version January 12, 1999

ELLIPTIC FUNCTIONS

P. Stevenhagen

Faculteit Wiskunde en Informatica
Universiteit van Amsterdam
1991–92

Contents

LITERATURE

[1] H. Weber, *Lehrbuch der Algebra, Band III: Elliptische Funktionen und algebraische Zahlen*, 2nd edition, Braunschweig, 1908; reprinted by Chelsea, New York.

The first systematic account of the theory of elliptic functions and the state of the art around the turn of the century. Preceding general class field theory and therefore incomplete. Contains a large number of actual calculations of class invariants.

[2] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions,* Iwanami Shoten and Princeton University Press, 1971

The standard modern reference. Includes the higher dimensional theory, due to Shimura, Taniyama and Weil.

[3] S. Lang, *Elliptic functions,* 2nd edition, Springer GTM 112, 1987

A basic reference for these notes. A modern approach, but less demanding than Shimura. Algebraic treatment of complex multiplication following Deuring. No proofs for the reduction theory of elliptic curves.

[4] M. Deuring, *Die Klassenkörper der komplexen Multiplikation,* Enzyklopädie der mathematischen Wissenschaften Band I2, Heft 10, Teil II, Teubner, 1958

Systematic account of the analytic theory in the spirit of Weber, Fueter and Hasse, proofs both with and without class field theory.

[5] Seminar on Complex Multiplication, Springer Lecture Notes in Mathematics 21, 1966

Notes of the 1957/58 IAS seminar at Princeton. The contributions by Serre, Borel and Iwasawa give a quick introduction to the analytic theory of complex multiplication.

[6] J. H. Silverman, *The Arithmetic of Elliptic Curves,* Springer GTM 106, 1986.

An algebraic approach to elliptic curves. Contains all the details on reduction left out by Lang, and much more—but hardly any complex multiplication.

[7] D.A. Cox, *Primes of the form $x^2 + ny^2$*, Wiley, 1989.

An approach to number theory based on a single problem, leading from quadratic forms and class groups via class field theory to complex multiplication. As down to earth as possible, careful explanations. Rather incomplete, but includes the class number one problem.

1. INTRODUCTION

In integral calculus, one considers various functions that are somewhat arbitrarily defined as inverses to standard functions like the sine and cosine and their hyperbolic analogues because they have the pleasant property of furnishing primitive functions for algebraic integrals like $\int \frac{dt}{\sqrt{1-t^2}}$ and $\int \frac{dt}{\sqrt{1+t^2}}$. These functions enlarge the class of integrals that can be computed explicitly, albeit in the form of inverses to transcendental functions. The kind of integral that arises when one allows the integrand to contain expressions of the form $\sqrt{f(t)}$, where $f(t)$ is a polynomial of degree 3 or 4, is called *elliptic*. Primitive functions for such integrals can be obtained in the form of inverses to so-called *elliptic functions*. In this section we describe this extension of integral calculus and show that the situation is very much similar to the more familiar case of the inverse trigonometric functions that occurs when f has degree 2. This similarity extends to number theoretic aspects of the functions under consideration and gives rise to the theory of *complex multiplication* that will be the main topic of these notes.

We consider integrals over the complex number field $\mathbf{C}$. In that case rational functions can be integrated explicitly because they have a partial fraction expansion as follows.

1.1. Lemma. *A basis of the field of rational functions $\mathbf{C}(t)$ over $\mathbf{C}$ is given by the set consisting of the monomials t^k with $k \in \mathbf{Z}_{\geq 0}$ and the fractions $(t-\alpha)^{-k}$ with $\alpha \in \mathbf{C}$ and $k \in \mathbf{Z}_{\geq 1}$.*

The basis elements can all easily be integrated, but already in this case there are the rational integrands $\frac{1}{t-\alpha}$ that give rise to transcendental functions $\log(t-\alpha)$.

We now pose ourselves the problem of evaluating integrals of the form $\int R(t, \sqrt{f(t)})dt$, where R is a rational function in two variables and $f \in \mathbf{C}[t]$ is a non-constant polynomial without double roots. More intrinsically, this means that we look at integrands that are algebraic of degree at most 2 over the rational functional field $\mathbf{C}(t)$. They can be written in the form $A + (B/\sqrt{f})$ with A and B in $\mathbf{C}(t)$, and as we already know how to integrate A we can further assume $A = 0$. By the lemma, the problem is then reduced to an evaluation of integrals

$$S_k(\alpha) = \int^x \frac{(t-\alpha)^k dt}{\sqrt{f(t)}} \qquad (\alpha \in \mathbf{C}, k \in \mathbf{Z}). \tag{1.2}$$

One actually needs only a small number of such integrals, see exercise 1.8.

If $\deg f = 1$ we are simply dealing with rational functions in $\sqrt{f}$, and we are back in the rational case by taking $\sqrt{f}$ as a new integration variable.

If $\deg f = 2$ a change of variables of the form $t \mapsto at + b$ shows that it suffices to consider the case $f = 1 - t^2$. As a characteristic example, we will study the behaviour of the map ϕ that is defined by

$$\phi(x) = \int_0^x \frac{dt}{\sqrt{1-t^2}}. \tag{1.3}$$

If we take x and the path of integration in the closed upper half plane $\bar{\mathcal{H}} = \{\mathrm{Im}(x) \geq 0\}$ and choose a branch of $\sqrt{1-t^2}$ on $\bar{\mathcal{H}}$ that is positive on the imaginary half-axis $i\mathbf{R}_{>0}$, then $\phi : \bar{\mathcal{H}} \to \mathbf{C}$ is a well-defined map. The real segment $[-1, 1]$ is mapped to $[-\pi/2, \pi/2]$. As the argument of $1 - t^2$ increases by $-\pi$ if t increases in the upper half plane from $1 - \epsilon$ to $1 + \epsilon$ for any small $\epsilon > 0$, the integrand increases by $\pi/2$ along this path and the half-line $[1, \infty)$ gets mapped to the vertical half-line $\{\pi/2 + iw : w > 0\}$. In the same way, $(-\infty, -1]$ is mapped to $\{-\pi/2 + iw : w > 0\}$, and it is now easy to see that ϕ maps the upper half plane $\mathcal{H}$ conformally onto the semi-infinite strip $\{z : -\pi/2 < \mathrm{Re}(z) < \pi/2 \text{ and } \mathrm{Im}(z) > 0\}$.

Two problems arise if we want to extend ϕ to the entire complex plane. First of all, the function $\sqrt{1-t^2}$ is two-valued on $\mathbf{C}$, so we have to make a branch cut in the plane, say along the real interval $[-1, 1]$, in order to have a single holomorphic branch. Secondly, the integral is path-dependent on $\mathbf{C}$, even if we make the suggested branch cut and avoid integration across this cut. More precisely, the integral is determined up to multiples of the value of the integral over a closed curve around the branch cut, i.e. up to multiples of

$$\oint_{|t|=R} \frac{dt}{\sqrt{1-t^2}} = 2\pi \qquad (R > 1).$$

There is a canonical solution to both problems. The ambiguity of the value of the integral is easily repaired if one takes this value not in $\mathbf{C}$ but in the factor group $\mathbf{C}/2\pi\mathbf{Z}$. Note that $\mathbf{C}/2\pi\mathbf{Z}$ is topologically a cylinder.

In order to avoid uniqueness problems with the function $\sqrt{1-t^2}$, one considers the integral not on $\mathbf{C}$, but on a surface C that is obtained by glueing together two copies of $\mathbf{C}$ along the branch cut $[-1, 1]$. Topologically, it is clear that such a surface is homeomorphic to a cylinder. It can be realized as a smooth complex curve C if one takes

$$C = \{(x, y) \in \mathbf{C}^2 : x^2 + y^2 = 1\} \subset \mathbf{C}^2,$$

i.e. the curve consisting of points of the form $(t, \pm\sqrt{1-t^2})$.

It is not hard to prove that ϕ induces a bijection $\phi : C \xrightarrow{\sim} \mathbf{C}/2\pi\mathbf{Z}$. This implies that we can use the *inverse* of ϕ to transport the group structure on $\mathbf{C}/2\pi\mathbf{Z}$ to C. In fact, it turns out that $\phi^{-1} : \mathbf{C}/2\pi\mathbf{Z} \to C$ rather than ϕ itself is the better map to look at. As in standard calculus, one derives that it is given by

$$\phi^{-1}(w) = (\sin w, \cos w),$$

and the well known addition formulae of the sine and cosine yield the following algebraic addition formula for points on C.

$$(x_1, y_1) \oplus (x_2, y_2) = (x_1y_2 + x_2y_1, x_1x_2 - y_1y_2) \tag{1.4}$$

Summarizing, we can say that the algebraic differential $\frac{dt}{\sqrt{1-t^2}}$ is defined most naturally on the complex curve C, and that integration of this differential establishes a bijection between C and the group $\mathbf{C}/2\pi\mathbf{Z}$. This bijection is actually a biholomorphic map furnishing an isomorphism of complex analytic manifolds, but we won't go into that at this point. The inverse function is of the form $(\Pi, \Pi') : \mathbf{C}/2\pi\mathbf{Z} \to C \subset \mathbf{C}^2$, where Π is a periodic function on $\mathbf{C}$ that satisfies an addition formula that is algebraic in terms of Π ad Π'.

We now turn to the case where the polynomial f in our integral $\int R(t)/\sqrt{f(t)}$ has degree 3 or 4. In this case, the integral is called *elliptic* as it is the kind of integral that arises when one tries to calculate arclengths on an ellipse. The case in which f has degree 4 is easily reduced to the case that $\deg(f) = 3$ by a Möbius transformation and is found in the exercises. We will take $\deg(f) = 3$, and in order to stress the analogy with 1.3 we will study the case $R(t) \equiv 1$ in detail. There are several ways to normalize f by an affine transformation $t \mapsto at + b$. If one maps two zeroes of f to 0 and 1, one obtains the *Legendre normal form* $dt/\sqrt{t(t-1)(t-\lambda)}$ of the differential, if one makes the sum of the zeroes of f equal to 0 and chooses the highest coefficient of f equal to 4 (for reasons that will become clear later on), one obtains the *Weierstrass normal form* $dt/\sqrt{4t^3 - g_2t - g_3}$ of the differential. We will use the first form in our example.

As in the quadratic case, we look at the function

$$\psi(x) = \int_{-\infty}^{x} \frac{dt}{\sqrt{t(t-1)(t-\lambda)}}. \tag{1.5}$$

Assume for simplicity that λ is real, say $0 < \lambda < 1$. Then we can use the same argument as we did for 1.3 and study the behaviour of ψ on the upper half plane first for a suitable branch of $\sqrt{t(t-1)(t-\lambda)}$. (This kind of transformation is known as a Schwarz-Christoffel transformation.) The image of the real axis is a union of four straight edges

$$(\psi(-\infty), \psi(0)] \cup [\psi(0), \psi(\lambda)] \cup [\psi(\lambda), \psi(1)] \cup [\psi(1), \psi(\infty))$$

intersecting at right angles. This time the integral is convergent for $|x| \to \infty$ in $\bar{\mathcal{H}}$, so we have $\psi(-\infty) = \psi(\infty) = 0$ and $\mathcal{H}$ is conformally mapped unto the interior of a rectangle having the origin and the ψ-values of 0, λ and 1 as edges. Just as in the previous case, we can extend ψ to a Riemann surface E that is obtained by glueing two copies of $\mathbf{C}$ along *two* branch cuts $[0, \lambda]$ and $[1, \infty)$. As ψ can be defined at infinity it is more convenient to glue Riemann spheres $\mathbb{P}^1(\mathbf{C}) = \mathbf{C} \cup \{\infty\}$ on which ∞ is a point rather than a limit. Topologically, it is clear (draw a picture!) that one obtains a surface E homeomorphic to a torus. It can be realized as a smooth complex curve in projective 2-space by taking

$$E = \{(x, y, z) : y^2z = x(x-z)(x-\lambda z)\} \subset \mathbb{P}^2(\mathbf{C}).$$

Note that as before, the points on the affine curve E_a in affine 2-space $\{z \neq 0\} \cong \mathbf{C}^2$ are of the form $(t, \pm\sqrt{t(t-1)(t-\lambda)})$. The only point 'at infinity' of E is the point $Z = (0, 1, 0)$, and we let $\psi(Z) = 0$.

An important difference with the quadratic case is that the values of ψ are well-defined only up to multiples of the values of *two* integrals along closed paths. The first is the integral around either of the branch cuts, which has the value $\omega_1 = 2(\psi(0) - \psi(-\infty)) = -2(\psi(1) - \psi(\lambda)) = 2\psi(0)$. The second is the integral through the two branch cuts, which has the value $\omega_2 = 2(\psi(\lambda) - \psi(0)) = 2\psi(1)$. Note that these two paths are exactly the two obvious incontractible paths on the torus.

Let $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ be the rectangular lattice spanned by ω_1 and ω_2. Then ψ has well-defined values in $\mathbf{C}/\Lambda$, which is also a torus. Exactly as in the previous case, we obtain a bijection $\psi : E \xrightarrow{\sim} \mathbf{C}/\Lambda$ that can be shown to be a complex analytic isomorphism. Using this bijection, the group structure of the torus $\mathbf{C}/\Lambda$ can be transported to the curve E, so that E becomes an abelian group. Writing $P(z) = \psi^{-1}(z)$ for $z \in \mathbf{C}/\Lambda$, it follows from the identity $\psi'(t) = 1/\sqrt{t(t-1)(t-\lambda)}$ that P satisfies the differential equation

$$(P')^2 = P(P-1)(P-\lambda).$$

More precisely, the inverse map $\psi^{-1} : \mathbf{C}/\Lambda \to E$ is given by $\psi^{-1}(z) = (P(z), P'(z)) \in E_a$ for $z \neq 0 \bmod \Lambda$ and $\psi(0) = Z$. The function P can be viewed as a double-periodic function on $\mathbf{C}$. Unlike $\sin(z)$, it has singularities at the lattice points $z \in \Lambda \subset \mathbf{C}$, but we will see in the next section that it does not have essential singularities like the sine function, which behaves so badly at infinity that we had no obvious analytic extension of the map ϕ to a projective curve. (See the exercises for this point.)

In the next section, we will systematically study double-periodic functions like P. Such functions arise from elliptic integrals like the integral $\psi(x)$ above and are therefore called elliptic functions. They parametrize complex curves like E that are homeomorphic to a torus. These curves are exactly the 'smooth projective curves of genus 1' and are known as *elliptic curves*.

We have seen that the addition formulae on the curve C are the algebraic addition formulae for the sine and cosine functions. In the next section, we will see that the addition formulae for the points on the elliptic curve E come from analogous formulae for for the elliptic functions P and P'. Such formulae were originally discovered in terms of ψ, i.e. for the elliptic integrals rather than for the elliptic functions. They go back to Euler and Legendre. The theory of elliptic functions was further developed by Abel, Jacobi and, somewhat later, Riemann. They discovered that differentials in which $\deg(f) > 4$ lead to curves of higher genus, i.e. curves that have more 'holes' than a complex torus. Integration of so-called holomorphic differentials on these curves are then used to map the curve into its Jacobian, which is an *abelian variety.*

In these notes, we will principally deal with arithmetic aspects of elliptic functions. The point here, already known to Abel, is that elliptic functions modulo 'algebraic lattices' like the ring of integers in an imaginary quadratic number field $K = \mathbf{Q}(\sqrt{-d})$ tend to assume algebraic values on K. In fact, these values generate *abelian* extensions of K and can even be used to generate the maximal abelian extension of K. This discovery goes back to Kronecker and Weber, whose names are also attached to the corresponding theorem over $\mathbf{Q}$. We will describe the theorems both for $\mathbf{Q}$ and K in terms of what we have done so far.

Consider the map $\phi : C \to \mathbf{C}/2\pi\mathbf{Z}$ described earlier. We have seen that ϕ^{-1} can be used to equip C with a group structure. Now consider the *torsion subgroup* of $\mathbf{C}/2\pi\mathbf{Z}$, which is $2\pi\mathbf{Q}/2\pi\mathbf{Z}$. The function ϕ^{-1} maps torsion elements to points $(\sin 2\pi q, \cos 2\pi q)$ whose coordinates are algebraic numbers that generate abelian extensions of $\mathbf{Q}$. One can formulate the Kronecker-Weber theorem in the following way.

1.6. Theorem. *Let L be the extension of $\mathbf{Q}$ obtained by adjoining the values of the function $\sin(2\pi x)$ for rational x. Then L is an abelian extension of $\mathbf{Q}$, and the maximal abelian extension of $\mathbf{Q}$ equals $\mathbf{Q}^{\mathrm{ab}} = L(\sqrt{-1})$.*

Of course there are more precise versions of this theorem, describing in detail the Galois groups of extensions obtained by adjoining the sine of an n-torsion element in $\mathbf{C}/2\pi\mathbf{Z}$. The formulation in terms of the sine function we have chosen is somewhat peculiar, but it stresses the remarkable fact that the abelian extensions of $\mathbf{Q}$ are generated by the values of an analytic function on the torsion elements of an analytic group.

The situation is slightly more complicated if K is an imaginary quadratic field with ring of integers $\mathcal{O}_K$. The main point is that an analytic isomorphism $\psi : E \to \mathbf{C}/\Lambda$ is not uniquely determined but only up to isomorphisms $\alpha : \mathbf{C}/\Lambda \xrightarrow{\alpha} \mathbf{C}/\alpha\Lambda$. This phenomenon of freedom of scaling already occurs in the 'rational case' of $\mathbf{C}/2\pi\mathbf{Z}$: if we had simply taken $\mathbf{C}/\mathbf{Z}$ and used the map $\Pi(z) = \sin(2\pi z)$ rather than $\sin(z)$, we would have obtained an analytic isomorphism $\phi^{-1} : z \mapsto (\Pi(z), \Pi'(z))$ with the curve $\tilde{C} = \{(x,y) : 4\pi^2x^2 + y^2 = 1\}$. This curve contains *no* points with algebraic coordinates, and ϕ is given by integration of the differential $\frac{dt}{\sqrt{1-4\pi^2t^2}}$.

In the case of the quadratic field K, it is not always possible to find an elliptic curve E, say in (affine) Weierstrass normal form

$$E = \{(x,y) : y^2 = 4x^3 - g_2x - g_3\},$$

such that the coefficients g_2 and g_3 are in K and such that there exists an analytic isomorphism $E \xrightarrow{\sim} \mathbf{C}/\alpha\mathcal{O}_K$. Replacing a lattice $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ by $\alpha\Lambda$ has the effect $g_2 \mapsto \alpha^{-4}g_2$ and $g_3 \mapsto \alpha^{-6}g_3$ on the coefficients of the Weierstrass equation for the corresponding elliptic curve E, so the value

$$j(\Lambda) = j(\omega_1/\omega_2) = 12^3 \frac{g_2^3}{g_2^3 - 27g_3^2}$$

only depends on ω_1/ω_2. It is called the *j-invariant* of the lattice Λ, and as a function on elements $\omega_1/\omega_2 \in \mathcal{H}$ it gives rise to a *modular function* on the upper half plane. The coefficient $12^3 = 1728$ is a standard normalization motivated by integrality properties of j

(cf. theorem 4.1). It is not hard to see that $\mathbf{Q}(j(\Lambda))$ is the smallest field over which one can define an elliptic curve $y^2 = 4x^3 - g_2x - g_3$ isomorphic to $\mathbf{C}/\Lambda$. Kronecker discovered that this field has a remarkable property when Λ is the ring of integers in a quadratic field.

1.7. Theorem. *Let $\mathcal{O}_K = \mathbf{Z}+\mathbf{Z}\tau_K$ be the ring of integers of an imaginary quadratic field K. Then $j(\mathcal{O}_K) = j(\tau_K)$ is algebraic over K, and $K(j(\tau_K))$ is the maximal unramified abelian extension of K.*

The field $H_K = K(j(\tau_K))$ is known as the *Hilbert class field* of K. The Galois group $\mathrm{Gal}(H_K/K)$ can be described explicitly: it is isomorphic to the class group of $\mathcal{O}_K$. This observation has been a starting point for *class field theory*, a theory describing abelian extensions of arbitrary number fields.

It turns out that a large part of the maximal abelian extension of K can be generated with values of the j-function.

1.8. Theorem. *Let K be imaginary quadratic and L the field obtained by adjoining the numbers $j(n\tau_K)$ for $n \in \mathbf{Z}_{\geq 1}$. Then L is algebraic over K, and it is the maximal abelian extension of K for which $\mathrm{Gal}(L/\mathbf{Q})$ is a dihedral group. The maximal abelian extension K^{ab} of K can be obtained from $L\mathbf{Q}^{\mathrm{ab}}$ by adjoining an infinite number of square roots.*

In order to obtain K^{ab} completely, one proceeds as for $\mathbf{Q}$. Let $E : y^2 = 4x^3 - g_2x - g_3$ be an elliptic curve isomorphic to $\mathbf{C}/\mathcal{O}_K$ that is defined over H_K. Then there is a complex analytic isomorphism $\mathbf{C}/\alpha\mathcal{O}_K \xrightarrow{\sim} E$ of the form $z \mapsto (\wp(z), \wp'(z))$ that is inverse to the integration of the differential $dt/\sqrt{t^3 - g_2t - g_3}$ on E, and we have the following analogue of 1.6.

1.9. Theorem. *Let K be imaginary quadratic of discriminant $D < -4$ with Hilbert class field H_K. Then the extension of H obtained by adjoining the values of the function $\wp(x)$ in the torsion points of $\mathbf{C}/\alpha\mathcal{O}_K$, with α chosen as above, is the maximal abelian extension of K.*

It is more elegant to suppress the reference to an element α in the theorem above by suitably normalizing the function $\wp$. This normalized $\wp$-function, which is defined in section 3, is called the *Weber function*.

Exercises.

1.1. Prove lemma 1.1. How should the lemma be modified if $\mathbf{C}$ is replaced by an arbitrary field?

1.2. Show that the closure $\bar{C} = \{(x,y,z) : x^2+y^2 = z^2\} \subset \mathbb{P}^2(\mathbf{C})$ of C in projective 2-space equals $C \cup (1,i,0) \cup (1,-i,0)$ under the identification of $\mathbf{C}^2$ with $\{z \neq 0\}$, and that the algebraic map $g : \mathbb{P}^1(\mathbf{C}) \to C$ given by $g(x,y) = (2xy, x^2-y^2, x^2+y^2)$ is bijective. Conclude that $\bar{C}$ is homeomorphic to the Riemann sphere $\mathbb{P}^1(\mathbf{C})$. [Note that this is in accordance with the construction of C by glueing two copies of $\mathbf{C}$ along a branch cut: $\bar{C}$ must be homeomorphic to 2 Riemann spheres glued along a branch cut, i.e. to a sphere.]

1.3. Show that any integral of the form $\int R(t, \sqrt{1-t^2})dt$ with R rational becomes rational after the substitution $t = \frac{2x}{1+x^2}$ or $t = \frac{1-x^2}{1+x^2}$. What is the relation with the previous exercise?

1.4. Construct a compactification $\overline{\mathbf{C}/2\pi\mathbf{Z}}$ of $\mathbf{C}/2\pi\mathbf{Z}$ by adding two points $i\infty$ and $-i\infty$ 'at infinity' and show that the map $\phi : C \to \mathbf{C}/2\pi\mathbf{Z}$ can be extended to a homeomorphism $\bar{C} \to \overline{\mathbf{C}/2\pi\mathbf{Z}}$, where $\bar{C}$ is the projective closure of C.

1.5. *(Periods of meromorphic functions.)* Let f be a meromorphic function on $\mathbf{C}$. A number $\omega \in \mathbf{C}$ is said to be a *period* of f if $f(z+\omega) = f(z)$ for all $z \in \mathbf{C}$. Let Λ be the set of periods of f, and suppose that f is non-constant.

a. Prove that Λ is a discrete subgroup of $\mathbf{C}$.

b. Deduce that Λ is of one of the three following forms:

$$\Lambda = \{0\} \qquad \Lambda = \mathbf{Z}\omega \quad (\omega \neq 0) \qquad \Lambda = \mathbf{Z}\omega_1 \oplus \mathbf{Z}\omega_2 \quad (\text{with } \mathbf{C} = \mathbf{R}\omega_1 + \mathbf{R}\omega_2)$$

1.6. Let f be a meromorphic function with non-zero period ω and define $q = q(z) = e^{2\pi i z/\omega}$. Prove that there exists a meromorphic function $\hat{f}$ on $\mathbf{C}^*$ such that $f(z) = \hat{f}(q)$, and show that the $\mathrm{ord}_q(\hat{f}) = \mathrm{ord}_z(f)$ for all $z \in \mathbf{C}$.

1.7. *(Legendre normal form)* Show that an elliptic differential $dt/\sqrt{f(t)}$ remains elliptic under a Möbius transformation $t \mapsto \frac{at+b}{ct+d}$. Deduce that f has the form $f(t) = ct(t-1)(t-\lambda)$ after a suitable transformation. Show also that there exists a Möbius transformation that brings f in the form $f(t) = (1-t^2)(1-k^2t^2)$.

1.8. Let $f \in \mathbf{C}[t]$ be a polynomial of degree d, and let $S_k(\alpha)$ be defined as in (1.2). Show that any integral of the form $\int \frac{R(t)dt}{\sqrt{f(t)}}$ with R rational can be written as the sum of an algebraic function $F(t)\sqrt{f(t)}$ and a finite linear combination of integrals in the set

$$\{S_{-1}(\alpha)\}_{\alpha \in \mathbf{C}} \cup \{(S_k(0)\}_{k=0}^{d-2}.$$

[Hint: If $f = \sum_i c_i(t-\alpha)^i$, then $(x-\alpha)^n\sqrt{f(x)} = \sum_{i=0}^{d}(n+\frac{1}{2}i)c_iS_{n-1+i}(\alpha)$.]

1.9. Let $k \in (0,1)$ be given and define the map $\phi : \overline{\mathcal{H}} \to \mathbf{C}$ on the closed upper half plane by

$$\phi(x) = \int_0^x \frac{dt}{\sqrt{(1-t^2)(1-k^2t^2)}}.$$

(Here integration is over a path in $\overline{\mathcal{H}}$ and the integrand is given the value 1 in 0.)

a. Show that ϕ maps the (open) upper half plane in $\mathbf{C}$ holomorphically onto the interior of a rectangle in $\mathbf{C}$ with vertices $\phi(-1)$ and $\phi(1)$ on the real axis and vertices $\phi(-1/k)$ and $\phi(1/k)$ in the upper half plane.

b. Make appropriate branch cuts and show that ϕ has a natural extension to a smooth curve in $\mathbb{P}^2(\mathbf{C})$ when its values are taken in $\mathbf{C}/\Lambda$, where Λ is the rectangular lattice generated by $4\phi(1)$ and $2(\phi(1/k) - \phi(1))$.

Define the *complete elliptic integrals of the first and second kind* with respect to the modulus k are defined as

$$K(k) = \int_0^1 \frac{dx}{\sqrt{(1-x^2)(1-k^2x^2)}}$$

$$E(k) = \int_0^1 \sqrt{(1-x^2)(1-k^2x^2)}\,dx.$$

c. Show that $\phi(1/k) - \phi(1) = iK(k')$, where the complementary modulus k' is defined by $k^2 + k'^2 = 1$. Conclude that Λ is generated by $4K(k)$ and $2iK(k')$.
[Hint: use the substitution $x \mapsto (1 - k'^2x^2)^{-1/2}$.]

d. Prove the identities:

$$K(k) = \int_0^{\pi/2} \frac{d\theta}{\sqrt{1-k^2\sin^2\theta}} \quad \text{and} \quad E(k) = \int_0^{\pi/2} \sqrt{1-k^2\sin^2\theta}\,d\theta.$$

1.10. Show that the arclength of the ellipse $(x/a)^2 + (y/b)^2 = 1$ with $a \geq b > 0$ is equal to $4aE(\sqrt{1-(b/a)^2})$.

1.11. A *lemniscate of Bernoulli* is the set L of points X in the Euclidean plane for which the product of the distances XP_1 and XP_2, with P_1 and P_2 given points at distance $P_1P_2 = 2d > 0$, is equal to d^2.

a. Show for a suitable choice of coordinates, the equation for L is $(x^2+y^2)^2 = x^2 - y^2$ or, in polar coordinates, $r^2 = \cos 2\phi$. Sketch this curve.

b. Show that the arclength of the 'unit lemniscate' in (a) equals $2\sqrt{2}K(1/\sqrt{2})$, and that this is also the value of the complete elliptic integral $4\int_0^1 \frac{dt}{\sqrt{1-t^4}}$.

[Note the similarity with the arclength of the unit circle, which is given by $4\int_0^1 \frac{dt}{\sqrt{1-t^2}}$.]

2. ELLIPTIC FUNCTIONS

In this section we will develop the basic theory of double-periodic functions encountered in the previous section.

An *elliptic function* with respect to a lattice $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ in $\mathbf{C}$ is a meromorphic function f on $\mathbf{C}$ that satisfies $f(z+\omega) = f(z)$ for all $\omega \in \Lambda$. Sums and quotients of elliptic functions are again elliptic functions, and the set $\mathfrak{M}_\Lambda$ of elliptic functions with period lattice Λ is an *elliptic function field*. It is usually identified with the field of meromorphic functions on the complex torus $T = \mathbf{C}/\Lambda$. By Liouville's theorem, the holomorphic functions in $\mathfrak{M}_\Lambda$ are the constant functions. Choosing a fundamental parallellogram F for Λ, we can count the residues $\mathrm{res}_w(f)$ and orders of vanishing $\mathrm{ord}_w(f)$ at points $w \in F$ by evaluating suitable integrals along ∂F.

2.1. Lemma. *Let $f \neq 0$ be an elliptic function modulo Λ. Then the following holds.*

(i) $\sum_{w\in F} \mathrm{res}_w(f) = 0$.

(ii) $\sum_{w\in F} \mathrm{ord}_w(f) = 0$.

(iii) $\sum_{w\in F} \mathrm{ord}_w(f) \cdot w \in \Lambda$.

The contents of the lemma can be conveniently rephrased in terms of divisors. A *divisor* on $T = \mathbf{C}/\Lambda$ is a formal linear combination of points of T with integer coefficients, i.e. an element of the *divisor group* $\mathrm{Div}(T) = \bigoplus_{w\in T} \mathbf{Z} \cdot (w)$. One defines the *degree* of a divisor $D = \sum_{w\in T} n_w \cdot (w)$ as $\deg(D) = \sum_w n_w$. An elliptic function $f \in \mathfrak{M}_\Lambda^*$ is determined up to multiplication by a non-zero constant by the corresponding divisor

$$(f) = \sum_{w\in T} \mathrm{ord}_w(f) \cdot (w) \in \mathrm{Div}(T).$$

Part (ii) of the lemma states that *principal divisors*, i.e. the divisors coming from non-zero elliptic functions, are in the subgroup $\mathrm{Div}^0(T)$ of divisors of degree zero. Let $\Sigma : \mathrm{Div}(T) \to T$ be the summation map $\sum_{w\in T} n_w \cdot (w) \mapsto \sum_{w\in T} n_w \cdot w$. Then we have a sequence

$$1 \longrightarrow \mathbf{C}^* \longrightarrow \mathfrak{M}_\Lambda^* \longrightarrow \mathrm{Div}^0(T) \xrightarrow{\Sigma} T \longrightarrow 0, \tag{2.2}$$

and the lemma states that this sequence is exact as soon as we prove that every divisor in $\ker \Sigma$ is principal. For this proof, we refer to the exercises.

The number of zeroes (or, equivalently, poles) of an elliptic function f, counted with multiplicity, is called the *order* of f. More precisely, it is the degree of the *polar divisor* $-\sum_{w:\mathrm{ord}_w(f)<0} \mathrm{ord}_w(f) \cdot (w)$ of f. By the lemma, any non-constant elliptic function has order at least 2. We will show that there exists an elliptic functions of order 2 by explicitly constructing the *Weierstrass $\wp$-function* for Λ. This is an elliptic function $\wp = \wp_\Lambda$ with double poles exactly at the points $\omega \in \Lambda$. It is defined by

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

Here $\Lambda' = \Lambda - \{0\}$. The convergence of the sum follows from the fact that the sum

$$G_k(\Lambda) = \sum_{\omega\in\Lambda'} \omega^{-k}$$

is convergent for $k > 2$. For integral $k > 2$, the series $G_k(\Lambda)$ is known as the *Eisenstein series of order* k. Note that $G_k = 0$ for $k > 1$ odd. The periodicity of the $\wp$-function follows from the fact that it is an even function whose derivative $\wp'(z) = -2\sum_{\omega\in\Lambda}(z-\omega)^{-3}$ is obviously periodic.

2.3. Theorem. *The elliptic function field relative to* Λ *equals* $\mathfrak{M}_\Lambda = \mathbf{C}(\wp_\Lambda, \wp'_\Lambda)$.

Proof. It suffices to prove that an even elliptic function f is a rational expression in $\wp$. When f is even, $\mathrm{ord}_w(f)$ is even at points w satisfying $w = -w \bmod \Lambda$ and (f) is a finite sum of the form

$$(f) = \sum_w n_w[(w) + (-w)] = \sum_w n_w[(w) + (-w) - 2(0)].$$

We may and do assume that no term with $w = 0$ occurs in the last sum. The functions f and $\prod_w(\wp(z) - \wp(w))^{n_w}$ have the same divisor, so their quotient is a constant. □

The function $\wp'$ is an odd elliptic function with polar divisor $3\cdot(0)$, so its 3 zeroes are the 3 points $\omega_1/2$, $\omega_2/2$ and $\omega_3/2 = (\omega_1+\omega_2)/2$ of order 2 in $\mathbf{C}/\Lambda$. The even function $(\wp')^2$ has divisor $\sum_{i=1}^3[2\cdot(\omega_i/2) - 2\cdot(0)]$, so the preceding proof and a look at the first term $\frac{4}{z^6}$ of the Laurent expansion of $(\wp')^2$ around 0 show that we have a differential equation

$$\begin{aligned}(\wp'(z))^2 &= 4\prod_{i=1}^3(\wp(z) - \wp(\omega_i/2))\\ &\overset{\text{def}}{=} 4\wp(z)^3 - g_1\wp(z)^2 - g_2\wp(z) - g_3.\end{aligned}$$

As the Laurent expansion of $\wp$ around 0 has no constant term, the function $(\wp')^2 - 4\wp^3$ has a pole of order 2 only at 0, whence $g_1 = 0$. The cubic polynomial in $\wp$ on the right hand side has distinct zeroes since the functions $\wp(z) - \wp(\omega_i/2)$ have order 2 and a double zero at $\omega_i/2$. Consequently, its discriminant Δ is non-zero. A more careful analysis of the differential equation using the Laurent-expansion

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

for $\wp(z)$ around $z = 0$ yields the following explicit expressions for the coefficients g_2 and g_3 in terms of Λ.

2.4. Theorem. *The* $\wp$*-function for* Λ *satisfies a Weierstrass equation*

$$(\wp'_\Lambda)^2 = 4\wp_\Lambda^3 - g_2\wp_\Lambda - g_3$$

with coefficients $g_2 = g_2(\Lambda) = 60G_4(\Lambda)$ *and* $g_3 = g_3(\Lambda) = 140G_6(\Lambda)$. *The discriminant* $\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2$ *does not vanish.*

One deduces from this differential equation that the Eisenstein series $G_k(\Lambda)$ are universal rational expressions in $g_2(\Lambda)$ and $g_3(\Lambda)$. It also follows that we have constructed the kind of map that was informally discussed in the introduction.

2.5. Theorem. *Let* $\Lambda \subset \mathbf{C}$ *be a lattice and* $E \subset \mathbb{P}^2(\mathbf{C})$ *be the elliptic curve with Weierstrass equation* $Y^2Z = 4X^3 - g_2(\Lambda)XZ^2 - g_3(\Lambda)Z^3$. *Then there is an analytic isomorphism* $\mathbf{C}/\Lambda \xrightarrow{\sim} E$ *defined by* $z \longmapsto [\wp(z) : \wp'(z) : 1]$ *for* $z \notin \Lambda$ *and* $0 \longmapsto [0 : 1 : 0]$.

By this isomorphism, we obtain an abelian group structure on E such that $[0 : 1 : 0]$ is the unit element of E. It has the following nice geometric interpretation. Let $L \subset \mathbb{P}^2(\mathbf{C})$ be the line with equation $aX + bY + cZ = 0$. Then $L \cap E$ consists of three (not necessarily distinct) points P_1, P_2, P_3, and 2.1 (iii) applied to the elliptic function $a\wp(z) + b\wp'(z) + c$ shows that $P_1 + P_2 + P_3 = O$ in the group E. From this it is straightforward to derive the addition formula for the $\wp$-function on $\mathbf{C}/\Lambda - \{0\}$:

$$\wp(z_1 + z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2 \qquad (z_1 \neq \pm z_2 \bmod \Lambda).$$

Algebraic theory. We have proved that every complex torus is in fact an *algebraic curve*, i.e. it is isomorphic to a complex projective curve given as the zero set in $\mathbb{P}^2(\mathbf{C})$ of a homogeneous *polynomial* in $\mathbf{C}[X, Y, Z]$. Knowing this, one can give a much more algebraic interpretation to everything we did so far. This interpretation uses the Riemann-Roch theorem [6], which gives for any divisor D on a smooth projective curve over a field K the K-dimension of the vector space of those K-rational functions on the curve that have polar divisor at most D. The meromorphic functions on a complex torus T are rational in $\wp$ and $\wp'$, so they correspond to rational functions on the corresponding elliptic curve under our isomorphism. The Riemann-Roch theorem tells us that the dimension of the $\mathbf{C}$-vector space of elliptic functions having polar divisor at most D equals $\deg(D)$ for every divisor D of positive degree. In particular, the space of elliptic functions having at most a simple pole is the 1-dimensional space of constant functions, and the space of functions having at most a double pole at $z = \alpha$ is generated by the constant function 1 and a function F that is unique up to transformations of the form $F \mapsto aF + b$. The Weierstrass $\wp$-function can be characterized as the unique elliptic function that has polar divisor $2 \cdot (0)$ and Laurent expansion $\sum_{k \geq -2} c_k z^k$ around its pole normalized by $c_{-2} = 1$ and $c_0 = 0$. The Weierstrass equation can be seen as a linear dependency between the seven functions $x = \wp$, $y = \wp'$, x^2, x^3, xy, y^2 and 1 in the 6-dimensional space of elliptic functions with polar divisor at most $6 \cdot (0)$. Its simple form comes from the clever choice of the coordinates x and y.

The approach via the Riemann-Roch theorem shows that any elliptic curve E over a field K—this is by definition a smooth projective curve over K of genus 1 containing a K-rational point O—can be equipped with an abelian group structure such that O is the neutral element. One considers the algebraic analogue

$$1 \longrightarrow K^* \longrightarrow K(E)^* \longrightarrow \mathrm{Div}^0(E) \longrightarrow \mathrm{Pic}^0(E) \longrightarrow 0$$

of the sequence (2.2), in which $K(E)$ is the field of rational functions on E (the *function field* of E) and the degree 0 part $\mathrm{Pic}^0(E)$ of the *divisor class group* $\mathrm{Pic}(E)$ is defined by exactness. The Riemann-Roch theorem implies that the map $\mathrm{Pic}^0(E) \to E$ sending the class of $(P)-(O)$ to P for any point $P \in E$ is a bijection (see the exercises). The resulting group structure on E has the same geometric interpretation as the one we gave in the complex case. If $x, y \in K(E)$ are functions having polar divisor $2 \cdot (O)$ and $3 \cdot (O)$—their existence is guaranteed by Riemann-Roch—then there is, by the same argument as before, a general Weierstrass equation

$$y^2 + a_1xy + a_3y = a_0x^3 + a_2x^2 + a_4x + a_6$$

with $a_0 \neq 0$. One can show that the map $E \to \mathbb{P}^2(K)$ mapping points $P \in E$ different from O to $[x(P), y(P), 1]$ and O to $[0, 1, 0]$ establishes an isomorphism between E and the projective curve in $\mathbb{P}^2(K)$ defined by the Weierstrass equation above.

Exercises.

2.1. Show that a non-constant elliptic function assumes every value on the Riemann sphere in some point on the torus.

2.2. *(Multiplicative construction of the $\wp$-function.)* The Weierstrass σ-function for a lattice Λ is defined by

$$\sigma(z) = \sigma_\Lambda(z) = z \prod_{\omega \in \Lambda'} (1 - \frac{z}{\omega}) e^{(z/\omega)+\frac{1}{2}(z/\omega)^2}.$$

a. Show that $\sigma_\Lambda(z)$ is an odd holomorphic function on $\mathbf{C}$ with simple zeroes at all $\omega \in \Lambda$, and that $\frac{d^2}{dx^2} \log \sigma_\Lambda(z) = -\wp_\Lambda(z)$.

b. Show that for each $\omega \in \Lambda$, there exist constants $a, b \in \mathbf{C}$ such that $\sigma(z+\omega) = e^{az+b}\sigma(z)$ for all $z \in \mathbf{C}$. [Such a function is called a *theta function* with respect to Λ.]

c. Prove the identity

$$\wp(z) - \wp(a) = -\frac{\sigma(z-a)\sigma(z+a)}{\sigma(a)^2\sigma(z)^2} \qquad (a \notin \Lambda).$$

2.3. *(Degeneracy of the $\wp$-function.)* Let ω be an element in $\mathbf{C} \setminus \mathbf{R}$.

a. Show that

$$\lim_{t\to\infty} \wp_{[t,\omega t]}(z) = \frac{1}{z^2}$$

for $z \in \mathbf{C}^*$, and that

$$\lim_{t\to\infty} \wp_{[1,it]}(z) = \frac{1}{\sin^2(\pi z)} + \frac{3}{\pi^2}$$

for $z \in \mathbf{C} \setminus \mathbf{Z}$. Show also that the convergence is uniform on every compact subset K of $\mathbf{C}^*$ and $\mathbf{C} \setminus \mathbf{Z}$, respectively.

b. What are the degenerate forms of the function $\sigma(z)$ corresponding to the two cases in a, and which identities replace that in part c of the previous exercise?

c. Explain why these two forms of degeneracy are called *additive* and *multiplicative*, respectively.

2.4. Show that the sequence (2.2) in the text is exact.
[Hint: if $\sum_w n_w = \sum_w n_w \cdot w = 0$, then $\prod_w \sigma(z-w)^{n_w}$ is elliptic with divisor $\sum_w n_w(w)$. If $\sum_w n_w \cdot w = \lambda \in \Lambda$, add the trivial divisor $(0) - (\lambda)$.]

2.5. Prove the duplication formula for the $\wp$-function:

$$\wp(2z) = -2\wp(z) + \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2$$

and show how it can be used to write $\wp(2z)$ as a rational function in $\wp(z)$.

2.6. Show that the derivative of the $\wp$-function satisfies

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

2.7. Let E be an elliptic curve over a field K. Show that the map $\mathrm{Pic}^0(E) \to E$ sending $(P)-(O)$ to P is a bijection, and that the induced group structure on E is such that any three points on E that are collinear under the Weierstrass-embedding in $\mathbb{P}^2(K)$ have sum 0.
[Hint: use Riemann-Roch to show that every divisor D of degree 0 is equivalent to a divisor $(P) - (O)$ and to show that (P) and (Q) are equivalent if and only if $P = Q$.]

2.8. The *Weierstrass ζ-function* for a lattice $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ in $\mathbf{C}$ is defined as $\zeta(z) = \frac{d}{dz}\log\sigma(z)$.

a. Show that $\zeta(z)$ has a partial fraction expansion

$$\zeta(z) = \frac{1}{z} + \sum_{\omega\in\Lambda'}\left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right).$$

b. Show that there exists a linear function $\eta : \Lambda \to \mathbf{C}$ such that $\zeta(z+\omega) = \zeta(z) + \eta(\omega)$ for $\omega \in \Lambda$ and $z \in \mathbf{C}$, and that $\eta(\omega) = 2\zeta(\omega/2)$ if $\omega \not= 2\Lambda$.

The numbers $\eta_i = \eta(\omega_i)$ $(i = 1, 2)$ are the *quasi-periods* of $\zeta(z)$.

c. Prove the *Legendre relation* $\eta_1\omega_2 - \eta_2\omega_1 = \pm 2\pi i$. What can you say about the sign?
[Hint: the right hand side equals $\oint \zeta(z)dz$ around a fundamental parallelogram.]

d. Show that $\sigma(z+\omega) = \pm e^{\eta(\omega)(z+\omega/2)}\sigma(z)$. What can you say about the sign?

2.9. *(Weil reciprocity law.)* For an elliptic function f and a divisor $D = \sum_{w\in T} n_w \cdot (w) \in \mathrm{Div}(T)$ on the complex torus T, we let $f(D) = \prod_w f(w)^{n_w} \in \mathbf{C}$. Prove that for any two elliptic functions f and g with disjoint divisors, we have

$$f((g)) = g((f)).$$

[Hint: write f and g as products of σ-functions.]

2.10. Let $G_k = \sum_{\omega \in \Lambda'} \omega^{-k}$ be the Eisenstein series of order k, and define $G_2 = G_1 = 0$ and $G_0 = -1$.

a. Show that $(k-1)(k-2)(k-3)G_k = 6\sum_{j=0}^{k}(j-1)(k-j-1)G_jG_{k-j}$ for all $k \geq 6$. [Hint: $\wp'' = 6\wp^2 - 30G_4$.]

b. Show that $G_8 = \frac{3}{7}G_4^2$, $G_{10} = \frac{5}{11}G_4G_6$ and $G_{12} = \frac{25}{143}G_6^2 + \frac{18}{143}G_4^3$ and that, more generally, every Eisenstein series can be computed recursively from G_4 and G_6 by the formula

$$(k^2-1)(k-6)G_k = 6\sum_{j=4}^{k-4}(j-1)(k-j-1)G_jG_{k-j}.$$

2.11. View G_k as a modular form of weight k on the upper half plane. and write $g_2 = 60G_4$ and $g_3 = 140G_6$.

a. Show that $\Delta = g_2^3 - 27g_3^2$ is a modular form of weight 12 that does not vanish on the upper half plane.

b. Prove that Δ is a cusp form.

c. Show that every modular form is a polynomial in g_2 and g_3 with coefficients in $\mathbf{C}$.

d. Show that g_2 and g_3 are algebraically independent over $\mathbf{C}$. Conclude that the graded algebra $M = \bigoplus_k M_k$ of modular forms is isomorphic to the graded polynomial ring $\mathbf{C}[X,Y]$ with weight$(X) = 2$, weight$(Y) = 3$. [Hint: the zeroes of g_2 and g_3 are distinct.]

2.12. Show that an elliptic curve over a field K of characteristic char$(K) \neq 2, 3$ can be given by an affine Weierstrass equation $y^2 = x^3 - a_4x - a_6$ with $4a_4^3 - 27a_6^2 \neq 0$.

3. MAPS BETWEEN ELLIPTIC CURVES

We have seen in the previous section that for every lattice $\Lambda \subset \mathbf{C}$, the torus $\mathbf{C}/\Lambda$ is isomorphic to the elliptic curve $E_\Lambda \subset \mathbb{P}^2(\mathbf{C})$ with affine Weierstrass equation

$$Y^2 = 4X^3 - g_2X - g_3, \tag{3.1}$$

where g_2 and g_3 are normalized Eisenstein series of order 4 and 6 with respect to Λ. By the Riemann-Roch theorem, every elliptic curve E over a field K of characteristic different from 2 or 3 is given by a Weierstrass equation of the form (3.1) with $g_2, g_3 \in K$ and $g_2^3 - 27g_3^2 \neq 0$. If $K = \mathbf{C}$, then the following theorem shows that E comes from a lattice. The proof will be given in the next section as an application of the j-function.

3.1. Uniformization theorem. *Let E be an elliptic curve over $\mathbf{C}$. Then there exists a lattice $\Lambda \subset \mathbf{C}$, unique up to multiplication by a constant in $\mathbf{C}^*$, such that there is an analytic isomorphism $\mathbf{C}/\Lambda \xrightarrow{\sim} E$.*

If Λ and M are lattices in $\mathbf{C}$, then the analytic maps $\mathbf{C}/\Lambda \to \mathbf{C}/M$ preserving the origin and the algebraic maps $E_\Lambda \to E_M$ preserving the unit element coincide, and they are easily described as coming from multiplication by elements in $\mathbf{C}$.

3.2. Lemma. *There are natural bijections between the following three sets:*
(i) $\{\alpha \in \mathbf{C} : \alpha\Lambda \subset M\}$;
(ii) *analytic maps $\mathbf{C}/\Lambda \to \mathbf{C}/M$ mapping 0 to 0;*
(iii) *algebraic maps $E_\Lambda \to E_M$ mapping O_Λ to O_M.*

The essential step in the proof consists of showing that every map in (ii) comes from a multiplication by some $\alpha \in \mathbf{C}$. This is done by lifting such a map to an analytic map $\mathbf{C} \to \mathbf{C}$ and observing that the derivative of this map is a holomorphic elliptic function, whence constant. □

In conjunction with the uniformization theorem, the lemma implies that the categories of complex lattices, complex tori with 'origin' and elliptic curves over $\mathbf{C}$ are equivalent when the appropriate morphisms between the objects are considered. As morphisms between groups admit a natural addition, the sets of morphisms in the lemma are actually *groups*. It follows from the description in (i) that morphisms between elliptic curves over $\mathbf{C}$ are homomorphisms. This is an algebraic fact, and it is true over any field K.

It follows from the lemma that two elliptic curves E_Λ and E_M are isomorphic if and only if $M = \alpha\Lambda$ for some $\alpha \in \mathbf{C}^*$. In that case we say that Λ and M are *homothetic*. In terms of the Weierstrass equation 3.1, we see that two Weierstrass equations with coefficients g_2, g_3 and g_2', g_3' yield isomorphic elliptic curves E and E' if and only if there exists $\alpha \in \mathbf{C}^*$ such that $g_2 = \alpha^4 g_2'$ and $g_3 = \alpha^6 g_3'$. Note that this proves the uniqueness part in the uniformization theorem. As a lattice Λ is uniquely determined by the values of $g_2(\Lambda)$ and $g_3(\Lambda)$, we also find the characterization of the j-function mentioned in section 1.

3.3. Theorem. *Define the j-invariant of an elliptic curve E with Weierstrass equation* 3.1 *as*

$$j_E = 1728\frac{g_2^3}{\Delta} = 1728\frac{g_2^3}{g_2^3 - 27g_3^2}.$$

Then $\mathbf{Q}(j_E)$ is the minimal field of definition for E. Two elliptic curves over $\mathbf{C}$ are isomorphic if and only if their j-invariants coincide.

The maps in 3.2(iii) are called *isogenies* between elliptic curves. If there exists a non-zero isogeny $E \to E'$, then E and E' are called *isogenous*. From the complex description of isogenies it is clear that they are always surjective with finite kernel if they are non-zero. The order of the kernel is the *degree* of the isogeny. The degree of the zero-isogeny is 0 by definition. This notion of the degree coincides with the definition in algebraic geometry, where the degree of an isogeny $f : E_1 \to E_2$ is defined as the degree of the extension $f^*K(E_2) \subset K(E_1)$ of the corresponding function fields.

The endomorphisms of an elliptic curve form a ring. If $E \cong E_\Lambda$, then $\mathrm{End}(E)$ is isomorphic to the *multiplicator ring* $\mathcal{O}(\Lambda) = \{x \in \mathbf{C} : x\Lambda \subset \Lambda\}$ of Λ. Since lattices are only interesting up to homothety, we can always assume that $\Lambda = [1, \tau] = \mathbf{Z} + \mathbf{Z}\tau$ with τ in the upper half plane.

3.4. Theorem. *Let $\Lambda = [1, \tau]$ be a lattice and $E = E_\Lambda$ the corresponding elliptic curve. Then the endomorphism ring* $\mathrm{End}(E)$ *is isomorphic to* $\mathbf{Z}$ *unless τ is imaginary quadratic. In the last case* $\mathrm{End}(E)$ *is an order $\mathcal{O}$ in* $\mathbf{Q}(\tau)$ *and Λ is a fractional $\mathcal{O}$-ideal.*

Elliptic curves with endomorphism ring strictly larger than $\mathbf{Z}$ are said to have *complex multiplication*. As a corollary, we see that the automorphism group $\mathrm{Aut}(E) = (\mathrm{End}(E))^*$ of an elliptic curve is finite and usually of order 2.

3.5. Corollary. *The automorphism group of an elliptic curve E is a finite cyclic group of order*

$$\#\,\mathrm{Aut}(E) = \begin{cases} 2 & \textit{if } j \neq 0, 1728; \\ 4 & \textit{if } j = 1728; \\ 6 & \textit{if } j = 0. \end{cases}$$

The two exceptional cases occur for curves having complex multiplication by i (then $g_3 = 0$) or a third root of unity ρ (then $g_2 = 0$). The *Weber-function* $h_\Lambda(z)$ mentioned in section 1, which is defined accordingly, is a normalized version of the Weierstrass function that has the important property of being invariant under *all* isomorphisms between elliptic curves, i.e. it satisfies $h_{\alpha\Lambda}(\alpha z) = h_\Lambda(z)$ for all $\alpha \in \mathbf{C}^*$. The Weber functions will be studied in detail in the next sections. One defines

$$h(z) = h_\Lambda(z) = \begin{cases} -2^7 3^5 \frac{g_2 g_3}{\Delta}\wp(z) & \text{if } j(\Lambda) \neq 0, 1728; \\ 2^8 3^4 \frac{g_2^2}{\Delta}\wp(z)^2 & \text{if } j(\Lambda) = 1728; \\ -2^9 3^6 \frac{g_3}{\Delta}\wp(z)^3 & \text{if } j(\Lambda) = 0. \end{cases}$$

As in the case of the j-function, the normalizing numerical factors are only there to ensure that the Weber functions have integral Fourier expansions. On the elliptic curve

$E = E_\Lambda$ with Weierstrass equation 3.1, the function $h_\Lambda(z) = h_E(z)$ is a normalized x-coordinate. It does not depend on the isomorphism class of E and provides a bijection $E/\operatorname{Aut}(E) \xrightarrow{\sim} \mathbb{P}^1(\mathbf{C})$.

If $E = E_\Lambda$, the isogenies $f \in \operatorname{End}(E)$ correspond to $\alpha \in \mathcal{O}(\Lambda)$ and the algebraic nature of these isogenies has the following formulation in terms of the Weierstrass $\wp$-function.

3.6. Theorem. *For every $\alpha \in \mathcal{O}(\Lambda) - \{0\}$ there exist coprime polynomials $A, B \in \mathbf{C}[X]$ of degree $N = \alpha\bar{\alpha}$ and $N-1$, respectively, such that $\wp = \wp_\Lambda$ satisfies*

$$\wp(\alpha z) = \frac{A(\wp(z))}{B(\wp(z))}.$$

Proof. The Laurent series around $z = 0$ shows that $\deg(A) = \deg(B) + 1$. If $\{a_i\}_{i=1}^N$ denotes the kernel of multiplication by α, then one easily shows that the zeroes of the polynomial $A(X) - \wp(\alpha z)B(X) \in \mathbf{C}[X]$ are given by $X = \wp(z + a_i)$. □

If $\alpha = n \in \mathbf{Z}$, then $N = n^2$ and the polynomials A and B can be expressed in terms of *division polynomials* that can be computed inductively. They are the elliptic analogues of the cyclotomic polynomials. The exercises give the necessary details.

If N is very small, one can work with power series expansions around $z = 0$ in order to find the coefficients. This approach gives a method to compute the j-invariants of some small quadratic orders. As an example, we compute $j(\Lambda)$ for $\Lambda = \mathbf{Z}[\sqrt{-2}]$. In this case $\mathcal{O}(\Lambda) = \mathbf{Z}[\sqrt{-2}]$ and the previous theorem with $\alpha = \sqrt{-2}$ shows that $\wp$-function satisfies an identity of the form

$$\wp(\sqrt{-2}z) = a\wp(z) + b + \frac{1}{c\wp(z) + d}.$$

Obviously, we must have $a = -\frac{1}{2}$ and $b = 0$ to have the right polar part. So far, everything is valid for all lattices $\lambda\Lambda$, so we may assume that $G_4(\Lambda) = G_6(\Lambda) = s$ after replacing Λ by a homothetic lattice. We then have $G_8 = \frac{3}{7}G_4^2 = \frac{3}{7}s^2$. Substituting the Laurent series

$$\wp(z) = z^{-2} + 3sz^2 + 5sz^4 + 3s^2z^6 + \ldots$$

in the relation $(\wp(\sqrt{-2}z) + \frac{1}{2}\wp(z))(c\wp(z) + d) = 1$ yields equations

$$9cs = -2 \qquad 5cs = ds \qquad 5ds = 8cs^2,$$

from which one easily deduces that $s = 25/8$. It follows that

$$j(\sqrt{-2}) = 1728\frac{(60s)^3}{(60s)^3 - 27(140s)^2} = 8000 = 20^3.$$

Exercises.

All elliptic curves in these exercises are supposed to be defined over $\mathbf{C}$ unless stated otherwise.

3.1. Let E_1 and E_2 be isogenous elliptic curves.
   a. Show that there exists lattices L_i such that $L_1 \subset L_2$ and $E_i \cong \mathbf{C}/L_i$ $(i = 1, 2)$.
   b. Deduce that $\mathrm{Hom}(E_1, E_2) \cong \mathbf{Z}$ unless E_1 and E_2 have complex multiplication by an order in the same quadratic field.

3.2. Let $\mathcal{O}$ be an order in an imaginary quadratic field. Show that there is a bijection between the class group $Cl(\mathcal{O})$ and the set of elliptic curves E (up to isomorphism) having $\mathrm{End}(E) \cong \mathcal{O}$.

3.3. Prove: if E and E' are defined over a field K of characteristic 0 and they are isomorphic as elliptic curves over the algebraic closure $\bar{K}$, then they are already isomorphic as elliptic curves over an extension of degree at most 6 of K. Show that degree 2 suffices if $\mathrm{End}(E) \cong \mathbf{Z}$.
[Hint: reduce to the case $K \subset \mathbf{C}$. This reduction is known as the *Lefschetz principle*.]

3.4. Show that the degree map $\mathrm{End}(E) \to \mathbf{Z}$ coincides with the norm map $N : \mathcal{O} \to \mathbf{Z}$ if E has complex multiplication with the imaginary quadratic order $\mathcal{O}$. Show also that an isogeny $E \to E'$ of elliptic curves of degree N gives rise to a function field extension $K(E') \subset K(E)$ of degree N.
[Hint: adapt the proof of theorem 3.7 to show that the x-coordinate on E is a rational function R in the x-coordinate on E', where R has numerator and denominator of degree N and $N - 1$.]

3.5. *(Dual isogenies.)* Let $f : E_1 \to E_2$ be an isogeny of elliptic curves. Show that there exists an isogeny $\hat{f} : E_2 \to E_1$ such that $\hat{f} \circ f \in \mathrm{End}(E)$ is the map given by multiplication by the degree $\deg f$.

3.6. Show that every morphism $f : E \to E'$ between elliptic curves (in the sense of algebraic geometry) is of the form $f(P) = g(P) + A$ with g an isogeny and $A \in E'$ a point depending only on f.

3.7. Show that every non-constant solution to the differential equation $(y')^2 = 4y^3 - g_2 y - g_3$ with $g_2^3 - 27g_3^2 \neq 0$ is given by $y(z) = \wp_\Lambda(z + a)$ with $a \in \mathbf{C}$ a constant and Λ the lattice with $g_i(\Lambda) = g_i$ $(i = 2, 3)$. Which are the constant solutions? What are the solutions if $g_2^3 - 27g_3^2 = 0$?
[Hint: in the singular case one has to distinguish $g_2 = g_3 = 0$ and $g_2 g_3 \neq 0$. Look at exercise 2.3.]

3.8. *(Division polynomials.)* Let $\wp$ be the Weierstrass $\wp$-function on a torus $T = \mathbf{C}/\Lambda$.
   a. Let $n \in \mathbf{Z}_{>1}$ be an integer. Show that $\wp(nz) - \wp(z)$ has n^2 double poles, located at the n-torsion points of T, and $2n^2$ simple zeroes, located at the $(n + 1)$-torsion points and $(n - 1)$-torsion points different from 0.
   b. Prove that there exists an elliptic function ψ_n for each $n \geq 1$ that has polar part nz^{1-n^2} in the Laurent series around $z = 0$ and satisfies

$$\psi_n(z)^2 = n^2 \prod_{\substack{nw=0 \in T \\ w \neq 0}} (\wp(z) - \wp(w)).$$

Deduce that

$$\wp(nz) = \wp(z) - \frac{\psi_{n+1}(z)\psi_{n-1}(z)}{\psi_n(z)^2}.$$

[Hint: the factors w and $-w$ give the same contribution to the product for ψ_n^2. If n is even, the factors with $w = -w \in T$ can be combined to yield $(\wp')^2$.]

c. Prove that there exist polynomials $\Psi_n(X) \in \mathbf{C}[X]$ of degree $\frac{1}{2}(n^2-1)$ (n odd) or $\frac{1}{2}(n^2-4)$ (n even) and with highest coefficient n (n odd) or $-n/2$ (n even) such that

$$\psi_n = \begin{cases} \Psi(\wp) & \text{if } n \text{ is odd;} \\ \wp'\Psi_n(\wp) & \text{if } n \text{ is even.} \end{cases}$$

Conclude that

$$\begin{aligned} \wp(nz) - \wp(z) &= -\frac{\Psi_{n+1}(\wp)\Psi_{n-1}(\wp)}{(\wp')^2\Psi_n(\wp)^2} && \text{if } n \text{ is odd;} \\ &= -\frac{(\wp')^2\Psi_{n+1}(\wp)\Psi_{n-1}(\wp)}{\Psi_n(\wp)^2} && \text{if } n \text{ is even.} \end{aligned}$$

d. Show that a point $P = (x, y)$ on the curve E_Λ with $2P \neq 0$ satisfies $nP = O$ if and only if $\Psi_n(x) = 0$.

3.9. *(Computation of division polynomials.)*

a. Show that the first few division polynomials are

$$\Psi_1 = 1 \qquad \Psi_2 = -1 \qquad \Psi_3 = 3X^4 - \tfrac{3}{2}g_2X^2 - 3g_3X - \tfrac{1}{16}g_2^2$$
$$\Psi_4 = -2X^6 + \tfrac{5}{2}g_2X^4 + 10g_3X^3 + \tfrac{5}{8}g_2^2X^2 + \tfrac{1}{2}g_2g_3X + g_3^2 - \tfrac{1}{32}g_2^3.$$

Take $\psi_0 = 0 = \Psi_0$.

b. Show that $\psi_{m+n}\psi_{m-n} = \psi_{m+1}\psi_{m-1}\psi_n^2 - \psi_{n+1}\psi_{n-1}\psi_m^2$ for $m \geq n > 0$.
[Hint: look at solutions of $\wp(mz) = \wp(nz)$.]

c. Set $f = 4X^3 - g_2X - g_3 \in \mathbf{C}[X]$ and derive the recursion formulas for the division polynomials:

$$\begin{aligned} \Psi_{2n+1} &= f^2\Psi_{n+2}\Psi_n^3 - \Psi_{n+1}\Psi_{n-1} && n \text{ even} \\ &= \Psi_{n+2}\Psi_n^3 - f^2\Psi_{n+1}\Psi_{n-1} && n \text{ odd} \\ \Psi_{2n} &= -\Psi_n(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n+1}^2\Psi_{n-2}). \end{aligned}$$

Conclude that the polynomials Ψ_n are universal polynomials in $\mathbf{Q}(g_2, g_3)[X]$.
[Hint: use b with (m, n) equal to $(n+1, n)$ and $(n+1, n-1)$ to find analogous formulae for the functions ψ_n first.]

3.10. Let E be an elliptic curve over an algebraically closed field of characteristic $p > 3$. Show that the n-torsion subgroup $E[n]$ of E is not an abelian group of type $n \times n$ if $p|n$.

3.11. Show that $j(\frac{1+\sqrt{-7}}{2}) = (-15)^3 = -3375$.

4. MODULAR FUNCTIONS

In the previous section, we showed that the isomorphism class of an elliptic curve E_Λ for a lattice $\Lambda \subset \mathbf{C}$ is determined by the j-invariant $j(\Lambda) = 1728 g_2(\Lambda)^3/(g_2(\Lambda)^3 - 27g_3(\Lambda)^2)$. As a function on the upper half plane $\mathcal{H} \subset \mathbf{C}$, the j-function is invariant under the action of $\Gamma = SL_2(\mathbf{Z})$, so it has a Fourier expansion in terms of $q = e^{2\pi i z}$.

4.1. Theorem. *The j-function is a holomorphic Γ-invariant function on $\mathcal{H}$ that induces a bijection $j : \Gamma\backslash\mathcal{H} \xrightarrow{\sim} \mathbf{C}$. As a function of $q = e^{2\pi i z}$, it has a pole of order 1 with residue 1 at $q = 0$ and an integral Laurent expansion*

$$j(q) = q^{-1} + R(q) \qquad \textit{with } R(q) \in \mathbf{Z}[[q]].$$

Proof. One first derives the Fourier expansions

$$G_{2k} = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n$$

for the Eisenstein series G_4 and G_6. Using the values $\zeta(4) = \pi^4/90$ and $\zeta(6) = \pi^6/945$ and the observation that $\sigma_3(n) \equiv \sigma_5(n) \bmod 12$ for all n, is it not hard to show that the discriminant function $\Delta = g_2^3 - 27g_3^2$ has a q-expansion of the form

$$\Delta(q) = (2\pi)^{12} q(1 + \textstyle\sum_{n\geq 1} c_n q^n) \qquad (c_n \in \mathbf{Z}).$$

(Alternatively, one can derive the product expansion $\Delta(q) = (2\pi)^{12}\prod_{n\geq 1}(1-q^n)^{24}$.) One has $1728 g_2^3 = (2\pi)^{12}(1 + \sum_{n\geq 1} d_n q^n)$ with $d_n \in \mathbf{Z}$, so the quotient $j = 1728 g_2^3/\Delta$ has a q-expansion of the required sort. Working out a few coefficients, one finds

$$R(q) = 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 + 333202640600q^5 + \ldots.$$

We saw in the previous section that the map $j : \Gamma\backslash\mathcal{H} \to \mathbf{C}$ is injective. As the image is both open and closed, it is also surjective. □

The preceding theorem 'explains' the normalizing factor 1728. It also shows that every complex number is the j-invariant of an elliptic curve, which completes the proof of the uniformization theorem 3.2.

It can be shown that the factor space $\Gamma\backslash\mathcal{H}$ inherits a natural structure of a Riemann surface from $\mathcal{H}$, and that the j-function is a complex analytic isomorphism between $\Gamma\backslash\mathcal{H}$ and $\mathbf{C}$. Thus $\Gamma\backslash\mathcal{H}$ is an algebraic curve isomorphic to the affine line $\mathbb{A}^1(\mathbf{C})$. It can be made into a complete projective curve isomorphic to $\mathbb{P}^1(\mathbf{C})$ by adding a point ∞ 'at infinity' corresponding to $q = 0$ under the exponential map $q = e^{2\pi i z}$.

A *modular function* f is a Γ-invariant meromorphic function on $\mathcal{H}$ that is meromorphic at infinity. The last condition means that the Fourier series $f(q) = \sum_{k\in\mathbf{Z}} a_k q^k$ is meromorphic at $q = 0$. From the point of view given above, modular functions are simply meromorphic functions on the complete Riemann surface $\Gamma\backslash\mathcal{H} \cup \{\infty\} \cong \mathbb{P}^1(\mathbf{C})$, and this explains the following theorem.

4.2. Theorem. *The field of modular functions consists of the rational functions in j.*

Proof. A modular function only has finitely many poles in $\Gamma\backslash\mathcal{H}$, so it becomes holomorphic on $\mathcal{H}$ after multiplication by a suitable polynomial in j. As j has a simple pole at ∞, one can now subtract a polynomial in j from the function obtained to make it holomorphic at ∞ as well. As a function that is holomorphic on $\mathcal{H} \cup \{\infty\}$ is constant, we are done. □

From the preceding proof one obtains the following important *q-expansion principle*: every holomorphic modular function f is a polynomial in j, and the coefficients of this polynomial are in the additive subgroup of $\mathbf{C}$ that is generated by the Fourier coefficients of f.

In order to obtain a richer collection of modular functions than only those in $\mathbf{C}(j)$, we will now consider modular functions of higher level. A function f is said to be *modular of level* $n > 1$ if, first of all, it is meromorphic on $\mathcal{H}$ and invariant for a subgroup $G \subset \Gamma$ containing the subgroup $\Gamma(n) = \ker[SL_2(\mathbf{Z}) \to SL_2(\mathbf{Z}/n\mathbf{Z})]$. Moreover, one requires that for each $\gamma \in \Gamma$, the Fourier expansion of $f(\gamma z)$ in $\mathbf{C}((q^{1/n}))$ has a pole of finite order at $q^{1/n} = 0$. If f is modular of level n, then so is $f \circ \gamma$ for every $\gamma \in \Gamma$. Indeed, for $\sigma \in \Gamma(n)$ and $\gamma \in \Gamma$ we have $\gamma\sigma\gamma^{-1} \in \Gamma(n)$ by normality and therefore

$$f \circ \gamma(\sigma z) = (f \circ \gamma\sigma\gamma^{-1})(\gamma z) = f \circ \gamma(z).$$

Thus Γ operates as a group of automorphisms on the field $\mathcal{F}_n$ of modular functions of level n. The subfield $\mathcal{F}_1 = \mathbf{C}(j)$ is invariant under Γ.

If f is modular of level n for a subgroup $G \supset \Gamma(n)$, then the Γ-orbit of f is finite and consists of the functions $f \circ \tau$ with τ ranging over a set of representatives of the right cosets of G in Γ. These functions are transitively permuted by Γ, and the polynomial $\prod(X - f \circ \tau)$ is in $\mathbf{C}(j)$ as its coefficients, being symmetric expressions in the functions $f \circ \tau$, are Γ-modular functions. It follows that $\mathcal{F}_n/\mathcal{F}_1$ is a normal algebraic extension on which $\Gamma/\Gamma(n)$ acts as a group of automorphisms with fixed field $\mathcal{F}_1$. Before we proceed to give generators for the extension and an explicit description of $\mathrm{Gal}(\mathcal{F}_n/\mathcal{F}_1)$, we study two modular functions of level n in some detail. The irreducible equations of these functions have coefficients in $\mathbf{Z}[j]$ and will be used in the next section to prove algebraicity and integrality statements for special values of the j-function itself. Their reduction modulo primes p will also play a key role.

For $n \in \mathbf{Z}_{>0}$, consider the function $j(nz) = (j \circ \sigma_n)(z)$ with $\sigma_n = \left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right)$. This is a modular function of level n for the congruence subgroup

$$\Gamma_0(n) = \sigma_n^{-1}\Gamma\sigma_n \cap \Gamma = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : \ c \equiv 0 \bmod n\}.$$

Let Δ_n be the set of primitive integral matrices of determinant n. If $\Lambda' \subset \Lambda$ are two lattices in $\mathbf{C}$, then Λ/Λ' is cyclic of order n if and only if $\Lambda' = \alpha\Lambda$ for some $\alpha \in \Delta_n$. By the elementary divisor theorem, this implies that $\Delta_n = \Gamma\sigma_n\Gamma$ with $\sigma_n = \left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

4.3. Lemma. *Define the finite set $A_n \subset \Delta_n$ by*

$$A_n = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Delta_n : \ 0 \le b < d\}.$$

(i) *The set Δ_n is a disjoint union of Γ-cosets $\Delta_n = \cup_{\alpha \in A_n} \Gamma\alpha$ that are transitivily permuted under the natural right action of Γ.*

(ii) *The elements of A_n correspond to the right cosets of $\Gamma_0(n)$ in Γ under $\sigma \mapsto \sigma_n^{-1}\Gamma\sigma \cap \Gamma$.*

It is shown in the exercises that the order $\psi(n) = [\Gamma : \Gamma_0(n)]$ of A_n is a multiplicative function given by

$$\psi(n) = n \cdot \prod\nolimits_{p|n} (1 + p^{-1}).$$

If $n = p$ is prime, one has $A_p = \{\sigma_i\}_{i=0}^{p}$ with $\sigma_i = \left(\begin{smallmatrix} 1 & i \\ 0 & p \end{smallmatrix}\right)$ for $0 \le i \le p-1$ and $\sigma_p = \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

The functions $j \circ \sigma$ for $\sigma \in A_n$ are transitively permuted under the right action of Γ and form the Γ-orbit of the function $j(nz)$. Thus, the coefficients of the n-th modular polynomial

$$\Phi_n(X) = \Phi_n(X, j) = \prod_{\sigma \in A_n} (X - j \circ \sigma)$$

are holomorphic modular functions in $\mathbf{C}[j]$. Fixing a root of unity $\zeta_n = e^{2\pi i/n} \in \mathbf{C}$, one has $\exp(2\pi i \frac{az+b}{d}) = \zeta_n^{ab} q^{a/d} = \zeta_d^b q^{a^2/n}$ and for each $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in A_n$ a meromorphic q-expansion

$$(j \circ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix})(q) = \zeta_d^{-b} q^{-a^2/n} + R(\zeta_d^b q^{a^2/n}) \in \mathbf{Z}[\zeta_n]((q^{1/n})).$$

By the q-expansion principle, the coefficients of $\Phi_n(X)$ are in $\mathbf{Z}[\zeta_n, j]$. Performing an automorphism $\zeta_n \to \zeta_n^r$ on the coefficients of their q-expansion transforms $(j \circ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right))(q)$ into $(j \circ \left(\begin{smallmatrix} a & rb \\ 0 & d \end{smallmatrix}\right))(q)$. It follows that Φ_n is in $\mathbf{Z}[X, j]$. It has the following properties.

4.4. Theorem. *For every integer $n \in \mathbf{Z}_{>1}$ the following holds.*

(i) *$\Phi_n(X, j)$ is the irreducible polynomial of $j \circ \sigma_n$ over $\mathbf{C}(j)$;*

(ii) *$\Phi_n(X, j) = \Phi_n(j, X) \in \mathbf{Z}[X, j]$;*

(iii) *$\Phi_n(j, j) \in \mathbf{Z}[j]$ has highest coefficient ± 1 when n is not a square;*

(iv) *$\Phi_p(X, j) \equiv (X - j^p)(X^p - j) \bmod p\mathbf{Z}[X, j]$ if p is prime.*

Proof. The irreducibility of $\Phi_n(X)$ follows from the fact that its zeroes are distinct and conjugate over $\mathbf{C}(j)$.

As the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix}\right)$ is in A_n, one has $\Phi_n(j(z/n), j(z)) = 0$ for all z, so $\Phi_n(j, X)$ has a root $j(nz)$ and is therefore divisible by $\Phi_n(X, j)$. The quotient $g(X, j)$ is in $\mathbf{C}[j, X]$ by Gauss's lemma and satisfies $g(X, j)g(j, X) = 1$, so its equals ± 1. The possibility -1 only occurs when $\Phi_n(j, j) = 0$, i.e. for $n = 1$.

If n is not a square, the polar terms q^{-1} and $\zeta_d^{-b}q^{-a^2/n}$ in $j - j \circ \binom{a\,b}{0\,d}$ do not cancel for any $\binom{a\,b}{0\,d} \in A_n$, so the highest coefficient of $\Phi_n(j,j)$, which is the lowest coefficient of the q-expansion of $\prod_\alpha (j - j\circ\alpha)$, must be a root of unity in $\mathbf{Z}$.

For the Kronecker congruence (iv) one observes that the q-expansions of the zeroes $j \circ \sigma_i$ $(0 \le i \le p)$ of $\Phi_p(X)$ satisfy

$$\begin{aligned}(j\circ\sigma_p)(q) &= j(q^p) \equiv j(q)^p \bmod p\mathbf{Z}((q))\\ (j\circ\sigma_i)(q) &= j(\zeta_p^i q^{1/p}) \equiv j(q^{1/p}) \bmod (1-\zeta_p)\mathbf{Z}[\zeta_p]((q^{1/p})) \qquad (0 \le i < p).\end{aligned}$$

It follows that the coefficients of the polynomial $\Phi_n(X) - (X - j^p)(X^p - j)$ are holomorphic modular functions with q-expansions in $(1-\zeta_p)\mathbf{Z}[\zeta_p]((q^{1/p})) \cap \mathbf{Z}((q)) = p\mathbf{Z}((q))$. By the q-expansion principle, they are in $p\mathbf{Z}[j]$. □

A similar treatment can be given to the $\Gamma_0(n)$-modular function

$$\phi_n(z) = n^{12}\frac{\Delta(nz)}{\Delta(z)}.$$

This is again a $\Gamma_0(n)$-modular function, as is easily verified. Under the action of Γ, the orbit of Γ consists of the functions

$$\phi_\sigma(z) = n^{12}\frac{(\Delta\circ\sigma)([z,1])}{\Delta(z)}$$

with $\sigma \in A_n$. For $\sigma = \binom{a\,b}{0\,d}$ one has $\phi_\sigma(z) = a^{12}\Delta(\sigma z)/\Delta(z)$. As for $j(nz)$, one can define a polynomial

$$\Psi_n(X) = \prod_{\sigma\in A_n}(X - \phi_\sigma) \in \mathbf{Z}[X,j].$$

Its constant coefficient has a simple form if n is prime.

4.5. Lemma. *For p a prime number the product $\prod_{\sigma\in A_p}\phi_\sigma(z)$ is constant and equals $(-1)^{p-1}p^{12}$.*

Proof. The product is a polynomial in j whose q-expansion begins with the constant term $p^{12}\prod_{i=0}^{p-1}\zeta_p^i = (-1)^{p-1}p^{12}$. □

There is the following congruence property for the ϕ-functions. It will be used in the next section.

4.6. Lemma. *Define for p a prime number and $A_p = \{\sigma_i\}_{i=0}^p$ the polynomial*

$$F(X,Y) = \sum_{i=0}^{p}(X - j\circ\sigma_i)\prod_{j\ne i}(Y - \phi_{\sigma_j}).$$

Then $F(X,Y)$ is in $\mathbf{Z}[X,Y,j]$ and one has the congruence

$$F(j^p, Y, j) \equiv 0 \bmod p\mathbf{Z}[Y,j].$$

Proof. The proof is analogous to that for the Kronecker congruence for Φ_p and deduces the congruence from the corresponding congruence for the q-expansions. □

In order to find generators for the full modular field $\mathcal{F}_N$, we use the Weber function from section 3. When defined with a proper normalizing factor as

$$h_{[1,\tau]}(w) = -2^7 3^5 \frac{g_2(\tau)g_3(\tau)}{\Delta(\tau)} \wp_{[1,\tau]}(w),$$

it has an integral expansion in terms of $q = e^{2\pi i\tau}$ and $q_w = e^{2\pi iw}$, which is given by

$$h_{[1,\tau]}(w) = P(q)\left[1 + 12\sum_{k=1}^{\infty} kq_w^k + 12\sum_{k,l=1}^{\infty} kq^{kl}(q_w^k + q_w^{-k} - 2)\right]$$

for some power series $P(q) \in q + q^2\mathbf{Z}[[q]]$. We consider $h_{[1,\tau]}(w)$ as a function of τ and evaluate it for w a torsion point of the lattice $[1,\tau]$. Thus, for $t = (t_1, t_2)$ a non-zero element of $\mathbf{Q}^2/\mathbf{Z}^2$, the *Fricke function* f_t is defined as

$$f_t(\tau) = h_{[1,\tau]}(t_1\tau + t_2).$$

If t has order n in $\mathbf{Q}^2/\mathbf{Z}^2$, then f_t is said to be primitive of level n. The natural right action of Γ on the Fricke functions is as follows.

4.7. Lemma. *For $\gamma \in \Gamma$ and $t \in \mathbf{Q}^2/\mathbf{Z}^2$ non-zero one has $f_t(\gamma\tau) = f_{t\gamma}(\tau)$.*

Proof. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ the homogeneity property $\wp_{k^{-1}\Lambda}(k^{-1}z) = k^{-2}\wp_\Lambda(z)$ of the $\wp$-function yields

$$\begin{aligned} f_t(\frac{a\tau+b}{c\tau+d}) &= -2^7 3^5 (c\tau+d)^{-2} \frac{g_2(\tau)g_3(\tau)}{\Delta(\tau)} \wp_{(c\tau+d)^{-1}[1,\tau]}((c\tau+d)^{-1}(t_1(a\tau+b) + t_2(c\tau+d))) \\ &= f_{t\gamma}(\tau). \end{aligned}$$

□

By the lemma, all Fricke functions of level n are $\Gamma(n)$-invariant. An inspection of the q-expansion of $f_a = h_q(e^{2\pi a_2 i}q^{a_1})$ shows that the Fricke functions of level n are modular functions of level n.

4.8. Theorem. *The Fricke functions f_t, with t ranging over the n-torsion elements in $\mathbf{Q}^2/\mathbf{Z}^2$, generate $\mathcal{F}_n$ over $\mathcal{F}_1 = \mathbf{C}(j)$. The natural action of Γ on $\mathcal{F}_n$ induces an isomorphism*

$$\mathrm{Gal}(\mathcal{F}_n/\mathcal{F}_1) \cong SL_2(\mathbf{Z}/n\mathbf{Z})/\{\pm 1\}.$$

Proof. An element $\gamma \in \Gamma$ that acts as the identity on $\mathcal{F}_n$ must fix $f_{1/n,0}$ and $f_{0,1/n}$. As $f_t = f_u$ if and only if $t = \pm u \in \mathbf{Q}^2/\mathbf{Z}^2$, this implies that $\gamma = \pm 1 \bmod \Gamma_0(n)$. It follows that the group $\Gamma/\pm\Gamma_0(n)$, which is isomorphic to $SL_2(\mathbf{Z}/n\mathbf{Z})/\{\pm 1\}$ by exercise 4.2, maps injectively into $\mathrm{Gal}(\mathcal{F}_n/\mathcal{F}_1)$. As the fixed field of the image is $\mathcal{F}_1$, we have an isomorphism. □

The Fricke functions of level n have q-expansions with coefficients in $\mathbf{Q}(\zeta_n)$, so they are algebraic over $\mathbf{Q}(j)$ and one can sharpen the preceding theorem by giving the Galois group of the modular function field F_n of level n over $\mathbf{Q}(j)$.

4.9. Theorem. *Let F_n be the extension of $\mathbf{Q}(j)$ that is generated by the Fricke functions f_t, with t ranging over the non-zero elements of $\frac{1}{n}\mathbf{Z}^2/\mathbf{Z}^2$. Then the natural action of $GL_2(\mathbf{Z}/n\mathbf{Z})$ on $\frac{1}{n}\mathbf{Z}^2/\mathbf{Z}^2$ induces an isomorphism*

$$\mathrm{Gal}(F_n/\mathbf{Q}(j)) \cong GL_2(\mathbf{Z}/n\mathbf{Z})/\{\pm 1\}.$$

The subfield corresponding to $SL_2(\mathbf{Z}/n\mathbf{Z})/\{\pm 1\}$ is $\mathbf{Q}(\zeta_n, j)$. This is the algebraic closure of $\mathbf{Q}$ in F_n, and the action of $\sigma \in GL_2(\mathbf{Z}/n\mathbf{Z})$ on a root of unity is given by $\sigma(\zeta_n) = \zeta_n^{\det\sigma}$.

Proof. We have an injection $F_n \subset \mathbf{Q}(\zeta_n, q^{1/n})$ coming from the q-expansions. Let σ_d for $d \in (\mathbf{Z}/n\mathbf{Z})^*$ be the automorphism of $\mathbf{Q}(\zeta_n, q^{1/n})$ that acts on $\mathbf{Q}(\zeta_n)$ by $\zeta_n \mapsto \zeta_n^d$ and maps $\sum_k c_k q^{k/n}$ to $\sum_k \sigma_d(c_k) q^{k/n}$. This induces an automorphism of F_n since one sees from the q-expansions that $\sigma_d(f_{(t_1,t_2)}) = f_{(t_1,dt_2)}$. It is an element of $\mathrm{Gal}(F_n/\mathbf{Q}(j))$ as σ_d is the identity on $\mathbf{Q}(j) \subset \mathbf{Q}((q))$. Obviously, σ_d is represented by the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$, and we have obtained $H_n = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) : d \in (\mathbf{Z}/n\mathbf{Z})^*\}$ as a subgroup of $\mathrm{Gal}(F_n/\mathbf{Q}(j))$.

By the previous theorem, we have an inclusion $SL_2(\mathbf{Z}/n\mathbf{Z})/\{\pm 1\} \subset \mathrm{Gal}(F_n/\mathbf{Q}(j))$, and the fixed field of this subgroup is $K(j)$, with K the algebraic closure of $\mathbf{Q}$ in F_n. From $K \subset \mathbf{Q}(\zeta_n, q^{1/n})$ we obtain $K \subset \mathbf{Q}(\zeta_n)$. As the short exact sequence

$$0 \longrightarrow SL_2(\mathbf{Z}/n\mathbf{Z})/\{\pm 1\} \longrightarrow GL_2(\mathbf{Z}/n\mathbf{Z})/\{\pm 1\} \xrightarrow{\det} (\mathbf{Z}/n\mathbf{Z})^* \longrightarrow 0$$

is split by $(\mathbf{Z}/n\mathbf{Z})^* \xrightarrow{\sim} H_n$, we have $\mathrm{Gal}(F_n/\mathbf{Q}(j)) \cong GL_2(\mathbf{Z}/n\mathbf{Z})/\{\pm 1\}$ and $K = \mathbf{Q}(\zeta_n)$ by degree considerations, and the action on the roots of unity follows is as stated. □

Now that we know the full Galois group $G_n = \mathrm{Gal}(F_n/\mathbf{Q}(j))$, it is not hard to identify the subfields corresponding to various subgroups. The function $j(nz)$ is $\Gamma_0(n)$-modular and H_n-invariant as it has a rational q-expansion. Its degree over $\mathbf{Q}(j)$ is $\psi(n)$, so we conclude that we have a Galois correspondence

$$\mathbf{Q}(j, j \circ \sigma_n) \leftrightarrow \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in G_n\}.$$

An element in this Galois group maps $f_{1/n,0}$ to $f_{a/n,b/n}$, so we find the field of modular functions in F_n with rational q-expansion to be

$$\mathbf{Q}(j, j \circ \sigma_n, f_{1/n,0}) \leftrightarrow H_n.$$

The smallest normal subgroup in $\{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in G_n\}$ consists of multiples of the identity, so we also have

$$\mathbf{Q}(j, j \circ \sigma : \sigma \in A_n) \leftrightarrow \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in G_n\} \cong (\mathbf{Z}/n\mathbf{Z})^*/\{\pm 1\}.$$

Exercises.

4.1. Let $\psi(n) = [\Gamma : \Gamma_0(n)] = \#A_n$.

a. Show that $\psi(n) = \sum_{d|n} \frac{\phi(e)}{e} d$ with $e = \gcd(n/d, d)$, and that ψ is a multiplicative function.

b. Show that $\psi(n) = n \cdot \prod_{p|n}(1 + p^{-1})$.

4.2. Let $n \in \mathbf{Z}_{>1}$. Show that the natural map $SL_k(\mathbf{Z}) \to SL_k(\mathbf{Z}/n\mathbf{Z})$ is surjective for every $k \geq 1$.
[Hint: it suffices to show that all diagonal matrices are in the image.]

4.3. Compute the order of $SL_k(\mathbf{Z}/n\mathbf{Z})$ for arbitrary k, then show that $\#SL_2(\mathbf{Z}/n\mathbf{Z}) = n\phi(n)\psi(n)$ and derive the formula for $\psi(n)$ from this.

4.4. Show that Γ acts properly discontinuous on $\mathcal{H}$, i.e. that every $z \in \mathcal{H}$ has a neighborhood U such that for every $\gamma \in \Gamma$ we have

$$\gamma U \cap U \neq \emptyset \Longleftrightarrow \gamma z = z.$$

Deduce from this that $j'(z) \neq 0$ unless z has a non-trivial isotropy group in $\bar{\Gamma} = \Gamma/\{\pm \mathrm{id}\}$, i.e. z is in the orbit of i or $\rho = e^{2\pi i/3}$. What are the orders of vanishing of $j'(z)$ at $z = i$ and $z = \rho$?

4.5. *(Picard's theorem)* Show that a non-constant entire function assumes all values in $\mathbf{C}$ with at most one exception.
[Hint: if f does not assume the values 0 and 1728, there exists a holomorphic function $g : \mathbf{C} \to \mathcal{H}$ such that $f = j \circ g$.]

4.6. Let $G \subset \Gamma$ be a subgroup of finite index k containing $\pm$ id. Denote by τ_i, $1 \leq i \leq k$, a set of representatives of right G-cosets in Γ.

a. Show that there exists an integer $t > 0$ such that every G-invariant meromorphic function f on $\mathcal{H}$ has a Fourier expansion in $\mathbf{C}(q^{1/t})$. Show also that $f \circ \gamma$ is meromorphic at infinity for all $\gamma \in \Gamma$ if and only if this is true for $\gamma = \tau_i$, $1 \leq i \leq k$.

b. Let F_G be the field of G-modular functions. Show that every $\gamma \in \Gamma$ induces an isomorphism $F_G \xrightarrow{\sim} F_{\gamma^{-1}G\gamma}$ over $\mathbf{C}(j)$, and that F_G is algebraic over $\mathbf{C}(j)$ of degree at most k.

c. Suppose that $G = \sigma^{-1}\Gamma\sigma \cap \Gamma$ for some $\sigma \in M_2^+(\mathbf{Q})$. Show that G is of finite index in Γ and that $[F_G : \mathbf{C}(j)] = [\Gamma : G]$. Find a generator of F_G over $\mathbf{C}(j)$.

4.7. Let E_1 and E_2 be elliptic curves. Prove that $\Phi_n(j(E_1), j(E_2)) = 0$ if and only there exists an isogeny $E_2 \to E_1$ of degree n with cyclic kernel.

4.8. Let $z \in \mathcal{H}$ be such that $j(z)$ is a root of the polynomial $\Phi_n(j, j) \in \mathbf{C}[j]$ for some $n > 1$. Prove that z is imaginary quadratic and that the lattice $[1, z]$ is an invertible $\mathcal{O}$-ideal for some quadratic order $\mathcal{O}$ that contains a primitive element of norm n. Show that the discriminant D of $\mathcal{O}$ satisfies $D \geq -4n$.

4.9. Show that $\mathcal{F}_2$ is generated over $\mathbf{C}(j)$ by $j(2z)$ and $j(z/2)$, and that $\mathrm{Gal}(\mathcal{F}_2/\mathbf{C}(j))$ is isomorphic to S_3.

4.10. Compute the Galois group of $\mathcal{F}_n$ over the normal closure of $\mathbf{C}(j, j \circ \sigma_n)$ over $\mathbf{C}(j)$.

4.11. (This exercise requires administrative skills or a computer algebra package.) Show that the coefficients of the modular polynomial $\Phi_2(X, j) = \sum_{k=0}^{3} a_i X^i$ are given by $a_3 = 1$ and

$$\begin{aligned} a_2 &= -j^2 + 1488j - 162000 \\ a_1 &= 1488j^2 + 40773375j + 8748000000 \\ a_0 &= j^3 - 162000j^2 + 8748000000j - 157464000000000, \end{aligned}$$

such that one has

$$\begin{aligned} \Phi_2(x, j) = & x^3 + j^3 - x^2j^2 + 1488(x^2j + xj^2) - 162000(x^2 + j^2) \\ & + 40773375xj + 8748000000(x + j) - 157464000000000. \end{aligned}$$

Check that $\Phi_2(j, j) = -j^4 + 2978j^3 + 40449375j^2 + 17496000000j - 157464000000000$ factors as

$$\Phi_2(j, j) = -(j - 8000)(j - 1728)(j + 3375)^2$$

and interpret the zeroes.

4.12. Show that $\mathbf{Q}(j, j \circ \sigma_n) = \mathbf{Q}(j, \phi_n)$ with $\phi_n(z) = n^{12}\Delta(nz)/\Delta(z)$.

4.13. Show that $\cup_k \mathcal{F}_{p^k}$ is a Galois extension of $\mathbf{C}(j)$ with group $SL_2(\mathbf{Z}_p)/\{\pm 1\}$. What is the Galois group of $\mathcal{F} = \cup_n \mathcal{F}_n$ over $\mathbf{C}(j)$? What are the corresponding statements over $\mathbf{Q}(j)$ for the fields F_n?

4.14. Let E be an elliptic curve with transcendental j-invariant j_E, defined over $\mathbf{Q}(j_E)$. Let $K = \mathbf{Q}(j_E, E[n])$ be the extension obtained by adjoining the coordinates of all n-torsion points of E to $\mathbf{Q}(j_E)$.

a. Show that K is a finite normal extension of $\mathbf{Q}(j_E)$.

b. Show that every automorphism τ of $\mathbf{C}$ over $\mathbf{Q}(j_E)$ yields an automorphism of the group $E[n] \cong (\mathbf{Z}/n\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z})$, and that this defines a homomorphism $G(\mathbf{Q}(j_E)) \to GL_2(\mathbf{Z}/n\mathbf{Z})$ on the absolute Galois group $G(\mathbf{Q}(j_E))$ of $\mathbf{Q}(j_E)$.

c. Show that the homomorphism in b is surjective and induces an isomorphism

$$\mathrm{Gal}(K/\mathbf{Q}(j_E)) \xrightarrow{\sim} GL_2(\mathbf{Z}/n\mathbf{Z})$$

for the field of n-torsion points. Show also that $\mathbf{Q}(\zeta_n)$ is the algebraic closure of $\mathbf{Q}$ in K, and that the action of of $\sigma \in \mathrm{Gal}(K/\mathbf{Q}(j_E))$ on $\mathbf{Q}(\zeta_n)$ is given by $\sigma(\zeta_n) = \zeta_n^{\det \sigma}$.

4.15. *(Weil pairing.)* For an elliptic function f and a divisor $D = \sum_{w \in T} n_w \cdot (w) \in \mathrm{Div}(T)$ on the complex torus T, we let $f(D) = \prod_w f(w)^{n_w} \in \mathbf{C}$ as in exercise 2.8. If D_1 and D_2 are divisors without common points such that $n \cdot D_i = (f_i)$, we define

$$\langle D_1, D_2 \rangle = \frac{f_1(D_2)}{f_2(D_1)}.$$

a. Show that $\langle D_1, D_2\rangle$ only depends on the equivalence class of D_1 and D_2 in $\mathrm{Div}(T)/\mathfrak{M}^*_\Lambda$, and that a skew-symmetric pairing

$$E_\Lambda[n] \times E_\Lambda[n] \longrightarrow \langle \zeta_n \rangle$$

is induced on the n-torsion points of E_Λ.

b. Let $[\omega_1, \omega_2]$ be an oriented basis for Λ, and denote by P_1 and P_2 the torsion points on E_Λ coming from ω_1/n and ω_2/n. Show that $\langle P_1, P_2\rangle = e^{-2\pi i/n}$ and deduce that the pairing is non-degenerate.
[Hint: use the Legendre relation.]

c. Let $\sigma \in GL_2(\mathbf{Z}/n\mathbf{Z})$ act in the natural way on $E_\Lambda[n] = (\mathbf{Z}/n\mathbf{Z}) \cdot P_1 \oplus (\mathbf{Z}/n\mathbf{Z}) \cdot P_2$. Show that $\langle \sigma P_1, \sigma P_2\rangle = \langle P_1, P_2\rangle^{\det \sigma}$ and use this to give an alternative proof for the last statement of the previous exercise.

4.16. *(Weil pairing again.)* Let E be an elliptic curve defined over $K = \mathbf{Q}(j_E)$ and $n > 1$ an integer. Let $T \in E[n]$ be a point of order n and $T' \in E$ a point satisfying $nT' = T$.

a. Show that there exist $f, g \in \overline{K}(E)$ with divisors $\mathrm{div}(f) = n((T) - (0))$ and $\mathrm{div}(g) = \sum_{P \in E[n]}((T' + P) - (P))$ such that $f(nx) = (g(x))^n$. Deduce that $e(S,T) = g(x + S)/g(x)$ is an n-th root of unity for every point $S \in E[n]$.

b. Show that $(S,T) \mapsto e(S,T)$ is a skew-symmetric pairing

$$E_\Lambda[n] \times E_\Lambda[n] \longrightarrow \langle \zeta_n \rangle$$

that is Galois equivariant, i.e. $e(\sigma S, \sigma T) = \sigma e(S,T)$ for all σ in the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$ of K. What is the relation with the previous exercise?
[Hint: in order to obtain $e(T,T) = 1$, observe that the functions $\prod_{i=0}^{n-1} f(x - iT)$ and $\prod_{i=0}^{n-1} g(x - iT')$ are constant, so $g(x) = g(x - T)$. If $g(x + S) = g(x)$ for all $S \in E[n]$, then $g(x) = h(nx)$ and $T = 0$.]

5. COMPLEX MULTIPLICATION

In this section we will use modular functions to generate class fields of imaginary quadratic fields. The proofs we give here are the classical proofs based on the congruences for modular polynomials derived in the previous section by analytical means, i.e. in terms of Fourier expansions.

An element $\tau \in \mathcal{H}$ for which $\mathbf{Q}(\tau)$ is imaginary quadratic is called a *singular modulus*. The singular moduli are exactly those elements $\tau \in \mathcal{H}$ for which the corresponding lattice $[1, \tau]$ has *complex multiplication*.

5.1. Lemma. *Let τ be a singular modulus and $\sigma \in \Delta_n$ a primitive matrix of determinant n. Then $j(\tau)$ and $\phi_\sigma(\tau)$ are algebraic integers, and $\phi_\sigma(\tau)$ divides n^{12}.*

Proof. If τ is an integral element of $K = \mathbf{Q}(\tau)$, the lattice $[1, \tau]$ is an order $\mathcal{O}$ of index f in the ring of integers $\mathcal{O}_K = [1, w_K]$ of K. The element $\alpha = f w_K \in \mathcal{O}$ is primitive, and its norm n is not a perfect square in $\mathbf{Z}$ if we choose w_K appropriately. As $\alpha\mathcal{O}$ is a cyclic sublattice of $\mathcal{O}$ of index n, we have $0 = \Phi_n(j(\alpha\mathcal{O}), j(\mathcal{O})) = \Phi_n(j(\mathcal{O}), j(\mathcal{O}))$, so $j(\tau) = j(\mathcal{O})$ is the root of a monic polynomial in $\mathbf{Z}[X]$ by 4.4. For the general case, one can choose an integer $k > 0$ such that $k\tau$ is integral. The relation $\Phi_k(j(\tau), j(k\tau)) = 0$ shows that $j(\tau)$ is integral over $\mathbf{Z}[j(k\tau)]$, whence over $\mathbf{Z}$.

Integrality of $\phi_\sigma(\tau)$ is immediate from the integrality of ϕ_n and its conjugates ϕ_σ over $\mathbf{Z}[j]$ proved in the previous section. If σ has determinant n, there exists $\sigma' \in \Delta_n$ such that $\sigma'\sigma = \left(\begin{smallmatrix} n & 0 \\ 0 & n \end{smallmatrix}\right)$, and the product of algebraic integers $\phi_{\sigma'}(\sigma\binom{\tau}{1}) \cdot \phi_\sigma(\tau)$ equals n^{12} as $\Delta(z)$ is homogeneous of degree -12. □

If $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal for some imaginary quadratic order $\mathcal{O}$ and $\mathfrak{b} \subset \mathcal{O}$ is an invertible ideal such that $\mathcal{O}/\mathfrak{b}$ is cyclic of order $b = N\mathfrak{b}$, there exists a matrix $B \in \Delta_b$ such that $\mathfrak{b}\mathfrak{a} = B(\mathfrak{a})$. In this situation, we write $\phi_\mathfrak{b}(\mathfrak{a}) = \phi_B(\mathfrak{a}) = b^{12}\Delta(\mathfrak{b}\mathfrak{a})/\Delta(\mathfrak{a})$. The notation $x \approx \mathfrak{b}$ means that the algebraic number x generates the ideal $\mathfrak{b}\mathcal{O}_M$ in some large number field M containing x and the $\mathcal{O}$-ideal $\mathfrak{b}$.

5.2. Lemma. *Let p be a prime number that does not divide the discriminant of the imaginary quadratic order $\mathcal{O}$, and suppose that p splits in $\mathcal{O}$ as $p\mathcal{O} = \mathfrak{p}\mathfrak{p}'$. Let $\mathfrak{a}$ be an invertible $\mathcal{O}$-ideal. Then we have $\phi_\mathfrak{p}(\mathfrak{a}) \approx \mathfrak{p}'^{12}$ and $\phi_{\mathfrak{p}'}(\mathfrak{a}) \approx \mathfrak{p}^{12}$, and $\phi_\sigma(\mathfrak{a})$ is a unit for each $\sigma \in \Delta_p$ satisfying $\sigma(\mathfrak{a}) \neq \mathfrak{p}\mathfrak{a}, \mathfrak{p}'\mathfrak{a}$.*

Proof. Choose an ideal $\mathfrak{b}$ of index b prime to p such that $\mathfrak{b}\mathfrak{p} = \lambda\mathcal{O}$ is principal. We have $\mathfrak{p} \neq \mathfrak{p}'$, and using the preceding lemma to compare the p-parts in both sides of the equality

$$\phi_\mathfrak{b}(\mathfrak{p}\mathfrak{a})\phi_\mathfrak{p}(\mathfrak{a}) = b^{12}p^{12}\lambda^{-12}$$

we obtain $\phi_\mathfrak{p}(\mathfrak{a}) \approx \mathfrak{p}'^{12}$. The result for $\phi_{\mathfrak{p}'}$ follows by symmetry, and the statement on units follows from the product relation in 4.5. □

A complete algebraic characterization of the j-invariants of singular moduli is given by the *first main theorem of complex multiplication*. It shows that the invariant of a singular modulus τ generates an abelian extension of $\mathbf{Q}(\tau)$, and that the Galois action can be given in terms of the multiplicator ring $\mathcal{O}_\tau$ of the lattice $[1, \tau]$. The theorem presupposes knowledge of class field theory for imaginary quadratic fields. In the proof, we will use the fact that an extension L/K of number fields is characterized by the set $S_{L/K}$ of primes of K that split completely in L. More precisely, if L and M are finite extensions of a number field K and the symmetric difference of $S_{L/K}$ and $S_{M/K}$ is a set of primes of K of Dirichlet density zero, then $L = M$.

5.3. Theorem. *Let τ be a singular modulus with multiplicator ring $\mathcal{O} = \mathcal{O}_\tau$. Then $j(\tau)$ generates the ring class field corresponding to the order $\mathcal{O}$ over $K = \mathbf{Q}(\tau)$. The class equation*

$$f_{\mathcal{O}} = \prod_{[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})} (X - j(\mathfrak{a})) \in \mathbf{Z}[X]$$

of $\mathcal{O}$ is the irreducible equation of $j(\tau)$ over K. There is the Artin isomorphism

$$\mathrm{Cl}(\mathcal{O}) \xrightarrow{\sim} \mathrm{Gal}(K(j(\tau))/K)$$

that maps every prime $\mathfrak{p} \subset \mathcal{O}$ that is coprime to the conductor of $\mathcal{O}$ to the Artin symbol $\sigma_\mathfrak{p} \in \mathrm{Gal}(K(j(\tau))/K)$, and if $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal one has

$$\sigma_\mathfrak{p}(j(\mathfrak{a})) = j(\mathfrak{p}^{-1}\mathfrak{a})$$

for almost all primes $\mathfrak{p} \subset \mathcal{O}$.

The numbers $j(\mathfrak{a})$ are known as the *class invariants* of the order $\mathcal{O}$.

5.4. Corollary. *If K is an imaginary quadratic field with ring of integers $\mathcal{O}_K$ and $\mathfrak{a}$ is any fractional $\mathcal{O}_K$-ideal, then $K(j(\mathfrak{a}))$ is the Hilbert class field of K. The element $j(\mathfrak{a})$ only depends on the ideal class of $\mathfrak{a}$, and the class equation*

$$f_{\mathcal{O}_K} = \prod_{[\mathfrak{a}] \in \mathrm{Cl}_K} (X - j(\mathfrak{a})) \in \mathbf{Z}[X]$$

is the irreducible equation of $j(\mathcal{O}_K)$ over K.

Proof. In order to show that $M = K(j(\tau))$ is the ring class field L of K corresponding to $\mathcal{O}$, it suffices to show that up to finitely many exceptions, a prime of degree 1 in $\mathcal{O}$ splits completely in L/K if and only if it splits completely in $K(j(\tau))/K$. By definition, a prime $\mathfrak{p} \subset \mathcal{O}$ of norm p prime to the conductor of $\mathcal{O}$ splits completely in L/K if and only if it is a principal ideal $\mathfrak{p} = \pi\mathcal{O}$. For these $\mathfrak{p}$ one has, writing $\mathfrak{a}$ for the $\mathcal{O}$-ideal $[1, \tau]$, an equality $j(\mathfrak{p}\mathfrak{a}) = j(\pi\mathfrak{a}) = j(\mathfrak{a}) = j(\tau)$. As $\mathfrak{p}\mathfrak{a} \subset \mathfrak{a}$ is a sublattice of index p, we have $\Phi_p(j(\mathfrak{p}\mathfrak{a}), j(\mathfrak{a})) = \Phi_p(j(\tau), j(\tau)) = 0$. By the Kronecker congruence, this implies

$$j(\tau)^p \equiv j(\tau) \bmod \mathfrak{P}\mathcal{O}_M$$

for each prime $\mathfrak{P}|\mathfrak{p}$ in the ring of integers $\mathcal{O}_M$ of M. Suppose that $\mathfrak{P}$ does not divide the finite index $[\mathcal{O}_M : \mathcal{O}_K[j(\tau)]]$. Then $j(\tau)$ generates the residue class field $\mathcal{O}/\mathfrak{P}$ over $\mathbf{F}_p$, and we have $\mathcal{O}_M/\mathfrak{P} = \mathbf{F}_p$ as $\alpha^p = \alpha \in \mathcal{O}/\mathfrak{P}$ for all $\alpha \in \mathcal{O}_M/\mathfrak{P}$. It follows that almost all primes of degree 1 in $\mathcal{O}$ that split completely in the ring class field L split completely in M.

Conversely, suppose that $\mathfrak{p}$ is a prime of degree 1 of K that splits completely in M/K. This implies $j(\mathfrak{a})^p \equiv j(\mathfrak{a}) \bmod \mathfrak{p}\mathcal{O}_M$. From the Kronecker congruence

$$(j(\mathfrak{a})^p - j(\mathfrak{p}\mathfrak{a}))\,(j(\mathfrak{a}) - j(\mathfrak{p}\mathfrak{a})^p) \equiv 0 \bmod p$$

we derive that $j(\mathfrak{a}) - j(\mathfrak{p}\mathfrak{a})$ is divisible by a prime over p in any sufficiently large number field. Thus, if we disregard the finite number of primes that are not coprime to the differences $j(\mathfrak{a}) - j(\mathfrak{b})$, with $[\mathfrak{a}] \neq [\mathfrak{b}] \in Cl(\mathcal{O})$, it follows that $j(\mathfrak{a}) = j(\mathfrak{p}\mathfrak{a})$. This implies that $\mathfrak{p}\mathfrak{a} = \pi\mathfrak{a}$, so $\mathfrak{p}$ is principal in $\mathcal{O}$ and splits therefore completely in L/K. This proves the other inclusion, and $M = K(j(\tau))$ is the ring class field corresponding to $\mathcal{O}$. As the only property of τ we used was that $[1, \tau]$ is an invertible $\mathcal{O}$-ideal, we see that $M = K(j(\mathfrak{a}))$ for *any* invertible $\mathcal{O}$-ideal.

We will now show that for $\mathfrak{p} \subset \mathcal{O}$ an ideal of prime norm p and $\mathfrak{a}$ an invertible $\mathcal{O}$-ideal, we almost always have the Frobenius congruence

$$j(\mathfrak{p}^{-1}\mathfrak{a}) \equiv j(\mathfrak{a})^p \bmod \mathfrak{P}$$

for every prime $\mathfrak{P}|\mathfrak{p}$ in M. One takes p coprime to the discriminant of $\mathcal{O}$ and applies lemma 4.6 for $X = j(\mathfrak{a})^p$ and $Y = \phi_{\mathfrak{p}'}(\mathfrak{a})$, with $\mathfrak{p}\mathfrak{p}' = p\mathcal{O}$:

$$\begin{aligned} F(j(\mathfrak{a})^p, \phi_{\mathfrak{p}'}(\mathfrak{a})) &= \sum_{i=0}^{p} (j(\mathfrak{a})^p - (j \circ \sigma_i)(\mathfrak{a})) \prod_{j \neq i} \big(\phi_{\mathfrak{p}'}(\mathfrak{a}) - \phi_{\sigma_j}(\mathfrak{a})\big) \\ &= (j(\mathfrak{a})^p - j(\mathfrak{p}'\mathfrak{a})) \prod_{\sigma_j \neq \sigma_{\mathfrak{p}'}} \big(\phi_{\mathfrak{p}'}(\mathfrak{a}) - \phi_{\sigma_j}(\mathfrak{a})\big) \equiv 0 \bmod \mathfrak{p}. \end{aligned}$$

By lemma 5.2, the product factor is a unit modulo $\mathfrak{p}$ in a sufficiently large number field, so this yields the desired congruence. As a consequence, we see that $\sigma_{\mathfrak{p}}(j(\mathfrak{a})) = j(\mathfrak{p}^{-1}\mathfrak{a})$ for all those $\mathfrak{p}$ of degree 1 that do not divide a difference of conjugates of class invariants. For primes of degree 2 the same equation holds as these primes split completely in M/K, so we have obtained the desired description of $\sigma_{\mathfrak{p}}$ for almost all $\mathfrak{p}$.

It follows from the explicit description of the Galois action on $j(\mathfrak{a})$ that the class invariants of $\mathcal{O}$ are conjugate over K, and that the class equation $f_{\mathcal{O}}$ is the irreducible polynomial of any of them. The complex conjugate of a zero $j(\mathfrak{a})$ of $f_{\mathcal{O}}$ is the zero $j(\overline{\mathfrak{a}})$, so $f_{\mathcal{O}}$ has coefficients in $K \cap \mathbf{R} = \mathbf{Q}$ that are algebraic integers, i.e. they are in $\mathbf{Z}$. □

It is possible to prove the preceding theorem without class field theory, i.e. without assuming the existence of a ring class field corresponding to $\mathcal{O}$. The hard part of the proof is then to show that $f_{\mathcal{O}}$ has coefficients in $\mathbf{Z}$. Once one knows that the class invariants are a complete set of conjugate elements over $\mathbf{Q}$, one can define an injective homomorphism $Cl(\mathcal{O}) \to \mathrm{Gal}(\Omega/K)$, with Ω the decomposition field of $f_{\mathcal{O}}$, that maps an ideal class $[\mathfrak{b}] \in Cl(\mathcal{O})$ to the automorphism $j(\mathfrak{a}) \mapsto j(\mathfrak{b}^{-1}\mathfrak{a})$. This is well-defined because the Frobenius congruence shows that this is the Frobenius automorphism at $\mathfrak{p}$ when $\mathfrak{p}$ is of degree 1 and coprime to the discriminant of $f_{\mathcal{O}}$. In order to prove surjectivity and the irreducibility of the class equation over K, it suffices to show that every single class invariant generates Ω over K. This follows again from the Frobenius congruence, as any automorphism of Ω/K that fixes $j(\mathfrak{a})$ fixes $j(\mathfrak{a})^p$ and therefore $j(\mathfrak{p}^{-1}\mathfrak{a})$ for almost all $\mathfrak{p}$. In order to finish the proof one still has to show that the isomorphism obtained is the Artin map. For primes of degree 1 we know this already, and for primes of K of degree 2 one uses the fact that $\Omega/\mathbf{Q}$ is dihedral to show that such primes split completely in Ω/K.

In order to complete the proof sketched above, one has to show the rationality of the polynomial $f_{\mathcal{O}}$. There are several ways to proceed, and they all use the explicit factorization of the modular polynomial as a product of $f_{\mathcal{O}}$'s.

5.5. Theorem. *For any integer $n > 1$, denote by $r(n, \mathcal{O})$ the number of non-associate elements α in the imaginary quadratic order $\mathcal{O}$ that are primitive and of norm n. Then the factorization of the modular polynomial is given by*

$$\Phi_n(X, X) = \prod_{\mathcal{O}} f_{\mathcal{O}}^{r(n,\mathcal{O})},$$

where the product is taken over all imaginary quadratic orders $\mathcal{O}$.

Proof. A complex number $z = j(w)$ is a zero of $\Phi_n(X, X)$ exactly when $j(\sigma w) = j(w)$ for some $\sigma \in A_n$ or, equivalently, when $\sigma w = w$ for some primitive matrix $\sigma \in M_2(\mathbf{Z})$ of determinant n. This is in turn equivalent to saying that $[1, \tau]$ has a sublattice $\sigma([1, w])$ that is primitive of index n and of the form $x \cdot [1, w]$. It follows that $j(w)$ is a singular j-invariant and that $\mathcal{O}_w$ is a quadratic order containing a primitive element x of norm n. More precisely, the number $r = r(n, \mathcal{O}_w)$ of such x (up to multiplication by units) is exactly the number of $\sigma \in A_n$ for which $j(\sigma w) = j(w)$. Thus, it suffices to show that $\Phi_n(X, X)$ has a zero of order r at $X = j(w)$, and we will achieve this by showing that the functions $\Phi_n(j(z), j(z))$ and $(j(z) - j(w))^r$ have the same order of vanishing at $z = w$. Writing $\Phi_n(j(z), j(z)) = \prod_{\sigma \in A_n}(j(\sigma z) - \sigma(z))$, one can express the quotient of these two functions as a product of a non-vanishing function at $z = w$ and factors of the form

$$A_\sigma = \frac{j(\sigma z) - j(z)}{j(z) - j(w)},$$

where $\sigma \in M_2(\mathbf{Z})$ is primitive of order n and satisfies $\sigma w = w$. If one passes to the limit $z \to w$, the factor A_σ takes the value $\sigma'(w)^k - 1$, where k is the order of vanishing of $j(z) - j(w)$ at $z = w$. It is elementary to show that this value is non-zero. □

By comparing degrees in the preceding theorem, one obtains class number relations due to Kronecker. If $h(D)$ denotes the class number of the order $\mathcal{O}_D$ of discriminant D and $r(n,D)=r(n,\mathcal{O}_D)$, these relations can be written as

$$\sum_D r(n,D)h(D)=\deg\Phi_n(X,X).$$

The degree on the right hand side is easily computed, and one can combine the formulae to obtain related formulae in which the constants $r(n,\mathcal{O}_D)$ no longer occur (cf. exercises).

From the preceding theorem, one can prove inductively that the class equation $f_{\mathcal{O}}$ is in $\mathbf{Z}[X]$. A more direct way uses the following lemma, which is also useful from a theoretical point of view as it shows how to compute $f_{\mathcal{O}}$ from suitable modular polynomials. It considers the polynomial $\Phi_{n,1}(X)$ that is the product of all irreducible factors $f_{\mathcal{O}}$ of $\Phi_n(X,X)$ that occur with exponent $r(n,\mathcal{O})=1$.

5.6. Lemma. *Writing f_D for the class equation of the order of discriminant D, one has $\Phi_{2,1}=f_{-4}\cdot f_{-8}$ and for $n>2$*

$$\Phi_{n,1}(X)=\begin{cases} f_{-4n}\cdot f_{-n} & \text{if } n\equiv 3 \bmod 4 \text{ but } n\neq 3k^2 \text{ for any } k>1;\\ f_{-4n} & \text{if } n\not\equiv 3 \bmod 4 \text{ or } n=3k^2 \text{ for some } k>1.\end{cases}$$

Proof. The element $\sqrt{-n}$ is up to sign the only primitive element of norm n in $\mathbf{Z}[\sqrt{-n}]$, so f_{-4n} is a factor of $\Phi_{n,1}$. For $n\equiv 3 \bmod 4$ this element is also contained in $\mathcal{O}_{-n}=\mathbf{Z}[(1+\sqrt{-n})/2]$. In this ring, it is up to units the only primitive element of norm n except when $n=3k^2$ for some odd $k>1$. (In this last case the non-associate element $(3k+\sqrt{-n})/2$ also has norm n.)

Conversely, suppose that α is up to units the only primitive element of norm n in $\mathcal{O}_D$. Then there exists $\epsilon\in\mathcal{O}^*$ such that $\alpha=\epsilon\bar{\alpha}$, and for $D<-4$ this implies that $\alpha=\pm\frac{1}{2}\sqrt{D}$ or $\alpha=\pm\sqrt{D}$ depending on the parity of D. It follows that $D=-4n$ or $D=-n$ as above. For $D=-4$ one has $\epsilon=\pm i$ and $\alpha=1\pm i$ giving rise to the special factorization of $\Phi_{2,1}$, and for $D=-3$ one concludes that all six elements of norm 3 are associate in $\mathcal{O}_{-3}$, so f_{-3} does divide $\Phi_{3,1}$. □

Explicit computations. In principle, the preceding lemma gives rise to a deterministic algorithm to compute the class equation of an imaginary quadratic order. As it involves the knowledge of explicit modular polynomials, which have coefficients that grow exponentially with n, this is not an efficient algorithm. Better results can be obtained if one computes the class equation directly from the definition, using a numerical approximation for the singular j-invariants that one knows to be the zeroes as soon as the class group of $\mathcal{O}$ has been computed. For instance, the order of discriminant -23 has class number 3, as one easily verifies by calculating the reduced quadratic forms $(1,1,6)$ and $(2,\pm1,3)$. The j-invariants of the corresponding moduli $(-1+\sqrt{-23})/2$ and $(\pm1+\sqrt{-23})/4$ have the approximate values

$$-3493225.6999699 \qquad \text{and} \qquad 737.8499849667\pm1764.0189386127\,i,$$

from which one easily computes the polynomial

$$\begin{aligned} f_{-23} &= X^3 + 3491750X^2 - 5151296875X + 12771880859375 \\ &= X^3 + 2 \cdot 5^3 \cdot 13967X^2 - 5^6 \cdot 329683X + (5^3 \cdot 11 \cdot 17)^3. \end{aligned}$$

The discriminant $\Delta(f_{-23}) = 5^{18} \cdot 7^{12} \cdot 11^4 \cdot 17^2 \cdot 19^2 \cdot 23$ shows that this polynomial does indeed generate a cubic cyclic extension of $\mathbf{Q}(\sqrt{-23})$. It also shows the additional complication lying in the fact that class invariants of orders of small discriminant are already quite large, and that $\mathcal{O}[j(\tau)]$ may have a large index in the ring of integers of the ring class field. In the example above, the same field is generated by the polynomial $X^3 + X^2 - 1$ whose zeroes are units that generate the ring of integers over $\mathcal{O}_K$.

If one takes the slightly larger example $D = -164$ with class number 8, the resulting polynomial is

$$\begin{aligned} f_{-164} = &X^8 - 296853791160440320\, X^7 \\ &- 16193638923387044095775392\, X^6 \\ &- 107971538653147206549839754035 2\, X^5 \\ &- 7201800935415258897234787053487102361 6\, X^4 \\ &- 829235917881182789541553860209199284224 0\, X^3 \\ &+ 5887658098871143194377169001255234662541248\, X^2 \\ &+ 716292304882512928715138362472485709784740265984\, X \\ &- 852636173252999994455687887498749426415404067061 76. \end{aligned}$$

The discriminant of this polynomial is a 497-digit number which factors as

$$\begin{aligned} \Delta(f_{-164}) = &- 2^{542} \cdot 13^{56} \cdot 17^{36} \cdot 23^{24} \cdot 29^{20} \cdot 31^{16} \cdot 41^6 \cdot 43^{10} \cdot 53^8 \cdot 59^6 \cdot 83^4 \cdot 89^6 \\ &97^2 \cdot 101^6 \cdot 103^2 \cdot 107^2 \cdot 109^4 \cdot 127^2 \cdot 131^4 \cdot 137^4 \cdot 139^2 \cdot 149^4 \cdot 157^2, \end{aligned}$$

and the constant coefficient is the cube of $-2^{16} \cdot 17^2 \cdot 23 \cdot 29^2 \cdot 41 \cdot 59 \cdot 107$. It is no coincidence that only small prime factors occur: there are theorems due to Deuring, Gross and Zagier that give a precise description of the primes that can divide a difference of two singular j-invariants.

Exercises.

5.1. Let K be a number field and L and M finite extensions of K. By the density of a set of primes of K we mean the Dirichlet density of this set inside the set of all primes of K. You may assume the Čebotarev density theorem in this exercise.

a. Show that the set of primes of K that are of degree 1 over $\mathbf{Q}$ has density 1.

b. Show that $L = K$ if $S_{L/K}$ has density 1.

b. Show that $L = M$ if the symmetric difference of $S_{L/K}$ and $S_{M/K}$ has density 1. What can you say if $S_{L/K} \subset S_{M/K}$?

5.2. Let $\mathcal{O}$ be an imaginary quadratic order with field of fractions K. Show that $j(\mathcal{O})$ is a real number, and that $\mathbf{Q}(j(\mathcal{O}))$ is the maximal real subfield of $K(j(\mathcal{O}))$. Determine when $\mathbf{Q}(j(\mathcal{O}))$ is normal over $\mathbf{Q}$ and when its normal closure is $K(j(\mathcal{O}))$.

5.3. Let $\sigma \in M_2(\mathbf{Z})$ be primitive of determinant n and suppose that $\sigma w = w$ for some $w \in \mathcal{H}$. If k is the order of vanishing of $j(z) - j(w)$ at $z = w$, show that $\sigma'(w)^k \neq 1$.

5.4. Show that the degree of the modular polynomial $\Phi_n(X, X)$ with $n > 1$ equals

$$2 \sum_{a|n \text{ and } a>\sqrt{n}} \frac{a}{e}\phi(e) + \phi(\sqrt{n}),$$

where $e = \gcd(a, n/a)$ and $\phi(\sqrt{n}) = 0$ if n is not a square.

5.5. Let $C_n = \deg(\Phi_n(X, X))$ be as in the previous exercise. Suppose that n is not a square.

a. If m ranges over the divisors of n of the form n/k^2, show that

$$\sum_m C_m = 2 \sum_{a|n \text{ and } a>\sqrt{n}} a.$$

If $D < 0$ is a quadratic discriminant, we say that a solution to the equation $x^2 - Dy^2 = 4n$ is *proper* if $y > 0$ and $\gcd(x, y) \leq 2$, with $\gcd(x, y) = 2$ allowed for n odd only.

b. Show that $r(n, D)$ is the number of proper solutions to $x^2 - Dy^2 = 4n$ if $D < -4$. What is the corresponding statement if $D = -3, -4$?

Let $h'(D)$ be the number of reduced quadratic forms of discriminant D, including the imprimitive forms, where forms $(x, 0, x)$ are counted with multiplicity $\frac{1}{2}$ and forms (x, x, x) with multiplicity $\frac{1}{3}$.

c. Show that $h(D) = h'(D)$ if $D < -4$ is a fundamental discriminant. What are $h'(-3)$ and $h'(-4)$?

d. Show that

$$h'(-4n) + 2 \sum_{k=1}^{[2\sqrt{n}]} h'(-4n + k^2) = 2 \sum_{a|n \text{ and } a>\sqrt{n}} a.$$

[Hint: the left hand side equals $\sum h((-4n + x^2)/y^2)$, where the sum is taken over all x, y, D with $y > 0$ that satisfy $x^2 - Dy^2 = 4n$.]

5.6. Show that for any integer $n > 1$, one has

$$r(n,D) = \begin{cases} 0 & \text{if } D < -4n; \\ 1 & \text{if } D = -4n; \\ 2 & \text{if } D = -4n+1. \end{cases}$$

How does this imply $\Phi_n(X,X) \in \mathbf{Z}[X] \Longrightarrow f_{\mathcal{O}} \in \mathbf{Z}[X]$?

5.7. Give an algorithm to compute $f_{\mathcal{O}}$ for arbitrary $\mathcal{O}$.
[Hint: One has to distinguish f_{-n} from f_{-4n} when $r(n,-n) = r(n,-4n) = 1$.]

5.8. Let $\mathcal{O}$ be the ring of integers of a quadratic field K and set $f_p(X) = \Phi_p(X, j(\mathcal{O})) \in H[X]$, with H the Hilbert class field of K.

a. Suppose that $\Delta(K) < -4$. Show that f_p is irreducible in $H[X]$ if and only if p is inert in $K/\mathbf{Q}$. Is the hypothesis on $\Delta(K)$ necessary?

b. Determine for each $\mathcal{O}$ the values of p for which f_p splits completely in $H[X]$?

c. Is f_p always separable over H?

5.9. Show that $j(\sqrt{-3}) = 54000 = 2^4 \cdot 3^3 \cdot 5^3$.
[Hint: Use the previous exercise.]

5.10. Show that all zeroes of $\Phi_3(X,X)$ are rational and determine the multiplicity of each of them. Then use the preceding exercise and the explicit values of the zeroes of $\Phi_2(X,X)$ to compute $j(\frac{1+\sqrt{-11}}{2})$.
[Hint: show that $\Phi_3(X,X) = -X^6 + 6 \cdot 744X^5 +$ lower order terms.]

5.11. Let ω_1, ω_2 and ω_3 be the zeroes of $X^3 - X^2 + 1$ and Ω the corresponding splitting field.

a. Show that $\Omega = \mathbf{Q}(\sqrt{-23}, \omega_1)$.

Let Tr denote the trace in the extension $K = \mathbf{Q}(\sqrt{-23}) \subset \Omega$.

b. Show that $(\mathrm{Tr}(\omega_i\omega_j))_{i,j=1}^3$ is the identity matrix. Deduce that Ω/K is unramified and that $\{\omega_1, \omega_2, \omega_3\}$ is a normal integral basis for Ω/K.

6. ORDERS OF CLASS NUMBER ONE

Class groups of imaginary quadratic orders were introduced by Gauss, who already observed that the orders $h(D)$ seem to grow when $D \to -\infty$, albeit irregularly. This would imply that there are only finitely many discriminants $D < 0$ for which $h(D) = 1$, and without too much effort one can produce a list that seems to be complete, i.e. one arrives at the following.

6.1. Theorem. *Let $\mathcal{O}$ be an imaginary quadratic order of class number* 1. *Then D is one of the nine values in* $\{-3, -4, -7, -8, -11, -19, -43, -67, -163\}$ *if $\mathcal{O}$ is a maximal order, and one of the four values in* $\{-12, -16, -27, -28\}$ *otherwise.*

This result was already conjectured by Gauss, but a valid proof has been given only much later by Heegner, Baker and Stark. Heegner's proof appeared in 1952 but was only accepted in 1967, when Stark produced an independent proof that turned out to be basically the same. Baker's proof, which uses different methods, appeared at the same time as Stark's. It had already been proved by Siegel in 1935 that there are only finitely many discriminants of class number one. More precisely, he showed that

$$h(D) > C_\epsilon |D|^{1/2} \qquad \text{for all } \epsilon > 0,$$

but the constant C_ϵ is non-effective. Subsequent refinements showed that there is at most one imaginary quadratic field of class number one besides those given in the preceding theorem, so the problem was to show that this tenth quadratic field cannot exist.

It should be pointed out that the situation appears to be very different for real quadratic fields. In this case the product of $h(D)$ and the regulator $R = \log|\epsilon_D|$ grows as $|D|^{1/2}$, and there seem to be infinitely many D's for which $h(D) = 1$. However, nothing has been proved in this direction.

If $D < -8$ is fundamental and $h(D) = 1$, we have $D = -p$ for some prime $p \equiv 3 \bmod 4$ by genus theory. In the case $p \equiv 7 \bmod 8$ the ring $\mathcal{O}_{-p} = \mathbf{Z}[(1 + \sqrt{-p})/2]$ contains an element of norm 2, so $p = 7$. In order to show that our list of fundamental discriminants is complete, it suffices to show that there are no primes $p \equiv 3 \bmod 8$ besides those listed that have $h(-p) = 1$. Once one knows the list of fundamental discriminants, it is straightforward to check that there are only 4 non-maximal orders of class number one. If $\mathcal{O}$ is the order of index $f > 1$ in some maximal order $\mathcal{O}_D$ of discriminant D and $h(\mathcal{O}) = 1$, one has $h(\mathcal{O}_D) = 1$ and

$$h(\mathcal{O})/h(\mathcal{O}_K) = \frac{f}{[\mathcal{O}_D^* : \mathcal{O}^*]} \prod_{p|f} (1 - \left(\frac{D}{p}\right)\frac{1}{p}) \tag{6.2}$$

equals 1. For $D < -4$ this implies that $f = 2$ and 2 splits in $\mathcal{O}_D$, so $f^2 D = -28$. For $D = -4$ one obtains $f = 2$ and $f^2 D = -16$, and for $D = -3$ one finds $f = 2$ or $f = 3$, leading to $f^2 D = -12$ or -27. Thus 6.1 is equivalent to the following statement.

6.3. Theorem. *Suppose $p \equiv 3 \bmod 8$ is prime and satisfies $h(-p) = 1$. Then we have $p \in \{3, 11, 19, 43, 67, 163\}$.*

The proof of 6.3 proceeds in several steps. One begins by studying the cube root γ_2 of the j-function, which is defined as the holomorphic branch

$$\gamma_2(z) = \sqrt[3]{j(z)} = \frac{g_2(z)}{\sqrt[3]{\Delta(z)}}$$

on the upper half plane that is real on the imaginary axis. The function $\gamma_2(z)$ is not a modular function, but its behavior under modular transformations is easily determined. From the q-expansion we see that $\gamma_2(z+1) = \zeta_3^{-1}\gamma(z)$, where $\zeta_3 = e^{2\pi i/3}$. We further have $\gamma_2(-1/z) = \gamma(z)$ as the cubes of these expressions coincide and they are equal and non-zero in $z = i$. From these two identities one can prove by induction on the length of $\binom{a\,b}{c\,d} \in SL_2(\mathbf{Z})$ as a word in $\binom{1\,1}{0\,1}$ and $\binom{0\,-1}{1\;\;0}$ that

$$\gamma_2(\frac{az+b}{cz+d}) = \zeta_3^{ac-ab+a^2cd-cd}\gamma_2(z).$$

In particular, we see that γ_2 is left invariant by transformations $\sigma = \binom{a\,b}{c\,d} \in SL_2(\mathbf{Z})$ satisfying $b \equiv c \equiv 0 \bmod 3$. For such σ we have $\sigma_3^{-1}\sigma\sigma_3 \in \Gamma_0(9)$, where $\sigma_3 = \binom{3\,0}{0\,1}$. Consequently, the function $\gamma_2 \circ \sigma_3$ is a $\Gamma_0(9)$-modular function. As its q-expansion is rational, we even have $\gamma_2(3z) \in \mathbf{Q}(j(9z), j(z))$.

The use of the function γ_2 in the proof of 6.3 stems from the following property.

6.4. Proposition. *Let D be an imaginary quadratic discriminant coprime to 3 and set*

$$\tau = \begin{cases} (3+\sqrt{D})/2. & \textit{if } D \textit{ is odd;} \\ \sqrt{D}/2 & \textit{if } D \textit{ is even.} \end{cases}$$

Then $\gamma_2(\tau)$ is an algebraic integer and we have $\mathbf{Q}(\gamma_2(\tau)) = \mathbf{Q}(j(\tau))$.

Proof. The hard part of the proof consists in showing the implication

$$\gamma_2(3z) \in \mathbf{Q}(j(9z), j(z)) \Longrightarrow \gamma_2(\tau) \in \mathbf{Q}(j(3\tau), j(\tau/3)). \tag{6.5}$$

Note first of all that this is *not* trivially true. We will assume this implication for the moment, and give the proof at the end of this section.

The multiplicator ring of $[\tau/3, 1]$ is the order $[3\tau, 1]$ (exercise 6.3), so 5.3 implies that $\gamma_2(3\tau)$ is contained in the ring class field of conductor 3 of $K = \mathbf{Q}(\tau)$. As 3 does not divide the discriminant of K, formula 6.2 shows that this ring class field has degree 2 or 4 over the Hilbert class field $K(j(\tau))$ of K. On the other hand, $\gamma_2(3\tau)$ is the cube root of $j(\tau)$, so the degree of $\gamma_2(3\tau)$ over $\mathbf{Q}(j(\tau))$ equals 1 as it divides both 3 and 8. □

The preceding lemma implies that for $p \geq 11$ a prime for which $h(-p) = 1$, the element $\gamma_2(\frac{3+\sqrt{-p}}{2})$ is a rational integer. This is the first important step in the proof of 6.3.

The function γ_2 is related to three other holomorphic functions f, f_1 and f_2 on the upper half plane that are real on the imaginary axis and may be characterized by the fact that their eighth powers are of degree 3 over the field $\mathbf{Q}(\gamma_2)$. More precisely, the following holds.

6.6. Proposition. *There exist holomorphic functions f, f_1 and f_2 on the upper half plane that are real and positive on the imaginary axis and that are uniquely characterized by the functional equations*

$$X^3 - \gamma_2 X + 16 = (X + f^8)(X - f_1^8)(X - f_2^8)$$

and

$$f_1(2z)f_2(z) = \sqrt{2}.$$

Proof. It is clear that the functions are uniquely determined by these conditions, with the second equation only needed to distinguish between f_1 and f_2. One starts with the Dedekind η-function, which is defined by its Fourier expansion $\eta(q) = q^{1/24}\prod_{n\geq 1}(1-q^n)$, and sets

$$f(z) = \zeta_{48}^{-1}\frac{\eta((z+1)/2)}{\eta(z)}, \qquad f_1(z) = \frac{\eta(z/2)}{\eta(z)}, \qquad f_2(z) = \sqrt{2}\,\frac{\eta(2z)}{\eta(z)}.$$

Note that the relation $f_1(2z)f_2(z) = \sqrt{2}$ follows immediately from the definition. From the Fourier expansions

$$f = q^{-1/48}\prod_{n \text{ odd}}(1+q^{n/2})$$
$$f_1 = q^{-1/48}\prod_{n \text{ odd}}(1-q^{n/2})$$
$$f_2 = \sqrt{2}q^{1/24}\prod_{n\geq 1}(1+q^n)$$

one reads off the identity $\eta f f_1 f_2 = \sqrt{2}\,\eta$, which implies

$$f(z)f_1(z)f_2(z) = \sqrt{2}. \tag{6.7}$$

The essential part of the proof consists in showing that the differences between the values of the Weierstrass-$\wp$-function in 2-torsion points are described by the functions η, f, f_1 and f_2. More precisely, let e_1, e_2 and e_3 be the three zeroes of the Weierstrass polynomial $4X^3 - g_2(z)X - g_3(z)$, i.e. the 2-division values $\wp_{[1,z]}(1/2)$, $\wp_{[1,z]}(z/2)$ and $\wp_{[1,z]}((z+1)/2))$. Then we have

$$\begin{aligned} e_2 - e_1 &= \pi^2\eta^4(z)f^8(z) \\ e_2 - e_3 &= \pi^2\eta^4(z)f_1^8(z) \\ e_3 - e_1 &= \pi^2\eta^4(z)f_2^8(z). \end{aligned} \tag{6.8}$$

Note that in view of 6.7, this yields the Fourier expansion

$$\Delta(z) = 16(e_1 - e_2)^2(e_1 - e_3)^2(e_2 - e_3)^2 = (2\pi)^{12}\eta^{24}(z) = (2\pi)^{12}q\prod_{n\geq 1}(1 - q^n)^{24}$$

for the Δ-function. It also gives the relation $f^8 = f_1^8 + f_2^8$ and, since we know by 6.7 that $f^8 f_1^8 f_2^8 = 16$, the identity for $(X + f^8)(X - f_1^8)(X - f_2^8)$ follows from it as soon as we show that

$$\gamma_2(z) = \frac{12g_2}{\Delta} = f^{16} - f_1^8 f_2^8 = f^{16} - \frac{16}{f^8} = \frac{f^{24} - 16}{f^8}.$$

This result can again be derived from 6.8 as we have

$$12g_2 = -48(e_1e_2 + e_1e_3 + e_2e_3) = 16((e_2 - e_1)^2 - (e_2 - e_3)(e_3 - e_1)).$$

Finally, the derivation of 6.8 itself proceeds by expressing the differences of $\wp$-values in terms of the σ-function (exercise 2.2c), and applying exercise 2.7cd before showing the identity in terms of Fourier expansions. □

The functions in 6.6 have been studied extensively by Weber since their values at singular moduli, which are obviously algebraic integers, can be used in many cases to generate class fields. For a complete account we refer to the paper by Schertz (Crelle **286/287** p. 46–74, 1976). We will use the following special case. For the proof we refer to the exercises.

6.9. Proposition. *Let $\mathcal{O}$ be the imaginary quadratic order of discriminant $D = -4p$ with $p \equiv 3 \bmod 4$ odd. Then we have $\mathbf{Q}(f(\sqrt{-p})^2) = \mathbf{Q}(j(\sqrt{-p}))$.* □

If we take for $p \geq 11$ is a prime for which $h(-p) = 1$, the field $\mathbf{Q}(j(\sqrt{-p}))$ is a real cubic field by 6.2. For $\tau = \frac{3+\sqrt{-p}}{2}$, one uses the functional equation from 6.5 and the transformation relation $f_1(z + 1) = \zeta_{48}^{-1}f(z)$ following from the Fourier expansions (cf. exercises) to obtain

$$f_2(\tau) = \sqrt{2}f_1(3 + \sqrt{-p})^{-1} = \sqrt{2}\zeta_{16}f(\sqrt{-p}).$$

It follows that $\alpha = \zeta_8^{-1}f_2(\tau)^2$ is integral and satisfies $\mathbf{Q}(\alpha) = \mathbf{Q}(f(\sqrt{-p})^2) = \mathbf{Q}(j(\sqrt{-p}))$. Thus, every prime $p \geq 11$ with $h(-p) = 1$ gives rise to an algebraic integer α and irreducible polynomials

$$f_{\mathbf{Q}}^{\alpha} = X^3 + aX^2 + bX + c$$
$$f_{\mathbf{Q}}^{\alpha^4} = X^3 - \gamma_2(\tau)X + 16$$

that are in $\mathbf{Z}[X]$. This imposes very strict conditions on $f_{\mathbf{Q}}^{\alpha}$ and $\gamma_2(\tau)$, since a direct computation of $f_{\mathbf{Q}}^{\alpha^4}$ from $f_{\mathbf{Q}}^{\alpha}$ yields—replacing α by $-\alpha$ if necessary—an equality $c = 2$ and subsequently

$$\gamma(\tau) = -(b^2 - 4a)^2 - 8(2b - a^2)$$
$$2(b^2 - 4a) = (2b - a^2)^2.$$

Setting $2Y = (b - a^2)$ and $-2X = a$ the second equation can be rewritten in the form $Y^2 = 2X(X^3 + 1)$. This Diophantine equation has exactly six integral solutions.

6.10. Proposition. *The only integral solutions* (X, Y) *to the equation*

$$Y^2 = 2X(X^3 + 1)$$

are $(-1, 0)$, $(0, 0)$, $(1, \pm 2)$ *and* $(2, \pm 6)$.

Proof. As X and $X^3 + 1$ are coprime, there absolute values are a square and twice a square and they do not have opposite signs. This leads to 4 cases:
(a) $X^3 + 1 = \square$ and $X = 2 \cdot \square$;
(b) $X^3 + 1 = -\square$ and $X = -2 \cdot \square$;
(c) $X^3 + 1 = 2 \cdot \square$ and $X = \square$;
(d) $X^3 + 1 = -2 \cdot \square$ and $X = -\square$.

Case (a) is the hardest case. However there is a neat proof by Euler using a descent argument (*Opera omnia*, vol. II, p. 56–58, 1738). It shows that the only positive rational number X for which $X^3 + 1$ is a rational square is $X = 2$.

Cases (b) through (d) can be dealt with in a more elementary way. If $X^3 + 1 = -Z^2$ has an integral solution, then $Z + i$ is a cube in $\mathbf{Z}[i]$ as $Z + i$ and $Z - i$ are coprime and there product equals $(-X)^3$. This implies $Z = 0$. Analogous arguments in $\mathbf{Z}[\sqrt{-2}]$ for $(-X)^3 = 1 + 2Z^2$ and in $\mathbf{Z}[\zeta_3]$ for $X^3 + 1 = 2Z^2$ yield the desired result. $\square$

The solutions give rise to six values

$$\gamma_2(\tau) = 0, -32, -96, -960, -5280, -640320$$

and a simple approximation

$$\gamma_2(\tau) \approx \sqrt[3]{744 - e^{\pi\sqrt{p}}}$$

which is accurate to at least 2 decimal places for $p \geq 11$ shows that the only primes $p \equiv 3 \bmod 8$ for which $h(-p)$ equals 1 are the six values in 6.3. This finishes the proof of 6.1 and 6.3 modulo the implication 6.5. $\square$

It is amusing to see how extremely accurate our approximation for $\gamma_2(\tau)$ is when $p = 163$:

$$\sqrt[3]{744 - e^{\pi\sqrt{163}}} = -640319.99999999999999999999999390...$$

The observation that $e^{\pi\sqrt{163}}$ is less than 10^{-12} away from an integer goes back to Hermite. It is caused by the fact that $q = e^{2\pi i z}$ is very small for $z = (1 + \sqrt{-163})/2$ and the corresponding integral j-invariant therefore very close to $q^{-1} + 744 = 744 - e^{\pi\sqrt{163}}$.

We still have to prove the implication 6.5. Before doing so, we prove a fundamental lemma that will also be useful in the next section. It allows us to conclude in many cases that the singular values $f(\tau)$ of a modular function $f \in \mathbf{Q}(j(z), j(nz))$ are contained in $\mathbf{Q}(j(\tau), j(n\tau))$.

6.11. Lemma. *Let $g \in F_n$ be a modular function of level n and $G(X) = G(X, j) \in \mathbf{Q}(j)[X]$ its irreducible polynomial over $F_1 = \mathbf{Q}(j)$. Then any element $f \in K = \mathbf{Q}(j, g)$ satisfies*

$$f \cdot G'(g) = H(g) \qquad \text{with} \qquad H(X) = \mathrm{Tr}_{K/F_1}\left[f \cdot \frac{G(X)}{X - g}\right] \in F_1[X].$$

Suppose that f and g are holomorphic on $\mathcal{H}$ and that $\tau \in \mathcal{H}$ is a modulus for which $g(\tau)$ is a simple zero of $G(X, j(\tau))$. Then $f(\tau)$ is contained in $\mathbf{Q}(j(\tau), g(\tau))$.

Proof. The formula in the lemma is nothing but the well known Lagrange interpolation formula, as $H(X)$ is the unique polynomial in $F_1[X]$ of degree at most $[F_1(g) : F_1] - 1$ that assumes the values $f^\sigma \cdot G'(g^\sigma)$ in each of the conjugates g^σ of g.

If f and g are holomorphic on $\mathcal{H}$, then $G(X)$ and $H(X)$ have coefficients that are holomorphic and therefore in $\mathbf{Q}[j]$. It follows that in this case $f \cdot G'(g)$ is a rational polynomial in j and g. If we specialize the variable to τ we have $G'(g(\tau)) \neq 0$ by assumption and consequently $f(\tau) \in \mathbf{Q}(j(\tau), g(\tau))$. □

Proof of 6.5. In view of the preceding lemma, it suffices to show that for τ as in 6.4, the polynomial $\frac{\partial}{\partial X}\Phi_9(X, \tau/3)$ does not have a zero at $X = 3\tau$. Indeed, assume the contrary. Then there exists a matrix $\sigma = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in A_9$ different from $\left(\begin{smallmatrix} 9 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for which the two lattices $\sigma([\tau/3, 1]) = [a\tau/3 + b, d]$ and $[3\tau, 1]$ are homothetic. These lattices are both of index 9 in $[\tau/3, 1]$, so the element $\lambda \in \mathbf{Q}(\tau)$ for which $\lambda \cdot [3\tau, 1] = [a\tau/3 + b, d]$ is of norm 1. Write $3\lambda = 3s + t\tau$, then we have

$$N(3\lambda) = 9s^2 + 3st(\tau + \bar{\tau}) + t^2\tau\bar{\tau} = 9,$$

which shows that 3 divides t, i.e. λ is a unit. If $D < -4$ it follows that our lattices are equal, contrary to the choice of σ. For $D = -4$ one has $\tau = i$ and one easily checks that $\lambda = i$ cannot occur, so the lattices are again equal. This finishes the proof of 6.5. □

Exercises.

6.1. Determine all non-principal imaginary quadratic orders for which the class number equals the class number of the corresponding principal order.

6.2. Show that the function $\gamma_2(z)$ transforms under the action of the modular group as

$$\gamma_2(\frac{az+b}{cz+d} = \zeta_3^{ac-ab+a^2cd-cd}\gamma_2(z).$$

Deduce that the subgroup $H$of Γ that leaves γ_2 invariant consists of the matrices $\binom{a\,b}{c\,d}$ satisfying $a \equiv d \equiv 0 \bmod 3$ or $b \equiv c \bmod 3$. What is the index of G in Γ? Is it a normal subgroup?

6.3. Let $\tau \in \mathbf{C}$ be an imaginary quadratic irrational with irreducible polynomial $aX^2 + bX + c \in \mathbf{Z}[X]$.

a. Show that $\mathbf{Z}[a\tau]$ is the multiplicator ring of the lattice $[1, \tau]$.

b. Let τ be as in proposition 6.4. Show that $\mathbf{Z}[3\tau]$ is the multiplicator ring of the lattice $[1, \tau/3]$.

6.4. Show that the functions η, f, f_1 and f_2 satisfy the following modular transformation laws.

$$\begin{aligned} \eta(z+1) &= \zeta_{24}\eta(z) & \eta(-1/z) &= \sqrt{-iz}\,\eta(z) \\ f(z+1) &= \zeta_{48}^{-1}f_1(z) & f(-1/z) &= f(z) \\ f_1(z+1) &= \zeta_{48}^{-1}f(z) & f_1(-1/z) &= f_2(z) \\ f_2(z+1) &= \zeta_{24}f_2(z) & f_2(-1/z) &= f_1(z) \end{aligned}$$

6.5. Let $\sum_i b_i X^i$ be the irreducible polynomial of the function g in lemma 6.11. Show that the coefficients of $H(X) = \sum_i a_i X^i$ are then given by

$$a_i = \sum_{k>i} b_k \mathrm{Tr}_{K/F_1}[fg^{k-i-1}].$$

6.6. Complete the following outline of the proof of 6.9.

7. THE PRINCIPAL IDEAL THEOREM

It has been known for a long time that the ideals of the ring of integers of a number field are not always principal, but that they become principal after passing to a suitable extension L of K. More precisely, for given K there always exists a finite extension L/K such that the natural map

$$\begin{aligned} Cl_K &\longrightarrow Cl_L \\ [\mathfrak{a}] &\longmapsto [\mathfrak{a}\mathcal{O}_H] \end{aligned}$$

between the class groups is the zero map. In this situation, one says that every ideal class of K *capitulates* in L. The field L is by no means uniquely determined by this property, nor is their a minimal field L when $Cl_K \neq 0$ (exercise 7.1). However, there is a canonical choice for L.

7.1. Principal ideal theorem. *Every ideal of a number field K becomes principal in the Hilbert class field H of K.*

Note that this property of the Hilbert class field is by no means obvious from its definition as maximal unramified abelian extension of K. The first result indicating a relation between capitulation and unramified abelian extensions is due to Hilbert. Theorem 96 from his Zahlbericht states that in an unramified cyclic extension of a number field K of prime degree, there is a non-principal ideal of K that capitulates. For arbitrary K, we do not in general have explicit generators in H for the ideals coming from K. The reason is that we know by class field theory that H exists, but not how to generate it explicitly. However, it was shown by Artin that the principal ideal theorem can be reduced to a purely group theoretical statement. This statement was proved shortly afterwards, in 1930, by Furtwängler.

We will prove the principal ideal theorem only for K imaginary quadratic. In this special case elliptic functions can be used to exhibit explicit generators in H for almost all primes of K. As the primes of degree 2 of K are already principal in K, one only has to look at primes of degree 1.

7.2. Theorem. *Let K be an imaginary quadratic field of K and $\mathfrak{p}$ a prime of degree one of K that does not divide 6 or the discriminant of K. Let $\mathfrak{a}$ be any ideal of K and $\mathfrak{p}'$ the conjugate of $\mathfrak{p}$ in K. Then $\phi_{\mathfrak{p}^2}(\mathfrak{a})$ is the 24-th power of some element x in the Hilbert class field H of K, and x generates $\mathfrak{p}'\mathcal{O}_H$.*

The proof of 7.2 is a refinement of lemma 5.2, which stated that $\phi_{\mathfrak{p}}(\mathfrak{a})$ generates the 12-th power of $\mathfrak{p}'$ in some extension field of K. If one replaces $\mathfrak{p}$ by $\mathfrak{p}^2$ in 5.2, the proof remains valid and it follows that the element $\phi_{\mathfrak{p}^2}(\mathfrak{a})$ in 7.2 generates $(\mathfrak{p}')^{24}$ in some extension of K. The problem comes down to showing that the singular values of a suitable branch of $\sqrt[24]{\phi_{\mathfrak{p}^2}(z)}$ lie in H. The situation is similar to that occurring in the case of the class number one problem, and so is the argument. One first shows that the 24-th root of

$\phi_n(z)$ is a modular function of level n for suitable n, and then that its singular values lie in the appropriate number field. This will involve a generalization of lemma 6.11 to the case where we have a singular modulus that leads to a multiple root of the irreducible polynomial for the modular function over $\mathbf{Q}(j)$.

The Dedekind η-function from the previous section satisfies $2\pi\eta^{24}(z) = \Delta(z)$, so we can define a 24-th root of the function ϕ_S for any rational 2×2 matrix S with positive determinant by

$$\sqrt[24]{\phi_S(z)} = \sqrt{\det(S)}\,\frac{\eta(S([z,1]))}{\eta(z)}.$$

For $S = \sigma_n = \binom{n\,0}{0\,1}$ we write $\phi_S = \phi_n$ as before, and we have $\sqrt[24]{\phi_n(z)} = \sqrt{n}\,\eta(nz)/\eta(z)$.

7.3. Lemma. *The function* $\sqrt[24]{\phi_n(z)}$ *is* $\Gamma_0(n)$*-modular when* $n \equiv 1 \bmod 24$. *We have* $\sqrt[24]{\phi_n(z)} \in \mathbf{Q}(j(z), j(nz))$ *if* n *is the square of an odd number.*

Proof. From the q-expansion of $\eta(z)$ it is clear that $\eta(z+1) = \zeta_{24}\eta(z)$. As we know that $\eta(z)$ is real on the imaginary axis and that $\Delta(z) = 2\pi\,\eta^{24}(z)$ satisfies $\Delta(-1/z) = z^{12}\Delta(z)$, we must have $\eta(-1/z) = \sqrt{-iz}\,\eta(z)$. It is straightforward to show inductively from these formulae that the general transformation rule for the η-function under an element $A = \binom{a\,b}{c\,d} \in \Gamma$ is

$$\eta(Az) = \zeta_{24}^{\epsilon(A)}\sqrt{-i(cz+d)}\,\eta(z),$$

where $\epsilon(A)$ is given by the explicit formula

$$\epsilon(A) = bd(1-c^2) + c(a+d) + 3(1-c_1) + 3a(c-c_1) + 3\lambda(a^2-1)/2$$

Here we let $c = 2^\lambda c_1$ with c_1 odd if $c \neq 0$ and $c_1 = 0$ otherwise. For $A = \binom{a\,b}{c\,d} \in \Gamma_0(n)$ we have $A = \sigma_n^{-1}A'\sigma_n$ with $A' = \binom{a\ \ nb}{c/n\ d} \in \Gamma$ and

$$\sqrt[24]{\phi_n(Az)} = \sqrt{n}\,\frac{\eta(\sigma_n(Az))}{\eta(Az)} = \sqrt{n}\,\frac{\eta(A'(nz))}{\eta(Az)} = \zeta_{24}^{\epsilon(A)-\epsilon(A')}\sqrt[24]{\phi_n(z)}.$$

If $n \equiv 1 \bmod 24$ we have $\epsilon(A) \equiv \epsilon(A') \bmod 24$ and $\sqrt[24]{\phi_n(z)}$ is $\Gamma_0(n)$-modular. If n is the square of an odd number, than $n \equiv 1 \bmod 24$ and $\sqrt{n} \in \mathbf{Q}$, so $\sqrt[24]{\phi_n(z)}$ must be in $\mathbf{Q}(j(z), j(nz))$ as it is a $\Gamma_0(n)$-modular function with rational q-expansion. □

If S is a primitive integral matrix of square determinant $n \equiv 1 \bmod 24$ the function $\sqrt[24]{\phi_S} \in F_n$ is a conjugate of $\sqrt[24]{\phi_n}$ over $\mathbf{Q}(j)$ and lies in $\mathbf{Q}(j(z), j(Sz))$. Taking for S the matrix describing multiplication by $\mathfrak{p}^2$ in the situation of 7.2, we see that we have to prove the implication

$$\sqrt[24]{\phi_S(z)} \in \mathbf{Q}(j(z), j(Sz)) \Longrightarrow \sqrt[24]{\phi_S(\mathfrak{a})} \in \mathbf{Q}(j(\mathfrak{a}), j(S\mathfrak{a})).$$

It is not in general true that $j(S\mathfrak{a})$ is a simple zero of $\Phi_n(X, j(\mathfrak{a}))$, so we first prove the following generalization of 6.11.

7.4. Lemma. *Let $S = S_1 \in A_n = \{S_i\}_{i=1}^{\psi(n)}$ be a primitive integral matrix of determinant n and suppose that for some $\alpha \in \mathcal{H}$ the number $j(S\alpha)$ is an r-fold zero of $\Phi_n(X, j(\alpha))$, say $j(S\alpha) = j(S_i\alpha)$ for $i = 1, 2, \ldots, r$. Then for every function $f_S \in \mathbf{Q}(j(z), j(Sz))$ the number $f_S(\alpha)$ is algebraic of degree at most r over $\mathbf{Q}(j(\alpha), j(S\alpha))$ and has its conjugates in the set $\{j(S_i(\alpha))\}_{i=1}^{r}$.*

Proof. Let $K/\mathbf{Q}(j)$ be the normal extension obtained by adjoining the zeroes $j \circ S_i$ of $\Phi_n(X, j)$ to $\mathbf{Q}(j)$ and G the Galois group of this extension. Denote by H the subgroup of G that permutes the functions $\{j \circ S_i\}_{i=1}^{r}$ among each other and K_0 the fixed field of H. The polynomial $F(X, z) = \prod_{i=1}^{r}(X - j(S_i z)) \in K_0[X]$ has the property that the polynomial $F^\sigma \in K[X]$ obtained by applying some element $\sigma \in G - H$ to its coefficients is different from F as it remains different if we specialize the coefficients by substituting $z = \alpha$. This implies that for $a \in \mathbf{Q}$ sufficiently general, the function $g(z) = F(a, z) \in K_0$ is not fixed by any $\sigma \in G - H$ and therefore generates K_0 over $\mathbf{Q}(j)$. Moreover, a can be chosen such that $g^\sigma(\alpha) = F^\sigma(a, \alpha)$ is different from $g(\alpha)$ for $\sigma \in G - H$. This implies that $g(\alpha)$ is a simple zero of the irreducible polynomial

$$G(X) = \prod_{\sigma \in G/H} (X - F^\sigma(a, z))$$

of g over $\mathbf{Q}(j)$. We can now apply lemma 6.11 to conclude that for every function $h \in \mathbf{Q}(j, g) = K_0$, we have $h(\alpha) \in \mathbf{Q}(j(\alpha), g(\alpha))$ and, since $g(\alpha) = (a - j(S\alpha))^r$, also $h(\alpha) \in \mathbf{Q}(j(\alpha), j(S\alpha))$.

We know that our given function $f_S \in \mathbf{Q}(j(z), j(Sz))$ is a zero of the polynomial $\prod_{i=1}^{r}(X - f_{S_i}) \in K_0$, so $\prod_{i=1}^{r}(X - f_{S_i}(\alpha))$ has coefficients in $\mathbf{Q}(j(\alpha), j(S\alpha))$ by what we just proved. The lemma follows immediately. □

We conclude the proof of 7.2 by applying the following lemma with $f_S = \sqrt[24]{\phi_S}$ and $\mathfrak{b} = \mathfrak{p}^2$.

7.5. Lemma. *Let $\mathfrak{a}$ be a fractional ideal in some imaginary quadratic number field K and S a matrix satisfying $S\mathfrak{a} = \mathfrak{b}\mathfrak{a}$ for some integral ideal $\mathfrak{b}$ in K. Suppose that some m-th power of $f_S \in \mathbf{Q}(j(z), j(Sz))$ has the form*

$$f_S^m(z) = \frac{H_1(S([z, 1]))}{H_2(z)}$$

for certain modular forms H_1 and H_2 of weight $g > 0$, and that $H_2(\mathfrak{a}) \neq 0$. Then $f_S(\mathfrak{a})$ is contained in $K(j(\mathfrak{a}))$.

Proof. We let n be the norm of $\mathfrak{b}$ and suppose that, in terms of the previous lemma, we have $j(S\mathfrak{a}) = j(S_i\mathfrak{a})$ exactly when $i = 1, 2, \ldots, r$. This implies that $S_i\mathfrak{a} = \lambda_i S\mathfrak{a} = \lambda_i \mathfrak{a}\mathfrak{b}$ for certain elements λ_i of norm 1 in K^*. If λ_i is integral, then we have $S_i\mathfrak{a} = S\mathfrak{a}$, so this happens for exactly one value of $i \in \{1, 2, \ldots, r\}$, say $i = 1$.

We know by the previous lemma that every conjugate of $f_S(\mathfrak{a})$ over $\mathbf{Q}(j(\mathfrak{a}), j(S\mathfrak{a})) \subset K(j(\mathfrak{a}))$ is of the form $f_{S_i}(\mathfrak{a})$. Let σ be an automorphism over $K(j(\mathfrak{a}))$ of order N mapping $f_S(\mathfrak{a})$ to $f_{S_i}(\mathfrak{a})$. From the identity

$$f_{S_i}^m(\mathfrak{a}) = \frac{H_1(S_i\mathfrak{a})}{H_2(\mathfrak{a})} = \frac{\lambda_i^{-g} H_1(S\mathfrak{a})}{H_2(\mathfrak{a})} = \lambda_i^{-g} f_S^m(\mathfrak{a})$$

it follows that $\lambda_i^{-gN} = 1$, so λ_i is a root of unity and $i = 1$. The element $f_{S_1}(\mathfrak{a})$ is the only conjugate of $f_S(\mathfrak{a})$ over $K(\mathfrak{a})$, so $f_S(\mathfrak{a})$ is in $K(j(\mathfrak{a}))$. □

This finishes the proof of 7.2.

Exercises.

7.1. Let K be a number field with non-trivial class group and F a finite normal extension of K.
   a. Show that there exists a finite extension L of K such that F and L are linearly disjoint over K and $Cl_K \to Cl_L$ is the zero map.
   b. Deduce that there exists an infinite collection $\{L_i\}_i$ of pairwise linearly disjoint normal extensions L_i of K such that an ideal of K capitulates in each L_i. In particular, there is no minimal extension L of K such that $Cl_K \to Cl_L$ is the zero map.

7.2. Find the Hilbert class field H of $K = \mathbf{Q}(\sqrt{-5})$ and determine generators in H for the primes over 3 in K.

7.3. Let K be a number field, H the Hilbert class field of K and H' the Hilbert class field of H.
   a. Show that H' is normal over K.

   Let S denote the Galois group of H'/K and T the subgroup corresponding to H.
   b. Show that $T = [S, S]$ and that $[T, T] = 0$.
   c. Show that there exist a homomorphism $V : S/[S, S] \to T/[T, T]$ and a commutative diagram

$$\begin{tikzcd}
Cl_K \arrow[r, "\text{can}"] \arrow[d, "\wr"] & Cl_H \arrow[d, "\wr"] \\
S/[S,S] \arrow[r, "V"] & T/[T,T]
\end{tikzcd}$$

   (The map V can be canonically defined for any subgroup T of finite index in a group S and is called the *transfer map*. When S is finite and $T = [S, S]$ it is the zero map.)

7.4. Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional ideal in the imaginary quadratic field K and suppose that $\mathfrak{b}$ is coprime to 6 and the discriminant of K. Let B be a matrix such that $B\mathfrak{a} = \mathfrak{a}\bar{\mathfrak{b}}^2$. Show that $\sqrt[24]{\phi_B(\mathfrak{a})}$ generates $\mathfrak{b}$ in the Hilbert class field of K.