Ruprecht-Karls-Universität Heidelberg

Fakultät für Mathematik und Informatik

Masterarbeit

zur Erlangung des akademischen Grades

Master of Science (M. Sc.)

On elliptic curves with complex multiplication, L-functions, and p-adic interpolation

vorgelegt von

Brandon Williams

25. Juli 2013

Betreuung: Prof. Dr. Otmar Venjakob

Abstrakt

In dieser Masterarbeit wird die Konstruktion eines p-adischen Maßes, das arithmetische Informationen über die L-Funktion einer elliptischen Kurve verkörpert, erklärt und bewiesen. Wir folgen der Arbeit [7] von Katz. Dabei werden Konzepte der Geometrie und Zahlentheorie besprochen, die für diese Konstruktion wichtig sind.

Abstract

In this thesis, we describe and prove Katz's construction of a p-adic measure that provides arithmetic information about the L-function associated to an elliptic curve. We follow Katz' paper [7]. A number of concepts from geometry and number theory necessary for this construction are introduced and explained.

Contents

Chapter 1

Introduction

Elliptic curves are among the most interesting objects of study in algebraic geometry and number theory. Being smooth, projective curves, they are 'nice' objects in that they satisfy the conditions of many important theorems, and their points have a natural structure of an abelian group, which is of arithmetic interest. In the case of an elliptic curve E over a number field F, it is known that the group $E(F)$ of F-rational points is fiinitely generated - this is the Mordell-Weil theorem (see [20], chapter VIII). Explicitly, we have

$$E(F) = \mathbb{Z}^r \times E_{tors}$$

for a finite torsion group E_{tors}. It turns out that E_{tors} is not terribly difficult to describe, but determining the rank r is extremely hard. No general procedure for finding r is known; however, a simple description has been conjectured, which we now describe.

The **Birch and Swinnerton-Dyer (BSD) conjecture** relates the rank r of the Mordell-Weil group $E(F)$ as well as other arithmetic data of E to the order of a special complex-analytic function $L(E, s)$ associated to E at the value $s = 1$. To be precise, it is claimed that the Taylor expansion of $L(E, s)$ around $s = 1$ is given by

$$L(E, s) = \frac{1}{(\#E_{tors})^2} \cdot \#\text{Ш}_{E/F} \cdot R_{E/F} \cdot \Omega_{E/F} \cdot \prod_{p|N} c_p (s-1)^r + [\text{higher order terms}],$$

where $\text{Ш}_{E/F}$ denotes the Tate-Shafarevich group of E over F; $R_{E/F}$ is the regulator, the determinant of an $r \times r$-matrix whose entries are given by the bilinear 'height' pairing applied to a system of generators of $E(F)$; $\Omega_{E/F}$ is the smallest positive real period of E; and the c_p are the Tamagawa numbers.

The BSD conjecture does not seem to be near any resolution. Indeed, a number of weaker subproblems are considered highly difficult; for example, except for certain special cases, it is not even known that $\#\text{Ш}_{E/F}$ is finite. In fact, the conjecture has been popularized by its inclusion in the Millennium Prize problems of the Clay Mathematics Institute, a compilation of seven problems widely considered to be among the most difficult and influential open problems in the field; six remain unsolved at this time.

The focus of this thesis is solely on the left-hand side of the conjecture; that is, the leading Taylor coefficient of the L-function $L(E, s)$. An immediate difficulty is that the sum defining $L(E, s)$ does not converge at $s = 1$; however, it is known that $L(E, s)$ may be extended analytically to all of $\mathbb{C}$. According to the conjecture, up to a controllable factor it should be an algebraic number, and so to understand it, it should be enough to understand it locally, at all primes. In this way we are led to look at p-adic functions that interpolate the values of $L(E, s)$. We will focus on elliptic curves E with complex multiplication; under this hypothesis, $L(E, s)$ is better understood.

An equivalent problem is that of finding a p-adic measure whose moments interpolate the values of $L(E, s)$. Several approaches exist in the literature, including the elliptic units popularized by Coates and Wiles in [1]. Here, we follow a different construction due to Katz [8], in which the p-adic measure to be found, thought of as a formal power series by Iwasawa theory, is constructed via Serre-Tate theory for moduli spaces. No known approach is valid for primes p that do not split in the field by which E has complex multiplication, but Katz' argument seems to provide some information in that case as well.

Acknowledgements

I would like to thank my advisor, Professor Dr. Otmar Venjakob, for suggesting this very interesting topic for my thesis. I also thank Dr. Thanasis Bouganis for many helpful, patient and motivating discussions. Also, I thank Konrad Fischer and Nithi Rungtanapirom for helping me with some difficulties involving algebraic geometry. Finally, I thank my family for their continued support.

Chapter 2

Review of algebraic geometry

It seems convenient to collect a number of the definitions and basic results in algebraic geometry that we will frequently need and to reproduce them here for easier reference. This chapter is not intended to offer much intuition on this subject. Most of the material is sourced from Hartshorne's book [6].

2.1 Sheaves

Definition 1. Let X be a topological space and $\mathfrak{C}$ be a category (standard examples for $\mathfrak{C}$ will be the categories of sets, abelian groups, commutative rings or modules over a ring). A **presheaf** $\mathcal{F}$ on X with values in $\mathfrak{C}$ consists of the data

$$\mathcal{F}(U) \in Ob(\mathfrak{C}),\ \ U \subseteq X \text{ open}$$

and $\mathfrak{C}$-morphisms

$$\operatorname{Res}^U_V : \mathcal{F}(U) \to \mathcal{F}(V),\ \ V, U \subseteq X \text{ open},\ V \subseteq U$$

such that $\operatorname{Res}^U_U = \mathrm{id}_U$ for each U, and for open sets $W \subseteq V \subseteq U$, $\operatorname{Res}^U_W = \operatorname{Res}^V_W \circ \operatorname{Res}^U_V$.
Elements of $\mathcal{F}(U)$ are called **sections** of $\mathcal{F}$ over U; elements of $\mathcal{F}(X)$ are called **global sections** of $\mathcal{F}$.
We will also use the notation $\Gamma(U, \mathcal{F}) := \mathcal{F}(U)$ and for $s \in \mathcal{F}(U)$, $s|_V := \operatorname{Res}^U_V(s)$.

$\mathcal{F}$ is called a **sheaf** if it satisfies the following local compatibility properties: let U, U_i, $i \in I$ be open subsets of X with $U = \cup_{i \in I} U_i$.
(i) If s, $t \in \mathcal{F}(U)$ with $s|_{U_i} = t|_{U_i}$ for every i, then $s = t$.
(ii) If we are given $s_i \in \mathcal{F}(U_i)$, $i \in I$ such that for every i, $j \in I$, $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$, then there is a section $s \in \mathcal{F}(U)$ with $s|_{U_i} = s_i\ \forall i \in I$.

A **morphism** of presheaves $\varphi : \mathcal{F} \to \mathcal{G}$ is a collection of $\mathfrak{C}$-morphisms $\varphi|_U : \mathcal{F}(U) \to \mathcal{G}(U)$ that respect restriction: for open subsets $V \subseteq U$, we have a commutative diagram

$$\begin{tikzcd}
\mathcal{F}(U) \arrow[r, "\varphi|_U"] \arrow[d, "\mathrm{Res}_V^U"] & \mathcal{G}(U) \arrow[d, "\mathrm{Res}_V^U"] \\
\mathcal{F}(V) \arrow[r, "\varphi|_V"] & \mathcal{G}(V)
\end{tikzcd}$$

A morphism of sheaves is a morphism of presheaves between two sheaves.

Definition 2. Let $\mathcal{F}$ be a presheaf on X. The **sheafification** $\mathcal{F}^+$ is a sheaf on X with a morphism $\psi : \mathcal{F} \to \mathcal{F}^+$ satisfying the following universal property: any morphism $\varphi : \mathcal{F} \to \mathcal{G}$ to a sheaf $\mathcal{G}$ extends uniquely to a morphism $\varphi^+ : \mathcal{F}^+ \to \mathcal{G}$, i.e. such that $\varphi = \varphi^+ \circ \psi$.
The sheafification of any presheaf exists and is unique up to unique isomorphism (see [6] II.1.2).

Let $\varphi : \mathcal{F} \to \mathcal{G}$ be a morphism of sheaves. Then the **kernel** of φ, given by $\mathrm{Ker}(\varphi)(U) := \mathrm{Ker}(\varphi|_U)$ defines a sheaf on X. In general, the analogous constructions with $\mathrm{Im}(\varphi|_U)$ or $\mathrm{Coker}(\varphi|_U)$ only give presheaves; we take $\mathrm{Im}(\varphi)$ and $\mathrm{Coker}(\varphi)$ to be their respective sheafifications.

Given a point $x \in X$ and a sheaf $\mathcal{F}$ on X, we therefore have 'information' $\mathcal{F}(U)$ about any open neighborhood U of x in X. By taking limits (in an algebraic sense), we get information about x itself:

Definition 3. The **stalk** of a presheaf $\mathcal{F}$ at x is

$$\mathcal{F}_x := \varinjlim_{x \in U} \mathcal{F}(U).$$

Elements of $\mathcal{F}_x$ may be thought of as tuples (s, U), $x \in U$, $s \in \mathcal{F}(U)$ modulo the equivalence

$$(s, U) \equiv (t, V) :\Leftrightarrow s|_{U \cap V} = t|_{U \cap V}.$$

Proposition 2.1.1. *A morphism $\varphi : \mathcal{F} \to \mathcal{G}$ of sheaves is injective / surjective (i.e.* $\mathrm{Ker}(\varphi) = 0$ *or* $\mathrm{Coker}(\varphi) = 0$*) if and only if, for every $x \in X$, the induced map $\varphi_x : \mathcal{F}_x \to \mathcal{G}_x$ is injective / surjective.*

Proof. See [6] II.1 □

Definition 4. Let $f : X \to Y$ be a continuous map between topological spaces. Let $\mathcal{F}$ be a sheaf on X. Then f induces a sheaf on Y, the **direct image** of $\mathcal{F}$, given by

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

Also, if $\mathcal{G}$ is a sheaf on Y, then f induces a sheaf on X, the **inverse image**, which is the sheafification of the presheaf

$$U \mapsto \varinjlim_{f(U)\subseteq V} \mathcal{G}(V),$$

where V runs through the open subsets of Y that contain $f(U)$ - this definition is necessarily more complicated, because $f(U)$ is not generally open in Y for an open U of X.

Both the direct and inverse image are functorial. They are related by the adjunction

$$\mathrm{Hom}(f^{-1}\mathcal{G}, \mathcal{F}) = \mathrm{Hom}(\mathcal{G}, f_*\mathcal{F});$$

that is, the inverse image functor is the left adjoint of the direct image functor.

2.2 Schemes

A **locally ringed space** $(X, \mathcal{O}_X)$ is a topological space X equipped with a sheaf of commutative rings $\mathcal{O}_X$ such that for any point $x \in X$, the stalk $\mathcal{O}_{X,x}$ at x is a local ring. A morphism

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

between locally ringed spaces is a tuple consisting of a continuous map $\varphi : X \to Y$ and a sheaf morphism $\varphi^{\#} : \mathcal{O}_Y \to \mathcal{O}_X$ whose induced maps on stalks

$$\varphi^{\#}_x : \mathcal{O}_{Y,\varphi(x)} \to \mathcal{O}_{X,x}, \;\; x \in X$$

are homomorphisms that map the maximal ideal at $\varphi(x)$ onto the maximal ideal at x.

For example, given a ring R, we construct its **spectrum** as a locally ringed space $\mathrm{Spec}\, R = (X, \mathcal{O}_X)$, where X is the space of prime ideals of R, together with the **Zariski topology**, given by

$$V \subseteq X \text{ closed } \Leftrightarrow V = \{\mathfrak{p} : \mathfrak{p}|\mathfrak{a}\} \text{ for an ideal } \mathfrak{a} \leq R.$$

The sheaf $\mathcal{O}_X$, called the **structure sheaf** of $\mathrm{Spec}\, R$, is determined on the following basis of the topology of X:

$$\mathcal{O}_X\big(D(f)\big) := \mathcal{O}_X\big(X \backslash V((f))\big) := R_f = \{\frac{a}{f^n} : a \in R\}, \;\; f \in R.$$

More generally, any locally ringed space that is isomorphic to the spectrum of a ring is called an **affine scheme**. A **scheme** is a locally ringed space that is locally affine; that is, a space $(X, \mathcal{O}_X)$ with an open cover $X = \cup_{i \in I} U_i$ such that $(U_i, \mathcal{O}_X|_{U_i})$ is an affine scheme for every i.

Example: Let $R = \bigoplus_{n \in \mathbb{N}_0} R_n$ be a graded ring. We define the scheme $\mathrm{Proj}\, R = (X, \mathcal{O}_X)$, where X is the space of homogeneous ideals that do not contain $\bigoplus_{n>0} R_n$, together with the topology

$$V \subseteq X \text{ closed } \Leftrightarrow V = \{\mathfrak{p} \in X : \mathfrak{p} | \mathfrak{a}\} \text{ for some homogeneous ideal } \mathfrak{a}.$$

The structure sheaf is again defined on a basis of the topology: for f homogeneous of degree $n > 0$, let $D_+(f) := X \backslash V((f))$ and we set

$$\mathcal{O}_X(D_+(f)) := R_{(f)} = (\text{degree 0 part of } R_f).$$

Any scheme that is isomorphic to $\mathrm{Proj}\, R$ for some graded ring R is called **projective**. For example, if $R = \mathbb{C}[X_0, ..., X_n]$, then $\mathrm{Proj}\, R$ is projective n-space. More generally, for any commutative unital ring R, we define

$$\mathbb{P}^n_R := \mathrm{Proj}\, R[X_0, ..., X_n]$$

with the natural grading by polynomial degrees.

Definition 5. A scheme X is called
(i) **connected**, **irreducible**, n-dimensional ($n \in \mathbb{N}$), or **quasicompact** if this is true for the underlying topological space X;
(ii) **locally Noetherian** if it admits an open cover by spectra of noetherian rings, and **Noetherian**, if it is both locally Noetherian and quasicompact;
(iii) **reduced** if $\mathcal{O}_X(U)$ is a reduced ring (contains no nilpotent elements other than 0) for every open subset $U \subseteq X$;
(iv) **integral** if it is irreducible and reduced; equivalently, if $\mathcal{O}_X(U)$ is an integral domain for every open $U \subseteq X$.

Morphisms of schemes are just morphisms of locally ringed spaces between schemes.
The point of view of schemes as functors described below will be important:

Definition 6. Let X and S be schemes. The S**-valued points** of X are morphisms $P : S \to X$. The set of S-valued points of X is denoted $X(S)$. Given a morphism $g : S \to T$, g induces a map

$$X(g) : X(T) \to X(S), \;\; Q \mapsto Q \circ g.$$

Definition 7. Let $f : X \to \operatorname{Spec} K$ be a morphism of schemes for some field K. The **K-rational points** of X are the points $x \in X$ with residue field $\kappa(x) := \mathcal{O}_{X,x}/\mathfrak{m}_x \cong K$.

Lemma 2.2.1. *Let $f : X \to \operatorname{Spec} K$ be a scheme over a field K. The closed K-rational points of X correspond to the K-valued points $P : \operatorname{Spec} K \to X$ with $f \circ P = \mathrm{id}$.*

Proof. Let P be any such K-valued point and consider its image $x = \mathrm{Im}(P) \in X$. Let $U = \operatorname{Spec} R$ be an open affine neighborhood of x. Then P is induced by a ring homomorphism $\varphi : R \to K$ that is surjective (since $f \circ P = \mathrm{id}$) and the ideal x of R is $\ker \varphi$. Therefore, x is a closed point with residue field $R/x \cong K$.
In the other direction, let $x \in X$ be a closed K-rational point and take an open affine neighborhood $\operatorname{Spec} R$, such that x is a maximal ideal of R with $R/x \cong K$. The surjective map $\varphi : R \to K$ induces a K-valued point $P : \operatorname{Spec} K \to \operatorname{Spec} R \to X$ with $P((0)) = x$, and $f \circ P = \mathrm{id}$. □

To make the concept of 'base change' in the category of schemes explicit, we define the fiber product:

Definition 8. Let X, Y, S be schemes and $f : X \to S$, $g : Y \to S$ morphisms. The **fiber product** of X and Y over S is a scheme $Z = X \times_S Y$ together with morphisms $p : Z \to X$ and $q : Z \to Y$ such that the diagram

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

commutes and satisfies the following universal property: for any commutative diagram of schemes

$$\begin{tikzcd}
T \arrow[r, "u"] \arrow[d, "v"] & X \arrow[d, "f"] \\
Y \arrow[r, "g"] & S
\end{tikzcd}$$

there is a unique morphism $\psi : T \to Z$ of schemes such that

$$\begin{tikzcd}
T \arrow[rrd, bend left] \arrow[rd, "\psi"] \arrow[rdd, bend right] & & \\
& Z \arrow[r, "p"] \arrow[d, "q"] & X \arrow[d, "f"] \\
& Y \arrow[r, "g"] & S
\end{tikzcd}$$

commutes.

Fiber products exist in the category of schemes; if $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$ and $S = \operatorname{Spec} R$ are affine schemes, then their fiber product is given by $X \times_S Y = \operatorname{Spec} A \otimes_R B$. The morphism q as above is called the **base change** of f from S to Y along g. Importantly, for any scheme T over S, there is a bijection of sets

$$X \times_S Y(T) \mapsto X(T) \times Y(T), \quad P \mapsto (\mathrm{pr}_X \circ P, \, \mathrm{pr}_Y \circ P).$$

In particular, for any morphism $f : X \to S$, the universal property of $X \times_S X$ gives us a morphism

$$\Delta_{X/S} : X \to X \times_S X,$$

the **diagonal morphism** of X over S, corresponding to the tuple of X-valued points $(\mathrm{id}_X, \mathrm{id}_X)$ on X.

Without giving much detail or intuition, we define a number of properties of morphisms:

Definition 9. A morphism $\varphi : X \to Y$ of schemes is called
(i) **quasicompact** if there is an affine cover $Y = \cup_{i \in I} \operatorname{Spec} R_i$ such that $\varphi^{-1}(\operatorname{Spec} U_i)$ is quasicompact for all i;
(ii) **locally of finite type** if there is an affine cover as above such that $\varphi^{-1}(\operatorname{Spec} R_i)$ is a union of spectra of finitely generated R_i-algebras for all i;
(iii) **of finite type** if it is quasicompact and locally of finite type;
(iv) **affine** if there is an affine cover as above such that $\varphi^{-1}(\operatorname{Spec} R_i)$ is affine for all i;
(v) **finite** if there is an affine cover as above such that $\varphi^{-1}(\operatorname{Spec} R_i)$ is isomorphic to the spectrum of an R_i-algebra that is finitely generated as an R_i-module;
(vi) a **closed immersion** if it is a homeomorphism onto its image, its image is closed in Y, and $\varphi^{\#}$ is surjective;
(vii) **separated** if $\Delta_{X/Y} : X \to X \times_Y X$ is a closed immersion;
(viii) **universally closed** if, for any morphism $f : Z \to Y$, the base change $X \times_Y Z \to Z$ of φ along f is a closed map;

(ix) **proper** if it is separated, universally closed and of finite type;
(x) **flat** if the induced map on stalks $\varphi_P : \mathcal{O}_{Y,f(P)} \to \mathcal{O}_{X,P}$ is flat, i.e. makes $\mathcal{O}_{X,P}$ a flat $\mathcal{O}_{Y,f(P)}$-module.

Definition 10. A **closed subscheme** of a scheme X is a scheme Z where there is a closed immersion $i : Z \hookrightarrow X$. We call $\mathrm{Ker}(i^{\#})$ the **ideal sheaf** associated to Z. Conversely, given a sheaf of ideals $\mathcal{I}$; i.e. where $\mathcal{I}(U) \leq \mathcal{O}_X(U)$ for every open U is an ideal, we can associate a closed subscheme Z as the support of $\mathcal{O}_X/\mathcal{I}$ with structure sheaf $\mathcal{O}_X/\mathcal{I}$.

2.3 Sheaves of modules

Definition 11. Let $(X, \mathcal{O}_X)$ be a scheme. An $\mathcal{O}_X$**-module**, or sheaf of $\mathcal{O}_X$-modules, is a sheaf $\mathcal{F}$ of abelian groups on X such that for any open set $U \subseteq X$, $\mathcal{F}(U)$ has the structure of an $\mathcal{O}_X(U)$-module, and that for $V \subseteq U$, the restriction map Res^U_V of $\mathcal{F}$ is a homomorphism of $\mathcal{O}_X(U)$-modules - where $\mathcal{F}(V)$ inherits the structure of an $\mathcal{O}_X(U)$-module via the ring homomorphism $\mathcal{O}_X(U) \to \mathcal{O}_X(V)$.

A **morphism** $\varphi : \mathcal{F} \to \mathcal{G}$ of $\mathcal{O}_X$-modules is a morphism of sheaves such that for any open subset $U \subseteq X$, the map $\mathcal{F}(U) \to \mathcal{G}(U)$ induced by φ is a homomorphism of $\mathcal{O}_X(U)$-modules.

If $\mathcal{F}$ and $\mathcal{G}$ are sheaves of modules on $(X, \mathcal{O}_X)$, we define their tensor product as the sheafification of the presheaf

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

which we denote by $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$. We also define

$$\mathcal{H}om(\mathcal{F}, \mathcal{G})(U) := \mathrm{Hom}_{\mathcal{O}_X|_U}(\mathcal{F}|_U, \mathcal{G}|_U).$$

Definition 12. An $\mathcal{O}_X$-module $\mathcal{F}$ is called **locally free** if there is an affine cover $\{U_i\}_{i \in I}$ of X such that $\mathcal{F}|_{U_i} \cong \bigoplus_{j \in J_i} \mathcal{O}_X|_{U_i}$ for some index set J_i for every $i \in I$; in this case, the **rank** of $\mathcal{F}$ on U_i is the cardinality of J_i. If $\mathcal{F}$ is locally free and everywhere of rank 1, we call it an **invertible sheaf**.

The suggestive name ‘invertible sheaf’ is appropriate in the following sense: if $\mathcal{L}$ is an invertible sheaf, define $\mathcal{L}^{-1} := \mathcal{H}om(\mathcal{L}, \mathcal{O}_X)$; then the natural morphism $\mathcal{L} \otimes_{\mathcal{O}_X} \mathcal{L}^{-1} \to \mathcal{O}_X$ is an isomorphism.

Example: Let $X = \mathrm{Spec}\, R$ be an affine scheme and M an R-module. Then M induces an $\mathcal{O}_X$-module $\widetilde{M}$ via

$$\widetilde{M}\big(D(f)\big) := M_f := M \otimes_R R_f = \{\frac{m}{f^n} : m \in M,\ n \in \mathbb{N}\},\ \ f \in R.$$

Generally, if $(X, \mathcal{O}_X)$ is a sheaf and $\mathcal{F}$ is an $\mathcal{O}_X$-module that is of the form $\widetilde{M_i}/U_i$ on an affine cover $X = \cup_{i \in I} U_i$, we call $\mathcal{F}$ **quasicoherent**. If the M_i are such that all submodules are finitely presented over R_i, we call $\mathcal{F}$ **coherent**; in the case that X is Noetherian, it is enough to require that M_i is finitely generated.

2.4 Sheaf cohomology

Let X be a scheme. We can consider 'taking global sections' to be a functor $\Gamma(X, -)$, defined on, for example, the category of abelian sheaves, of $\mathcal{O}_X$-modules or of quasicoherent $\mathcal{O}_X$-modules, and mapping to the category of abelian groups, or to $\Gamma(X, \mathcal{O}_X)$-modules, respectively. In all cases, $\Gamma(X, -)$ is right-exact. It is known ([6], III.2) that all of the above categories have enough injective objects; that is, for any object A, there exists an exact sequence

$$0 \to A \to I^0 \to I^1 \to ...$$

with injective objects $I^\bullet$.

Definition 13. Let $\mathcal{F}$ be an abelian sheaf on X. The **cohomology groups** of $\mathcal{F}$ are the right-derived functors of $\Gamma(X, -)$ at $\mathcal{F}$; that is, we take any injective resolution

$$0 \to \mathcal{F} \to \mathcal{I}^\bullet$$

and set

$$H^k(X, \mathcal{F}) := R^k\Gamma(X, \mathcal{F}) = H^k(\Gamma(X, \mathcal{I}^\bullet)).$$

By standard arguments of homological algebra, this is independent up to isomorphism of the choice of $\mathcal{I}^\bullet$.

There are other ways of computing sheaf cohomology than by finding an injective resolution. For example, we define the Godement resolution: for any sheaf $\mathcal{F}$ on a scheme X, define the sheaf

$$G(\mathcal{F})(U) := \prod_{x \in U} \mathcal{F}_x, \;\; U \subseteq X \text{ open}.$$

There is a natural morphism $d^0 : \mathcal{F} \to G(\mathcal{F})$. Now define $G^0 := G(\mathcal{F})$ and for $k > 0$,

$$G^k := G(\mathrm{Coker}(d^{k-1})), \;\; d^k : G^{k-1} \to G^k.$$

Then the cohomology of $\mathcal{F}$ can be computed as the cohomology of the complex $G^\bullet$.

Another construction, more adapted to computation, is the Čech complex.

Definition 14. Let $\mathcal{U} = (U_i)_{i=1}^n$ be a finite cover of X by open subsets. Let I_p be the set of all subsets of $\{1, ..., n\}$ having $p+1$ elements, and for $J \in I_p$ define $X_J := \cap_{i \in J} U_i$. We define

$$\check{C}^p(\mathcal{U}, \mathcal{F}) := \prod_{J \in I_p} \mathcal{F}(U_J)$$

together with the coboundaries

$$\mathrm{d}^p : \check{C}^{p-1}(\mathcal{U}, \mathcal{F}) \to \check{C}^p(\mathcal{U}, \mathcal{F}), \;\; (s_J)_{J \in I_{p-1}} \mapsto \Big(\sum_{i=0}^{p} (-1)^i s_{J \setminus \{j_i\}} \Big)_{J = \{j_0 < ... < j_p\} \in I_p}.$$

This gives us a cochain complex

$$\check{C}^0(\mathcal{U}, \mathcal{F}) \longrightarrow \check{C}^1(\mathcal{U}, \mathcal{F}) \longrightarrow \check{C}^2(\mathcal{U}, \mathcal{F}) \longrightarrow ...$$

called the **Čech complex**. The cohomology groups $\check{H}^k(\mathcal{U}, \mathcal{F}) := H^k(\check{C}^\bullet(\mathcal{U}, \mathcal{F}))$ are called the **Čech cohomology** of $\mathcal{F}$ with respect to the cover $\mathcal{U}$.

Čech cohomology is usually much easier to calculate than sheaf cohomology via derived functors as above. However, they do not give the same results in general - we need for the scheme X and sheaf $\mathcal{F}$ to be ‘nice enough’. To be precise, we have the following comparison result:

Theorem 2.4.1. *Let X be a noetherian, separated scheme and $\mathcal{U}$ a finite cover of X by open affine sets. Let $\mathcal{F}$ be a quasicoherent sheaf of $\mathcal{O}_X$-modules. Then there are natural isomorphisms, functorial in $\mathcal{F}$:*

$$\check{H}^p(\mathcal{U}, \mathcal{F}) \xrightarrow{\sim} H^p(X, \mathcal{F}), \;\; p \geq 0.$$

Proof. See [6] III.4.5 □

2.5 Algebraic curves

Let K be an algebraically closed field.

Definition 15. An **algebraic curve** C/K is a one-dimensional projective variety over K. Its **genus** is

$$g := \dim_K H^1(C, \mathcal{O}_C).$$

Recall that the term variety means that C is integral and separated and the implied map $C \to \operatorname{Spec} K$ is of finite type. Classically, C can be thought of as the locus of zeros of some homogeneous polynomial $P(x, y, z)$ in three variables.

The **function field** $K(C)$ of C is the field of fractions of $\Gamma(U, \mathcal{O}_C)$ for any open affine subset $U \subseteq C$; these are all isomorphic. It is known ([6] I.6) that there is an antiequivalence of categories

$$\begin{pmatrix}\text{algebraic curves over } K\\ \text{with surjective morphisms}\end{pmatrix} \leftrightarrow \begin{pmatrix}\text{field extensions of } K \text{ of transcendence degree } 1\\ \text{with field homomorphisms fixing } K\end{pmatrix}.$$

Here, a curve C is mapped to its function field $K(C)$, and a morphism $\varphi : C_1 \to C_2$ is mapped to

$$\varphi^* : K(C_2) \to K(C_1), \quad f \mapsto f \circ \varphi;$$

where $f \in K(C)$ is interpreted as a function $f : C \to K$. The **degree**, **separability degree** and **inseparability degree** of φ are defined as the respective degree of the field extension $K(C_1)/\varphi^* K(C_2)$.

Of course, any morphism of curves over a field of characteristic 0 must be separable. In characteristic $p > 0$, any extension of fields can be factored into a separable and purely inseparable extension, and so this carries over to morphisms of curves:

Lemma 2.5.1. *Let $\varphi : C_1 \to C_2$ be a morphism of curves over a field of characteristic $p > 0$. Then φ factors as $\mathrm{Frob}_q \circ \psi$, where $q = \deg_i(\varphi)$, Frob_q is the q-th power Frobenius map coming from the Frobenius $x \mapsto x^q$ on $K(C_1)$, and ψ is separable.*

Proof. Let L be the separable closure of $\varphi^* K(C_2)$ in $K(C_1)$, such that we have the tower of extensions

$$K(C_1)/L/\varphi^* K(C_2)$$

where $K(C_1)/L$ is purely inseparable, $[K(C_1) : L] = q$ and $L/\varphi^* K(C_2)$ is separable. It follows that $K(C_1)^q$ is contained in L, and since $[K(C_1) : L] = q = [K(C_1) : K(C_1)^q]$, we have $L = K(C_1)^q$. The inclusions

$$\varphi^* K(C_2) \longrightarrow K(C_1)^q \longrightarrow K(C_1)$$

correspond to morphisms

$$C_1 \xrightarrow{\mathrm{Frob}_q} C_1 \xrightarrow{\psi} C_2$$

that combine to give φ. □

Chapter 3

Elliptic Curves

3.1 Elliptic curves over fields

Let $K = \overline{K}$ be an algebraically closed field.

Definition 16. An **elliptic curve** over K is a smooth curve $f : E \to \operatorname{Spec} K$ over K of genus 1, together with a distinguished K-rational point O.

For any subfield $L \subset K$, we define $E(L)$ to be the set of L-rational points of E.

The study of elliptic curves is actually much more explicit than this definition suggests. One can show using the Riemann-Roch theorem that elliptic curves are exactly the projective varieties given by a **Weierstrass equation**

$$E : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

with elements $a_i \in K$ and nonsingular discriminant; that is, $E(K)$ is the locus of solutions of this equation in projective space $\mathbb{P}^2_K$. If we assume that $\operatorname{char} K \neq 2, 3$ (which greatly simplifies calculations), this can be manipulated to an equation of the form

$$E : Y^2Z = X^3 + pXZ^2 + qZ^3$$

with $p, q \in K$. Letting $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ be dehomogenized coordinates, we will also write this as

$$E : y^2 = x^3 + px + q;$$

the locus of solutions is then $E(K)\backslash O$, with O given in projective coordinates by $[0 : 1 : 0]$.

Definition 17. (i) The **discriminant** of the Weierstrass equation $y^2 = x^3 + px + q$ is

$$\Delta(p, q) := -16(4p^3 + 27q^2).$$

(ii) The j**-invariant** of the Weierstrass equation $y^2 = x^3 + px + q$ with $\Delta(p,q) \neq 0$ is

$$j(p,q) := \frac{1728 \cdot 4p^3}{4p^3 + 27q^2}.$$

The Weierstrass equation describing a given elliptic curve is not unique, and neither is the discriminant. However, the j-invariant lives up to its name:

Theorem 3.1.1. *Two Weierstrass equations define isomorphic elliptic curves if and only if they have the same j-invariant.*

Proof. See [20] III.1.4 □

One fundamental aspect of elliptic curves is their group law. There is a natural way of adding two points on an elliptic curve to give a third that makes $E(K)$ an abelian group with neutral element O.

Definition 18. The **Weil divisors** on an elliptic curve E are elements

$$D = \sum_{P \in E(K)} n_P \cdot (P) \in \bigoplus_{P \in E(K)} \mathbb{Z}.$$

The **degree** of a divisor $D = \sum_P n_P \cdot (P)$ is

$$\deg D := \sum_{P \in E(K)} n_P.$$

The divisors of degree 0 over K form a subgroup that we denote $\mathrm{Div}^0(E)$. A divisor is **principal** if it is of the form

$$\operatorname{div} f := \sum_{P \in E(K)} \mathrm{ord}_P(f) \cdot (P)$$

for some rational function $f \in K(E) := \Gamma(E, \mathrm{Quot}(\mathcal{O}_E))$.

It is known that $\operatorname{div} K(E) \subseteq \mathrm{Div}^0_K(E)$. ([20] III.3.1). We define the **degree** 0 **divisor class group**

$$\mathrm{Pic}^0(E) := \mathrm{Div}^0(E)/\mathrm{Im}(\mathrm{div}).$$

Theorem 3.1.2. *The map*

$$\kappa : E(K) \to \mathrm{Pic}^0(E), \;\; P \mapsto [(P) - (O)]$$

is a bijection of sets. The group law on $\mathrm{Pic}^0(E)$ *induces a group law on* $E(K)$*. If* K/L *is a field extension, then the* L*-rational points* $E(L)$ *form a subgroup of* $E(K)$*.*

Proof. See [20], III.3.4 □

3.2 Elliptic functions and elliptic curves over $\mathbb{C}$

The most important case for us will be that of elliptic curves over the base field $\mathbb{C}$ - by fixing a complex embedding, the results will be applicable to elliptic curves over number fields. This theory has a strong connection to complex analysis. We will show that elliptic curves over $\mathbb{C}$ are essentially the quotient spaces of $\mathbb{C}$ by lattices, and that the rational functions on elliptic curves correspond to meromorphic and doubly periodic functions.

In this section, we fix a lattice Λ and generating periods $\omega_1, \omega_2 \in \mathbb{C}$, i.e. $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, and ω_1 and ω_2 are linearly independent over $\mathbb{R}$.

Definition 19. An **elliptic function** is a meromorphic function $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ which is periodic with respect to Λ:

$$\forall \omega \in \Lambda,\ \forall z \in \mathbb{C} :\ \ f(z+\omega) = f(z).$$

Immediate examples of elliptic functions are the constant functions. One promising approach to giving non-trivial examples is the series

$$E_k(z) := \sum_{\omega \in \Lambda} \frac{1}{(z+\omega)^k} \ \ (k \geq 3);$$

these converge absolutely and uniformly on compact subsets of $\mathbb{C} \backslash \Lambda$, and the periodicity is clear. Uniform convergence implies that they can be differentiated by terms, so we get

$$\frac{d}{dz} E_k(z) = -kE_{k+1}(z) \ \ \forall k \geq 3.$$

Difficulties arise in the cases $k = 1$ and $k = 2$, because the series no longer converges absolutely. We define another series to take the role of E_2:

Definition 20. The **Weierstrass $\wp$-function** is an elliptic function defined by the series

$$\wp(z) := \frac{1}{z^2} + \sum_{\omega \in \Lambda \backslash \{0\}} \Big(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \Big).$$

It follows that $\wp'(z) = -\frac{2}{z^3} - \sum_{\omega \neq 0} \frac{2}{(z+\omega)^3} = -2E_3(z)$.
These functions are essentially the only elliptic functions. We will make this statement precise soon; for now, we prove some results about elliptic functions.

Lemma 3.2.1. *(i) Any holomorphic elliptic function is constant.*
(ii) An elliptic function f has finitely many poles modulo Λ, and it holds $\sum_{z \in \mathbb{C}/\Lambda} \mathrm{Res}(f; z) = 0$ for any set of their representatives.

Proof. (i) Let f be holomorphic and elliptic. By continuity, f is bounded on the convex hull M of 0, ω_1, ω_2 and $\omega_1+\omega_2$, and by periodicity it is bounded everywhere. Liouville's theorem implies that f is constant.
(ii) The set of poles of f is discrete, and therefore finite on the compact set M. The residue theorem gives

$$\sum_{z\in M}\mathrm{Res}(f;z)=\frac{1}{2\pi i}\int_{\partial M}f(w)dw$$

$$=\frac{1}{2\pi i}\Big(\int_0^{\omega_1}f(w)dw+\int_{\omega_1}^{\omega_1+\omega_2}f(w)dw+\int_{\omega_1+\omega_2}^{\omega_2}f(w)dw+\int_{\omega_2}^{0}f(w)dw\Big),$$

where the integrals are taken over each line segment, respectively; substituting w for $w-\omega_2$ in the third integral and $w-\omega_1$ in the fourth, we find

$$\int_{\omega_1+\omega_2}^{\omega_2}f(w)dw=\int_{\omega_1}^{0}f(w-\omega_2)dw=-\int_0^{\omega_1}f(w)dw$$

and so the third and first integrals cancel each other; similarly, the fourth and second integrals cancel each other, so the sum of all is zero. □

The following result follows:

Proposition 3.2.2. *(i) Any elliptic function w.r.t. a lattice Λ without poles in $\mathbb{C}\backslash\Lambda$ is a finite linear combination of $1,\wp$ and $E_k,\ k\geq 3$.*
(ii) Any even elliptic function w.r.t. Λ without poles in $\mathbb{C}\backslash\Lambda$ is a polynomial in $\wp$.

Proof. (i) Note that $\wp(z)-\frac{1}{z^2}$ and $E_k(z)-\frac{1}{z^k}$ $(k\geq 3)$ have removable singularities in 0. Now let $f(z)$ be an elliptic function which is holomorphic on $\mathbb{C}\backslash\Lambda$, and write it as a Laurent series $f(z)=\sum_{k=-N}^{\infty}a_kz^k$ centered at 0. (ii) of the above lemma implies that $a_{-1}=\mathrm{Res}(f;z)=0$; and therefore

$$f-a_{-2}\wp(z)-\sum_{k=3}^{N}a_{-k}E_k(z)$$

is a holomorphic elliptic function, i.e. a constant.
(ii) We will use induction on the order of its pole in 0. Since f is even, the order of its pole must be even. If it is zero, f is constant and the result is trivial. Otherwise, letting $2n$ denote the order and a_{-2n} the corresponding coefficient of the Laurent series centered at 0, we see that $f-a_{-2n}\wp^n$ is even and has a pole of lesser order than $2n$

$$\text{(because } \wp^n(z)=\frac{1}{z^{2n}}+\{\text{higher terms}\})$$

so it is a polynomial in $\wp$. □

We can now show a general structure theorem with little effort:

Theorem 3.2.3. *Every elliptic function w.r.t. Λ is a rational function in $\wp$ and $\wp'$.*

Proof. Let f be an even elliptic function; recall that f has only finitely many poles modulo Λ. If $a \notin \Lambda$ is a pole of f, we can multiply f by an appropriate power of $\wp(z) - \wp(a)$ to get a function with fewer poles; after a short inductive step, we may assume without loss of generality that f has no poles outside of Λ, and therefore is a polynomial in $\wp$.
For general f, we have

$$f(z) = \frac{f(z) + f(-z)}{2} + \wp'(z)\frac{f(z) - f(-z)}{2\wp'(z)}$$

where $\frac{f(z)+f(-z)}{2}$ and $\frac{f(z)-f(-z)}{2\wp'(z)}$ are even elliptic functions. □

The results until now have limited the possibilities for elliptic functions; we now give a result which guarantees the existence of elliptic functions with certain poles and zeros.

Definition 21. A **divisor** is an element of the direct sum $\oplus_{z \in \mathbb{C}/\Lambda}\mathbb{Z}$. The divisor associated to an elliptic function f is

$$\mathrm{div} f = \sum_{z \in \mathbb{C}/\Lambda} \mathrm{ord}(f; z)(z).$$

Theorem 3.2.4. *The divisor* $\sum_{z \in \mathbb{C}/\Lambda} a_z(z)$ *comes from an elliptic function if*

$$\sum_{z \in \mathbb{C}/\Lambda} a_z = 0 \text{ and } \sum_{z \in \mathbb{C}/\Lambda} a_z z = 0.$$

Proof. We will construct such a function explicitly. To do this, we introduce the **Weierstrass σ-function**, which is defined via an absolutely convergent product

$$\sigma(z) := z \prod_{\omega \in \Lambda \setminus \{0\}} \Big((1 - \frac{z}{\omega}) \exp(\frac{z}{\omega} + \frac{1}{2}(\frac{z}{\omega})^2)\Big).$$

This follows the method given by the Weierstrass product theorem to construct an entire function with zeros exactly in the points of Λ. Its logarithmic derivative is

$$\frac{\sigma'(z)}{\sigma(z)} = \frac{1}{z} + \Big(\sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{z + \omega} - \frac{1}{\omega} - \frac{z}{\omega^2}\Big);$$

the derivative of this, in turn, is then $-\wp(z)$.

For any fixed $\omega_0 \in \Lambda$, $\frac{\sigma(z+\omega_0)}{\sigma(z)}$ is entire without zeros, and therefore expressible as $\exp(h(z))$ for some entire function $h(z)$. After some algebraic manipulation we find

$$h''(z) = \Big(\frac{\sigma'(z + \omega_0)}{\sigma(z + \omega_0)}\Big)' - \Big(\frac{\sigma'(z)}{\sigma(z)}\Big)' = \wp(z) - \wp(z + \omega_0) = 0,$$

so $h(z)$ is a linear polynomial; this implies the addition formula

$$\sigma(z + \omega_0) = C_0 \sigma(z) e^{\eta_0 z}$$

for constants C_0 and η_0 that depend on ω_0.

Choose now fixed representatives z_k for the nontrivial components of the given divisor, and define the function

$$f(z) := \prod_k \sigma(z - z_k)^{a_k}.$$

Then for $\omega_0 \in \Lambda$,

$$\frac{f(z+\omega_0)}{f(z)} = \prod_k C_0^{a_k} \exp(a_k \eta_0 (z - a_k)) = \Big(C_0 \exp(\eta_0 z)\Big)^{\sum a_k} \exp(-\eta_0 \sum a_k z_k) = 1.$$

Thus f is elliptic; and it is easily seen that $(f) = \sum_{z \in \mathbb{C}/\Lambda} a_z(z)$. □

The proof of 2.2.2(ii) shows that we can express the even function $\wp'(z)^2 = 4E_3(z)^2$ as a cubic polynomial in $\wp$. To construct this, we look at the Laurent series.

Proposition 3.2.5. *Denote by G_{2j}, $j \geq 2$ the* ***homogeneous Eisenstein series***

$$G_{2j} := \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{\omega^{2j}}.$$

Then the Laurent expansions of $\wp$ and E_k at 0 are given by

$$\wp(z) = \frac{1}{z^2}\Big(1 + \sum_{n=2}^{\infty} (2n-1) G_{2n} z^{2n}\Big)$$

and

$$E_k(z) = \frac{1}{z^k}\Big(1 + (-1)^k \sum_{n=2}^{\infty} \binom{2n-1}{k-1} G_{2n} z^{2n}\Big).$$

Proof. The function $\wp(z) - \frac{1}{z^2}$ is holomorphic on a neighborhood of 0; successively differentiating gives

$$\frac{d^k}{dz^k}(\wp(z) - \frac{1}{z^2}) = (-1)^k (k+1)! \Big(E_{k+2}(z) - \frac{1}{z^{k+2}}\Big)$$

and evaluating this at zero gives the k-th power series coefficient

$$\frac{1}{k!}\frac{d^k}{dz^k}(\wp(z) - \frac{1}{z^2})|_{z=0} = (-1)^k (k+1) G_{k+2};$$

since $G_k = 0$ for odd k, the result follows.
The second Laurent series can be obtained similarly, or by successive differentiation of the first. □

Proposition 3.2.6.

$$\wp'(z)^2 = 4\wp(z)^3 - 60 G_4 \wp(z) - 140 G_6.$$

Proof. From the above Laurent series follows

$$\wp(z)^3 = \frac{1}{z^6}\Big(1 + 3G_4z^4 + 5G_6z^5 + ...\Big)^3 = \frac{1}{z^6} + 36G_4\frac{1}{z^2} + 60G_6 + ...$$

and

$$\wp'(z)^2 = \frac{4}{z^6}\Big(1 - 2G_4z^4 - 10G_6z^6 - ...\Big)^2 = \frac{4}{z^6} - 24G_4\frac{1}{z^2} - 80G_6 - ...$$

It follows that

$$\wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) = -140G_6 + ...$$

and being a holomorphic elliptic function, it must be equal to its constant term $-140G_6$. □

The numbers $60G_4$ and $140G_6$ will appear often. They are called **Weierstrass invariants** and denoted by g_2 and g_3, respectively.

The differential equation satisfied by $\wp$ bears a strong resemblance to the Weierstrass equation defining an elliptic curve. In fact, it defines the structure of an elliptic curve on the torus $\mathbb{C}/\Lambda$. We will describe this soon: first, it needs to be observed that the discriminant of that Weierstrass equation will be nonzero.

Lemma 3.2.7. *The zeros of* $4X^3 - g_2X - g_3$ *are distinct, and given by* $\wp(\frac{\omega_1}{2})$, $\wp(\frac{\omega_2}{2})$ *and* $\wp(\frac{\omega_1+\omega_2}{2})$.

Proof. This is because

$$\wp'(\frac{\omega_1}{2}) = -\wp'(-\frac{\omega_1}{2}) = -\wp'(\frac{\omega_1}{2}),$$

since $\wp'$ is an odd elliptic function, and therefore $\wp'(\frac{\omega_1}{2}) = 0$. $\frac{\omega_2}{2}$ and $\frac{\omega_1+\omega_2}{2}$ are analogous. These zeros are distinct: assume without loss of generality that $\wp(\frac{\omega_1}{2}) = \wp(\frac{\omega_2}{2}) =: c \in \mathbb{C}$. We have

$$0 = \sum_{z\in\mathbb{C}/\Lambda} \mathrm{Res}(\frac{\wp'}{\wp - c}; z) = \sum_{z\in\mathbb{C}/\Lambda} \mathrm{ord}(\wp - c; z) \geq 2$$

since $\wp - c$ has only one pole modulo Λ, of order 2 in $z = 0$, and a zero of order at least 2 in both $\frac{\omega_1}{2}$ and $\frac{\omega_2}{2}$ (because $\wp'(\frac{\omega_i}{2}) = 0$), which are distinct modulo Λ. This is a contradiction. □

Theorem 3.2.8. *Let* E_Λ *be the projective elliptic curve*

$$E_\Lambda : Y^2Z = 4X^3 - g_2XZ^2 - g_3Z^3.$$

Then the map

$$\psi : \mathbb{C}/\Lambda \to E_\Lambda, \ \ z + \Lambda \mapsto [\wp(z) : \wp'(z) : 1], \ \ 0 + \Lambda \mapsto [0 : 1 : 0]$$

is an analytic isomorphism of Riemann surfaces. Under ψ*, the group law on* E_Λ *corresponds to addition on* $\mathbb{C}/\Lambda$*, and rational functions from* E_Λ *to* $\mathbb{C}$ *correspond to elliptic functions with respect to* Λ.

Proof. E_Λ inherits the structure of a Riemann surface with respect to the atlas

$$P = [x : y : 1] \mapsto x \text{ if } \frac{dy^2}{dy} = 2y \neq, 0$$
$$P = [x : y : 1] \mapsto y \text{ if } \frac{d(4x^3 - g_2x - g_3)}{dx} = 12x^2 - g_2 \neq 0,$$
$$O = [0 : 1 : 0] \mapsto 0.$$

The structure on $\mathbb{C}/\Lambda$ is defined in the obvious way. ψ is analytic outside of $0 \in \mathbb{C}/\Lambda$ since $\wp$ and $\wp'$ are analytic outside of Λ, and ψ is analytic in 0 because $\frac{\wp}{\wp'}$ has only removable singularities in Λ.

As a nonconstant map between compact Riemann surfaces, ψ must be a covering map (i.e. discrete and bicontinuous) of some degree $d \geq 0$, which means that the fiber over any point of E_Λ contains exactly d elements. From the commutative diagram

$$\begin{tikzcd}
\mathbb{C}/\Lambda \arrow[rr, "\psi"] \arrow[dr, "\wp"] & & E_\Lambda \arrow[dl, "x"] \\
& \mathbb{P}_1(\mathbb{C}) &
\end{tikzcd}$$

where $\wp$ is a covering map of degree 2 as it is an elliptic function of order 2, and the coordinate function x is a covering map of degree 2; it follows that ψ has degree one and is therefore an isomorphism.

Under ψ, the rational functions on E_Λ correspond to the rational functions in $\wp$ and $\wp'$, which are exactly the elliptic functions (or rather, the meromorphic functions on $\mathbb{C}/\Lambda$).

For the final statement, let z_1 and $z_2 \in \mathbb{C}/\Lambda$ be arbitrary and find an elliptic function f whose divisor is given by

$$\text{div} f = (z_1 + z_2) - (z_1) - (z_2) + (0).$$

Let $\psi^* : \mathbb{C}(E_\Lambda) \to \mathbb{C}(\mathbb{C}/\Lambda)$ be the isomorphism on function fields induced by ψ; then $\psi^* R = f$ for some rational function R on E_Λ and it holds

$$\text{div} R = (\psi(z_1 + z_2)) - (\psi(z_1)) - (\psi(z_2)) + (\psi(0)).$$

Since the latter is a principal divisor, and it holds that

$$\sum_P n_P(P) \text{ principal divisor } \implies \bigoplus_P n_P P = O,$$

it follows that $\psi(z_1 + z_2) = \psi(z_1) \oplus \psi(z_2)$. □

Remark: ψ maps the natural differential $dz = \frac{d\wp(z)}{\wp'(z)}$ to $\frac{dx}{y}$. We can recover Λ as the lattice of values $\int_\gamma \frac{dx}{y}$, where $\gamma \in \pi(E_\Lambda)$ is an element of the topological fundamental group.

We have now constructed a large class of elliptic curves over $\mathbb{C}$. In fact, any such curve is isomorphic to a E_Λ for an appropriately chosen lattice Λ. The proof of this will take some additional effort. Motivated by the case of the C_Λ, we make the following definition:

Definition 22. The j**-function** is defined on lattices Λ by

$$j(\Lambda) := \frac{1728 g_2^3}{g_2^3 - 27 g_3^2}.$$

If we replace Λ by a scalar multiple $z\Lambda$, $z \in \mathbb{C}^\times$, it remains the same:

$$j(z\Lambda) = \frac{1728(z^{-4}g_2)^3}{(z^{-4}g_2)^3 - 27(z^{-6}g_3)^2} = j(\Lambda).$$

By multiplying Λ with either $\frac{1}{\omega_1}$ or $\frac{1}{\omega_2}$, as appropriate, we can obtain a lattice of the form $\mathbb{Z} \oplus \mathbb{Z}\tau$ with $\mathfrak{Im}[\tau] > 0$; we then define

$$j(\tau) := j(\mathbb{Z} \oplus \mathbb{Z}\tau).$$

It is therefore clear that $j(\tau + 1) = j(\tau)$ and $j(-\tau^{-1}) = j(\tau)$.

Lemma 3.2.9. *Let* $\mathfrak{H} = \{z \in \mathbb{C} : \ \mathfrak{Im}[z+ > 0\}$. *Then* $j : \mathfrak{H} \to \mathbb{C}$ *is surjective.*

Proof. j is holomorphic, since $g_2^3 - 27g_3^2$ has no zeros; this is up to a factor of 16 the discriminant of $4X^3 - g_2X - g_3$, which we saw previously to have distinct roots for every lattice in $\mathbb{C}$. The open mapping theorem implies that $j(\mathfrak{h})$ is open.
One can show that $j(\tau)$ is unbounded as $\mathfrak{Im}(\tau)$ becomes large; indeed, its Fourier series is given by

$$j(\tau) = q^{-1} + 744 + 196884q + ... \ \ (q = e^{2\pi i \tau}).$$

] If (w_k), $w_k = j(z_k)$, is any convergent sequence in $j(\mathfrak{H})$, then the $\mathfrak{Im}(z_k)$ must be bounded; therefore, we can choose representatives for these in a shortened fundamental domain $\{\tau \in \mathfrak{H} : |\tau| \geq 1, \ |\mathfrak{Re}(\tau)| \leq 1, \ |\mathfrak{Im}(\tau) \leq M\}$. This is a compact set, and so (z_k) has a converging subsequence; if its limit is denoted z, then we have $j(z) = \lim_{k\to\infty} w_k \in j(\mathfrak{H})$.

Therefore, $j(\mathfrak{H})$ is both open and closed in $\mathbb{C}$; as it is nonempty, it must be all of $\mathbb{C}$. □

Theorem 3.2.10. *Every elliptic curve over* $\mathbb{C}$ *is isomorphic over* $\mathbb{C}$ *to a curve of the form* E_Λ.

Proof. Let

$$E : Y^2 = X^3 + aX + b$$

be a given Weierstrass equation. Then we can find a lattice Λ in $\mathbb{C}$ such that $j(E) = j(\Lambda)$, which is the j-invariant of $j(E_\Lambda)$ by construction. Therefore, C is isomorphic to E_Λ over $\mathbb{C}$. □

Theorem 3.2.11. *Two elliptic curves E_{Λ_1} and E_{Λ_2} are isomorphic over $\mathbb{C}$ if and only if the lattices Λ_1 and Λ_2 are* ***homothetic****, that is,*

$$\exists \alpha \in \mathbb{C}^\times : \ \Lambda_1 = \alpha\Lambda_2.$$

Proof. If the lattices are homothetic, then they have the same j-invariant; this implies that the curves E_{Λ_1} and E_{Λ_2} are isomorphic. On the other hand, if E_{Λ_1} and E_{Λ_2} are isomorphic, then $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are analytically isomorphic as Riemann surfaces; this is induced by an analytic map $g : \mathbb{C} \to \mathbb{C}$ such that

$$\forall \omega \in \Lambda_1, \ \forall z \in \mathbb{C} : \quad g(z + \omega) - g(z) \in \Lambda_2.$$

Since Λ_2 is discrete, $g(z+\omega) - g(z)$ must be constant for fixed ω; thus $g'(z)$ is a holomorphic elliptic function, and is therefore a constant α^{-1}. We find $\Lambda_1 = \alpha\Lambda_2$. □

Similarly, it may be seen that two curves E_{Λ_1} and E_{Λ_2} are **isogenous**, i.e. there exists a nonconstant morphism $\varphi : E_{\Lambda_1} \to E_{\Lambda_2}$ sending O to O, if and only if there exists $\alpha \in \mathbb{C}$ with $\Lambda_1 \subseteq \alpha\Lambda_2$.

3.3 Reduction

Consider a field K with a discrete valuation $v : K^\times \to \mathbb{Z}$; this extends uniquely to a valuation $\overline{v} : \overline{K} \to \mathbb{Q}$ on a fixed algebraic closure of K. Let $\mathcal{O}_K := \{x \in K : v(x) \geq 0\}$ be the valuation ring of v and $\mathfrak{m}$ its maximal ideal. Assume in the following that the residue field $k := R/\mathfrak{m}$ is perfect.

An elliptic curve E/K is given by a Weierstrass equation, and this choice is not unique. By an appropriate change of variables, we may choose a Weierstrass equation with coefficients in R. Any such change of variables will change the discriminant by a power of 12 and therefore its valuation by a multiple of 12; see [20] III.1.3.

Definition 23. The R-scheme $f : X \hookrightarrow \mathbb{P}^2_R \to \operatorname{Spec} R$ defined by this Weierstrass equation over R is called a **model** for E. If $v(\Delta)$ is minimal among all models, it is called a **minimal model**. The **special fiber**

$$\tilde{E} := f^{-1}(\mathfrak{m}) = X \times_{\operatorname{Spec} R} \operatorname{Spec} k$$

is called the **reduction** of E at v.

The reduction of E at any valuation of K remains a projective curve of genus 1. In general, it may not be non-singular; however, it has at most one singularity:

Lemma 3.3.1. *Let X/k be the projective variety given by a Weierstrass equation. Then X has at most one singularity.*

Proof. For simplicity assume that $\operatorname{char} k \neq 2, 3$; then, X is given by an equation of the form

$$X : y^2 = x^3 + px + q.$$

At any singularity of X, both partial derivatives must vanish; that is, $2y = 3x^2 + p = 0$. It follows that $y = 0$ and x is a double root of $x^3 + px + q$; there can be at most one such point. □

At any singular point (x_0, y_0) of X, the equation $f(x, y) = y^2 - x^3 - px - q$ is given by a Taylor expansion

$$f(x,y) - f(x_0, y_0) = \Big((y - y_0) - \alpha(x - x_0)\Big)\Big((y - y_0) - \beta(x - x_0)\Big) - (x - x_0)^3$$

for some $\alpha, \beta \in \overline{K}$. The tangent lines to X in (x_0, y_0) are given by

$$y - y_0 = \alpha(x - x_0), \;\; y - y_0 = \beta(x - x_0).$$

We distinguish four cases:

Definition 24. Let E/K be an elliptic curve and v a discrete valuation of K.
(i) E has **good reduction** at v if $\tilde{E}$ is nonsingular - i.e. an elliptic curve over k.
(ii) E has **additive reduction** at v if it has a singularity and $\alpha = \beta$.
(iii) E has **split multiplicative reduction** at v if it has a singularity and $\alpha \neq \beta$, $\alpha, \beta \in K$.
(iv) E has **non-split multiplicative reduction** at v if it has a singularity and $\alpha \neq \beta$, $\alpha, \beta \notin K$.

Example: Over $\mathbb{Q}$, no elliptic curve can have good reduction at every prime p - because no Weierstrass equation with integer coefficients can be given such that the discriminant is a unit.

Proposition 3.3.2. *(i) Let E be an elliptic curve over K and v a valuation. Then there is a finite extension L/K such that $E \times_K L$ has either good or split multiplicative reduction over L at v_L, the valuation of L extending K.*
(ii) If E has good or multiplicative reduction at v and L/K is a finite extension of fields, then $E \times_K L$ has good or multiplicative reduction, respectively, at v_L.

Proof. See [20] VII.5.4 □

We say that E has **potential good** or **potential multiplicative** reduction at v if there is $E \times_K L$ has good or multiplicative reduction at v_L for some finite extension L/K. There is a simple criterion for potential good reduction:

Proposition 3.3.3. *E has potential good reduction at v if and only if $v(j(E)) \geq 0$.*

Proof. See [20] Silverman VII.5.5 □

Isogenies are respected by (good) reduction:

Proposition 3.3.4. *Let E_1 and E_2 be two elliptic curves over K with good reduction at $\mathfrak{p}$. Then*

$$\operatorname{Hom}(E_1, E_2) \to \operatorname{Hom}(\tilde{E_1}, \tilde{E_2}), \quad \varphi \mapsto \tilde{\varphi}$$

is injective, and for any isogeny $\varphi : E_1 \to E_2$, $\deg \varphi = \deg \tilde{\varphi}$.

Proof. See [19] II.4.4 □

3.4 Elliptic curves as S-schemes

In the most general case, we can consider elliptic curves not necessarily defined over a field, but rather over an arbitrary ring; or, even more generally, over an arbitrary scheme.

Definition 25. Let S be a scheme. An **elliptic curve** over S is a scheme E, together with a proper, smooth morphism $f : E \to S$ and a closed immersion $O : S \to E$, such that $f \circ O = \mathrm{id}_S$ and that all fibers

$$E_s := E \times_S \operatorname{Spec} k(s), \quad s \in S$$

are geometrically connected (i.e. connected over the algebraic closure) curves of genus 1 over $k(s)$.

In the case that $S = \operatorname{Spec} K$ for some algebraically closed field K, this generalizes the classical definition. Morally, we may think of E as a family of elliptic curves E_s, parameterized by the points of S - this is the point of view of deformation theory.

Perhaps surprisingly, if $S = \operatorname{Spec} R$ is affine, where R is noetherian and without nontrivial nilpotents or idempotents, any elliptic curve E over S is given by a Weierstrass equation with coefficients in R; that is, there are elements $a_1, a_3, a_2, a_4, a_6 \in R$ with

$$E = \operatorname{Proj}\Big(R[X, Y, Z]/(Y^2 Z + a_1 XYZ + a_3 YZ^2 - X^3 - a_2 X^2 Z - a_4 XZ^2 - a_6 Z^3)\Big);$$

we write this as

$$E : Y^2 + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3.$$

As in the case of elliptic curves over a field, one shows this by applying a relativized version of the Riemann-Roch theorem.

Continuing the analogy, as elliptic curves over fields have a group structure, elliptic curves over schemes have the structure of a group scheme. First, we recall a definition:

Definition 26. A **group scheme** G over S is an S-scheme $f : G \to S$ together with morphisms $\mu : G \times_S G \to G$, $e : S \to G$ and $i : G \to G$ satisfying
(i) μ is associative; that is, $\mu \circ (\mu \times_S \mathrm{id}_G) = \mu \circ (\mathrm{id}_G \times_S \mu)$ as maps from $G \times_S G \times_S G$ to G;
(ii) e is the identity section; that is, $\mu \circ (\mathrm{id}_G \times_S e)$ and $\mu \circ (e \times_S \mathrm{id})$ are the canonical isomorphisms $G \times_S S \to G$ and $S \times_S G \to G$;
(iii) $\mu \circ (i \times_S \mathrm{id}_G) \circ \Delta_{G/S} = \mu \circ (\mathrm{id}_G \times_S i) \circ \Delta_{G/S} = e \circ f$ as a morphism $G \to G$.

A group scheme structure on a scheme G is equivalent to giving a group structure on the sets $G(T)$ that is functorial in the S-scheme T.

Theorem 3.4.1. *Any elliptic curve E/S is a group scheme. This is given by the following data: for any S-scheme T and points $P, Q, R \in E(T)$, $P + Q = R$ if and only if for the invertible sheaves $\mathcal{O}(P), \mathcal{O}(Q), \mathcal{O}(R)$ corresponding to P, Q, R as Cartier divisors, there exists an invertible sheaf $\mathcal{L}$ on T with*

$$\mathcal{O}(P) \otimes \mathcal{O}(Q) \otimes \mathcal{O}(\infty)^{-1} \cong \mathcal{O}(R) \otimes f_T^*(\mathcal{L})$$

as sheaves on $E \times_S T$.

In other words, $E(T)$ receives the group structure of the relative Picard group

$$\mathrm{Pic}^{(0)}(E \times_S T/T).$$

Proof. See [10], 2.1.2. □

Chapter 4

Differentials and de Rham cohomology

4.1 Review of spectral sequences

Let $\mathcal{C}$ be an abelian category.

Definition 27. A **spectral sequence** in $\mathcal{C}$ is a collection of objects $E_r^{p,q}$ of $\mathcal{C}$, $p, q \in \mathbb{Z}$, $r \geq r_0$ for some integer r_0, together with boundary morphisms $d_r : E_r^{p,q} \to E_r^{p-r,q+r-1}$ satisfying $d_r \circ d_r = 0$, and such that

$$E_{r+1}^{p,q} = \operatorname{Ker}[E_r^{p,q} \xrightarrow{d_r} E_r^{p-r,q+r-1}]/\operatorname{Im}[E_r^{p+r,q-r+1} \xrightarrow{d_r} E_r^{p,q}];$$

i.e. E_{r+1} is the homology of E_r.

The following construction of a spectral sequence will be especially important. Let

$$C^\bullet : ... \to C^{-1} \to C^0 \to C^1 \to ...$$

be a filtered cochain complex over $\mathcal{C}$ (that is, a filtered object in the category of cochain complexes over $\mathcal{C}$) with filtration

$$... \hookrightarrow F^n(C^\bullet) \hookrightarrow ... \hookrightarrow F^1(C^\bullet) \hookrightarrow F^0(C^\bullet) = C$$

compatible with the boundary d of $C^\bullet$; that is, $d(F^k(C^\bullet)^{(n)}) \hookrightarrow F^k(C^\bullet)^{(n+1)}$.
We define

$$E_0^{p,q} := F^p(C^\bullet)^{(p+q)}/F^{p+1}(C^\bullet)^{(p+q)},$$

and for $r \geq 1$,

$$Z_r^{p,q} := \operatorname{Ker} F^p(C^\bullet)^{(p+q)} \xrightarrow{d_0^{p,q}} C^{(p+q+1)} \twoheadrightarrow F^{p+r}(C^\bullet)^{(p+q+1)}$$

and

$$B_r^{p,q} := F^p(C^\bullet)^{(p+q)} \cap \operatorname{Im} F^{p-r+1}(C^\bullet) \overset{d_0^{p,q-r}}{\longrightarrow} C^{(p+q)},$$

and finally

$$E_r^{p,q} := Z_r^{p,q} / \Big(B_r^{p,q} + Z_{r-1}^{p,q} \Big);$$

if we set $Z_{-1}^{p,q} := Z_0^{p,q}$, this also agrees with the previous definition of E_0. Together with the boundary map $d_r : E_r^{p,q} \to E_r^{p+r,q-r+1}$, the restriction of the boundary map of $C^\bullet$, this forms the **spectral sequence associated to $C^\bullet$.**

Definition 28. A spectral sequence $E_r^{p,q}$ **abuts** to a double complex E_∞ (written $E_r \Rightarrow E_\infty$) if, for every pair (p,q), there exists an integer r_0 so that for all $r \geq r_0$, both boundaries $d_r^{p-r,q+r-1}$ and $d_r^{p,q}$ are zero; in this case, the sequence $(E_r^{p,q})_{p,q}$ stabilizes and we take $E_\infty^{p,q} = E_r^{p,q}$ for large enough r.

Consider now an additive functor $G : \mathcal{C} \to \mathcal{C}'$ between abelian categories, and assume that $\mathcal{C}$ has enough injectives.

Lemma 4.1.1. *Let A be a finitely filtered object of $\mathcal{C}$ with filtration $F^k(A)$, $k \geq 0$. Then A admits an injective resolution $A \to I^\bullet$, where $I^\bullet$ is a finitely filtered complex with filtration $F^k(I^\bullet)$, $k \geq 0$ and such that $F^k(I^\bullet)$ is an injective resolution of $F^k(A)$ for every k.*

Proof. This is 13.6.2 in EGA 3 ([4]). □

Fix any such injective resolution $A \to I^\bullet$. Then $G(A) \to G(I^\bullet)$ also satisfies the above lemma, where the filtration is given by $F^k(G(I^\bullet)) := G(F^k(I^\bullet))$. We may consider the spectral sequence $E_r^{p,q}$ associated to the complex $G(A) \to G(I^\bullet)$. This is independent of the injective resolution and is called the **spectral sequence of G relative to A.**

It holds that $E_r^{p,q}$ abuts to the cohomology $R^q G(A)$ of $G(A)$, the filtration being given by

$$F^p(R^q G(A)) = \mathrm{Im} R^q G(F^p(A)) \longrightarrow R^q G(A)],$$

and the E_1 terms are calculated as $E_1^{p,q} = R^{p+q} G(gr^p(A))$, where $gr^p(A) = F^p(A)/F^{p+1}(A)$ is the p-th associated graded object.

Another important example of spectral sequences are those that arise from double complexes. Let $C^{\bullet,\bullet}$ be a collection of objects of $\mathcal{C}$ together with differentials

$$d_I^q : C^{p,q} \longrightarrow C^{p-1,q}, \;\; d_{II}^p : C^{p,q} \longrightarrow C^{p,q-1}$$

satisfying $d_I \circ d_{II} + d_{II} \circ d_I = 0$. Then we may define the **total complex** $T^\bullet := \mathrm{Tot}(C^{\bullet,\bullet})$ given by $T^n = \bigoplus_{p+q=n} C^{p,q}$ and whose differential is given by $d_I + d_{II}$. There are two natural filtrations of $\mathrm{Tot}(C^{\bullet,\bullet})$:

$$F_I^k(T^\bullet) := \bigoplus_{\substack{p+q=n\\ p\geq k}} C^{p,q}, \;\; F_{II}^k(T^\bullet) := \bigoplus_{\substack{p+q=n\\ q\geq k}} C^{p,q},$$

and these filtrations induce spectral sequences ${}^I E_r^{p,q}$ and ${}^{II} E_r^{p,q}$. Both abut to the cohomology of T; that is,

$${}^I E_r^{p,q} \Rightarrow H^{p+q}(T), \;\; {}^{II} E_r^{p,q} \Rightarrow H^{p+q}(T),$$

although in general do not give the same filtration on $H^\bullet(T)$.

4.2 Differentials

To define differentials on schemes, it is useful to first define them on affine schemes - or rather, on rings. Let $f : R \to A$ be a morphism of commutative unital rings; via f, we understand elements of R as elements of A.

Definition 29. The module $\Omega^1_{A/R}$ of **1-forms** on A is the A-module generated by symbols $\mathrm{d}a$, $a \in A$ modulo the relations

$$\mathrm{d}(a+b) = \mathrm{d}a + \mathrm{d}b, \;\; \mathrm{d}(ab) = a\,\mathrm{d}b + b\,\mathrm{d}a, \;\; \mathrm{d}r = 0$$

for $a, b \in A$ and $r \in R$.

By construction, the obvious map $\mathrm{d}; A \longrightarrow \Omega^1_{A/R}$ is a derivation. It is universal in the following sense: given any derivation $D : A \longrightarrow M$ in another A-module M, there is a unique homomorphism $\psi : \Omega^1_{A/R} \longrightarrow M$ of A-modules satisfying $D = \psi \circ \mathrm{d}$.

For any $n \geq 1$, we define the module of ***n*-forms** as the n-fold exterior product

$$\Omega^n_{A/R} := \wedge^n \Omega^1_{A/R}.$$

The map $\mathrm{d} : A \to \Omega^1_{A/R}$ induces morphisms

$$\mathrm{d}^{(n)} : \Omega^n_{A/R} \longrightarrow \Omega^{(n+1)}_{A/R}, \;\; a \cdot \mathrm{d}x_1 \wedge ... \wedge \mathrm{d}x_n \mapsto \mathrm{d}a \wedge \mathrm{d}x_1 \wedge ... \wedge \mathrm{d}x_n.$$

Since $\mathrm{d}1 = 0$, it is clear that $\mathrm{d}^{(n+1)} \circ d^{(n)}$ for every n, so this gives a cochain complex

$$\Omega^\bullet_{A/R} : \; 0 \longrightarrow A \xrightarrow{\mathrm{d}^0} \Omega^1_{A/R} \xrightarrow{\mathrm{d}^1} \Omega^2_{A/R} \xrightarrow{\mathrm{d}^2} ...$$

called the **(algebraic) de Rham complex** of A/R. The modules

$$H^n_{dR}(A) := H^n(\Omega^\bullet_{A/R}) = \mathrm{Ker}[d^{(n)}]/\mathrm{Im}[d^{(n-1)}]$$

are called the **de Rham cohomology modules** of A; here $\mathrm{d}^0 = \mathrm{d}$ and $\mathrm{d}^{-1} = 0$.

Now let $f : X \to S$ be a morphism of schemes.

Definition 30. There is a unique quasicoherent $\mathcal{O}_X$-module on X, denoted by $\Omega^1_{X/S}$, such that for any open affine subsets $V \subseteq S$, $U \subseteq f^{-1}(V)$ and for any $x \in U$,

$$\Omega^1_{X/S}|_U \cong (\Omega^1_{\mathcal{O}_X(U)/\mathcal{O}_V(V)})^{\sim} \text{ and } (\Omega^1_{X/S})_x \cong \Omega^1_{\mathcal{O}_{X,x}/\mathcal{O}_{S,f(x)}}.$$

$\Omega^1_{X/S}$ is called the sheaf of **1-forms** of X over S.

As before, we define the sheaf of n-forms as $\Omega^n_{X/S} := \wedge^n \Omega^1_{X/S}$; that is, the sheaf associated to the presheaf

$$U \mapsto \wedge^n \Gamma(U, \Omega^1_{X/S}).$$

Together with the exterior differentials $\mathrm{d}^{(n)} : \Omega^{(n)}_{X/S} \longrightarrow \Omega^{(n+1)}_{X/S}$ this gives the **algebraic de Rham complex**

$$\Omega^\bullet_{X/S} : \ 0 \longrightarrow \mathcal{O}_X \longrightarrow \Omega^1_{X/S} \longrightarrow \Omega^2_{X/S} \longrightarrow ...$$

of sheaves of $\mathcal{O}_X$-modules.

The cohomology objects of this complex are sheaves of $\mathcal{O}_X$-modules. To get modules in the classical sense, we instead take the hypercohomology - that is, we form the total complex

$$\mathrm{Tot}\Big(C^p(\Omega^q_{X/S})\Big)^{(n)}_{p,q\geq 0} := \bigoplus_{p+q=n} C^p(\Omega^q_{X/S}),$$

where $C^\bullet(\Omega^q_{X/S})$ is the Godement resolution, and take its cohomology. We define

$$H^n_{dR}(X/S) := \mathbb{H}^n(\Omega^\bullet_{X/S}) = H^n(\mathrm{Tot}(C^\bullet(\Omega^\bullet_{X/S}))).$$

In view of the functor $f_* : \mathrm{Mod}(\mathcal{O}_X) \to \mathrm{Mod}(\mathcal{O}_S)$, we are taking the hyperderived functors

$$H^n_{dR}(X/S) = \mathbb{R}^n f_* \Omega^\bullet_{X/S}.$$

There are natural spectral sequences ${}^I E^{p,q}_r$ and ${}^{II} E^{p,q}_r$ that abut to $H^\bullet_{dR}(X/S)$ - those associated to the double complex $\Gamma(X, C^p(\Omega^q_{X/S}))$. The E_1-terms are given by

$${}^I E^{p,q}_1 = H^q(C^{p,\bullet}), \ \ {}^{II} E^{p,q}_1 = H^p(C^{\bullet,q}).$$

We call ${}^I E_r$ and ${}^{II} E_r$ the **Hodge to de Rham spectral sequences**. They are useful for computation - in several important cases (for example, smooth varieties over an algebraically closed field of characteristic 0), they degenerate at E_1.

4.3 Differentials on an elliptic curve

We now calculate the de Rham cohomology of an elliptic curve $f : E \to S$, where $S = \operatorname{Spec} R$ is affine noetherian. The above considerations are more difficult than necessary: since E is well-behaved, we can use Čech cohomology instead of taking Godement resolutions.

Recall that E is given by a Weierstrass equation

$$E : Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3;$$

it is convenient (though not necessary) to assume that 6 is invertible in R, in which case we can take a Weierstrass equation of the form

$$E : Y^2Z - X^3 - pXZ^2 - qZ^3.$$

There is a natural affine cover given by dehomogenization: we take

$$U = \operatorname{Spec} R[x,y]/(y^2 - x^3 - px - q) \text{ and } V = \operatorname{Spec} R[t,z]/(z - t^3 - ptz^2 - qz^3),$$

using dehomogenized variables $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$, $t = \frac{X}{Y}$, $z = \frac{Z}{Y}$. With respect to this cover, the Čech complexes are quite simple: we only need to consider one intersection $U \cap V$, so all terms C^k, $k \geq 2$ vanish. We get the commutative diagram

$$\begin{tikzcd}
C^0(E,\mathcal{O}_E) \arrow[r] \arrow[d] & C^1(E,\mathcal{O}_E) \arrow[r] \arrow[d] & 0 \\
C^0(E,\Omega^1_{E/S}) \arrow[r] \arrow[d] & C^1(E,\Omega^1_{E/S}) \arrow[r] \arrow[d] & 0 \\
0 & 0 &
\end{tikzcd}$$

where we have $C^0(E,\mathcal{F}) = \Gamma(U,\mathcal{F}) \times \Gamma(V,\mathcal{F})$, $C^1(E,\mathcal{F}) = \Gamma(U \cap V,\mathcal{F})$ and $C^2(E,\mathcal{F}) = 0$ for $\mathcal{F} = \Omega^k_{E/S}$, $k = 0,1,2,....$ Taking hypercohomology, we see that

$$H^0_{dR}(E/R) = \operatorname{Ker}[\mathcal{O}_E(U) \oplus \mathcal{O}_E(V) \to \mathcal{O}_E(U \cap V) \oplus \Omega^1_{E/R}(U) \oplus \Omega^1_{E/R}(V)]$$

$$(s_U, s_V) \mapsto (s_U|_{U\cap V} - s_V|_{U\cap V}, \mathrm{d}s_U, \mathrm{d}s_V);$$

such tuples are exactly those that glue to global sections, so $H^0_{dR} = \Gamma(E,\mathcal{O}_E)$.

We have $H^1_{dR}(E/R) = Z^1/B^1$, where

$$Z^1 = \operatorname{Ker}[\mathcal{O}_E(U \cap V) \oplus \Omega^1_{E/R}(U) \oplus \Omega^1_{E/R}(V) \to \Omega^1_{E/R}(U \cap V)]$$

$$(f, \omega_U, \omega_V) \mapsto \omega_U - \omega_V - \mathrm{d}f$$

and

$$B^1 = \operatorname{Im}[\mathcal{O}_E(U) \oplus \mathcal{O}_E(V) \to \mathcal{O}_E(U \cap V) \oplus \Omega^1_{E/R}(U) \oplus \Omega^1_{E/R}(V)].$$

There is an injective map

$$H^0(E, \Omega^1_{E/R}) \to H^1_{dR}(E/R)$$

that is induced by $\omega \mapsto (\omega|_U, \omega|_V, 0)$; this is injective because if $(\omega|_U, \omega|_V, 0)$ is a coboundary, then we have $\omega|_U = \mathrm{d}f_U$, $\omega|_V = \mathrm{d}f_V$ and $0 = f_U - f_V$, so the sections f_U and f_V are equal on $U \cap V$ and glue to a global section $f \in \Gamma(E, \mathcal{O}_E)$ such that $\omega = \mathrm{d}f = 0$.

We also have a map

$$H^1_{dR}(E/R) \to H^1(E, \mathcal{O}_E), \;\; [(\omega_U, \omega_V, f)] \mapsto [f];$$

this is well-defined because for any de Rham coboundary $(\omega_U, \omega_V, f) \in B^1$, $[f] = 0$ in

$$H^1(E, \mathcal{O}_E) = \mathcal{O}_E(U \cap V)/\{f|_{U\cap V} - g|_{U\cap V} : f \in \mathcal{O}_E(U), \; g \in \mathcal{O}_E(V)\}.$$

This map is surjective: for any given f, it is possible to adjust $\mathrm{d}f$ by a regular differential on V (an element of $\Omega^1_{E/R}(V)$) to get a regular differential on U - this can be done by choosing a global section ω of $\Omega^1_{E/R}$ and considering differentials $g \cdot \omega$ with $g \in K(E)$; the Riemann-Roch theorem guarantees the existence of a g that will work.

Consider now the sequence

$$0 \to H^0(E, \Omega^1_{E/R}) \to H^1_{dR}(E/R) \to H^1(E, \mathcal{O}_E) \to 0.$$

This is exact: the composition of the maps is clearly zero, and if $(\omega_U, \omega_V, f_U - f_V)$ is a cochain in the kernel of the second map, such that f_U ir regular on U and f_V regular on V, then it differs from $(\omega_U - \mathrm{d}(f_U), \omega_V - \mathrm{d}(f_v), 0)$ by a coboundary and so is equal to it in $H^1_{dR}(E/R)$.

We have $(\omega_U - \mathrm{d}f_U)|_{U\cap V} - (\omega_V - \mathrm{d}f_V)|_{U\cap V} = \omega_U|_{U\cap V} - \omega_V|_{U\cap V} - \mathrm{d}(f_U - f_V) = 0$ since we started with an element of the kernel; so ω_U and ω_V come from a global section $\omega \in \Omega^1_{E/R}(E)$, and $(\omega_U, \omega_V, f_U - f_V)$ is the image of ω.

In particular, $H^1(E, \mathcal{O}_E)$ is a free R-module of rank 1 (the genus of E), and $H^0(E, \Omega^1_{E/R})$ is by Serre duality as well - so $H^1_{dR}(E/R)$ is a free R-module of rank 2.

Finally, we note that $H^2_{dR}(E/R)$ is a free R-module of rank 1. This allows one to make the following definition:

Definition 31. The **de Rham pairing** is the perfect, alternating pairing

$$(-,-)_{dR} : H^1_{dR}(E/R) \times H^1_{dR}(E/R) \xrightarrow{\wedge} H^2_{dR}(E/R) \xrightarrow{Tr} R,$$

where $\wedge$ is the exterior product (i.e. de Rham cup product) and Tr is the trace map of Grothendieck-Serre duality.

This can be explicitly given in terms of 'residue' morphisms on the points of E. We only note here that $(\frac{\mathrm{d}x}{y}, \frac{x\mathrm{d}x}{y})_{dR} = 1$.

4.4 Connections

Let R be an integral domain and X a smooth scheme over R, $\mathcal{F}$ a quasicoherent $\mathcal{O}_X$-module.

Definition 32. A **connection** on $\mathcal{F}$ is a morphism

$$\nabla : \mathcal{F} \to \mathcal{F} \otimes_{\mathcal{O}_X} \Omega^1_{X/R}$$

of sheaves of $\mathcal{O}_X$-modules, such that for every open subset $U \subseteq X$,
(i) $\nabla_U : \mathcal{F}(U) \to \mathcal{F}(U) \otimes_{\mathcal{O}_X(U)} \Omega^1_{X/R}(U)$ is R-linear;
(ii) For any sections $s \in \mathcal{O}_X(U)$, $x \in \mathcal{F}(U)$,

$$\nabla_U(sx) = x \otimes \mathrm{d}s + s\nabla_U(x).$$

The corresponding concept in differential geometry is also called a 'covariant derivative' and may be thought of as a way of transporting, locally or even infinitesimally, information along the sheaf $\mathcal{F}$ in a coherent way.

A section $s \in \mathcal{F}(U)$ is called **horizontal** (with respect to ∇) if $\nabla_U(s) = 0$.

Any connection ∇ induces morphisms of $\mathcal{O}_X$-modules

$$\nabla^{(k)} : \mathcal{F} \otimes_{\mathcal{O}_X} \Omega^k_{X/R} \to \mathcal{F} \otimes_{\mathcal{O}_X} \Omega^{k+1}_{X/R};$$

for any open $U \subseteq X$ and sections $x \in \mathcal{F}(U)$, $\omega \in \Omega^k_{X/R}$,

$$\nabla^{(k)}(x \otimes \omega) := x \otimes \mathrm{d}\omega + (-1)^k \nabla(x) \wedge \omega,$$

where if $\nabla(x) = \sum_i x_i \otimes \omega_i$, $\nabla(x) \wedge \omega := \sum_i x \otimes (\omega_i \wedge \omega)$.

Definition 33. The **curvature** K of a connection is the morphism

$$K = \nabla^{(1)} \circ \nabla : \mathcal{F} \to \mathcal{F} \otimes_{\mathcal{O}_X} \Omega^2_{X/R}.$$

We call ∇ **integrable** if its curvature is everywhere zero.

If ∇ is an integrable connection, it follows that $\nabla^{(k+1)} \circ \nabla^{(k)} \equiv 0$ for every $k \geq 0$ and we get a cochain complex

$$\mathcal{F} \otimes_{\mathcal{O}_X} \Omega^\bullet_{X/R} :\ 0 \longrightarrow \mathcal{F} \xrightarrow{\nabla} \mathcal{F} \otimes \Omega^1_{X/R} \xrightarrow{\nabla^{(1)}} \mathcal{F} \otimes_{\mathcal{O}_X} \Omega^2_{X/R} \longrightarrow \dots$$

The **de Rham cohomology** of X with coefficients $(\mathcal{F}, \nabla)$ is defined as the hypercohomology

$$H^k_{dR}(X; \mathcal{F}, \nabla) := \mathbb{H}^k(\mathcal{F} \otimes_{\mathcal{O}_X} \Omega^\bullet_{X/R}).$$

4.5 The Gauss-Manin connection

Let $\pi : X \to S$ be a smooth morphism between smooth schemes over R. Then we have the cotangent sequence

$$0 \to \pi^*\Omega^1_{S/R} \to \Omega^1_{X/R} \to \Omega^1_{X/S} \to 0$$

of locally free sheaves of $\mathcal{O}_X$-modules; this is always right-exact, and left-exact because π is smooth. This gives a canonical filtration of complexes

$$... \subseteq F^2(\Omega^\bullet_{X/R}) \subseteq F^1(\Omega^\bullet_{X/R}) \subseteq F^0(\Omega^\bullet_{X/R}) = \Omega^\bullet_{X/R},$$

where

$$F^k(\Omega^\bullet_{X/R}) = \mathrm{im}[\Omega^{\bullet-k}_{X/R} \otimes_{\mathcal{O}_X} \pi^*\Omega^k_{S/R} \to \Omega^\bullet_{X/R}].$$

This is compatible with the exterior product; that is,

$$F^j(\Omega^\bullet_{X/R}) \wedge F^k(\Omega^\bullet_{X/R}) \subseteq F^{j+k}(\Omega^\bullet_{X/R}).$$

The associated graded objects are

$$\mathrm{gr}^k(\Omega^\bullet_{X/R}) = F^k(\Omega^\bullet_{X/R})/F^{k+1}(\Omega^\bullet_{X/R}) \cong \Omega^{\bullet-k}_{X/S} \otimes_{\mathcal{O}_X} \pi^*\Omega^k_{S/R}.$$

Let $E_r^{p,q}$ be the spectral sequence induced by the (finite) filtration of $\Omega^\bullet_{X/R}$; it follows that $E_r^{p,q} \Rightarrow R^{p+q}f_*\Omega^\bullet_{X/R}$, and that

$$E_1^{p+q} = R^{p+q}f_*(\mathrm{gr}^p(\Omega^\bullet_{X/R})) \cong \Omega^p_{S/R} \otimes R^q f_*\Omega^\bullet_{X/S}.$$

The sheaf $R^q f_*\Omega^\bullet_{X/S}$ is the cohomology (in the usual sense) of the de Rham complex, and will be called the **de Rham cohomology sheaf**

$$\mathcal{H}^q_{dR}(X/S) := R^q f_*\Omega^\bullet_{X/S}.$$

Definition 34. The map

$$\nabla_{GM} := d_1^{0,q} : E_1^{0,q} = \mathcal{H}^q_{dR}(X/S) \longrightarrow \Omega^1_{S/R} \otimes_{\mathcal{O}_S} \mathcal{H}^q_{dR}(X/S) = E_1^{1,0}$$

is called the **Gauss-Manin connection** of X/S.

It must be checked that this actually defines a connection - however, linearity is not difficult, and the product rule also holds. The curvature of ∇_{GM} is $d_1^{1,q} \circ d_1^{0,q} \equiv 0$; so ∇_{GM} is integrable.

The real importance of the Gauss-Manin connection is that it provides a natural way of defining partial derivatives. Let $D \in \mathrm{Der}_R(\mathcal{O}_S, \mathcal{O}_S)$ be any derivation. By the universal property of Ω^1, this corresponds to a homomorphism of $\mathcal{O}_S$-modules $D \in \mathrm{Hom}_{\mathcal{O}_S}(\Omega^1_{S/R}, \mathcal{O}_S)$. We can then define

$$\nabla_D : \mathcal{H}^q_{dR}(X/S) \xrightarrow{\nabla_{GM}} \Omega^1_{S/R} \otimes_{\mathcal{O}_S} \mathcal{H}^q_{dR}(X/S) \xrightarrow{D\otimes \mathrm{id}} \mathcal{O}_S \otimes_{\mathcal{O}_S} \mathcal{H}^q_{dR}(X/S) \cong \mathcal{H}^q_{dR}(X/S).$$

Chapter 5

Formal groups

5.1 Formal schemes and formal groups

Definition 35. Let X be a noetherian scheme and Z a closed subscheme with ideal sheaf $\mathcal{I}$. The **formal completion** of X along Z is the locally ringed space

$$(\hat{X}, \mathcal{O}_{\hat{X}}) = (Z, \varprojlim_{n \in \mathbb{N}} \mathcal{O}_X/\mathcal{I}^n).$$

Here,

$$\varprojlim_{n \in \mathbb{N}} \mathcal{O}_X/\mathcal{I}^n := [U \mapsto \varprojlim_{n \in \mathbb{N}} \mathcal{O}_X(U)/\mathcal{I}^n(U)];$$

this construction also happens to be the inverse limit in the category of sheaves of abelian groups. Thus, we essentially restricting ourselves with $\hat{X}$ to the subscheme Z; however, $\varprojlim \mathcal{O}_X/\mathcal{I}^n$ may be thought of as giving infinitesimally more 'information' about the surroundings of Z than $\mathcal{O}_Z$ alone.

The formal completion of X is not generally a scheme. It is an example of a different type of structure that we now describe:

Definition 36. A Noetherian **formal scheme** $(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}})$ is a locally ringed space with a finite open cover $\mathfrak{X} = \cup_{i \in I} \mathfrak{U}_i$ such that each $(\mathfrak{U}_i, \mathcal{O}_{\mathfrak{X}}|_{\mathfrak{U}_i})$ is isomorphic to the completion of a Noetherian scheme X_i along a closed subscheme Y_i.

Morphisms of Noetherian formal schemes are morphisms of locally ringed spaces between Noetherian formal schemes.

Example: Let X be a Noetherian scheme and P a closed point on X. Then the completion of X along P is given by $(\{P\}, \hat{O}_P)$, where $\hat{O}_P$ is the completion of the local ring $\mathcal{O}_{X,P}$.

Definition 37. Let A be a noetherian topological ring that is complete and separated; that is, there is an open ideal $\mathcal{I}$ of A whose powers form a basis of open neighborhoods of 0. The **formal spectrum** of A is the formal scheme $\mathrm{Spf}\, A$, whose topological space consists of the open ideals of A (equivalently, the prime ideals of $A/\mathcal{I}$), and whose structure sheaf is defined by

$$\mathcal{O}_{\mathrm{Spf}\, A} = \varprojlim_{n \in \mathbb{N}} A/\mathcal{I}^n.$$

Explicitly, if $f \in A$ and $D(f)$ is the set of open prime ideals not containing f, $\mathcal{O}_{\mathrm{Spf}\, A}\big(D(f)\big) = \hat{A}_f$ is the completion of the local ring A_f. Any formal scheme that is isomorphic to the formal spectrum of a topological ring is called **affine**.

In analogy to schemes, there is an algebraic characterization of morphisms of formal schemes that map to an affine formal scheme:

Lemma 5.1.1. *Let $\mathfrak{X}$ be a noetherian formal scheme and $\mathrm{Spf}\, A$ a noetherian affine formal scheme. Then the morphisms $f : \mathfrak{X} \to \mathrm{Spf}\, A$ correspond exactly to continuous ring homomorphisms $A \to \Gamma(\mathfrak{X}, \mathcal{O}_{\mathfrak{X}})$.*

Definition 38. Let $\mathfrak{X}$ be a noetherian formal scheme. A **formal group** $\mathfrak{G}$ over $\mathfrak{X}$ is a group object in the category of noetherian formal schemes over $\mathfrak{X}$; that is, $f : \mathfrak{G} \to \mathfrak{X}$ is a formal scheme equipped with morphisms $\mu : \mathfrak{G} \times \mathfrak{G} \to \mathfrak{G}$ (multiplication), $e : S \to \mathfrak{G}$ (identity) and $i : \mathfrak{G} \to \mathfrak{G}$ (inversion) that satisfy the usual properties. In other words, for any formal scheme $\mathfrak{T}$ over $\mathfrak{X}$, the morphisms $\mathfrak{T} \to \mathfrak{G}$ over $\mathfrak{X}$ have a group structure that is functorial in $\mathfrak{T}$.

A formal group $\mathfrak{G}$ over an affine scheme $\mathrm{Spec}\, R$ is called **smooth** (or a **formal Lie group**) if there is an isomorphism

$$\mathfrak{G} \cong \mathrm{Spf}\, R[|X_1, ..., X_d|]$$

to the power series ring over R in d variables for some $d \geq 1$. We call d the **dimension** of $\mathfrak{G}$.

In any smooth formal group, the multiplication morphism is encoded in certain power series. For simplicity we adopt the notation $R[|\underline{X}|] := R[|X_1, ..., X_d|]$. Write $\mathfrak{G} = \mathrm{Spf}\, R[|\underline{X}|]$; then, the multiplication morphism $\mu : \mathfrak{G} \times \mathfrak{G} \to \mathfrak{G}$ corresponds to a comultiplication

$$m : R[|\underline{X}|] \to R[|\underline{X}|] \otimes_R R[|\underline{X}|] \cong R[|\underline{X}, \underline{Y}|];$$

it is determined by the images of the variables X_i, which are power series $F_i \in R[|\underline{X}, \underline{Y}|]$. The data of these power series is called a **formal group law**.

Example: (i) Let R be a noetherian ring and $\mathbb{G}_a := \mathrm{Spf}\, R[X]$ the additive group scheme over R - as a functor, it maps an R-formal scheme $\mathfrak{T}$ to the additive group $\Gamma(\mathfrak{T}, \mathcal{O}_{\mathfrak{T}})$. Indeed, the morphisms from $\mathfrak{T}$ to $\mathbb{G}_a(R)$ correspond to ring morphisms from $R[X]$ to $\Gamma(\mathfrak{T}, \mathcal{O}_{\mathfrak{T}})$ that fix R, and so uniquely to choices of where X maps to. As a group, the image is clearly functorial in $\mathfrak{T}$. The 'multiplication' morphism $\mathbb{G}_a \times_R \mathbb{G}_a \to \mathbb{G}_a$ is given on rings by

$$R[X] \to R[X] \otimes_R R[X] \cong R[X,Y], \;\; X \mapsto X \otimes 1 + 1 \otimes X \mapsto X + Y.$$

The **formal additive group** $\hat{\mathbb{G}}_a$ is the formal completion of $\mathbb{G}_a$ along its identity section $e : \operatorname{Spec} R \to \operatorname{Spec} R[X]$ (corresponding to the augmentation $X \mapsto 0$); the corresponding comultiplication is still given by $X \mapsto X + Y$.

(ii) Let $\mathbb{G}_m := \operatorname{Spec} R[X, X^{-1}]$ be the multiplicative group scheme that maps R-formal schemes $\mathfrak{T}$ to the group of units $\Gamma(\mathfrak{T}, \mathcal{O}_{\mathfrak{T}})^{\times}$. The multiplication $\mathbb{G}_m \times_R \mathbb{G}_m \mapsto \mathbb{G}_m$ is given by

$$R[X, X^{-1}] \to R[X, X^{-1}] \otimes_R R[X, X^{-1}] \cong R[X, Y, X^{-1}, Y^{-1}], \;\; X \mapsto X \otimes X \mapsto XY.$$

The **formal multiplicative group** $\hat{\mathbb{G}}_m$ is the formal completion of $\mathbb{G}_m$ along its identity section $e : \operatorname{Spec} R \to \operatorname{Spec} R[X, X^{-1}]$ (corresponding to $X \mapsto 1$). It is smooth: we have $\mathbb{G}_m \cong \operatorname{Spf} R[|X|]$ by sending X to $1 + X$. The multiplication $\hat{\mathbb{G}}_m \times_R \hat{\mathbb{G}}_m \to \hat{\mathbb{G}}_m$ is represented by

$$R[|X|] \to R[|X,Y|], X \mapsto (1 + X)(1 + Y) - 1 = X + Y + XY.$$

5.2 Formal group laws

Our goal is to understand the formal group $\hat{E}$ corresponding to an elliptic curve E/R. This turns out to be a formal group law (this is non-trivial) and it seems easier to study the properties of $\hat{E}$ via power series. The explicitness allows the proof of a powerful structure theorem of formal group laws over algebraically closed fields, which will translate to the situation we need.

It will be helpful to fix a notation for multiindices here. Given variables $X_1, ..., X_n$ and a tuple $\alpha = (\alpha_1, ..., \alpha_n)$ of nonnegative integers, we define

$$|\alpha| = \sum_{k=1}^{n} \alpha_k$$

and

$$X^{\alpha} = \prod_{k=1}^{n} X_k^{\alpha_k}.$$

Let R be a commutative ring with a unit. We use the notation

$$R[|\underline{X}|] := R[|X_1, ..., X_n|]$$

to denote the ring of formal power series in n variables, as long as the number of variables is clear or at least unimportant.

Definition 39. A **formal group law** of dimension n over R is a tuple $\mathbb{G}$ of n power series

$$\mathbb{G}_1, ..., \mathbb{G}_n \in R[|\underline{X}, \underline{Y}|]$$

in $2n$ variables $X_1, ..., X_n$, $Y_1, ..., Y_n$ with the following properties:

(i) $\forall k: \ \mathbb{G}_k(\underline{X}, \underline{0}) = \mathbb{G}_k(\underline{0}, \underline{X}) = X_k$, and
(ii) $\mathbb{G}_k(\mathbb{G}(\underline{X}, \underline{Y}), \underline{Z}) = \mathbb{G}_k(\underline{X}, \mathbb{G}(\underline{Y}, \underline{Z}))$.

The formal group law $\mathbb{G}$ is **commutative** if for all k,

(iii) $\mathbb{G}_k(\underline{X}, \underline{Y}) = \mathbb{G}_k(\underline{Y}, \underline{X})$.

We call $R[|X|]$ the **coordinate ring** of $\mathbb{G}$.

Convention: In the following, we tacitly assume that all formal group laws discussed are commutative. Accordingly, we write $\underline{X} +_{\mathbb{G}} \underline{Y}$ to be $\mathbb{G}(\underline{X}, \underline{Y})$.

A formal group law is then a set of power series that, under composition with itself, behaves according to the axioms of a group (without specified elements). In this sense, (i) represents the existence of a neutral element, (ii) the associative law, and (iii) the commutative law for abelian groups. It is also clear that the power series associated to formal group schemes satisfy these conditions. The one axiom missing is the existence of unique inverses; however, this is implied. First:

Lemma 5.2.1 (Jacobi criterion)**.** *Let $g(X)$ be a power series with $g(0) = 0$. There exists a power series $f \in R[|\underline{X}|]$ with $f(g(X)) = X$ if and only if*

$$\det\left(\frac{\partial g_i}{\partial X_j}\right)_{ij} \in R^{\times}.$$

Proposition 5.2.2. *Let $\mathbb{G}(\underline{X}, \underline{Y})$ be a formal group. Then there exists a unique tuple of n power series $i_1(\underline{X}), ..., i_n(\underline{X})$ with the property*

$$\mathbb{G}(\underline{X}, i(\underline{X})) = \mathbb{G}(i(\underline{X}), \underline{X}) = 0.$$

Proof. For $i = 1, ..., n$, set $g_i(\underline{X}, \underline{Y}) := X_i - F_i(\underline{X}, \underline{Y})$. It follows

$$(\frac{\partial g_i}{\partial Y_j})|_{X,Y=0} = -(\frac{\partial F_i}{\partial Y_j})|_{X,Y=0} = -\delta_{ij},$$

so $\det(\frac{\partial g_i}{\partial Y_j}|_{Y=0}) \in R^{\times}$. This implies the existence of power series $h_i(\underline{X}, \underline{Y})$ with $g_i(\underline{X}, h(\underline{X}, \underline{Y}))$. Take $i(\underline{X}) := h(\underline{X}, \underline{X})$. □

We will also write $\underline{X} -_{\mathbb{G}} \underline{Y}$ to denote $\mathbb{G}(\underline{X}, i(\underline{Y}))$.

We have seen the simplest and arguably most important examples of formal group laws in the previous section: namely, the additive formal group law

$$\mathbb{G}_a(X,Y) = X + Y$$

and the multiplicative formal group law

$$\mathbb{G}_m(X,Y) = (1+X)(1+Y) - 1 = X + Y + XY.$$

Definition 40. Let $\mathbb{F}$ and $\mathbb{G}$ be formal group laws of respective dimensions m and n. A **morphism** $\varphi : \mathbb{F} \to \mathbb{G}$ is a tuple of power series

$$\varphi(\underline{X}) = \Big(\varphi_1(X_1, ..., X_n), ..., \varphi_m(X_1, ..., X_n)\Big)$$

such that $\varphi_k(\underline{0}) = 0$ for all k and that

$$\varphi\Big(\underline{X} +_{\mathbb{F}} \underline{Y}\Big) = \varphi(\underline{X}) +_{\mathbb{G}} \varphi(\underline{Y}).$$

A morphism φ of formal group laws induces a homomorphism of coordinate rings

$$\varphi^* : R[|X_1, ..., X_m|] \to R[|X_1, ..., X_n|], \;\; X_k \mapsto \varphi_k.$$

The composition of two morphisms is defined as the composition of the underlying power series. As usual, $\varphi : \mathbb{F} \to \mathbb{G}$ is called an **isomorphism** if there exists a left- and right-inverse morphism $\psi : \mathbb{G} \to \mathbb{F}$.

Example: If R is a field of characteristic 0, we have a familiar-looking isomorphism

$$\mathbb{G}_a \to \mathbb{G}_m, \;\; X \mapsto \sum_{n=1}^{\infty} \frac{1}{n!} X^n = \exp(X) - 1.$$

5.3 Differentials

Let R be a commutative unital ring as above. We can consider the R-module of 1-forms $\Omega^1_{R[|\underline{X}|]/R}$, generated by symbols $\mathrm{d}F$, $F \in R[|\underline{X}|]$ with the usual relations.

Lemma 5.3.1. *$\Omega^1_{R[|\underline{X}|]/R}$ is a free R-module with basis $\mathrm{d}X_1$,...,$\mathrm{d}X_n$.*

Proof. $\mathrm{d}X_1$,...,$\mathrm{d}X_n$ generate $\Omega^1_{R[|\underline{X}|]/R}$, because for any $f \in R[|X|]$, we have

$$\mathrm{d}(f) = \sum_{k=1}^{n} \frac{\partial f}{\partial X_k} \, \mathrm{d}X_k.$$

On the other hand, if $\sum_{k=1}^n \lambda_k \mathrm{d}X_k = 0$ for any $\lambda_k \in R$, it follows $\mathrm{d}\Big(\sum_{k=1}^n \lambda_k X_k\Big) = 0$ and so $\sum_{k=1}^n \lambda_k X_k \in R$, so $\lambda_k = 0$ for all k. □

Let $f : R[|X_1, ..., X_m|] \to R[|Z_1, ..., Z_n|]$ be a morphism of rings. Then f induces a morphism of modules

$$f_* : \Omega^1_{R[|\underline{X}|]/R} \to \Omega^1_{R[|\underline{Z}|]/R}, \ \ \mathrm{d}X_k \mapsto \mathrm{d}(f(X_k)).$$

Definition 41. Let $\mathbb{G}$ be a formal group law over R. A 1-form

$$\omega = \sum_{k=1}^{n} f_k(\underline{X}) \, \mathrm{d}X_k \in \Omega^1_{R[|\underline{X}|]/R}$$

is called **$\mathbb{G}$-invariant** if

$$\sum_{k=1}^{n} f_k(\mathbb{G}(\underline{X}, \underline{Y})) \frac{\partial \mathbb{G}_k}{\partial Y_j}(\underline{X}, \underline{Y}) = f_j(\underline{Y})$$

for each $j = 1, ..., n$.

In other words, if $\mu : R[|\underline{X}|] \to R[|\underline{X}, \underline{Y}|]$ is given by $X_k \mapsto \mathbb{G}_k$ and we take

$$i_1 : R[|\underline{X}|] \to R[|\underline{X}, \underline{Y}|], \ \ X_k \mapsto X_k$$

and

$$i_2 : R[|\underline{X}|] \to R[|\underline{X}, \underline{Y}|], \ X_k \mapsto Y_k,$$

then we are requiring $\mu_* \omega = (i_1)_* \omega + (i_2)_* \omega$.

Proposition 5.3.2. *The $\mathbb{G}$-invariant differentials on $R[|\underline{X}|]$ form a submodule $\Omega^1_{\mathbb{G}}$ of $\Omega^1_{R[|\underline{X}|]/R}$. There is an isomorphism of R-modules*

$$\Omega^1_{\mathbb{G}} \to R^n, \ \ \sum_{k=1}^{n} f_k(\underline{X}) \, \mathrm{d}X_k \mapsto (f_1(0), ..., f_n(0)).$$

Proof. Any invariant differential $\omega = f_1 \, \mathrm{d}X_1 + ... + f_n \, \mathrm{d}X_n$ is uniquely determined by the values $f_1(0), ..., f_n(0)$ by

$$\omega = \begin{pmatrix} f_1(0) & ... & f_n(0) \end{pmatrix} \Big(\frac{\partial \mathbb{G}_i}{\partial Y_j}(\underline{X}, 0) \Big)^{-1} \begin{pmatrix} \mathrm{d}X_1 \\ \vdots \\ \mathrm{d}X_n \end{pmatrix}.$$

On the other hand, any such differential defined by values $f_1(0), ..., f_n(0)$ is $\mathbb{G}$-invariant. □

In particular, in the case of a one-dimensional formal group we may speak of 'the' invariant differential ω having $\omega(0) = 1$.

Example: The invariant diifferential of $\hat{\mathbb{G}}_a(X, Y) = X + Y$ is $\omega = \mathrm{d}X$.
The invariant differential of $\hat{\mathbb{G}}_m(X, Y) = X + Y + XY$ is $\omega = (1+X)^{-1} \, \mathrm{d}X = \sum_{k=0}^{\infty} (-X)^k \, \mathrm{d}X$.

One application of this is the following:

Proposition 5.3.3. *Every one-dimensional, commutative formal group law $\mathbb{G}$ over a field K of characteristic 0 is isomorphic to the additive formal group law $\hat{\mathbb{G}}_a$.*

Proof. Let $\omega = f(X)\,\mathrm{d}X$ be the invariant differential of $\mathbb{G}$ and define the **logarithm**

$$\ell(X) := \int \omega = \int f(X)\,\mathrm{d}X$$

as the antiderivative of f with $\ell(0) = 0$. This is an isomorphism: the invariance of ω implies $\omega(X) = \omega(\mathbb{G}(X, Y))$, and therefore

$$\ell(\mathbb{G}(X, Y)) = \ell(X) + g(Y)$$

for some function $g(Y)$ - by setting $X = 0$, we see that $g(Y) = \ell(Y)$.
This implies that ℓ is a homomorphism. It is an isomorphism by the Jacobi criterion. □

5.4 The formal group of an elliptic curve

Let S be a noetherian scheme and $f : E \to S$ an elliptic curve with $e : R \to E$ its section 'at infinity'. Via e we understand S as a closed subscheme $\infty \subseteq E$. We let $\hat{E}$ be the formal completion of E along ∞.

Proposition 5.4.1. *There is an affine cover $S = \cup_{i=1}^{n} U_i$, $U_i \cong \operatorname{Spec} A_i$, and isomorphisms of formal schemes*

$$\hat{E}_{U_i} \cong \operatorname{Spf} R[|T|],$$

*where $E_{U_i} := E \times_S U_i$, and $\hat{E}_{U_i}$ its formal completion along $\infty \times_S U_i$. Any such isomorphism is called a **formal parameterization** of E_{U_i} at ∞, and T a **formal parameter**.*

Proof. We will use the following lemma:

Lemma 5.4.2. *Let $(X, \mathcal{O}_X)$ be a noetherian scheme and $(X, \mathcal{F})$ a closed subscheme on the same topological space. If $(X, \mathcal{F})$ is affine, then $(X, \mathcal{O}_X)$ is affine.*

Proof. Let $X_1 := (X, \mathcal{F})$ be given by the sheaf of ideals $\mathcal{I}$ of $\mathcal{O}_X$. Since X is noetherian, $\mathcal{I}$ is nilpotent - on a finite cover $(U_i)_{i \in I}$ by affine noetherian schemes, $\mathcal{I}(U_i)$ is contained in the nilradical of $\mathcal{O}_X(U_i)$, which, being finitely generated, is itself nilpotent. Pick $n \geq 1$ with $\mathcal{I}^n = 0$. Now let X_k be the closed subscheme corresponding to $\mathcal{I}^k$. By induction on k, it is enough to show that X_2 is affine. □

Now consider the affine subscheme $\infty \cong \operatorname{Spec} R$ of E, with defining ideal sheaf $\mathcal{I}$. The previous lemma implies that the subschemes ∞_n corresponding to $\mathcal{I}^n$ are also affine, isomorphic to $\operatorname{Spec} R_n$ for some rings R_n; the closed immersions $\infty \hookrightarrow \infty_n$ give surjective ring homomorphisms $R_n \to R$.

The cokernels $\mathcal{J}_n := \text{Coker}[\infty \to \infty_n] = (\text{Ker}[R_n \to R])^\sim$ are locally free $\mathcal{O}_X$-modules of rank n, which can be checked on stalks. By passing to an affine cover U_i of S that trivializes the $\mathcal{J}_n$, we can find a generator T of $\mathcal{J}_1$ whose powers $T, ..., T^k$ generate $\mathcal{J}_k$ for all k; this gives isomorphisms $A_i[|T|]/(T^k) \cong A_i[T]/(T^k) \cong R_k$ and finally Spf $A[|T|] \cong \hat{E}_{U_i}$. □

The application of this that we use will be

Theorem 5.4.3. *Let R be a discrete valuation ring, and E/R an elliptic curve. Then there exists a formal parameterization*

$$\hat{E} \cong \text{Spf}\, R[|T|]$$

of E at ∞. In particular, $\hat{E}$ is given by a formal group law $\Phi_E(X, Y) \in R[|X, Y|]$.

5.5 Formal groups over finite fields

Let K be an separably closed field of characteristic $p > 0$.

Definition 42. (i) Let $\mathbb{F}$ and $\mathbb{G}$ be two (one-dimensional commutative) formal groups laws over K, and $f : \mathbb{F} \to \mathbb{G}$ a homomorphism. The **height** $h(f)$ of f is the greatest integer such that f is a power series in X^{p^h}; the height of the zero map is defined to be ∞.
(ii) Let $\mathbb{G}$ be a (one-dimensional commutative) formal group over K. Consider the multiplication-by-p homomorphism

$$[p] : \mathbb{G} \mapsto \mathbb{G}.$$

The **height** h of $\mathbb{G}$ is the height of $[p]$.

Theorem 5.5.1 (Lazard)**.** *Two (one-dimensional commutative) formal groups over K are isomorphic if and only if they have equal height.*

Proof. See [5], III.2 Theorem 2. □

For example, the height of $\mathbb{G}_m$ is 1, because $[p]$ is given by the power series $(1+X)^p - 1 = X^p$. The height of $\mathbb{G}_a$ is ∞, because $[p] \equiv 0$. By Lazard's theorem, they are nonisomorphic over K.

Theorem 5.5.2. *Let E be an elliptic curve over K. Then $\hat{E}$ has height either* 1 *or* 2*.*

Proof. Consider $[p] : \hat{E} \to \hat{E}$, which is induced by multiplication-by-p $[p] : E(K) \to E(K)$ on the K-rational points of E. This is an isogeny of degree p^2, and it is inseparable. The result follows from the lemma below: □

Lemma 5.5.3. *Let $0 \neq \varphi : E_1 \to E_2$ be an isogeny of elliptic curves over K and $f : \hat{E}_1 \to \hat{E}_2$ the induced homomorphism of formal group (laws). Then*

$$p^{h(f)} = \deg_i(\varphi).$$

Proof. It is enough to show this for the cases that φ is the $q = p^r$-power Frobenius map or that f is separable, as all isogenies can be written as a composition of these and both sides of the claim are multiplicative. However, in the first case, $\deg_i(\varphi) = q$ and $f(X) = X^q$; in the second case, choose invariant differentials ω_1 on E_1 and ω_2 on E_2, both adapted to the formal parameter X on $\hat{E}_1$ and $\hat{E}_2$, respectively. We have $\deg_i(\varphi) = 1$ and $\varphi^*\omega_2 \neq 0$, so

$$f'(0)\omega_1 = \omega_2 \circ f(X) = (\varphi^*\omega_2)(X) \neq 0 \in K[|X|]\mathrm{d}X.$$

It follows that $f'(0) \neq 0$ and so $h(f) = 0$. □

If $\hat{E}$ has height two, we call E **supersingular**; otherwise, we call E **ordinary**. Of course, elliptic curves are nonsingular by definition, so supersingular elliptic curves are never singular - this is only terminology.

Chapter 6

Complex multiplication

6.1 Preliminary results

Let E be an elliptic curve defined over a subfield F of $\mathbb{C}$. The **endomorphisms** of E are isogenies $\psi : E(F) \to E(F)$. They have the structure of a ring $\mathrm{End}_F(E)$: we define

$$(\psi + \phi)(P) := \psi(P) \oplus \phi(P)$$

and use composition as multiplication.

We always have a map

$$[\,] : \mathbb{Z} \to \mathrm{End}_F(E), \;\; n \mapsto [n]$$

where $[n]$ is defined by successive addition or subtraction of the identity $[1] := id$. In many cases, this map gives us every endomorphism; we are interested here in the cases where it doesn't.

Theorem 6.1.1. *The endomorphism ring of any elliptic curve E defined over F is isomorphic to either $\mathbb{Z}$ or an order $\mathcal{O}$ of an imaginary quadratic number field K. In the latter case, we say that E has **complex multiplication** by $\mathcal{O}$.*

Proof. See [20] VI.6.1 □

$\mathrm{End}_F(E)$ can be canonically identified with a subring of F: we have an injection

$$i : \mathrm{End}_F(E) \hookrightarrow \mathrm{End}_F(\Omega_{E/F}(E)) = F, \;\; \phi \mapsto \phi^*.$$

For this reason, we may always assume without loss of generality that K is a subfield in F.

It will make everything easier if we assume now that our elliptic curves with complex multiplication have it by the full ring of integers $\mathcal{O}_K$ of K. This is not terribly restrictive; we cannot assume this up to isomorphism, but at least up to isogeny:

Lemma 6.1.2. *Let E/F be an elliptic curve with complex multiplication by an order $\mathcal{O}$ of K. Then there exists an elliptic curve E'/F with $End_F(E') = \mathcal{O}_K$ and an isogeny $\phi : E \to E'$ defined over F.*

Proof. See [16], 5.3. □

The importance of this is that, given an elliptic curve E with complex multiplication by $\mathcal{O}_K$, we can give an isomorphism $E \cong \mathbb{C}/\Lambda := E_\Lambda$ for some lattice Λ which is fixed by $\mathcal{O}_K$. By multiplying with an appropriate constant, we can replace Λ with a homothetic lattice contained in K - this is just a fractional ideal of K.

Lemma 6.1.3. *Let $\mathfrak{a} \neq (0)$ be an ideal of $\mathcal{O}_K$, where E has complex multiplication by $\mathcal{O}_K$. Denote by $E[\mathfrak{a}]$ the subgroup of points fixed by every endomorphism of $\mathfrak{a}$. Then there is a natural isomorphism of $\mathcal{O}_K$-modules*

$$E[\mathfrak{a}] \cong \mathcal{O}_K/\mathfrak{a}.$$

Proof. Let Λ be a fractional ideal of K such that $E \cong \mathbb{C}/\Lambda$; then we have

$$E[\mathfrak{a}] \cong \mathfrak{a}^{-1}\Lambda/\Lambda \cong \mathcal{O}_K/\mathfrak{a}.$$

□

Proposition 6.1.4. *Let Cl_K be the ideal class group of K. Then Cl_K acts simply transitively on the isomorphism classes of elliptic curves defined over F with endomorphism ring $\mathcal{O}_K$, where the action is given by*

$$[\mathfrak{a}] \cdot [\mathbb{C}/\Lambda] := [\mathbb{C}/(\mathfrak{a}^{-1}\Lambda)].$$

Proof. If we assume that Λ is a nonzero fractional ideal, then $\mathfrak{a}^{-1}\Lambda$ is one as well. The action is well defined, because $\mathbb{C}/\Lambda \cong \mathbb{C}/\alpha\Lambda$ for any $\alpha \in \mathcal{O}_K$, and we have

$$[\mathfrak{a}] \cdot ([\mathfrak{b}]) \cdot [\mathbb{C}/\Lambda] = [\mathbb{C}/\mathfrak{a}^{-1}\mathfrak{b}^{-1}\Lambda] = [\mathbb{C}/(\mathfrak{a}\mathfrak{b})^{-1}\Lambda] = ([\mathfrak{a}][\mathfrak{b}]) \cdot [\mathbb{C}/\Lambda].$$

To show transitivity, let Λ_1 and Λ_2 be two nonzero fractional ideals of K; then it follows that

$$[\Lambda_2^{-1}\Lambda_1] \cdot [\mathbb{C}/\Lambda_1] = [\mathbb{C}/\Lambda_2\Lambda_1^{-1}\Lambda_1] = [\mathbb{C}/\Lambda_2].$$

To see that the action is simply transitive, assume that $[\mathfrak{a}] \cdot [\mathbb{C}/\Lambda] = [\mathfrak{b}] \cdot [\mathbb{C}/\Lambda]$ for some fractional ideal Λ. Then $\mathfrak{a}^{-1}\Lambda$ and $\mathfrak{b}^{-1}\Lambda$ are homothetic, so there is a $c \in \mathbb{C}^\times$ such that $\mathfrak{a}^{-1}\Lambda = c\mathfrak{b}^{-1}\Lambda$. In particular,

$$c\mathfrak{a}\mathfrak{b}^{-1}\Lambda = \Lambda = c^{-1}\mathfrak{a}^{-1}\mathfrak{b}\Lambda.$$

Since $c\mathfrak{a}\mathfrak{b}^{-1}$ and $c^{-1}\mathfrak{a}^{-1}\mathfrak{b}$ map Λ to itself, they contain endomorphisms of $\mathbb{C}/\Lambda$ and are therefore both contained in $\mathcal{O}_K$; so they both must be equal to $\mathcal{O}_K$. It follows that $\mathfrak{a} = c\mathfrak{b}$, and so $c \in K$ and $[\mathfrak{a}] = [\mathfrak{b}]$ in Cl_K. □

6.2 Class field theory

The deep connection between complex multiplication of elliptic curves and global class field theory compels us to use a number of definitions and theorems from the latter area. We provide a review of the concepts which will be useful later in this section. Proofs can be found in [14] or in a number of other textbooks on algebraic number theory.

Let K be a finite field extension of $\mathbb{Q}$. If $\mathfrak{p}$ is a place of the ring of integers $\mathcal{O}_K$, let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$ and $v_\mathfrak{p}$ the associated valuation.

Definition 43. Let L/K be a finite Galois extension of fields, and $\mathfrak{p}$ an ideal of K which is unramified in L. Let $\mathfrak{P}$ be an ideal of L lying over $\mathfrak{p}$. Let l and k be the remainder fields of $L_\mathfrak{P}$ and $K_\mathfrak{p}$, respectively. Then we have isomorphisms

$$G(\mathfrak{P}) \cong \mathrm{Gal}(L_\mathfrak{P}/K_\mathfrak{p}) \cong \mathrm{Gal}(l/k),$$

where $G(\mathfrak{P}) = \{\sigma \in \mathrm{Gal}(L/K) : \ \sigma\mathfrak{P} = \mathfrak{P}\}$ is the decomposition group of $\mathfrak{P}$. The cyclic group $\mathrm{Gal}(l/k)$ is generated by the Frobenius automorphism; its image in $\mathrm{Gal}(L/K)$, which generates $G(\mathfrak{P})$, is called the **Frobenius element** of $\mathrm{Gal}(L/K)$ at $\mathfrak{P}$, denoted $(\mathfrak{P}, L/K)$.

Lemma 6.2.1. *Use the notation as above. For any $\sigma \in \mathrm{Gal}(L/K)$,*

$$(\sigma\mathfrak{P}, L/K) = \sigma(\mathfrak{P}, L/K)\sigma^{-1}.$$

Proof. Let $x \in \mathcal{O}_L$. Then we have

$$\sigma(\mathfrak{P}, L/K)\sigma^{-1}x \equiv \sigma(\sigma^{-1}x)^q \equiv x^q \pmod{\sigma\mathfrak{P}}$$

where $q = \#k$. This implies that $\sigma(\mathfrak{P}, L/K)\sigma^{-1}$ is the Frobenius element at $\sigma\mathfrak{P}$. □

In particular, if L/K is abelian, then the Frobenius elements $(\mathfrak{P}, L/K)$, $\mathfrak{P}|\mathfrak{p}$, are all equal; we denote this element by $(\mathfrak{p}, L/K)$.

Lemma 6.2.2. *Let $M/L/K$ be a tower of Galois extensions; let $\mathfrak{P}$ be a prime of L lying over $\mathfrak{p}$, and $\mathfrak{Q}$ a prime of M lying over $\mathfrak{P}$. Then*
(i) $(\mathfrak{Q}, M/K)|_L = (\mathfrak{P}, L/K)$.
(ii) $(\mathfrak{Q}, M/L) = (\mathfrak{Q}, M/K)^f(\mathfrak{P}/\mathfrak{p})$.

Proof. One easily shows that in both cases, the elements in question correspond to the Frobenius automorphism on the residue fields. □

Definition 44. Let L/K be a finite abelian extension, and let S be a set of primes of K containing all those that ramify in L. Let I_K^S be the subgroup of the ideal group I_K generated by those primes not in S. The **Artin reciprocity map** is given by

$$(-, L/K) : I_K^S \to \mathrm{Gal}(L/K), \ \prod_{i=1}^{t} \mathfrak{p}_i^{n_i} \mapsto \prod_{i=1}^{t} (\mathfrak{p}_i, L/K)^{n_i}.$$

The Artin map factors through $N_{L/K}(I_L^S)$, where I_L^S is generated by the primes of L lying over primes in S; this follows from the previous lemma, using the fact that

$$N_{L/K}(\mathfrak{P}) = \mathfrak{p}^{f(\mathfrak{P}/\mathfrak{p})}$$

for any prime $\mathfrak{P}$ lying over the prime $\mathfrak{p}$ of K.

Definition 45. A **modulus** of K is a function

$$m : \{\text{places of } K\} \to \mathbb{N}_0$$

such that $m(\mathfrak{p}) \geq 0$ and $m(\mathfrak{p}) = 0$ for almost all $\mathfrak{p}$; $m(\mathfrak{p}) \in \{0, 1\}$ if $\mathfrak{p}$ is infinite and real; and $m(\mathfrak{p}) = 0$ if $\mathfrak{p}$ is complex.

We will also write the modulus m as a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m(\mathfrak{p})}.$$

Given a modulus $\mathfrak{m}$, we define the set

$$S(\mathfrak{m}) := \{\mathfrak{p} : m(\mathfrak{p}) > 0\}$$

of primes dividing $\mathfrak{m}$, and the group $K_{m,1}$ of principal (fractional) ideals (x) such that x is positive under all real embeddings of K, and $x - 1 \in \mathfrak{p}^{m(\mathfrak{p})}$ for all finite $\mathfrak{p}$. We have $K_{\mathfrak{m},1} \subseteq I^{S(\mathfrak{m})}$.

$$C_{\mathfrak{m}} := I_K^{S(\mathfrak{m})} / K_{\mathfrak{m},1}$$

is called the **ray class group** of K modulo $\mathfrak{m}$.

Theorem 6.2.3 (Artin reciprocity)**.** *Let L/K be a finite abelian extension. Then there exists a modulus $\mathfrak{m}$ such that $S := S(\mathfrak{m})$ contains all primes of K that ramify in L and such that $K_{\mathfrak{m},1} \subseteq \mathrm{Ker}(-, L/K)$, and the Artin map factors to an isomorphism*

$$I_K^S / (K_{\mathfrak{m},1} N_{L/K}(I_L^S)) \to \mathrm{Gal}(L/K).$$

Theorem 6.2.4 (Takagi existence theorem)**.** *Let $\mathfrak{m}$ be a modulus and $S = S(\mathfrak{m})$. Let H be a congruence subgroup modulo $\mathfrak{m}$, i.e.*

$$K_{\mathfrak{m},1} \subseteq H \subseteq I_K^S.$$

Then there exists a finite abelian extension L/K such that $H = K_{\mathfrak{m},1} N_{L/K}(I_L^S)$.

By Artin reciprocity, we then have an isomorphism

$$I_K^S / H \cong \mathrm{Gal}(L/K).$$

L is called the **class field** of H.
In particular, the class field $K_{(\mathfrak{m})}$ of $K_{\mathfrak{m},1}$ is called the **ray class field** modulo $\mathfrak{m}$, and the Artin map induces an isomorphism $C_{\mathfrak{m}} \cong \mathrm{Gal}(K_{(\mathfrak{m})}/K)$.

Definition 46. The **Hilbert class field** H of K is the ray class field for the modulus $\mathfrak{m} = 1$. It is therefore the maxmimal unramified abelian extension of K. Artin reciprocity gives an isomorphism

$$Cl(K) \cong \mathrm{Gal}(H/K)$$

where $Cl(K)$ is the ideal class group of K.

Theorem 6.2.5 (Principal ideal theorem)**.** *Let $\mathfrak{a}$ be an ideal of K and let H be the Hilbert class field of K. Then $\mathfrak{a}\mathcal{O}_H$ is a principal ideal.*

Theorem 6.2.6 (Chebotarev density theorem)**.** *Let L/K be a finite Galois extension and let C be a conjugacy class in $\mathrm{Gal}(L/K)$. Then the set of primes $\mathfrak{p}$ of K such that $C = \{(\mathfrak{P}, L/K) : \mathfrak{P}|\mathfrak{p}\}$ has analytic density $|C|/[L : K]$ in the set of all primes of K.*

Here, we say a set of primes T has analytic density δ if

$$\lim_{s \to 1_+} \frac{\sum_{\mathfrak{p} \in T} \mathfrak{N}(\mathfrak{p})^{-s}}{\delta \log \frac{1}{1-s}} = 1.$$

We now introduce another perspective of class field theory - not in terms of ideals, as above, but rather in terms of ideles. The ideles of K form a group that captures information about all completions of K simultaneously and provide a more natural, if less familiar, framework in which the results above may be understood. Importantly, we no longer worry about ramification of primes and can deal with all abelian extensions (even infinite) simultaneously.

Definition 47. The group of **ideles** of K is the restricted product

$$\mathfrak{I}_K := \{s = (s_{\mathfrak{p}})_{\mathfrak{p}} \in \prod_{\mathfrak{p}} K_{\mathfrak{p}}^{\times} : \ s_{\mathfrak{p}} \in U_{\mathfrak{p}} \text{ for almost all } \mathfrak{p}\}.$$

Here, $U_{\mathfrak{p}}$ is the ring $\mathcal{O}_{K_{\mathfrak{p}}}^{\times}$ if $\mathfrak{p}$ is finite and $K_{\mathfrak{p}}^{\times}$ otherwise.

The ideles of K form a topological group, where a basis of open sets is given by sets of the form $\prod_{\mathfrak{p}} U_{\mathfrak{p}}$, where $U_{\mathfrak{p}} \subseteq K_{\mathfrak{p}}^{\times}$ is open for all $\mathfrak{p}$, and $U_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}^{\times}$ for almost all $\mathfrak{p}$. Via

$$K^{\times} \hookrightarrow \mathfrak{I}_K, \ \ x \mapsto (x)_{\mathfrak{p}},$$

$K^{\times}$ becomes a discrete subgroup of $\mathfrak{I}_K$. The quotient

$$\mathfrak{C}_K := \mathfrak{I}_K / K^{\times}$$

is called the **idele class group** of K.

Definition 48. Let L/K be a finite field extension. The **norm** map is given by

$$N_{L/K} : \mathfrak{I}_L \to \mathfrak{I}_K, \ \ (s_{\mathfrak{P}})_{\mathfrak{P}} \mapsto (\prod_{\mathfrak{P}|\mathfrak{p}} N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} s_{\mathfrak{P}})_{\mathfrak{p}}.$$

There is also a natural map from ideles to ideals, sending $s \in \mathfrak{I}_K$ to $(s) := \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}} s_{\mathfrak{p}}}$.

Theorem 6.2.7 (Artin reciprocity - ideles)**.** *Let K^{ab} be the maximal abelian extension of K. There is a unique continuous homomorphism (the **Artin reciprocity map**)*

$$[-, K] : \mathfrak{I}_K \to \mathrm{Gal}(K^{ab}/K), \ \ s \mapsto [s, K]$$

such that for any finite abelian extension L/K and idele $s \in \mathfrak{I}_L$ whose ideal (s) is not divisible by primes that ramify in L,

$$[s, K]|_L = ((s), L/K).$$

In addition, the following properties hold:
(i) $[-, K]$ is surjective and $K^{\times} \subseteq \mathrm{Ker}[-, K]$.
(ii) If L/K is a finite abelian extension, then

$$[s, L]|_{K^{ab}} = [N_{L/K} s, K] \ \ \forall s \in \mathfrak{I}_L.$$

(iii) If $\mathfrak{p}$ is a prime of K and L/K is abelian and unramified at $\mathfrak{p}$, and π is an idele of K with a uniformizer of $\mathcal{O}_{\mathfrak{p}}$ in its $\mathfrak{p}$-th component and units elsewhere, then

$$[\pi, K]|_L = (\mathfrak{p}, L/K).$$

Theorem 6.2.8. *Let $\mathfrak{m}$ be a modulus for K, $K_{(\mathfrak{m})}$ the ray class field of K modulo $\mathfrak{m}$, and*

$$U_{\mathfrak{m}} := \{s \in \mathfrak{I}_K : s_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^{\times}, \ s_{\mathfrak{p}} - 1 \in \mathfrak{p}^{m(\mathfrak{p})} \text{ for all finite } \mathfrak{p}, \ s_{\mathfrak{p}} > 0 \text{ for real } \mathfrak{p}\},$$

which is an open subgroup of $\mathfrak{I}_K$. Then the Artin map factors to an isomorphism

$$[-, K] : \mathfrak{I}_K / K^{\times} U_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Gal}(K_{(\mathfrak{m})}/K).$$

6.3 The main theorem and applications

Let E/F be an elliptic curve over the number field F with complex multiplication by $\mathcal{O}_K$, given by a choice of Weierstrass equation

$$E : y^2 = x^3 + px + q.$$

For an automorphism $\sigma \in \mathrm{Aut}(\mathbb{C}/\mathbb{Q})$, we define a second elliptic curve E^σ by the Weierstrass model

$$E^\sigma : y^2 = x^3 + \sigma(p)x + \sigma(q).$$

There is a natural group homomorphism, also denoted by σ:

$$\sigma : E(\mathbb{C}) \to E^\sigma(\mathbb{C}), \;\; (x, y) \mapsto (\sigma(x), \sigma(y)), \;\; O \mapsto O.$$

Additionally, find a fractional ideal $\Lambda \subseteq K$ such that there is an isomorphism

$$\xi : \mathbb{C}/\Lambda \to E.$$

In this setting, we can formulate Shimura's 'main theorem' of complex multiplication:

Theorem 6.3.1. *Let s be an idele of K with $\sigma|_{K^{ab}} = [s, K]$. Then there is a unique isomorphism*

$$\xi' : \mathbb{C}/s^{-1}\Lambda \to E^\sigma$$

which makes the diagram below commutative:

$$\begin{tikzcd}
K/\Lambda \arrow[r, "\xi"] \arrow[d, "s^{-1}"] & E_{tors} \arrow[d, "\sigma"] \\
K/s^{-1}\Lambda \arrow[r, "\xi'"] & E^\sigma_{tors}
\end{tikzcd}$$

Here, E_{tors} denotes the torsion subgroup of $E(\mathbb{C})$, and E^σ_{tors} is defined similarly.

Proof. See [18], theorem 5.4. □

Theorem 6.3.2. *(i) $j(E)$ generates the Hilbert class field of K.*
(ii) $j(E)$ is an algebraic integer.

Proof. Let $\sigma \in \mathrm{Aut}(\mathbb{C}/K)$ Then

$$j(E) = j(E)^\sigma \Leftrightarrow E \cong E^\sigma \Leftrightarrow \mathbb{C}/\mathfrak{a} \cong \mathbb{C}/s\mathfrak{a}$$

for the idele s from the main theorem. This is true iff $|s_\mathfrak{p}|_\mathfrak{p} = 1$ for all finite places $\mathfrak{p}$, and so

$$s \in K^\times \prod_{\mathfrak{p}\nmid\infty} \mathcal{O}_\mathfrak{p}^\times \prod_{\mathfrak{p}|\infty} K^\times$$

$$\Leftrightarrow \overline{s} \in C_K^1 = N_{H/K} C_H = \mathrm{Ker}[(-, H/K)]$$

by global class field theory (note that any $\mathfrak{p}|\infty$ is a complex place), and therefore if and only if σ is the identity on H; so we must have $j(E) \in H$.
(ii) See [18], 4.6. □

As a corollary, we see that any elliptic curve with complex multiplication has everywhere potential good reduction - its j-invariant has a non-negative valuation at every prime.

Theorem 6.3.3. *There exists a Hecke character $\psi_E : \mathfrak{I}_F \to \mathbb{C}^\times$, i.e. ψ_E is a continuous homomorphism with $\psi_E(F^\times) = 1$), of the idele class group with the following properties:*
(i) Let $x \in \mathfrak{I}_F$ have norm $y = N_{F/K} x \in \mathfrak{I}_K$. Then

$$\psi_E(x)\mathcal{O} = y_\infty^{-1} y \mathcal{O} \subseteq \mathbb{C}.$$

(ii) Let $x \in I_F$ be finite (1 at all archimedean places) and $\mathfrak{p}$ a prime ideal of K. Then $\psi_E(x)(y)_\mathfrak{p}^{-1} \in \mathcal{O}_\mathfrak{p}^\times$ and for $P \in E[\mathfrak{p}^\infty]$ we have

$$(x, F^{ab}/F)P = \psi_E(x)(y)_\mathfrak{p}^{-1} P.$$

(iii) For an ideal $\mathfrak{q}$ of F with $U_\mathfrak{q} = \{x \in F_\mathfrak{q} : v_\mathfrak{q}(x) = 0\}$, $\psi_E(U_\mathfrak{q}) = 1$ if and only if E has good reduction at $\mathfrak{q}$.

Proof. Let $\sigma = (x, F^{ab}/F) \in \mathrm{Gal}(F^{ab}/F)$. Then we have $(y, K^{ab}/K) = \sigma|_{K^{ab}}$, since the Artin reciprocity symbol commutes with inflation and corestriction. Clearly $E^\sigma = E$, and so by Theorem 1 we have an isomorphism

$$\xi^{-1} \circ \xi' : \mathbb{C}/y^{-1}\mathfrak{a} \to \mathbb{C}/\mathfrak{a},$$

which must be a multiplication by some element $z \in K^\times$ such that $z\mathcal{O} = y\mathcal{O}$. We define

$$\psi_E(x) := y_\infty^{-1} z.$$

Then ψ_E is a well-defined group homomorphism: for $x_1, x_2 \in I_F$ with $\psi_E(x_i) = y_\infty^{-1} z_i$ we have by uniqueness in Theorem 1 that $\xi^{-1}\xi'_{x_1 x_2} = \xi^{-1}\xi'_{x_1}\xi^{-1}\xi'_{x_2}$ which represents multiplication by $z_1 z_2$. Condition (i) is immediate. We also see that for any prime $\mathfrak{p}$ in K, $\psi_E(x)(y)_\mathfrak{p}^{-1} \in \mathcal{O}_\mathfrak{p}^\times$ holds.
For any number $k \in \mathbb{N}$, we have a commutative diagram from Theorem 1:

$$\begin{tikzcd}
\mathfrak{p}^{-k}\mathfrak{a}_{\mathfrak{p}}/\mathfrak{a}_{\mathfrak{p}} \arrow[r, "\sim"] \arrow[d, "y_{\mathfrak{p}}^{-1}"] & \mathfrak{p}^{-k}\mathfrak{a}/\mathfrak{a} \arrow[r, "\xi"] \arrow[d, "y^{-1}"] & E[\mathfrak{p}^k] \arrow[d, "\sigma"] \\
\mathfrak{p}^{-k}y_{\mathfrak{p}}^{-1}\mathfrak{a}_{\mathfrak{p}}/y_{\mathfrak{p}}^{-1}\mathfrak{a}_{\mathfrak{p}} \arrow[r, "\sim"] & \mathfrak{p}^{-k}y^{-1}\mathfrak{a}/y^{-1}\mathfrak{a} \arrow[r, "z\cdot\xi"] & E[\mathfrak{p}^k]
\end{tikzcd}$$

which completes the proof of (ii).
(iii) Let $\mathfrak{q}$ be a prime in F and p a rational prime with $\mathfrak{q} \nmid (p)$. For any $u \in U_{\mathfrak{q}}$, $(u, F^{ab}/F)$ acts on $T_p(E)$ via multiplication by $\psi_E(u)$ (by (ii)). However, $T_{\mathfrak{q}} := (U_{\mathfrak{q}}, F^{ab}/F)$ is the inertia group of $\mathfrak{q}$. By the Neron-Ogg-Shafarevich criterion,

$$\psi_E(U_{\mathfrak{q}}) = 1 \Leftrightarrow T_{\mathfrak{q}} \text{ acts trivially on } T_p(E) \Leftrightarrow E \text{ has good reduction at } p.$$

□

Let $\mathfrak{f}_E$ be the conductor of ψ_E: we will consider ψ_E as a character on the ideal group by first mapping ideals $\mathfrak{p}$ with an element π of order one ($\mathrm{ord}_{\mathfrak{p}}\pi = 1$) to the idele $(x_{\mathfrak{p}})_{\mathfrak{p}}$ with π in the $\mathfrak{p}$-coordinate and 1 elsewhere; then mapping into $\mathbb{C}$ as earlier. This is well-defined (independent of the choice of π) as long as ψ_E is unramified at $\mathfrak{p}$, that is, if $\psi_E(U_{\mathfrak{p}}) = 1$. If ψ_E is ramified at $\mathfrak{p}$, we set $\psi_E(\mathfrak{p}) = 0$.

By definition, $\mathfrak{f}$ is then the largest ideal such that ψ_E can be defined on the ray class group mod $\mathfrak{f}$. In particular, E has good reduction at all primes not dividing $\mathfrak{f}$.

Lemma 6.3.4 (ψ_E on ideals). *(i) Let $\mathfrak{a}$ be an ideal of F coprime to $\mathfrak{f}$. Then $\psi_E(\mathfrak{a})\mathcal{O} = N_{F/K}(\mathfrak{a})$.*
(ii) Let $\mathfrak{q}$ be an prime ideal of F that is coprime to $\mathfrak{f}$, and $\mathfrak{a}$ an ideal of $\mathcal{O}$ that is coprime to $\mathfrak{q}$. Then $(\mathfrak{q}, F(E[\mathfrak{a}])/F) = \psi_E(\mathfrak{q})$.
(iii) If $\mathfrak{q}$ is an ideal of F at which E has good reduction, and $(q) = N_{F/\mathbb{Q}}(\mathfrak{q})$, then $\psi_E(\mathfrak{q}) \in K$ (understood as an automorphism of E) reduces modulo $\mathfrak{q}$ to the Frobenius morphism ϕ_q.

Proof. (i) and (ii) are immediate from Theorem 3 (i),(ii) following the definition of ψ_E as a character of the ideal group.
(iii): Let $P \in E_{tors}$ have order prime to $\mathfrak{q}$ and $\overline{P}$ its reduction mod $\mathfrak{q}$. Then for any prime $\mathfrak{a}$ as in (ii)

$$\overline{\psi_E(\mathfrak{q})P} = \overline{(\mathfrak{q}, F(E[\mathfrak{a}])/F)P} = \varphi_q\overline{P},$$

since the reciprocity symbol gives exactly the Frobenius element. Since endomorphisms are determined by ℓ-torsion for any prime ℓ, the result follows. □

Finally, the reduction of elliptic curves with complex multiplication at a prime of good reduction can be described in more detail. Recall that in this case, the elliptic curve as everywhere potential good reduction, so that by enlarging the field of definition F we can assume that it has everywhere good reduction.

Theorem 6.3.5. *An elliptic curve E/F with complex multiplication by $\mathcal{O}_K$ has ordinary reduction at a prime $\mathfrak{P}$ of F if and only if $(p) := \mathfrak{P} \cap \mathbb{Q}$ splits in K.*

Proof. See [12], 13.4 (Theorem 12). □

Chapter 7

The L-function

The theory (and notation) of L-functions begins with Dirichlet. While Euler considered what is now known as the Riemann zeta function $\sum_{n=1}^{\infty} \frac{1}{n^s}$ and proved a product expansion over the rational primes, Dirichlet extended this to consider functions of the form $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$, $a_n \in \mathbb{C}$. Series of this type may be thought of as generating functions for the sequence (a_n), and are often better behaved when the sequence (a_n) possesses a natural 'multiplicative' structure.

For example, if a_n is a multiplicative sequence - that is, for any coprime numbers m, n we have $a_{mn} = a_m a_n$ - we have the **Euler product**

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \text{ prime}} \Big(\sum_{k=0}^{\infty} \frac{a_{p^k}}{p^{ks}} \Big)$$

as a formal identity; the product on the right as the same convergence properties as the sum on the left. In the case of a strictly multiplicative sequence - that is, for *any* m, n we have $a_{mn} = a_m a_n$ - the Euler product may be written as

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - a_p p^{-s}}.$$

Both Dirichlet series and product representations are commonly used to define special functions - we will mostly consider the latter.

Standard questions include convergence, existence of functional equations, locations of zeros and poles, and existence of interesting special values - for example, values at integers, or the behavior of the L-function near its singularities. In the case of L-functions associated to elliptic curves (the definition is given later), interesting results are known - for example, an analogy of the Riemann hypothesis shows that all its zeros must have real part 1/2 - but conjectures remain numerous. In particular, the Birch and Swinnerton-Dyer conjecture attempts to predict the rank of an elliptic curve over a number field (and other arithmetic information) in terms of an associated L-function at the point $s = 1$.

7.1 The ζ-function

An **arithmetic scheme** is a scheme X where the natural morphism $f : X \to \operatorname{Spec}\mathbb{Z}$ is of finite type.

Definition 49. Let X be an arithmetic scheme. We define the **zeta function**

$$\zeta_X(s) := \prod_{x\in|X|} \frac{1}{1-N(x)^{-s}},$$

where $N(x)$ is the cardinality of the residue field $\kappa(x)$ at x, and $|X|$ denotes the set of closed points of X.

That this is well-defined requires some explanation. First note that the residue fields at x are always finite: this follows from the following lemma.

Lemma 7.1.1. *Let A be a field that is finitely generated as a $\mathbb{Z}$-algebra. Then A is finite.*

Proof. If A has characteristic $p > 0$, this follows from Noether normalization: since A is 0-dimensional, it is finitely generated as a module over $\mathbb{F}_p$ and therefore finite. If A has characteristic 0, then it is a flat $\mathbb{Z}$-module and so $\operatorname{Spec} A \to \operatorname{Spec}\mathbb{Z}$ is flat and of finite type. By exercise III.9.1 in Hartshorne's book ([6]) it is an open map. However, its image is only the zero ideal $\{(0)\} \subseteq \operatorname{Spec}\mathbb{Z}$ and this is not open - a contradiction. □

In particular, if x is a closed point, then $f(x) = (p)$ is a maximal ideal of $\mathbb{Z}$ - indeed, $\kappa(x)$ is a finite field extension of the residue field $\kappa(f(x))$ on Spec $\mathbb{Z}$, and is also a finite field. Additionally, for any $n \in \mathbb{N}$ there are only finitely many closed points on each fiber X_p with residue field of cardinality less than n. To see this, note first that the closed points on X_p are exactly the closed points on the reduced subscheme $(X_p)_{red}$, and so it is enough to assume that X_p is reduced. Now the base change $\overline{f} : X_p \to \operatorname{Spec}\mathbb{F}_p$ is of finite type, hence quasicompact, so by passing to a finite cover we may then assume that X_p is affine. Finally, for every finite field extension $\mathbb{F}_q$ of $\mathbb{F}_p$, $X_p(\mathbb{F}_q)$ is finite, being the set of zeros in $\mathbb{F}_q$ of finitely many polynomials in over $\mathbb{F}_p$. Since any closed point x with residue field $\kappa(x)$ of cardinality $p^e \leq q$ induces an inclusion map $\kappa(x) \to \mathbb{F}_q$, corresponding uniquely to a morphism $\operatorname{Spec} K \to X$, there can be only finitely many such points.

The zeta function may be represented as a Dirichlet series. For $n \in \mathbb{N}$, let a_n denote the number of ways to write $n = \prod_{i=1}^k N(x_i)^{v_i}$ with closed points $x_i \in |X|$ and $v_i \in \mathbb{N}$ (for $n = 1$, we also consider the empty product); then there is a formal equality

$$\zeta_X(s) = \prod_{x\in|X|} \frac{1}{1-N(x)^{-s}} = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Theorem 7.1.2. *For any $s \in \mathbb{C}$ with $\mathfrak{Re}(s) > \dim X$, the product $\zeta_X(s)$ converges absolutely. It describes a holomorphic function without zeros.*

Proof. See [15] 1.6 □

Note also that in the case of convergence, we have a decomposition $\zeta_X(s) = \prod_p \zeta_{X_p}(s)$ over the fibers of f.

Example: Let $X = \operatorname{Spec} \mathbb{Z}$. Then the residue field of $x = (p) \in |X|$ is $\mathbb{F}_p$, and we see that

$$\zeta_X(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}} = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

is the Riemann zeta function; this converges for $\mathfrak{Re}(s) > \dim \mathbb{Z} = 1$.

Example: Let $X = \operatorname{Spec} \mathcal{O}_K$, where K is a number field and $\mathcal{O}_K$ its ring of integers. Then

$$\zeta_X(s) = \prod_{(0) \neq \mathfrak{p} \text{ prime}} \frac{1}{1 - \mathfrak{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-s}} = \sum_{(0) \neq \mathfrak{a}} \frac{1}{\mathfrak{N}_{K/\mathbb{Q}}(\mathfrak{a})^s}$$

is the Dedekind zeta function of K; here, $\mathfrak{a}$ traverses the nonzero ideals of $\mathcal{O}_K$. This series converges for $\mathfrak{Re}(s) > \dim \mathcal{O}_K = 1$.

The decomposition of ζ_X over the fibers X_p implies that it is useful to first study the positive characteristic; that is, where X is taken as a scheme of finite type over some finite field $\mathbb{F}_q$, so every residue field is an extension of $\mathbb{F}_q$. For each closed point $x \in |X|$ let $\deg(x) := [\kappa(x) : \mathbb{F}_q]$; that is, $N(x) = q^{\deg(x)}$. Then in a half-plane of convergence, we have

$$\log \zeta_X(s) = \sum_{x \in |X|} -\log(1 - N(x)^{-s}) = \sum_{x \in |X|} \sum_{k=1}^{\infty} \frac{q^{-sk \cdot \deg(x)}}{k}$$

$$= \sum_{n=1}^{\infty} \sum_{k \cdot \deg(x)} \frac{1}{k} q^{-ns} = \sum_{n=1}^{\infty} \sum_{\deg(x) | n} \frac{q^{-ns}}{n} = \sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{q^n})}{n} q^{-ns}.$$

This motivates the definition

$$Z_X(T) := \exp\Big(\sum_{n=1}^{\infty} \frac{\#X(\mathbb{F}_{q^n})}{n} T^n \Big),$$

so that $Z_X(q^{-s}) = \zeta_X(s)$.

Theorem 7.1.3 (Weil conjectures)**.** *Let X be a smooth projective variety over $\mathbb{F}_q$, and set $d := \dim X$.*

(i) (Rationality) $Z_X(T)$ is a rational function in T. In fact, there are integral polynomials

$P_k(T) \in \mathbb{Z}[T]$, $k = 0, ..., 2d$, where $P_0(T) = 1-T$, $P_{2d}(T) = 1-q^dT$ and complex factorizations $P_k(T) = \prod_j (1 - \alpha_{jk}T)$, $\alpha_{jk} \in \mathbb{C}$ such that

$$Z_X(T) = \frac{P_1(T) \cdot P_3(T) \cdot ... \cdot P_{2n-1}(T)}{P_0(T) \cdot P_2(T) \cdot ... \cdot P_{2n}(T)}.$$

(ii) (Functional equation) Let $e = \sum_{k=0}^{2n} (-1)^k \deg P_k$ (the Euler characteristic of X); then Z_X satisfies an identity of the form

$$Z_X(q^{-d}T^{-1}) = \pm q^{de/2} T^e Z_X(T).$$

(iii) (Riemann Hypothesis) For each $1 \leq k \leq 2d-1$ and every j, $|\alpha_{jk}| = q^{k/2}$.
(iv) (Betti numbers) If X is the reduction modulo a prime ideal of a variety Y over a number field $K/\mathbb{Q}$, then $\deg P_k$ is the k-th Betti number of the complex variety $Y \times_K \operatorname{Spec} \mathbb{C}$ with any embedding $K \hookrightarrow \mathbb{C}$.

Proof. It would be hopeless to attempt to prove this in the scope of this thesis. The case of elliptic curves is more elementary, and a proof for this is given in [20] V.2. □

In the special case of an elliptic curve E over $\mathbb{F}_q$, the Weil conjectures give us a simple description of its zeta function. We can realize E as the reduction modulo a prime of some elliptic curve E' over a number field, and so the first Betti number is $\dim_{\mathbb{C}} H^1(E'(\mathbb{C})) = 2g = 2$. Therefore, there is an algebraic integer α with

$$Z_E(s) = \frac{(1-\alpha T)(1-\overline{\alpha}T)}{(1-T)(1-qT)}.$$

We find

$$\sum_{n=1}^{\infty} \frac{\#E(\mathbb{F}_{q^n})}{n} T^n = \sum_{n=1}^{\infty} \frac{1}{n} T^n + \sum_{n=1}^{\infty} \frac{q^n}{n} T^n - \sum_{n=1}^{\infty} \frac{\alpha^n}{n} T^n - \sum_{n=1}^{\infty} \frac{\overline{\alpha}^n}{n} T^n$$

and therefore $\#E(\mathbb{F}_{q^n}) = q^n - 1 - \alpha^n - \overline{\alpha^n}$. This result is due to Hasse.

By the Riemann hypothesis, we have $\alpha\overline{\alpha} = q$. Therefore, we may write the above as

$$Z_E(T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)},$$

where $a = \alpha + \overline{\alpha} = q - 1 - \#E(\mathbb{F}_q)$.

Now take E to be an elliptic curve over the number field K. We have the decomposition

$$\zeta_E(s) = \prod_{\mathfrak{p}} \zeta_{E_{\mathfrak{p}}}(s)$$

where the product is taken over all primes $(0) \neq \mathfrak{p}$ of $\mathcal{O}_K$. For all but finitely many primes, the fiber $E_{\mathfrak{p}}$ actually defines an elliptic curve over $\mathcal{O}_K/\mathfrak{p}$, and we have found a satisfying description of its zeta function above. Otherwise, $E_\mathfrak{p}$ has a single singularity, and the zeta function turns out to be

$$\zeta_{E_\mathfrak{p}}(s) = \frac{1 - aq^{-s}}{(1-q^{-s})(1-q^{1-s})},$$

where $a_=1$ in the case of split multiplicative reduction, $a = -1$ for non-split multiplicative reduction, and $a = 0$ for additive reduction.

Definition 50. The **local L-function** of E at $\mathfrak{p}$ is given by

$$L_\mathfrak{p}(E, s) := (1-q^{-s})(1-q^{1-s})\zeta_{E_\mathfrak{p}}(s) = \begin{cases} 1 - \mathfrak{a}_p q^{-s} + q^{1-2s} & \text{: good reduction} \\ 1 - \mathfrak{a}_p q^{-s} & \text{: bad reduction.} \end{cases}$$

where $a_\mathfrak{p} = q - 1 - \#E_\mathfrak{p}(\mathcal{O}_K/\mathfrak{p}), 1, -1$ or 0 is defined as above.

$$L(E, s) := \prod_\mathfrak{p} L_\mathfrak{p}(E, s) = \frac{\zeta_E(s)}{\zeta(s)\zeta(s-1)}$$

is called the **L-function** of E.

7.2 L-functions and Galois representations

The L-function associated to an elliptic curve over the number field K is known to arise from a general construction of L-functions associated to Galois representations; here, one introduces the Tate module T_ℓ, on which $\mathrm{Gal}(\overline{K}/K)$ acts.

Definition 51. Let G be a topological group. A **representation** of G is a continuous homomorphism

$$\rho : G \to \mathrm{GL}(V),$$

where V is a finite-dimensional vector space over a field K. If H is a subgroup of G, the **invariant subspace** V^H of V is

$$V^H := \{v \in V : \rho(h)(v) = v \, \forall h \in H\}.$$

Consider now $G = \mathrm{Gal}(L/K)$ where L/K is a finite Galois extension of number fields. Let $\mathfrak{p}$ be a nonzero prime of K; recall that for any prime $\mathfrak{P}$ of L lying over $\mathfrak{p}$, the **inertia subgroup** $I(\mathfrak{P}/\mathfrak{p})$ consists of those automorphisms $\sigma \in G$ that map $\sigma(\mathfrak{P}) = \mathfrak{P}$ and for which the induced map $\overline{\sigma} : \mathcal{O}_K/\mathfrak{P} \to \mathcal{O}_K/\mathfrak{P}$ is the identity.

We denote here by $\mathrm{Frob}_\mathfrak{P}$ the Frobenius element $(\mathfrak{P}, L/K)$ of L/K at $\mathfrak{P}$; this is the unique automorphism with

$$\mathrm{Frob}_\mathfrak{P}(x) \equiv x^q \mod \mathfrak{P} \;\; \forall x \in \mathcal{O}_K$$

with $q := \#\mathcal{O}_K/\mathfrak{p}$. For any two primes $\mathfrak{P}_1$ and $\mathfrak{P}_2$ over $\mathfrak{p}$, $\rho(\mathfrak{P}_1)$ and $\rho(\mathfrak{P}_2)$ are conjugates; therefore, they leave $V^{I(\mathfrak{P}_1/\mathfrak{p})} = V^{I(\mathfrak{P}_2/\mathfrak{p})} =: V^{I(\mathfrak{p})}$ fixed and have equal characteristic polynomials on $V^{I(\mathfrak{p})}$. In particular, the characteristic polynomial depends only on the coset $\mathrm{Frob}_\mathfrak{p}$ in $\mathrm{Gal}(L/K)$.

Definition 52. The **Artin L-function** associated to ρ is

$$L(\rho, s) := \prod_{\mathfrak{p}} \frac{1}{\det\Big(1 - \rho(\mathrm{Frob}_\mathfrak{p})\mathfrak{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-s}\Big)|_{V^{I(\mathfrak{p})}}}.$$

Now let E be an elliptic curve over the number field K. For any prime $\ell \neq p$, we have the torsion groups $E[\ell^n] = \mathrm{Ker}[\ell^n]$.

Lemma 7.2.1. *There is an isomorphism $E[\ell^n] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.*

20. III.6.4(b) □

We then define the **Tate module**

$$T_\ell(E) := \varprojlim E[\ell^n] \cong \varprojlim \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \cong \mathbb{Z}_\ell^2.$$

The group $\mathrm{Gal}(\overline{K}/K)$ acts on $E[\ell^n]$: for an $\overline{K}$-valued point $P \in E[\ell^n]$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$, denote also by σ the morphism $\sigma : \mathrm{Spec}\,\overline{K} \to \mathrm{Spec}\,\overline{K}$, and define $\sigma \cdot P := P \circ \sigma$. This makes sense because

$$[\ell^n] \circ (\sigma \cdot P) = [\ell^n] \circ (P \circ \sigma) = ([\ell^n] \circ P) \circ \sigma = 0.$$

The action carries over to an action of $\mathrm{Gal}(\overline{K}/K)$ on $T_\ell(E)$. Define the $\mathbb{Q}_\ell$-vector space $V := T_\ell(E) \otimes_{\mathbb{Q}_\ell} \mathbb{Q}_\ell$; then we have a group representation

$$\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}(V) \cong \mathrm{GL}_2(\mathbb{Q}_\ell).$$

Definition 53. The L-function we associate to this representation is

$$L(\rho, s) = \prod_{\mathfrak{p}} \frac{1}{\det\Big(1 - \rho(\mathrm{Frob}_\mathfrak{p})\mathfrak{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-s}\Big)|_{V^{I(\mathfrak{p})}}}.$$

This definition is inspired by the preceding theory of Artin L-functions. Since the characteristic polynomial of each $\mathrm{Frob}_\mathfrak{p}$ has rational coefficients ([20] V.2.3), we may interpret $L(\rho, s)$ as a complex-valued function (up to a question of convergence). Remarkably, this is independent of ℓ; indeed,

Theorem 7.2.2. *We have $L(\rho, s) = L(E, s)$; that is, the L-function associated to the Galois representation ρ is the same as the L-function associated to the arithmetic scheme E.*

Proof. By [20] V.2.3, if E has good reduction at $\mathfrak{p}$,

$$\det \rho(\mathrm{Frob}_{\mathfrak{p}}) = q = \#\mathcal{O}_K/\mathfrak{p} \text{ and } \operatorname{tr} \rho(\mathrm{Frob}_{\mathfrak{p}}) = q + 1 - \#\tilde{E}(\mathbb{F}_q).$$

The factor for $\mathfrak{p}$ then becomes $(1 - (q + 1 - \#\tilde{E}(\mathbb{F}_q))q^{-s} + q \cdot q^{1-2s})^{-1}$.

If E has additive reduction, $V^{I(\mathfrak{p})} = 0$, and so the corresponding factor is 1. In the case of multiplicative reduction, that is, E has a node singularity, $V^{I(\mathfrak{p})}$ is one-dimensional; if the reduction is split - that is, if the two tangent lines are defined over $\mathbb{F}_q$ - the Frobenius acts as the identity and we have a factor $1 - q^{-s}$; if the reduction is non-split, the tangents are defined only over a quadratic extension of $\mathbb{F}_q$ and the corresponding factor becomes $1 + q^{-s}$.

In particular, we see that the factors corresponding to every $\mathfrak{p}$ in both L-functions are equal. □

7.3 The L-function and complex multiplication

Generally, the L-function of an elliptic curve defined over $\mathcal{O}_K$ is equal to the L-function of an appropriate 2-dimensional representation of $\mathrm{Gal}(\overline{K}/K)$. In the case of complex multiplication, it can actually be factored into L-functions of one-dimensional representations. The properties of these so-called Hecke L-series are better understood; in turn, this gives a better understanding of elliptic curves with complex multiplication as opposed to without.

Recall that a Hecke character ψ of a number field $F/\mathbb{Q}$ is a continuous homomorphism $\psi : \mathfrak{I}_F \to \mathbb{C}^\times$ from the ideles of F with $\psi^(F^\times) = 1$. If $\mathfrak{p}$ is an ideal of F at which ψ is not ramified, we defined $\psi(\mathfrak{p}) := \psi(x)$ for an idele $x = (x_{\mathfrak{p}})_{\mathfrak{p}}$ with $x_{\mathfrak{q}} = 1$, $\mathfrak{q} \neq \mathfrak{p}$ and $x_{\mathfrak{p}}$ a uniformizer at $\mathfrak{p}$; this is independent of the choice of uniformizer. This is extended multiplicatively to a character on ideals by defining $\psi(\mathfrak{p}) = 0$ if ψ ramifies at $\mathfrak{p}$. The **Hecke L-series** associated to ψ is

$$L(\psi, s) = \prod_{\mathfrak{p}} \frac{1}{(1 - \psi(\mathfrak{p})\mathfrak{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-s})};$$

that is, the Artin L-function associated to the one-dimensional representation ψ.

We give a slightly different definition of conductor here (as opposed to chapter 6) to keep track of ramification data at infinite places:

Definition 54. The **conductor** of the Hecke character ψ is the unique ideal $\mathfrak{f}$ of F and set of real valuations Ω such that ψ is a primitive character of the ray class group modulo $\mathfrak{f}\Omega$, i.e.

$$\psi((x)) = 1 \Leftrightarrow x \in 1 + \mathfrak{f},\ v(x) > 0\ \forall v \in \Omega.$$

If ψ has conductor $\mathfrak{f}\Omega$, we have the representation as a Dirichlet series

$$L(\psi, s) = \prod_{\mathfrak{p}} \frac{1}{(1 - \psi(\mathfrak{p})\mathfrak{N}(\mathfrak{p})^{-s})} = \sum_{\mathfrak{a}} \frac{\psi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s},$$

where the sum is taken over all integral ideals $\mathfrak{a}$ coprime to $\mathfrak{f}$; indeed, these are exactly the ideals for which $\psi(\mathfrak{a})$ is nonzero.

Theorem 7.3.1. *The L-function $L(\psi, s)$ associated to a Hecke character ψ has an analytic continuation on all of $\mathbb{C}$ and satisfies a functional equation.*

Proof. This result is due to Hecke, and an elegant adelic proof that better motivates the 'gamma factors' is given in Tate's doctoral thesis [21]. The functional equation is found by adding the appropriate Euler factors at the Archimedian places - these involve the usual Gamma function Γ on $\mathbb{C}$. Assuming ψ is primitive with conductor $\mathfrak{f}\Omega$,

$$\Lambda(\psi, s) = \varepsilon\Lambda(\psi^{-1}, 1 - s),$$

where we set $\Lambda(\psi, s)$ to be

$$L(\psi, s) \cdot (\mathfrak{N}_{F/\mathbb{Q}}(\mathfrak{f})|\Delta_F|)^{s/2} \Big(\prod_{v \text{ complex}} \frac{2\Gamma(s)}{(2\pi)^s} \Big) \Big(\prod_{v \in \Omega \text{ real}} \frac{\Gamma((s+1)/2)}{\pi^{(s+1)/2}} \Big) \Big(\prod_{v \notin \Omega \text{ real}} \frac{\Gamma(s/2)}{\pi^{s/2}} \Big),$$

Δ_F being the discriminant of $F/\mathbb{Q}$, and the root number ε is a product $\prod_{\mathfrak{p}} \epsilon_{\mathfrak{p}}$ satisfying $|\varepsilon| = 1$:

$$\varepsilon_{\mathfrak{p}} = \begin{cases} 1 & : \mathfrak{p} < \infty \text{ and } \psi \text{ and } K \text{ are nonramified at } \mathfrak{p} \\ 1 & : \mathfrak{p} = v \text{ is infinite and } v \notin \Omega \\ i = \sqrt{-1} & : \mathfrak{p} = v \in \Omega \text{ is real} \\ \psi(D_{\mathfrak{p}}) & : \psi \text{ is nonramified and } F \text{ ramified at } \mathfrak{p} \\ \frac{1}{\mathfrak{N}_{F/\mathbb{Q}}\mathfrak{f}} \sum_{a \in \mathcal{O}_{F_{\mathfrak{p}}}/\mathfrak{f}_{\mathfrak{p}}} \psi_{\mathfrak{p}}(a) e^{2\pi i \cdot \mathrm{tr}(a/d)} & : \psi \text{ is ramified at } \mathfrak{p} \end{cases}$$

where $\mathfrak{D}_{\mathfrak{p}}$ is the different ideal of $F_{\mathfrak{p}}/\mathbb{Q}_p$ and $(d) = \mathfrak{D}_{\mathfrak{p}}\mathfrak{f}_{\mathfrak{p}}$, and where the trace is understood as a class $\mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow \mathbb{Q}/\mathbb{Z}$, so $e^{2\pi i \cdot \mathrm{tr}(a/d)}$ is well-defined. The last case above is a Gauss sum over the local character $\psi_{\mathfrak{p}}$ of ψ_E at $\mathfrak{p}$. □

Theorem 7.3.2. *Let E be an elliptic curve defined over F with complex multiplication by $K \subseteq F$. Let ψ_E be the Hecke character associated to E. Then*

$$L(E, s) = L(\psi_E, s) \cdot L(\overline{\psi}_E, s).$$

Proof. We will show that the factors at each prime of F of both functions are equal. Recall that E has potential good reduction everywhere, since its j-invariant is integral. Therefore, it cannot have multiplicative reduction at any prime.

For any prime $\mathfrak{p}$ at which E has good reduction, the Euler factor of $L(E,s)$ is $1 - a_{\mathfrak{p}}q^{-s} + q^{1-2s}$. By lemma 4.4.3,

$$\psi_E(\mathfrak{p})\overline{\psi_E(\mathfrak{p})} = N_{K/\mathbb{Q}}(\psi_E(\mathfrak{p})) = \mathfrak{N}_{K/\mathbb{Q}}N_{F/K}(\mathfrak{p}) = q.$$

Also,

$$\#\tilde{E}(\mathcal{O}_K/\mathfrak{p}) = \deg(1-\varphi_{\mathfrak{p}}) = \deg(1-\psi_E(\mathfrak{p})),$$

since $\psi_E(\mathfrak{p})$ reduces to the Frobenius morphism on $\mathcal{O}_K/\mathfrak{p}$. Finally, it follows that

$$a_{\mathfrak{p}} = q + 1 - \#\tilde{E}(\mathcal{O}_K/\mathfrak{p}) = q + 1 - (1-\psi_E(\mathfrak{p}))(1-\overline{\psi_E(\mathfrak{p})}) = \psi_E(\mathfrak{p}) + \overline{\psi_E(\mathfrak{p})}.$$

Therefore,

$$1 - a_{\mathfrak{p}} + q^{1-2s} = (1-\psi_E(\mathfrak{p})q^s)(1-\overline{\psi_E(\mathfrak{p})}q^s).$$

If E has bad (and therefore, additive) reduction at $\mathfrak{p}$, the Euler factor of $L(E,s)$ is 1. Also, ψ_E must be ramified at $\mathfrak{p}$, so the Euler factors of $L(\psi_E,s)$ and $L(\overline{\psi_E},s)$ at $\mathfrak{p}$ are both 1. □

Combining this with the functional equation for Hecke L-series,

Corollary 7.3.3. *Let E/F be an elliptic curve with complex multiplication by $K \subseteq F$. Then $L(E,s)$ has an analytic continuation to all of $\mathbb{C}$, and satisfies the functional equation*

$$\Lambda(E,s) = \epsilon\Lambda(E,2-s),$$

where

$$\Lambda(E,s) = (\mathfrak{N}_{F/\mathbb{Q}}(\mathfrak{f}) \cdot |\Delta_F|)^s(2\pi)^{-s[F:\mathbb{Q}]}\Gamma(s)^{[F:\mathbb{Q}]}L(E,s)$$

and $\mathfrak{f}$ is the conductor of ψ_E; and $\epsilon \in \{\pm 1\}$.

Proof. ψ_E and $\overline{\psi_E}$ are Hecke characters with the same conductor $\mathfrak{f}$, where F has no real embeddings and $[F:\mathbb{Q}]/2$ complex embeddings. Consider also that because, for ideals $\mathfrak{a}$ coprime to $\mathfrak{f}$,

$$\psi_E(\mathfrak{a})\overline{\psi_E}(\mathfrak{a}) = N_{K/\mathbb{Q}}\psi_E(\mathfrak{a}) = \mathfrak{N}_{F/\mathbb{Q}}(\mathfrak{a}),$$

it follows that $\overline{\psi_E} = \psi_E^{-1} \cdot \mathfrak{N}_{F/\mathbb{Q}}$; so for $\mathfrak{Re}(s)$ appropriately large,

$$L(\overline{\psi_E},s) = \sum_{\mathfrak{a}} \frac{\overline{\psi_E}(\mathfrak{a})}{\mathfrak{N}_{F/\mathbb{Q}}(\mathfrak{a})^s} = \sum_{\mathfrak{a}} \frac{\psi_E^{-1}(\mathfrak{a})}{\mathfrak{N}_{F/\mathbb{Q}}(\mathfrak{a})^{s-1}} = L(\psi_E^{-1}, s-1).$$

Therefore,

$$\Lambda(E,s) = (\mathfrak{N}_{F/\mathbb{Q}}(\mathfrak{f}) \cdot |\Delta_F|)^s(2\pi)^{-s[F:\mathbb{Q}]}\Gamma(s)^{[F:\mathbb{Q}]}L(\psi_E,s)L(\psi_E^{-1},s-1)$$

$$= \Lambda(\psi_E, s)\Lambda(\psi_E^{-1}, s-1)(\mathfrak{N}_{F/\mathbb{Q}}(\mathfrak{f}) \cdot |\Delta_F|)^{1/2}(\frac{\Gamma(s)}{8\pi\Gamma(s-1)})^{\frac{1}{2}[F:\mathbb{Q}]}$$

$$= \underbrace{\varepsilon(\psi_E)\varepsilon(\psi_E^{-1})(-1)^{[F:\mathbb{Q}]/2}}_{=:\epsilon}\Lambda(\psi_E^{-1}, 1-s)\Lambda(\psi_E, 2-s)(\mathfrak{N}_{F/\mathbb{Q}}(\mathfrak{f}) \cdot |\Delta_F|)^{1/2}(\frac{\Gamma(2-s)}{8\pi\Gamma(1-s)})^{[F:\mathbb{Q}]/2}$$

$$= \epsilon L(\psi_E, 2-s)L(\psi_E^{-1}, 1-s)(\mathfrak{N}_{F/\mathbb{Q}}(\mathfrak{f}) \cdot |\Delta_F|)^{2-s}(2\pi)^{(2-s)[F:\mathbb{Q}]}\Gamma(2-s)^{[F:\mathbb{Q}]}$$

$$= \epsilon\Lambda(E, 2-s),$$

where $\epsilon = (-1)^{[F:\mathbb{Q}]/2}\prod_{\mathfrak{p}}(\varepsilon_{\mathfrak{p}}(\psi)\varepsilon_{\mathfrak{p}}(\psi^{-1}))$ is an element of norm 1 and may be seen to be invariant under complex conjugation; therefore $\epsilon \in \{\pm 1\}$ as claimed.

□

Chapter 8

p-adic interpolation

Let p be a rational prime. We may consider a sequence of p-adic numbers $(f_n)_{n\in\mathbb{Z}}$ as a function $f : \mathbb{Z} \to \mathbb{Q}_p$, and ask whether it can be extended to a continuous p-adic function $f' : \mathbb{Z}_p \to \mathbb{Q}_p$; this is called **$p$-adic interpolation**. It is not difficult to give conditions for the existence and uniqueness of such a function:

Theorem 8.0.1. *Let $f : \mathbb{Z} \to \mathbb{Q}_p$ be a function. f extends to a continuous function*

$$f' : \mathbb{Z}_p \to \mathbb{Q}_p$$

if and only if f is bounded and uniformly continuous; that is,

$$\forall \varepsilon > 0\ \exists \delta > 0\ \forall x, y \in \mathbb{Z} : \quad |x - y|_p < \delta \Rightarrow |f(x) - f(y)|_p < \varepsilon,$$

or equivalently,

$$\forall a \in \mathbb{N}\ \exists b \in \mathbb{N}\ \forall x, y \in \mathbb{Z} : \quad x \equiv y \pmod{p^b} \Rightarrow f(x) \equiv f(y) \pmod{p^a}.$$

In this case, the extension f' is unique.

Proof. The uniqueness follows immediately from the fact that $\mathbb{Z}$ is a dense subset of $\mathbb{Z}_p$.
It is clear that the conditions are necessary: if the continuous function f' is given, then its restriction to the compact subset $\mathbb{Z}$ must be bounded and uniformly continuous. On the other hand, if f is bounded and uniformly continuous, we can form the function

$$f' : \mathbb{Z}_p \to \mathbb{Q}_p, \quad x = \lim_{k\to\infty} x_k \mapsto \lim_{k\to\infty} a(x_k),$$

where (x_k) is a Cauchy sequence in $\mathbb{Z}$ with limit $x \in \mathbb{Z}_p$ - the definition of f' is independent of which x_k are used, and this gives a continuous function which restricts to f. □

In fact, it is enough to specify values f_n for $n \in \mathbb{N}$, as $\mathbb{N}$ by itself is dense in $\mathbb{Z}$ and so the argument still holds.

Uniform p-adic continuity may be extremely difficult to check. In practice, p-adic interpolation is more interesting in the other direction; it is often feasible to construct a continuous interpolating p-adic function by other, algebraic means and use its existence to prove the p-adic uniform continuity and boundedness of the given function f.

8.1 p-adic measures

Let $C(\mathbb{Z}_p, \mathbb{Q}_p)$ be the $\mathbb{Q}_p$-Banach space of continuous functions from $\mathbb{Z}_p$ to $\mathbb{Q}_p$ together with the supremum norm.
A **p-adic measure** μ on $\mathbb{Z}_p$ is a continuous linear map

$$\mu : C(\mathbb{Z}_p, \mathbb{Q}_p) \to \mathbb{Q}_p.$$

Instead of $\mu(f)$ we will also write $\int_{\mathbb{Z}_p} f(x) d\mu(x)$, and call $\mu(f)$ the integral of f with respect to μ. This notation may be motivated by the following analogy to Riemann sums:

$$\mu(f) = \lim_{n\to\infty} \sum_{k=0}^{p^n-1} f(k)\mu(\mathcal{I}_{k+p^n\mathbb{Z}_p}),$$

where $\mathcal{I}_{k+p^n\mathbb{Z}_p} = 1$ on $k + p^n\mathbb{Z}_p$ and 0 otherwise is the indicator function.

Since any open ball $U \subseteq \mathbb{Z}_p$ is also closed, the indicator function $\mathcal{I}_U$ is continuous; thus we may define the integrals

$$\int_U f(x)d\mu(x) := \mu(f \cdot \mathcal{I}_U).$$

We will denote the space of p-adic measures by $M(\mathbb{Z}_p, \mathbb{Q}_p)$. $M(\mathbb{Z}_p, \mathbb{Q}_p)$ is a normed space with respect to the operator norm

$$\|\mu\| := \sup\{\frac{|\mu(f)|_p}{\|f\|} : f \neq 0\}.$$

The following important result of p-adic analysis is very well known:

Theorem 8.1.1 (Mahler expansion). *Any continuous function $f \in C(\mathbb{Z}_p, \mathbb{Q}_p)$ is represented by an everywhere convergent Newton series*

$$f(x) = \sum_{n=0}^{\infty} f_n \binom{x}{n},$$

where $\binom{x}{n} = \frac{x(x-1)\dots(x-n+1)}{n!}$. The coefficients are unique and given by the formula

$$f_n = \sum_{k=0}^{n} f(k)\binom{n}{k}(-1)^{n-k} \in \mathbb{Q}_p.$$

Additionally, $(f_n)_n$ is a null sequence ($f_n \to 0$), and $\|f\|_\infty = \sup|f_n|$.

On the other hand, it is not difficult to see that, given any null sequence of coefficients f_n, the sum

$$f(x) := \sum_{n=0}^{\infty} f_n \binom{x}{n}$$

converges on $\mathbb{Z}_p$ and defines a continuous function - this is because the functions $\binom{x}{n}$ map $\mathbb{Z}$ to $\mathbb{Z}$ and by density and continuity $\mathbb{Z}_p$ to $\mathbb{Z}_p$, so have norm at most 1.

Definition 55. The **Mahler transform** (or **Amice transform**) of a measure μ is given by the formal power series

$$\mathcal{M}(\mu) := \sum_{n=0}^{\infty} \Big(\int_{\mathbb{Z}_p} \binom{x}{n} d\mu(x) \Big) T^n \in \mathbb{Q}_p[|T|].$$

Let $\mathbb{Q}_p[|T|]^b$ be the subspace of $\mathbb{Q}_p[|T|]$ of formal power series with bounded coefficients, together with the norm

$$\| \sum_{n=0}^{\infty} a_n T^n \|_\infty := \sup a_n.$$

Theorem 8.1.2. *$\mathcal{M} : M(\mathbb{Z}_p, \mathbb{Q}_p) \to \mathbb{Q}_p[|T|]^b$ is an isometric isomorphism of normed $\mathbb{Q}_p$-vector spaces.*

Proof. It is clear that $\mathcal{M}$ is a linear map.

Surjectivity: let $\sum_{n=0}^{\infty} a_n T^n \in \mathbb{Q}_p[|T|]^b$. Define the measure

$$\mu(f) := \sum_{n=0}^{\infty} a_n f_n,$$

where $f = \sum_{n=0}^{\infty} f_n \binom{x}{n}$ is the Mahler series expansion of f. (Recall that (f_n), and so also $(a_n f_n)$ tends to zero.) It follows that

$$\mathcal{M}(\mu) = \sum_{n=0}^{\infty} \mu(\binom{x}{n}) T^n = \sum_{n=0}^{\infty} \Big(\sum_{k=0}^{\infty} \delta_{nk} a_k \Big) T^n = \sum_{n=0}^{\infty} a_n T^n,$$

noting that the k-th coefficient of the Mahler series for $\binom{x}{n}$ is δ_{nk}.

For isometry (and in particular, injectivity), note that $\|\binom{x}{n}\| = 1$, because the function $\binom{x}{n}$ maps $\mathbb{Z}$ to $\mathbb{Z}$ and by continuity $\mathbb{Z}_p$ to $\mathbb{Z}_p$. Given any measure $\mu \in M(\mathbb{Z}_p, \mathbb{Q}_p)$ with $\mathcal{M}(\mu) = \sum_{n=0}^{\infty} a_n T^n$, we then have

$$|a_n|_p = |\mu(\binom{x}{n})|_p \leq \|\mu\| \| \binom{x}{n} \| = \|\mu\|.$$

This implies $\|\mathcal{M}(\mu)\|_\infty \leq \|\mu\|$.

On the other hand, for any $f = \sum_{n=0}^{\infty} f_n \binom{x}{n} \in C(\mathbb{Z}_p, \mathbb{Q}_p)$,

$$\begin{aligned}
\|\mathcal{M}(\mu)\|_\infty \|f\|_\infty &= (\sup_{n\in\mathbb{N}} |\int_{\mathbb{Z}_p} \binom{x}{n} d\mu(x)|_p) \cdot (\sup_{n\in\mathbb{N}} |f_n|_p) \\
&\geq \sup_{n\in\mathbb{N}} |\int_{\mathbb{Z}_p} f_n \binom{x}{n} d\mu(x)|_p \\
&\geq |\sum_{n=0}^{\infty} \int_{\mathbb{Z}_p} f_n \binom{x}{n} d\mu(x)|_p = |\sum_{n=0}^{\infty} \mu(f_n \binom{x}{n})|_p = |\mu(f)|_p.
\end{aligned}$$

It follows that

$$\|\mathcal{M}(\mu)\|_\infty \geq \sup\{\frac{|\mu(f)|_p}{\|f\|_\infty} : f \neq 0\} = \|\mu\|.$$

□

8.2 The p-adic zeta function

The p-adic zeta function plays an important role in the theory of cyclotomic fields (for example, its study leads to a proof of Fermat's last theorem for regular primes). In this section, we will give an analytic construction of it due to Kubota and Leopoldt. For us, this will be useful to motivate p-adic interpolation of L-functions attached to elliptic curves and to demonstrate the pattern of construction we will follow there as well.

Define, via the Maclaurin series

$$\frac{z}{e^z - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} z^n,$$

the **Bernoulli numbers** B_n. These satisfy $B_0 = 1$ and the recurrence equation

$$B_n = \delta_{0n} - \sum_{k=0}^{n-1} \binom{n}{k} \frac{B_k}{n-k+1},$$

hence are rational.

We will p-adically interpolate the fractions $(-1)^{n+1}\frac{B_n}{n}$, $n \geq 1$. The resulting function is called the **p-adic zeta function**, because it takes the same special values as the Riemann zeta function: for any integer $k \geq 0$,

$$\zeta(-k) = (-1)^k \frac{B_{k+1}}{k+1}.$$

First, for $x \in \mathbb{Z}_p^\times$, we have $x^{-1}\binom{x}{n} \in \mathbb{Z}_p$ for all $n \in \mathbb{N}$, so it follows that

$$\frac{x}{(1+T)^x - 1} - \frac{1}{T} = (1 + \sum_{n=2}^{\infty} x^{-1} \binom{x}{n} T^{n-1})^{-1} \cdot (\sum_{n=2}^{\infty} x^{-1} \binom{x}{n} T^{n-2}) \in \mathbb{Z}_p[|T|] \subseteq \mathbb{Q}_p[|T|]^b.$$

Here, $(1+T)^x := \sum_{n=0}^{\infty} \binom{x}{n} T^n$.

By our previous results, we find a measure $\mu_x \in M(\mathbb{Z}_p, \mathbb{Q}_p)$ that satisfies

$$\mathcal{M}(\mu_x) = \frac{1}{T} - \frac{x}{(1+T)^x - 1}.$$

Theorem 8.2.1. *The moments of μ_x are given by $(-1)^n(1-x^{n+1})\zeta(-n)$; i.e.*

$$\int_{\mathbb{Z}_p} y^n d\mu_x(y) = (-1)^n(1-x^{n+1})\zeta(-n).$$

Proof. Consider for $x \in \mathbb{N}$ the function

$$f_a(z) := \frac{1}{e^z - 1} - \frac{x}{e^{xz} - 1}.$$

A Taylor series expansion gives

$$f_x(z) = \sum_{n=0}^{\infty} \frac{B_{n+1}}{(n+1)!}(1-x^{n+1})z^n,$$

so

$$\frac{d^n}{dz^n} f_x(z)|_{z=0} = \frac{B_{n+1}}{n+1}(1-x^{n+1}) = (-1)^n(1-x^{n+1})\zeta(-n).$$

Being an equality of polynomials in the variable x, and because $\mathbb{N} \subseteq \mathbb{Z}_p$ is dense, this is generally true for $x \in \mathbb{Z}_p$.

The lemma below will give us, with $D = (1+T)\frac{d}{dT}$,

$$\int_{\mathbb{Z}_p} y^n d\mu_x(y) = D^n(\frac{1}{T} - \frac{x}{(1+T)^x - 1})|_{T=0}$$

$$= \frac{d^n}{dz^n} f_x(z)|_{z=0} = (-1)^n(1-x^{n+1})\zeta(-n),$$

by formally substituting $z = \log(1+T)$ and $D = e^z(\frac{dT}{dz})^{-1}\frac{d}{dz} = \frac{d}{dz}$.

□

Lemma 8.2.2. *For any p-adic measure μ and integer $k \geq 0$,*

$$\int_{\mathbb{Z}_p} x^k d\mu = D^k \mathcal{M}(\mu)(T)|_{T=0},$$

with the differential operator $D := (1+T)\frac{d}{dT}$.

Proof. Define $\lambda : C(\mathbb{Z}_p, \mathbb{Q}_p) \to \mathbb{Q}_p$ via $\lambda(f) := \mu(x \cdot f(x))$. Then λ is continuous (indeed, we have $\|\lambda\| \leq \|\mu\|$) and we calculate:

$$\mathcal{M}(\lambda) = \sum_{n=0}^{\infty} \Big(\int_{\mathbb{Z}_p} x \binom{x}{n} d\mu(x) \Big) T^n = \sum_{n=0}^{\infty} \Big(\int_{\mathbb{Z}_p} (n+1)\binom{x}{n+1} + n\binom{x}{n} d\mu(x) \Big) T^n$$

$$= (1+T)\sum_{n=0}^{\infty}\frac{d}{dT}\Big(\int_{\mathbb{Z}_p}\binom{x}{n}d\mu(x)\Big)T^n = D\mathcal{M}(\mu).$$

The result follows from induction on k: assuming

$$D^k\mathcal{M}(\mu)(T)|_{T=0} = \int_{\mathbb{Z}_p} d\mathcal{M}^{-1}(D^k\mathcal{M}(\mu))(x) = \int_{\mathbb{Z}_p} x^k d\mu(x)$$

(which is clear for $k=0$) for arbitrary μ, it follows from the above that

$$\int_{\mathbb{Z}_p} x^{k+1}d\mu(x) = \int_{\mathbb{Z}_p} x^k d\lambda(x) = D^k\mathcal{M}(\lambda)(T)|_{T=0} = D^{k+1}\mathcal{M}(\mu)(T)|_{T=0}.$$

□

The existence of such a measure implies that certain special values of Riemann's zeta function are p-adically close. This result is due to Kubota and Leopoldt and extends a result of Kummer.

Theorem 8.2.3 (Kummer's congruences)**.** *Let $a \geq 0$ be an integer and*

$$h \equiv k \not\equiv 0(\text{mod} p^a(p-1))$$

be even natural numbers. Then

$$(1-p^{h-1})\frac{B_h}{h} \equiv (1-p^{k-1})\frac{B_k}{k}(\text{mod} p^{a+1}).$$

8.3 Multivariate interpolation

It is worth mentioning that the correspondence between p-adic measures and power series extends to the case of several variables. This relies on a multivariate Mahler's theorem:

Theorem 8.3.1. *Let W be a complete and separated $\mathbb{Z}_p$-algebra with respect to the p-adic topology, and let $r \geq 1$ be an integer. Any continuous function $f \in C(\mathbb{Z}_p^r, W)$ is represented by an everywhere convergent Newton series*

$$f(x_1,...,x_r) = \sum_{k_1=0}^{\infty}...\sum_{k_r=0}^{\infty} a_{\underline{k}}\binom{x_1}{k_1}...\binom{x_r}{k_r}.$$

The coefficients $a_{\underline{k}} \in W$ are unique and converge to zero as $|\underline{k}| = \sum_{i=1}^r k_i \to \infty$.

On the other hand, it is not difficult to see that, given a sequence of coefficients $a_{\underline{k}} \in W$ that tend to zero as $|\underline{k}| \to \infty$, the sum

$$f(x) := \sum_{k_1=1}^{\infty}...\sum_{k_r=1}^{\infty} a_{\underline{k}}\binom{x_1}{k_1}...\binom{x_r}{k_r}$$

is well-defined and gives a continuous function $f : \mathbb{Z}_p^r \to W$.

This leads us as before to define the **Mahler transform** of a measure $\mu : C(\mathbb{Z}_p^r, W) \to W$:

$$\mathcal{M}(\mu) := \sum_{k_1=0}^{\infty} ... \sum_{k_r=0}^{\infty} \Big(\int_{\mathbb{Z}_p^r} \binom{x_1}{k_1} ... \binom{x_r}{k_r} \mathrm{d}x_1 ... \mathrm{d}x_r \Big) T_1^{k_1} ... T_r^{k_r} \in W[|T_1, ..., T_r|].$$

The Mahler transform is bijective; its inverse is given as follows. If $\sum_{\underline{k}} a_{\underline{k}} \in W[|T_1, ..., T_r|]$ is a given power series, the corresponding measure μ with $\mathcal{M}(\mu) = \sum a_{\underline{k}}$ is given by

$$f(x_1, ..., x_r) = \sum_{\underline{k}} a_{\underline{k}} \binom{x_1}{k_1} ... \binom{x_r}{k_r} \implies \mu(f) = \sum_{\underline{k}} a_{\underline{k}} f_{\underline{k}}.$$

Of course, μ may also be described by its moments - that is, the value it takes on the monomial $\underline{x}^{\underline{k}} = x_1^{k_1} ... x_r^{k_r}$. This is given by

$$\int_{\mathbb{Z}_p^r} \underline{x}^{\underline{k}} \mathrm{d}\mu = [(1 + x_1) \frac{\partial}{\partial x_1}]^{k_1} ... [(1 + x_r) \frac{\partial}{\partial x_r}]^{k_r} f|_{x=0},$$

after an calculation analogous to 8.2.3.

Chapter 9

Damerell's theorem

Before attempting to construct a p-adic analogue of the L-function attached to an elliptic curve, it is important to meaningfully interpret its values as p-adic numbers. As a matter of fact, the values of $L(z; E)$ at integers are regularly behaved, and up to a power of π and of the fundamental period of E, even algebraic. This result is due to Damerell [3] and its proof is much more involved than the analogous result for the Riemann ζ-function. Our proof is based on Weil's book [22].

9.1 The Hecke L-series and Eisenstein sums

We consider again the L-function $L(\psi_E, s)$ of the Hecke character ψ_E associated to some elliptic curve E, defined over a number field F, with complex multiplication by the quadratic imaginary field K.

Lemma 9.1.1. *There exists a Hecke character $\varphi : I_K \to \mathbb{C}^\times$ of K satisfying*

$$\psi_E = \varphi \circ N_{F/K}.$$

Proof. This is essentially by construction: if $N_{F/K}(x) = y$, then $\psi_E(x) = y_\infty^{-1} z$ depends only on y. Therefore, for general $y \in \mathfrak{I}_K \subseteq I_F$, we can set $\varphi(y) := \psi(y)$. □

It follows that

$$L(\psi_E, s) = \prod_{\mathfrak{p}} \frac{1}{1 - \psi_E(\mathfrak{p})\mathfrak{N}_{F/\mathbb{Q}}(\mathfrak{p})^{-s}} = \prod_{\mathfrak{p}} \frac{1}{1 - \varphi(N_{F/K}\mathfrak{p})\mathfrak{N}_{K/\mathbb{Q}}(N_{F/K}\mathfrak{p})^{-s}}.$$

Proposition 9.1.2. *Assume that F/K is abelian. Then*

$$L(\psi, s) = \prod_{\chi \in \mathrm{Gal}(F/K)^\vee} L(\chi\varphi, s).$$

Proof. This requires some explanation. First, if $\mathfrak{f}$ is the conductor of F/K, recall that Artin reciprocity gives an isomorphism

$$\mathrm{Gal}(F/K) \cong I_K^{\mathfrak{f}}/K_{\mathfrak{f}} N_{F/K} I_F^{\mathfrak{f}},$$

and this allows us to view characters χ of the Galois group as Hecke characters of K; a character

$$\chi : \mathrm{Gal}(L/K) \to \mathbb{C}^\times$$

corresponds to the Hecke character

$$\psi_\chi : I_K \to \mathbb{C}^\times, \;\; s \mapsto \chi((s, L/K)).$$

As a character of ideals, this means $\psi_\chi(\mathfrak{p}) = \chi(\mathrm{Frob}_{\mathfrak{p}})$.

Now we consider the L-factor at primes $\mathfrak{P}$ of F, lying over the prime $\mathfrak{p}$ of K. We need only consider primes $\mathfrak{p}$ at which φ is unramified (and therefore ψ at $\mathfrak{P}$), because the L-factors will be trivial otherwise. Let $f = f(\mathfrak{P}/\mathfrak{p})$ be the relative degree; that is, $f = [F_{\mathfrak{P}} : K_{\mathfrak{p}}]$, and let $r = [L : K]/f$ be the number of primes lying above $\mathfrak{p}$. Then

$$\prod_{\mathfrak{P}|\mathfrak{p}} \frac{1}{1 - \psi(\mathfrak{P})\mathfrak{N}_{F/\mathbb{Q}}(\mathfrak{P})^{-s}} = \prod_{\mathfrak{P}|\mathfrak{p}} \frac{1}{1 - \varphi(\mathfrak{p})^f \mathfrak{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-sf}} = \frac{1}{(1 - \varphi(\mathfrak{p})^f \mathfrak{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-sf})^r}$$

$$= \prod_{\zeta^f = 1} \frac{1}{(1 - \zeta\varphi(\mathfrak{p})\mathfrak{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-s})^r}$$

$$= \prod_{\chi \in \mathrm{Gal}(F_{\mathfrak{P}}/K_{\mathfrak{p}})^\vee} \frac{1}{(1 - \varphi_\chi(\mathfrak{p})\varphi(\mathfrak{p}\mathfrak{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-s})^r},$$

for any $\mathfrak{P}$ lying over $\mathfrak{p}$, since the Galois group $\mathrm{Gal}(F_{\mathfrak{P}}/K_{\mathfrak{p}})$ is cyclic of order f. There are exactly r ways to lift any character χ to a character of the Galois group $\mathrm{Gal}(F/K)$, and so

$$... = \prod_{\chi \in \mathrm{Gal}(F/K)^\vee} \frac{1}{1 - \varphi_\chi(\mathfrak{p})\varphi(\mathfrak{p})\mathfrak{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-s}}.$$

Combining all the factors, we see

$$L(\psi, s) = \prod_{\chi \in \mathrm{Gal}(F/K)^\vee} L(\varphi_\chi \varphi, s) =: \prod_{\chi \in \mathrm{Gal}(F/K)^\vee} L(\chi\varphi, s).$$

□

In this way, at least in the case that E is defined over an abelian extension of K, we are reduced to considering Hecke characters defined over K itself.

Now let $L(\varphi, s)$ be a Hecke L-function for some Hecke character φ of K. Then $L(\varphi, s)$ is a linear combination

$$L(\varphi, s) = \sum_{\mathfrak{a} \neq 0} \frac{\varphi(\mathfrak{a})}{\mathfrak{N}_{K/\mathbb{Q}}(\mathfrak{a})^s} = \frac{1}{|\mathcal{O}_K^\times|} \sum_{j=1}^{h} \frac{\varphi(\mathfrak{a}_j)}{\mathfrak{N}_{K/\mathbb{Q}}(\mathfrak{a}_j)} \sum_{\alpha \in \mathcal{O}_K} \frac{\varphi((\alpha))}{N_{K/\mathbb{Q}}(\alpha)^s}$$

$$= \sum_{j=1}^{h} \frac{\varphi(\mathfrak{a}_j)}{\mathfrak{N}_{K/\mathbb{Q}}(\mathfrak{a}_j)} \sum_{x_i \in \mathcal{O}_K^\times / 1+\mathfrak{f}} \sum_{\alpha \in 1+\mathfrak{f}} \frac{\overline{\alpha}^a}{\alpha^b}$$

where h is the class number of K, $\mathfrak{a}_1$,...,$\mathfrak{a}_h$ represent the ideal class group, $\mathfrak{f}$ is the conductor of φ and a, b are integers that depend on φ.

Given any integer $k \geq 3$ where the first L-function $L(E, s)$ converges, the above motivates that arithmetic information (algebraicity, p-adic properties, and so on) about $L(E, k)$ can be derived from considering the Eisenstein sums

$$G_{k,r}(\mathcal{O}_K) := \sum_{\alpha \neq 0} \frac{\overline{\alpha}^r}{\alpha^{k+r}}, \quad r \geq 0.$$

These sums have also attracted interest on their own. Surprisingly, up to an easily controlled factor, these are algebraic numbers - this is a result due to Damerell.

9.2 Eisenstein functions

Definition 56 (Eisenstein trigonometric functions)**.** For $z \in \mathbb{C}$ and $k \geq 1$ define the series

$$e_k(z) := \lim_{M \to \infty} \sum_{m=-M}^{m} (z+m)^{-k}.$$

If $k \geq 2$, this series converges absolutely and uniformly on compact sets, and therefore defines a periodic, meromorphic function on $\mathbb{C}$ with poles in $\mathbb{Z}$ which may be differentiated by terms. $e_1(z)$ is also periodic, meromorphic and differentiable by terms (although the series does not converge uniformly); indeed, e_1 is the well-known partial fractions decomposition of the cotangent

$$e_1(z) = \pi \cot(\pi z),$$

and the function obtained by termwise differentiation is its actual derivative

$$-e_2(z) = -\frac{\pi^2}{\sin^2 \pi z}.$$

For this reason, the functions e_k will be referred to as trigonometric functions.

For the rest of this section, we will assume that ω_1 and ω_2 are complex variables whose domain is restricted in such a way that ω_1 and ω_2 define a lattice, and that $\frac{\omega_2}{\omega_1} = \tau$ has positive imaginary part.

Definition 57 (Eisenstein elliptic functions)**.** For $z \in \mathbb{C}$ and $k \geq 1$ define

$$E_k(z;\omega_1,\omega_2) := \lim_{M\to\infty} \sum_{m=-M}^{M} \Big(\lim_{N\to\infty} \sum_{n=-N}^{N} (z+m\omega_1+n\omega_2)^{-k} \Big).$$

If $k \geq 3$, this series above converges absolutely and uniformly on compact sets, and is the same as the E_k which was defined in Chapter 2. We previously found the Laurent series

$$E_k(z;\omega_1,\omega_2) = \frac{1}{z^k}\Big(1+(-1)^k \sum_{j=1}^{\infty} \binom{2j-1}{k-1} G_{2j}(\omega_1,\omega_2) z^{2j}\Big);$$

here G_{2j} is the Eisenstein series

$$G_{2j}(\omega_1,\omega_2) = \sum_{(m,n)\neq(0,0)} (m\omega_1+n\omega_2)^{-2j}, \;\; j \geq 2,$$

and the value of G_2 is unimportant, because $\binom{1}{k-1}$ is zero for $k \geq 3$. With some additional care for the limit processes involved, one can also derive the analogous identities

$$E_1(z;\omega_1,\omega_2) = \frac{1}{z}\Big(1 - \sum_{j=1}^{\infty} G_{2j}(\omega_1,\omega_2) z^{2j}\Big)$$

and

$$E_2(z;\omega_1,\omega_2) = \frac{1}{z^2}\Big(1 + \sum_{j=1}^{\infty} (2j-1) G_{2j}(\omega_1,\omega_2) z^{2j}\Big),$$

if

$$G_2(\omega_1,\omega_2) := \lim_{M\to\infty} \sum_{m=-M}^{M} \Big(\lim_{N\to\infty} \sum_{\substack{n=-N \\ (m,n)\neq(0,0)}}^{N} (m\omega_1+n\omega_2)^{-2} \Big).$$

In particular, we have

$$E_2(z) = \wp(z) + G_2.$$

Most importantly, E_k is doubly periodic for $k \geq 2$. This is not true for E_1. Since we can write

$$E_1(z) = \frac{1}{\omega_1}\Big(e_1(\frac{z}{\omega_1}) + \sum_{n=1}^{\infty}\Big(e_1(\frac{x+n\omega_2}{\omega_1}) + e_1(\frac{x-n\omega_2}{\omega_1})\Big)\Big),$$

it is clear that E_1, with e_1, is periodic with respect to ω_1. However, we have

$$E_1(z+\omega_2) - E_1(z) = \lim_{N\to\infty} \frac{1}{u}\Big(e_1(\frac{z+(N+1)\omega_2}{\omega_1}) - e_1(\frac{z-N\omega_2}{\omega_1})\Big)$$

$$= \frac{\pi}{u} \lim_{N\to\infty} \Big(\cot\frac{\pi z + (N+1)\pi\omega_2}{\omega_1} + \cot\frac{\pi z - N\pi\omega_2}{\omega_1} \Big) = \frac{2\pi i}{u}.$$

To work around this, we define $E_1^*(z) := E_1(z) + \frac{\pi\overline{u}}{Au} z - \frac{\pi\overline{z}}{A}$, where

$$A = \frac{1}{2i}(v\overline{u} - u\overline{v})$$

is the area of the complex parallelogram with sides u and v; it follows that $E_1^*(z)$ is doubly periodic and real-analytic, although no longer holomorphic. We note that this function appears in Damerell's paper [3] under the name $h(z)$.

Lemma 9.2.1. *The following trigonometric formula holds for $x, y \in \mathbb{C}$:*

$$e_2(x)e_2(y) - (e_2(x) + e_2(y))e_2(x+y) = 2e_3(x+y)(e_1(x) + e_1(y)).$$

Proof. The following identity of rational functions is easily verified:

$$\frac{1}{p^2q^2} = \frac{1}{(p+q)^2}\Big(\frac{1}{p^2} + \frac{1}{q^2}\Big) + \frac{2}{(p+q)^3}\Big(\frac{1}{p} + \frac{1}{q}\Big).$$

After substituting $p = x + m$ and $q = y + n - m$ and taking the appropriate sum,

$$\lim_{M\to\infty} \sum_{m=-M}^{M} \Big((x+m)^{-2}(y+n-m)^{-2} - (x+m)^{-2}(x+y+n)^{-2} - (y+n-m)^{-2}(x+y+n)^{-2}\Big)$$

$$= \frac{2}{(x+y+n)^3}\Big(e_1(x) + e_1(y+n)\Big) = \frac{2}{(x+y+n)^3}\Big(e_1(x) + e_1(y)\Big).$$

Both sides are absolutely convergent with respect to n, and summing over both for $n = -\infty$ to ∞ gives

$$e_2(x)e_2(y) - e_2(x)e_2(x+y) - e_2(y)e_2(x+y) = 2e_3(x+y)\Big(e_1(x) + e_1(y)\Big)$$

as claimed. □

Theorem 9.2.2 (Eisenstein differential equation)**.** *The following differential equation holds:*

$$\frac{2\pi i}{u}\frac{\partial E_1}{\partial \omega_2} = E_3 - E_1E_2.$$

Proof. Summing over the identity in the previous lemma gives

$$u^4\Big(E_2(z)E_2(w) - (E_2(z) + E_2(w))E_2(z+w)\Big)$$

$$= 2u^4E_3(z+w)\Big(E_1(z) + E_1(w)\Big) - 2\sum_{m=-\infty}^{\infty} \frac{2\pi i m}{u} e_3(\frac{z+w+m\omega_2}{\omega_1}),$$

and because of absolute convergence we may substitute

$$\frac{\partial}{\partial \omega_2}\sum_{m=-\infty}^{\infty} e_2(\frac{z+w+m\omega_2}{\omega_1}) = -2\sum_{m=-\infty}^{\infty} me_3(\frac{z+w+m\omega_2}{\omega_1}).$$

We then have

$$E_2(z)E_2(w) - \Big(E_2(z) + E_2(w)\Big)E_2(z+w) = 2E_3(z+w)\Big(E_1(z) + E_1(w)\Big) + \frac{2\pi i}{u}\frac{\partial E_2}{\partial \omega_2}(z+w).$$

For a fixed $w \notin \Lambda$, we use the Maclaurin series

$$E_k(z+w) = \sum_{j=0}^{\infty} \binom{j+k-1}{j} (-1)^j E_{j+k}(w) z^j$$

(which is derived from $E_k'(w) = -kE_{k+1}(w)$ for all k) to expand both sides of the equation as power series in z; the left-hand side is

$$\begin{aligned} &\Big(E_2(w)z^{-2} + E_2(w)G_2 + ...\Big) \\ -&\Big(z^{-2} + G_2 + E_2(w) + 3G_4 z^2 + ...\Big)\Big(E_2(w) - 2E_3(w)z + 3E_4(w)z^2\Big) \\ &= 2E_3(w)z^{-1} - (E_2(w)^2 + 3E_4(w))z^0 + ... \end{aligned}$$

and the right-hand side:

$$2\Big(E_3(w) - 3E_4(w)z + ...\Big)\Big(z^{-1} + E_1(w) - G_2 z + ...\Big) + \frac{2\pi i}{u}\Big(\frac{\partial E_2}{\partial \omega_2}(w) - 2\frac{\partial E_3}{\partial \omega_2}(w)z + ...\Big)$$

$$= 2E_3(w)z^{-1} + (2E_3(w)E_1(w) - 6E_4(w) + \frac{2\pi i}{u}\frac{\partial E_2}{\partial \omega_2}(w))z^0 + ...$$

Equating constant terms shows that

$$\frac{2\pi i}{u}\frac{\partial E_2}{\partial \omega_2}(w) = 3E_4(w) - 2E_1(w)E_3(w) - E_2(w)^2.$$

Integrating both sides of the above with respect to w, we see that

$$\frac{2\pi i}{u}\frac{\partial E_1}{\partial \omega_2}(w) = E_3(w) - E_1(w)E_2(w) + C$$

for some constant C; since both $\frac{2\pi i}{u}\frac{\partial E_1}{\partial \omega_2}(w)$ and $E_3(w) - E_1(w)E_2(w)$ are odd functions of w, we have $C = 0$. □

This may be translated into a differential equation relating Eisenstein series:

Corollary 9.2.3. *For any $k \geq 1$,*

$$\frac{2\pi i}{u}\frac{\partial G_{2k}(\omega_1, \omega_2)}{\partial \omega_2} = k(2k+3)G_{2k+2}(\omega_1, \omega_2) - k\sum_{j=1}^{k} G_{2j}(\omega_1, \omega_2)G_{2k-2j+2}(\omega_1, \omega_2).$$

9.3 Algebraicity results

Lemma 9.3.1. *Let Λ be a lattice generated by ω_1 and ω_2, and Λ' a linear transformation of Λ, generated by $a\omega_1 + b\omega_2$ and $c\omega_1 + d\omega_1$ with $a, b, c, d \in \mathbb{Z}$. Then for any $k \geq 2$,*

$$G_{2k}(\Lambda') \in \mathbb{Q}\Big(G_4(\Lambda), G_6(\Lambda)\Big).$$

Proof. Let $N := |ad - bc|$; then Λ' has index N in Λ, and $N\Lambda$ has index N in Λ'. Letting S be a set of representatives for $\Lambda'/N\Lambda$ containing 0, we have

$$G_{2k}(\Lambda') = \sum_{s\in S}\sum_{w\in\Lambda}(Nw+s)^{-2k} = N^{-2k}G_{2k}(\Lambda) + N^{-2k}\sum_{s\in S\setminus\{0\}} E_{2k}(\frac{s}{N},\Lambda).$$

Let R be a set of representatives for $\Lambda/N\Lambda$ containing S; we then have for any $j \geq 2$ that

$$\sum_{r\in R} E_j(\frac{z+r}{N},\Lambda) = \sum_{r\in R}\sum_{\omega\in\Lambda}(\frac{z+r+N\omega}{N})^{-j} = N^j\sum_{\omega\in\Lambda}(z+r)^{-j} = N^jE_j(z;\Lambda).$$

With $\wp(z) = E_2(z) - G_2$, since the number of terms in the sum is N^2, it also holds that

$$\sum_{r\in R}\wp(\frac{z+r}{N}) = N^2\wp(z).$$

Since any of the powers E_{2k}^n of E_{2k} can be expressed as a polynomial in E_j, $j \geq 3$ and in $\wp$, we see that $\sum_{r\in R} E_{2k}(\frac{z+r}{N},\Lambda)^n$ is a polynomial in E_j, $j \geq 3$ and $\wp$ as well. Using Newton's algorithm, this also holds for the symmetric polynomials in $E_j(\frac{z+r}{N},\Lambda)$; it follows that the functions $E_j(\frac{z+r}{N})$ and $\wp(\frac{z+r}{N})$ themselves are algebraic over $\mathbb{Q}(\wp(z,\Lambda), E_j(z,\Lambda),\ j \geq 3)$; since we have

$$\sum_{r\neq 0}\wp(\frac{r}{N}) = \sum_{r\neq 0}E_2(\frac{r}{N}) - \sum_{r\neq 0}G_2 = (N^2-1)G_2 - (N^2-1)G_2 = 0,$$

one derives that $E_{2k}(\frac{s}{N},\Lambda)$ is algebraic over $\mathbb{Q}(G_k,\ k \geq 3)$ for every $s \in S \subseteq R$, and by the recurrence formula for the Eisenstein series also algebraic over $\mathbb{Q}(G_4, G_6)$. □

Assume in the following that Λ is a lattice such that the elliptic curve $\mathbb{C}/\Lambda$ has complex multiplication by $\mathcal{O}_K$ for some imaginary quadratic number field K.

Lemma 9.3.2. *If $G_6(\Lambda) \neq 0$, then $G_4(\Lambda)^3G_6(\Lambda)^{-2}$ is algebraic over $\mathbb{Q}$.*

Proof. Let $\alpha \in \mathcal{O}_K$, $\alpha \notin \mathbb{Z}$. Since Λ has complex multiplication by $\mathcal{O}_K$, it follows that $\alpha\Lambda \subseteq \Lambda$; thus there exists an integral matrix such that

$$\begin{pmatrix}\alpha\omega_1 & \alpha\omega_2\end{pmatrix} = \begin{pmatrix}\omega_1 & \omega_2\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix},$$

ω_1 and ω_2 being generators of Λ as before.

We have $G_4(\alpha\Lambda) = \alpha^{-4}G_4(\Lambda)$ and $G_6(\alpha\Lambda) = \alpha^{-6}G_6(\Lambda)$. We also have that

$$f_4 := G_4(a\omega_1 + c\omega_2, b\omega_1 + d\omega_2) - \alpha^{-4}G_4(\omega_1,\omega_2) \not\equiv 0$$

as a function of ω_1 and ω_2 - since α is not an endomorphism of every linear transformation of Λ. Since the previous lemma shows that f_4 is always algebraic over $\mathbb{Q}(G_4(\Lambda), G_6(\Lambda))$, we can find a polynomial $F \neq 0$ with

$$F(f_4, G_4(\omega_1,\omega_2), G_6(\omega_1,\omega_2)) \equiv 0;$$

without loss of generality assuming that F is not a multiple of f_4, otherwise writing $F = f_4^m \cdot G$ and using continuity to show that $G(f_4, G_4(\omega_1, \omega_2), G_6(\omega_1, \omega_2)) \equiv 0$. Since our lattice Λ satisfies $f_4(\Lambda) = 0$, it follows that $F(0, G_4, G_6) = 0$ as a non-trivial relation. The homogeneity of G_4 and G_6 in ω_1 and ω_2 of respective degrees 4 and 6 imply, after distributing out of F, out, that $G_4^3 G_6^{-2}$ is algebraic over $\mathbb{Q}$. □

Let $\{1, \tau\}$ be a basis for $\mathcal{O}_K$ over $\mathbb{Z}$, where $\mathfrak{Im}[\tau] > 0$.

Theorem 9.3.3.

$$\Delta(\tau) := (60G_4(1,\tau))^3 - 27(140G_6(1,\tau))^2 = (2\pi q)^{12} \prod_{n=1}^{\infty} (1-q^n)^{24}$$

where $q := e^{2\pi i \tau}$.

Proof. This formula is well-known. □

Theorem 9.3.4. *Let* $\Omega := 2\pi |q|^{1/12} \prod_{n=1}^{\infty} (1-q^n)^2$. *Then* $G_4(\Omega \mathcal{O}_K)$ *and* $G_6(\Omega \mathcal{O}_K)$ *are algebraic over* $\mathbb{Q}$.

Proof. If $G_6(\mathcal{O}_K) = 0$ (as occurs in the case $K = \mathbb{Q}(i)$) we have

$$G_4(\Omega \mathcal{O}_K)^3 = (\frac{G_4(\mathcal{O}_K)}{\Omega^4})^3 = \frac{\Delta(\mathcal{O}_K)}{\pm 60^3 \Delta(\mathcal{O}_K)} = \pm \frac{1}{60^3}$$

and the claim is obvious.

Otherwise, we know that $G_4(\mathcal{O}_K)^3 G_6(\mathcal{O}_K)^{-2}$ is algebraic. It follows that

$$\Delta(\tau) = 60^3 G_4(\mathcal{O}_K)^3 - 27 \cdot 140^2 G_6(\mathcal{O}_K)^2 = G_4(\mathcal{O}_K)^3 \Big(60^3 - 27 \cdot 140^2 (G_4(\mathcal{O}_K)^3 G_6(\mathcal{O}_K)^{-2})^{-1}\Big)$$

$$= G_6(\mathcal{O}_K)^2 \Big(60^3 (G_4(\mathcal{O}_K)^3 G_6(\mathcal{O}_K)^{-2}) - 27 \cdot 140^2\Big).$$

Therefore

$$G_4(\Omega \mathcal{O}_K)^3 = \pm \frac{G_4(\mathcal{O}_K)^3}{\Delta(\tau)} = \pm \frac{1}{60^3 - 27 \cdot 140^2 (G_4(\mathcal{O}_K)^3 G_6(\mathcal{O}_K)^2)^{-1}}$$

and

$$G_6(\Omega \mathcal{O}_K)^2 = \pm \frac{G_6(\mathcal{O}_K^2)}{\Delta(\tau)} = \pm \frac{1}{60^3 G_4(\mathcal{O}_K)^3 G_6(\mathcal{O}_K)^{-2} - 27 \cdot 140^2},$$

which shows that both are algebraic. □

Definition 58. For $k \geq 3$ and $r \geq 0$ and a lattice Λ in $\mathbb{C}$, define

$$E_{k,r}(z, \Lambda) := \sum_{\omega \in \Lambda} \frac{(\overline{z+\omega})^r}{(z+w)^{k+r}}.$$

Also define $G_{k,r}(\Lambda)$ as the value of $E_{k,r}(z) - \overline{z}^r z^{-k-r}$ at $z = 0$.

Theorem 9.3.5. *For any imaginary quadratic number field K, letting A be the area of a fundamental parallelogram of the lattice $\mathcal{O}_K$ and $k \geq 3$, $r \geq 0$,*

$$B_{k,r} := \frac{(-1)^k (k+r-1)! \pi^r G_{k,r}(\mathcal{O}_K)}{2A^r \Omega^{k+2r}}$$

is algebraic over $\mathbb{Q}$; in fact, it lies in the number field $\mathbb{Q}\Big(G_4(\Omega\mathcal{O}_K), G_6(\Omega\mathcal{O}_K)\Big)$.

Proof. Fix a basis $\{1, \tau\}$, $\mathfrak{Im}[\tau] > 0$ of $\mathcal{O}_K$. We then have $A = \frac{\tau - \overline{\tau}}{2i}$. The series $E_{k,r}(z, \omega_1, \omega_2)$ is not holomorphic due to its dependence on $\overline{z}$, but may be understood as a real-analytic function in the $\mathbb{R}$-valued variables $z, \overline{z}, \omega_1, \overline{\omega_1}, \omega_2, \overline{\omega_2}$.

Define the differential operator

$$\mathcal{D} := \overline{z}\frac{\partial}{\partial z} + \overline{\omega_1}\frac{\partial}{\partial \omega_1} + \overline{\omega_2}\frac{\partial}{\partial \omega_2}.$$

Recalling the function $E_1^*(z)$ from earlier, we define inductively

$$E_k^*(z) := -\frac{1}{k}\frac{\partial E_{k-1}^*}{\partial z}(z),$$

so that $E_2^*(z) = E_2(z) - \frac{\pi}{A}$ and $E_k^*(z) = E_k(z)$ for any $k \geq 3$. Define $G_{k,r}^*$ to be the value of $E_{k,r}^*(z) - \overline{z}^r z^{-k-r}$ at $z = 0$, which then equals $G_{k,r}$ for $k \geq 3$.

By an inductive argument, we find

$$E_{k,r}(z, \omega_1, \omega_2) = \frac{(-1)^{k+r-1}}{(k+r-1)!}\mathcal{D}^r \frac{\partial^{k-1}}{\partial z^{k-1}} E_1(z).$$

It follows that

$$G_{k,r} = \frac{(-1)^r}{(k+r-1)(k+r-2)...(k)}\mathcal{D}^r G_k.$$

Applying the Eisenstein differential equation from above, we see that

$$G_{2k+1,1}^* = -\frac{1}{2k}\mathcal{D}G_{2k}^* = \frac{A}{\pi}\Big(\frac{2k+3}{2}G_{2k+2}^* - \frac{1}{2}\sum_{r=1}^{k} G_{2r}^* G_{2k-2r+2}^*\Big),$$

and by repeated application of $\mathcal{D}$ it follows that

$$G_{k,r}^* = \frac{A^r}{(2\pi)^r (k+r-1)(k+r-2)...(k)} P_{k,r}(G_2^*, G_4^*, G_6^*, ...G_{k+2r}^*)$$

where P is a polynomial with rational coefficients.

For $j \geq 4$, we know $G_j^* = G_j$ to be algebraic over $\mathbb{Q}$ by 9.3.1 and 9.3.4. It is enough to show this for G_2^*, and the proof is given analogously. Let $\alpha \in \mathcal{O}_K$, $\alpha \notin \mathbb{Z}$, and let S be a set of representatives for $\mathcal{O}_K/(\alpha)$ containing 0. Then we have

$$\alpha^{-2}\sum_{s \in S} E_2^*(\frac{z+s}{\alpha}, \mathcal{O}_K) = E_2^*(z, \mathcal{O}_K)$$

and therefore

$$G_2^* = \frac{1}{\alpha(\alpha - \overline{\alpha})} \sum_{s \neq 0} \Big(E_2^*(\frac{s}{\alpha}) - G_2^* \Big) = \frac{1}{\alpha(\alpha - \overline{\alpha})} \sum_{s \neq 0} \wp(\frac{s}{\alpha}),$$

where we use the fact that $N := \alpha\overline{\alpha}$ terms appear in the sum on the left-hand side. The same argument as in 9.3.1 shows that $\wp(\frac{s}{\alpha}) = \wp(\frac{\overline{\alpha}s}{N})$ is algebraic over $\mathbb{Q}(G_4, G_6)$ - and so G_2^* is as well. □

Chapter 10

Katz's measure

Let E be an elliptic curve over $\mathbb{C}$ with complex multiplication by $\mathcal{O}_K$ for some imaginary quadratic number field K. Choose an invariant differential on E such that the reduction of ω at every place of $\mathcal{O}_{\overline{\mathbb{Q}}}$ is regular. Let p be a prime that splits in K, let L/K be a finite extension of K over which E has everywhere good reduction, and let W be the ring of integers of the maximal unramified extension of $L_{\mathfrak{p}}$, the completion of L at some prime $\mathfrak{p}$ lying over p; by extending scalars, we understand (E, ω) as an elliptic curve defined over W.

Recall that the algebraic numbers $B(k, r)$ were defined by

$$B(k,r) = \frac{(-1)^k (k+r-1)! \pi^r}{2A^r \Omega^{k+2r}} G_{k,r}(\mathcal{O}_K).$$

The goal of this chapter is to explain Katz's proof of the below theorem.

Theorem 10.0.1. *There exists a unit $c \in W^\times$ and for any $b \in \mathbb{Z}$ coprime to p, a W-valued p-adic measure $\mu(c, b)$ on $\mathbb{Z}_p \times \mathbb{Z}_p$ such that*

$$\int_{\mathbb{Z}_p \times \mathbb{Z}_p} x^{k-3} y^r \,\mathrm{d}\mu(c,b) = 2c^{k+2r}(b^k - 1) B(k,r).$$

Proof. First, we recall that giving a W-valued p-adic measure μ on $\mathbb{Z}_p \times \mathbb{Z}_p$ is equivalent to specifying a power series $f \in W[|X, Y|]$: letting $D_X = (1+X)\frac{\partial}{\partial X}$ and $D_Y = (1+Y)\frac{\partial}{\partial Y}$, the requirement on f is that

$$D_X^{k-3} D_Y^r (f)|_{X,Y=0} = 2c^{k+2r}(b^k - 1) B(k,r), \quad k \geq 3, r \geq 0.$$

We interpret this by noting that $W[|X, Y|]$ is the coordinate ring of $\hat{\mathbb{G}}_m \times \hat{\mathbb{G}}_m$ over W, and D_X and D_Y are the standard invariant derivations.

Since p splits in K, E has good ordinary reduction $\tilde{E}$ at the chosen prime $\mathfrak{p}$. This means that the formal group law $\hat{\tilde{E}}$ is a one-dimensional formal group law of height one over the algebraically closed residue field $k = W/\mathfrak{m}$. By Lazard's theorem, $\hat{\bar{E}} \cong \hat{\mathbb{G}}_m$ over k. An argument using Hensel's lemma shows that this extends to an isomorphism of formal group laws $\hat{E} \cong \hat{\mathbb{G}}_m$ over W - see [13], 4.3.3. We fix one such isomorphism $\varphi : \hat{E} \to \hat{\mathbb{G}}_m$. Then there exists some $c \in W^\times$ such that $\varphi_*(c^{-1}\omega) = \frac{1}{1+X}\mathrm{d}X$, since the invariant differentials on both form a free W-module of rank one; this will be the c in the theorem.

We now consider the universal formal W-deformation E^{univ} of E - that is, the elliptic curve

$$E^{univ} : Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

over the ring $W[a_1, a_2, a_3, a_4, a_6]$. The formal moduli space $\hat{M}$ is the formal completion of $\mathrm{Spec}W[a_1, a_2, a_3, a_4, a_6]$ at a point corresponding to a Weierstrass equation for E, and φ extends to an isomorphism

$$\varphi : \hat{E}^{univ} \to \hat{M} \times \hat{\mathbb{G}}_m$$

of formal groups over W. This also gives us a natural choice of invariant differential ω^{univ} on E^{univ} - namely, the one that restricts to the pullback $\varphi^*(\frac{1}{1+X}\mathrm{d}X)$ from $\hat{\mathbb{G}}_m$ on $\hat{E}^{univ}$.

There is also an isomorphism $\hat{M} \cong \hat{\mathbb{G}}_m$ of formal group laws over W that we now describe. Recall that $H^1_{dR}(E/W)$ is a free W-module of rank 2. The invariant differential ω is nonzero in $H^1_{dR}(E/W)$, and so we can extend it to a basis u, v such that $u = c^{-1}\omega$ and that $u \wedge v = 1$ in $\Omega^2_{E/R} \cong \mathcal{O}_E$. By modifying v by some multiple of u, we may assume that this basis is adapted to the action of $\mathcal{O}_K$ on $H^1_{dR}(E/W)$; that is,

$$[\alpha]^*(u) = \alpha \cdot u, \;\; [\alpha]^*(v) = \overline{\alpha} \cdot v, \;\; \alpha \in \mathcal{O}_K.$$

Now extend scalars to $H^1_{dR}(E^{univ}/M) \otimes \mathrm{Div}(\hat{M})$, where

$$\mathrm{Div}(\hat{M}) = \{\sum_{n=0}^{\infty} \frac{a_n}{n!}T^n : a_n \in W\}$$

is the ring of divided power series and where T is a formal parameter of $\hat{M}$. After allowing divided powers, the Gauss-Manin connection ∇_{GM} on $H^1_{dR}(E^{univ}/M)$ becomes trivial, so we can extend u, v to a horizontal basis U, V - this amounts to finding local solutions of a particular differential equation, induced by the necessary linear relationship between ω, $\frac{\mathrm{d}}{\mathrm{d}T}(\omega)$ and $\frac{\mathrm{d}^2}{\mathrm{d}T^2}(\omega)$ where T is some parameter for M - we know that $H^1(E/M)$ has rank two. The invariant differential $\frac{1}{1+X}\mathrm{d}X$ on $\hat{\mathbb{G}}_m$ corresponds to an invariant differential

$$\varphi^*(\frac{1}{1+X}\mathrm{d}X) = U + L \cdot V, \text{ where } L \in \mathrm{Div}(\hat{M}),$$

where L corresponds to the logarithm on $\hat{\mathbb{G}}_m$.

This shows that $\hat{E}^{univ} \cong \hat{\mathbb{G}}_m \times \hat{\mathbb{G}}_m$ as formal group laws over W. The natural invariant derivations $(1+X)\frac{\partial}{\partial X}$ and $(1+Y)\frac{\partial}{\partial Y}$ on $\hat{\mathbb{G}}_m \times \hat{\mathbb{G}}_m$ correspond by our explicit description of the above isomorphism to the derivations $\frac{d}{dL}$ and D, respectively, where D is dual to the invariant differential ω on E^{univ}.

Finally, we construct the power series f on $\hat{E}^{univ}$. We pick a parameter Z such that

$$\omega^{univ} = (1 + [\text{higher powers of } Z])\mathrm{d}Z.$$

Any two rational functions on E^{univ} whose expansion around ∞ begin with $Z^{-2} + ...$ differ by a constant, because their difference lies in the one-dimensional (by Riemann-Roch) space $\Gamma(E^{univ}, \mathcal{L}(\infty))$. Therefore, applying D to any such series gives a power series $\wp'(Z)$. We define

$$f(Z) = b^3\wp'(bZ) - \wp'(Z) \in W[|Z|].$$

To show that the choice of f is correct, we need to argue that

$$(\frac{d}{dL})^r(D^{k-3}(f))|_{0,0} = 2c^{k+2r}(b^k - 1)B(k,r).$$

Intuitively, at least in the case $r = 0$ and $c = 1$, in transcendental notation (if we think of E^{univ} as a complex elliptic curve $\mathbb{C}/\mathcal{O}_K$) the $\wp'$ is actually the derivative of the Weierstrass $\wp$-function, and the result follows from the previous chapter, recalling that $\wp'$ is also E_3 and that D in this case represents $\frac{d}{dz}$. The result in general will follow after connecting $\frac{d}{dL}$ with the differential operator

$$\mathcal{D} = \overline{z}\frac{\partial}{\partial z} + \overline{\omega_1}\frac{\partial}{\partial \omega_1} + \overline{\omega_2}\frac{\partial}{\partial \omega_2}.$$

By the Serre-Tate theory, L corresponds to $\log(1+X) = \log(T)$ where $T = 1+X$ is the given local parameter on $\hat{\mathbb{G}}_m$. In this sense, $\frac{d}{dL}$ operates as $T\frac{d}{dT}$. It is known that this p-adic operator corresponds to the Weil operator

$$W = \frac{-\pi}{A}\Big(\overline{\omega}_1\frac{\partial}{\partial \omega_1} + \overline{\omega}_2\frac{\partial}{\partial \omega_2}\Big)$$

where $A(\omega_1, \omega_2) = \mathfrak{Im}[\overline{\omega}_1\omega_2]$ is the ‘signed area’ function; see [9], 2.3.38, 2.6.7 and 2.6.26. Since we evaluate $z = 0$, this is the operator we need. □

Chapter 11

Example: the Legendre family

Let $E : y^2 = x(x-1)(x-\lambda)$ be the Legendre elliptic curve over the moduli space

$$M = \operatorname{Spec} \mathbb{Z}[\frac{1}{2}, \lambda, \frac{1}{\lambda(\lambda-1)}];$$

this is the universal elliptic curve over $\mathbb{Z}[\frac{1}{2}]$, or generally over rings where 2 is invertible. $\omega = \frac{\mathrm{d}x}{2y}$ is a natural global differential on E. Pick any λ_0 such that the curve $y^2 = x(x-1)(x-\lambda_0)$ has complex multiplication by some $\mathcal{O}_K$, and let $\hat{M}$ be the completion of M at the point $\lambda = \lambda_0$.

To differentiate ω with respect to λ, we look at the Gauss-Manin connection on E. Note that M is a smooth relative curve over $R := \operatorname{Spec} \mathbb{Z}[\frac{1}{2}]$, so in the defining filtration for ∇_{GM} (see 4.4)

$$... \subseteq F^2(\Omega^\bullet_{E/R}) \subseteq F^1(\Omega^\bullet_{E/R}) \subseteq \Omega^\bullet_{E/R},$$

$$F^k(\Omega^\bullet_{E/R}) := \operatorname{im}[\Omega^{\bullet-k}_{E/R} \otimes_{\mathcal{O}_E} \pi^*\Omega^k_{M/R} \to \Omega^\bullet_{E/R}],$$

we have $F^k(\Omega^\bullet_{E/R}) = 0$ for $k \geq 2$. Therefore, instead of the filtration spectral sequence, we are left with only the exact sequence of complexes

$$0 \longrightarrow \pi^{-1}\Omega^1_{M/R} \otimes_{\pi^{-1}\mathcal{O}_M} \Omega^{\bullet-1}_{E/R} \longrightarrow \Omega^\bullet_{E/R} \longrightarrow \Omega^\bullet_{E/M} \longrightarrow 0.$$

The Gauss-Manin connection is now the transfer map on cohomology

$$\nabla_{GM} : \mathcal{H}^k_{dR}(E/M) = H^k(\Omega^\bullet_{E/M}) \xrightarrow{\delta} H^{k+1}(\pi^{-1}\Omega^1_{M/R} \otimes_{\pi^{-1}\mathcal{O}_M} \Omega^{\bullet-1}_{E/M})$$

$$= \Omega^1_{M/R} \otimes_{\mathcal{O}_M} H^k(\Omega^\bullet_{E/M}) = \Omega^1_{M/R} \otimes_{\mathcal{O}_M} \mathcal{H}^k_{dR}(E/M).$$

We now calculate $\nabla_{GM}(\omega)$. Take $\frac{\mathrm{d}x}{2y} \in \Omega^1_{E/R}$ as a lift of ω; then

$$\mathrm{d}(\omega) = \mathrm{d}(\frac{1}{2y}\mathrm{d}x) = \mathrm{d}(\frac{1}{2y}) \wedge \mathrm{d}x = \mathrm{d}x \wedge \frac{1}{2y^2}\mathrm{d}y.$$

Since $y^2 = x(x-1)(x-\lambda) =: f(x,\lambda)$, we have

$$2y\mathrm{d}y = \partial_x f \mathrm{d}x + \partial_\lambda f \mathrm{d}\lambda$$

and so

$$2y\mathrm{d}x \wedge \mathrm{d}y = \partial_\lambda f \mathrm{d}x \wedge \mathrm{d}\lambda.$$

Therefore, we can write the above as

$$\mathrm{d}\omega = \mathrm{d}x \wedge \frac{1}{2y^2}\mathrm{d}y = \frac{\partial_\lambda f}{4y^3}\mathrm{d}x \wedge \mathrm{d}\lambda \in \Omega^2_{E/R}.$$

A preimage of this in $\Omega^1_{M/R} \otimes_{\mathcal{O}_M} \Omega^1_{E/R}$ is given by $\mathrm{d}\lambda \otimes -\frac{\partial_\lambda f}{4y^3}\mathrm{d}x$, and its cohomology class is $\nabla_{GM}(\omega)$. We can now apply the derivation $\frac{\partial}{\partial\lambda}$ to see that

$$\frac{\partial}{\partial\lambda}(\omega) := (\frac{\partial}{\partial\lambda} \otimes \mathrm{id})(\nabla_{GM}(\omega)) = -\frac{\partial_\lambda f}{4y^3}\mathrm{d}x = \frac{\mathrm{d}x}{4y(x-\lambda)}.$$

We can write this another way. Let $g(x,\lambda) := \frac{-3x+2-\lambda}{\lambda(\lambda-1)}$ and $h(x,\lambda) = \frac{x(x-1)}{\lambda(\lambda-1)}$, so we have

$$-\partial_\lambda f = g \cdot f + h \cdot \partial_x f.$$

Then it holds that

$$-\frac{\partial_\lambda f}{4y^3}\mathrm{d}x = (\frac{g}{4y} + \frac{h \cdot \partial_x f}{4y^3})\mathrm{d}x = \frac{g + 2\partial_x h}{4y}\mathrm{d}x - \mathrm{d}\Big(\frac{h}{2y}\Big);$$

here we note that over M, λ is a constant, and so $2y\mathrm{d}y = \partial_x f \mathrm{d}x$. Therefore, the above lies in the same cohomology class as

$$\frac{g + 2\partial_x h}{2}\frac{\mathrm{d}x}{2y} = \frac{x-\lambda}{2\lambda(\lambda-1)}\omega.$$

With the operator $D := 2\lambda(\lambda-1)\frac{\partial}{\partial\lambda}$, we see that $D(\omega) = (x-\lambda)\omega$ and that

$$(\omega, D(\omega))_{dR} = (\omega, x\omega)_{dR} = 1.$$

A similar computation shows that $D^2(\omega) = D(x\omega) - \lambda D(\omega) = -\lambda(\lambda-1)\omega$: calculating directly, we find $\frac{\partial}{\partial\lambda}(x\omega) = \frac{-x\partial_\lambda f}{4y^3}\mathrm{d}x$, and the claim follows from $y^2\mathrm{d}x = f\mathrm{d}x \equiv x\partial_x f\mathrm{d}x$ as cohomology classes.

By modifying $D(\omega)$ with a scalar multiple of ω, we get the unique basis u, v of $H^1_{dR}(E|_{\lambda=\lambda_0}/R)$:

$$u = \omega|_{\lambda=\lambda_0}, \quad v = (D(\omega) - e\omega)|_{\lambda=\lambda_0}$$

adapted to the action of $\mathcal{O}(K)$ (as in the previous section) for some $e \in \mathfrak{d} \otimes \mathcal{O}_K[1/2]$, $\mathfrak{d}$ being the different of K. We extend u, v to a horizontal basis of $H^1_{dR}(E/M)$ by finding the local solutions (as divided power series) $\alpha(\lambda)$, $\beta(\lambda)$ of the equation $D^2 f + \lambda(\lambda-1)f = 0$. Explicitly, this is Euler's hypergeometric differential equation

$$\lambda(1-\lambda)\frac{d^2 f}{d\lambda^2} + (1-2\lambda)\frac{df}{d\lambda} - \frac{1}{4}f = 0$$

for the hypergeometric function ${}_2F_1(a,b,c;\lambda)$ with $a = b = \frac{1}{2}$ and $c = 1$. We require the boundary conditions

$$\alpha(\lambda_0) = 1, \;\; D\alpha(\lambda_0) = e, \;\; \beta(\lambda_0) = 0, \;\; D\beta(\lambda_0) = 1,$$

and set $U = D(\beta)\cdot\omega - \beta\cdot D(\omega)$ and $V = -D(\alpha)\cdot\omega + \alpha D(\omega)$; these are clearly horizontal with respect to ∇_{GM} and extend u, v. Then ω is given by

$$\omega = \alpha U + \beta V,$$

and the 'natural' invariant differential ω^{univ} on E is

$$\omega^{univ} = U + LV = \frac{1}{\alpha}\omega$$

where $L = \frac{\beta}{\alpha}$. The invariant derivation dual to ω^{univ} is then

$$D^{univ} = 2\alpha y \cdot \frac{d}{dx},$$

and the derivation d/dL is found by noting that L satisfies $D(L) = \frac{1}{\alpha^2}$; indeed, we have

$$D(L) = \frac{D(\beta)\alpha - D(\alpha)\beta}{\alpha^2}$$

where $D(D(\beta)\alpha - D(\alpha)\beta) = D^2(\beta)\alpha - \beta D^2(\alpha) = 0$ and where the value of $D(\beta)\alpha - D(\alpha)\beta$ at λ_0 is 1. This implies

$$\frac{d}{dL} = \Big(\frac{d}{d\lambda}(L)\Big)^{-1}\frac{d}{d\lambda} = \alpha^2 2\lambda(\lambda-1)\frac{d}{d\lambda}.$$

For any given b, the function f to be taken is

$$f = 2\alpha^3(b^3[b]^*(y) - y).$$

Bibliography

[1] Coates, J. and Wiles, A. *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. 39 (1977), 223-251.

[2] Colmez, P. *Fontaine's rings and p-adic L-functions*, Lecture notes (2004).

[3] Damerell, R.M. *L-functions of elliptic curves with complex multiplication, I*, Acta Arith. 17 (1970), 287-301.

[4] Dieudonné, J. and Grothendieck, A. *Éléments de géométrie algébrique III*, Publ. Math. de l'I.H.É.S. 11 (1961), 5-167.

[5] Fröhlich, A. *Formal groups*, Springer-Verlag (1968).

[6] Hartshorne, R. *Algebraic geometry*, Springer-Verlag (1977).

[7] Hindry, M. *Introduction to zeta and L-functions from arithmetic geometry and some applications*, Lecture notes (2010).

[8] Katz, N. *p-adic L-functions, Serre-Tate local moduli, and ratios of solutions of differential equations.* Proc. Int. Cong. Math.: Helsinki (1978), 365-371.

[9] Katz, N. *p-adic L-functions for CM fields.* Invent. Math. 49 (1978), 199-297.

[10] Katz, N. and Mazur, B. *Arithmetic moduli of elliptic curves.* Princeton Univ. Press (1985).

[11] Katz, N. and Oda, T. *On the differentiation of de Rham cohomology classes with respect to parameters.* J. Math. Kyoto Univ. 8-2 (1968), 199-213.

[12] Lang, S. *Elliptic functions.* Second edition. Springer-Verlag (1987)

[13] Lubin, J. *One-parameter formal Lie groups over p-adic integer rings.* Ann. Math. 80 (1964), 464-484; Correction *ibid.* 84 (1966), 372.

[14] Milne, J. *Class field theory*, v. 4.02. Available online at http://www.jmilne.org, 2013.

[15] Raskin, S. *The Weil conjectures for curves.* 2007. Available online at http://math.uchicago.edu/ mitya/beilinson/SamREU07.pdf, 2013.

[16] Rubin, K. *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer.* Invent. Math. 64 (1981), 455-470.

[17] de Shalit, E. *Iwasawa theory of elliptic curves with complex multiplication: p-adic L-functions.* Academic Press, Inc. (1987).

[18] Shimura, G. *Introduction to the arithmetic theory of automorphic functions.* Princeton Univ. Press (1971).

[19] Silverman, J. *Advanced topics in the arithmetic of elliptic curves.* Springer-Verlag (1994).

[20] Silverman, J. *Arithmetic of elliptic curves.* Springer-Verlag (1986).

[21] Tate, J.T. *Fourier analysis in number fields and Hecke's zeta-functions.* Algebraic Number Theory (Proc. Instr. Conf.) (1965), 305-347.

[22] Weil, A. *Elliptic functions according to Eisenstein and Kronecker.* Springer-Verlag (1976).

[23] Zink, T. *Cartiertheorie kommutativer formaler Gruppen.* B.G. Teubner Verlag (1984).