Theory of Elliptic curves over an arbitrary Scheme

A thesis submitted to
Indian Institute of Science Education and Research Pune
in partial fulfillment of the requirements for the
BS-MS Dual Degree Programme

Thesis Supervisor: Dr. Sreekar M Shastry

by
H. Guhan Venkat
April, 2012

Indian Institute of Science Education and Research Pune
Sai Trinity Building, Pashan, Pune India 411021

This is to certify that this thesis entitled ”Theory of Elliptic curves over an arbitrary Scheme” submitted towards the partial fulfillment of the BS-MS dual degree programme at the Indian Institute of Science Education and Research Pune, represents work carried out by H. Guhan Venkat under the supervision of Dr. Sreekar M Shastry.

H. Guhan Venkat

Thesis committee:
Dr. Sreekar M Shastry
Dr. Baskar Balasubramanyam

Professor A. Raghuram
Coordinator of Mathematics

Dedicated to the memory of my father, M. Harikumar (1954-2010)

Acknowledgments

First and foremost, I thank my thesis supervisor Dr. Sreekar M Shastry profusely for the incredible number of hours he spent regularly advising me - from teaching me basic Arithmetic geometry to carefully writing up the minutes of every meeting to proof read several drafts of this thesis.

I also wish to thank the Mathematics group at IISER Pune, specifically Professors A. Raghuram, Rama Mishra, Baskar Balasubramanyam, Anupam Kumar Singh, Soumen Maity, Ayan Mahalanobis, R. Parthasarathi and Pranay Goel, for their tremendous effort in creating a terrific atmosphere which has shaped my still growing interest in Mathematics. I am also greatly indebted to Professors L.S. Shashidhara and Sudarshan Ananth for their encouragement.

This work would not have materialised and I would have been lost mid way if not for the continuous support of Akshaa Vatwani, Sarthak Parikh, Surojit Sural, Manoj Sahu, Jay Shah, Roshni Bano and many others. I owe any success I may achieve in life to my family for the encouragement they provided me in taking up this bold endeavour.

Abstract

Theory of Elliptic curves over an arbitrary Scheme

by H. Guhan Venkat

This thesis presents an exposition of the basic theory of Elliptic curves over an arbitrary Scheme with emphasis on the group scheme structure, the structure of the N-torsion points on the group scheme, various applications of the Rigidity lemma as well as applications of the dual isogeny for elliptic curves over finite fields such as the Riemann hypothesis.

Contents

Chapter 1

Some Algebraic Geometry

In this review chapter, we recall various properties of schemes and of morphisms between them. We will also recall some important results for which we will give explicit references.

1.1 Properties of Schemes

Throughout this chapter, we let $(X, \mathcal{O}_X)$ denote an arbitrary scheme (we will usually suppress $\mathcal{O}_X$ from the notation and write simply X).

Definition 1. *By a sheaf of $\mathcal{O}_X$-modules, we mean a sheaf $\mathcal{F}$ on X such that for every open set $U \subseteq X$, $\mathcal{F}(U)$ has the additional structure of an $\mathcal{O}_X(U)$-module.*

Definition 2. *By an ideal sheaf, we mean a sheaf of $\mathcal{O}_X$-module $\mathcal{I}$, such that for every $U \subseteq X$ open, $\mathcal{I}(U)$ is an ideal in $\mathcal{O}_X(U)$.*

Definition 3. *An open subscheme of a scheme X is a scheme U, with underlying topological space an open subset of X such that its structure sheaf $\mathcal{O}_U$ is the restriction of the structure sheaf $\mathcal{O}_X \mid_U$, i.e. for $U' \subseteq U$ open, $\mathcal{O}_U(U') \cong \mathcal{O}_X(U')$. An open immersion of schemes is a scheme morphism $f : X \to Y$ such that $f(X)$ is isomorphic to an open subscheme of Y.*

Definition 4. *A closed immersion is a scheme morphism $f : Y \to X$ such that topologically, $f(Y)$ is homeomorphic to a closed subset of X and the induced map on the structure sheafs $f^\# : \mathcal{O}_X \to f_*\mathcal{O}_Y$ of sheaves on X is surjective. We can formulate the definition of closed subschemes as equivalence class of closed immersions, i.e.*

immersions $f : Y \to X$ and $f' : Y' \to X$ are equivalent if there is an isomorphism $i : Y' \to Y$ such that $f' = f \circ i$.

We now review how to associate a sheaf of $\mathcal{O}_X$ ideals to a closed subscheme of X.

Remark 1. *Given a closed subscheme Y of X (with closed immersion denoted by $i : Y \to X$), we define its ideal sheaf, denoted $\mathcal{I}_Y$, to be the kernel of the morphism $i^{\#} : \mathcal{O}_X \to i_*\mathcal{O}_Y$.*

Remark 2. *Whenever we say that X is a scheme over S, or X is an S-scheme (denoted by X/S), we mean that X is a scheme with a given morphism $f : X \to S$. S will be called the base scheme.*

Definition 5. *Given two S-schemes, $X \xrightarrow{f} S$ and $Y \xrightarrow{g} S$, we define the fiber product of X and Y over S, denoted by $X \times_S Y$, to be a scheme with morphisms pr_1 and pr_2 which makes the following diagram commutative :*

$$\begin{tikzcd} X \times_S Y \arrow[r, "pr_1"] \arrow[d, "pr_2"] & X \arrow[d, "f"] \\ Y \arrow[r, "g"] & S \end{tikzcd}$$

such that for any other S-scheme Z with morphisms $\phi : Z \to X$ and $\gamma : Z \to Y$ which satisfies the commutative diagram :

$$\begin{tikzcd} Z \arrow[r, "\phi"] \arrow[d, "\gamma"] & X \arrow[d, "f"] \\ Y \arrow[r, "g"] & S \end{tikzcd}$$

there exists a unique morphism $\theta : Z \to X \times_S Y$ such that $\phi = pr_1 \circ \theta$ and $\gamma = pr_2 \circ \theta$.

Yoneda's lemma

Definition 6. *Let $\mathcal{A}$ be a category and let $\mathcal{SETS}$ denote the category of sets. A functor*

$$\mathcal{F} : \mathcal{A} \to \mathcal{SETS}$$

is called representable if there exists an object $X \in \mathcal{A}$ such that for all $Y \in \mathcal{A}$

$$\mathcal{F}(Y) = \mathrm{Mor}_{\mathcal{A}}(Y, X)$$

In this case, we say X represents $\mathcal{F}$.

Definition 7 (Functor of points)**.** *Given $X \in \mathcal{A}$, we associate to X a natural covariant functor $h_X : \mathcal{A} \to \mathcal{SETS}$ given by $h_X(Y) := \mathrm{Mor}_{\mathcal{A}}(Y, X)$. The functor h_X is called the functor of points of X.*

Yoneda's lemma states that the object X is determined uniquely by its functor of points h_X.

Lemma 1. [Yoneda's lemma] *Let $\mathcal{A}$ be a category and let X, Y be two objects in $\mathcal{A}$. Then there is an isomorphism between* $\mathrm{Hom}(X, Y)$ *and* $\mathrm{Hom}(h_X, h_Y)$*.*

Proof. First we show injectivity. Let f and $g \in \mathrm{Hom}(X, Y)$ such that $f_K = g_K$ for all $K \in C$, where $f_K, g_K : h_X(K) \to h_Y(K)$. Now for $K = X$, we get that $f_X = g_X$. But for $\mathrm{Id}_X \in h_X(X)$. Since

$$f_X(Id_X) = f \quad \text{and} \quad g_X(Id_X) = g$$

we get that $f = g$ which shows the injectivity. It now suffices to establish the surjectivity. Let $\phi \in \mathrm{Hom}(h_X, h_Y)$. We need to associate to it a unique morphism $f \in \mathrm{Hom}(X, Y)$. Set $f := \phi_X(Id_X)$. For $K \in C$, let $p \in h_X(K)$. We need to show that $\phi_K(p) = f \circ p$. Now $\phi_K(p) \in h_Y(K)$ is given by the composition

$$K \xrightarrow{p} X \to Y \tag{1.1}$$

Now consider

$$K \xrightarrow{p} X \xrightarrow{Id_X} X \to Y$$

which does not change the image of K as in equation (1.1). But this is the same as $p \circ \phi_X(Id_X)$ which is $p \circ f$. Hence we get that $\phi_K(p) = f \circ p$ which proves the lemma. □

Definition 8. *A group scheme over S is an S-scheme X with a section $e : S \to X$ and S-morphisms $\rho : X \to X$ and $m : X \times_S X \to X$ such that the following set of diagrams*

$$\begin{tikzcd}
G \times_S G \times_S G \arrow[r, "m \times id"] \arrow[d, "id \times m"'] & G \times_S G \arrow[d, "m"'] & G \arrow[r, "(e \circ \pi, id)"] \arrow[d, "(id, e \circ \pi)"] & G \times_S G \arrow[d, "m"'] \\
G \times_S G \arrow[r, "m"] & G & G \times_S G \arrow[r, "m"] & G
\end{tikzcd}$$

$$\begin{tikzcd}
G \arrow[r, "(inv{,}id)"] \arrow[d, "(id{,}inv)"'] & G \times_S G \arrow[d, "m"] \\
G \times_S G \arrow[r, "m"] & G
\end{tikzcd}$$

commute.

Remark 3. *Alternatively, by Yoneda's lemma, a group object in* $\mathrm{SCH}_{/S}$ *is an* S*-group scheme with a morphism* $G \times_S G \to G$ *such that, the induced map on the functor if points*

$$G(T) \times G(T) \to G(T)$$

make $G(T)$ *a group for every* $T \in \mathrm{SCH}_{/S}$*.*

1.2 Properties of Morphisms of Schemes

Definition 9. *A morphism* $f : X \to Y$ *is said to be of locally of finite type if we can find an open affine covering,* $\{V_i = Spec(B_i)\}$ *of* Y *such that for all* i*, we can find an affine open cover of* $f^{-1}(V_i)$ *denoted by* $\{U_{i,j} = Spec(A_{i,j})\}$ *such that each* $A_{i,j}$ *is a finitely generated* B_i*-algebra. Further,* f *is said to be of finite type if for all* i*, the cover* $\{U_{i,j}\}$ *can be chosen to be finite.*

Given a morphism between schemes, $f : X \to Y$, the **diagonal morphism** is the unique morphism $\Delta : X \to X \times_Y X$, such that the projection onto each component of $X \times_Y X$ is the identity map : id : $X \to X$. By the Yoneda's lemma, the diagonal morphism is equivalent to the set theoretic diagonal on the points : $\Delta_T : X(T) \to X(T) \times X(T)$.

Definition 10. *A morphism* $f : X \to Y$ *is separated if the diagonal morphism* $\Delta : X \to X \times_Y X$ *is a closed immersion.*

A morphism $f : X \to Y$ is *universally closed* if it is closed and for all Y-schemes T, the base change morphism : $f_T : X \times_Y T \to T$ is also closed.

Definition 11. *A morphism* $f : X \to Y$ *is proper if it is separated, of finite type and universally closed.*

Unramified, etale and smooth morphisms

Definition 12. *Let R be a ring. An R-module M is defined to be flat if for every injective homomorphism of R-modules : $N \to N'$, the induced R-module homomorphism, $N \otimes_R M \to N' \otimes_R M$ is also injective.*

Definition 13. *A morphism $f : X \to Y$ is said to be flat at $x \in X$ if $\mathcal{O}_{X,x}$ is a flat $\mathcal{O}_{Y,f(x)}$-module. f is **flat** if it is flat at every point of X.*

Definition 14. *A morphism $f : X \to Y$ is said to be unramified at $x \in X$ if the homomorphism of local rings $\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x}$ has the property that $\mathfrak{m}_{f(x)}\mathcal{O}_{X,x} = \mathfrak{m}_x$. Further the morphism is said to be étale at x if it is both unramified and flat at $x \in X$.*

Remark 4. *We say that $f : X \to Y$ is étale (resp. unramified) if it is étale (resp. unramified) at every $x \in X$.*

Definition 15. *A geometric point is a morphism $\mathrm{Spec}(k) \xrightarrow{\bar{x}} X$ such that k is an algebraically closed field.*

Definition 16. *A morphism $f : X \to Y$ is said to be smooth of relative dimension n if it is flat, locally of finite presentation and for every geometric point $\bar{y} \in Y$, the geometric fiber $X_{\bar{y}} := X \times_Y Spec(k(\bar{y}))$ is a smooth n-dimensional variety over $k(\bar{y})$.*

Remark 5. *For Y locally noetherian, $f : X \to Y$ is smooth of relative dimension n at $x \in X$ if and only if there exists a neighbourhood U of x such that*

$$\begin{tikzcd} U \arrow[r, "g"] \arrow[dr] & \mathbb{A}^n_Y \arrow[d] \\ & Y \end{tikzcd}$$

such that g is etale and p is the projection, $\mathbb{A}^n_Y = \mathbb{A}^n_{\mathbf{Z}} \times Y \xrightarrow{p} Y$. f is smooth of relative dimension n if and only if it is smooth of relative dimension n at all $x \in X$.

Definition 17. *An abelian scheme over S of relative dimension g is a proper, smooth, group scheme $\mathcal{A} \to S$ whose geometric fibers are connected and of dimension g.*

1.3 The relative Picard functor and Cartier divisors

The relative Picard functor

Let S be an arbitrary scheme and let us fix a morphism $f : X \to S$. We define the *absolute picard functor*, $\mathrm{Pic_X}$, to be the functor

$$\mathrm{Pic_X} : \mathrm{(Schemes/S)} \to \mathrm{(Abelian\ Groups)}$$

given by $\mathrm{Pic}_X(T) := \mathrm{Pic(X_T)}$, the group of isomorphism classes of invertible sheaves on $X_T := X \times_S T$.

Definition 18. *The relative Picard functor* $\mathrm{Pic_{X/S}}$ *is defined as*

$$\mathrm{Pic_{X/S}}(T) := \mathrm{Pic}(X_T)/\mathrm{Pic}(T).$$

We shall make an assumption that $\mathcal{O}_S \cong f_*\mathcal{O}_X$ and that the morphism $f : X \to S$ has a section. We will show later that this assumption holds in the case of elliptic curves.

Remark 6. *Under the above assumptions, the relative Picard functor is isomorphic to its associated sheaf under certain Grothendieck topologies namely fppf, Zariski and étale. This is beyond the scope of this thesis and we will not treat Grothendieck topologies in detail.*

Definition 19. *The Picard scheme, if it exists, is the scheme representing the relative Picard functor* $\mathrm{Pic_{X/S}(T)} = \mathrm{Pic(X_T)/Pic(T)}$*. We shall denote such a scheme by* $\mathfrak{Pic}_{X/S}$*.*

When such a scheme $\mathfrak{Pic}_{X/S}$ exists, by $\mathfrak{Pic}^0_{X/S}$, we denote the union of the connected components of the identity at all the fibers, i.e.,

$$\mathfrak{Pic}^0_{X/S} := \cup_{s\in S}\mathfrak{Pic}^0_{X_s/k_s}$$

We now state an important result due to Grothendieck about the representability of $\mathrm{Pic}_{X/S}$.

Theorem 1. *When $f : X \to S$ is a smooth projective curve with geometrically connected fibers, $\mathfrak{Pic}_{X/S}$ exists and is separated. Further, $\mathfrak{Pic}^0_{X/S}$ is an abelian scheme.*

Proof. See Theorem 1, p. 210 in [2]. □

Definition 20. *$\mathfrak{Pic}^0_{X/S}$ is called the Jacobian of X over S.*

Cartier Divisors

We follow Section 1, Chapter 1 of [10] closely. Let X be an S-scheme as before.

Definition 21. *A closed subscheme $D \subset X$ is called an effective Cartier divisor if it is S-flat and its ideal sheaf, say $I(D)$ is an invertible $\mathcal{O}_X$-module.*

Remark 7. *Locally on S, say $S = Spec(R)$, we can find an affine open cover $\{U_i\}$ of X with $U_i = Spec(A_i)$, where A_i is an R-algebra. Then, for an effective Cartier divisor $D \subseteq X$, $D \cap U_i$ is cut out by a single equation $f_i = 0$, $f_i \in A_i$ such that it is not a zero divisor and A_i/f_iA_i is a flat R-module. The exact sequence on X*

$$0 \to I(D) \to O_X \to O_D \to 0 \tag{1.2}$$

restricts on each $U_i = \mathrm{Spec}(A_i)$ to the sequence

$$0 \to A_i \xrightarrow{\times f_i} A_i \to A_i/f_iA_i \to 0.$$

Definition 22. *Let $\mathcal{L}$ be an invertible $\mathcal{O}_X$-module and let $U = \mathrm{Spec}(A)$ be an affine open which trivializes $\mathcal{L}$. Let g be a generator of $\mathcal{L} \mid_U$ as an $\mathcal{O}_X \mid_U$-module. Hence for a global section $\ell \in \mathrm{H}^0(X, \mathcal{L})$, we can write $\ell \mid_U = gh$. The scheme of zeroes of ℓ is the closed subscheme obtained by glueing the pieces corresponding to $A \to A/hA$.*

For two effective Cartier divisors D and D' in X/S, we can define their sum, denoted $D + D'$ as the effective Cartier divisor in X/S, locally cut out by the product of the equations which cut out D and D'. Specifically, for $S = Spec(R)$ and on an affine open $\mathrm{Spec}(A)$ of X, if D and D' are cut out by the equations $f = 0$ and $g = 0$ respectively, $(f, g \in A)$ then $D + D'$ is cut out by $fg = 0$.

For an effective Cartier divisor, D in X/S, we can consider its inverse $I^{-1}(D)$, the unique $\mathcal{O}_X$-module such that $I(D) \otimes_{\mathcal{O}_X} I^{-1}(D) \cong \mathcal{O}_X$. Multiplying (1.1) by $I^{-1}(D)$, we have

$$0 \to \mathcal{O}_X \to I^{-1}(D) \to \mathcal{O}_D \otimes_{\mathcal{O}_X} I^{-1}(D) \to 0.$$

Alternatively, for a pair $(\mathcal{L}, \ell)$, where $\mathcal{L}$ is an invertible $\mathcal{O}_X$-module and $\ell \in \mathrm{H}^0(X, \mathcal{L})$, a global section which satisfies the following short exact sequence of $\mathcal{O}_X$-modules

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

with $\mathcal{L}/\mathcal{O}_X$ flat over S. Then the *scheme of zeroes* of the section ℓ of $\mathcal{L}$ can be shown to be an *effective Cartier divisor.* The *Picard group* is the group of effective Cartier divisors, $(\mathcal{L}, \ell)$ under the group operation given by tensor product over $\mathcal{O}_X$ (See 1.1.3, Chapter 2 of [10]).

Definition 23. *A smooth curve is a smooth morphism $f : X \to S$ of relative dimension one with geometrically connected fibers.*

Lemma 2. *For X/S a smooth curve, every section $s \in X(S)$ defines an effective Cartier divisor which we denote by $[s]$.*

Proof. See Lemma 1.2.2 in [10]. □

Definition 24. *Let X/S be a proper smooth curve and D an effective Cartier divisor. Zariski locally on S, the affine ring of D is a locally free R-module of finite rank, for $S = Spec(R)$. We define the degree of D, denoted by deg(D) to be the rank of this R-module. Alternatively, given an effective Cartier divisor as a pair $(\mathcal{L}, \ell)$ satisfying the exact sequence*

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

we define its degree to be the rank of the R-module $\mathrm{H}^0(X, \mathcal{L}/\mathcal{O}_X)$

Lemma 3. *Let C/S be a smooth curve and let $[s]$ an effective Cartier divisor. $[s]$ is proper over S and of degree one if and only if it is the effective Cartier divisor associated to a section $s \in C(S)$. Moreover s is determined uniquely.*

Proof. See Lemma 1.27 of Chapter 1 in [10]. □

Cartier divisors on the Affine line

In this section, we disucss in detail the construction of *effective Cartier divisors* for the Affine line. Let $S := \mathrm{Spec}(R)$ be an affine noetherian scheme (i.e. R is a noetherian ring) and let X be $\mathbb{A}^1_R := \mathrm{Spec}(R[x])$. By definition, the effective Cartier divisors in $\mathbb{A}^1_R$ are the closed subschemes $\mathrm{Spec}(R[x]/(f))$, where (f) is the ideal generated by the element f in $R[x]$, such that $R[x]/(f)$ is a flat R-module. Since R is noetherian, $R[x]/f$ is flat over R if and only if it is locally free and hence f is a monic polynomial.

We see that the sum of two *effective Cartier divisors* in $\mathbb{A}^1_R$, say $D_1 = \mathrm{Spec}(R[x]/f_1)$ and $D_2 = \mathrm{Spec}(R[x]/f_2)$ is given by

$$D_1 + D_2 = \mathrm{Spec}(R[x]/(f_1 f_2))$$

where $(f_1 f_2)$ is the ideal generated by the product of the polynomials f_1 and f_2 in $R[x]$.

Let $s \in \mathbb{A}^1_R(R)$ be a section. Then we know that s is induced by a ring homomorphism (which we continue to denote by s) $s : R[x] \to R$ such that

$$R \hookrightarrow R[x] \xrightarrow{s} R \tag{1.3}$$

where $R \hookrightarrow R[x]$ is the usual injection, is the identity on R. Since, s is uniquely determined by the image of x, the set of sections, $\mathbb{A}^1_R(R)$ correspond to the ideals of the form $(x - a)$ for all $a \in R$. Moreover, $R[x]/(x - a)$ is a flat R-module, since it is isomorphic to R. This verifies Lemma 2.

Let $f \in R[x]$ be a polynomial of degree d and let D be the Cartier divisor associated to f, i.e $D = \mathrm{Spec}(R[x]/f)$. Dy definition, the degree of D, $\deg(D)$, is the rank of the module R-module $R[x]/f$ which is the degree of the polynomial f. Thus we get that

$$\deg(D) = \deg(f) = d$$

When D is of degree one, we know that for $D = \mathrm{Spec}(R[x]/f)$, degree of f is one and hence $f = x - a$ for some $a \in R$. The ring homomorphism $R[x] \xrightarrow{s} R$ given by $x \mapsto a$ gives rise to a morphism on the schemes $\mathrm{Spec}(R) \to \mathbb{A}^1_R$ and hence a section $s \in \mathbb{A}^1_R(R)$. Conversely, by above, every section corresponds to an effective Cartier divisor, D of degree one. This verifies Lemma 3.

Chapter 2

The Group structure

Definition 25. *Let S be an arbitrary scheme. An elliptic curve over S is a proper smooth curve with geometrically connected fibres of genus one with a given (identity) section $e : S \to E$.*

For a section $P \in E(S)$, we denote by $I(P)$ the ideal sheaf of P as an effective Cartier divisor of degree one and by $I^{-1}(P)$ its inverse ideal sheaf (i.e. $I(P) \otimes_{\mathcal{O}_E} I^{-1}(P) \cong \mathcal{O}_E$).

2.1 Cohomology and Base Change

We follow Mumford's Abelian Varieties [16] as well as Brian Osserman's notes [18] in the subject for this section.

Let us assume that we have a morphism $f : X \to S$ and a quasi-coherent $\mathcal{O}_X$-module $\mathcal{F}$ which is $\mathcal{O}_S$ flat. Consider the following commutative diagram,

$$\begin{tikzcd}
X' \arrow[r, "q"] \arrow[d, "f'"] & X \arrow[d, "f"] \\
S' \arrow[r, "p"] & S
\end{tikzcd}$$

where S' is an S-scheme and X' is the base change $X \times_S S'$. Denote by $\mathcal{F}' = q^*\mathcal{F}$ which is $\mathcal{O}'_S$ flat. We say that *cohomology and base change commute for* $\mathcal{F}$ in degree i when $p^*(\mathrm{R}^i f_*\mathcal{F}) \cong \mathrm{R}^i f'_*(\mathcal{F}')$

Theorem 2. *Let $f : X \to S$ be a proper morphism with S locally Noetherian and let $\mathcal{F}$ be a coherent $\mathcal{O}_X$-module which is $\mathcal{O}_S$-flat. The following are equivalent*

(a) Cohomology and base change commute for $\mathcal{F}$ in degree i
(b) Cohomology commutes with base change for every $s \in S$ for $\mathcal{F}$ in degree i.
(c) The canonical map $\mathrm{R}^i f_*(\mathcal{F}) \to \mathrm{H}^i(X_s, \mathcal{F}_s)$ is surjective.

Proof. See Theorem 1.2 in [18]. □

Theorem 3. *Let $f : X \to S$ be a proper morphism of Noetherian schemes with $\mathcal{F}$ a coherent $\mathcal{O}_X$-module flat over S. Further assume that S is reduced and connected. Then the following are equivalent :*
(i) $s \to \dim_{k(s)} \mathrm{H}^i(X_s, \mathcal{F}_s)$ is a constant function.
(ii) $\mathrm{R}^i f_*(\mathcal{F})$ is a locally free sheaf $\mathcal{E}$ on S such that for all $s \in S$, the natural map

$$\mathcal{E} \otimes_{\mathcal{O}_S} k(s) \to \mathrm{H}^i(X_s, \mathcal{F}_s)$$

is an isomorphism. Further, when these conditions are satisfied, we also have for all $s \in S$ that

$$\mathrm{R}^{i-1} f_*(\mathcal{F}) \otimes_{\mathcal{O}_s} k(s) \to \mathrm{H}^{i-1}(X_s, \mathcal{F}_s)$$

is an isomorphism.

Proof. See Corollary 2, Section II.5 of [16]. □

Lemma 4. *If S is reduced and $\mathcal{F}$ is a coherent sheaf of $\mathcal{O}_Y$-module such that $\dim_{k(y)}[\mathcal{F} \otimes_{\mathcal{O}_Y} k(y)] = r$ for all $y \in Y$, then $\mathcal{F}$ is locally free of rank r on Y.*

Proof. See Lemma 1, Section II.5 of [16]. □

Theorem 4. *Let $f : X \to S$ and $\mathcal{F}$ be as above except that S need not be reduced. If there exists some integer i such that $\mathrm{H}^i(X_s, \mathcal{F}_s)$ vanishes, then for all $s \in S$, the natural map*

$$\mathrm{R}^{i-1} f_*(\mathcal{F}) \otimes_{\mathcal{O}_S} k(s) \to \mathrm{H}^{i-1}(X_s, \mathcal{F}_s)$$

is an isomorphism.

Proof. See Corollary 3, Setion II.5 of [16]. □

Corollary 1. *Let $f : E \to S$ be an elliptic curve. Further let us assume that the base S is reduced and connected. Then the map*

$$\mathcal{O}_S \to f_* \mathcal{O}_E$$

is an isomorphism.

Proof. Since E is an elliptic curve, we have $\mathrm{H}^0(E_s, \mathcal{O}_{E_s}) = k(s)$. Hence, by Theorem 3 above, $f_*\mathcal{O}_E$ is a locally free sheaf on S and $\bar{\phi} : f_*\mathcal{O}_E \otimes_{\mathcal{O}_S} k(s) \to \mathrm{H}^0(E_s, \mathcal{O}_{E_s}) = k(s)$ is an isomorphism. By Nakayama's lemma

Lemma 5. [Nakayama] *Let R be a local ring with unique maximal ideal $\mathfrak{m}$ and let M be a finitely generated module over R. Then, a basis for the vector space $M/\mathfrak{m}M$ lifts to a minimal set of generators of M.*

we can lift the basis element $\bar{\phi}(e)$ of $f_*\mathcal{O}_E \otimes_{\mathcal{O}_S} k(s)$, for $e \in k(s)$ a fixed basis of $k(s)$ (from the isomorphism $\bar{\phi}$) to a generator $\phi(e)$ for $f_*\mathcal{O}_E$ as an $\mathcal{O}_S$-module. Then the natural $\mathcal{O}_S$-module homomorphism

$$\mathcal{O}_S \to f_*\mathcal{O}_E$$

sending 1 to $\phi(e)$ is an isomorphism. □

2.2 Group Law

Due to lack of suitable reference, we shall assume that the base scheme S, is reduced.

Theorem 5 (Abel)**.** *There exists a unique structure of commutative group-scheme on E/S for S reduced such that for any S-scheme T and any three points $P, Q, R \in E(T) = E_T(T)$; we have*

$$P + Q = R$$

if and only if there exists an invertible sheaf $\mathcal{L}_0$ on T and an isomorphism of invertible sheaves on E_T

$$I^{-1}(P) \otimes I^{-1}(Q) \otimes I(0) \cong I^{-1}(R) \otimes f_T^*(\mathcal{L}_0)$$

where $f : E \to S$ is the structure map and $f_T : E_T \to T$ is the base change to T.

Proof. We transport the group-scheme structure (note that it is enough to give a group structure on the functor of points $E(T)$ for all S-schemes T) to E from the identity component, Pic^0, of the *relative Picard functor*.

We show this via several steps. Let $\mathrm{Pic}^1(E_T/T)$ denote the set of equivalence classes of invertible sheaves $\mathcal{L}$ on E_T which are fiber by fiber of degree one where the equivalence relation is given by

$$\mathcal{L} \sim \mathcal{L} \otimes f_T^*(\mathcal{L}_0)$$

for some invertible sheaf $\mathcal{L}_0$ on T. Now consider the map on the points

$$E(T) \to \mathrm{Pic}^1(E_T/T) \tag{2.1}$$

given by

$$P \mapsto \text{the class of } \ I^{-1}(P)$$

If we show that this map is bijective , then for $P, Q \in E(T)$, the invertible sheaf on E_T given by

$$I^{-1}(P) \otimes I^{-1}(Q) \otimes I(0)$$

which is fiber-by-fiber of degree one, is isomorphic to

$$I^{-1}(R) \otimes f_T^*(\mathcal{L}_0)$$

for some unique $R \in E(T)$. Therefore if the group law exists, it is unique. We now further compose the above map with the bijection

$$\mathrm{Pic}^1(E_T/T) \to \mathrm{Pic}^0(E_T/T)$$

given by the map

$$\mathcal{L} \mapsto \mathcal{L} \otimes I(0)$$

Thus if we show that the map in (1) is bijective, we can transport the group law from Pic^0 (given by the tensor product of Cartier divisors) onto $E(T)$ via the established bijections to get a group structure on $E(T)$. Replacing E/S by E_T/T, it is enough to consider the case $T = S$. We now show that it suffices to establish 2.1 Zariski locally on S, i.e. if we are given invertible sheaves $\mathcal{L}$ and $\mathcal{L}'$ on E and an affine open covering $U_i = \mathrm{Spec}(R_i)$ on S, invertible sheaves $\mathcal{L}_{0,i}$ on U_i and isomorphisms

$$\phi_i : \mathcal{L} \to \mathcal{L}' \otimes f^*(\mathcal{L}_{0,i})$$

on $f^{-1}(U_i)$, then there exists an $\mathcal{L}_0$ on S and an isomorphism

$$\phi : \mathcal{L} \cong \mathcal{L}' \otimes f^*(\mathcal{L}_0)$$

By Corollary 1 above, we have

$$f_*(\mathcal{O}_E) \cong \mathcal{O}_S$$

Since $f^*\mathcal{L}_{0,i}$ is a locally free sheaf on $\mathcal{O}_E$, we get that

$$f_*f^*\mathcal{L}_{0,i} \cong \mathcal{L}_{0,i}$$

Consider the locally invertible sheaves on $\mathcal{O}_S$

$$f_*(\mathcal{L}^{-1} \otimes \mathcal{L}'), \qquad f_*(\mathcal{L} \otimes (\mathcal{L}')^{-1}) \tag{2.2}$$

From the isomorphism ϕ_i, we get the two sets of equations

$$\begin{array}{rccc} & \mathcal{L} & \cong & \mathcal{L}' \otimes f^*(\mathcal{L}_{0,i}) \\ \Longrightarrow & f^*(\mathcal{L}_{0,i}^{-1}) & \cong & \mathcal{L}^{-1} \otimes \mathcal{L}' \\ \Longrightarrow & f_*f^*\mathcal{L}_{0,i}^{-1} & \cong & f_*(\mathcal{L}^{-1} \otimes \mathcal{L}') \\ & \mathcal{L}_{0,i}^{-1} & \cong & f_*(\mathcal{L}^{-1} \otimes \mathcal{L}') \end{array}$$

$$\begin{array}{rccc} & \mathcal{L} & \cong & \mathcal{L}' \otimes f^*(\mathcal{L}_{0,i}) \\ \Longrightarrow & \mathcal{L} \otimes \mathcal{L}'^{-1} & \cong & f_*\mathcal{L}_{0,i} \\ \Longrightarrow & f_*(\mathcal{L} \otimes \mathcal{L}'^{-1}) & \cong & f_*f^*(\mathcal{L}_{0,i}) \\ & f_*(\mathcal{L} \otimes \mathcal{L}'^{-1}) & \cong & \mathcal{L}_{0,i} \end{array}$$

Thus the two invertible sheaves defined in 2.2 are inverses to each other. Let us denote the second one $\mathcal{L}_0$, and write

$$\mathcal{L}'' = \mathcal{L}' \otimes f^*(\mathcal{L}_0)$$

we find isomorphisms $f_*(\mathcal{L}^{-1} \otimes \mathcal{L}'') \cong \mathcal{O}_S \cong f_*(\mathcal{L} \otimes (\mathcal{L}'')^{-1})$ under the unit section $1 \in \Gamma(S, \mathcal{O}_S) = \Gamma(S, f_*\mathcal{O}_E) = \Gamma(E, \mathcal{O}_E)$ is the required isomorphism

$$\mathcal{L} \cong \mathcal{L}''.$$

Thus we can reduce to the case when $S = \operatorname{Spec}(R)$ is affine. We now state a result from EGA IV (translated) which will enable us to further reduce to the case that R is noetherian.

Theorem 6. *Let A be a ring, X an A-scheme.*
(i) The following conditions are equivalent :
a) X is finitely presented over A.

b) There is a noetherian ring A_0, a scheme X_0 of finite type over A_0, a ring homomorphism $A_0 \to A$, and an A-isomorphism $X_0 \otimes_{A_0} A \cong X$.

Proof. This is Proposition 8.9.1 of EGA IV. □

We now construct the inverse map under this reduction to establish the bijection.

Lemma 6. *Let $\mathcal{L}$ be an invertible sheaf on E, fiber-by-fiber of degree one. Then $f_*\mathcal{L}$ is an invertible sheaf on S compatible with arbitrary change of base.*

Proof. Note that by Riemann-Roch theorem and Serre Duality, the zeroth and first cohomology groups of the fibers are $\mathrm{H}^0(E_s, \mathcal{L}_s) = k(s)$ and $\mathrm{H}^1(E_s, \mathcal{L}_s) = 0$ for all $s \in S$. Hence, by Theorem 4 above, we have $\mathrm{R}^0 f_*\mathcal{L} \otimes k(s) \cong \mathrm{H}^0(E_s, \mathcal{L}_s) = k(s)$ which shows that $f_*\mathcal{L}$ is a locally free sheaf on S. □

Now since $f_*\mathcal{L}$ is invertible on S, Zariski locally on S, we choose an $\mathcal{O}_S$ basis l of $f_*\mathcal{L}$.

Lemma 7. *Locally over S, the pair $(\mathcal{L}, l)$ on E defines an effective Cartier divisor in E.*

Proof. It suffices to show that

$$0 \to \mathcal{O}_E \xrightarrow{l} \mathcal{L} \to \mathcal{L}/\mathcal{O}_E \to 0 \tag{2.3}$$

is an exact sequence with $\mathcal{L}/\mathcal{O}_E$ flat over $\mathcal{O}_S$. Define $\mathcal{G} := \mathcal{L}/\mathcal{O}_E$. Since $S = \mathrm{Spec}(R)$ where R is a noetherian ring, it is enough to show that $\mathcal{G}$ is locally free over S. Since by assumption $\mathcal{L}$ is fiber-by-fiber of degree one, by definition we have

$$\dim_{k(s)} \mathrm{H}^0(E_s, \mathcal{G} \otimes k(s)) = 1$$

By Lemma 4 above, $\mathcal{G}$ is locally free of rank one over $\mathcal{O}_S$ and hence in particular flat. Therefore, the pair $(\mathcal{L}, \ell)$ is an effective Cartier divisor on E/S. □

Further since $\mathcal{L}$ is fiber-by-fiber of degree one it is of the form $I(P)$ for $P \in E(S)$, a unique section. Hence the map $\mathrm{Pic}^1(E/S) \to E(S)$ given by $\mathcal{L} \mapsto$ *the scheme cut out by a local on S, $\mathcal{O}_S$ basis of $f_*\mathcal{L}$* is a bijection and in particular inverse to the map defined in (1). Thus we get a *group scheme* structure on E/S by giving a group structure on its functor of points via the *relative Picard functor.* □

Chapter 3

The structure of $E[N]$

Theorem 7. *Let S be an arbitrary scheme, E/S an elliptic curve and $N \geq 1$ an integer. Then the S-homomorphism "multiplication by N"*

$$[N] : E \to E$$

is finite locally free of rank N^2. Further, if N is invertible on S (i.e. $1/N \in \mathcal{O}_S(U)$ for all $U \subseteq S$ open), its group scheme theoretic kernel $E[N]$ is finite etale over S.

Proof. When $S = \mathrm{Spec}(\mathbb{C})$, then E is a torus of the form $\mathbb{C}/L$ for a lattice $L \subset \mathbb{C}$ and say $L = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ with $\mathrm{Im}(\omega_1/\omega_2) > 0$. Then $E[N] \cong L/N$ which is a free $\mathbb{Z}/N\mathbb{Z}$ module of rank two with basis $\omega_1/N, \omega_2/N$.

By section 2.2, Chapter 2 in [10], Zariski locally on S, we know that E is given by a smooth Weierstrass cubic in $\mathbb{P}^2_S := \mathbb{P}^2_{\mathbb{Z}} \times_{\mathrm{Spec}(\mathbb{Z})} S$ with origin $(0,0,1)$ and conversely any smooth Weierstrass cubic in $\mathbb{P}^2_S$ is an elliptic curve over S with origin $(0,0,1)$. Hence by reducing to the universal case, we can assume that S is the open set in $\mathrm{Spec}(\mathbb{Z}[a_1,a_2,a_3,a_4,a_6])$ over which the cubic

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

is smooth. Now S is regular and $E \to S$ is smooth. Hence by

Theorem 8. *Let Y be a regular locally Noetherian scheme and let $f : X \to Y$ be a smooth morphism. Then X is also regular.*

Proof. See Theorem 3.36, pp. 142-143 of [13]. □

we conclude that E itself is regular. We now show that $[N] : E \to E$ is finite and flat.

Lemma 8. *Let $A \to B$ be a quasi-finite local homomorphism of regular local rings of the same dimension. Then B is flat over A.*

Proof. See Corollary 3.6, p.95 in [1]. □

Since every finite morphism between schemes is automatically quasi-finite (this is Remark (2.2), Chapter VI, p. 110 of [1]) and since E is regular, by the above lemma, we are reduced to showing that $[N] : E \to E$ is a finite morphism. Now consider the commutative diagram

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

Denote by $g_i : E \to S$ the structure morphism of the i$^{\text{th}}$ copy of E. Then $g_1 = [N] \circ g_2$ is proper and g_2 is also proper and hence by

Lemma 9. *If $f : X \to Y$ and $g : Y \to Z$ are two morphisms anf if $g \circ f$ is proper and g is separated, then f is proper.*

Proof. This is Corollary 4.8(e), pp. 102-103 of [7] □

Since every proper morphism is separated, we get that $E \xrightarrow{[N]} E$ is itself proper. Hence by the following theorem

Theorem 9. *Let $f : X \to Y$ be a proper morphism with finite fibers. Then f is a finite morphism*

Proof. See Exercise 4.6 of Section 4, Chapter II, p. 106 of [7]. □

Hence it suffices to show that the morphism $[N]$ has finite fibers. Further by

Lemma 10. *Let $f : X \to Y$ be a morphism of S-schemes of finite presentation. Then f verifies one of the following conditions: flat, smooth, etale, an open immersion, isomorphism, flat and local complete intersection if only if for every geometric point $\bar{s}$ in S, the corresponding map on the fibers $f_{\bar{s}} : X_{\bar{s}} \to Y_{\bar{s}}$ verifies the said condition.*

Proof. See (7.4) in [5], pp. 170-171. □

it suffices to show this over geometric fibers of S.

Proposition 1. *Let X be a proper regular curve over Spec(k) for k an algebraically closed field and let $f : X \to Y$ be a morphism over Spec(k). Then either (1) $f(X) =$ a point (i.e f is constant) or (2) $k(X)$ is a finite extension of $k(Y)$ and f is a finite morphism.*

Proof. See Proposition 6.8, Chapter II, p. 137 of [7] □

Thus $[N]$ is either finite flat or it is a constant.

Lemma 11. *If char$(k) \nmid N$, then $[N]$ is an etale morphism*

Proof. To show that the morphism is etale, it suffices to show that the tangent map of $[N]$ at the origin is an isomorphism (See [19]). Since we consider $E/\mathrm{Spec}(k)$ we can consider the tangent space via points in the dual numbers i.e., for $k[\epsilon] = k[x]/(x^2)$ we have a natural map $\mathrm{Spec}(k) \to \mathrm{Spec}(k[\epsilon])$ via the ring homomorphism sending $\epsilon \mapsto 0$. Thus we get a map $E(k[\epsilon]) \to E(k)$. We then have

$$\mathcal{T}_E(0) = \{Q \in E(k[\epsilon]) \mid Q \mapsto 0\}$$

Thus $[N] : E \to E$ induces a homomorphism $\mathcal{T}_E(0) \to \mathcal{T}_E(0)$. Clearly the map on the tangent spaces is again given by the multiplication by N homomorphism since $[N]$ is a homomorphism of group schemes (hence a group homomorphism $E(T) \xrightarrow{[N]} E(T)$ for all S-schemes T). This proves the lemma if $\mathrm{char}(k) \nmid N$. □

Over $S[1/N]$, $[N]$ is finite flat and fiber-by-fiber etale (hence in particular unramified). But note that for $y = [N](x)$ where $y, x \in E$, the quotient $\mathcal{O}_{E,x}/m_y\mathcal{O}_{E,x}$ remains unaltered when we pass from E to the fiber E_y and hence this shows that $[N]$ is finite flat and unramified or in other words *finite etale*. We still have to show in the general case that $[N]$ is always finite flat. We thus have to show that on an elliptic curve E/k for k an algebraically closed field, $[N]$ is not a constant map. Now for any integer M prime to N and char(k), $E(k)$ has M^2 points of order M. Since $(N, M) = 1$, the restriction of $[N]$, which is multiplication by N, to $E(k)[M]$ - the M-torsion points, is a non trivial automorphism and hence $[N]$ is non-constant and hence finite flat. Because S is noetherian, finiteness along with flatness implies locally free. Since S is a noetherian connected base scheme, the degree of $[N]$ is the same as that over the fiber of any geometric point of S by

Proposition 2. *Let $f : E' \to E$ be a homomorphism between elliptic curves over a scheme S. For any integer $d \geq 0$, the locus of $s \in S$ such that $\deg(f_{\bar{s}}) = d$ for a geometric point $\bar{s}$ over s is open and closed. If $\deg(f_{\bar{s}}) = d$ for all $\bar{s}$, then f is finite locally free of degree d when $d > 0$ and $f = 0$ when $d = 0$.*

Proof. See Proposition 1.1 of [4] for instance. □

Taking any $\mathbb{C}$-valued point, we immediately get that $[N]$ has degree N^2. □

Chapter 4

Rigidity and Isogenies

4.1 Rigidity

Theorem 10. [Rigidity] *Let X, Y and Z be reduced irreducible schemes over $S = Spec(k)$ for k any field. Suppose that X is proper over S. Let $f : X \times_S Y \to Z$ be a morphism with $f(X \times y_0) = z_0$ for two closed points $y_0 \in Y$ and $z_0 \in Z$. Then there exists a morphism $g : Y \to Z$ such that $f = g \circ p$ for the projection $p : X \times_S Y \to Y$.*

Proof. See Section 4, pp. 43-44 of [16]. □

Corollary 2. *Let S be an arbitrary scheme and let E_1 and E_2 be elliptic curves over S. Then any S-morphism $f : E_1 \to E_2$ such that $f(0) = 0$ is a homomorphism.*

Proof. We first establish the Corollary on every fiber. Hence, let $S = \mathrm{Spec}(k)$ for k a field. We apply Rigidity to the morphism

$$F : E_1 \times_S E_1 \to E_2, \tag{4.1}$$

given by

$$F = f \circ m_{E_1} - m_{E_2} \circ (f, f), \tag{4.2}$$

where m_E denotes the usual addition law on the elliptic curve E. In other words, F on the points is given by $F(x, y) = f(x +_{E_1} y) - (f(y) +_{E_2} f(x))$. Now since $F(E_1 \times \{0\}) = 0_{E_2}$, by Rigidity, there exists $g : E_1 \to E_2$ such that $f = g \circ p_2$ where $p_2 : E_1 \times_S E_1 \to E_1$ is the projection onto the second factor. We get

$$F(x, y) = F(0, y) = g \circ p(y)$$

for all $x, y \in E_1 \times_S E_1$. But, also $F(\{0\} \times y) = f(0 + y) - f(0) - f(y) = 0$ for all $y \in E_1$. Hence fiber-by-fiber, F is the zero morphism. This completes the proof that over an arbitrary base scheme S, $f : E_1 \to E_2$ is a group-scheme homomorphism. □

Corollary 3. *The structure of the S-group-scheme on E/S given by Abel's Theorem is the unique such structure for which "$0''$ is the identity element.*

Proof. Assume that there exists a different group structure given by

$$m'_{E_1} : E_1 \times_S E_1 \to E_1$$

Apply Corollary 3 with $E_2 = E_1$, $m_{E_2} = m'_{E_1}$ and $f = \mathrm{id}_{E_1}$. Then we get

$$m_{E_1}(x, y) - m'_{E_2}(x, y) = 0$$

□

Definition 26. *Let X, Y be non-singular curves over $S = Spec(k)$ for k an algebraically closed field. If $f : X \to Y$ is a finite morphism, we define the degree of f (deg(f)) to be the degree of the field extension $[K(X) : K(Y)]$.*

Theorem 11. *Let S be an arbitrary scheme and E_1 and E_2 elliptic curves over S and $f : E_1 \to E_2$ an S-homomorphism. Then either $f = 0$ or f is finite locally free.*

Proof. See Proposition 1.1 of [4]. □

Definition 27. *An isogeny is a homomorphism, $f : E \to E'$, of S-group schemes that satisfies deg(f_s) $= d \neq 0$ for all $s \in S$. By the above theorem, it is equivalent to f being finite locally free.*

4.2 Quotients by a group scheme

We now describe the concept of a quotient of a group scheme. Let H be an S-group scheme and X an S-scheme. A *right action* of H on X is a morphism $a : X \times_S H \to X$ such that for every S-scheme T, the map on the points $X(T) \times H(T) \to X(T)$ is a right action of the group $H(T)$ on the set $X(T)$. Further, we call an action *strictly free* if the morphism

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

i.e., the morphism inducing $(x, h) \mapsto (x, xh)$ on the functors is both injective on the functors and a closed immersion. For a given right action H on X, we call a morphism $f : X \to Y$ *constant on orbits* if

$$f \circ a = f \circ \mathrm{pr}_1 : X \times_S H \to Y,$$

that is, if $f(xh) = f(x)$, all $x \in X(T), h \in H(T)$ for any S-scheme T.

Theorem 12. *(Grothendieck) Let H be a finite flat group scheme over S a locally noetherian scheme such that it acts strictly freely on a scheme X of finite type over S. Further if every orbit is contained in an affine open set, then the category of morphisms $X \to Z$ constant on orbits has an initial object; i.e., an S-scheme Y and a morphism $u : X \to Y$ constant on orbits such that for every morphism $v : X \to Z$, which is constant on orbits, there is a unique morphism $f : Y \to Z$ such that $v = f \circ u$. We denote $Y := X/H$. Further the morphism $u : X \to X/H$ has the following properties :*
(i) X is finite flat over X/H.
(ii) For every S-scheme T, the map $X(T)/H(T) \to (X/H)(T)$ is injective.
(iii) If $S = Spec(R)$, $H = Spec(B)$ and $X = Spec(A)$ are affine, then $X/H = Spec(A_0)$, where A_0 is the subring of A where the two homomorphisms $\widetilde{\mathrm{pr}}_1, \widetilde{a} : A \to A \otimes_R B$ coincide.

Proof. See Tate's paper in [20]. □

The main application of Grothendieck's Theorem stated above is when $X = G$ an S-group scheme and $H \subset G$ is a finite flat closed subgroup scheme, the action $G \times_S H \to G$ given by the restriction of the multiplication map $G \times_S G \to G$. Then the quotient scheme G/H is called the *scheme of left cosets* of H in G. Also, G acts on the left of the scheme G/H such that the diagram

$$\begin{tikzcd} G \times_S G \arrow[r, "\mathrm{id}\times u"] \arrow[d, "m"'] & G \times_S (G/H) \arrow[d, "\text{left action of } G"] \\ G \arrow[r, "u"] & G/H \end{tikzcd}$$

commutes. Further when H acts trivially on G/H or in other words when H is normal, we get a morphism $G/H \times G/H \to G/H$ which makes G/H an S-group scheme and the canonical injection $u : G \to G/H$ an S-group homomorphism.

Example 1. *Let R be a ring of characteristic p. We now compute the quotient group scheme $\mathbb{G}_a/\alpha_{p^r}$. By Grothendieck's Theorem above, we have*

$$\mathbb{G}_a/\alpha_{p^r} = \mathit{Spec}(R_0)$$

where $R_0 \subset R[x]$ is a subring such that on R_0, the morphisms $R[x] \xrightarrow{\tilde{m}} R[x] \otimes_R R[x]/(x^{p^r})$, given by $r(x) \mapsto r(x) \otimes 1 + 1 \otimes r(x)$ and $R[x] \xrightarrow{\tilde{\mathrm{pr}}_1} R[x] \otimes_R R[x]/(x^{p^r})$ given by $r(x) \mapsto r(x) \otimes 1$ coincide. Thus we get, $R_0 = \{r(x) \in R[x] \mid r(x) \in (x^{p^r})\}$ or in other words $\mathbb{G}_a/\alpha_{p^r} = \mathit{Spec}R[x^{p^r}]$.

Theorem 13. *Let $f : E \to E'$ be an isogeny (in other words, a non-zero S-homomorphism) and let $G := f^{-1}(0)$ be the scheme-theoretic kernel. Then $E' \cong E/G$.*

Proof. We will first describe the quotient E/G. Note that G acts on E by the restriction of the group action

$$G \times_S E \xrightarrow{m} E.$$

Let $\bigcup_i U_i = \mathrm{Spec}(R_i)$ be an affine open covering of S. We will construct the quotients E/G over each R_i and glue them together. By the definition of quotient as an initial object which is *constant on orbits*, we are justified in gluing along the overlaps of the U_i's (See Grothendieck's Theorem stated above). Hence we may assume that E is an elliptic curve over $\mathrm{Spec}(R)$. Now if we can find a G-invariant affine open covering $\{V_i\}_i = \{\mathrm{Spec}(A_i)\}_i$ of E (i.e. $gV_i \subset V_i$ for all i), then by Grothendieck's recipe, ibid., the quotient V_i/G is given by the spectrum of the G-invariant subring of A_i. We can then glue each V_i/G to get the quotient E/G. Since $E/\mathrm{Spec}(R)$ is projective, every G-orbit Gx (for all $x \in E$) is contained in an affine open subset V. Then $\bigcap_{g \in G} gV$ is a G-invariant affine open neighbourhood of x. Thus we can form the quotient E/G over each U_i and further glue them to form the quotient E/G over S. Now since, by definition, G is the scheme theoretic kernel,

$$E \xrightarrow{f} E'$$

f is constant on orbits of G and hence by the *universal property* of quotients, we have

$$E \xrightarrow{u} E/G \xrightarrow{v} E'$$

such that $v \circ u = f$. Since f is a surjective map, we know that in particular $E/G \xrightarrow{v} E'$

is surjective. Further, it is injective too since the scheme-theoretic kernel of f is the same as the scheme-theoretic kernel of u. This proves that v is an isomorphism or in other words $E' \cong E/G$. □

4.3 The dual Isogeny and Hasse's theorem.

Definition 28. *Let E, E' be elliptic curves over an arbitrary scheme S and let $f : E \to E'$ be an isogeny. We have a morphism of functors*

$$f^t : Pic^0(E'/S) \to Pic^0(E/S)$$

given by $\mathcal{L} \mapsto f^*\mathcal{L}$, the inverse image under f of $\mathcal{L}$. Now, f^t is a S-homomorphism and hence by Abel's Theorem (See Chapter 2), we get an isogeny

$$f^t : E' \to E \tag{4.3}$$

which we define as the dual isogeny of f.

Theorem 14. *With notation as above, let f have constant fibral degrees N. Then $f^t \circ f = f \circ f^t = [N], (f^t)^t = f, [N]^t = [N]$ and $deg(f^t) = N$.*

Proof. See Section 2.6 in [10]. □

We will now consider the case when the base scheme has positive characteristic and review the *Frobenius* and *Verschiebung* morphisms.

4.3.1 Frobenius and Verschiebung

Let S be a scheme of characteristic p. We then have a morphism

$$\mathrm{Fr}^{\mathrm{abs}} : S \to S$$

called the *absolute Frobenius*. It is given as the identity map on the underlying topological spaces of S but on the structure sheaf $\mathcal{O}_S$, it is the map of raising to the p-power.

For $f : X \to S$ be an S-scheme we denote by $X^{(p)}$ the fiber product:

$$\begin{tikzcd}
X^{(p)} \arrow[r] \arrow[d] & X \arrow[d, "f"'] \\
S \arrow[r, "\mathrm{Fr}^{\mathrm{abs}}"] & S
\end{tikzcd}$$

Now by the universal property of fiber products, the unique morphism

$$\mathrm{Fr} : X^{(p)} \to X. \tag{4.4}$$

is called the *Frobenius* morphism. The Frobenius is an S-morphism.

Example 2. *Let k be a perfect field of characteristic p. Let $S = Spec(k)$ and let X be*

$$X = Spec(k[x_1, \dots, x_n]/(f_1, \dots, f_m)).$$

Then we have that the scheme $X^{(p)}$ is

$$X^{(p)} = Spec(k[x_1, \dots, x_n]/(g_1, \dots, g_m)).$$

where the g_i are obtained from f_i by raising each coefficient of f_i to the p-power. The Frobenius morphism is then induced by the homomorphism

$$k[x_1, \dots, x_n]/(g_1, \dots, g_m) \to k[x_1, \dots, x_n]/(f_1, \dots, f_m),$$

which is determined by $x_i \mapsto x_i^p$ for $i = 1, \dots, n$.

When G is a finite flat commutative group scheme over S, we denote by G^t the *dual group scheme* of G. Now, consider the morphism

$$\mathrm{Fr}^t : G^t \to (G^t)^{(p)}$$

Upon dualizing, we obtain a morphism which we call the *Verschiebung* and denote it by Ver := $\mathrm{Ver}_{G^{(p)}}$

$$\mathrm{Ver} := \mathrm{Fr}^t : G^{(p)} \to G.$$

Remark 8. *The Verschiebung is a group homomorphism satisfying*

$$Fr_G \circ Ver = [p]_{G^{(p)}}, \qquad Ver_{G^{(p)}} \circ Fr_G = [p]_G$$

4.4 Riemann hypothesis for elliptic curves over finite fields

Corollary 4. (1) *If $f : E \to E$ is an S-endomorphism of an elliptic curve over a connected base S, there exists an integer called trace(f) such that $f^t + f = \mathit{trace}(f)$.*
(2) *In End(E), f is a root of the polynomial in $\mathbb{Z}[x]$*

$$x^2 - \mathit{trace}(f)x + \mathit{deg}(f) = 0 \tag{4.5}$$

(3) *We have the inequality*

$$(\mathit{trace}(f))^2 \leq 4\mathit{deg}(f).$$

Proof. For (1), note that

$$\deg(1+f) = (1+f)(1+f^t) = 1 + \deg(f) + \mathrm{trace}(f) \ \in \ \mathbb{Z}.$$

For (2), plugging in f in equation 4.5 above, we get

$$f^2 - (f^t + f)f + f^t f = 0.$$

Now consider the quadratic form given by the polynomial in consideration, i.e., the form given by

$$P(x,y) = x^2 - \mathrm{trace}(f)xy + \deg(f)y^2 \tag{4.6}$$

Note that for all integers $n, m \ \in \ \mathbb{Z}$, $P(n,m) = \deg(n - mf) \geq 0$. Hence the quadratic form must be positive definite or in other words, it has a positive discriminant, i.e.,

$$d = 4\deg(f).1 - (\mathrm{trace}(f))^2 \geq 0 \tag{4.7}$$

which proves the inequality in part (3). □

Theorem 15. [Hasse] *If E is an elliptic curve over the finite field $\mathbb{F}_q$ (for $q = p^n$ a prime power), then*

$$\mid a_q \mid := \mid (q+1) - \#E(\mathbb{F}_q) \mid \leq 2\sqrt{q}$$

Proof. Let Frob$_{p^n}$ denote the *Frobenius* morphism on E induced by the absolute p^n-Frobenius on Spec$(\mathbb{F}_q)$.

$$\begin{tikzcd}
E^{(q)} \arrow[r, "\mathrm{Frob}_{p^n}"] \arrow[d] & E \arrow[d] \\
\mathrm{Spec}(\mathbb{F}_q) \arrow[r, "\mathrm{Frob}_{p^n}=Id"] & \mathrm{Spec}(\mathbb{F}_q)
\end{tikzcd}$$

Now it follows that $P \in E(\mathbb{F}_q)$ if and only if $P \in E^{(q)}(\mathbb{F}_q)$ and thus,

$$\#E(\mathbb{F}_q) = \#\mathrm{Ker}(1 - \mathrm{Frob}_{p^n}) = \deg(1 - \mathrm{Frob}_{p^n}) = (1 - \mathrm{Frob}_{p^n}^t)(1 - \mathrm{Frob}_{p^n})$$

and hence we get that

$$\#E(\mathbb{F}_q) = 1 - \mathrm{trace}(\mathrm{Frob}_{p^n}) + \deg(\mathrm{Frob}_{p^n})$$

Since $\deg(\mathrm{Frob}_{p^n}) = \deg(\mathrm{Ver}_{p^n})$ and $\mathrm{Frob}_{p^n} \circ \mathrm{Ver}_{p^n} = [p^n]$, we get that $\deg(\mathrm{Frob}_{p^n}) = p^n = q$. Since $a_q := (q+1) - \#E(\mathbb{F}_q)$, we get that $a_q = \mathrm{trace}(\mathrm{Frob}_{p^n})$. Now by (3) in the Corollary above,

$$\mathrm{trace}(\mathrm{Frob}_{p^n})^2 \leq 4\deg(\mathrm{Frob}_{p^n}) = 4q$$

or in other words

$$\mid a_q \mid \leq 2\sqrt{q}$$

□

Definition 29. *We define the zeta function for $E_{/\mathbb{F}_q}$ by*

$$Z_E(t) = \frac{1 - a_q t + qt^2}{(1-t)(1-qt)}$$

where $a_q = q + 1 - \#E(\mathbb{F}_q)$ is as defined above.

Theorem 16. [Riemann Hypothesis] *Let $s = \sigma + it$ be a complex variable. If $Z_E(q^{-s}) = 0$, then* $\mathrm{Re}(s) = 1/2$.

Proof. We know that if $Z_E(q^{-s}) = 0$, then q^s is a root of the polynomial

$$f(x) = x^2 - a_q x + q$$

But, by Hasse's theorem above, the discriminant of f, $a_q^2 - 4q \leq 0$. Hence the roots of $f(x)$, r_1, r_2, are either repeated or are complex conjugates. In particular $\mid r_1 \mid = \mid r_2 \mid$.

Also, since $r_1 r_2 = q$, we have that $\mid r_1 \mid = \mid r_2 \mid = \sqrt{q}$. But since one of $r_i = q^s$, we get that $\mid q^s \mid = \sqrt{q}$ and hence $\mathrm{Re}(s) = 1/2$. □

Bibliography

[1] Altman, A., and Kleiman, S., *Introduction to Grothendieck Duality theory*, Springer Lecture Notes in Mathematics, 146, 1970.

[2] Bosch, Lütkebohmert, Raynaud, *Neron Models*, Springer-Verlag 1989.

[3] Conrad, Brian, *Applications of Base Change for Coherent Cohomology*, MATH 248B Course Handouts, math.stanford.edu/ conrad/248BPage/handouts/cohom.pdf.

[4] Conrad, Brian, *Isogenies and Level Structure*, MATH 248B Course Handouts, math.stanford.edu/ conrad/248BPage/handouts/level.pdf.

[5] Deligne, P. and Rapoport, M., *Les Schmas de Modules de Courbes Elliptiques* in Modular Functions of One Variable II, P. Deligne (ed.) W. Kuyk (ed.), Lecture Notes in Mathematics, 349, Springer, 1973.

[6] Goren, Eyal Z., *Lectures on Hilbert Modular Varieties and Modular Forms*, CRM Monograph Series, Vol. 14, American Mathematical Society, 2001.

[7] Hartshorne, R., *Algebraic Geometry*, Springer Graduate Texts in Mathematics, 52, 1977.

[8] Hartshorne, R., *Residues and Duality*, Lecture Notes in Mathematics, 20, 1966.

[9] Hida, H. *Geometric Modular Forms and Elliptic Curves*, World Scientific, 2000.

[10] Katz, Nicholas. M., Mazur, Barry. *Arithmetic Moduli of Elliptic Curves* 108, Annals of Mathematical Studies, Princeton University Press, 1985.

[11] Kleiman, Steven L., *The Picard Scheme* in Fundamental Algebraic Geometry, Fantechi et al., Mathematical Surveys and Monographs, AMS, Volume 123, 2005.

[12] Lang, Serge. *Algebra*, 211, Graduate Texts in Mathematics, Springer-Verlag, 2002.

[13] Liu, Qing, *Algebraic Geometry and Arithmetic Curves*, 6, Oxford Graduate Texts in Mathematics, 2002.

[14] Mathew, Akhil, Flatness, semicontinuity and base-change, Available online at http://people.fas.harvard.edu/ amathew/semicontinuity.pdf.

[15] Milne, James, *Lectures on Etale Cohomology*, Availabe online, 2008.

[16] Mumford, David M., *Abelian Varities*, Oxford Univ. Press, Oxford, 1970.

[17] Mumford, D., Forgaty, J., Kirwan, F.,, *Geometric Invariant Theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 34, Springer-Verlag, 1992.

[18] Osserman, Brian, *Notes on Cohomology and Base Change*, Available online.

[19] *Etale morphism*, Available online at http://planetmath.org/encyclopedia/Etale.html.

[20] Tate, John *Finite Flat Group Schemes* in Modular Forms and Fermat's Last Theorem, Cornell, Gary, Silverman, Joseph, H., Stevens Glenn, Springer Verlag 1997.