Elliptic Curves, Modular Forms and p-adic Heights

Khalil Besrour

Thesis submitted in partial fulfillment of the requirements for the degree of
Master of Science Mathematics and Statistics[1]

Department of Mathematics and Statistics
Faculty of Science
University of Ottawa

© Khalil Besrour, Ottawa, Canada, 2021

[1]The M.Sc. program is a joint program with Carleton University, administered by the Ottawa-Carleton Institute of Mathematics and Statistics

Abstract

The aim of this thesis is to provide an introduction to the study of elliptic curves and modular forms over general commutative rings or schemes. We will recall a few aspects of the classical theory of these objects (over the complex numbers) while placing emphasis on the geometric picture. Moreover, we will formulate the theory of elliptic curves in the modern language of algebraic geometry following the work of Katz [10] and Mazur [13]. In addition, we provide an application of $p-$adic modular forms to the theory of $p-$adic heights on elliptic curves.

Résumé

Le but de cette thèse de maitrise sera d'introduire le lecteur à l'étude des courbes elliptiques et des formes modulaires définies sur des anneaux commutatifs ou plus généralement des schémas quelconques. On va rappeler la théorie analytique classique des formes modulaires en mettant l'accent sur l'aspect géométrique de ces objets. Après, on va redéfinir la notion de courbe elliptique dans le language moderne de la géométrie algébrique en suivant les travaux de Katz [10] et de Mazur [13]. Finalement, on va donner un exemple d'application des formes modulaires $p-$adiques dans l'étude des hauteurs $p-$adiques sur les courbes elliptiques.

Dedications

À ma mère Afifa pour son amour inconditionnel et à mon père Adel pour sa sagesse inépuisable. À mes soeurs Zeineb, Nour et May pour leur joie de vivre. À ma tante Amel pour m'avoir partagé sa passion des mathématiques. À mon oncle Sadok et ma tante Janine pour avoir été ma famille sur cette rive opposée de l'Atlantique. Finalement, à mes amis Kais, Éric, Sandrine, Florence, Fadhel et Younes pour les beaux moments partagés.

Acknowledgement

I would like to thank my supervisor Dr. Abdellah Sebbar for his valuable advice and encouragement.

I would also like to thank the staff of the Department of Mathematics and Statistics at the university of Ottawa for their support during all my studies.

Contents

Introduction

Classically, a modular form f of weight k is a holomorphic function over the extended complex upper half plane

$$\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\},$$

such that, for every $z \in \mathbb{H}^*$ and $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ the group of matrices with integer coefficients and determinant 1, we have :

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z).$$

Although this is a practical definition when one is trying to prove that a given holomorphic function on $\mathbb{H}^*$ is a modular form, it is not immediately clear from the above functional equation why such objects are useful or important to be studied. So if we hope to generalize the theory of modular forms to a vaster algebraic setting, we have to find an alternative and more geometric way of defining them. If one looks at the set of orbits $X(1)$ of the group action of $SL_2(\mathbb{Z})$ on the extended upper half plane given by

$$z \mapsto \frac{az+b}{cz+d} \quad \text{for all } z \in \mathbb{H}^*,$$

one can show that it is actually a Riemann surface. What is even more interesting is that modular forms of weight k correspond in a natural way to global sections of the sheaf of $k-$fold differential forms over the $X(1)$. In this way, we reduced the problem of understanding modular forms to the problem of understanding a geometric object which is $X(1)$. On the other hand, the Riemann surface $X(1)$ arises in what is called the moduli problem for elliptic curves over $\mathbb{C}$. Indeed, $X(1)$ arises naturally as the compactification of some space $Y(1)$ whose points are in a one-to-one correspondence with the set of all elliptic curves over $\mathbb{C}$. This will motivate sections 1.2 and 1.3 of the first chapter while section 1.1 will consist of a small introduction to the language of algebraic geometry following Hartshorne [7], Hida [8] and Grothendieck [4] [5] [6].

In the second chapter, we cover the basics of the theory of elliptic curves over general schemes usually denoted $E_{/S}$ or simply $E \to S$. We start by introducing the notion of effective Cartier divisors which will enable us to prove the existence and uniqueness of the group structure on these new and more general elliptic curves. It is stated as follows:

Theorem 0.0.1. *Let $E \to S$ be an elliptic curve, then E/S has a unique structure of a commutative group scheme having $0 : S \to E$ as the identity such that, for any S-scheme T and any points A, B and C in $E_T(T) := (E \times_S T)(T)$, we have*

$$A + B = C \iff I(A)^{-1} \otimes I(B)^{-1} \otimes I(O) \cong I(C)^{-1} \otimes f_T^* L_0,$$

for some L_0 an invertible sheaf over T.

Furthermore, it turns out that we still can express elliptic curves locally by a Weierstrass equation of the form

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

for elements $a_i \in A$ where $Spec(A) \subseteq S$ is a subscheme. We end Chapter II with an introduction to moduli problems from an algebraic geometric point of view and then we discuss the moduli problem for elliptic curves with $\Gamma(N)$-structure i.e. an elliptic curve plus an isomorphism

$$\alpha_N : E[N] \to (\mathbb{Z}/n\mathbb{Z})_S \times_S (\mathbb{Z}/n\mathbb{Z})_S,$$

where $E[N]$ denotes the scheme of $N-$torsion points of E. Indeed, we will have that, whenever N is invertible in S, there exists a universal elliptic curve

$$\mathbb{E} \to Y(N)$$

over some affine smooth curve $Y(N)$ over S such that the above morphism is finite. The normalization of $Y(N)$ is denoted $X(N)$ and is a proper smooth curve over S.

We follow the work of Katz [10] and chapter 2 of [8] and assume the reader's acquaintance with the basics of sheaf Cohomology and formal schemes as covered in Hartshorne [7].

In the last Chapter, we give a definition of general modular forms over arbitrary schemes and we give a few nontrivial examples. We finally define $p-$adic modular forms and we put a particular emphasis on $\mathbb{E}_2$ the Katz $p-$adic modular form of weight k. The first attempt to defining modular forms $p-$adically was introduced by Serre in [17]. He simply took $p-$adic modular forms to be the $p-$adic limit of

the $q-$expansions of classical modular forms with arbitrary weights. The weight of such forms is the $p-$adic limit of the weights of the classical modular forms. In his attempt to generalize the work of Serre from the point of view of the theory of moduli of elliptic curves [13], Katz gave an alternative (and geometric) definition for $p-$adic modular forms that we will introduce later on.

We will end this chapter by giving an example of a seemingly altogether different construction on elliptic curve but that will involve computing values of the $p-$adic modular form $\mathbb{E}_2$. Indeed, $\mathbb{E}_2$ will play a crucial role in understanding a $p-$adic height $h_p : E(\mathbb{Q}) \to \mathbb{Q}_p$ on elliptic curves over $\mathbb{Q}$. There is no universal definition of what a height function is exactly as such definitions depend on how the construction will be used, but they are usually functions on the points of an elliptic curve E that behave nicely under the group operation. Later in the chapter, we give the explicit formula for one such height h_p

$$h_p(P) = \frac{1}{p} \log_p \left(\frac{\sigma_p(P)}{d(P)} \right),$$

for certain elements $P \in E(\mathbb{Q})$ and we define each of the terms above. By construction, the $p-$adic height h_p will verify the two properties:

1. Quadratic law: For all $n \in \mathbb{Z}$ and $A \in E(\mathbb{Q})$, we have

$$h_p(nA) = n^2 h_p(A).$$

2. Parallelogram law: For all $A, B \in E(\mathbb{Q})$, we have

$$h_p(A+B) + h_p(A-B) = 2h_p(A) + 2h_p(B).$$

This gives rise to a natural pairing $(\ ,\ )_p : E(\mathbb{Q}) \times E(\mathbb{Q}) \to \mathbb{Q}_p$ called the Mazur-Tate $p-$adic pairing and defined as

$$(A, B)_p = \frac{1}{2} \left(h_p(A+B) - h_p(A) - h_p(B) \right),$$

which is bilinear and symmetric. This pairing is used in defining the $p-$adic regulator of an elliptic curve. Given a set of generators $P_1, \ldots, P_r$ of $E(\mathbb{Q})/E(\mathbb{Q})_{tor}$, we define

$$\mathrm{Reg}_p(E) = \det((P_i, P_j)_{1 \leq i,j \leq r}).$$

If $r = 0$, then we put $\mathrm{Reg}_p(E) = 1$. It is conjectured by Schneider [16] that the Mazur-Tate $p-$adic pairing is non-degenerate i.e. that $\mathrm{Reg}_p(E) \neq 0$.

Chapter 1

Background

1.1 Background From Algebraic Geometry

The study of moduli spaces is intrinsically a geometric problem. Most of the questions that we ask will be formulated in the language of modern algebraic geometry. This is more of a necessity than of a choice, the geometric objects we study (moduli spaces) might not be varieties in the classical sense (open subsets of an irreducible closed subset of an n-dimensional projective space). And even if they were, we want to study moduli spaces without having to worry about embeddings in projective spaces (just like we study topological manifolds abstractly). In the following sections, we give a compact review of the modern theory of algebraic geometry. Our main references will be [7] and [12]. We will speak intensively in the language of categories while assuming various results of commutative algebra as presented in [1].

1.1.1 The language of sheaves

Let X be a topological space and let $\mathbf{TOP}(X)$ be the set of open subspaces of X. It is easy to check that $\mathbf{TOP}(X)$ is actually a category where the morphisms are the inclusion maps. Let $\mathfrak{C}$ be a small category, We define a presheaf of $\mathfrak{C}$ on X as a contravariant functor $\mathbf{TOP}(X) \to \mathfrak{C}$. In particular, when $\mathfrak{C}$ is the category of abelian groups, we define:

Definition 1.1.1. *A **presheaf** of abelian groups $\mathcal{F}$ on X is the following data:*

- *For every open subset U of X, we assign an abelian group $\mathcal{F}(U)$.*
- *Whenever $U \subseteq V$ is an inclusion of open sets in X, we have a restriction map*

$$r_{V,U} : \mathcal{F}(V) \to \mathcal{F}(U).$$

These maps respect the following properties:

- *For all open sets $U \subseteq X$, $r_{U,U} = Id_U$.*
- *Whenever $U \subseteq V \subseteq W$ is an inclusion of open subsets of X, we have*

$$r_{W,U} = r_{V,U} \circ r_{W,V}.$$

From now on, unless we explicitly state otherwise, presheaves on topological spaces are presheaves of abelian groups.

Let X be a topological space, $\mathcal{F}$ a presheaf on X and let $U \subseteq X$ be an open subset. The elements of $\mathcal{F}(U)$ are called sections of $\mathcal{F}$ over U and are sometimes also denoted by

$$\mathcal{F}(U) := \Gamma(U, \mathcal{F}) := \mathrm{H}^0(U, \mathcal{F}).$$

If $s \in \mathcal{F}(U)$ and $V \subseteq U$ then we often denote the image $r_{U,V}(s)$ by $s|_V$ or s_V and call it the restriction of s to V.

By global sections of $\mathcal{F}$ on X, we mean the elements of $\mathcal{F}(X)$.

Definition 1.1.2. *Let X be a topological space and $\mathcal{F}$ be a presheaf (of abelian groups) on X. We say that $\mathcal{F}$ is a **sheaf** if the following two conditions are satisfied:*

- *For all open sets U in X and $U = \bigcup_{i\in I} U_i$ an open covering, if s is a section in $\mathcal{F}(U)$ and if $s|_{U_i} = 0_{U_i}$ for all $i \in I$, then $s = 0_U$.*
- *For all open sets U in X and $U = \bigcup_{i\in I} U_i$ an open covering, if we are given sections s_{U_i} over U_i for each $i \in I$ such that*

$$s_i \mid_{U_i \cap U_j} = s_j \mid_{U_i \cap U_j} \quad \text{for all } i, j \in I,$$

then there exists a section s over U such that, for all $i \in I$,

$$s \mid_{U_i} = s_i.$$

Intuitively, the above definition is stating that a sheaf is a presheaf where sections on a sheaf can be defined locally (condition 1) as long as they are compatible in the intersections (condition 2).

Moreover, one can easily deduce from the definition that, for any sheaf $\mathcal{F}$ on a topological space, $\mathcal{F}(\emptyset) = \{0\}$.

Example 1.1.1. *The presheaf of continuous (resp. differentiable) functions $\mathcal{O}_X$ on a real manifold M is a sheaf. Indeed, function are, by construction, defined locally (by that we mean that is order to define a function on an open set in M, it suffices*

to define it point by point). Similarly, continuity (resp. differentiability) is defined locally (i.e. at every point).

The presheaf of bounded functions on a real manifold is not a sheaf because functions can be locally bounded but not globally (the identity map $Id : \mathbb{R} \to \mathbb{R}$ is locally bounded but no globally).

Remark 1.1.1. *Instead of defining a presheaf (resp. sheaf) on a topological space X by specifying its structure on every open set, one can restrict oneself to open sets of some basis $\mathcal{B}$ of open sets of X. We call such structure a $\mathcal{B}-$presheaf (resp. $\mathcal{B}-$sheaf) and it is defined just by replacing open sets by basic open sets in the above definitions.*

One can easily show that a $\mathcal{B}-$presheaf (resp. $\mathcal{B}-$sheaf) extends uniquely (up to isomorphism) to a presheaf (resp. sheaf) structure over X. The details can be found in Remark 2.6 *of* [*12*, II].

Definition 1.1.3. *Let $\mathcal{F}$ be a presheaf on a topological space X and let $P \in X$. We define the* ***stalk*** *of $\mathcal{F}$ at P to be the direct limit*

$$\mathcal{F}_P = \varinjlim_{p \in U} \mathcal{F}(U) := \{(s, U) \mid U \text{ neighborhood of } P \text{ and } s \in \mathcal{F}(U)\}/_\sim ,$$

where $(s, U) \sim (t, V)$ if and only if there exists $W \subseteq U \cap V$ neighborhood of P such that

$$s|_W = t|_W.$$

We denote the equivalence class of a section s on a neighborhood U of P by either $[(s, U)]$ or simply s_P.

Remark 1.1.2. *Direct limits of abelian groups are abelian groups and they come with natural group homomorphisms $\mathcal{F}(U) \to \mathcal{F}_P$ that send a section s over U to its equivalence class s_P in $\mathcal{F}_P$.*

Sheaves are therefore determined by their stalks. This is made precise in the following proposition.

Proposition 1.1.1. *Let X be a topological space and $\mathcal{F}$ be a sheaf on X. Let U be open in X, then the natural group homomorphism*

$$\pi \colon \mathcal{F}(U) \to \prod_{p \in U} \mathcal{F}_P,$$

that maps $s \mapsto (s_p)_{p \in U}$ is injective.

Proof: The proof is basically the first property of sheaves. Suppose a section s over U is mapped to 0 on every stalk i.e. $s_P = 0$ for all $P \in U$. By definition, this

means that $s|_{U_p} = 0$ for some U_p small enough open neighborhood of P. Clearly

$$U = \bigcup_{p \in P} U_P.$$

Hence, by the first property of sheaves, $s = 0$. This proves that π is injective. ∎

Definition 1.1.4. *Let $\mathcal{F}$ and $\mathcal{G}$ be presheaves on a topological space X. A **morphism of presheaves** $\varphi : \mathcal{F} \to \mathcal{G}$ is a collection of homomorphisms*

$$\{\varphi_U : \mathcal{F}(U) \to \mathcal{G}(U) \mid U \text{ open in } X\},$$

that are compatible with the restriction maps i.e. whenever $U \subseteq V$ are open subsets of X, the following diagram commutes.

$$\begin{array}{ccc} \mathcal{F}(V) & \xrightarrow{\varphi_V} & \mathcal{G}(V) \\ \downarrow{\scriptstyle r_{V,U}} & & \downarrow{\scriptstyle r'_{V,U}} \\ \mathcal{F}(U) & \xrightarrow{\varphi_U} & \mathcal{G}(U). \end{array}$$

Let X be a topological space. If we formulate the definition of a presheaf on X as some functor $\mathcal{F} : \mathbf{TOP}(X) \to \mathbf{Ab}$, then a morphism of presheaves $\mathcal{F} \to \mathcal{G}$ on X corresponds to a natural transformation from the functor $\mathcal{F}$ to $\mathcal{G}$. We now have constructed the category of presheaves on X which we denote by $\mathbf{PSh}(X)$. The category of sheaves on X will be a full subcategory of $\mathbf{PSh}(X)$ which means that morphisms of sheaves are exactly the morphisms of presheaves. The notation used for the category of sheaves on X will be $\mathbf{Sh}(X)$.

Remark 1.1.3. *Let $\mathcal{F}$ and $\mathcal{G}$ be presheaves on a topological space X and let P be an element of X. In a natural way, a morphism of presheaves $\varphi : \mathcal{F} \to \mathcal{G}$ induces a morphism of stalks*

$$\begin{aligned} \varphi \colon \mathcal{F}_P &\to \mathcal{G}_P \\ [(s, U)] &\mapsto [(\varphi_U(s), U)]. \end{aligned}$$

This is well defined. Indeed, suppose $(s, U) \sim (t, V)$, then there exists W small enough neighborhood of P where $s|_W = t|_W$. And so

$$\begin{aligned} [(\varphi_U(s), U)] &= [(\varphi_U(s)|_W, W)] \\ &= [(\varphi_W(s|_W)|, W)] \\ &= [(\varphi_W(t|_W)|, W)] \\ &= [(\varphi_U(t), V)]. \end{aligned}$$

The second equality follows from the commutativity of the above diagram.

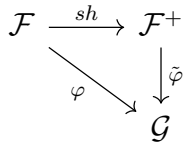
Remark 1.1.4. *Fix a topological space X and let $\varphi : \mathcal{F} \to \mathcal{G}$ be a morphism of presheaves on X. The* ***kernel presheaf*** *$Ker(\varphi)$ on X is given by $U \mapsto Ker(\varphi_U)$ where the restriction maps are the same as for $\mathcal{F}$. In a similar fashion, one defines the* ***image presheaf*** *$Im_{pre}(\varphi)$ by sending $U \mapsto Im(\varphi_U)$ and taking the same restriction maps as for $\mathcal{G}$.*

Now, if $\varphi : \mathcal{F} \to \mathcal{G}$ is a morphism of sheaves then the kernel presheaf is a sheaf while the image presheaf might not be (The second condition fails in general). Indeed, even if we have compatible sections $(s_i)_{i\in I}$ in $\mathcal{G}$ that are images of sections $(f_i)_{i\in I}$ in $\mathcal{F}$, the $(f_i)_{i\in I}$ might not be compatible and so they cannot be patched together into a global section. Now, being mapped to 0 is clearly a local condition on sections (it suffices to be checked at each stalk). And so whenever we have compatible local sections $(f_i)_{i\in I}$ in $\mathcal{F}$ that are mapped to 0, we can patch them together in a unique way into a global section f ($\mathcal{F}$ being a sheaf) that is in the kernel of φ.

To fix the problem of the image of a morphism of sheaves not being a sheaf (and for various other reasons), we introduce the sheafification morphism.

Proposition 1.1.2. *Let $\mathcal{F}$ be a presheaf on a topological space X. There exists a sheaf $\mathcal{F}^+$ and a morphism of presheaves $sh : \mathcal{F} \to \mathcal{F}^+$ such that:*

For any sheaf $\mathcal{G}$, a morphism of presheaves $\varphi : \mathcal{F} \to \mathcal{G}$ factors uniquely through the sheafification morphism $sh : \mathcal{F} \to \mathcal{F}^+$ i.e. there exists a unique morphsim of sheaves $\tilde{\varphi} : \mathcal{F}^+ \to \mathcal{G}$ making the following diagram commute:



Moreover, the pair $(\mathcal{F}^+, sh)$ is unique up to isomorphsim.

The sheaf $\mathcal{F}^+$ is called the **sheafification** of $\mathcal{F}$ and the morphism sh is called the sheafification morphism.

Proof: A proof of this result is given in [7, II.1.6]. ∎

Let φ be a morphism of sheaves. We define the image sheaf $\mathrm{Im}(\varphi)$ (resp. cokernel sheaf $\mathrm{Coker}(\varphi)$) of φ as the sheafification of the image presheaf (resp. cokernel presheaf). A sequence of sheaves

$$\mathcal{F} \xrightarrow{f} \mathcal{G} \xrightarrow{g} \mathcal{H}$$

is exact if $\mathrm{Im}(f) = \mathrm{Ker}(g)$ as sheaves. Moreover, exactness can be checked at the

level of stalks as shown in the following proposition.

Proposition 1.1.3. *Let X be a topological space and let $f : \mathcal{F} \to \mathcal{G}$ and $g : \mathcal{G} \to \mathcal{H}$ be morphisms of sheaves. The following statements are equivalent :*

1. *The sequence $\mathcal{F} \xrightarrow{f} \mathcal{G} \xrightarrow{g} \mathcal{H}$ of sheaves on X is exact.*
2. *The sequence $\mathcal{F}_P \xrightarrow{f_P} \mathcal{G}_P \xrightarrow{g_P} \mathcal{H}_P$ of abelian groups is exact for all $P \in X$.*

Proof: A proof of this result can be found in [12, II.2.18]. ∎

Remark 1.1.5. *Suppose we have a continuous map of topological spaces*

$$f : X \to Y.$$

Let $\mathcal{F}$ be a presheaf (resp. sheaf) on X. The map f induces a presheaf (resp. sheaf) structure on Y called the pushforward sheaf of f, denoted $f_*\mathcal{F}$ and defined by

$$f_*\mathcal{F}(U) := \mathcal{F}(f^{-1}(U)).$$

We also have a dual notion. If $\mathcal{F}$ is a presheaf or a sheaf on Y then f induces a presheaf structure on X called the pullback sheaf of f, denoted by $f^*\mathcal{F}$ and defined as

$$f^*\mathcal{F}(U) := \varinjlim_{f(U)\subseteq V} \mathcal{F}(V).$$

Whenever $\mathcal{F}$ is a sheaf, we abuse notation and denote the sheafification of the presheaf $f^*\mathcal{F}$ also by $f^*\mathcal{F}$.

1.1.2 Schemes

We start by introducing a topological notion which generalizes topological manifolds.

Definition 1.1.5. *A ringed space consists of the data of a topological space X and a sheaf of rings $\mathcal{O}_X$ on X. A locally ringed space is a ringed topological space $(X, \mathcal{O}_X)$ such that the stalks $\mathcal{O}_{X,x}$ are local rings for all $x \in X$.*

We call $\mathcal{O}_X$ the structure sheaf of X. For every $x \in X$, we denote the maximal ideal of $\mathcal{O}_{X,x}$ by m_x and the residue field $\mathcal{O}_{X,x}/m_x$ by $k(x)$.

Definition 1.1.6. *A morphism of locally ringed spaces*

$$(f, f^{\#}) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$$

consists of a continuous map of topological spaces $f : X \to Y$ and a morphism of sheaves over Y

$$f^{\#} : \mathcal{O}_Y \to f_*\mathcal{O}_X,$$

such that the induced map on stalks $f_x^{\#} : \mathcal{O}_{Y,f(x)} \to f^*\mathcal{O}_{X,x}$ is a local morphism of rings (i.e. $f_x^{\#}(m_{f(x)}) \subseteq m_x$).

Two important classes of morphisms of locally ringed spaces are open immersions and closed immersions. We say that a morphism of locally ringed spaces

$$(f, f^{\#}) : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$$

is an open immersion if f is an open immersion (as a continuous map of topological spaces) and $f^{\#}$ is an isomorphism of sheaves over Y.

We say that $(f, f^{\#})$ is a closed immersion if f is a closed immersion of topological spaces and $f^{\#}$ is a surjective morphism of sheaves over Y. If we denote the kernel sheaf of $f^{\#}$ by $\mathcal{I} := ker(f^{\#})$, we have a canonical exact sequence

$$0 \longrightarrow \mathcal{I} \longrightarrow \mathcal{O}_Y \longrightarrow f_*\mathcal{O}_X \longrightarrow 0.$$

When the context is clear, we sometimes write $\mathcal{O}_X$ instead of $f_*\mathcal{O}_X$.

Example 1.1.2. *Let R be a ring. We denote by $Spec(R)$ the set of prime ideals of R. We endow $Spec(R)$ with a topology called the Zariski topology where closed sets are the sets of the form*

$$V(I) := \{p \in Spec(R) \mid I \subseteq p\},$$

for subsets I of R. One can see immediately that $V(I) = V((I))$ where (I) is the ideal generated by I. These indeed verify the axioms of a topology on $Spec(R)$ as shown in [7, II.2.1]. *One immediately notices that*

$$V(I) = \bigcap_{f \in I} V(f).$$

Therefore, every open set $D(I) := V(I)^c$ can be written as the union of open sets of the form $D(f)$ for $f \in R$. We call them basic open sets as they form a basis for the topology on $Spec(R)$.

We also define a sheaf structure $\mathcal{O}_{Spec(R)}$ on $Spec(R)$. As we have already discussed, it is enough to define it on a basis of open sets. Let

$$\mathcal{O}_{Spec(R)}(D(f)) := R_f,$$

where R_f denotes the localization of R at $S = \{1, f, f^2, f^3, \dots\}$. Moreover, whenever $D(g) \subseteq D(f)$, it follows that $g \in \sqrt{(f)}$ (the radical of the ideal (f)) and therefore f is invertible in R_g and we have a natural morphism

$$R_f \to R_g.$$

This morphism plays the role of the restriction map. Also, one has that if $D(g) = D(f)$ then $\sqrt{(f)} = \sqrt{(g)}$ and therefore $R_f = R_g$ proving that $\mathcal{O}_{Spec(R)}(D(f))$ doesn't depend on f. This makes $(Spec(R), \mathcal{O}_{Spec(R)})$ into a ringed space with the following properties.

Proposition 1.1.4. *Let R be a ring and let $X = Spec(R)$. We have*

$$\mathcal{O}_{Spec(R)}(Spec(R)) = R.$$

Moreover, for all $p \in Spec(R)$,

$$\mathcal{O}_{Spec(R),p} = R_p,$$

where R_p denotes the localization of R by the multiplicative set $S = R - p$.

Proof: This is shown in [7, II.2.2]. ∎

Remark 1.1.6. *The second part of the proposition implies that $(Spec(R), \mathcal{O}_{Spec(R)})$ is a locally ringed space.*

Definition 1.1.7. *An affine scheme is a ringed space isomorphic to $(Spec(R), \mathcal{O}_{Spec(R)})$ for some ring R.*

Definition 1.1.8. *A scheme S is a ringed space that is locally isomorphic to an affine scheme i.e. S has an open cover $\{U_i\}_{i \in I}$ and there exist rings $\{R_i\}_{i \in I}$ such that*

$$(S, \mathcal{O}_S)|_{U_i} \cong (Spec(R_i), \mathcal{O}_{Spec(R_i)}).$$

In particular, a scheme is a locally ringed space. We think of the category of schemes as a full subcategory of the category of locally ringed spaces therefore :

Definition 1.1.9. *A morphism of schemes is a morphism of locally ringed spaces. Similarly, an open or closed immersion of schemes is an open or closed immersion of locally ringed spaces.*

Given a morphism $f : S \to T$ of schemes, the induced morphism of sheaves

$$f^{\#} : \mathcal{O}_T \to f_* \mathcal{O}_S,$$

restricted to T, gives a ring homomorphism

$$\mathcal{O}_T(T) \to \mathcal{O}_S(S).$$

Hence, we have a canonical map

$$\rho : Mor(S,T) \to Hom_{rings}(\mathcal{O}_T(T), \mathcal{O}_S(S)).$$

Now, suppose we are given a morphism of rings $\phi : A \to B$, then we have a map of sets

$$\begin{aligned} f : Spec(B) &\to Spec(A) \\ p &\mapsto \phi^{-1}(p). \end{aligned}$$

This map is continuous because $f^{-1}V(a) = V(\phi(a))$ for all $a \in A$ and the $\{V(a)\}_{a\in A}$ form a basis for the topology on $Spec(A)$. Moreover, the canonical morphisms of rings $\phi_a : A_a \to B_{\phi(a)}$ define, as stated in Remark 1.1.1, a morphism of sheaves

$$f^{\#} : \mathcal{O}_{Spec(A)} \to f_*\mathcal{O}_{Spec(B)}.$$

Hence $\phi : A \to B$ induces a morphism of schemes

$$(f, f^{\#}) : Spec(B) \to Spec(A).$$

All these results we discussed can be put together in the following more general result

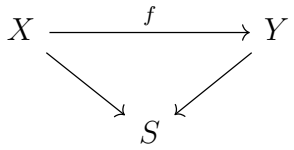
Theorem 1.1.1. *Let $f : S \to Spec(R)$ be a morphism of schemes, then the map ρ described above induces a bijection*

$$Mor(S, Spec(R)) \longleftrightarrow Hom_{rings}(R, \mathcal{O}_S(S)).$$

Proof: A detailed proof of this result and of the above discussion are given in [12, II.3.25]. ∎

In particular, the theorem implies that there is an equivalence of categories between the category of rings and the (opposite) category of affine schemes.

Remark 1.1.7. *Let us fix a scheme S. By a scheme X over S (or simply an $S-$scheme X), we mean a scheme X endowed with a morphism of schemes $X \to S$. By a morphism $f : X \to Y$ of $S-$schemes, we mean a morphism $X \to Y$ of schemes such that the diagram*



commutes. Given a fixed schemes S, we can talk about the category of schemes over S.

If $S = Spec(R)$ for some ring R, we may interchange the use of R and $Spec(R)$. We might write $R-$schemes (resp. $R-$morphisms) instead of $Spec(R)-$schemes (resp. $Spec(R)-$morphisms).

If X and T are $S-$schemes, we call $T-$valued points of X (or simply $T-$points) and we denote by $X(T)$ the set $Hom_S(T, X)$ of $S-$morphisms $T \to X$. If $T = Spec(R)$ then $X(R) := X(Spec(R))$.

To an $S-$scheme X corresponds a functor

$$F_X : (S-\text{schemes}) \to (\text{Sets}),$$

that sends $T \mapsto X(T)$. Composition is given as follows; if $\phi : T \to T'$ is a map of $S-$schemes, then $F_X(\phi) : X(T') \to X(T)$ sends $u \mapsto u \circ \phi$. This makes F_X into a contravariant functor. Moreover, Yoneda's lemma states that F_X characterizes the $S-$scheme X which means that if X and Y are $S-$schemes such that $F_X = F_Y$ then $X = Y$.

Let X and Y be $S-$schemes. The fiber product of X and Y over S is an $S-$scheme $X \times_S Y$ together with $S-$morphisms

$$p_1 : X \times_S Y \to X \quad \text{and} \quad p_2 : X \times_S Y \to Y,$$

having the universal property of the pullback of both maps $X \to S$ and $Y \to S$. If $S = Spec(R)$, we will denote the fiber product over $Spec(R)$ as $X \times_R Y$. Fiber products of schemes always exist and a detailed construction is given in [7, II.3.3].

Definition 1.1.10. *If X is a $Y-$scheme and $f : Y' \to Y$ is a morphism of schemes then, by base extension of X by f, we mean the $Y'-$scheme $X \times_Y Y' \to Y'$ where the morphism is taken to be the projection on the second component.*

Remark 1.1.8. *If $f : X \to Y$ is a morphism of schemes and $y \in Y$, let $k(y)$ be the residue field at y. We have a natural morphism*

$$y : Spec\ k(y) \to Y,$$

that sends the unique point of Spec $k(y)$ to y. This allows us to define the fiber of the morphism f over the point y as

$$X_y := X \times_Y Spec\ k(y),$$

and it is naturally a scheme over the residue field $k(y)$.

Definition 1.1.11. *A scheme X is locally noetherian if it can be covered by affine schemes $\{Spec(R_i)\}_{i\in I}$ where the R_i are noetherian rings. We say it is noetherian if I is finite.*

We say that a scheme X is connected if it is connected as a topological space. Similarly, we say it is irreducible if it is irreducible as a topological space i.e. it cannot be written as the union of two closed proper subsets.

Definition 1.1.12. *A scheme X is reduced if it can be covered by affine schemes $\{Spec(R_i)\}_{i\in I}$ where the R_i are reduced i.e. they have no nonzero nilpotent elements.*

Definition 1.1.13. *A scheme X is integral if it can be covered by affine schemes $\{Spec(R_i)\}_{i\in I}$ where the R_i are integral domains.*

One can show that if X is locally noetherian (resp. reduced, integral) then, for every affine open $Spec(R) \subseteq X$, R is noetherian (resp. reduced, integral) [12, II].

We are usually more interested in the properties of morphisms of schemes $f : S \to T$ rather than the properties of the schemes themselves.

Definition 1.1.14. *We say that a morphism $f : S \to T$ is of finite type (resp. finite presentation) if, for every $Spec(A) \subseteq T$ affine open subset, we can cover $f^{-1}(Spec(A))$ by open affine subsets $\{Spec(B_i)\}$ where each B_i is a finitely generated (resp. finitely presented) $A-$algebra.*

We say that f is a finite morphism if, for every $Spec(A) \subseteq T$ affine open subset, its preimage $f^{-1}(Spec(A))$ is affine equal to $Spec(B)$ where B is a finitely generated $A-$module.

In practice, one only needs to show the properties of finite type and finiteness on an open affine cover of Y (instead on every affine open subset of Y) [12, III].

Let $f : X \to Y$ be a morphism of schemes. The identity map $\mathrm{Id} : X \to X$ induces, by the universal property of fiber product, a morphism

$$\Delta : X \to X \times_Y X$$

of $Y-$schemes called the diagonal morphism relative to f.

Definition 1.1.15. *A morphism of schemes $f : X \to Y$ is separated if the diagonal morphism relative to f is a closed immersion.*

We say that a morphism of schemes $f : X \to Y$ is closed if it is closed as a continuous map of topological spaces i.e. it sends closed subsets of X to closed subsets of Y.

More generally, we say that $f : X \to Y$ is universally closed if, under any morphism $Y' \to Y$, the base extension

$$f' : X \times_Y Y' \to Y'$$

is a closed morphism.

Definition 1.1.16. *A morphism of schemes $f : X \to Y$ is proper if it is separated, of finite type and universally closed.*

Recall that an R-module M is flat if the functor

$$M \otimes - \ : \mathbf{R\text{-}mod} \to \mathbf{R\text{-}mod}$$

is exact.

Definition 1.1.17. *A morphism of schemes $f : X \to Y$ is flat if the induced maps on stalks, i.e.*

$$f_P : \mathcal{O}_{Y,f(P)} \to \mathcal{O}_{X,P},$$

for every $P \in X$, make each $\mathcal{O}_{X,P}$ into a flat $\mathcal{O}_{Y,f(P)}$-module.

We introduce the notion of sheaf modules.

Definition 1.1.18. *Let $(X, \mathcal{O}_X)$ be a ringed space. A sheaf of $\mathcal{O}_X-$modules (or simply an $\mathcal{O}_X-$module) is a sheaf $\mathcal{F}$ on X such that $\mathcal{F}(U)$ is an $\mathcal{O}_X(U)-$module for every open subset $U \subseteq X$ and such that, whenever $V \subseteq U$, we have that*

$$(af)|_V = a|_V f|_V,$$

for every $a \in \mathcal{O}_X(U)$ and $f \in \mathcal{F}(U)$.

A morphism $\mathcal{F} \to \mathcal{G}$ of $\mathcal{O}_X-$modules is a morphism of sheaves on X such that, for every open set $U \subseteq X$, the map $\mathcal{F}(U) \to \mathcal{G}(U)$ is a morphism of $\mathcal{O}_X(U)-$modules.

We obviously have the usual notions of kernel, image, quotient and even direct sum of $\mathcal{O}_X-$modules. An important construction is the tensor product of $\mathcal{O}_X-$modules. Let $\mathcal{F}$ and $\mathcal{G}$ be $\mathcal{O}_X-$modules, then $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$ is the sheafification of the presheaf

$$U \mapsto \mathcal{F}(U) \otimes_{\mathcal{O}(U)} \mathcal{G}(U).$$

Definition 1.1.19. *Let $(X, \mathcal{O}_X)$ be a ringed space and let $\mathcal{F}$ be an $\mathcal{O}_X-$module. We say that $\mathcal{F}$ is free it is isomorphic to a direct sum of copies of $\mathcal{O}_X$.*
We say that $\mathcal{F}$ is locally free if it can be covered by open sets U_i for which $\mathcal{F}|_{U_i}$ are free $\mathcal{O}_x|_{U_i}$-modules.

Suppose X is connected and $\mathcal{F}$ is a locally free sheaf on $(X, \mathcal{O}_X)$. Now let U be an open set that trivializes $\mathcal{F}$ i.e.

$$\mathcal{F}|_U \cong \bigoplus_{i=1}^{n} \mathcal{O}_X|_U,$$

then it is clear that n is constant on X and we say that X has rank n.

Definition 1.1.20. *Let $(X, \mathcal{O}_X)$ be a ringed space. A locally free sheaf of rank 1 on X is called an invertible sheaf.*

1.2 Modular forms

The aim of this section will be to define the the Riemann Surface

$$Y(N) := \Gamma(N)\backslash\mathbb{H}$$

and its natural compactification $X(N)$.

Definition 1.2.1. *The complex Upper Half Plane* $\mathbb{H}$ *is*

$$\mathbb{H} := \{z \in \mathbb{C} \mid Im(z) > 0\}.$$

The extended complex Upper Half Plane $\mathbb{H}^*$ *is the disjoint union*

$$\mathbb{H}^* := \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}.$$

We call the the elements of $\mathbb{P}^1(\mathbb{Q})$ cusps of $\mathbb{H}^*$.

Remark 1.2.1. *We define a topology on* $\mathbb{H}^*$*. For* $z \in \mathbb{H}$*, we take the usual neighborhoods contained in* $\mathbb{H}$*. For the cusp* ∞*, we take as a basis the neighborhoods*

$$\{z \in \mathbb{H} \mid Im(z) > M\} \quad \textit{for all } M \geq 0.$$

Finally, for the cusps $q \in \mathbb{Q}$*, we take the system of neighborhoods*

$$\{q\} \cup \{ \textit{ interior of the semi-circle of radius } r \textit{ around } q \textit{ in } \mathbb{H} \},$$

for all $r > 0$*.*

The group $SL_2(\mathbb{R})$ of 2 by 2 matrices with coefficients in $\mathbb{R}$ and with determinant 1 acts on $\mathbb{H}$ in the following way:

$$\text{For } \alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{R}), \text{ we define } \alpha z := \frac{az+b}{cz+d}\,.$$

The action (as a function) is well defined because of the formula

$$Im(\alpha z) = \frac{Im(z)}{|cz+d|^2}\,.$$

Now we also check that it is indeed a group action :

Let $\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $\beta = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ be elements of $Sl_2(\mathbb{R})$ then we have that

$$\begin{aligned} \beta(\alpha z) = \alpha\left(\frac{az+b}{cz+d}\right) &= \frac{a'\frac{az+b}{cz+d} + b'}{c'\frac{az+b}{cz+d} + d'} \\ &= \frac{a'az + a'b + b'cz + b'd}{c'az + c'd + d'cz + d'd} \\ &= \frac{(a'a + b'c)z + (a'b + b'd)}{(c'a + +d'c)z + (c'd + d'd)} \\ &= (\beta\alpha)(z)\ . \end{aligned}$$

We are interested in certain families of discrete subgroups of $SL_2(\mathbb{R})$. One in particular is

Definition 1.2.2. *The modular group is the subgroup $SL_2(\mathbb{Z})$ (also denoted $\Gamma(1)$) of $SL_2(\mathbb{R})$ defined as*

$$SL_2(\mathbb{Z}) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{R}) \mid a, b, c, d \in \mathbb{Z} \right\}.$$

In a similar fashion, we define for all $N \in \mathbb{N}_{>1}$, the subgroup

$$\Gamma(N) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \mid a, d \equiv 1 \ [mod\ N] \ \text{ and } \ b, c \equiv 0 \ [mod\ N] \right\}.$$

Remark 1.2.2. *Two examples of elements of $\Gamma(1)$ are $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ which corresponds to the map $z \mapsto z + 1$ and $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ which corresponds to $z \mapsto \frac{-1}{z}$.*

One can actually show that these generate the whole modular group i.e.

$$\Gamma(1) = \langle\, T, S \,\rangle.$$

A proof of this is given in [20, I.*1.6].*

The action of $\Gamma(N)$ on $\mathbb{H}$ can be extended to $\mathbb{H}^*$ in the following way : For $(x, y) \in \mathbb{P}^1(\mathbb{Q})$ and for $\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(N)$, we define

$$\alpha(a, b) := (ax + by, cx + dy).$$

This allows us to make sense of the classes of orbits

$$Y(N) := \Gamma(N)\backslash\mathbb{H}$$

and

$$X(N) := \Gamma(N)\backslash\mathbb{H}^*.$$

The elements of $X(N) - Y(N)$ are called the cusps of $\Gamma(N)$. For $N = 1$, one easily shows that the only cusp of $\Gamma(1)$ is the equivalence class of $[\infty]$. And because every $\Gamma(N)$ is a finite index subgroup of $\Gamma(1)$, it follows that $\Gamma(N)$ has finitely many cusps.

Both $Y(N)$ and $X(N)$ are given the quotient topology via the canonical projections

$$p : \mathbb{H} \to Y(N) \quad \text{and} \quad \tilde{p} : \mathbb{H}^* \to X(N).$$

One shows that both are Hausdorff spaces and that $X(N)$ is compact. Moreover, there is a natural complex structure on $Y(N)$ where meromorphic (resp. holomorphic) functions on $Y(N)$ correspond to meromorphic (resp. holomorphic) functions on $\mathbb{H}$ invariant under $\Gamma(N)$. In a similar fashion, a meromorphic (resp. holomorphic) functions on $X(N)$ correspond to meromorphic (resp. holomorphic) functions on $\mathbb{H}^*$ invariant under $\Gamma(N)$. The detailed proofs of these results can be found in Chapter 1 of [18].

Definition 1.2.3. *A modular function for $\Gamma(N)$ is a meromorphic function over $X(N)$, in other words it is a meromorphic function f on $\mathbb{H}^*$ verifying:*

1. $f(\alpha z) = f(z)$ *for all* $\alpha \in \Gamma(N)$.
2. *f is meromorphic at the cusps of* $\Gamma(N)$.

We make precise condition (2) above. We denote $\Gamma(1)_\infty$ the stabilizer of ∞ i.e.

$$\begin{aligned}
\Gamma(1)_\infty &:= \{\alpha \in \Gamma(1) \mid \alpha(\infty) = \infty\} \\
&= \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \mid \begin{bmatrix} a & b \\ c & d \end{bmatrix} (1,0) = (1,0)\} \\
&= \{\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \mid (a,c) = (1,0)\} \\
&= \{\begin{bmatrix} \pm 1 & b \\ 0 & \pm 1 \end{bmatrix} \mid b \in \mathbb{Z}\} \\
&\cong \{\pm 1\} \times \mathbb{Z}\,.
\end{aligned}$$

Because $\Gamma(N)_\infty$ is a subgroup of finite index of $\Gamma(1)_\infty$, there exists an element $\alpha \in \Gamma(N)$ such that

$$\alpha = \pm \begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix},$$

for some $h \in \mathbb{N}$. It follows from (1) that

$$f(z) = f(\alpha z) = f(z + h).$$

Hence f can be expressed as a Fourier series, i.e.

$$f(z) = f^*(q),$$

where $q = e^{\frac{2\pi i z}{h}}$ and $0 < |q| < r$ for some $r > 0$. We say that f is meromorphic (resp. holomorphic) at ∞ if f^* is meromorphic (resp. holomorphic) at 0. For other cusps $c \neq \infty$, we know that there exists $\gamma \in \Gamma(1)$ such that $c = \gamma(\infty)$, then the function g that maps

$$z \mapsto f(\gamma z)$$

is clearly meromorphic and invariant under $\gamma^{-1}\Gamma(N)\gamma$. We say that f is meromorphic (resp. holomorphic) at c if $f(\gamma z)$ is meromorphic (resp. holomorphic) at ∞.

Example 1.2.1. *The group $\Gamma(1)$ is generated by S and T. Therefore a meromorphic function $f : \mathbb{H} \to \mathbb{C}$ is a modular function over $\Gamma(1)$ if*

1. $f(z + 1) = f(z)$.
2. $f(-1/z) = f(z)$.
3. $f(z) = f^*(q) = \sum_{m \geq -M} a_m q^m$ *where* $q = e^{2\pi i z}$.

Definition 1.2.4. *A modular form of weight k for $\Gamma(N)$ is a holomorphic function f on $\mathbb{H}^*$ verifying:*

1. $f(\alpha z) = (cz + d)^k f(z)$ *for all* $z \in \mathbb{H}$ *and* $\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(N)$.
2. *f is holomorphic at the cusps of $\Gamma(N)$.*

From (1), it follows that $f(z + h) = f(z)$ for some $h > 0$. This allows us, as in the case of modular functions, to define holomorphy at the cusps.

If we replace the conditions about holomorphy over $\mathbb{H}$ and the cusps by simply imposing that the function is meromorphic at these points, we get the notion of a weakly modular form (or simply meromorphic modular form).

Remark 1.2.3. *We gave a clear analytic geometric descriptions for meromorphic (resp. holomorphic) modular functions over $\Gamma(N)$ as meromorphic (resp. holomorphic) functions over $X(N)$. We also have a geometric interpretation of modular forms of arbitrary weight. This will be the inspiration for generalizing modular forms to arbitrary rings in Chapter 3.*

Let $k \in \mathbb{Z}$. Consider a $k-$fold differential

$$\omega = f(z)(dz)^k$$

on $\mathbb{H}$ where f is a meromorphic function over $\mathbb{H}$ and the product of dz is the tensor product. One might ask the question :

Under which restriction on f is ω invariant under the action of $\Gamma(N)$?

In other words, we want that for all $\lambda = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(N)$,

$$f(\lambda z)(d\lambda z)^k = f(z)(dz)^k.$$

On the right-hand side, we have

$$\begin{aligned} f(\lambda z)(d\lambda z)^k &= f(\lambda z)((\lambda z)' dz)^k \\ &= f(\lambda z)\left((\lambda z)'\right)^k (dz)^k \\ &= f(\lambda z)\left(\left(\frac{az+b}{cz+d}\right)'\right)^k (dz)^k \\ &= f(\lambda z)\left(\frac{1}{(cz+d)^{2k}}\right)(dz)^k . \end{aligned}$$

It follows that

$$f(\lambda z) = (cz+d)^{2k} f(z) .$$

Hence, a geometric interpretation for (meromorphic) modular forms of weight $2k$ is as $\Gamma(N)-$invariant $k-$fold differential forms over $\mathbb{H}^*$ or simply $k-$fold differential forms over $X(N)$.

1.3 Elliptic curves over the Complex numbers

In this section, we relate the modular curve $X(1)$ to the classification of elliptic curves. We cover in details the complex case in order to motivate the more general Chapter 2.

Let Λ be a lattice in $\mathbb{C}$ i.e. a discrete subgroup of $\mathbb{C}$ that contains an $\mathbb{R}-$basis for $\mathbb{C}$. Every lattice is of the form

$$\Gamma = \omega_1\mathbb{Z} + \omega_2\mathbb{Z},$$

where ω_1 and ω_2 are non-zero elements of $\mathbb{C}$ s.t. $\omega_2/\omega_1 \notin \mathbb{R}$.

Let Λ_1 and Λ_2 be two lattices in $\mathbb{C}$. Morphisms $\Lambda_1 \to \Lambda_2$ are $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 \subseteq \Lambda_2.$$

This gives us a category that we will denote **Latt**. We say that two lattices Λ_1 and Λ_2 are homothetic if they are isomorphic in **Latt** i.e. there exists $\alpha \in \mathbb{C}$ such that

$$\alpha\Lambda_1 = \Lambda_2.$$

We usually denote homothetic lattices by the symbol $\Lambda_1 \sim \Lambda_2$.

To a lattice $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, we can associate a connected fundamental domain

$$D := \{t_1\omega_1 + t_2\omega_2 \mid 0 \leq t_1, t_2 < 1\}.$$

This gives a natural bijection $D \to \mathbb{C}/\Lambda$.

Definition 1.3.1. *Let Λ be a lattice. An elliptic function relative to Λ is a meromorphic function $f : \mathbb{C} \to \mathbb{C}$ that verifies :*

$$f(z+\omega) = f(z), \qquad \text{for all } z \in \mathbb{C} \text{ and } \omega \in \Lambda.$$

It is clear that a holomorphic modular function is constant because it is clearly bounded over $\mathbb{C}$ and hence constant (by Liouville's Theorem). More generally, we have that

Theorem 1.3.1. *Let f be an elliptic function relative to a lattice Λ. We have that*

1. $\sum_{\omega \in \mathbb{C}/\Lambda} res_\omega(f) = 0.$
2. $\sum_{\omega \in \mathbb{C}/\Lambda} ord_\omega(f) = 0.$
3. $\sum_{\omega \in \mathbb{C}/\Lambda} ord_\omega(f)\,\omega \in \Lambda.$

Proof: These are various consequences of the Residue Theorem. The details can be found in [19, VI.2.2] ∎

Definition 1.3.2. *The order of an elliptic function over Λ is the number of poles (with multiplicities) in a fundamental parallelogram of Λ.*

An implication of the above theorem is that every non-constant elliptic function f has order at least 2. Indeed, suppose f has exactly one pole ω (with multiplicity), then it follows from (1) of the above theorem that

$$res_{\omega}(f) = 0.$$

Hence f is holomorphic at ω and therefore over all $\mathbb{C}$, making it constant by Liouville's theorem.

In the following few results, we describe an important family of non-constant elliptic functions.

Definition 1.3.3. *Let $\Lambda \subseteq \mathbb{C}$ be a lattice. The Weierstrass $\wp$-function associated to Λ is given by the series*

$$\wp_{\Lambda}(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \Big(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \Big).$$

If Λ is clear from the context, we might just write $\wp(z)$. We have the following theorem about the Weierstrass function:

Theorem 1.3.2. *Let Λ be a lattice in $\mathbb{C}$. The Weierstrass $\wp$ function is an even elliptic function of order 2 having a double pole with residue 0 exactly at the lattice points.*

Proof: A proof of this result can be found in [19, VI.3.1], ∎

For a fixed lattice Λ, it is clear that the set of elliptic functions with respect to Λ is a field which we denote by $\mathbb{C}(\Lambda)$. It clearly contains the constant functions $\mathbb{C}$ and the Weierstrass $\wp$-functions with all its derivatives. Actually, we have the much stronger result :

Theorem 1.3.3. *Let Λ be a lattice, we have*

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp, \wp').$$

Proof: This is proved in [19, VI.3.2]. ∎

It is obvious that $\wp''$ is an elliptic function. Hence, the above theorem indicates that there is an algebraic description of $\wp''$ as a rational function of $\wp$ and $\wp'$. We want to give this description explicitly.

To have a better understanding of $\wp$, we expand it as a Laurent series around $z = 0$. We get the following result.

Theorem 1.3.4. *Let Λ be a lattice in $\mathbb{C}$. The Laurent expansion of $\wp$ at $z = 0$ is*

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(\Lambda)z^{2n},$$

where $G_{2k}(\Lambda)$ is called the Eisenstein series of weight $2k$ for Λ and is defined as

$$G_{2k}(\Lambda) = \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \frac{1}{\omega^{2k}}.$$

Proof: We fix a lattice Λ. For z small enough (precisely $|z| < |\omega|$ for all $\omega \neq 0$ in the lattice), we have that

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(1-z/\omega)^2} - 1\right) = \sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}}.$$

Therefore

$$\begin{aligned}
\wp(z) &= \frac{1}{z^2} + \sum_{\omega\neq 0}\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}} \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty}\sum_{\omega\neq 0}(n+1)\frac{z^n}{\omega^{n+2}} \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty}\Big(\sum_{\omega\neq 0}\frac{1}{\omega^{n+2}}\Big)(n+1)z^n \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty}\Big(\sum_{\omega\neq 0}\frac{1}{\omega^{2n+2}}\Big)(2n+1)z^{2n} \\
&= \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}z^{2n}.
\end{aligned}$$

Let us fix a lattice Λ. Now if we write explicitly the first terms of the Laurent expansions of

$$\begin{aligned}\wp'(z)^2 &= 4z^{-6} - 24G_4 z^{-2} - 80G_6 + \dots \\ \wp(z)^3 &= z^{-6} + 9G_4 z^{-2} + 15G_6 + \dots \\ \wp(z) &= z^{-2} + 3G_4 z^2 + \dots\end{aligned}$$

Combining these terms, we find that the elliptic function f, defined as

$$f := \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z),$$

has no poles at 0 hence no poles at the points of the lattice. Now recall that $\wp$ had already no poles away from Λ then so does f. This shows that f is holomorphic and therefore constant with value

$$f(z) = f(0) = -140G_6.$$

As a standard notation, we usually write

$$g_2 = g_2(\Lambda) = 60G_4(\Lambda) \quad \textit{and} \quad g_3 = g_3(\Lambda) = 140G_6(\Lambda).$$

Thus, f being equal to $-g_3$, we have an equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

This looks indeed like the equation of an elliptic curve. Furthermore

Theorem 1.3.5. *Let Λ be a lattice in $\mathbb{C}$, then the curve*

$$E : y^2 = 4x^3 - g_2 x - g_3$$

is an elliptic curve over $\mathbb{C}$. Moreover, the map

$$\begin{aligned}\phi : \mathbb{C}/\Lambda &\to E(\mathbb{C}) \subseteq \mathbb{P}^2(\mathbb{C}) \\ z &\mapsto [\wp(z) : \wp'(z) : 1] \\ 0 &\mapsto [0 : 1 : 0]\end{aligned}$$

is an isomorphism of Riemann Surfaces and a group homomorphism.

Proof: A proof of this theorem can be found in [19, VI.5.1.1]. ∎

We just showed that every lattice Λ in $\mathbb{C}$ induces, in a natural way, an elliptic curve $E_\Lambda(\mathbb{C})$. Moreover, the Uniformization Theorem [18, IV.2] states that every elliptic curve $E(\mathbb{C})$ is given by some lattice Λ i.e. that $E(\mathbb{C}) \cong E_\Lambda(\mathbb{C})$ for some lattice Λ. We actually have an even stronger result :

Theorem 1.3.6. *There is an equivalence of Categories*

$$\left\{ \begin{array}{l} \textit{Objects: Elliptic curves over } \mathbb{C} \\ \textit{Maps: Isogenies} \end{array} \right\} \Longleftrightarrow \left\{ \begin{array}{l} \textit{Objects: Lattices over } \mathbb{C} \textit{ up to homothety} \\ \textit{Maps: Morphisms of lattices} \end{array} \right\}$$

Proof: A proof is given in [19, VI.5.3] ∎

The above theorem says that in order to understand elliptic curves over $\mathbb{C}$, it suffices to study lattices. We denote by $\mathcal{L}$ the set of lattices in $\mathbb{C}$ and by $\mathcal{L}/\mathbb{C}^*$ their set of homothety classes.

Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$. We assume that

$$Im(\frac{\omega_2}{\omega_1}) > 0.$$

If not then we switch ω_1 and ω_2. We have that

$$\begin{aligned} \Lambda &= \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \\ &= \omega_2(\mathbb{Z}\frac{\omega_1}{\omega_2} + \mathbb{Z}) \\ &\sim \mathbb{Z}\frac{\omega_1}{\omega_2} + \mathbb{Z}. \end{aligned}$$

This shows that we have a surjective map

$$\begin{aligned} \mathbb{H} &\to \mathcal{L}/\mathbb{C}^* \\ \tau &\mapsto [\mathbb{Z}\tau + \mathbb{Z}]. \end{aligned}$$

This function is clearly not injective, however we have the following result:

Proposition 1.3.1. *Let τ and τ' be elements of $\mathbb{H}$. Then τ and τ' have the same image in the above map if and only if there exists an element $\gamma \in \Gamma(1)$ such that $\gamma\tau = \tau'$.*

Proof: Indeed, if τ and τ' induce the same lattice (up to homothety) i.e. there exists $\mu \in \mathbb{C}^*$ such that

$$\mathbb{Z}\tau + \mathbb{Z} = \mathbb{Z}\mu\tau' + \mathbb{Z}\mu.$$

This implies that

$$\tau = a\mu\tau' + b\mu \quad \text{and} \quad 1 = c\mu\tau' + d\mu,$$

for some $a, b, c, d \in \mathbb{Z}$. Therefore

$$\tau = \frac{a\tau' + b}{c\tau' + d},$$

where $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is an invertible matrix i.e. it has determinant ± 1. Since

$$Im(\tau) = \frac{(ad - bc)Im(\tau')}{|c\tau' + d|^2},$$

we conclude that $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma(1)$.

It is easy to see that this is a sufficient condition. Indeed, if $\tau' = \frac{a\tau+b}{c\tau+d}$ then

$$\mathbb{Z}\tau' + \mathbb{Z} \sim (c\tau + d)(\mathbb{Z}\tau' + \mathbb{Z}) = \mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d).$$

Now $d(a\tau+b)-b(c\tau+d) = \tau$ and $-c(a\tau+b)+a(c\tau+d) = 1$. Therefore

$$\mathbb{Z}\tau + \mathbb{Z} \subseteq \mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d).$$

Similarly

$$\mathbb{Z}(a\tau + b) + \mathbb{Z}(c\tau + d) \subseteq (\mathbb{Z}a + \mathbb{Z}c)\tau + (\mathbb{Z}b + \mathbb{Z}d) = \mathbb{Z}\tau + \mathbb{Z},$$

because $\gcd(a, c) = \gcd(b, d) = 1$. We conclude that

$$\mathbb{Z}\tau' + \mathbb{Z} \sim \mathbb{Z}\tau + \mathbb{Z}.$$

∎

Remark 1.3.1. *It follows from the proposition that we have a bijection*

$$\begin{aligned} Y(1) := \Gamma(1)\backslash\mathbb{H} &\to \mathcal{L}/\mathbb{C}^* \\ [\tau] &\mapsto [\mathbb{Z}\tau + \mathbb{Z}]. \end{aligned}$$

In other words, by Theorem 1.3.6*, there is a correspondence between "points" of* $Y(1)$ *and isomorphism classes of elliptic curves over* $\mathbb{C}$*.*

Now recall that one way of looking at modular functions and modular forms is as meromorphic functions and invariant differentials over the "compactification" of $Y(1)$ *(and more generally* $Y(N)$*). This way of looking at modular forms is the key to generalize them to arbitrary rings (and even schemes). This will be done in details in the following chapters.*

Chapter 2

Elliptic curves and their Moduli

2.1 Cartier divisors

In this section, we will introduce the notion of Cartier divisor necessary for developing the general theory of elliptic curves. We will mainly follow the first chapter of [13] and the second chapter of [8] using various result of algebraic geometry from various sources but mainly [7].

Let us fix an arbitrary scheme S and let X be a scheme over S.

Definition 2.1.1. *An effective Cartier divisor of X over S is an S-morphism of sheaves $i : D \to X$ such that*

1. *The morphism $i : D \to X$ is a closed immersion.*
2. *D is flat over S.*
3. *The induced ideal sheaf $I(D)$ is an invertible O_X-module.*

The three condition $(1-3)$ are local on the target. Hence, this will allow us to reduce many of the questions about effective Cartier divisors to the affine case.

Proposition 2.1.1. *Let $S = Spec(R)$ be an affine scheme and X a scheme over S. If $D \to X$ is a closed subscheme then the following statements are equivalent:*

1. *D is an effective Cartier divisor.*
2. *For all $x \in D$, there exists an affine neighborhood $U = Spec(A) \subseteq X$ such that*

$$U \cap D = Spec(A/(f)),$$

where f is not a zero-divisor and $A/(f)$ is a flat R-module.

Proof: We start by showing that (1) $\implies$ (2). If we are given an effective Cartier divisor D of X over S, then the canonical exact sequence on X

$$0 \longrightarrow I(D) \longrightarrow O_X \longrightarrow O_D \longrightarrow 0$$

becomes, when restricted to a neighborhood $U = Spec(A)$ of x and after applying the global sections functor, an exact sequence

$$0 \longrightarrow A \xrightarrow{f} A \longrightarrow A/fA \longrightarrow 0,$$

where the inclusion map is determined by f the image of 1. Hence $D \cap U = Spec(A/fA)$ and we immediately see that

1. f is not a zero-divisor (because $A \to A$ is injective).
2. A_i/f_iA_i is flat over R (flatness being local).

We now show that (2) $\implies$ (1). Suppose we have $D \to X$ is closed subscheme that has an affine open covering in X denoted $\{U_i = Spec(A_i)\}_{i\in I}$ such that $D \cap U_i = Spec(A_i/f_iA_i)$ where f_i verifies properties 1 and 2 above.

Then $\{U_i\}_{i\in I} \cup (X - D)$ is an open covering of X and

$$I(D)|_{U_i} \cong \widetilde{f_iA_i} \cong \tilde{A}_i \cong O_X|_{U_i}.$$

Obviously

$$I(D)|_{X-D} = O_X|_{X-D},$$

proving that $I(D)$ is an invertible sheaf. Finally, we recall that flatness is local on the source and that

$$O_D|_{U_i} \cong Spec(A_i/f_iA_i)$$

is flat over S. Hence D is an effective Cartier divisor. ∎

Whenever we have an effective Cartier divisor $i : D \to X$ or more generally a closed immersion, we have a canonical exact sequence of sheaves on X

$$0 \longrightarrow I(D) \longrightarrow O_X \longrightarrow O_D \longrightarrow 0,$$

where we identify O_D with i_*O_D. Now we tensor the above exact sequence with the invertible sheaf $I(D)^{-1}$ and we get an exact sequence

$$0 \longrightarrow O_X \xrightarrow{l_D} I(D)^{-1} \longrightarrow O_D \otimes I(D)^{-1} \longrightarrow 0,$$

where l_D is a global section of $I(D)^{-1}$ and the image of "1" in the inclusion $O_X \to I(D)^{-1}$.

Definition 2.1.2. *Let X be a scheme and L an invertible sheaf over X. We call a global section l on L regular if l induces an injection $O_x \to L$ where $1 \mapsto l$ (in other term l corresponds affine locally to multiplication by an element that is not a zero divisor).*

This gives a map of sets

$$\{ \text{ Effective Cartier divisors on } X/S \} \to \left[(L,l) \mid \begin{array}{l} L \text{ invertible sheaf on } X \text{ and} \\ l \text{ regular global section on } L \end{array} \right]_{\sim}$$

where D is mapped to $[I(D)^{-1}, l_D]$. The equivalence relation is

$$(L,l) \sim (L^{'}, l^{'}) \iff L \cong_{\phi} L^{'} \text{ and } \phi(l^{'}) = ul \quad \text{for some } u \in H^0(X,L)^{\times}.$$

One can check that this map is injective and if one drops the flateness condition for effective Cartier divisors, one actually gets a bijection as shown in [8, p. 107] . The inverse image maps (L,l) to the topological space $D = Supp(L/lO_X)$ and sheaf $O_D = L/O_X \otimes_{O_X} L^{-1}$.

2.2 Properties of effective Cartier divisors

Now suppose we are given two effective Cartier divisors D and $D^{'}$ in X/S. Suppose that D is affine locally given by (U_i, f_i) and $D^{'}$ is given by (U_i, g_i) as in Proposition 2.1.1. We define the sum $D + D^{'}$ as the closed subscheme induced by the ideal sheaf $I(D)I(D^{'})$. This is clearly invertible as

$$I(D)I(D^{'}) := I(D) \otimes_{O_X} I(D^{'}).$$

Now both injections $i : O(D) \to O_X$ and $j : O(D^{'}) \to O_X$ induce a morphism

$$I(D) \otimes_{O_X} I(D^{'}) \to O_X \otimes_{O_X} O_X \cong O_X,$$

which affine locally corresponds to

$$A_i \xrightarrow{f_i g_i} A_i.$$

Now we know that f_i and g_i are not zero-divisors then so is $f_i g_i$. Moreover, we have a canonical exact sequence of R-modules

$$0 \longrightarrow A/(f_i) \xrightarrow{\times g_i} A/(f_i g_i) \longrightarrow A/(g_i) \longrightarrow 0.$$

exhibiting $A/(f_i g_i)$ as an extension of flat modules hence it is also flat [7, p 254]. This shows that $D + D^{'}$ is indeed an effective Cartier divisor.

From the point of view of invertible sheaves and regular sections, the notion of adding effective Cartier divisor is non-other than the usual operation we have on invertible sheaves i.e.

$$D + D' = (L, l) + (L^{'}, l') := (L \otimes L', l \otimes l')$$

It is immediate that $l \otimes l'$ is regular (locally it corresponds to product of non-zero-divisors) and the map is well defined.

Remark 2.2.1. *The above discussion allows us to relate the notion of effective Cartier divisors to the classical Cartier divisors on a scheme. As in [7, p 141], a Cartier divisor on a scheme X can be described as an affine cover $U_i = Spec(A_i)_{i\in I}$ of X and to each U_i we associate an element $f_i = \frac{a_{i,1}}{a_{i,2}}$ in the total quotient ring of A such that*

$$\frac{f_i}{f_j} \in H^0(U_i \cap U_j, O_X^{\times}).$$

One can show that any Cartier divisor D on X/S can be written as the difference of two effective Cartier divisors [8, p 108] i.e

$$D = D_1 - D_2 \quad \textit{where } D_1 \textit{ and } D_2, \textit{ are effective Cartier divisors.}$$

Lemma 2.2.1. *Let $T \to S$ be a morphism of schemes and let D be an effective Cartier divisor on X over S. We have the following:*

1. *The base change morphism is $D_T \to X_T$ is an effective Cartier divisor.*
2. *If $f : Y \to X$ is a flat morphism of S-schemes then the pullback $f^*(D)$ is also an effective Cartier divisor on Y over S.*

Proof: A proof of both these results is given in [10, p 5]. ∎

We state a criteria that will help us determine whenever a given closed subscheme is actually an effective Cartier divisor.

Proposition 2.2.1. *Let X be a flat scheme of finite type over a locally noetherian scheme S. Let $D \to X$ be a closed subscheme, then the following statements are equivalent.*

1. *$D \to X$ is an effective Cartier divisor.*
2. *For all geometric points $s : Spec(k) \to S$, the morphism*

$$D \otimes Spec(k) \to X \otimes Spec(k)$$

is an effective Cartier divisor over k.

Proof: A proof can be found in [10, p 7]. ∎

Whenever we have a morphism $X \to A$ of finite presentation and we want to show a property P of this morphism that we know is stable under base change, we can reduce the problem to showing the property P for a scheme X of finite type over a noetherian ring. This is a technical result proven by Grothendieck, rigorously stated:

Lemma 2.2.2. *Let A be a ring and X be a scheme over A. The following statements are equivalent :*

1. *X is finitely presented over A.*
2. *There exists a noetherian ring A_0, a scheme X_0 of finite type over A_0 and a ring morphism $A_0 \to A$ such that we have an isomorphism*

$$X \cong X_0 \otimes_{A_0} A.$$

Proof: Grothendieck shows this in [6, prop 8.9.1]. ∎

Now we go back to the theory of Cartier divisors in the case of smooth curves.

Definition 2.2.1. *A smooth curve C/S is a morphism of schemes $C \to S$ which is separated, smooth, of finite presentation and of relative dimension* 1.

Proposition 2.2.2. *Let C/S be a smooth curve. Then any section $s : S \to C$ is an effective Cartier divisor.*

Proof: We know that every section of a separated morphism of schemes is a closed immersion [4, Corr 5.4.6] but it is not necessarily a Cartier divisor.

The notion of effective Cartier divisor is local on S so let us take $S = Spec(R)$. Furthermore, because $C \to R$ is of finite presentation, we can assume by the lemma 2.2.2 that R is noetherian. Now proposition 2.2.1 allows us to reduce to the case where k is an algebraically closed field. Hence we work with a smooth curve over k. We only have to show that $I(s)$ is an invertible sheaf.

Let $Spec(A)$ be an irreducible neighborhood in X. A is a domain because it is irreducible and reduced (smooth $\implies$ reduced), it is also of Krull dimension 1 and it is a finitely generated k-algebra hence noetherian. Finally, because a smooth morphism implies regular geometric fibers, A is a regular domain and therefore it is integrally closed. By definition

$$\text{Dimension 1} + \text{Noetherian} + \text{Integrally closed} \iff \text{Dedekind.}$$

We conclude that A is a Dedekind domain. We recall the canonical exact sequence

$$0 \longrightarrow I(s) \longrightarrow O_X \longrightarrow O_s \longrightarrow 0.$$

In $X - \{s\}$ the result is trivial. But, when restriction to A then to s (we think of it as maximal ideal), the sequence becomes

$$0 \longrightarrow I(s)_s \longrightarrow A_s \longrightarrow k \longrightarrow 0$$

Therefore it is clear that $I(s)_s = mA_s$ is the maximal ideal of A_s. Now, because A is Dedekind and therefore A_s is a discrete valuation ring, the maximal ideal mA_s is principal and therefore there exists $a \in A_s$ such that

$$mA_s = aA_s,$$

making mA_s a free A_s-module of rank 1.

∎

When the effective Cartier divisor D is proper (as a morphism $D \to S$), we have an even stronger result:

Proposition 2.2.3. *Let $C \to S$ be a smooth curve and let $D \to C$ be a closed immersion. The following statements are equivalent :*

1. *$D \to S$ is finite, flat and of finite presentation.*
2. *$D \to S$ is a proper effective Cartier divisor in C/S.*

Proof: This is shown in [13, p 8]. ∎

In particular, if $C \to S$ is proper then every effective Cartier divisor is proper because closed immersion are proper and

$$D \to C \to S$$

is the composition of a proper morphism hence is itself proper.

This allows to define the degree of proper effective Cartier divisors. This notion is going to be, by definition, local on S. So let $S = Spec(R)$ be an affine scheme.

Definition 2.2.2. *Let $C \to S$ be a smooth curve and D a proper effective Cartier divisor on C/S. Then we call degree of D and denote $deg(D)$ the rank of the locally free R-module M defined by $D = Spec(M)$.*

This definition indeed makes sense. Because $S = Spec(R)$ is affine and $D \to S$ is finite hence $D = Spec(M)$ is also affine making M is a finitely generated R-module which is flat hence is locally free.

Proposition 2.2.4. *Let C/S be a smooth curve and let D_1 and D_2 two effective Cartier divisors proper over S. The following statements are true:*

1. *The effective Cartier divisor $D_1 + D_2$ is proper over S and*

$$deg(D_1 + D_2) = deg(D_1) + deg(D_2).$$

2. *If C' is another smooth curve over S and*

$$f : C' \to C$$

is a finite flat S-morphism of degree $deg(f)$ then $f^*(D)$ is an effective Cartier divisor on C'/S that is also proper over S, moreover

$$deg(f^*(D)) = deg(f)deg(D).$$

3. *Let $T \to S$ be a morphism of schemes, then $D_T := D \otimes_S T$ is an effective Cartier divisor in C_T which is proper over T and*

$$deg(D_T) = deg(D).$$

Proof: All these results can be found in [13, p 11] ∎

Remark 2.2.2. *Whenever C/S is proper, one can extend the notion of the degree to the set $Div(C/S)$. By Remark* 2.2.1 *and Proposition* 2.2.4*, it makes sense to define*

$$deg(D) = deg(D_1) - deg(D_2),$$

where $D = D_1 - D_2$ and D_1, D_2 are effective Cartier divisors.

When k is a field, the classical notion of degree of a divisor of a curve, as introduced in [19], is equivalent to the degree introduced above.

Proposition 2.2.5. *Let C/S be a smooth curve. Let $[s] : S \to C$ be section of $C \to S$, the induced effective Cartier divisor is proper and of degree* 1*.*

Moreover, any effective Cartier divisor $D \to C$ over D which is proper and of degree 1 *is equal to $[s]$ for a section $s : S \to C$.*

Proof: An S-morphism of schemes $S \to C$ induces a commutative diagram

$$\begin{array}{ccc} S & \longrightarrow & C \\ & \searrow^{id} & \downarrow \\ & & S \end{array}$$

From this the result is obvious as the identity morphism $id : S \to S$ is trivially proper and of degree 1.

For the second part of the proposition, we have a commutative diagram

$$\begin{array}{ccc} D & \longrightarrow & C \\ & \searrow & \downarrow \\ & & S \end{array}$$

Affine locally on S, the morphism $D \to S := Spec(A)$ is affine as shown in Proposition 2.2.3. Therefore there exists a ring M such that $D = Spec(M)$. M is both an A-algebra (therefore $M \cong M \otimes_R M$) and an invertible R-modules (hence there exists an R-module M' such that $M \otimes_R M' \cong R$) and so

$$M \cong M \otimes_R R \cong M \otimes_R M \otimes_R M' \cong M \otimes_R M' \cong R,$$

which shows that $D \cong S$ as schemes and hence $D \to C$ actually corresponds to an element in $C(S)$.

∎

2.3 Elliptic curves over general schemes

Elliptic curves (and more generally abelian varieties) are specific elements of a bigger class of objects called group schemes.

Definition 2.3.1 (Group Scheme)**.** *Let S be scheme. A group scheme over S is an S-scheme G equipped with a S-morphisms $m : G \times_S G \to G$, $i : G \to G$ and $e_G : S \to G$ verifying the group axioms i.e. the following diagrams commute:*

1. *Identity element*

$$\begin{array}{ccc} S \times_S G & \xrightarrow{e_g \times 1} & G \times_S G \\ & \searrow^{p_2} & \downarrow m \\ & & G \end{array} \qquad \begin{array}{ccc} G \times_S S & \xrightarrow{1 \times e_G} & G \times_S G \\ & \searrow^{p_1} & \downarrow m \\ & & G \end{array}$$

2. *Inverse element*

$$\begin{array}{ccccc} G \times_S G & & \xrightarrow{1 \times i} & & G \times_S G \\ {\scriptstyle \Delta_S}\uparrow & & & & \downarrow m \\ G & \longrightarrow & S & \xrightarrow{e_G} & G \end{array} \qquad \begin{array}{ccccc} G \times_S G & & \xrightarrow{i \times 1} & & G \times_S G \\ {\scriptstyle \Delta_S}\uparrow & & & & \downarrow m \\ G & \longrightarrow & S & \xrightarrow{e_G} & G \end{array}$$

   where $\Delta_G : G \to G \times_S G$ is the diagonal morphism.

3. *Associativity of the multiplication*

$$\begin{array}{ccc} G \times_S G \times_S G & \xrightarrow{m \times 1} & G \times_S G \\ \downarrow 1 \times m & & \downarrow m \\ G \times_S G & \xrightarrow{m} & G \end{array}$$

A morphism of group S-schemes from G to H is a morphism $\phi : G \to H$ of S-schemes that is compatible with both multiplication maps on G and H i.e. making the following diagram commutes

$$\begin{array}{ccc} G \times_S G & \xrightarrow{\phi \times \phi} & H \times_S H \\ \downarrow m_G & & \downarrow m_H \\ G & \xrightarrow{\phi} & H \end{array}$$

Example 2.3.1.

1. *The additive group scheme $\mathbb{G}_a$ over $\mathbb{Z}$ is defined as $Spec(\mathbb{Z}[x]) \to Spec(\mathbb{Z})$. In this case, the group addition is a map of schemes*

$$m : \mathbb{G}_a \times_{\mathbb{Z}} \mathbb{G}_a \to \mathbb{G}_a,$$

where

$$\mathbb{G}_a \times_{\mathbb{Z}} \mathbb{G}_a = Spec(\mathbb{Z}[x]) \times_{\mathbb{Z}} Spec(\mathbb{Z}[x]) = Spec(\mathbb{Z}[x] \otimes_{\mathbb{Z}} \mathbb{Z}[x]) = Spec(\mathbb{Z}[x, y]).$$

Hence, $m : Spec(\mathbb{Z}[x, y]) \to Spec(\mathbb{Z}[z])$ is the map of schemes induced by the ring homomorphism $\mathbb{Z}[z] \to \mathbb{Z}[x, y]$ that maps $z \mapsto x + y$.

More generally the group scheme $\mathbb{G}_{a/S}$ over an arbitrary scheme S is defined as $\mathbb{G}_a \times_{\mathbb{Z}} S$.

2. *Similarly, we define the multiplicative group scheme $\mathbb{G}_m$ over $\mathbb{Z}$ as*

$$Spec(\mathbb{Z}[x, x^{-1}]) \to Spec(\mathbb{Z}).$$

The group multiplication is defined in a similar fashion as for $\mathbb{G}_a$. Also we define $\mathbb{G}_{m/S}$ over an arbitrary scheme S simply as $\mathbb{G}_m \times_{\mathbb{Z}} S$.

3. *When G is both a variety and a group scheme over a field k, we call it a group variety. An elliptic curve E/k (and more generally an abelian variety) is an example of a commutative group variety.*

Let S be an arbitrary scheme.

Definition 2.3.2. *An elliptic curve is a proper smooth curve $f : E \to S$ such that*

1. *It has a section $0 : S \to E$.*
2. *The curve is fiber by fiber connected.*
3. *For all geometric points $s \in S$, we have an isomorphism*

$$f_* \Omega_{E_s/s} \cong k(s).$$

In other words, E has genus equal to 1.

We start with a few cohomological results that will turn out to be crucial in studying elliptic curves over arbitrary schemes. We will start with general results due to Grothendieck.

Theorem 2.3.1. *Let $f : X \to S$ be a proper morphism of noetherian schemes and let F be a coherent sheaf on X. For all $i \in \mathbb{N}$, the sheaf $R^i f_* F$ is coherent.*

Proof: This is shown in [5, 3.2.1]. ∎

Theorem 2.3.2. *Let $f : X \to Y$ be a proper morphism of noetherian schemes and let F be a coherent sheaf on X flat over Y. Let $y \in Y$ and denote by X_y the fiber of f over y and by $F(y)$ the pullback of F under $X_y \to X$. Them we have the following*

1. *If the the base change map [7,* III *12.5]*

$$\phi_p(y) := R^p f_* F \otimes k(y) \to H^p(X_y, F(y))$$

is surjective, then it is an isomorphism.

2. *Moreover, whenever $\phi_p(y)$ is surjective, we have that*

$$\phi_{p-1}(y) \text{ is surjective } \iff R^p f_* F \text{ is a free sheaf in a neighborhood of } y.$$

If the above conditions hold for all $y \in Y$, then the formation of $R^p f_* F$ commutes with arbitrary base changes.

Proof: A detailed proof of this result is presented in this paper [21]. ∎

We apply this theorem to prove some cohomological statements about elliptic curves. Let $E \to S$ be an elliptic curve:

Lemma 2.3.1. *Let L be an invertible sheaf on E which is fiber by fiber of degree* 1*, then*

1. *$R^1 f_* L = 0$.*
2. *$f_* L$ is an invertible sheaf on S compatible with base change.*

Proof: Let $y \in S$. By Serre's duality [7, III.7],

$$H^1(E_s, L(y)) \quad \text{is dual to} \quad H^0(E_s, L(y)^{-1} \otimes \Omega_{E_y/y}).$$

Now, by the Riemann-Roch theorem [12, Ch 7.3],

$$H^0(E_s, L(y)^{-1} \otimes \Omega_{E_y/y})$$

vanishes because $Deg(L(y)^{-1} \otimes \Omega_{E_y/y}) < 0$. Therefore

$$H^1(E_s, L(y)) = 0.$$

We conclude, by Theorem 2.3.2, that

$$R^1 f_* L \otimes k(y) = 0.$$

Affine locally, a basis of the $k(y)$-vector space $R^1 f_* L \otimes k(y)$ extends to $O_{Y,y}$-module $R^1 f_* L$ (Nakayama's lemma) hence, for all $y \in Y$, we have that $(R^1 f_* L)_y = 0$. We conclude that

$$R^1 f_* L = 0.$$

Now we apply the second part of the Theorem twice. When $p = 1$, we get that $\phi_0(y)$ is surjective. Now with $p = 0$, we have that

$$\phi_{-1}(y) \text{ is surjective } \iff f_* F \text{ is a free sheaf in a neighborhood of } y.$$

The right hand side is trivially true because $H^i(-)$ vanishes for $i < 0$. Hence we conclude that $f_* L$ is locally free and with formation compatible with base change. To check that the rank of $f_* L$ over S is one, we look at a change of bases with a geometric section $\bar{k}(y) \to S$. We have that

$$f_* L(y) \cong H^0(E_y, L(y)) \cong \bar{k}(y),$$

where the first isomorphism is part one of the above theorem and the second isomorphism follows from the Riemann-Roch theorem.

∎

Theorem 2.3.3. *Let $f : E \to S$ be an elliptic curve, then E/S has a unique structure of a commutative group scheme having $0 : S \to E$ as the identity such that, for any S-scheme T and any points A, B and C is $E_T(T) := (E \times_S T)(T)$, we have*

$$A + B = C \iff I(A)^{-1} \otimes I(B)^{-1} \otimes I(O) \cong I(C)^{-1} \otimes f_T^* L_0,$$

for some L_0 an invertible sheaf over T.

Proof: Let $Pic^{(1)}(E_T/T)$ denote the set of isomorphism classes of invertible sheaves L on E_T which are of degree 1 (fiber-by-fiber) modulo the equivalence

$$L \sim L \otimes f_T^*(L_0),$$

for any invertible sheaf L_0 on T. The heart of the proof is showing that the map (of sets)

$$\begin{aligned} E(T) &\to Pic^{(1)}(E_T/T) \\ P &\mapsto [I^{-1}(P)] \end{aligned}$$

is a bijection. Once we show that, it means that for every $A, B \in E(T)$, the invertible sheaf

$$I^{-1}(A) \otimes I^{-1}(B) \otimes I(0)$$

is of degree 1 (fiber-by-fiber) hence (the above map being bijective) there exists a unique $C \in E(T)$ such that

$$I^{-1}(A) \otimes I^{-1}(B) \otimes I(0) \cong I^{-1}(C) \otimes f_T^*(L_0).$$

This proves that if the group structure exists it has to be unique. For the existence of the group structure, it follows from the isomorphism

$$\begin{aligned} Pic^{(1)}(E_T/T) &\to Pic^{(0)}(E_T/T) \\ [I^{-1}(P)] &\mapsto [I^{-1}(P) \otimes I(0)], \end{aligned}$$

where $Pic^{(0)}(E_T/T)$ is the abelian group of isomorphism classes of invertible sheaves L on E_T which are of degree 0 (fiber-by-fiber) modulo the equivalence class

$$L \sim L \otimes f_T^*(L_0),$$

for any invertible sheaf L_0 on T. The group structure on $E(T)$ is, by construction, the pullback of the group structure on $Pic^{(0)}(E_T/T)$ via the isomophism. It remains to show the bijectivity of

$$E(S) \to Pic^{(1)}(E/S)$$

for every scheme S. We claim that it is enough to show this for S affine and noetherian and even more generally if we have $\{U_i\}_{i\in I}$ a cover of S and L and L' invertible sheaves on E such that on each open subscheme $f^{-1}(U_i)$ of E, we have

$$\varphi_i : L \cong L' \otimes f^*(L_{0,i}),$$

for some $L_{0,i}$ an invertible sheaf over U_i then we can extend these isomrphisms to an isomorphism

$$L \cong L^{'} \otimes f_T^*(L_0).$$

This is shown in details in [13, p 65]. We finally prove the theorem, let $L \in Pic^{(0)}(E_S/S)$ where S is affine noetherian. By Lemma 2.3.1, f^*L is an invertible sheaf over S. We shrink S even further so that

$$f^*L \cong O_S.$$

Let l be the image of 1_S into $f^*L(S) = H^0(E, L)$ and we claim that (L, l) is a relative effective Cartier divisor on E/S. Indeed, because l generates the sheaf f^*L, we have an exact sequence

$$0 \longrightarrow O_E \xrightarrow{\ l\ } L \longrightarrow L/O_E \longrightarrow 0$$

and the flatness of L/O_E over E is shown in [8, p 124]. Hence (L, l) being an effective Cartier divisor which is fiber-by-fiber of degree 1 corresponds by proposition 2.2.5 to an element in $P \in E(S)$ thus describing an inverse map to the function defined at the beginning. ∎

Remark 2.3.1. *We will denote*

$$\underline{\omega}_{E/S} := f_*\Omega_{E/S}.$$

As it is shown in [8, II.*2.2], the sheaf $R^1 f_* O_E$ is locally invertible. Thus, by Serre's duality, $\underline{\omega}_{E/S}$ is isomorphic to the dual of $R^1 f_* O_E$ and in particular is also invertible.*

We work affine locally, so suppose that $\underline{\omega}_{E/S}$ is trivial on $S = Spec(R)$ via an isomorphism determined by mapping global sections $1 \mapsto \omega$. By definition, ω corresponds to a nowhere vanishing global section of $\Omega_{E/S}$ (which is therefore locally invertible) because $(\Omega_{E/S}, \omega)$ an effective Cartier divisor of degree 0 i.e.

$$\Omega_{E/S} \cong O_E.$$

Following [8, 2.2.4], if we take the completion of E along the ideal sheaf $I([0])$ induced by the zero section, we get an isomorphism of formal group schemes

$$h : \hat{E} \cong Spf(A[[T]]).$$

(The theory of formal group schemes is introduced in [7, II*]). Let us denote*

$$F(T)dT := h_*\omega,$$

where ω is a the formal completion of a nowhere vanishing one form on E/S. Therefore $F(T) \in A[[T]]^\times$ and so

$$\omega = (u + a_1 T + a_2 T^2 + ...)dT,$$

where $u \in A^\times$. By sending $T \mapsto T' := u^{-1}T$ we get an isomorphism

$$Spf(A[[T']]) \cong Spf(A[[T]]),$$

where

$$\omega = (1 + a_1 T' + a_2 (T')^2 + ...)dT'.$$

2.4 The Weierstrass equation

Following [13, II.2], we want to embed an elliptic curve E/S into $\mathbb{P}^2_S$ (it turns out that we might have to restrict S). Let us consider the invertible sheaf $I([0])^{-n}$ which has degree n, this is clearly an effective Cartier divisor and we have an exact sequence

$$0 \longrightarrow O_E \longrightarrow I([0])^{-n} \longrightarrow I([0])^{-n}/O_E \longrightarrow 0.$$

By right exactness of the push-forward functor f_* and Lemma 2.3.1, we get a long exact sequence

$$0 \longrightarrow f_*O_E \longrightarrow f_*I([0])^{-n} \longrightarrow f_*(I([0])^{-n}/O_E) \longrightarrow R^1f_*O_E \longrightarrow R^1f_*I([0])^{-n}.$$

Now, we claim that $R^1f_*(I([0])^{-n})$ vanishes. We proceed fiber by fiber

$$R^1f_*(I([0])^{-n}) \otimes k(s) \cong H^1(E_s, I([0])_s^{-n}) \cong H^0(E_s, I([0])_s^n \otimes \Omega_{E/S}).$$

Because $\deg(I([0])_s^n \otimes \Omega_{E/S}) = -n < 0$, the Riemann-Roch theorem implies that

$$H^0(E_s, I([0])_s^n \otimes \Omega_{E/S}) = 0.$$

Therefore we conclude that

$$R^1f_*(I([0])^{-n}) = 0$$

The above exact sequence becomes

$$0 \longrightarrow f_*O_E \longrightarrow f_*I([0])^{-n} \longrightarrow f_*(I([0])^{-n}/O_E) \longrightarrow R^1f_*O_E \longrightarrow 0.$$

It follows that $f_*I([0])^{-n}$ is locally free [8, Cor 1.10.5] and of rank n (by exactness of the above sequence). Now, by shrinking S if necessary, we may assume that $f_*I([0])^{-n}$ is free for $1 \leq n \leq 6$ and that ω is an O_S-basis for $\underline{\omega}_{E/S}$.

We have the following

$$H^0(E, I([0])^{-1}) = A.$$

Similarly

$$H^0(E, I([0])^{-2}) = A + Ax.$$

Now, since x has a pole of order exactly 2 at $[0]$ i.e.

$$x = \frac{u}{T^2} + \frac{a_{-1}}{T} + a_0 + a_1T + ...$$

where $u \in A^{\times}$, we can normalize the above equality by replacing x by $u^{-1}x$ so that

$$x = \frac{1}{T^2} + \text{ terms of higher order .}$$

Similarly

$$H^0(E, I([0])^{-3}) = A + Ax + Ay,$$

and we normalize y (that has order 3) so that

$$y = \frac{-1}{T^3} + \text{ terms of higher order}$$

Finally, it is clear from the above and from the orders of x and y at 0 that

$$H^0(E, I([0])^{-4}) = A + Ax + Ay + Ax^2$$

$$H^0(E, I([0])^{-5}) = A + Ax + Ay + Ax^2 + Axy,$$

and that

$$\begin{aligned} H^0(E, I([0])^{-6}) &= A + Ax + Ay + Ax^2 + Axy + Ax^3 \\ &= A + Ax + Ay + Ax^2 + Axy + Ay^2. \end{aligned}$$

It follows from the normalization of x and y that $y^2 - x^3$ has a pole of order less than 6 at [0] hence, we have a relation of the form

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

for elements $a_i \in A$. Now, our "local embedding" follows from the following two propositions :

Proposition 2.4.1. *Let S be an affine scheme and T be a scheme over S. If L is an invertible sheaf on T and $t_1, .., t_n \in H^0(T, L)$ generate L, then there exists a unique morphism*

$$\phi : T \to \mathbb{P}^n_S$$

such that $L \cong \phi^* O(1)$ and $t_i = \phi^*(x_i)$.

Proof: This result is Theorem 7.1 in [7, II]. ∎

We call ϕ the morphism associated to the invertible sheaf L and global sections $t_1, .., t_n \in H^0(T, L)$.

Proposition 2.4.2. *Let S be an affine scheme and let C/S be a smooth and proper curve of genus g. If D/S is an effective Cartier divisor with $deg(D) \geq 2g+1$, then the morphism $C \to \mathbb{P}^n_S$ associated to the invertible sheaf $I^{-1}(D)$ and a choice of a base for its global section is a closed immersion.*

Proof: This is shown in Corollary 2.1.7 of [8, II]. ∎

If we go back to our case of an elliptic curves E/S for S small enough affine scheme, we conclude that E/S can be embedded in $\mathbb{P}^2_S$ via the effective Cartier divisor $I([0])^{-3}$. This allows us to think about elliptic curves as projective curves given locally by affine equations of the form

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

where $a_i \in A$ and $S = Spec(A)$.

Theorem 2.4.1. *Let E/S be an elliptic curve and N a positive integer. Then the multiplication by N morphism (over S)*

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

is finite and locally free of rank N^2. Moreover, if S is a scheme over $\mathbb{Z}[\frac{1}{n}]$ then $E[N]$ is finite and étale such that it is isomorphic to

$$\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

locally on S.

Proof: A proof of this result can be found in [13, p 73]. ∎

Definition 2.4.1. *Let E be an elliptic curve over a scheme S and let N be a positive integer. We call a $\Gamma(N)-$structure on E/S an isomorphism*

$$\alpha_N : E[N] \to (\mathbb{Z}/n\mathbb{Z})_S \times_S (\mathbb{Z}/n\mathbb{Z})_S.$$

We sometimes also call α_N a level N structure.

2.5 The Moduli problem

Definition 2.5.1. *Let C be a small Category and let*

$$F : C \to Set$$

be a covariant (resp. contravariant) functor. We say that the functor F is representable if it is naturally isomorphic to the functor $Hom_C(A,.)$ (resp. $Hom_C(.,A)$) for some object $A \in Obj(C)$.

Let S be a scheme. Consider the Category Ell/S whose objects are pairs (E,T) consisting of an S-scheme T and an elliptic curves E over T. Now, for two objects (E,T) and (E',T') in Ell/S, a morphism

$$(E,T) \to (E',T')$$

consists of an S-morphism $T \to T'$ and a T'-morphism $E \to E'$.

Definition 2.5.2. *Let S be a fixed scheme. A moduli problem P for elliptic curves over S is a contravariant functor*

$$P : Ell/S \to Set.$$

A P-structure on an elliptic curve (E,T) is an element of $P(E,T)$.

A moduli problem P is said to be representable if it is representable as a functor on Ell/S i.e. if there exists a elliptic curve $\mathbb{E}$ over an S-scheme S_P and a functorial isomorphism

$$P(E/T) \cong Hom_{Ell/S}(E/T, \mathbb{E}/S_P).$$

We say that P is relatively representable if, for all E/S' in Ell/S, the contravariant functor

$$P_{E/S'} : Sch/S' \to Set$$

that sends a scheme T over S' to $P(E_T/T)$ is representable. In that case, we also denote the S'-scheme that represents the above functor by $P_{E/S'}$.

Definition 2.5.3. *Let S be a scheme and $\mathcal{P}$ be a property of morphisms of schemes (finite, finitely presented, proper, ...). Let*

$$P : Ell/S \to Set$$

be a moduli problem, we say that P has the property $\mathcal{P}$ if P is relatively representable and, for all E/S' in Ell/S, the morphism

$$E \to S'$$

has the property $\mathcal{P}$.

Theorem 2.5.1. *Let S be a scheme and let*

$$P : Ell/S \to Set$$

be a moduli problem representable by some universal elliptic curve

$$f : \mathbb{E} \to S_P.$$

The contravariant functor

$$\tilde{P}\colon Sch/S \to Set$$
$$S' \mapsto \left\{ [E/S', \alpha] \;\middle|\; \begin{array}{l} E/S' \text{ elliptic curve over } S' \text{ and} \\ \alpha \text{ an element of } P(E/S') \end{array} \right\}$$

is representable by the S-scheme S_P. The notation $[.,.]$ means that we look at the natural isomorphism class of such objects.

Proof: Let $\mu : S' \to S_P$ be a morphism of schemes, we have a commutative diagram

$$\begin{array}{ccc} \mathbb{E}_{S'} & \xrightarrow{p_2} & \mathbb{E} \\ {\scriptstyle f'}\downarrow & & \downarrow{\scriptstyle f} \\ S' & \xrightarrow{\mu} & S_P \end{array}$$

where $\mathbb{E}_{S'} := \mathbb{E}$ is a base extension defined up to S-isomorphism. Moreover,

$$p_2 : \mathbb{E}_{S'} \to \mathbb{E}$$

is a morphism of elliptic curves over S hence it corresponds, by representability of P, to an element $\alpha \in P(E/S)$. This defines a natural transformation

$$Hom_S(., S_P) \to \tilde{P}.$$

This is indeed an isomorphism. Given a pair $(E/S', \alpha)$, an element $\alpha \in P(E/S')$ corresponds to a morphism of elliptic curves (over S)

$$E/S' \to \mathbb{E}/S_P$$

hence, in particular, to a morphism

$$S' \to S_P.$$

This is a natural transformation making the above morphism of functors an isomorphism.

∎

The natural isomorphism

$$Hom_S(., S_P) \cong \tilde{P}$$

gives rise to a canonical element, i.e. the image of the identity morphism Id_{S_P}. We will denote it by $[(\mathbb{E}/S_P, \tilde{\alpha})]$.

Remark 2.5.1. *Let $N \in \mathbb{Z}_{>0}$ be a positive integer. We are interested in the following moduli problem which is given by the functor*

$$\Gamma(N)_S(E/T) = \{\Gamma(N) - \textit{Structures on } E/T\}.$$

Theorem 2.5.2. *Let $E \to S$ be an elliptic curve, the functor $Sch/S \to Set$ that maps*

$$T \mapsto \{\Gamma(N) - \textit{Structures on } E_T/T\}$$

is representable i.e. the moduli problem $\Gamma(N)_S$ is relatively representable.

Moreover $\Gamma(N)_S$ is finite and, when S is a scheme over $\mathbb{Z}[\frac{1}{N}]$, it is étale.

Proof: [13, prop 3.6] and [13, prop 3.7.1] ∎

We want some kind of inverse to the above theorem.

Definition 2.5.4. *Let S be a scheme and $P : Ell/S \to Set$ be a moduli problem. We say that P is rigid if, for every elliptic curve E/S' in Ell/S and $\alpha \in P(E/S)$, the pair $(E/S', \alpha)$ has no non-trivial automorphisms.*

In particular, we immediately see that if P is representable then it is rigid.

Finally, we state a general Theorem about moduli problems of elliptic curves.

Theorem 2.5.3. *Let S be an affine scheme and $P : Ell/S \to Set$ be a relatively representable and affine moduli problem . The following statements are equivalent*

1. *P is rigid.*
2. *P is representable.*

And in this case, $\tilde{P}$ is also representable by an S-scheme S_P which is affine. Moreover, if P is étale then the S-scheme S_P is a smooth affine curve.

Proof: [10, Thm 4.7.0] and [10, Cor 4.7.1] ∎

Let $N \geq 3$ be an integer. All the previous results will allow us to solve the moduli problem $\Gamma(N)_S$ for S a connected affine scheme defined by

$$\Gamma(N)_S(E/T) = \{\Gamma(N) - \text{Structures on } E/T\}.$$

Theorem 2.5.2 states that $\Gamma(N)_S$ is relatively representable and finite (hence affine). Moreover, it is shown in [13, Cor 2.7.2] that $\Gamma(N)_S$ is rigid and that it is therefore representable by some elliptic curve

$$\mathbb{E} \to S_{\Gamma(N)},$$

for an affine S-scheme $S_{\Gamma(N)}$. Moreover, if N is invertible in S, then $S_{\Gamma(N)}$ is an affine smooth curve over S and we denote it by

$$Y(N) := S_{\Gamma(N)}.$$

We state various results about $Y(N)$ following [10, 1.4]. We have a morphism of schemes

$$j : Y(N) \to \mathbb{A}^1_S.$$

This corresponds, at the level of points, to the usual j-function that maps an elliptic curves E/R (for some S-algebra R) to its corresponding j-invariant in R. The morphism j is finite and flat. Now, if we consider it as a morphism

$$j : Y(N) \to \mathbb{P}^1_S,$$

then, by the process of normalization described in [13, 8.6], we get a proper smooth curve $X(N)$ over S.

Chapter 3

Modular Forms and Applications

3.1 Modular forms over general schemes

In this chapter, we introduce a generalization of the classical theory of complex modular forms (described in chapter 1). This theory was formulated by Katz in his paper [10] in order to extend modular forms to elliptic curves over more general schemes.

We recall that, for an elliptic curve

$$f : E \to S,$$

we previously defined the invertible sheaf

$$\underline{\omega}_{E/S} := f_*\Omega_{E/S}.$$

Let R be a commutative ring. For $S = Spec(R)$ affine, we can choose a basis ω of $\underline{\omega}_{E/S}$ (defined up to multiplication by a scalar $\lambda \in R^\times$) which corresponds to a nowhere vanishing section of $\Omega_{E/S}$ on E.

We fix a ground commutative ring R_0.

Definition 3.1.1. *A modular form of weight k and level 1 over the ring R_0 is a rule f that assigns to any elliptic curve E over an R_0-scheme S a global section $f(E/S)$ of $\underline{\omega}_{E/S}^{\otimes k}$ such that*

1. *$f(E/S)$ is defined up to S-isomorphisms of the elliptic curve E/S.*
2. *The formation of $f(E/S)$ is compatible with base changes i.e. if*

$$g : S' \to S$$

is a morphism of R_0-schemes then

$$f(E'_S/S') = g^* f(E/S).$$

If we restrict to affine R_0-schemes, we can formulate an alternative definition

Definition 3.1.2. *A modular form of weight k and level 1 over the ring R_0 is a rule f that assigns to a pair $(E/R, \omega)$ (that consists of an elliptic curve E over an R_0-algebra R and a basis ω of $\underline{\omega}_{E/R}$) an element $f(E/R)$ of R such that*

1. *$f(E/R, \omega)$ is defined up to R-isomorphisms of the pair $(E/R, \omega)$.*
2. *The formation of $f(E/R, \omega)$ is compatible with extensions of scalars i.e. if*

$$g : R \to R'$$

is a morphism of R_0-algebras then

$$f(E_{R'}/R', \omega') = g(f(E/R, \omega)).$$

3. *For all $\lambda \in R^\times$, we have $f(E/R, \lambda\omega) = \lambda^{-k} f(E/R, \omega)$.*

Remark 3.1.1. *The equivalence of both definition is obvious. Indeed, if one has a modular form of weight of the second kind and of weight k for some fixed ground ring R_0, one defines*

$$f(E/R) := f(E/R, \omega)\, \omega^{\otimes k}.$$

This definition is independent of the choice of ω because, for all $\lambda \in R^\times$, we have

$$f(E/R, \lambda\omega)\, (\lambda\omega)^{\otimes k} = \lambda^{-k} f(E/R, \omega)(\lambda)^k\, \omega^{\otimes k} = f(E/R, \omega)\, \omega^{\otimes k}.$$

We will denote the R_0-module of modular forms of weight k and level n over R_0 by $M(R_0, 1, k)$.

Definition 3.1.3. *The Tate curve is the elliptic curve $Tate(q)$ over $\mathbb{Z}((q))$ defined by the equation*

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

where

$$a_4 = -5\sum_{n=1}^{\infty} \sigma_3(n) q^n \quad \text{and} \quad a_6 = -\frac{1}{12}(5\sum_{n=1}^{\infty} \sigma_3(n) q^n + 7\sum_{n=1}^{\infty} \sigma_5(n) q^n)$$

and σ_k is the usual sigma function defined as

$$\sigma_k(n) = \sum_{d|n} d^k,$$

where the sum is taken over the positive divisors.

Moreover, the canonical differential of the above Tate curve is

$$\omega_{can} := \frac{dx}{2y + x}.$$

This is covered in the Appendix 1 of [10].

By base extension, the elliptic curve $(Tate(q), \omega_{can})$ over the ring $\mathbb{Z}((q))$ extends to an elliptic curve (with a corresponding invariant differential) $(Tate(q), \omega_{can})_{R_0}$ over $\mathbb{Z}((q)) \otimes R_0$.

Remark 3.1.2. *Over the complex numbers, the Tate curve parametrizes all elliptic curves (by Weierstrass parametrization). Although, this is not true in general.*

Definition 3.1.4. *Let f be a modular form of weight k and level 1 over the ring R_0. We say that f is holomorphic at ∞ if*

$$f((Tate(q), \omega_{can})_{R_0}) \ \text{ is in } \ \mathbb{Z}[[q]] \otimes R_0.$$

Definition 3.1.5. *Let f be a modular form of weight k and level 1 over the ring R_0. We say that f is a cusp form if*

$$f((Tate(q), \omega_{can})_{R_0}) \ \text{ is in } \ q\mathbb{Z}[[q]] \otimes R_0.$$

The Laurent series $f((Tate(q), \omega_{can})_{R_0})$ is called the $q-$expansion of the modular form f.

We denote the R_0-modules of holomorphic modular forms of weight k and level 1 over R_0 by $S(R_0, 1, k)$.

Remark 3.1.3. *We immediately see the resemblance between Katz's definition of (holomorphic) modular forms and the alternative way of defining the classical complex modular forms introduced in the first chapter. Rigorously showing that both definitions are equivalent (when $R_0 = \mathbb{C}$) uses the theorems of GAGA (Géométrie algébrique et géométrie analytique). A detailed exposition can be found in [2].*

3.2 p-adic modular forms

Let R be an $\mathbb{F}_p$-algebra for some prime p and let E be an elliptic curve over R.

Definition 3.2.1. *Let S be an $\mathbb{F}_p$-scheme. The absolute Frobenious endomorphism on S is a morphism of schemes*

$$F : S \to S,$$

consisting of the identity map at the level of the underlying topological space of S and to the $\mathbb{F}_p$-endomorphism

$$x \mapsto x^p$$

at the level of the sheaf $\mathcal{O}_S$.

We introduce an important example of a modular form over $\mathbb{F}_p$ called the Hasse invariant and denoted by A. Let R be an $\mathbb{F}_p$-algebra and let E be an elliptic curve over R with ω a basis for $\underline{\omega}_{E/R}$.

The Frobenious endomorphism $F : \mathcal{O}_E \to \mathcal{O}_E$ induces a p-linear endomorphism of the R-module $H^1(E, \mathcal{O}_E)$ denoted by

$$F^* : H^1(E, \mathcal{O}_E) \to H^1(E, \mathcal{O}_E).$$

Let $\eta \in H^1(E, \mathcal{O}_E)$ be the dual of ω (by Serre duality). We define $A(E, \omega)$ to be the element of R such that

$$F^*(\eta) = A(E, \omega)\eta.$$

Indeed, if we replace ω by $\lambda\omega$ for some $\lambda \in R^\times$ then to η will correspond $\lambda^{-1}\eta$ and

$$\begin{aligned} A(E, \omega)\eta = F^*(\eta) &= \lambda^p F^*(\lambda^{-1}\eta) \\ &= \lambda^p A(E, \lambda\omega)(\lambda^{-1}\eta) \\ &= \lambda^{p-1} A(E, \lambda\omega)\eta, \end{aligned}$$

which shows that

$$A(E, \lambda\omega) = \lambda^{1-p} A(E, \omega),$$

proving that A is a modular form of level 1 and weight $p-1$ defined over $\mathbb{F}_p$. One can prove the holomorphy of A at ∞ by computing its q-expansion, this is shown in [10, II] and one gets

$$A(Tate(q), \omega_{can}) = 1.$$

Next, we will introduce another family of modular forms using an important result, due to Katz, called the q-expansion principle. It is stated as follows

Theorem 3.2.1. *Let $R \subseteq L$ be a ring extension and let f be a holomorphic modular form of weight k over L. If the coefficients of the q-expansion of f are elements of R then f is a holomorphic modular form of weight k over R.*

Proof: This is proved in [10]. ∎

Example 3.2.1. *Recall that an important class of (classical) modular forms over $\mathbb{C}$ is given by the class of Eisenstein series of weights $2k$ (for $k > 1$) given by*

$$E_{2k}(\tau) = \frac{1}{2\zeta(2k)} \sum_{(m,n)\in\mathbb{Z}^2\setminus(0,0)} \frac{1}{(m+n\tau)^{2k}},$$

and whose q-expansions are given by

$$E_{2k}(\tau) = 1 - \frac{4k}{B_{2k}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n.$$

As the coefficients of E_{2k} are clearly elements of $\mathbb{Q}$, we conclude that the Eisenstein series are modular forms over $\mathbb{Q}$.

We finally introduce p-adic modular forms. We fix a prime $p \geq 5$ and R_0 a p-adically complete ring (usually the p-adic integers $\mathbb{Z}_p$ or the ring of integers of a finite extension of $\mathbb{Q}_p$).

Remark 3.2.1. *For a prime $p \geq 1$, we consider the Eisenstein series*

$$\mathbb{E}_{p-1}(\tau) = 1 - \frac{2p-2}{B_{p-1}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n, \quad \text{where } q = e^{2\pi i \tau}.$$

The Clausen-von Staudt congruence states that $v_p(B_{p-1}) = -1$. This implies that $\mathbb{E}_{p-1}$ can be reduced modulo p and the result has q-expansion equal to 1 exactly like the Hasse invariant. By the q-expansion principle, we conclude that

$$A = \mathbb{E}_{p-1} \pmod{p}.$$

In other terms, $\mathbb{E}_{p-1}$ is a lift of A to the ring $\mathbb{Z}_{(p)}$.

The idea of Katz is to define p-adic modular forms as functions of elliptic curves whose Hasse invariant (or rather a lift of the Hasse invariant) is away from 0. This has the advantage of removing supersingular elliptic curves and curves with supersingular reduction from the definition of modular forms.

Definition 3.2.2. *A p-adic modular form (à la Katz) of rank k and growth condition r is a rule f that sends a triple $(E/R, \omega, Y)$ consisting of*

- *An elliptic curve E over an R_0-algebra R in which p is nilpotent.*
- *A nowhere vanishing differential $\omega \in H^0(E, \Omega^1_{E/R})$.*
- *An element $Y \in R$ such that $Y \cdot \mathbb{E}_{p-1}(E/R, \omega) = 1$.*

to an element of R such that

1. *f does not depend on the isomorphism class of the triple $(E/R, \omega, Y)$ and the formation of $f(E/R, \omega, Y)$ is compatible with extensions of scalars.*
2. *For all $\lambda \in R^\times$, we have*
$$f(E/R, \lambda\omega, \lambda^{p-1}Y) = \lambda^{-k} f(E/R, \omega, Y).$$
3. *For all integers $n \geq 1$, we have that*
$$f((Tate(q), \omega_{can}, 1)_{R_0/p^n R_0}) \in R_0/p^n R_0[[q]].$$

An important example of a $p-$adic modular forms is the Eisenstein series of weight 2.

Definition 3.2.3. *The weight 2 Katz $p-$adic modular Eisenstein series $\mathbb{E}_2$ is a $p-$adic modular form of weight 2 that has a $q-$expansion*
$$\mathbb{E}_2(q) = 1 - 24\sum_{n=1}^{\infty} \sigma_1(n) q^n.$$

The existence of $\mathbb{E}_2$ is shown in Chapter V of [9].

3.3 Application : p-adic heights

Let E be an elliptic curve over $\mathbb{Q}$ (and more generally over a number field K). In the classical theory of elliptic curves arises the notion of real heights over E. Height functions are maps
$$h : E(\mathbb{Q}) \to \mathbb{R}$$
that "behave well" under the group structure of $E(\mathbb{Q})$. The importance of this notion of heights is seen in proving the Mordell-Weil theorem which states that the abelian group $E(\mathbb{Q})$ is finitely generated. If $P = (x, y) \in E(\mathbb{Q})$, then we can define the naive real height as
$$h_{naive}(P) = log(max\{|x|, 1\})$$
This turns out to be "almost" a quadratic form up to a constant. Néron wanted to find an actual quadratic form that only differs from the naive height by a constant. Tate gave a simple such construction called the canonical Néron-Tate height
$$\hat{h} : E(\mathbb{Q}) \to \mathbb{R}$$
and defined by
$$\hat{h}(P) = \lim_{N\to\infty} \frac{1}{4^N} h_{naive}(2^N P).$$
This canonical height satisfies the properties

1. $\hat{h}(mP) = m^2\hat{h}(P)$ for all $m \in \mathbb{Z}$ and $P \in E(\mathbb{Q})$.
2. $\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q)$ for all $P, Q \in E(\mathbb{Q})$.
3. There exists $C > 0$ such that $\forall P \in E(\mathbb{Q}), \quad |\hat{h}(P) - \hat{h}_{naive}(P)| < C$.

A detailed proof of these results can be found in [20, VIII]. We want to also have a notion of heights on elliptic curves over $\mathbb{Q}$ (and more generally on number fields) that takes values in $\mathbb{Q}_P$.

Fix a prime $p \geq 5$. In this section, we fix E an elliptic curve over $\mathbb{Q}$ given by a Weierstrass equation

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

We denote by ω its invariant differential given by

$$\omega = \frac{dx}{2y + a_1x + a_3}.$$

Assume E has a good ordinary reduction over the prime p which means that, if we reduce the above equation of E modulo the prime p, we still get an elliptic curve over the field $\mathbb{F}_p$.

Let $P \in E(\mathbb{Q})$. If P is a torsion point (i.e. $nP = 0$ for some $n \geq 1$) then we put

$$h_p(P) = 0.$$

Otherwise, we assume that P reduces to 0 in $E(\mathbb{F}_p)$ and to a non-singular point in $E(\mathbb{F}_l)$ for all primes l where E doesn't have a good reduction. We define

$$h_p(P) = \frac{1}{p}\log_p\left(\frac{\sigma_p(P)}{d(P)}\right).$$

If $P \in E(\mathbb{Q})$ does not verify the above two properties then nP, for some $n \geq 2$, does. In that case, we define

$$h_p(P) = \frac{1}{n^2}h_p(nP).$$

In the following sections, we define and study the notation introduced above i.e. $\log_p$, $d(P)$ and $\sigma_p(P)$. But before that, we state the following result from [15] that it is quite similar to the real case :

Theorem 3.3.1. *The $p-$adic height $h_p : E(\mathbb{Q}) \to \mathbb{Q}_p$ satisfies the followings properties:*

1. *The Quadratic law:* $\forall n \in \mathbb{Z}$ *and* $A \in E(\mathbb{Q})$, *we have*

$$h_p(nA) = n^2h_p(A).$$

2. The Parallelogram law: $\forall A, B \in E(\mathbb{Q})$, *we have*

$$h_p(A+B) + h_p(A-B) = 2h_p(A) + 2h_p(B).$$

3.3.1 The denominator of a rational point

We have the following classical result:

Theorem 3.3.2. *Let E be an elliptic curve given by the Weierstrass equation above. If $P = (x, y) \in E(\mathbb{Q})$ is a nonzero point then there exists unique integers $a, b \in \mathbb{Z}$ and $d \in \mathbb{Z}_{>0}$ such that gcd $(a, d) =$ gcd $(b, d) = 1$ and*

$$P = (x, y) = \left(\frac{a}{d^2}, \frac{b}{d^3} \right).$$

Proof: A proof of a more general result for elliptic curves over a unique factorization domain (or even a Krull domain) can be found in section 2.2 of [3]. ∎

If $P = (x, y) \in E(\mathbb{Q})$ is nonzero then we call denominator of P, and we denote by $d(P)$ the positive integer d of the above theorem.

3.3.2 The $p-$adic logarithm

Consider the power series over $\mathbb{Q}_p$ given by

$$\log_p(x+1) = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots.$$

We claim that the above series converges whenever $|x|_p < 1$. Indeed, it suffices to show that $\mathrm{ord}_p\left(\frac{x^n}{n}\right) \to \infty$.

This follows from the fact that

$$\begin{aligned} \mathrm{ord}_p\left(\frac{x^n}{n}\right) &= n\ \mathrm{ord}_p(x) - \mathrm{ord}_p(n) \\ &\geq n - log_p(n), \end{aligned}$$

which clearly tends to infinity. The log_p in the above equation is the usual logarithm defined over $\mathbb{R}_{>0}$, not to be confused with the $p-$adic logarithm we are about to define. We have a map

$$\log_p : 1 + p\mathbb{Z}_p \to \mathbb{Q}_p.$$

Under multiplication, this is a group homomorphism as one has to show (easily) that

$$\log_p\left((1+x)(1+y)\right) = \log_p(1+x) + \log_p(1+y),$$

for all $x, y \in p\mathbb{Z}_p$. Moreover, by imposing $\log_p(p) = 0$, we extend $\log_p$ to all of $\mathbb{Q}_p^*$ as follows : Every element $q \in \mathbb{Q}_p^*$ can be written uniquely as

$$q = p^{-ord_p(q)}u,$$

where u is a unit in $\mathbb{Z}_p$. Writing u in its $p-$adic expansion and using Fermat's Little Theorem, we find that

$$u^{p-1} \in 1 + p\mathbb{Z}_p.$$

Therefore, we define

$$\log_p(q) := \frac{1}{p-1}\log_p(u^{p-1}).$$

We get a group homomorphism

$$\mathbb{Q}_p^* \to \mathbb{Q}_p,$$

called the $p-$adic logarithm and denoted by $\log_p$.

3.3.3 The $p-$adic sigma function

Following Chapter IV of Silverman, we look at the completion of the local ring $\mathbb{Q}[E]_O$ at the origin O. Explicitly, we consider the Laurent expansion of x and y and the invariant differential ω at the parameter $t = \frac{x}{y}$ of the formal group. We have

$$\begin{aligned} x(t) &= t^{-2} - a_1t^{-1} - a_2 + \dots, \\ y(t) &= -t^{-3} + a_1t^{-2} + a_2t^{-1} + \dots, \\ \omega(t) &= \left(1 + a_1t + (a_1^2 + a_2)t^2 + \dots\right) dt. \end{aligned}$$

The following theorem due to Mazur and Tate defines the $p-$adic sigma function.

Theorem 3.3.3. *There exists a unique odd function $\sigma(t) = t + \cdots \in t\mathbb{Z}_p[[t]]$ and a unique $c \in \mathbb{Z}_p$ that satisfy the formal differential equation*

$$x(t) + c = -\frac{d}{\omega}\left(\frac{1}{\sigma}\frac{d\sigma}{\omega}\right).$$

Moreover the constant c is equal to

$$c = \frac{a_1^2 + 4a_2 - 12\mathbb{E}_2(E,\omega)}{12},$$

where $\mathbb{E}_2$ is the weight 2 Katz $p-$adic modular form.

Proof: This result was proven by Mazur and Tate in [14]. ∎

For $P = (x, y) \in E(\mathbb{Q})$, by $\sigma(P)$ we mean $\sigma(\frac{x}{y})$. By now, we have given a complete definition of the $p-$adic height $h_p(P)$. The most mysterious quantity this far is the sigma function and we still have to explain how it relates to $p-$adic modular forms.

Once we can explicitly compute the constant c above, the differential equation of the above theorem gives an explicit way to compute $\sigma(P)$. This is done by solving the formal differential equation. So, suppose we have the value of $\mathbb{E}(E, \omega)$, then we denote by

$$z(t) := \int \frac{\omega}{dt} = t + \frac{a_1}{2}t + \frac{a_1^2 + a_2}{3}t^3 + \cdots \in t\mathbb{Q}[[t]].$$

Because the constant term is zero and the linear term is a unit, there exists a power series $F(z) \in z\mathbb{Q}[[z]]$ such that $t = F(z(t))$. The first terms of this series are :

$$F(z) = z - \frac{a_1}{2}z^2 + \frac{a_1^2 - 2a_2}{6}z^3 + \dots.$$

We denote by $x(z) := x(F(z))$ and we compute the first coefficients of its series. We have that

$$\begin{aligned}\frac{1}{F(z)} &= z^{-1}\frac{1}{1 - \frac{a_1}{2}z + \frac{a_1^2 - 2a_2}{6}z^2 + \dots} \\ &= z^{-1}\left(1 + \frac{a_1}{2}z + \frac{a_1^2 + 4a_2}{12}z^2 + \dots\right).\end{aligned}$$

Also,

$$\frac{1}{F(z)^2} = z^{-2}\left(1 + a_1 z + \frac{5a_1^2 + 8a_2}{12}z^2 + \dots\right).$$

We are now able to compute the expansion of $x(z)$ and we get :

$$\begin{aligned}x(z) &= \frac{1}{F(z)^2} - \frac{a_1}{F(z)} - a_2 + \dots \\ &= \frac{1}{z^2} + \frac{-a_1^2 - 4a_2}{12} + \text{ terms of higher order ....}\end{aligned}$$

Now, we write the right hand side of the differential equation in the variable z. Since $z = \int \frac{\omega}{dt}$, then $dz = \omega$ and

$$-\frac{d}{\omega}\left(\frac{1}{\sigma}\frac{d\sigma}{\omega}\right) = -\frac{d}{\omega}\left(\frac{d\,\log(\sigma)}{\omega}\right) = -\frac{dz}{\omega}\frac{d}{dz}\left(\frac{d\,\log(\sigma)}{\omega}\right) = -\frac{d}{dz}\left(\frac{d\,\log(\sigma)}{dz}\right).$$

Recall that $\sigma(t) \in t\mathbb{Q}_p[[t]]$ and therefore $\sigma(z) := \sigma(F(z)) \in z\mathbb{Q}_p[[z]]$. We write $\sigma = z\sigma_0$ and we plug in the differential equation. We now have

$$-x(z) - c + \frac{1}{z^2} = \frac{d^2}{dz^2} \left(\log(\sigma_0) \right).$$

But the left hand side $-x(z) - c + \frac{1}{z^2}$ is actually in $\mathbb{Q}_p[[z]]$ and so we can actually integrate (formally with zero constants) the left hand side twice to find σ_0. We get that

$$\sigma(z) = z \exp\left(\int \int \left[-x(z) + \frac{1}{z^2} - \frac{a_1^2 + 4a_2 - 12\mathbb{E}_2(E,\omega)}{12} \right] dz\, dz \right).$$

Finally, we write $\sigma(t) = \sigma(z(t))$ and we find the sigma function whose existence is guaranteed by the above theorem.

So we finally reduced the problem of computing $p-$adic heights on elliptic curves to a simple computation of the $p-$adic modular form $\mathbb{E}_2$ at (E, ω). In their paper [15], Mazur, Stein and Tate propose two methods of calculating the value of $\mathbb{E}_2(E, \omega)$. The first method is elementary and consists on computing the constant c directly from the differential equation of the above theorem. This is described is details in Section 3.3 of [15]. More interestingly, there exists a more efficient method for computing $\mathbb{E}_2$ using the $p-$adic de Rham Cohomology group H^1_{dr} of E. This goes past the scope of this thesis but it is covered in [11] and in the Appendix of [10].

Bibliography

[1] M. F. Atiyah, I.G.MacDonald. Introduction To Commutative Algebra. Addison-Wesley Publishing Company, Inc. (1969).

[2] W. Chen. Katz Modular Forms. https://www.williamyunchen.com/. August 2020.

[3] I. Connell. Elliptic Curve Handbook. https://webs.ucm.es/BUCM/mat/doc8354.pdf (1999).

[4] A. Grothendieck. Eléments de Géométrie Algébrique. I. Le langage des schémas. (French) Inst. Hautes Etudes Sci. Publ. Math. No. 4 (1960).

[5] A. Grothendieck. Eléments de Géométrie Algébrique. III. Etude Cohomologique des faisceaux cohérants. (French) Inst. Hautes Etudes Sci. Publ. Math. No. 11 (1961).

[6] A. Grothendieck. Eléments de Géométrie Algébrique. IV. Etudes locales des schémas et des morphismes de schémas. (French) Inst. Hautes Etudes Sci. Publ. Math. No. 20 (1964).

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

[8] H. Hida. Geometric Modular Forms and Elliptic Curves (Second Edition). World Scientific (2012).

[9] N. Katz. P-adic interpolation of real analytic Eisenstein series. Annals of Mathematics, Volume 104 (1976).

[10] N. Katz . P-adic Properties of Modular Schemes and Modular Forms. Modular Functions of One Variable III. Lecture Notes in Mathematics, vol 350 (page 69-190). Springer, Berlin, Heidelberg (1972).

[11] K. S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. J. Ramanujan Math. Soc. 16 (2001).

[12] Q. Liu. Algebraic Geometry and Arithmetic Curves. Oxford Graduate Texts in Mathematics 6, Oxford University Press (2002).

[13] N. Katz, B. Mazur. Arithmetic Moduli of Elliptic Curves. Annals of Mathematics Studies, Volume 108, Princeton University Press (1985).

[14] B. Mazur, J.Tate. The p-adic sigma function. Duke Mathematical Journal Vol. 62, No. 3 (1991).

[15] B. Mazur, W. Stein, J.Tate. Computation of $p-$adic heights and Log convergence. Doc. Math. (Extra Vol.):577–614 (2006).

[16] P. Schneider. P-adic height pairings. I. Invent. Math., 69(3):401–409, (1982).

[17] J. P. Serre. Formes modulaires et fonctions zêta p-adiques. Modular functions of one variable, III pp. 191–268. Lecture Notes in Math., Vol. 350 (1973).

[18] G. Shimura. Introduction to the Arithmetic Theory of Automorphic Functions. Publications of the Mathematical Society of Japan, Volume 11, Princeton University Press (1971).

[19] J. H. Silverman. The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, Volume 106, 2nd edition, Springer (2016).

[20] J. H. Silverman. Advanced Topics in the Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, Volume 106, 2nd edition, Springer (2016).

[21] E. Tengan. A Proof of Grothendieck's Base Change Theorem. arXiv:1312.7320 [math.AG] (2013).