TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

Diploma thesis

Elliptic curves and functions

Author:
Christoph Hutle
Hagenmüllergasse 33
1030 Vienna

Supervisor:
Univ.-Prof. Dipl.-Ing. Dr. Michael Drmota

August 30, 2012

To my parents, Dorothea and Ditmar Hutle.

Preface

This diploma thesis gives an overview of the extensive theory of elliptic functions and elliptic curves. The main focus is on the connection and overlappings of these theories: Using elliptic functions, it is possible to confer a group structure to many types of elliptic curves.

The first chapter introduces elliptic functions, doubly periodic, meromorphic functions on the complex plane. Some important properties are given about elliptic functions in general as well as for its prototype, the Weierstrass $\wp$-function.

The second chapter describes the basic theory of elliptic curves over arbitrary fields. While initially, the approach is completely different from the one in chapter 1, we see later, that we can use elliptic functions (and most of all $\wp$) to describe and even parametrize most of the elliptic curves. In the end of chapter 2, an outline to Mordells theory is given, which is an important result about the structure of elliptic curves over the field of rational numbers.

In the last chapter, we consider elliptic curves finite fields and introduce the L-series to an arbitrary elliptic curve, which contains information about the reduction of that curve modulo all primes. There are many useful results, but also open questions regarding these L-series. The most interesting open question is the conjecture of Birch and Swinnerton-Dyer, which is one of seven Millenium Prize Problems in mathematics. A small historical overview on the development of recent results is also stated.

Elliptic curves have applications in various fields of mathematics: Algebraic number theory (it is possible to prove Fermats Last Theorem using elliptic curves and modular forms), Cryptography (EEC-Cryptography is based on elliptic curves over finite fields) and different kinds of Analysis (many types of integrals can be solved by using elliptic functions).

I tried to write this thesis in a simple readable style, so that it can be well understood by any mathematician or physicist with basic knowledges in the fields of complex analysis, linear algebra, algebra and number theory.

Using this opportunity, I would like to give some acknowledges to several people, who supported me, while writing this thesis:

My special thanks goes on the first place to Prof. Dr. Michael Drmota, for his excellent assistance and supervision, when writing this thesis.

I also like to thank Prof. Dr. Hans Havlicek for his friendly support, not only in connection with my diploma thesis, but also during my time as a student assistant in the department of Differential Geometry and Geometric Structures. It was a honour to work with him and it also expanded my mathematical knowledge further.

Another thank goes to Iván Blanco for proofreading as well as to some of my fellow students: First of all Junjian Yang, for his local assistance when I was finishing my diploma thesis while being on a traineeship in Finland as well as for many good suggestions and constructive criticism to my work. And also to Florian Besau and Astrid Berg, for a very helpful collaboration during my whole study time in Vienna.

My studies and this thesis would not have been possible without the abiding support of my parents. I have to thank them a lot. I am also very grateful to Teresa Fritzsche, Thomas Mehlsack, Patricia Hesselaar, my sister Susanne Hutle and my brother Dr. Martin Hutle. They all supported me much.

Christoph Hutle, 2012

Contents

1 Elliptic functions **6**

1.1 Lattices . . . 6

1.2 Meromorphic functions . . . 11

1.3 Elliptic functions . . . 13

1.4 The $\wp$-function of Weierstrass . . . 17

1.5 Differential equations for the Weierstrass $\wp$-function. . . . 22

1.6 Conjugation-invariant lattices . . . 26

1.7 Discriminant and j-invariant of a given lattice . . . 27

1.8 Fourier series expansions of important parameters . . . 30

1.9 The inversion theorem . . . 32

1.10 The field of elliptic functions . . . 34

2 Elliptic curves **36**

2.1 The projective plane . . . 36

2.2 Planar curves . . . 37

2.3 Elliptic curves . . . 41

2.4 Elliptic curves over $\mathbb{C}$ and the inversion theorem . . . 47

2.5 Intersection formulas . . . 50

2.6 The Mordell-Weil Theorem . . . 53

3 L-functions and further applications **62**

3.1 Singular points . . . 62

3.2 Reduction modulo p . . . 65

3.3 Global minimal Weierstrass equations . . . 68

3.4 Dirichlet series and Euler products . . . 72

3.5 Zeta functions and L-functions . . . 75

3.6 Hasse's theorem . . . 77

3.7 The conjecture of Birch and Swinnerton-Dyer . . . 79

Chapter 1

Elliptic functions

In this chapter, I would like to give an overview over the wide-ranged theory of elliptic functions.

Elliptic functions are meromorphic periodic functions on the complex plane $\mathbb{C}$ with quite interesting and useful properties. Historically, elliptic functions were discovered as inverse functions of elliptic integrals; these in turn were studied in connection with the problem of the arc length of an ellipse, whence the name derives.

The most important elliptic function is the Weierstrass $\wp$-function. As a kind of prototype, we will be able to generate the field of all elliptic functions in an easy way from $\wp$ and its derivative $\wp'$.

Moreover, the Weierstrass $\wp$ function is the key to the connection between elliptic functions and elliptic curves, which we will discuss in chapter 2.

Most of the information given in this chapter is taken from [KK]. The study of elliptic functions is closely related to the study of modular functions and modular forms, a relationship proven by the modularity theorem. We won't outline this approach much, but further information can also be found in [KK]

1.1 Lattices

Our first aim is to study lattices on the n-dimensional euclidean space $\mathbb{R}^n$ over $\mathbb{R}$. As an important special case, we identify the two-dimensional euclidean space $\mathbb{R}^2$ with $\mathbb{C}$. All properties for lattices in $\mathbb{R}^2$ are absolutely the same for lattices in $\mathbb{C}$, since both have the same vector space structure over $\mathbb{R}$.

In section 1.2, we will see, how lattices in $\mathbb{C}$ appear as periods of some special class of meromorphic functions.

From now on, we will use the following unambigeous notation: For $C, D \subseteq$

$\mathbb{R}^n$ (resp. $\mathbb{C}$) and $\omega \in \mathbb{R}^n$ (resp. $\mathbb{C}$) we write $C + D$, $C\omega$ for

$$\begin{aligned} C + D &:= \{c + d : c \in C, d \in D\}. \\ C\omega &:= \{c\omega : c \in C\}. \end{aligned}$$

Definition 1.1.1. Let $\mathbb{R}^n$ be the n-dimensional euclidean space ($n \geq 1$). We call a subset Ω of $\mathbb{R}^n$ a *lattice*, if there exists a vector basis $\{\omega_1, \omega_2, \cdots, \omega_n\}$, such that $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 + \cdots + \mathbb{Z}\omega_n$. The n-tuple $(\omega_1, \omega_2, \cdots, \omega_n)$ is called a *basis* of the lattice Ω.

With Ω being a lattice in $\mathbb{R}^n$, quite obviously the set $\lambda\Omega := \{\lambda\Omega : \omega \in \Omega\}$ is also a lattice in $\mathbb{R}^n$, if $0 \neq \lambda \in \mathbb{R}$.

Definition 1.1.2. We call a closed subset D of a topological space X *discrete*, if for all $x \in X$ there exists a neighborhood U of x, such that $U \cap D$ is finite.

For our purpose, we will only need the case of X being the euclidean space $\mathbb{R}^n$.

In this case, *discrete* is equivalent to saying, that the set $\{z \in D : |z| \leq \rho\}$ is finite for all $\rho > 0$.

We will need the following proposition later:

Proposition 1.1.3. *Let $c_1, \ldots, c_n \in \Omega$ linear independent. Then, for $i = 1, \ldots, n$, we have the following: There are i linearly independent vectors $\omega_1, \ldots, \omega_n \in \Omega$ such that*

$$\begin{aligned} c_1 &= u_{11}\omega_1 \\ c_2 &= u_{21}\omega_1 + u_{22}\omega_2 \\ &\cdots \qquad\qquad\qquad\qquad \textit{where } u_{jk} \in \mathbb{Z}, u_{jj} \neq 0 \\ c_i &= u_{i1}\omega_1 + \cdots + u_{ii}\omega_i \end{aligned}$$

and

$$\text{lin}\{\omega_1, \ldots \omega_i\} \cap \Omega = \{u_1\omega_1 + \ldots u_i\omega_i : u_j \in \mathbb{Z}\}.$$

Proof. We prove this statement by induction: For $i = 1$, choose among all points of Ω on the line $\text{lin}\{c_1\}$ one with the minimum positive distance from 0, say ω_1. Since Ω is discrete, this is possible. Then the assertion above holds for $i = 1$ with this ω_1.

Next, let $i < n$ and assume, that the assertion above holds for i.

Consider the unbounded parallelotope

$$P = \{\alpha_1\omega_1 + \ldots \alpha_i\omega_i + \alpha c_{i+1} : 0 \leq \alpha_j < 1, \alpha \in \mathbb{R}\}.$$

All points of P, which are sufficiently far from 0 have arbitrarily large distance from $\text{lin}\{\omega_1, \ldots \omega_i\}$. Since $(P \cap \Omega) \backslash \text{lin}\{\omega_1, \ldots \omega_i\} \supseteq \{c_{i+1}\} \neq 0$ and since Ω is discrete, we thus may choose a point $\omega_{i+1} \in P \cap L$, which is not contained in $\mathrm{lin}\{\omega_1, \ldots, \omega_i\}$ and has minimum distance from $\mathrm{lin}\{\omega_1, \ldots, \omega_i\}$. Then

$$\omega_1, \ldots, \omega_i, \omega_{i+1} \in \Omega \text{ are linearly independent.} \tag{1.1}$$

Next, note that, for any point of Ω in $\mathrm{lin}\{\omega_1, \ldots \omega_1, \omega_{i+1}\}$, we obtain a point of P by adding a suitable integer linear combination of $\omega_1, \ldots, \omega_i$. These two points then have the same distance from $\mathrm{lin}\{\omega_1, \ldots \omega_i\}$. Thus, ω_{i+1} has minimum distance from $\mathrm{lin}\{\omega_1, \ldots \omega_i\}$, not only among all points of $(P \cap \Omega) \setminus \mathrm{lin}\{\omega_1, \ldots, \omega_1\}$, but also among all points of $(\mathrm{lin}\{\omega_1, \ldots, \omega_i, \omega_{i+1}\} \cap \Omega) \setminus \mathrm{lin}\{\omega_1, \ldots, \omega_i\}$. This yields, in particular,

$$\{\alpha_1 \omega_1 + \ldots \alpha_i \omega_i + \alpha_{i+1} \omega_{i+1} : 0 \leq \alpha_j < 1\} \cap \Omega = \{0\}. \tag{1.2}$$

We now show, that

$$\mathrm{lin}\{\omega_1, \ldots \omega_{i+1}\} \cap \Omega = \{u_1 \omega_1 + \ldots u_i \omega_i + u_{i+1} \omega_{i+1} : u_j \in \mathbb{Z}\}. \tag{1.3}$$

Let $x \in \mathrm{lin}\{\omega_1, \ldots \omega_{i+1}\} \cap \Omega$. Hence $x = u_1 \omega_1 + \cdots + u_{i+1} \omega_{i+1}$ with suitable $u_i \in \mathbb{R}$. Then

$$x - \lfloor u_1 \rfloor \omega_1 - \cdots - \lfloor u_{i+1} \rfloor \omega_{i+1} \in \{\alpha_1 \omega_1 + \ldots \alpha_{i+1} \omega_{i+1} : 0 \leq \alpha_j < 1\} \cap \Omega = \{0\}.$$

by (1.2) and thus $x = \lfloor u_1 \rfloor \omega_1 + \cdots + \lfloor u_{i+1} \rfloor \omega_{i+1}$. Comparing the two representations of x and taking into account the fact, that $\omega_1, \ldots \omega_{i+1}$ are linearly independent by (1.1), it follows that $u_j = \lfloor u_j \rfloor \in \mathbb{Z}$, for $j = 1, \ldots, i+1$. Thus, the left-hand side in (1.3) is contained in the right-hand side. Since the converse is obvious, the proof of (1.3) is complete.

By definition of ω_{i+1},

$$c_{i+1} \in (\mathrm{lin}\{\omega_1, \ldots, \omega_{i+1}\} \cap \Omega) \setminus \mathrm{lin}\{\omega_1, \ldots \omega_i\}.$$

Thus (1.3) yields

$$c_{i+1} = u_{i+1\,1} \omega_1 + \cdots + u_{i+1\,i+1} \omega_{i+1} \text{ where } u_{i+1\,j} \in \mathbb{Z}, u_{i+1\,i+1} \neq 0.$$

Considering this, the induction is complete, concluding the proof of the proposition. □

An important characterization of lattices is given by the following

Theorem 1.1.4. *Let $\Omega \subset \mathbb{R}^n$ be a lattice. Then the following statements are equivalent:*

1. *Ω is a lattice.*

2. *Ω is a discrete subgroup of $\mathbb{R}^n$, which is not contained in a hyperplane.*

Proof. (1) $\Rightarrow$ (2): Let $\{\omega_1, \ldots, \omega_n\}$ be a basis of Ω. If ℓ, m are integer linear combinations of $\omega_1, \ldots, \omega_n$, then so is $\ell - m$. Hence Ω is a sub-group of $\mathbb{R}^n$.

For the proof, that Ω is discrete, note that

$$\{\alpha_1\omega_1 + \cdots + \alpha_n\omega_n : -1 < \alpha_i < 1\} \cap \Omega = \{0\}. \tag{1.4}$$

Let $\rho > 0$ be the radius of a ball with centre at 0, which is contained in the open parallelotope in 1.4. Then the distance from 0 to any point of $\Omega\backslash\{0\}$ is at least ρ.

Therefore, we have $||\ell - m|| \geq \rho$ for $\ell, m \in \Omega$, $\ell \neq m$. If Ω is not discrete, it contains a bounded infinite subset. This subset then has at least one accumulation point. Any two distinct points of this subset, which are sufficiently close to the accumulation point, have distance less than ρ. This contradiction concludes the proof, that Ω is discrete.

Furthermore, Ω is not contained in a hyperplane since it contains the points 0, ω_1, $\ldots\omega_n$.

(2) $\Rightarrow$ (1): It is sufficient to show the following:
There are n linear independent vectors $\omega_1, \ldots, \omega_n \in \Omega$ such that

$$\Omega = \{u_1\omega_1 + \cdots + u_n\omega_n : u_i \in \mathbb{Z}\}. \tag{1.5}$$

This is an immediate consequence of the case $i = n$ of the proposition 1.1.3. □

Different bases of a given lattice are related in a rather simple way.

We call a quadratic matrix *unimodular*, if its determinant equals ±1. Therefore, unimodular integer $n \times n$-matrices are exactly the integer $n \times n$-matrices, which have an inverse integer matrix. Thus, we denote the set of all unimodular integer matrices with $\mathrm{GL}(n; \mathbb{Z})$.

Theorem 1.1.5. *Let $\{\omega_1, \ldots, \omega_n\}$ be a basis of a lattice Ω in $\mathbb{R}^n$. Then the following statements hold:*

1. *n vectors $\omega'_1, \ldots, \omega'_n$ belongs to Ω if and only if there exists an integer $n \times n$-matrix U with*

$$(\omega'_1, \ldots, \omega'_n) = (\omega_1, \ldots, \omega_n) \cdot U^T. \tag{1.6}$$

2. *$\{\omega'_1, \ldots, \omega'_n\}$ form a basis of Ω, if and only if U is unimodular, i.e. $U \in \mathrm{GL}(n; \mathbb{Z})$.*

Proof. 1.: This follows directly from the definition of a lattice, since each point of a lattice is an integer linear combination of $\{\omega_1, \ldots, \omega_n\}$.

2.: If $\{\omega'_1, \ldots, \omega'_n\}$ is also a basis of Ω, it follows from 1. that, conversely

$$(\omega_1, \ldots, \omega_n) = (\omega'_1, \ldots, \omega'_n) \cdot V^T, \tag{1.7}$$

where V is a suitable integer $n \times n$-matrix. From (1.6) and (1.7) we conclude that

$$(\omega_1', \dots, \omega_n') = (\omega_1, \dots, \omega_n)U^T = (\omega_1', \dots, \omega_n')V^T U^T = (\omega_1', \dots, \omega_n')(UV)^T.$$

Since $\omega_1', \dots, \omega_n'$ are linerly independent and thus $(\omega_1', \dots, \omega_n')$ is a non-singular $n \times n$-matrix, it follows that $\det(UV)^T = 1$ or $\det U \det V = 1$. Since U and V are integer matrices, their determinants are also integers. This shows $\det U = \pm 1$.

Conversely, if $U \in \mathrm{GL}(n; \mathbb{Z})$, there exists $V := U^{-1} \in \mathrm{GL}(n; \mathbb{Z})$ and (1.6) implies (1.7). Thus, every ω_i is an integer linear combination of the vectors $\omega_1', \dots, \omega_n'$. Since every vector of Ω is also an integer linear combination of $\omega_1, \dots, \omega_n$, it follows, that each vector of Ω is an integer linear combination of the vectors $\omega_1', \dots, \omega_n'$.

Since U is regular, $\omega_1', \dots, \omega_n'$ are also linearly independent.

Hence $\{\omega_1', \dots, \omega_n'\}$ form a basis. □

Corollary 1.1.6. *Let Ω be a lattice in $\mathbb{C}$ and (ω_1, ω_2) a basis of Ω. Then the following holds for $\omega_1', \omega_2' \in \mathbb{C}$:*

1. *ω_1' and ω_2' belong to Ω if and only if there exist (clearly unique) integers a, b, c, d, so that*

$$\begin{aligned} \omega_1' &= a\omega_1 + b\omega_2 \\ \omega_2' &= c\omega_1 + d\omega_2. \end{aligned}$$

2. *(ω_1', ω_2') form a basis of Ω, if and only if $ad - bc \neq 0$.*

Proof. This statement follows directly from theorem 1.1.5 by $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. □

Definition 1.1.7. Given a basis $\{\omega_1, \dots, \omega_d\}$ of a lattice Ω, the corresponding *fundamental parallelotope* $\diamond(\omega_1, \dots, \omega_n)$ is defined by:

$$\diamond(\omega_1, \dots, \omega_n) = \{\alpha_1\omega_1 + \dots + \alpha_n\omega_n : 0 \leq \alpha_i < 1\}. \tag{1.8}$$

This term is legitimated, because for all $v \in \mathbb{R}^n$, there exists a unique ω in Ω, so that $v - \omega \in \diamond(\omega_1, \dots, \omega_n)$.

In a similar way, we can define any *period parallelotope* to a given basis point $u \in \mathbb{R}^n$ by

$$\diamond(u; \omega_1, \dots, \omega_n) = \{u + \alpha_1\omega_1 + \dots + \alpha_n\omega_n : 0 \leq \alpha_i < 1\}. \tag{1.9}$$

Remark 1.1.8. The volume of $\diamond(\omega_1, \dots, \omega_n)$ is given by $|\det(\omega_1, \dots, \omega_n)|$, if $\omega_1, \dots, \omega_n$ is a basis of Ω. It follows from theorem 1.1.5, that this determinant is actually independent of the particular choice of a basis $\omega_1, \dots, \omega_n$ of Ω. Therefore every period parallelotope to a given lattice Ω has the same volume and we may denote this value by $\mathrm{Vol}\,\Omega$.

Let us again regard the case of the complex plane:

Corollary 1.1.9. *Let Ω be a lattice in $\mathbb{C}$. The area* $\operatorname{Vol}\Omega$ *of a fundamental parallelogram $\diamond(\omega_1, \omega_2)$ (and therefore of every period parallelogram too) is given by*

$$\operatorname{Vol}\Omega := |\Im(\omega_1 \cdot \overline{\omega_2})|.$$

where $\Im$ denotes the imaginary part of a complex number.

The formula is independent of the choice of the basis (ω_1, ω_2) of Ω.

Proof. It follows from remark 1.1.8 that

$$\operatorname{Vol}\Omega := \left|\det\begin{pmatrix} \Re(\omega_1) & \Re(\omega_2) \\ \Im(\omega_1) & \Im(\omega_2) \end{pmatrix}\right|.$$

Now, one may easily check, that $|\Re(\omega_1)\Im(\omega_2) - \Re(\omega_2)\Im(\omega_1)| = |\Im(\omega_1 \cdot \overline{\omega_2})|$. □

Further interesting results about lattices in euclidean vector spaces, like Minkowski's First and Second Fundamental Theorem or the Minkowski-Hlawka Theorem can be found in [PG].

With a view to elliptic curves, we will now fully constrain on lattices in $\mathbb{C}$.

1.2 Meromorphic functions

Definition 1.2.1. We call a function f *meromorphic* on $\mathbb{C}$, if there exists a closed, discrete subset $D_f \subset \mathbb{C}$, such that $f : \mathbb{C}\backslash D_f \to \mathbb{C}$ is holomorphic with poles at the points D_f.
If f is not holomorphically continuable in a point $c \in \mathbb{C}$, then it exists a positive integer m and a neighborhood U of c, such that

$$(z-c)^m \cdot f(z) \quad \text{is bounded at } U\backslash\{c\}. \tag{1.10}$$

In this case, we call c a *pole* of f.
If f is a meromorphic function, there is for every point $c \in \mathbb{C}$ an integer n, a neighborhood U of c and a holomorphic function $g : U \to \mathbb{C}$ with the property

$$f(z) = (z-c)^n \cdot g(z) \quad \text{for all } z \in U\backslash\{c\} \text{ and } g(c) \neq 0.$$

We then call $n =: \operatorname{Ord}_c f$ the *order of f in $\mathbb{C}$*.

(Therefore, each pole has negative order, each zero has positive order, depending on its multiplicity).

From the theory of complex analysis, recall the

Theorem 1.2.2 (Identity theorem)**.** *Let $G \subseteq \mathbb{C}$ be a domain and $f : G \to \mathbb{C}$ an analytic function in G. If the set $\{z \in G : f(z) = 0\}$ has an accumulation point in G, then $f = 0$.*

Lemma 1.2.3. *Let f, g be meromorphic functions. Then, αf $(\alpha \in \mathbb{C})$, $f + g$, $f \cdot g$ and $1/f$ are also meromorphic functions and it holds*

$$D_{\alpha f} = D_f,\ \alpha \neq 0, \quad D_{f+g} \subset D_f \cup D_g, \quad D_{fg} \subset D_f \cup D_g.$$

Proof. For αf, $f + g$ and $f \cdot g$, this is an immediate consequence of (1.10). From the identity theorem 1.2.2, it follows, that the zero set of a holomorphic function $f \neq 0$ is always discrete and closed in $\mathbb{C}$. Therefore, $1/f$ is meromorphic too. □

Corollary 1.2.4. *The set of all meromorphic functions on $\mathbb{C}$ form a field.*

We will denote this field with $\mathcal{M}$.

Next, we will study periods of meromorphic function. The fundamental-lemma will give a characterization of all types of periodic meromorphic functions.

Definition 1.2.5. Let f be a meromorphic function on $\mathbb{C}$. We call $\omega \in \mathbb{C}$ a *period* of f, if

- $D_f + \omega = D_f$ and
- $f(z + \omega) = f(z)$ for all $z \in \mathbb{C} \backslash D_f$

holds.

With $\operatorname{Per} f$, we denote the set of all periods of f. Obviously, $0 \in \operatorname{Per} f$ for every $f \in \mathcal{M}$ and it is also easy to see, that $\operatorname{Per} f$ is a subgroup of $(\mathbb{C}, +)$.

For a constant function f, $\operatorname{Per} f = \mathbb{C}$.

Lemma 1.2.6. *If $f \in \mathcal{M}$ is not constant,* $\operatorname{Per} f$ *is a closed subgroup of $(\mathbb{C}, +)$.*

Proof. If $\operatorname{Per} f$ is not discrete, there are pairwise different $\omega_n \in \operatorname{Per} f, n \geq 1$, so that $\lim_{n\to\infty} \omega_n$ exists. Since D_f is always closed, it follows $D_f + \omega = D_f$. Thus, if f is holomorphic in a point $c \in \mathbb{C}$, then f is also holomorphic in $c + \omega$. From $f(c) = f(c + \omega_n)$ for all $n \geq 1$, we now conclude that $f(c) = f(c + \omega)$, because f is particularly continuous. The identity theorem 1.2.2 now implies, that f is constant. □

Corollary 1.2.7 (fundamental-lemma)**.** *If $f \in \mathcal{M}$ is not constant, exactly one of the following cases occures:*

1. $\operatorname{Per} f = 0$

2. *There exists an $\omega_f \in \mathbb{C}\backslash\{0\}$ (unique except for the sign) such that* $\operatorname{Per} f = \mathbb{Z}\omega_f$.

3. $\operatorname{Per} f$ *is a lattice in* $\mathbb{C}$*, so* $\operatorname{Per} f = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ *with* $\omega_1, \omega_2 \in \mathbb{C}$ *linearly independent.*

   In this case, we can choose ω_1*,* ω_2 *such that* $\tau := \omega_1/\omega_2$ *meets* $\Im\tau > 0$ *and* $|\tau| \geq 1$.

Proof. If $\operatorname{Per} f \neq 0$, there exists an $\omega_f \in \operatorname{Per} f$ with

$$0 < |\omega_f| = \inf\{|\omega| : 0 \neq \omega \in \operatorname{Per} f\}.$$

Assume the case, that $\operatorname{Per} f$ lies completely on the line $\mathbb{R}\omega_f$. Then we can prove $\mathbb{Z}\omega_f = \operatorname{Per} f$ as follows:

$\mathbb{Z}\omega_f \subseteq \operatorname{Per} f$ is obvious, because $\operatorname{Per} f$ is a subgroup of $\mathbb{C}$. For $\omega \in \operatorname{Per} f$, there exists an $\alpha \in \mathbb{R}$ with $\omega = \alpha\omega_f$ according to our assumption. Choose $m \in \mathbb{Z}$ with $|\alpha - m| < 1$ and $|\omega - m\omega_f| = |\alpha - m| \cdot |\omega_f| < |\omega_f|$. Since ω, ω_f both belong to $\operatorname{Per} f$, $\omega - m\omega_f \in \operatorname{Per} f$ too, which implies $\omega = m\omega_f$, since $|\omega_f|$ was chosen minimal. Therefore $\mathbb{Z}\omega_f = \operatorname{Per} f$ is shown for this case.

In the other case $\operatorname{Per} f$ is a discrete subgroup (see 1.2.6), which is not contained in a line. By theorem 1.1.4, we see, that $\operatorname{Per} f$ is a lattice.

From the fact that ω_1, ω_2 are linearly independent over $\mathbb{R}$, it follows that $\Im\tau \neq 0$. Without loss of generality, we can say that $|\tau| > 0$ (otherwise we substitute ω_1 by $-\omega_1$. If required, we can also interchange ω_1, ω_2 so, that $|\omega_1| \geq |\omega_2|$ to obtain $|\tau| \geq 1$. □

The use of τ will turn out later.

1.3 Elliptic functions

In this section, $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ is always a lattice in $\mathbb{C}$.

Definition 1.3.1. A meromorphic function f on $\mathbb{C}$ is called *elliptic* relating to Ω, if Ω is contained in the set of periods of f, i.e. $\Omega \subseteq \operatorname{Per} f$.

This means:

- $D_f + \omega = D_f \quad \text{for all } \omega \in \Omega$
- $f(z + \omega) = f(z) \quad \text{for all } \omega \in \Omega \text{ and } z \in \mathbb{C}\backslash D_f$

These two conditions are already true, if they hold for a basis of Ω.

From the theory of complex analysis, we know, that for $0 \neq f \in \mathcal{M}$ and $c \in \mathbb{C}$, there exists a Laurent expansion of the form

$$f(z) = \sum_{n \geq m} a_n (z - c)^n, \quad a_m \neq 0,$$

which converges locally uniformly.

The *residuum* of f in c is given by $\operatorname{res}_c f := a_{-1}$.

The order $\operatorname{Ord}_c f$ of f in c (see definition 1.2.1) is in this representation quite obviously given by m.

If f is an elliptic function relating to Ω, $\omega \in \Omega$ and z any point in a suitable neighborhood of $c + \omega$, it follows from

$$f(z) = f(z - \omega) = \sum_{n \geq m} a_n(z - [c + \omega])^n,$$

that

$$\operatorname{Ord}_{c+\omega} f = \operatorname{Ord}_c f \quad \text{as well as} \operatorname{res}_{c+\omega} f = \operatorname{res}_c f \tag{1.11}$$

Hence, if c is a pole of f, $c + \omega$ is a pole too for every $\omega \in \Omega$. The same holds for zeros.

Since poles cannot accumulate in a compact set, we get:

Proposition 1.3.2. *The set of all elliptic functions relating to a lattice Ω form a subfield of $\mathcal{M}$, which contains all constant functions. We will denote this field by $\mathcal{K}(\Omega)$. Each $f \in \mathcal{K}(\Omega)$ has only finitely many poles in every period parallelogram.*

Lemma 1.3.3. *Let $f(z) \in \mathcal{K}(\Omega)$. Then also $f'(z) \in \mathcal{K}(\Omega)$ and $g(z) := f(nz + \omega) \in \mathcal{K}(\Omega)$, if $0 \neq n \in \mathbb{Z}, \omega \in \mathbb{C}$.*

Proof. Follows directly from definition 1.3.1 □

Now, we like to formulate four theorems about elliptic functions, which hearken back to Liouville. (Here, these are the theorems 1.3.4, 1.3.5, 1.3.7 and 1.3.9. All these theorems give important information about the structure of elliptic functions:

Theorem 1.3.4. *If $f \in \mathcal{K}(\Omega)$ is holomorphic, then f is already constant.*

Proof. Let P be a period parallelogram. Since the closure of P is compact, f is bounded, i.e. there exists a $C > 0$ such that $|f(z)| \leq C$ for all $z \in P$. For arbitrary $z \in \mathbb{C}$, there exists an $\omega \in \Omega$ such that $z + \omega \in P$. Now we see from $|f(z)| = |f(z + \omega)| \leq C$, that f is bounded in $\mathbb{C}$. The classic Liouville theorem then yields, that f is constant. □

Theorem 1.3.5. *Consider $f \in \mathcal{K}(\Omega)$ and P a period parallelogram of Ω. Then*

$$\sum_{c \in P} \operatorname{res}_c f = 0. \tag{1.12}$$

Proof. The number of poles of f in P is finite, hence the sum is finite. Because of (1.11), the sum (1.12) is also not dependent on the choice of the period parallelogram. Hence, we can choose the basis point u without loss of generality so, that no singularities lie on the boundary ∂P of P. Now, we consider the integral of f along ∂P.

From the residue theorem, we obtain

$$\begin{aligned} \pm\ & 2\pi i \sum_{c\in P} \operatorname{res}_c f \\ = & \int_u^{u+\omega_1} f(z)\,dz + \int_{u+\omega_1}^{u+\omega_1+\omega_2} f(z)\,dz + \int_{u+\omega_1+\omega_2}^{u+\omega_2} f(z)\,dz + \int_{u+\omega_2}^{u} f(z)\,dz \\ = & \int_u^{u+\omega_1} (f(z) - f(z+\omega_2))\,dz + \int_{u+\omega_2}^{u} (f(z) - f(z+\omega_1))\,dz. \end{aligned}$$

Since $f \in \mathcal{K}(\Omega)$, the right-hand side equals 0. □

Corollary 1.3.6. *Each elliptic function with period parallelogram P, that is not constant, has either a pole of order* 2 *(with residue* 0*) or at least two different poles in P.*

Proof. This follows directly from theorem 1.3.4 and theorem 1.3.5. □

Theorem 1.3.7. *If $f \in \mathcal{K}(\Omega)$ is not constant and P a period parallelogram of Ω, then for each $\omega \in \mathbb{C}$ it holds*

$$\sum_{c\in P} \operatorname{Ord}_c(f-\omega) = 0. \tag{1.13}$$

Therefore, the number of poles of f in P equals the number of ω-points of f in P for all $\omega \in \mathbb{C}$, if we count multiplicities.

In particular, we see that each non constant $f \in \mathcal{K}(\Omega)$ takes on every value in $\mathbb{C}$.

Proof. Because of Lemma 1.3.3, the function $g(z) := \frac{f'(z)}{f(z)-\omega}$ is also elliptic relating to Ω.

We now show, that

$$\operatorname{res}_c g = \operatorname{Ord}_c(f-\omega). \tag{1.14}$$

For $n := \operatorname{Ord}_c(f-\omega) = 0$, this is trivial. So assume, that $n \neq 0$. We then can write $f(z) - \omega = (z-c)^n \cdot h(z)$ with a suitable holomorphic function h. From

$$g(z) = \frac{f'(z)}{f(z)-\omega} = \frac{(z-c)^n h'(z) + n(z-c)^{n-1}h(z)}{(z-c)^n h(z)} = \frac{n}{z-c} + \frac{h'(z)}{h(z)},$$

we obtain (1.14), since h(z) is holomorphic.

Then, (1.13) follows from theorem 1.3.5.

Since f is not constant, if follows from theorem 1.3.4, that f has at least one pole in P. So the add-on is also true. □

From the theory of complex analysis, we obtain the following theorem:

Theorem 1.3.8 (theorem of the zero-counting integral)**.** *Let f be a meromorphic function on a domain $D \subseteq \mathbb{C}$. Then, for a smooth, closed and rectifiable curve $\gamma \subset D$ which does not contain any poles and zeros, the following equation holds:*

$$\frac{1}{2\pi i}\int_\gamma \frac{f'(z)}{f(z)}\,dz = N_f - P_f,$$

where N_f and P_f denote the number of zeros resp. poles of f in the inner of γ.

Theorem 1.3.9. *Let $0 \neq f \in \mathcal{K}(\Omega)$ and P a period parallelogram, then*

$$\sum_{c\in P}(\operatorname{Ord}_c f)\cdot c \in \Omega \tag{1.15}$$

holds.

Proof. For the proof, we use the same method as in theorem 1.3.5. From theorem 1.3.8, we obtain

$$\begin{aligned} 2\pi i\sum_{c\in P}(\operatorname{Ord}_c f)\cdot c &= \int_{\partial P} z\cdot\frac{f'(z)}{f(z)}\,dz \\ = \quad & \pm\Big(\int_u^{u+\omega_1} z\frac{f'(z)}{f(z)} - (z+\omega_2)\frac{f'(z+\omega_2)}{f(z+\omega_2)}\,dz + \\ + \quad & \int_{u+\omega_2}^{u} z\frac{f'(z)}{f(z)} - (z+\omega_1)\frac{f'(z+\omega_1)}{f(z+\omega_1)}\,dz\Big) \\ = \quad & \pm\left(\omega_1\int_u^{u+\omega_2}\frac{f'(z)}{f(z)}\,dz - \omega_2\int_u^{u+\omega_1}\frac{f'(z)}{f(z)}\,dz\right). \end{aligned}$$

The last equality follows from periodicity, i.e. $f(z) = f(z+\omega_j)$. From the theory of complex analysis, we then know, that $\int_u^{u+\omega_j}\frac{f'(z)}{f(z)}\,dz \in 2\pi i\mathbb{Z}$ for $j \in \{1,2\}$. So, (1.15) is proven. □

If we count poles and zeros of a non-constant $f \in \mathcal{K}(\Omega)$ with multiplicities, we get from theorem 1.3.7 points $a_1,\ldots,a_r$ and $b_1,\cdots,b_r$ in P, such that f has zeros exactly in $a_1,\cdots,a_r$ and poles exactly in $b_1,\ldots,b_r$. Multiplicity is in both cases expressed by the number of repetitions of the point.

With this notation, theorem 1.3.9 means

$$a_1+\cdots+a_r \equiv b_1+\cdots+b_r \mod \Omega. \tag{1.16}$$

r is called the *order* of the elliptic function f.

Theorem 1.3.4 states, that every elliptic function of order 0 is constant. Corollary 1.3.6 predicates, that there is no elliptic function of order 1.

Later, we will see, that $r \geq 2$ and (1.16) is already sufficient for the existence of an elliptic function with the specified poles and zeros.

1.4 The $\wp$-function of Weierstrass

We now define, what will turn out to be a key example of an elliptic function relative to a given lattice Ω. This function is called the *Weierstrass $\wp$-function.* It is denoted $\wp_\Omega$ or simply $\wp$, if the lattice is fixed throughout the discussion. We set

$$\wp := \wp_\Omega := z^{-2} + \sum_{0 \neq \omega \in \Omega} \left((z-\omega)^{-2} - \omega^{-2} \right), \, z \in \mathbb{C} \backslash \Omega. \tag{1.17}$$

It is not obvious to see, why the sum in (1.17) is convergent and $\wp$ is a well-defined function. To see this, we will first need to collect some information about multiple infinite series.

To a given lattice $\Omega \in \mathbb{C}$ with basis $\{\omega_1, \omega_2\}$, we define

$$\delta := \delta(\omega_1, \omega_2) := \sup\{|z - \omega| : z, \omega \in \diamond(\omega_1, \omega_2)\}$$

as the *diameter* of the fundamental parallelogram. For $\rho > 0$, let A_ρ be the number of lattice points in the closed circle around 0 with radius ρ, i.e.

$$A_\rho := \#\{\omega \in \Omega : |\omega| \leq \rho\}.$$

Lemma 1.4.1. *For all $\rho \geq \delta$,*

$$\frac{\pi}{\operatorname{Vol}\Omega}(\rho - \delta)^2 \leq A_\rho(\Omega) \leq \frac{\pi}{\operatorname{Vol}\Omega}(\rho + \delta)^2.$$

Proof. We compare the sets

$$K_\rho := \{z \in \mathbb{C} : |z| \leq \rho\} \quad \text{and} \quad M_\rho := \bigcup_{\omega \in \Omega, |\omega| \leq \rho} \diamond(\omega; \omega_1, \omega_2)$$

and their areas $\pi\rho^2$ resp. $\operatorname{Vol}\Omega \cdot A_\rho(\Omega)$. From the definition of δ, it follows, that

$$K_{\rho-\delta} \subset M_\rho \subset K_{\rho+\delta}.$$

Regarding the areas, this yields

$$\pi(\rho - \delta)^2 \leq A_\rho(\Omega) \cdot \operatorname{Vol}(\Omega) \leq \pi(\rho + \delta)^2,$$

hence the assertion. □

Lemma 1.4.2 (convergence-lemma)**.**

The series $\sum_{0 \neq \omega \in \Omega} |\omega|^{-\alpha}$ converges, if $\alpha > 2$.

Proof. For a finite set $\emptyset \neq E \subset \Omega\backslash\{0\}$, define $M := \max\{|\omega| : \omega \in E\}$. From lemma 1.4.1, we obtain a $c_2 > 0$ with

$$A_{n+1}(\Omega) - A_n(\Omega) \leq \frac{\pi}{\operatorname{Vol}\Omega}[(n+1+\delta)^2 - (n-\delta)^2] \leq c_2 n$$

□

for all $n \geq \delta$. With

$$c_1 := \sum_{0\neq\omega\in\Omega, |\omega|\leq\delta+1} |\omega|^{-\alpha}$$

we get

$$\begin{aligned} \sum_{\omega\in E} |\omega|^{-\alpha} &\leq \sum_{n\in\mathbb{N},\, \delta<n<M} (A_{n+1}(\Omega) - A_n(\Omega))n^{-\alpha} \\ &\leq c_1 + c_2 \sum_{n=1}^{\infty} n^{1-\alpha} =: C < \infty. \end{aligned}$$

Remark 1.4.3. It also holds, that the series $\sum_{0\neq\omega\in\Omega} |\omega|^{-\alpha}$ does not converge, if $\alpha \leq 2$. For $\alpha \leq 0$, this is trivial, for $0 < \alpha \leq 2$, this is proven in [KK], 1.9.

Corollary 1.4.4. *The so-called* Eisenstein series

$$G_k := G_k(\Omega) := \sum_{0\neq\omega\in\Omega} \omega^{-k} \quad \textit{for } k \geq 3 \tag{1.18}$$

are absolutely convergent. For odd $k \geq 3$, $G_k(\Omega) = 0$.

Proof. The absolute convergence follows directly from lemma 1.4.2.

Since an absolutely convergent series can be rearranged according to the Riemann series theorem and because for each $\omega \in \Omega$ also $-\omega \in \Omega$, we obtain $G_k = (-1)^k G_k$, so $G_k = 0$, if k is odd. □

Remark 1.4.5. Regarding the Fourier series expansion of G_k, it outcomes, that $G_k \neq 0$, if k is even.

Lemma 1.4.6. *Let* $K \subset \{(\omega_1, \omega_2) \in \mathbb{C}\times\mathbb{C}; \omega_2 \neq 0, \omega_1/\omega_2 \notin \mathbb{R}\}$ *be a compact set. Then, there exist absolute terms* α, β, *such that*

$$\beta|m_1 i + m_2| \leq |m_1\omega_1 + m_2\omega_2| \leq \alpha|m_1 i + m_2| \tag{1.19}$$

for all $m_1, m_2 \in \mathbb{R}$ *and* $(\omega_1, \omega_2) \in K$.

Proof. For $m_1, m_2 = 0$, the statement is trivial.

Elsewise, choose $r > 0$ such that $m_1^2 + m_2^2 = r^2$, i.e. $|m_1 i + m_2| = r$. The continuous function $(\omega_1, \omega_2, m_1, m_2) \to |m_1\omega_1 + m_2\omega_2|$ takes on a maximum a and a minimum b on the compact set $K \times \{(m_1, m_2) \in \mathbb{R}\times\mathbb{R} : m_1^2 + m_2^2 = r^2\}$. Since ω_1 and ω_2 are linearly independent over $\mathbb{R}$, $m_1\omega_1 + m_2\omega_2 \neq 0$ holds. Define $\alpha := a/r$ and $\beta = b/r$. Both are positive values, which satisfy (1.19). □

Proposition 1.4.7. *The series of the function*

$$\wp(z;\omega_1,\omega_2) := z^{-2} + \sum_{0\neq\omega\in\mathbb{Z}\omega_1+\mathbb{Z}\omega_2} \left((z-\omega)^{-2} - \omega^{-2}\right),\ z \in \mathbb{C}\backslash\Omega.$$

is absolutely and uniformly convergent on each compact set in

$$\{(z;\omega_1,\omega_2) \in \mathbb{C}\times\mathbb{C}\times\mathbb{C} : \omega_2 \neq 0, \omega_1/\omega_2 \notin \mathbb{R}, z \notin \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2\}. \quad (1.20)$$

Proof. Let K be such a compacta in (1.20). We choose $\rho > 0$ such that

$$K \subset K_\rho \times K', \quad K_\rho := \{z \in \mathbb{C} : |z| \leq \rho\}.$$

For K', we choose β like in lemma 1.4.6. Then for all $(z;\omega_1,\omega_2) \in K$ and $(m_1, m_2) \in \mathbb{Z}$ with $|m_1 i + m_2| \geq (\rho+1)/\beta$, it holds, that $|\omega| \geq \rho + 1$ for $\omega = m_1\omega_1 + m_2\omega_2$.

Therefore,

$$\begin{aligned}\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| &= \left|\frac{2z\omega - z^2}{\omega^2(z-\omega)^2}\right| = \left|\frac{2 - z/\omega}{(1-z/\omega)^2}\right| \cdot \frac{|z|}{|\omega|^3} \\ &\leq \frac{3}{(1-\rho/(\rho+1))^2} \cdot \frac{\rho}{|\omega|^3} \leq \frac{3\rho(\rho+1)^2}{\beta^3|m_1 i + m_2|^3}.\end{aligned}$$

Since there are only finitely many tuples $(m_1, m_2) \in \mathbb{Z}\times\mathbb{Z}$ with $|m_1 i + m_2| \leq (\rho+1)/\beta$, the statement follows from the absolute convergence of the Eisenstein series $G_3(\mathbb{Z}i + \mathbb{Z})$ (see corollary 1.4.4). □

Quite analogously, we get the following result:

Lemma 1.4.8. *For $k \in \mathbb{N}$, $k \geq 3$ and a fixed lattice Ω, the series*

$$\sum_{\omega\in\Omega} (z-\omega)^{-k}$$

converges absolutely and uniformly on every compacta in $\mathbb{C}\backslash\Omega$.

Proposition 1.4.9. *The Weierstrass $\wp$-function*

$$\wp(z) := \wp_\Omega(z) := z^{-2} + \sum_{0\neq\omega\in\Omega} \left((z-\omega)^{-2} - \omega^{-2}\right),\ z \in \mathbb{C}\backslash\Omega. \quad (1.21)$$

is absolutely and uniformly convergent in every compacta of $\mathbb{C}$, which does not contain a lattice point. $\wp$ is an even elliptic function with respect to Ω and has poles of order 2 in the lattice points of Ω with residue 0. In $\mathbb{C}\backslash\Omega$, $\wp$ is holomorphic.

The Laurent expansion at the point 0 has the form

$$\wp(z) = z^{-2} + a_2 z^2 + \dots \quad (1.22)$$

Proof. The convergence follows directly from proposition 1.4.7.

We set $\rho > 0$ arbitrary and $K_\rho := \{z \in \mathbb{C} : |z| < \rho\}$. Now we split

$$\wp(z) = z^{-2} + \sum_{\omega < \rho+1} \left((z-\omega)^{-2} - \omega^{-2}\right) + \sum_{|\omega| \geq \rho+1} \left((z-\omega)^{-2} - \omega^{-2}\right).$$

Here, the first finite sum is meromorphic on K_ρ. The second sum is holomorphic on K_ρ because of proposition 1.4.7. Hence $\wp|_{K_\rho}$ has poles exactly in the points $\Omega \cap K_\rho$. These poles are of order 2 and have residue 0.

To see, that $\wp$ is an even function, note, that $\wp(-z) = \wp(z)$, since the right side of (1.21) remains unchanched, if z is replaced by $-z$ and ω is replaced by $-\omega$. But summing over $\omega \in \Omega$ is the same as summing over $-\omega \in \Omega$.

Substituting z by 0 in the sum of (1.21), we obtain 0, hence the Laurent expansion at 0 has the constant coefficient 0. Since $\wp$ is even, all odd coefficients vanish. This yields (1.22).

It remains to show the periodicity, i.e. $\wp(z+\omega) = \wp(z)$ for all $\omega \in \Omega$ and $z \in \mathbb{C}\backslash\Omega$, so that $\wp$ is an elliptic function.

Because the expression in (1.21) is convergent, we can regard the derivative of $\wp$.

$$\wp'(z) = -2 \sum_{\omega \in \Omega} (z-\omega)^{-3}, \quad z \in \mathbb{C}\backslash\Omega. \tag{1.23}$$

This series is also convergent due to lemma 1.4.8. Since replacing z by $z+\omega$ merely rearranges the terms in the sum in (1.23), it follows, that $\wp'(z+\omega) = \wp'(z)$ for $\omega \in \Omega$. For a basis ω_1, ω_2 of Ω, we then get $\wp(z+\omega_j) = \wp(z) + c_j$ with absolute values c_j and $j \in \{1,2\}$. If we set $z = \omega_1/2$ resp. $z = \omega_2/2$, we obtain $c_1 = c_2 = 0$, since $\wp$ is an even function. Therefore $\wp(z+\omega_j) = \wp(z)$ for $j \in \{1,2\}$ and since (ω_1, ω_2) form a basis, $\wp$ has all $\omega \in \Omega$ as periods. □

Remark 1.4.10. From proposition 1.4.9, we see, that $\wp'$ is an odd function with poles of order 3 at the lattice points Ω. On $\mathbb{C}\backslash\Omega$, $\wp'$ is holomorphic.

Let us now specify the zeros of $\wp'$:

Lemma 1.4.11. *For $\omega \in \Omega$ and $\omega/2 \notin \Omega$, it holds, that $\omega/2$ is a zero of order* 1 *of $\wp'$. Conversely, every zero of $\wp'$ has this form.*

Proof. From periodicy and since $\wp'$ is an odd function, we get $\wp'(z+\omega) = \wp'(z) = -\wp'(-z)$. If $\omega/2 \notin \Omega$, i.e. $\omega/2$ is no pole of $\wp$ and $\wp'$, we may set $z := -\omega/2$ and obtain $\wp'(\omega/2) = -\wp'(\omega/2)$, hence $\wp'(\omega/2) = 0$.

To proof the converse, let ω_1, ω_2 be a basis of Ω. In the fundamental parallelogram $P := \diamond(\omega_1, \omega_2)$, we have at least three different zeros at the points $\omega_1/2$, $\omega_2/2$ and $(\omega_1+\omega_2)/2$. In remark 1.4.10, we saw, that $\wp'$ has only one pole in P at the point 0. That pole has order 3. Due to theorem

1.3.7, the number of zeros of $\wp'$ in P equals the number of poles of $\wp'$ in P, counting multiplicities.

Therefore, these three zeros are already all zeros of $\wp'$ in P and all of them have order 1.

So, if z is an arbitrary zero of $\wp'$, then there exists $\omega' \in \Omega$ with $z - \omega' \in P$. Then $z - \omega'$ is one of the three points $\omega_1/2$, $\omega_2/2$, $(\omega_1 + \omega_2)/2$. So z also has the form $z = \omega/2$ with $\omega \in \Omega$ and $\omega/2 \notin \Omega$. □

Now let us regard zeros (or more generally ω-points) of $\wp$ itself:

Lemma 1.4.12. *Let P be an arbitrary period parallelogram of Ω. For each $z \in \mathbb{C}$ with*

$$z \neq \wp(\omega/2), \quad \textit{for all } \omega \in \Omega, \quad \textit{such that } \omega/2 \notin \Omega, \tag{1.24}$$

there are exactly two different points $u, v \in P$ with $\wp(u) = \wp(v) = z$. In this case, $u + v \in \Omega$.

Conversely, if there are two different $u, v \in P$ with $\wp(u) = \wp(v) = z$, then (1.24) holds.

Proof. Since there is only one pole of $\wp$ in P of order 2, it follows from 1.3.7, that the number of z-points in P (counting multiplicities) is also 2. Now distinguish the following cases:

- There is only one $u \in P$ with $\wp(u) = z$. Then u is a z-point of order 2 and it follows, that $\wp'(u) = 0$. From lemma 1.4.11, we then get a contradiction to our condition (1.24).
- There are two different points $u, v \in P$ with $\wp(u) = \wp(v) = z$. It then follows from theorem 1.3.9, that $u + v \in \Omega$.

□

To summarize, let ω_1, ω_2 be a basis of Ω and $P := \diamond(\omega_1, \omega_2)$ the corresponding fundamental parallelogram. Using the notation

$$e_k := \wp(\omega_k/2), \quad k \in \{1,2,3\} \text{ with } \omega_3 := \omega_1 + \omega_2, \tag{1.25}$$

we obtain from lemma 1.4.11 and lemma 1.4.12, that

$$\wp(z) - e_k \text{ has exactly one zero of order 2 in } P \text{ for } k \in \{1,2,3\} \tag{1.26}$$

$$\wp(z) - \omega \text{ has two zeros of order 1 in } P \text{ for } \omega \notin \{e_1, e_2, e_3\} \tag{1.27}$$

Since $\omega_1, \omega_2, \omega_3$ are all pairwise disjoint, (1.26) yields, that

$$e_1, e_2, e_3 \text{ are pairwise disjoint.} \tag{1.28}$$

The definition of e_1, e_2, e_3 depends on the elected basis, but a basis change only permutates these values.

1.5 Differential equations for the Weierstrass $\wp$-function.

Next, we want to give two important differential equations for $\wp$. We will need these results later.

Theorem 1.5.1. *For all $z \in \mathbb{C}\backslash\Omega$, the equation*

$$\wp'^2(z) = 4 \cdot (\wp(z) - e_1) \cdot (\wp(z) - e_2) \cdot (\wp(z) - e_3) \tag{1.29}$$

holds.

Proof. Let P again be the fundamental parallelogram $\diamond(\omega_1, \omega_2)$. Regard the elliptic function

$$f(z) := 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)$$

From (1.26), we see, that f has zeros exactly at the points $\omega_1/2, \omega_2/2, \omega_3/2$, all of them of order 2. Lemma 1.4.11 implies, that the same holds for $\wp'^2$. As a product of three functions with a pole of order 2 in 0, f has a pole of order 6 at 0. This is the only pole of f in P. From the formula (1.23), we see, that $\wp'^2$ also has a pole of order 6 at 0. From theorem 1.3.7, we obtain, that this is the only pole of $\wp'^2$ in P.

Therefore, the function $\wp'^2/f$ is an elliptic function without poles, i.e. holomorphic and because of theorem 1.3.4 constant.

Since the coefficient of z^{-6} in the Laurent expansion at 0 equals 4 in both cases, we see, that this constant value is 1. Hence, $\wp'^2 = f$. □

For the second important differential equation for $\wp$, we first need to calculate the coefficient in the Laurent expansion (1.22).

For this, consider again the Eisenstein series

$$G_k := G_k(\Omega) := \sum_{0 \neq \omega \in \Omega} \omega^{-k} \quad \text{for } k \geq 4 \text{ even,} \tag{1.30}$$

from corollary 1.4.4. Also in corollary 1.4.4, we saw, that for odd $k \geq 3$, the series G_k equals 0.

Setting

$$\gamma := \gamma(\Omega) := \min\{|\omega| : 0 \neq \omega \in \Omega\}$$

we get the following

Theorem 1.5.2. *For all $z \in \mathbb{C}$ and $0 < |z| < \gamma(\Omega)$, we have the Laurent expansion*

$$\wp(z) = z^{-2} + \sum_{n=2}^{\infty} (2n-1) G_{2n} \cdot z^{2n-2} = z^{-2} + 3G_4 z^2 + 5G_6 z^4 + 7G_8 z^6 + \ldots \tag{1.31}$$

Proof. Since

$$\frac{1}{(1-t)^2} = \frac{d}{dt}\left(\frac{1}{1-t}\right) = \sum_{m=1}^{\infty} mt^{m-1} \quad \text{for } |t| < 1,$$

we get for an arbitrary $\omega \in \mathbb{C}\backslash\{0\}$

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \frac{1}{\omega^2}\left(\frac{1}{(1-\frac{z}{\omega})} - 1\right) = \sum_{m=2}^{\infty} m \cdot \frac{z^{m-1}}{\omega^{m+1}}, \quad |z| < \gamma,$$

and therefore

$$\wp(z) = z^{-2} + \sum_{0 \neq \omega \in \Omega} \left(\sum_{m=2}^{\infty} m \cdot \frac{z^{m-1}}{\omega^{m+1}}\right), \quad 0 < |z| < \gamma. \tag{1.32}$$

Because of

$$\left| m \cdot \frac{z^{m-1}}{\omega^{m+1}} \right| \leq \gamma m \left(\frac{|z|}{\gamma}\right)^{m-1} \cdot |\omega|^{-3}$$

and the convergence lemma 1.4.2, the series in (1.32) is absolutely convergent in both m and ω.

Now, we may rearrange the series according to the Riemann series theorem and so we get

$$\wp(z) = z^{-2} + \sum_{m \geq 2} mG_{m+1} \cdot z^{m-1}, \quad 0 < |z| < \gamma.$$

Since $G_k = 0$ for odd k, as seen in corollary 1.4.4, the statement is proven. □

Definition 1.5.3. The so-called *Weierstrass-invariants* g_2, g_3 are given by

$$g_2 := g_2(\Omega) := 60G_4(\Omega) \tag{1.33}$$

$$g_3 := g_3(\Omega) := 140G_6(\Omega) \tag{1.34}$$

This notation is quite standard in the literature.

The indication *invariants* will explain itself later.

Now we can state the second differential equation for $\wp$:

Theorem 1.5.4. *The Weierstrass $\wp$-function meets the following differential equation:*

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3. \tag{1.35}$$

Proof. To ease our notation in the proof, we use the *Landau*-notation:

If for a function f, there exists a constant C, such that $|f(z)| \leq C|z|^k$ for all z in a suitable neighborhood of 0, we shortly write $\mathcal{O}(z^k)$ for it.

Based on

$$\wp(z) = z^{-2} + 3G_4 z^2 + 5G_6 z^4 + \mathcal{O}(z^6), \tag{1.36}$$

(see 1.31), we calculate

$$\begin{aligned} \wp^2(z) &= z^{-4} + 6G_4 + 10G_6 z^2 + \mathcal{O}(z^3), \\ \wp^3(z) &= z^{-6} + 9G_4 z^{-2} + 15G_6 + \mathcal{O}(z), \\ \wp'(z) &= -2z^{-3} + 6G_4 z + 20G_6 z^3 + \mathcal{O}(z^4), \\ \wp'^2(z) &= 4z^{-6} - 24G_4 z^{-2} - 80G_6 + \mathcal{O}(z). \end{aligned}$$

Using definition 1.5.3, we then get

$$\wp'^2(z) - 4\wp^3(z) + g_2\wp(z) + g_3 = \mathcal{O}(z). \tag{1.37}$$

As a linear combination of $\wp$ and $\wp'$, the left-hand side of (1.37) is an elliptic function with poles only in Ω. But (1.37) also includes, that the left-hand-side is holomorphic at 0 and therefore a globally holomorphic function. From theorem 1.3.4, it follows, that this function is constant. Again due to 1.37, we see, that

$$\wp'^2(z) - 4\wp^3(z) + g_2\wp(z) + g_3 = 0.$$

□

Corollary 1.5.5. *Another differential equation for $\wp$ is given by*

$$2\wp'' = 12\wp^2 - g_2 \tag{1.38}$$

Proof. This follows immediately by differentiating equation (1.35). □

Proposition 1.5.6. *For $n \geq 4$, we have the recursion formula*

$$(n-3)(2n+1)(2n-1)G_{2n} = 3 \cdot \sum_{\substack{p\geq 2, q\geq 2 \\ p+q=n}} (2p-1)(2q-1)G_{2p}G_{2q}. \tag{1.39}$$

Proof. We insert the Laurent series (1.31) into the differential equation (1.38) and obtain

$$\begin{aligned} &\sum_{n\geq 2}(2n-1)(2n-2)(2n-3)G_{2n}z^{2n-4} + 30G_4 \\ &= 12\sum_{n\geq 2}(2n-1)G_{2n}z^{2n-4} + 6\sum_{p\geq 2}\sum_{q\geq 2}(2p-1)(2q-1)G_{2p}G_{2q}z^{2p+2q-4}. \end{aligned}$$

A comparison of coefficients yields the wanted result. □

This formula specially implies

$$\begin{aligned} 7G_8 &= 3G_4^2, \\ 11G_{10} &= 5G_4G_6, \\ 143G_{12} &= 42G_4G_8 + 25G_6^2 = 18G_4^3 + 25G_6^2. \end{aligned}$$

Corollary 1.5.7. *For $k \geq 8$, we have*

$$G_k \in \mathbb{Q}[G_4, G_6].$$

Proof. This is an immediate consequence of proposition 1.5.6. □

Theorem 1.5.8. *Let Ω be a lattice in $\mathbb{C}$ and g_2, g_3 its Weierstrass invariants. Then, each meromorphic, non-constant solution f of the differential equation*

$$f'^2 = 4f^3 - g_2 f - g_3$$

in a domain $G \subset \mathbb{C}$ is given by $f(z) = \wp(z+w), z \in \mathbb{C}$ with a suitable $w \in \mathbb{C}$. For $f \in \mathcal{M}$ being such a solution, Ω is the corresponding lattice of f.

Therefore, the lattice Ω is uniquely determined by $g_2(\Omega)$ and $g_3(\Omega)$, resp. by $G_4(\Omega)$ and $G_6(\Omega)$.

Proof. Let f be a meromorphic and non-constant solution of the given differential equation in a domain $G \subset \mathbb{C}$. If f is holomorphic in a disc $U \subset G$ with center u and $f' \neq 0$ in U, then we can choose a suitable square root to obtain $f' = \sqrt{4f^3 - g_2 f - g_3}$. Due to lemma 1.4.12, we may choose a $w \in \mathbb{C}$, such that $\wp(w+u) = f(u)$. By substituting w by $-w-2u$ if necessary, we may additionally assume, that $\wp'(w+u) = f'(u)$.

So, the two functions $f(z)$ and $g(z) := \wp(z+w)$ both conform to the same differential equation of first order and accord at the point u. So it follows from the existence and uniqueness theorem of Picard-Lindelöf, that $f(z) = g(z)$ for all $z \in U$. The identity theorem 1.2.2 then implies, that $f(z) = g(z)$ globally, since the set of zeros of the difference function $(f-g)(z)$ has every point in U as an accumulation point.

Because for the $\wp$-function the set of poles equals the period lattice, Ω is also the corresponding period lattice of f.

Together with corollary 1.5.7, this yields, that Ω is already uniquely determined by g_2 and g_3. □

We will see later, that for any two values $c_2, c_3 \in \mathbb{C}$ such that $c_2^3 - 27c_3^2 \neq 0$, there exists a lattice Ω, such that $c_2 = g_2(\Omega)$ and $c_3 = g_3(\Omega)$.

Theorem 1.5.9. *For an indeterminate x, it holds, that*

$$4x^3 - g_2 x - g_3 = 4(x-e_1)(x-e_2)(x-e_3). \tag{1.40}$$

Proof. Since $\wp$ takes on at least three different values, we obtain this result by comparing the differential equations in theorem 1.5.1 and theorem 1.5.4. □

Corollary 1.5.10. *The following equations hold:*

$$\begin{aligned} 0 &= e_1 + e_2 + e_3. && (1.41)\\ g_2 &= -4(e_1e_2 + e_2e_3 + e_3e_1). && (1.42)\\ g_3 &= 4e_1e_2e_3. && (1.43)\end{aligned}$$

Proof. We get this by comparison of coefficients in theorem 1.5.9. □

1.6 Conjugation-invariant lattices

In this short section, we want to give some simple properties about the special class of conjugation-invariant lattices. The following results will not be needed for the rest of this chapter, but are undoubtly interesting and have consequences in chapter 2, when we deal with elliptic curves over $\mathbb{R}$.

Definition 1.6.1. We call a lattice Ω *conjugation-invariant*, if for $\omega \in \Omega$ its complex conjugate $\overline{\omega}$ is also in Ω, i.e. $\Omega = \overline{\Omega}$. The most important examples for conjugation-invariant lattices are

- the *rectangular lattice*: $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ with $\frac{1}{i}\omega_1, \omega_2 \in \mathbb{R}^+$,
- the *hexagonal lattice*: $\Omega = \mathbb{Z}\rho + \mathbb{Z}$ with $\rho := \frac{1}{2}(1 + i\sqrt{3})$.

Proposition 1.6.2. *Let Ω be a conjugation-invariant lattice, then*

$$\overline{\wp_\Omega(z)} = \wp_\Omega(\overline{z}) \quad \text{and} \quad \overline{\wp'_\Omega(z)} = \wp'_\Omega(\overline{z}).$$

Specially for $z \in \mathbb{C}\backslash\Omega$, it holds that

- *$\wp_\Omega(z)$ is real for $z \in \mathbb{R}$ and $z \in i\mathbb{R}$,*
- *$\wp'_\Omega(z)$ is real for $z \in \mathbb{R}$ and purely imaginary for $z \in i\mathbb{R}$.*

Proof. We get this directly from the definition and the fact, that $\wp$ is en even function, whereas $\wp'$ is an odd function. □

Now we can give the following characterization:

Theorem 1.6.3. *For a lattice $\Omega = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, the following statements are equivalent:*

1. *$g_2(\Omega)$ and $g_3(\Omega)$ are both real values.*
2. *All $G_k(\Omega)$, for $k \geq 4$ even, are real.*

3. *Either all of the three values e_1, e_2, e_3 are real or one is real and the other two are complex conjugates of each other.*

4. *Ω is conjugation-invariant.*

Proof. (1) $\Leftrightarrow$ (2): Use definition 1.5.3 and proposition 1.5.6.

(1) $\Rightarrow$ (3): By theorem 1.5.9, we see, that e_1, e_2, e_3 are exactly the roots of the real polynomial $4x^3 - g_2x - g_3$. So one is real and the others are either complex conjugate or real too.

(1) $\Leftarrow$ (3): Use 1.42 and (1.43)

(1) $\Leftrightarrow$ (4): This equivalence follows from $\overline{g_2(\Omega)} = g_2(\overline{\Omega}), \overline{g_3(\Omega)} = g_3(\overline{\Omega})$ and the fact, that Ω is uniquely defined by g_2 and g_3 due to theorem 1.5.8. □

1.7 Discriminant and j-invariant of a given lattice

Definition 1.7.1. To a given lattice Ω, we define the *discriminant* Δ by

$$\Delta := \Delta(\Omega) := g_2^3 - 27g_3^2 \tag{1.44}$$

Proposition 1.7.2. *It holds, that*

$$\Delta = 16(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2 \neq 0.$$

Proof. From (1.41) and (1.42), we get

$$\begin{aligned} g_2 &= 2(e_1^2 + e_2^2 + e_3^2) & (1.45)\\ g_2^2 &= 16(e_1^2e_2^2 + e_2^2e_3^2 + e_3^2e_1^2). & (1.46)\end{aligned}$$

Using (1.42), (1.45) and (1.46), we further obtain

$$2(e_1 - e_2)^2 = 2(e_1^2 + e_2^2) - 4e_1e_2 = 2g_2 - 2e_3^2 + 4e_3(e_1 + e_2) = 2g_2 - 6e_3^2$$

and so

$$(e_1 - e_2)^2 = g_2 - 3e_3^2.$$

We get similar equalities by interchanging e_1, e_2 and e_3. Now calculate

$$\begin{aligned} &16(e_1 - e_2)^2(e_2 - e_3)^2(e_3 - e_1)^2\\ &= 16(g_2 - 3e_1^2)(g_2 - 3e_2^2)(g_2 - 3e_3^2)\\ &= 16g_2^3 - 3 \cdot 16g_2^2(e_1^2 + e_2^2 + e_3^2)\\ &+ 9 \cdot 16g_2(e_1^2e_2^2 + e_2^2e_3^2 + e_3^2e_1^2) - 27 \cdot 16e_1^2e_2^2e_3^2.\end{aligned}$$

Using (1.45), (1.46) and (1.43), we see, that this expression equals $g_2^3 - 27g_3^2$, i.e. Δ.

Since e_1,e_2 and e_3 are pairwise disjoint due to (1.28), $\Delta \neq 0$. □

We will see, that every nonzero value appears as a determinant to a suitable lattice.

To prove this, we will first need to collect some more information about discriminants using the notion of the *absolute invariant*:

Definition 1.7.3. The value

$$j := j(\Omega) := (12g_2)^3/\Delta \tag{1.47}$$

is called the *absolute invariant* of the lattice Ω.

One important property of the absolute invariant j is given by the following

Theorem 1.7.4. *For two lattices Ω and Ω' in $\mathbb{C}$, the following statements are equivalent:*

1. *There exists a nonzero $\lambda \in \mathbb{C}$, such that $\Omega' = \lambda\Omega$.*
2. *$j(\Omega) = j(\Omega')$*

Proof. (1) ⇒ (2): From our definition of the Eisenstein series in (1.18), we obtain $G_k(\Omega') = G_k(\lambda\Omega) = \lambda^{-k}G_k(\Omega)$ for $k \geq 3$. This implies, using the respective definition, that

$$\begin{aligned} g_2(\Omega') = g_2(\lambda\Omega) &= \lambda^{-4}g_2(\Omega), && (1.48)\\ g_3(\Omega') = g_3(\lambda\Omega) &= \lambda^{-6}g_3(\Omega), && (1.49)\\ \Delta(\Omega') = \Delta(\lambda\Omega) &= \lambda^{-12}\Delta(\Omega), && (1.50)\\ j(\Omega') = j(\lambda\Omega) &= j(\Omega), && (1.51) \end{aligned}$$

hence (2).

(2) ⇒ (1): Consider the case $j(\Omega') = j(\Omega) \neq 0$. Then, there exists a $0 \neq \lambda \in \mathbb{C}$, such that

$$g_2(\Omega') = \lambda^{-4}g_2(\Omega) = g_2(\lambda\Omega).$$

By replacing λ by $i\lambda$ if necessary, we can assume, that $g_2(\Omega') = g_2(\lambda\Omega)$ and also $g_3(\Omega') = g_3(\lambda\Omega)$. We then get $\Omega' = \lambda\Omega$ by theorem 1.5.8.

Otherwise, if $j(\Omega') = j(\Omega) = 0$, we have $g_2(\Omega) = g_2(\Omega') = 0$ as well as $g_3(\Omega) \neq 0$ and $g_3(\Omega') \neq 0$ due to 1.7.2. We then get (1) in an analogous way. □

We now want to introduce a new kind of notation, which will be useful in order to show the inversion theorem:

If (ω_1, ω_2) is a basis of Ω, we can write

$$\wp(z; \omega_1, \omega_2) := \wp_\Omega \quad \text{and} \quad G_k := G_k(\Omega) \quad \text{for } k \geq 3.$$

Since neither $\wp$ nor G_k are dependent of the choice of our basis, corollary 1.1.6 yields

$$\wp(z;\omega_1',\omega_2') = \wp(z;\omega_1',\omega_2') \text{ and } G_k(\omega_1',\omega_2') = G_k(\omega_1,\omega_2) \text{ for } k \geq 3. \quad (1.52)$$

if

$$\begin{aligned}\omega_1' &= a\omega_1 + b\omega_2 \\ \omega_2' &= c\omega_1 + d\omega_2\end{aligned}$$

with $a, b, c, d \in \mathbb{Z}$, $ad - bc = \pm 1$.

As a basis of Ω, ω_1, ω_2 are linearly independent over $\mathbb{R}$, so $\tau := \omega_1/\omega_2 \notin \mathbb{R}$. Since for every basis (ω_1, ω_2) of Ω, (ω_1', ω_2') is also a basis of Ω, we may assume without loss of generality, that $\Im(\tau) > 0$. This is the case, if and only if the triagle $(0, \omega_2, \omega_1)$ is positively oriented.

From the definitions, we see that if $0 \neq \lambda \in \mathbb{C}$, it holds that

$$\begin{aligned}\wp(\lambda z; \lambda\omega_1, \lambda\omega_2) &= \lambda^{-2}\wp(z;\omega_1,\omega_2), \\ G_k(\lambda\omega_1, \lambda\omega_2) &= \lambda^{-k} G_k(\omega_1,\omega_2) \quad \text{for } k \geq 3.\end{aligned}$$

It then follows by (1.52), that

$$\wp(z;\omega_1,\omega_2) = \omega_2^{-2}\wp(z/\omega_2;\tau,1) \text{ and } G_k(\omega_1,\omega_2) = \omega_2^{-k} G_k(\tau,1) \text{ for } k \geq 3.$$

So assuming $\omega_2 = 1$ is no major restriction, if we study elliptic functions over Ω and we can work with lattices of the form

$$\Omega = \mathbb{Z}\tau + \mathbb{Z} \text{ with } \tau \in \mathcal{H},$$

where $\mathcal{H}$ discribes the *upper half-plane*:

$$\mathcal{H} := \{\tau \in \mathbb{C} : \Im\tau > 0\}$$

Due to

$$\tau' := \frac{\omega_1'}{\omega_2'} = \frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2} = \frac{a\tau + b}{c\tau + d} \quad \text{and} \quad \Im\tau' = \frac{ad - bc}{|c\tau + d|^2} \cdot \Im\tau \qquad (1.53)$$

we may only allow integer values a, b, c, d with $ad - bd = 1$, if we change over from a basis $(\tau, 1)$ of Ω to a basis $(\tau', 1)$ of $\frac{1}{c\tau+d}$ with $\tau' \in \mathcal{H}$.

So, (1.52) can be written as

$$\begin{aligned}\wp\left(\frac{z}{c\tau+d}; \frac{a\tau+b}{c\tau+d}, 1\right) &= (c\tau+d)^2 \cdot \wp(z;\tau,1) \qquad (1.54) \\ G_k\left(\frac{a\tau+b}{c\tau+d}, 1\right) &= (c\tau+d)^k \cdot G_k(\tau,1) \quad \text{for } k \geq 4, \qquad (1.55)\end{aligned}$$

with integers a, b, c, d such that $ad - bc = 1$.

We will shortly write $j(\tau)$ for the absolute invariant j of the lattice $\mathbb{Z}\tau + \mathbb{Z}$.

Theorem 1.7.5. *For $\tau, \tau' \in \mathcal{H}$ with $j(\tau') = j(\tau)$ there exist integers a, b, c, d with $ad - bc = 1$, such that*

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

Proof. According to our premises, $j(\mathbb{Z}\tau' + \mathbb{Z}) = j(\mathbb{Z}\tau + \mathbb{Z})$. From theorem 1.7.4, it follows, that $\mathbb{Z}\tau' + \mathbb{Z} = \mathbb{Z}\lambda\tau + \mathbb{Z}\lambda$ for a $0 \neq \lambda \in \mathbb{C}$. So $(\tau', 1)$ and $(\lambda\tau, \lambda)$ are two bases of a lattice. Due to corollary 1.1.6, there exist integers a, b, c, d with $\tau' = a\lambda\tau + b\lambda, 1 = c\lambda\tau + d\lambda$ and $ad - cb = \pm 1$, so $\tau' = \frac{a\tau+b}{c\tau+d}$. Since τ and τ' both lie in $\mathcal{H}$, equation (1.53) yields $ad - bc = 1$. □

We will need the use of these approaches and results in order to prove the inversion theorem for elliptic functions. First though, we need to calculate the power series expansions of $j(\tau)$.

1.8 Fourier series expansions of important parameters

Our next aim will be to prove the inversion theorem for elliptic functions. For this, we will need the Fourier series expansions of the discriminant $\Delta(\tau)$ and the j-invariant $j(\tau)$ of a lattice $\mathbb{Z}\tau + \mathbb{Z}$.

Like in the definitions 1.5.3, 1.7.1 and 1.7.3, we introduce

$$\begin{aligned} g_2(\tau) &:= 60G_4(\tau) \\ g_3(\tau) &:= 140G_6(\tau) \\ \Delta(\tau) &:= g_2^3(\tau) - 27g_3^2(\tau). \end{aligned}$$

It can be shown (compare [KK] for a detailed proof), that the Fourier expansions of $g_2(\tau)$ and $g_3(\tau)$ are as follows:

$$g_2(\tau) = \frac{(2\pi)^4}{12}\left(1 + 240 \cdot \sum_{m=1}^{\infty} \sigma_3(m) \cdot e^{2\pi i m\tau}\right), \tag{1.56}$$

$$g_3(\tau) = \frac{(2\pi)^6}{216}\left(1 - 540 \cdot \sum_{m=1}^{\infty} \sigma_5(m) \cdot e^{2\pi i m\tau}\right), \tag{1.57}$$

where $\sigma_k(m) := \sum_{d \in \mathbb{N}, d|m} d^k$. Both are holomorphic in $\mathcal{H}$.

Theorem 1.8.1. *The discriminant $\Delta(\tau)$ has a Fourier series expansion of the form*

$$\Delta(\tau) = (2\pi)^{12} \cdot \sum_{m=1}^{\infty} \tau(m) \cdot e^{2\pi i m\tau}, \ \tau \in \mathcal{H}, \tag{1.58}$$

with integer coefficients $\tau(m)$ and $\tau(1) = 1$. The discriminant $\Delta : \mathcal{H} \to \mathbb{C}$ is a holomorphic function with $\Delta(\tau) \neq 0$ for all $\tau \in \mathcal{H}$ and

$$\Delta\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{12}\Delta(\tau) \tag{1.59}$$

for all integers a, b, c, d with $ad - bc = 1$.

The denotation of the coefficients in (1.58) with $\tau(m)$ is a tradition. The two different meanings of τ should not cause any confusion here.

Proof. We abbreviate

$$\begin{aligned} A &:= \sum_{m=1}^{\infty} \sigma_3(m) \cdot e^{2\pi i m\tau}, \\ B &:= \sum_{m=1}^{\infty} \sigma_5(m) \cdot e^{2\pi i m\tau}. \end{aligned}$$

Then, (1.56) and (1.57) imply

$$\Delta(\tau) = \frac{(2\pi)^{12}}{1728}((1+240A)^3 - (1-504B)^2) = (2\pi)^{12}(e^{2\pi i\tau} + \dots), \tag{1.60}$$

with a power series in $e^{2\pi i\tau}$ on the right-hand side.

To see, that the coefficients are in $\mathbb{Z}$, note, that $d^3 \equiv d^5 \pmod{12}$ for $d \in \mathbb{Z}$ and so $\sigma(m) \equiv \sigma_5(m) \pmod{12}$ for $m \in \mathbb{N}$. Refering to the coefficients, we have $A \equiv B \pmod{12}$. Now we calculate modulo $1728 = 12^3$ and obtain

$$(1 + 240A)^3 - (1 - 504B)^2 \equiv 12^2(5A + 7B) \equiv 0 \pmod{12^3}.$$

Hence the denominator in (1.60) cancels in all coefficients.

Since g_2 and g_3 are holomorphic, Δ is it too. We obtain $\Delta(\tau) \neq 0$ by corollary 1.7.2. The relation (1.59) follows quite directly from (1.55). □

In the next step, we want to calculate a power series expansion of the absolute invariant j, which was defined (see definition 1.7.3) as

$$j(\tau) = (12g_2(\tau))^3/\Delta(\tau), \ \tau \in \mathcal{H}.$$

Because of theorem 1.8.1, $j(\tau)$ is defined for all values $\tau \in \mathcal{H}$.

Before we can get a similar series for j, we need the following proposition:

Proposition 1.8.2. *Let f and g be power series*

$$f(q) = \sum_{n\geq 0} a_n q^n, \quad g(q) = \sum_{n\geq 0} b_n q^n, \quad a_n, b_n \in \mathbb{Z},$$

which are convergent for $|q| < 1$ with $g(q) \neq 0$ for $|q| < 1$. Then f/g is also a power series with integer coefficients, convergent for $|q| < 1$.

Proof. With f and g is also f/g holomorphic for $|q| < 1$ and so there exists a power series expansion, whose coefficients we denote with c_n. From

$$\left(\sum_{n\geq 0} c_n q^n\right) \cdot \left(\sum_{n\geq 0} b_n q^n\right) = \sum_{n\geq 0} a_n q^n$$

and $b_0 = 1$, we get the recursion formula

$$c_0 = a_0, \quad c_m = a_m - \sum_{n=0}^{m-1} c_n b_{m-n},\ m \geq 1.$$

So, the c_n are all integers. □

Theorem 1.8.3. *The absolute invariant $j : \mathcal{H} \to \mathbb{C}$ is holomorphic and has a Fourier expansion of the form*

$$j(\tau) = e^{-2\pi i\tau} + \sum_{m\geq 0} j_m \cdot e^{2\pi i m\tau} = e^{-2\pi i\tau} + 744 + 196884 \cdot e^{2\pi i\tau} + \ldots$$

and $j_m \in \mathbb{Z}$. It holds, that

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau) \quad \text{for all integers } a, b, c, d \text{ with } ad - bc = 1. \tag{1.61}$$

Proof. Since g_2 and Δ are holomorphic, j is it too. After separating a factor $e^{2\pi i\tau}$ from Δ, we can use proposition 1.8.2 and obtain the Fourier expansion of j by (1.56) and (1.58). The equation (1.61) is a consequence of (1.59) and (1.55). □

1.9 The inversion theorem

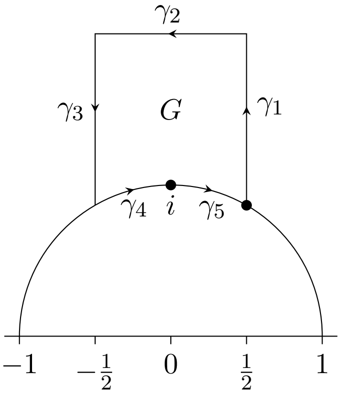
In this section, we will prove the very important inversion theorem, based on the results, that we obtained about the j-invariant. This theorem will be the key to the connection between the theory of elliptic functions and the theory of elliptic curves, that we will treat in chapter 2.

Theorem 1.9.1. *For each $c \in \mathbb{C}$, there exists a value $\tau \in \mathcal{H}$ with $j(\tau) = c$.*

Proof. Suppose, $j(\tau) \neq c$ for all $\tau \in \mathcal{H}$. Then $F(\tau) := \frac{j'(\tau)}{j(\tau)-c}$ is holomorphic in $\mathcal{H}$. Now consider the integral

$$\int_\gamma F(\tau)\, d\tau,\ \gamma = \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4 + \gamma_5$$

along the path $\gamma = \partial G$ from the figure:



From (1.61), it follows, that

$$F(\tau+1) = F(\tau), \quad F(-1/\tau) = \tau^2 F(\tau).$$

So, we have $\int_{\gamma_1} F(\tau)\,d\tau + \int_{\gamma_3} F(\tau)\,d\tau = \int_{\gamma_4} F(\tau)\,d\tau + \int_{\gamma_5} F(\tau)\,d\tau = 0$.

Due to proposition 1.8.2 and theorem 1.8.3, $F(\tau)$ has a Fourier expansion of the form

$$F(\tau) = \sum_{m\geq 0} a_m e^{2\pi i m\tau}, \quad a_0 = -2\pi i.$$

So we have $\int_{\gamma_2} F(\tau)\,d\tau = 2\pi i$. By the residue theorem, we get

$$2\pi i \cdot \sum_{\tau\in G} \mathrm{Ord}_\tau(j-c) = \int_\gamma F(\tau)\,d\tau = 2\pi i.$$

This is a contradiction. So there exists a $\tau \in \mathcal{H}$ with $j(\tau) = c$. □

Corollary 1.9.2 (Inversion theorem)**.** *For $c_2, c_3 \in \mathbb{C}$ with $c_2^3 - 27c_3^2 \neq 0$, then there exists a unique lattice Ω with $c_2 = g_2(\Omega)$ and $c_3 = g_3(\Omega)$.*

Proof. According to theorem 1.9.1, there exists a lattice Ω such that $j(\Omega) = \frac{(12c_2)^3}{c_2^3-27c_3^2}$.

Consider the case $c_2 = 0$. Then, $j(\Omega) = 0$, i.e. $g_2(\Omega) = 0$ and $g_3(\Omega) \neq 0$. Now choose a $0 \neq \lambda \in \mathbb{C}$ such that $g_3(\Omega) = \lambda^6 c_3$. By (1.49), it follows, that $g_3(\lambda\Omega) = \lambda^{-6} g_3(\Omega) = c_3$ and $g_2(\lambda\Omega) = \lambda^{-4} g_2(\Omega) = 0 = c_2$.

If $c_2 \neq 0$, we have $j(\Omega) \neq 0$ and $g_2(\Omega) \neq 0$. Now choose a $0 \neq \lambda \in \mathbb{C}$ with $g_2(\Omega) = \lambda^4 c_2$. It follows $g_2(\lambda\Omega) = c_2$ and due to $j(\lambda\Omega) = j(\Omega)$ we obtain $c_3^2 = g_3^2(\lambda\Omega)$. If necessary, we substitute λ by $i\lambda$ and so get the existence of the wanted lattice.

The uniqueness follows (in both cases) directly from theorem 1.5.8. □

1.10 The field of elliptic functions

We want to end this chapter with a quite important algebraic theorem, that gives us an idea, why the Weierstrass $\wp$-function is so important to understand the theory of all elliptic functions.

To start with, we see from the definition of $\wp$, that in a polynomial in $\wp$, poles can not be eliminated. Therefore, $\wp$ is not algebraic, but transcendent over the field $\mathbb{C}$ and the field $\mathbb{C}(\wp)$ is isomorphic to the field of all rational functions over $\mathbb{C}$.

Theorem 1.10.1. *The following statements hold:*

1. *The even elliptic functions relating to Ω are just the rational functions in $\wp$.*
2. $\mathcal{K}(\Omega) = \mathbb{C}(\wp)[\wp']$.
3. *The degree of the field expansion of $\mathcal{K}(\Omega)$ over $\mathbb{C}(\wp)$ is exactly* 2.

Proof. 1.: Let $f \in \mathcal{K}(\Omega)$ be an elliptic function, that is even and not constant. Furthermore, let m be the number of poles of f in a period parallelogram (counting multiplicities), P a fundamental parallelogram of Ω and $N := \{c \in P : f'(c) = 0\}$. We see, that N is finite.

We now prove the following statement:

The number m is even, $m = 2k$. For each complex number $u \notin f(N)$, there exist pairwise disjoint points

$$c_1, \dots, c_k,\, c'_1, \dots c'_k \in P,\ c_j + c'_j \in \Omega \quad \textit{for } j = 1, \dots, k, \tag{1.62}$$

such that f takes on the value u exactly at the points (1.62) in P, each with multiplicity 1.

By theorem 1.3.7, we see, that the number of u-points of f is also m. Let $c \in P$ be given with $f(c) = u$. Since f is even, we also have $f(-c) = u$ and so there exists a $\omega \in \Omega$ such that $c' := \omega - c \in P$ and $f(c') = u$. If $c' = c$, then for arbitrary z, we have $f(c+z) = f(\omega-c+z) = f(-c+z) = f(c-z)$, hence $f'(c+z) = -f'(c-z)$ and so it would follow $f'(c) = 0$, i.e. $u \in f(N)$, which contradicts our presumption. So c and c' are disjoint. From this, we see, that all u-points appear pairwise and since $u \notin f(N)$, every u-point has multiplicity 1. So, the statement above is proven.

Now, we want to show, that f is a rational function in $\wp$. Choose $v \neq u$ with $v \notin f(N)$. From the statement above, we see, that there exist points

$$d_1, \dots, d_k,\, d'_1, \dots, c'_k,\, d_j + d'_j \in \Omega \quad \text{for } j = 1, \dots, k,$$

such that f takes on the value v in P exactly at these points, each with multiplicity 1. Then, the elliptic function

$$g(z) := \frac{f(z) - u}{f(z) - v}$$

has zeros in P exactly at $c_1, \dots, c_k, c'_1, \dots, c'_k$, (each of order 1) and poles in P exactly at $d_1, \dots, d_k, d'_1, \dots, d'_k$, (each of order 1), because all poles of f vanish.

If we now choose e_1, e_2, e_3 like in (1.25) and u, v different from those three points, then the function

$$h(z) := \frac{(\wp(z) - \wp(c_1)) \dots (\wp(z) - \wp(c_k))}{(\wp(z) - \wp(d_1)) \dots (\wp(z) - \wp(c_d))}$$

has the same poles and zeros as g.

So the quotient g/h is holomorphic and therefore constant due to theorem 1.3.4. Hence $g \in \mathbb{C}(\wp)$, and since $f = \frac{vg-u}{g-1}$, f is a rational function in $\wp$.

2.: If $f \in \mathcal{K}(\Omega)$ is not constant, we can write $f = g + h\wp'$ with $g(z) := \frac{1}{2}(f(z) + f(-z))$ and $h(z) := \frac{1}{2\wp'(z)}((f(z) - f(-z))$. Obviously g and h both belong to $\mathcal{K}(\Omega)$ and are even. So statement 1 yields, that g and h are rational functions of $\wp$.

3.: On the one hand side, $\wp' \notin \mathbb{C}(\wp)$, since $\wp'$ is an odd function, on the other hand side, theorem 1.5.4 implies that the degree is not higher than 2. □

Hence we see, that each $f \in \mathcal{K}(\Omega)$ can be written in the form

$$f = R(\wp) + Q(\wp) \cdot \wp', \tag{1.63}$$

where R, Q are rational functions over $\mathbb{C}$. So we can discribe elliptic functions in a very easy way using the $\wp$-function.

We now can give the following

Corollary 1.10.2. *Let x, y be independent indeteminants over $\mathbb{C}$. Then*

$$\mathcal{K}(\Omega) \cong \mathbb{C}(x)[y]/I(x,y),$$

where $I(x,y)$ is the principal ideal generated by $y^2 - 4(x-e_1)(x-e_2)(x-e_3)$ in $\mathbb{C}(x)[y]$.

Proof. We define a ring-homomorphism $\Phi : \mathbb{C}(x)[y] \to \mathcal{K}(\Omega)$ by $x \to \wp, y \to \wp'$. By theorem 1.10.1, Φ is surjective. Now we write a $\phi \in \mathbb{C}(x)[y]$ after division with remainder over the field $\mathbb{C}(x)$ in the form

$$\phi(x,y) = (y^2 - 4(x-e_1)(x-e_2)(x-e_3)) \cdot q(x,y) + r(x,y)$$

where $q, r \in \mathbb{C}(x)[y]$ and the degree of r is lower than 2. Due to theorem 1.5.4, ϕ is in the kernel of Φ, if $r(\wp, \wp') = 0$. Because of (1.63), this means $r(x,y) = 0$. So the kernel of Φ is exactly $I(x,y)$ and the statement follows from the fundamental theorem on homomorphisms for rings. □

Since two elements of $\mathcal{K}(\Omega)$ are algebraically dependent, we also get the following

Corollary 1.10.3. *For $f, g \in \mathcal{K}(\Omega)$, it exists a non-trivial polynomial $P(x,y) \in \mathbb{C}[x,y]$, such that $P(f,g) = 0$.*

Chapter 2

Elliptic curves

An elliptic curve is, easily spoken, a smooth cubic in the projective plane over an arbitrary field K. Being smooth means, that it is free from cusps or self-intersections.

Using the theory of elliptic functions, it can be shown that elliptic curves defined over the complex numbers correspond to embeddings of the torus into the complex projective plane. The torus is also a commutative group, and in fact this correspondence is also a group isomorphism.

One can show, that such an elliptic curve can be regarded as a commutative group not only over $\mathbb{C}$, but over every field in a similar way. This is called the *group law* for elliptic curves. There is one infinite point on each elliptic curve, which plays a special role. It is the zero element of the group.

Elliptic curves are especially important in number theory, and constitute a major area of current research; for example, they were used in the proof, by Andrew Wiles, of Fermat's Last Theorem. More details can be found in [AW2] and [TW]. They also find applications in cryptography (see the article elliptic curve cryptography) and integer factorization.

2.1 The projective plane

For our further considerations, it is useful to introduce the concept of a projective plane. The main disadvantages of the affine plane $K \times K$, where K is a field, lies in the fact, that these set of points are not topologically compact, which make the affine plane somehow incomplete.

This leads to many distinctions of cases: For example, two different lines intersect in just one point, if they are not parallel. Therefore, we add one additional (infinite) point to each line, such that two lines have the same point at infinity, if and only if they are parallel in the affine plane. The set of all infinite points builds another line - the line at infinity.

This leads to the fact, that we do not have to differ between parallel and non-parallel lines. Also it is much easier to describe the characteristics of a curve in infinity. This also makes it is easy to see, that ellipses, hyperbolas and parabolas are, projectively seen, the same thing, if we regard the line at infinity like any other line.

Definition 2.1.1. Let K be a field. The *projective plane* $P_2(K)$ is defined as the quotient of $\{(x, y, z) \in K^3 \backslash \{(0, 0, 0)\}\}$ by an equivalence relation $\sim$, where $(x', y', z') \sim (x, y, z)$ if $(x', y', z') = \lambda(x, y, z)$ for some $\lambda \in K\backslash\{0\}$. Therefore, the coordinates of a point are only defined up to scaling. We will write $(x : y : z)$ for the point represented by these coordinates.

A line in $P_2(K)$ then is defined by a nonzero polynomial $L = ax + by + cz$ with fixed $a, b, c \in K$. We regard L and $L' = a'x + b'y + c'z$ to be the same line, if (a', b', c') is a multiple of (a, b, c). Therefore the locus

$$L(K) = \{(x, y, z)|ax + by + cz = 0\}$$

is well defined in $P_2(K)$ and we will speak of the line $L(K)$ in $P_2(K)$.

In this definition, we can also identify points in $P_2(K)$ as lines through the null point $(0, 0, 0)$ in the three-dimensional affine space K^3.

The affine plane K^2 has a standard one-one imbedding into $P_2(K)$: Namely we map a vector (x, y) into $(x : y : 1)$. The set, that is missed by the image is the set, where $z = 0$, which is called the *line at infinity.* Any point $(x : y : 0)$ in $P_2(K)$ is therefore aid to be a point at infinity.

For all other points, we can define the reverse map by mapping $(x : y : z) \in P_2(K)$ onto $(x/z, y/z)$, which then is in K^2.

Remark 2.1.2. In the same manner, we can define the projective space $P_n(K)$, which is connected with the affine space K^{n-1}. But as we are interested in planar curves, we will only work with $P_2(K)$.

Further informations and approaches to this can be found in many books about projective geometry.

2.2 Planar curves

Definition 2.2.1. Let $K[x, y, z]$ be the set of all polynomials with indeterminates x, y, z.

A polynomial $F \in K[x, y, z]$ is called *homogeneous* of degree d, if it has the form

$$F = \sum_{r+s+t=d} a_{rst} x^r y^s z^t.$$

A *projective planar curve of degree d* over a field K is given by a homogeneous polynomial $0 \neq F \in K[x, y, z]$ of degree d.

Again, two curves are regarded as the same curve, if they are multiples of each other. The locus

$$F(K) = \{(x : y : z)|F(x, y, z) = 0\}$$

is well defined in $P_2(K)$, since F is homogeneous. We speak of the curve $F(K)$ in $P_2(K)$.

In the special case that $d = 1, 2, 3$, the curve is called a *line*, *conic*, or *cubic*, respectively.

Definition 2.2.2. An *affine planar curve* C over a field K is given by a non-constant polynomial $f \in K[x, y]$.

We identify this polynomial with the set of all points $(x, y) \in K^2$ with $f(x, y) = 0$ and shortly write $f(K)$ for it.

Now we want to give a connection between affine and a projective planar curves:

Given an affine curve $f(K)$ by a polynomial $f(x, y)$ of highest degree d, we can define $F(x, y, z) := z^d f(x/z, y/z)$, which is a homogeneous polynomial of degree d. Therefore $F(K)$ is a projective planar curve. We call it *the projective closure* of $f(K)$. By identifying $P_2(K)$ with K^2 according to the standard imbedding, we can regard $F(K)$ as a continuation of the affine part $f(K)$. The new points $F(K)\backslash f(K)$, i.e. the points in $F(K)$ with $z = 0$ are exactly the infinite points of the curve.

Conversely, if $F(K)$ is a projective planar curve of degree d, then $f(x, y) := F(x, y, 1)$ is a polygone of maximal degree d. We call $f(K)$ the *affine part* of C. In the case that $F = az^d$, the affine part is empty, because $f = a$ does not define an affine curve. This means that all points of $F(K)$ are on the line at infinity. In all other cases $f(K)$ is an affine curve in K^2, not necessarily of degree d.

These operations are almost inverse: The affine part of a projective closure of an affince curve $f(K)$ is again $f(K)$. The projective closure of the affine part of a projective curve $F(K)$ is again $F(K)$, if F is not divisible by z.

We now want to study projective planar curves. It will turn out, that a projective planar curve of degree d and a line intersect in exactly d points, counting multiplicities. For this, we need to give a proper definition of this intersection multiplicity:

Definition 2.2.3. Let $P = (p_1 : p_2 : p_3) \in P_2(K)$ be a point, $L(K)$ a projective line over K (given by $L : ax + by + cz = 0$) and $F(K)$ a projective curve F (given by a polynomial $F : F(x, y, z) = 0$). We assume, that $ax + by + cz$ is not a divisor of F, else the line $L(K)$ would be contained in $F(K)$.

We now define the *intersection multiplicity* $i(L, F; P)$ of the point P with respect to L and F as follows:

For $P \notin L(K) \cap F(K)$, we set $i(L, F; P) := 0$. Else, we solve L for one variable (for example $z = -\frac{a}{c}x - \frac{b}{c}y$ if $c \neq 0$) and insert it into F. We get a homogeneous polynomial H in two variables, which is divisible by

$(p_1y - p_2x)$ (respective $(p_1z - p_3x)$ or $(p_2z - p_3y)$, if we eliminated another variable instead of z). The multiplicity of this factor then is $i(L, F; P)$.

It is easy to see, that this definition is independent of our choice, which variable we eliminate.

Example 2.2.4. Consider the curve $F(K)$ given by $F : y^2z - x^3 + xz^2$. For the line given by $y = 0$, we obtain $H : -x^3 + xz^2 = x(x + z)(-x + z)$, so we have intersection multiplicity 1 in each one of the points $(0 : 0 : 1)$, $(-1 : 0 : 1)$ and $(1 : 0 : 1)$.

Taking the line $x - z = 0$ instead, we get $H : xy^2$ by eliminating z, so the intersection point $(1 : 0 : 1)$ has multiplicity 2. (This line will turn out to be the *tangent* on F(K) at this point. The definition of a tangent will be given later.)

Finally, we look at the line $z = 0$. In this case, we have $H : -x^3$, so we even have an intersection point of multiplicity 3 at $(0 : 1 : 0)$. (This line will turn out to be an *inflexion tangent*)

Theorem 2.2.5. *Let $F(K)$ be a projective planar curve of degree d and $L(K)$ given by $L : ax + by + cz$ a projective line, which is not contained in $F(K)$. Then*

$$\sum_{P \in L(\overline{K}) \cap F(\overline{K})} i(L, F; P) = d,$$

where $\overline{K}$ denotes the algebraic closure of K.

Proof. Without loss of generality, we can assume, that $c \neq 0$. We set $a' := -a/c$, $b' := -b/c$, so the line equation of $L(K)$ is given by $z = a'x + b'y$. Inserting this into F, we get $H(x, y) = F(x, y, a'x + b'y)$. This is a homogeneous polynomial of degree d in $K[x, y]$.

Due to the fundamental theorem of algebra, this polynomial splits into linear factors in $\overline{K}[x, y]$:

$$H(x, y) = \alpha(\eta_1 x - \zeta_1 y)^{d_1}) \cdots (\eta_k x - \zeta_k y)^{d_k}).$$

For each intersection point $P = (p_1 : p_2 : p_3) \in L(\overline{K}) \cap F(\overline{K})$, we have $H(p_1, p_2) = 0$ as well as $p_3 = a'p_1 + b'p_2$ - and conversely such a point is an intersetion point.

So the intersection points are exactly $(\zeta_1 : \eta_1 : a'\zeta_1 + b'\eta_1)$, $\ldots$, $(\zeta_k : \eta_k, a'\zeta_k + b'\eta_k)$ and their multiplicities are per definition $d_1, \ldots, d_k$. But as $d_1 + \cdots + d_k = d$, this concludes the proof. □

Remark 2.2.6. This theorem is a special case of the *theorem of Bézout*, which states, that two projective curves of degree d_1 and d_2 intersect in exactly d_1d_2 points.

The proof of this theorem requires some deeper knowledge in algebraic geometry.

In analysis, we are mainly interested in somehow "smooth" objects, i.e. objects which are not only contineous, but also have some differentiability properties.

Since we do not have any topology, we need another suitable definition, because we can not derivate by using limits of differential quotients. However, we can use the following definition:

Definition 2.2.7. We call an affine planar curve given by $f(x, y) = 0$ *smooth* in a point $P = (p_1, p_2) \in F(\overline{K})$, if the partial derivation in P, $\frac{\partial f}{\partial x}(p_1, p_2)$ and $\frac{\partial f}{\partial y}(p_1, p_2)$ do not both equal 0.

Analogous, we call a projective planar curve given by $F(x, y, z) = 0$ *smooth* in a point $P = (p_1 : p_2 : p_3) \in F(\overline{K})$, if

$$\left(\frac{\partial F}{\partial x}(p_1, p_2, p_3), \frac{\partial F}{\partial y}(p_1, p_2, p_3), \frac{\partial F}{\partial z}(p_1, p_2, p_3)\right) \neq (0, 0, 0).$$

We call a curve (affine or projective) F *smooth*, if it is smooth in all points $P \in F(\overline{K})$. Otherwise, we say, F is *singular.*

Any point P, where the curve F is not smooth, is called a *singular point* of F.

Remark 2.2.8. A point on an affine curve $f(K)$ is a singular point, if and only if it is a singular point on the projective closure of $f(K)$. This follows quite obviously from the fact, that it doesn't matter, if we set $z = 1$ before or after derivating a curve in the projective closure of $f(K)$.

Example 2.2.9. We take the curve $F : y^2z - x^3 - z^3$ from example 2.2.4. Is it smooth? Each singularity point (p_1, p_2, p_3) has to satisfy

$$-3p_1^2 = 2p_2p_3 = p_2^2 - 3p_3^2 = 0.$$

If $\mathrm{char}(K) \neq 2, 3$, this implies $p_1 = p_2 = p_3 = 0$. But since $(0 : 0 : 0)$ is not a point in the projective plane, $F(K)$ is smooth.

The affine curve $y^2 = x^3 - x^2$ is not smooth in $P = (0, 0)$, since both derivatons $3x^2 - 2x$ and $2y$ equal 0 there.

The curve $F(x, y, z) = x^3 - 6xz^2 + 6yz^2 - y^3$ is well-defined over $K = \mathbb{Q}$, is smooth at every point of $F(\mathbb{Q})$ ans has a singular point ar $(\sqrt{2}, \sqrt{2}, 1)$. So the curve is singular.

Definition 2.2.10. If F is smooth in P, then there exists a unique line L through $P = (p_1 : p_2 : p_3)$, such that $i(L, F; P) \geq 2$. This line is called the *tangent line* on F in P and is given by the equation

$$\frac{\partial F}{\partial x}(p_1, p_2, p_3)\, x + \frac{\partial F}{\partial y}(p_1, p_2, p_3)\, y + \frac{\partial F}{\partial z}(p_1, p_2, p_3)\, z = 0.$$

If $i(L, F; P) \geq 3$, we say, that P is an *inflection point* of F.

2.3 Elliptic curves

In this section, we will introduce elliptic curves (over arbitrary fields):

Definition 2.3.1. An *elliptic curve* over a field K is a smooth projective cubic E over K, which is given by an equation of the form

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{2.1}$$

with coefficients $a_1, a_2, a_3, a_4, a_6 \in K$.

A cubic of the form (2.1) is said to be the *Weierstrass form.*

The corresponding *affine Weierstrass form* is given by the equation of the affine part:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2}$$

The notation is absolutely standard. The subscripts can be seen to indicate the degree of homogenity of the corresponding term under a certain change of variables.

We now state some very important properties about elliptic curves:

Proposition 2.3.2. *Let $E(K)$ be a curve in Weierstrass form (not necessarily smooth) over a field K like in definition 2.3.1. Then $E(K)$ has exactly one point at infinity, namely $(0 : 1 : 0)$. E is smooth in $(0 : 1 : 0)$ and the tangent at E in $(0 : 1 : 0)$ is the line at infinity $z = 0$. Moreover, $(0 : 1 : 0)$ is an inflection point of E.*

Proof. To find points at infinity, we have to set $z = 0$ in equation (2.1). It remains the term $x^3 = 0$, so $(0 : 1 : 0)$ is the only point at infinity (independent of our choice of the field K) and the intersection multiplicity of the line at infinity with E is 3, so $(0 : 1 : 0)$ is an inflection point of E.

To prove, that E is smooth in $(0 : 1 : 0)$, we regard the partial derivations of E evaluated at that point. Derivating (2.1) by z, we get a single term y^2 as well as several other terms, which include x or z, so $\frac{\partial E}{\partial z}(0 : 1 : 0) \neq 0$. Therefore $(0 : 1 : 0)$ is not a singular point.

Since E is smooth in $(0 : 1 : 0)$ and the intersection multiplicity is ≤ 2, we see, it follows, that the line at infinity $z = 0$ is the tangent at that point. □

Since the behaviour of an elliptic curve at its only infinite point is so well understood by proposition 2.3.2, we can study much of the behaviour of the curve by working with the affine form (2.2).

This form has the advantage, that the notation is simpler.

Definition 2.3.3. Let $E(K)$ be an elliptic curve. An *admissible change of variables* in a Weierstrass equation (2.2) is one of the form

$$x' = u^2x + r \quad \text{and} \quad y' = u^3y + su^2x + t \tag{2.3}$$

with $u, r, s, t \in K$ and $u \neq 0$. Projectively seen, this is a transformation

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = \Phi \begin{pmatrix} x \\ y \\ z \end{pmatrix} \quad \text{with} \quad \Phi := \begin{pmatrix} xu^2 & 0 & r \\ su^2 & u^3 & t \\ 0 & 0 & 1 \end{pmatrix}. \tag{2.4}$$

It fixes $(0 : 1 : 0)$ and carries the tangent $z = 0$ to the same line.

Two elliptic curves over the same field K, that are related by an admissible change of variable are said to be *isomorphic*.

Proposition 2.3.4. *Let $E(K)$ be an elliptic curve over K. For* $\text{char}(K) \neq 2$*, $E(K)$ is isomorphic to an elliptic curve $E'(K)$ of the form*

$$E' : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6. \tag{2.5}$$

If additionally $\text{char}(K) \neq 3$*, we can futher simplify (2.5) to a form*

$$y^2 = x^3 - 27c_4x - 54c_6. \tag{2.6}$$

Equation (2.6) is said to be the short Weierstrass form *and is the standard form for elliptic curves, if* $\text{char}(K) \neq 2, 3$.

Proof. Based on the affine form (2.2), we use the following notation:

$$\begin{aligned} b_2 &:= a_1^2 + 4a_2 \\ b_4 &:= 2a_4 + a_1a_3 \\ b_6 &:= a_3^2 + 4a_6 \\ b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned} \tag{2.7}$$

and

$$\begin{aligned} c_4 &:= b_2^2 - 24b_4 \\ c_6 &:= -2b_2^3 + 36b_2b_4 - 216b_6. \end{aligned} \tag{2.8}$$

In the first simplification of (2.2), we complete the square by replacing $y + \frac{1}{2}(a_1x + a_3)$ by $\frac{1}{2}y$. The result is equation is

$$E' : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6, \tag{2.9}$$

with b_2, b_4, b_6 as in (2.7). (The coefficient b_8 will play a role later in this section.) This yields the first result.

In the second simplification (assuming additionally, that $\text{char}(K) \neq 3$), we replace (x, y) in (2.5) by $\left(\frac{x-3b_2}{36}, \frac{y}{108}\right)$ and the result is (2.6). □

Remark 2.3.5. By substituting (x, y) by $(36x, 108y)$ in (2.6), we get the form

$$y^2 = 4x^3 - g_2x - g_3, \tag{2.10}$$

where

$$g_2 := c_4/12 \quad \text{and} \quad g_3 := c_6/216. \tag{2.11}$$

This form will be very useful later, when we consider the special case $K = \mathbb{C}$.

Definition 2.3.6. For any field K, we introduce the *discriminant* Δ of a cubic in Weierstrass form (2.2) by the formula

$$\Delta := -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \tag{2.12}$$

with b_2, b_4, b_6, b_8 as in (2.7). When $\mathrm{char}(K) \neq 2, 3$, we can solve for Δ by the formula

$$1728\Delta = c_4^3 - c_6^2. \tag{2.13}$$

If we substitute c_4 and c_6 by g_2 and g_3 like in (2.11), we get

$$\Delta = g_2^3 - 27g_3^2. \tag{2.14}$$

This strongly reminds us of definition 1.7.1 and we will see later, when we discuss the connection between elliptic curves and elliptic functions, that this is essentially the absolute same concept.

Our next aim will be to show, that a cubic in Weierstrass-form is smooth (and so an elliptic curve) if and only if $\Delta \neq 0$.

This is, what makes the concept of Δ so important for elliptic curves.

However, before we can proof this, we need to give more informations about discriminants of cubic polynomials:

Definition 2.3.7. Let

$$f(x) = x^3 - \alpha x^2 + \beta x - \gamma = (x - r_1)(x - r_2)(x - r_3) \tag{2.15}$$

be a monic cubic polynomial over K with roots in $\overline{K}$. Here α, β and γ are given by the elementary symmetric polynomials

$$\alpha = r_1 + r_2 + r_3, \quad \beta = r_1 r_2 + r_1 r_3 + r_2 r_3, \quad \gamma = r_1 r_2 r_3. \tag{2.16}$$

We can check, that

$$\det \begin{pmatrix} 1 & 1 & 1 \\ r_1 & r_2 & r_3 \\ r_1^2 & r_2^2 & r_3^2 \end{pmatrix} = (r_3 - r_2)(r_3 - r_1)(r_2 - r_1) \tag{2.17}$$

and that

$$\begin{pmatrix} 1 & 1 & 1 \\ r_1 & r_2 & r_3 \\ r_1^2 & r_2^2 & r_3^2 \end{pmatrix} \begin{pmatrix} 1 & r_1 & r_1^2 \\ 1 & r_2 & r_2^2 \\ 1 & r_3 & r_3^2 \end{pmatrix} = \begin{pmatrix} 3 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4, \end{pmatrix} \tag{2.18}$$

where $\sigma_i := r_1^i + r_2^i + r_3^i$ for $1 \leq i \leq 4$. The *discriminant* d of $f(x)$ is given by

$$d := (r_1 - r_2)^2 (r_1 - r_3)^2 (r_2 - r_3)^2. \tag{2.19}$$

For a cubic polynomial, that is not monic, we define d to be the same as for the multiple that is monic. If we then replace x by x/C in a cubic, the discriminant gets multiplied by C^6 (since each root gets multiplied by C).

Lemma 2.3.8. *The discriminant of the polynomial $f(x)$ in (2.15) is given by*

$$d = \det \begin{pmatrix} 3 & \sigma_1 & \sigma_2 \\ \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_2 & \sigma_3 & \sigma_4, \end{pmatrix} \tag{2.20}$$

where

$$\begin{aligned} \sigma_1 &= \alpha, \\ \sigma_2 &= \alpha^2 - 2\beta \\ \sigma_3 &= \alpha^3 - 3\alpha\beta + 3\gamma \\ \sigma_4 &= \alpha^4 - 4\alpha^2\beta + 2\beta^2 + 4\alpha\gamma. \end{aligned}$$

Proof. The determinant formula follows directly from (2.17), (2.18) and (2.19). Then, $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ are symmetric polynomials in r_1, r_2, r_3 and hence are polynomials in the elementary symmetric polynomials α, β, γ. There is an algorithms for finding the polynomials in α, β, γ and application of it yields the above expression for $\sigma_1, \sigma_2, \sigma_3, \sigma_4$. These expressions can be verified by direct computation. □

Corollary 2.3.9. *For the cubic polynomial $f(x) = x^3 + px + q$, the discriminant is $d = -4p^3 - 27q^2$.*

Proof. This is the special case of lemma 2.3.8 in which $\alpha = 0, \beta = p$ and $\gamma = -q$. □

Example 2.3.10. The easiest case is a cubic polynomial $f(x)$ defined over $\mathbb{R}$. The discriminant d is 0 if and only if f has a repeated root. If the three roots are real, then $d \geq 0$. If f has one real root r_1 and one pair of complex conjugate roots r_2 and $r_2 = \overline{r_2}$, then $(r_1 - r_2)(r_1 - \overline{r_2})$ is real and $(r_2 - \overline{r_2})$ is imaginary. Since d is the square of the product, d is ≤ 0.

In the general case, $d = 0$ for a cubic polynomial, if and only if at least two of the roots are equal.

The relevance of the discriminant d for detecting singularities of cubics in Weierstrass form is as follows:

Proposition 2.3.11. *If C is a nonzero element of K and if* $\mathrm{char}(K) \neq 2$, *then the planar curve*

$$y^2 = C(x^3 - \alpha x^2 + \beta x - \gamma) \tag{2.21}$$

is smooth, if and only if $f(x) = C(x^3 - \alpha x^2 + \beta x - \gamma)$ has distinct roots in $\overline{K}$.

Proof. Since proposition 2.3.2 showed, that there can be no singularity on the line at infinity, the curve is singular, if and only if there exists a $\overline{K}$-rational point $(x_0 : y_0 : 1)$ on the curve where the following three equations are all satisfied:

$$
\begin{aligned}
0 &= \frac{\partial}{\partial x} = 3x_0^2 - 2\alpha x_0 + \beta & (2.22)\\
0 &= \frac{\partial}{\partial y} = 2y_0 & (2.23)\\
0 &= \frac{\partial}{\partial z} = C(-\alpha x_0^2 + 2\beta x_0 - 3\gamma) - y_0^2. & (2.24)
\end{aligned}
$$

Equations (2.23), (2.21) and (2.22) are equivalent with

$$0 = y_0 = f(x_0) = f'(x_0),$$

and (2.24) is redundant, giving the extra condition $3f(x_0) - x_0 f'(x_0) = 0$. Thus the only candidates for singular points over $\overline{K}$ are $(x_0 : 0 : 1)$, where x_0 is a root of f and such a candidate $(x_0 : 0 : 1)$ is singular, if and only if x_0 is a multiple root of f. □

Proposition 2.3.12. *If* $\mathrm{char}(K) \neq 2$, *let* d_b *and* d_c *be the discriminants of the cubic polynomials on the right sides of (2.5) and (2.6), respectively.*

Then

$$d_c = 2^{12}3^{12}d_b \tag{2.25}$$

and

$$\Delta = 2^4 d_b. \tag{2.26}$$

Proof. Consider the case $\mathrm{char}(K) \neq 3$: Apart from translations, (2.6) is obtained from (2.5) by replacing x by x/C with $C = 6^2$ and we have seen that this effect on discriminants is to multiply them with C^6. Thus (2.25) follows. By corollary 2.3.9 and (2.13), we have

$$d_c = -4(-27c_4)^3 - 27(-54c_6)^2 = 2^2 \cdot 3^9 \cdot 12^3\Delta.$$

Then, (2.26) follows from (2.25)

If $\mathrm{char}(K) = 3$, it is immediate from corollary 2.3.9, that $d_c = 0$ and hence (2.25) is valid. The discriminant d_b of (2.5) is the same as that of (2.21) with

$$\alpha = -\frac{b_2}{4}, \quad \beta = \frac{b_4}{2}, \quad \gamma = -\frac{b_6}{4}, \quad C = 4.$$

Since $3 = 0$, lemma 2.3.8 says that

$$d_b = 2\sigma_1\sigma_2\sigma_3 - \sigma_2^3 - \sigma_1^2\sigma_4 = -\sigma_1\sigma_2\sigma_3 - \sigma_2^3 - \sigma_1^2\sigma_4$$

where

$$\begin{aligned}\sigma_1 &= \alpha\\ \sigma_2 &= \alpha^2+\beta\\ \sigma_3 &= \alpha^3\\ \sigma_4 &= \alpha^4-\alpha^4-\alpha^2\beta-\beta^2+\alpha\gamma\end{aligned}$$

with

$$\alpha=-b_2,\quad \beta=-b_4\quad \gamma=-b_6.$$

Substituting gives

$$d_b=-\beta^3+\alpha^2\beta^2-\alpha^3\gamma=b_4^3+b_2^2b_4^2-b_2^3b_6. \tag{2.27}$$

Meanwhile, in any characteristic, we can check that

$$4b_8=b_2b_6-b_4^2.$$

Therefore in characteristic 3,

$$\Delta=-b_2^2b_8+b_4^3=-b_2^3b_6+b_2^2b_4^2+b_4^3.$$

Comparing this equation with (2.27), we see, that $\Delta=d_b$ and so (2.26) follows. □

Now, we are ready to prove the following important theorem:

Theorem 2.3.13. *A cubic $E(K)$ in Weierstrass form like in (2.1) is singular, if and only if $\Delta=0$.*

Proof. Suppose $\mathrm{char}(K)\neq 2$. Then $E(K)$ is singular, if and only if (2.5) is singular, if and only if the right side of (2.5) has a repeated root (by proposition 2.3.11), if and only if $d_b=0$, if and only if $\Delta=0$.

Suppose, $\mathrm{char}(K)=2$. Then, Δ reduces to

$$\begin{aligned}\Delta &= b_2^2b_8+b_6^2+b_2b_4b_6\\ &= a_1^6a_6+a_1^5a_3a_4+a_1^4a_2a_3^2+a_1^4a_4^2+a_3^4+a_1^3a_3^3.\end{aligned}$$

Meanwhile, just as in the first paragraph of proposition 2.3.11, E can have singularities only at $\overline{K}$-rational points $(x_0:y_0:1)$ on the curve and it has a singularity at such a point, if and only if

$$0 = \frac{\partial}{\partial x}=a_1y_0+x_0^2+a_4 \tag{2.28}$$

$$0 = \frac{\partial}{\partial y}=a_1x_0+a_3 \tag{2.29}$$

$$0 = \frac{\partial}{\partial z}=y_0^2+a_1x_0y_0+a_2x_0^2+a_6. \tag{2.30}$$

Equation (2.30) is redundant, being the sum of the curve, x_0 times (2.28) and y_0 times (2.29).

Suppose, $a_1 = 0$. Then, $\Delta = 0$ if and only if $a_3 = 0$, if and only if (2.29) holds. To complete this case, it is enough to show, that the system

$$\begin{aligned} y_0^2 &= x_0^3 + a_2 x_0^2 + a_4 x_0 + a_6 \\ 0 &= x_0^2 + a_4 \end{aligned}$$

has a solution in $\overline{K}$. But we have only to choose $x_0 \in \overline{K}$ so, that the second equation holds, substitute it into the first equation and choose $y_0 \in \overline{K}$ so, that the first equation holds.

Now suppose, $a_1 \neq 0$. Then, (2.29) and (2.28) successively give

$$x_0 = a_1^{-1} a_3 \quad \text{and} \quad y_0 = a_1^{-3} a_3^2 + a_1^{-1} a_4.$$

Substitution of these values for x and y in the difference of the two sides of (2.2) gives

$$\begin{aligned} &(a_1^{-6} a_3^4 + a_1^{-2} a_4^2) + (a_1^{-3} a_3^3 + a_1^{-1} a_3 a_4) + (a_1^{-3} a_3^3 + a_1^{-1} a_3 a_4) + \\ &\qquad + a_1^{-3} a_3^3 + a_1^{-2} a_2 a_3^2 + a_1^{-1} a_3 a_4 + a_6, \end{aligned}$$

and the equation at the beginning of the proof says, that this is just $a_1^{-6}\Delta$. Thus (x_0, y_0) satisfies (2.2), yielding $(x_0 : y_0 : 1)$ as a singular point, if and only if $\Delta = 0$. This concludes the proof of the theorem. □

2.4 Elliptic curves over $\mathbb{C}$ and the inversion theorem

Now, we are ready to give the connection between elliptic curves and elliptic functions:

Theorem 2.4.1 (Fundamental inversion theorem)**.** *Consider a lattice Ω in $\mathbb{C}$. Then, the set*

$$E(\Omega) := \{(x, y) \in \mathbb{C}^2 : y^2 = 4x^3 - g_2 x - g_3\}$$

is an elliptic curve in $\mathbb{C}^2$ in affine Weierstrass-form. We call it the (affine) elliptic curve generated by Ω*.*

Conversely, for any elliptic curve in $\mathbb{C}^2$, there exists a unique lattice Ω, that generates E.

Proof. From the definition, it is clear, that $E(\Omega)$ is an affine cubic in $\mathbb{C}^2$. Proposition 1.7.2 shows, that $\Delta \neq 0$ and since the discriminant for elliptic curves was defined in an analogous way (see (2.10) and (2.14)), theorem 2.3.13 yields, that this affine cubic is smooth. So we have an elliptic curve.

Conversely, given an elliptic curve E, we can use the form (2.10), since $\operatorname{char}\mathbb{C} = 0$. Since $\Delta \neq 0$ due to theorem 2.3.13, we can use the inversion theorem 1.9.2 to find the corresponding lattice Ω, which generates E. □

Remark 2.4.2. In a similar way, we have the *projective elliptic curve generated by* Ω:

$$\overline{E}(\Omega) := \{(x:y:z) \in P_2(\mathbb{C}) : y^2z = 4x^3 - g_2xz^2 - g_3z^3\}.$$

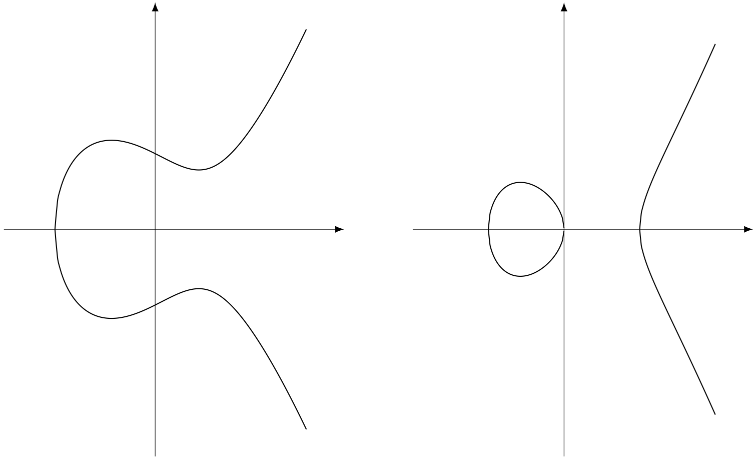
It is the projective closure of $E(\Omega)$.

Remark 2.4.3. In the same manner, we can use $\mathbb{R}$ or $\mathbb{Q}$ instead of $\mathbb{C}$ in the proof of theorem 2.4.1 to see, that the elliptic curves in $\mathbb{R}^2$ resp. $\mathbb{Q}^2$ are exactly

$$\begin{aligned} E_{\mathbb{R}}(\Omega) &:= \{(x,y) \in \mathbb{R}^2 : y^2 = 4x^3 - g_2x - g_3\} \quad \text{for } g_2, g_3 \in \mathbb{R}, \\ E_{\mathbb{Q}}(\Omega) &:= \{(x,y) \in \mathbb{Q}^2 : y^2 = 4x^3 - g_2x - g_3\} \quad \text{for } g_2, g_3 \in \mathbb{Q}. \end{aligned}$$

These sets are called the *real part* resp. the *rational part* of $E(\Omega)$, since they are clearly subsets of $E(\Omega)$.

Remark 2.4.4. The Weierstrass invariants g_2, g_3 are real if and only if Ω is a conjugation-invariant lattice due to theorem 1.6.3. Hence the elliptic curves over $\mathbb{R}^2$ correspond with conjugation-invariant lattices. Depending on whether $4x^3 - g_2x - g_3$ has one or three real roots, we then obtain the following graphs for the real part:



Since each lattice Ω is connected with its $\wp$-function, we even get a parametrisation of the elliptic curve $E(\Omega)$:

Theorem 2.4.5. *Let P be an arbitrary period parallologram of Ω. We can identify P with the set $\mathbb{C}/\Omega$ by reasons of periodicy.*

The mapping

$$\Phi : (\mathbb{C}/\Omega)\backslash\{\Omega\} \to E(\Omega), \quad \Phi(u + \Omega) := (\wp(u), \wp'(u)),$$

is a bijection.

Proof. The differential equation of theorem 1.5.4 shows, that the range of Φ is contained in $E(\Omega)$. For $(x, y) \in E$ choose u with $\wp(u) = x$ by lemma 1.4.12. Then it holds that $y^2 = 4x^3 - g_2x - g_3 = \wp'(u)^2$, again by theorem 1.5.4. If necessary, we may substitute u by $-u$ to get $\wp'(u) = y$. So (x, y) is in the range of Φ, hence Φ is surjective.

Let $u_1, u_2 \in \mathbb{C}$ be with $(\wp(u_1), \wp'(u_1)) = (\wp(u_2), \wp'(u_2))$. If $\wp'(u_1) \neq 0$, we see by lemma 1.4.11 and lemma 1.4.12, that $u_1 + u_2 \in \Omega/2$ and $u_1, u_2 \neq \{\omega/2 : \omega \in \Omega\}$. But since $\wp'$ is an odd function, it follows, that $u_1 \equiv u_2 \pmod{\Omega}$. If $\wp'(u_1) = 0$, it follows from lemma 1.4.11 and , that (1.26), that $u_1, u_2 \equiv \omega_1/2, \omega_2/2, \omega_3/2 \pmod{\Omega}$. But as the values $\wp(\omega_k/2) = e_k$, $k = 1, 2, 3$ are all disjoint due to (1.28), it is $u_1 \equiv u_2 \pmod{\Omega}$ also in this case. Thus, Φ is injective. □

We can also regard the projective closure $\overline{E}(\Omega)$ and define the following bijection:

$$\overline{\Phi} : \mathbb{C}/\Omega \to \overline{E}(\Omega), \quad \overline{\Phi}(u + \Omega) := \begin{cases} (\wp(u) : \wp'(u) : 1), & \text{for } z \notin \Omega \\ (0 : 1 : 0), & \text{for } z \in \Omega \end{cases}.$$

By using the standard imbedding from section 2.2, we can regard $\overline{\Phi}$ as a continuation of Φ. So we will also write Φ for it in future.

With the parametrisation Φ, we can convey the group structure of $\mathbb{C}/\Omega$ on the set $\overline{E}$: For $P, Q \in \overline{E}$, we define an addition by

$$P + Q := \Phi(\Phi^{-1}(P) + \Phi^{-1}(Q)), \tag{2.31}$$

at which the addition in $\mathbb{C}/\Omega$ is given by $(u + \Omega) + (v + \Omega) := (u + v) + \Omega$.

We then get this important theorem about elliptic curves (in $\mathbb{C}$):

Theorem 2.4.6. *With the composition defined in (2.31), $\overline{E}(\Omega)$ is a commutative group with identity element $(0 : 1 : 0)$. The mapping*

$$\Phi : \mathbb{C}/\Omega \to \overline{E}(\Omega)$$

then is a group isomorphism. So for $t \in \mathbb{C} \backslash \Omega$, we have

$$-(\wp(t), \wp'(t)) = (\wp(-t), \wp'(-t)) = (\wp(t), -\wp'(t)),$$

and for $u, v \in \mathbb{C}$ with $u, v, u + v \notin \Omega$, we have

$$(\wp(u), \wp'(u)) + (\wp(v), \wp'(v)) = (\wp(u + v), \wp'(u + v)). \tag{2.32}$$

Proof. This is just, how we defined it. □

Our next aim will be to find a way to calculate the sum of two points P, Q on an elliptic curve without knowing about the lattice Ω.

2.5 Intersection formulas

Let E be an elliptic curve. From theorem 2.2.5, we already know, that each line intersects in exactly three points. This will turn out to be the key to calculate our addition directly from the curve.

We will work here with the affine form of an elliptic curve. This has the advantage, that this is easier to work with, but the disadvantage, that we have to exclude the point $(0:1:0)$ for our next considerations. However, since $(0:1:0)$ is the identity element in our group, we know anyway, how addition works for it.

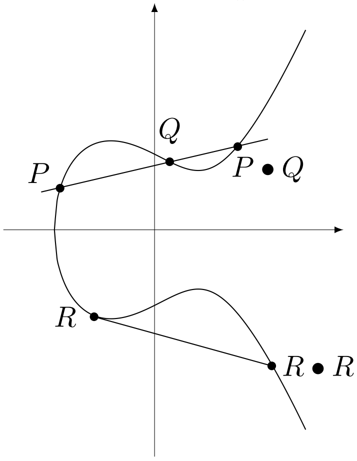
So let $P = (x_P, y_P), Q = (x_Q, y_Q)$ be two points on a curve. If $x_P \neq x_Q$, we may consider the complex line $L_{P,Q}$ through P and Q:

$$y = a_{P,Q}x + b_{P,Q},$$

where $a_{P,Q}$ and $b_{P,Q}$ are given by

$$\begin{aligned} a_{P,Q} &:= \frac{y_P - y_Q}{x_P - x_Q}, \\ b_{P,Q} &:= y_P - a_{P,Q}x_P = \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}. \end{aligned}$$

This line will intersect the curve in a third point. In case, that the curve has a nontrivial real part, we might have the following situation:



We define the point $P \bullet Q$ by

$$x_{P\bullet Q} := \frac{1}{4}a_{P,Q}^2 - x_P - x_Q \tag{2.33}$$

$$y_{P\bullet Q} := a_{P,Q}x_{P\bullet Q} + b_{P,Q} \tag{2.34}$$

Obviously, $P \bullet Q$ lies on the line L.

Lemma 2.5.1. *For all $x \in \mathbb{C}$, we have*

$$4x^3 - g_2x - g_3 = 4(x - x_P)(x - x_Q)(x - x_{P\bullet Q}) + (a_{P,Q}x + b_{P,Q})^2. \tag{2.35}$$

Proof. Obviously, the coefficients of x^3 are the same on both sides. Due to (2.33), this holds also for the coefficients of x^2. So, (2.35) reduces to an equation of the form $g_2x + g_3 = Ax + B$ with $A, B \in \mathbb{C}$. But since (2.35) is true for the two points $x = x_P$ and $x = x_Q$, that lie on E, it follows $A = g_2$ and $B = g_3$ for all $x \in \mathbb{C}$. □

So, we found the third intersection point of L with E:

Corollary 2.5.2. *For $P, Q \in E$ with $x_P \neq x_Q$, it holds that $P \bullet Q \in E$.*

Proof. This follows directly from lemma 2.5.1 by setting $x = x_{P\bullet Q}$. □

Therefore, we call the formulas (2.33) and (2.34) *intersection formulas.*

Next consider the case, that $P = Q$: Instead of taking the connecting line, we take the tangent line in $P \in E$. Again, we suppose, that $y_P \neq 0$.

We set

$$\begin{aligned} a_P &:= \frac{12x_P^2 - g_2}{2y_P}, \\ b_P &:= y_P - a_P x_p. \end{aligned}$$

, The line $y = a_P x + b_P$ then is the tangent in P at E. Now define

$$\begin{aligned} x_{P\bullet P} &:= \frac{1}{4}a_P^2 - 2x_P, &(2.36)\\ y_{P\bullet P} &:= a_P x_{P\bullet P} + b_P. &(2.37) \end{aligned}$$

Lemma 2.5.3. *For all $x \in \mathbb{C}$, the following equation holds:*

$$4x^3 - g_2x - g_3 = 4(x - x_P)^2(x - x_{P\bullet P}) + (a_{P,Q}x + b_{P,Q})^2. \qquad (2.38)$$

Again, the coefficients of x^3 concur and due to (2.36), this holds also for the coefficients of x^2. For $x = x_P$, the formula (2.38) holds and due to our choice of a_P and b_P, this is also true for the derivated equation of (2.38).

Corollary 2.5.4. *For $P \in E$ with $y_P \neq 0$, it holds, that $P \bullet P \in E$.*

Proof. This follows directly from lemma 2.5.3 by setting $x = x_{P\bullet P}$. □

So, counting intersection multiplicities, the third intersection point of the tangent in P on E is given by $P \bullet P$. Equation (2.36) and (2.37) are also called *intersection formulas.*

Last, we want to consider the case, where our line is parallel to the y-axis, i.e. $x_P = x_Q$ or $y_P = 0, P = Q$. In this case, there is no third intersection point in the affine form of E, but we may define $P \bullet P := (0 : 1 : 0)$ in the projective closure and so get the third intersection point in this case.

Our next aim will be to connect our new operator $\bullet$ with the addition, that we defined in (2.31). We will see, that this operator is almost, what we need - except for a kind of conjugation.

Let us regard the function Φ, that we defined as

$$\Phi : \mathbb{C}/\Omega \to \overline{E}(\Omega), \quad \Phi(u+\Omega) := \begin{cases} (\wp(u) : \wp'(u) : 1), & \text{for } z \notin \Omega \\ (0:1:0), & \text{for } z \in \Omega \end{cases}.$$

For $u, v \in \mathbb{C}$, we define the points $P, Q \in \overline{E}$ by $P := \Phi(u+\Omega)$ and $Q := \Phi(v+\Omega)$.

Lemma 2.5.5. *For $u, v, w \in \mathbb{C}\backslash\Omega$ with $u+v+w \in \Omega$, such that $u+\Omega$, $v+\Omega$ and $w+\Omega$ are pairwise disjoint, we have*

$$P \bullet Q = \Phi(w+\Omega).$$

Proof. The elliptic function $f(z) := \wp'(z) - (a_{P,Q}\wp(z) + b_{P,Q})$ has a pole of order 3 at 0 and so it has 3 zeros in $\mathbb{C}/\Omega$ by theorem 1.3.7. By construction, it is $f(u) = f(v) = 0$ and from theorem 1.3.9, we see, that $f(w) = 0$. So, P, Q and $\Phi(w+\Omega)$ are the three intersection points of the line between P and Q with E. This proves the lemma. □

Now, we define the operator $*$ as follows: For a point $P = (x_P, y_P) \in \mathbb{C}^2$, we set $P^* := (x_P, -y_P)$.

As a final result, we then get the following

Theorem 2.5.6. *The addition $(P,Q) \to P+Q$ on E is given by*

$$\begin{aligned} P+Q &= (P \bullet Q)^*, \quad \textit{for } x_P \neq x_Q, \\ 2P &= (P \bullet P)^*, \quad \textit{for } y_P \neq 0, \end{aligned}$$

so we can add as follows:

$$\begin{aligned} x_{P+Q} &:= \frac{1}{4}a_{P,Q}^2 - x_P - x_Q, \\ y_{P+Q} &:= -a_{P,Q}x_{P+Q} - b_{P,Q} \end{aligned}$$

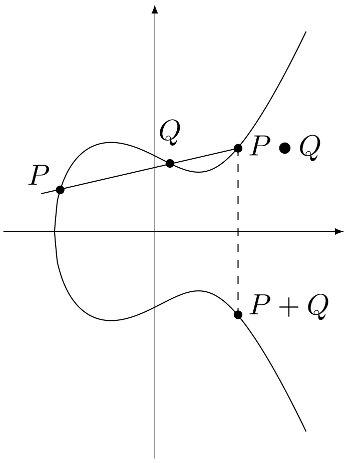
for $x_P \neq x_Q$ and

$$\begin{aligned} x_{2P} &:= \frac{1}{4}a_P^2 - 2x_P, \\ y_{2P} &:= -a_P x_{2P} - b_P. \end{aligned}$$

for $y_P \neq 0$.

Additionally, it holds, that

$$-P = P^* = (x_P, -y_P). \tag{2.39}$$



Proof. For $\wp(u) \neq \wp(v)$, (2.31) and lemma 2.5.5 yield

$$\begin{aligned} P+Q &= \Phi(\Phi^{-1}(P)+\Phi^{-1}(Q)) = \Phi(u+v+\Omega) = \Phi(-w+\Omega) \\ &= (\wp(w), -\wp'(w)) = (\Phi(w+\Omega))^* = (P \bullet Q)^*. \end{aligned}$$

The other statements follow from the respective definitions and from theorem 2.4.6. □

So we have seen, that it is possible to introduce a group operation, +, on the elliptic curve over $\mathbb{C}$ with the following property: Considering the point at infinity to be the identity 0 of the group, a straight line intersects the curve at the points P, Q and R if and only if $P+Q+R=0$ in the group.

We might also take this as a definition for our addition and the question arises, if we always get such a commutative group, independent on the choice of our field K. The answer is yes. It can even be shown that the set of K-rational points $E(K)$ on the curve (including the point at infinity) forms a subgroup of our group. This is, what is said to be the *group law of elliptic curves.* A detailed proof for this more universal theorem can be found in [AK]. The main idea however is the following: Let P, Q are two K-rational points on the curve. Applying Bézout's theorem yields that $P+Q \in E(\overline{K})$. Now one uses the fact that if a cubic polynomial defined over K has two roots in K, the third one is also in K.

2.6 The Mordell-Weil Theorem

We have seen some of the structure and properties of elliptic curves over $\mathbb{C}$ (parametrized by the $\wp$-function) and $\mathbb{R}$ (its real part, if existent). The aim of this section is to describe the structure of the group $E(\mathbb{Q})$:

It will turn out, that we can consider points of finite order and points of infinite order separately. This section largely provides an overview of results in this area; few theorems are actually proved.

Since the characteristics of $\mathbb{Q}$ is 0, we can make an admissible change of variables, such that $E(\mathbb{Q})$ is given by an equation of the form

$$E: y^2 = x^3 + ax^2 + bx + c. \tag{2.40}$$

For the considerations of this chapter, let always $E(\mathbb{Q})$ be an elliptic curve over $\mathbb{Q}$ like in (2.40) and ∞ denote the infinite point in the projective closure at $(0:1:0)$.

Definition 2.6.1. We say that a point $P \in E(\mathbb{Q})$ has m-torsion if $mP = \infty$. (Writing mP just means adding P to itself m times).

As a motivation, let us first regard the special case of a, b, c being integer coordinates:

It turns out, that we can easily characterize the set of 2-torsion points, denoted by $E(\mathbb{Q})[2]$. Clearly, $2\infty = \infty$. Otherwise, let $P = (x_0, y_0)$ be an affine point such that $2P = \infty$, or, equivalently, $P = -P$. Since the negative of a point is just that point reflected around the x-axis due to theorem 2.5.6, a point (x_0, y_0) is its own inverse, if it lies on the x-axis, i.e. $y_0 = 0$. Then, x_0 is a solution of the equation $f(x) = x^3 + ax^2 + bx + c = 0$. Since we assumed, that a, b, c are integers, each rational solution of this polynomial equation must already be integer. This is, because the denominator of each such solution must divide the coefficient of x^3, which is 1.

Thus, in this case, we get a point of order two for every integral root of $f(x)$. The set of 2-torsion points actually forms a subgroup of $E(\mathbb{Q})$. This subgroup, $E(\mathbb{Q})[2]$, is either the trivial group, $\mathbb{Z}/2\mathbb{Z}$, or $Z/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, depending on whether $f(x)$ has zero, one or three integral roots.

It can be shown, that for each $m \geq 1$ and for any $P \in E(\mathbb{Q})[m]$, this point P will have integer coordinates. Furthermore, the discriminant Δ of $f(x)$ is given by $4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$. Then either $y_0 = 0$ (and $m = 2$), or $y^2|\Delta$. This result is known as the *Nagell-Lutz theorem.*

Proposition 2.6.2. *For an elliptic curve*

$$E: y^2 = x^3 + ax^2 + bx + c. \tag{2.41}$$

with integer coordinates, there exists an algorithm to check, if a point $P \in E(\mathbb{Q})$ has finite order.

Proof. We simply calculate P, $2P$, $3P$, etc., until an m is found such that either $mP = \infty$ (then, P is an m-torsion point) or mP does not have integer coordinates, or the y-coordinate of mP does not divide the discriminant (in these two cases, P is not a torsion point). Since there are only finitely many integers which divide Δ, the algorithm will terminate after finitely many steps. □

However, the group $E(\mathbb{Q})$ could contain elements of infinite order, as well. That this can happen is evidenced for example by the elliptic curve

$$y^2 = x^3 + 17.$$

One can check, that the point $P = (1/4, 33/8)$ lies on the curve. But its coordinates are not integers, while all points of finite order have integer coordinates. So P must be of infinite order.

It turns out that, even though the group $E(\mathbb{Q})$ may not be finite and there are elements of infinite order, $E(\mathbb{Q})$ is always finitely generated: There exists a finite set of points so that any other point is equal to some linear combination of that set of points: $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$, where T is a finite commutative group. In other words, there is a set of points $P_1, P_2, \ldots, P_r$ so, that for a $Q \in E(\mathbb{Q})$, we can always find integers $c_1, \ldots, c_r$ and a $F \in T$ such that $Q = F + c_1P_1 + c_2P_2 + \cdots + c_rP_r$. r is called the *rank* of the elliptic curve. It is the size of a smallest torsion-free generating set.

This theorem was proved by Mordell in 1922, and subsequently generalized to arbitrary abelian varieties over number fields by Weil, compare [LM] and [AWe1], [AWe2].

The proof given here assumes that there is a rational point of order two on the curve. While the theorem is true without this assumption, the proof is somewhat simpler if we can stay in the rational numbers. Now, if E is a curve given in Weierstrass form, then a rational point of order two looks like $(x_0, 0)$. We can make an admissible change of varibales, $(x, y) \to (x - x_0, y)$ which sends $(x_0, 0)$ to $(0, 0)$. Such a change does not affect the structure of the group $E(\mathbb{Q})$. Thus, given the restriction that we are considering curves with a rational two-torsion point, we can assume that E is given by $y^2 = x^3 + ax^2 + bx$, not necessarily with integer coefficients.

Our first goal is to show that the image of the multiplication-by-two map $[2] : E(\mathbb{Q}) \to E(\mathbb{Q})$ has finite index. The approach taken here is to break the map $[2]$ into two pieces, and show that the image at each step has finite index.

Initially, we need to find a group G and a pair of maps $f : E(\mathbb{Q}) \to G, g : G \to E(\mathbb{Q})$ so, that $g(f(P)) = [2](P) = 2P$.

For any particular curve E, we pick a related elliptic curve E' and map $\varphi : E(\mathbb{Q}) \to E'(\mathbb{Q})$ and $\psi : E'(\mathbb{Q}) \to E(\mathbb{Q})$. These will be given by explicit formulas. Some of the motivation for the specific choices of E, φ and ψ is given in [ST].

Given a curve $E : y^2 = x^3 + ax^2 + bx$, define the curve E' by

$$\begin{aligned} E' : y^2 &= x^3 + a'x^2 + b'x \\ a' &:= -2a \\ b' &:= a2 - 4b. \end{aligned}$$

In a sense, E and E' are duals of each other. Applying the construction twice yields $E'' : y^2 = x^3 + (-2 \cdot -2a)x^2 + (4a^2 - 4(a^2 - 4b))x$, or $y^2 =$

$x^3 + 4ax^2 + 16b$. This is almost the same as the original curve, E; for if (x_0, y_0) is a point on E, then $(4x_0, 8y_0)$ must be a point on E''. It's similarly easy to identify a point on E'' with a point on E. In fact, the two curves are isomorphic via this identification. This will be useful in constructing the maps φ and ψ.

Define the map $\varphi : E \to E'$ by $(x, y) \to (\frac{y^2}{x^2}, y\frac{x^2-b}{x^2})$. This is well-defined everywhere on E except ∞, and the two-torsion point $(0, 0)$, which is the only point on E with a zero x-coordinate. We can extend the definition to everywhere on E.

$$\varphi : E \to E', \quad \varphi(x, y) := \begin{cases} \left(\frac{y^2}{x^2}, y\frac{x^2-b}{x^2}\right) & \text{for } P = (x, y) \neq (0, 0), \infty \\ \infty' & \text{for } P = (0, 0) \text{ or } P = \infty. \end{cases}$$

Here, ∞' is the point at infinity on E'.

One can use an identical construction to get a map from E' to E''. What we actually want, however, is a map from E' back to the original curve, E. Thus, we combine the above map with $(x, y) \to (x/4, y/8)$ to define ψ:

$$\psi : E' \to E, \quad \varphi(x, y) := \begin{cases} \left(\frac{y'^2}{4x'^2}, y\frac{x'^2-b}{8x'^2}\right) & \text{for } P = (x', y') \neq (0, 0), \infty \\ \infty & \text{for } P = (0, 0) \text{ or } P = \infty'. \end{cases}$$

The maps φ and ψ are partially characterized by the following proposition:

Proposition 2.6.3. *Let E, E', φ and ψ be defined as above. Then the following statements hold:*

1. *The maps φ and ψ are homomorphisms.*
2. *The kernel of φ is $\{(0, 0), \infty\}$, and the kernel of ψ is $\{(0, 0), \infty'\}$.*
3. *The composition of the maps is multiplication by two, i.e., $\psi \circ \varphi = [2]$, and $\varphi \circ \psi = [2]'$.*

Proof. The proof of this proposition is simple, but tedious; the approach is merely indicated here. Proving that φ is a homomorphism is a matter of verifying that the group law is preserved: $\varphi(P + Q) = \varphi(P) + \varphi(Q)$. So we have to confirm, that the rational functions obtained through addition and application of φ match up as they should. The price of having such concrete definitions of φ and the group law is that many cases must be separately checked. Of course, if φ is a homomorphism, then ψ is too, because of the way it was constructed.

Showing that $\ker \varphi = \{(0, 0), \infty\}$ is trivial, given the definition of φ; all other points are mapped to affine points on E'. The same argument works for ψ.

Finally, $\psi \circ \varphi(P) = 2P$. This, too, can be verified through purely algebraic computations. □

Thus far, we have broken multiplication by two into two maps, as promised. We now give the following

Proposition 2.6.4. *Let A and B be abelian groups with homomorphisms $\varphi : A \to B$ and $\psi : B \to A$, such that $\psi \circ \varphi = [2]A$ and $\varphi \circ \psi = [2]B$. Also, suppose that $[B : \varphi(A)]$ and $[A : \psi(B)]$ are both finite. Then the index $[A : 2A]$ is finite.*

Proof. The proof is straight-forward. Take $a_1, \dots, a_m$ and $b_1, \dots, b_n$ to be coset representatives for $\psi(B)$ in A and $\varphi(A)$ in B, respectively. Now one shows that the set $\{a_i + \psi(b_j)\}$ is a complete set of coset representatives for $2A$ in A. □

Applying this proposition we find that $[E(Q) : 2E(Q)]$ is finite, as desired, if we are able to show that the index of the image of each map is finite, i.e., that $[E'(\mathbb{Q}) : \varphi(E(\mathbb{Q}))]$ and $[E(\mathbb{Q}) : \psi(E'(\mathbb{Q}))]$ are both finite.

This is the hardest part of the proof. As before, the approach is to (seemingly arbitarily) define a map, and then show that it behaves nicely. The following definitions and lemmas will be stated for the $\varphi : E \to E'$ half of the problem; the analogous statements for ψ can be made and proven in the same way.

We can define a map $\alpha' : E'(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$, where $\mathbb{Q}^*$ is the multiplicative group of rational units, and $\mathbb{Q}^{*2}$ is the subgroup consisting of perfect squares. So $\mathbb{Q}^*/\mathbb{Q}^{*2}$ is like the nonzero rational numbers, with two elements identified if their quotient is the square of a rational number.

$$\alpha' : E'(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2},\ \alpha'(x', y') := \begin{cases} x' \mod \mathbb{Q}^{*2} & \text{for } P = (x', y') \neq (0,0) \\ 1 \mod \mathbb{Q}^{*2} & \text{for } P = (0,0) \\ b' \mod \mathbb{Q}^{*2} & \text{for } P = \infty'. \end{cases}$$

Now, one can proof the following proposition, which characterizes the behaviour of α':

Proposition 2.6.5. *Let E, E', φ and α' be as above. Then the following statements hold:*

1. *The map $\alpha' : E'(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ is a homomorphism of groups.*

2. *The kernel of α' is $\varphi(E(\mathbb{Q}))$ and α' induces a natural injection $\frac{E'(\mathbb{Q})}{\varphi(E(\mathbb{Q}))} \hookrightarrow \frac{Q^*}{Q^{*2}}$.*

3. *Let $p_1, \dots, p_r$ be distinct primes dividing b'. Then the image of α' is contained in the subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ with representatives*

$$\{(-1)^{\epsilon_0} p_1^{\epsilon_1} p_2^{\epsilon_2} \dots p_r^{\epsilon_r} \ : \ \epsilon \in \{0,1\}\} \subset \mathbb{Q}^*/\mathbb{Q}^{*2}.$$

We do not give a proof here, but an overview of it is given in [JA]. Using this proposition, we can show the following consequence:

Corollary 2.6.6. *The index* $[E'(\mathbb{Q}) : \varphi(E(\mathbb{Q}))]$ *is finite.*

Proof. Let R^* be the subgroup of $\mathbb{Q}^*$ given by

$$R^* := \{\pm p^{e_1} p^{e_2} \cdots p^{e_r} \ : \ e_i \in \mathbb{Z}\}.$$

The size of R^*/R^{*2} is easily seen to be 2^{r+1}, and $E'(\mathbb{Q})/\varphi(E(\mathbb{Q}))$ maps injectively into it due to proposition 2.6.5. So the index $[E'(\mathbb{Q}) : \varphi(E(\mathbb{Q}))] \leq 2^{r+1}$, and is certainly finite. □

In a similar way, it can be shown, that $[E(\mathbb{Q}) : \psi(E'(\mathbb{Q}))]$ is also finite.

Since $[E(\mathbb{Q}) : 2E(\mathbb{Q})] = [E(\mathbb{Q}) : \psi\varphi(E(\mathbb{Q}))]$, we can use proposition 2.6.4 and get the following

Theorem 2.6.7. *Let* $2E(\mathbb{Q})$ *denote the subgroup obtained by doubling all the points in* $E(\mathbb{Q})$*:* $2E(\mathbb{Q}) = \{2P : P \in E(\mathbb{Q})\}$*. Then the index* $[E(\mathbb{Q}) : 2E(\mathbb{Q})]$ *is finite.*

This is the first half of the Mordell-Weil theorem.

The other half of the Mordell-Weil theorem requires a notion of the *height* of a point. This yields a tool which is useful in establishing a set's finitude.

The classic method of descent uses the absolute value function in order to show that, for example, a given polynomial has no integer solutions: One shows that, given a particular integer solution, one can produce another solution whose absolute value is strictly smaller. This yields a contradiction: On one hand, one claims that there is an infinite sequence of integers with strictly decreasing absolute value. On the other hand, the set of integers with absolute value less than some particular value is finite.

This notion of the size of a solution works quite well for studying integers. However, it is not as well suited to studies of rational solutions to equations. The key fact used in the strategy outlined above is that, for any bound B, the set $\{x \in \mathbb{Z} : |x| \leq B\}$ is finite. If we let x take on rational values, however, this assertion is no longer true. For example, one could take the set $\{1, \frac{1}{2}, \frac{1}{3}, \dots\}$. We need a slightly different measure of the size of a rational number.

Let us define the height of a rational number x to be the maximum of the absolute value of its numerator and denominator. More formally,

Definition 2.6.8. Let $x = \frac{m}{n}$ be a rational number, where m and n are relatively prime. Then, the *height function* is given by $H(x) := \max\{|m|, |n|\}$.

This enjoys the same sort of finiteness property described above. Specifically, for any B, the set $\{x \in \mathbb{Q} : H(x) \leq B\}$ is finite.

Now this definition can be extended to the rational points on an elliptic curve. Let $P = (x, y)$ be an affine point on the curve and define $H(P) := H(x)$. A similar finiteness property still holds, namely $\{P \in E(\mathbb{Q}) : H(P) \leq B\}$ is finite for any fixed bound B. This is because there are only finitely many choices for the x-coordinate, and any value of x yields at most two points on the curve E.

The height function behaves somewhat multiplicatively on the rationals; it makes sense to compare $H(x)H(y)$ to $H(xy)$. Notationally, however, it is desirable to have a function, which acts additively. There is an addition law on points on an elliptic curve, while there is no multiplication function. So we define the logarithmic height as follows:

Definition 2.6.9. Given a point (x, y) on the curve, the *logarithmic height* is given by

$$h(x) := \log H(x).$$

Since for any rational number x, $H(x)$ is at least 1, we see, that $h(x)$ is always a nonnegative real number.

To prove the Mordell-Weil theorem, one must establish certain properties of this height function:

Proposition 2.6.10. *Define the logarithmic height function $h : E(\mathbb{Q}) \to \mathbb{R}$ as above. Then the following statements hold:*

1. *For every $B \in \mathbb{R}$, the set $\{P \in E(\mathbb{Q}) : h(P) \in B\}$ is finite.*
2. *For every $P_0 \in E(\mathbb{Q})$ there is a constant κ_0, depending only on P_0 and E, such that $h(P + P_0) \leq 2h(P) + \kappa_0$ for all $P \in E(\mathbb{Q})$.*
3. *There is a constant κ, depending only on E, such that $h(2P) \geq 4h(P) - \kappa$.*

Proof. The first part of this proposition follows directly from the discussion above.

The proof of the latter two parts can be read in [ST]. Essentially, one works with the concrete descriptions of the addition laws, and attempts to compute the height of the resulting value. This can be a little intricate. The quotients given by the addition formulae are not necessarily in reduced lowest form. One must show that there is not too much cancellation between the numerator and the denominator, in order to put a lower bound on the resulting height. □

Given the proposition 2.6.10 of the height function and theorem 2.6.7, we can prove the desired theorem:

Theorem 2.6.11 (Mordell-Weil)**.** *Let $E(\mathbb{Q})$ be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})$ is finitely generated.*

Proof. We prove this theorem for elliptic curves E only for the case, in which there exists a rational point of order two.

Theorem 2.6.7 says that the group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, so we can take a finite set of representatives $\mathcal{Q} = \{Q_1, Q_2, \dots, Q_r\}$ for the cosets of $2E(\mathbb{Q})$ in $E(\mathbb{Q})$.

The second part of proposition 2.6.10 yields, that for each Q_i, there exists a κ_i, such that $h(Q_i + P) \leq 2h(P) + \kappa_i$ for all rational points P. Since there are only finitely many Q_i, we can take κ' to be the maximum of these κ_i. Thus

$$h(Q_i + P) \leq 2h(P) + \kappa' \quad \text{for all } Q_i \in \mathbb{Q} \text{ and } P \in E(\mathbb{Q}). \tag{2.42}$$

Let κ be the constant from the same proposition, such that

$$h(2P) \geq 4h(P) - \kappa. \tag{2.43}$$

Then the set $\mathcal{R} := \{P \in E(Q) : h(P) \leq \kappa' + \kappa\}$ is finite, as well. As we will see shortly, $\mathcal{Q} \cup \mathcal{R}$ already generates all of $E(\mathbb{Q})$.

To prove this claim, we must show that any $P \in E(\mathbb{Q})$ can be written as a combination of elements of $\mathcal{Q} \cup \mathcal{R}$.

In a way, this proof is inductive. Indeed, if the error-terms κ and κ' were zero, one could prove the theorem by induction on the height. Even with the error term, however, the proof is elementary.

The point P must have a coset representative $Q_{i_1} \in E(\mathbb{Q})/2E(\mathbb{Q})$ with $P - Q_{i_1} \in 2E(\mathbb{Q})$. So there is a P_1, such that $P - Q_{i_1} = 2P_1$. Similarly, we can find an index i_2 and a point P_2 so that $P_1 - Q_{i_2} = 2P_2$. In fact, we can continue this chain as far as we like. Substituting after the m-th iteration, we find

$$\begin{aligned} P &= Q_{i_1} + 2(Q_{i_2} + 2(Q_{i_3} + \cdots + P_m)\cdots)) \\ &= Q_{i_1} + 2Q_{i_2} + 4Q_{i_3} + \cdots + 2^{m-1}Q_{i_m} + 2^m P_m. \end{aligned}$$

Each of the Q_{i_j} is in $\mathcal{Q}$, of course. If we can show, that we can pick a (finite) m so, that $P_m \in \mathcal{Q} \cup \mathcal{R}$, we are finished.

The strategy is to show that the logarithmic height decreases enough at each step to force P_m into $\mathcal{R}$. We want to show that at, say, the j-th step of the chain, the size is decreasing.

From (2.42) and (2.43), we get

$$4h(P_j) \leq h(2P_j) + \kappa = h(P_{j-1} - Q_{i_j}) + \kappa \leq 2h(P_{j-1}) + \kappa' + \kappa.$$

Now we can isolate $h(P_j)$ as follows:

$$\begin{aligned} h(P_j) &\leq \frac{1}{2}h(P_{j-1}) + \frac{\kappa' + \kappa}{4} \\ &= \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - (\kappa' + \kappa)). \end{aligned}$$

If $h(P_{j-1}) \leq \kappa' + \kappa$, then we are done, since $P_{j-1} \in \mathcal{R}$. Otherwise, $h(P_j) \leq \frac{3}{4}h(P_{j-1})$. The height is decreasing by a factor of 3/4 at every step. After some finite number of steps, the height of $h(P_m)$ will be less than the bound $\kappa' + \kappa$, and so P_m will be in $\mathcal{R}$. This concludes the proof of the Mordell-Weil theorem. □

Corollary 2.6.12. *Every elliptic curve $E(\mathbb{Q})$ can be written in the form $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$. T is uniquely defined, finite and commutative and called the* Torsion subgroup *of E, r is the* rank *of E.*

Proof. This is an immediate consequence from theorem 2.6.11 and the fundamental theorem of finitely generated abelian groups. □

Chapter 3

L-functions and further applications

In the last chapter, we gave an overview of important results about elliptic curves over the fields $\mathbb{C}$, $\mathbb{R}$ and $\mathbb{Q}$. In this chapter, we want to focus on finite fields of characteristics p, where p is a prime. More exactly, we will define the reduction of an elliptic curve modulo some prime p. We will see, that we can describe much information about an elliptic curve and its reductions modulo all primes with its L-function. This leads to some quite interesting results in number theory.

3.1 Singular points

Singular Weierstrass curves arise for certain primes p when a Weierstrass curve with integral coefficients is considered modulo p. Such curves are easy to analyze and we shall note some ot their features in this section.

Let E be a singular Weierstrass curve over a field K. We saw in proposition 2.3.2 that the infinite point $(0 : 0 : 1)$ on the curve is nonsingular. So we have only to analyze points (x, y) in the affine plane. We will see, that there is only one singularity and that, under a mild restriction on K, it occurs at a rational point (x_0, y_0).

We then can make an admissible change of variables to translate (x_0, y_0) to the origin $(0, 0)$. This leads to a projective curve of the form

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{3.1}$$

with $a_6 = 0$, like in (2.1) . The condition that $\frac{\partial}{\partial x}$ give 0 at $(0 : 1 : 0)$ means, that $a_4 = 0$ and the condition, that $\frac{\partial}{\partial y}$ give 0 at $(0 : 1 : 0)$ means, that $a_3 = 0$. Thus, E is given in affine form by the equation

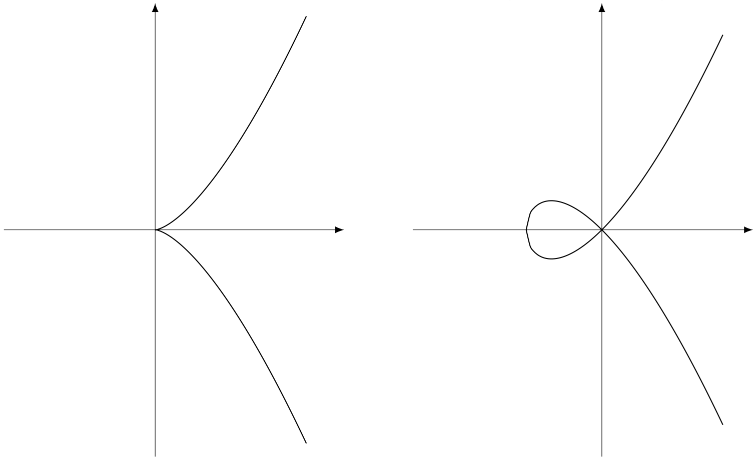
$$y^2 + a_1xy = x^3 + a_2x^2. \tag{3.2}$$

We can factor $y^2 + a_1xy - a_2x^2$ over $\overline{K}$, obtaining

$$(y - \alpha x)(y - \beta x) = x^3 \quad \text{with } \alpha, \beta \in \overline{K}. \tag{3.3}$$

We say, that a singular point $(0, 0)$ is a *cusp* , if $\alpha = \beta$, or a *node* , if $\alpha \neq \beta$.

Pictures of the two kinds of behaviour (with $a_1 = 0$) are as follows:



We now get the following theorem about singular planar curves:

Theorem 3.1.1. *For a singular Weierstrass curve E over a field K, there is only one singular point (x_0, y_0). It is K-rational, if either*

1. $\mathrm{char}(K) \neq 2$ *or*
2. $\mathrm{char}(K) = 2$ *and K is closed under the operation of taking square roots (as is the case, when K is a finite field of characteristics* 2*).*

The point (x_1, y_1) is a cusp, if $c_4 = 0$ or a node, if $c_4 \neq 0$, using the notation from (2.8).

Proof. If $\mathrm{char}(K) \neq 2$, we can apply, without loss of generality, a projective transformation to eliminate the a_1 and a_3 terms. By proposition 2.3.11, the curve will be singular, if and only if the cubic polynomial f in x has a repeated root. In this case, f and f' have a greatest common divisor g over K with degree ≥ 1 and the singular points are $(x_0, 0)$, where x_0 ranges over the roots of g.

If g has degree 1, its unique root x_0 is in K and $(x_0, 0)$ is the unique singular point. If g has degree 2, its two roots x_0 and x_0' must be equal, since otherweise x_0 and x_0' would both be roots of multiplicity ≥ 2 for the cubic polynomial f. Since we can conclude $x_0 = x_0'$, x_0 is in K and $(x_0, 0)$ is the unique singular point.

If $\mathrm{char}(K) = 2$, the singular points are the points (x_0, y_0) on the affine curve over $\overline{K}$, satisfying the two equations

$$\begin{aligned} 0 &= \frac{\partial}{\partial x} = a_1 y_0 + x_0^2 + a_4 \\ 0 &= \frac{\partial}{\partial y} = a_1 x_0 + a_3, \end{aligned}$$

from (2.28) and (2.29). If $a_1 \neq 0$, the second equation uniquely determines x_0 and the first equation then uniquely determines y_0. The resulting point (x_0, y_0) is K-rational. If $a_1 = 0$, the first equation forces $x_0^2 + 4 = 0$. In characteristics 2, square roots are unique and the second assumption 2 says, that x_0 is in K. Since the second equation shows $a_3 = 0$, y_0 is given by

$$y_0^2 = x_0^3 + a_2 x_0^2 + a_4 x_0 + a_6$$

and again exists in K. It is unique in $\overline{K}$ under the assumption 2.

Return to general K. Under the translation over $\overline{K}$, that moves (x_0, y_0) to the origin, c_4 is unaffected. Thus it is enough to decide cusp vs. node in (3.2). From (2.7) and (2.8), the value of c_4 is

$$c_4 = b_2^2 - 24 b_4 = (a_1^2 + 4a_2)^2 - 24(2a_4 + a_1 a_3) = (a_1^2 + 4a_2)^2.$$

If $\mathrm{char}(K) \neq 2$, the discriminant of $y^2 + a_1 xy - a_2 x^2$ is $a_1^2 + 4a_2$, which is 0, if and only if $c_4 = 0$; hence $\alpha = \beta$ (and there is a cusp) if and only if $c_4 = 0$.

If $\mathrm{char}(K) = 2$, then

$$(y - \alpha x)^2 = y^2 + a_1 xy - a_2 x^2$$

says $a_1 = 0$ and $\alpha^2 = a_2$. Hence, $\alpha = \beta$ (and there is a cusp) if and only if $a_1 = 0$, which happens if and only if $c_4 = 0$. □

It will be useful to distinguish two subcases of nodes:

Definition 3.1.2. We say, that a node is in *split case*, if the mombers α and β of (3.3) lie in K. In the contrary case, α and β lieb in a nontrivial quadratic extension of K and we say, that the node is in a *nonsplit case.*

Theorem 3.1.3. *For the singular Weierstrass equation E in (3.2), the map*

$$t \to (t^2 + a_1 t - a_2, t(t^2 + a_1 t - a_2)$$

carries $K \backslash \{\alpha, \beta\}$ one-one onto $E(K) \backslash \{\infty, (0,0)\}$, where ∞ stands for the infinite point $(0:1:0)$ in the projective closure. If K is a finite field with $|K|$ elements, the nonsingular set $E(K) \backslash \{(0,0)\}$ therefore has

$|K| - 1$ *elements, if $(0,0)$ is a split-case node.*
$|K| + 1$ *elements, if $(0,0)$ is a nonsplit-case node.*
$|K|$ *elements, if $(0,0)$ is a cusp.*

Proof. In (3.2), $x = 0$ gives only $y = 0$ and $(0, 0)$ is singular. Thus, any nonsingular point of $E(K)\backslash\{\infty\}$ has $y = tx$ for a unique member t of K. Substituting tx for y in (3.2) and using $x \neq 0$, we are led to

$$t^2 + a_1 t - a_2 = x.$$

Then also y is $t(t^2 + a_1 t - a_2)$ and K maps onto the affine solutions of (3.2). To exclude $x = 0$ from the image, we must exclude the roots of $t^2 + a_1 t - a_2$; these are α and β. Once, $x = 0$ is not in the image, the map is one-one, since t is recovered as y/x. The numerology, if K is a finite field is then clear. □

3.2 Reduction modulo p

We begin with the definition of a p-adic norm on $\mathbb{Q}$, p being a prime:

Definition 3.2.1. Let p be a prime and $r \neq 0$ be in $\mathbb{Q}$. We write $r = p^n u/v$ with integers u and v such that u, v, p are all relatively prime, i.e. the greatest common divisor of two of these values equals 1. The definition of the *p-adic norm* then is $|r|_p := p^{-n}$. By convention, we define $|0|_p := 0$.

Lemma 3.2.2. *The p-adic norm has the following properties:*

1. $|r + s|_p \leq \max\{|r|_p, |s|_p\}$, *with equality, if* $|r|_p \neq |s|_p$,
2. $|rs|_p = |r|_p |s|_p$.

Proof. Property (ii) is obvious from the definition. For (i), we write $r = p^n u/v$ and $s = p^{n'} u'/v'$. Without loss of generality, we may assume $n \leq n'$. Writing

$$r + s = p^n \left(\frac{u}{v} + p^{n'-n} \frac{u'}{v'} \right) = p^n \frac{uv' + p^{n'-n} u'v}{vv'}$$

with vv' and p being relatively prime. Then we obtain (i) directly. □

Remark 3.2.3. Property (i) is called the *ultrametric inequality.* It implies $|r+s|_p \leq |r|_p + |s|_p$. If we define $d(x, y) = |x-y|_p$, then the latter inequality implies the triangle inequality for d and d is therefore a metric on $\mathbb{Q}$.

Definition 3.2.4. We say, that $r \in \mathbb{Q}$ is *p-integral* , if $|r|_p \leq 1$. Due to lemma 3.2.2, the p-integral elements form a subring of $\mathbb{Q}$ containing $\mathbb{Z}$. Those with $|r|_p < 1$ form an ideal in this subring; they of course have $|r|_p \leq p^{-1}$.

Let $\mathbb{Z}_p$ be the finite field with p elements. The p-integral elements of $\mathbb{Q}$ can be reduced modulo p : If $r = p^n u/v$ is p-integral, i.e. if $n \geq 0$, then we define $r_p(r) \in \mathbb{Z}_p$ by

$$r_p(r) = \begin{cases} uv^{-1} \mod p & \text{if } n = 0 \\ 0 & \text{if } n > 0. \end{cases}$$

Then, $r_p : \{p\text{-integral elements}\} \to \mathbb{Z}_p$ is a ring homomorphism.

In preparation for considering plane curves, we can try to use r_p to get a map of the affine plane over $\mathbb{Q}$ to the affine plane over $\mathbb{Z}_p$, but the best we can get is a map defined on

$$\{(r, s) | r \text{ and } s \text{ are } p\text{-integral}\}$$

as $r_p(r, s) := (r_p(r), r_p(s))$. To correct this deficiency, we work with curves projectively as follows:

To define $r_p : P_2(\mathbb{Q}) \to P_2(\mathbb{Z}_p)$, we let

$$r_p(x : y : z) = (r_p(x) : r_p(y) : r_p(z)), \tag{3.4}$$

where $(x : y : z)$ are coordinates of the point in question chosen so that x, y, z all have $|\cdot|_p \le 1$ and at least one of them has $|\cdot|_p = 1$. Such a representative of a point in $P_2(\mathbb{Q})$ is sait to be *p-reduced* . Note that if a general $(x : y : z)$ is given, we can multiply a suitable p^n to obtain a p-reduced representative. A p-reduced representative is unique up to a factor with $|\cdot|_p = 1$. Therefore r_p is well defined as a map of all of $P_2(\mathbb{Q})$ into $P_2(\mathbb{Z}_p)$.

Using (3.4), we can reduce projective plane curves modulo p. Let $F \in \mathbb{Q}[x, y, z]_m$ be a plane curve of degree m. Multiplying the coefficients of F by a constant, we may assume that all the coefficients have $|\cdot|_p \le 1$ and at least one has $|\cdot|_p = 1$. Then we can reduce the coefficients modulo p, obtaining a nonzero polynomial $F_p \in \mathbb{Z}_p[x, y, z]_m$. Although F_p is not defined uniquely, it is defined uniquely up to a nonzero scalar. Therefore its zero locus $F_p(\mathbb{Z}_p)$ is well defined.

Proposition 3.2.5. *Let $F \in \mathbb{Q}[x, y, z]_m$ be a plane curve. Under the reduction homomorphism $r_p : P_2(\mathbb{Q}) \to P_2(\mathbb{Z}_p)$ given in (3.4), the image of $F(\mathbb{Q})$ is contained in $F_p(\mathbb{Z}_p)$.*

Proof. We normalize the coefficients of F as described above. Now let $(x : y : z)$ be a reduced representative of a point in $P_2(\mathbb{Q})$. Then

$$\begin{aligned} (x : y : z) \in F(\mathbb{Q}) &\Leftrightarrow F(x : y : z) = 0 \\ &\Rightarrow r_p(F(x : y : z)) = 0 \\ &\Leftrightarrow F_p(r_p(x) : r_p(y) : r_p(z)) = 0 \\ &\Leftrightarrow F_p(r_p(x : y : z)) = 0 \\ &\Leftrightarrow r_p(x : y : z) \in F_p(Z_p). \end{aligned}$$

□

Proposition 3.2.6. *Suppose $F \in \mathbb{Q}[x, y, z]_m$ is a plane curve, $L \in \mathbb{Q}[x, y, z]_1$ is a line and $P = (x_0 : y_0 : z_0)$ is a point on L. If F_p and L_p are reductions of F and L modulo p, then the intersection multiplicities satisfy*

$$i(L, F; P) \le i(L_p, F_p; r_p(P)). \tag{3.5}$$

Proof. Without loss of generality, we may assume, that $(x_0 : y_0 : z_0)$ is a p-reduced representative and that the coefficients of F and L are normalized as they supposed to be. Choose a p-reduced representative $(x' : y' : z') \neq (x_0 : y_0 : z_0)$ of a point P' of L and form

$$\begin{aligned} \psi(t) &= F(P + tP') = F(x_0 + tx'_0 : y_0 + ty'_0 : z_0 + tz'_0) \\ &= t^r F'_r + \cdots + t^m F'_m, \end{aligned}$$

with $F'_r \neq 0$. Now it is not difficult to see, that $i(L, F; P)$ equals the order of vanishing at $t = 0$ of $\psi(t)$. This yields, that the left side of (3.5) is r. Recomputing $\psi(t)$ modulo p (i.e. in $\mathbb{Z}_p[t]$), we see the same way, that the right side of (3.5) is $\geq r$. □

Let us apply proposition 3.2.5 and proposition 3.2.6 to elliptic curves E over $\mathbb{Q}$. For studying $E(\mathbb{Q})$, we may make an admissible change of variables to make all coefficients of E be in $\mathbb{Z}$. Then, we can assume E being in Weierstrass form with all coefficients in $\mathbb{Z}$. To apply the above theory, we consider the projective form (2.1) of E. The coefficients of E are all in $\mathbb{Z}$ and hence are p-integral. Also zy^2 and x^3 have coefficient 1. Thus passage to E_p is given simply by writing (2.1) with coefficients considered in $\mathbb{Z}_p$, no preliminary normalization is needed.

The discriminant of E_p is clearly given by

$$\Delta_p = \Delta \mod p.$$

Thus, E_p is smooth, if and only if $p \nmid \Delta$. Our reduction map on $E(\mathbb{Q})$ is a mapping

$$r_p : E(\mathbb{Q}) \to E_p(\mathbb{Z}_p) \tag{3.6}$$

by proposition 3.2.5.

Proposition 3.2.7. *If E_p is smooth, then the map r_p in (3.6) is a group homomorphism.*

Proof. Since $r_p(0 : 1 : 0) = (0 : 1 : 0)$, r_p carries the infinite point ∞ of E to the infinite point ∞_p of E_p. We apply proposition 3.2.6. Since the sum of intersection multiplicities over a line is ≤ 3 by theorem 2.2.5, the proposition gives $r_p(P \bullet Q) = r_p(P) \bullet r_p(Q)$. Thus

$$\begin{aligned} r_p(P + Q) &= r_p(\infty \bullet (P \bullet Q)) = r_p(\infty) \bullet r_p(P \bullet Q) \\ &= r_p(\infty \bullet (r_p(P) \bullet r_p(Q)) \\ &= \infty_p \bullet (r_p(P) \bullet r_p(Q)) = r_p(P) + r_p(Q), \end{aligned}$$

according to the group law. So, r_p is a group homomorphism. □

3.3 Global minimal Weierstrass equations

Let E be an elliptic curve over $\mathbb{Q}$. Later, we want to define the L-function of E, which is a certain Euler product, that takes into account information about the reduction of E modulo each prime p. This section will deal with some preliminaries, that make the definition invariant under admissible changes of variables over $\mathbb{Q}$.

From the start, we may assume, that the equation of E is given in Weierstrass form, as in (2.1) and (2.2), i.e.

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$$

or its affine form

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

with integer coefficients. The discriminant Δ will then be an integer too and the p-adic norm will satisfy $|\Delta|_p \leq 1$ with equality if and only if $p \nmid \Delta$.

Definition 3.3.1. A Weierstrass form like above is called *minimal* for the prime p, if the power of p dividing Δ cannot be decreased by making an admissible change of variables over $\mathbb{Q}$ with the property, that the new coefficients are p-integral. It is the same to say, that $|\Delta|_p$ cannot be increased by such a change of variables. The equation is called a *global minimal Weierstrass equation*, if it is minimal for all primes and if its coefficients are integers.

Before considering existence and uniqueness questions for these notions, it will be helpful to have close at hand detailed formulas for an admissible change of variables. Such a change of variables is given as in (2.3.3) by

$$x = u^2x' + r \quad \text{and} \quad y = u^3y' + su^2x' + t. \tag{3.7}$$

The effect on the coefficients a_i of the Weierstrass equation and of the related coefficients b_i, c_i and Δ is given in the table below. The new coefficients are denoted by primes.

$$\begin{aligned}
ua'_1 &= a_1 + 2s \\
u^2a'_2 &= a_2 - sa_1 + 3r - s^2 \\
u^3a'_3 &= a_3 + ra_1 + 2t \\
u^4a'_4 &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\
u^6a'_6 &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \\
\\
u^2b'_2 &= b_2 + 12r \\
u^4b'_4 &= b_4 + rb_2 + 6r^2 \\
u^6b'_6 &= b_6 + 2rb_4 + r^2b_2 + 4r^3 \\
u_8b'_8 &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \\
\\
u^4c'_4 &= c_4 \\
u^6c'_6 &= c_6 \\
u^{12}\Delta' &= \Delta.
\end{aligned}$$

Lemma 3.3.2. *Suppose, p is a prime and all the coefficients a_i in the Weierstrass equation are p-integral. If $|\Delta|_p > p^{-12}$ or $|c_4|_p > p^{-4}$ or $|c_6|_p > p^{-6}$, then the equation is minimal for the prime p.*

Conversely, if $p > 3$ and $|\Delta|_p \leq p^{-12}$ and $|c_4|_p \leq p^{-4}$, then the equation is not minimal for the prime p.

Proof. Suppose, a change of variables like in (3.7) leads to a system of p-integral coefficients with a new discriminant Δ', such that $1 \geq |\Delta'|_p > |\Delta|_p$. Since $u^{12}\Delta' = \Delta$, we have $|u|_p^{12}|\Delta'|_p = |\Delta|_p$, so that $|u|_p \leq p^{-1}$, and

$$|\Delta|_p = |u|_p^{12}|\Delta'|_p \leq p^{-12}.$$

The arguments for c_4 and c_6 are similar.

Conversely, let $p > 3$ and $|\Delta|_p \leq p^{-12}$ and $|c_4|_p \leq p^{-4}$. Then, equation (2.13) gives $1728\Delta = c_4^3 - c_6^2$. Since $|1728|_p = 1$, we see, that $|c_6|_p \leq p^{-6}$. From proposition 2.3.4, we see that there is an admissible change of variables leading from (2.2) to

$$y^2 = x^3 - 27c_4x - 54c_6$$

with discriminant $\Delta' = 2^{12}3^{12}\Delta$. If we make an admissible change of variables like in (3.7) with $u = p$ and $r = s = t = 0$, we are led to

$$y^2 = x^3 - 27(c_4p^{-4})x - 54(c_6p^{-6}).$$

This has p-integral coefficients, since $|c_4p^{-4}|_p \leq 1$ and $|c_6p^{-6}|_p \leq 1$ and the discriminant $\Delta'' = p^{-12}\Delta'$ has $|\Delta''|_p = p^{12}|\Delta'|_p = p^{12}|\Delta|_p$. Hence the given equation was not minimal for the prime p. □

Remark 3.3.3. This proof shows, how constructively to achieve minimality simultaneously for all primes $p > 3$.

Proposition 3.3.4. *Fix a prime p and an elliptic curve E over $\mathbb{Q}$. Then, the following statements hold:*

1. *There exists an admissible change of variables for E over $\mathbb{Q}$, such that the resulting equation is minimal for the prime p.*
2. *If E has p-integral coefficients, then the change of variables in 1) has u, r, s, t all p-integral.*
3. *Two equations that are minimal for the prime p and that come from E are related by an admissible change of variables, in which $|u|_p = 1$ and r, s, t are p-integral.*

Proof. 1.: Without loss of generality, we may assume, that E has p-integral coefficients (or actually integral coefficients). Then, $|\Delta|_p \leq 1$. Since the range of $|\cdot|_p$ is discrete away from 0, $|\Delta|_p$ can be increased only finitely many times, if we are to maintain $|\Delta|_p \leq 1$. Hence, in finitely many steps, we can pass to an equation minimal for the prime p.

2.: Let E have coefficients $\{a_i\}$ and let the minimal equation have coefficients $\{a_i'\}$. Since $|\Delta'|_p \geq |\Delta|_p$, we must have $|u|_p \leq 1$ due to the last equation of the table. From (2.7), we see, that all $\{b_i\}$ and $\{b_i'\}$ are p-integral. Suppose $p \neq 3$. If $|r|_p > 1$, then the equation

$$u_8 b_8' = b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4$$

in the table has $3r^4$ as strictly the largest term in p-norm on the right side. This is a contradiction. If $p = 3$, we can argue similarly with the equation for $u^6 b_6'$ from the table and the term $4r^3$ to see, that $|r|_p \leq 1$. Similar arguments with $u^2 a'$ and $-s^2$, and then with $u^6 a_6'$ and $-t^2$ give $|s|_p \leq 1$ and $|t|_p \leq 1$.

3.: We apply 2) to the change of variables relating two minimal equations, finding that $|u|_p \leq 1$ and that r, s, t are p-integral. Applying 2) to the inverse change of variables, which involves u^{-1}, we see, that $|u^{-1}|_p \leq 1$. Thus, $|u|_p = 1$. □

For the proof of the next statement, we recapitulate the Chinese Remainder Theorem from the basic number theory:

Theorem 3.3.5 (Chinese Remainder Theorem). *Given a set of simultaneous congruences*

$$x \equiv a_i \mod m_i$$

for $i = 1, \ldots, r$ and for which the m_i are pairwise relatively prime, there exists a solution of this set of congruences, given by

$$x \equiv a_1 b_1 \frac{M}{m_1} + \cdots + a_r b_r \frac{M}{m_r} \mod M,$$

where

$$M = m_1 m_2 \cdots m_r$$

and the b_i are determined from

$$b_i \frac{M}{m_i} \equiv 1 \mod m_i$$

Theorem 3.3.6 (Néron). *If E is an elliptic curve over $\mathbb{Q}$, then there exists an admissible change of variables over $\mathbb{Q}$, such that the resulting equation is a global minimal Weierstrass equation. Two such resulting global minimal Weierstrass equations are related by an admissible change of variables with $u \pm 1$ and with $r, s, t \in \mathbb{Z}$.*

Proof. The uniqueness follows immediately from the third statement of proposition 3.3.4. So we are to prove existence:

Without loss of generality, we may assume, that E has integer coefficients a_i. For each p dividing Δ, choose an admissible change of variables $\{u_p, r_p, s_p, t_p\}$ over $\mathbb{Q}$, such that the resulting equation has coefficients $a_{i,p}$ and is minimal for the prime p. By the second statement of proposition 3.3.4, the rationals u_p, r_p, s_p, t_p are p-integral. If the new discriminant is denoted Δ_p, then the last formula of the table gives

$$|u_p|_p^{12} |\Delta_p|_p = |\Delta|_p. \tag{3.8}$$

Let us write

$$u_p = p^{d_p} v_p \quad \text{with } |v_p|_p = 1. \tag{3.9}$$

and define

$$u = \prod_{p|\Delta} p^{d_p}.$$

We shall make an admissible change of variables $\{u, r, s, t\}$ in the original equation, that leads to an equation with integer coefficients a'_i and discriminant Δ'. Since $u^{12}\Delta' = \Delta$, we have

$$|\Delta'|_p = |u|_p^{-12} |\Delta|_p = |u_p|_p^{-12} |\Delta|_p = |\Delta_p|_p$$

by (3.8). Thus, the new equation is minimal for all p, hence is globally minimal.

For each p with $p|\Delta$, let us write $r_p = p^{\rho_p} m_p / n_p$ with m_p and n_p in $\mathbb{Z}$ and with $|m_p|_p = |n_p|_p = 1$. Let n_p^{-1} be an inverse to n_p modulo p^{6d_p}. We set up the congruence

$$r \equiv p^{\rho_p} m_p n_p^{-1} \mod p^{6d_p}. \tag{3.10}$$

By the Chinese Remainder Theorem 3.3.5, we can find an integer r, such that (3.10) is satisfied for all p with $p|\Delta$. Then $|n_p r - p^{\rho_p} m_p|_p \leq p^{-6d_p}$ and

$$|r - r_p|_p \leq p^{-6d_p}$$

for all p. Similarly, we can find integers s and t, such that

$$|s - s_p|_p \leq p^{-6d_p} \quad \text{and} \quad |t - t_p|_p \leq p^{-6d_p}$$

for all p.

Our admissible change of variables $\{u, r, s, t\}$ is now defined and we are left with showing, that the new coefficients $\{a'_i\}$ are integers. We do this by checking for each prime p, that $|a'_1|_p \leq 1, \ldots, |a'_6|_p \leq 1$, using the formulas from the table. For $p \nmid \Delta$, there is no problem: Since $|u|_p = 1$ and r, s, t are integers, we have $|a'_i|_p \leq 1$. For $p|\Delta$, we estimate each $|a'_i|_p$. These estimates are similar and we illustrate with a'_2 only: We have

$$\begin{aligned} u^2 a'_2 &= a_2 - s a_1 + 3r - s^2 \\ &= (a_2 - s_p a_1 + 3r_p - s_p^2) - (s - s_p) a_1 + 3(r - r_p) - (s^2 - s_p^2) \\ &= u_p^2 a'_{2,p} - (s - s_p) a_1 + 3(r - r_p) - (s - s_p)(s + s_p). \end{aligned}$$

So we get

$$\begin{aligned} |u|_p^2 |a'_2|_p &\leq \max\{|u_p^2|_p |a'_{2,p}|_p, |(s - s_p) a_1|_p, |3(r - r_p)|_p, |(s - s_p)(s + s_p)|_p\} \\ &\leq \max\{|u_p^2|_p, |s - s_p|_p, |r - r_p|_p\} \text{ since } u_p, r_p, s_p, t_p \text{ are } p\text{-integral} \\ &\leq \max\{|u_p^2|_p, p^{-6d_p}\} \leq |u_p^2|_p \quad \text{by (3.9).} \end{aligned}$$

By the definition of u, it holds $|u|_p^2 = |u_p^2|_p$. Thus, $|a'_2|_p \leq 1$, and the proof is complete. □

The argument in theorem 3.3.6 is constructive, provided, we know how to produce, for each individual p, an equation, that is minimal for the prime p. The proof of lemma 3.3.2 shows, how to produce such an equation for primes $p > 3$. An algorithm of Tate, which we do not discuss here, handles the cases $p = 2$ and $p = 3$.

3.4 Dirichlet series and Euler products

Definition 3.4.1. A series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ with a_n and s complex is called a *Dirichlet series.*

The first result shows, that the region of convergence and the region of absolute convergence are each right half planes in $\mathbb{C}$ (unless it is equal to the empty set or all of $\mathbb{C}$. However, these half planes may not be the same: $\sum_{n=1}^{\infty} \frac{(-1)^n}{n^s}$ is convergent for $\Re(s) > 0$ and absolutely convergent for $\Re(s) > 1$.

Proposition 3.4.2. *Let $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ be a Dirichlet series. Then the following statements hold:*

1. *If the series is convergent for $s = s_0$, then it is convergent uniformly on compact sets for $\Re(s) > \Re(s_0)$ and the sum of the series is analytic in this region.*
2. *If the series is absolutely convergent for $s = s_0$, then it is uniformly absolutely convergent for $\Re(s) \geq \Re(s_0)$.*
3. *If the series is convergent for $s = s_0$, then it is absolutely convergent for $\Re(s) > \Re(s_0) + 1$.*
4. *If the series is convergent at some s_0 and sums to 0 in a right half plane, then all the coefficients are 0.*

Proof. The proof uses the *summation by parts* formula: If $\{u_n\}$ and $\{v_n\}$ are sequences and if $U_n = \sum_{k=1}^{n} u_k$ for $n \geq 0$, then $1 \leq M \leq N$ implies

$$\sum_{n=M}^{N} u_n v_n = \sum_{n=M}^{N-1} U_n(v_n - v_{n+1}) + U_N v_N - U_{M-1} v_M. \tag{3.11}$$

Details for this proof can be found in [AK] and will be omitted here. □

Example 3.4.3. The most important example of a Dirichlet series is the *Riemann zeta function*, which is defined as $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$. It is initially defined and analytic for $\Re(s) > 1$ and can be extended meromorphically for $\Re(s) > 0$. Its only pole is at $s = 1$, the pole has order 1.

The Riemann zeta function plays a pivotal role in analytic number theory and has applications in physics, probability theory, and applied statistics. By using a functional equation, it can be shown, that the Riemann zeta function has zeros at $-2, -4, -6, \ldots$. These are called the *trivial zeros*, in the sense that their existence is relatively easy to prove. It is known that any non-trivial zero lies in the open strip $\{s \in \mathbb{C} : 0 < \Re(s) < 1\}$. The Riemann hypothesis, considered one of the greatest unsolved problems in mathematics, asserts that any non-trivial zero s has $\Re(s) = \frac{1}{2}$.

We are now able to give a connection between Dirichlet series and infinite products:

An infinite product $\prod_{n=1}^{\infty} a_n$ with $a_n \in \mathbb{C}$ and with no factor 0 is said to *converge*, if the sequence of partial products converges and the limit is not 0. A necessary condition for convergence is that $a_n \to 1$.

Consider a formal product

$$\prod_{p \text{ prime}} (1 + a_p p^{-s} + \cdots + a_{p^m} p^{-ms} + \cdots). \tag{3.12}$$

If this product is expanded without regard to convergence, the result is the Dirichlet series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$, where $a_1 = 1$ and a_n is given by

$$a_n = a_{p_1}^{r_1} \cdots a_{p_k}^{r_k} \qquad \text{if } n = p_1^{r_1} \cdots p_k^{r_k}. \tag{3.13}$$

Suppose, that the Dirichlet series is in fact absolutely convergent in some right half plane. Then every rearrangement is absolutely convergent to the same sum and the same conclusion is valid for subseries: If E is a finite set of primes and $N(E)$ is defined as the set of positive integers requiring only members of E for their factorisation, we have

$$\prod_{p \in E} (1 + a_p p^{-s} + \cdots + a_p^m p^{-ms} + \cdots) = \sum_{n \in N(E)} \frac{a_n}{n^s}.$$

Consequently the infinite product has a limit in the half plane of absolute convergence of the Dirichlet series and the limiting product (3.12) equals the sum of the series. The sum of the series is 0 only if one of the factors on the left side is 0. In particular, the sum of the series cannot be identically 0, by the last statement of proposition 3.4.2. Thus, (3.12) can equal only this one Dirichlet series.

Conversely if an absolutely convergent Dirichlet series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ has the property, that its coefficients are *multiplicative*, i.e.

$$a_1 = 1 \quad \text{and} \quad a_{mn} = a_m a_n \quad \text{whenever } m \text{ and } n \text{ are relatively prime,}$$

then we can form the product (3.12) and recover the given series by expanding (3.12) and using (3.13). In this case, we say, that the Dirichlet series has (3.12) as an *Euler product.* Many functions in elementary number theory give rise to multiplicative sequences, an example is $a_n = \varphi(n)$, where φ is the Euler φ-function.

If the coefficients are *strictly multiplicative*, i.e.

$$a_1 = 1 \quad \text{and} \quad a_{mn} = a_m a_n \quad \text{for all } m \text{ and } n,$$

then the p-th factor of (3.12) simplifies to

$$1 + a_p p^{-s} + \cdots + (a_p p^{-s})^m + \cdots = \frac{1}{1 - \frac{a_p}{p^s}}. \tag{3.14}$$

In this case, our Dirichlet series has a *first degree Euler product*:

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - \frac{a_p}{p^s}}. \tag{3.15}$$

Conversely, an Euler product of the form (3.15) forces the coefficients of the Dirichlet series to be strictly multiplicative.

A Dirichlet series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ with $|a_n| \leq n^c$ for some real c is absolutely convergent for $\Re(s) > c + 1$. This fact leads us to a convergence criterion for first degree Euler products:

Proposition 3.4.4. *A first degree Euler product* $\prod\limits_{p\ prime} \frac{1}{1-\frac{a_p}{p^s}}$ *with* $|a_p| \leq p^c$ *for some real* c *and all primes* c *defines an absolutely convergent Dirichlet series (and hence a valid identity (3.15)) for* $\Re(s) > c+1$.

Proof. The coefficients a_n are strictly multiplicative and thus $|a_n| \leq n^c$ for all n. The absolute convergence follows. □

For application with elliptic curves, we also need other kinds of Euler products: To isolate the notion of degree of an Euler product, let us write (3.14) as a formal identity

$$1 + a_p X + \cdots + a_p^m X^m + \cdots = \frac{1}{1 - a_p X}.$$

Here, the denominator on the right is a polynomial of degree ≤ 1 with constant term 1 and it is in the sense, that the Euler product (3.15) has degree 1. The expansion (3.12) is called a *k-th degree Euler product*, if for each prime p, there is a polynomial $P_p(X) \in \mathbb{C}[X]$ having degree $\leq k$ and zero constant term, such that

$$1 + a_p X + \cdots + a_p^m X^m + \cdots = \frac{1}{1 - P_p(X)}$$

as a formal identity. Let us factor $1 - P_p(X)$ over $\mathbb{C}$ as

$$1 - P_p(X) = (1 - r_p^{(1)} X) \cdots (1 - r_p^{(k)} X).$$

We call the complex numbers $r_p^{(j)}$ the *reciprocal roots* of $1 - P_p(X)$.

Proposition 3.4.5. *A k-th degree Euler product* $\prod\limits_{p\ prime} \frac{1}{1-P_p(p^{-s})}$, *whose reciprocal roots satisfy* $|r_p^{(j)}| \leq p^c$ *for some real value* c *and all primes* p *defines an absolutely convergent Dirichlet series for* $\Re(s) > c+1$. *For such* s, *the sum of the Dirichlet series equals the Euler product.*

Proof. We apply proposition 3.4.4 to $\prod\limits_{p \text{ prime}} [1 - s_p^{(j)} p^{-s}]$ for each j. The product of absolutely convergent Dirichlet series can be rearranged without affecting the sum and the result is an absolutely convergent Dirichlet series. □

3.5 Zeta functions and L-functions

To define the L-function of an elliptic curve E over $\mathbb{Q}$, we assume, that E is given by a globally minimal Weierstrass equation. This condition is no loss of generality in view of theorem 3.3.6.

For each prime p, we consider the reduction E_p of E modulo p. We have seen, that E_p is defined over $\mathbb{Z}_p$ and is singular, if and only if $p \mid \Delta$. In both the singular and the nonsingular cases, we define

$$a_p := p + 1 - \#E_p(\mathbb{Z}_p), \tag{3.16}$$

where $E_p(\mathbb{Z}_p)$ is as usual the set of projective solutions, i.e. the points on the reduced curve.

Definition 3.5.1. The *local L-factor* for the prime p is the formal power series given by

$$L_p(u) = \begin{cases} \frac{1}{1-a_pu+pu^2} & \text{if } p \nmid \Delta \\ \frac{1}{1-a_pu} & \text{if } p \mid \Delta \end{cases} \tag{3.17}$$

The *L-function* of E is the product of the local L-factor with u replaced in the p-th factor by p^{-s}:

$$L(s,E) = \prod_{p|\Delta} \left[\frac{1}{1-a_pp^{-s}}\right] \prod_{p\nmid\Delta} \left[\frac{1}{1-a_pp^{-s}+p^{1-2s}}\right]. \tag{3.18}$$

An elementary convergence result for this Euler product is given in the next proposition. This result will be improved in the next section:

Proposition 3.5.2. *The following statements hold:*

1. *For every prime p,* $|a_p| \leq p$.
2. *For* $p \nmid \Delta$*, the reciprocal roots of* $1 - a_pu + pu^2$ *are* $\leq p$ *in absolute value.*
3. *The Euler product defining* $L(s,E)$ *converges for* $\Re(s) > 2$ *and is given there by an absolutely convergent Dirichlet series.*

Proof. The members of $E_p(\mathbb{Z}_p)$ include the infinite points $(0:1:0)$ and cannot consist of more than two other points for each x in $\mathbb{Z}_p$. Thus, $1 \leq \#E_p(\mathbb{Z}_p) \leq 2p+1$ and so $|a_p| \leq p$. This proves statement 1).

The reciprocal roots are $\frac{1}{2}(a_p \pm \sqrt{a_p^2 - 4p})$, which is $\leq |a_p|$ in absolute value. Thus, 1) implies 2).

Statement 3) is an immediate consequence of 2) and proposition 3.4.5. □

When $p|\Delta$, we can calculate a_p exactly. According to theorem 3.1.1, when there is a singularity, there is only one and it is classified as a cusp, a split case of a node od a nonsplit case of a node. Adding one for the singularity, we arrive (due to theorem 3.1.3) the following formula for a_p, when $p|\Delta$:

$$a_p = \begin{cases} 0 & \text{for the case of a cusp} \\ +1 & \text{for the split case of a node} \\ -1 & \text{for the nonsplit case of a node.} \end{cases} \tag{3.19}$$

An arithmetically defined L-function typically is part of a more naturally defined *zeta-function* or a variant of such a function. In the case at hand, the zeta-function $Z(u, E_p)$ is a generating function, that encodes, how many points are on the curve in each finite extension of $\mathbb{Z}_p$. If $\mathbb{F}_{p^n}$ denotes the field of p^n elements, the definition is

$$Z(u, E_p) := \exp\left(\sum_{n=1}^{\infty} \frac{\#E_p(\mathbb{F}_{p^n})u^n}{n}\right).$$

The definition is arranged so, that additive formulas for $\#E_p(\mathbb{F}_{p^n})$ make multiplicative contributes to $Z(u, E_p)$: Operationally one calculates with the formula

$$u\frac{d}{du}\log Z(u, E_p) = \sum_{n=1}^{\infty} \#E_p(\mathbb{F}_{p^n})u^n.$$

For our elliptic curve, calculation of $Z(u, E_p)$ leads to a combination of three polynomials, two appearing in the denominator and one in the numerator:

$$Z(u, E_p) = \begin{cases} \frac{1-a_pu+pu^2}{(1-u)(1-pu)} & \text{if } p \nmid \Delta \\ \frac{1-a_pu}{(1-u)(1-pu)} & \text{if } p \mid \Delta. \end{cases}$$

Substituting $u = p^{-s}$ and taking product of the factors $Z(p^{-s}, E_p)$ over all primes p yields

$$\prod_{p \text{ prime}} (u, E_p) = \prod_{p\nmid\Delta} \frac{1 - a_pp^{-s} + p^{1-2s}}{(1-p^{-s})(1-p^{1-s})} \prod_{p|\Delta} \frac{1 - a_pp^{-s}}{(1-p^{-s})(1-p^{1-s})}.$$

The factors $\prod \frac{1}{1-p^{-s}}$ and $\prod \frac{1}{1-p^{1-s}}$ are just the Euler products of the Riemann zeta-function $\zeta(s)$ resp. $\zeta(s-1)$ and give no useful information about E. The remaining polynomial is just $L(s, E)^{-1}$, which encodes a great deal of information.

So $L(s, E)$ is basically the product over the zeta-functions with $u = p^{-s}$ for all primes p.

3.6 Hasse's theorem

The goal of this section is to establish the following improvement of proposition 3.5.2. It is proven by H. Hasse in 1933, see [HH].

Theorem 3.6.1 (Hasse)**.** *Let E be an elliptic curve over $\mathbb{Q}$ with integer coefficients. For each prime $p \nmid \Delta$, let E_p be the reduction modulo p. Then*

$$|p + 1 - \#E_p(\mathbb{Z}_p)| < 2\sqrt{p}. \tag{3.20}$$

Proof. The full proof of this theorem is quite laborious. We will just give a short sketch of a proof, that is due to Yuri Manin, [YM]:

First, we discard of the cases $p = 2$ and $p = 3$. For these values of p, we have $p < 2\sqrt{p}$. In these cases, (3.20) therefore follows from the first statement of proposition 3.5.2.

For $p > 3$, we can make an admissible change of variables, that does not affect the condition $p \nmid \Delta$, does not change $\#E_p(\mathbb{Z}_p)$ and brings the equation of E into the form

$$y^2 = x^3 + ax + b. \tag{3.21}$$

We may therefore assume, from the outset, that E is given by (3.21).

We shall work with the nonsingular cubic

$$Y^2 = \frac{X^3 + aX + b}{x^3 + ax + b} \tag{3.22}$$

defined over the field $\mathbb{Z}_p(x)$ of rational functions with coefficients in $\mathbb{Z}_p$.

Two solutions are

$$(X, Y) = (x, 1) \quad \text{and} \quad (X, Y) = (x^p, (x^3 + ax + b)^{\frac{1}{2}(p-1)}).$$

From the group law, we know, that the projective solutions of (3.22) over $\mathbb{Z}_p(x)$ form a group with identity ∞.

We form the group element

$$T_n := (x^p, (x^3 + ax + b)^{\frac{1}{2}(p-1)}) + n(x, 1) \tag{3.23}$$

for each integer n with $-\infty < n < \infty$. We define a corresponding sequence of integers $d_n \geq 0$ as follows: If $T_n = \infty$, then $d_n := 0$. Otherwise, T_n is of the form (X_n, Y_n); in this case, we reduce X_n to lowest terms in $\mathbb{Z}_p(x)$ and we let d_n be the larger of the degree of the numerator and the degree of the denominator of X_n.

Now, one can proof the following two statements:

$$d_{-1} - d_0 - 1 = \#E_p(\mathbb{Z}_p) - p - 1. \tag{3.24}$$

and

$$d_{n-1} + d_{n+1} = 2d_n + 2 \quad \text{for } -\infty < n < \infty. \tag{3.25}$$

Given these equations, it is not difficult anymore to prove the theorem: By induction forwards and backwards from the basis $n = 0$ and $n = -1$, we obtain from (3.25) the formula

$$d_n = n^2 - (d_{-1} - d_0 - 1)n + d_0. \tag{3.26}$$

Substitution from (3.24) and use of $d_0 = p$ gives

$$d_n = n^2 + a_p n + p,$$

where $a_p = p+1-\#E_p(\mathbb{Z}_p)$ as in (3.16). The d_n's are degrees of polynomials and therefore ≥ 0. Moreover, two consecutive d_n's cannot both be 0. Since a_p is an integer, it follows, that $r^2+a_pr+p \geq 0$ for all real r. The discriminant of this polynomial then must be ≤ 0 and thus $|a_p| \leq 2\sqrt{p}$. This completes the proof of theorem 3.6.1.

□

Corollary 3.6.2. *The Euler product defining $L(s, E)$ converges for $\Re(s) > \frac{3}{2}$ and is given there by an absolutely convergent Dirichlet series.*

Proof. Let $p \nmid \Delta$. If $a_p = p+1-\#E_p(\mathbb{Z}_p)$, the reciprocal roots r of $1-a_pu+pu^2$ are $r = \frac{1}{2}(a_p \pm \sqrt{a_p^2 - 4p})$. By theorem 3.6.1, the square root in this expression is imaginary. Hence, due to Pythagoras, $|r|^2 = \frac{1}{4}(a_p^2+(4p-a_p^2)) = p$ and $|r| = \sqrt{p}$. The corollary therefore follows from proposition 3.4.5 with $c := 1/2$. □

3.7 The conjecture of Birch and Swinnerton-Dyer

Helmut Hasse also conjectured, that $L(s, E)$ could be extended by analytic continuation to the whole complex plane. This conjecture was first proved by Max Deuring for elliptic curves with complex multiplication. It was subsequently shown to be true for all elliptic curves, as a consequence of the Taniyama-Shimura theorem, also known as the *modularity theorem*:

In mathematics the modularity theorem states, that elliptic curves over $\mathbb{Q}$ are related to modular forms. A modular form is a holomorphic function on the upper half-plane satisfying a certain kind of functional equation and growth condition. We do not give a more detailed definition about modular forms here. A more detailed approach to this topic can be found in [KK].

Yutaka Taniyama stated a preliminary (slightly incorrect) version of the conjecture at the 1955 international symposium on algebraic number theory in Tokyo and Nikko. G. Shimura and Y. Taniyama worked on improving its rigor until 1957, see [TS]. Weil rediscovered the conjecture in 1957, and showed in [AWe3] that it would follow from the (conjectured) functional equations for some twisted L-series of the elliptic curve; this was the first serious evidence that the conjecture might be true.

The conjecture attracted considerable interest when G. Frey (1986) suggested in [GF], that the Taniyama-Shimura-Weil conjecture implies Fermat's Last Theorem. He did this by attempting to show that any counterexample to Fermat's Last Theorem would give rise to a non-modular elliptic curve. However, his argument was not complete. The extra condition which was needed to link Taniyama-Shimura-Weil to Fermat's Last Theorem was identified by J. Serre in 1987 ([JS]) and became known as the *epsilon conjecture.* In [KR], K. Ribet (1990) proved the epsilon conjecture, thereby proving that the Taniyama-Shimura-Weil conjecture implied Fermat's Last Theorem. A. Wiles (1995), with some help from Richard Taylor, proved the Taniyama-Shimura-Weil conjecture for all semistable elliptic curves, which was strong enough to yield a proof of Fermat's Last Theorem, see [AW2].

The full Taniyama-Shimura-Weil conjecture was finally proved by F. Diamond (1996), R. Taylor (1999), and C. Breuil (2001) who, building on Wiles' work, incrementally chipped away at the remaining cases until the full result was proved in 2001. (Compare the references in [FD], [CDT] and [BCDT]. The now fully proved conjecture became known as the modularity theorem.

Now let us give a more precise idea of this analytic continuation of $L(s, E)$: By adding a few more analytic factors to the L-function, we obtain a function $\Lambda(s, E)$, that satisfies a remarkably simple function equation. Let

$$\Gamma(z) := \int_0^\infty t^{z-1} e^{-t} \, dt$$

be the Γ-function, which meets $\Gamma(n) = (n-1)!$ for all integers n. Then, Γ is a meromorphic function on $\mathbb{C}$ with poles at the non-positive integers.

Theorem 3.7.1. *There is a unique positive integer $N = N_E$ and a sign $\epsilon = \epsilon_E \in \{\pm 1\}$, such that the function*

$$\Lambda(s, E) := N^{\frac{s}{2}} \cdot (2\pi)^{-s} \cdot \Gamma(s) \cdot L(s, E)$$

extends to a complex analytic function on all $\mathbb{C}$, that satisfies the functional equation

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

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

Proof. We do not give a proof of this theorem here. The basic idea is the following: One can prove, that the L-series of a modular form analytically continues and satisfies the given functional equation. Since the Taniyama-Shimura theorem states, that an elliptic curve defined over $\mathbb{Q}$ is modular, this already implies our statement. A full proof to this theorem can be found in [NK]. □

The integer $N = N_E$ is called the *conductor* of E and $\epsilon = \epsilon_E$ is called the *sign* in the functional equation for E or the *root number* of E. One can prove, that the primes that divide N are the same as the primes, that divide the discriminant Δ.

Definition 3.7.2. Since $L(s, E)$ can be analytically continued to a holomorphic function on all $\mathbb{C}$, this implies, that $L(s, E)$ has a power series expansion about the point $s = 1$:

$$L(s, E) = c_0 + c_1(s - 1) + c_2(s - 1)^2 + \cdots$$

Define the *analytic rank* r_{an} of E to be the order of vanishing of $L(s, E)$ at $s = 1$, i.e.

$$L(s, E) = c_{r_{an}}(s - 1)^{r_{an}} + \cdots .$$

This completely analytic definition of a rank is very different from the purely algebraic kind of rank, that we defined in corollary 2.6.12. Nevertheless, there is a very weighty conjecture, that claims, that these two ranks are actually the same:

Conjecture 3.7.3 (Birch, Swinnerton-Dyer)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then the algebraic and analytic ranks of E are the same.*

This problem is extremely difficult. The conjecture was made in the 1960s, and hundreds of people have thought about it for over 4 decades. Its status as one of the most challenging mathematical questions has become widely recognised. It is one of the Clay Mathematics Institute's seven Millennium Prize Problems, see [KD].

I will describe some historical backgrounds about the Birch-Swinnerton-Dyer conjecture. Around 1960, Bryan Birch and Peter Swinnerton-Dyer formulated a conjecture which determines the algebraic rank r of an elliptic curve E over $\mathbb{Q}$. The idea is that an elliptic curve with a large value of r has a large number of rational points and should therefore have a relatively large number of solutions modulo a prime p on the average as p varies. For a prime p, we let $N(p)$ be the number of pairs of integers (x, y) on the elliptic curve E reduced modulo p.

Then the Birch-Swinnerton-Dyer conjecture in its crudest form said, that we should have an asymptotic formula

$$\prod_{p<x} \frac{N(p) + 1}{p} \sim C \cdot (\log x)^r \quad \text{as } x \to \infty$$

for some constant $C > 0$. This in turn led them to make a general conjecture about the behaviour of a curve's L-function $L(s, E)$ at $s = 1$, namely 3.7.3. This was a far-sighted conjecture for that time, because the analytic continuation of $L(s, E)$ there was only established for curves with complex multiplication, which were also the main source of numerical examples. But since the Taniyama-Shimura-conjecture is proven, we know, that there exists an analytic continuation of $L(s, E)$ on $\mathbb{C}$ and so a power series expansion at the point $s = 1$ for all elliptic curves E. The original work of Birch and Swinnerton-Dyer can be found in [BS].

The Birch and Swinnerton-Dyer conjecture has been proved only in special cases:

- From the modularity theorem, one can infer, that it is possible to generalize elliptic curves over $\mathbb{Q}$ to an elliptic curve over an arbitrary algebraic number field (an *algebraic number field* is a finite and hence algebraic field extension of the field of rational numbers). Since there is not always a unique factorization of numbers in a product of prime numbers. The failure of unique factorization is measured by the *class number.*

  In 1976, John Coates and Andrew Wiles proved in [CW] that if E is a curve with complex multiplication and $L(1, E)$ is not 0, then E has only a finite number of rational points, in the case of class number 1. This was extended to all imaginary quadratic fields by Nicole Arthaud.

- In 1983, Benedict Gross and Don Zagier showed in [GZ], that if a modular elliptic curve has a first-order zero at $s = 1$, then it has a rational point of infinite order. This is known as the *Gross-Zagier theorem.*

- In 1990, Victor Kolyvagin showed in [VK] that a modular elliptic curve E for which $L(1, E)$ is not zero has rank 0, and a modular elliptic curve E for which $L(1, E)$ has a first-order zero at $s = 1$ has rank 1.

- Since 1999, the Taniyama-Shimura is proven, which extends the previous results about modular elliptic curves to all elliptic curves over the rationals.

However, nothing has been proved for curves with rank greater than 1, although there is extensive numerical evidence for the truth of the conjecture.

An important consequence of the Birch-Swinnerton-Dyer conjecture is the following proposition:

Proposition 3.7.4. *Let E be an elliptic curve over $\mathbb{Q}$. If Conjecture 3.7.3 is true, then there is an algorithm to compute the rank of E.*

Proof. We will only give a basic idea of this proof:

By naively searching for points in $E(\mathbb{Q})$, we obtain a lower bound on r, which is closer and closer to the true rank r, the longer we run the search. At some point this lower bound will equal r, but without using further information we do not know when that will occur.

On the other hand, we can for any k compute $L^{(k)}(1, E)$ to any desired precision. Such computations yield upper bounds on r_{an}. In particular, if we compute $L^{(k)}(1, E)$ and it is nonzero (to the precision of our computation), then $r_{an} \leq k$. Eventually this method will also converge to give an upper bound on r_{an}, though again without further information we do not know when our computed upper bound on r_{an} equals to the true value of r_{an}.

Since we are assuming that Conjecture 3.7.3 is true, we know that $r = r_{an}$, hence at some point the lower bound on r computed using point searches will equal the upper bound on r_{an} computed using the L-series. At this point, by Conjecture 3.7.3, we know the true value of r. □

Remark 3.7.5. Let E be an elliptic curve over $\mathbb{Q}$. It can even be shown, that given the rank r, then there is an algorithm to compute $E(\mathbb{Q})$. A proof of this statement can be found in [WS].

Another consequence of the Birch-Swinnerton-Dyer conjecture lies in pure number theory:

Definition 3.7.6. In mathematics, a *congruent number* is a positive integer that is the area of a right triangle with three rational number sides.

Example 3.7.7. The sequence of integer congruent numbers starts with

$$5, 6, 7, 13, 14, 15, 20, 21, 22, 23, 24, 28, 29, 30, 31, 34, 37, 38, 39, 41, 45, 46, \ldots$$

For example, 5 is a congruent number because it is the area of a $20/3, 3/2, 41/6$ triangle. Similarly, 6 is a congruent number because it is the area of a $3, 4, 5$ triangle. 3 is not a congruent number.

The question of determining whether a given rational number is a congruent number is called the congruent number problem. This problem has still not been brought to a successful resolution.

Tunnell's theorem (see 3.7.8 below) provides an easily testable criterion for determining whether a number is congruent; but his result relies on the Birch and Swinnerton-Dyer conjecture, which we know, is still unproven.

Theorem 3.7.8 (Tunnell). *For a given square-free integer n, define*

$$\begin{aligned} A_n &= \#\{x, y, z \in \mathbb{Z} : n = 2x^2 + y^2 + 32z^2\} \\ B_n &= \#\{x, y, z \in \mathbb{Z} : n = 2x^2 + y^2 + 8z^2\} \\ C_n &= \#\{x, y, z \in \mathbb{Z} : n = 8x^2 + 2y^2 + 64z^2\} \\ D_n &= \#\{x, y, z \in \mathbb{Z} : n = 8x^2 + 2y^2 + 16z^2\}. \end{aligned}$$

Tunnell's theorem states that supposing n is a congruent number, if n is odd then $2A_n = B_n$ and if n is even then $2C_n = D_n$.

Conversely, if the Birch and Swinnerton-Dyer conjecture holds true for elliptic curves of the form $y^2 = x^3 - n^2x$, these equalities are sufficient to conclude that n is a congruent number.

Index

L-function, 76
p-adic norm, 65
p-integral value, 65
p-reduced point, 66

absolute invariant, 28
affine planar curve, 38
analytic rank, 81

conductor, 80
congruent number, 83
conic, 38
conjugation-invariant lattice, 26
cubic, 38
cusp, 63

Dirichlet series, 72
discrete set, 7
discriminant, 27, 43

Eisenstein series, 18
elliptic curve, 41
elliptic function, 13

fundamental parallelotope, 10

height function, 59
homogeneous polynomial, 37

inflection points, 40
intersection multiplicity, 38
isomorphic elliptic curves, 41

lattice, 7
line, 37

meromorphic function, 11
modularity theorem, 79
multiplicativity, 74

node, 63

pole, 11
projecive plane, 37
projective planar curve, 37

rank, 61
reciprocal root, 75
reduction modulo p, 65
residuum, 14

singular curve, 40
singular point, 40
smooth curve, 40

tangent line, 40
torsion subgroup, 61

ultrametric inequality, 65
unimodular matrix, 9

Weierstrass $\wp$-function, 17
Weierstrass form, 41
Weierstrass-invariants, 23

Bibliography

[AK] Anthony W. Knapp: Elliptic Curves

[AW1] Andrew J. Wiles: The Birch and Swinnerton-Dyer Conjecture

[AW2] Andrew J. Wiles: Modular Elliptic Curves and Fermat's last Theorem

[AWe1] André Weil: Variétés abéliennes et courbes algébriques

[AWe2] André Weil: Courbes algébriques et variétés abéliennes. Sur les courbes algériques et les varietés qui s'en deduisent

[AWe3] André Weil: Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen

[BB] Bryan J. Birch: Elliptic Curves over $\mathbb{Q}$: A progress report

[BCDT] C. Breuil & B. Conrad & F. Diamond & R. Taylor: On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises

[BS] Bryan Birch & Peter Swinnerton-Dyer: Notes on Elliptic Curves (II)

[CDT] B. Conrad & F. Diamond & R. Taylor: Modularity of certain potentially Barsotti-Tate Galois representations

[CW] John Coates & Andrew J. Wiles: On the conjecture of Birch and Swinnerton-Dyer

[FD] Fred Diamond: On deformation rings and Hecke rings

[GF] Gerhard Frey: Links between stable elliptic curves and certain Diophantine equations

[GZ] Benedict Gross & Don Zagier: Heegner points and derivatives of L-series

[HH] Helmut Hasse: Zur Theorie der abstrakten elliptischen Funktionenkörper I, II, III

[JA] Jeff Achter: On Computing the Rank of Elliptic Curves

[JS] Jean-Pierre Serre: Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)

[JT] Jerrold B. Tunnell: A Classical Diophantine Problem and Modular Forms of Weight 3/2

[KD] Keith J. Devlin: The Millennium Problems: The Seven Greatest Unsolved Mathematical Puzzles of Our Time

[KK] Max Koecher & Aloys Krieg: Elliptische Funktionen und Modulformen

[KR] Kenneth A. Ribet: On modular representations of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) arising from modular forms

[LM] Louis Mordell: On the rational solutions of the indeterminate equations of the third and fourth degrees

[NK] Neal Koblitz: Introduction to Elliptic Curves and Modular Forms

[PG] Peter M. Gruber: Geometry of numbers

[ST] J. Silverman & J. Tate: Rational Points on Elliptic Curves

[TS] Y. Taniyama & G. Shimura: Complex Multiplication of Abelian Varieties

[TW] Richard Taylor & Andrew Wiles: Ring Theoretic Properties of Certain Hecke Algebras

[VK] Victor Kolyvagin: On the Mordell-Weil and Shafarevich-Tate groups for elliptic Weil curves

[WS] William A. Stein: The Birch and Swinnerton-Dyer Conjecture, a Computational Approach

[YM] Yuri I. Manin: On cubic congruences to a prime modulus