1
Elliptic functions

In complex multiplication the abelian extensions of an imaginary quadratic number field are generated by the coefficients of suitable elliptic curves together with the coordinates of torsion points in terms of values of elliptic functions and modular functions, as explained in Chapter 6. Moreover, using elliptic functions, we will study rings of integers and unit groups, and we will find explicit constructions for them later in Chapters 7 and 8. Therefore, besides the parametrisation of elliptic curves by the Weierstrass $\wp$ function and its derivative, we need to study more closely the σ function and the η function that are involved in, for example, the calculations of discriminants in Chapter 7. The resolvent formula of section 1.7 and the p-adic limits will be needed for the Galois module structure of Chapter 8. For the same reason we will study Weierstrass equations that will also be used in the applications to cryptography in Chapter 10. The division polynomials in section 1.5 will be crucial for the proof of Berwick's congruences in Chapter 9.

1.1 Values of elliptic functions

In the complex plane we fix a lattice, i.e. a free abelian group of rank 2,

$$\mathfrak{L} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2,$$

generated by two over $\mathbb{R}$ linearly independent numbers ω_1, ω_2. Any two such numbers are called a basis of $\mathfrak{L}$, and we write

$$\mathfrak{L} = [\omega_1, \omega_2].$$

A function $f : \mathbb{C} \to \mathbb{C} \cup \{\infty\}$ is called **elliptic** with respect to $\mathfrak{L}$ if f is meromorphic and if the points of $\mathfrak{L}$ are periods of f:

$$f(z + \omega) = f(z) \text{ for all } \omega \in \mathfrak{L}.$$

For a fixed number $\gamma \in \mathbb{C}$ and a basis ω_1, ω_2 of $\mathfrak{L}$ the set

$$F = F_\gamma = \{\gamma + x_1\omega_1 + x_2\omega_2 \mid 0 \le x_j < 1\}$$

is a systems of repesentatives of $\mathbb{C}/\mathfrak{L}$ and is called a **fundamental parallelogram** for $\mathfrak{L}$. It is therefore sufficient to study the values of an elliptic function on a fundamental parallelogram.

Theorem 1.1.1 *Let f be a non-constant elliptic function without poles on the boundary of F. Then the sum of its residues in F is equal to zero:*

$$\sum_{z\in F} Res(f,z) = 0.$$

Proof By periodicity of f we have the equalities

$$\int_\gamma^{\gamma+\omega_j} f(z)dz = \int_{\gamma+\omega}^{\gamma+\omega_j+\omega} f(z)dz = -\int_{\gamma+\omega_j+\omega}^{\gamma+\omega} f(z)dz$$

for every $\omega \in \mathfrak{L}$. So in the integral of f along the boundary of F_γ the integrals along opposite edges cancel out. The assertion of Theorem 1.1.1 now follows from the theorem of residues. □

Applying Theorem 1.1.1 to $\frac{f}{f-w}$, $w \in \mathbb{C}$, for an elliptic function f, the argument principle tells us:

Theorem 1.1.2 *Let f be a non-constant elliptic function. Then for every $w \in \mathbb{C} \cup \{\infty\}$ the number of solutions $a \in F$ of the equation $f(a) = w$, counted according to multiplicity, is equal to the number of poles of f in F. This number is called the order of f.*

Let f be a non-constant elliptic function. Then for $a \in \mathbb{C}$ we define the **order** of f at a to be the unique number $m \in \mathbb{Z}$ such that $g_a(z) := \frac{f(z)}{(z-a)^m}$ is holomorphic in a and $g_a(a) \neq 0$.

Theorem 1.1.3 *Let a_j be the points in F, where the non-constant elliptic function f has non-vanishing order m_j. Then*

$$\sum_j m_j = 0 \qquad \text{and} \qquad \sum_j m_j a_j \in \mathfrak{L}.$$

Proof The first assertion is a special case of Theorem 1.1.2. We prove the second assertion. Since there are only finitely many zeros and poles

in F, we can shift F such that all poles and zeros of f are in the interior of F and not on the boundary. According to the residue theorem we then have

$$2\pi i \sum_j m_j a_j = \int_{\partial F} z \frac{f'(z)}{f(z)} dz.$$

Now, combining, as in the proof of Theorem 1.1.1, the integrals along opposite edges, we obtain on the right-hand side an expression of the form

$$\int_{\gamma}^{\gamma+\omega_1} z\frac{f'(z)}{f(z)}dz - \int_{\gamma+\omega_2}^{\gamma+\omega_1+\omega_2} z\frac{f'(z)}{f(z)}dz = \int_{\gamma}^{\gamma+\omega_1} \omega_2 \frac{f'(z)}{f(z)}dz$$
$$= \omega_2 \int_{f(\overline{\gamma,\gamma+\omega_1})} \frac{du}{u} = \omega_2 2\pi i k, \quad k \in \mathbb{Z},$$

where $\overline{\gamma,\gamma+\omega_1}$ denotes the path from γ to $\gamma+\omega_1$. This makes the assertion clear. □

From the second assertion of Theorem 1.1.3 we further obtain

Theorem 1.1.4 *An elliptic function with at most one pole of order 1 in F is constant.*

1.2 The functions $\sigma(z|\mathfrak{L})$, $\zeta(z|\mathfrak{L})$ and $\wp(z|\mathfrak{L})$

We start by constructing the most important functions used in the sequel. They can all be derived from the **Weierstrass σ function** of a lattice $\mathfrak{L}$:

$$\sigma(z) = z \prod_{\omega\in\mathfrak{L}\setminus\{0\}} (1-\tfrac{z}{\omega})e^{\frac{z}{\omega}+\frac{1}{2}\frac{z^2}{\omega^2}}.$$

Absolute convergence and holomorphy of the defining product for $\sigma(z)$ follow from:

Lemma 1.2.1 *For $k \geq 3$ the series $\sum_{\omega\in\mathfrak{L}\setminus\{0\}} \frac{1}{\omega^k}$ is absolutely convergent.*

Proof Observing that for $n \in \mathbb{N}$ there are $8n$ lattice points in

$$\mathfrak{L}_n = \{x_1\omega_1+x_2\omega_2 \mid (x_1,x_2) \in [-n,n]\times\{\pm n\}\cup\{\pm n\}\times[-n,n]\}, \quad n \in \mathbb{N},$$

we obtain

$$\sum_{n=1}^{N}\sum_{\omega\in\mathfrak{L}_n}\frac{1}{|\omega|^k}\le\frac{8}{\delta^k}\sum_{n=1}^{N}\frac{1}{n^{k-1}}\text{ with }\delta=\min\{|\omega|\mid\omega\in\mathfrak{L}_1\},$$

which implies the assertion of Lemma 1.2.1. □

All elliptic functions can be derived from σ though σ itself is not elliptic. Taking a logarithmic derivative we first obtain the **elliptic zeta function**

$$\zeta(z)=\frac{d}{dz}\log(\sigma(z))=\frac{\sigma'(z)}{\sigma(z)}=\frac{1}{z}+\sum_{\omega\in\mathfrak{L}\setminus\{0\}}\left[\frac{1}{z-\omega}+\frac{1}{\omega}+\frac{z}{\omega^2}\right],$$

then, by differentiation we obtain the **Weierstrass $\wp$ function**

$$\wp(z)=-\zeta'(z)=\frac{1}{z^2}+\sum_{\omega\in\mathfrak{L}\setminus\{0\}}\left[\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right]\tag{1.1}$$

and its derivative

$$\wp'(z)=-2\sum_{\omega\in\mathfrak{L}}\frac{1}{(z-\omega)^3}.$$

$\wp'$ is meromorphic by definition and clearly elliptic because the series for $\wp'$ is absolutely convergent. Moreover we have:

Theorem 1.2.2 *$\wp$ is an elliptic function.*

Proof $\wp'$ being elliptic implies that $\wp(z+\omega_j)=\wp(z)+c_j$ with a constant c_j. Setting $z=-\frac{\omega_j}{2}$ and, keeping in mind that $\wp$ is an even function without a pole at $-\frac{\omega_j}{2}$, we find that $c_j=0$. Therefore, $\wp$ is elliptic. □

On the other hand σ and ζ are not elliptic, as can be seen by the following theorem in combination with Theorem 1.2.5. By integration we obtain from Theorem 1.2.2 the transformation formulae:

Theorem 1.2.3 *For $\omega\in\mathfrak{L}$ we have*

$$\zeta(z+\omega)=\zeta(z)+\eta(\omega),$$
$$\sigma(z+\omega)=\psi(\omega)e^{\eta(\omega)(z+\frac{\omega}{2})}\sigma(z)$$

with a constant $\eta(\omega)$, the so-called quasi-period, and the factor

$$\psi(\omega)=\begin{cases}1\text{ for }\omega\in2\mathfrak{L},\\-1\text{ for }\omega\in\mathfrak{L}\setminus2\mathfrak{L}.\end{cases}$$

Clearly, the map $\eta : \mathfrak{L} \to \mathbb{C}$, defined by the transformation formula of the zeta function, is an additive homomorphism. Further, by the unique representation

$$z = z_1\omega_1 + z_2\omega_2, \quad z_j \in \mathbb{R},$$

for $z \in \mathbb{C}$ we can extend η to $\mathbb{C}$ by

$$\eta(z) := z_1\eta_1 + z_2\eta_2$$

with $\eta_j = \eta(\omega_j), j = 1, 2$. Now we define:

$$l(u, w) := u\eta(w) - \eta(u)w \qquad \text{for } u, w \in \mathbb{C}.$$

Further, to simplify notation, we set

$$z^* := \eta(z)$$

and

$$\zeta^*(z) := \zeta(z) - z^*,$$
$$\sigma^*(z) = e^{-\frac{zz^*}{2}}\sigma(z).$$

The transformation formulae of Theorem 1.2.3 can then be written as:

Theorem 1.2.4 *For $\tau \in \mathfrak{L}$ we have*

$$\zeta^*(z+\tau) = \zeta^*(z),$$

$$\sigma^*(z+\tau) = \psi(\tau)e^{\frac{1}{2}l(z,\tau)}\sigma^*(z).$$

Therefore, ζ^* is periodic with respect to $\mathfrak{L}$ but not elliptic. For a better understanding of the factor $e^{\frac{1}{2}l(z,\tau)}$ in the transformation formula of σ^* we need:

Theorem 1.2.5 (Legendre Relation) *Let ω_1, ω_2 be a basis of the lattice $\mathfrak{L}$ with $\Im(\frac{\omega_1}{\omega_2}) > 0$. Then the quasi-periods $\eta_j = \eta(\omega_j)$ of the zeta function satisfy*

$$\omega_1\eta_2 - \omega_2\eta_1 = 2\pi i.$$

Proof We assume 0 to be an interior point of F. Then, $\zeta(z)$ has exactly one pole of order 1 in F. So, by the theorem of residues

$$2\pi i = \int_{\partial F} \zeta(z)dz.$$

Using the transformation formula of the zeta function and adding up integrals along opposite edges as in the proof of Theorem 1.1.1, this becomes

$$-\int_{\gamma+\omega_1}^{\gamma} \eta_2 dz - \int_{\gamma}^{\gamma+\omega_2} \eta_1 dz = \omega_1\eta_2 - \omega_2\eta_1,$$

which proves Theorem 1.2.5. □

From Theorem 1.2.5 we now obtain:

Lemma 1.2.6 *For $u = u_1\omega_1 + u_2\omega_2$, $w = w_1\omega_1 + w_2\omega_2$ we have*

$$l(u,w) = 2\pi i(u_1w_2 - u_2w_1),$$

hence

$$e^{l(u,w)} = 1, \text{ for } u, w \in \mathfrak{L}.$$

Further, we have the rules

$$\begin{aligned} l(au,w) &= al(u,w), \text{ for } a \in \mathbb{R}, \\ l(au,w) &= l(u,\bar{a}w) \text{ for } a \in \mathbb{C}. \end{aligned}$$

Proof Let ω_1, ω_2 be a basis of $\mathfrak{L}$ with $\Im(\frac{\omega_1}{\omega_2}) > 0$. Then, by definition of l and Legendre's relation in Theorem 1.2.5

$$l(u,w) = 2\pi i(u_1w_2 - u_2w_1) = det\begin{pmatrix} u_1 & u_2 \\ w_1 & w_2 \end{pmatrix} 2\pi i,$$

with the real coordinates u_j, w_j in the representations $u = u_1\omega_1 + u_2\omega_2, w = w_1\omega_1 + w_2\omega_2$. The first two assertions now follow immediately. To prove the third, let A be the representing matrix of a with respect to the basis ω_1, ω_2,

$$a\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = A\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}.$$

Then, $det(A)A^{-1}$ is the matrix belonging to $\bar{a}$, and the coordinates of au and $\bar{a}w$ are given by

$$(u_1,u_2)A \quad \text{and} \quad (w_1,w_2)det(A)A^{-1}.$$

Hereafter, the third assertion of the lemma follows from the above representation of l as a determinant, observing that $N(a) = det(A)$. □

1.3 Construction of elliptic functions

A non-constant elliptic function f has only a finite number of points modulo $\mathfrak{L}$, where its order is different from 0 (zeros or poles). Let these points be:

$$a_1, \dots, a_s \text{ with orders } m_1, \dots, m_s.$$

Then, according to Theorem 1.1.3,

$$\sum_{j=1}^{s} m_j = 0 \text{ and } \sum_{j=1}^{s} m_j a_j \in \mathfrak{L}. \tag{1.2}$$

Conversely, for $a_j \in \mathbb{C}$ and $m_j \in \mathbb{Z}$ satisfying (1.2), an elliptic function is defined by

$$g(z) = \prod_{j=1}^{s} \left(e^{z a_j^*} \sigma(z - a_j) \right)^{m_j}, \tag{1.3}$$

having the same zeros and poles including orders as f. To see this, we use the transformation formula of the σ function for $\omega \in \mathfrak{L}$:

$$g(z+\omega) = \psi(\omega)^{\sum m_j} e^{\omega(\sum m_j a_j)^* - \omega^*(\sum m_i a_j)} g(z).$$

Herein the exponent of e is a multiple of $2\pi i$ due to Legendre's relation and the relation $\sum m_j a_j \in \mathfrak{L}$. Further, by asumption $\sum m_j = 0$. So we have $g(z+\omega) = g(z)$. Hence g is elliptic.

The function $\frac{f}{g}$ must be constant by Theorem 1.1.4, and we have proved the following theorem:

Theorem 1.3.1 (Abel–Jacobi) *Let $a_1, \dots, a_s \in \mathbb{C}$ and $m_1, \dots, m_s \in \mathbb{Z} \setminus \{0\}$. There exists an elliptic function f, such that the a_i are mod $\mathfrak{L}$ the only points, where the order of f is non-zero and equal to m_i iff condition (1.2) is satisfied. Every such function is, up to a constant factor, equal to the product in (1.3).*

As an example we consider the function $\wp(z) - \wp(a)$ for $a \in \mathbb{C} \setminus \mathfrak{L}$. Here we have $a_1 = a$, $a_2 = -a$, $a_3 = 0$; $m_1 = m_2 = 1$, $m_3 = -2$. Therefore, by Theorem 1.3.1

$$\wp(z) - \wp(a) = C \frac{\sigma(z-a)\sigma(z+a)}{\sigma(z)^2}$$

with a constant C. To determine C, we multiply both sides of the equation by $\sigma(z)^2$ and take the limit for $z \to 0$. This shows that $C = \frac{1}{\sigma(a)^2}$,

and the first assertion of the following theorem is proved. To prove the second assertion, we divide the first formula by $z-a$ and take the limit for $a \to z$.

Theorem 1.3.2

(i) $\wp(z) - \wp(a) = -\frac{\sigma(z-a)\sigma(z+a)}{\sigma(a)^2\sigma(z)^2}$ *for* $a \in \mathbb{C} \setminus \mathfrak{L}$.

(ii) $\wp'(z) = -\frac{\sigma(2z)}{\sigma(z)^4}$.

Clearly, the set of elliptic functions with respect to a lattice is a field under addition and multiplication. In the sequel it will be denoted by $\mathbb{C}_{\mathfrak{L}}$. Using the results of section 1.1, it follows:

Theorem 1.3.3 $\mathbb{C}_{\mathfrak{L}}$ *is generated over* $\mathbb{C}$ *by* $\wp$ *and* $\wp'$*:* $\mathbb{C}_{\mathfrak{L}} = \mathbb{C}(\wp, \wp')$.

Proof First, we show every even elliptic function to be a rational function of $\wp$. Therefore, we need:

Lemma 1.3.4 *Let* f *be an even function from* $\mathbb{C}_{\mathfrak{L}} \setminus \mathbb{C}$ *and* $a \in \mathbb{C}$ *with* $2a \in \mathfrak{L}$*. Then, the order of* f *at* a *is divisible by 2.*

Proof Writing down the Taylor expansion of f at a,

$$f(z) = c_m(z-a)^m + c_{m+1}(z-a)^{m+1} + \ldots, \quad c_m \neq 0,$$

we find

$$f(z) = f(-z+2a) = f(a+(a-z)) = (-1)^m c_m (z-a)^m + \ldots$$

Hence m must be even. □

Lemma 1.3.5 $\wp'(z)$ *is of order 3 and has three simple zeros at the half-periods*

$$w_1 = \frac{\omega_1}{2}, \; w_2 = \frac{\omega_1+\omega_2}{2}, \; w_3 = \frac{\omega_2}{2}.$$

For $a \in \mathbb{C} \setminus \mathfrak{L}$ *the function* $\wp(z) - \wp(a)$ *has a simple zero at each of the points* $\pm a$ *if* $2a \notin \mathfrak{L}$ *and a zero of order 2 at* a *if* $2a \in \mathfrak{L}$.

Proof $\wp'$ being an odd function, we can conclude, using the Taylor expansion as in the proof of Lemma 1.3.4, that the half-periods are zeros of $\wp'(z)$. Moreover, since $\wp'$ has order 3, these are modulo $\mathfrak{L}$ the

only zeros. The assertion of Lemma 1.3.5 about $\wp$ now follows because $\wp$ has order 2. □

Proof of Theorem 1.3.3. First, we let f be a non-constant *even* elliptic function with $a_1, .., a_s$ being modulo $\mathfrak{L}$ all points where f has an order $m_j \neq 0$. We set $m'_j = m_j$ resp. $m'_j = \frac{m_j}{2}$ if $2a_j \notin \mathfrak{L}$ resp. $2a_j \in \mathfrak{L}$. Then, by Lemma 1.3.5 the function

$$g(z) = f(z) \prod_{j=1}^{s} (\wp(z) - \wp(a_j))^{-m'_j}$$

can only have zeros or poles in $\mathfrak{L}$ and Theorem 1.1.3 tells us that g must be constant, so f is a rational function of $\wp$. □

Now, let f be an arbitrary elliptic function. We write f as the sum of an even and an odd function,

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

which is a linear combination of 1 and $\wp'$ with coefficients, that are even elliptic functions and thus rational functions in $\wp$. This proves the assertion of Theorem 1.3.3.

1.4 Algebraic and geometric properties of elliptic functions

The **Eisenstein series** of a lattice $\mathfrak{L}$,

$$G_m(\mathfrak{L}) := {\sum_{\omega \in \mathfrak{L}}}' \frac{1}{\omega^{2m}}, \quad m \geq 2,$$

are absolutely convergent by Lemma 1.2.1. We set

$$g_2 = g_2(\mathfrak{L}) = 60 G_2(\mathfrak{L}),$$
$$g_3 = g_3(\mathfrak{L}) = 140 G_3(\mathfrak{L}).$$

Theorem 1.4.1 *$\wp$ and $\wp'$ satisfy the algebraic equation*

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

The polynomial $4X^3 - g_2X - g_3$ has three pairwise different zeros

$$e_j = \wp(w_j), \quad j = 1, 2, 3,$$

with the half-periods w_j. Its discriminant is

$$\Delta(\mathfrak{L}) = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2.$$

For every lattice

$$\Delta(\mathfrak{L}) \neq 0,$$

and by known formulae, we find

$$\Delta(\mathfrak{L}) = g_2^3 - 27g_3^2.$$

For the proof we need:

Lemma 1.4.2 *In a neighbourhood of zero $\wp$ has the Laurent expansion*

$$\wp(z) = \frac{1}{z^2} + \sum_{m=1}^{\infty} (2m+1)G_{m+1}(\mathfrak{L})z^{2m}.$$

Proof In the series (1.1) of $\wp$ we write

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

Then, because of absolute convergence, we can interchange summation over ω with summation over n. Further, observing that $\sum_{\omega\in\mathfrak{L}}{}' \frac{1}{\omega^k} = 0$ for every odd $k \geq 3$, we obtain the Laurent expansion of our assertion. □

Proof of Theorem 1.4.1. Writing the function

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

in terms of the Laurent expansion of Lemma 1.4.2 we find that g has no poles and $g(0) = 0$. Therefore, by Theorem 1.1.2, $g = 0$, which proves the first assertion. To prove the remaining assertions, we observe that $\wp'(w_i) = 0$ according to Lemma 1.3.5 for every half-period w_i. The polynomial $4X^3 - g_2X - g_3$ therefore has the zeros $\wp(w_j), j = 1, 2, 3$. Moreover, these are pairwise different because $\wp'(w_j) = 0$ and thus $\wp$ has order 2 at w_j. This finishes the proof of Theorem 1.4.1. □

Theorem 1.4.1 gives rise to a bijection

$$z + \mathfrak{L} \mapsto Q(z) := \begin{cases} (1 : \wp(z) : \wp'(z)) \text{ if } z \notin \mathfrak{L}, \\ \left(\frac{1}{\wp'(z)} : \frac{\wp(z)}{\wp'(z)} : 1\right) \text{ if } \wp'(z) \neq 0 \end{cases} \tag{1.4}$$

between $\mathbb{C}/\mathfrak{L}$ and the projective curve

$$E := \{(t : x : y) \in \mathbb{P}^2(\mathbb{C}) \mid y^2t = 4x^3 - g_2xt^2 - g_3t^3\}.$$