Jeremias Yehdegho, BSc

Elliptic Curves, Modular Curves and a Theorem of André

MASTER'S THESIS

to achieve the university degree of

Diplom-Ingenieur

Master's degree programme: Mathematical Computer Science

submitted to

Graz University of Technology

Supervisor

O.Univ.-Prof. Dr.phil. Robert Tichy

Institute of Analysis and Number Theory

Graz, September 2016

AFFIDAVIT

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present master‘s thesis.

Date

Signature

Elliptic Curves, Modular Curves and a Theorem of André

Jeremias Yehdegho

September 15, 2016

Contents

Introduction

Yves André, in his book "G-Functions and Geometry"[And89], asks if a curve, which lies inside a Shimura variety and contains infinitely many special points, is a Shimura subvariety. In 1998 he was able to prove:

Theorem 0.0.1 (André's Theorem[And98]). Let $C \subseteq \mathbb{A}^2$ be an algebraic curve such that C is neither a vertical nor a horizontal line and suppose C contains infinitely many special points, then C is a modular curve.

The notion of a Shimura variety is highly technical and we confine ourselves to mentioning that the varieties involved in André's theorem, i.e. $\mathbb{A}^2$, which parametrizes pairs of elliptic curves, modular curves, which parametrize isogenies between elliptic curves with cyclic kernel, and (certain) vertical and horizontal lines, are Shimura varieties. Moreover a point $(j_1, j_2) \in \mathbb{A}^2$ is called special if each coordinate is the j-invariant of a CM elliptic curve.

Both, CM elliptic curves (among elliptic curves) and modular curves (among spaces parametrizing elliptic curves) are exceptional and in this sense André's theorem is an instance of what Zannier calls an *unlikely intersection*[ZM12].

In the meantime, Frans Oort[Oor97] extended the conjecture to arbitrary Shimura subvarieties (instead of just curves) and since then significant progress has been made going in various directions, among others:

- Bas Edixhoven, Bruno Klingler and Andrei Yafaev[EY03; Yaf06; KY14] and others give proofs conditional on the Generalized Riemann Hypothesis.
- Jonathan Pila[Pil09] and others use o-minimal theory to give unconditional proofs. Recently, using such methods, Jacob Tsimerman[Tsi15] announced a proof for moduli spaces of principally polarized abelian varieties.
- Lars Kühne[Küh12] and independently Yuri Bilu, David Masser and Umberto Zannier[BMZ13] show André's theorem using transcendence theory and give effective variations of the theorem. In 2014, Gisbert Wüsholz fixed a gap in Kühne's argument and proves a fully effective version of André's theorem[Wü14].

Like the proof of André, the proofs of Bilu, Masser, Zannier, Kühne and Wüstholz are split into two parts corresponding to modular curves and vertical and horizontal lines respectively. Where André uses Siegel's (ineffective) class number estimate in the modular curve case, Bilu, Masser, Zannier, Kühne and Wüstholz use Baker's theory of linear forms in logarithms. I will follow their argument and use Wüstholz' presentation is my main reference.

In the vertical and horizontal line case, André, Bilu, Masser and Zannier use Masser's (effective) transcendence measure, whereas Kühne and Wüstholz use linear forms in elliptic logarithms. Unfortunately, their methods are beyond my abilities and I will present the easier argument from Bilu, Masser

and Zannier. The effectivity of parts of their argument, which the authors consider a "standard affair", is presented only in brief and I am unable to conclude full effectivity however an expert may very well disagree with my assessment. I will prove, using a theorem of Bilu and Borichev[BB13], the effectivity in some special cases.

In 2014 I was fortunate to attend lectures by Gisbert Wüstholz, which introduced me to this subject and spawned this thesis at the suggestion of my advisor Robert Tichy. I am particularly grateful to them.

Before André's theorem can be proved, Chapter 1 develops elliptic curves from a minimalist approach to varieties. Using the Riemann-Roch theorem, elliptic curves are shown to be isomorphic to curves given by short Weierstraß equations. An abelian group structure is placed on the underlying set of an elliptic curve and the geometry of divisors is then used to show that this group structure coincides with the geometric chord and tangent group law. Morphisms which respect this group law are studied and finally the j-invariant is introduced and shown to be an invariant.

Chapter 2 develops the theory of complex tori in the style of the previous chapter, where Riemann surfaces assume the role of smooth algebraic curves, complex tori are introduced as (group) quotients of $\mathbb{C}$ and the topological properties of this quotient are used to study the meromorphic functions on a torus. These meromorphic functions will satisfy an equation of an elliptic curve and the algebraic j-invariant will give rise to an analytic pendant with rich properties.

In Chapter 3, the category of elliptic curves and the category of complex tori are shown to be equivalent. Essential for this task is the unique Riemann surface structure on an elliptic curve, which uses the implicit function theorem of Appendix A. Once the uniformization theorem is shown, the accessible nature of complex tori is used to classify the endomorphism rings of elliptic curves and to single out the class of CM elliptic curves.

In Chapter 4, the Fourier expansion of the j-invariant is shown and where the j-invariant satisfies a transformation law for $\mathrm{SL}_2(\mathbb{Z})$, an analogue is introduced which satisfies a transformation law for certain subgroups of $\mathrm{SL}_2(\mathbb{Z})$. These subgroups turn out to be intimately connected with cyclic sublattices, respectively isogenies of elliptic curves with cyclic kernel, and modular curves are shown to parametrize these isogenies.

In Chapter 5, the height of a polynomial and an algebraic number is defined and used to show that the number of algebraic numbers of bounded height and degree is finite. Moreover the relation between the height and the discriminant of the endomorphism ring of a CM elliptic curve is investigated. The j-invariant is compared with the function $q(\tau)^{-1} = e^{-2\pi i\tau}$ and their asymptotic similarity is explicitly measured. Lastly, the proof of André's theorem is given and the effectivity of the argument is discussed.

1. Elliptic Curves

This chapter will provide the basic tools from algebraic geometry used throughout this thesis. While this thesis is about moduli spaces of complex elliptic curves, the fact that these can be defined over algebraic extensions of $\mathbb{Q}$ is secondary to the goal of this thesis and hence the approach used here will not be the one of schemes. Rather, a more concrete approach following Chapter 1 of Hartshorne's "Algebraic Geometry" [Har77] and Silverman's "The Arithmetic of Elliptic Curves" [Sil09] will be used, where varieties will be given by sets of points inside either some affine n-space $\mathbb{A}^n (= \mathbb{A}^n(\mathbb{C}))$ or projective n-space $\mathbb{P}^n (= \mathbb{P}^n(\mathbb{C}))$.

1.1. Varieties

Definition 1.1.1. [Har77, p. 1] Let $n \geq 1$ be a natural number. The affine n-space $\mathbb{A}^n$ is, as a set, $\mathbb{C}^n$. Sometimes it will be useful to consider $\mathbb{A}^n$ with the topology of $\mathbb{C}^n$, in which case we explicitly refer to this topology as the *complex topology*.

Definition 1.1.2. [Har77, p. 8ff] Let $n \geq 1$ be a natural number. The projective n-space $\mathbb{P}^n$ is, as a set, defined to be

$$\mathbb{C}^{n+1} - \{0\} / \sim,$$

where $\sim$ is the equivalence relation

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n) :\Longleftrightarrow \exists \lambda \in \mathbb{C}^\times : \forall i \in \{0, \ldots, n\} : x_i = \lambda y_i.$$

The equivalence classes will be denoted by $(x_0 : \cdots : x_n)$. As before, the quotient topology will be useful at times and is also called the *complex topology*.

Definition 1.1.3. [Har77, p. 2ff] Let $T \subseteq \mathbb{C}[X_1, \ldots, X_n]$ be a set of polynomials. The *zero set* of T in $\mathbb{A}^n$ is defined as

$$\mathcal{V}(T) = \{\underline{x} \in \mathbb{A}^n \mid \forall f \in T : f(\underline{x}) = 0\}.$$

Clearly, the zero set of T coincides with the zero set of $\langle T \rangle$ and since $\mathbb{C}[X_1, \ldots, X_n]$ is Noetherian, the ideal $\langle T \rangle$ has finitely many generators $f_1, \ldots, f_N \in \langle T \rangle$ such that

$$\mathcal{V}(T) = \mathcal{V}(\langle T \rangle) = \mathcal{V}(\langle f_1, \ldots, f_N \rangle) = \mathcal{V}(f_1, \ldots, f_N).$$

For a subset V of $\mathbb{A}^n$, the *ideal of* V is defined as

$$I(V) = \{f \in \mathbb{C}[X_1, \ldots, X_n] \mid \forall \underline{x} \in V : f(\underline{x}) = 0\}.$$

Definition 1.1.4. [Har77, p. 9ff] A polynomial $f \in \mathbb{C}[X_0, \ldots, X_n]$ is called *homogeneous of degree d* if every monomial in f has degree d. For $(x_0, \ldots, x_n) \in (x_0 : \cdots : x_n) \in \mathbb{P}^n$ and $\lambda \in \mathbb{C}^\times$, we evaluate

$$f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n).$$

While it makes no sense to evaluate a homogeneous polynomial on a projective point, the set of projective points on which f vanishes is well-defined. Let T be a set of homogeneous polynomials in $\mathbb{C}[X_0, \ldots, X_n]$, then the *zero set* of T in $\mathbb{P}^n$ is defined as

$$\mathcal{V}(T) = \{\underline{x} \in \mathbb{P}^n \mid \forall f \in T : f(\underline{x}) = 0\}.$$

An ideal in $\mathbb{C}[X_0, \ldots, X_n]$ is called *homogeneous* if it can be generated by a set of homogeneous polynomials. As before, the zero set $\mathcal{V}(T)$ coincides with $\mathcal{V}(\langle T \rangle)$ and since $\mathbb{C}[X_0, \ldots, X_n]$ is Noetherian, the homogeneous ideal $\langle T \rangle$ has a finite generating set $f_1, \ldots f_N$, consisting of homogeneous polynomials, such that

$$\mathcal{V}(T) = \mathcal{V}(\langle T \rangle) = \mathcal{V}(\langle f_1, \ldots, f_N \rangle) = \mathcal{V}(f_1, \ldots, f_N).$$

For a subset V of $\mathbb{P}^n$, the *ideal of* V is defined as

$$I(V) = \langle f \in \mathbb{C}[X_0, \ldots, X_n] \mid f \text{ homogeneous}, \forall \underline{x} \in V : f(\underline{x}) = 0 \rangle.$$

Definition + Proposition 1.1.5 (The Zariski Topology). Let $\{T_i \mid i \in I\}$, S, T either be a sets of polynomials in $\mathbb{C}[X_1, \ldots, X_n]$ or sets of homogeneous polynomials in $\mathbb{C}[X_0, \ldots, X_n]$.

1. $\mathcal{V}\left(\bigcup_{i \in I} T_i\right) = \bigcap_{i \in I} \mathcal{V}(T_i)$
2. $\mathcal{V}(T) \cup \mathcal{V}(S) = \mathcal{V}(ST)$
3. a) $\mathcal{V}(0) = \mathbb{A}^n$ and $\mathcal{V}(\mathbb{C}[X_1, \ldots, X_n]) = \varnothing$ (affine case)
   b) $\mathcal{V}(0) = \mathbb{P}^n$ and $\mathcal{V}(X_0, \ldots, X_n) = \varnothing$ (projective case)

The zero sets on $\mathbb{A}^n$ and $\mathbb{P}^n$ are the closed sets of the *Zariski topology*. Unless otherwise mentioned, the affine and projective n-space carry the Zariski topology.

Proof. [Har77, Proposition 1.1., 2.1., p. 2,9] ∎

Theorem 1.1.6 (Nullstellensätze). Let $\mathfrak{a}$ be a (homogeneous) ideal, S and T be sets of (homogeneous) polynomials and let V and W be subsets of $\mathbb{A}^n$ (respectively $\mathbb{P}^n$).

1. If $T \subseteq S$, then $\mathcal{V}(T) \supseteq \mathcal{V}(S)$. If $V \subseteq W$, then $I(V) \supseteq I(W)$.
2. $I(\mathcal{V}(\mathfrak{a})) = \sqrt{\mathfrak{a}}$ and $\mathcal{V}(I(V)) = \overline{V}$, where $\overline{V}$ is the closure of V.
3. An algebraic set is irreducible if and only if its ideal is a prime ideal.

Proof. [Har77, Prop. 1.2., Cor. 1.4, Ex. 2.1., p. 3,4,11] ∎

Proposition 1.1.7. [Har77, p. 5, Proposition 1.5.]

1. Any descending chain of algebraic sets in $\mathbb{A}^n$ (respectively $\mathbb{P}^n$) becomes stationary.

2. Any algebraic set in $\mathbb{A}^n$ (respectively $\mathbb{P}^n$) is a finite union of irreducible algebraic sets.

Proof. 1. Let $X_0 \supseteq X_1 \supseteq \ldots$ be a descending chain of algebraic sets, then $I(X_0) \subseteq I(X_n) \subseteq \ldots$ is an ascending chain of (homogeneous) ideals, which becomes stationary since $\mathbb{C}[X_1, \ldots, X_n]$ (respectively $\mathbb{C}[X_0, \ldots, X_n]$) is Noetherian. It follows that $X_0 = \mathcal{V}(I(X_0)) \supseteq X_1 = \mathcal{V}(I(X_1)) \supseteq \ldots$ becomes stationary.
2. Let Ω be the set of algebraic sets which are not a finite union of irreducible algebraic sets and suppose Ω is not empty. By 1, Ω contains a minimal element X which is not irreducible, since otherwise $X = X$ is a finite union of irreducible algebraic sets. Thus $X = Y \cup Z$, for Y and Z algebraic and by the minimality of X, Y and Z are the union of some irreducible algebraic sets $Y_1, \ldots, Y_r$ and $Z_1, \ldots, Z_s$. Hence

$$X = Y \cup Z = Y_1 \cup \ldots \cup Y_r \cup Z_1 \cup \ldots \cup Z_s$$

is a finite union of irreducible algebraic sets. ∎

Definition 1.1.8. [Har77, p. 3,10] An *affine variety* is an irreducible algebraic set inside some $\mathbb{A}^n$. Open subsets of affine varieties are called *quasi-affine varieties*. Similarly, an irreducible algebraic set inside some $\mathbb{P}^n$ is called *projective variety* and their open subsets are called *quasi-projective varieties*. A *variety* is any or the former.

Definition 1.1.9. [Har77, p. 4,10] Let $X \subseteq \mathbb{A}^n$ be an affine variety, then the *affine coordinate ring of X* is defined as

$$\mathbb{C}[X] = \mathbb{C}[X_1, \ldots, X_n]/I(X).$$

Its quotient field, which exists since $I(X)$ is prime, is called the *function field of X*. If $Y \subseteq \mathbb{P}^m$ is a projective variety, the *homogenous coordinate ring of Y* is defined as

$$\mathbb{C}[Y] = \mathbb{C}[Y_0, \ldots, Y_m]/I(Y).$$

Given two homogeneous polynomials $f, g \in \mathbb{C}[Y_0, \ldots, Y_n]$ of equal degree d we can evaluate $\frac{f}{g}$ at a projective point $P \in \mathbb{P}^n$ provided $g(P) \neq 0$, since

$$\frac{f(\lambda Y_0, \ldots, \lambda Y_n)}{g(\lambda Y_0, \ldots, \lambda Y_n)} = \frac{\lambda^d f(Y_0, \ldots, Y_n)}{\lambda^d g(Y_0, \ldots, Y_n)}$$

and the function field of Y is defined as

$$\mathbb{C}(Y) = \left\{ \frac{f}{g} \mid f, g \in \mathbb{C}[Y] \text{ homogeneous of equal degree, } g \neq 0 \right\}.$$

The *dimension* of a variety is defined to be the transcendence degree over $\mathbb{C}$ of the function field of its Zariski closure.

Definition 1.1.10. [Har77, p. 31] Let $X = \mathcal{V}(f_1, \ldots, f_k)$ be variety lying inside either $\mathbb{A}^n$ or $\mathbb{P}^n$. A point $P \in X$ is called *regular (or non-singular or smooth)* if it is not a solution of the system

$$\frac{\partial f_i}{\partial X_j} = 0,$$

where $i = 1, \ldots, k$ and $j = 0, \ldots, n$ in the projective case and $j = 1, \ldots, n$ in the affine case. If every point in X satisfies this property, the variety is called *regular (or non-singular or smooth)*.

Definition + Proposition 1.1.11. Let X and Y be varieties and assume that $Y \subseteq \mathbb{A}^n$ is quasi-affine. An n-tuple $(f_1, \ldots, f_n)$ of rational functions on X is called a *pre-rational map* if the domain U on which all f_i are defined is dense and open in X and

$$\forall P \in U : (f_1(P), \ldots, f_n(P)) \in Y.$$

Two pre-rational maps $(f_1, \ldots, f_n)$ and $(g_1, \ldots, g_n)$ are equivalent if they coincide on the intersection of their domains. An equivalence class of pre-rational maps is called a *rational map* and is written $(f_1, \ldots, f_n) \colon X \dashrightarrow Y$.

If $Y \subseteq \mathbb{P}^n$ is quasi-projective, we say that call a $(n+1)$-tuple $(f_0, \ldots, f_n)$ a *pre-rational map* if the domain U on which all f_i are defined is dense and open in X and

$$\forall P \in U : (f_0(P) : \cdots : f_n(P)) \in Y.$$

Two pre-rational maps $(f_0, \ldots, f_n)$ and $(g_0, \ldots, g_n)$ are equivalent if they coincide on the intersection of their domains. An equivalence class of pre-rational maps is called a *rational map* and is written $(f_0 : \cdots : f_n) \colon X \dashrightarrow Y$.

A rational map φ is a *regular morphism* if φ is defined at every point in X. A regular morphism $\varphi \colon X \to Y$ is an isomorphism if there exists a regular morphism $\psi : Y \to X$ such that $\varphi \circ \psi$ and $\psi \circ \varphi$ are the identity maps on the respective varieties.

Proof. [Silo9, p. 11ff] ∎

Proposition 1.1.12. For $i \in \{0, 1, \ldots, n\}$ let U_i be the quasi-projective variety $\mathbb{P}^n \setminus \mathcal{U}(X_i)$, then

$$\varphi_i : \begin{cases} \mathbb{A}^n & \longrightarrow & U_i \\ (y_0, \ldots, y_{i-1}, y_{i+1}, \ldots, y_n) & \longmapsto & (y_0 : \cdots : y_{i-1} : 1 : y_{i+1} : \cdots : y_n) \end{cases}.$$

and

$$\varphi_i : \begin{cases} U_i & \longrightarrow & \mathbb{A}^n \\ (X_0 : \cdots : X_{i-1} : X_i : X_{i+1} : \cdots : X_n) & \longmapsto & \left(\frac{X_0}{X_i}, \ldots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \ldots, \frac{X_n}{X_i}\right) \end{cases}$$

are mutually inverse regular morphisms. The maps φ_i are called *affine charts* on $\mathbb{P}^n$.

Proof. [Har77, p. 10ff, 18, Prop. 2.2., 3.3.] ∎

Proposition 1.1.13 (The Segre Embedding). Let m and n be natural numbers. The function

$$\varphi \colon \begin{cases} \mathbb{P}^m \times \mathbb{P}^n & \longrightarrow & \mathbb{P}^{mn+m+n} \\ ((x_0 : \cdots : x_m), (y_0 : \cdots : y_n)) & \longmapsto & (x_i y_j)_{0 \le i \le m, 0 \le j \le n} \end{cases}$$

is injective. We identify $\mathbb{P}^m \times \mathbb{P}^n$ with its image, which is a projective variety in $\mathbb{P}^{mn+m+n}$.

Proof. [Har77, p. 13, Ex. 2.14.] ∎

Definition + Proposition 1.1.14. A rational map $\varphi\colon X \dashrightarrow Y$ is called *dominant* if there exists an open subset $U \subseteq X$ such that $\varphi \restriction_U$ is a morphism and $\varphi(U) \subseteq Y$ is dense. A dominant rational map $\varphi\colon X \dashrightarrow Y$ induces a morphism of $\mathbb{C}$-algebras

$$\varphi^*\colon \begin{cases} \mathbb{C}(Y) & \longrightarrow & \mathbb{C}(X) \\ f & \longmapsto & f \circ \varphi \end{cases}$$

and the degree $\deg \varphi$ of φ is defined as $[\mathbb{C}(X) : \varphi^*\mathbb{C}(Y)]$. The degree of φ is 1 if and only if there exists a dominant rational map $\psi\colon Y \dashrightarrow X$ such that $\varphi \circ \psi$ and $\psi \circ \varphi$ are the identities (as rational maps) on the respective varieties.

Proof. [Har77, p. 25ff, Theorem 4.4.] ∎

Corollary 1.1.15. Let X be a variety and $Y \subseteq X$ any open and dense subvariety, then $\mathbb{C}(X) = \mathbb{C}(Y)$. In particular if X is quasi-projective, $\mathbb{C}(X)$ is isomorphic to the function field of $\mathbb{C}(X \cap U_i)$, where U_i is an affine chart on X.

Proof. Since Y is open and dense, the inclusion is a rational map of degree 1. ∎

1.2. Algebraic curves

Definition 1.2.1. An *(algebraic) curve* is a one-dimensional variety.

Proposition 1.2.2. [Silo9, p. 19, Proposition 2.1] Let C be a curve, $\varphi\colon C \dashrightarrow \mathbb{P}^n$ a rational map and $P \in C$. If P is a regular point, φ is regular at P and if C is regular, φ is a morphism.

Proof. Let $\psi = (f_0 : \cdots : f_n)$, t be a uniformizing parameter at P and $k = \min_{i=0,\ldots,n} v_P(f_i)$, then

$$(f_0 : \cdots : f_n) = (t^{-k} f_0 : \cdots : t^{-k} f_n)$$

and hence φ is regular at P since $v_P(t^{-k} f_i) \geq 0$. ∎

Definition 1.2.3. [Silo9, p. 27, 28] Let C be a smooth algebraic curve. The group of divisors $\mathrm{Div}C$ on C is defined as the free abelian group generated by the set C. A divisor $D \in \mathrm{Div}C$ is written as

$$D = \sum_{P \in C} n_P P$$

with $n_P = 0$ for almost all $P \in C$. Further we let $v_P(D) = n_P$ and define the degree of D as $\deg D = \sum_{P \in C} n_P$. The subgroup $\mathrm{Div}^0 C$ contains all divisors of degree 0. If $f \in \mathbb{C}(C)^\times$ is a rational function on C we define

$$(f) = \sum_{P \in C} v_P(f) P$$

and call it the principal divisor of f. Two divisors D and D' are called *equivalent* if they differ by a principal divisor, i.e. $D = D' + (f)$ for some $f \in \mathbb{C}(C)$.

Definition 1.2.4. [Sil09, p. 30] Let C be a smooth algebraic curve. The $\mathbb{C}(C)$-space of differentials $\Omega(C)$ is the space generated by the symbols $\{df \mid f \in \mathbb{C}(C)\}$ modulo the relations

$$\begin{aligned} d(f+g) &= df + dg \\ dfg &= fdg + gdf \\ da &= 0, \forall a \in \mathbb{C}. \end{aligned}$$

Definition + Proposition 1.2.5. Let C be a smooth algebraic curve and ω a differential on C. For every point $P \in C$ there exists a rational function f_P such that

$$\omega = f_P dt,$$

where t is a uniformizing parameter at P. For almost all points we have $v_P(f_P) = 0$ and hence we can define the divisor associated with ω as

$$(\omega) = \sum_{P \in C} v_P(f_P)P.$$

the dimension of $\Omega(C)$ as a $\mathbb{C}(C)$-vector space is 1 and for all $f \in \mathbb{C}(C)$ and all $\omega \in \Omega(C)$ the divisor corresponding to $f\omega$ is equal to $(f) + (\omega)$.

Proof. [Sil09, p. 31ff, Proposition 3.4., Remark 4.4.] ∎

Definition + Proposition 1.2.6. Let C be a smooth algebraic curve and D a divisor on C. The *Riemann-Roch space* of D

$$L(D) = \{f \in \mathbb{C}(C)^\times \mid \forall P \in C : v_P(f) \geq -v_P(D)\} \cup \{0\}$$

is a finite-dimensional $\mathbb{C}$-vector space.

Proof. [Sil09, p. 34, Proposition 5.2.] ∎

Since $(f\omega) = (f) + (\omega)$ and the dimension of $\Omega(C)$ is 1, all divisors corresponding to a differential are equivalent and we define:

Definition 1.2.7. Let C be a smooth curve and ω any non-zero differential on C. The dimension g of $L((\omega))$ is called the *genus* of C.

Throughout the chapter a central tool is the Riemann-Roch theorem:

Theorem 1.2.8 (Riemann-Roch). Let C be a smooth algebraic curve with genus g, D a divisor and K a divisor corresponding to a differential, then

$$\dim_{\mathbb{C}} L(D) = \deg D + 1 - g + \dim_k L(K - D).$$

Moreover $\dim_{\mathbb{C}} L(K - D) = 0$ if $\deg D \geq 2g - 1$ and $\deg K = 2g - 2$.

Proof. [Mir95, p. 192, Theorem 3.11.] ∎

1.3. Elliptic Curves

Definition 1.3.1. [Silo9, p. 59] A smooth projective curve E of genus 1 together with a point $O \in E$ is called *elliptic curve*.

Proposition 1.3.2. [Silo9, p. 59ff, Prop. 3.1.] Let E be an elliptic curve and O a point on E.

1. There exist rational functions $x, y \in \mathbb{C}(E)$ and coefficients $a_1, a_3, a_2, a_4, a_6 \in \mathbb{C}$ such that

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.1}$$

2. The rational map

$$\varphi\colon \begin{cases} E & \dashrightarrow & \mathcal{V}(F) \subseteq \mathbb{P}^2 \\ P & \longmapsto & (x(P) : y(P) : 1) \end{cases},$$

is a morphism of degree 1, where

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3.$$

Proof. 1. The Riemann-Roch theorem ensures that

$$\dim_{\mathbb{C}} L(nO) = n,$$

for $n \geq 1$ and $\dim_{\mathbb{C}} L(O) = 1$. Thus there exist rational functions $x \in L(2O) \setminus L(O)$ and $y \in L(3O) \setminus L(2O)$ such that

$$\begin{aligned} L(O) &= \operatorname{span}_{\mathbb{C}}\{1\} \\ L(2O) &= \operatorname{span}_{\mathbb{C}}\{1, x\} \\ L(3O) &= \operatorname{span}_{\mathbb{C}}\{1, x, y\} \\ L(4O) &= \operatorname{span}_{\mathbb{C}}\{1, x, y, x^2\} \\ L(5O) &= \operatorname{span}_{\mathbb{C}}\{1, x, y, x^2, xy\}. \end{aligned}$$

The rational functions x^3 and y^2 both have a pole of order 6 at O, hence $y^2 - x^3$ has a pole of order at most 5 and is contained in $L(5O)$. It follows that there exists a $\mathbb{C}$-linear combination

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

2. Since E is a smooth curve, every rational map with domain E is a morphism. The degree $\deg\varphi$ is equal to

$$[\mathbb{C}(E) : \varphi^*\mathbb{C}(\mathcal{V}(F))] = [\mathbb{C}(E) : \mathbb{C}(x, y)]$$

and divides both $[\mathbb{C}(E) : \mathbb{C}(x)]$ and $[\mathbb{C}(E) : \mathbb{C}(y)]$. These degrees are equal to the degrees of the pole divisors $(x)_\infty = 2O$ and $(y)_\infty = 3O$, hence $\deg\varphi$ divides both 2 and 3 and must therefore be equal to 1[Silo9, p. 61, Corollary 3.1.1.]. ∎

An equation of the form (1.1) is said to be in in *long Weierstraß form*. Since we only deal with elliptic curves over the complex numbers it is possible to obtain a simpler model by first completing the square on the left-hand-side, i.e.

$$\begin{aligned} y^2 + a_1xy + a_3y &= y^2 + 2\frac{a_1x + a_3}{2}y + \left(\frac{a_1x + a_3}{2}\right)^2 - \left(\frac{a_1x + a_3}{2}\right)^2 \\ &= \left(y + \frac{a_1x + a_3}{2}\right)^2 - \left(\frac{a_1x + a_3}{2}\right)^2. \end{aligned}$$

We obtain a new equation and an isomorphism

$$\begin{array}{ccc} E & \longrightarrow & E' : Y'^2Z' = X'^3 + b_2X'^2Z' + b_4X'Z'^2 + b_6Z'^3 \\ (X : Y : Z) & \longmapsto & \left(X : Y - \frac{a_1X+a_3}{2} : Z\right) \end{array}.$$

A second simplification is given by a *Tschirnhaus transformation*

$$\left(x' - \frac{b_2}{3}\right)^3 + b_2\left(x' - \frac{b_2}{3}\right)^2 + b_4\left(x' - \frac{b_2}{3}\right) + b_6 = x''^3 + c_4x'' + c_6,$$

which yields another isomorphism

$$\begin{array}{ccc} E' & \longrightarrow & E'' \\ (X' : Y' : Z') & \longmapsto & \left(X' - \frac{b_2}{3} : Y' : Z'\right) \end{array}.$$

If we were to consider elliptic curves over different fields than $\mathbb{C}$, the above simplifications would still be possible as long as 2 and 3 are invertible. The simplified equation

$$Y^2Z = X^3 + AXZ^2 + BZ^3$$

is called a *short Weierstraß equation* [Silo9, p. 42ff]. As we have shown just now, every elliptic curve has a model given by a short Weierstraß equation. The question arises whether every curve given by a short Weierstraß equation is an elliptic curve?

Proposition 1.3.3. [Silo9, p. 59, Proposition 3.1.] Let E be the curve given by $Y^2Z = X^3 + AXZ^2 + BZ^3$, then the following are equivalent

1. E is an elliptic curve
2. E is smooth
3. The discriminant Δ of $x^3 + Ax + B$ is not 0.

Proof. 1 $\Longrightarrow$ 2. By definition.
2 $\Longrightarrow$ 3. Let $F(X, Y, Z) = Y^2Z - X^3 - AXZ^2 - BZ^3$ and suppose $X^3 + AX + B = (X - e_1)(X - e_2)^2$, then the system of equations

$$\left\{F(X, Y, Z), \frac{\partial F}{\partial X} = -3X^2 - AZ^2, \frac{\partial F}{\partial Y} = -2YZ, \frac{\partial F}{\partial Z} = Y^2 - 2AXZ - 3BZ^2\right\} \tag{1.2}$$

has the solution $(e_2 : 0 : 1)$.
$3 \implies 2$. Let $(x_0 : y_0 : z_0)$ be a singular point, that is, a solution of (1.2). If $z_0 = 0$, the other coordinates are 0 as well, which is not a point in $\mathbb{P}^2$ and we may assume that $z_0 = 1$. Solving the system for A and B gives

$$A = -3x_0^2 \text{ and } B = 2x_0^3$$

and it follows that

$$4A^3 + 27B^2 = 4(-3x_0^2)^3 + 27(2x_0^3)^2 = 0,$$

which is just Δ.
$2 \implies 1$. The Riemann-Roch theorem ensures that the degree of any differential is equal to $2g - 2$ and it suffices to show for one differential ω that $\deg \omega = 0$. Let e_1, e_2 and e_3 be the zeros of $x^3 + Ax + B$, then the rational function $x - e_i$ has a zero of order 2 at the point $P_i = (e_i : 0 : 1)$ and a pole of order 2 at O. It follows that

$$x - e_i = t_i^2,$$

where t_i is a uniformizing parameter at P_i and

$$\frac{1}{x} = t_O^2,$$

where t_O is a uniformizing parameter at O. We can compute

$$v_{P_i}(dx) = v_{P_i}(d(x - e_i)) = v_{P_i}(dt_i^2) = v_{P_i}(2t_i dt_i) = 1$$

and

$$v_O(dx) = v_O\left(x^2 d\frac{1}{x}\right) = v_O(t_O^{-4} dt_O^2) = v_O(t_O^{-3} dt_O) = -3,$$

since $0 = d\frac{x}{x} = d\frac{1}{x} - \frac{1}{x^2}dx$. It follows that $\deg((dx)) = 3 - 3 = 0$ and hence $g = 1$. ∎

Convention. From now on an elliptic curve is a curve of genus 1 given by a short Weierstraß equation.

With the previous Proposition we can now say that elliptic curves are parametrized by the points

$$(A, B) \in \mathbb{A}^2 \setminus \{4A^3 + 27B^2 \neq 0\}.$$

As it will turn out, there exists a "smaller", more canonical *moduli space*, which also parametrizes elliptic curves and has the property that isomorphic curves correspond to the same point (which the above space does not satisfy). Before we can construct this space, we need to know what a morphism of elliptic curves is.

Definition 1.3.4. [Silo9, p. 66] Let E and E' be elliptic curves. A morphism $\varphi\colon E \to E'$ is called *isogeny* or *morphism of elliptic curves*, if $\varphi(O) = O$.

Lemma 1.3.5. Let $\varphi\colon E \to E'$ be a non-constant morphism of elliptic curves, then φ is surjective and has finite degree.

Proof. If φ is non-constant it induces a morphism of $\mathbb{C}$-algebras

$$\varphi^*\colon \begin{cases} \mathbb{C}(E') & \longrightarrow & \mathbb{C}(E) \\ f & \longmapsto & f \circ \varphi \end{cases}$$

and a field extension $\mathbb{C}(E)/\varphi^*\mathbb{C}(E')$. Since both $\mathbb{C}(E)$ and $\mathbb{C}(E')$ have transcendence degree 1 and are finitely generated (for example by the rational functions x and y in Proposition 1.3.2), the extension $\mathbb{C}(E)/\varphi^*\mathbb{C}(E')$ is finite and algebraic.

For $P \in E'$, there exists a rational function $f \in L(2O) \setminus L(O)$ by the Riemann-Roch theorem and it follows that its inverse f^{-1} has a single zero at P of order 2. The pull-back $f^{-1} \circ \varphi$ must have a zero, since otherwise it would be constant, which is impossible by the injectivity of φ^*. Thus, if $Q \in E$ is a zero of $f^{-1} \circ \varphi$, then $\varphi(Q)$ is a zero of f^{-1}, which is only possible if $\varphi(Q) = P$.[1] ∎

Let us now introduce the group law of an elliptic curve. We will try to do this in a most economical fashion, first by giving a bijection of an elliptic curve with a group constructed from it and then showing that the induced group structure is given by a morphism.

Definition 1.3.6. [Sil09, p. 28] The *Picard group of divisors of degree* 0 of a smooth algebraic curve E is defined as

$$\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/(\mathbb{C}(E)^\times).$$

Let $\varphi\colon E \to E'$ be a morphism, then the push-forward of divisors

$$\varphi_*\colon \begin{cases} \mathrm{Pic}^0(E) & \longrightarrow & \mathrm{Pic}^0(E') \\ \sum_i n_i P_i & \longmapsto & \sum_i n_i \varphi(P_i) \end{cases}$$

turns the Picard group into a functor from the category of smooth algebraic curves to the category of abelian groups.

Proposition 1.3.7. [Sil09, p. 61ff, Prop. 3.4.d] Let E be an elliptic curve and $O \in E$ the point at infinity, then

$$\Phi\colon \begin{cases} E & \longrightarrow & \mathrm{Pic}^0(E) \\ P & \longmapsto & P - O + (\mathbb{C}(E)^\times) \end{cases}$$

is a bijection.

Proof. First, note that $\deg(P - O) = 0$ and hence Φ is well-defined. For the injectivity, suppose there exist points P and P' such that

$$P - O + (f) = P' - O + (f'),$$

where $f, f' \in \mathbb{C}(E)^\times$. Then $P - P' = \left(\frac{f}{f'}\right)$ and hence the rational function $\frac{f}{f'}$ has, if $P \neq P'$, a single, simple zero P, which is impossible since $L(P) = \mathbb{C}$. It follows that $P = P'$ and Φ is injective. Next, let D be a divisor of degree 0, then $D + O$ has degree 1 and is equivalent to an effective divisor of degree 1, i.e. a prime divisor P. In other words

$$D + (\mathbb{C}(E)^\times) = P - O + (\mathbb{C}(E)^\times)$$

and surjectivity follows. ∎

[1] This argument is a variation of [Oss, p. 7, Theorem 6.1.]

This bijection endows the *set* E with a group structure via

$$\mu\colon \begin{cases} E\times E & \longrightarrow & E \\ (P,Q) & \longmapsto & \Phi^{-1}\left(\Phi(P)+\Phi(Q)\right) \end{cases}$$

and

$$\iota\colon \begin{cases} E & \longrightarrow & E \\ P & \longmapsto & \Phi^{-1}(-\Phi(P)) \end{cases}$$

with the neutral element O. To show that μ and ι are morphisms we need the notion of a *hyperplane divisor*.

Definition 1.3.8. [Mir95, p. 135ff] Let $H \subseteq \mathbb{P}^2$ be a hyperplane given by a linear homogeneous polynomial $h \in \mathbb{C}[X,Y,Z]$. For an elliptic curve E the hyperplane divisor $(H \cap E)$ is defined via

$$v_P((H\cap E)) = \begin{cases} 0 & \text{if } P \notin H\cap E \\ v_P\left(\frac{h}{g}\right) & \text{where } g \text{ is any linear homogeneous polynomial such that } g(P)\neq 0 \end{cases}.$$

Note that the valuation at a point $P \in H \cap E$ is well-defined since

$$v_P\left(\frac{h}{g}\right) = v_P\left(\frac{hg'}{gg'}\right) = v_P\left(\frac{h}{g'}\right) + v_P\left(\frac{g'}{g}\right) = v_P\left(\frac{h}{g'}\right).$$

Lemma 1.3.9. [Sil09, p. 63, Prop. 3.4.e] Let E be an elliptic curve, then any two hyperplane divisors on E are equivalent.

Proof. Let h and h' be two linear homogeneous polynomials and denote by H and H' the corresponding hyperplanes. For $P \in E$ and g linear homogeneous polynomial with $h(P) \neq 0$, we compute

$$v_P\left(\frac{h}{h'}\right) = v_P\left(\frac{hg}{h'g}\right) = v_P\left(\frac{h}{g}\right) - v_P\left(\frac{h'}{g}\right) = v_P\left((H\cap E) - (H'\cap E)\right).$$

It follows that $(H \cap E) - (H' \cap E) = \left(\frac{h}{h'}\right)$. ∎

Using hyperplane divisors we can construct the well-known geometric chord and tangent addition of points on an elliptic curve $E : Y^2Z = X^3 + AXZ + BZ^3$. First, let us compute the degree of one (and hence of all) hyperplane divisors. Let $H : Y = 0$, then

$$H \cap E = \{P_1, P_2, P_3\},$$

where $\frac{X}{Z}(P_i)$ is a root of $x^3 + Ax + B$, and we now know that every hyperplane intersects E in exactly three points (counted with multiplicity). For the two points P and Q to be added, we define the hyperplane $H : h = 0$ as the hyperplane spanned by P and Q if $P \neq Q$, or as the tangent hyperplane at P if $P = Q$. In the latter case, we find the equation for $h = aX + bY + cZ$ by requiring

$$\begin{aligned} h(P) &= 0 \\ \frac{\partial h}{\partial X}(P) &= a = \frac{\partial f}{\partial X}(P) \\ \frac{\partial h}{\partial Y}(P) &= b = \frac{\partial f}{\partial Y}(P) \\ \frac{\partial h}{\partial Z}(P) &= c = \frac{\partial f}{\partial Z}(P). \end{aligned}$$

Note that this will give the coefficients only up to a scaling factor but since $\mathcal{U}(aX + bY + cZ) = \mathcal{U}(\lambda aX + \lambda bY + \lambda cZ)$, this does not change the resulting hyperplane H. Given the points P and Q and the hyperplane H, we find a third point R of $H \cap E$. Let H' be the hyperplane spanned by R and O (again taking the tangent hyperplane if $R = O$) and denote by R^* the third point in $H' \cap E$. Since $(H \cap E) \sim (H' \cap E)$, we obtain

$$P + Q + R \sim R + R^* + O.$$

Eliminating R and subtracting $2O$ from both sides gives

$$(P - O) + (Q - O) \sim (R^* - O),$$

respectively $\Phi(P) + \Phi(Q) = \Phi(R^*)$. Finally, since finding the third intersection point of $H \cap E$ is given by rational functions F, G and H, μ and ι are a rational maps defined everywhere and therefore morphisms[Sil09, p. 63, Prop. 3.4.e].

Now that the group law of elliptic curves is established we can say what this means for isogenies.

Proposition 1.3.10. [Sil09, p. 71, Theorem 4.8.] Let $\varphi\colon E \to E'$ be an isogeny, then φ is a group homomorphism.

Proof. Consider the commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E' \\ \downarrow{\scriptstyle \Phi} & & \downarrow{\scriptstyle \Phi'} \\ \mathrm{Pic}^0(E) & \xrightarrow{\varphi_*} & \mathrm{Pic}^0(E') \end{array},$$

where the vertical maps and φ_* are group homomorphisms and hence $\varphi = \Phi'^{-1} \circ \varphi_* \circ \Phi$ is also a group homomorphism. ∎

It follows that for two elliptic curves E and E', the set $\mathrm{Hom}(E, E')$ is an abelian group and the set of endomorphisms $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ is a ring with composition as multiplication.[Sil09, p. 67]

1.4. The j-invariant of an Elliptic Curve

We return to the problem of finding a moduli space for elliptic curves. Our earlier attempt at a parameter space $\mathbb{A}^2 \setminus \{4A^3 + 27B^2\}$ has the disadvantage that different points correspond to isomorphic elliptic curves, e.g. $(0, 1)$ and $(0, 2)$. Here we use the *j-invariant* to construct the "best possible" moduli space, in which every point corresponds to exactly one isomorphism class of elliptic curves.

Definition 1.4.1. Let $E : Y^2Z = X^3 + AXZ^2 + BZ^3$ be an elliptic curve. The j-invariant of E is defined as

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

Theorem 1.4.2. [Sil09, p. 45ff, Prop. 1.4.]

1. Let E and E' be elliptic curves, then $E \cong E'$ if and only if $j(E) = j(E')$.

2. For every $j_0 \in \mathbb{C}$ there exists an elliptic curve E_0 such that $j(E_0) = j_0$.

Remark. More conceptually the theorem states that the map

$$j\colon \begin{cases} \mathrm{Ell}/\cong & \longrightarrow & \mathbb{C} \\ E & \longmapsto & j(E) \end{cases}$$

is well-defined and bijective.

Proof. 1. Let $E : Y^2Z = X^3 + AXZ^2 + BZ^3$ and $E' : Y'^2Z' = X'^3 + A'X'Z'^2 + B'Z'^3$ elliptic curves and let $\varphi\colon E \to E'$ be an isomorphism, then φ restricted to the 2-torsion points is an isomorphism

$$\varphi\colon \begin{cases} E[2] & \longrightarrow & E'[2] \\ (e_i : 0 : 1) & \longmapsto & (e_i' : 0 : 1) \end{cases},$$

where e_1, e_2 and e_3 are the roots of $x^3 + Ax + B$ and similarly e_1', e_2' and e_3' are the roots of $x'^3 + A'x' + B'$. The function

$$\varphi^*\left(\frac{X'}{Z'} - e_i'\right)$$

has a zero at $(e_i : 0 : 1)$ and a pole at O, each of order 2 and hence

$$\varphi^*\left(\frac{X'}{Z'}\right) = \lambda\frac{X}{Z},$$

and similarly

$$\varphi^*\left(\frac{Y'}{Z'}\right) = \mu\frac{Y}{Z},$$

for some $\lambda, \mu \in \mathbb{C}^\times$. It follows that

$$0 = \varphi^*(0) = \varphi^*\left(\left(\frac{Y'}{Z'}\right)^2 - \left(\frac{X'}{Z'}\right)^3 - A'\frac{X'}{Z'} - B'\right) = \mu^2\left(\frac{Y}{Z}\right)^2 - \lambda^3\left(\frac{X}{Z}\right)^3 - A'\lambda\frac{X}{Z} - B'$$

and we compare this with the defining equation of E to obtain $\lambda A' = \mu^2 A$, $B' = \mu^2 B$ and $\lambda^3 = \mu^2$ and hence

$$j(E') = 1728\frac{4A'^3}{4A'^3 + 27B'^2} = 1728\frac{4\frac{\mu^6}{\lambda^3}A^3}{4\frac{\mu^6}{\lambda^3}A^3 + 27\mu^4B^2} = 1728\frac{4A^3}{4A^3 + 27B^2} = j(E).$$

Now, suppose that $j(E) = j(E') \neq 0, 1728$, then algebraic manipulation of the equation $j(E) = j(E')$ yields

$$\frac{A^3}{A'^3} = \frac{B^2}{B'^2} \tag{1.3}$$

and we choose $u \in \mathbb{C}^\times$ such that $A = u^4A'$ and $B = u^6B'$. If $j(E) = j(E') = 0$, we choose $u \in \mathbb{C}^\times$ such that $B = u^6B'$ and finally, if $j(E) = j(E') = 1728$, we choose $u \in \mathbb{C}^\times$ such that $A = u^4A'$. Then

$$\begin{array}{ccc} E & \longrightarrow & E' \\ (X : Y : Z) & \longmapsto & \left(\frac{X}{u^2} : \frac{Y}{u^3} : Z\right) \end{array}$$

is an isomorphism of E and E'.
2. If $j_0 \in \mathbb{C} \setminus \{0, 1728\}$, the curve

$$E_0 : Y^2Z = X^3 - \frac{j_0}{48(j_0 - 1728)} XZ^2 + \frac{j_0}{864(j_0 - 1728)} Z^3$$

has j-invariant j_0 and is also defined over $\mathbb{Q}(j_0)$. If $j_0 \in \{0, 1728\}$ curves $E_0 : Y^2Z = X^3 + Z^3$ and $E_0 : Y^2Z = X^3 + XZ^2$ have j-invariant 0 and 1728, respectively. ■

2. Complex Tori

The goal of this chapter is to establish a theory parallel to the theory of elliptic curves, where the role of smooth algebraic curves is assumed by Riemann surfaces, elliptic curves correspond to complex tori and we prove the corresponding results:

1. The isogenies between complex tori form abelian groups (Proposition 1.3.10 and the following discussion),
2. The field of meromorphic functions on a complex torus (Proposition 1.3.2),
3. The j-invariant of a complex torus/lattice is an invariant (Theorem 1.4.2).

Where we used the purely algebraic Riemann-Roch theorem before, the approach of this chapter only requires a little topology and facts from complex analysis and while I make some omissions, these are minor technicalities.

2.1. Riemann Surfaces

Definition 2.1.1. [Mir95, p. 1] Let X be a topological space and $U \subseteq X$ open. A homeomorphism

$$\varphi\colon U \to V,$$

where V is an open subset of $\mathbb{C}$, is called a *chart*. Two charts $\varphi\colon U \to V$ and $\varphi'\colon U' \to V'$ are *compatible* if either $U \cap U' = \emptyset$ or the *transition function*

$$\varphi' \circ \varphi^{-1}\colon \varphi(U \cap U') \to \varphi'(U \cap U')$$

is holomorphic. Note that this relation is symmetric by the inverse function theorem.

Convention. Phrases like "Let X be a topological space and $\varphi\colon U \to V$ a chart (on X)" carry the implied meaning that $U \subseteq X$ and $V \subseteq \mathbb{C}$ are open.

Definition 2.1.2. [Mir95, p. 3ff] Let X be a topological space. A set of pairwise compatible charts $\mathcal{A} = \{\varphi_i\colon U_i \to V_i \mid i \in I\}$ is called *atlas* if $X = \bigcup_{i\in I} U_i$.

Two atlases $\mathcal{A}$ and $\mathcal{A}'$ are *compatible* if all charts in $\mathcal{A}$ are compatible with all charts in $\mathcal{A}'$. Equivalently, $\mathcal{A}$ and $\mathcal{A}'$ are compatible if $\mathcal{A} \cup \mathcal{A}'$ is an atlas on X. Using Zorn's lemma, there exists for every atlas $\mathcal{A}$ a unique maximal atlas $\overline{\mathcal{A}}$ such that all atlases compatible with $\mathcal{A}$ are contained in $\overline{\mathcal{A}}$.

Definition 2.1.3. [Mir95, p. 4, Definition 1.18.] A topological space X together with an atlas $\mathcal{A}$ is called *Riemann surface* if X is connected, Hausdorff and has a countable basis.

Example. [Mir95, p. 4, Example 1.19.] The affine line $\mathbb{C}$ with atlas comprising the chart $\mathrm{id}\colon \mathbb{C} \to \mathbb{C}$ is a Riemann surface.

Definition 2.1.4. [Mir95, p. 38, Definition 3.1.] Let X and Y be Riemann surfaces and $x \in X$. A function $F\colon X \to Y$ is called *holomorphic at x* if there exist charts $\varphi\colon U \to V$ and $\varphi'\colon U' \to V'$ with $x \in U$ and $F(x) \in U'$ such that

$$\varphi' \circ F \circ \varphi^{-1}\colon \varphi(U \cap f^{-1}(U')) \to V'$$

is holomorphic at $\varphi(x)$. The function F is called *morphism (of Riemann surfaces)* if it is holomorphic at every point in X.

Remark. [Mir95, p. 39, Lemma 3.3.a., Lemma 3.5.b.] Since the transition functions between charts are by definition holomorphic, a function F is holomorphic at $x \in X$ with respect to φ and φ' if and only if it is holomorphic with respect to any other charts (at x and $f(x)$).

Moreover, the identity map and the composition of two morphisms are again morphisms and hence Riemann surfaces with morphisms form a category RS.

Proposition 2.1.5. Let $F\colon X \to Y$ be a bijective morphism, then $F^{-1}\colon Y \to X$ is also a morphism.

Proof. [Mir95, p. 40, Proposition 3.9.] ∎

Definition 2.1.6. [Mir95, p. 39, Example 3.4.] Let X be a Riemann surface. A morphism $f\colon X \to \mathbb{C}$ is called *holomorphic function (on X)*. Concretely, f is a function such that for every chart $\varphi\colon U \to V$ on X, the composition $f \circ \varphi^{-1}\colon V \to \mathbb{C}$ is holomorphic.

Lemma 2.1.7. Let X be a compact Riemann surface and $f\colon X \to \mathbb{C}$ a holomorphic function, then f is constant.

Proof. [Mir95, p. 29, Proposition 1.37.] ∎

Definition 2.1.8. [Mir95, p. 42] Let X be a Riemann surface. A function $f\colon X \to \mathbb{C} \cup \{\infty\}$ is called *meromorphic at $x \in X$* if there exists an open neighbourhood U of x such that $f \restriction_U = \frac{g}{h}$, where g and h are holomorphic functions with $h \not\equiv 0$. The function f is called *meromorphic* if it is meromorphic at every point of X.

Immediately we see that holomorphic functions are meromorphic and that the set of meromorphic functions on a Riemann surface X form a field denoted $\mathcal{M}(X)$. A morphism $F\colon X \to Y$ of Riemann surfaces induces a morphism of fields

$$F^*\colon \left\{ \begin{array}{ccc} \mathcal{M}(Y) & \longrightarrow & \mathcal{M}(X) \\ f & \longmapsto & f \circ F \end{array} \right. .$$

We will pursue this further when we investigate elliptic functions.

2.2. Complex Tori

Definition 2.2.1. A subgroup $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subseteq \mathbb{C}$ is called a *lattice* if $\{\omega_1, \omega_2\}$ is an $\mathbb{R}$-basis of $\mathbb{C}$. For a lattice Λ the quotient group $\mathbb{C}/\Lambda$ endowed with the complex topology is called a *complex torus*.

Lemma 2.2.2. [Mir95, p. 9] Let Λ be a lattice. The space $\mathbb{C}/\Lambda$ is connected, Hausdorff, has a countable basis and the quotient map $\pi\colon \mathbb{C} \to \mathbb{C}/\Lambda$ is a covering.

Proof. In order to see that $\mathbb{C}/\Lambda$ is connected, suppose $\mathbb{C}/\Lambda = U_0 \cup U_1$ with U_0 and U_1 pairwise disjoint and open. Then the preimages $\pi^{-1}(U_0)$ and $\pi^{-1}(U_1)$ are open and disjoint and cover $\mathbb{C}$, which is impossible. For the Hausdorff property, let $z + \Lambda \neq z' + \Lambda$ be two points on $\mathbb{C}/\Lambda$, then $z \notin z' + \Lambda$ and since $\Lambda \subseteq \mathbb{C}$ is discrete, z is also not a limit point of $z' + \Lambda$. It follows that there exists an $\varepsilon > 0$ such that $B_\varepsilon(z) \cap B_\varepsilon(z' + \omega) = \emptyset$ for all $\omega \in \Lambda$ and the images of $B_\varepsilon(z)$ and any $B_\varepsilon(z' + \omega)$ separate $z + \Lambda$ and $z' + \Lambda$ in $\mathbb{C}/\Lambda$. Finally, the countable-basis-property follows immediately from the quotient map $\pi\colon \mathbb{C} \to \mathbb{C}/\Lambda$ being an open map.

Let $\delta = \min_{\omega \neq \omega' \in \Lambda} |\omega - \omega'|$ be the length of the shortest lattice vector and let $z \in \mathbb{C}$. The set

$$\{B_{\frac{\delta}{4}}(z + \omega) \mid \omega \in \Lambda\}$$

consists of pairwise disjoint open balls, each of which is homeomorphic to $B_{\frac{\delta}{4}}(z) + \Lambda \subseteq \mathbb{C}/\Lambda$ via π. Since π is open and surjective, every point in $\mathbb{C}/\Lambda$ has such an evenly covered open neighbourhood. ∎

Proposition 2.2.3. [Mir95, p. 9] Let Λ be a lattice. The space $\mathbb{C}/\Lambda$ can be equipped uniquely with a Riemann surface structure such that the quotient map $\pi\colon \mathbb{C} \to \mathbb{C}/\Lambda$ is a morphism.

Proof. We define charts on $\mathbb{C}/\Lambda$ for all evenly covered open subsets $U \subseteq \mathbb{C}/\Lambda$ as

$$\varphi\colon U \to \tilde{U},$$

where $\tilde{U}$ is any sheet above U. The transition functions for different U and sheets $\tilde{U}$ are translations and hence these are compatible and form an atlas. Let now $z \in \mathbb{C}$, U an evenly covered neighbourhood of $\pi(z)$ and $\tilde{U}$ the sheet above U containing z, then

$$\varphi \circ \pi \circ \mathrm{id}^{-1} = \mathrm{id}\colon \tilde{U} \to \tilde{U}$$

is holomorphic at $\mathrm{id}(z) = z$ and hence π is a morphism.

Finally, suppose there exists another atlas $\mathcal{A}$ on $\mathbb{C}/\Lambda$ such that $\pi\colon \mathbb{C} \to \mathbb{C}/\Lambda$ is a morphism. Let $\tilde{U}$ be a sheet above U, then

$$\pi\colon \tilde{U} \to U$$

is a bijective morphism and hence its inverse $\varphi\colon U \to \tilde{U}$ is compatible with $\mathcal{A}$ and it follows that $\mathcal{A}$ itself is compatible with the atlas constructed above. ∎

Definition 2.2.4. Let $\mathbb{C}/\Lambda'$ be another complex torus. A morphism $\varphi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$, which maps $0 + \Lambda$ to $0 + \Lambda'$, is called *isogeny*.

Remark. Clearly the identity and the composition of two isogenies are isogenies. It follows that the complex tori together with isogenies form a subcategory of the category of Riemann surfaces called Tori.

Theorem 2.2.5. [Silo9, p. 171ff, Theorem 4.1.] Let $\varphi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ be an isogeny, then there exists a unique holomorphic function $\tilde{\varphi}(z) = \alpha z$, where $\alpha \in \mathbb{C}$ such that $\alpha\Lambda \subseteq \Lambda'$, and

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \hookrightarrow & \mathbb{C} & \xrightarrow{\pi_\Lambda} & \mathbb{C}/\Lambda & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tilde{\varphi}\restriction_\Lambda} & & \downarrow{\scriptstyle \tilde{\varphi}} & & \downarrow{\scriptstyle \varphi} & & \\ 0 & \longrightarrow & \Lambda' & \hookrightarrow & \mathbb{C} & \xrightarrow{\pi_{\Lambda'}} & \mathbb{C}/\Lambda' & \longrightarrow & 0 \end{array} \tag{2.1}$$

is a commutative diagram of abelian groups.

Proof. The existence of the lift $\tilde{\varphi}$ follows from Lemma B.0.4, where $\tilde{\varphi}$ is locally given by the composition of a chart, φ and the projection. All of these are morphisms and hence $\tilde{\varphi}$ is also a morphism.

Let $\omega \in \Lambda$, then $\tilde{\varphi}(z+\omega) - \tilde{\varphi}(z) \in \Lambda'$ for all $z \in \mathbb{C}$. Since $\tilde{\varphi}(z+\omega) - \tilde{\varphi}(z)$ is a holomorphic function with discrete image, it must be constant and its derivative (with respect to z) satisfies

$$\tilde{\varphi}'(z+\omega) - \tilde{\varphi}'(z) = 0.$$

In other words, $\tilde{\varphi}'(z)$ is a holomorphic Λ-invariant function and $\sup_{z\in\mathbb{C}}|\tilde{\varphi}(z)|$ is already assumed in the closure of

$$F = \{x\omega_1 + y\omega_2 \mid x, y \in [0,1)\}$$

and hence $\tilde{\varphi}'(z)$ is constant by Liouville's theorem [Silo9, p. 161, Proposition 2.1.]. It follows that $\tilde{\varphi}$ is a linear polynomial in z and since $\tilde{\varphi}(0) = 0$, it has the form $\tilde{\varphi}(z) = \alpha z$ for some $\alpha \in \mathbb{C}$. Since $\pi_{\Lambda'} \circ \tilde{\varphi}(\Lambda) = 0$, the image $\tilde{\varphi}(\Lambda) = \alpha\Lambda$ is contained in Λ'. ∎

Corollary 2.2.6. [Silo9, p. 171ff, Theorem 4.1.] There is an isomorphism of abelian groups

$$\Phi\colon \left\{ \begin{array}{ccc} \mathrm{Hom}_{\mathrm{Tori}}(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda') & \longrightarrow & \{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda'\} \\ \varphi & \longmapsto & \frac{\tilde{\varphi}}{z} \end{array} \right. .$$

Proof. The existence and injectivity of this map follows immediately from Theorem 2.2.5. To show that Φ is surjective, let $\alpha \in \mathbb{C}$ such that $\alpha\Lambda \subseteq \Lambda'$, U be an evenly covered open subset of $\mathbb{C}/\Lambda$ and $\tilde{U}$ a sheet above. The restriction $\tilde{\pi}\colon \tilde{U} \to U$ of the quotient map is an isomorphism of Riemann surfaces and hence the map $(z+\Lambda \mapsto \alpha z + \Lambda')$ is on U given by $\pi_{\Lambda'} \circ (z \mapsto \alpha z) \circ \tilde{\pi}^{-1}$ and thus a morphism of Riemann surfaces. Finally, let $\varphi, \psi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ be isogenies. Then the holomorphic function

$$\widetilde{\varphi+\psi} - \tilde{\varphi} - \tilde{\psi}$$

has its image lying inside the discrete set Λ' and therefore must be constant. Since 0 is mapped to 0, the function is equal to 0 and the homomorphism property follows. ∎

Corollary 2.2.7. [Silo9, p. 173, Corollary 4.1.1.] Let $\varphi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ be an isogeny, then the kernel $\ker\varphi$ is isomorphic to the cokernel $\operatorname{coker}\tilde{\varphi}\restriction_\Lambda$. In particular φ is an isomorphism if $\Lambda = \Phi(\varphi)\Lambda'$ and we call two lattices *homothetic* if there exists an $\alpha \in \mathbb{C}^\times$ such that $\Lambda = \alpha\Lambda'$.

Proof. Apply the snake lemma to (2.1). ∎

2.3. Elliptic Functions

For a torus $\mathbb{C}/\Lambda$ we will now determine the field of meromorphic functions $\mathcal{M}(\mathbb{C}/\Lambda)$. Note that the morphism of fields

$$\begin{array}{ccc} \mathcal{M}(\mathbb{C}/\Lambda) & \longrightarrow & \mathcal{M}(\mathbb{C}) \\ f & \longmapsto & f \circ \pi \end{array}$$

maps the meromorphic functions on a torus isomorphically to

$$\mathbb{C}(\Lambda) := \{f \in \mathcal{M}(\mathbb{C}) \mid \forall z \in \mathbb{C} \forall \omega \in \Lambda : f(z+\omega) = f(z)\}$$

and such functions are called *elliptic functions (with respect to Λ).*

Definition 2.3.1. [Sil09, p. 165] Let Λ be a lattice, then the Weierstraß $\wp$-function is defined (formally, for now) as

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{0 \neq \omega \in \Lambda} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right). \tag{2.2}$$

In order to show that $\wp$ is a meromorphic function we need the following lemma:

Lemma 2.3.2. [Sil09, p. 165, 178, Theorem 3.1.a., Exercise 6.2.] Let Λ be a lattice and s a real number greater than 2, then

$$G_s = \sum_{0 \neq \omega \in \Lambda} \omega^{-s}$$

converges absolutely.

Proof. We split G_s into two parts

$$\begin{aligned} G_s &= \sum_{0 \neq \omega \in \Lambda} \omega^{-s} \\ &= \sum_{\substack{0 \neq \omega \in \Lambda \\ |\omega| < 1}} \omega^{-s} + \sum_{\substack{0 \neq \omega \in \Lambda \\ |\omega| \geq 1}} \omega^{-s}. \end{aligned}$$

and note that the former has only finitely many terms. For the latter we let $r \in \mathbb{N}$ and consider the annulus $A_r = \{z \in \mathbb{C} \mid r \leq |z| < r+1\}$, then

$$\sum_{\substack{0 \neq \omega \in \Lambda \\ |\omega| \geq 1}} |\omega|^{-s} = \sum_{r=1}^{\infty} \sum_{\omega \in A_r \cap \Lambda} |\omega|^{-s} \leq \sum_{r=1}^{\infty} \sum_{\omega \in A_r \cap \Lambda} r^{-s}. \tag{2.3}$$

Let N_r be the number of lattice points in A_r and let $\delta = \min_{\omega \neq \omega' \in \Lambda} |\omega - \omega'|$ be the length of the shortest lattice vector in Λ. For every lattice point in A_r we put a ball of radius $\rho = \min\{\frac{\delta}{2}, \frac{1}{2}\}$ around it. These balls may extend beyond A_r but they certainly lie inside the larger annulus $\{z \in \mathbb{C} \mid r-1 \leq |z| < r+2\}$ and hence the area of all balls can be estimated as

$$N_r \rho^2 \pi \leq (r+2)^2 \pi - (r-1)^2 \pi = 6r\pi - 3\pi$$

and consequently $N_r \leq \frac{6}{\rho^2} r - \frac{3}{\rho^2}$. We may use this to further estimate (2.3) as follows

$$\sum_{r=1}^{\infty} \sum_{\omega \in A_r \cap \Lambda} r^{-s} = \sum_{r=1}^{\infty} N_r r^{-s} \leq \frac{6}{\rho^2} \sum_{r=1}^{\infty} r^{-s+1} - \frac{3}{\rho^2} \sum_{r=1}^{\infty} r^{-s}.$$

Both sums converge since $s > 2$. ∎

Corollary 2.3.3. Let Λ be a lattice and $2k+1$ an odd natural number, then $G_{2k+1} = 0$.

Proof. All summands come as pairs $\omega^{-(2k+1)}$, $-\omega^{-(2+1)}$ and since the summands can be rearranged, it follows that $G_{2k+1} = 0$. ∎

Theorem 2.3.4. [Cox89, p. 200ff, Theorem 10.1.] Let Λ be a lattice. The series

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{0 \neq \omega \in \Lambda} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

defines an even elliptic function with respect to Λ and has a pole of order 2 at every lattice point.

Proof. Let $\Omega \subseteq \mathbb{C} \setminus \Lambda$ be a compact set and $R = 2 \max_{z \in \Omega} |z|$, then

$$\wp(z;\Lambda) = \sum_{\substack{\omega \in \Lambda \\ |\omega| < R}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) + \sum_{\substack{\omega \in \Lambda \\ |\omega| \geq R}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right),$$

where the first sum is a finite sum. For the second sum we rearrange the absolute value of a summand

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right| = \left| \frac{\omega^2 - (z-\omega)^2}{\omega^2 (z-\omega)^2} \right| = \left| \frac{z(2\omega - z)}{\omega^2 (z-\omega)^2} \right|.$$

and use the triangle inequality to obtain

$$\left| \frac{z(2\omega - z)}{\omega^2 (z-\omega)^2} \right| \leq \frac{|z|(2|\omega| + |z|)}{|\omega|^2 (|\omega| - |z|)^2} \leq \frac{|z| \frac{5}{2} |\omega|}{|\omega|^2 (\frac{1}{2}|\omega|)^2} = |z| \frac{10}{|\omega|^3},$$

since for $z \in \Omega$, $|z| \leq \frac{1}{2} R \leq \frac{1}{2} |\omega|$. The sum

$$\sum_{0 \neq \omega \in \Lambda} \frac{1}{|\omega|^3}$$

converges by Lemma 2.3.2 and hence $\wp(z;\Lambda)$ converges absolutely and uniformly on every compact $\Omega \subseteq \mathbb{C} \setminus \Lambda$ by the Weierstraß M-test.

Since $\wp$ converges absolutely, interchanging $z \mapsto -z$ in the definition does not change the function, hence $\wp$ is even. In order to show that $\wp$ is elliptic, consider its derivative, which can be computed termwise as

$$\wp'(z;\Lambda) = -2 \sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}. \tag{2.4}$$

Similarly to before, this sum is absolutely and uniformly convergent on compact subsets of $\mathbb{C} \setminus \Lambda$ and hence holomorphic on $\mathbb{C} \setminus \Lambda$. Substituting $z \mapsto z + \omega_0$ for some $\omega_0 \in \Lambda$ does not change the series, hence $\wp'(z;\Lambda)$ is an elliptic function. For $\omega_0 \in \Lambda$ consider the derivative

$$(\wp(z+\omega_0;\Lambda) - \wp(z;\Lambda))' = \wp'(z+\omega_0;\Lambda) - \wp'(z;\Lambda),$$

which is 0 since $\wp'$ is elliptic and hence $\wp(z+\omega_0;\Lambda) - \wp(z;\Lambda) = c \in \mathbb{C}$. Specializing z to $-\frac{\omega_0}{2}$ gives

$$c = \wp\left(-\frac{\omega_0}{2};\Lambda\right) - \wp\left(-\frac{\omega_0}{2};\Lambda\right) = 0,$$

since $\wp$ is even. It follows that $\wp(z+\omega_0;\Lambda) = \wp(z;\Lambda)$ and hence $\wp$ is elliptic. Lastly, by the definition of $\wp(z;\Lambda)$, it has a pole of order 2 at 0 and hence at every lattice point. ∎

Corollary 2.3.5. [Cox89, p. 202, 216, Exercise 10.2.] Let Λ be a lattice. The derivative of the Weierstraß $\wp$ function is an odd, elliptic function with poles of order three at every lattice point.

Lemma 2.3.6. Let f be an elliptic function with respect to a lattice Λ, then

1. If f is holomorphic, it is constant.
2. $\sum_{z\in F} \operatorname{Res}_z(f) = \sum_{z\in F} v_z(f) = 0$.
3. If f is non-constant, it has at least 2 poles in F (counted with multiplicity).

Proof. [Silo9, p. 162ff, Theorem 2.2., Corollary 2.3.] ∎

Theorem 2.3.7. [Huso4, p. 172ff, Theorem 3.3] Let Λ be a lattice, then $\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z;\Lambda), \wp'(z;\Lambda))$.

Proof. Since $\wp(z;\Lambda)$ and $\wp'(z;\Lambda)$ are elliptic functions only one inclusion has to be shown. Let f be an elliptic function, then

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

is a decomposition into an even and an odd elliptic function. Moreover if $f(z)$ is an odd elliptic function, $f(z)\wp'(z;\Lambda)$ is even and it suffices to show that every even elliptic function is in $\mathbb{C}(\wp(z;\Lambda))$. Suppose now that $f(z)$ is an even elliptic function, then $v_0(f) = 2m$ and hence $f(z)\wp(z;\Lambda)^m$ is an even elliptic function holomorphic and non-zero at every point in Λ.

The poles and zeros of $f(z)\wp(z;\Lambda)^m$ in F come in pairs ω, ω' such that $\omega + \omega' \in \Lambda$ since f is even. If $\omega \not\equiv \omega' \mod \Lambda$, we multiply $f(z)\wp(z;\Lambda)^m$ with a factor

$$f_\omega(z) = (\wp(z;\Lambda) - \wp(\omega;\Lambda))^{v_\omega(f)}$$

such that $v_\omega(f(z)f_\omega(z)) = v_{\omega'}(f(z)f_\omega(z)) = 0$. If $\omega \equiv \omega' \mod \Lambda$, the order of $f(z)\wp(z;\Lambda)^m$ at $\omega = \omega'$ is even and we multiply $f(z)\wp(z;\Lambda)^m$ with

$$f_\omega(z) = (\wp(z;\Lambda) - \wp(\omega;\Lambda))^{\frac{v_\omega(f)}{2}}.$$

Similarly, the product $f(z)\wp(z;\Lambda)^m f_\omega(z)$ is holomorphic and non-zero at ω and it follows that

$$f(z)\wp(z;\Lambda)^m \prod_\omega f_\omega(z)$$

is a holomorphic elliptic function and thus constant by Lemma 2.3.6. ∎

Lemma 2.3.8. [Cox89, p. 202ff, Lemma 10.3.] Let Λ be a lattice. The Laurent expansion of $\wp(z;\Lambda)$ near 0 is

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(\Lambda)z^{2n}.$$

Proof. For $|z|$ sufficiently small we may insert the Taylor expansion

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

into the definition of $\wp(z;\Lambda)$, i.e.

$$\begin{aligned}\wp(z;\Lambda) &= \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus\{0\}}\sum_{n=1}^{\infty}(n+1)\frac{z^n}{\omega^{n+2}} \\ &= \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}(\Lambda)z^{2n},\end{aligned}$$

where we used that $G_{\text{odd}}(\Lambda) = 0$ by Corollary 2.3.3. ∎

Proposition 2.3.9. [Cox89, p. 200ff, Theorem 10.1.] Let Λ be a lattice. The Weierstraß $\wp$ function and its derivative $\wp'$ satisfy the algebraic relation

$$\wp'(z;\Lambda)^2 = 4\wp(z;\Lambda)^3 - g_2(\Lambda)\wp(z;\Lambda) - g_3(\Lambda), \tag{2.5}$$

where $g_2(\Lambda) = 60G_4(\Lambda)$ and $g_3(\Lambda) = 140G_6(\Lambda)$.

Proof. We compute the derivatives of $\wp(z;\Lambda)$ and $\wp'(z;\Lambda)$ using Lemma 2.3.8 as

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

and

$$\wp'(z;\Lambda) = -\frac{2}{z^3} + \sum_{n=1}^{\infty}(2n+1)(2n)G_{2n+2}z^{2n-1}.$$

Let $f(z) = \wp'(z;\Lambda)^2 - 4\wp(z;\Lambda)^3 + 60G_4\wp(z;\Lambda) + 140G_6$ and consider the Laurent expansions

$$\begin{aligned}\wp'(z;\Lambda)^2 &= \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + O(z^2) \\ \wp(z;\Lambda)^3 &= \frac{1}{z^6} + \frac{9G_4}{z^2} + 15G_6 + O(z^2) \\ \wp(z;\Lambda) &= \frac{1}{z^2} + O(z^2),\end{aligned}$$

then $f(z) = 0 + O(z^2)$ is a holomorphic elliptic function and hence constant by Lemma 2.3.6. Moreover $f(0) = 0$ and the claim follows. ∎

Corollary 2.3.10. [Cox89, p. 207, Lemma 10.12.] Let $k \geq 2$, then $G_{2k} \in \mathbb{C}[G_4, G_6]$.

Proof. We take the differential equation in (2.5) and differentiate again to obtain

$$\wp''(z;\Lambda) = 6\wp(z;\Lambda)^2 - \frac{g_2(\Lambda)}{2}.$$

The Laurent expansions of $\wp(z;\Lambda)$ and its derivatives yield the recursion

$$(2n+3)(n-2)(2n+1)G_{2n+2} = 3\sum_{i=1}^{n-2}(2i+1)(2(n-1-i)+1)G_{2i+2}G_{2(n-1-i)+2}.$$

■

Corollary 2.3.11. [Sil09, p. 170, Prop. 3.6.a] Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice, then the discriminant

$$\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2$$

of the polynomial $4X^3 - g_2(\Lambda)X - g_3(\Lambda)$ is not 0.

Proof. Let $\omega_3 = \omega_1 + \omega_2$, then for $i = 1, 2, 3$ we have

$$\wp'\left(\frac{\omega_i}{2}\right) = -\wp'\left(-\frac{\omega_i}{2}\right) = -\wp'\left(\frac{\omega_i}{2}\right) = 0$$

and hence

$$0 = \wp'\left(\frac{\omega_i}{2};\Lambda\right)^2 = 4\wp\left(\frac{\omega_i}{2};\Lambda\right)^3 - g_2\wp\left(\frac{\omega_i}{2};\Lambda\right) - g_3.$$

Consider the elliptic function $h_i(z) = \wp(z;\Lambda) - \wp\left(\frac{w_i}{2};\Lambda\right)$. By the above argument h_i has a zero of order 2 at $\frac{\omega_i}{2}$ and since $\wp$ has a single pole of order 2 inside F it follows that there are no other zeros inside F and thus

$$h_i\left(\frac{\omega_j}{2}\right) = \wp\left(\frac{\omega_j}{2};\Lambda\right) - \wp\left(\frac{\omega_i}{2};\Lambda\right) \neq 0$$

for $i \neq j$. ■

2.4. The j-invariant of a Lattice

Here we wish to prove the an analogue of Theorem 1.4.2 for complex tori, respectively lattices. The invariant, which is also called j-invariant, is constructed by means of the j-invariant of an elliptic curve and the differential equation in (2.5). The transformation properties of g_2 and g_3 will make this j-invariant not only a function of lattices but rather on the *upper half-plane*

$$\mathfrak{h} = \{\tau \in \mathbb{C} \mid \operatorname{Im}\tau > 0\},$$

where it is holomorphic and also satisfies a similar transformation property, which is used to show that this j-invariant is indeed an invariant.

Definition + Proposition 2.4.1. [Ser73, p. 78ff, Theorem 1. & 2.] The upper half-plane $\mathfrak{h}$ is acted on by $\mathrm{SL}_2(\mathbb{Z})$ via Möbius transformations

$$\begin{array}{ccc} \mathrm{SL}_2(\mathbb{Z}) \times \mathfrak{h} & \longrightarrow & \mathfrak{h} \\ \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \tau\right) & \longmapsto & \frac{a\tau+b}{c\tau+d} \end{array}.$$

The set

$$F = \{\tau \in \mathfrak{h} \mid -\frac{1}{2} \leq \mathrm{Re}\,\tau \leq 0, |\tau| \geq 1\} \cup \{\tau \in \mathfrak{h} \mid 0 < \mathrm{Re}\,\tau < \frac{1}{2}, |\tau| > 1\}$$

is called the *fundamental region* and is a system of coset representatives of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{h}$.

Proof. Let $\tau \in \mathfrak{h}$ and let

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

then $\mathrm{Im}\,\gamma\tau = \frac{\mathrm{Im}\,\tau}{|c\tau+d|^2}$. Since c and d are integers, we may choose γ such that $\mathrm{Im}\,\gamma\tau$ is maximized and we define $\tau' = T^n\gamma\tau$, where

$$T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

with n such that $-\frac{1}{2} \leq \mathrm{Re}\,\tau' = \mathrm{Re}\,\gamma\tau + n < \frac{1}{2}$. If $|\tau'| < 1$, then

$$\mathrm{Im}\left(\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\tau\right) = \mathrm{Im}\left(-\frac{1}{\tau}\right) > 1,$$

which contradicts the maximality of $\mathrm{Im}\,\gamma\tau$ and it follows that $\tau' \in F$.

Suppose now that there exist $\tau, \tau' \in F$ and a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau' = \gamma\tau$. Without loss of generality, we may assume that $|c\tau + d| \leq 1$, if not, we simply replace τ, τ' and γ with τ', τ and γ^{-1}. Since $|\tau| \geq 1$ it follows that $|c| \leq 1$ and we consider the three cases:

- $c = 0$. Then $d = \pm 1$,
$$\gamma = \begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix}$$
and it follows that $\tau' = \tau + b$. Due to the restriction on the real parts of τ and τ', both must coincide.

- $c = 1$. Then d must be one of $\{0, -1, 1\}$. If $d = 1$, then $|\tau + d| = 1$, which is only possible of $\tau = \frac{-1+\sqrt{-3}}{2}$. Since $\det\gamma = 1$ it follows that $a - b = 1$ and hence
$$\gamma\tau = \frac{a\tau + b}{\tau + 1} = \frac{a\tau + a - 1}{\tau + 1} = a - \frac{1}{\tau + 1} = a + \tau.$$
Again, due to the restriction on the real parts of τ and $a + \tau$ it follows that
$$\gamma = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

and $\tau = \gamma\tau$.

If $d = 0$, then $|\tau| = 1$ and since $\det\gamma = 1$ it follows that $b = -1$, whence

$$\gamma\tau = \frac{a\tau - 1}{\tau} = a - \frac{1}{\tau}.$$

Since $|\tau| = |-\frac{1}{\tau}| = 1$ it follows that either $a = 0$ and then $\tau = i$ or $a = 1$ and then $\tau = \frac{-1+\sqrt{-3}}{2}$. In either case it follows that $\tau = \tau'$.

- $c = -1$. We can invoke the previous case by replacing γ with $-\gamma$.

■

Corollary 2.4.2. [Ser73, p. 78ff, Theorem 1. & 2.] The group $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Proof. Clearly, the determinants of S and T are 1 and hence $\langle S, T\rangle \subseteq \mathrm{SL}_2(\mathbb{Z})$. In the previous proof we have shown that for every $\tau \in \mathfrak{h}$, the orbit $\langle S, T\rangle\tau$ contains an element of F and if $\tau' = \gamma\tau$ with $\tau, \tau' \in F$, then $\gamma \in \langle S, T\rangle$. Let now $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and let $\tau \in F \setminus \{i, \frac{-1+\sqrt{-3}}{2}\}$, then there exists a $\gamma' \in \langle S, T\rangle$ such that

$$\gamma'\gamma\tau \in F$$

and it follows that $\tau = \gamma'\gamma\tau$ and therefore $\gamma'\gamma \in \langle S, T\rangle$, respectively $\gamma \in \langle S, T\rangle$. ■

Lemma 2.4.3. [Ser73, p. 83, Proposition 4.] For $\tau \in \mathfrak{h}$, let $G_4(\tau) = G_4(\Lambda_\tau)$ and $G_6(\tau) = G_6(\Lambda_\tau)$, then $G_4(\tau)$ and $G_6(\tau)$ converge absolutely and uniformly in F and satisfy for

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

the transformation law $G_{2i}(\gamma\tau) = (c\tau + d)^{2i} G_{2i}(\tau)$. Further, the limit $\lim_{\tau\to\infty} G_{2i}(\tau)$ exists and is equal to $2\zeta(4)$ respectively $2\zeta(6)$.

Proof. We have already shown that G_{2i} converges absolutely in Lemma 2.3.2 and hence it defines a function on $\mathfrak{h}$. We proceed by showing that for $\tau \in F$, G_{2i} is uniformly convergent and hence defines a holomorphic function. Using the series definition of G_{2i} we then obtain the transformation property and from this the holomorphicity on all of $\mathfrak{h}$. Finally, using the uniform convergence, we compute the value at infinity. Let $\tau \in F$, then

$$|m + n\tau|^2 = m^2 + 2mn\,\mathrm{Re}\,\tau + n^2|\tau|^2 \geq m^2 - mn + n^2 = |m - n\rho|^2,$$

where $\rho = \frac{1+i\sqrt{3}}{2}$. It follows that

$$|G_{2i}(\tau)| \leq \sum_{m,n}{}' \frac{1}{|m + n\tau|^{2i}} \leq \sum_{m,n}{}' \frac{1}{|m - n\rho|^{2i}} = \sum_{m,n}{}' \frac{1}{|m + n\rho|^{2i}},$$

where the last equality comes from the absolute convergence of $G_{2i}(\rho)$ and hence $G_{2i}(\tau)$ is uniformly convergent in F by the Weierstraß M-test. Let

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

and $\tau \in F$, then

$$G_{2i}(\gamma\tau) = \sum_{m,n}{}' \frac{1}{\left(m + n\frac{a\tau+b}{c\tau+d}\right)^{2i}} = (c\tau+d)^{2i} \sum_{m,n}{}' \frac{1}{(md+nb+\tau(mc+na))^{2i}}.$$

The map $m, n \mapsto md+nb, mc+na$ permutes the indices since γ is invertible and the transformation property follows from the absolute convergence of G_{2i}. The uniform convergence implies

$$\lim_{\tau\to\infty} G_{2i}(\tau) = \sum_{m,n}{}' \lim_{\tau\to\infty} \frac{1}{(m+n\tau)^{2i}} = \sum_{m}{}' \frac{1}{m^{2i}} = 2\zeta(2i).$$

■

Definition 2.4.4. [Ser73, p. 89] Let Λ be a lattice and let $E_\Lambda : Y^2Z = X^3 - \frac{g_2}{4}XZ^2 - \frac{g_3}{4}Z^3$ be the corresponding elliptic curve. The j-invariant of Λ is defined as

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

Since $g_i(\lambda\Lambda) = \lambda^{-2i}g_i(\Lambda)$, the j-invariant is constant on homothety-classes and hence we may define, for $\tau \in \mathfrak{h}$, $j(\tau) = j(\Lambda_\tau)$.

Theorem 2.4.5. [Cox89, p. 206ff, Theorem 10.9., p. 221ff, Theorem 11.2.] The j-invariant is an invariant of homothety-classes of lattices and for every $j_0 \in \mathbb{C}$ there exists a lattice Λ such that $j(\Lambda) = j_0$.

Proof. Suppose $j(\Lambda) = j(\Lambda')$ for two lattices Λ and Λ', then, just like in the algebraic case in Theorem 1.4.2, we obtain

$$g_i(\Lambda') = \lambda^{-2i}g_i(\Lambda) = g_i(\lambda\Lambda)$$

for some $\lambda \in \mathbb{C}$. With Corollary 2.3.10 it follows that

$$\wp(z;\Lambda') = \wp(z;\lambda\Lambda)$$

and since Λ' is the set of poles of $\wp(z;\Lambda')$ and $\lambda\Lambda$ is the set of poles of $\wp(z;\lambda\Lambda)$ it follows that $\Lambda' = \lambda\Lambda$.

For the surjectivity, we first mention that $j(\tau)$ is the quotient of holomorphic functions with the denominator $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2 \neq 0$ and thus j is holomorphic on $\mathfrak{h}$ and the image $j(\mathfrak{h})$ is open. In order to show that the image is closed, we let $(j(\tau_k))_{k\geq 0}$ be a sequence in $\mathbb{C}$ converging to $w \in \mathbb{C}$. Due to the $\mathrm{SL}_2(\mathbb{Z})$ invariance of j, we may assume that $\tau_k \in F$ and if there exists a subsequence $(\tau_{k'})$with Im $\tau_{k'}$ unbounded, it follows that $(j(\tau_{k'}))$ converges to ∞. Thus the elements of the sequence (τ_k) lie inside a compact set and hence there exists a convergent subsequence $(\tau_{k''}) \to \tau^*$ and by continuity $j(\tau^*) = w$ and hence $j(\mathfrak{h})$ is closed. As the only non-empty open and closed subset of $\mathbb{C}$ is $\mathbb{C}$, j is surjective. ■

3. Analytic = Algebraic

In this chapter the different notions of elliptic curves and complex tori are merged. More precisely, it will be shown that the category of elliptic curves with isogenies is equivalent to the category of complex tori with isogenies. With the more accessible complex tori, we can determine the endomorphism rings of elliptic curves and define an exceptional class, so called CM curves, among the elliptic curves. In the second part, the endomorphism rings of these curves will be investigated further.

3.1. Uniformization

In order to show the advertised equivalence of categories, we equip elliptic curves with a unique Riemann surface structure using the implicit function theorem A.0.2.

Theorem 3.1.1. [Mir95, p. 16, Proposition 3.6.] Let $E \subseteq \mathbb{P}^2$ be a smooth projective curve. Then there exists a unique Riemann surface structure on E such that regular functions on Zariski-open subsets are holomorphic.

Lemma 3.1.2. [Mir95, p. 11, 15] Let E be an open and connected subset of a smooth curve given by $F(X,Y,Z) = 0 \subseteq \mathbb{P}^2$, then E can be equipped with a unique Riemann surface structure such that regular functions on Zariski-open subsets are holomorphic.

Proof. Equipped with the complex topology E inherits the Hausdorff and second-countability properties from $\mathbb{P}^2$. The construction of the charts at a point P depends on which affine chart P lies and we describe the process only for points of the shape $P = (x : y : 1)$. For points of different shape, the process works similarly. If $\frac{\partial F}{\partial Y}(P) \neq 0$, then the implicit function theorem A.0.2 provides a holomorphic function $f : V \to U$ such that

$$U_0 := E \cap V \times U \times \{1\} = \{(z : f(z) : 1) \mid z \in V\}$$

and we define the chart $\varphi_0 : U_0 \to V; (z : f(z) : 1) \mapsto z$. If $\frac{\partial F}{\partial X}(P) \neq 0$, we obtain the chart $\varphi_1 : U_1 \to V'; (g(w) : w : 1) \to w$. Suppose that $U_0 \cap U_1 \neq \emptyset$, then the transition function

$$\begin{array}{ccc} \varphi_0(U_0 \cap U_1) & \longrightarrow & \varphi_1(U_0 \cap U_1) \\ z & \longmapsto & w = f(z) \end{array},$$

is holomorphic. Verifying the compatibility for different charts works similarly. Let U_{Zar} be a Zariski-open subset of E, $f : U_{\text{Zar}} \to \mathbb{C}$ a regular function and $\varphi : U \subseteq U_{\text{Zar}} \to V$ a chart, then

$$f \circ \varphi^{-1} : V \to \mathbb{C}$$

is holomorphic, since φ is holomorphic and f is locally given by a quotient of polynomials, regular on U_{Zar}. Finally, since the coordinate projections are regular functions on affine charts, these projections

restricted to sufficiently small open sets are holomorphic, bijective and therefore charts compatible with every Riemann surface structure on E with the property that regular functions are holomorphic. It follows that there is exactly one Riemann surface structure on E which makes regular function holomorphic. ∎

Proof. [Oss, p. 7, Theorem 6.1.] It remains to show that every smooth projective curve is connected. Suppose E is the disjoint union of E_0 and E_1 with E_0 connected. Since E_0 is both open and closed in E, it is a compact Riemann surface using the above lemma. For a point $P \in E_1$ consider the divisor nP. By the Riemann-Roch theorem

$$\dim nP = n + 1 - g > 0$$

for $n \gg 0$ and hence there exists a rational function f, which is regular everywhere but P. In particular f is regular on E_0 and hence defines a holomorphic function on E_0. By the maximum modulus principle f is constant on E_0 with value c and therefore the non-constant rational function $f - c$ has infinitely many zeros, which is impossible. ∎

Earlier, we have already shown how to obtain an elliptic curve from a lattice and we now show that this association is surjective.

Lemma 3.1.3. [Cox89, p. 224, Corollary 11.7.] Let $E\colon Y^2Z = X^3 + AXZ + BZ^3$ be an elliptic curve, then there exists a unique lattice Λ such that $A = -\frac{g_2(\Lambda)}{4}$ and $B = -\frac{g_3(\Lambda)}{4}$. In other words

$$\left(\wp(z;\Lambda) : \frac{\wp'(z;\Lambda)}{2} : 1\right) \in E$$

for all $z \in \mathbb{C}$.

Proof. First, suppose that $j(E) \in \{0, 1728\}$. In either case, one of the coefficients A or B is 0 and we can take the lattices $\lambda\mathbb{Z}[\rho]$, respectively $\lambda\mathbb{Z}[i]$, where λ is chosen such that $A = -\frac{g_3(\lambda\mathbb{Z}[i])}{4}$ if $j(E) = 1728$, or $B = -\frac{g_2(\lambda\mathbb{Z}[\rho])}{4}$ if $j(E) = 0$.

Now, suppose $j(E) \notin \{0, 1728\}$, then, by Theorem 1.4.2 and Theorem 2.4.5, there exists a lattice Λ' such that $j(E) = j(\Lambda')$. Let $\lambda \in \mathbb{C}$ such that $A = -\frac{g_2(\lambda\Lambda')}{4}$, then

$$1 = \frac{A^3}{\left(-\frac{g_2(\lambda\Lambda')}{4}\right)^3} = \frac{B^2}{\left(-\frac{g_3(\lambda\Lambda')}{4}\right)^2} \quad \text{(cf. (1.3))}$$

and hence $B = \pm\frac{g_3(\lambda\Lambda')}{4}$. If it has the wrong sign, the lattice $i\lambda\Lambda'$ satisfies $g_2(i\lambda\Lambda') = g_2(\lambda\Lambda')$ and $g_3(i\lambda\Lambda') = -g_3(\lambda\Lambda')$. ∎

The next theorem is the first part of the uniformization of elliptic curves and relates the objects of the respective categories.

Theorem 3.1.4. [Huso4, p. 176, Theorem 4.3] Let $\mathbb{C}/\Lambda$ be a complex torus and E_Λ the corresponding elliptic curve, then

$$\exp_\Lambda : \begin{cases} \mathbb{C}/\Lambda & \longrightarrow & E_\Lambda \\ z+\Lambda & \longmapsto & \left(\wp(z;\Lambda) : \frac{\wp'(z;\Lambda)}{2} : 1\right) \end{cases}$$

is an isomorphism of Riemann surfaces and abelian groups.

Proof. The charts on $\mathbb{C}/\Lambda$ are given by mapping an evenly covered open subset to a sheet above in $\mathbb{C}$, and the charts on E_Λ are given by the coordinate projections. It follows that for $z \notin \Lambda$, the holomorphicity of $\wp(z;\Lambda)$ and $\wp'(z;\Lambda)$ imply that $\exp_\Lambda$ is a morphism on $(\mathbb{C}\setminus\Lambda)/\Lambda$. Since E_Λ lies in the projective space $\mathbb{P}^2$, we may multiply $\exp_\Lambda$ with $\frac{2}{\wp'(z;\Lambda)}$, whence

$$z+\Lambda \mapsto \left(2\frac{\wp(z;\Lambda)}{\wp'(z;\Lambda)} : 1 : \frac{2}{\wp'(z;\Lambda)}\right)$$

extends $\exp_\Lambda$ to a morphism on $\mathbb{C}/\Lambda$ and in particular it follows that $\exp_\Lambda(0+\Lambda) = (0:1:0)$.

Let $(x:y:1) \in E_\Lambda$, then the elliptic function $\wp(z;\Lambda) - x$ has exactly two zeros z_1 and z_2 in the fundamental region F by Lemma 2.3.6 with $\wp'(z_1;\Lambda) = -\wp'(z_2;\Lambda) = \pm y$. It follows that there exists exactly one $z \in F$ such that $\exp_\Lambda(z+\Lambda) = (x:y:1)$ and further

$$\exp_\Lambda(-z+\Lambda) = (x:-y:1) = -\exp_\Lambda(z+\Lambda). \tag{3.1}$$

As shown before, $\exp_\Lambda(0+\Lambda) = (0:1:0)$ and since this is the only point of E_Λ at infinity, the map $\exp_\Lambda$ is bijective.

For the homomorphism property consider points $P, Q, R \in E_\Lambda$ such that $P+Q = R$. In Chapter 1 we have shown that $P, Q, -R$ span a hyperplane $H : X + \mu Y + \nu Z$ and for $f(z) = \wp(z;\Lambda) + \mu\wp'(z;\Lambda) + \nu$ it follows that $f(z) = 0$ if and only if $\exp_\Lambda(z+\Lambda) \in \{P, Q, -R\}$. But the sum of the zeros of an elliptic function inside the fundamental domain F lies in Λ by Lemma 2.3.6 and with (3.1) we obtain

$$\exp_\Lambda(\exp_\Lambda^{-1}(P) + \exp_\Lambda^{-1}(Q)) = R = P + Q = \exp_\Lambda(\exp_\Lambda^{-1}(P)) + \exp_\Lambda(\exp_\Lambda^{-1}(Q)).$$

■

With the uniformization map $\exp_\Lambda$, we can relate the arrows:

Theorem 3.1.5. [Silo9, p. 171ff, Theorem 4.1.] Let $\exp_\Lambda : \mathbb{C}/\Lambda \to E$ and $\exp_{\Lambda'} : \mathbb{C}/\Lambda' \to E'$ be uniformizations of elliptic curves, then

$$\begin{array}{ccc} \mathrm{Hom}_{\mathrm{Ell}}(E,E') & \longrightarrow & \mathrm{Hom}_{\mathrm{Tori}}(\mathbb{C}/\Lambda, \mathbb{C}/\Lambda') \\ \varphi & \longmapsto & \exp_{\Lambda'}^{-1} \circ \varphi \circ \exp_\Lambda \\ \exp_{\Lambda'} \circ \psi \circ \exp_\Lambda^{-1} & \longmapsfrom & \psi \end{array}$$

is an isomorphism of abelian groups.

Proof. Both types of isogenies are surjective and map the identity to the identity, thus it remains to show that a regular morphism becomes a morphism of Riemann surfaces, vice versa.

Let $\varphi\colon E \to E'$ be a non-zero isogeny, then φ is given by

$$(X : Y : Z) \mapsto (F(X,Y,Z) : G(X,Y,Z) : H(X,Y,Z)),$$

where F, G and H are rational functions which can be chosen to be regular at a point $P \in E$ by Proposition 1.2.2. By construction, there exist charts $f\colon U \to V$ near P and $g\colon U' \to V'$ near $\varphi(P)$ given by coordinate projections and hence $g \circ \varphi \circ f^{-1}$ is given by a regular and hence holomorphic function.

Conversely, a non-zero isogeny $\psi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is given by $\psi(z+\Lambda) = \alpha z + \Lambda'$ by Theorem 2.2.5 with $\alpha \in \mathbb{C}^\times$ such that $\alpha\Lambda \subseteq \Lambda'$. Thus $\exp_{\Lambda'} \circ \psi \circ \exp_\Lambda^{-1}$ is given by

$$\left(\wp(z;\Lambda) : \frac{\wp'(z;\Lambda)}{2} : 1\right) \mapsto \left(\wp(\alpha z;\Lambda') : \frac{\wp(\alpha z;\Lambda')}{2} : 1\right)$$

and since $\alpha\Lambda \subseteq \Lambda'$ it follows for all $\omega \in \Lambda$ that

$$\wp(\alpha(z+\omega);\Lambda') = \wp(\alpha z + \underbrace{\alpha\omega}_{\in\Lambda'};\Lambda') = \wp(\alpha z;\Lambda')$$

and hence $\wp(\alpha z;\Lambda')$ is an elliptic function *with respect to* Λ and thus a rational function in $\wp(z;\Lambda)$ and $\wp'(z;\Lambda)$ by Theorem 2.3.7. The same holds for $\wp'(\alpha z;\Lambda)$ and hence $\exp_{\Lambda'} \circ \psi \circ \exp_\Lambda^{-1}$ is a rational map and a morphism by Proposition 1.2.2. ∎

3.2. Endomorphisms

With the uniformization theorem at hand, the endomorphism ring of an elliptic curve E is isomorphic to

$$\{\alpha \in \mathbb{C} \mid \alpha\Lambda \subseteq \Lambda\},$$

where Λ is the corresponding lattice. We start with a rough classification of these rings into two classes.

Lemma 3.2.1. [Silo9, p. 176, Theorem 5.5.] Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \sim \Lambda_\tau$ be a lattice, then $\operatorname{End} E_\Lambda$ is either isomorphic to $\mathbb{Z}$ or to an order $\mathfrak{o}$ in an imaginary quadratic extension $K/\mathbb{Q}$, in which case $K = \mathbb{Q}(\tau)$.

Proof. Clearly $\operatorname{End} E_\Lambda$ contains a copy of the integers, since $n\Lambda \subsetneq \Lambda$ for $n > 1$. Thus, suppose there exists an $\alpha \in \mathbb{C} \setminus \mathbb{Z}$ such that $\alpha\Lambda \subseteq \Lambda$, i.e.

$$\alpha\omega_2 = a\omega_2 + b\omega_1$$
$$\alpha\omega_1 = c\omega_2 + d\omega_1$$

for $a, b, c, d \in \mathbb{Z}$. Dividing these two equations yields

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

and thus τ satisfies $c\tau^2 + (d-a)\tau - b = 0$. Since $\tau \in \mathfrak{h}$ it must be imaginary quadratic and if we divide $\alpha\omega_2 = a\omega_2 + b\omega_1$ by ω_1 we obtain

$$\alpha\tau = a\tau + b$$

and hence $\alpha \in \mathbb{Q}(\tau)$. Lastly, α induces a linear map $\lambda \mapsto \alpha\lambda$ and is therefore a root of the characteristic polynomial of this map, i.e.

$$0 = \alpha^2 - \operatorname{tr}(\alpha)\alpha + \det\alpha = \alpha^2 - (a+d)\alpha + ad - bc.$$

It follows that α is integral and $\mathfrak{o} = \{\alpha \in \mathbb{Q}(\tau) \mid \alpha\Lambda \subseteq \Lambda\}$ is an order. ∎

Definition 3.2.2. An elliptic curve E is said to have *complex multiplication*, respectively E is called a *CM curve*, if its endomorphism ring is larger than the integers.

Next, we wish to classify these orders further in terms of the discriminant and relate it to the discriminant of (the minimal polynomial of) τ.

Theorem 3.2.3. [Cox89, p. 103, 117, Exercise 5.7.] Let $K = \mathbb{Q}(\sqrt{d})$ be an imaginary quadratic extension of $\mathbb{Q}$ with d a squarefree negative integer. Further, let

$$\Delta_K = \begin{cases} 4d & \text{if } d \equiv 2,3 \mod 4 \\ d & \text{if } d \equiv 1 \mod 4 \end{cases}$$

and

$$\sigma_{\Delta_K} = \begin{cases} 0 & \text{if } \Delta_K \equiv 0 \mod 4 \\ 1 & \text{if } \Delta_K \equiv 1 \mod 4 \end{cases},$$

then

$$\mathfrak{o}_K = \mathbb{Z} + \mathbb{Z}\omega_{\Delta_K},$$

where $\omega_{\Delta_K} = \frac{\sigma_{\Delta_K} + \sqrt{\Delta_K}}{2}$, and Δ_K is the discriminant of $\mathfrak{o}_K$.

Proof. It is easy to see that ω_{Δ_K} is integral, hence it suffices to show that for $u, v \in \mathbb{Q}$ and $u + v\omega_{\Delta_K}$ contained in $\mathfrak{o}_K$ it follows that $u, v \in \mathbb{Z}$. Suppose first that $d \equiv 1 \mod 4$, then

$$(u + v\omega_{\Delta_K}) - (u + v\overline{\omega_{\Delta_K}}) = v\sqrt{d} \in \mathfrak{o}_K$$

and $v^2 d \in \mathbb{Z}$. As d is squarefree it follows that $v \in \mathbb{Z}$ and thus $u = (u + v\omega_{\Delta_K}) - v\omega_{\Delta_K}$ as well.

Suppose now that $d \equiv 2,3 \mod 4$ and recall that the norm and trace

$$\mathrm{N}(u + v\sqrt{d}) = u^2 - v^2 d, \mathrm{Tr}(u + v\sqrt{d}) = 2u$$

are both integers. It follows that $4u^2 - 4v^2 d \in 4\mathbb{Z}$ and $4v^2 d \in \mathbb{Z}$. Since d is squarefree we obtain $2v \in \mathbb{Z}$ and the congruence

$$(2u)^2 - (2v)^2 d \equiv 0 \mod 4.$$

We have that $d \equiv 2,3 \mod 4$ and every integral square is congruent to either 0 or 1 modulo 4, thus $2u$ and $2v$ must be congruent to 0 modulo 4 and hence $u, v \in \mathbb{Z}$.

Finally, we can compute the discriminant

$$\det\left(\begin{pmatrix}1 & \omega_{\Delta_K}\\ 1 & \overline{\omega_{\Delta_K}}\end{pmatrix}\right)^2 = (\overline{\omega_{\Delta_K}} - \omega_{\Delta_K})^2 = \begin{cases}4d & \text{if } d \equiv 2,3 \mod 4\\ d & \text{if } d \equiv 1 \mod 4\end{cases} = \Delta_K.$$

■

Proposition 3.2.4. [HK13, p. 118ff, Theorem 5.1.7.] Let $\mathfrak{o} \subseteq \mathfrak{o}_K$ be any order, then there exists a unique natural number f, called the conductor of f, such that

$$\mathfrak{o} = \mathbb{Z} + f\mathfrak{o}_K = \mathbb{Z} + \mathbb{Z}f\omega_{\Delta_K}$$

and $\Delta(\mathfrak{o}) = f^2\Delta_K$.

Proof. Since $\mathbb{Z}$-submodules of free $\mathbb{Z}$-modules are again free and since $\mathfrak{o}$ is strictly larger than $\mathbb{Z}$ it follows that $\mathfrak{o} = \mathbb{Z} + \mathbb{Z}\omega$ and there exist integers e, f such that $\omega = e + f\omega_{\Delta_K}$. Without loss of generality we may assume that $f \in \mathbb{N}$, then the index of $\mathfrak{o}$ in $\mathfrak{o}_K$ is given by

$$\det\left(\begin{pmatrix}1 & e\\ 0 & f\end{pmatrix}\right) = f$$

and thus $f\omega_{\Delta_K} \in \mathfrak{o}$. We now have a tower of orders $\mathfrak{o}_K \supseteq \mathfrak{o} \supseteq \mathbb{Z} + \mathbb{Z}f\omega_{\Delta_K}$ with

$$(\mathfrak{o}_K : \mathfrak{o}) = (\mathfrak{o}_K : \mathbb{Z} + \mathbb{Z}f\omega_{\Delta_K}) = f$$

and hence $\mathfrak{o} = \mathbb{Z} + \mathbb{Z}f\omega_{\Delta_k}$ and its discriminant is

$$\Delta(\mathfrak{o}) = \det\left(\begin{pmatrix}1 & f\omega_{\Delta_K}\\ 1 & \overline{f\omega_{\Delta_K}}\end{pmatrix}\right) = f^2\Delta_K.$$

■

Now that we can describe every order simply by its conductor, we can give another description more reminiscent of Theorem 3.2.3 using its discriminant.

Corollary 3.2.5. [HK13, p. 118ff, Theorem 5.1.7.] Let $\mathfrak{o}_\Delta$ be an order of discriminant Δ and let

$$\omega_\Delta = \frac{\sigma_\Delta + \sqrt{\Delta}}{2},$$

where

$$\sigma_\Delta = \begin{cases}0 & \text{if } \Delta \equiv 0 \mod 2\\ 1 & \text{if } \Delta \equiv 1 \mod 2\end{cases},$$

then $\mathfrak{o}_\Delta = \mathbb{Z} + \mathbb{Z}\omega_\Delta$.

Proof. Let f be the conductor of $\mathfrak{o}_\Delta$, then $\Delta = f^2\Delta_K$ and

$$\det\left(\begin{pmatrix}1 & \omega_\Delta\\ 1 & \overline{\omega_\Delta}\end{pmatrix}\right)^2 = (f\sqrt{\Delta_K})^2 = f^2\Delta_K.$$

It follows that $\mathbb{Z} + \mathbb{Z}\omega_\Delta$ is the unique order of conductor f. ■

Proposition 3.2.6. [HK13, p. 129ff, Theorem 5.3.1.] Let $\tau \in F$ be an imaginary quadratic algebraic number, $aX^2 + bX + c \in \mathbb{Z}[X]$ its primitive, integral minimal polynomial and $\Delta = b^2 - 4ac$ its discriminant. Then $\mathfrak{o}_\Delta$ is the endomorphism ring of $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$ and Λ_τ is an invertible, fractional $\mathfrak{o}_\Delta$-ideal.

Proof. Using the previous corollary, we can write $\mathfrak{o}_\Delta$ as $\mathbb{Z} + \mathbb{Z}\omega_\Delta$ with $\omega_\Delta = \frac{\sigma_\Delta + \sqrt{\Delta}}{2}$, where

$$\sigma_\Delta \equiv \Delta \equiv b^2 - 4ac \equiv b^2 \equiv b \mod 2.$$

First, we will show that $\mathfrak{o}_\Delta$ is contained in $\operatorname{End}\Lambda_\tau$, that is

$$\mathfrak{o}_\Delta \Lambda_\tau = \mathbb{Z} + \mathbb{Z}\omega_\Delta + \mathbb{Z}\tau + \mathbb{Z}\omega_\Delta\tau \subseteq \Lambda_\tau,$$

thus we only need

$$\omega_\Delta = \frac{\sigma_\Delta + \sqrt{\Delta}}{2} = \frac{\sigma_\Delta + b - b + \sqrt{\Delta}}{2} = \frac{\sigma_\Delta + b}{2} + a\frac{-b + \sqrt{\Delta}}{2a} \in \Lambda_\tau,$$

and

$$\omega_\Delta\tau = \frac{\sigma_\Delta + \sqrt{\Delta}}{2}\frac{-b + \sqrt{\Delta}}{2} = -c + \frac{\sigma_\Delta - b}{2}\tau \in \Lambda_\tau.$$

It follows that Λ_τ is a $\mathfrak{o}_\Delta$-module and we have furthermore

$$\begin{aligned} a\Lambda_\tau\overline{\Lambda_\tau} &= \mathbb{Z}a + \mathbb{Z}a\tau + \mathbb{Z}a\overline{\tau} + \mathbb{Z}a\tau\overline{\tau} \\ &= \mathbb{Z}a + \mathbb{Z}\frac{-b + \sqrt{\Delta}}{2} + \mathbb{Z}\frac{-b - \sqrt{\Delta}}{2} + \mathbb{Z}c \\ &= \mathbb{Z}a + \mathbb{Z}b + \mathbb{Z}c + \mathbb{Z}\frac{-b + \sqrt{\Delta}}{2} \\ &= \mathbb{Z} + \mathbb{Z}\frac{-b + \sqrt{\Delta}}{2}, \end{aligned}$$

where the last equality comes from the primitivity of the minimal polynomial, i.e. $(a, b, c) = 1$. Moreover $b \equiv \sigma_\Delta \mod 2$ and hence the latter is equal to $\mathfrak{o}_\Delta$. Finally, we obtain

$$\operatorname{End}\Lambda_\tau = \mathfrak{o}_\Delta \operatorname{End}\Lambda_\tau = a\Lambda_\tau\overline{\Lambda_\tau} \operatorname{End}\Lambda_\tau = a\Lambda_\tau\overline{\Lambda_\tau} = \mathfrak{o}_\Delta.$$

■

Corollary 3.2.7. [Cox89, p. 212, Corollary 10.20.] Let $\mathfrak{o}$ be an order in K, then there exists a bijection

$$\begin{array}{ccc} \{\mathfrak{o}\text{-CM elliptic curves}\}/\cong & \longrightarrow & \mathrm{Cl}(\mathfrak{o}) \\ E \mathrel{\widehat{=}} \Lambda_\tau & \longmapsto & [\Lambda_\tau] \end{array}$$

Proof. For an $\mathfrak{o}$-CM curve E with corresponding lattice Λ, the normalized lattice Λ_τ is an invertible $\mathfrak{o}$-ideal and gives rise to a class in $\mathrm{Cl}(\mathfrak{o})$. Clearly, if $[\Lambda_\tau] = [\Lambda_{\tau'}]$, there exists a $\lambda \in \operatorname{Quot}\mathfrak{o}$ such that $\Lambda_\tau = \lambda\Lambda_{\tau'}$ but then the curves corresponding to Λ_τ and $\Lambda_{\tau'}$ are isomorphic and hence the map is injective and well-defined. For $[\mathfrak{a}] \in \mathrm{Cl}(\mathfrak{o})$, the fractional ideal $\mathfrak{a}$ is a lattice and hence there exists an elliptic curve $E \cong \mathbb{C}/\mathfrak{a}$ with complex multiplication by $\mathfrak{o}$. ■

The finiteness of the class number of an order $\mathfrak{o}$ implies that the number of isomorphism classes of elliptic curves with complex multiplication by $\mathfrak{o}$ is finite. Later we will introduce *heights* and reproof this.

4. Modular Everything

The previous chapters showed that the j-invariant classifies isomorphism classes, respectively homothety classes, of elliptic curves, complex tori and lattices and that the moduli space of these objects is $\mathbb{A}^1$. The goal of this chapter is to construct moduli spaces, again algebraic curves, of more general objects, namely two elliptic curves E and E' with an isogeny $\varphi\colon E \to E'$ such that $\ker\varphi$ is cyclic. The approach is reminiscent of what we did before: Construct *two* functions which map the upper half-plane to $\mathbb{A}^2$ and show that the image is a curve and that every point corresponds uniquely to an "isomorphism class of isogenies". In order to construct this map, we first have to investigate the j-invariant a bit more and then introduce an analogue for certain subgroups of $\mathrm{SL}_2(\mathbb{Z})$. As a bonus, we easily get the algebraicity of the j-invariant of a CM curve.

4.1. More on the j-invariant

Here, we introduce a class functions which behave like the j-invariant and show that all such functions are rational functions in j. While we're at it, more properties of the j-invariant needed for the proof of Theorem 0.0.1 are shown.

Definition 4.1.1. [Ser73, p. 80ff, Definition 2., 3., 4.] Let k be an integer. A *weakly modular function of weight k* is a meromorphic function $f\colon \mathfrak{h} \to \mathbb{C} \cup \{\infty\}$ such that

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau).$$

Since $f(\tau + 1) = f(\tau)$, every weakly modular function has a Fourier expansion

$$f(\tau) = \sum_{n=-\infty}^{\infty} a_n q(\tau)^n, \quad q(\tau) = e^{2\pi i \tau}$$

and f is called *modular function (of weight k)* or *f is meromorphic at the cusps* if $a_n = 0$ for almost all $n < 0$. If all $a_n = 0$ for all negative indices f is called a *modular form (of weight k)* or *f is holomorphic at the cusps*. A modular form which is 0 at the cusps, i.e. the coefficient a_0 is 0, is called a *cusp form*.

Remark. A pedestrian argument shows that modular forms form a graded $\mathbb{C}$-algebra $M_* = \bigoplus_{k\in\mathbb{Z}} M_k$, where M_k denotes the $\mathbb{C}$-vector space of modular forms of weight k. Furthermore, M_* contains the graded ideal $S_* = \bigoplus_{k\in\mathbb{Z}} S_k$, where S_k denotes the $\mathbb{C}$-vector space of cusp forms of weight k. Lastly, the set of modular functions of weight 0 form a field.

Lemma 4.1.2. [Ser73, p. 92, Proposition 8.] The functions G_4, G_6 and Δ are modular forms of weight 4, 6 and 12 respectively.

Proof. The holomorphicity on $\mathfrak{h}$ and the transformation property were already shown in Lemma 2.4.3 and it remains to verify that the Fourier expansions have the desired form. We use the identities

$$\pi \cot(\pi\tau) = \frac{1}{\tau} + \sum_{m\geq 1}\left(\frac{1}{\tau+m} + \frac{1}{\tau-m}\right)$$

and

$$\pi \cot(\pi\tau) = \pi i \frac{q(\tau)+1}{q(\tau)-1} = \pi i - \frac{2\pi i}{1-q(\tau)} = \pi i - 2\pi i \sum_{n\geq 0} q(\tau)^n,$$

both of which hold for all $\tau \in \mathfrak{h}$. Equating them and differentiating $2k$ times gives

$$\sum_{m\in\mathbb{Z}} \frac{1}{(m+\tau)^{2k}} = \frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{m\geq 1} m^{2k-1} q(\tau)^m.$$

Setting $\tau = n\tau$ and summing over $n \geq 1$ gives

$$\begin{aligned}
\sum_{n\geq 1}\sum_{m\in\mathbb{Z}} \frac{1}{(m+n\tau)^{2k}} &= \sum_{n\geq 1}\sum_{m\geq 1} \frac{(2\pi i)^{2k}}{(2k-1)!} m^{2k-1} q(\tau)^{nm} \\
&= \frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{m\geq 1}\sum_{d|m} d^{2k-1} q(\tau)^m \\
&= \frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{m\geq 1} \sigma_{2k-1}(m) q(\tau)^m.
\end{aligned}$$

Since the left-hand-side remains the same after replacing n by $-n$, summing over $n \neq 0$ gives

$$\sum_{n\neq 0}\sum_{m\in\mathbb{Z}} \frac{1}{(m+n\tau)^{2k}} = \frac{2(2\pi i)^{2k}}{(2k-1)!} \sum_{m\geq 1} \sigma_{2k-1}(m) q(\tau)^m.$$

Adding $\sum_{m\neq 0} \frac{1}{m^{2k}}$ to both sides shows that G_4 and G_6 are modular forms. Tracing through the definition, it can be seen that $g_2(\tau)^3$, $g_3(\tau)^2$ and $g_2(\tau)^3 - 27g_3(\tau)^2$ are modular forms of weight 12. ∎

Theorem 4.1.3 (Jacobi). The identity

$$\Delta(\tau) = (2\pi)^{12} q(\tau) \prod_{n\geq 1} (1-q(\tau)^n)^{24}$$

holds for all $\tau \in \mathfrak{h}$.

Proof. [Ser73, p. 95ff, Theorem 6.] ∎

Theorem 4.1.4. [Cox89, p. 225, Theorem 11.8.] The j-invariant is a modular function of weight 0. Its Fourier expansion

$$j(\tau) = \sum_{n\geq -1} c_n q(\tau)^n = \frac{1}{q(\tau)} + 744 + O(q(\tau))$$

has non-negative, integral coefficients.

Proof. By definition the j-invariant is the quotient of two modular forms of weight 12, with the denominator nowhere 0 by Lemma 2.3.11, and hence it is a modular function of weight 0. With the Fourier expansions of $g_2(\tau)$ and $\Delta(\tau)$ we find

$$\begin{aligned} j(\tau) &= 1728\frac{\left(\frac{120\pi^4}{90} + 20(2\pi)^4 \sum_{n\geq 1} \sigma_3(n)q(\tau)^n\right)^3}{(2\pi)^{12}q(\tau)\prod_{n\geq 1}(1-q(\tau)^n)^{24}} \\ &= \frac{(1 + 240\sum_{n\geq 1} \sigma_3(n)q(\tau)^n)^3}{q(\tau)\prod_{n\geq 1}(1-q(\tau)^n)^{24}} \\ &= \frac{1}{q(\tau)} + 744 + O(q(\tau)). \end{aligned}$$

Since $\prod_{n\geq 1}(1-q(\tau)^n)^{24} \in \mathbb{Z}[\![q(\tau)]\!]^\times$, the Fourier expansion of j has integral coefficients and since $(1-q(\tau)^n)^{-1} = 1 + q(\tau)^n + O(q(\tau)^{2n})$ and $1 + 240\sum_{n\geq 1} \sigma_3(n)q(\tau)^n$ have non-negative coefficients, the coefficients of j-invariant are non-negative as well. ∎

Theorem 4.1.5. The order of vanishing of $f(\tau) = j(\tau) - j(\sigma)$ is 1 unless $\sigma \in \mathrm{SL}_2(\mathbb{Z})i$, where the order is 2, or $\sigma \in \mathrm{SL}_2(\mathbb{Z})\frac{-1+\sqrt{-3}}{2}$, where the order is 3.

Proof. [Cox89, p. 221ff, Theorem 11.2.] ∎

Theorem 4.1.6. [Cox89, p. 226ff, Theorem 11.9.] The field of modular functions is $\mathbb{C}(j(\tau))$. Moreover the subring of modular functions holomorphic on $\mathfrak{h}$ is $\mathbb{C}[j(\tau)]$ and the subring of modular functions holomorphic on $\mathfrak{h} \cup \{\infty\}$ is $\mathbb{C}$.

Proof. Let $f(\tau)$ be a modular function holomorphic on $\mathfrak{h} \cup \{\infty\}$. We will show that $f(\mathfrak{h} \cup \{\infty\})$ is compact, whence the maximum modulus principle shows that f is constant. Thus, let $(j(\tau_k))_{k\geq 0}$ be a sequence in $f(\mathfrak{h} \cup \{\infty\})$ and by the $\mathrm{SL}_2(\mathbb{Z})$-invariance of f we may assume that $\tau_k \in F$. If there exists a subsequence $(\tau_{k^*})_{k^*\geq 0}$ such that $\operatorname{Im}\tau_{k^*} \to \infty$, then $f(\tau_{k^*}) \to f(\infty)$ is a convergent subsequence in the image. If the imaginary parts are bounded by some B, the elements of the sequence are contained in the compact set $\overline{F} \cap \{\tau \mid \operatorname{Im}\tau \leq B\}$ and hence there exist a convergent subsequences $(\tau_{k^*})_{k^*\geq 0}$ and $f(\tau_{k^*})_{k^*\geq 0}$.

Suppose now that $f(\tau)$ is a modular function holomorphic on $\mathfrak{h}$, then the Fourier expansion of f has finitely many terms in negative powers of $q(\tau)$ and hence there exists a polynomial $A(X) \in \mathbb{C}[X]$ such that $f(\tau) - A(j(\tau))$ is a modular function holomorphic on $\mathfrak{h} \cup \{\infty\}$ and thus constant.

Finally, suppose $f(\tau)$ is any modular function, then, since $f(\tau)$ is meromorphic, the number of poles of f inside $\overline{F}$ is finite and hence

$$f(\tau) \prod_{\substack{\tau^* \in F \\ v_{\tau^*}(f)<0}} (j(\tau) - j(\tau^*))^{-v_{\tau^*}(f)}$$

is modular and holomorphic in $\mathfrak{h}$ and hence a polynomial in $j(\tau)$. ∎

4.2. Cyclic Sublattices and Congruence Subgroups

As before, instead of working with cyclic isogenies of elliptic curves directly, we use lattices. The cyclic isogenies of elliptic curves correspond to sublattices $\Lambda' \subseteq \Lambda$, such that Λ/Λ' is cyclic. These sublattices will be classified in terms of matrices and closely related subgroups of $\mathrm{SL}_2(\mathbb{Z})$ are introduced.

Theorem 4.2.1 (Smith Normal Form). Let γ be an integral matrix, then there exist transformation matrices $\eta, \eta' \in \mathrm{SL}_2(\mathbb{Z})$ such that

$$\eta\gamma\eta' = \begin{pmatrix} d_2 & 0 \\ 0 & d_1 \end{pmatrix}$$

with $d_1 \mid d_2$. Furthermore d_1 is, up to sign, the greatest common divisor of all 1×1-minors (i.e. the entries of γ) and d_2 is, up to sign, the greatest common divisor of all 2×2-minors (i.e. $\det \gamma$).

Proof. [Roto3, p. 688, Theorem 9.58., p. 691, Theorem 9.64.] ∎

Lemma 4.2.2. [Ros94, p. 28, Lemma 1.5.4.] Let $N \geq 1$ be an integer and

$$\gamma = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Then there exists a matrix $\Gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\Gamma \equiv \gamma \mod N$.

Proof. Write γ as the product

$$\gamma = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -a^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

and let $A, A' \in \mathbb{Z}$ such that $A \equiv a \mod N$ and $A' \equiv a^{-1} \mod N$. Then

$$\Gamma = \begin{pmatrix} 1 & A \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -A' & 1 \end{pmatrix} \begin{pmatrix} 1 & A \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

is a lift of γ. ∎

Corollary 4.2.3. Let $N \geq 1$ be an integer, then

$$\pi_N : \begin{cases} \mathrm{SL}_2(\mathbb{Z}) & \longrightarrow & \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \\ \Gamma & \longmapsto & \Gamma \mod N \end{cases}$$

is a surjective group homomorphism.

Proof. The residue map is a ring homomorphism and thus π is a homomorphism of groups. Let γ be a matrix in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ and Δ any matrix in $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$ such that $\Delta \equiv \gamma \mod N$. Then there exist matrices $\eta, \eta' \in \mathrm{SL}_2(\mathbb{Z})$ such that $\eta\Delta\eta'$ is a Smith normal form. By the previous lemma, $\pi_N(\Delta)$ lifts to $\Gamma \in \mathrm{SL}_2(\mathbb{Z})$ and hence $\eta^{-1}\Gamma\eta'^{-1} \in \mathrm{SL}_2(\mathbb{Z})$ is a lift of γ.[1] ∎

[1] Taken from M. Brandenburg's comment in [ebe]

Definition 4.2.4. [Kob84, p. 99ff] Let $N \geq 1$ be an integer. The kernel $\Gamma(N)$ of π_N is called the *principal congruence subgroup of level N*. Any subgroup of $\mathrm{SL}_2(\mathbb{Z})$ containing a $\Gamma(N)$ is called *congruence subgroup*. The group $\mathrm{SL}_2(\mathbb{Z})$ is also denoted by $\Gamma(1)$. Clearly, congruence subgroups have finite index in $\mathrm{SL}_2(\mathbb{Z})$.

Example. [Kob84, p. 99ff] Let $N \geq 1$ be an integer, then

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \mod N \right\}$$

is a congruence subgroup.

Proposition 4.2.5. Let $N \geq 1$ be an integer and denote by $M^{\mathrm{cyc}}(N)$ the set of matrices with Smith normal form $\mathrm{diag}(N, 1)$, then there is a bijection

$$\begin{array}{ccc} \Gamma_0(N)\backslash\Gamma(1) & \longrightarrow & \Gamma(1)\backslash M^{\mathrm{cyc}}(N) \\ \Gamma_0(N)\gamma & \longmapsto & \Gamma(1)\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\Gamma_0(N)\gamma \end{array} . \tag{4.1}$$

Proof. First, let us note that $\Gamma(1)\,\mathrm{diag}(N, 1)\Gamma_0(N) = \Gamma(1)\,\mathrm{diag}(N, 1)$ since

$$\Gamma(1)\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\Gamma_0(N) \ni \eta\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ Nc & d \end{pmatrix} = \eta\begin{pmatrix} a & Nb \\ c & d \end{pmatrix}\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma(1)\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$\Gamma(1)\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \ni \gamma\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} = \gamma\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma(1)\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\Gamma_0(N).$$

Let $\Gamma_0(N)\gamma \neq \Gamma_0(N)\gamma'$ be two cosets and assume $\Gamma(1)\,\mathrm{diag}(N, 1)\gamma = \Gamma(1)\,\mathrm{diag}(N, 1)\gamma'$, then there exist $\eta, \eta' \in \Gamma(1)$ such that

$$\eta\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\gamma = \eta'\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\gamma',$$

respectively

$$\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\gamma'\gamma^{-1}\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \eta'^{-1}\eta \in \Gamma(1).$$

The lower left entry of the matrix $\mathrm{diag}(N, 1)\gamma'\gamma^{-1}\,\mathrm{diag}(N, 1)^{-1}$ can only be integral if the matrix $\gamma'\gamma^{-1}$ lies in $\Gamma_0(N)$, that is $\Gamma_0(N)\gamma = \Gamma_0(N)\gamma'$, which is impossible. Let $\Gamma(1)\sigma \in \Gamma(1)\backslash M^{\mathrm{cyc}}(N)$, then there exist matrices $\eta, \eta' \in \mathrm{SL}_2(\mathbb{Z})$ such that $\eta\sigma\eta' = \mathrm{diag}(N, 1)$ and it follows that

$$\Gamma(1)\sigma = \Gamma(1)\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\eta'^{-1} = \Gamma(1)\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\Gamma_0(N)\eta'^{-1}.$$

■

Lemma 4.2.6. [Milo6, p. 203, Lemma 4.15.] Let $N \geq 1$ be an integer and let

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M^{\text{cyc}}(N),$$

then there exists a representative $\sigma \in \Gamma(1)\gamma$ such that

$$\sigma = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix},$$

with $a' > 0, d' > 0, 0 \leq b' < d'$ and $\gcd(a', b', d') = 1$.

Proof. Suppose $a \neq 0$ and $c \neq 0$ and let $c = aq + r, |r| < |a|$ be the division with remainder, then

$$\begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ r & * \end{pmatrix}.$$

Now, multiplying with S, we switch the rows (and change signs) and repeat until the lower left entry is 0. If the signs on the diagonal entries are wrong, we can multiply with $S^2 = -I$ and multiplying with a matrix of the form $T^{q'}$, we can ensure that $0 \leq b' < d'$. Finally, the restriction on $\gcd(a', b', d')$ follows from the Smith normal forms of γ and σ being the same. ∎

Definition 4.2.7. [Cox89, p. 235] Let Λ be a lattice and $N \geq 1$ be an integer. A sublattice $\Lambda' \subseteq \Lambda$ is called *cyclic of index* N if Λ/Λ' is a cyclic group of order N.

Proposition 4.2.8. [Cox89, p. 235, Lemma 11.24.] Let $\Lambda' \subseteq \Lambda$ be lattices, then Λ' is a cyclic sublattice of index N if and only if there exists a matrix $\sigma \in M^{\text{cyc}}(N)$ such that $\Lambda' = \sigma\Lambda$. In particular, if $\Lambda = \Lambda_\tau$, then Λ' is homothetic to $\Lambda_{\sigma\tau}$.

Proof. Follows from the Smith normal form. ∎

Definition 4.2.9. [Cox89, p. 237] Let R be a commutative $\mathbb{Z}$-algebra. An element $\alpha \in R$ is called *primitive* if there exists no $\beta \in R$ and no $n \in \mathbb{Z}_{>1}$ such that $\alpha = n\beta$.

Lemma 4.2.10. [Cox89, p. 237, Corollary 11.27] Let $\mathfrak{o}$ be an order in the imaginary quadratic field K, Λ an invertible $\mathfrak{o}$-ideal and $\alpha \in \mathfrak{o}$. Then $\alpha\Lambda \subseteq \Lambda$ is a cyclic sublattice of index $N(\alpha)$ if and only if α is primitive.

Proof. Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ and let

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be the matrix representing α, then $(\Lambda : \alpha\Lambda) = |\det \gamma| = |N(\alpha)|$. The ring $\mathfrak{o}$ is by construction isomorphic to a matrix ring $\operatorname{End}\Lambda$ and thus α is primitive in $\mathfrak{o}$ if and only if the corresponding γ is primitive in $\operatorname{End}\Lambda$, which holds if and only if $\gcd(a, b, c, d) = 1$. ∎

4.3. Modular Curves

Earlier modular forms and functions were introduced as certain well-behaved functions satisfying a transformation property under $\mathrm{SL}_2(\mathbb{Z})$. We now extend the notion of a modular function of weight 0 to the subgroups $\Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$ and as for the j-invariant we construct the field of all such functions. In doing so, the modular curves will appear as the vanishing set of the minimal polynomials of $j(N\tau)$ over $\mathbb{C}(j(\tau))$.

Definition 4.3.1. [Cox89, p. 225] Let $N \geq 1$ be an integer. A modular function (of weight 0) and *level* $\Gamma_0(N)$ is a meromorphic function $f : \mathfrak{h} \to \mathbb{C} \cup \{\infty\}$ such that

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) : f(\gamma\tau) = f(\tau)$$

and

$$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : f(\gamma\tau) = \sum_{n \geq n_0} a_n q(\tau)^{\frac{n}{N}}$$

(by that we mean $f(\gamma\tau)$ has a Fourier expansion with finitely many terms in negative powers of $q(\tau)^{\frac{1}{N}}$). Clearly, the modular functions of weight 0 introduced earlier have level $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$.

Lemma 4.3.2. [Cox89, p. 226ff, Theorem 11.9.] Let $N \geq 1$ be an integer. The functions $j(\tau)$ and $j(N\tau)$ are modular functions of weight 0 and level $\Gamma_0(N)$.

Proof. Earlier it was shown that $j(\tau)$ is modular with level $\mathrm{SL}_2(\mathbb{Z})$, hence it is also modular with weight $\Gamma_0(N)$. Let

$$\gamma = \begin{pmatrix} a & b \\ cN & d \end{pmatrix} \in \Gamma_0(N),$$

then

$$j(N\gamma\tau) = j\left(\frac{a(N\tau) + bN}{c(N\tau) + d}\right) = j\left(\begin{pmatrix} a & bN \\ c & d \end{pmatrix} N\tau\right) = j(N\tau).$$

By Lemma 4.2.6, the $\mathrm{SL}_2(\mathbb{Z})$ orbit of $\gamma \in M^{\mathrm{cyc}}(N)$ contains an element

$$\sigma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

with $a > 0, d > 0$ and $(a, b, d) = 1$. With such a representative we may compute the Fourier expansion

$$\sum_{n \geq -1} c_n q\left(\frac{a\tau + b}{c}\right)^n = \sum_{n \geq -1} c_n q\left(\frac{b}{c}\right)^n q(a^2\tau)^{\frac{n}{N}} = \sum_{n \geq -1} c_n q\left(\frac{b}{c}\right)^n q(\tau)^{\frac{a^2 n}{N}}$$

and hence $j(N\tau)$ is modular of level $\Gamma_0(N)$. ∎

Lemma 4.3.3. Let $\gamma, \gamma' \in \mathrm{SL}_2(\mathbb{Z})$. If $\Gamma_0(N)\gamma \neq \Gamma_0(N)\gamma'$, then $j(N\gamma\tau) \neq j(N\gamma'\tau)$.

Proof. By Proposition 4.2.5 $\Gamma(1)\operatorname{diag}(N,1)\Gamma_0(N)\gamma \neq \Gamma(1)\operatorname{diag}(N,1)\Gamma_0(N)\gamma'$ and by Theorem 2.4.5 $j(N\gamma\tau) \neq j(N\gamma\tau')$. ∎

Lemma 4.3.4. [Cox89, p. 229ff] Let $\{\gamma_1, \ldots, \gamma_r\}$ be a set of right-coset representatives of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$, then

$$\Phi_N^{\mathrm{PRE}}(X,\tau) = \prod_{i=1}^{r}(X - j(N\gamma_i\tau)) \tag{4.2}$$

is a polynomial in $\mathbb{C}[X, j(\tau)]$.

Proof. We will show that the coefficients (as a polynomial in X) are modular functions with respect to $\Gamma(1)$, holomorphic on $\mathfrak{h}$, and hence polynomials in $j(\tau)$ by Theorem 4.1.6. By Proposition 4.2.5, the value of $j(N\gamma\tau)$ depends only on the class $\Gamma_0(N)\gamma$ and by the previous lemma, the map $j(N\gamma_i\tau) \mapsto j(N\gamma_i\gamma\tau)$ permutes the factors in (4.2) and it follows that for all $\gamma \in \Gamma(1)$

$$\Phi_N^{\mathrm{PRE}}(X,\gamma\tau) = \Phi_N^{\mathrm{PRE}}(X,\tau).$$

Since the coefficients are polynomials in modular functions of level $\Gamma_0(N)$, their Fourier expansions have only finitely many terms in negative powers of $q(\tau)^{\frac{1}{N}}$ and hence they are modular of level $\Gamma(1)$. Finally, the functions $j(N\gamma_i\tau)$ are holomorphic on $\mathfrak{h}$ and hence $\Phi_N^{\mathrm{pre}}(X,\tau) \in \mathbb{C}[X, j(\tau)]$. ∎

The polynomial $\Phi_N(X,Y) \in \mathbb{C}[X,Y]$ such that $\Phi_N(X, j(\tau)) = \Phi_N^{\mathrm{PRE}}(X,\tau)$ is called the *N-th modular polynomial* and the curve $Y_0(N) = \mathcal{V}(\Phi_N) \subseteq \mathbb{A}^2$ is called the N-th modular curve.

Lemma 4.3.5. [Mil06, p. 184ff, Theorem 2.3.] The N-th modular polynomial $\Phi_N(X,Y)$ is irreducible for all $N \geq 1$.

Proof. By definition $\Phi_N(j(N\tau), j(\tau)) = 0$ and thus $j(N\tau)$ is algebraic over $\mathbb{C}(j(\tau))$. Let $f(X, j(\tau)) \in \mathbb{C}(j(\tau))[X]$ be the minimal polynomial of $j(N\tau)$ over $\mathbb{C}(j(\tau))$. For γ a right-coset representative of $\Gamma_0(N)\Gamma(1)$ we evaluate $f(j(N\tau), j(\tau)) = 0$ at $\gamma\tau$ and obtain

$$0 = f(j(N\gamma\tau), j(\gamma\tau)) = f(j(N\gamma\tau), j(\tau)),$$

since $j(\gamma\tau) = j(\tau)$, which shows that every root of $\Phi_N(X, j(\tau))$ is also a root of $f(X, j(\tau))$. With Lemma 4.3.3 we have that the roots of $\Phi_N(X, j(\tau))$ are distinct and hence $\Phi_N(X, j(\tau))$ is the minimal polynomial of $j(N\tau)$ over $\mathbb{C}(j(\tau))$. ∎

Lemma 4.3.6. [Cox89, p. 231, Theorem 11.18.] The N-th modular polynomial $\Phi_N(X,Y)$ has integral coefficients for all $N \geq 1$.

Proof. Let

$$\Phi_N(X, j(\tau)) = f_r(\tau)X^r + \ldots + f_0(\tau),$$

then the coefficients $f_i(\tau)$ are symmetric polynomials in $j(N\gamma_j\tau)$, where γ_j are the coset representatives of $\Gamma_0(N)\backslash\mathrm{SL}_2(\mathbb{Z})$ and hence $f_i(\tau) \in \mathbb{Z}[\zeta_N]((q(\tau)^{\frac{1}{N}}))$. Let π be an automorphism in the Galois

group of $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ acting on $\mathbb{Q}(\zeta_N)((q(\tau)^{\frac{1}{N}}))$ via the coefficients, then

$$\begin{aligned}\pi(j(N\gamma_j\tau)) = \pi(j(\sigma\tau)) &= \sum_{n\geq -1} c_n \pi\left(\zeta_N^{abn}\right) q(\tau)^{\frac{a^2 n}{N}} \\ &= \sum_{n\geq -1} c_n \zeta_N^{kabn} q(\tau)^{\frac{a^2 n}{N}},\end{aligned}$$

where $\pi(\zeta_N) = \zeta_N^k$ with $\gcd(k, N) = 1$. Setting $b' = kb$ and working backwards yields

$$\sum_{n\geq -1} c_n \zeta_N^{ab'n} q(\tau)^{\frac{a^2 n}{N}} = j\left(\frac{a\tau + b'}{d}\right) = j(N\gamma'\tau).$$

Note that $\gcd(a, b', d) = 1$ since $\gcd(N, k) = 1$. In other words, π permutes the $j(N\gamma_j\tau)$ and hence fixes the coefficients $f_i(\tau)$, which then must be contained in $\mathbb{Z}((q(\tau)))$. By construction there exist polynomials $A_i(X)$ such that $f_i(\tau) = A_i(j(\tau))$ and since the coefficients of $f(\tau)$ and $j(\tau)$ are integral, so are the coefficients of A and it follows that $\Phi_N \in \mathbb{Z}[X, Y]$. ∎

Theorem 4.3.7. [Cox89, p. 226ff, Theorem 11.9.] The field of modular functions with respect to $\Gamma_0(N)$ is equal to $\mathbb{C}(j(\tau), j(N\tau))$.

Proof. As shown earlier, the functions $j(\tau)$ and $j(N\tau)$ are both modular with respect to $\Gamma_0(N)$. For $f(\tau)$ a modular with respect to $\Gamma_0(N)$ we define

$$G(X, \tau) = \sum_{i=1}^{r} f(\gamma_i\tau) \prod_{j\neq i} (X - j(N\gamma_j\tau)) \tag{4.3}$$

and let $\gamma \in \Gamma(1)$, then $\gamma_i \mapsto \gamma_i\gamma$ permutes the summands in (4.3), hence $G(X, \gamma\tau) = G(X, \tau)$ and similarly to the proof of Lemma 4.3.4 it follows that $G(X, \tau) \in \mathbb{C}(j(\tau))[X]$. Moreover we have that

$$\prod_{j\neq 1} (j(N\tau) - j(N\gamma_j\tau)) = \frac{\partial \Phi_N}{\partial X}(j(N\tau), j(\tau))$$

and thus

$$G(j(N\tau), \tau) = f(\tau)\frac{\partial \Phi_N}{\partial X}(j(N\tau), j(\tau)).$$

As Φ_N was shown to be irreducible, $\frac{\partial \Phi_N}{\partial X}(j(N\tau), j(\tau)) \neq 0$ and $f(\tau)$ can be expressed as a quotient of polynomials in $j(\tau)$ and $j(N\tau)$. ∎

Theorem 4.3.8. [Cox89, p. 235, Theorem 11.23.] Let $N \geq 1$ be an integer. The N-th modular curve $Y_0(N)$ parametrizes pairs of homothety classes of lattices $(\Lambda'\mathbb{C}^\times, \Lambda\mathbb{C}^\times)$, where $\Lambda' \subseteq \Lambda$ is a cyclic sublattice of index N.

Proof. Let (x, y) be a point in $Y_0(N)$, then, there exists, up to homothety, a lattice Λ_τ such that $y = j(\tau)$ since the j-invariant is surjective. By construction x is equal to some $j(N\gamma\tau)$, where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, and since $\mathrm{diag}(N, 1)\gamma \in M^{\mathrm{cyc}}(N)$,

$$\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \gamma\Lambda_\tau \subseteq \Lambda_\tau$$

is a cyclic sublattice of index N.

Conversely, for any pairs of lattices Λ', Λ with $\Lambda' \subseteq \Lambda$ a cyclic sublattice of index N, there exists a matrix

$$\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M^{\text{cyc}}(N),$$

such that $\Lambda' = \sigma\Lambda$. The Smith normal form of this matrix is then

$$\eta\sigma\eta' = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}.$$

Multiplying with η'^{-1} we obtain $\eta\sigma = \operatorname{diag}(N, 1)\eta'^{-1}$ and thus

$$\Lambda' = \sigma\Lambda = \eta\sigma\Lambda = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \eta'^{-1}\Lambda$$

and it follows that $j(\Lambda') = j(N\eta'^{-1}\tau)$, where $\Lambda \sim \Lambda_\tau$ and hence the homothety classes of Λ' and Λ define a unique point on $Y_0(N)$. ∎

Corollary 4.3.9. The modular curve $Y_0(N)$ parametrizes isogenies of elliptic curves of degree N with cyclic kernel.

Proof. Let $\varphi\colon E \to E'$ be an isogeny, then

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & \mathbb{C} & \longrightarrow & E & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \Lambda' & \longrightarrow & \mathbb{C} & \longrightarrow & E' & \longrightarrow & 0 \end{array}$$

is a commutative diagram of abelian groups with the middle vertical arrow an isomorphism and the cokernel Λ/Λ' is isomorphic to the kernel $\ker\varphi$ by the snake lemma. ∎

Corollary 4.3.10. [Cox89, p. 237, Theorem 11.1.] Let E be an elliptic curve with complex multiplication by $\mathfrak{o}$, then $j(E)$ is algebraic.

Proof. Let Λ be a lattice corresponding to the elliptic curve E and let $\mathfrak{o} = \mathbb{Z} + \mathbb{Z}f\omega_\Delta$, then $f\omega_\Delta$ is primitive. Further let $N = |N(f\omega_\Delta)|$, then

$$0 = \Phi_N(j(f\omega_\Delta\Lambda), j(\Lambda)) = \Phi_N(j(\Lambda), j(\Lambda)),$$

since $f\omega_{\Delta_K}\Lambda \sim \Lambda$ and thus $j(E) = j(\Lambda)$ is algebraic. ∎

Theorem 4.3.11 (Class field theory of imaginary quadratic fields). The absolute Galois group $G_{\mathbb{Q}}$ acts transitively on $\{j(E) \mid \operatorname{End} E = \mathfrak{o}\}$. In particular if $\tau = \frac{-b+\sqrt{\Delta}}{2a}$, there exists an automorphism π such that

$$j(\tau)^\pi = j(\mathfrak{o}).$$

Proof. [Cox89, p. 220ff, Theorem 11.1.] ∎

5. The Theorem of André

We now present the proof of André's Theorem following the paper [BMZ13] by Bilu, Masser and Zannier, borrowing many details from Wüstholz [Wü14]. The "modular curve"-case in both papers is more or less identical, whereas in the "line"-case Wüstholz performs a difficult (read: too difficult for me) calculation to arrive at a linear form in two elliptic logarithms, and Bilu, Masser and Zannier (and already André) use the transcendence measure of Masser fairly effortlessly. However, their omission to detail the effectivity of this step leaves a bitter taste and we use a theorem of Eisenstein, specifically a version by Bilu and Borichev [BB13], to give explicit bounds and constants where possible. Alas, this argument depends on the ability to compute the inverse function of j and an ineffective gap remains.

In order to clarify the presentation, we will first give the proof without spending any thought on effectivity and use continuity arguments to ensure the existence of the relevant bounds and constants.

5.1. Ingredients

Definition 5.1.1. [Bak75, p. 2, p. 70] Let f be a polynomial in $\mathbb{C}[X_1, \dots, X_n]$. The *(naive) height* of f is defined as

$$H(f) = \max_{i_1,\dots,i_n} |f_{i_1,\dots,i_n}|,$$

where $f_{i_1,\dots,i_n}$ is the coefficient of $X^{i_1} \cdots X^{i_n}$ in f. For $\alpha \in \overline{\mathbb{Q}}$ and $f \in \mathbb{Z}[X]$ its primitive minimal polynomial we define the (naive) height of α as $H(\alpha) = H(f)$.

Corollary 5.1.2. The set of algebraic numbers with bounded height and bounded degree is finite.

Proof. The set of integral polynomials with bounded degree and bounded coefficients is finite. ∎

Theorem 5.1.3 (Gelfond's Lemma). Let $f(X) = f_1(X) \cdots f_r(X)$ be a factorization of a complex polynomial, then

$$H(f_1) \cdots H(f_r) \leq e^{\deg f} H(f).$$

In particular, if $f \in \mathbb{Z}[X]$ and $\alpha \in \overline{\mathbb{Q}}$ with $f(\alpha) = 0$, then $H(\alpha) \leq e^{\deg f} H(f)$.

Proof. [Bak75, p. 122ff, Lemma 2.] ∎

Lemma 5.1.4. Let $\alpha \in \overline{\mathbb{Q}}$ with integral, primitive minimal polynomial $f(X) = \sum_{i=0}^{n} f_i X^i \in \mathbb{Z}[X]$ and let $\rho \in \mathbb{Q}^\times$, then

$$H(\rho\alpha) \leq H(\rho)^n H(\alpha).$$

Proof. Let $\frac{r}{s}$ be the reduced fraction of ρ, then

$$\tilde{f}(X) = r^n f\left(\frac{s}{r}X\right) = f_n s^n X^n + f_{n-1} s^{n-1} r X^{n-1} + \ldots + r^n f_0 \in \mathbb{Z}[X]$$

is the integral, primitive minimal polynomial of $\rho\alpha$ and thus $H(\rho\alpha) \leq H(\rho)^n H(\alpha)$. ∎

Lemma 5.1.5. Let τ and τ' be imaginary quadratic numbers with primitive, integral minimal polynomials $aX^2 + bX + c$ and $a'X^2 + b'X + c'$ respectively, then

$$H(\tau + \tau') \leq 10e^4 \max\{H(\tau), H(\tau')\}^4.$$

Proof. We compute an integral, primitive polynomial $f(Z)$ with $\deg f = 4$ and $f(\tau + \tau') = 0$ in SAGE [Dev16]:

```
var('a,b,c,ap,bp,cp')
R.<X,Y,Z>=PolynomialRing(Frac(QQ[a,b,c,ap,bp,cp]), order="lex")
I=R.ideal([a*X^2+b*X+c,ap*Y^2+bp*Y+cp,Z-X-Y])
GB=I.groebner_basis()
f(Z)=(a*ap)^2*GB[-1]
```

The coefficients of $f(Z)$ are homogeneous polynomials in a, b, c, a', b', c' of degree 4 with at most 10 terms. Since τ and τ' need not be algebraically independent, we use Gelfond's inequality, which increases the constant factor by e^4. ∎

Lemma 5.1.6. Let $\tau = \frac{-b+\sqrt{\Delta}}{2a}$ be imaginary quadratic with integral, primitive minimal polynomial $aX^2 + bX + c$. Further suppose $\tau \in F$, then $H(\tau) \leq 2|\Delta|$.

Proof. If $\tau \in F$, then $|\operatorname{Re}\tau| = \left|\frac{b}{2a}\right| \leq \frac{1}{2}$ and $\frac{\sqrt{|\Delta|}}{2a} \geq \frac{\sqrt{3}}{2}$ and it follows that

$$|b| \leq |a| \leq \frac{\sqrt{|\Delta|}}{\sqrt{3}}.$$

The norm $N(\tau)$ is equal to c and we estimate

$$|c| = |N(\tau)| = \left|\frac{b^2 - \sqrt{\Delta}}{4a^2}\right| \leq \frac{1}{4} + \sqrt{|\Delta|} \leq \frac{5}{4}\sqrt{|\Delta|}.$$

Combining the estimates for $|a|$, $|b|$ and $|c|$ we obtain the crude estimate $H(\tau) \leq 2|\Delta|$. ∎

Corollary 5.1.7. Let τ_1, τ_2 be imaginary quadratic and let ρ be a rational number, then

$$H(2(\tau_2 - \rho\tau_1)) \leq 320e^4 H(\rho)^4 \max\{|\Delta_1|, |\Delta_2|\}^4.$$

Lemma 5.1.8. Let $F(X, Y) \in \mathbb{C}[X, Y]$ and let $u \in \mathbb{C}$, then

$$H(F(X, Y + u)) \leq (2|u|)^{\deg F} \deg(F)^2 H(F).$$

Proof. The coefficient of $X^i Y^j$ in $F(X, Y + u)$ is

$$\sum_{k=j}^{\deg_Y F} f_{i,j} \binom{k}{j} u^{k-j}$$

and we estimate crudely

$$\left|\sum_{k=j}^{\deg_Y F} f_{i,j} \binom{k}{j} u^{k-j}\right| \leq \sum_{i,j} |f_{i,j}| (2|u|)^{\deg F} \leq (2|u|)^{\deg F} \deg(F)^2 H(F).$$

∎

Note that there are different notions of height functions, e.g. the *Weil height*, which makes estimating the height of sums and products of algebraic numbers more natural. We stick with the naive height because it is easy to compute and the transcendence results used in the proof, due to Baker [Bak75] and Masser [ZM12], both use naive heights:

Theorem 5.1.9. Fix a branch for log and let $\alpha_0, \alpha_1, \beta_0 \in \overline{\mathbb{Q}}^\times$ with

$$\begin{aligned} A &\geq \max\{H(\alpha_0), H(\alpha_1)\}, \\ B &\geq \max\{H(\beta_0), 2\}, \\ d &\geq \max\{\deg \alpha_0, \deg \alpha_1, \deg \beta_0\}. \end{aligned}$$

Let

$$\Lambda = \beta_0 \log \alpha_0 - \log \alpha_1,$$

then there exists an effectively computable constant C_B depending on A and d, such that either $\Lambda = 0$ or $|\Lambda| > B^{-C_B}$.

Proof. [Bak75, p. 31, Theorem 3.1.] ∎

Baker's theorem appears in an exponential version and we need the following lemma:

Lemma 5.1.10. Let $z \in \mathbb{C}$ with $|e^z - 1| \leq \frac{1}{2}$, then $|z| \leq 2|e^z - 1|$.

Proof. Since $|e^z - 1| \leq \frac{1}{2}$, we estimate with the Taylor expansion of the logarithm

$$|z| = |\log(1 + x)| = \left| \sum_{n \geq 1} \frac{(-1)^{n+1} x^n}{n} \right| \leq \sum_{n \geq 1} \frac{|x|^n}{n} \leq |x| \sum_{n \geq 0} \frac{1}{2^n} = 2|e^z - 1|.$$

∎

Corollary 5.1.11. With notation as above. If $|\alpha_0^{\beta_0} \alpha_1^{-1} - 1| \leq \frac{1}{2}$, then either

$$|\alpha_0^{\beta_0} \alpha_1^{-1} - 1| > \frac{1}{2} B^{-C_B},$$

or $\alpha_0^{\beta_0} \alpha_1^{-1} = 1$.

Theorem 5.1.12. Let $\sigma \in \mathbb{C}$ with $j(\sigma) \in \overline{\mathbb{Q}}$ and let $\tau \in \overline{\mathbb{Q}}$ be imaginary quadratic. Then there exists an effectively computable constant C_M depending on σ, such that either $\tau = \sigma$ or

$$\log|\tau - \sigma| > -C_M(1 + (\log H(\tau))^4).$$

Proof. [ZM12, p. 143ff, Appendix E] ∎

Next, we will investigate the similarity of the functions $j(\tau)$ and $q(\tau)^{-1}$ for large $\operatorname{Im} \tau$ and give explicit bounds for their difference.

Lemma 5.1.13. [Wü14, Lemma 2.1., Corollary 2.1.] Let $\tau \in F$ and suppose $\operatorname{Im}\tau \geq \frac{\log 1728}{2\pi}$, then

$$1 - 1728e^{-2\pi \operatorname{Im}\tau} \leq |j(\tau)q(\tau)| \leq 1 + 1728e^{-2\pi \operatorname{Im}\tau}$$

and if $\operatorname{Im}\tau \geq \frac{\log 3456}{2\pi}$ we further have $\frac{1}{2} \leq |j(\tau)q(\tau)| \leq 2$.

Proof. The latter inequalities follow from the first since $|1728e^{-2\pi \operatorname{Im}\tau}| \leq \frac{1}{2}$ for $\operatorname{Im}\tau \geq \frac{\log 3456}{2\pi}$. We use the Fourier expansion of $j(\tau)$ and the triangle inequalities to obtain

$$\left|1 - \left|q(\tau)\sum_{n\geq 0} c_n q(\tau)^n\right|\right| \leq |j(\tau)q(\tau)| \leq 1 + \left|q(\tau)\sum_{n\geq 0} c_n q(\tau)^n\right|.$$

Since $|q(\tau)| = e^{-2\pi \operatorname{Im}\tau} \leq e^{-2\pi}$ for $\operatorname{Im}\tau \geq 1$, we can estimate

$$\left|q(\tau)\sum_{n\geq 0} c_n q(\tau)^n\right| \leq e^{-2\pi \operatorname{Im}\tau}\sum_{n\geq 0} c_n e^{-2\pi n} = e^{-2\pi \operatorname{Im}\tau}(j(i) - e^{2\pi}) \leq 1728e^{-2\pi \operatorname{Im}\tau}, \tag{5.1}$$

which gives the upper bound. If $\operatorname{Im}\tau \geq \frac{\log 1728}{2\pi}$ it follows that (5.1) is less than or equal to 1 and hence the outer absolute value in the lower bound can be omitted, i.e.

$$\left|1 - \left|q(\tau)\sum_{n\geq 0} c_n q(\tau)^n\right|\right| \geq 1 - \left|q(\tau)\sum_{n\geq 0} c_n q(\tau)^n\right| \geq 1 - 1728e^{-2\pi \operatorname{Im}\tau}.$$

∎

In the proof we also have to relate $j(\tau)^{-\rho}$ and $q(\tau)^{\rho}$, for $\rho \in \mathbb{Q}_{>0}$, which takes a bit more effort.

Lemma 5.1.14. [Wü14, Proposition 2.1.] Let $\rho \in \mathbb{R}_{>0}$ and suppose $\operatorname{Im}\tau \geq \frac{2\rho + \log 3456}{2\pi}$, then

$$j(\tau)^{-\rho} - q(\tau)^{\rho} = q(\tau)^{1+\rho}\vartheta(q(\tau))$$

with $|\vartheta(q(\tau))| \leq 3456e^{2\rho}$.

Proof. We write $j(\tau)q(\tau)$ as

$$j(\tau)q(\tau) = 1 + q(\tau)\sum_{n\geq 0} c_n q(\tau)^n = 1 + q(\tau)\phi(q(\tau)) = 1 + x \tag{5.2}$$

and note that, by Lemma 5.1.13, $|x|$ is bounded by $\frac{1}{2}$ if $\operatorname{Im}\tau \geq \frac{\log 3456}{2\pi}$. We compute the ρ-th power of $j(\tau)q(\tau)$ as

$$e^{\rho\log(1+x)} = \sum_{n\geq 0}\frac{\rho^n}{n!}\left(\sum_{m\geq 1}\frac{(-1)^{m+1}x^m}{m}\right)^n = 1 + x\sum_{n\geq 1}\frac{\rho^n}{n!}\left(\sum_{m\geq 0}\frac{(-1)^m x^m}{m+1}\right)^n = 1 + x\psi(x) \tag{5.3}$$

and we bound $\psi(x)$ by

$$|\psi(x)| \leq \sum_{n\geq 1}\frac{\rho^n}{n!}\left(\sum_{m\geq 0}\frac{|x|^m}{m+1}\right)^n \leq \sum_{n\geq 1}\frac{\rho^n}{n!}\left(\sum_{m\geq 0}|x|^m\right)^n \leq \sum_{n\geq 0}\frac{(2\rho)^n}{n!} = e^{2\rho},$$

thus $|x\psi(x)| \leq \frac{1}{2}$ if $\operatorname{Im}\tau \geq \frac{2\rho+\log 3456}{2\pi}$. We now invert (5.3) to obtain

$$j(\tau)^{-\rho}q(\tau)^{-\rho} = \frac{1}{1+x\psi(x)} = 1 - \frac{x\psi(x)}{1+x\psi(x)},$$

respectively

$$j(\tau)^{-\rho} - q(\tau)^{\rho} = q(\tau)^{1+\rho}\frac{\phi(q(\tau))\psi(x)}{1+x\psi(x)}$$

and we estimate

$$\left|\frac{\phi(q(\tau))\psi(x)}{1+x\psi(x)}\right| \leq 1728\frac{|\psi(x)|}{1-|x\psi(x)|} \leq 3456e^{2\rho}.$$

■

Corollary 5.1.15. [Wü14, Lemma 2.5.] Let $\tau_1, \tau_2 \in F$, $\gamma \in \mathbb{C}$ and $c, \rho \in \mathbb{R}_{>0}$ with

$$\operatorname{Im}\tau_1 \geq \frac{2\rho + \log 3456 + \rho\log 4 + \log|\gamma|}{2\pi\rho}$$

and suppose that the inequalities

$$|j(\tau_1)^{\rho}j(\tau_2)^{-1}\gamma^{-1} - 1| \leq ce^{-2\pi\rho\operatorname{Im}\tau_1} \tag{5.4}$$

and

$$|q(\tau_1)^{-\rho}q(\tau_2)| \leq 4^{\rho}|\gamma| \tag{5.5}$$

hold. We may then replace $j(-)$ with $q(-)^{-1}$ in (5.4) to obtain

$$|q(\tau_1)^{-\rho}q(\tau_2)\gamma^{-1} - 1| \leq c'e^{-2\pi\min\{1,\rho\}\operatorname{Im}\tau_1},$$

at the cost of the worse constant

$$c' = 2^{\rho}c + 13824e + 3456e^{\rho}$$

Proof. We write $|q(\tau_1)^{-\rho}q(\tau_2)\gamma^{-1} - 1|$ as

$$\left|\frac{q(\tau_2) - \gamma q(\tau_1)^{\rho}}{\gamma q(\tau_1)^{\rho}}\right| = \left|\frac{j(\tau_2)^{-1} - \gamma j(\tau_1)^{-\rho} - j(\tau_2)^{-1} + q(\tau_2) + \gamma j(\tau_1)^{-\rho} - \gamma q(\tau_1)^{\rho}}{\gamma q(\tau_1)^{\rho}}\right|,$$

which we bound using the triangle inequality by

$$\underbrace{\left|\frac{j(\tau_2)^{-1} - \gamma j(\tau_1)^{-\rho}}{\gamma q(\tau_1)^{\rho}}\right|}_{I} + \underbrace{\left|\frac{j(\tau_2)^{-1} + q(\tau_2)^{-1}}{\gamma q(\tau_1)^{\rho}}\right|}_{II} + \underbrace{\left|\frac{j(\tau_1)^{-\rho} - q(\tau_1)^{\rho}}{q(\tau_1)^{\rho}}\right|}_{III}.$$

For the first absolute value we have

$$I = |j(\tau_1)q(\tau_1)|^{-\rho}|j(\tau_2)^{-1}j(\tau_1)^{\rho}\gamma^{-1} - 1| \leq 2^{\rho}ce^{-2\pi\rho\operatorname{Im}\tau_1}$$

by Lemma 5.1.13. For the second absolute value we use (5.5) and Lemma 5.1.14 with $\rho = 1$ to obtain

$$II \leq \frac{3456e|q(\tau_2)^2|}{|\gamma q(\tau_1)^\rho|} \leq 13824e|q(\tau_1)^\rho|.$$

Note that since we have (5.5), τ_2 fulfills the requirements of the both Lemmas, i.e. $\operatorname{Im}\tau_2 \geq \frac{\rho+\log 3456}{2\pi}$ as soon as $\operatorname{Im}\tau_1 \geq \frac{2\rho+\log 3456+\rho\log 4+\log|\gamma|}{2\pi\rho}$. Finally, we bound the last absolute value using Lemma 5.1.14 again to obtain

$$III \leq 3456e^\rho|q(\tau_1)|$$

and the desired inequality follows. ∎

5.2. The Proof

Definition 5.2.1. A point $(x, y) \in \mathbb{A}^2$ is called *special* if there exist $\tau_1, \tau_2 \in \mathfrak{h}$, each imaginary quadratic, such that $x = j(\tau_1)$ and $y = j(\tau_2)$.

Let $C = \mathcal{V}(F) \subseteq \mathbb{A}^2$ be an algebraic curve with $F(X, Y) \in \overline{\mathbb{Q}}[X, Y]$. We embed $\mathbb{A}^2$ into $\mathbb{P}^1 \times \mathbb{P}^1$ and denote by $\overline{C}$ the Zariski closure of C in $\mathbb{P}^1 \times \mathbb{P}^1$. We are interested in $\overline{C}$ at infinity, that is, the points in

$$\overline{C} \cap (\mathbb{P}^1 \times \{\infty\} \cup \{\infty\} \times \mathbb{P}^1)$$

and we note that $(\infty, \infty) \in \overline{C}$ if $(0, 0)$ is a root of $X^{\deg_X F} Y^{\deg_Y F} F\left(\frac{1}{X}, \frac{1}{Y}\right)$, $(x, \infty) \in \overline{C}$ if $(x, 0)$ is a root of $Y^{\deg_Y F} F\left(X, \frac{1}{Y}\right)$ and similarly $(\infty, y) \in \overline{C}$ if $(0, y)$ is a root of $Y^{\deg_X F} F\left(\frac{1}{X}, Y\right)$. In particular, if C is not a line, $\overline{C} \cap \mathbb{P}^1 \times \{\infty\}$ and $\overline{C} \cap \{\infty\} \times \mathbb{P}^1$ are always non-empty.

Theorem 5.2.2. [And98; BMZ13; Wü14] Let $C \subseteq \mathbb{A}^2$ be a curve defined by $F(X, Y) \in \overline{\mathbb{Q}}[X, Y]$ and

$$(j(\tau_1), j(\tau_2)) = \left(j\left(\frac{-b_1 + \sqrt{\Delta_1}}{2a_1}\right), j\left(\frac{-b_2 + \sqrt{\Delta_2}}{2a_2}\right)\right) \in C$$

a special point.

1. If $(\infty, \infty) \in \overline{C}$ and $|\Delta_1| \geq |\Delta_2|$, then there exists a constant B_{modular} such that

   $$|\Delta_1| \leq B_{\text{modular}}$$

   or $(j(\tau_1), j(\tau_2))$ lies on some modular curve $Y_0(N)$ with $N \leq \deg(F)^2$.

2. If $(\infty, j(\sigma)) \in \overline{C}$ and $|\Delta_1| \geq |\Delta_2|$, then there exists a constant B_{line} such that

   $$|\Delta_1| \leq B_{\text{line}}$$

   or $(j(\tau_1), j(\tau_2))$ lies on the line $\mathbb{A}^1 \times \{j(\sigma)\}$.

Analogous statements hold if $|\Delta_1| \leq |\Delta_2|$.

In the proofs of both cases we replace $P = (j(\tau_1), j(\tau_2)) \in C$ with

$$P^\pi \in C^\pi,$$

where $\pi \in G_{\mathbb{Q}}$ is chosen such that $j(\tau_1)^\pi = j(\mathfrak{o}_{\Delta_1})$ if $|\Delta_1| \geq |\Delta_2|$ and $j(\tau_2)^\pi = j(\mathfrak{o}_{\Delta_2})$ if $|\Delta_2| \geq |\Delta_1|$. This is justified since modular curves are defined over $\mathbb{Z}$ and are geometrically irreducible and the Galois conjugate of a line is still a line.

Modular Case. [Wü14] Let $(j(\tau_1), j(\tau_2)) \in C$ with $\tau_1 = \frac{\sigma_{\Delta_1} + \sqrt{\Delta_1}}{2}$ and $|\Delta_1| \geq |\Delta_2|$. Further, let $\tilde{F}$ be the reciprocal of F, that is

$$\tilde{F}(X, Y) = X^{\deg_X F} Y^{\deg_Y F} F\left(\frac{1}{X}, \frac{1}{Y}\right),$$

and hence $\tilde{F}(0, 0) = 0$ and $H(\tilde{F}) = H(F)$. The local parametrization theorem A.0.4 provides a Puiseux series

$$Y(x) = \sum_{n \geq 1} a_n x^{\frac{n}{e}} = a_k x^{\frac{k}{e}} + x^{\frac{k+1}{e}} \Theta\left(x^{\frac{1}{e}}\right) \tag{5.6}$$

with $\max\{k, e\} \leq \deg F$ and convergence radius c_1. In particular it follows that $\left(X, \frac{Y(X^e)}{X^k}\right)$ is a root of $G(X, Y) = X^{-m} \tilde{F}(X, X^k Y)$, where $m \in \mathbb{N}_0$ is chosen to be the largest integer such that $G(X, Y)$ is a polynomial, and thus $G(0, a_k) = 0$ and a_k is algebraic with degree bounded by $(\deg F)^2$ and height bounded by $e^{(\deg F)^2} H(F)$ by virtue of Gelfond's Lemma. We restrict the convergence radius to $c_2 = \frac{c_1}{2}$, thereby ensuring that $\Theta(t)$ is holomorphic in $\overline{B_{c_2}(0)}$ and thus $|\Theta(t)| \leq c_3$.

Inserting $x = j(\tau_1)^{-1}, Y(x) = j(\tau_2)^{-1}$ into (5.6) yields

$$j(\tau_2)^{-1} = a_k j(\tau_1)^{-\frac{k}{e}} + j(\tau_1)^{-\frac{k+1}{e}} \Theta\left(j(\tau_1)^{-\frac{1}{e}}\right)$$

which we rearrange as

$$j(\tau_2)^{-1} j(\tau_1)^{\frac{k}{e}} a_k^{-1} - 1 = j(\tau_1)^{-\frac{1}{e}} \Theta\left(j(\tau_1)^{-\frac{1}{e}}\right) \tag{5.7}$$

and

$$j(\tau_2)^{-1} j(\tau_1)^{\frac{k}{e}} = a_k + j(\tau_1)^{-\frac{1}{e}} \Theta\left(j(\tau_1)^{-\frac{1}{e}}\right).$$

For both we choose $\operatorname{Im} \tau_1$ sufficiently large, use the upper bound for $|\Theta(t)|$ and combine with Lemma 5.1.13 to obtain

$$|j(\tau_2)^{-1} j(\tau_1)^{\frac{k}{e}} a_k^{-1} - 1| \leq c_3 |q(\tau_1)^{\frac{1}{e}}|$$

and

$$|q(\tau_2) q(\tau_1)^{-\frac{k}{e}}| \leq 4^{\frac{1}{e}} |a_k|.$$

Lemma 5.1.15 now shows that

$$|q(\tau_2) q(\tau_1)^{-\frac{k}{e}} a_k^{-1} - 1| \leq c_4 e^{-\frac{2\pi \operatorname{Im} \tau_1}{e}}$$

and if $\operatorname{Im}\tau_1 \geq \frac{\log c_4+\log 2}{2\pi}$ Corollary 5.1.11 shows that

$$-C_{\mathrm{B}} \log B < \log(2c_4) - \frac{2\pi \operatorname{Im}\tau_1}{e}$$

or $2(\tau_2 - \frac{k}{e}\tau_1)\log(-1) - \log a_k = 0$. Since we have assumed that $|\Delta_1| \geq |\Delta_2|$, Corollary 5.1.7 shows that B is bounded by $c_5|\Delta_1|^4$ and after some algebraic manipulation we end up with an inequality of the form

$$|\Delta_1| \leq c \log|\Delta_1| + c',$$

with $c > 0$, which eventually becomes inconsistent for $|\Delta_1|$ large enough. If so $(-1)^{2\left(\tau_2 - \frac{k}{e}\tau_1\right)} = a_k \in \overline{\mathbb{Q}}$, which is, by the theorem of Gelfond-Schneider [Bak75, p. 11, Theorem 2.4.], impossible unless $2\left(\tau_2 - \frac{k}{e}\tau_1\right) = 0$ and then

$$\tau_2 = \frac{k}{e}\tau_1 = \begin{pmatrix} k & 0 \\ 0 & e \end{pmatrix} \tau_1,$$

and hence $(j(\tau_1), j(\tau_2)) \in Y_0(ke)$. ∎

Line Case. [BMZ13] Let $(\infty, j(\sigma)) \in \overline{C}$, $(j(\tau_1), j(\tau_2)) \in C$ and assume again that $\tau_1 = \frac{\sigma_{\Delta_1}+\sqrt{\Delta_1}}{2}$ and $|\Delta_1| \geq |\Delta_2|$. Unlike before, we introduce a partial reciprocal polynomial

$$\tilde{F}(X, Y) = X^{\deg_X F} F\left(\frac{1}{X}, Y\right),$$

which satisfies $\tilde{F}(0, j(\sigma)) = 0$, $H(F) = H(\tilde{F})$ and $\deg_X(F) = \deg_X(\tilde{F})$. As before, the local parametrization theorem provides a convergent Puiseux series

$$Y(x) = j(\sigma) + \sum_{n\geq 1} a_n x^{\frac{n}{e}}$$

with convergence radius c_1, which is used to obtain the inequality

$$|j(\tau_2) - j(\sigma)| \leq c_2 e^{-2\pi\rho \operatorname{Im}\tau_1} \tag{5.8}$$

for $\operatorname{Im}\tau_1$ sufficiently large. Let

$$\kappa = \begin{cases} 1 & \text{if } \sigma \neq i, \frac{-1+\sqrt{-3}}{2} \\ 2 & \text{if } \sigma = i \\ 3 & \text{if } \sigma = \frac{-1+\sqrt{-3}}{2} \end{cases}$$

then, by Theorem 4.1.5, the function

$$\phi(\tau_2) = \frac{j(\tau_2) - j(\sigma)}{(\tau_2 - \sigma)^\kappa},$$

is holomorphic and non-zero in a closed disk $\overline{B_r(\sigma)}$ and hence there exists a constant $c_3 > 0$ such that $|\phi(\tau_2)| \geq c_3$, respectively

$$|j(\tau_2) - j(\sigma)| \geq c_3|\tau_2 - \sigma|^\kappa. \tag{5.9}$$

Combining (5.8) and (5.9) yields

$$\kappa \log|\tau_2 - \sigma| \leq \log \frac{c_2}{c_3} - 2\pi\rho \operatorname{Im} \tau_1,$$

which we combine with Masser's transcendence measure 5.1.12, Lemma 5.1.6 and the assumption that $|\Delta_1| \geq |\Delta_2|$ to obtain

$$-\kappa C_{\mathrm{M}}(1 + (\log 2 + \log|\Delta_1|)^4) \leq \log \frac{c_2}{c_3} - \pi\rho|\Delta_1|$$

or $\tau_2 = \sigma$. As before, if $|\Delta_1|$ is sufficiently large, the inequality becomes inconsistent and then $(j(\tau_1), j(\tau_2)) \in \mathbb{A}^1 \times \{j(\sigma)\}$. ∎

Proof of 0.0.1. By definition C contains infinitely many special, hence algebraic, points and is therefore defined over $\overline{\mathbb{Q}}$. As shown in Corollary 5.1.2 the number of singular moduli $j\left(\frac{-b+\sqrt{\Delta}}{2a}\right)$ with $|\Delta|$ bounded is finite and Theorem 5.2.2 implies that all but finitely many special points lie on finitely many vertical or horizontal lines, or finitely many modular curves. Since C is assumed to be irreducible, of pure dimension 1 and not equal to a vertical or horizontal line, it must be a modular curve. ∎

5.3. Effectivity

We will now sketch how to make the previous proof partially effective. Our main tool for this task is a theorem of Bilu and Borichev:

Theorem 5.3.1 (Bilu-Borichev). Let $F(X, Y) \in \overline{\mathbb{Q}}[X, Y]$ be irreducible and

$$\Psi(X) = \sum_{k \geq \kappa} a_k X^{\frac{k}{e}} \in \overline{\mathbb{Q}}((X^{\frac{1}{e}}))$$

a formal Puiseux series satisfying $F(X, \Psi(X)) = 0$. Further, let $\Delta_Y(F)$ be the normalized discriminant of $F(X, Y) \in \mathbb{C}[X][Y]$ such that the coefficient of the smallest power of X in $\Delta_Y(F)$ is 1. Then

$$|a_k| \leq A' A^{\frac{k}{e} - \lfloor \frac{\kappa}{e} \rfloor}$$

for all $k \geq \kappa$, with $A' = 3H(F)$ and $A = \max\{2H(\Delta_Y(F)), (6H(F))^{\deg_Y(F)}\}$.

Proof. [BB13, Theorem 6.3.] ∎

In the proof we used convergent Puiseux $\Psi(x)$ series at a point x_0 with convergence radius given by the distance between x_0 and the nearest branch point. All branch points can be computed by, for example, computing a Gröbner basis of the polynomial system

$$\{F(X, Y), \frac{\partial F}{\partial Y}(X, Y)\}.$$

However, the theorem of Bilu and Borichev already provides explicit lower bounds for the convergence radius, so we might just as well take these. In (5.6), instead of using continuity, the theorem of Bilu-Borichev allows us to estimate

$$\left|\Theta\left(x^{\frac{1}{e}}\right)\right| \leq \sum_{n \geq k+1} A' A^{\frac{n}{e}} |x|^{\frac{n}{e}}$$

and for $x \leq \frac{1}{2A}$ we obtain with a geometric series argument the upper bound $2A$. The same argument is used for the upper bound in the "line" case and we do not repeat it.

For the lower bound in (5.9) we construct an auxiliary polynomial $G(X,Y)$ in several steps. First, let $\tilde{F}(X,Y)$ be the partial reciprocal with $\tilde{F}(0,j(\sigma)) = 0$, then define

$$\hat{F}(X,Y) = \tilde{F}(X, Y + j(\tau_2))$$

and hence $\hat{F}(0, j(\sigma) - j(\tau_2)) = 0$ and the height of $\hat{F}$ can be estimated using Lemma 5.1.8 in terms of $H(F)$ and $|j(\tau_2)|$, which can be effectively bounded using (5.8). Finally, we define

$$G(X,Y) = Y^{\deg_Y F} \hat{F}\left(X, \frac{1}{Y}\right),$$

such that

$$G(0, (j(\tau_2) - j(\sigma))^{-1}) = 0$$

and we may use the theorem of Bilu-Borichev for this polynomial and obtain

$$|j(\tau_2) - j(\sigma)| \geq c_3$$

for $|j(\tau_1)| \geq c_4$. As in the proof, we require r be a non-zero radius around σ such that $\phi(\tau_2) \neq 0$ for $\tau_2 \in \overline{B_r(\sigma)} \setminus \{\sigma\}$. By the maximum modulus principle, the minimum of $|\phi(\tau_2)|$ is assumed at the boundary and hence

$$\min_{|\tau_2 - \sigma| \leq r} \left| \frac{j(\tau_2) - j(\sigma)}{(\tau_2 - \sigma)^\kappa} \right| = \min_{|\tau_2 - \sigma| = r} \left| \frac{j(\tau_2) - j(\sigma)}{(\tau_2 - \sigma)^\kappa} \right| \geq \frac{1}{r^\kappa} |j(\tau_2) - j(\sigma)| \geq \frac{c_3}{r^\kappa},$$

respectively

$$|j(\tau_2) - j(\sigma)| \geq \frac{c_3}{r^\kappa} |\tau_2 - \sigma|^\kappa.$$

The missing piece of the puzzle is the radius r, which depends of course on σ. If, for example, σ is close to i, then $-\frac{1}{\sigma}$ is also close to i and r must be small enough to exclude $-\frac{1}{\sigma}$ since otherwise the assumption that the minimum of

$$\left| \frac{j(\tau_2) - j(\sigma)}{(\tau_2 - \sigma)^\kappa} \right|$$

is assumed at the boundary of $B_r(\sigma)$ and is bounded by an effective constant, is no longer true.

A. Local Parametrizations of Algebraic Curves

Convention. All algebraic curves are assumed to be plane curves. While the results presented here hold in general, this restriction simplifies a few definitions.

Let $C\colon F(X,Y) = 0 \subseteq \mathbb{A}^2$ be an affine algebraic curve and P a point on C. We are seeking a *local parametrization* at P, that is, a(n ideally) holomorphic function $\varphi\colon B_\varepsilon(0) \to \mathbb{C}$ such that

$$C \cap (B_\varepsilon(0) \times U) = \{(z, \varphi(z)) \mid z \in B_\varepsilon(0)\},$$

where $U \subseteq \mathbb{C}$ is open.

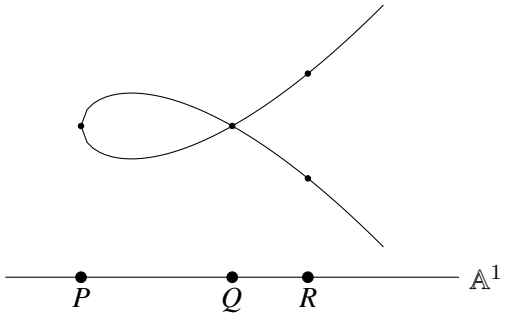

Figure A.1.: The singular curve $Y^2 = X^3 + X^2$ and the coordinate projection

As can be seen in Figure A, the number of preimages of a point $x_0 \in \mathbb{A}^1$ is equal to the number of distinct roots of $f(x_0, Y) \in \mathbb{C}[Y]$. If this polynomial has multiple roots, the point x_0 is called a *branch point (with respect to x)* and its preimages corresponding to the multiple roots are called *ramification points (with respect to x).* Clearly, y_0 is a multiple root of $f(x_0, Y)$ if and only if $\frac{\partial f}{\partial Y}(x_0, y_0) = 0$ and it follows that a singular point $Q \in C$ is a ramification point for both coordinate projections x and y and a non-singular point is unramified with respect to at least one coordinate projection. In this sense, finding a local parametrizations at a singular points is entirely subsumed by finding local parametrizations at ramified points.

We begin with the unramified case, for which the Implicit Function Theorem will give a holomorphic local parametrization.

Lemma A.0.1. [FS09, p. 270] Let $C \subseteq \mathbb{C}$ a closed, non-intersecting loop in positive orientation and D the domain bounded by C. Moreover let $f\colon D \to \mathbb{C} \cup \{\infty\}$ be a meromorphic and $g\colon D \to \mathbb{C}$ a holomorphic function. Then

$$I := \frac{1}{2\pi i} \int_C g(z) \frac{f'(z)}{f(z)} dz = \sum_{z_0 \in D} g(z_0) v_{z_0}(f).$$

In particular, if f is holomorphic on D and $g = 1$, respectively $g(z) = z$, the integral I counts the zeros of f in D, respectively I is the sum of all zeros in D.

Proof. It suffices to check this for a single zero or pole in D, as the general case then follows from the residue theorem. Thus let z_0 in D, then $f(z) = (z - z_0)^{v_{z_0}(f)}\tilde{f}(z)$, with $\tilde{f}(z)$ holomorphic and non-zero on D. Elementary manipulation shows that

$$\frac{f'(z)}{f(z)} = \frac{v_{z_0}(f)}{z - z_0} + \frac{\tilde{f}'(z)}{\tilde{f}(z)},$$

where the latter fraction is holomorphic on D and hence

$$I = \frac{1}{2\pi i}\int_C g(z)\frac{f'(z)}{f(z)}dz = \frac{1}{2\pi i}\int_C g(z)\frac{v_{z_0}(f)}{z - z_0}dz = g(z_0)v_{z_0}(f)$$

by the residue theorem. ∎

Theorem A.0.2 (Implicit Function Theorem). [For99, p. 52ff, Lemma 8.7.] Let $F(X, Y)$ be a polynomial in $\mathbb{C}[X, Y]$ and let 0 be a simple zero of $F(0, Y)$. Then there exists a real number $\varepsilon > 0$ and a holomorphic function φ such that $\varphi(0) = 0$ and

$$F(x, \varphi(x)) = 0,$$

for all x with $|x| < \varepsilon$.

Proof. The function $F\colon \mathbb{C}^2 \to \mathbb{C}$ is continuous, hence there exists a radius $r > 0$ such that $F(0, Y)$ has a single zero inside $\{y \in \mathbb{C} \mid |y| < r\}$ and no zeros on the boundary $\{y \in \mathbb{C} \mid |y| = r\}$. Again, by the continuity of F, there exists a radius $r' > 0$ such that

$$F(x, y) \neq 0, \forall (x, y) \in \{(x, y) \in \mathbb{C}^2 \mid |x| < r', |y| = r\} =: \Omega.$$

Consequently the function

$$\frac{\frac{\partial F}{\partial Y}(x, y)}{F(x, y)}$$

is analytic in Ω and the integral

$$n(x) = \frac{1}{2\pi i}\int_{|y|=r'} \frac{\frac{\partial F}{\partial Y}(x, y)}{F(x, y)}dy$$

defines a function $n(x)$ which counts the number of zeros of $F(x, Y)$ with $|Y| < r$ by Lemma A.0.1. As this function is analytic, locally constant and satisfies $n(0) = 1$, it follows that $n(x) = 1$ for all x with $|x| < r'$ and hence, by the same reasoning as before, the analytic function

$$\varphi(x) = \frac{1}{2\pi i}\int_{|y|=r} y\frac{\frac{\partial F}{\partial Y}(x, y)}{F(x, y)}dy$$

satisfies $\varphi(0) = 0$ and $F(x, \varphi(x)) = 0$ for $|x| < r'$. ∎

If the covering is ramified, the implicit function theorem is no longer applicable and we have to extend the notion of a local parametrization.

Definition A.0.3. Let z be an indeterminate, $e \in \mathbb{N}$ and $n_0 \in \mathbb{Z}$. A series

$$f(z) = \sum_{n \geq n_0} a_n z^{\frac{n}{e}}$$

is called a *formal Puiseux series*. It is convergent (with convergence radius r) if $f(z^e)$ is a convergent Laurent series (with convergence radius $r^{\frac{1}{e}}$). A convergent Puiseux series is not a function but for a choice of $\xi^{\frac{1}{e}}$ it can be evaluated like a convergent powerseries.

Theorem A.0.4. [FS09, p. 495ff, Theorem VII.7] Let $F(X, Y) \in \mathbb{C}[X, Y]$ be irreducible with $F(0, 0) = 0$, then there exists a natural number $e \leq \deg_Y F$, a radius $r > 0$ and a holomorphic function $\Psi \colon B_r(0) \to \mathbb{C}$ such that

$$F(z^e, \Psi(z)) = F\left(z, \Psi\left(z^{\frac{1}{e}}\right)\right) = 0.$$

The radius r can be chosen as the distance between 0 and the nearest root of $F(0, Y)$.

Proof. Consider F as polynomial in Y, that is

$$F(X, Y) = f_n(X)Y^n + f_{n-1}(X)Y^{n-1} + \ldots + f_0(X) \in \mathbb{C}[X][Y]$$

and denote by $\Delta_Y(F)(X) \in \mathbb{C}[X]$ its discriminant. Since F is irreducible, $\Delta_Y(F)(X)$ is not identically 0 and more precisely $\Delta_Y(F)(x_0) = 0$ if and only if there exists a $y_0 \in \mathbb{C}$ such that

$$F(x_0, y_0) = \frac{\partial F}{\partial Y}(x_0, y_0) = 0,$$

or, in other words, x_0 is a branch point of the covering $x \colon \mathcal{U}(F) \to \mathbb{A}^1$. Let $r > 0$ be the distance between 0 and the nearest branch point, then $\Delta_Y(F)(x_1) \neq 0$ for all x_1 with $0 < |x_1| < r$ and for such an x_1, the polynomial $F(x_1, Y)$ has n pairwise distinct roots $y_1, \ldots, y_n$.

Using the implicit function theorem we find analytic functions

$$Y_1, \ldots, Y_n \colon B_\varepsilon(x_1) \to \mathbb{A}^1,$$

which satisfy $Y_i(x_1) = y_i$ and $F(\xi, Y_i(\xi)) = 0$ for $|x_1 - \xi| < \varepsilon$. As this works for all x_1 with $0 < |x_1| < r$, the functions Y_i can be analytically continued to $\tilde{Y}_i \colon B_r^\circ(0) \to \mathbb{A}^1$. Note that these functions need not be single-valued and we define $\pi(Y_i)$ the function obtained by analytically continuing Y_i counter clock-wise around the origin (see Figure A.2) and then restricting it back to a neighbourhood of x_1. As this function satisfies $F(\xi, \pi(Y_i)(\xi)) = 0$ and the process is reversible, it follows that π is a permutation of $Y_1, \ldots, Y_n$.

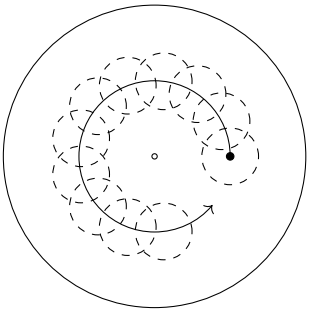

Figure A.2.: Continuing the local parametrizations around the branch point

By the continuity of polynomial roots, we may pick a function $\tilde{Y}_i(\xi)$ such that $\lim_{\xi\to 0} \tilde{Y}_i(\xi) = 0$. Then there exists a minimal $e \in \mathbb{N}$ such that $\pi^e(\tilde{Y}_i) = \tilde{Y}_i$ and we define

$$\Phi(\xi) = \tilde{Y}_i(\xi^e),$$

which is holomorphic for $0 < |\xi|^e < r$ and satisfies $F(\xi^e, \Phi(\xi)) = 0$. Lastly, we have $\lim_{\xi\to 0} \Phi(\xi) = 0$ and hence Φ can be analytically continued to $B_r(0)$ by Morera's theorem [FS09, p. 743, B.6.]. ∎

B. Covering spaces

Definition B.0.1. [Hato2, p. 56] Let $p\colon \tilde{X} \to X$ be a continuous function. An open subset U of X is called *evenly covered*, if $p^{-1}(U)$ is a disjoint union of open subsets, called *sheets*, of $\tilde{X}$, each homeomorphic to U via p.

The map p is called a *covering (map)*, or $\tilde{X}$ is said to be a *covering space* of X, if every $x \in X$ is contained in an evenly covered open neighbourhood.

Definition B.0.2. [Hato2, p. 25] Let X be a topological space. A path in X is a continuous function $f\colon [0,1] \to X$. For two paths $f, g\colon [0,1] \to X$ with $f(1) = g(0)$, the concatenation $f \cdot g$ is defined as

$$f \cdot g(t) = \begin{cases} f(2t) & \text{if } 0 \le t \le \frac{1}{2} \\ g(2(1-t)) & \text{if } \frac{1}{2} < t \le 1 \end{cases}.$$

By abuse of notation we will sometimes call any continuous function $f\colon [a,b] \to X$, with $a < b \in \mathbb{R}$, a path in X and for another path $g\colon [b,c] \to X$ with $b < c$ and $f(b) = g(b)$, we let

$$f \cdot g(t) = \begin{cases} f(t) & \text{if } a \le t \le b \\ g(t) & \text{if } b < t \le c \end{cases}$$

be the concatenation.

Lemma B.0.3. [Path lifting][Hato2, p. 29ff, Theorem 1.7] Let $p\colon \tilde{X} \to X$ be a covering, $f\colon [0,1] \to X$ a path and $\tilde{x} \in p^{-1}(f(0))$. Then there exists a unique path $\tilde{f}\colon [0,1] \to \tilde{X}$ such that

$$\begin{array}{ccc} & & \tilde{X} \\ & \overset{\tilde{f}}{\nearrow} & \big\downarrow p \\ [0,1] & \xrightarrow{f} & X \end{array}$$

commutes and $\tilde{f}(0) = \tilde{x}$.

Proof. Suppose first that $f([0,1])$ is contained in an evenly covered open set $U \subseteq X$. Let $\tilde{U}$ be the unique sheet above U with $\tilde{x} \in \tilde{U}$ and let $\tilde{p}$ be the restriction of p to $\tilde{U}$. Then $\tilde{f} = \tilde{p}^{-1} \circ f\colon [0,1] \to \tilde{X}$ is a path with $\tilde{f}(0) = \tilde{x}$ and $p \circ \tilde{f} = f$. Moreover it is the unique path with these properties since $\tilde{p}$ is a homeomorphism.

The general case follows from the previous by splitting the path f into finitely many subpaths, each of which has its image inside an evenly covered set, lifting them and gluing the lifts together.

The image $f([0,1]) \subseteq X$ is compact and since X has a cover by evenly covered open subsets, there exists a finite partition

$$0 = t_0 < t_1 < \cdots < t_{n-1} < t_n = 1$$

and evenly covered open subsets $U_1, \ldots, U_n$, such that $[t_{i-1}, t_i] \subseteq U_i$. Denote by $f_{i-1,i}$ the restriction of f to $[t_{i-1,i}, t_i]$. By the previous case $f_{0,1}$ lifts to a unique path $\tilde{f}_{0,1}\colon [0, t_1] \to \tilde{X}$ with $\tilde{f}_{0,1}(0) = \tilde{x}$ and $p \circ \tilde{f}_{0,1} = f$. Replacing $\tilde{x}$ with $\tilde{f}_{0,1}(t_1)$, we obtain a unique lift $\tilde{f}_{1,2}\colon [t_1, t_2] \to \tilde{X}$ with $\tilde{f}_{1,2}(t_1) = \tilde{f}_{0,1}(t_1)$. Repeating this process we obtain the unique path

$$\tilde{f} = \tilde{f}_{0,1} \centerdot \ldots \centerdot \tilde{f}_{n-1,n}\colon [0,1] \to \tilde{X}$$

for which $\tilde{f}(0) = \tilde{x}$ and $p \circ \tilde{f} = f$. ∎

Lemma B.0.4. [Hat02, p. 61ff, Proposition 1.33, 1.34] Let $p\colon \mathbb{C} \to X$ and $q\colon \mathbb{C} \to Y$ be covering maps and $F\colon X \to Y$ a surjective, continuous function such that $F(p(0)) = q(0)$. Then there exists a unique continuous lift $\tilde{F}\colon \mathbb{C} \to \mathbb{C}$ such that

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\tilde{F}} & \mathbb{C} \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle q} \\ X & \xrightarrow{F} & Y \end{array}$$

commutes and $\tilde{F}(0) = 0$.

Proof. Let $z \in \mathbb{C}$ and $f_z\colon [0,1] \to \mathbb{C}$ a path with $f_z(0) = 0$ and $f_z(1) = z$. Then $F \circ p \circ f_z$ is a path in Y, which lifts, by Lemma B.0.3, to a unique path $\tilde{f}_z\colon [0,1] \to \mathbb{C}$ such that $\tilde{f}_z(0) = 0$ and we define $\tilde{F}(z) = \tilde{f}_z(1)$. To see that this is well-defined, let $g\colon [0,1] \to \mathbb{C}$ be another path with $g(0) = 0$ and $g(1) = z$. Then

$$g^{-1} \centerdot f_z\colon [0,1] \to \mathbb{C}$$

is a path with $g^{-1} \centerdot f_z(0) = g^{-1} \centerdot f_z(1) = 0$ and $g^{-1} \centerdot f_z\left(\frac{1}{2}\right) = z$. The path $h = F \circ p \circ (g^{-1} \centerdot f_z)$ lifts to a path $\tilde{h}\colon [0,1] \to \mathbb{C}$ with $\tilde{h}\left(\frac{1}{2}\right) = \tilde{f}_z(1) = \tilde{g}(1) = \tilde{F}(z)$.

Next, we want to give a local description of $\tilde{F}$. Let $U \subseteq X$ and $U' \subseteq Y$ be evenly covered with $F(U) \subseteq U'$. Moreover let $\tilde{p}\colon \tilde{U} \to U$ and $\tilde{q}\colon \tilde{U}' \to U'$ be sheets above. Let $z_0, z_1 \in \tilde{U}$ and let f be a path such that $f(0) = 0$, $f\left(\frac{1}{2}\right) = z_0$ and $f(1) = z_1$. Further suppose that $f\left([\frac{1}{2}, 1]\right)$ is contained in $\tilde{U}$. By the construction of the path lift

$$\tilde{F}(z_1) = \tilde{q}^{-1} \circ F \circ p(z_1)$$

for all $z_1 \in \tilde{U}$. It follows that $\tilde{F}$ is locally given by continuous functions and hence is continuous itself. ∎

Bibliography

[And89] Y. André. *G-Functions and Geometry*. Springer, 1989.

[And98] Yves André. "Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire". In: *Journal für die reine und angewandte Mathematik (Crelles Journal)* 1998.505 (1998), pp. 203–208.

[Bak75] A. Baker. *Transcendental Number Theory*. Cambridge Mathematical Library. Cambridge University Press, 1975.

[BB13] Yuri Bilu and Alexander Borichev. "Remarks on Eisenstein". In: *Journal of the Australian Mathematical Society* 94.02 (2013), pp. 158–180.

[BMZ13] Y. Bilu, D. Masser, and U. Zannier. "An effective "Theorem of André" for CM-points on a plane curve". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 154 (01 Jan. 2013).

[Cox89] D.A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*. Pure and applied mathematics. Wiley, 1989.

[Dev16] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.2)*. `http://www.sagemath.org`. 2016.

[ebe] Sean Eberhard (http://math.stackexchange.com/users/23805/sean eberhard). *Why is the quotient map $SL_n(\mathbb{Z})$ to $SL_n(\mathbb{Z}/p\mathbb{Z})$ is surjective?* Mathematics Stack Exchange. URL: `http://math.stackexchange.com/q/321832`.

[EY03] B. Edixhoven and A. Yafaev. "Subvarieties of Shimura varieties". In: *Annals of Mathematics* 157.2 (2003), pp. 621–645.

[For99] O. Forster. *Lectures on Riemann Surfaces*. Graduate Texts in Mathematics. Springer, 1999.

[FS09] P. Flajolet and R. Sedgewick. *Analytic Combinatorics*. Cambridge University Press, 2009. URL: `http://algo.inria.fr/flajolet/Publications/AnaCombi/anacombi.html`.

[Har77] R. Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1977.

[Hat02] A. Hatcher. *Algebraic Topology*. Cambridge University Press, 2002. URL: `https://www.math.cornell.edu/~hatcher/AT/ATpage.html` (visited on 02/09/2016).

[HK13] F. Halter-Koch. *Quadratic Irrationals: An Introduction to Classical Number Theory*. Chapman & Hall/CRC Pure and Applied Mathematics. CRC Press, 2013.

[Hus04] D. Husemöller. *Elliptic Curves*. Graduate Texts in Mathematics. Springer, 2004.

[Kob84] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms*. Graduate texts in mathematics. Springer-Verlag, 1984.

[KY14] B. Klingler and A. Yafaev. "The André-Oort conjecture". In: *Annals of Mathematics* 180 (2014), pp. 867–952.

[Küh12] L. Kühne. "An effective result of André-Oort type". In: *Annals of Mathematics* 176.1 (2012), pp. 651–671.

[Mil06] J.S. Milne. *Elliptic Curves*. BookSurge Publishers, 2006, pp. 238+viii. ISBN: 1-4196-5257-5.

[Mir95] R. Miranda. *Algebraic Curves and Riemann Surfaces*. Graduate Studies in Mathematics. American Mathematical Society, 1995.

[Oor97] F. Oort. "Canonical liftings and dense sets of CM-points". In: *Arithmetic geometry (Cortona, 1994)* 37 (1997), pp. 228–234.

[Oss] B. Osserman. *Algebraic Geometry Notes: Complex Varieties and the Analytic Topology*. URL: `https://www.math.ucdavis.edu/~osserman/classes/248B-W12/notes/analytic.pdf`.

[Pil09] J. Pila. "Rational points of definable sets and results of André–Oort–Manin–Mumford type". In: *International Mathematics Research Notices* 2009.13 (2009), pp. 2476–2507.

[Ros94] J. Rosenberg. *Algebraic K-Theory and Its Applications*. Graduate Texts in Mathematics. Springer, 1994.

[Rot03] J.J. Rotman. *Advanced Modern Algebra*. Graduate Studies in Mathematics. American Mathematical Society, 2003.

[Ser73] J.P. Serre. *A Course in Arithmetic*. Graduate Texts in Mathematics. Springer, 1973.

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics. Springer, 2009.

[Tsi15] J. Tsimerman. "A proof of the Andre-Oort conjecture for A_g". In: *arXiv preprint arXiv:1506.01466* (2015).

[Wü14] G. Wüstholz. "A note on the conjectures of André–Oort and Pink". In: *Bulletin of the Institute of Mathematics, Academia Sinica (New Series)* 9 (2014), pp. 735–779.

[Yaf06] A. Yafaev. "A conjecture of Yves Andre's". In: *Duke Mathematical Journal* 132.3 (2006), pp. 393–407.

[ZM12] U. Zannier and D.W. Masser. *Some Problems of Unlikely Intersections in Arithmetic and Geometry*. Annals of mathematics studies. Princeton University Press, 2012.