kunneth's formula [SP, Lemma 33.29.1] yields

$$H^n(X, p_1^*\mathcal{F} \otimes p_2^*\mathcal{G}) \cong \bigoplus_{p+q=n} H^p(\mathbb{P}^1, \mathcal{F}) \otimes H^q(\mathbb{P}^1, \mathcal{G})$$

When $\mathcal{F} = \mathcal{G} = \mathcal{O}_{\mathbb{P}^1}$, we have $H^1(X, \mathcal{O}_X) = 0$ and $H^2(X, \mathcal{O}_X) = 0$ because for all $i \geq 1$, $H^i(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1})$ vanish. And the long exact sequence above becomes

$$0 \to H^0(X, \mathcal{O}_X(-Z)) \to k \to H^0(Z, \mathcal{O}_Z) \to H^1(X, \mathcal{O}_X(-Z)) \to 0$$

and

$$0 \to H^1(Z, \mathcal{O}_Z) \to H^2(X, \mathcal{O}_X(-Z)) \to 0$$

Riemann-Roch theorem for $\mathbb{P}^1$ yields

$$h^0(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(n)) = \max\{0, n+1\}, \quad h^1(\mathbb{P}^1, \mathcal{O}_{\mathbb{P}^1}(n)) = \max\{0, -n-1\}$$

By Kunneth's formula, we have $\mathcal{O}_X(-Z) = \mathcal{O}_X(-2,-2)$, and therefore, $H^0(X, \mathcal{O}_X(-Z)) = 0, H^1(X, \mathcal{O}_X(-Z)) = 0$ and $h^2(X, \mathcal{O}_X(-Z)) = 1$. This yields by the long exact sequence that $h^0(Z, \mathcal{O}_Z) = 1$ and $h^1(Z, \mathcal{O}_Z) = 1$. This shows that Z is a curve of genus one in $\mathbb{P}^1 \times \mathbb{P}^1$.

3.9 Families of genus one curves

We can also define the relative version of genus one curves. Throughout the section, we will fix a base scheme S.

Definition 3.9.1. A *family of curves of genus one* is a pair (C, f) where C is an algebraic space over S and $f : C \to S$ the structure morphism such that f is proper, flat of finite presentation, and all geometric fibers of f are smooth curves of genus one.

Example 3.9.2. Let $R = k[x_0, x_1]$, where k is a field of characteristic $p \neq 3$. We consider the curve $(C) : x_0X_0^3 + x_1X_1^3 + X_2^3 = 0$ over $\operatorname{Spec} R = \mathbb{A}_k^2$. By taking partial derivatives, we can see that the only singular fiber of (C) is at $(0, 0)$. Hence, (C) is a curve of genus one over $\mathbb{A}_k^2 \setminus \{(0, 0)\}$.

Furthermore, one can also define the stack of genus one curve. We denote $(\mathrm{Aff}\,/S)$ the category of affine schemes over S, and $\mathcal{M}_{1,0}$ a category over $(\mathrm{Aff}\,/S)$. Objects of $\mathcal{M}_{1,0}$ are of the form (C, f, T), where T is an affine scheme, and (C, f) is a family of genus one curve over T. Given two objects (C, f, T) and (C', f', T'), a morphism between is a pair (g, h) where $g : X \to X'$ and $h : S \to S'$ are morphisms of algebraic spaces such that the diagram

$$\begin{array}{ccc} C & \xrightarrow{a} & C' \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f'} \\ S & \xrightarrow{h} & S' \end{array}$$

is Catersian. This is a category with a functor $\mathcal{M}_{1,0} \to (\mathrm{Aff}\,/S)$ sending (C, f, T) to T. We shall prove in the next section that $\mathcal{M}_{1,0}$ is an algebraic stack.

Remark 3.9.3. Given an algebraic space C, if there exists an affine scheme B with a morphism $f : C \to B$ such that (C, f) is a family of curves of genus one over B, then B is unique, up to isomorphism. More precisely, if such B, f exist, because $f : C \to B$ is proper, smooth with integral geometric fibers, we have $f_*\mathcal{O}_C \cong \mathcal{O}_{\operatorname{Spec} B}$ [EGA III, 7.8.6]. And this yields $\Gamma(C, \mathcal{O}_C) \cong \Gamma(B, \mathcal{O}_{\operatorname{Spec} B}) = B$.

3.10 The algebraicity of $\mathcal{M}_{1,0}$

In this section, we will prove $\mathcal{M}_{1,0}$ is a stack over $(\mathrm{Aff}\,/S)_{fppf}$.

Proposition 3.10.1. *The category $\mathcal{M}_{1,0}$ is a stack over $(\mathrm{Aff}/S)_{fppf}$.*

Proof. From the definition of morphisms in $\mathcal{M}_{1,0}$, we can see that it is a category fibered in groupoids over $(\mathrm{Aff}/S)_{fppf}$. We now prove that all descent datum are effective. Let U be a scheme over S, and $\{U_i \to U\}$ an fppf covering. Let $((C_i, f_i), \phi_{ij})$ be a descent datum, i.e. (C_i, f_i) are family of curves of genus one over U_i, and $\phi_{ij} : C_i|_{U_i \times_U U_j} \to C_j|_{U_i \times_U U_j}$ are isomorphisms for all i, j satisfying the cocycle condition. By [SP, Lemma 79.11.3], that says every descent datum for algebraic spaces is effective, we obtain an algebraic space (C, f) over U such that $f_i : C_i \to U_i$ is the restriction of $f : C \to U$ to U_i. By descent of morphisms of algebraic spaces [SP, Chapter 72], f is flat, proper of finite presentation, and all geometric fibers of f are smooth curves of genus one. We therefore see that all descent datum is effective. We will next prove that for any family of genus one curves C_1, C_2 in $\mathcal{M}_{1,0}(U)$, $\mathrm{Hom}(C_1, C_2)$ is a sheaf, but it is clear because for any covering $\{U_i \to U\}$, and any $\phi_i \in \mathrm{Hom}(C_1|_{U_i}, C_2|_{U_j})$ such that ϕ_i and ϕ_j agree on $U_i \times_U U_j$, we can glue to obtain a morphism ϕ from C_1 to C_2. By Proposition 2.5.5, $\mathcal{M}_{1,0}$ is a stack. □

To prove the algebraicity of the stack $\mathcal{M}_{1,0}$, we will prove that

- The diagonal morphism $\Delta : \mathcal{M}_{1,0} \to \mathcal{M}_{1,0} \times_S \mathcal{M}_{1,0}$ is representable by algebraic spaces.
- There is a smooth surjective morphism $U \to \mathcal{M}_{1,0}$, where U is a scheme.

To prove the first fact, take any T in (Aff/S), any morphism from T to $\mathcal{M}_{1,0} \times \mathcal{M}_{1,0}$ is given by a pair (X_1, T, f_1), (X_2, T, f_2), where $f_1 : X_1 \to T$ and $f_2 : X_2 \to T$ are family of curves of genus one. The fiber product

$$(\mathcal{M}_{1,0} \times_{\mathcal{M}_{1,0} \times \mathcal{M}_{1,0}} T)(B) = \{(X, B, f), g : B \to T, (X, B, f) \cong g^*(X_1, T, f_1) \cong g^*(X_2, T, f_2)\}$$

And this is exactly $\mathrm{Isom}(X_1, X_2)(B)$. By [SP, Proposition 97.4.3], the Isom sheaf is representable by an algebraic space. And this yields the diagonal morphism is representable.

For the second fact, it is an easy consequence of the following facts

- The stack $\mathcal{M}_{1,1}$ is a Deligne Mumford stack over $(\mathrm{Aff}/S)_{fppf}$.
- The forgetful functor $\mathcal{M}_{1,1} \to \mathcal{M}_{1,0}$ is representable, surjective and smooth.

The first fact was proved in our earlier section. For the second fact, take any scheme B in (Aff/S) and a morphism from $B \to \mathcal{M}_{1,0}$. By Yoneda's lemma, such a morphism is given by a family of curves C of genus one over B. The fiber product $B \times_{\mathcal{M}_{1,0}} \mathcal{M}_{1,1}$ over some affine scheme T is $\{(E, T, f, \sigma), E \cong C_T\}$. It means over T, C_T is a family of elliptic curve, and this is characterized by a section from $T \to C_T$. This yields the fiber product above over T is exactly $\mathrm{Hom}_T(T, C_T)$, and hence, the product is representable by C. Now, because $C \to B$ is smooth, proper, by definition, the forgetful functor $\mathcal{M}_{1,1} \to \mathcal{M}_{1,0}$ is smooth and proper. By the discussion above, we have

Theorem 3.10.2. *The category $\mathcal{M}_{1,0}$ over $(\mathrm{Aff}/S)_{fppf}$ is an Artin stack.*

We note that $\mathcal{M}_{1,0}$ is not a Deligne-Mumford stack, because over an algebraically closed field k, the automorphism group of a genus one curve is not finite. For details, we refer to [V89, p. 666].

3.11 The Picard group of $\mathcal{M}_{1,0}$

In this section, we will compute the Picard group of $\mathcal{M}_{1,0}$. Mumford [M64] showed that over an algebraically closed field k with characteristic $p \neq 2, 3$, the Picard group of the stack $\mathcal{M}_{1,1}$ is $\mathbb{Z}/12\mathbb{Z}$. Later, Fulton and Olsson [FO10] show that over a base scheme S, where either 2 is invertible on S or S is reduced, then

$$\mathrm{Pic}(\mathcal{M}_{1,1}) \cong \mathbb{Z}/12\mathbb{Z} \times \mathrm{Pic}(\mathbb{A}^1_S)$$

We recall that if $f : C \to S$ is a family of genus one curves, then $R^1 f_* \mathcal{O}_C$ is an invertible sheaf on S [M64, Section 5]. When S is spectrum of a field k, then the global sections of $R^1 f_* \mathcal{O}_C$ is exactly $H^1(C, \mathcal{O}_C)$, which is a vector space of dimension 1 over k. Because higher direct images behaves well under pull back (by flat base change theorem [SP, Lemma 30.5.2]) and composition, this defines an invertible sheaf Λ on $\mathcal{M}_{1,1}$, which is called Hodge bundle. In [FO10], the Hodge bundle is defined to be $f_* \Omega^1_{C/S}$, but by Grothendieck-Serre duality [Hi, Theorem 2.1.1], they are dual of each other. And Fulton and Olsson [FO10] showed that over a base field, Λ is the generator of the group $\mathrm{Pic}(\mathcal{M}_{1,1})$.

Lemma 3.11.1. *The forgetful functor $f : \mathcal{M}_{1,1} \to \mathcal{M}_{1,0}$ is representable, and moreover $f_*\mathcal{O}_{\mathcal{M}_{1,1}} = \mathcal{O}_{\mathcal{M}_{1,0}}$.*

Proof. The first part of the lemma is already proved in the previous section. For the second part, if $f : C \to S$ be a proper, flat morphism with integral geometric fibers, then $f_*\mathcal{O}_C = \mathcal{O}_S$ [EGA III, 7.8.6], and this implies that $f_*\mathcal{O}_{\mathcal{M}_{1,0}} = \mathcal{O}_{\mathcal{M}_{1,1}}$. □

As a corollary, we have $f_*\mathbb{G}_m = \mathbb{G}_m$. The category of abelian sheaves on an algebraic stack is an abelian category with enough injectives. Apply Grothendieck's speactral sequence to the composition of functor $f_* : \mathrm{Ab}(\mathcal{M}_{1,0}) \to \mathrm{Ab}(\mathcal{M}_{1,0})$ and the global section functor $\Gamma : \mathrm{AbSh}(\mathcal{M}_{1,0}) \to \mathrm{Ab}$. Using the five terms exact sequence [Weibel, 5.8.3], we have

$$0 \to \mathrm{Pic}(\mathcal{M}_{1,0}) \to \mathrm{Pic}(\mathcal{M}_{1,1}) \to H^1(\mathcal{M}_{1,0}, R^1 f_*\mathbb{G}_m) \to H^2(\mathcal{M}_{1,0}, \mathbb{G}_m) \to H^2(\mathcal{M}_{1,1}, \mathbb{G}_m)$$

It means the pull back map $f^* : \mathrm{Pic}(\mathcal{M}_{1,0}) \to \mathrm{Pic}(\mathcal{M}_{1,1})$ is injective. According to the definition, f forgets the section, and the invertible sheaf Λ is defined independently from the section, Λ is in the image of f^*. And this yields $\mathrm{Pic}(\mathcal{M}_{1,0}) = \mathbb{Z}/12\mathbb{Z}$.

We conclude this section by the following

Theorem 3.11.2. *Over a field k, the Picard group of $\mathcal{M}_{1,0}$ is $\mathbb{Z}/12\mathbb{Z}$, and it is generated by the class of the Hodge bundle.*

3.12 A geometric description of $\mathcal{M}_{1,0}$

In this section, we give a geometric description of the stack $\mathcal{M}_{1,0}$. We recall that over fields, there are close relations between curves of genus one and elliptic curves. Namely, if C is a curve of genus one over k, then $\mathrm{Pic}^0_{C/k}$ is an elliptic curve E over k, and moreover, C is an E-homogeneous space. This observation holds true in relative settings.

Proposition 3.12.1. *$\mathcal{M}_{1,0}$ is isomorphic to the classifying stack of elliptic curves, i.e. $\mathcal{M}_{1,0} \cong B_{\mathcal{M}_{1,1}}\mathcal{E}$, where $\mathcal{E}$ is the universal elliptic curve over $\mathcal{M}_{1,1}$.*

Proof. Let $g : C \to S$ be any curve of genus 1, we denote $\mathrm{Pic}^1_{C/S}$ the subspace of $\mathrm{Pic}_{C/S}$, such that locally it is given by line bundle of degree 1 on geometric fibers of g. By the proof of Theorem 2.4.2, $C \cong \mathrm{Pic}^1 C/S$. Furthermore, if g has a section, then $C \cong \mathrm{Pic}^0_{C/S}$.

We recall, over a scheme S, objects of $B_{\mathcal{M}_{1,1}}\mathcal{E}$ are pairs (C, E), where E is an elliptic curve over S, and C is an E-torsor. One can build a morphism, over a base scheme S

$$\begin{aligned} \rho : \mathcal{M}_{1,0}(S) &\longrightarrow B_{\mathcal{M}_{1,1}}\mathcal{E}(S) \\ C &\longmapsto (C, \mathrm{Pic}^0_{C/S}) \end{aligned}$$

This morphism is well-defined, since $C \cong \mathrm{Pic}^1_{C/S}$ and Pic^1 is a Pic^0-torsor. Conversely, let E be an elliptic curve over a scheme S, and C is an E-torsor, then C is indeed a curve of genus 1 over S. It is because if we take an fppf covering $C \to S$, then $C \to C \times_S C$ has the diagonal section, and $C \times_S C$ becomes an elliptic curve over C. By descent, properness, smoothness of C/S can be deduced. For any geometric point $\mathrm{Spec}\,\Omega \to S$, C_Ω is an E_Ω-torsor. And this follows by the classical result that C_Ω is a curve of genus 1.

And one can define

$$\begin{aligned} \psi : B_{\mathcal{M}_{1,1}}\mathcal{E} &\longrightarrow \mathcal{M}_{1,0}(S) \\ (C, E) &\longmapsto C \end{aligned}$$

Because $E \cong \mathrm{Pic}^0_{E/S}$ whenever E/S is an elliptic curve, we can easily check that ψ, and ρ are indeed quasi-inverse of each other. And that finishes our proof. □

Chapter 4

Cohomological Descent and Applications

In this chapter, we will recall the construction of cohomology of groups, and also the machinery of cohomology descent and its applications in computing some cohomology groups of certain algebraic stacks.

4.1 Group cohomology

We will recall definitions and constructions of group cohomology in this section. Throughout the section, we will fix a group G.

Definition 4.1.1. A G-module is an abelian group M together with a map $G \times M \to M$ sending (g, m) to gm satisfying

- For all $\sigma, \tau \in G$ and $m \in M$, $\sigma(\tau m) = (\sigma\tau)m$.
- For all $m \in M$, $1_G m = m$.
- For all $m_1, m_2 \in M$ and $\sigma \in G$, $\sigma(m_1 + m_2) = \sigma m_1 + \sigma m_2$.

There are typical examples of G-modules we can look at.

Example 4.1.2. Let k be a field, and K/k a Galois extension with Galois group G. Obviously, $K^\times$ is a G-module.

Example 4.1.3. Let M be an abelian group, then M is indeed an $\mathrm{Aut}(M)$-module, where $\mathrm{Aut}(M)$ is the group of automorphisms of M.

The category of G-modules is an abelian category, and in the first subsection, we will construct the cohomology groups of a G-module via cohain complex. The main goal of the section is to prove that cohomology of groups form universal delta functors.

4.1.1 Cochain description of group cohomology

In this subsection, we will define group cohomology via cochain complex. The main result of this section is to prove that group cohomology form a delta functor, in the sense of Grothendieck [G57]. Throughout this subsection, we will fix a G-module M.

Denote

$$C^i(G,M) \stackrel{\text{def}}{=} \{\varphi : G^i \to M\}$$

the set of all maps from $G^i \to M$, for $i \geq 0$. This set comes with a natural abelian group structure defined by $(\varphi_1+\varphi_2)(\sigma_1,...\sigma_i) = \varphi_1(\sigma_1,...,\sigma_i)+\varphi_2(\sigma_1,...,.\sigma_i)$. Let $\varphi \in C^i(G,M)$, we have the *differential map* $d^i : C^i(G,M) \to C^{i+1}(G,M)$ is defined as

$$(d^i\varphi)(\sigma_1,...,\sigma_{i+1}) = \sigma_1\varphi(\sigma_2,...,\sigma_{i+1})+\sum_{j=1}^{i}(-1)^j\varphi(\sigma_1,...\sigma_j\sigma_{j+1},...,\sigma_{i+1})+(-1)^{i+1}\varphi(\sigma_1,...,\sigma_i)$$

Lemma 4.1.4. *The following diagram*

$$0 \xrightarrow{d^{-1}} C^0(G,M) \xrightarrow{d^0} C^1(G,M) \xrightarrow{d^1} ...$$

is a complex.

Proof. We shall prove that for all $n \geq 0$, $d^{n+1} \circ d^n = 0$. For any $\varphi : G^n \to M$, we define

$$\phi_j(\sigma_1,...,\sigma_{n+1}) \stackrel{\text{def}}{=} \begin{cases} \sigma_1\varphi(\sigma_2,...,\sigma_{n+1}) & j = 0 \\ (-1)^j\varphi(\sigma_1,...,\sigma_j\sigma_{j+1},\sigma_{n+1}) & 1 \leq j \leq n \\ (-1)^{n+1}\varphi(\sigma_1,...,\sigma_n) & j = n+1 \end{cases}$$

Moreover, we can also define

$$\phi_{ji} \stackrel{\text{def}}{=} \begin{cases} \sigma_1\phi_j(\sigma_2,...,\sigma_{n+2}) & i = 0 \\ (-1)^i\phi_j(\sigma_1,...,\sigma_i\sigma_{i+1},...,\sigma_{n+1}) & 1 \leq i \leq n+1 \\ (-1)^{n+2}\phi_j(\sigma_1,...,\sigma_{n+1}) & i = n+2 \end{cases}$$

This then yields

$$(d^{n+1} \circ d^n)(\varphi)(\sigma_1, ..., \sigma_{n+2}) = \sum_{j=0}^{n+1} \sum_{i=0}^{n+2} \phi_{ji}(\sigma_1, ..., \sigma_{n+2})$$

We shall prove that for $0 \leq j \leq n+1, j+1 \leq i \leq n+2$, $\phi_{ji} + \phi_{i-1,j} = 0$. The result will follow if we write down ϕ_{ij} as a $(n+2) \times (n+3)$ matrix and cancel out each pair $(\phi_{ji}, \phi_{i-1,j})$ till $j = n+1, i = n+2$.

Assume first that $1 \leq j \leq n, i > j+1$, then a direct computation shows that

$$\phi_{ji}(\sigma_1, ..., \sigma_{n+2}) = (-1)^{i+j} \varphi(\sigma_1, ..., \sigma_j \sigma_{j+1}, ..., \sigma_i \sigma_{i+1}, ..., \sigma_{n+2})$$

and

$$\phi_{i-1,j} = (-1)^{i+j-1} \varphi(\sigma_1, ..., \sigma_j \sigma_{j+1}, ..., \sigma_i \sigma_{i+1}, ..., \sigma_{n+2})$$

And this yields $g_{ji} + g_{i-1,j} = 0$. The remaining cases follows similarly. □

The previous lemma shows that, for all $i \geq -1$, $\operatorname{Im} d^i \subset \ker d^{i+1}$, and we define

$$H^i(G, M) \stackrel{\text{def}}{=} \ker d^i / \operatorname{Im} d^{i-1} (i \geq 0)$$

And $H^i(G, M)$ is called the *i-th cohomology group of M*. There is an easy observation on H^0.

Lemma 4.1.5. *We have $H^0(G, M) = \{m \in M | \sigma m = m, \forall \sigma \in G\}$.*

Proof. There is a bijection between M and $C^0(G, M)$ defined by $m \mapsto \varphi_m$, where $\varphi_m(1_G) = m$. The differential map $d^0 : C^0(G, M) \to C^1(G, M)$ is defined by $(d^0 \varphi_m)(\sigma) = \sigma \varphi_m(1_G) - \varphi(1_G) = \sigma m - m$. This then follows that $\ker d^0 = H^0(G, M) = \{m \in M | \sigma m = m, \forall \sigma \in G\}$. □

We will next describe the functorial properties of group cohomology in terms of differential maps.

Lemma 4.1.6. *Let $f : M \to N$ be a G-module homomorphism, then the induced map $f^i : C^i(G, M) \to C^i(G, N)$ sending φ to $f \circ \varphi$ satisfying $d^i_N \circ f^i = f^i \circ d^i_M$.*

Proof. Let $\varphi : G^i \to M$ be a map. We have

$$(d^i \circ \alpha^i)(\varphi)(\sigma_1, ..., \sigma_{i+1}) = d^i(\alpha \circ \varphi)(\sigma_1, ..., \sigma_i)$$

$$= \sigma_1(\alpha \circ \varphi)(\sigma_2, ..., \sigma_{i+1}) - \sum_{j=1}^{i} (-1)^j (\alpha \circ \varphi)(\sigma_1, ...\sigma_j\sigma_{j+1}, ..., \sigma_i) + (-1)^{i+1}(\alpha \circ \varphi)(\sigma_1, ..., \sigma_i)$$
$$= \alpha \circ d^i\varphi(\sigma_1, ..., \sigma_i) = (\alpha^{i+1} \circ d^i)(\varphi)(\sigma_1, ..., \sigma_i)$$

□

Lemma 4.1.7. *Assume*

$$0 \to M \xrightarrow{\iota} N \xrightarrow{\pi} P \to 0$$

is an exact sequence of G-modules. Then the induced diagram

$$0 \to C^i(G, M) \xrightarrow{\iota^i} C^i(G, N) \xrightarrow{\pi^i} C^i(G, P) \to 0$$

is also exact.

Proof. It is not difficult to check that the induced map ι^i is injective and π^i is surjective. Moreover, because $\pi \circ \iota = 0$, it follows that $\pi^i \circ \iota^i = 0$, i.e. $\operatorname{Im} \iota^i \subset \ker \pi^i$. Now, let $\varphi : G^i \to N$ be a map such that $\pi \circ \varphi(\sigma_1, ..., \sigma_i) = 0$ for all $(\sigma_1, ..., \sigma_i) \in G^i$. We have $\varphi(\sigma_1, ..., \sigma_i) \in \ker \pi = \operatorname{Im} \iota$. We define a map $\phi : G^i \to M$ such that $\phi(\sigma_1, ..., \sigma_i) = m$ where $m \in M$ satisfying $\varphi(\sigma_1, ..., \sigma_i) = \iota(m)$. The map ϕ is well-defined and this shows that $\ker \pi^i \subset \operatorname{Im} \iota^i$. Hence, the induced sequence is also exact. □

We shall prove that cohomology of groups form delta functors, whose definition will be recalled.

Definition 4.1.8. Let $\mathcal{A}, \mathcal{B}$ be abelian categories. A *delta functor* is a collection of additive functors $T = \{T^i\}_{i \geq 0}$ from $\mathcal{A}$ to $\mathcal{B}$ and for each short exact sequence in $\mathcal{A}$

$$0 \to M \to N \to P \to 0,$$

a family of morphisms $\{\delta^i\}_{i \geq 0}$ such that there is an exact sequence in $\mathcal{B}$

$$... \to T^i(M) \to T^i(N) \to T^i(P) \xrightarrow{\delta^i} T^{i+1}(M) \to T^{i+1}(N) \to T^{i+1}(P) \xrightarrow{\delta^{i+1}} ...$$

Moreover, if there is another exact sequence

$$0 \to M' \to N' \to P' \to 0$$

in $\mathcal{A}$ such that there is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & N & \longrightarrow & P & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' & \longrightarrow & N' & \longrightarrow & P' & \longrightarrow & 0 \end{array}$$

then there exists morphisms in $\mathcal{B}$ making the the following diagram commute

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & T^0(M) & \longrightarrow & T^0(N) & \longrightarrow & T^0(P) & \xrightarrow{\delta^0} & T^1(M) & \longrightarrow & \dots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & T^0(M') & \longrightarrow & T^0(N') & \longrightarrow & T^0(P') & \xrightarrow{\delta^0} & T^1(M') & \longrightarrow & \dots \end{array}$$

The delta functor T is said to be *universal* if for any given delta functor S and any given natural transformation from T^0 to S^0, then for each i, there exists a unique natural transformation from T^i to S^i such that for any short exact sequence

$$0 \to M \to N \to P \to 0$$

in $\mathcal{A}$, the diagram

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & T^0(M) & \longrightarrow & T^0(N) & \longrightarrow & T^0(P) & \xrightarrow{\delta^0_T} & T^1(M) & \longrightarrow & \dots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & S^0(M') & \longrightarrow & S^0(N') & \longrightarrow & S^0(P') & \xrightarrow{\delta^0_S} & T^1(M') & \longrightarrow & \dots \end{array}$$

is commutative.

We are now ready for the main result of this subsection.

Proposition 4.1.9. *Assume $0 \to M \to N \to P$ is an exact sequence of G-modules, then there exists homomorphisms $\delta_i (i \geq 0)$ making the diagram*

$$0 \to H^0(G, M) \to H^0(G, N) \to H^0(G, P) \xrightarrow{\delta^0} H^1(G, M) \to H^1(G, N) \to H^1(G, P) \xrightarrow{\delta^1} \dots$$

exact. Moreover, the construction is natural, in the sense that if we have another exact sequence

$$0 \to M' \to N' \to P' \to 0$$

such that there are morphisms

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \longrightarrow & N & \longrightarrow & P & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & M' & \longrightarrow & N' & \longrightarrow & P' & \longrightarrow & 0 \end{array}$$

then there exists homomorphisms making the diagram

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & H^0(G,M) & \longrightarrow & H^0(G,N) & \longrightarrow & H^0(G,P) & \xrightarrow{\delta^0} & H^1(G,M) & \longrightarrow & \dots \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H^0(G,M') & \longrightarrow & H^0(G,N') & \longrightarrow & H^0(G,P') & \xrightarrow{\delta^0} & H^1(G,M') & \longrightarrow & \dots \end{array}$$

Say another word, cohomology of groups forms delta functors.

Proof. By Lemma 4.1.6 and Lemma 4.1.7, for all $j \geq 0$, there is a commutative diagram diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C^j(G,M) & \longrightarrow & C^j(G,N) & \longrightarrow & C^j(G,P) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & C^{j+1}(G,M) & \longrightarrow & C^{j+1}(G,N) & \longrightarrow & C^{j+1}(G,P) & \longrightarrow & 0 \end{array}$$

where rows are exact. By taking the corresponding sequence of cokernels ($j = i-1$) and kernels ($j = i+1$), we get the following commutative diagram

$$\begin{array}{ccccccccc} & & C^i(G,M)/\operatorname{Im} d_M^i & \longrightarrow & C^i(G,N)/\operatorname{Im} d_N^i & \longrightarrow & C^i(G,P)/\operatorname{Im} d_P^i & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \ker d_M^{i+1} & \longrightarrow & \ker d_N^{i+1} & \longrightarrow & \ker d_P^{i+1} & & \end{array}$$

where rows are exact. Now, by snake lemma, we obtain the following exact sequence

$$H^i(G,M) \to H^i(G,N) \to H^i(G,P) \xrightarrow{\delta^i} H^{i+1}(G,M) \to H^{i+1}(G,N) \to H^{i+1}(G,P).$$

The naturality of this construction is a consequence of Lemma 4.1.6 and the existence of $\{\delta_i\}_{i\geq 0}$. □

4.1.2 Projective resolutions and universal property of cohomology of groups

In this subsection, we will prove that the cohomology of groups defined earlier form the universal delta functors. Firstly, we will see how cohomology of groups can be deduced from a projective resolution of the trivial G-module $\mathbb{Z}$. Using this, we can prove that the higher cohomology of co-induced modules vanish.

Denote P_r the free $\mathbb{Z}$-module generated by tuples $(\sigma_0, ..., \sigma_r)$, where $\sigma_i \in G$. We define a map $d_r : P_r \to P_{r-1}$ by sending $(\sigma_0, ..., \sigma_r) \mapsto \sum_{i=0}^{r}(-1)^i(\sigma_0, ..., \hat{\sigma_i}, ..., \sigma_r)$. And it can be seen that

$$... \xrightarrow{d_{r+1}} P_r \xrightarrow{d_r} P_{r-1} \xrightarrow{d_{r-1}} ... \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} \mathbb{Z} \to 0 \ (*)$$

is a complex of G-modules, where G acts trivially on $\mathbb{Z}$, and G acts diagonally on P_r.

Lemma 4.1.10. *The complex (*) is exact.*

Proof. From the definition, we can see that d_0 is surjective, and this shows $P_0 \xrightarrow{d_0} \mathbb{Z} \to 0$ is exact. Furthermore, it is a routine to check that $d_{r-1} \circ d_r = 0$. Fix $\sigma \in G$, let us define the map $e_r : P_r \to P_{r+1}$ defined by $(\sigma_0, ..., \sigma_r) \mapsto (\sigma, \sigma_0, ..., \sigma_r)$, then it can be seen easily that $d_{r+1}e_r + e_{r-1}d_r = \mathrm{id}_{P_r}$. And so, $\alpha \in \ker d_r$ implies that $d_{r+1} \circ e_r(\alpha) = \alpha$, i.e. $\alpha \in \mathrm{Im}(d_{r+1})$. So, the sequence above is exact. □

A homomorphism of abelian groups $\tilde{\varphi} : P_r \to M$ is in $\mathrm{Hom}_G(P_r, M)$ if and only if $\sigma\tilde{\varphi}(\sigma_0, ..., \sigma_r) = \tilde{\varphi}(\sigma\sigma_0, ..., \sigma\sigma_r)$. And the map induced from $\mathrm{Hom}_G(P_r, M)$ to $\mathrm{Hom}_G(P_{r+1}, M)$ is exactly $d^r\tilde{\varphi} \overset{\text{def}}{=} \tilde{\varphi} \circ d_r$. Explicitly,

$$(d^r\tilde{\varphi})(\sigma_0, ..., \sigma_{r+1}) = (\tilde{\varphi} \circ d_r)(\sigma_0, ..., \sigma_{r+1}) = \sum_{i=0}^{r+1} (-1)^i \tilde{\varphi}(\sigma_0, ..., \hat{\sigma}_i, ..., \sigma_{r+1})$$

We denote

$$\widetilde{C^r}(G, M) \overset{\text{def}}{=} \mathrm{Hom}_G(P_r, M) = \{\tilde{\varphi} : G^{r+1} \to M | \sigma\tilde{\varphi}(\sigma_0, ..., \sigma_r) = \tilde{\varphi}(\sigma\sigma_0, ..., \sigma\sigma_r)\}$$

And the map $\tilde{d^r} : \widetilde{C^r}(G, M) \to \widetilde{C^{r+1}}(G, M)$ is defined to be $\widetilde{\varphi} \mapsto d^r\widetilde{\varphi}$. On the other hand, we will prove that

Lemma 4.1.11. *There is a bijective map ϕ^r between $\widetilde{C^r}(G, M)$ and $C^r(G, M)$ defined by $\varphi(\sigma_1, ..., \sigma_r) \overset{\text{def}}{=} \widetilde{\varphi}(1, \sigma_1, \sigma_1\sigma_2, ..., \sigma_1...\sigma_r)$, for all $\sigma_1, ..., \sigma_r \in G$. Moreover, $d^r \circ \phi^r = \phi^{r+1} \circ \tilde{d^r}$.*

Proof. Assume that $\widetilde{\varphi_1}(1, \sigma_1, ..., \sigma_1...\sigma_r) = \varphi(\sigma_1, ..., \sigma_r) = \widetilde{\varphi_2}(1, \sigma_1, ..., \sigma_1...\sigma_r)$, for all $\sigma_i \in G$, for all $\sigma_i \in G$. If we let $\tau_i \overset{\text{def}}{=} \sigma_{i-1}^{-1}\sigma_i$, then

$$\widetilde{\varphi_1}(\sigma_0, ..., \sigma_r) = \sigma_0\widetilde{\varphi_1}(1, \sigma_0^{-1}\sigma_1, ..., \sigma_0^{-1}\sigma_r) = \sigma_0\widetilde{\varphi_1}(1, \tau_1, ..., \tau_1...\tau_r) =$$

$$= \sigma_0\varphi(\sigma_0^{-1}\sigma_1, \sigma_1^{-1}\sigma_2, ..., \sigma_{r-1}^{-1}\sigma_r) = \sigma_0\widetilde{\varphi_2}(1, \sigma_0^{-1}\sigma_1, ..., \sigma_0^{-1}\sigma_r) = \widetilde{\varphi_2}(\sigma_0, ..., \sigma_r)$$

So we get $\widetilde{\varphi_1} = \widetilde{\varphi_2}$. Now, take any $\varphi : G \to M$, we have to define $\widetilde{\varphi} \in \widetilde{C^r}(G, M)$, such that $\widetilde{\varphi}(1, \sigma_1, ..., \sigma_1...\sigma_r) = \varphi(\sigma_1, ..., \sigma_r)$. We define

$$\widetilde{\varphi}(\sigma_0, ..., \sigma_r) \overset{\text{def}}{=} \sigma_0\widetilde{\varphi}(\sigma_0^{-1}\sigma_1, ..., \sigma_{r-1}^{-1}\sigma_r)$$

And it is easy to check that $\widetilde{\varphi}(1, \sigma_1, \sigma_1\sigma_2, ..., \sigma_1...\sigma_r) = \varphi(\sigma_1, ..., \sigma_r)$. Moreover,

$$\sigma\widetilde{\varphi}(\sigma_0, ..., \sigma_r) = \sigma\sigma_0\widetilde{\varphi}(\sigma_0^{-1}\sigma_1, ..., \sigma_{r-1}^{-1}\sigma_r)$$

And $\widetilde{\varphi}(\sigma\sigma_0, ..., \sigma\sigma_r) = \sigma\sigma_0\varphi(\sigma_0^{-1}\sigma_1, ..., \sigma_{r-1}^{-1}\sigma_r)$. And hence, $\widetilde{\varphi} \in \widetilde{C^{r+1}}(G, M)$. The identity $d^r \circ \phi^r = \phi^{r+1} \circ \tilde{d}^r$ is easy to check. □

We thus get an important

Corollary 4.1.12. *For any G-module M, there are isomorphisms*

$$H^r(\mathrm{Hom}_G(P_\bullet, M)) \cong H^r(G, M)$$

for all $r \geq 0$.

Next, we will define co-induced modules and prove that their higher cohomology vanish.

Definition 4.1.13. Let N be an abelian group, we define $\mathrm{CoInd}(N)$ the set of all maps $\varphi : G \to N$.

We can equip $\mathrm{CoInd}(N)$ a structure of a G-module by defining $(\sigma\varphi)(\tau) \stackrel{\text{def}}{=} \varphi(\tau\sigma)$ and $(\varphi_1 + \varphi_2)(\sigma) \stackrel{\text{def}}{=} \varphi_1(\sigma) + \varphi_2(\sigma)$.

Lemma 4.1.14. *Let M be a G-module and M_0 its underlying abelian group, then there is an embedding from M into $\mathrm{CoInd}(M_0)$.*

Proof. Let $m \in M$, we can define $\varphi_m : G \to M_0$ defined by $\varphi_m(\sigma) \stackrel{\text{def}}{=} \sigma m$ for all $\sigma \in G$. Consider the map $M \to \mathrm{CoInd}(M_0)$ defined by $m \mapsto \varphi_m$. It can be checked easily that this is an injective G-module homomorphism. □

There is also an important property of co-induced modules.

Lemma 4.1.15. *Let M be a G-module and N an abelian group, then there is a canonical isomorphism of groups*

$$\mathrm{Hom}_G(M, \mathrm{CoInd}(N)) \cong \mathrm{Hom}_{\mathbb{Z}}(M_0, N)$$

Proof. Let $\alpha : M_0 \to N$ be a homomorphism of abelian group, we define a map $\beta : M \to \mathrm{CoInd}(N)$ by $\alpha(m)(\sigma) \overset{\text{def}}{=} \beta(\sigma m)$. It is easy to check that β is indeed a homomorphism of G-modules. Conversely, let $\alpha : M \to \mathrm{CoInd}(N)$ be a G-module homomorphism. We can define $\beta : M \to N$ by $\beta(m) \overset{\text{def}}{=} \alpha(m)(1_G)$. □

Remark 4.1.16. The previous lemma says that the forgetful functor from $\mathrm{G\text{-}mod}$ to Ab has a right adjoint $\mathrm{CoInd}(-)$.

Now, if M is a co-induced module, say $M = \mathrm{CoInd}(N)$ for some abelian group N. From the complex

$$0 \to \mathrm{Hom}_G(P_0, M) \to \mathrm{Hom}_G(P_1, M) \to ...$$

we thus get by Lemma 4.1.15 an isomorphism complex

$$0 \to \mathrm{Hom}_{\mathbb{Z}}(P_0, N) \to \mathrm{Hom}_{\mathbb{Z}}(P_1, N) \to ...$$

This yields by Corollary 4.1.12 that $H^r(G, M) \cong H^r(\mathrm{Hom}_{\mathbb{Z}}(P_\bullet, N))$, which is $\mathrm{Ext}^r(\mathbb{Z}, N)$. Because $\mathbb{Z}$ is clearly a free $\mathbb{Z}$-module, the r-th ext-group vanishes for $r \geq 1$. And we hence obtain the following

Theorem 4.1.17. *The cohomology of groups satisfies the conditions of universal delta functors.*

Proof. By Proposition 4.1.8, cohomology of groups form delta functors. By Grothendieck [G57, Proposition 2.2.1], it is sufficient to prove that for any G-module M, there is an embedding M into a G-module N such that $H^i(G, N)$ vanish for all $i \geq 1$. By Lemma 4.1.14, we can choose N to be $\mathrm{CoInd}(M_0)$, where M_0 is the underlying abelian group of M. And it follows by our earlier remarks that $H^i(G, \mathrm{CoInd}(M_0))$ vanish for all $i \geq 1$. □

4.2 Coholomogical descent

Cohomological descent is a standard technique to compute cohomology of an algebraic stack, when we know explicitly its smooth covering. We refer to [O, II.4] or [SP, Chapter 84] for standard references on cohomology descent. The discussion in [BR] is also helpful. During the this and the next section, arrows in spectral sequences of the first page are $(p, q) \to (p + 1, q)$, and arrows in second page are $(p, q) \to (p + 2, q - 1)$.

We recall that a *simplicial object* $X_\bullet$ in a category $\mathcal{C}$ is a functor from $\Delta \to \mathcal{C}$, where Δ is the category of ordered sets of the form $[n] \stackrel{\text{def}}{=} \{0, 1, ..., n\}$ and morphisms are order preserving maps. We can define the notions of sheaves and cohomology on simplicial object $X_\bullet$.

Let X_n be the object of $\mathcal{C}$ defined by the image of $[n]$ in Δ, a *sheaf on* $X_\bullet$ is a collection of sheaves on X_n such that they are compatible with morphisms in Δ. By [SP, Lemma 84.2.9], there is a resolution for the constant sheaf $\mathbb{Z}$ on $X_\bullet$, and this is similar to the projective resolution of $\mathbb{Z}$ we discussed in Section 4.1.2:

$$... \to \mathbb{Z}_{X_2} \to \mathbb{Z}_{X_1} \to \mathbb{Z}_{X_0} \to 0.$$

And by using some results from spectral sequences of double complexes, we obtain the following spectral sequence for any abelian sheaf $\mathcal{F}$ on $X_\bullet$

$$E_1^{p,q} = H^q(X_p, \mathcal{F}|_{X_p}) \Rightarrow H^{p+q}(X_\bullet, \mathcal{F}). \tag{4.1}$$

If we add the object $\{-1\}$ into the category Δ with the unique morphism from $\{-1\}$ to $[n]$, then the image S of $\{-1\}$ into the category $\mathcal{C}$ is called the *augmentation* of $X_\bullet$. In $\mathcal{C}$, there exists a morphism from X_n to S induced from the map of simplicial sets. Let $S_\bullet$ be the constant simplicial object respect to S, then those morphisms from X_n to S induce a morphism $a : X_\bullet \to S_\bullet$. Therefore, there is a natural pullback functor

$$a^* : Sh(S) \to Sh(X_\bullet)$$

and its adjoint a_*. We say that the adjoint pair (a^*, a_*) is a *morphism of cohomological descent* if the natural functor

$$\mathrm{id} \to Ra_* \circ a^*$$

in $D_+(S)$, the derived category of bounded above complexes of abelian sheaves on S, is an isomorphism. If this is the case, then for any abelian sheaf $\mathcal{F}$ on S, we have $H^n(X_\bullet, \mathcal{F}|_X) \cong H^n(S, \mathcal{F})$, and the spectral sequence (4.1) descents to

$$E_1^{p,q} = H^q(X_p, \mathcal{F}|_{X_p}) \Rightarrow H^{p+q}(S, \mathcal{F})$$

There are several conditions for cohomological descent, we refer to [BR] or [O, II.4] for more details. We now come to the main theorem of the section.

Theorem 4.2.1 (O. 2.4.26). *Let $\mathcal{X}$ be an algebraic stack over $(\mathrm{Sch}/S)_{fppf}$, and X a sheaf on $(\mathrm{Sch}/S)_{fppf}$, such that there exists a covering $\pi : X \to \mathcal{X}$. Denote X_n the $(n+1)$-fold product $X \times_{\mathcal{X}} ... \times_{\mathcal{X}} X$, then for any abelian sheaf $\mathcal{F}$ on $\mathcal{X}$, there is a spectral sequence*

$$E_1^{p,q} = H^q(X_p, \mathcal{F}) \Rightarrow H^{p+q}(\mathcal{X}, \mathcal{F})$$

Furthermore, when $\mathcal{X} = [X/G]$ is a quotient stack for some group scheme G over S, then the spectral sequence in the second page satisfies

$$E_2^{p,q} = H^q(G, H^p(X, \mathcal{F})) \Rightarrow H^{p+q}([X/G], \mathcal{F})$$

4.3 Cohomology of BG, G is a constant group scheme

To compute the cohomology of BG, we will use the results of the previous section. Applying Theorem 4.2.1 to the covering $\mathrm{Spec}\, k \to BG$, where G is a constant group scheme over k, $\mathcal{F}$ is a quasi-coherent $\mathcal{O}_{\mathcal{X}}$-module, we obtain

$$E_2^{0,0} = H^0(G, H^0(\mathrm{Spec}\, k, \mathcal{F}|_{\mathrm{Spec}\, k})) = H^0(G, \mathcal{F}|_{\mathrm{Spec}\, k}) \Rightarrow H^0(BG, \mathcal{F})$$

Because $E_2^{0,0} = E_\infty^{0,0}$ is already stable, we obtain that $H^0(G, \mathcal{F}|_{\mathrm{Spec}\, k}) \cong H^0(BG, \mathcal{F})$. Consider two following functors

$$F_1 : \mathcal{O}_{\mathcal{X}}\text{-mod} \longrightarrow \mathrm{Ab} \quad \mathcal{F} \longmapsto H^0(\mathcal{X}, \mathcal{F}),$$

$$F_2 : \mathcal{O}_{\mathcal{X}}\text{-mod} \longrightarrow \mathrm{Ab} \quad \mathcal{F} \longmapsto H^0(G, \mathcal{F}|_{\mathrm{Spec}\, k}),$$

where $\mathcal{O}_X$-mod is the category of quasi-coherent $\mathcal{O}_{\mathcal{X}}$-modules, Ab is the category of abelian groups. The functor F_1 is clearly left exact, and the functor F_2 is the composition of

$$\mathcal{F} \mapsto \mathcal{F}|_{\mathrm{Spec}\, k} \mapsto H^0(\mathrm{Spec}\, k, \mathcal{F}|_{\mathrm{Spec}\, k}) \mapsto (H^0(\mathrm{Spec}\, k, \mathcal{F}_{\mathrm{Spec}\, k}))^G.$$

Moreover $R^0F_1 = R^0F_2$, this yields, by the theory of δ-functor, that their derived functors are the same. Hence, we obtain $H^i(\mathcal{X}, \mathcal{F}) \cong H^i(G, \mathcal{F}|_{\mathrm{Spec}\, k})$ for any quasi-coherent $\mathcal{O}_{\mathcal{X}}$-module $\mathcal{F}$.

4.4 Cohomology of $B\mathbb{G}_a$

We can use the same technique to compute the cohomology of $B\mathbb{G}_a$. Looking at the zeroth row in the first page, we have

$$H^0(\operatorname{Spec} k, \mathbb{G}_m) \to H^0(\mathbb{G}_a, \mathbb{G}_m) \to H^0(\mathbb{G}_a \times \mathbb{G}_a, \mathbb{G}_m) \to \cdots$$

Because $\mathbb{G}_a^{\times p}$ is indeed $\mathbb{A}_k^p$, and $\Gamma(\mathbb{A}_k^p, \mathbb{G}_m) = k^\times$. We then have for p is odd, d^p is an isomorphism, and for p is even, d^p is the zero map.

The first row of the first page is

$$H^1(\operatorname{Spec} k, \mathbb{G}_m) \to H^1(\mathbb{G}_a, \mathbb{G}_m) \to H^1(\mathbb{G}_a \times \mathbb{G}_a, \mathbb{G}_m) \to \cdots$$

We recall that the *Chow group* $CH_i(X)$ of a variety X is defined to be the group of i-dimensional cycles modulo the group of i-th cycles rationally equivalent to zero. And $CH_n(\mathbb{G}_a^p) = 0$ except when $n = p$, and this yields $H^1(\mathbb{G}_a^p, \mathbb{G}_m) = A^1(\mathbb{G}_a^p)$ is trivial. Now, Theorem 4.2.1 again yields $H^2(\operatorname{Spec} k, \mathbb{G}_m) = H^2(B\mathbb{G}_a, \mathbb{G}_m)$.

4.5 Cohomology of BA

In [S19], the author computed the cohomology of classifying stack of an elliptic curve. Using the same method, we obtain the cohomology of the classifying stack of an abelian variety.

Theorem 4.5.1. *Let A be an abelian variety, and BA the classifying stack of A-torsors, then $H^2(BA, \mathbb{G}_m) \cong Br(k) \oplus \operatorname{Pic}^0(A)$, where $\operatorname{Pic}^0(A) \subset \operatorname{Pic}(A)$ is the group of numercally trivial invertible sheaf on A.*

Proof. There is a canonical identification between $\operatorname{Spec} k \times_k A^{\times p}$ and $\operatorname{Spec} k \times_{BA} \ldots \times_{BA} \operatorname{Spec} k$ ($p+1$ times) via

$$(x, a_1, ..., a_p) \mapsto (a_1 ... a_p x, a_1 ... a_{p-1} x, ..., x)$$

Using this, we obtain

$$E_1^{p,0} = H^0(A^{\times p}, \mathbb{G}_m) = \Gamma(A^{\times p}, \mathcal{O}_{A^{\times p}})^\times = k^\times$$

Because there is a section from $\operatorname{Spec} k \to A$, the complex

$$0 \to E_1^{0,0} \to E_1^{1,0} \to \dots$$

is acyclic. And this yields $E_2^{3,0} = 0$.

Next,

$$E_1^{1,1} = H^1(A, \mathbb{G}_m) = \operatorname{Pic}(A), E_1^{2,1} = H^1(A^{\times 2}, \mathbb{G}_m) = \operatorname{Pic}(A \times A)$$

Moreover $E_1^{0,1} = H^1(\operatorname{Spec} k, \mathbb{G}_m) = 0$, by Hilbert theorem 90. The arrows on the first page is as follows

$$E_1^{0,1} \to E_1^{1,1} \to E_1^{2,1}$$

We obtain $E_2^{1,1} = \ker(\operatorname{Pic}(A) \to Pic(A \times A))$. This map is induced from simplicial maps between $A \times A \to A$ via the identification above, and it is $m^* - p_1^* - p_2^*$. By definition, the kernel of this map is $\operatorname{Pic}^0(A)$. Because the arrow on the second page is $E_2^{-1,2} \to E_2^{1,1} \to E_2^{3,0}$ and because $E_2^{3,0} = 0$, we can see that $E_2^{1,1}$ is already stable and it is $\operatorname{Pic}^0(A)$.

Finally, the composition $\operatorname{Spec} k \to BA \to \operatorname{Spec} k$ is the identity. And this yields $H^2(\operatorname{Spec} k, \mathbb{G}_m)$ appears in the direct summand of $H^2(BA, \mathbb{G}_m)$, and the other is $E_2^{1,1} = \operatorname{Pic}^0(E)$. And $E_1^{0,2} = H^2(\operatorname{Spec} k, \mathbb{G}_m) = Br(k)$. □

Bibliography

[A69] M. Artin: *Algebraization of formal moduli I*. In: D. C. Spencer and S. Iyanaga (ed.), Global analysis (Papers in honor of K. Kodaira), 21-71, Univ. Tokyo Press, Tokyo.

[BR] B. Conrad: *Cohomological descent*, available at https://math.stanford.edu/ conrad/papers/hypercover.pdf.

[A74] M. Artin: *Versal deformations and algebraic stacks*. Invent. Math. 27 (1974), 165–189.

[DM69] P. Deligne, D. Mumford: *The irreducibility of the space of curves of given genus.* Inst. Hautes Études Sci. Publ. Math. No. 36 (1969), 75–109.

[FGAE] B. Fantechi, L. Göttsche, L. Illusie, S. Kleiman, N. Nitsure, A. Vistoli: *Fundamental algebraic geometry. Grothendieck's FGA explained*. Mathematical Surveys and Monographs, 123.

[FO10] W. Fulton, M. Olsson: *The Picard group of* $\mathcal{M}_{1,1}$. Algebra Number Theory 4 (2010), 87–104.

[G57] A. Grothendieck: *Sur quelques points d'algèbre homologique,* Tohoku Math. J. (2) 9 (1957), 119–221.

[EGA] A. Grothendieck, J. Dieudonne.: *Elements de Geometrie Algebrique*, Chap. I, II, III, IV, Pub. Math. IHES, 4(I), 8(II), 11, 17 (III), 20, 24, 28, 32 (IV).

[SGA I] A. Grothendieck, M. Raynaud: *Revêtements étales et groupe fondamental.* Lecture Notes in Math., 224, Springer-Verlag, Berlin, 1964.

[H] R. Hartshorne: *Algebraic geometry*, Graduate Texts in Mathematics, Springer-Verlag, Berlin, 1977.

[Hi] H. Hida: *Geometric modular forms and elliptic curves*, World Scientific Publishing Co. Pte. Ltd., Hackensack, 2000.

[KM] N. Katz, B. Mazur: *Arithmetic moduli of elliptic curves.* Annals of Mathematics Studies, 108. Princeton University Press, Princeton, NJ, 1985.

[IR] K. Ireland, M. Rosen: *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, Springer-Verlag, Berlin, 1990.

[LM] G. Laumon, L. Moret-Bailly: *Champs algebriques*, volume 39 of Ergebnisse der Mathematik und ihrerGrenzgebiete (3). A Series of Modern Surveys in Mathematics. Springer-Verlag, Berlin, 2000.

[Mil] J. S. Milne: *Etale Cohomology.* Princeton University Press, Princeton, New Jersey, 1980.

[M64] D. Mumford: *Picard groups of moduli problems*. In: O. Schilling (ed.), Arithmetical algebraic geometry, 33-81, Harper & Row, New York.

[M74] D. Mumford: *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, 5, 1974.

[O] M. Olsson: *Algebraic spaces and stacks.* American Mathematical Society Colloquium Publications, 62.

[R] M. Raynaud: *Faisceaux amples sur les schemas en groupes et les espaces homogenes.*, Lecture Notes in Mathematics 119, Springer-Verlag, 1970.

[S19] M. Shin: *Computations of the cohomological Brauer group of some algebraic stacks.* Dissertation, UC Berkeley, https://escholarship.org/uc/item/0vs1x3g5.

[S21] S. Schroeer: *Algebraic spaces that become schemeatic after ground field extension.* To appear in Math. Nachr.

[Sil] J. H. Silverman: *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, Springer-Verlag, Berlin, 2000.

[SP] Stacks project authors: *Stacks Project*, http://stacks.math.columbia.edu, 2018.

[V89] A. Vistoli: *Intersection theory on algebraic stacks and their moduli spaces*. Invent. Math. 97, 613-670 (1989).