Joachim Wehler

Modular Forms and Elliptic Curves

DRAFT, Release 1.50

April 16, 2021

I prepared these notes for the participants of the lectures. The lecture took place at the mathematical department of LMU (Ludwig-Maximilians-Universität) at Munich. The first time during the winter term 2017/18 and then during the winter term 2020/21. Some parts of the notes rely on notes of an unpublished lecture of O. Forster.

Compared to the oral lecture in class these written notes contain some additional material.

I thank all participants - in particular W. Hensgen - for pointing out some errors and for their proposals for improvement. Please report to

wehler@math.lmu.de

any further errors or typos, adding the version of the lecture notes.

Release notes:

- *Release 1.50*: Update acknowledgment.
- *Release 1.49*: Chapter 5. Remark 5.15 moved from Chapter 7. Chapter 7. Revision.
- *Release 1.48*: Chapter 6. Revision, Lemma 6.21 added.
- *Release 1.47*: Chapter 5. Proposition 5.9 added.
- *Release 1.46*: Chapter 3 and Chapter 2. Revision.
- *Release 1.45*: Chapter 4. Revision.
- *Release 1.44*: Chapter 5. Revision.
- *Release 1.43*: Chapter 5. Theorem 5.25 proof corrected.
- *Release 1.42*: Chapter 5. Theorem 5.25 corrected. Chapter 6 minor revisions.
- *Release 1.41*: Chapter 7. Section 7.2 added. Chapter 5. Theorem 5.23 expanded. Theorem 5.25 expanded and corollary integrated.
- *Release 1.40*: Chapter 7. Section 7.1 added.
- *Release 1.39*: Chapter 4. Proposition 4.25 expanded.
- *Release 1.38*: Chapter 6. Sections 6.1 and 6.2 added.
- *Release 1.37*: Chapter 5. Section 5.2, Lemma 5.24 replaced by new version, subsequent Corollary added, Theorem 5.25 adapted, renumbering, Section 5.3 added.
- *Release 1.36*: Chapter 5. Section 5.2, Proposition 5.28 added, minor revision.
- *Release 1.35*: Chapter 5. Section 5.2 added.
- *Release 1.34*: Chapter 5. Section 5.1, minor revision.
- *Release 1.33*: Chapter 4. Example 4.39 expanded.
- *Release 1.32*: Chapter 5. Section 5.1 added.
- *Release 1.31*: Chapter 4. Section 4.2, Definition 4.19 expanded, Lemma 4.30 and Theorem 4.31 clarified, Remark 4.27 added, renumbering, minor revision. Section 4.3 added.

- *Release 1.30*: Chapter 4. Section 4.2, Example 4.36 added, minor revision.
- *Release 1.29*: Chapter 3, Lemma 3.4, exponent of determinant changed. Chapter 4, Example 4.4 added. Renumbering, Section 4.2 added.
- *Release 1.28*: Chapter 4. Proposition 4.8, proof corrected. Section 4.1, minor revisions.
- *Release 1.27*: Chapter 2, Remark 2.30, formulas corrected by extended Legendre symbol and Kronecker symbol. Chapter 4, Proposition 4.6 added, minor revisions, renumbering. List of results updated.
- *Release 1.26*: Chapter 3, proof of Lemma 3.4: formula corrected. Chapter 4, minor revisions
- *Release 1.25*: Chapter 4, Section 4.1 added.
- *Release 1.24*: Minor revisions.
- *Release 1.23*: Minor revisions.
- *Release 1.22*: Chapter 3 completed.
- *Release 1.21*: Section 3.2, some typos corrected.
- *Release 1.20*: Minor revisions.
- *Release 1.19*: Minor revisions.
- *Release 1.18*: Chapter 2, Remark 3.5 added.
- *Release 1.17*: Minor revisions.
- *Release 1.16*: Chapter 2, Remark 2.8, Example 2.11, Lemma 2.26 corrected. Chapter 3, Section 3.1 reordered.
- *Release 1.15*: Chapter 3, Remark 3.7 added, Remark 3.7 expanded, minor revisions, renumbering.
- *Release 1.14*: Minor revisions.
- *Release 1.13*: Chapter 3, Section 3.2 added. List of results added.
- *Release 1.12*: Chapter 1, Proposition 1.19 added, renumbering. Chapter 2, Remark 2.17 added, renumbering. Chapter 3, Section 3.1 added.
- *Release 1.11*: Chapter 2 completed.
- *Release 1.10*: Chapter 2, Section 2.2 correction of some typos.
- *Release 1.9*: Chapter 1, revision of Corollary 1.9 and 1.10, Lemma 1.13, Corollary 1.15 and Theorem 1.21. Further minor revisions.
- *Release 1.8*: Chapter 2 minor revision.
- *Release 1.7*: Chapter 2 minor revision, some additions.
- *Release 1.6*: Chapter 2 minor revision.
- *Release 1.5*: Chapter 2, Sections 2.1 and 2.2 added.
- *Release 1.4*: Chapter 1, minor revision.
- *Release 1.3*: Introduction added.
- *Release 1.2*: Chapter 1, minor revision.
- *Release 1.1*: Complete revision, starting with Chapter 1.

Contents

Introduction

Modular Forms and elliptic curves are a classical domain from mathematics. At least, since the proof of Fermat's last conjecture the domain attracts widespread attention. The domain of Modular Forms integrates the three mathematical disciplines Complex Analysis, Algebraic Geometry, and Algebraic Number Theory.

Elliptic curves can be investigated by different mathematical methods.

- Algebraic geometry: Elliptic curves are the zero-sets of polynomials.
- Complex analytic geometry: When considered as Riemann surfaces then elliptic curves are complex tori.
- Arithmetic geometry: Elliptic curves can be defined over different fields, e.g. over $\mathbb{Q}$ or $\mathbb{F}_p$ and over the ring $\mathbb{Z}$.

The algebraic point of view identifies complex elliptic curves with smooth cubic hypersurfaces of $\mathbb{P}^2$. Hence elliptic curves are the first ones in the series of cubic hypersurfaces in complex projective space $\mathbb{P}^n$, $n \geq 2$. The higher dimensional cubics are also challenging examples, see [29, Chap.V, §4], [31].

Chapter 1 introduces elliptic functions as doubly periodic, meromorphic functions in the complex plane $\mathbb{C}$. The period group is a lattice $\Lambda \subset \mathbb{C}$. The main tool to study elliptic function is the residue theorem.

Chapter 2 characterizes elliptic functions as meromorphic functions on the torus $\mathbb{C}/\Lambda$. The classes of biholomorphically equivalent complex tori are the orbits of a group action of the modular group

$$\Gamma \times \mathbb{H} \to \mathbb{H}$$

The quotients

$$\Gamma_0(N) \setminus \mathbb{H}$$

of the restricted action of the Hecke congruence subgroups

$$\Gamma_0(N) \subset \Gamma$$

are Riemann surfaces with compactifications $X_0(N)$.

Chapter 3 introduces modular forms and cusp forms as holomorphic functions on $\mathbb{H} \cup \{\infty\}$ with a certain transformation behaviour with respect to the $\Gamma_0(N)$-action. These functions unreveal themselves as meromorphic differential forms on the modular curve $X_0(N)$. The Riemann-Roch theorem computes the dimensions of the vector spaces of modular forms and cusp forms.

Chapter 4 makes a new start from the viewpoint of algebraic geometry: Complex tori embed as elliptic curves into the complex projective plane. They can be represented as non-singular cubic curves, defined as zero set of a Weierstrass polynomial. The main tool to represent a complex torus as an elliptic curve is the Weierstrass $\wp$-function and its differential equation. Conversely, each complex elliptic curve arises as embedding of a complex torus.

Choosing different fields for the coefficents of the Weierstrass polynomials allows to consider elliptic curves defined over $\mathbb{C}, \mathbb{Q}, \mathbb{Z}$ or even over the finite fields $\mathbb{F}_p$. The focus of the chapter are some relations between complex analytic geometry, algebraic geometry and arithmetic geometry.

Chapter 5 considers families of Hecke operators, which are linear endomorphisms on the finite dimensional vector spaces of modular forms. Each family of Hecke operators acts on a given vector space of modular forms of fixed weight. On the corresponding subspace of cusp forms the family can be diagonalized simultaneously, a result which relies on the Petersson scalar product. As an application the chapter proves some theorems from algebraic number theory related to Lagrange, Jacobi, Ramanujan, Mordell and other mathematicians.

In the second, more advanced part of the lecture notes Chapter 6 deals with deeper applications of the theory of modular forms to algebraic number theory. The chapter investigates the relation between tori with complex multiplication and imaginary quadratic number fields. The main role is played by the modular invariant j. As an application the chapter proves a lower bound of the class number.

The final Chapter 7 gives an outlook to the modularity theorem for elliptic curves, which plays the dominant role in Wiles' proof of the Fermat conjecture. A second section gives an outlook to the moonshine relation between the Fourier coefficients of the modular j-invariant and the dimensions of the irreducible representations of the monster group, which at day culminates in the work of Borcherds.

It is also the aim of these lecture notes to illustrate their results and the outlook by a series of numerical calculations using a computer algebra system.

PARI files

Chapter 1:

- `Weierstrass_p_function_08`: Laurent expansion of the Weierstrass $\wp$-function and its derivative, cf. Remark 1.14.

Chapter 2

- `modular_curve_as_covering`: Genus, degree and further parameters of modular curve $X_0(N)$, cf. Remark 2.30.

Chapter 3

- `Congruence_subgroup_19`: Dimension of $M_k(\Gamma_0(p^n))$ via Riemann-Roch, cf. Remark 3.27.

Chapter 4

- `Torus_to_Weierstrass_equation_01`: The plane cubic of an embedded torus, cf. Example 4.4
- `Elliptic_curve_plot_06`: Plot of some plane cubics, cf. Example 4.29.
- `Elliptic_curve_02`: Invariants of some plane cubics, cf. Example 4.29.
- `Elliptic_curve_weierstrass_equation_12`: Global minimal Weierstrass polynomial and its discriminant, cf. Example 4.39.
- `Elliptic_curve_Hasse_estimate_05`: Hasse estimate for number of $\mathbb{F}_p$-rational points, cf. Remark 4.42.
- `Elliptic_curve_04_02`: Analytic rank of elliptic curves, cf. Remark 4.47.

Chapter 5

- `Hecke_matrix_02`: Hecke operator $T_2 \in End(S_{28}(\Gamma))$, cf. Example 5.14.

- `Congruence_subgroup_20`: Oldforms and newforms for different $\Gamma_0(N)$, cf. Example 5.30.

- `Modular_forms_theta_01`: 4-squares theorem and similar decompositions, cf. Example 5.39.

Chapter 6

- `modular_polynomial_01`: Modular polynomials of different levels, cf. Example 6.9.

- `modular_polynomial_02`: The polynomials Φ_m and their factorization, cf. Example 6.11.

Chapter 7

- `Elliptic_curve_taniyama_10`: Illustration of Wiles' theorem by some numerical examples, cf. Example 7.7.

The PARI-files of these lecture notes are contained in a separate folder. It is recommended to download all of them together, because some of them will call other files. After downloading the PARI files into the working directory of PARI a given file can be called by the command

```
\r filename
```

For more information see the PARI manual from the PARI homepage.

Part I
General Theory

The context of Chapter 1 is complex analysis on domains in the complex plane. The base field is the field $\mathbb{C}$ of complex numbers. We develop the theory of elliptic functions, i.e. doubly periodic meromorphic functions. Classical tools are Laurent series and the residue theorem for meromorphic functions. The period group of doubly periodic functions are lattices in $\mathbb{C}$.

The view point of Chapter 2 are compact Riemann surfaces. We continue working with the base field $\mathbb{C}$, but now the domain is a complex manifold. The most simple example of a compact Riemann surface is the Riemann sphere $\mathbb{P}^1(\mathbb{C})$. Meromorphic functions are holomorphic maps into the Riemann sphere. A second class of compact Riemann surfaces are complex tori. The doubly periodic meromorphic functions from Chapter 1 are meromorphic functions on a complex torus. The main tools from the theory of Riemann surfaces are line bundles, divisors and the Theorem of Riemann-Roch. The set of isomorphy classes of complex tori turns out to be the orbit space of the modular group $SL(2,\mathbb{Z})$ acting on the upper half plane $\mathbb{H}$. We show that the compactified orbit space is biholomorphic equivalent to $\mathbb{P}^1(\mathbb{C})$.

Chapter 4 switches from the analytic theory to an algebraic context. We consider the Riemann sphere from an algebraic point of view and study non-singular curves C in the projective space $\mathbb{P}^1(\mathbb{C})$, now equipped with the Zariski topology. These curves are the zero set of one or more homogeneous polynomials. The smallest subfield $k \subset \mathbb{C}$ which comprises their coefficients is the field of definition of C. As a consequence we extend the range of base fields under consideration to the field $\mathbb{Q}$ and to the residue fields $\mathbb{F}_{p^n}$ of $\mathbb{Z}$. The Weierstrass $\wp$-function and its derivative $\wp'$ from Chapter 1 embedd a given torus into $\mathbb{P}^2(\mathbb{C})$. The image is as an elliptic curve E. It is the zero set of a Weierstrass polynomial F, a homogeneous polynomial of degree 3. If all coefficients of F are rational and if in addition a Q-valued point of E exists, then E is a rational elliptic curve. The existence of a rational point $O \in E(\mathbb{Q})$ allows to equip $E(\mathbb{Q})$ with an additive group structure having O as neutral element. Rational elliptic curves have a Weierstrass polynomial F with integer coefficients. We study the reduction E_p of E modulo the primes $p \in \mathbb{Z}$. The sequence $(card\ E_p)_{p\ prime}$ encodes important arithmetic properties of a rational elliptic curve.

Chapter 3 takes up the study of the modular group from Chapter 2. We extend the operation of $\Gamma := SL(2,\mathbb{Z})$ on $\mathbb{H}$ to an operation on the vector space of holomorphic functions on $\mathbb{H}$. Those functions which are symmetric with respect to this operation are named resp. modular forms and cusp forms. All of them develop into a Fourier series around the point ∞. Due to their symmetry modular forms correspond bijectively to meromorphic sections of the line bundle Ω^1 and its tensor products defined on the compactified orbit space $\mathbb{P}^1(\mathbb{C})$. The complex vector spaces of sections are finite dimensional, their dimension can be computed by the theorem of Riemann-Roch. Taking the tensor product as multiplication provides the direct sum of these vector spaces with the structure of a finitely generated graded algebra forms $M_*(\Gamma) = \oplus_k M_k(\Gamma)$. The grading is given by the weight of the modular forms. The algebra of modular forms $M_*(\Gamma)$ contains the ideal of cusp forms $S_*(\Gamma) = \oplus_k S_k(\Gamma)$. On $M_*(\Gamma)$ acts the family of Hecke operators as an Abelian algebra of endomorphisms. The ideal $S_*(\Gamma)$ is stable with respect to this

action. Each component $S_k(\Gamma)$ has a basis of eigenforms with respect to the Hecke algebra. For each eigenform f the family of eigenvalues reveals remarkable relations from the arithmetic of the Fourier coefficients of f. These relations make up the *magic of modular forms*.

Chapter 1
Elliptic functions

The chapter starts with complex analysis in the plane. Subsequently the results are translated into the language of Riemann surface. Here they are combined with some results from algebraic topology. A final section applies the Riemann-Roch theorem to prove Abel's theorem about divisors on complex tori.

1.1 The field of elliptic functions

The present section deals with complex analysis in the plane, i.e. we study holomorphic and meromorphic functions on domains in the complex plane $\mathbb{C}$.

The trigonometric functions *sin* and *cos* are examples of periodic holomorphic functions, while *tan* and *cot* are periodic meromorphic. All periods of these functions are integer multiples of respectively 2π and π. Elliptic functions are meromorphic with period group isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$.

Recall that a meromorphic function on a domain $G \subset \mathbb{C}$ is a holomorphic function

$$f : G \setminus S \to \mathbb{C}$$

with a discrete closed subset $S \subset G$ of poles of f - but no essential singularities.

Definition 1.1 (Period of a meromorphic function). Consider a meromorphic function f on a domain G. A number $\omega \in \mathbb{C}$ is a *period* of f if

- for all $z \in G$ also $z \pm \omega \in G$
- and for all $z \in G \setminus P$
$$f(z+\omega) = f(z).$$

Only seemingly Definition 1.1 excludes the poles from the definition of periodicity. A pole z_0 of f is an isolated singularity of f. Therefore the function f expands into a convergent Laurent series around z_0

$$f(z) = \sum_{n \geq n_0}^{\infty} a_n \cdot (z - z_0)^n$$

with coefficients

$$a_n = \frac{1}{2\pi i} \int\limits_{|z-z_0|=\varepsilon} \frac{f(z)}{(z-z_0)^{n+1}}\, dz \text{ for suitable } \varepsilon > 0.$$

If f has the period ω then the Laurent expansions of f around z_0 and $z_0 + \omega$ are the same because the integrands attain the same value at z and $z + \omega$. Hence periodicity of f includes also the poles.

Example 1.2 (Periodic meromorphic functions).

1. The functions $\sin, \cos : \mathbb{C} \to \mathbb{C}$ are holomorphic with period $\omega = 2\pi$.

2. The tangent-function is meromorphic on $\mathbb{C}$ with singularities $(\pi/2) + k\pi$, $k \in \mathbb{Z}$, and period $\omega = \pi$.

3. The exponential function $\mathbb{C} \to \mathbb{C}^*, z \mapsto e^{2\pi i z}$, is holomorphic with period $\omega = 1$.

If a meromorphic function f has a period $\omega \neq 0$ one can ask for the set of all periods. Apparently elements of the form $k\omega$, $k \in \mathbb{Z}$ are also periods of f. How many independent periods of f exist?

Definition 1.3 (Discrete subgroup). A subgroup $\Gamma \subset (\mathbb{C}, +)$ is a *discrete subgroup*, if the subspace topology of Γ is discrete, i.e. any $g \in \Gamma$ has an open neighbourhood $U \subset \mathbb{C}$ with

$$U \cap \Gamma = \{g\}.$$

Proposition 1.4 (Period group). *Consider a non-constant meromorphic function f on a domain $G \subset \mathbb{C}$. The set Γ_f of all periods of f is a discrete subgroup of $\mathbb{C}$. It is named the* period group *of f.*

Proof. i) Apparently Γ_f is a subgroup.

ii) If Γ_f were not discrete then a convergent sequence $(\omega_n)_{n\in\mathbb{N}}$ of pairwise distinct periods $\omega_n \in \Gamma_f$ would exist.

Hence for an arbitrary but fixed $z_0 \in G$, which is not a pole of f, and for all $n \in \mathbb{N}$

$$f(z_0) = f(z_0 + \omega_n).$$

The identity theorem implies that f is constant, a contradiction, q.e.d.

Proposition 1.5 (Discrete subgroups of $(\mathbb{C},+)$). *Each discrete subgroup*

$$\Gamma \subset (\mathbb{C},+)$$

belongs to one of the following types:

1. Rank $= 0$*:*
$$\Gamma = \{0\}$$
2. Rank $= 1$*:*
$$\Gamma = \mathbb{Z}\omega = \{m \cdot \omega : m \in \mathbb{Z}\}$$
with a suitable element $\omega \in \mathbb{C}^*$.
3. Rank $= 2$*:*
$$\Gamma = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 = \{m_1 \cdot \omega_1 + m_2 \cdot \omega_2 : \ m_1, m_2 \in \mathbb{Z}\}$$
with $\omega_1, \omega_2 \in \mathbb{C}$ linearly independent over the base field $\mathbb{R}$. The subgroup Γ is named a lattice*.*

For a proof see [1, Chap. 7, Sect. 2.1].

Note. If we specify a lattice in the form

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

we will assume that the basis (ω_1, ω_2) is *positively oriented*, i.e.

$$det \begin{pmatrix} Re\ \omega_1 & Re\ \omega_2 \\ Im\ \omega_1 & Im\ \omega_2 \end{pmatrix} > 0.$$

Definition 1.6 (Elliptic function). Consider a non-constant meromorphic function f on a domain $G \subset \mathbb{C}$ with period group Γ_f.

- If *rank* $\Gamma_f \geq 1$ then f is named *periodic*.

- If *rank* $\Gamma_f = 2$ then f is named *doubly periodic*. Its period group

$$\Gamma_f = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

is also named the *period lattice* of f, see Figure 1.1. The subset

$$P = \{\lambda_1\omega_1 + \lambda_2\omega_2 : 0 \leq \lambda_1, \lambda_2 < 1\}$$

is the *fundamental period parallelogram* of f with respect to the basis (ω_1, ω_2).

A doubly periodic meromorphic function on $\mathbb{C}$ is an *elliptic function* with respect to a lattice Λ if

$$\Lambda \subset \Gamma_f$$

i.e. if all lattice points $\omega \in \Lambda$ are periods of f.

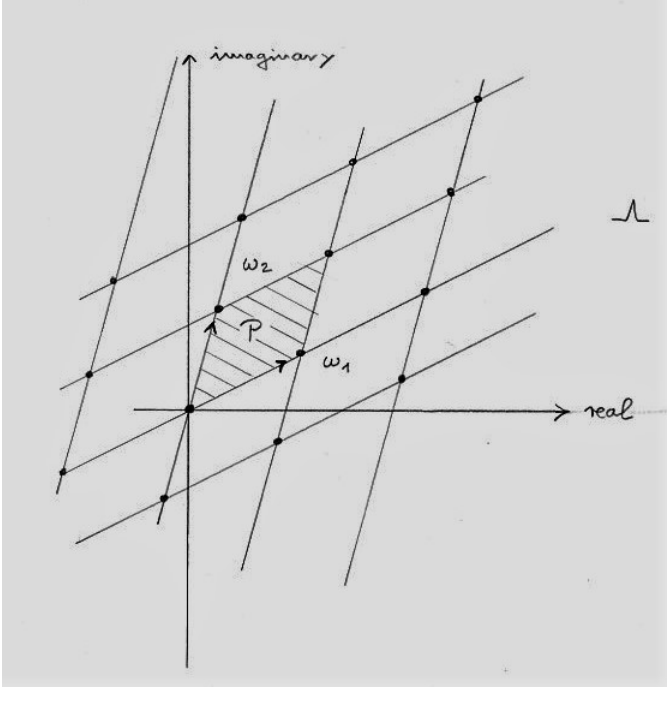


Fig. 1.1 Period lattice Λ

Which elliptic functions do exist? Proposition 1.7 shows that it is not interesting to study the subclass of holomorphic elliptic functions. Therefore we will focus on

meromorphic functions with poles. See Proposition 1.8, and its corollaries about the value attainment of elliptic functions.

Proposition 1.7 (Constant elliptic functions). *Any holomorphic elliptic function*

$$f : \mathbb{C} \to \mathbb{C}$$

is constant.

Proof. An entire function f is holomorphic and attends the maximum of its modulus on its closed period parallelogram which is a compact set. Being a bounded entire function, f is constant according to Liouville's theorem, q.e.d.

Proposition 1.8 (Residue theorem for elliptic functions). *An elliptic function f with period parallelogram P satisfies*

$$\sum_{\zeta \in P} res_\zeta(f) = 0.$$

Proof. The boundary ∂P comprises only finitely many poles of f. Therefore we can choose a number $a \in \mathbb{C}$ such the boundary of the translated period parallelogram

$$P_a := a + P$$

contains no poles of f. The residue theorem implies

$$\frac{1}{2\pi i} \int_{\partial P_a} f(z)\, dz = \sum_{\zeta \in P_a} res_\zeta(f) = \sum_{\zeta \in P} res_\zeta(f).$$

The integrand on the left-hand side is doubly periodic. Therefore the integration along opposite sides of the period parallelogram cancels and the whole integral vanishes, q.e.d.

Corollary 1.9 (Poles and zeros of elliptic functions).

1. *There are no elliptic functions f with one pole of order $= 1$ modulo the period lattice Γ_f and no other pole mod Γ_f.*

2. *There are no elliptic functions f with only one zero of order $= 1$ modulo the period lattice Γ_f and no other zero mod Γ_f.*

Proof. 1. A pole of order 1 at $a \in \mathbb{C}$ has $res_a(f) \neq 0$, which contradicts Proposition 1.8.

2. Apply part 1) to the elliptic function $1/f$, q.e.d.

Corollary 1.10 (Counting poles and zeros of elliptic functions). *Any non-constant elliptic function f attains modulo each lattice*

$$\Lambda \subset \Gamma_f$$

all values $a \in \mathbb{C} \cup \{\infty\}$ with the same multiplicity. In particular, f has mod Λ the same number of poles and zeros taken with multiplicity.

Proof. The case $a \neq \infty$ reduces to the second claim by considering the function $f - a$. It has the same poles as f. Therefore it suffices to show that f has the same number of zeros and poles, taken with multiplicity. Moreover it suffices to prove the theorem for $\Lambda = \Gamma_f$.

We apply Proposition 1.8 to the meromorphic function f'/f and obtain

$$\sum_{\zeta \in P} res_\zeta \left(\frac{f'}{f} \right) = 0.$$

Each residue evaluates to

$$res_\zeta \left(\frac{f'}{f} \right) = \begin{cases} k & \text{f has a zero of order } k \text{ at } \zeta \\ -k & \text{f has a pole of order } k \text{ at } \zeta \end{cases}$$

q.e.d.

1.2 The Weierstrass $\wp$-function

In the present section we consider an arbitrary but fixed lattice

$$\Lambda := \mathbb{Z}\, \omega_1 + \mathbb{Z}\, \omega_2.$$

We use the notation $\Lambda' := \Lambda \setminus \{0\}$. Moreover P denotes the fundamental period parallelogram of Λ.

The $\wp$-function of Λ is a distinguished elliptic function: All elliptic functions of the given lattice Λ derive from $\wp$ and its derivative $\wp'$.

Lemma 1.11 (Lattice constants). *For $k > 2$ the infinite series*

$$G_{\Lambda,k} := \sum_{\omega \in \Lambda'} \frac{1}{\omega^k}$$

is absolutely convergent. Its value is named the lattice constant *of Λ.*

Proof. We choose the exhaustion of Λ by the sequence $(\Lambda_n)_{n\in\mathbb{N}}$ of disjoint sets of indices of increasing modulus

$$\Lambda_n := \{\mu\cdot\omega_1+\nu\cdot\omega_2\in\Lambda:\ \mu,\nu\in\mathbb{Z};\ |\mu|,|\nu|\le n \text{ and } (|\mu|=n \text{ or } |\nu|=n)\},$$

i.e.

$$\Lambda = \dot{\bigcup}_{n\in\mathbb{N}}\Lambda_n.$$

Then

$$card\ \Lambda_n = 8n.$$

A suitable constant c exists with $|\omega|\ge c\cdot n$ for all $n\in\mathbb{N}$ and for all $\omega\in\Lambda_n$. Therefore

$$\sum_{\omega\in\Lambda_n}\frac{1}{|\omega|^k}\le\frac{8\cdot n}{c^k\cdot n^k}\le\left(\frac{8}{c^k}\right)\cdot\frac{1}{n^{k-1}}.$$

For $k>2$

$$\sum_{n=1}^{\infty}\frac{1}{n^{k-1}}<\infty.$$

Therefore the claim follows from

$$\sum_{\omega\in\Lambda'}\frac{1}{\omega^k}=\sum_{n=1}^{\infty}\left(\sum_{\omega\in\Lambda_n}\frac{1}{\omega^k}\right),\ q.e.d.$$

We will study elliptic functions with period lattice Λ. According to Corollary 1.9 a candidate f for the most simple example would have only one pole mod Λ, the pole having order $=2$ and residue $=0$. The Laurent expansion of f around $z_0=0$ would start

$$f(z)=\frac{1}{z^2}+a_1\cdot z+O(2).$$

Being doubly periodic, f would have poles exactly at the points $\omega\in\Lambda$. The following Theorem 1.12 shows that such a function actually exists.

Theorem 1.12 (Weierstrass $\wp$-function). *For each lattice Λ the series*

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

is absolutely and compactly convergent for all $z\in\mathbb{C}\setminus\Lambda$. It defines an even elliptic function $\wp$ with respect to Λ, named the Weierstrass $\wp$-function *of Λ. The pole set of $\wp$ is Λ, each pole has order $=2$.*

If we consider only the first summand with fixed z then

$$\frac{1}{(z-\omega)^2}\sim\frac{1}{\omega^2}.$$

Therefore the series with these summands alone does not converge. We will show that the difference

$$\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}$$

is proportional to

$$\frac{1}{\omega^3}.$$

Therefore the series $\wp(z)$ converges.

Note: TeX reserves the separate symbol "backslash wp" to denote the Weierstrass function $\wp$.

Proof. We recall the definition of compact convergence of a sequence $(f_\nu)_{\nu\in\mathbb{N}}$ of meromorphic functions on a domain $G\subset\mathbb{C}$, cf. [62]: For each compact subset $K\subset G$ exists an index $\nu_0\in\mathbb{N}$ such that

- for all $\nu>\nu_0$ the function f_ν has no pole in K
- the sequence $(f_\nu)_{\nu>\nu_0}$ is uniformly convergent on K.

i) *Meromorphic with pole set* Λ: For each compact set $K\subset\mathbb{C}$ only finitely many summands of $\wp$ have a pole in K. We show that the remaining series converges absolutely and uniform on K: Choose an arbitrary but fixed $R>0$. For

$$|z|\le R \text{ and } 2R\le|\omega|$$

holds

$$\frac{|\omega|}{2}-|z|\ge 0.$$

The triangle inequality

$$|z-\omega|=|\omega-z|\ge||\omega|-|z||=\left|\frac{|\omega|}{2}-|z|+\frac{|\omega|}{2}\right|\ge\frac{|\omega|}{2}$$

implies the estimate

$$\left|\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right|=\left|\frac{\omega^2-(z-\omega)^2}{\omega^2\cdot(z-\omega)^2)}\right|\le\frac{|-z^2+2z\omega|}{|\omega|^2\cdot\left(\frac{|\omega|}{2}\right)^2}\le 4\cdot\frac{|z|^2+2\cdot|z|\cdot|\omega|}{|\omega|^4}\le$$

$$\le 4\cdot\frac{|z|^2}{|\omega|^4}+8\cdot\frac{|z|}{|\omega|^3}\le\frac{4\cdot R^2}{2\cdot R\cdot|\omega|^3}+8\cdot\frac{R}{|\omega|^3}=10\cdot\frac{R}{|\omega|^3}$$

independent from $|z|<R$.

According to Lemma 1.11 the series

$$\sum_{\omega\in\Lambda'}\frac{1}{\omega^3}$$

converges absolutely. For $|z|\le R$ we decompose the series with respect to the summation over $\omega\in\Lambda$

$$\left[\frac{1}{z^2}+\sum_{\omega\in\Lambda',|\omega|<2R}\left(\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right)\right]+\left[\sum_{\omega\in\Lambda,|\omega|\ge 2R}\left(\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right)\right]$$

The first summand is meromorphic with poles exactly at the points $z\in\Lambda\cap D_{2R}(0)$. The second summand converges absolutely and compactly on $D_{2R}(0)$ due to Lemma 1.11, and defines a holomorphic function on $D_{2R}(0)$.

Because R can be choosen arbitrary, the series $\wp$ is compact convergent and defines a meromorphic function on $\mathbb{C}$ with pole set Λ.

ii) *Even function with periods from* Λ:

- $\wp$ is even: It is admissible to rearrange the summation by replacing ω by $-\omega$, because the series is absolute convergent

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

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

- $\wp$ has periods from Λ: The derivative is

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

Apparently for each fixed $\omega_0\in\Lambda$

$$\wp'(z+\omega_0)=\wp'(z)$$

after rearranging the summation by replacing ω by $\omega-\omega_0$. As a consequence

$$\wp(z+\omega_j)=\wp(z)+c_j$$

with two suitable constants $c_j\in\mathbb{C},\ j=1,2$.

For $j=1,2$ choosing the specific arguments

$$z:=-\omega_j/2,$$

and using that $\wp$ is even implies

$$\wp(\omega_j/2) = \wp((-\omega_j/2)+\omega_j) = \wp(-\omega_j/2)+c_j = \wp(\omega_j/2)+c_j$$

Hence

$$c_j = 0,\ q.e.d.$$

Lemma 1.13 (Half-periods of a lattice). *Consider a lattice*

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

and denote by

$$Z_{(\omega_1,\omega_2)} := \left\{ \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2} \right\}$$

the set of half-periods of its fundamental period parallelogram with respect to (ω_1,ω_2). *The derivative* $\wp'$ *of the Weierstrass function* $\wp$ *of* Λ *has mod* Λ

- *a pole of order* $= 3$ *at* $0 \in \mathbb{C}$ *and no other poles,*
- *and exactly three zeros, represented by the points of* $Z_{(\omega_1,\omega_2)}$.

Proof. Consider $u \in Z_{(\omega_1,\omega_2)}$. According to Theorem 1.12 the function $\wp$ has no pole at u. The derivative $\wp'$ has the same pole set as $\wp$. Because $\wp$ is even, the function $\wp'$ is an odd elliptic function

$$\wp'(u) = -\wp'(-u) = -\wp'(-u+2u) = -\wp'(u).$$

Therefore

$$\wp'(u) = 0,$$

i.e. each point of $Z_{(\omega_1,\omega_2)}$ is a zero of $\wp'$ within the fundamental period parallelogram. Hence $\wp'$ has at least three zeros mod Λ.

Moreover $\wp'$ like $\wp$ has a single pole at $0 \in \mathbb{C}$ mod Λ. The pole of $\wp'$ has order $= 3$. Corollary 1.10 implies that $\wp'$ has exactly three zeros mod Λ. As a consequence, the points of $Z_{(\omega_1,\omega_2)}$ represent exactly the zeros of $\wp'$, and each zero has order $= 1$, q.e.d.

Note that the determination of the two zeros mod Λ of $\wp$ is much more delicate [19].

Remark 1.14 (Weierstrass function $\wp$). Figure 1.2 shows the Laurent expansion around $0 \in \mathbb{C}$ of the Weierstrass function $\wp$ and its derivative $\wp'$ for the two lattices Λ

- with basis $(1, \rho = e^{2\pi i/3})$
- and basis $(1, i)$.

See PARI file "Weierstrass_p_function_08". The numerical calculation confirms that $\wp$ is an even function and that $\wp'$ vanishes at the half-lattice points of Λ.

```
====================================================
Weierstrass p-function, Start

Lattice with normalized periods (omega_1,omega_2) = (-1/2 + 0.8660254038*I,1)

Weierstrass p-function wp:

x^-2 + 0.0000000000*x^2 + 29.31515847*x^4 + 0.0000000000*x^6 + 0.0000000000*x^8 + 66.10603969*x^10 + 0.0000000000*x^12 + O(x^14)

Derivation wp_prime:

-2*x^-3 + 0.0000000000*x + 117.2606339*x^3 + 0.0000000000*x^5 + 0.0000000000*x^7 + 661.0603969*x^9 + 0.0000000000*x^11 + O(x^13)

wp_prime at half-lattice points =
-1/4 + 0.4330127019*I: 0.000000000000000000000000000000000001730233709 - 0.000000000000000000000000000000000002162792136*I
1/2: 0.0000000000 + 0.0000000000*I
1/4 + 0.4330127019*I: -0.000000000000000000000000000000000001730233709 - 0.000000000000000000000000000000000002162792136*I

Weierstrass p-function, End
====================================================
```

```
====================================================
Weierstrass p-function, Start

Lattice with normalized periods (omega_1,omega_2) = (I,1)

Weierstrass p-function wp:

x^-2 + 9.453636006*x^2 + 0.000000000000000000000000000000000006577345622*x^4 + 29.79041125*x^6 + 0.000000000000000000000000000000000
1695813584*x^8 + 43.32733914*x^10 + 0.000000000000000000000000000000000003562578745*x^12 + O(x^14)

Derivation wp_prime:

-2*x^-3 + 18.90727201*x + 0.000000000000000000000000000000000002630938249*x^3 + 178.7424675*x^5 + 0.000000000000000000000000000000001
356650867*x^7 + 433.2733914*x^9 + 0.000000000000000000000000000000000004275094495*x^11 + O(x^13)

wp_prime at half-lattice points =
1/2*I: 0.000000000000000000000000000000000002635703419*I
1/2: 0.0000000000
1/2 + 1/2*I: 0.0000000000 - 0.000000000000000000000000000000000002635703419*I

Weierstrass p-function, End
====================================================
```

Fig. 1.2 Laurent expansion of $\wp$ and $\wp'$ and vanishing at half-lattice points

Theorem 1.12 shows that the $\wp$-function of the lattice Λ has all points from Λ as periods. Corollary 1.15 shows the other direction: There are no additional periods, i.e. $\Gamma_\wp = \Lambda$.

Corollary 1.15 (Period lattice of $\wp$ and $\wp'$). *The Weierstrass function $\wp$ of the lattice Λ and its derivative $\wp'$ have the period lattice Λ, i.e.*

$$\Lambda = \Gamma_\wp = \Gamma_{\wp'}$$

i.e. the only periods of $\wp$ and of $\wp'$ are the points from Λ.

Proof. We know

$$\Lambda \subset \Gamma_\wp \subset \Gamma_{\wp'}$$

Here the first inclusion has been shown in Theorem 1.12, while the second inclusion is obvious. We show

$$\Gamma_{\wp'} \subset \Lambda :$$

Let $\omega \in \Gamma_{\wp'}$ be a period of $\wp'$. Then

$$\wp'(\omega/2) = \wp'((\omega/2) - \omega) = \wp'(-\omega/2) = -\wp'(\omega/2).$$

Either $\omega/2$ is not a pole of $\wp'$. Then $\omega/2$ is a zero of $\wp'$ and 1.13 implies $\omega/2 \in \Lambda/2$ or $\omega \in \Lambda$.

Or $\omega/2$ is a pole of $\wp'$. Then Theorem 1.12 implies $\omega/2 \in \Lambda$, and in particular $\omega \in \Lambda$, q.e.d.

Proposition 1.16 (Coefficients of the Laurent expansion of $\wp$). *The Weierstrass function $\wp$ of Λ has the Laurent expansion around zero*

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} a_{2k} \cdot z^{2k}$$

with coefficients derived from the lattice constants of Λ

$$a_{2k} = (2k+1) \cdot G_{\Lambda, 2k+2}.$$

Proof. We determine for $\omega \neq 0$ the Taylor series of

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}$$

around $0 \in \mathbb{C}$: Taking the derivative

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

and expanding into a geometric series

$$\frac{-1}{z-\omega} = \frac{1}{\omega - z} = \frac{1/\omega}{1-(z/\omega)} = (1/\omega) \cdot \sum_{\nu=0}^{\infty} (1/\omega)^{\nu} \cdot z^{\nu}$$

shows

$$\frac{1}{(z-\omega)^2} = (1/\omega) \cdot \sum_{\nu=1}^{\infty} \nu \cdot (1/\omega)^{\nu} \cdot z^{\nu-1} = \sum_{\nu=0}^{\infty} (\nu+1) \cdot \frac{1}{\omega^{\nu+2}} \cdot z^{\nu}$$

and

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \sum_{\nu=1}^{\infty} (\nu+1) \frac{1}{\omega^{\nu+2}} \cdot z^{\nu}.$$

Because $\wp$ is even and the series converges absolutely, see Theorem 1.12, we obtain after rearrangement and using that $\wp$ is even

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

$$= \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) \left(\sum_{\omega\in\Lambda'} \frac{1}{\omega^{2k+2}} \right) z^{2k},\ q.e.d.$$

Theorem 1.17 (Differential equation of $\wp$). *The Weierstrass function $\wp$ of the lattice Λ satisfies the differential equation*

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

with the constants

$$g_2 := g_{\Lambda,2} := 60\cdot G_{\Lambda,4},\ g_3 := g_{\Lambda,3} := 140\cdot G_{\Lambda,6}$$

derived from the lattice constants.

Proof. To simplify the notation we omit the index Λ from the lattice constants $G_{\Lambda,k}$. Due to Proposition 1.16 the Laurent expansions start

$$\wp(z) = \frac{1}{z^2} + \sum_{k\geq 1} (2k+1)\cdot G_{2k+2}\cdot z^{2k} = \frac{1}{z^2} + 3\cdot G_4\cdot z^2 + 5\cdot G_6\cdot z^4 + O(6)$$

$$\wp'(z) = -\frac{2}{z^3} + 6\cdot G_4\cdot z + 20\cdot G_6\cdot z^3 + O(5)$$

$$\wp'(z)^2 = \frac{4}{z^6} - \frac{24\cdot G_4}{z^2} - 80\cdot G_6 + O(2)$$

$$\wp(z)^2 = \frac{1}{z^4} + 6\cdot G_4 + 10\cdot G_6\cdot z^2 + O(4)$$

$$\wp(z)^3 = \frac{1}{z^6} + \frac{6\cdot G_4}{z^2} + 10\cdot G_6 + \frac{3\cdot G_4}{z^2} + 5\cdot G_6 + O(2) = \frac{1}{z^6} + \frac{9\cdot G_4}{z^2} + 15\cdot G_6 + O(2)$$

Therefore all summands of order < 1 of the sum

$$\wp'^2 - 4\cdot\wp^3 + g_2\cdot\wp + g_3$$

cancel and

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

The left-hand side is an elliptic function. The right-hand side shows that the function is even holomorphic and vanishes at $0\in\mathbb{C}$. According to Proposition 1.7 the left-hand side is constant, i.e. zero, q.e.d.

Theorem 1.18 (Field of elliptic functions). *The field $\mathscr{M}(\Lambda)$ of elliptic functions with respect to the lattice Λ is a field extension of $\mathbb{C}$ of transcendence degree $= 1$, more precisely*

$$\mathscr{M}(\Lambda) = \mathbb{C}(\wp)[\wp']$$

with $\wp'$ algebraic over the field $\mathbb{C}(\wp)$ with quadratic minimal polynomial

$$F(T) = T^2 - 4\cdot\wp^3 + g_2\cdot\wp + g_3 \in \mathbb{C}(\wp)[T]$$

with the lattice constants

$$g_2 := 60\cdot G_{\Lambda,4},\ g_3 := 140\cdot G_{\Lambda,6}.$$

Note the equality $\mathbb{C}(\wp)[\wp'] = \mathbb{C}(\wp)(\wp')$ because $\wp'$ is algebraic over $\mathbb{C}(\wp)$.

Proof. i) Due to Theorem 1.17 we have

$$F(\wp') = 0 \in \mathbb{C}(\wp).$$

The derivative $\wp'$ is odd while $\wp$ is even. Therefore $\wp' \notin \mathbb{C}(\wp)$, and the minimal polynomial F must have degree ≥ 2.

ii) Consider an elliptic function $f \in \mathscr{M}(\Lambda),\ f \neq 0$. We show $f \in \mathbb{C}(\wp,\ \wp')$.

- We first consider the case that f has pole set Λ.

  The unique pole of f mod Λ has order $k \geq 2$ due to Corollary 1.9. We prove

  $$f \in \mathbb{C}(\wp, \wp')$$

  by induction on the pole order k.

  If $k = 2$ then for suitable $c \in \mathbb{C}$ the function

  $$f - c\cdot\wp$$

  has at most a single pole mod Λ of order < 2. Therefore the function is holomorphic, and even constant due to Corollar 1.7.

  For the induction step assume $k > 2$. On one hand, for even $k = 2m$ a suitable constant $c \in \mathbb{C}$ exists such that $f - c\cdot\wp^m$ has only poles of order $< k$. Therefore

  $$f - c\cdot\wp^m \in \mathbb{C}(\wp, \wp')$$

  by induction assumption. On the other hand, for odd $k = 2m+1$ a suitable constant $c \in \mathbb{C}$ exists such that

  $$f - c\cdot\wp^{m-1}\cdot\wp'$$

has only poles of order $< k$. By induction assumption

$$f - c \cdot \wp^{m-1} \wp' \in \mathbb{C}(\wp, \wp').$$

In both cases

$$f \in \mathbb{C}(\wp, \wp').$$

- Eventually, we consider the case of an arbitrary pole set of f.

  Then f has mod Λ only finitely many poles $z_\nu \in P \setminus \Lambda, \nu = 1, ..., n$. The function $\wp$ is holomorphic in $P \setminus \Lambda$. Hence for suitable constants $k_1, ..., k_n \in \mathbb{N}$ the function

$$f(z) \cdot \prod_{\nu=1}^{n} (\wp(z) - \wp(z_\nu))^{k_\nu}$$

has poles at most in Λ. According to the first part

$$f(z) \cdot \prod_{\nu=1}^{n} (\wp(z) - \wp(z_\nu))^{k_\nu} \in \mathbb{C}(\wp, \wp').$$

Therefore

$$f \in \mathbb{C}(\wp, \wp'),\ q.e.d.$$

Proposition 1.19 (Discriminant). *For a given lattice*

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$$

the cubic polynomial

$$G_\Lambda(T) := 4T^3 - g_2 \cdot T - g_3 \in \mathbb{C}[T],\ g_2 := 60 \cdot G_{\Lambda,4},\ g_3 := 140 \cdot G_{\Lambda,6}$$

has three pairwise distinct zeros: The values $\wp(\omega) \in \mathbb{C}$ at the half-period points of Λ

$$\omega \in Z_\Lambda := \{\omega_1/2,\ \omega_2/2,\ (\omega_1 + \omega_2)/2\}$$

As a consequence, the discriminant

$$discr(G_\Lambda) = \frac{1}{2^4} \cdot (g_2^3 - 27 \cdot g_3^2) \in \mathbb{C}$$

of the polynomial $G_\Lambda(T)$ is non-zero, in particular

$$g_2^3 - 27 \cdot g_3^2 \neq 0.$$

Proof. 1. *Pairwise distinct zeros*: The differential equation of $\wp'$ from Theorem 1.17 implies

$$\wp'(\omega)^2 = 4 \cdot \wp(\omega)^3 - g_2 \cdot \wp(\omega) - g_3 = G_\Lambda(\wp(\omega))$$

Due to Lemma 1.13

$$\omega \in Z_\Lambda \implies G_\Lambda(\wp(\omega)) = 0$$

and the function $\wp$ assumes at the half-period $\omega \in Z_\Lambda$ the value $\wp(\omega)$ with multiplicity at least $= 2$ because $\wp\,'(\omega) = 0$. In case

$$\wp(\omega) = \wp(\omega') \text{ for } \omega \neq \omega' \in Z_\Lambda$$

the elliptic function $\wp$ would assume the value $\wp(\omega)$ with multiplicity at least $= 4$. We would obtain a contradiction to Corollary 1.10 that the elliptic function $\wp$ assumes *mod* Λ each value with multiplicity $= 2$. Hence

$$\wp(\omega) \neq \wp(\omega').$$

2. *Discriminant*: One checks the discriminant formula

$$discr(G_\Lambda) = \frac{1}{2^4} \cdot (g_2^3 - 27 \cdot g_3^2) \in \mathbb{C},$$

e.g. see [33, Cor. 3.4]. By definition the discriminant of a polynomial is non-zero iff the zeros of the polynomial are pairwise distinct, q.e.d.

1.3 Abel's theorem

The zeros and poles of an elliptic functions cannot be prescribed in an arbitrary way: Abel's Theorem states a sufficient and necessary condition.

We continue fixing an arbitrary lattice

$$\Lambda := \mathbb{Z}\,\omega_1 + \mathbb{Z}\,\omega_2,$$

keeping the notations $\Lambda\,' := \Lambda \setminus \{0\}$ and P denoting the fundamental period parallelogram of Λ.

Proposition 1.20 (Zero and pole divisor). *Consider an elliptic function and denote by $A = (a_i)_{i=1,\dots,n}$ its family of zeros in P and by $B = (b_i)_{i=1,\dots,n}$ its family of poles in P. Then $n \geq 2$ and*

$$\sum_{i=1,\dots,n} a_i - \sum_{i=1,\dots,n} b_i \in \Lambda.$$

Note that each point p of A and B appears as often as its multiplicity as zero or pole of f indicates. By Corollary 1.9 holds $n \geq 2$, and by Corollary 1.10 both families A and B have the same cardinality.

Proof. We consider a translation

$$P_a := P + a$$

of the fundamental parallelogram such that f has neither zeros nor poles on the boundary ∂P_a. With a counter-clockwise orientation of ∂P_a the residue theorem gives

$$\frac{1}{2\pi i}\int_{\partial P_a} z\cdot\frac{f'(z)}{f(z)}\,dz = \sum_{p\in P_a} res_p\left(z\cdot\frac{f'(z)}{f(z)}\right).$$

- Right-hand side: Assume $ord(f;\ p) = k \in \mathbb{Z}^*$. Then

$$\begin{cases} p \text{ is a zero of } f \text{ of order } k & \text{if } k>0 \\ p \text{ is a pole of } f \text{ of order } k & \text{if } k<0 \end{cases}$$

  In a neighbourhood of p

$$\frac{f'(z)}{f(z)} = \frac{k}{z-p} + f_1(z)$$

  with f_1 holomorph. As a consequence

$$z\cdot\frac{f'(z)}{f(z)} = (p+(z-p))\cdot\frac{f'(z)}{f(z)} = \frac{p\cdot k}{z-p} + f_2(z)$$

  with f_2 holomorph. Therefore

$$res_p\left(z\cdot\frac{f'(z)}{f(z)}\right) = p\cdot k$$

  and

$$\sum_{p\in P_a} res_p\left(z\cdot\frac{f'(z)}{f(z)}\right) = \sum_{i=1}^{n} a_i - \sum_{i=1}^{n} b_i.$$

- Left-hand side: Denote by A,B,C,D the vertices of P_a, counter-clockwise oriented.

$$\int\limits_{\overrightarrow{AB}+\overrightarrow{CD}} z\cdot\frac{f'(z)}{f(z)}\,dz = \int\limits_{\overrightarrow{AB}} (z-(z+\omega_2))\cdot\frac{f'(z)}{f(z)}\,dz = -\omega_2\int\limits_{\overrightarrow{AB}}\frac{f'(z)}{f(z)}\,dz = -\omega_2\cdot[\log f(z)]_A^B$$

  Here *log f* denotes a branch of the logarithm in a simply-connected neighbourhood of the line AB.

$$\int\limits_{\overrightarrow{AB}+\overrightarrow{CD}} z\cdot\frac{f'(z)}{f(z)}\,dz = \omega_2\cdot(\log f(A) - \log\ f(B)).$$

  Because

$$f(A) = f(B)$$

an integer $m_2 \in \mathbb{Z}$ exists with

$$\log f(A) - \log f(B) = 2\pi i \cdot m_2.$$

A similar argument for the lines $\overrightarrow{BC}$ and $\overrightarrow{DA}$ provides a second constant $m_1 \in \mathbb{Z}$, such that finally

$$\frac{1}{2\pi i} \cdot \int_{\partial P_a} z \cdot \frac{f'(z)}{f(z)}\, dz = m_1 \cdot \omega_1 + m_2 \cdot \omega_2 \in \Lambda,\ q.e.d.$$

Theorem 1.21 (Abel's theorem). *Consider $n \geq 2$ and two finite families of complex points*

$$A := (a_i)_{i=1,\ldots,n},\ B := (b_i)_{i=1,\ldots,n} \subset \mathbb{C}$$

with A and B pairwise disjoint mod Λ. Then are equivalent:

- *There exists an elliptic function $f \in \mathscr{M}(\Lambda)$ which has mod Λ the zero set A and the pole set B*
- *The points of A and B satisfy*

$$\sum_{i=1}^{n} a_i - \sum_{i=1}^{n} b_i \in \Lambda.$$

Proof. Proposition 1.20 proves that the zero set and the pole set of f satisfy the condition stated above. In order to prove the opposite direction of the theorem assume two sets A and B with the property stated above. Without restriction we may assume

$$\sum_{j=1}^{n} (a_j - b_j) = 0$$

as an equation, not just a congruence; otherwise replace a_1 by a suitable point which is congruent *mod* Λ. The proof for the existence of a suitable elliptic function f is by induction.

Start of induction $n = 2$: If

$$a_1 - b_1 = b_2 - a_2$$

then consider

$$z_0 := \frac{a_1 + a_2 + b_1 + b_2}{4}.$$

Geometrically the point z_0 is the center of the parallelogram with vertices the points a_1, a_2, b_1, b_2. We may assume $z_0 = 0$, otherwise we translate all coordinates by $-z_0$. As a consequence, the two conditions state

$$a_1 = -a_2 \text{ and } b_1 = -b_2.$$

Depending on the position relative Λ of a_1 and b_1 we now distinguish the following cases for the choice of f:

- $a_1,\ b_1 \notin \Lambda$: The even function

  $$g(z) := \wp(z) - \wp(a_1)$$

  has

  – a simple zero at a_1 and at a_2 if $a_1 \not\equiv a_2 \mod \Lambda$, and a zero of order $= 2$ at $a_1 \equiv a_2$ otherwise

  – and a pole of order $= 2$ at $z = 0$.

  An analogous result holds for the function

  $$h(z) := \wp(z) - \wp(b_1).$$

  Hence the quotient

  $$f := \frac{g}{h} = \frac{\wp - \wp(a_1)}{\wp - \wp(b_1)}$$

  has zeros exactly the zeros of g and poles exactly the zeros of h, while the poles of g and h at the origin cancel.

- $a_1 \in \Lambda$: Then $b_1 \notin \Lambda$. Set

  $$f := \frac{1}{\wp - \wp(b_1)}$$

- $b_1 \in \Lambda$: Then $a_1 \notin \Lambda$. Set

  $$f := \wp - \wp(a_1)$$

Hence f is elliptic with prescribed zeros and poles.

Induction step $n \geq 2,\ n \mapsto n+1$: If mod Λ

$$(a_1 - b_1) + \ldots + (a_n - b_n) + (a_{n+1} - b_{n+1}) \equiv 0$$

then choose $\tilde{a}_n \in \mathbb{C}$ with

$$\tilde{a}_n \equiv (a_1 - b_1) + \ldots + (a_{n-1} - b_{n-1}) + a_n.$$

Then mod Λ

$$(a_1 - b_1) + \ldots + (a_{n-1} - b_{n-1}) + (a_n - \tilde{a}_n) \equiv 0$$

and

$$(\tilde{a}_n + a_{n+1}) - (b_n + b_{n+1}) \equiv 0.$$

Depending on the position of $\tilde{a}_n$ relative Λ we distinguish the following cases:

- $\tilde{a}_n \not\equiv a_j$ *for all* $j = 1,...,n$: First we exclude the two exceptional cases $\tilde{a}_n \equiv b_n$ and $\tilde{a}_n \equiv b_{n+1}$: They lead to respectively

$$a_{n+1} \equiv b_{n+1} \text{ and } a_{n+1} \equiv b_n$$

which has been excluded by assumption.
For the remaining general cases, by induction assumption two elliptic functions exist

$$f_1 \in \mathscr{M}(\Lambda)$$

with zeros $(a_1,...,a_n)$ and poles $(b_1,...,b_{n-1},\tilde{a}_n)$ and

$$f_2 \in \mathscr{M}(\Lambda)$$

with zeros $(\tilde{a}_n, a_{n+1})$ and poles (b_n, b_{n+1}).

- $\tilde{a}_n \equiv a_n$: Then

$$(a_1 - b_1) + ... + (a_{n-1} - b_{n-1}) \equiv 0$$

By induction assumption two elliptic functions exist

$$f_1 \in \mathscr{M}(\Lambda)$$

with zeros $(a_1,...,a_{n-1})$ and poles $(b_1,...,b_{n-1})$ and

$$f_2 \in \mathscr{M}(\Lambda)$$

with zeros (a_n, a_{n+1}) and poles (b_n, b_{n+1}).

- $\tilde{a}_n \not\equiv a_n,\ \tilde{a}_n \equiv a_j$ *for at least one* $j = 1,...,n-1,$ *w.l.o.g.* $\tilde{a}_n \equiv a_1$: Then

$$(a_n - b_1)(a_2 - b_2) + ... + (a_{n-1} - b_{n-1}) \equiv 0$$

and

$$(a_1 + a_{n+1}) - (b_n + b_{n+1}) \equiv 0.$$

Similarly to the previous case by induction assumption two elliptic functions exist

$$f_1 \in \mathscr{M}(\Lambda)$$

with zero set $(a_2,...,a_n)$ and pole set $(b_1,...,b_{n-1})$ and

$$f_2 \in \mathscr{M}(\Lambda)$$

with zero (a_1, a_{n+1}) and poles (b_n, b_{n+1}).

In all cases the elliptic function

$$f := f_1 \cdot f_2 \in \mathscr{M}(\Lambda)$$

has the prescribed zeros $(a_1,...,a_{n+1})$ and poles $(b_1,...,b_{n+1})$, q.e.d.

Corollary 1.22 (Elliptic functions with pole of order $= 3$). *An elliptic function $f \in \mathscr{M}(\Lambda)$ with a pole mod Λ at $0 \in \Lambda$ of order $= 3$ and no other poles mod Λ, has exactly three zeros a_1, a_2, a_3 mod Λ. They satisfy*

$$a_1 + a_2 + a_3 = 0 \text{ mod } \Lambda.$$

Corollary 1.22 applies to $f = \wp'$, see Lemma 1.13.

The lenghty case-by-case analysis in the proof of Theorem 1.21 indicates: To define elliptic functions as functions in the complex plane with a certain priodicity is not the best context. Therefore we will consider in Section 2.1 elliptic functions simply as meromorphic functions on the torus. The torus is a compact Riemann surface. Abel's theorem generalizes to all compact Riemann surfaces. Phrasing and proving the theorem uses advanced results from the theory of Riemann surfaces, see [21, §20].

Chapter 2
The modular group Γ and its Hecke congruence subgroups $\Gamma_0(N)$

2.1 The moduli space of complex tori and group actions

An elliptic function f with lattice Λ, as studied in Chapter 1, has as natural domain of definition not the complex plane $\mathbb{C}$. Due to its periodicity the natural domain of definition for f is the quotient $\mathbb{C}/\Lambda$, a complex torus: Elliptic functions are meromorphic functions on the torus.

Therefore the present section investigates complex analysis on complex tori. We will prove that the equivalence classes of complex tori up to biholomorphic isomorphisms depend on one complex parameter. The parameter space can be choosen as quotient of the upper half-plane

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

with respect to the action of $SL(2,\mathbb{Z})$ as group of fractional-linear transformations.

The basis of a lattice

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

is not uniquely determined. Two positively oriented bases generate the same lattice if and only if they are equivalent modulo $SL(2,\mathbb{Z})$, i.e. iff they belong to the same orbit of the following $SL(2,\mathbb{Z})$-action:

Lemma 2.1 (Different bases of a given lattice). *Denote by*

$$M := \left\{ (\omega_1, \omega_2) \text{ basis of } \mathbb{R}^2 \text{ with } det \begin{pmatrix} \omega_1 & \omega_2 \\ | & | \end{pmatrix} > 0 \right\}$$

the set of positively oriented *bases of* $\mathbb{R}^2$. *The set* $\mathscr{R}$ *of all lattices* $\Lambda \subset \mathbb{C}$ *is the set of (left) equivalence classes of* M

$$SL(2,\mathbb{Z})\backslash M$$

with respect to the equivalence relation induced by the map

$$SL(2,\mathbb{Z}) \times M \to M, \left(\gamma, \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}\right) \mapsto \begin{pmatrix}\omega_1'\\ \omega_2'\end{pmatrix} := \gamma \cdot \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}.$$

Proof. The invertible matrices $\gamma \in M(2\times 2,\mathbb{Z})$ have determinant ± 1. Because both bases are positively oriented we have $det\ \gamma = 1$, q.e.d.

Two tori belonging to different lattices may be biholomorphically equivalent. The following Definition 2.2 introduces a name for the relation between lattices with isomorphic tori.

Definition 2.2 (Similar lattices). Two lattices $\Lambda,\ \Lambda' \subset \mathbb{C}$ are *similar* if a complex number $a \in \mathbb{C}^*$ exists with

$$\Lambda' = a \cdot \Lambda.$$

Proposition 2.3 (Holomorphic maps between tori). *Consider a holomorphic map*

$$F : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$$

between two tori with $F(0) = 0$. Then a uniquely determined number $a \in \mathbb{C}$ exists such that the following diagram commutes

$$\begin{array}{ccc} \mathbb{C} & \overset{\mu_a}{\dashrightarrow} & \mathbb{C} \\ {\scriptstyle p_1}\downarrow & & \downarrow{\scriptstyle p_2} \\ \mathbb{C}/\Lambda_1 & \xrightarrow{F} & \mathbb{C}/\Lambda_2 \end{array}$$

Here μ_a denotes the multiplication by a and $p_i,\ i = 1,2$, denote the canonical projections.

In particular, any holomorphic map between tori which fixes the neutral element is a group homomorphism.

Note: Due to the commutativity of the diagram in Proposition 2.3 the multiplier $a \in \mathbb{C}$ satisfies

$$a \cdot \Lambda_1 \subset \Lambda_2.$$

Proof. The composition

$$F \circ p_1 : \mathbb{C} \to \mathbb{C}/\Lambda_2$$

starts from the simply-connected domain $\mathbb{C}$. Therefore it lifts to the total space $\mathbb{C}$ of the covering projection p_2. It provides a holomorphic map

$$\tilde{F} : \mathbb{C} \to \mathbb{C},$$

uniquely determined by the condition $\tilde{F}(0) = 0$. Comutativity of the lifting diagram shows: For all $z \in \mathbb{C}, \omega \in \Lambda_1$,

$$\tilde{F}(z+\omega) - \tilde{F}(z) \in \Lambda_2.$$

The lattice Λ_2 is discrete and $\tilde{F}$ is continous. Therefore

$$\tilde{F}(z+\omega) - \tilde{F}(z)$$

does not depend on z. As a consequence for all $z \in \mathbb{C}$

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

Hence $\tilde{F}'$ is a holomorphic and elliptic. Therefore $\tilde{F}'$ is a constant $a \in \mathbb{C}$, and for all $z \in \mathbb{C}$

$$\tilde{F}(z) = a \cdot z$$

The uniqueness of a follows from the fact that μ_a induces the zero map F iff for all $z \in \mathbb{C}$ holds $a \cdot z \in \Lambda_2$. Because $\Lambda_2 \subset \mathbb{C}$ is discrete and $a \cdot 0 = 0$ we have $a \cdot z = 0$ for all $z \in \mathbb{C}$, which implies $a = 0$, q.e.d.

Corollary 2.4 (Lattices of biholomorphically equivalent tori). *Two tori*

$$T_1 = \mathbb{C}/\Lambda_1 \text{ and } T_2 = \mathbb{C}/\Lambda_2$$

are biholomorphically equivalent iff their lattices Λ_1 and Λ_2 are similar.

Proof. i) Assume the existence of a biholomorphic map

$$F : T_1 \to T_2$$

satisfying without restriction $F(0) = 0$. Proposition 2.3 provides a commutative diagram

$$\begin{array}{ccc} \mathbb{C} & \overset{\mu_a}{\dashrightarrow} & \mathbb{C} \\ {\scriptstyle p_1}\downarrow & & \downarrow{\scriptstyle p_2} \\ \mathbb{C}/\Lambda_1 & \xrightarrow{F} & \mathbb{C}/\Lambda_2 \end{array}$$

with μ_a the multiplication by a complex number $a \in \mathbb{C}$, satisfying

$$\mu_a \cdot \Lambda_1 \subset \Lambda_2.$$

Analogously, there exists a complex number $b \in \mathbb{C}$ with μ_b the unique lift of F^{-1} fixing the origin. Then the map

$$\mu_b \circ \mu_a = \mu_{b \cdot a}$$

is the unique lift of

$$id_{\mathbb{C}/\Lambda_1} = F^{-1} \circ F$$

fixing the origin. Hence

$$b \cdot a = 1.$$

In particular

$$a,\ b \in \mathbb{C}^*$$

and

$$a \cdot \Lambda_1 = \Lambda_2.$$

ii) Assume

$$\Lambda_2 = a \cdot \Lambda_1$$

with $a \in \mathbb{C}^*$. Then the multiplication

$$\mu_a : \mathbb{C} \to \mathbb{C},$$

induces a biholomorphic map $F : T_1 \to T_2$, q.e.d.

Theorem 2.5 (Biholomorphic equivalence classes of complex tori).

1. *Any complex torus is biholomorphic equivalent to a torus $T = \mathbb{C}/\Lambda$ with a* normalized *lattice*

$$\Lambda = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau \subset \mathbb{C}$$

with $\tau \in \mathbb{H}$ in the upper half-plane.

2. *The period τ of a normalized lattice is determined up to a fractional linear transformation with integer coefficients. Hence two tori*

$$\mathbb{C}/\Lambda_\tau \text{ and } \mathbb{C}/\Lambda_{\tau'}$$

with normalized lattices

$$\Lambda_\tau = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau \text{ and } \Lambda_{\tau'} = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau'$$

are biholomorphic equivalent iff

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

for a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}).$$

Proof. 1. Consider an arbitrary torus $T = \mathbb{C}/\Lambda$ with a lattice satisfying

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

and $det\ (\omega_1\ \ \omega_2) > 0$. Then

$$\tau := \frac{\omega_2}{\omega_1}$$

satisfies $Im\ \tau > 0$ and the lattice Λ is similar to the normalized lattice

$$\Lambda_\tau := \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau$$

due to

$$\frac{1}{\omega_1} \cdot \Lambda = \Lambda_\tau.$$

According to Corollary 2.4 the two tori T and $T' := \mathbb{C}/\Lambda_\tau$ are biholomorphic equivalent.

2. i) Assume

$$\tau' = \gamma \cdot \tau = \frac{a\ \tau + b}{c\ \tau + d}\ with\ \gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}).$$

Set

$$\begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix} := \gamma \cdot \begin{pmatrix} \tau \\ 1 \end{pmatrix},\ \text{i.e. } \omega_2 = a\tau + b,\ \omega_1 = c\tau + d.$$

The base change implies

$$\mathbb{Z} \cdot \omega_1 + \mathbb{Z} \cdot \omega_2 = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau = \Lambda_\tau.$$

As a consequence

$$\frac{1}{\omega_1} \cdot \Lambda_\tau = \Lambda_{\tau'}$$

because

$$\tau' = \frac{\omega_2}{\omega_1}.$$

The lattices Λ_τ and $\Lambda_{\tau'}$ are similar. Hence the tori $\mathbb{C}/\Lambda_\tau$ and $\mathbb{C}/\Lambda_{\tau'}$ are biholomorphic equivalent according to Corollary 2.4.

ii) For the opposite direction assume that two tori with normalized lattices

$$\mathbb{C}/\Lambda_\tau \text{ and } \mathbb{C}/\Lambda_{\tau'}, \tau, \tau' \in \mathbb{H},$$

are biholomorphic equivalent. According to Corollary 2.4 a number $\alpha \in \mathbb{C}^*$ exists with

$$\Lambda_{\tau'} = \alpha \cdot \Lambda_\tau.$$

As a consequence

$$\Lambda_{\tau'} = \mathbb{Z} \cdot \alpha + \mathbb{Z} \cdot \alpha \cdot \tau.$$

Therefore a matrix

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z})$$

exists with

$$\begin{pmatrix}\tau'\\1\end{pmatrix} = \gamma \cdot \begin{pmatrix}\alpha\tau\\\alpha\end{pmatrix},$$

i. e.

$$\tau' = \frac{a\cdot\alpha\tau + b\cdot\alpha}{c\cdot\alpha\tau + d\cdot\alpha} = \frac{a\cdot\tau+b}{c\cdot\tau+d},\ q.e.d.$$

Theorem 2.5 shows the consequences when two points of $\mathbb{H}$ are related by an element of the group $SL(2,\mathbb{Z})$. We formalize this relation by the concept of a group *acting* on a topological space.

Definition 2.6 (Group action).

1. Consider a topological group G with neutral element $e \in G$ and a topological space X. A *left action* of G on X is a continuous map

   $$\phi : G\times X \to X,\ (g,x) \mapsto gx,$$

   also written $g(x) := gx$, satisfying the following properties: For all $g_1, g_2 \in G$ and for all $x \in X$

   - $ex = x$
   - $g_1(g_2x) = (g_1g_2)x$

2. Consider a group action G on X.

   - The action is *faithful* if for all $g \in G,\ g \neq e$, exists $x \in X$ with $gx \neq x$, i.e. no group element different from e acts in a trivial way.
   - A *fixed point* of the group action is a point $x \in X$ with $gx = x$ for all $g \in G$. The action is *fixed-point-free* if it has no fixed points.
   - The *isotropy group* of a point $x \in X$ is the subgroup

     $$G_x := \{g \in G :\ gx = x\} \subset G.$$

   - The *orbit* of $x \in X$ is the subspace

     $$\{gx \in X :\ g \in G\} \subset X$$

     Two points of X are equivalent with respect to the group action if they belong to the same orbit. The set of equivalence classes is the *orbit space* $G\backslash X$, the set of orbits of the action. The canonical map to the orbit set is denoted

     $$\pi : X \to G\backslash X,\ x \mapsto [x].$$

- A *fundamental domain* $\mathscr{F}$ of the group action is a subset $\mathscr{F} \subset X$ such that the restriction
$$\pi|\mathscr{F} : \mathscr{F} \to G\backslash X$$
is bijective. Depending on eventual additional properties of the group action one looks for fundamental domains with specific additional properties.

- The action is *transitive* if the whole set X is a single orbit, i.e. if for any two points $x_1, x_2 \in X$ exists $g \in G$ with $x_2 = gx_1$.

Apparently all points of the same orbit have conjugated isotropy groups because
$$G_{gx} = g \cdot G_x \cdot g^{-1}.$$

Theorem 2.5 deals with the specific group action from Definition 2.7.

Definition 2.7 (Action of $SL(2,\mathbb{Z})$ on $\mathbb{H}$). The $SL(2,\mathbb{Z})$-*left action* on $\mathbb{H}$ is the map
$$\Phi : SL(2,\mathbb{Z}) \times \mathbb{H} \to \mathbb{H},\ (\gamma,\tau) \mapsto \gamma(\tau) := \frac{a\tau+b}{c\tau+d},\ \gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Remark 2.8 (Action of $SL(2,\mathbb{Z})$ and extensions).

1. *Imaginary part*: If $\tau \in \mathbb{H}$ and
$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{R})^+ := \{A \in GL(2,\mathbb{C}) :\ det\ A > 0\}$$
then
$$Im\ \gamma(\tau) = det(\gamma) \cdot \frac{Im\ \tau}{|c\tau+d|^2}$$
As a consequence
$$\tau \in \mathbb{H} \implies \gamma(\tau) \in \mathbb{H}.$$
Hence the map from Definition 2.7 extends to an action
$$GL(2,\mathbb{R})^+ \times \mathbb{H} \to \mathbb{H},\ \gamma(\tau) := \frac{a\tau+b}{c\tau+d}$$
which apparently restricts to an action of all subgroups of $GL(2,\mathbb{R})^+$, in particular to $\Gamma \subset GL(2,\mathbb{R})^+$.

Due to Theorem 2.5 the biholomorphic equivalence classes of complex tori correspond bijectively to the points of the orbit space $SL(2,\mathbb{Z})\backslash\mathbb{H}$. Hence the orbit space is named the *moduli space* of 1-dimensional complex tori.

Note: The orbit space is read "$\mathbb{H}$ modulo $SL(2,\mathbb{Z})$".

2. *Action of Γ on $\mathbb{H}^*$*: We have

$$z \in \mathbb{R} \implies \gamma(z) \in \mathbb{R} \cup \{\infty\} \text{ and } z \in \mathbb{Q} \implies \gamma(z) \in \mathbb{Q} \cup \{\infty\}$$

Moreover, due to

$$\frac{az+b}{cz+d} = \frac{a+(b/z)}{c+(d/z)}$$

we can extend γ to the argument ∞ by setting

$$\gamma(\infty) := \begin{cases} \infty & \text{if } d \neq 0 \text{ and } c = 0 \\ \\ \dfrac{a}{c} & \text{otherwise} \end{cases}$$

Set

$$\mathbb{H}^* := \mathbb{H} \dot\cup \mathbb{Q} \dot\cup \{\infty\}$$

Then the extension

$$\Phi : SL(2,\mathbb{Z}) \times \mathbb{H}^* \to \mathbb{H}^*, (\gamma, z) \mapsto \gamma(z),$$

is well-defined.

Note. The proof of Theorem 2.28 will provide $\mathbb{H}^*$ with a specific topology which induces on $\mathbb{Q} \subset \mathbb{H}$ a topology different from the subspace topology of $\mathbb{Q} \subset \mathbb{C}$ and also different neighbourhoods of $\infty \in \mathbb{H}^*$.

Definition 2.9 (Modular group, Hecke conguence subgroups and cusps).

1. The *modular group* is the group

$$\Gamma := SL(2,\mathbb{Z})$$

2. For a positive integer $N \in \mathbb{N}^*$ the *Hecke congruence subgroup of level N* is the subgroup

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : \ c \equiv 0 \mod N \right\} \subset \Gamma$$

The canonical left action of Γ from Remark 2.8 on $\mathbb{H}^*$ restricts to a left action

$$\Phi_N : \Gamma_0(N) \times \mathbb{H}^* \to \mathbb{H}^*.$$

3. Points $\tau \in \mathbb{H}$ with non-trivial isotropy group, i.e. $\Gamma_\tau \supsetneq \{\pm id\}$, are named *elliptic points* of $\Gamma_0(N)$. Half the order of the isotropy group

$$h_\tau := \frac{ord\ \Gamma_0(N)_\tau}{2}$$

is named the *period* of τ. An orbit is named an *elliptic orbit* if at least one point of the orbit - and hence all points - are elliptic.

4. The orbits of the points $\tau \in \mathbb{Q} \cup \{\infty\}$ are named the *cusps* of $\Gamma_0(N)$. The set of cusps is denote by $cusp(\Gamma_0(N))$. The *width* (Deutsch: "Breite") of the cusp passing through

$$\tau \in \mathbb{Q} \cup \{\infty\}$$

is the index of the isotropy groups

$$h_\tau := [\Gamma_\tau : \Gamma_0(N)_\tau]$$

Remark 2.10 (Modular group and congruence subgroups).

1. Apparently,

$$\Gamma = \Gamma_0(1)$$

2. For all $N \geq 1$ the element

$$-id \in \Gamma_0(N)$$

acts trivially on $\mathbb{H}$, i.e. for all $\tau \in \mathbb{H}$

$$-id \in \Gamma_0(N)_\tau$$

The elements

$$\pm id \in \Gamma_0(N)$$

are the only elements which act trivially on $\mathbb{H}$. Therefore some authors apply the name modular group to the quotient

$$PSL(2,\mathbb{Z}) := SL(2,\mathbb{Z})/\{\pm id\}.$$

We will not follow this convention. Because one can study also the action of certain subgroups of $SL(2,\mathbb{Z})$ which do not contain the element $-id$.

3. Corollary 2.18 will show that the isotropy groups of all elliptic points from Definition 2.9 are finite groups. But the isotropy group $\Gamma_\infty \subset \Gamma$ is an infinite group, more specific

$$\Gamma_\infty = <\pm T> \text{ with translation } T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$$

4. Theorem 2.28 will show the importance to consider the group action not only on the open upper half-plane $\mathbb{H}$ but also on its "closure" $\mathbb{H}^*$.

Example 2.11 (Cusps of Γ, $\Gamma_0(2)$, $\Gamma_0(4)$ and $\Gamma_0(11)$). See [17, Sect. 3.8], and the PARI commands *mfcusps*, *mfnumcusps*, *mfcuspwidth*.

1. For $N \in \mathbb{N}$ the number $\varepsilon_\infty(\Gamma_0(N))$ of cusps is

$$\sum_{d|N} \phi(gcd(d, N/d))$$

with the sum extending over all positive divisors d of N, and ϕ denoting the Euler function defined as

$$\Phi(n) := card\ (\mathbb{Z}/n\mathbb{Z})^*$$

2. The group Γ has a single cusp

- *Orbit of the point* 0:

$$\mathbb{Q} \cup \{\infty\}$$

with $width = 1$. All rationals $p/q \in \mathbb{Q}$ belong to the Γ-orbit of ∞, see Remark 2.8.

3. The group $\Gamma_0(2)$ has two cusps

- *Orbit of the point* 0:

$$\left\{ \frac{p}{q} \in \mathbb{Q} :\ (p,q) = 1,\ q \text{ odd} \right\}$$

with $width = 2$.

- *Orbit of the point* $1/2$:

$$\left\{ \frac{p}{q} \in \mathbb{Q} :\ (p,q) = 1,\ p \neq 0,\ q \text{ even} \right\} \cup \{\infty\}$$

with $width = 1$.

4. The group $\Gamma_0(4)$ has three cusps

- *Orbit of the point* 0:

$$\left\{ \frac{p}{q} \in \mathbb{Q} :\ (p,q) = 1,\ q \text{ odd} \right\}$$

with $width = 4$.

- *Orbit of the point* $1/2$:

$$\left\{ \frac{p}{q} \in \mathbb{Q} : \ (p,q) = 1, \ p \neq 0, \ q \text{ even, not divisible by } 4 \right\}$$

with $width = 1$.

- *Orbit of the point* $1/4$:

$$\left\{ \frac{p}{q} \in \mathbb{Q} : \ (p,q) = 1, \ p \neq 0, \ q \text{ divisible by } 4 \right\} \cup \{\infty\}$$

with $width = 1$.

5. The group $\Gamma_0(11)$ has two cusps

- *Orbit of the point* 0:

$$\left\{ \frac{p}{q} \in \mathbb{Q} : \ (p,q) = 1, \ q \text{ not divisible by } 11 \right\}$$

with $width = 11$.

- *Orbit of the point* $1/11$:

$$\left\{ \frac{p}{q} \in \mathbb{Q} : \ (p,q) = 1, \ p \neq 0, \ q \text{ divisible by } 11 \right\} \cup \{\infty\}$$

with with $width = 1$.

Lemma 2.12 (Divisor lemma). *Consider three integers $a, b, c \in \mathbb{Z}$ with*

$$gcd(a,b,c) = 1.$$

Then exists an integer $r \in \mathbb{Z}$ such that

$$gcd(a + r \cdot b, c) = 1.$$

Proof. E.g. [36, Kap. II, §3 Lemma]: We claim that

$$r := \prod_{p|c, p\nmid a} p$$

satisfies the claim. Otherwise assume the existence of a prime q satisfying

$$q \mid gcd(a+r\cdot b, c).$$

- *Case* $q \mid a$: Then $q \mid rb$. Because $q \nmid r$ then $q \mid b$. Therefore

$$gcd(a,b,c,) \neq 1,$$

  a contradiction.

- *Case* $q \nmid a$: Then $q \mid r$ by definition of r. Because $q \mid a+rb$ also $q \mid a$, a contradiction, q.e.d.

Lemma 2.13 (Exact sequence of congruence subgroups). *Consider* $N \in \mathbb{N}^*$. *There exists a canonical exact sequence of Abelian groups*

$$1 \to \Gamma(N) \to \Gamma \xrightarrow{\pi} SL(2,\mathbb{Z}/N\mathbb{Z}) \to 1$$

with the principal congruence subroup of level N

$$\Gamma(N) := \left\{ A \in \Gamma : \ A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}$$

and

$$SL(2,\mathbb{Z}/N\mathbb{Z}) := \{B \in M(2\times 2, \mathbb{Z}/N\mathbb{Z}) : \ det\ B = 1 \in (\mathbb{Z}/N\mathbb{Z})^*\}$$

and the residue morphism

$$\pi : \Gamma \to SL(2,\mathbb{Z}/N\mathbb{Z}),\ A \mapsto \overline{A}.$$

Proof. i) *kernel*: Apparently $ker\ \pi = \Gamma(N)$.

ii) *Surjectivity*: E.g.see [36, Kap. II, §3 Satz]. Assume a given

$$\overline{A} = \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ \\ \overline{\gamma} & \overline{\delta} \end{pmatrix} \in SL(2,\mathbb{Z}/N\mathbb{Z})$$

We may assume

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M(2\times 2, \mathbb{Z}),$$

and w.l.o.g $\gamma \neq 0$, otherwise set $\gamma = N$. The condition about the determinant

$$det\ \overline{A} = 1 \in \mathbb{Z}/N\mathbb{Z}$$

implies

$$\alpha\delta - \beta\gamma \equiv 1 \mod N,$$

and therefore

$$gcd(\gamma, \delta, N) = 1.$$

Lemma 2.12 provides an integer $r \in \mathbb{Z}$ satisfying

$$gcd(\gamma, d) = 1$$

for

$$d := \delta + rN.$$

On one hand, from the determinant

$$\alpha d - \beta\gamma = \alpha\delta - \beta\gamma + \alpha rN = 1 + sN$$

with a suitable integer $s \in \mathbb{Z}$. On the other hand

$$gcd(\gamma, d) = 1$$

provides an equation

$$\gamma y - dx = s$$

with suitable integers $x,\ y \in \mathbb{Z}$.

Consider the matrix

$$\tilde{A} := \begin{pmatrix} \alpha + xN & \beta + yN \\ \gamma & d \end{pmatrix} \in M(2 \times 2, \mathbb{Z})$$

Then

$$\pi(\tilde{A}) = \pi(A) = \overline{A}$$

and

$$det\ \tilde{A} = (\alpha + xN) \cdot d - (\beta + yN) \cdot \gamma = 1 + sN + N(xd - y\gamma) = 1,$$

which implies $\tilde{A} \in \Gamma$ and finishes the proof of the Lemma, q.e.d.

Proposition 2.14 (Index of Hecke congruence subgroups). *For any integer $N \geq 1$ holds the index formula*

$$[\Gamma : \Gamma_0(N)] = N \cdot \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

Here the product ranges over all prime factors p of N.

In particular, all Hecke congruence subgroups have finite index in the modular group.

Proof. See also [53, Chap. 1.6].

i) *Transitivity of the index formula*: We extend the exact sequence from Lemma 2.13 to the commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Gamma(N) & \longrightarrow & \Gamma & \xrightarrow{\pi} & SL(2,\mathbb{Z}/N\mathbb{Z}) & \longrightarrow & 1 \\ & & \uparrow{\scriptstyle id} & & \uparrow & & \uparrow{\scriptstyle \psi} & & \\ 1 & \longrightarrow & \Gamma(N) & \longrightarrow & \Gamma_0(N) & \longrightarrow & \Gamma_0(N)/\Gamma(N) & \longrightarrow & 1 \end{array}$$

The induced map

$$\psi : \Gamma_0(N)/\Gamma(N) \to SL(2,\mathbb{Z}/N\mathbb{Z})$$

is injective with image

$$im\ \psi = \left\{ \begin{pmatrix} \overline{\alpha} & \overline{\beta} \\ 0 & \overline{\alpha}^{-1} \end{pmatrix} \right\} \subset SL(2,\mathbb{Z}/N\mathbb{Z})$$

Apparently

$$[\Gamma_0(N) : \Gamma(N)] = card(im\ \psi) = \phi(N) \cdot N$$

with the Euler function ϕ. The exact sequence of the first line of the diagram implies

$$[\Gamma : \Gamma(N)] = card\ SL(2,\mathbb{Z}/N\mathbb{Z}).$$

The transititvity of the index function implies

$$[\Gamma : \Gamma_0(N)] \cdot [\Gamma_0(N) : \Gamma(N)] = [\Gamma : \Gamma(N)]$$

ii) *Factorisation*: The prime factorisation of integers

$$N = \prod_{j=1}^{k} p_j^{e_j}$$

implies the factorisation of the Euler function

$$\phi(N) = \prod_{j=1}^{k} p^{e_j} \cdot \left(1 - \frac{1}{p_j}\right)$$

with the Euler factors

$$\phi(p^e) = p^e \cdot \left(1 - \frac{1}{p}\right),$$

and the factorisation of the $SL(2,-)$-groups due to the Chinese remainder theorem

$$SL(2,\mathbb{Z}/N\mathbb{Z}) \simeq \prod_{j=1}^{k} SL\left(2,\mathbb{Z}/p_j^{e_j}\mathbb{Z}\right).$$

One has

$$card\ SL\left(2,\mathbb{Z}/p_j^{e_j}\mathbb{Z}\right) = p_j^{3e_j}\left(1-\frac{1}{p_j^2}\right),$$

see [53, Chap. 1.6] and [17, Exerc. 1.2.3]. For a proof see also [28, Cor. 2.8] and use for the reduction from GL to SL the exact sequence of the determinant

$$1 \to SL(2,\mathbb{Z}/p^e\mathbb{Z}) \to GL(2,\mathbb{Z}/p^e\mathbb{Z}) \xrightarrow{det} (\mathbb{Z}/p^e\mathbb{Z})^* \to 1.$$

And also

$$[\Gamma : \Gamma(N)] = card\ SL(2,\mathbb{Z}/N\mathbb{Z}),$$

see part i). It follows

$$[\Gamma : \Gamma(N)] = \prod_{j=1}^{k} card\ SL\left(2,\mathbb{Z}/p_j^{e_j}\mathbb{Z}\right) =$$

$$= \prod_{j=1}^{k} p_j^{3e_j}\left(1-\frac{1}{p_j^2}\right) = N^2 \cdot \prod_{j=1}^{k} p_j^{e_j} \cdot \left(1-\frac{1}{p_j^2}\right) =$$

$$= N^2 \cdot \prod_{j=1}^{k} p_j^{e_j} \cdot \left(1-\frac{1}{p_j}\right)\left(1+\frac{1}{p_j}\right) = N^2 \cdot \phi(N) \cdot \prod_{j=1}^{k}\left(1+\frac{1}{p_j}\right)$$

Hence

$$[\Gamma : \Gamma_0(N)] = \frac{[\Gamma : \Gamma(N)]}{[\Gamma_0(N) : \Gamma(N)]} =$$

$$= \frac{N^2 \cdot \phi(N) \cdot \prod_{j=1}^{k}\left(1+\frac{1}{p_j}\right)}{N \cdot \phi(N)} = N \cdot \prod_{p|N}\left(1+\frac{1}{p}\right),\ q.e.d.$$

Example 2.15 (Right cosets of congruence subgroups). See the PARI-command *mfcosets*.

1. The subgroup $\Gamma_0(2)$ has index

$$[\Gamma : \Gamma_0(2)] = 3$$

with the set of right coset representatives

$$\left\{id,\ J := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ U^2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}\right\}$$

for

$$U := \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$$

2. The subgroup $\Gamma_0(4)$ has index

$$[\Gamma : \Gamma_0(4)] = 6$$

with the set of right coset representatives

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\}.$$

2.2 Topology of the orbit space of the Γ-action

The section continues the study of the moduli space of complex tori. We denote by

$$\Phi : \Gamma \times \mathbb{H} \to \mathbb{H}, (\gamma, \tau) \mapsto \gamma(\tau) := \frac{a\tau + b}{c\tau + d}, \ \gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

the continuous Γ-left action introduced in Remark 2.8. Our final aim is to provide the orbit space

$$Y := \Gamma \backslash \mathbb{H}$$

with an analytic structure and to compactify the resulting Riemann surface to obtain a compact Riemann surface X. The latter will be named the *modular curve* of the action Φ. We proceed along the following steps:

- Constructing a Hausdorf topology on Y, see Theorem 2.21.
- Constructing an analytic structure on Y, see Section 2.3 Proposition 2.27.
- Compactifying Y to a compact Riemann surface X, see Section 2.3 Theorem 2.28.

To provide the orbit space of a group action with a suitable topological or differentiable structure is always a subtle task. In the present context the problem is intensified by the fact that the modular group does not operate freely, see Theorem 2.16: There are elliptic points. The difficulty consist in dealing with the elliptic points with respect to the Hausdorff property and with respect to complex charts on the quotient.

The modular group Γ contains the two distinguished elements

- *Reflection at the y-axis and dividing by squared absolute value*:

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \Gamma, \ S(\tau) = -1/\tau = \frac{-\overline{\tau}}{|\tau|^2}.$$

- *Translation by one*:

$$T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma,\ T(\tau) = \tau + 1.$$

Theorem 2.16 (Fundamental domain and elliptic points of the Γ-action).

1. *The modular group Γ is generated by the two elements $S,\ T \in \Gamma$ which satisfy*

$$S^4 = id,\ (ST)^6 = id.$$

2. *The orbit space $Y = \Gamma\backslash\mathbb{H}$ of the action*

$$\Phi : \Gamma \times \mathbb{H} \to \mathbb{H},\ (\gamma, \tau) \mapsto \gamma(\tau),$$

maps bijectively to the set

$$\mathscr{D} := \{\tau \in \mathbb{H} : |\tau| > 1 \text{ and } -1/2 \leq Re\ \tau < 1/2\} \cup \{\tau \in \mathbb{H} : |\tau| = 1 \text{ and } -1/2 \leq Re\ \tau \leq 0\},$$

the standard fundamental domain *of Φ.*

3. *The action Φ has exactly two elliptic points $\tau_0 \in \mathscr{D}$. Their isotropy groups are cyclic:*

- $\tau_0 = i$ *with*

$$\Gamma_i =< S >\subset \Gamma,\ ord\ \Gamma_i = 4,$$

- $\tau_0 = \rho := e^{2\pi i/3}$ *with*

$$\Gamma_\rho =< ST >\subset \Gamma,\ ord\ \Gamma_\rho = 6.$$

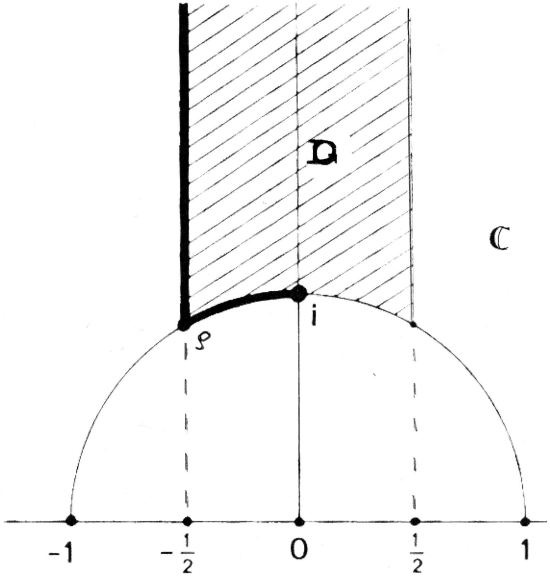


Fig. 2.1 Fundamental domain $\mathscr{D}$ of the modular group Γ shaded, from [29]

Figure 2.1 shows the fundamental domain $\mathscr{D}$ of the modular group. In order to exclude pairs of congruent points within $\mathscr{D}$ one has to exclude part of the boundary of $\mathscr{D}$. This convention is followed by [29] but not by all references. Most references name *fundamental domain* the closure $\overline{\mathscr{D}}$.

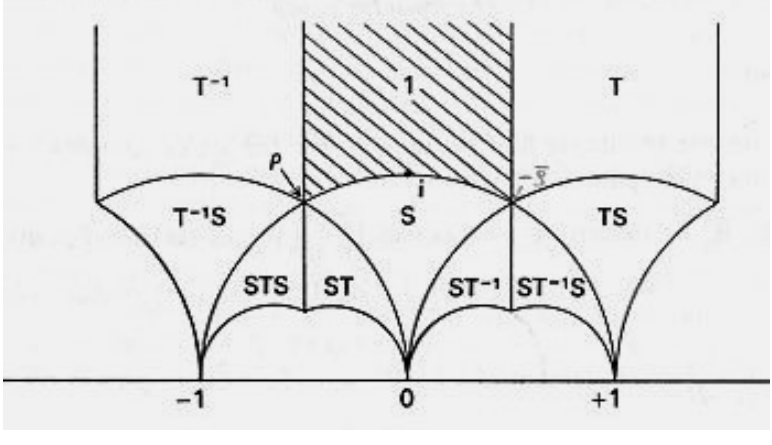


Fig. 2.2 Some translates of the fundamental domain of Γ, from [52, Chap. VII, Fig. 1]

Figure 2.2 shows some translates of the fundamental domain of Γ under the elements $T, S \in \Gamma$ and their products.

Proof. The three parts of the subsequent proof do not correspond one to one to the three parts of the theorem. Note that the subgroup

$$\{\pm id\} \subset \Gamma$$

operates on $\mathbb{H}$ in a trivial way and that $S^2 = -id$.

i) *The domain $\mathscr{D}$*: Denote by

$$G := < S, T > \subset \Gamma$$

the subgroup generated by the two distinguished elements. We show: Any given point $\tau \in \mathbb{H}$ is equivalent to a point $\tau' \in \mathscr{D} \mod G$.

We choose an element $\gamma_0 \in G$ with $Im\ \gamma_0(\tau)$ maximal. Such choice is possible because

$$Im\ \gamma(\tau) = \frac{Im\ \tau}{|c \cdot \tau + d|^2} \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G.$$

The translation $T \in \Gamma$ does not change the imaginary part of its argument. Therefore we may assume

$$-1/2 \leq Re\ \gamma_0(\tau) < 1/2.$$

In addition, $|\gamma_0(\tau)| \geq 1$ because otherwise

$$Im\ (S \circ \gamma_0)(\tau) = Im \left(\frac{-\overline{\gamma_0(\tau)}}{|\gamma_0(\tau)|^2} \right) > Im\ \gamma_0(\tau).$$

- If $|\gamma_0(\tau)| > 1$ then $\tau' := \gamma_0(\tau)$.
- If $|\gamma_0(\tau)| = 1$ but $0 < Re\ \gamma_0(\tau) \leq 1/2$ then

$$\tau' := (S \circ \gamma_0)(\tau).$$

In both cases $\tau' \in \mathscr{D}$.

ii) *Isotropy groups and fundamental domain*: Consider two points $\tau, \tau' \in \mathscr{D}$ with

$$\tau' = \gamma(\tau), \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

We show $\tau = \tau'$, and the latter equation implies $\gamma \in \Gamma_\tau$.

We may assume without restriction $Im\ \tau' \geq Im\ \tau$. Then

$$Im\ \tau' = \frac{Im\ \tau}{|c\cdot\tau+d|^2}.$$

implies

$$|c\cdot\tau+d| \le 1.$$

Because $Im\ \tau \ge \sqrt{3}/2$ only the cases $c = 0,\ \pm 1$ are possible:

- *Case 1,* $c = 0$: Then $d = \pm 1$ and $a = d$. Without restriction $a = d = 1$, hence

  $$\tau' = \tau + b,\ b \in \mathbb{Z}.$$

  Because $Re\ \tau' = (Re\ \tau) + b$ we obtain $b = 0$; i.e. $\tau = \tau'$ and

  $$\gamma = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \pm\, id \in \Gamma_\tau.$$

- *Case 2,* $c = 1$: Then $|\tau + d| \le 1$, which implies $d \in \{0, \pm 1\}$.

  Case 2a, $d = 0$: If $d = 0$ then $b = -1$ and

  $$\tau' = \frac{a\cdot\tau - 1}{\tau} = a - (1/\tau),\ a \in \mathbb{Z}.$$

  Due to $\tau \in \mathscr{D}$ the equation

  $$|c\cdot\tau+d| = |\tau| \le 1$$

  implies $|\tau| = 1$. Hence

  $$1/\tau = \overline{\tau} \text{ and } \tau' + \overline{\tau} = a \in \mathbb{Z}$$

  which implies

  $$Re\ \tau' + Re\ \tau = a \in \mathbb{Z} \text{ and } Im\ \tau' = Im\ \tau.$$

  Therefore: Either $a = 0$ and $\tau = i$ which implies

  $$\tau' = -(1/\tau) = i = \tau$$

  and

  $$\gamma = \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \pm S \in \Gamma_i.$$

  Or $a = -1$ and $\tau = \rho$ which implies

  $$\tau' = -1 - (1/\tau) = \rho = \tau$$

  and

  $$\gamma = \pm \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} = \pm (ST)^2 \in \Gamma_\rho.$$

  Case 2b, $d = \pm 1$: If $d = \pm 1$ then

$$|c\cdot\tau+d| = |\tau\pm 1| \leq 1.$$

Because of $\tau, \tau' \in \mathscr{D}$ the case $d=-1$ with $|\tau-1|\leq 1$ is excluded. Therefore $d=1$ leaving

$$|\tau+1| = |\tau-(-1)| \leq 1.$$

As a consequence, $\tau=\rho$ and

$$ad-bc = a-b = 1 \text{ and } \tau' = \frac{a\cdot\rho+b}{\rho+1} = a+\rho,$$

hence $a=0$, $\tau'=\rho=\tau$ and

$$\gamma = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = ST \in \Gamma_\rho.$$

- *Case 3,* $c=-1$: This case reduces to case 2, $c=1$, by considering $-\gamma_0$.

iii) $G=\Gamma$: Consider an arbitrary element $\gamma\in\Gamma$ and the point

$$\tau_0 := 2\cdot i \in \mathscr{D}.$$

Due to part i) an element $\gamma_0 \in G$ exists with

$$(\gamma_0\circ\gamma)(\tau_0) \in \mathscr{D}.$$

Due to part ii) the two points of $\mathscr{D}$ coincide

$$\tau_0 = (\gamma_0\circ\gamma)(\tau_0) \in \mathscr{D},$$

i.e.

$$\gamma_0\circ\gamma \in \Gamma_{\tau_0} = \{\pm id\}$$

which implies $\gamma\in G$, q.e.d.

Remark 2.17 (Presentation of the modular group and fundamental domain of its subgroups).

1. Consider the element

$$U := -TS = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \in SL(2,\mathbb{Z})$$

which satisfies $U^3 = id$. Apparently also

$$G = < S,\, U > .$$

Therefore Theorem 2.16 implies that the two elements S and U generate the group $SL(2,\mathbb{Z})$. One can show that all relations of the generators are generated by

$$S^4 = U^3 = S^2U \cdot (US^2)^{-1} = id,$$

i.e. that

$$SL(2,\mathbb{Z}) =< S,\ U;\ S^4, U^3, S^2U \cdot (US^2)^{-1} >$$

is a presentation of $SL(2,\mathbb{Z})$, see [36, Kap. II, §2 Bemerk.].

2. Denote by

$$PSL(2,\mathbb{Z}) := SL(2,\mathbb{Z})/\{\pm id\}$$

the corresponding *projective-linear group*, which acts faithful on $\mathbb{H}$, and by

$$\pi : SL(2,\mathbb{Z}) \to PSL(2,\mathbb{Z}),\ A \mapsto \overline{A},$$

the canonical quotient map. The projective-linear group has the two cyclic subgroups

$$H_1 :=< \overline{S} >\simeq \mathbb{Z}/2\mathbb{Z} \text{ and } H_2 :=< \overline{U} >\simeq \mathbb{Z}/3\mathbb{Z}.$$

One can show

$$PSL(2,\mathbb{Z}) = H_1 * H_2 =< \overline{S}, \overline{U}; \overline{S}^2, \overline{U}^3 >$$

as the *free product*, see the short argument from [3] and also [52, Chap. VII, § 1, Rem.].

3. For a subgroup $K \subset \Gamma$ with finite index $J := [G : K] < \infty$ each decomposition

$$\Gamma = \dot{\bigcup}_{j\in J} \gamma_j \cdot K,\ \gamma_j \in \Gamma,$$

into left cosets provides a fundamental domain

$$\mathscr{D}(K) := \dot{\bigcup}_{j\in J} \gamma_i^{-1}(\mathscr{D})$$

of the induced K-action, which derives from the standard fundamental domain $\mathscr{D}$ of Γ. In the following we will always choose fundamental domains $\mathscr{D}(K) \subset \mathbb{H}$ which originate as translates of $\mathscr{D}$. These fundamental domains are measurable subsets of $\mathbb{H}$.

Corollary 2.18 (Elliptic points). *For $N \geq 1$ the action*

$$\Phi : \Gamma_0(N) \times \mathbb{H} \to \mathbb{H}$$

has finitely many elliptic orbits. Each elliptic point $\tau \in \mathbb{H}$ has the finite isotropy group

$$\Gamma_0(N)_\tau = \Gamma_\tau \cap \Gamma_0(N).$$

Proof. Theorem 2.16 shows: The action of Γ has exactly two elliptic points $i,\ \rho \in \mathscr{D}$, and both have finite isotropy groups. The index formula from Proposition 2.14 implies the finiteness of

$$[\Gamma : \Gamma_0(N)] =: k.$$

According to Remark 2.17 each finite coset decomposition

$$\Gamma = \bigcup_{j=1}^{k} \gamma_j \cdot \Gamma_0(N),\ \gamma_j \in \Gamma,$$

provides the fundamental domain of the $\Gamma_0(N)$-action

$$\mathscr{D}(\Gamma_0(N)) := \bigcup_{j=1}^{k} \gamma_j^{-1}(\mathscr{D})$$

e.g. see Figure 2.3. For each $j = 1,...,k$ and each point $\tau \in \gamma_j^{-1}(\mathscr{D})$ the group morphism

$$\Gamma_0(N)_\tau \to \Gamma_{\gamma_j(\tau)},\ \gamma \mapsto \gamma_j \cdot \gamma \cdot \gamma_j^{-1},$$

injects $\Gamma_0(N)_\tau$ into $\Gamma_{\gamma_j(\tau)}$. Hence the elliptic points of $\Gamma_0(N)$ contained in $\mathscr{D}(\Gamma_0(N))$ are contained in the finite set

$$\bigcup_{j=1}^{k} \gamma_j^{-1}(i) \cup \bigcup_{j=1}^{k} \gamma_j^{-1}(\rho),\ q.e.d.$$

Figure 2.3 shows the fundamental domain of $\Gamma_0(13)$. The fundamental domain $\mathscr{D}(\Gamma_0(13))$ splits into 14 disjoint translates of $\mathscr{D}$ according to the index formula from Proposition 2.14

$$[\Gamma : \Gamma_0(13)] = 14$$

For further explanations of Figure 2.3 see [17, Fig. 3.1 and Exerc. 3.1.4].

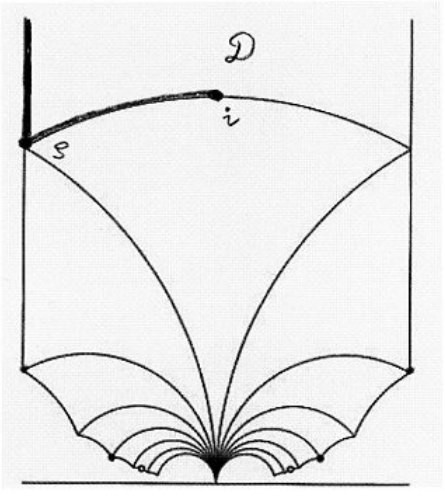


Fig. 2.3 Fundamental domain of $\Gamma_0(13)$, adapted from [17, Fig. 3.1]

The following Lemma 2.19 about the local behaviour of the action Φ covers the main step for proving the Hausdorff property of the quotient topoplogy with respect to the quotient map

$$\mathbb{H} \to \Gamma \backslash \mathbb{H}.$$

Lemma 2.19 (Properly discontinuous group action). *Any two points $\tau_1, \tau_2 \in \mathbb{H}$ have neighbourhoods*

$$U_i \subset \mathbb{H},\ i = 1,2,$$

such that for all $\gamma \in \Gamma$:

$$\gamma(U_1) \cap U_2 \neq \emptyset \implies \gamma(\tau_1) = \tau_2.$$

In particular: Any point $\tau \in \mathbb{H}$ has a neighbourhood $U \subset \mathbb{H}$ such that for all $\gamma \in \Gamma$:

$$\gamma(U) \cap U \neq \emptyset \implies \gamma \in \Gamma_\tau.$$

The set U has no elliptic points except possibly τ.

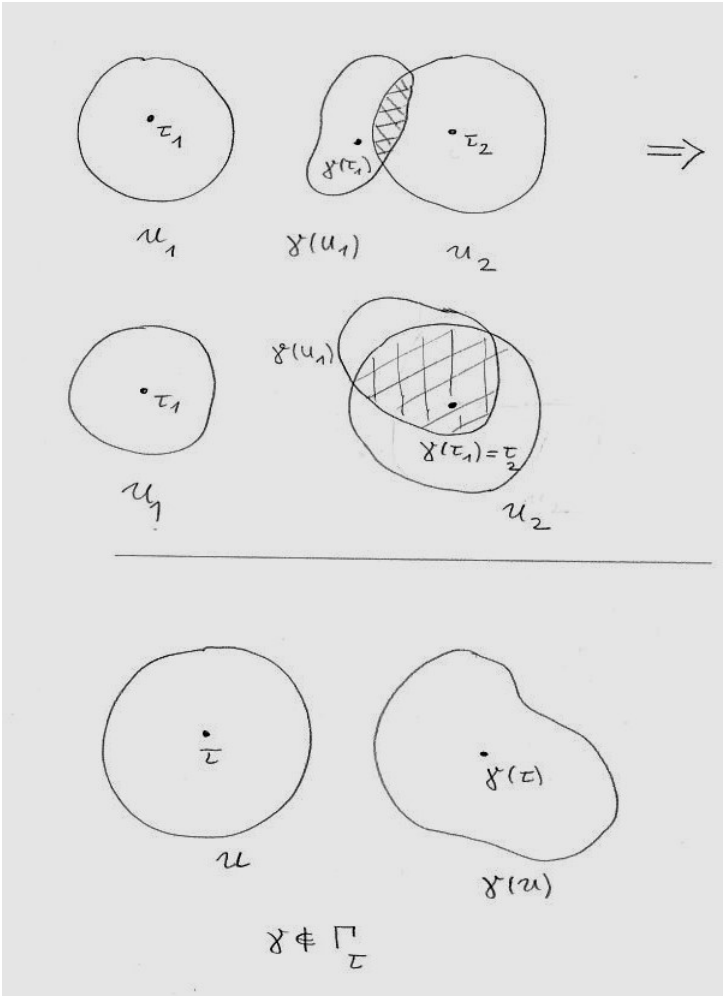


Fig. 2.4 Local behaviour of the action of the modular group, see Lemma 2.19

Figure 2.4 visualizes Lemma 2.19: If an element $\gamma \in \Gamma$ maps a point of the distinguished neighbourhood U_1 of τ_1 to the distinguished neighbourhhood U_2 of τ_2, then γ maps τ_1 to τ_2. The add-on states: If $\gamma \in \Gamma$ does not fix τ, then γ moves all points from U to the complement of U.

Proof. 1. *Introducing a finiteness condition*: We choose two relatively compact neighbourhoods

$$V_i \subset\subset \mathbb{H} \text{ of } \tau_i,\ i = 1,2,$$

and show: Only finitely many matrices $\gamma \in \Gamma$ exists with

$$\gamma(V_1) \cap V_2 \neq \emptyset.$$

The idea is to consider the extension of the group action of Γ to $SL(2,\mathbb{R})$, see Remark 2.8,

$$\Phi : SL(2,\mathbb{R}) \times \mathbb{H} \to \mathbb{H}, (\gamma, \tau) \mapsto \gamma(\tau) := \frac{a\tau + b}{c\tau + d}, \ \gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

which provides a compact isotropy group of the point i

$$SL(2,\mathbb{R})_i = SO(2,\mathbb{R}) :$$

One checks

$$\gamma(i) = i \iff a = d \text{ and } b = -c,$$

hence

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SO(2,\mathbb{R}).$$

The action Φ of $SL(2,\mathbb{R})$ is transitive because any point $\tau \in \mathbb{H}$ belongs to the orbit of i: If

$$\tau = x + iy$$

then $\gamma_\tau(i) = \tau$ for the matrix

$$\gamma_\tau := \begin{pmatrix} \sqrt{y} & \frac{x}{\sqrt{y}} \\ 0 & \frac{1}{\sqrt{y}} \end{pmatrix} = \frac{1}{\sqrt{y}} \cdot \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \in SL(2,\mathbb{R}).$$

As a consequence for any two points $e_1, e_2 \in \mathbb{H}$ and any $\gamma \in SL(2,\mathbb{R})$:

$$\gamma(e_1) = e_2 \iff \gamma \in \gamma_{e_2} \cdot SO(2,\mathbb{R}) \cdot \gamma_{e_1}^{-1}$$

according to the following commutatice diagram

$$\begin{array}{ccc} e_1 & \xrightarrow{\ \gamma\ } & e_2 \\ {\scriptstyle \gamma_{e_1}^{-1}}\downarrow & & \uparrow{\scriptstyle \gamma_{e_2}} \\ i & \dashrightarrow & i \end{array}$$

If a matrix $\gamma \in \Gamma$ satisfies $\gamma(V_1) \cap V_2 \neq \emptyset$ then also for the closure

$$\gamma(\overline{V}_1) \cap \overline{V}_2 \neq \emptyset$$

and

$$G := \{\gamma \in SL(2,\mathbb{R}) : \gamma(\overline{V}_1) \cap \overline{V}_2 \neq \emptyset\} = \bigcup_{e_1 \in \overline{V}_1, e_2 \in \overline{V}_2} \gamma_{e_2} \cdot SO(2,\mathbb{R}) \cdot \gamma_{e_1}^{-1}.$$

Because γ_e and its inverse γ_e^{-1} depend continuously on $e \in \mathbb{H}$, the latter set on the right-hand side is the continuous image of the compact set

$$\overline{V}_2 \times SO(2,\mathbb{R}) \times \overline{V}_1$$

under the continuous map

$$\overline{V}_2 \times SO(2,\mathbb{R}) \times \overline{V}_1 \to SL(2,\mathbb{R}),\ (e_2,\gamma,e_1) \mapsto \gamma_{e_2} \cdot \gamma \cdot \gamma_{e_1}^{-1},$$

and therefore compact itself. Its intersection

$$G \cap \Gamma$$

with the discrete group Γ is finite.

2. *Shrinking V_1 and V_2*: According to the first part only finitely many $\gamma \in \Gamma$ exist with

$$\gamma(V_1) \cap V_2 \neq \emptyset.$$

In particular, the set

$$G_\Gamma := \{\gamma \in \Gamma :\ \gamma(V_1) \cap V_2 \neq \emptyset \text{ and } \gamma(\tau_1) \neq \tau_2\}$$

is finite. Therefore, after finitely many steps we can shrink the neighbourhoods V_1 and V_2 to neighbourhoods U_1 and U_2 with

$$\gamma(U_1) \cap U_2 = \emptyset \text{ iff } \gamma(\tau_1) \neq \tau_2 :$$

For each $\gamma \in G_\Gamma$ we have

$$\gamma(\tau_1) \neq \tau_2.$$

Because $\mathbb{H}$ is a Hausdorff space we choose for each $\gamma \in G_\Gamma$ two disjoint neighbourhoods of respectively $\gamma(\tau_1)$ and τ_2 in $\mathbb{H}$

$$U_{1,\gamma} \subset \mathbb{H},\ U_{2,\gamma} \subset \mathbb{H} \text{ and } U_{1,\gamma} \cap U_{2,\gamma} = \emptyset,$$

and define two neighbourhoods of respectively τ_1 and τ_2 in $\mathbb{H}$

$$U_1 := V_1 \cap \left(\bigcap_{\gamma \in G_\Gamma} \gamma^{-1}(U_{1,\gamma}) \right),\ U_2 := V_2 \cap \left(\bigcap_{\gamma \in G_\Gamma} U_{2,\gamma} \right).$$

Then for all $\gamma \in G_\Gamma$

$$\gamma(U_1) \cap U_2 = \emptyset.$$

3. *Isotropy group Γ_τ*: The add-on is the specific case

$$\tau = \tau_1 = \tau_2.$$

Apply part 2) and set

$$U := U_1 \cap U_2$$

4. *Elliptic points form a discrete subset*: Each

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,\ \gamma \neq \pm id,$$

fixes at most one point $z \in \mathbb{H}$: If $z \in \mathbb{H}$ and $\gamma(z) = z$ then z satisfies the quadratic equation

$$cz^2 + (d-a)z - b = 0$$

If

$$c \neq 0 \text{ or } d \neq a \text{ or } b \neq 0$$

the equation has at most two solutions, counted with multiplicity. The same quadratic equation is also satisfied by $\bar{z}$. Because $z \neq \bar{z}$, the equation has no further solution. Hence there is no

$$z' \in \mathbb{H},\ z' \neq z,$$

satisfying $\gamma(z') = z'$. For any elliptic point $\tau' \in U$ exists

$$\gamma \in \Gamma_{\tau'},\ \gamma \neq \pm id.$$

Because

$$\tau' \in \gamma(U) \cap U$$

the previous part of the proof implies

$$\gamma \in \Gamma_\tau$$

and therefore $\tau = \tau'$, q.e.d.

Lemma 2.20 (Openness of the canonical projection onto the orbit space). *Denote by*

$$p : \mathbb{H} \to Y := \Gamma \backslash \mathbb{H}$$

the canonical projection onto the orbit space of the action

$$\Phi : \Gamma \times \mathbb{H} \to \mathbb{H}$$

and provide Y with the corresponding quotient topology. Then p is an open map.

Proof. By definition of the quotient topology a subset $U \subset Y$ is open iff

$$p^{-1}(U) \subset \mathbb{H}$$

is open.

For each arbitrary but fixed $\gamma \in \Gamma$ its orbit map, the restriction

$$\Phi(\gamma, -) : \mathbb{H} \to \mathbb{H},\ \tau \mapsto \gamma(\tau),$$

is continuous with inverse the orbit map of γ^{-1}

$$\Phi(\gamma^{-1}, -) : \mathbb{H} \to \mathbb{H},\ \tau \mapsto \gamma^{-1}(\tau).$$

Hence the orbit map $\Phi(\gamma, -)$ is a homeomorphism.

In order to prove the openness of p we consider an open set $U \subset \mathbb{H}$ and prove the openness of $p(U) \subset Y$: The inverse image

$$p^{-1}(p(U)) = \bigcup_{\gamma \in \Gamma} \gamma(U)$$

is open as union of open sets. Hence

$$p(U) \subset Y$$

is open by definition of the quotient topology, q.e.d.

Theorem 2.21 (Hausdorff topology of the orbit space). *The quotient topology on the orbit space*

$$Y := \Gamma \backslash \mathbb{H}$$

is Hausdorff.

Proof. Consider two distinct points $y_1 \neq y_2 \in Y$. For $j = 1, 2$ chooose two points $\tau_j \in \mathbb{H}$ with $p(\tau_j) = y_j$. The assumption

$$p(\tau_1) \neq p(\tau_2)$$

implies: For all $\gamma \in \Gamma$

$$\gamma(\tau_1) \neq \tau_2.$$

As a consequence, Lemma 2.19 provides two open neighbourhoods $U_j \subset \mathbb{H}$ of respectively τ_1 and of τ_2 with

$$\gamma(U_1) \cap U_2 = \emptyset$$

for all $\gamma \in \Gamma$. Hence

$$p(U_1) \cap p(U_2) = \emptyset.$$

Lemma 2.20 implies that the sets $p(U_j) \subset Y,\ j = 1,2$ are open. Hence they are disjoint open neighbourhoods of respectively

$$y_1 = p(\tau_1) \text{ and } y_2 = p(\tau_2),\ q.e.d.$$

With Theorem 2.21 the present section has obtained its first goal. Its second goal is to embed the result into the general context: Which properties ensure that a set of equivalence classes becomes a Hausdorff space when provided with the quotient topology with respect to the canonical projection? We introduce the general concept of a *proper* group action in Definition 2.22 and prove the Hausdorff criterion from Lemma 2.24.

Definition 2.22 (Proper group action). Consider a continuous action

$$G \times X \to X,\ (g,x) \mapsto g(x),$$

of a locally compact group G on a locally compact space X. The action is a *proper group action* if

$$\sigma : G \times X \to X \times X,\ (g,x) \mapsto (x, g(x)),$$

is a proper map, i.e. if the inverse image of a compact set is again compact.

Note. The image of the map σ from Definition 2.22 is the equivalence relation

$$R \subset X \times X$$

which the group action induces on X.

Corollary 2.23 (Proper action of the modular group). *The action of the modular group*

$$\Phi : \Gamma \times \mathbb{H} \to \mathbb{H}$$

is a proper group action.

Proof. Consider a compact subset

$$K \subset \mathbb{H} \times \mathbb{H}.$$

In order to show the compactness of

$$\sigma^{-1}(K) \subset \Gamma \times \mathbb{H}$$

it suffices to show that $\sigma^{-1}(K)$ is sequentially compact. We claim: Any sequence

$$(\gamma_\nu, \tau_\nu)_{\nu \in \mathbb{N}}$$

in $\sigma^{-1}(K)$ has a convergent subsequence. Due to compactness of K we may assume that the image sequence

$$(\sigma(\gamma_\nu, \tau_\nu))_{\nu\in\mathbb{N}} = (\tau_\nu, \gamma_\nu(\tau_\nu))_{\nu\in\mathbb{N}}$$

is convergent. Set

$$x_1 := \lim_{\nu\to\infty} \tau_\nu,\ x_2 := \lim_{\nu\to\infty} \gamma_\nu(\tau_\nu) \text{ (pointwise convergence)}.$$

We have to derive from the convergent sequences of points in $\mathbb{H}$

$$(\tau_\nu)_{\nu\in\mathbb{N}} \text{ and } (\gamma_\nu(\tau_\nu))_{\nu\in\mathbb{N}}$$

the existence of a convergent subsequence of group elements $(\gamma_\nu)_{\nu\in\mathbb{N}} \in \Gamma$:

Lemma 2.19 implies the existence of open neighbourhoods $U_i \subset \mathbb{H}$ of $x_i,\ i = 1,2$, such that for all $\gamma \in \Gamma$

$$\gamma(U_1) \cap U_2 \neq \emptyset \implies \gamma(x_1) = x_2.$$

Due to the pointwise convergence for all $\nu \in \mathbb{N}$ but finitely many indices

$$\tau_\nu \in U_1 \text{ and } \gamma_\nu(\tau_\nu) \in U_2,$$

hence

$$\gamma_\nu(U_1) \cap U_2 \neq \emptyset.$$

The lemma implies

$$\gamma_\nu(x_1) = x_2$$

The set

$$\{\gamma \in \Gamma : \gamma(x_1) = x_2\}$$

has the same cardinality as the isotropy group Γ_{x_1}. The latter is a finite group due to Theorem 2.16. A subsequence $(\gamma_\nu)_{\nu\in\mathbb{N}}$ becomes stationary, hence convergent, q.e.d.

Lemma 2.24 (Hausdorff criterion for an equivalence relation). *Let X be a topological space and*

$$R \subset X \times X$$

an equivalence relation on X. Then the set of equivalence classes X/R provided with the quotient topology with respect to the canonical map

$$p : X \to X/R$$

is a Hausdorff spaces if both of the following conditions are satisfied:

- *The map p is open*

- *The equivalence relation $R \subset X \times X$ is closed.*

Proof. See [18, Chap. VII, 1.6]: Consider $x, y \in X$ with

$$p(x) \neq p(y)$$

as classes in X/R. Then $(x,y) \notin R$. Because $R \subset X \times X$ is closed, there is a neighbourhood

$$U \times V \subset (X \times X) \setminus R$$

of $(x,y) \in X \times X$. Openness of p implies the existence of neigbourhoods

$$p(U), p(V) \subset X/R$$

of respectively $p(x)$ and $p(y)$ with

$$p(U) \cap p(V) = \emptyset, \ q.e.d.$$

With the new concepts and results the proof of the Hausdorff property from Theorem 2.21 reads as follows:

Corollary 2.25 (Hausdorff topology of the orbit space). *The quotient topology on the orbit space*

$$Y := \Gamma \backslash \mathbb{H}$$

is Hausdorff.

Proof. We apply Lemma 2.24: First, Lemma 2.20 states that p is an open map. Secondly, we have

$$R = \sigma(\Gamma \times \mathbb{H}) \subset \mathbb{H} \times \mathbb{H}$$

According to Corollary 2.23 the map

$$\sigma : \Gamma \times \mathbb{H} \to \mathbb{H} \times \mathbb{H}$$

is proper, and therefore a closed map. Therefore Lemma 2.24 implies: The orbit space Y, provided with the quotient topology, is a Hausdorff space, q.e.d.

As a consequence of the Hausdorff property of the orbit space Y each orbit

$$p^{-1}(y) \subset \mathbb{H}, \ y \in Y,$$

of the Γ-action is closed.

2.3 Modular curves $X(\Gamma_0(N))$ as compact Riemann surfaces

The elliptic points of the group action are those points which complicate the introduction of a complex structure on the orbit space Y. To overcome this difficulty we make a detailed study of the group action in the neighbourhood of an elliptic point. Fortunately, here the action restricts to the action of the isotropy group and the latter turns out as a group of rotations. The statement of the following Lemma 2.26 is trivial for non-elliptic points.

For elliptic points it relies on the Lemma of Schwarz. Lemma 2.26 states: Locally the isotropy group of an elliptic point $\tau \in \mathbb{H}$ with period h_τ acts as the group of rotations of a disk around the origin with angles a multiple of $2\pi/h_\tau$.

Lemma 2.26 (Isotropy group acting as group of rotations). *For any point $\tau \in \mathbb{H}$ exist*

- *a neighbourhood $U_\tau \subset \mathbb{H}$ of τ such that for all $\gamma \in \Gamma$*

$$\gamma(U_\tau) \cap U_\tau \neq \emptyset \implies \gamma \in \Gamma_\tau,$$

- *and a fractional linear transformation $\lambda_\tau \in GL(2,\mathbb{C})$ satisfying*

$$\lambda_\tau : U_\tau \xrightarrow{\simeq} \Delta_\tau$$

with a disc $\Delta_\tau = \{z \in \Delta : |z| < r_\tau\}$ for a suitable radius $r_\tau > 0$

such that: For all $\gamma \in \Gamma_\tau$ the conjugate map

$$\tilde{\gamma}_\tau := \lambda_\tau \circ \gamma \circ \lambda_\tau^{-1} : \Delta_\tau \to \Delta_\tau$$

from the commutative diagram

$$\begin{array}{ccc} U_\tau & \xrightarrow{\ \gamma\ } & \gamma(U_\tau) \\ {\scriptstyle\lambda_\tau}\downarrow & & \downarrow{\scriptstyle\lambda_\tau} \\ \Delta_\tau & \xrightarrow{\ \tilde{\gamma}_\tau\ } & \Delta_\tau \end{array}$$

is a rotation around $0 \in \Delta_\tau$. The angle of rotation is an integer multiple of $2\pi/h_\tau$.

Proof. Due to Theorem 2.16 w.l.o.g.

$$\tau \in \{i,\ \rho\}.$$

Denote by

$$\lambda_\tau : \mathbb{P}^1 \to \mathbb{P}^1,\ \lambda_\tau(z) := \frac{z-\tau}{z-\overline{\tau}},$$

the fractional linear automorphism of $\mathbb{P}^1$ with $\lambda(\mathbb{H}) = \Delta$ and

$$\lambda_\tau(\tau) = 0,\ \lambda_\tau(\overline{\tau}) = \infty.$$

The following diagram commutes for all $\gamma \in \Gamma_\tau$

$$\begin{array}{ccc} \mathbb{H} & \xrightarrow{\ \gamma\ } & \mathbb{H} \\ {\scriptstyle\lambda_\tau}\downarrow & & \downarrow{\scriptstyle\lambda_\tau} \\ \Delta & \xrightarrow{\ \tilde{\gamma}_\tau\ } & \Delta \end{array}$$

The conjugate

$$\tilde{\gamma}_\tau := \lambda_\tau \circ \gamma \circ \lambda_\tau^{-1} : \Delta \to \Delta$$

has the fixed point $0 \in \Delta$. The non-trivial isotropy groups are

$$\Gamma_i = < S > \text{ and } \Gamma_\rho = < ST > .$$

For $\tau \in \{i,\ \rho\}$ one checks

$$|\tilde{\gamma}_\tau'(0)| = |\gamma'(\tau)| = 1$$

because in particular

$$|S'(i)| = |(ST)'(\rho)| = 1.$$

The Lemma of Schwarz implies that

$$\tilde{\gamma}_\tau : \Delta \to \Delta$$

is a rotation

$$\tilde{\gamma}_\tau(z) = e^{k\cdot(2\pi i/h_\tau)} \cdot z,\ k \in \{0, 1, ..., h_\tau - 1\}$$

We choose a disk $\Delta_\tau \subset \Delta$ such that the neighbourhood of $\tau \in \mathbb{H}$

$$U_\tau := \lambda_\tau^{-1}(\Delta_\tau)$$

satisfies the properties from Lemma 2.19. Then restricting the above digram proves the claim, q.e.d.

In order to obtain a complex structure on the orbit space, the Hausdorff space

$$Y = \Gamma \backslash \mathbb{H},$$

we introduce charts on Y with holomorphic transition functions using the canonical projection

$$p : \mathbb{H} \to Y.$$

Around the class $p(\tau) \in Y$ of an elliptic point $\tau \in \mathbb{H}$ we may consider the isotropy groups Γ_τ as cyclic groups of rotations of a disk Δ_τ due to Lemma 2.26. Assume

$$(1/2) \cdot ord\ \Gamma_\tau = h_\tau =: k.$$

Then in a neighbourhood Δ_τ of $\lambda_\tau(\tau)$ the function

$$z \mapsto z^k$$

foliates the k different segments of the disk Δ_τ, which are eqivalent under the Γ_τ-action, to an open set $W_\tau \subset \mathbb{C}$, see Figure 2.5, and induces a chart

$$p(U_\tau) \xrightarrow{\phi_\tau} W_\tau.$$

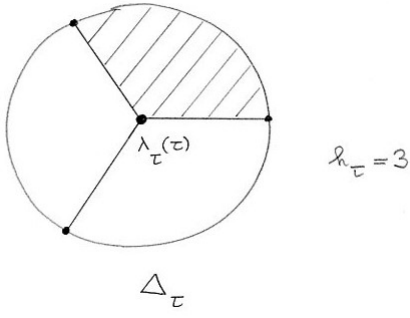


Fig. 2.5 The three equivalent segments of the disk Δ_τ of an elliptic point $\tau \in \mathbb{H}$ with $h_\tau = 3$

Proposition 2.27 (Analytic structure of the orbit space). *On the orbit space*

$$Y = \Gamma \backslash \mathbb{H}$$

exists an analytic structure such that Y becomes a Riemann surface and the canonical projection

$$p : \mathbb{H} \to Y$$

becomes a holomorphic map.

Considered from a general point of view the complex manifold Y is the *coarse moduli space* of complex tori.

Proof. i) *Homeomorphisms*: For each $\tau \in \mathbb{H}$ choose a neighbourhood $U_\tau \subset \mathbb{H}$ of τ with the properties from lemma 2.26. Using the notation from the lemma define

$$pow_\tau : \Delta_\tau \to \mathbb{C}, z \mapsto z^{h_\tau},$$

and set

$$W_\tau := pow_\tau(\Delta_\tau)$$

Eventually, define a chart of Y around $y = p(\tau) \in Y$

$$\phi_\tau : p(U_\tau) \to W_\tau$$

as the commutative completion of the following diagram

$$\begin{array}{ccc} U_\tau & \xrightarrow{p|U_\tau} & p(U_\tau) \\ \lambda_\tau \downarrow & & \downarrow \phi_\tau \\ \Delta_\tau & \xrightarrow{pow_\tau} & W_\tau \end{array}$$

The map ϕ_τ is

- well-defined and bijective according to Lemma 2.26 because for all $\gamma \in \Gamma \setminus \Gamma_\tau$

  $$\gamma(U_\tau) \cap U_\tau = \emptyset.$$

  The different inverse images under $p|U_\tau$ of a given point from $p(U_\tau)$ are identified by $pow_\tau \circ \lambda_\tau$,
- continuous, because p is open,
- open, because λ_τ and pow_τ are open.

As a consequence, ϕ_τ is a homeomorphism.

ii) *Explicit form of the transition functions*: We show that the family

$$\mathfrak{A} := (\phi_\tau : p(U_\tau) \to W_\tau)_{\tau \in \mathbb{H}}$$

is a complex atlas of Y.

Assume two charts

$$\phi_{\tau_i} : p(U_{\tau_i}) \to W_{\tau_i}$$

around points $y_i = p(\tau_i) \in Y,\ i = 1,2$, and assume

$$p(U_{\tau_1}) \cap p(U_{\tau_2}) \neq \emptyset.$$

To simplify the subscripts we set

$$U_i := U_{\tau_i}, \phi_i := \phi_{\tau_i}, \lambda_i := \lambda_{\tau_i}, h_i := h_{\tau_i}, W_{\tau_i} := W_i,\ i = 1,2.$$

Consider a point

$$x \in p(U_1) \cap p(U_2),$$

see Figure 2.6.

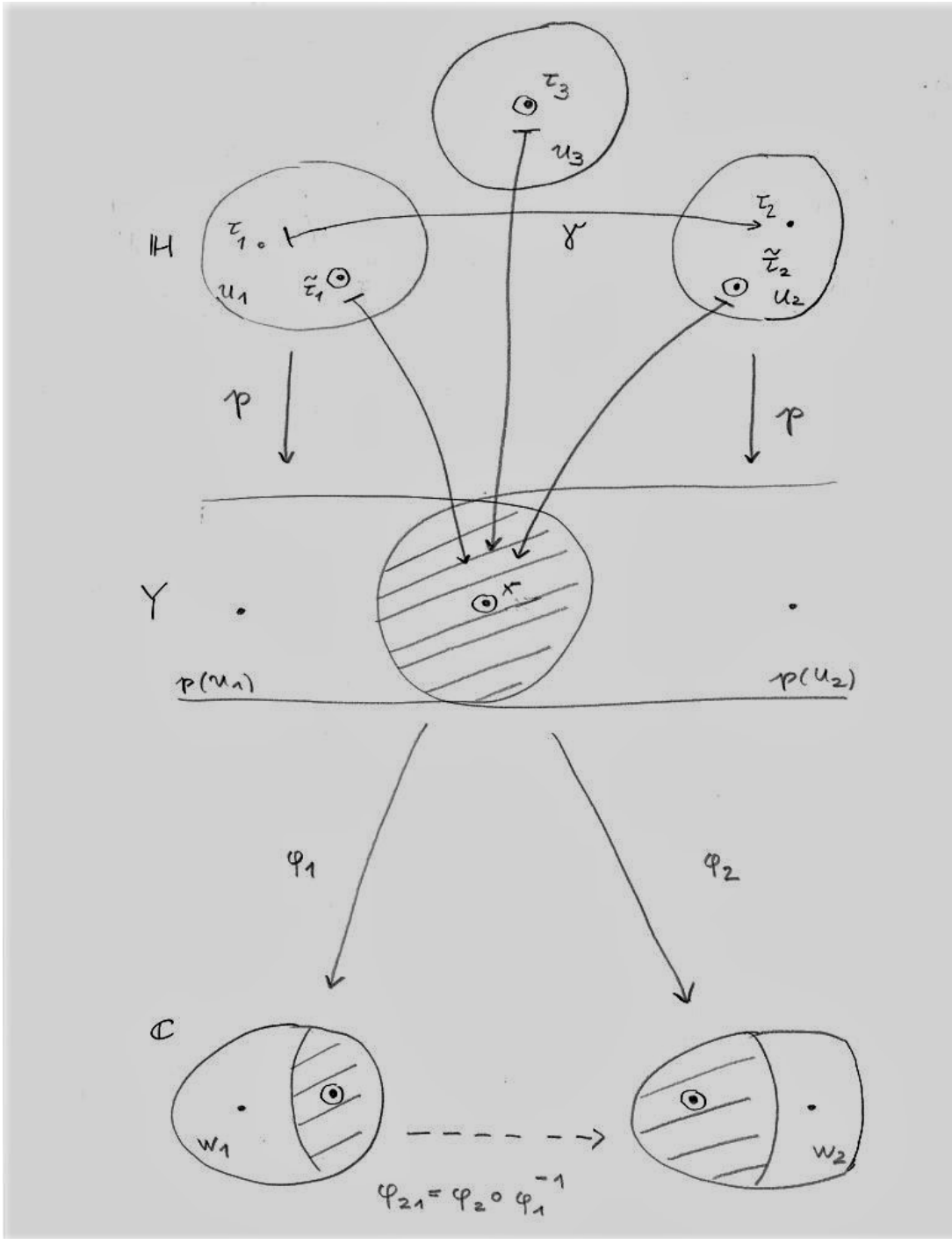


Fig. 2.6 Transition functions of Y

We show that the transition function

$$\phi_{2,1} := \phi_2 \circ \phi_1^{-1}$$

is holomorphic in a neighbourhood of $\phi_1(x) \in W_1 \subset \mathbb{C}$: By definition of ϕ_i two points $\tilde{\tau}_i \in U_i,\ i = 1,2$, exist with

$$\lambda_i(\tilde{\tau}_i)^{h_i} = \phi_i(x),\ i = 1,2.$$

They satisfy $\tilde{\tau}_2 = \gamma(\tilde{\tau}_1)$ for a suitable $\gamma \in \Gamma$. Hence for $q \in \mathbb{C}$ in a neighbourhood of $\phi_1(x)$ the transition functions attains the value

$$\phi_{2,1}(q) = \left((\lambda_2 \circ \gamma \circ \lambda_1^{-1})(q^{1/h_1})\right)^{h_2}$$

We have to prove: Taking the h_1-root does not prevent the holomorphy of the map.

iii) *Holomorphy of the transition functions*: We prove the non-trivial case $h_1 > 1$, i.e. we assume that the orbit $x \in X$ is elliptic.

- Case $\phi_1(x) = 0 \in W_1$, i.e. $\tilde{\tau}_1 = \tau_1$:

  The point

  $$\tau_1 = \tilde{\tau}_1$$

  is elliptic. Therefore also $\tilde{\tau}_2 = \gamma(\tilde{\tau}_1) \in U_2$ is elliptic. Because τ_2 is the only elliptic point in U_2 we obtain $\tilde{\tau}_2 = \tau_2$, and

  $$\tau_2 = \gamma(\tau_1) \text{ and } h := h_2 = h_1.$$

  By construction of $\lambda_i,\ i = 1,2$, the composition of fractional linear transformations

  $$\lambda_2 \circ \gamma \circ \lambda_1^{-1}$$

  is a fractional linear transformation of $\mathbb{P}^1$ mapping 0 to 0 and ∞ to ∞. Therefore a matrix

  $$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{C})$$

  exists with

  $$\lambda_2 \circ \gamma \circ \lambda_1^{-1} = A$$

  and

  $$A \cdot (0\ 1)^\top = (0\ 1)^\top,\ A \cdot (1\ 0)^\top = (1\ 0)^\top.$$

  With respect to the injection

  $$\mathbb{C} \hookrightarrow \mathbb{P}^1,\ z \mapsto (z:1),$$

  – the vector $(0\ 1)^\top \in \mathbb{C}^2$ represents the point $(0:1) \in \mathbb{P}^1$ and the point $0 \in \mathbb{C}$,

– while the vector $(1\ 0)^\top \in \mathbb{C}^2$ represents the point $(1:0) \in \mathbb{P}^1$ and the point $\infty \in \mathbb{C} \cup \{\infty\}$.

As a consequence

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

and

$$\phi_{2,1}(q) = \left((\lambda_2 \circ \gamma \circ \lambda_1^{-1})(q^{1/h})\right)^h = \left(A(q^{1/h})\right)^h = ((a \cdot q^{1/h})/d)^h = (a/d)^h \cdot q.$$

Therefore $\phi_{2,1}$ is linear, and hence holomorphic in a neighbourhood of $0 = \phi_1(x)$.

- Case $\phi_2(x) = 0 \in W_2$, i.e. $\tilde{\tau}_2 = \tau_2$:

  The previous case shows the holomorphy of $\phi_{1,2}$ in a suitable neighbourhood. Because the map is bijective, its inverse $\phi_{2,1}$ is holomorphic.

- Case $\phi_1(x) \in W_1$ arbitrary, i.e. $\tilde{\tau}_1 \in U_1$ arbitrary:

  We reduce this case to the other two cases. Choose $\tau_3 \in \mathscr{D}$ with $p(\tau_3) = x$ and consider the chart

  $$\phi_{\tau_3} : U_{\tau_3} \to W_{\tau_3}$$

  with the shorthand

  $$U_3 := U_{\tau_3}, \phi_3 := \phi_{\tau_3}, W_3 := W_{\tau_3}.$$

  In a suitable neighbourhood W of x with

  $$W \subset (p(U_1) \cap p(U_2) \cap p(U_3))$$

  we have

  $$\phi_{1,2} = \phi_{1,3} \circ \phi_{3,2}.$$

  The right-hand side is holomorphic due to part i) and ii). Therefore $\phi_{1,2}$ is holomorphic, q.e.d.

The important steps in the proof of Proposition 2.27 and its prerequisites:

- The modular group acts properly.
- Isotropy groups act as rotations (Lemma of Schwarz).
- Suitable fractional-linear maps $\lambda : \mathbb{H} \xrightarrow{\simeq} \Delta$.

The upper half-plane has a canonical boundary point, the point ∞. The extension of the group action from Remark 2.8 shows that one has to consider also the rational line $\mathbb{Q}$, but not $\mathbb{R} \setminus \mathbb{Q}$, as part of the boundary.
When extending the Euclidean topology of $\mathbb{H}$ to a topology on $\mathbb{H}^*$, one has to define the neighbourhoods in $\mathbb{H}^*$ of the additional points from

$$\mathbb{Q} \cup \{\infty\}.$$

First, surprisingly as a neighbourhood basis of $\infty \in \mathbb{H}^*$ one does not take the complements of compact sets in $\mathbb{C}$ as one does for the point

$$\infty \in \mathbb{P}^1$$

from the Riemann sphere, alias projective space. Instead one takes the sets

$$\{z \in \mathbb{C} : \ Im\, z > R\} \cup \{\infty\},\ R > 0,$$

i.e. the complements of sets with bounded imaginary part. Secondly, one translates neighbourhoods of ∞ to neighbourhoods of a rational $q \in \mathbb{Q}$ by fractional-linear transformations $\gamma \in \Gamma$ with

$$\gamma(\infty) = q.$$

The resulting neighbourhood basis of a point $q \in \mathbb{Q}$ are disks in $\mathbb{H}$ with q a point on the Euclidean boundary of the disk, see Figure 2.7. The second step is determined by the requirement, that the modular group acts as group of homeomorphisms on $\mathbb{H}^*$. The new topology of $\mathbb{H}^*$ induces on $\mathbb{Q}$ the discrete topology. Apparently the latter is finer than the topology induced on $\mathbb{Q}$ by the Euclidean topology of $\mathbb{R}$.

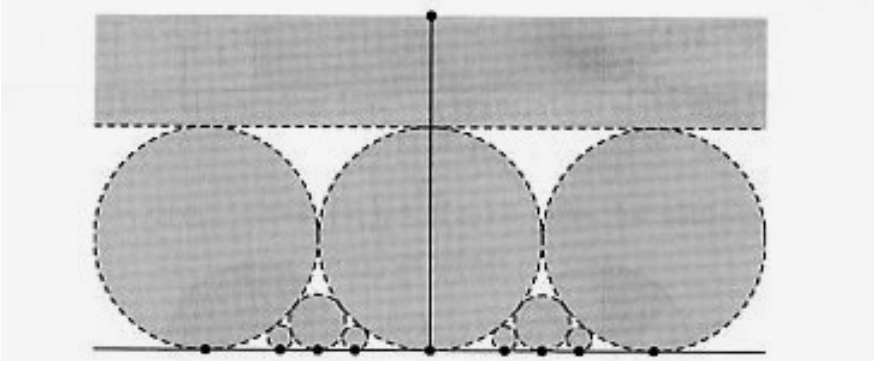


Fig. 2.7 Neighbourhoods of infinity and of some rational points from $\mathbb{H}^*$, from [17, Fig. 2.5]

Theorem 2.28 (The modular curve of the modular group). *Consider the action of the modular group Γ on the extended upper half-plane*

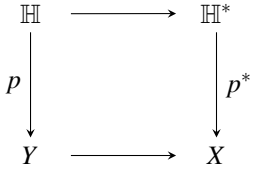
$$\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}.$$

according to Remark 2.8.

1. *On the orbit space*

$$X := \Gamma \backslash \mathbb{H}^*$$

exists the structure of a compact Riemann surface such that the following diagram commutes with canonical projections p and p^* and canonical injections in the horizontal direction



2. *The Riemann surface X is biholomorphic equivalent to* $\mathbb{P}^1$.

Proof. i) *Topology on* $\mathbb{H}^*$: Take as neighbourhood basis of ∞ for the topology on $\mathbb{H}^*$ the sets

$$U_R := \{\tau \in \mathbb{H} : Im\ \tau > R\} \cup \{\infty\},\ R > 0,$$

and as neighbourhood basis of

$$q := a/c \in \mathbb{Q},\ gcd(a,c) = 1,$$

the sets

$$\gamma(U_R),\ R > 0,\ \gamma = \begin{pmatrix} a & * \\ c & * \end{pmatrix} \in \Gamma,$$

because

$$\gamma(\infty) = q$$

due to Remark 2.8. These neighbourhood bases together with the open sets of $\mathbb{H}$ generate a topology on $\mathbb{H}^*$ with $\mathbb{H} \subset \mathbb{H}^*$ an open subspace.

Note. Because fractional linear transformations from Γ take lines to circles or lines the neighbourhoods of $\gamma(U_N)$ are circles tangent to the real axis at the distinguished point $a/c \in \mathbb{Q}$. Hence neighbourhoods of ∞ and of rational points are completely different from their counterpart with respect to the Euclidan topology, see Figure 2.7.

ii) *Hausdorff quotient topology on* $\Gamma \backslash \mathbb{H}^*$: We provide the set

$$X := \Gamma \backslash \mathbb{H}^*$$

with the quotient topology with respect to the canonical projection

$$p^* : \mathbb{H}^* \to X.$$

Then p^* is an open map: The proof is the same as the corresponding proof for Lemma 2.20. The proof uses only the fact that the quotient arises from a group action.

In order to show that X is Hausdorff we consider two points

$$x_i = p^*(\tau_i) \in X,\ \tau_i \in \mathbb{H}^*,\ i = 1,2, \text{ and assume } x_1 \neq x_2.$$

We distinguish the following cases:

- $\tau_1 \in \mathbb{H},\ \tau_2 \in \mathbb{Q} \cup \{\infty\}$: W.l.o.g. $\tau_2 = \infty$. For each

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

  the formula

  $$Im\ \gamma(\tau) = \frac{Im\ \tau}{|c \cdot \tau + d|^2} = \frac{Im\ \tau}{(c \cdot Re\ \tau + d)^2 + c^2 \cdot (Im\ \tau)^2} \leq$$

  $$\leq Im\ \tau \cdot \begin{cases} \dfrac{1}{d^2} & c = 0 \\ \dfrac{1}{c^2 \cdot (Im\ \tau)^2} & c \neq 0 \end{cases} \leq \begin{cases} Im\ \tau & c = 0 \\ \dfrac{1}{Im\ \tau} & c \neq 0 \end{cases} \leq \max\{Im\ \tau, 1/Im\ \tau\}$$

  shows

  $$Im\ \gamma(\tau) \leq max\{Im\ \tau, 1/(Im\ \tau)\},$$

  independently from γ. Therefore a relatively compact neighbourhood

  $$U_1 \subset\subset \mathbb{H}$$

  of τ_1 and a neighbourhood

  $$U_2 \subset \mathbb{H}^*$$

  of $\tau_2 = \infty$ exist such that for all $\gamma \in \Gamma$

  $$\gamma(U_1) \cap U_2 = \emptyset.$$

  As a consequence

  $$p^*(U_1) \cap p^*(U_2) = \emptyset.$$

- $\tau_1, \tau_2 \in \mathbb{H}$: This case has been considered already by Corollary 2.25.

iii) *Compactness of X*: Denote by $\overline{\mathscr{D}}^{\mathbb{H}} \subset \mathbb{H}$ the closure of $\mathscr{D}$ with respect to $\mathbb{H}$. Then

$$\overline{\mathscr{D}} := \overline{\mathscr{D}}^{\mathbb{H}} \cup \{\infty\} \subset \mathbb{H}^*$$

is compact with respect to $\mathbb{H}^*$: Consider an open covering $(U_i)_{i\in I}$ of $\overline{\mathscr{D}}$. If $\infty \in U_{i_0}$ then for suitable $R > 0$:

$$\{\tau \in \overline{\mathscr{D}}^{\mathbb{H}} : Im\ \tau > R\} \cup \{\infty\} \subset U_{i_0}.$$

The remaining set

$$\{\tau \in \overline{\mathscr{D}}^{\mathbb{H}} : Im\ \tau \leq R\}$$

is compact in $\mathbb{H}$, and therefore covered by a finite subcovering of $(U_i)_{i\in I}$. As a consequence X is compact as continuous image via p^* of the compact set

$$\overline{\mathscr{D}} \subset \mathbb{H}^*.$$

One has

$$Y = X \setminus \{p^*(\infty)\}.$$

Therefore $Y \subset X$ is an open subset.

iv) *Charts of the modular curve*: In order to define a chart

$$\phi_\infty : p^*(U_\infty) \to W_\infty$$

around the cusp

$$x = p^*(\infty) \in X$$

we consider the neighbourhood of $\infty \in \mathbb{H}^*$

$$U_\infty := U_2 = \{\tau \in \mathbb{H} : Im\ \tau > 2\} \cup \{\infty\}.$$

We define

$$pow_\infty : U_\infty \to \Delta,\ \tau \mapsto \begin{cases} e^{2\pi i\cdot\tau} & \text{if } \tau \neq \infty \\ 0 & \text{if } \tau = \infty \end{cases}$$

and set

$$W_\infty := pow_\infty(U_\infty) \subset \Delta.$$

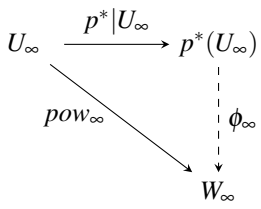
For two points $\tau_i \in U_\infty, i = 1,2$,

$$p^*(\tau_2) = p^*(\tau_1) \iff \tau_2 = \gamma(\tau_1) \text{ for a suitable } \gamma \in \Gamma$$

$$\iff \tau_2 = \tau_1 + m \text{ for a suitable } m \in \mathbb{Z}, \text{ due to Theorem 2.16,}$$

$$\iff pow_\infty(\tau_2) = pow_\infty(\tau_1).$$

We define the chart ϕ_∞ as the commutative completion of the diagram



One shows analogously to the proof of Proposition 2.27 that the map ϕ_∞ is a homeomorphism.

Eventually we have to show that the charts of Y and the chart ϕ_∞ are compatible, It suffices to prove the compatibility of the chart

$$\phi_\infty : p^*(U_\infty) \to W_\infty$$

around $p^*(\infty)$ with the chart

$$\phi_\tau : p(U_\tau) = p^*(U_\tau) \to W_\tau$$

around an arbitrary point $p(\tau),\ \tau \in \mathbb{H}$. We may assume that U_τ does not contain an elliptic point, and therefore that

$$\phi_\tau \circ (p^*|U_\tau)$$

is injective and biholomorphic. Hence the transition function of the two charts is holomorphic.

v) *Modular curve* $X \simeq \mathbb{P}^1$: The image of the fundamental domain

$$Y = p(\mathscr{D})$$

is homeomorphic to the plane $\mathbb{C}$: Identify points on the left and right boundary of $\mathscr{D}$ and equivalent points of $\mathscr{D}$ on the left part of the unit circle and on the right part. Therefore the compactification of Y is homeomorphic to the 1-point compactification of $\mathbb{C}$, i.e. X is homeomorphic to S^2. The only complex structure on the sphere S^2 is the complex projective space $\mathbb{P}^1(\mathbb{C})$, cf. [63], q.e.d.

For the biholomorphy

$$X \simeq \mathbb{P}^1$$

a formal proof will be given in Corollary 3.16. This second proof uses the modular invariant j from the theory of modular forms.

Definition 2.29 (Modular curve of Γ). The compact Riemann surface from Theorem 2.28

$$X(1) := X(\Gamma) := \Gamma\backslash\mathbb{H}^*$$

is named the *modular curve of* Γ or simply the *modular curve*.

An analogous construction of a modular curve can be made for each congruence subgroup $\Gamma_0(N) \subset \Gamma$.

Remark 2.30 (Modular curves of the congruence subgroups). Generalizing the construction of the modular curve

$$X(1) = \Gamma\backslash\mathbb{H}^*$$

from Theorem 2.28 one can introduce for each Hecke congruence subgroup

$$\Gamma_0(N) \subset \Gamma,\ N \in \mathbb{N},$$

a complex structure on the orbit space

$$X_0(N) := \Gamma_0(N)\backslash\mathbb{H}^* = (\Gamma_0(N)\backslash\mathbb{H}) \dot\cup \mathit{Cusp}(\Gamma_0(N)),$$

see [17, Prop. 2.4.2ff.] The resulting compact Riemann surface $X_0(N)$ is named the *modular curve* of $\Gamma_0(N)$.

1. *Branched covering of modular curves*: The inclusion of groups

   $$\Gamma_0(N) \hookrightarrow \Gamma(1)$$

   induces a holomorphic branched covering

   $$f : X_0(N) \to X(1)$$

   of compact Riemann surfaces. The covering has degree

   $$deg\ f = [\Gamma : \Gamma_0(N)] = N \cdot \prod_{p|N} \left(1 + \frac{1}{p}\right),$$

   see [17, Exerc. 3.1.1] and Proposition 2.14.

2. *Genus of modular curves*: The Riemann-Hurwitz formula, e.g., [63], applied to the covering

   $$f : X_0(N) \to X(1) \simeq \mathbb{P}^1$$

   computes the genus of the modular curves of the Hecke congruence subgroups as

$$g(X_0(N)) = 1 + \frac{b(f)}{2} - deg\ f$$

with

$$b(f) = \sum_{x \in X_0(N)} b(f;\, x)$$

the total branching order of f.

A detailed investigation of the elliptic points and of the cusps of the action of $\Gamma_0(N)$ shows the *genus formula*

$$g(X_0(N)) = 1 + \frac{deg\ f}{12} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3} - \frac{\varepsilon_\infty}{2}$$

with ε_2, ε_3 and ε_∞ denoting the number of elliptic points of respectively period 2 and 3 and the number of cusps of the action of $\Gamma_0(N)$, see [17, Theor. 3.1.1].

The ε-constants can be computed as

$$\varepsilon_\infty = \sum_{d|N} \Phi(gcd(d, N/d)),$$

see Example 2.11, and ε_2 and ε_3 are the numbers of solutions in $\mathbb{Z}/N\mathbb{Z}$ of the equations respectively

$$x^2 + 1 = 0 \text{ and } x^2 - x + 1 = 0.$$

Using the quadratic residue symbol for $n \in \{-1, -3\}$ and extended to all primes p

$$\left(\frac{-1}{p}\right) := \begin{cases} 0 & \text{if } p = 2 \\ 1 & \text{if } p \equiv 1 \mod 4 \\ -1 & \text{if } p \equiv 3 \mod 4 \end{cases}$$

and

$$\left(\frac{-3}{p}\right) := \begin{cases} 0 & \text{if } p = 3 \\ 1 & \text{if } p \equiv 1 \mod 3 \\ -1 & \text{if } p \equiv 2 \mod 3 \end{cases}$$

one obtains, see [17, Cor. 3.7.2, Exerc. 3.7.6] and [53, Theor. 1.43]:

$$\varepsilon_2 = \begin{cases} \prod_{p|N} \left(1 + \left(\frac{-1}{p}\right)\right) & \text{if } 4 \nmid N \\ 0 & \text{otherwise} \end{cases}$$

and

$$\varepsilon_3 = \begin{cases} \prod_{p|N} \left(1 + \left(\frac{-3}{p}\right)\right) & \text{if } 9 \nmid N \\ 0 & \text{otherwise} \end{cases}$$

3. *Estimate of the genus* $g(X_0(N))$: As a corollary of the genus formula the constants from part 2) satisfy the estimate

$$2 \cdot g(X_0(N)) - 2 + \frac{\varepsilon_2}{2} + \frac{2\varepsilon_3}{3} + \varepsilon_\infty > 0.$$

4. *Modular curves of prime level*: For a prime $p \in \mathbb{N}$ and $k := p+1$ the modular curve $X_0(p)$ has the genus

$$g(X_0(p)) = \begin{cases} \left\lfloor \frac{k}{12} \right\rfloor - 1 & \text{if } k \equiv 2 \mod 12 \\ \left\lfloor \frac{k}{12} \right\rfloor & \text{otherwise} \end{cases}$$

In particular,

$$g(X_0(2)) = 0,\ g(X_0(11)) = 1,\ g(X_0(13)) = 0 \text{ and } g(X_0(17)) = 1$$

5. *Numerical example*: See the PARI-file "modular_curve_as_covering". For the computation of the extended quadratic residue symbol PARI provides the command

kronecker(a,p).

The Kronecker symbol is defined for arbitrary integer $a \in \mathbb{Z}$ and arbitrary primes including $p = 2$ by extending the Legendre symbol:

- *Odd prime* p:

$$kronecker(a,p) := \left(\frac{a}{p}\right) \text{ for odd } p$$

- *Even prime* $p = 2$:

$$kronecker(a,2) := \begin{cases} 0 & \text{if } a \text{ even} \\ (-1)^{(a^2-1)/8} & \text{otherwise} \end{cases}$$

The Kronecker symbol satisfies

- *Odd prime* p:

$$kronecker(-4,p) = \left(\frac{-4}{p}\right) = \left(\frac{2}{p}\right)^2 \cdot \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right)$$

- *Even prime* $p = 2$:

$$kronecker(-4,2) = 0 = \left(\frac{-1}{2}\right) \text{ and } kronecker(-3,2) = -1 = \left(\frac{-3}{2}\right)$$

Hence

$$\varepsilon_2 = \begin{cases} \prod_{p|N}(1 + kronecker(-4,p)) & \text{if } 4 \nmid N \\ 0 & \text{otherwise} \end{cases}$$

and

$$\varepsilon_3 = \begin{cases} \prod_{p|N}(1 + kronecker(-3,p)) & \text{if } 9 \nmid N \\ 0 & \text{otherwise} \end{cases}$$

Figure 2.8 shows the invariants of the covering

$$X_0(p) \to X(1)$$

for all primes $p < 100$.

```
modular_curve_as_covering: Start
modular_curve_as_covering: Modular curve X_0(N)
as branched covering of modular curve X(1).

(N, genus, d, eps_2, eps_3, eps_inf)=(2, 0, 3, 1, 0, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(3, 0, 4, 0, 1, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(5, 0, 6, 2, 0, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(7, 0, 8, 0, 2, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(11, 1, 12, 0, 0, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(13, 0, 14, 2, 2, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(17, 1, 18, 2, 0, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(19, 1, 20, 0, 2, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(23, 2, 24, 0, 0, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(29, 2, 30, 2, 0, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(31, 2, 32, 0, 2, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(37, 2, 38, 2, 2, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(41, 3, 42, 2, 0, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(43, 3, 44, 0, 2, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(47, 4, 48, 0, 0, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(53, 4, 54, 2, 0, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(59, 5, 60, 0, 0, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(61, 4, 62, 2, 2, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(67, 5, 68, 0, 2, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(71, 6, 72, 0, 0, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(73, 5, 74, 2, 2, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(79, 6, 80, 0, 2, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(83, 7, 84, 0, 0, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(89, 7, 90, 2, 0, 2)
(N, genus, d, eps_2, eps_3, eps_inf)=(97, 7, 98, 2, 2, 2)
modular_curve_as_covering: End
```

Fig. 2.8 Modular curves $X_0(N) \to X(1)$

Chapter 3
The algebra of modular forms

Modular forms are holomorphic functions on $\mathbb{H}$ distinguished by two properties:

1. On one hand, they have the modular group as group of symmetries.

2. On the other hand, they expand into a Fourier series around the point ∞ with rational Fourier coefficients after normalization.

The interplay of these two properties is coined "The magic of modular forms" [65]. Therefrom arises a series of remarkable identities between the Fourier coefficients of modular forms. In many cases these identities imply interesting statements about arithmetic functions. We will see examples in Section **??** and Chapter 6.

In general, one introduces modular forms as functions on $\mathbb{H}$ with a certain transformation behaviour with respect to the action of the modular group or its congruence subgroups. The basic examples are the Eisenstein series, see Section 3.2. A meromorphic quotient of certain modular forms is the modular invariant j, see Definition 3.15, a key object of the whole theory. From a more abstract point of view, modular forms are differential forms on the modular curves, which are compact Riemann surfaces, see Theorem 3.17. The Riemann-Roch theorem computes the dimensions of the different vector spaces of modular forms.

3.1 Modular forms and cusp forms

Modular forms are holomorphic functions on $\mathbb{H}$ which transform in a simple manner under the operation of the congruence subgroups $\Gamma_0(N)$ and extend to $\mathbb{H}^*$ in a certain holomorphic way. These functions have a discrete non-Abelian group of symmetries.

We introduce modular forms as analytical objects which are invariant under transformation of the modular group Γ or its Hecke subgroups $\Gamma_0(N)$. In a second step, such invariant objects can be considered analytical objects on the modular curves $X_0(N)$. Because the modular curves are compact Riemann surfaces one cannot expect interesting objects when restricting to invariant holomorphic *functions*. Instead one has to consider more general holomorphic and meromorphic differential forms.

We start from the general context of representation theory of the group Γ, i.e. we introduce a Γ-action on certain vector spaces of holomorphic differential forms.

Proposition 3.1 (Γ-invariant differential forms). *Denote by*

$$W^1 := H^0(\mathbb{H}, \Omega^1_{\mathbb{H}})$$

the vector space of holomorphic differential forms on the upper half-plane $\mathbb{H}$.

1. *The map*
$$\Phi^1 : W^1 \times \Gamma \to W^1,\ (\omega, \gamma) \mapsto \Phi^1(\omega, \gamma) := \gamma^* \omega,$$
is a Γ-right action. For
$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,\ \omega = f\, d\tau \in W^1 \text{ and } \tau \in \mathbb{H}$$
holds
$$\Phi^1(\omega, \gamma)(\tau) := (\gamma^* \omega)(\tau) = (f \circ \gamma)(\tau)\ \frac{d\tau}{(c\tau + d)^2}$$
2. *For even $k \in \mathbb{N}$ set*
$$\Omega^{k/2} := \Omega^{\otimes k/2}_{\mathbb{H}} \text{ and } W^{k/2} := H^0(\mathbb{H}, \Omega^{k/2})$$
and
$$\Phi^{k/2} : W^{k/2} \times \Gamma \to W^{k/2},\ (\omega, \gamma) \mapsto \Phi^{k/2}(\omega, \gamma) := \gamma^* \omega.$$
For
$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,\ \omega = f\, (d\tau)^{k/2} \in W^{k/2} \text{ and } \tau \in \mathbb{H}$$
holds
$$\Phi^{k/2}(\omega, \gamma)(\tau) := ((\gamma^*)^{k/2} \omega)(\tau) = (f \circ \gamma)(\tau)\ \frac{(d\tau)^{k/2}}{(c\tau + d)^k}$$
3. *For even $k \in \mathbb{N}$,*
$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma \text{ and } \omega = f\, (d\tau)^{k/2} \in W^{k/2}$$

holds the equivalence which characterizes invariant differential forms:

$$\gamma^*\omega = \omega \iff f(\tau) = (f\circ\gamma)(\tau)\,\frac{1}{(c\tau+d)^k} \text{ for all } \tau\in\mathbb{H}.$$

Note. In the context of modular forms $\Omega^{k/2}$ denotes the tensor product of Ω^1 not the exterior product.

Proof. 1. We have

$$\Phi^1(\omega,\gamma_1\cdot\gamma_2) = (\gamma_1\cdot\gamma_2)^*\omega = \gamma_2^*(\gamma_1^*\omega) = \Phi^1(\Phi^1(\omega,\gamma_1),\gamma_2)$$

Moreover

$$(d\gamma)(\tau) = d\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{a(c\tau+d)-(a\tau+b)c}{(c\tau+d)^2}\,d\tau = \frac{1}{(c\tau+d)^2}\,d\tau$$

Therefore

$$(\Phi^1(f\,d\tau,\gamma))(\tau) := (\gamma^*(f\,d\tau))(\tau) = f(\gamma(\tau))\,(d\gamma)(\tau) = (f\circ\gamma)(\tau)\,\frac{d\tau}{(c\tau+d)^2}$$

2. For even $k>2$ the proof is analogous by applying the derivation separately for each tensor factor $d\tau$, q.e.d.

Proposition 3.1 shows: For even $k\in\mathbb{N}$ the invariant differential forms from the fixed space of the Γ-representation

$$f\,d\tau^{k/2}\in(W^{k/2})^\Gamma$$

are characterized by holomorphic coefficient functions $f\in\mathscr{O}(\mathbb{H})$ satisfying

$$f(\tau) = (f\circ\gamma)(\tau)\cdot\frac{1}{(c\tau+d)^k}$$

for all

$$\gamma = \begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\Gamma \text{ and } \tau\in\mathbb{H}.$$

If these coefficent functions extend holomorphically to $\infty\in\mathbb{H}^*$ they will be named *modular functions* of weight $=k$. The factors

$$\frac{1}{(c\tau+d)^k}$$

from their transformation law will be isolated and termed *factors of automorphy*, see Definition 3.3.

For the translation

$$T := \begin{pmatrix} a & b \\ c & d \end{pmatrix} := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$$

the factors of automorphy satisfy for all $\tau \in \mathbb{H}$

$$\frac{1}{c\tau + d} = 1.$$

Hence

$$T^*(f\ (d\tau)^{k/2}) = f\ (d\tau)^{k/2} \iff f(\tau+1) = f(\tau) \text{ for all } \tau \in \mathbb{H},$$

and the latter equality means that the function f has the period $= 1$. Hence f expands into a convergent Fourier series

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

similar to the trigonometric function

$$cos(2\pi z) = \frac{1}{2}\left(e^{2\pi i \cdot z} + e^{-2\pi i \cdot z}\right).$$

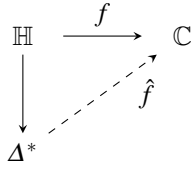
The holomorphic map

$$\mathbb{H} \to \Delta^*, \tau \mapsto e^{2\pi i \tau},$$

surjects to the punctured unit disk

$$\Delta^* := \{z \in \mathbb{C} : 0 < |z| < 1\}.$$

Here neighbourhoods of $\infty \in \mathbb{H}^*$ with respect to the topology of $\mathbb{H}^*$ from Theorem 2.28 are mapped to neighbourhoods of zero. A meromorphic function on $\mathbb{H}$ with period $= 1$ induces a corresponding meromorphic function $\hat{f}$ on Δ^* according to the following diagram



Set

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

Definition 3.2 (q-expansion and Fourier coefficients). Consider a meromorphic function f on $\mathbb{H}$ invariant with respect to the operation of T and the induced meromorphic function $\hat{f}$ on Δ^* with

$$\hat{f}(q) := \hat{f}(e^{2\pi i\tau}) := f(\tau).$$

1. The function f is named *meromorphic at* ∞
   - if $\hat{f}$ has an isolated singularity at 0 and
   - if this singularity is a pole or a removable singularity.
2. If f is meromorphic at ∞ then the induced function $\hat{f}$ has a Laurent expansion around 0
   $$\hat{f}(q) = \sum_{n=n_0}^{\infty} a_n \cdot q^n,\ q = e^{2\pi i\tau},$$
   with a suitable $n_0 \in \mathbb{Z}$. The Laurent expansion is named the *q-expansion* of f, and the elements $(a_n)_{n\geq n_0}$ are the *Fourier coefficients* of f.
3. A function f, meromorphic at ∞, is named *holomorphic at* ∞ if $n_0 \in \mathbb{N}$, i.e. if $0 \in \Delta$ is a removable singularity of $\hat{f}$. In this case one defines
   $$f(\infty) := \hat{f}(0).$$

Note: For a meromorphic function f on $\mathbb{H}$, invariant with respect to T:

$$f \text{ holomorphic at } \infty \iff \lim_{Im\ \tau\to\infty} |f(\tau)| < \infty \iff$$
$$\iff \exists\, R > 0 : |f(\tau)| \text{ bounded for } Im\ \tau \geq R.$$

Modular forms will not be necessarily invariant under the operation of $\Gamma_0(N)$, but they multiply with a factor of automorphy which is a holomorphic function without zeros. We define the concept in a slightly more general context.

Definition 3.3 (Factor of automorphy). Consider the left group action

$$\Phi : GL(2,\mathbb{R})^+ \times \mathbb{H} \to \mathbb{H},\ (\gamma,\tau) \mapsto \gamma(\tau) := \frac{a\tau+b}{c\tau+d},\ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

which extends the group action of the modular group Γ to $GL(2,\mathbb{R})^+$. The map

$$h : GL(2,\mathbb{R})^+ \times \mathbb{H} \to \mathbb{H},\ h(\gamma,\tau) := c\tau + d,$$

is named the *factor of automorphy* of Φ.

The translation $T \in SL(2,\mathbb{Z})$ has the factor of automorphy $h(T,-) = 1$.

Lemma 3.4 (Transformation of the factors of automorphy).

1. *The factors of automorphy satisfy the composition rule*

$$h(B\cdot A,\tau)=h(B,\,A(\tau))\cdot h(A,\tau);\; A,B\in GL(2,\mathbb{R})^{+},\;\tau\in\mathbb{H}.$$

2. *Consider the vector space*

$$V:=\{f:\mathbb{H}\to\mathbb{C}\}$$

of complex-valued functions on $\mathbb{H}$*. For any* $k\in\mathbb{Z}$ *the map*

$$V\times GL(2,\mathbb{R})^{+}\to V,\;(f,\gamma)\mapsto f[\gamma]_k,$$

with

$$f[\gamma]_k(\tau):=f(\gamma(\tau))\cdot h(\gamma,\tau)^{-k}\cdot(det\;\gamma)^{k-1},\;\tau\in\mathbb{H},$$

is a right group action of $GL(2,\mathbb{R})^{+}$ *on the vector space* V*.*

In the definition of $f[\gamma]_k$ from Lemma 3.4 the exponent of $det\;\gamma$ is not uniform in the literature. We use the exponent $(k-1)$ from [17, Exerc. 1.2.11], while [35, Chap. III, §3] uses the exponent $k/2$. The choice of the exponent $(k-1)$ will later simplify Definition 5.10.

Note that in Lemma 3.4 the group $GL(2,\mathbb{R})^{+}$ is written on the right-hand side of the vector space V.

Proof. Consider $A,B\in GL(2,\mathbb{R})^{+}$ and $\tau\in\mathbb{H}$.

1.
$$A\cdot\begin{pmatrix}\tau\\1\end{pmatrix}=\begin{pmatrix}A(\tau)\\1\end{pmatrix}\cdot h(A,\tau).$$

Here we distinguish between the matrix product of A with a vector on the left-hand side and the fractional linear transformation $A(\tau)$ on the right-hand side.

Applying this identity to the product $B\cdot A$

$$(B\cdot A)\cdot\begin{pmatrix}\tau\\1\end{pmatrix}=\begin{pmatrix}(B\cdot A)(\tau)\\1\end{pmatrix}\cdot h(B\cdot A,\tau).$$

Left-hand side:

$$B\cdot\left(A\cdot\begin{pmatrix}\tau\\1\end{pmatrix}\right)=B\cdot\left(\begin{pmatrix}A(\tau)\\1\end{pmatrix}\cdot h(A,\tau)\right)=\begin{pmatrix}B(A(\tau))\\1\end{pmatrix}\cdot h(B,A(\tau))\cdot h(A,\tau).$$

Equating with the right-hand side gives for the lower row

$$h(B\cdot A,\tau)=h(B,A(\tau))\cdot h(A,\tau),$$

hence for the upper row

$$(B\cdot A)(\tau)=B(A(\tau)).$$

2. Starting with the right-hand side we compute

$$((f[B]_k)[A]_k)(\tau)=(f[B]_k)(A(\tau))\cdot h(A,\tau)^{-k}(det\ A)^{k-1}=$$

$$=f(B(A(\tau)))\cdot h(B,A(\tau))^{-k}\cdot h(A,\tau)^{-k}\cdot(det\ B)^{k-1}\cdot(det\ A)^{k-1}=$$

$$=f((B\cdot A)(\tau))\cdot h(B\cdot A,\tau)^{-k}\cdot(det\ (B\cdot A))^{k-1}=f[B\cdot A]_k(\tau).$$

Here the penultimate equality holds due the result from part 1) and due to the equality

$$(B\cdot A)(\tau)=B(A(\tau))$$

from the proof of part i). Hence

$$f[B\cdot A]_k=(f[B]_k)[A]_k,\ q.e.d.$$

Remark 3.5 (Meromorphy and holomorphy at the cusps). The Fourier expansion from Definition 3.2 is well-defined for holomorphic functions $f:\mathbb{H}\to\mathbb{C}$ wich are invariant with respect to the translation T. The modular group Γ has only a single cusp, the orbit comprising ∞ and all rationals $q\in\mathbb{Q}$. But Hecke congruence subgroups $\Gamma_0(N),\ N\geq 2$, have several cusps, each comprising a different subset of rationals $q\in\mathbb{N}$.

Fix a Hecke congruence subgroup $\Gamma_0(N)$, a weight $k\in\mathbb{Z}$, and a rational $q=\dfrac{a}{c}\in\mathbb{Q}$. How to extend a holomorphic function

$$f:\mathbb{H}\to\mathbb{C}$$

with

$$f[\gamma]_k=f$$

for all $\gamma\in\Gamma_0(N)$ to the point $q\in\mathbb{Q}$ in a meromorphic or holomorphic way?

We consider the canonical surjective group homomorphism

$$\Gamma\to PSL(2,\mathbb{Z}):=\Gamma/\{\pm\mathbb{1}\},\ \alpha\mapsto\overline{\alpha}.$$

The image $\overline{\Gamma}_\infty\subset PSL(2,\mathbb{Z})$ of the isotropy group $\Gamma_\infty\subset\Gamma$ is generated by the translation:

$$\overline{\Gamma}_\infty=<T>=\{T^k:\ k\in\mathbb{Z}\}\simeq\mathbb{Z}$$

If $\alpha\in\Gamma$ with

$$q=\alpha(\infty)$$

then

$$\Gamma_0(N)_q \simeq \alpha^{-1} \cdot \Gamma_0(N)_q \cdot \alpha \subset \Gamma_\infty$$

or

$$\overline{\Gamma_0(N)}_q \simeq \overline{\alpha}^{-1} \cdot \overline{\Gamma_0(N)}_q \cdot \overline{\alpha} \subset \overline{\Gamma}_\infty \simeq \mathbb{Z}$$

For

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ define } \gamma := \alpha \cdot T^N \cdot \alpha^{-1} = \begin{pmatrix} * & * \\ -Nc^2 & * \end{pmatrix} \in \Gamma_0(N)_q$$

Then $\overline{\gamma} \in \overline{\Gamma_0(N)}_q$. Because $< T^N > \subset \Gamma_\infty$ is a subgroup of finite index, the same holds for

$$< \gamma > \subset \Gamma_q \text{ and for } < \overline{\gamma} > \subset \overline{\Gamma}_q$$

We obtain

$$1 \leq h_q := [\Gamma_q : \Gamma_0(N)_q] = [\overline{\Gamma}_q : \overline{\Gamma_0(N)}_q] < \infty$$

Lemma 3.4 shows

$$(f[\alpha]_k)[T^{h_q}]_k = f[\alpha \cdot T^{h_q}]_k = f[\gamma \cdot \alpha]_k = (f[\gamma]_k)[\alpha]_k = f[\alpha]_k$$

Hence $f[\alpha]_k$ is invariant under T^{h_q} and has a Fourier series

$$(f[\alpha]_k)(\tau) = \sum_{n=-\infty}^{\infty} a_n \cdot \hat{q}^n, \ \hat{q} := e^{2\pi i \cdot \tau / h_q}$$

The function $f[\alpha]_k$ is named *meromorphic* respectively *holomorphic* at ∞ iff $f[\alpha]_k$ has at $\hat{q} = 0$ at most a pole respectively a removable singularity. Note that the order of $f[\alpha]_k$ at $\hat{q} = 0$ does not depend on the choice of α.

The fundamental object of the whole theory is the *modular form*. We introduce modular forms of the modular group Γ respectively its Hecke congruence subgroups $\Gamma_0(N)$ as the coefficient functions of the invariant differential forms from Proposition 3.1 which extend to $\infty \in \mathbb{H}^*$. It turns out that modular forms are meromorphic differential forms on the modular curve $X_0(N)$, see Theorem 3.17.

Definition 3.6 (Modular forms and automorphic forms).

1. *Modular forms and automorphic forms of the modular group*: Consider an integer $k \in \mathbb{Z}$ and a meromorphic function f on $\mathbb{H}$.

   - The function f is *weakly modular of weight k* with respect to Γ if for all $\gamma \in \Gamma$ and for all $\tau \in \mathbb{H}$

$$f(\gamma(\tau)) \cdot \frac{1}{(c\tau + d)^k} = f(\tau), \ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

- The function f is an *automorphic form of weight k* with respect to Γ if f is weakly modular of weight k and meromorphic at ∞.

- The function f is a *modular form of weight k* with respect to Γ if f is weakly modular of weight k, holomorphic on $\mathbb{H}$ and holomorphic at ∞.

- A modular form f of weight k vanishing at all points of the cusp of Γ, i.e.

$$f(\infty) = 0$$

  is a *cusp form of weight k* with respect to Γ.

- An *automorphic function* with respect to Γ is an automorphic form of weight $= 0$, i.e. satisfying

$$f \circ \gamma = f.$$

  Similarly, a *modular function* is a modular form of weight $= 0$.

- On denotes by

$$A_k(\Gamma) \supset M_k(\Gamma) \supset S_k(\Gamma)$$

  the vector spaces of automorphic forms with respect to Γ of weight k, the subspace of modular forms, and the subspace of cusp forms.

2. *Modular forms of congruence subgroups*: Consider a congruence subgroup $\Gamma_0(N)$ with a positive integer $N \in \mathbb{N}^*$.

   - A *modular form* of weight $k \in \mathbb{Z},\ k \in \mathbb{Z}$, with respect to $\Gamma_0(N)$ is a holomorphic function

$$f : \mathbb{H} \to \mathbb{C}$$

     with the following properties: For all $\gamma \in \Gamma_0(N)$ holds

$$f[\gamma]_k = f,$$

     and for all $\alpha \in \Gamma$ the function $f[\alpha]_k$ is holomorphic at ∞ in the sense of Remark 3.5.

   - A modular form f of weight $k \in \mathbb{Z},\ k \in \mathbb{Z}$, with respect to $\Gamma_0(N)$ is named a *cusp form* of weight $k \in \mathbb{Z}$ with respect to $\Gamma_0(N)$ if for all $\alpha \in \Gamma$ the function $f[\alpha]_k$ is holomorphic at ∞, and its Fourier series in the sense of Remark 3.5 vanishes at $\hat{q} = 0$.

3. *Automorphic forms of congruence subgroups*: An automorphic form of weight $k,\ k \in \mathbb{Z}$, with respect to $\Gamma_0(N)$ is a meromorphic function on $\mathbb{H}$ with the following properties: For all $\gamma \in \Gamma_0(N)$ holds

$$f[\gamma]_k = f,$$

and for all $\alpha \in \Gamma$ the function $f[\alpha]_k$ is meromorphic at ∞ in the sense of Remark 3.5.

We denote by

$$A_k(\Gamma_0(N)) \supset M_k(\Gamma_0(N)) \supset S_k(\Gamma_0(N))$$

the complex vector space of respectively automorphic forms, modular forms, and cusp forms of weight k with respect to $\Gamma_0(N)$.

Definition 3.6, part 2) and 3) generalize part 1): For $\gamma \in \Gamma$ holds $det\ \gamma = 1$, hence

$$f[\gamma]_k(\tau) = (f \circ \gamma)(\tau) \cdot \frac{1}{(c\tau + d)^k}$$

Note that Definition 3.6 uses the weight convention from [17, Chap. 1.1]. Some sources use a different weight convention. In the literature also the notation to discriminate between modular *functions* and modular *forms* is not uniform.

As a consequence of Theorem 2.16 and Lemma 3.4 it is sufficient to require in Definition 3.6, part 1) the transformation law only for the two generators S, T of Γ.

Remark 3.7 (Modular forms of odd weight). A modular form of a congruence subgroup $\Gamma_0(N)$, $N \in \mathbb{N}$, of odd weight $k \in \mathbb{Z}$ satisfies for all $\tau \in \mathbb{H}$ and for the particular element

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

the equation

$$f(\tau) = f[\gamma]_k(\tau) = f(\gamma(\tau)) \cdot (-1)^k = f(\tau) \cdot (-1)^k.$$

Therefore $f = 0$ is the only modular function of $\Gamma_0(N)$ of odd weight.

3.2 Eisenstein series and the algebra of modular forms of Γ

We will now construct for the modular group $\Gamma = SL(2, \mathbb{Z})$ explicit modular forms G_k of even weight $k \geq 4$ and a distinguished holomorphic function G_2, which behaves in a different way under the Γ-action. To achieve the construction we need the convergence of certain infinite series. Lemma 3.8 provides the necessary prerequisites.

The whole section will use the unbranched covering projection

$$q : \mathbb{H} \to \Delta^*,\ \tau \mapsto q(\tau) := e^{2\pi i \cdot \tau},$$

to study the number theoretic properties of modular forms f by considering the Fourier coefficients of their Fourier expansion

$$\hat{f}(q) = \sum_{n=0}^{\infty} a_n \cdot q^n$$

Lemma 3.8 (Fourier series and partial fraction). *Assume $k \in \mathbb{N}$. Consider $\tau \in \mathbb{C}$ and set*

$$q := e^{2\pi i \cdot \tau}.$$

1. *For $k \geq 2$ and $Im\ \tau \neq 0$*

$$\sum_{n \in \mathbb{Z}} \frac{1}{(\tau + n)^k} = \frac{(-2\pi i)^k}{(k-1)!} \cdot \begin{cases} \sum\limits_{r=1}^{\infty} r^{k-1} \cdot q^r & Im\ \tau > 0 \\ (-1)^k \cdot \sum\limits_{r=1}^{\infty} r^{k-1} \cdot q^{-r} & Im\ \tau < 0 \end{cases}$$

2. *The double series*

$$\sum_{m,d=1}^{\infty} d \cdot q^{md}$$

satisfies the prerequisites of the rearrangement theorem, i.e. there exists a constant K such that for all finite subsets $A,\ B \subset \mathbb{N}^*$ holds

$$\sum_{m \in A, d \in B} d \cdot |q|^{md} \leq K$$

3. *For even $k \geq 2$, $Im\ \tau > 0$,*

$$\sum_{m \in \mathbb{Z}^*} \left(\sum_{n \in \mathbb{Z}} \frac{1}{(m\tau + n)^k} \right) = \frac{2\,(2\pi i)^k}{(k-1)!} \cdot \sum_{n=1}^{\infty} \sigma_{k-1}(n)\ q^n$$

is absolutely convergent.

Here for each $k \geq 2$ the arithmetic function

$$\sigma_{k-1} : \mathbb{N}^* \to \mathbb{N}^*,\ \sigma_{k-1}(n) := \sum_{d|n} d^{k-1},$$

adds the $(k-1)$-powers of the positive integer divisors of n.

Proof. 1. i) We first consider the case $Im\ \tau > 0$. The proof compares the partial fraction and the Fourier expansion of the cotangent function.

- Partial fraction, see [62]:

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

- Fourier series

$$\pi \cdot \cot(\pi\tau) = \pi \, \frac{\cos(\pi\tau)}{\sin(\pi\tau)} = (-i\pi) \cdot \frac{1+q}{1-q} = -\pi i - 2\pi i \sum_{m=1}^{\infty} q^m.$$

Here the second equality results from the Euler formulas

$$cos\ \pi\tau = \frac{1}{2}(e^{i\pi\tau} + e^{-i\pi\tau}) \text{ and } sin\ \pi\tau = \frac{1}{2i}(e^{i\pi\tau} - e^{-i\pi\tau})$$

which imply

$$\cot(\pi\tau) = i \cdot \frac{e^{i\pi\tau} + e^{-i\pi\tau}}{e^{i\pi\tau} - e^{-i\pi\tau}} = i \cdot \frac{q+1}{q-1} = (-i) \cdot \frac{1+q}{1-q}$$

The third equality uses the geometric series

$$\frac{1+q}{1-q} = (1+q) \sum_{m=0}^{\infty} q^m = 1 + 2 \sum_{m=1}^{\infty} q^m$$

which is absolutely convergent because $|q| < 1$ due to $\tau \in \mathbb{H}$.

Equating both expansions gives

$$\frac{1}{\tau} + \sum_{m=1}^{\infty} \left(\frac{1}{\tau+m} + \frac{1}{\tau-m} \right) = -\pi i - 2\pi i \sum_{m=1}^{\infty} q^m,$$

and successive $(k-1)$-times differentiation with respect to τ shows

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

ii) For $Im\ \tau < 0$ we use

$$(\tau+n)^k = (-1)^k \cdot (-\tau-n)^k$$

Hence

$$\sum_{n \in \mathbb{Z}} \frac{1}{(\tau+n)^k} = (-1)^k \cdot \sum_{n \in \mathbb{Z}} \frac{1}{(-\tau-n)^k} = (-1)^k \cdot \sum_{n \in \mathbb{Z}} \frac{1}{(-\tau+n)^k}$$

Part i) applied to $-\tau$ implies

$$(-1)^k \cdot \sum_{n\in\mathbb{Z}} \frac{1}{(-\tau+n)^k} = \frac{(-2\pi i)^k}{(k-1)!} \cdot (-1)^k \cdot \sum_{r=1} r^{k-1} \cdot q^{-r}$$

which proves the claim.

2. Consider $\tau \in \mathbb{H}$ with $q := e^{2\pi i\tau}$ real and $0 < q < 1$.

   For any real $x \in [0,1[$ the geometric series satisfies

   $$\sum_{d=0}^{\infty} x^d = \frac{1}{1-x}$$

   Taking the derivative and multiplying by x shows

   $$\sum_{d=1}^{\infty} d \cdot x^d = \frac{x}{(1-x)^2}$$

   For arbitrary but fixed $m \geq 1$ set $x := q^m < 1$

   $$\sum_{m=1}^{\infty} \left(\sum_{d=1}^{\infty} d \cdot q^{md} \right) = \sum_{m=1}^{\infty} \left(\sum_{d=1}^{\infty} d \cdot (q^m)^d \right) = \sum_{m=1}^{\infty} \frac{q^m}{(1-q^m)^2}$$

   The last series is convergent because for fixed q

   $$\lim_{m\to\infty} |1-q^m|^2 = 1.$$

   Set

   $$K := \sum_{m=1}^{\infty} \frac{q^m}{(1-q^m)^2}$$

   As a consequence

   $$\sum_{m\in A, d\in B} d \cdot q^{md} \leq K.$$

   For arbitrary $\tau \in \mathbb{H}$ we have

   $$q := e^{2\pi i\tau} \text{ with } 0 \leq |q| < 1$$

   Hence w.l.o.g. we may assume q real with $0 \leq q < 1$, which proves the claim.

3. We split the exterior summation $\sum_{m\in\mathbb{Z}^*}$ into

   $$\sum_{m<0} \text{ where } Im(m\tau) < 0 \text{ and } \sum_{m>0} \text{ where } Im(m\tau) > 0.$$

   Due to part 1) for each $m \in \mathbb{Z}^*$ exists the interior series

$$\sum_{n\in\mathbb{Z}} \frac{1}{(m\tau+n)^k} = \frac{(2\pi i)^k}{(k-1)!} \cdot \begin{cases} \sum_{r=1}^{\infty} r^{k-1} \cdot q^{-rm} & \text{if } m<0 \\ \sum_{r=1}^{\infty} r^{k-1} \cdot q^{rm} & \text{if } m>0 \end{cases}$$

Hence for even $k \geq 2$

$$\sum_{m\in\mathbb{Z}^*} \left(\sum_{n\in\mathbb{Z}} \frac{1}{(m\tau+n)^k} \right) = 2 \cdot \frac{(2\pi i)^k}{(k-1)!} \cdot \sum_{m=1}^{\infty} \left(\sum_{r=1}^{\infty} r^{k-1} \cdot q^{rm} \right).$$

The latter series is convergent: For $k \geq 4$ any rearrangement of the original double series is permitted. For $k=2$ the result of part 2) allows to apply the rearrangement theorem to the double series

$$\sum_{m,r=1}^{\infty} r \cdot q^{rm},\ |q|<1.$$

We rearrange the series by changing the indices of summation from (m,r) to $(n=rm, d|n)$:

$$\sum_{m=1}^{\infty} \left(\sum_{r=1}^{\infty} r^{k-1} \cdot q^{rm} \right) = \sum_{n=1}^{\infty} \left(\sum_{d|n} d^{k-1} \cdot q^n \right) = \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n.$$

Eventually for all even $k \geq 2$

$$\sum_{m\in\mathbb{Z}^*} \left(\sum_{n\in\mathbb{Z}} \frac{1}{(m\tau+n)^k} \right) = 2 \cdot \frac{(2\pi i)^k}{(k-1)!} \cdot \sum_{n=1}^{k} \sigma_{k-1}(n) \cdot q^n,\ q.e.d.$$

Eisenstein series are the lattice constants of normalized lattices

$$\Lambda_{1,\tau} = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau$$

when considered as functions of the argument $\tau \in \mathbb{H}$. Eisenstein series are explicit representations of modular forms.

Theorem 3.9 (Eisenstein series, $k \geq 4$). *Consider an even integer $k \geq 4$.*

1. *The* Eisenstein series

$$G_k(\tau) := {\sum_{(c,d)\in\mathbb{Z}^2}}' \frac{1}{(c\tau+d)^k}$$

is absolutely and compactly convergent for $\tau \in \mathbb{H}$.

The series defines a modular form G_k of Γ of weight k with

$$G_k(\infty) = 2\zeta(k).$$

Here

$$\zeta(s) := \sum_{n=1}^{\infty} (1/n^s),\ Re\ s > 1,$$

denotes the Riemann ζ-function.

2. The Eisenstein series $G_k \in M_k(\Gamma)$ has the Fourier expansion

$$G_k(\tau) = 2\zeta(k) + 2\,\frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n,\ q = e^{2\pi i \tau}.$$

Proof. i) *Convergence and transformation*: For $\tau \in \mathbb{H}$ consider the normalized lattice

$$\Lambda_\tau := \mathbb{Z} + \mathbb{Z}\tau$$

and for $k \geq 4$ its lattice constants $G_{\Lambda_\tau,k}$. Apparently

$$G_k(\tau) := G_{\Lambda_\tau,k}$$

The series $G_{\Lambda,k}$ is absolute convergent due to Lemma 1.11, hence allows arbitrary rearrangement. With respect to the translation

$$T : \mathbb{H} \to \mathbb{H},\ \tau \mapsto T(\tau) := \tau + 1,$$

we obtain

$$G_k(\tau) = G_k(\tau + 1).$$

With respect to the reflection

$$S : \mathbb{H} \to \mathbb{H},\ \tau \mapsto S(\tau) := \frac{-1}{\tau}$$

we have

$$G_k(S(\tau)) \cdot h(S,\tau)^{-k} = \frac{1}{\tau^k} \cdot G_k(-(1/\tau)) = \frac{1}{\tau^k} \cdot {\sum_{(c,d)\in\mathbb{Z}^2}}' \frac{1}{(-c(1/\tau)+d)^k} = G_k(\tau).$$

Because S and T generate the modular group, Lemma 3.4 implies for all $\gamma \in \Gamma$ and for all $\tau \in \mathbb{H}$

$$G_k(\tau) = G_k(\gamma(\tau)) \cdot h(\gamma,\tau)^{-k},\ \text{i.e. } G_k = G_k[\gamma]_k$$

ii) *Fourier expansion and holomorphy*: We split the summation over

$$(c,d) \in \mathbb{Z}^2, (c,d) \neq (0,0),$$

into the simple sum for (c,d) with $c = 0$ and $d \in \mathbb{Z}^*$ and the double sum with $c \in \mathbb{Z}^*$ and $d \in \mathbb{Z}$. Then Lemma 3.8, part 3) implies

$$G_k(\tau) = \sum_{(c,d)\in\mathbb{Z}^2}{}' \frac{1}{(c\tau+d)^k} = \sum_{d\in\mathbb{Z}^*} \frac{1}{d^k} + \sum_{c\in\mathbb{Z}^*, d\in\mathbb{Z}} \frac{1}{(c\tau+d)^k} =$$

$$= 2\zeta(k) + \frac{2\,(2\pi i)^k}{(k-1)!} \cdot \sum_{n=1}^{\infty} \sigma_{k-1}(n)\, q^n,\ q = e^{2\pi i\cdot\tau}.$$

The Fourier expansion, a convergent power series, proves the holomorphy of G_k in $\mathbb{H}$ and at the point ∞, q.e.d.

In order to get rid of the transcendent values in the Fourier expansion of G_k one divides by the value of the Riemann ζ-function.

Definition 3.10 (Normalized Eisenstein series). For even $k \geq 4$ one defines the *normalized Eisenstein series*

$$E_k := \frac{G_k}{2\zeta(k)} \in M_k(\Gamma)$$

Corollary 3.11 (Normalized Eisenstein series). *For each $k \geq 4$ all Fourier coefficients of the normalized Eisenstein series are rational, more precisely*

$$E_k(\tau) = 1 - \frac{2k}{B_k} \cdot \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n \in M_k(\Gamma),\ q = e^{2\pi i\cdot\tau}$$

Proof. 1. *Euler relation of Bernoulli numbers*: See [20, Kap. VII, Satz 4.1]. We relate the cotangent function to the Bernoulli numbers $(B_n)_{n\in\mathbb{N}}$. The Bernoulli numbers are the generators of the power series

$$\frac{z}{e^z - 1} =: \sum_{n=0}^{\infty} \frac{B_n}{n!} \cdot z^n.$$

We compute

$$\cot\, z = \frac{cos\, z}{sin\, z} = i \cdot \frac{e^{iz} + e^{-iz}}{e^{iz} - e^{-iz}} = i \cdot \frac{e^{2iz} + 1}{e^{2iz} - 1} = i + \frac{2i}{e^{2iz} - 1}$$

and use the vanishing of Bernoulli numbers with odd index ≥ 3 and $B_0 = 1,\ B_1 = -1/2$

$$z \cdot cotz = iz + \frac{2iz}{e^{2iz} - 1} = iz + 1 - \frac{2iz}{2} + \sum_{\mu=1}^{\infty} \frac{B_{2\mu}}{(2\mu)!} \cdot (2iz)^{2\mu} = 1 + \sum_{\mu=1}^{\infty} (-1)^{\mu} \frac{2^{2\mu}}{(2\mu)!} \cdot B_{2\mu} \cdot z^{2\mu}$$

- On one hand from the definition of the Bernoulli numbers - replacing z by πz -

$$\pi z \cdot cot(\pi z) = 1 + \sum_{\mu=1}^{\infty} (-1)^{\mu} \cdot \frac{2^{2\mu}}{(2\mu)!} \cdot \pi^{2\mu} \cdot B_{2\mu} \cdot z^{2\mu}$$

- On the other hand the partial fraction of the cotangent function

$$\pi z \cdot cot(\pi z) = 1 + z \sum_{\nu=1}^{\infty} \frac{2z}{z^2 - \nu^2}$$

and the geometric series

$$\frac{1}{z^2 - \nu^2} = -\frac{1}{\nu^2} \cdot \sum_{\mu=0}^{\infty} \left(\frac{z^2}{\nu^2} \right)^{\mu}$$

imply

$$\pi z \cdot cot(\pi z) = 1 + 2z^2 \cdot \sum_{\nu=1}^{\infty} \left(-\frac{1}{\nu^2} \cdot \sum_{\mu=0}^{\infty} \left(\frac{z^2}{\nu^2} \right)^{\mu} \right) =$$

$$= 1 - 2 \sum_{\mu=1}^{\infty} \left(\sum_{\nu=1}^{\infty} \frac{1}{\nu^{2\mu}} \right) z^{2\mu}$$

Comparing the coefficients of both series representing

$$\pi z \cdot cot(\pi z)$$

implies the Euler relation

$$2 \cdot \zeta(2\mu) := 2 \cdot \sum_{\nu=1}^{\infty} \frac{1}{\nu^{2\mu}} = (-1)^{\mu+1} \frac{2^{2\mu}}{(2\mu)!} \cdot \pi^{2\mu} \cdot B_{2\mu}$$

2. *Rationality of the Fourier coefficients*: The Fourier expansion of the Eisenstein series G_k from Theorem 3.9 and Part 1) show

$$E_k(\tau) := \frac{G_k(\tau)}{2\zeta(k)} = 1 - \frac{2k}{B_k} \cdot \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n \in M_k(\Gamma).$$

All Bernoulli numbers are rational due to the recursion formula for $N \in \mathbb{N}^*$

$$\sum_{n=0}^{N} \binom{N+1}{n} \cdot B_n = 0 \text{ with } B_0 = 1.$$

As a consequence, all Fourier coefficients of E_k are rational, q.e.d.

Concerning the first values of Bernoulli numbers

$$\left(k, \zeta(k), B_k, -\frac{2k}{B_k} \right)$$

one has

$$(2, \pi^2/6, 1/6, -24)$$
$$(4, \pi^4/(2\cdot 3^2\cdot 5), -1/30, 240)$$
$$(6, \pi^6/(3^3\cdot 5\cdot 7), 1/42, -504)$$
$$(8, \pi^8/(2\cdot 3^3\cdot 5^2\cdot 7), -1/30, 480)$$
$$(10, \pi^{10}/(3^5\cdot 5\cdot 7\cdot 11), 5/66, -264)$$
$$(12,\ 691\cdot \pi^{12}/(3^6\cdot 5^3\cdot 7^2\cdot 11\cdot 13), -691/2730, 65520/691)$$

For $k \in \{4,6,8\}$ the numerical value of B_k implies that all Fourier coefficients of E_k are not only rational but are integers.

Remark 3.12 (Eisenstein series).

1. *Rationality of the Fourier coefficients*: The result from Corollary 3.11 is remarkable: The invariance of the holomorphic function E_k under the right action of the modular group implies the rationality of the Fourier coefficients of E_k. The Fourier coefficients of these holomorphic functions are not arbitrary numbers from $\mathbb{C}$ but rationals from $\mathbb{Q}$. This rationality is the reason for the "magic of modular forms" revealed by later applications. See also Proposition 3.14.

2. *Weight* $k \geq 4$: For even $k > 2$ the Eisenstein series G_k relate to the lattice constants $G_{\Lambda,k}$ of an arbitrary lattice with positively oriented basis

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

as follows: Set $\tau := \omega_2/\omega_1 \in \mathbb{H}$. Then

$$G_{\Lambda,k} = \frac{1}{\omega_1^{\,k}}\, G_k(\tau).$$

3. *Weight* $k = 2$: Similar to the series

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}$$

in one dimension, in two dimensions the series

$$\sum_{(m,n)\in\mathbb{Z}^2}{}' \frac{1}{(m\tau+n)^2}$$

is not absolutely convergent. Anyhow, in both cases some specific orders of summation provide certain finite values. In the 2-dimensional case we define the Eisenstein series

$$G_2(\tau) := 2 \cdot \sum_{n=1}^{\infty} \frac{1}{n^2} + \sum_{m \in \mathbb{Z}^*} \left(\sum_{n \in \mathbb{Z}} \frac{1}{(m\tau + n)^2} \right), \ \tau \in \mathbb{H}.$$

Lemma 3.8, part 3) implies that the sum on the right-hand side is convergent with Fourier series

$$G_2(\tau) = 2 \cdot \zeta(2) - 8\pi^2 \cdot \sum_{n=1}^{\infty} \sigma_1(n) \cdot q^n, \ q = e^{2\pi i \cdot \tau}.$$

The equality

$$\zeta(2) = \pi^2/6$$

implies for the normalized Eisenstein series of weight $k = 2$

$$E_2(\tau) := \frac{G_2(\tau)}{2\zeta(2)} = 1 - 24 \cdot \sum_{n=1}^{\infty} \sigma_1(n) \cdot q^n, \ q = e^{2\pi i \cdot \tau}.$$

The convergent Fourier representation shows: G_2 is holomorphic on $\mathbb{H} \cup \{\infty\}$ due to Lemma 3.8, part 3), and invariant with respect to translation.

4. *Transformation of G_2*: With respect to the reflection $S \in \Gamma$ the Eisenstein series G_2 transforms as

$$(G_2[S]_2)(\tau) := G_2(S\tau) \cdot \frac{1}{\tau^2} = G_2(\tau) - \frac{2\pi i}{\tau}$$

or

$$(G_2[\gamma]_2)(\tau) = G_2(\tau) - 2\pi i c \cdot h(\gamma, \tau)^{-1}$$

for general

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

see [36, Kap. III, § 6, Abschn. 1] or [17, Exerc. 1.2.8]. In particular, G_2 is not weakly modular. The lack of modularity is due to the conditional convergence of G_2.

Proposition 1.19 dealt with the discriminant of the cubic polynomial from the differential equation of the Weierstrass function $\wp$ of a lattice. Definition 3.13 shows: These discriminants are the values of a modular form.

Definition 3.13 (Discriminant form). The *discriminant form* is the modular form of Γ of weight $k = 12$ defined as

$$\Delta := g_2^3 - 27 \cdot g_3^2 : \mathbb{H} \to \mathbb{C}$$

derived from the Eisenstein series

$$g_2 := 60 \cdot G_4,\ g_3 := 140 \cdot G_6.$$

In Definition 3.13 the letters g_2 and g_3 designate modular functions, not the constants from Theorem 1.17, which denote the value at the period τ of a given normalized lattice

$$\Lambda = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau.$$

Proposition 3.14 (Fourier coefficients of the dicriminant form). *All Fourier coefficients of the* normalized discriminant form

$$\frac{\Delta}{(2\pi)^{12}} \in M_{12}(\Gamma)$$

are integers:

$$\frac{\Delta(q)}{(2\pi)^{12}} = \sum_{n=0}^{\infty} \tau_n \cdot q^n \in \mathbb{Z}\{q\},\ q = e^{2\pi i \cdot \tau},$$

with $\tau_0 = 0$ *and* $\tau_1 = 1$.

In particular $\Delta \in S_{12}(\Gamma)$ *is a cusp form of weight* 12*, and the zero at* $\infty \in \mathbb{H}^*$ *has order* $= 1$.

The Fourier coefficients $\tau_n,\ n \geq 0$, are the subject of certain of Ramanujan's well-known conjectures, see Definition 5.31.

Proof. i) *Fourier series*: We refer to Definition 3.10 of the normalized Eisenstein series and their Fourier series expansion from Corollary 3.11

$$E_4 = 3^2 \cdot 5 \cdot \frac{G_4}{\pi^4} = 1 + 240 \cdot \sum_{n=1}^{\infty} \sigma_3(n) \cdot q^n$$

$$E_6 = \frac{3^3 \cdot 5 \cdot 7}{2} \cdot \frac{G_6}{\pi^6} = 1 - 504 \cdot \sum_{n=1}^{\infty} \sigma_5(n) \cdot q^n.$$

We have

$$g_2 = 60 \cdot G_4 = \frac{2^2}{3}\,\pi^4 \cdot E_4 \text{ and } g_3 = 140 \cdot G_6 = \frac{2^3}{3^3}\,\pi^6 \cdot E_6.$$

Hence

$$\Delta = g_2^3 - 3^3 g_3^2 = \pi^{12} \cdot \frac{2^6}{3^3}(E_4^3 - E_6^2) = (2\pi)^{12} \cdot \frac{E_4^3 - E_6^2}{2^6 \cdot 3^3} = (2\pi)^{12} \cdot \frac{E_4^3 - E_6^2}{1728}$$

and eventually

$$\frac{\Delta}{(2\pi)^{12}} = \frac{E_4^3 - E_6^2}{2^6 \cdot 3^3} = \frac{E_4^3 - E_6^2}{1728}.$$

We set as shorthand

$$X_k(q) := \sum_{n=1}^{\infty} \sigma_k(n) \cdot q^n$$

and obtain

$$\frac{\Delta}{(2\pi)^{12}} = \frac{(1 + 240 \cdot X_3)^3 - (1 - 504 \cdot X_5)^2}{2^6 \cdot 3^3}$$

When denoting by

$$Q = Q(q)$$

the numerator of the latter fraction, then

$$Q = (3 \cdot 240 \cdot X_3 + 3 \cdot 240^2 \cdot X_3^2 + 240^3 \cdot X_3^3) + (1008 \cdot X_5 - 504^2 \cdot X_5^2)$$

ii) *Fourier coefficients* $\tau_0 = 1,\ \tau_1 = 1$: In lowest order in q with

$$X_3(q) = q + O(2) \text{ and } X_5(q) = q + O(2)$$

we get

$$Q(q) = 3 \cdot 240 \cdot q + 1008 \cdot q + O(2) = 1728 \cdot q + O(2)$$

which proves $\tau_0 = 0$ and $\tau_1 = 1$.

iii) *Fourier coefficients* $\tau_n \in \mathbb{Z},\ n \geq 2$: The remaining part of the proof reduces to the claim that also all other coefficients of the series Q are divisible by

$$1728 = 2^6 \cdot 3^3 = (2^2 \cdot 3)^3 = 12^3$$

We compute

$$Q = (3 \cdot 240 \cdot X_3 + 3 \cdot 240^2 \cdot X_3^2 + 240^3 \cdot X_3^3) + (1008 \cdot X_5 - 504^2 \cdot X_5^2)$$

$$Q \equiv 3 \cdot 240 \cdot X_3 + 1008 \cdot X_5 \equiv 12^2 (5 \cdot X_3 + 7 \cdot X_5) \mod 12^3$$

To complete the proof we have to show that all coefficients of the power series

$$5 \cdot X_3 + 7 \cdot X_5$$

are divisible by 12. We show even more: For all $d \in \mathbb{Z}$

$$5 \cdot d^3 + 7 \cdot d^5 \equiv 0 \mod 12$$

According to the Chinese remainder theorem the claim reduces to the two congruences

$$5 \cdot d^3 + 7 \cdot d^5 \equiv 0 \; mod \; 3 \text{ and } 5 \cdot d^3 + 7 \cdot d^5 \equiv 0 \; mod \; 4$$

or

$$d^5 \equiv d^3 \; mod \; 3, \; mod \; 4.$$

The latter two congruences reduce to

- If $d^3 \not\equiv 0 \; mod \; 3$ then $d^2 \equiv 1 \; mod \; 3$,
- and: if $d^3 \not\equiv 0 \; mod \; 4$ then $d^2 \equiv 1 \; mod \; 4$

The congruences have to be checked for

$$d \in \{1,2\} \subset \mathbb{Z}/3\mathbb{Z} = \{0,1,2\} \text{ and } d \in \{1,3\} \subset \mathbb{Z}/4\mathbb{Z} = \{0,1,2,3\},$$

which can be easily done, q.e.d.

Definition 3.15 (Modular invariant j). The *modular invariant* j is the automorphic function, defined as the quotient of two modular forms of weight $= 12$,

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

Corollary 3.16 (Modular curve and modular invariant j). *The modular invariant is a biholomorphic map*

$$j : X(1) \xrightarrow{\simeq} \mathbb{P}^1$$

which maps the cusp of $X(1)$ *to* $\infty \in \mathbb{P}^1$.

Proof. Proposition 1.19 implies that j is a holomorphic function on $\mathbb{H}$ because the denominator Δ has no zeros in $\mathbb{H}$. The Fourier expansion of

$$\frac{\Delta}{(2\pi)^{12}}$$

from Proposition 3.14 and the equality

$$G_4(\infty) = 2\zeta(4) \neq 0$$

from Theorem 3.9 show that j has a pole of order $= 1$ at the point ∞. Because j is even an automorphic *function*, it is a meromorphic function on the modular curve, i.e. a holomorphic map

$$j : X(1) \xrightarrow{\simeq} \mathbb{P}^1.$$

Because all fibres of j have the same multiplicity $= 1$, the map j is biholomorphic, q.e.d.

Continuing with the investigation started in Proposition 3.1 we now set out to show: Modular forms of weight k are those meromorphic differential forms on the modular curves $X_0(N)$ which are multiples of a certain divisor which depends on the level N and the weight k. Hence modular forms are the holomorphic sections of certain line bundles on the modular curves. Applying the Riemann-Roch theorem we draw several conclusions. In detail:

- We recall the Riemann-Roch theorem on a compact Riemann surface X with genus $g(X)$ for a divisor $D \in Div(X)$, and also Serre duality, see [63]:

$$dim\ H^0(X,\mathscr{O}_D) - dim\ H^1(X,\mathscr{O}_D) = 1 - g(X) + deg\ D.$$

  We will use also the notation

$$deg\ \mathscr{O}_D := deg\ D.$$

  The canonical divisor $K \in Div(X)$ has degree

$$deg\ K = 2g(X) - 2.$$

  Serre-duality allows to replace the cohomology group H^1 by the dual of a cohomology group H^0

$$H^1(X,\mathscr{O}_D) = H^0(X,\mathscr{O}_{K-D})^\vee.$$

  Moreover, for each divisor $D \in Div(X)$ with $deg\ D < 0$

$$dim\ H^0(X,\mathscr{O}_D) = 0.$$

- We derive a formula for the dimension of the vector spaces $M_k(\Gamma)$. Section 3.3 will generalize the computation to $M_k(\Gamma_0(N))$.

- Chapter 4 will show: Any complex elliptic curve arises from a complex torus. More precisely, the elliptic curve is parametrized by the two meromorphic functions $\wp_\Lambda$ and $\wp'_\Lambda$ defined on a suitable torus $\mathbb{C}/\Lambda$, see Theorem 4.28.

We recall the canonical projection to the modular curve

$$p : \mathbb{H}^* \to X := \Gamma\backslash\mathbb{H}^*,$$

skipping the $*$-superscript used in the notation from Theorem 2.28. We introduce the class notation

$$[\tau] = p(\tau) \in X.$$

In addition we use the floor function: For $x \in \mathbb{R}$

$$\lfloor x \rfloor := max\{n \in \mathbb{Z} :\ n \leq x\}.$$

Theorem 3.17 (Modular forms are meromorphic differential forms on the modular curve). *Consider an even weight $k \geq 0$.*

1. Differential forms*: The map of vector spaces is injective*

$$\alpha : M_k(\Gamma) \to H^0\left(X, \mathscr{M} \otimes_{\mathscr{O}} \Omega^{\otimes k/2}\right),\ f \mapsto \omega_f,$$

with ω_f the well-defined meromorphic differential form on X induced by the Γ-invariant modular form on $\mathbb{H}$

$$f(\tau)\ (d\tau)^{k/2}$$

2. The distinguished divisor*: Consider the divisor*

$$D_k := \left\lfloor \frac{k}{4} \right\rfloor \cdot [i] + \left\lfloor \frac{k}{3} \right\rfloor \cdot [\rho] + \frac{k}{2} \cdot [\infty] \in Div(X).$$

The attachment

$$U \mapsto \Omega_{\Gamma,k}(U),\ U \subset X\ open,$$

with

$$\Omega_{\Gamma,k}(U) := \left\{ \omega \in H^0(U, \mathscr{M} \otimes_{\mathscr{O}} \Omega^{\otimes k/2}) :\ \omega \neq 0\ and\ div\ \omega \geq -D_k|U \right\} \cup \{0\}$$

is a sheaf $\Omega_{\Gamma,k}$ on X. The sheaf $\Omega_{\Gamma,k}$

- *is a subsheaf of the sheaf of meromorphic differential forms, i.e.*

$$\Omega_{\Gamma,k} \subset \mathscr{M} \otimes_{\mathscr{O}} \Omega^{\otimes k/2}$$

- *and is isomorphic to the line bundle*

$$\mathscr{L}_{\Gamma,k} := \mathscr{O}_{(k/2)\cdot K + D_k} \in Pic(X)$$

of multiples of the divisor $-((k/2)\cdot K + D_k)\ \in Div(X))$ with $K \in Div(X)$ the canonical divisor of X.

3. Meromorphic differential forms on the modular curve*: The image of the map α from part 1) is*

$$\alpha(M_k(\Gamma)) = H^0(X, \Omega_{\Gamma,k}).$$

In particular, sections of the sheaf $\Omega_{\Gamma,k}$, i.e. certain *meromorphic* differential forms, correspond bijectively to *holomorphic* sections of the line bundle $\mathscr{L}_{\Gamma,k}$.

Proof. Cf. [50, §4]. The numbers of the different parts of the proof do not correspond one-to-one to the sections of the theorem.

i) *Definition of* α: If $f \in M_k(\Gamma)$ then Proposition 3.1 implies that the modular group leaves invariant the differential form

$$f(\tau)\ (d\tau)^{k/2}$$

on $\mathbb{H}$. Hence the latter defines a meromorphic form ω_f on X with pullback

$$f(\tau)\ (d\tau)^{k/2} := p^*\omega_f :$$

One considers first the form ω_f outside the three points which are the orbits of the two elliptic points and the cusp. Secondly one extends ω_f holomorphically into these exceptional points by using Riemann's extension theorem for bounded holomorphic functions.

ii) *Distinguished divisor*: The sheaf $\Omega_{\Gamma,k}$ is well-defined. The definition of the divisor D_k results from the following relation between the order of f at $t \in \mathbb{H}^*$ and the order of ω_f at $[t] \in X$:

$$ord_t f = \begin{cases} ord_{[\infty]}\ \omega_f + k/2 & t = \infty \\ \\ h_t \cdot ord_{[t]}\ \omega_f + (k/2)\cdot(h_t - 1) & t \in \mathbb{H} \end{cases}$$

Here h_t denotes the period of t. The order of a meromorphic differential form

$$\omega \in H^0\left(X, \mathscr{M} \otimes_{\mathscr{O}} \Omega^{\otimes k/2}\right)$$

at a point $x \in X$ is defined as follows: Choose a chart of X around x

$$q : U \to V \subset \mathbb{C}$$

and represent

$$\omega | U = f \cdot (dq)^{k/2}$$

Then

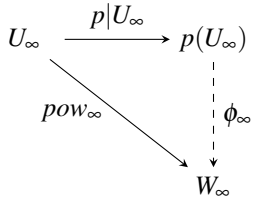
$$ord_x \omega := ord_x f,$$

independently from the choice of the chart. To prove the order relation for $t \in \{i,\ \rho,\ \infty\}$ we use the local form of

$$p : \mathbb{H}^* \to X$$

and the charts around t from Theorem 2.28 and Proposition 2.27. We denote by τ points from $U_t \subset \mathbb{H}$ and by q points from $W_t \subset \mathbb{C}$:

- For $t = \infty \in \mathbb{H}^*$ we recall the chart pow_∞ around t and the chart ϕ_∞ around the cusp $[\infty]$ from the diagram



For $\tau \in U_\infty$

$$q(\tau) := pow_\infty(\tau) := \begin{cases} e^{2\pi i\tau} & \tau \neq \infty \\ 0 & \tau = \infty \end{cases}$$

We denote by τ the points on $U_\infty \subset \mathbb{H}$ and by q the points on $W_\infty \subset \Delta \subset \mathbb{C}$. Then

$$dq = 2\pi i q \, d\tau \text{ and } (dq)^{k/2} = (2\pi i)^{k/2} q^{k/2} \, (d\tau)^{k/2}$$

which implies

$$(d\tau)^{k/2} = \frac{1}{(2\pi i)^{k/2}} \cdot \frac{(dq)^{k/2}}{q^{k/2}}$$

The order relation relates

$$ord_\infty f = ord(\hat{f};\ q = 0) = ord(p^*\omega_f;\ \tau = \infty)$$

to

$$ord_{[\infty]}\omega_f = ord((\phi_\infty^{-1})^*\omega_f;\ q = 0) = ord(h;\ q = 0)$$

with

$$h(q) \ (dq)^{k/2} := (\phi_\infty^{-1})^*\omega_f$$

The commutative diagram

$$p = \phi^{-1} \circ pow_\infty \text{ implies } p^* = pow_\infty^* \circ (\phi_\infty^{-1})^*$$

On one hand

$$p^*\omega_f = f(\tau) \ (d\tau)^{k/2}$$

On the other hand,

$$pow_\infty^* \left((\phi_\infty^{-1})^*\omega_f\right) = pow_\infty^* \left(h(q) \ (dq)^{k/2}\right) = h(q(\tau)) \cdot (2\pi i)^{k/2} \cdot q(\tau)^{k/2} \ (d\tau)^{k/2}$$

Hence

$$f(\tau) = h(q(\tau)) \cdot (2\pi i)^{k/2} \cdot q(k(\tau))^{k/2}$$

and

$$\hat{f}(q) = h(q) \cdot (2\pi i)^{k/2} \cdot q^{k/2}$$

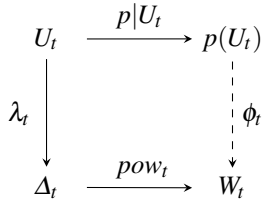
which implies

$$ord(\hat{f};\ q = 0) = ord(h;\ q = 0) + k/2$$

or

$$ord_\infty f = ord_{[\infty]}\omega_f + k/2$$

- For $t \in \{i, \rho\}$ we recall the chart ϕ_t from the following diagram



The map

$$\lambda_t : U_t \xrightarrow{\simeq} \Delta_t$$

is biholomorphic. For the order calculation we assume w.l.o.g.

$$\lambda_t = id \text{ and } U_t = \Delta_t$$

The isotropy group Γ_t acts on U_t by multiplication by an e-th root of unity with

$$e := h_t$$

For $\tau \in U_t$

$$q(\tau) := pow_t(\tau) := \tau^e$$

Therefore

$$dq = e \cdot \tau^{e-1}\, d\tau \text{ and } (dq)^{k/2} = e^{k/2} \cdot \tau^{(k/2)\cdot(e-1)}\, (d\tau)^{k/2}$$

If

$$\omega_f(q) = g(q)\, (dq)^{k/2}$$

then

$$(p^*\omega_f)(\tau) = \omega_f(q(\tau)) = g(q(\tau)) \cdot e^{k/2} \cdot \tau^{(k/2)\cdot(e-1)}\, (d\tau)^{k/2} = f(\tau)\, (d\tau)^{k/2}$$

As a consequence

$$f(\tau) = g(q(\tau)) \cdot \tau^{(k/2)\cdot(e-1)} \cdot e^{k/2}$$

By definition

$$ord_{[t]}\omega_f = ord_0 g$$

Hence

$$ord_t f = e \cdot ord_0 g + (k/2) \cdot (e-1) = e \cdot ord_{[t]}\omega_f + (k/2) \cdot (e-1) =$$

$$= h_t \cdot ord_{[t]}\omega_f + (k/2)\cdot(h_t - 1)$$

Summing up

$$ord_t f = ord_{[t]}\ \omega_f \text{ if } t \in \mathscr{D} \setminus \{i,\ \rho,\ \infty\}$$
$$ord_i f = 2 \cdot ord_{[i]}\ \omega_f + k/2$$
$$ord_\rho f = 3 \cdot ord_{[\rho]}\ \omega_f + k$$
$$ord_\infty f = ord_{[\infty]}\ \omega_f + k/2$$

or, because for all $t \in \mathbb{H}^*$ holds $ord_t f \geq 0$:

$$ord_{[t]}\ \omega_f = ord_t f \geq 0 \text{ if } t \in \mathscr{D} \setminus \{i,\ \rho,\ \infty\}$$

$$ord_{[i]}\ \omega_f = 1/2 \cdot ord_i f - k/4 \geq -k/4, \text{ hence } ord_{[i]}\ \omega_f \geq -\lfloor k/4 \rfloor$$
$$ord_{[\rho]}\ \omega_f = 1/3 \cdot ord_\rho f - k/3, \text{ hence } ord_{[\rho]}\ \omega_f \geq -\lfloor k/3 \rfloor$$
$$ord_{[\infty]}\ \omega_f = ord_\infty f - k/2, \text{ hence } ord_{[\infty]}\omega_f \geq -k/2$$

which finishes the proof of the order relations. As a consequence

$$\alpha(M_k(\Gamma)) \subset \left\{ \omega \in H^0\left(X, \mathscr{M} \otimes_{\mathscr{O}} \Omega^{\otimes k/2}\right) : div\ \omega \geq -\left\lfloor \frac{k}{4} \right\rfloor \cdot [i] - \left\lfloor \frac{k}{3} \right\rfloor \cdot [\rho] - \frac{k}{2} \cdot [\infty] \right\}$$

Conversely, each $\omega \in H^0(X, \Omega_{\Gamma,k})$ defines the modular form $f \in M_k(\Gamma)$ with

$$f(\tau)\ (d\tau)^{k/2} = p^*\omega$$

iii) *Line bundle*: It is well known that the sheaves of multiples of a divisor are line bundles. The sheaf of multiples of the sum of two divisors is the tensor product of the sheaves of multiples of each summand, see [63], q.e.d.

The formulas in the proof of Theorem 3.17, part 2) show: While a modular form f on $\mathbb{H}^*$ is holomorphic when considered as a function, the representing differential form ω_f on the modular curve X may have poles. Actually, it is the divisor of ω_f which encodes the information about f.

In the language of line bundles, modular forms of weight $= k$ are the sections of the line bundle $\mathscr{L}_{\Gamma,k}$ on the modular curve:

$$M_k(\Gamma) \simeq H^0(X, \mathscr{L}_{\Gamma,k})$$

Example 3.18 (Cusp forms $S_2(\Gamma)$).

1. There are no cusp forms of weight $= 2$, i.e.

$$S_2(\Gamma) = 0.$$

Proof. Each cusp form

$$f \in S_k(\Gamma)$$

is holomorphic on $\mathbb{H}^*$ and vanishes at $\infty \in \mathbb{H}^*$. Hence

$$ord_\tau f \geq 0,\ \tau \in \mathbb{H}, \text{ and } ord_\infty f \geq 1.$$

The order relations from Theorem 3.17 imply

$$\omega_f := \alpha(f) \in H^0(X(1), \Omega_{\Gamma,k})$$

satisfies for $\tau \in \mathscr{D} \setminus \{[i],\ [\rho],\ [\infty]\}$

$$ord_{[\tau]}\omega_f = ord_{[\tau]} f \geq 0,$$

in particular for $k = 2$:

$$ord_{[i]}\omega_f = (1/2)(ord_i f - 1) \geq -(1/2), \text{ hence } ord_{[i]}\omega_f \geq 0$$

$$ord_{[\rho]}\omega_f = (1/3)(ord_\rho f - 2) \geq -(2/3), \text{ hence } ord_{[\rho]}\omega_f \geq 0$$

$$ord_{[\infty]}\omega_f = ord_\infty f - 1 \geq 0$$

Therefore

$$\Omega_{\Gamma,2} \simeq \Omega$$

and ω_f is holomorphic, i.e.

$$\omega_f \in H^0(X, \Omega)$$

The group $H^0(X, \Omega)$ vanishes because

$$dim\, H^0(X, \Omega) = g(X) = g(\mathbb{P}^1),\ q.e.d.$$

2. The formula generalizes to Hecke congruence subgroups as the isomorphy of vector spaces:

$$S_2(\Gamma_0(N)) \simeq H^0(X_0(N), \Omega)$$

which implies

$$dim\, S_2(\Gamma_0(N)) = g(X_0(N)),$$

see Corollary 3.28.

The calculation from Example 3.18 carries over to arbitrary even weights $k \in \mathbb{Z}$.

Corollary 3.19 (Dimension of $M_k(\Gamma)$). *The vector spaces $M_k(\Gamma)$ of modular forms of even weight $k \geq 0$ have the following dimensions:*

$$dim\, M_k(\Gamma) = \begin{cases} \lfloor k/12 \rfloor & k \equiv 2 \mod 12 \\ \lfloor k/12 \rfloor + 1 & otherwise \end{cases}$$

For the dimension of the vector space $S_k(\Gamma)$ of cusp forms see Lemma 3.23.

Proof. We have

$$M_k(\Gamma) \simeq H^0(X, \mathscr{L}_{\Gamma,k}).$$

For $k = 0$ we have on the compact Riemann surface $X \simeq \mathbb{P}^1$

$$dim\, M_0(\Gamma) = dim\, H^0(X, \mathscr{O}) = 1.$$

Therefore we are left with even $k > 0$:

i) *Serre duality and Riemann-Roch theorem*: By Serre-duality for each $k > 0$

$$dim\, H^1(X, \mathscr{L}_{\Gamma,k}) = dim\, H^0(X, \mathscr{L}_{\Gamma,k}^{\vee} \otimes_{\mathscr{O}} \mathscr{O}_K) = dim\, H^0(X, \mathscr{O}_{-(k/2)\cdot K - D_k + K})$$

Now

$$deg\ (-(k/2)\cdot K - D_k + K) = ((k/2)-2) - \lfloor k/4 \rfloor - \lfloor k/3 \rfloor \leq$$

$$\leq ((k/2)-2) - ((k/4)-1) - ((k/3)-1) = k/2 - k/4 - k/3 = k\cdot(1/2 - 1/4 - 1/3) < 0$$

As a consequence

$$0 = dim\, H^0(X, \mathscr{L}_{\Gamma,k}^{\vee} \otimes_{\mathscr{O}} \mathscr{O}_K) = dim\, H^1(X, \mathscr{L}_{\Gamma,k})$$

The Riemann-Roch theorem implies for $\mathscr{L}_{\Gamma,k} = \mathscr{O}_{(k/2)K + D_k}$

$$dim\, M_k(\Gamma) = dim\, H^0(X, \mathscr{L}_{\Gamma,k}) = 1 - g(X) + (k/2)(-2) + \lfloor k/4 \rfloor + \lfloor k/3 \rfloor + k/2 =$$

$$= 1 - k + \lfloor k/4 \rfloor + \lfloor k/3 \rfloor + k/2 = 1 - (k/2) + \lfloor k/3 \rfloor + \lfloor k/4 \rfloor$$

ii) *Evaluating the formula for* dim $M_k(\Gamma)$: We consider the different values of even $k \mod 12$ separately. We make the ansatz

$$k = \alpha \cdot 12 + \beta,\ \beta \in \{0, 2, ..., 10\}$$

and compute for all values of β

$$1 - (k/2) + \lfloor k/3 \rfloor + \lfloor k/4 \rfloor$$

- Residue $\beta = 0$:

$$1 - 6\alpha + 4\alpha + 3\alpha = 1 + \alpha = 1 + \lfloor k/12 \rfloor$$

- Residue $\beta = 2$:

$$1 - (6\alpha + 1) + \lfloor 4\alpha + 2/3 \rfloor + \lfloor 3\alpha + 2/4 \rfloor = 1 - (6\alpha + 1) + 4\alpha + 3\alpha = \alpha = \lfloor k/12 \rfloor$$

- Residue $\beta \in \{4,6,8,10\}$:

$$1-(6\alpha+\beta/2)+\lfloor 4\alpha+\beta/3\rfloor+\lfloor 3\alpha+\beta/4\rfloor=$$

$$=1-6\alpha-\beta/2+4\alpha+\lfloor\beta/3\rfloor+3\alpha+\lfloor\beta/4\rfloor=1+\alpha+(-\beta/2+\lfloor\beta/3\rfloor+\lfloor\beta/4\rfloor)=$$

$$=1+\alpha=1+\lfloor k/12\rfloor$$

q.e.d.

In particular

$dim\, M_0=1, dim\, M_2=0,\ dim\, M_4=dim\, M_6=dim\, M_8=dim\, M_{10}=1,\ dim\, M_{12}=2.$

The non-zero vector spaces in the last line are spanned by the Eisenstein series $G_4,\ G_6$ and their products. Only M_{12} contains a non-zero cusp form, namely the discriminant modular form Δ.

Apparently the numerical value $dim\, H^0(X,\mathscr{L}_{\Gamma,k})$ can be obtained without applying the theorem of Riemann-Roch and Serre duality in the proof of Corollary 3.19: On the modular curve $X\simeq\mathbb{P}^1$ each line bundle $\mathscr{L}$ is determined by its degree m, and for $m\geq 0$

$$dim H^0(\mathbb{P}^1,\mathscr{L})=m+1.$$

We gave the proof in the above form, because Theorem 3.26 will generalize the proof to the modular curves $X_0(N)$ of the Hecke congruence subgroups.

Corollary 3.20 (Weight formula for modular forms). *Consider an even integer $k\geq 4$ and a modular form $f\in M_k(\Gamma)$. Then the sum of the orders of f satisfies the following equation:*

$$ord_\infty f+\frac{1}{2}ord_i f+\frac{1}{3}ord_\rho f+\sum_\tau{}' ord_\tau f=\frac{k}{12}$$

Here the symbol $\sum'_\tau$ denotes the summation over all points $\tau\in\mathscr{D}\setminus\{i,\ \rho\}$.

Proof. We recall the relation between the order of $f\in M_k(\Gamma)$ at a point τ and the order of the differential form $\omega_f\in H^0(X,\mathscr{M}\otimes_{\mathscr{O}}\Omega^{\otimes k/2})$ at the point $[\tau]\in X$ established during the proof of Theorem 3.17:

$$ord_\infty f=ord_{[\infty]}\ \omega_f+k/2$$

$$ord_i f=2\ ord_{[i]}\ \omega_f+k/2$$

$$ord_\rho f=3\ ord_{[\rho]}\ \omega_f+k$$

$$ord_\tau f=ord_{[\tau]}\ \omega_f,\ \tau\in\mathscr{D}\setminus\{i,\ \rho,\ \infty\}.$$

The modular curve X has genus $g = 0$ according to Corollary 3.16. Therefore the line bundle Ω_X has degree $= -2$, and the tensor product ${\Omega_X}^{\otimes k/2}$ has degree

$$= (-2) \cdot k/2 = -k$$

which implies

$$deg\ div(\omega_f) = -k.$$

As a consequence

$$ord_\infty\ f + \frac{1}{2}\, ord_i\ f + \frac{1}{3}\, ord_\rho\ f + \sum_\tau{}'\ ord_\tau\ f =$$

$$= \left(ord_{[\infty]}\ \omega_f + \frac{k}{2} \right) + \left(ord_{[i]}\ \omega_f + \frac{k}{4} \right) + \left(ord_{[\rho]}\ \omega_f + \frac{k}{3} \right) + \sum_\tau{}' ord_{[\tau]}\ \omega_f =$$

$$= deg\ div(\omega_f) + \frac{k}{2} + \frac{k}{4} + \frac{k}{3} = -k + \frac{k}{2} + \frac{k}{4} + \frac{k}{3} = \frac{k}{12},\ q.e.d.$$

Corollary 3.21 (Specific values and Fourier coefficents of the modular invariant j).

1. *The modular invariant*

$$j : X(1) \to \mathbb{P}^1$$

attains the distinguished values

$$j([i]) = 1728 \text{ and } j([\rho]) = 0.$$

2. *All Fourier coefficents $(b_n)_{n \geq -1}$ of the modular invariant*

$$j(q) = \sum_{n=-1}^{\infty} b_n \cdot q^n$$

are integers, and $b_{-1} = 1$.

Proof. 1. Corollary 3.20 implies $G_4(\rho) = 0$ and $G_6(i) = 0$. The definition

$$j = 1728 \cdot \frac{{g_2}^3}{{g_2}^3 - 27{g_3}^2}$$

implies the values of j at the distinguished orbits.

2. To compute the Fourier expansion of

$$j = 2^6 \cdot 3^3 \cdot \frac{g_2^3}{\Delta}$$

we use the definition

$$g_2 = \frac{2^2}{3} \cdot \pi^4 \cdot E_4, \text{ hence } g_2^3 = \frac{2^6}{3^3} \cdot \pi^{12} \cdot E_4^3,$$

and secondly the formula from Proposition 3.14

$$\frac{\Delta(\tau)}{(2\pi)^{12}} = \sum_{n=1}^{\infty} \tau_n \cdot q^n \in \mathbb{Z}\{q\},\ q = e^{2\pi i \cdot \tau}.$$

We obtain

$$j = \left(2^6 \cdot 3^3\right) \cdot \frac{g_2^3}{\Delta} = \left(2^6 \cdot 3^3\right) \cdot \left(\frac{2^6}{3^3} \cdot E_4^3 \cdot \pi^{12}\right) \cdot \frac{1}{\Delta} =$$

$$= \frac{E_4^3}{\Delta/(2\pi)^{12}} = \frac{E_4^3}{\sum\limits_{n=1}^{\infty} \tau_n \cdot q^n} = \frac{1}{q} \cdot \frac{E_4^3}{1 + \sum\limits_{n=2}^{\infty} \tau_n \cdot q^{n-1}} =$$

$$= \frac{1}{q} \cdot E_4^3 \cdot \sum_{m=0}^{\infty} \left((-1)^m \cdot \sum_{n=2}^{\infty} \tau_n \cdot q^{n-1}\right)^m = \frac{1}{q} \cdot (1 + O(q))$$

by applying the formula of the geometric series and using

$$E_4(q) = 1 + O(q)$$

from Corollary 3.11 and the fact, that E_4 has integer Fourier coefficents, q.e.d.

Corollary 3.22 (The field of automorphic functions).

1. *If an automorphic function $f \in A_0(\Gamma)$ is holomorphic on $\mathbb{H}$ with Fourier series*

$$f(\tau) = \sum_{n \geq -k} c_n \cdot q^n,\ c_{-k} \neq 0,$$

for a suitable $k \in \mathbb{N}$, then a poylnomial $P(X) \in \mathbb{C}[X]$ of degree k exists with

- $f = P(j)$,
- *and all coefficients of $P(X)$ are $\mathbb{Z}$-linear combinations of the Fourier coefficients $c_{-k}, \ldots, c_{-1}, c_0$.*

2. *The field of automorphic functions, which equals the field of meromorphic functions on the modular curve X, is*

$$A_0(\Gamma) = \mathbb{C}(j).$$

Thanks to Corollary 3.16 the second part of Corollary 3.22 is a disguised version of the well-known fact that the field of meromorphic functions on $\mathbb{P}^1$ is $\mathbb{C}(z)$, the field of rational functions in one complex variable.

Proof. 1. The proof goes by induction on k: If $k = 0$ than f is a modular function, hence equals the constant c_0. For the induction step $k-1 \mapsto k$ consider the function

$$g := f - c_{-k} \cdot j^k.$$

The function g has at most a pole of order $= k-1$ at ∞. Therefore the induction assumption applies to g.

2. Each automorphic function $f \in A_0(\Gamma)$ can be considered a meromorphic function $f \in \mathscr{M}(\mathbb{P}^1)$ on the projective space. Denote by

$$A := \{x_1, ..., x_n\} \subset \mathbb{H} \cup \{\infty\} \text{ and } B = \{y_1, ..., y_n\} \subset \mathbb{H} \cup \{\infty\}$$

the respective zero set and pole set of f, counted with multiplicity. Both sets have the same cardinality because a non-constant holomorphic map between compact Riemann surfaces attains each value with the same multiplicity, see [63]. Then

$$g := \prod_{\nu=1}^{n} \frac{j - j(x_\nu)}{j - j(y_\nu)} \in A_0(\Gamma)$$

has the same zero set and pole set as f. The quotient f/g has no poles and zeros on $\mathbb{H} \cup \{\infty\}$. According to part 1) a constant $a \in \mathbb{C}$ exists with

$$a = \frac{f}{g}$$

or

$$f = a \cdot g \in \mathbb{C}(j), \ q.e.d.$$

Lemma 3.23 (Exact sequence for cusp forms). *Denote by*

$$\varepsilon : M_k(\Gamma) \to \mathbb{C}, f \mapsto f(\infty),$$

the evaluation with kernel $S_k(\Gamma)$ and by

$$\mu_\Delta : M_{k-12}(\Gamma) \to M_k(\Gamma), \ f \mapsto f \cdot \Delta,$$

the multiplication with the discriminant form. Then for even $k \geq 4$: The following sequence of vector space morphisms is exact

$$0 \to M_{k-12}(\Gamma) \xrightarrow{\mu_\Delta} M_k(\Gamma) \xrightarrow{\varepsilon} \mathbb{C} \to 0.$$

In particular:

- *For even $k \geq 4$:*
$$M_k(\Gamma) = S_k(\Gamma) \oplus \mathbb{C} \cdot G_k,$$
and the multiplication by the discriminant modular form Δ defines a vector space isomorphism
$$\mu_\Delta : M_{k-12}(\Gamma) \xrightarrow{\simeq} S_k(\Gamma).$$
- *For $k < 0$:*
$$dim\, M_k = 0$$

As a consequence, the formulas from Corollary 3.19 allow to compute the dimension of $S_k(\Gamma)$. A partial generalization of Lemma 3.23 will be proved in Corollary 3.28.

Proof. i) Exactness on the right-hand side: For even $k \geq 4$ the Eisenstein series $G_k \in M_k(\Gamma)$ satisfies
$$G_k(\infty) = 2 \cdot \zeta(k) \neq 0.$$
Therefore ε is surjective.

ii) Exactness in the middle: If $f \in M_k(\Gamma)$ with $\varepsilon(f) = 0$, i.e.
$$f \in S_k(\Gamma)$$
then the quotient
$$g := \frac{f}{\Delta}$$
is holomorphic on $\mathbb{H}$, because Δ has no zero on $\mathbb{H}$ due to Proposition 1.19. In addition g is holomorphic at the point ∞ because Δ has a zero of order 1 at ∞ according to Proposition 3.14. Hence $g \in M_{k-12}(\Gamma)$. In addition, the composition
$$\varepsilon \circ \mu_\Delta = 0$$
is obvious.

iii) Exactness on the left-hand side: Apparently the map μ_Δ is injective.

iv) As a consequence
$$dim\, S_k(\Gamma) = 0 \text{ for } k \in \{0, 2, 4, 6, 8, 10\}.$$
Then iteratively for all even $k < 0$
$$dim\, M_k(\Gamma) = 0$$
because for all even $k \in \mathbb{Z}$
$$M_{k-12}(\Gamma) \xrightarrow{\mu_\Delta} S_k(\Gamma)$$
is injective, q.e.d.

The result $dim\, M_k(\Gamma) = 0$ if $k < 0$ generalizes to Hecke congruence subgroups: For $k < 0$

$$dim\, M_k(\Gamma_0(N)) = 0,$$

see [66, Prop. 3].

Theorem 3.24 (Algebra of modular forms). *The associative algebra*

$$M_*(\Gamma) := \left(\bigoplus_{k \geq 0} M_{2k}(\Gamma), +, \cdot \right)$$

of modular forms of the module group Γ is commutative and freely generated by the two Eisenstein series

$$G_4 \in M_4(\Gamma) \text{ and } G_6 \in M_6(\Gamma).$$

The subalgebra of cusp forms

$$S_*(\Gamma) := \bigoplus_{k \geq 0} S_{2k}(\Gamma) \subset M_*(\Gamma)$$

is a principal ideal generated by $\Delta \in S_{12}(\Gamma)$.

Proof. One checks for $k \neq k'$

$$M_{2k}(\Gamma) \cap M_{2k'}(\Gamma) = \{0\}.$$

i) *Generated by G_4 and G_6*: We prove the claim about $M_k(\Gamma)$ by reducing successively the weight. The even integer $k \geq 4$ decomposes as

$$k = 4 \cdot \alpha + 6 \cdot \beta$$

with non-negative integers $\alpha, \beta \in \mathbb{Z}$. Hence

$$G_4^\alpha \cdot G_6^\beta \in M_k \text{ and } \varepsilon \left(G_4^\alpha \cdot G_6^\beta \right) \neq 0$$

Consider an arbitrary element $f \in M_k$. For suitable $\lambda \in \mathbb{C}$

$$\varepsilon \left(f - \lambda \cdot G_4^\alpha \cdot G_6^\beta \right) = \left(f - \lambda \cdot G_4^\alpha \cdot G_6^\beta \right) (\infty) = 0.$$

According to Lemma 3.23 an element $g \in M_{k-12}$ exists with

$$f - \lambda \cdot G_4^\alpha \cdot G_6^\beta = \Delta \cdot g.$$

The claim follows by repeating the argument with $g \in M_{k-12}(\Gamma)$, and using

$$M_4(\Gamma) = \mathbb{C} \cdot G_4 \text{ and } M_6(\Gamma) = \mathbb{C} \cdot G_6$$

due to Corollary 3.19.

ii) *Freely generated*: The generators G_4 and G_6 are even algebraically independent. Assume the existence of a polynomial $P \in \mathbb{C}[T_1, T_2]$ with

$$P(G_4, G_6) = 0.$$

We may assume that all monomials of $P(G_4, G_6)$ have the same weight. The case

$$P(G_4, G_6) = a \cdot G_4^m + G_6 \cdot \hat{P}(G_4, G_6),\ a \in \mathbb{C}^*,$$

is excluded because $G_4(i) \neq 0$, but $G_6(i) = 0$. Analogously the case

$$P(G_4, G_6) = b \cdot G_6^m + G_4 \cdot \hat{P}(G_4, G_6),\ b \in \mathbb{C}^*,$$

is excluded because $G_6(\rho) \neq 0$, but $G_4(\rho) = 0$. Hence the product $G_4 G_6$ divides $P(G_4, G_6)$, i.e.

$$P(G_4, G_6) = G_4 G_6 \cdot \hat{P}(G_4, G_6) = 0.$$

Iteration of the argument for

$$\hat{P}(G_4, G_6) = 0 \text{ with } deg\ \hat{P} < deg\ P$$

proves the claim $P = 0$ by descending induction.

iii) *Ideal of cusp forms*: According to Lemma 3.23 any cusp form is a multiple of Δ, q.e.d.

3.3 Generalization to Hecke congruence subgroups $\Gamma_0(N)$

In an analogous way to Theorem 3.17, also modular forms of a Hecke congruence subgroup $\Gamma_0(N)$, $N \in \mathbb{N}$, are meromorphic differential forms on the corresponding modular curve $X_0(N)$. Essentially, one has to take into account that a congruence subgroup has more than one cusp and that cusps may have distinct width. Therefore the width of the cusps enters as an additional parameter when determining local coordinates around the cusps of the modular curve. In addition, one cannot use a standard atlas like on $X = \mathbb{P}^1$ but one has to deal with atlases in a generic way.

Recall from Remark 2.30 the branched covering

$$f : X_0(N) \to X(\Gamma) \simeq \mathbb{P}^1$$

of degree

$$deg\ f = N \cdot \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

and the genus formula

$$g(X_0(N)) = 1 + \frac{deg\ f}{12} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3} - \frac{\varepsilon_\infty}{2}$$

Moreover, we recall the canonical projection from the extended half-plane

$$p : \mathbb{H}^* \to X_0(N) := \Gamma_0(N) \backslash \mathbb{H}^*$$

The aid to represent modular forms of $M_k(\Gamma_0(N))$, which are defined as functions on $\mathbb{H}^*$, as meromorphic differential forms on the modular curve $X_0(N)$ are the divisors

$$D_k := \left\lfloor \frac{k}{4} \right\rfloor \cdot \sum_{\substack{x \in X_0(N) \\ x \text{ elliptic} \\ h_x = 2}} x + \left\lfloor \frac{k}{3} \right\rfloor \cdot \sum_{\substack{x \in X_0(N) \\ x \text{ elliptic} \\ h_x = 3}} x + \frac{k}{2} \cdot \sum_{\substack{x \in X_0(N) \\ x \text{ cusp}}} x \in Div(X_0(N)), \text{ even } k \geq 0.$$

They have degree

$$deg\ D_k = \left\lfloor \frac{k}{4} \right\rfloor \cdot \varepsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \cdot \varepsilon_3 + \frac{k}{2} \cdot \varepsilon_\infty$$

For each fixed even $k \geq 0$ the divisor D_k singles out those meromorphic differential forms from

$$H^0\left(X_0(N), \mathscr{M} \otimes_{\mathscr{O}} \Omega^{\otimes k/2}\right)$$

which arise from modular forms under the canonical injection

$$\alpha : M_k(\Gamma_0(N)) \to H^0\left(X_0(N), \mathscr{M} \otimes_{\mathscr{O}} \Omega^{\otimes k/2}\right),\ g \mapsto \omega_g,$$

with ω_g the well-defined differential form satisfying

$$p^* \omega_g(\tau) = g(\tau)\ (d\tau)^{k/2}.$$

Lemma 3.25 (Order relation). *Consider a Hecke congruence subgroup $\Gamma_0(N)$ and an even weight $k \geq 0$.*

1. Definition of α*: The map*

$$\alpha : M_k(\Gamma_0(N)) \to H^0\left(X_0(N), \mathscr{M} \otimes_{\mathscr{O}} \Omega^{\otimes k/2}\right),\ g \mapsto \omega_g,$$

with ω_g the well-defined differential form satisfying

$$p^* \omega_g(\tau) = g(\tau)\ (d\tau)^{k/2}$$

is well-defined.

2. Order relation*: The order of a modular form g and the order of the meromorphic differential form*

$$\omega_g = \alpha(g)$$

relate as

$$ord_\tau g = \begin{cases} ord_{[\tau]}\omega_g + k/2 & [\tau] \text{ cusp} \\ \\ h_\tau \cdot ord_{[\tau]}\omega_g + k/2 \cdot (h_\tau - 1) & \tau \in \mathbb{H} \end{cases}$$

Proof. Each modular form $g \in M_k(\Gamma_0(N))$ is a holomorphic function on $\mathbb{H}$. The function g defines on $\mathbb{H}$ the $\Gamma_0(N)$-invariant holomorphic differential form

$$g(\tau)\ (d\tau)^{k/2}$$

Therefore $g(\tau)\ (d\tau)^{k/2}$ defines on the open Riemann surface

$$Y_0(N) := p(\mathbb{H})$$

a meromorphic differential form

$$\omega_g \in H^0\left(Y_0(N), \mathscr{M} \otimes \Omega^{\otimes k/2}\right)$$

with singularities at most the finitely many orbits of elliptic points $\tau \in \mathbb{H}$.

Moreover $\Gamma_0(N)$ has only finitely many cusps, see Example 2.11. For arbitrary $q \in \mathbb{Q}$ and

$$\beta \in \Gamma \text{ with } q = \beta(\infty)$$

each modular form $g \in M_k(\Gamma_0(N))$ has a well-defined order

$$ord_q g := ord_\infty g[\beta]_k$$

independent from the choice of β. Hence ω_g extends as meromorphic differential form to the compactified modular curve

$$\omega_g \in H^0\left(X_0(N), \mathscr{M} \otimes \Omega^{\otimes k/2}_{X_0(N)}\right)$$

A cumbersome calculation by using charts, see [17, Sect. 3.3.], shows that the order relations from the proof of Theorem 3.17 carry over: These formula show that the map α is well-defined. The map α is injective, and via pullback of differential forms also surjective, q.e.d.

On a compact Riemann surface line bundles and divisors correspond to each other bijectively, see [63]. Theorem 3.26 introduces the line bundles of meromorphic differential forms induced by the distinguished divisors D_k on the modular curves.

Theorem 3.26 (The line bundle of modular forms). *Consider a Hecke congruence subgroup*

$$\Gamma_0(N),\ N \in \mathbb{N},$$

and an even weight $k \geq 0$.

On the modular curve $X_0(N)$ with canonical divisor $K \in Div(X_0(N))$ the line bundle

$$\mathscr{L}_{N,k} := \mathscr{O}_{(k/2)\cdot K + D_k} \in Pic(X_0(N))$$

with the divisor

$$D_k := \left\lfloor \frac{k}{4} \right\rfloor \cdot \sum_{\substack{x \in X_0(N) \\ x\ elliptic \\ h_x = 2}} x + \left\lfloor \frac{k}{3} \right\rfloor \cdot \sum_{\substack{x \in X_0(N) \\ x\ elliptic \\ h_x = 3}} x + \frac{k}{2} \cdot \sum_{\substack{x \in X_0(N) \\ x\ cusp}} x \in Div(X_0(N))$$

of degree

$$deg\ D_k = \left\lfloor \frac{k}{4} \right\rfloor \cdot \varepsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \cdot \varepsilon_3 + \frac{k}{2} \cdot \varepsilon_\infty \geq 0$$

satisfies:

- Meromorphic differential forms*:*

  $$\mathscr{L}_{N,k} \simeq \Omega_{N,k}$$

  with the subsheaf of meromorphic differential forms on $X_0(N)$

  $$\Omega_{N,k} \subset \mathscr{M} \otimes_{\mathscr{O}} \Omega^{\otimes k/2}$$

  defined by

  $$\Omega_{N,k}(U) := \{\omega \in H^0(U, \mathscr{M} \otimes_{\mathscr{O}} \Omega^{\otimes k/2}) : \omega \neq 0\ and\ div\ \omega \geq -D_k|U\} \cup \{0\}$$

  for each open $U \subset X_0(N)$

- Global sections*: Consider the canonical map*

  $$\alpha : M_k(\Gamma_0(N)) \to H^0(X_0(N), \mathscr{M} \otimes_{\mathscr{O}} \Omega^{\otimes k/2}),\ g \mapsto \omega_g,$$

  with ω_g the unique differential form with

  $$p^* \omega_g = g(\tau)\ (d\tau)^{k/2}.$$

  Here $p : \mathbb{H}^* \to X_0(N)$ denotes the canonical projection. Then

$$H^0(X_0(N),\mathscr{L}_{N,k}) \simeq H^0(X_0(N),\Omega_{N,k}) =$$

$$= im\ \left[\alpha : M_k(\Gamma_0(N)) \to H^0\left(X_0(N),\mathscr{M}\otimes_{\mathscr{O}}\Omega^{\otimes k/2}\right)\right]$$

- Cohomology*: For* $k \geq 2$

$$H^1(X_0(N),\mathscr{L}_{N,k}) = 0$$

- Dimension of vector space of sections*: For* $k \geq 2$

$$dim\ H^0(X_0(N),\mathscr{L}_{N,k}) = (g(X_0(N))-1)\cdot(k-1) + deg\ D_k,$$

and for $k = 0$

$$\mathscr{L}_{N,0} \simeq \mathscr{O},\ hence\ dim\ H^0(X_0(N),\mathscr{L}_{N,0}) = 1.$$

Proof. We set

$$g := g(X_0(N))$$

i) *Estimating the degree of* $(k/2)\cdot K + D_k$: By definition

$$\mathscr{L}_{N,k} = \mathscr{O}_{(k/2)\cdot K + D_k}.$$

Using the estimates

$$\lfloor k/4 \rfloor \geq (k/4) - 1/2 \text{ and } \lfloor k/3 \rfloor \geq (k/3) - 2/3$$

and the genus formula for $X_0(N)$ we obtain for the degree of the corresponding divisor for $k \geq 2$

$$deg\ ((k/2)\cdot K + D_k) \geq \left(\frac{k}{2}\cdot(2g-2)\right) + \left(\frac{k-2}{4}\cdot\varepsilon_2 + \frac{k-2}{3}\cdot\varepsilon_3 + \frac{k}{2}\cdot\varepsilon_\infty\right) =$$

$$= (2g-2) + \frac{k-2}{2}\cdot\left(2g-2+\frac{\varepsilon_2}{2}+\frac{2}{3}\cdot\varepsilon_3+\varepsilon_\infty\right)+\varepsilon_\infty =$$

$$= (2g-2) + \frac{k-2}{2}\cdot\left(\frac{deg\ f}{6}\right)+\varepsilon_\infty > 2g-2$$

ii) *Vanishing of dim* $H^1(X_0(N),\mathscr{L}_{N,k})$: We apply Serre's duality theorem in the form

$$H^1(X_0(N),\mathscr{L}_{N,k}) = H^0(X_0(N),\mathscr{L}_{N,k}^\vee\otimes_{\mathscr{O}}\Omega)^\vee$$

and estimate for even $k \geq 2$ due to part i)

$$deg\ (-((k/2)\cdot K + D_k) + K) < (2-2g) + (2g-2) = 0$$

Hence

$$dim\ H^1(X_0(N),\mathscr{L}_{N,k}) = dim\ H^0(X_0(N),\mathscr{L}_{N,k}^\vee\otimes_{\mathscr{O}}\Omega) = 0$$

iii) *Riemann-Roch theorem for* $\mathscr{L}_{N,k}$: The Riemann-Roch theorem proves the dimension formula

$$dim\, H^0(X_0(N), \mathscr{L}_{N,k}) = 1 - g + deg\, ((k/2) \cdot K + D_k) =$$

$$= 1 - g + deg\, ((k/2) \cdot K) + deg\, D_k = (k-1)(g-1) + deg\, D_k,\ q.e.d.$$

Remark 3.27 (Modular forms of Hecke congruence subgroups). Figure 3.1 shows different modular curves as coverings of $\mathbb{P}^1$ and the dimension of their vector spaces of modular forms, see PARI file "Congruence_subgroup_19". The last column shows the numerical value

$$dim\, H^0(X(\Gamma_0(N)), \mathscr{L}_{N,k})$$

computed by applying the Riemann-Roch theorem to the line bundle $\mathscr{L}_{N,k}$.

```
Congruence subgroups_19, Start

Modular forms of congruence subgroups Gamma_0(p**n)

Parameter: p_min = 2, p_max = 7, n_max = 4, weight = 4

h0_RR = dimension via Riemann-Roch theorem

(p,n) = (2,0), q = p^n = 1, X(Gamma_0(1)): (deg, genus, dim M_4, h0_RR) = (1,0,1,1)
(p,n) = (2,1), q = p^n = 2, X(Gamma_0(2)): (deg, genus, dim M_4, h0_RR) = (3,0,2,2)
(p,n) = (2,2), q = p^n = 4, X(Gamma_0(4)): (deg, genus, dim M_4, h0_RR) = (6,0,3,3)
(p,n) = (2,3), q = p^n = 8, X(Gamma_0(8)): (deg, genus, dim M_4, h0_RR) = (12,0,5,5)
(p,n) = (2,4), q = p^n = 16, X(Gamma_0(16)): (deg, genus, dim M_4, h0_RR) = (24,0,9,9)

(p,n) = (3,0), q = p^n = 1, X(Gamma_0(1)): (deg, genus, dim M_4, h0_RR) = (1,0,1,1)
(p,n) = (3,1), q = p^n = 3, X(Gamma_0(3)): (deg, genus, dim M_4, h0_RR) = (4,0,2,2)
(p,n) = (3,2), q = p^n = 9, X(Gamma_0(9)): (deg, genus, dim M_4, h0_RR) = (12,0,5,5)
(p,n) = (3,3), q = p^n = 27, X(Gamma_0(27)): (deg, genus, dim M_4, h0_RR) = (36,1,12,12)
(p,n) = (3,4), q = p^n = 81, X(Gamma_0(81)): (deg, genus, dim M_4, h0_RR) = (108,4,33,33)

(p,n) = (5,0), q = p^n = 1, X(Gamma_0(1)): (deg, genus, dim M_4, h0_RR) = (1,0,1,1)
(p,n) = (5,1), q = p^n = 5, X(Gamma_0(5)): (deg, genus, dim M_4, h0_RR) = (6,0,3,3)
(p,n) = (5,2), q = p^n = 25, X(Gamma_0(25)): (deg, genus, dim M_4, h0_RR) = (30,0,11,11)
(p,n) = (5,3), q = p^n = 125, X(Gamma_0(125)): (deg, genus, dim M_4, h0_RR) = (150,8,43,43)
(p,n) = (5,4), q = p^n = 625, X(Gamma_0(625)): (deg, genus, dim M_4, h0_RR) = (750,48,203,203)

(p,n) = (7,0), q = p^n = 1, X(Gamma_0(1)): (deg, genus, dim M_4, h0_RR) = (1,0,1,1)
(p,n) = (7,1), q = p^n = 7, X(Gamma_0(7)): (deg, genus, dim M_4, h0_RR) = (8,0,3,3)
(p,n) = (7,2), q = p^n = 49, X(Gamma_0(49)): (deg, genus, dim M_4, h0_RR) = (56,1,18,18)
(p,n) = (7,3), q = p^n = 343, X(Gamma_0(343)): (deg, genus, dim M_4, h0_RR) = (392,26,105,105)
(p,n) = (7,4), q = p^n = 2401, X(Gamma_0(2401)): (deg, genus, dim M_4, h0_RR) = (2744,201,714,714)
```

Fig. 3.1 Dimension formulas for modular forms of weight $k = 4$ of $\Gamma_0(p^n)$

Apparently

$$M_0(\Gamma_0(N)) \simeq \mathbb{C},\ N \in \mathbb{N},$$

which implies

$$dim\ M_0(\Gamma_0(N)) = 1 \text{ and } dim\ S_0(\Gamma_0(N)) = 0.$$

Corollary 3.28 (Codimension of cusp forms of Hecke congruence subgroups). *Consider a congruence subgroup*

$$\Gamma_0(N),\ N \in \mathbb{N}.$$

1. *For even weight $k \geq 4$ the subspace of cusp forms*

$$S_k(\Gamma_0(N)) \subset M_k(\Gamma_0(N))$$

has codimension $= \varepsilon_\infty$, the number of cusps of $X_0(N)$. In particular, the codimension does not depend on the weight k.

2. *For weight $k = 2$ cusp forms are exactly the holomorphic differential forms on the modular curve. Hence*

$$dim\ S_2(\Gamma_0(N)) = g(X_0(N)).$$

For the computation of ε_∞ in the general case see Example 2.11.

Proof. Set

$$g := g(X_0(N))$$

and consider the divisor $D_k \in Div(X_0(N))$ from Theorem 3.26, and define the divisor

$$D_k^\infty := \sum_{\substack{x \in X_0(N) \\ x \text{ cusp}}} (-1) \cdot x + D_k \in Div(X_0(N))$$

and the correponding line bundle

$$\mathscr{L}_{N,k}^\infty = \mathscr{O}_{(k/2)\cdot K + D_k^\infty} \in Pic(X_0(N)$$

with

$$deg\ \mathscr{L}_{N,k}^\infty = -\varepsilon_\infty + deg\ \mathscr{L}_{N,k}.$$

The order relations imply for even $k \geq 2$

$$H^0\left(X_0(N), \mathscr{L}_{N,k}^\infty\right) =$$

$$= \left\{\omega_h \in H^0(X_0(N), \Omega_{N,k}) :\ ord_x \omega_h \geq (k/2) - 1 \text{ for all cusps } x \in X_0(N)\right\} =$$

$$= \{h \in M_k(\Gamma_0(N)) :\ ord_t h \geq 1 \text{ for all } t \in \mathbb{H}^* \text{ with } [t] \text{ cusp}\} = S_k(\Gamma_0(N))$$

1. $k \geq 4$: The formula from the proof of Theorem 3.26 shows for even $k \geq 4$

$$deg\ \mathscr{L}^{\infty}_{N,k} \geq 2g-2+\frac{k-2}{2}\cdot\frac{deg\ f}{6} > 2g-2$$

because $deg\ f \geq 1$. Hence $H^1\left(X_0(N), \mathscr{L}^{\infty}_{N,k}\right) = 0$ because

$$deg\ (\mathscr{L}^{\infty}_{N,k})^{\vee} \otimes_{\mathscr{O}} \Omega^1 < -(2g-2)+(2g-2) = 0,$$

and the Riemann-Roch theorem implies

$$dim\ S_k(\Gamma_0(N)) = dim\ H^0\left(X_0(N), \mathscr{L}^{\infty}_{N,k}\right) =$$

$$= dim\ H^0\left(X_0(N), \mathscr{L}_{N,k}\right) - \varepsilon_{\infty} = dim\ M_k(\Gamma_0(N)) - \varepsilon_{\infty}.$$

2. $k = 2$: The explicit form of D^{∞}_2 shows

$$D^{\infty}_2 = 0 \in Div(X_0(N)),$$

which implies

$$\mathscr{L}^{\infty}_{N,2} = \mathscr{O}_K = \Omega^1$$

and

$$S_2(X_0(N)) = H^0(X_0(N), \Omega),\ q.e.d.$$

Chapter 4
Elliptic curves

The present chapter ties quite closely with Section 2.1 on tori. We now bridge complex analysis and algebraic geometry.

Section 4.1 shows that each complex torus is an algebraic variety in the complex projective space $\mathbb{P}^2$. The variety is the zero set of a cubic polynomial.

Section 4.2 introduces elliptic curves as projective-algebraic varieties of genus $= 1$ defined over arbitrary subfields of $\mathbb{C}$. We show that elliptic curves correspond bijectively to the smooth zero set of cubic polynomials, the Weierstrass polynomials. The passage to algebraic geometry allows to investigate the points of elliptic curves with coordinates in distinguished subfields of $\mathbb{C}$.

4.1 Embedding tori as plane cubic hypersurfaces

Generalizing the 1-dimensional projective space $\mathbb{P}^1$ we introduce the higher-dimensional complex projective spaces $\mathbb{P}^n$.

Definition 4.1 (n-dimensional projective space). For $n \in \mathbb{N}$ consider the quotient

$$\mathbb{P}^n := (\mathbb{C}^{n+1} \setminus \{0\})/\sim$$

with respect to the equivalence relation

$$z = (z_0, ..., z_n) \sim w = (w_0, ..., w_n) \ :<=> \exists \lambda \in \mathbb{C}^* : \ w = \lambda \cdot z$$

and with the canonical projection onto equivalence classes

$$\pi : \mathbb{C}^{n+1} \setminus \{0\} \to \mathbb{P}^n, \ z \mapsto [z].$$

For $z = (z_0, ..., z_n) \in \mathbb{C}^{n+1} \setminus \{0\}$ the expression

$$(z_0 : ... : z_n) := \pi(z) \in \mathbb{P}^n$$

is named the *homogeneous coordinate* of $\pi(z)$. The quotient topology is named the Euclidean topology of $\mathbb{P}^n$. The space $\mathbb{P}^n$ is named the n-dimensional complex *projective space*.

One considers $\mathbb{C}^n \subset \mathbb{P}^n$ via the injection

$$\mathbb{C}^n \hookrightarrow \mathbb{P}^n,\ (z_1, ..., z_n) \mapsto (1 : z_1 : ... : z_n).$$

Definition 4.2 (Standard atlas of $\mathbb{P}^n$). The *standard atlas* of $\mathbb{P}^n$ is the family

$$\mathscr{U} := (U_i)_{i=0,...,n}$$

with the open sets

$$U_i := \{(z_0 : ... : z_n) \in \mathbb{P}^n :\ z_i \neq 0\},\ i = 0, ..., n.$$

and for each $i = 0, ..., n$ as i-th *standard chart* the homeomorphism

$$\phi_i : U_i \to \mathbb{C}^n,\ (z_0 : ... : z_n) \mapsto \left(\frac{z_0}{z_i}, ..., \frac{z_{i-1}}{z_i}, \hat{\frac{z_i}{z_i}}, \frac{z_{i+1}}{z_i}, ..., \frac{z_n}{z_i}\right).$$

Here the "hat" indicates omission of the term. The transformation between two charts ϕ_j and ϕ_i with $i < j$ is the map

$$\psi_{ij} := \phi_i \circ \phi_j^{-1} : \phi_j(U_i \cap U_j) \to \phi_i(U_i \cap U_j),$$

$$\left(w_0, ..., w_{j-1}, \hat{1}, w_{j+1}, ..., w_n\right) \mapsto \left(\frac{w_0}{w_i}, ..., \frac{w_{i-1}}{w_i}, \hat{1}, \frac{w_{i+1}}{w_i}, ..., \frac{w_{j-1}}{w_i}, \frac{1}{w_i}, \frac{w_{j+1}}{w_i}, ..., \frac{w_n}{w_i}\right)$$

Theorem 4.3 shows once more the importance of the Weierstrass function $\wp$ and of its differential equation for $\wp'$ in the theory of complex tori.

Theorem 4.3 (The embedding theorem for tori). *Consider a complex torus*

$$T := \mathbb{C}/\Lambda$$

with lattice

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2.$$

Set

$$g_2 := 60 \cdot G_{\Lambda,4},\ g_3 := 140 \cdot G_{\Lambda,6},$$

and denote by $\wp = \wp_\Lambda$ the Weierstrass function of Λ. The map

$$\phi : T \to \mathbb{P}^2,\ p \mapsto \begin{cases} (1 : \wp(p) : \wp'(p)) & \text{if } p \neq 0 \\ (0:0:1) & \text{if } p = 0 \end{cases}$$

maps the torus T biholomorphically onto the cubic hypersurface $E \subset \mathbb{P}^2$ defined by the cubic polynomial

$$F_{hom}(X_0, X_1, X_2) = X_2^2 X_0 - (4X_1^3 - g_2 \cdot X_1 X_0^2 - g_3 \cdot X_0^3) \in \mathbb{C}[X_0, X_1, X_2],$$

which is the homogenization of

$$F(X,Y) = Y^2 - (4X^3 - g_2 X - g_3) \in \mathbb{C}[X,Y].$$

Proof. The subsequent proof of Theorem 4.3 relies heavily on the properties of $\wp$ and $\wp'$ from Section 1.2.

i) *Equation of $\phi(T)$*: The differential equation of the Weierstrass function $\wp$

$$(\wp')^2 = \wp^3 - g_2 \cdot \wp - g_3$$

implies

$$\phi(T \setminus \{0\}) \subset E_{aff} := \{(x,y) \in \mathbb{C}^2 :\ y^2 = 4 \cdot x^3 - g_2 \cdot x - g_3\}$$

The closure of the affine algebraic set

$$E_{aff} \subset \mathbb{C}^2 \subset \mathbb{P}^2$$

is the projective algebraic variety $E \subset \mathbb{P}^2$, see Figure 4.1, the zero set in $\mathbb{P}^2$ of

$$F_{hom}(X_0, X_1, X_2),$$

cf. [29, Chap. I, Exerc. 2.9].

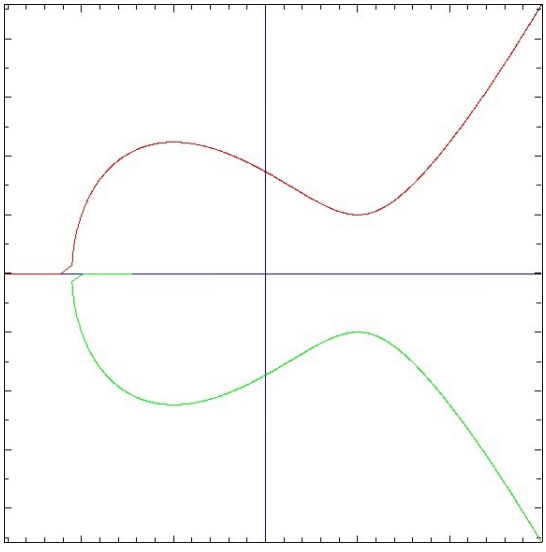


Fig. 4.1 Real points of E_{aff}

ii) *Holomorphy of* ϕ: To check holomorphy in a neighbourhood of $0 \in T$ we choose an open neighbourhood $U \subset T$ of the origin such that $\wp'$ has no zeros in U. On

$$U^* := U \setminus 0$$

one obtains by diving the homogeneous coordinate by $\wp'$

$$\phi|U^* = (1 : \wp : \wp') = (1/\wp' : \wp/\wp' : 1),$$

which converges with limit

$$\lim_{z \to 0} \phi(z) = (0 : 0 : 1) := O \in \mathbb{P}^2$$

because $\wp$ and $\wp'$ have poles at 0 of order respectively $= 2$ and 3. Hence $0 \in T$ is a removable singularity of ϕ.

iii) *Injectivity of* ϕ: The holomorphic map

$$\wp : T \to \mathbb{P}^1$$

is a branched covering of degree $= 2$, while the holomorphic map

$$\wp' : T \to \mathbb{P}^1$$

is a branched covering of degree $= 3$. To give an indirect proof of the injectivity of ϕ assume two distinct points

$$z \neq w \in T \setminus \{0\}$$

with

$$(\wp(z), \wp'(z)) = (\wp(w), \wp'(w)) \in \mathbb{C}^2.$$

Then

$$\wp(z) = \wp(w) \text{ implies } w = -z$$

due to Corollary 1.10 and because $\wp$ is an even function due to Theorem 1.12. Moreover

$$\wp'(z) = \wp'(w) = \wp'(-z) = -\wp'(z) \text{ implies } \wp'(z) = 0.$$

Lemma 1.13 implies that

$$z = [\omega/2],\ \omega \in \Lambda \text{ and } w = -z \in T$$

are two distinct classes of half-period points of Λ. But $\wp$ attains at z the value $\wp(z)$ with multiplicity $= 2$, hence $\wp$ assumes the value $\wp(z) = \wp(w)$ with multiplicity ≥ 4, a contradiction.

iv) *The image of* ϕ: The only non-affine point is

$$E \setminus E_{aff} = O = \phi(0).$$

Consider an affine point

$$(1 : x : y) \in E.$$

The $\wp$-function is a non-constant holomorphic map

$$\wp : T \to \mathbb{P}^1,$$

in particular it is surjective: There exists $z \in T$ with

$$\wp(z) = x.$$

The function $\wp$ is even, therefore also

$$\wp(-z) = x.$$

From

$$y^2 = 4x^3 - g_2 \cdot x - g_3 = 4\wp(z)^3 - g_2 \cdot \wp(z) - g_3 = \wp'(z)^2$$

follows:

- Either
$$y = \wp'(z) \text{ and } \phi(z) = (1 : x : y).$$
- Or
$$y = -\wp'(z) = \wp'(-z) \text{ and } \phi(-z) = (1 : x : y)$$

v) *Smoothness of E*:

- A point $(x_0, y_0) \in \mathbb{C}^2$ is a singular point of E_{aff} iff it satisfies the three equations

$$0 = F(x_0, y_0) = y_0^2 - (4x_0^3 - Ax_0 - B),\ A := g_2,\ B := g_3,$$

$$\frac{\partial F}{\partial y}(x_0, y_0) = 2y_0 = 0 \text{ and } \frac{\partial F}{\partial x}(x_0, y_0) = -12x_0^2 + A = 0$$

  Introducing the cubic poynomial

$$f(x) := 4x^3 - Ax - B \in \mathbb{C}[x]$$

  the condition is equivalent to

$$f(x_0) = 0 \text{ and } f'(x_0) = 0.$$

  The latter condition is equivalent to x_0 being a multiple zero of f, i.e. to the vanishing of the discriminant of f

$$\Delta_f = A^3 - 27B^2.$$

  Proposition 1.19 implies $\Delta_f \neq 0$.

- To prove the non-singularity of E at the point $O = (0:0:1) \in \mathbb{P}^2$ we consider the standard coordinate of $\mathbb{P}^2$ around the point O

$$\phi_2 : U_2 \to \mathbb{C}^2,\ (z_0 : z_1 : z_2) \mapsto (u, \mathrm{v}) := \left(\frac{z_0}{z_2},\ \frac{z_1}{z_2}\right).$$

  We have

$$\phi_2(E \cap U_2) = \{(u, \mathrm{v}) \in \mathbb{C}^2 :\ f(u, \mathrm{v}) = 0\}$$

  with

$$f(u, \mathrm{v}) := u - (4 \cdot \mathrm{v}^3 - A \cdot u^2 \cdot \mathrm{v} - B \cdot u^3).$$

  Then the partial derivatives are

$$\frac{\partial f}{\partial u}(u, \mathrm{v}) = 1 - (2 \cdot A \cdot u \cdot \mathrm{v} - 3 \cdot B \cdot u^2) \text{ and } \frac{\partial f}{\partial \mathrm{v}}(u, \mathrm{v}) = -12 \cdot \mathrm{v}^2 + A \cdot u^2$$

  hence

$$\nabla f(0,0) = (1,0) \neq 0.$$

  The non-singular projective algebraic curve $E = \phi(T) \subset \mathbb{P}^2$ is connected, hence a compact Riemann surface with the induced analytic structure as a hypersurface of $\mathbb{P}^2$.

vi) *Biholomorphy*: The map

$$\phi : T \to E$$

between Riemann surfaces is a bijective holomorphic map, hence it is biholomorphic, q.e.d.

Example 4.4 (Embedding tori as plane cubics). The PARI script `Torus_to_Weierstrass_equation_01` computes a cubic equation in $\mathbb{P}^2$ for a given torus $T = \mathbb{C}/\Lambda$, see Figure 4.2. Real values are approximated by rationals.

```
=====================================================
Torus_to_Weierstrass_equation_01, Start

Lattice (omega_1,omega_2) = (I,1), modular invariant (rat. appr.) j = 1728

lattice_base = [1, I]

(g_2, g_3) = (189.0727201, 0.00000000000000000000000000000000001841656774), rat. approx. = (10399/55, 0)

Cubic (rat. approx.): Y^2 = 4*X^3-(10399/55)*X - (0), discriminant = 216290077/32

-----------------------------------------------------------

Lattice (omega_1,omega_2) = (-1/2 + 0.8660254038*I,1), modular invariant (rat. appr.) j = 0

lattice_base = [1, -1/2 + 0.8660254038*I]

(g_2, g_3) = (0.0000000000, 820.8244371), rat. approx. = (0, 46787/57)

Cubic (rat. approx.): Y^2 = 4*X^3-(0)*X - (46787/57), discriminant = -421083/19

-----------------------------------------------------------

Torus_to_Weierstrass_equation_01, End
=====================================================
```

Fig. 4.2 Embedding tori as plane cubics

The embedding result of Theorem 4.3 is a particular case of the general question: How to obtain holomorphic maps

$$X \to \mathbb{P}^n$$

with X a compact a complex manifold X?

The underlying construction is even more general. It is not restricted to complex analysis. Section 4.2 deals with an example from algebraic geometry. The present section recalls the general construction in the context of compact Riemann surfaces X, see also [63]. The pivotal objects are the twisted line bundle on $\mathbb{P}^n$ and very ample line bundles on X. In the following we shall not distinguish between a line bundle and the invertible sheaf of its holomorphic sections. We shall employ in both cases the same notation

$$\mathscr{L} \in Pic(X).$$

Definition 4.5 (The twisted line bundle on $\mathbb{P}^n$). The *twisted line bundle* $\mathscr{O}(1)$ on $\mathbb{P}^n$ is defined with respect to the standard atlas of $\mathbb{P}^n$ by the cocycle

$$g = (g_{ij}) \in Z^1(\mathscr{U}, \mathscr{O}^*)$$

with

$$g_{ij}(z_0 : \ldots : z_n) := \frac{z_j}{z_i},\ 0 \leq i \neq j \leq n.$$

Proposition 4.6 (Sections of $\mathscr{O}(1)$). *The sections of $\mathscr{O}(1)$ on $\mathbb{P}^n$ correspond bijectively to the linear polynomials $HPol(1) \subset \mathbb{C}[z_0, \ldots, z_n]$, i.e. the map*

$$HPol(1) \to H^0(\mathbb{P}^n, \mathscr{O}(1)),\ z_k \mapsto s_k,\ k = 0, \ldots, n.$$

Here $s_k \in H^0(\mathbb{P}^n, \mathscr{O}(1))$ is defined with respect to the i-th standard chart by the holomorphic functions

$$s_{k,i} : U_i \to \mathbb{C},\ s_{k,i}(z_0 : \ldots : z_n) := \frac{z_k}{z_i}$$

Proof. The map defined above on the standard charts provide a section

$$s_k := (s_{k,i})_{i=0,\ldots,n} \in H^0(\mathbb{P}^n, \mathscr{O}(1))$$

because

$$g_{ij} \cdot s_{k,j} = \frac{z_j}{z_i} \cdot \frac{z_k}{z_j} = \frac{z_k}{z_i} = s_{k,i},\ q.e.d.$$

Proposition 4.6 generalizes to sections of the tensor powers

$$\mathscr{O}(k) := \mathscr{O}(1)^{\otimes k},\ k \in \mathbb{N},$$

cf. also [63].

In order that a line bundle $\mathscr{L}$ on a Riemann surface X defines a holomorphic map

$$\phi_{\mathscr{L}} : X \to \mathbb{P}^n$$

to a projective space, the line bundle $\mathscr{L}$ has to be *globally generated*.

Definition 4.7 (Base-point, globally generated line bundle). Consider a Riemann surface X and a line bundle $\mathscr{L}$ on X.

1. A point $x \in X$ is a *base-point* of $\mathscr{L}$ if each section $\sigma \in H^0(X, \mathscr{L})$ satisfies $\sigma(x) = 0$. Note
$$\sigma(x) = 0 \iff \sigma_x \in \mathfrak{m}_x \mathscr{L}_x$$
with $\mathscr{L}_x$ the stalk of $\mathscr{L}$ at $x \in X$ and
$$\mathfrak{m}_x \subset \mathscr{O}_x$$
the maximal ideal of the stalk $\mathscr{O}_x$ of the structure sheaf at $x \in X$.

2. The line bundle is *globally generated* or *base-point-free* if it has no base-points, i.e. if for each $x \in X$ exists a section $\sigma \in H^0(X, \mathscr{L})$ such that the germ $\sigma_x \in \mathscr{L}_x$ generates the stalk $\mathscr{L}_x$ as $\mathscr{O}_x$-module. The latter condition is equivalent to $\sigma(x) \neq 0$.

Proposition 4.8 (Holomorphic maps to projective spaces). *Consider a compact Riemann surface X and a globally generated line bundle $\mathscr{L}$ on X. After choosing a basis*
$$(\sigma_i)_{i=0,\ldots,n} \in H^0(X, \mathscr{L})$$
the map
$$\phi_{\mathscr{L}} : X \to \mathbb{P}^n,\ x \mapsto (\sigma_0(x) : \ldots : \sigma_n(x)),$$
is well-defined, independent from the chosen trivialization of $\mathscr{L}$ in a neighbourhood of $x \in X$, and holomorphic. It induces an isomorphism
$$\phi_{\mathscr{L}}^*(\mathscr{O}(1)) \simeq \mathscr{L}$$
with $\phi_{\mathscr{L}}^*(\mathscr{O}(1))$ the pull-back of the twisted line bundle.

Proof. We set
$$\phi := \phi_{\mathscr{L}}.$$
i) *Definition*: We consider the definition of ϕ in a suitable open neighbourhood U of x. On U we choose a trivialization to identify the line bundle $\mathscr{L}$ with the structure sheaf $\mathscr{O}$. Hence sections from $H^0(U, \mathscr{L})$ become holomorphic functions. Because $\mathscr{L}$ is globally generated there is an index $j \in \{0, \ldots, n\}$ with
$$\sigma_j(x) \neq 0.$$
Hence the point
$$(\sigma_0(x) : \ldots : \sigma_n(x)) \in \mathbb{P}^n$$
is well-defined. It is independent of the choice of the chart and of the isomorphism
$$\mathscr{L}|U \simeq \mathscr{O}|U.$$
Apparently the map ϕ is holomorphic on U.

ii) *Pullback of the twisted line bundle*: For each $i = 0, ..., n$ the sets

$$X_i := \phi^{-1}(U_i) = \{x \in X : \ (\sigma_i)_x \notin \mathfrak{m}_x \mathscr{L}_x\}$$

form an open covering $(X_i)_{i=0,...,n}$ of X because $\mathscr{L}$ is globally generated.
For $i = 0, ..., n$ the canonical morphisms between the rings of local sections

$$\mathscr{O}(1)(U_i) \to \phi_*(\mathscr{L})(U_i) = \mathscr{L}(X_i) \text{ induced by } s_i|U_i \mapsto \sigma_i|X_i$$

define a canonical sheaf morphism on $\mathbb{P}^n$

$$\mathscr{O}(1) \to \phi_* \mathscr{L}$$

The latter corresponds to a sheaf morphism on X

$$\phi^*(\mathscr{O}(1)) \to \mathscr{L},$$

because the two functors ϕ^* and ϕ_* are adjoint, see [29, Chap. II, § 5], i.e. there is a canonical group isomorphim

$$Hom_{\mathscr{O}_X}(\phi^*(\mathscr{O}(1)), \mathscr{L}) \simeq Hom_{\mathscr{O}_{\mathbb{P}^n}}(\mathscr{O}(1), \phi_* \mathscr{L})$$

The induced morphism

$$\phi^*(\mathscr{O}(1)) \to \mathscr{L}$$

between the two line bundles is an isomorphism because it is an isomorphism on stalks: If for a given $i \in \{0, ..., n\}$

$$x \in X_i \subset X \text{ and } y := \phi(x) \in U_i \subset \mathbb{P}^n$$

then according to the definition of the analytic inverse image sheaf

$$(\phi^* \mathscr{O}(1))_x = \mathscr{O}(1)_y \otimes_{\mathscr{O}_{\mathbb{P}^n, y}} \mathscr{O}_{X,x} \to \mathscr{L}_x, \ (s_i)_y \otimes 1 \mapsto (\sigma_i)_x, \ q.e.d.$$

Theorem 4.9 provides a geometric criterion for the map provided by a globally generated line bundle $\mathscr{L}$ to be a closed embedding.

Theorem 4.9 (Projective embedding induced by a line bundle). *Consider a compact Riemann surface X and a globally generated line bundle $\mathscr{L}$ on X. Then the induced map*

$$\phi_{\mathscr{L}} : X \to \mathbb{P}^n$$

is a holomorphic closed embedding iff $\mathscr{L}$ satisfies both of the following properties:

1. Separating points*: For any two distinct points $p \neq q \in X$ exists a section*

$$\sigma \in H^0(X, \mathscr{L}) \text{ with } \sigma(p) \neq 0 \text{ but } \sigma(q) = 0$$

or vice versa.

2. Separating tangent vectors*: For all $x \in X$ the map*

$$d_{\mathscr{L},x} : \{\sigma \in H^0(X,\mathscr{L}) : \ \sigma_x \in \mathfrak{m}_x\mathscr{L}_x\} \to \mathfrak{m}_x\mathscr{L}_x/\mathfrak{m}_x^2\mathscr{L}_x, \ \sigma \mapsto [\sigma_x],$$

is surjective.

For the proof of Theorem 4.9 see [63].

Remark 4.10 (Separating points and tangent vectors). We explain the meaning of the two statements from Theorem 4.9.

1. *Separating points*: The homogeneous coordinates of a given point in $\mathbb{P}^n$ do not fix the value of the components. But it is determined whether a component is zero or not zero. Therefore for each pair of points $p \neq q \in X$

$$\phi_{\mathscr{L}}(p) \neq \phi_{\mathscr{L}}(q)$$

if at least one component of the left-hand side is different from zero while the same component on the right-hand side is zero.

2. *Separating tangent vectors*: A holomorphic mapping is an embedding in the neighbourhood of a point $x \in X$ if the Jacobi map at x does not vanish. The latter condition is equivalent to the fact that at x the push-forward of tangent vectors is injective, equivalently the pull-back of cotangent vectors is surjective: We consider the isomorphy of $\mathscr{O}_x$-modules - respectively of complex vector spaces -

$$\mathfrak{m}_x\mathscr{L}_x/\mathfrak{m}_x^2\mathscr{L}_x \simeq (\mathfrak{m}_x/\mathfrak{m}_x^2) \otimes_{\mathscr{O}_x} \mathscr{L}_x = T_x^1 \otimes_{\mathscr{O}_x} \mathscr{L}_x$$

with the cotangent space

$$T_x^1 := \mathfrak{m}_x/\mathfrak{m}_x^2$$

of X at x. Then the map

$$d_{\mathscr{L},x} : \{\sigma \in H^0(X,\mathscr{L}) : \ \sigma_x \in \mathfrak{m}_x\mathscr{L}_x\} \to T_x^1 \otimes_{\mathscr{O}_x} \mathscr{L}_x$$

is induced by the total differential d_x of holomorphic functions: A section

$$\sigma \in H^0(X,\mathscr{L}) \text{ with } \sigma_x \in \mathfrak{m}_x\mathscr{L}_x$$

factorizes in a suitable neighbourhood U of x as

$$\sigma = f \cdot \sigma_1$$

with a holomorphic function $f \in \mathscr{O}(U)$ satisfying $f_x \in \mathfrak{m}_x$ and a holomorphic section $\sigma_1 \in \mathscr{L}(U)$. Then

$$d_{\mathscr{L},x}(\sigma) = d_x f \otimes \sigma_1 \in T_x^1 \otimes_{\mathscr{O}_x} \mathscr{L}_x$$

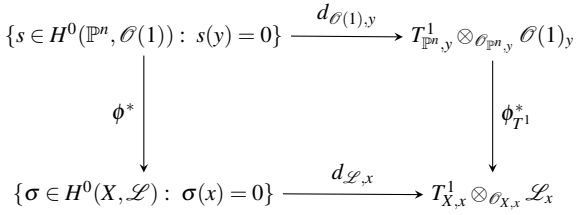


Fig. 4.3 Separating tangent vectors

The commutative diagram from Figure 4.3 with

$$y := \phi(x)$$

and surjective maps

$$d_{\mathcal{O}(1),y} \text{ and } \phi^*$$

shows: The pull-back $\phi^*_{T^1}$ is surjective if and only if $d_{\mathscr{L},x}$ is surjective.

Definition 4.11 (Very ample line bundle). A globally generated line bundle $\mathscr{L}$ on a compact Riemann surface X is *very ample* if the induced map

$$\phi_{\mathscr{L}} : X \to \mathbb{P}^n$$

is an embedding.

A globally generated line bundle $\mathscr{L}$ on X has enough sections to define a holomorphic map

$$\phi_{\mathscr{L}} : X \to \mathbb{P}^n.$$

If $\mathscr{L}$ is very ample then there are enough sections that $\phi_{\mathscr{L}}$ is even an embedding. Due to the compactness of X its image under an embedding is always closed.

Notation 4.12. *For a line bundle $\mathscr{L}$ on a Riemann surface X and a divisor $D \in Div(X)$ we denote by*

$$\mathscr{L}_D := \mathscr{L} \otimes_{\mathcal{O}} \mathcal{O}_D$$

the sheaf of meromorphic sections of $\mathscr{L}$ which are multiples of the divisor $-D$. The sheaf $\mathscr{L}_D$ is isomorphic to a line bundle.

Consider a line bundle $\mathscr{L}$ on a compact Riemann surface X. Theorem 4.13 states a numerical criterion for the dimension of the vector spaces

$$H^0(X,\mathscr{L}_D),\ D \in Div(X),$$

which ensures that the map

$$\phi_{\mathscr{L}} : X \to \mathbb{P}^n$$

is well-defined and a closed embedding. This criterion is very helpful in the applications because the dimension on the vector spaces in question can often be computed by using the theorem of Riemann-Roch in combination with Serre duality.

Theorem 4.13 (Very-ampleness criterion). *Consider a compact Riemann surface X. For a line bundle $\mathscr{L}$ on X are equivalent:*

- *The line bundle $\mathscr{L}$ is very ample.*
- *For any two not necessarily distinct points $p,\ q \in X$ the corresponding point divisors*

$$P := 1 \cdot p,\ Q := 1 \cdot q \in Div(X)$$

satisfy

$$dim\ H^0(X,\mathscr{L}_{-(P+Q)}) = dim\ H^0(X,\mathscr{L}) - 2.$$

Proof. i) *Assume the validity of the dimension formula*: The formula implies for any two point divisors $P,\ Q \in Div(X)$

$$H^0(X,\mathscr{L}_{-(P+Q)}) \subsetneq H^0(X,\mathscr{L}_{-P}) \subsetneq H^0(X,\mathscr{L})$$

and each proper inclusion has codimension $= 1$ because it is defined by a single linear equation.

- The equation

$$h^0(X,\mathscr{L}_{-P}) = h^0(X,\mathscr{L}) - 1.$$

states that the kernel of the evaluation

$$H^0(X,\mathscr{L}) \to \mathscr{L}_p/\mathfrak{m}_p\mathscr{L}_p \simeq \mathbb{C},\ \sigma \mapsto [\sigma_p],$$

has codimension $= 1$. Hence p is not a base-point of $\mathscr{L}$. As a consequence, the line bundle $\mathscr{L}$ is globally generated and

$$\phi_{\mathscr{L}} : X \to \mathbb{P}^n$$

is well-defined.

- The equation

$$H^0(X,\mathscr{L}_{-(P+Q)}) \subsetneq H^0(X,\mathscr{L}_{-P})$$

implies that for any pair of distinct points $p,\ q \in X$ there exists a section

$$\sigma \in H^0(X,\mathscr{L}_{-P}) \setminus H^0(X,\mathscr{L}_{-(P+Q)})$$

i.e. satisfying

$$\sigma(p) = 0 \text{ but } \sigma(q) \neq 0.$$

Hence the sheaf $\mathscr{L}$ separates points.

- The dimension formula shows for any point $p \in X$ with point divisor $P \in Div(X)$

$$H^0(X, \mathscr{L}_{-2P}) \subsetneq H^0(X, \mathscr{L}_{-P})$$

has codimension $= 1$. Hence there exists a section

$$\sigma \in H^0(X, \mathscr{L}_{-P}) \setminus H^0(X, \mathscr{L}_{-2P})$$

which implies the surjectivity of the composition of the canonical maps

$$H^0(X, \mathscr{L}_{-P}) \to \mathfrak{m}_{X,p}\mathscr{L}_p \to \mathfrak{m}_{X,p}\mathscr{L}_p / \mathfrak{m}^2_{X,p}\mathscr{L}_p$$

due to

$$dim_{\mathbb{C}}(\mathfrak{m}_{X,p}/\mathfrak{m}^2_{X,p}) = 1.$$

Therefore $\mathscr{L}$ separates tangent vectors.

ii) *Assume $\mathscr{L}$ very ample*: Theorem 4.9 implies that $\mathscr{L}$ separates points and tangent vectors. Separating points implies for all point divisors $P \neq Q \in Div(X)$

$$dim\, H^0(X, \mathscr{L}_{-(P+Q)}) = dim\, H^0(X, \mathscr{L}) - 2.$$

Separating tangent vectors implies for each point divisor $P \in Div(X)$

$$dim\, H^0(X, \mathscr{L}_{-2P}) = dim\, H^0(X, \mathscr{L}) - 2,\ q.e.d.$$

Remark 4.14 (Projective embedding of compact Riemann surfaces). As a consequence of the very-ampleness criterion from Theorem 4.13 one can prove: Each compact Riemann surface X embeds holomorphically into a projective space.

1. If $g(X) \geq 2$ then the tri-canonical line bundle $\Omega^{\otimes 3} \in Pic(X)$ is very ample, see [63].

2. For a complex torus $X = \mathbb{C}/\Lambda$ holds $\Omega \simeq \mathscr{O}$, hence

$$g(X) := dim\, H^0(X, \Omega) = 1$$

Consider the divisor

$$D := 3 \cdot 0 \in Div(X)$$

with the point $0 \in X$ being the origin. Then the line bundle

$$\mathscr{L} := \mathscr{O}_D \in Pic(X)$$

is very ample according to Theorem 4.13: As a consequence of $\Omega \simeq \mathscr{O}$, for two point divisors

$$P = 1 \cdot p,\ Q = 1 \cdot q \in Div(X)$$

holds

$$dim\, H^1(X, \mathscr{L}_{-(P+Q)}) = dim\, H^0(X, \mathscr{O}_{-D+(P+Q)}) = 0$$

because

$$deg\ (-D + (P+Q)) = -3 + 2 = -1 < 0$$

Hence

$$dim\, H^0\left(X, \mathscr{L}_{-(P+Q)}\right) = 1 - g(X) + deg\ \mathscr{L} - 2 = dim\, H^0(X, \mathscr{L}) - 2$$

The Riemann-Roch theorem implies

$$dim\, H^0(X, \mathscr{L}) = dim\, H^0(X, \mathscr{O}_D) = deg\ D = 3$$

Apparently, a basis of $H^0(X, \mathscr{O}_D)$ is the family of linearly independent elements

$$(1, \wp, \wp')$$

which gives a second proof for the embedding from Theorem 4.3.

4.2 Elliptic curves over subfields of $\mathbb{C}$

Complex Analysis of several variables or Complex Analytic Geometry on one hand, and on the other hand Algebraic Geometry are mathematical theories with many concepts in common and also several concepts in parallel. We compile the following GAGA-dictionary (Géométrie Algébrique et Géométrie Analytique).

Proposition 4.15 (Dictionary: Complex Analytic Geometry - Algebraic Geometry).

Complex Analytic Geometry	***Algebraic Geometry***
Complex Manifold	*Smooth variety*
Euclidean topology	*Zariski topology*
Compact complex manifold	*Smooth projective algebraic variety*
Compact Riemann surface	*Projective algebraic curve*
Genus	
Stein manifold	*Smooth affine variety*
Structure sheaf $\mathcal{O}_X$	
Holomorphic function	*Regular function*
Meromorphic function	*Rational function*
Local ring $\mathcal{O}_{X,x}$	
Line bundle	
Very ampleness	
Divisor	
Sheaf Ω_X *of differential forms*	
Cohomology	
Riemann-Roch Theorem	
Serre Duality	

The table relates concepts from complex analytix geometry on the left-hand side with concepts from algebraic geometry on the right-hand side. But not any compact manifold, and not even any compact Kaehler manifold has a counter part in Algebraic Geometry. Hence not any instance of a concept on the left-hand side of the table induces a correponding instance on the right-hand side. On both sides there are objects which cannot be studied by methods from the other side.

In Algebraic Geometry a variety is assumed to be irreducible. *Irreducibility* corresponds to *connectedness* in the case of manifolds. If one skips the requirement of smoothness one obtains the irreducible reduced complex space as the analogue of a variety.

Remark 4.16 recalls varieties as the basic objects of classical algebraic geometry. Varieties are irreducible by definition, hence they are defined by prime ideals. But different from manifolds varieties may have singularities. Hence varieties are the analogue of reduced and irreducible complex spaces. We distinguish between their field k of definition and the algebraic closure $\overline{k}$ where the points of the variety have their coordinates. As a topological space varieties will be equipped with the Zariski topology.

Recall that a field k is *perfect* if each irreducible polynomial with coefficients from k is separable, i.e has pairwise distinct roots in an algebraic closure $\overline{k}$. All fields in the present section will be assumed perfect. The relevant examples of perfect fields are the fields k of characteristic $= 0$ or the finite fields $k = \mathbb{F}_p$ of prime characteristic $= p$.

Remark 4.16 (Algebraic variety with structure sheaf). Consider a perfect field k and denote by $\overline{k}$ the algebraic closure of k.

1. *Variety*: An *affine algebraic variety* X is the zero set

$$X = V(\mathfrak{a}) \subset \mathbb{A}^n(\overline{k}) = \overline{k}^n$$

of a prime ideal $\mathfrak{a} \subset \overline{k}[X_1, ..., X_n]$, i.e.

$$X := \{x \in \mathbb{A}^n(\overline{k}) : \ f(x) = 0 \text{ for all } f \in \mathfrak{a}\}.$$

The ring

$$R := \overline{k}[X_1, ..., X_n]/\mathfrak{a}$$

is the *affine coordinate ring* of X.

If $\mathfrak{a}$ can be generated by polynomials from $k[X_1, ..., X_n]$, then X is *defined over* k, denoted X/k. The smallest subfield of $\overline{k}$ with this property is named the *field of definition* of X.

2. A *projective algebraic variety* X is the zero set

$$X = V(\mathfrak{a}) \subset \mathbb{P}^n(\overline{k})$$

of a prime ideal

$$\mathfrak{a} \subset \overline{k}[X_0, ..., X_n],$$

generated by homogeneous polynomials, i.e.

$$X := \{(x = (x_0 : ... : x_n) \in \mathbb{P}^n(\bar{k}) : f(x) = 0 \text{ for all homogeneous } f \in \mathfrak{a}\}.$$

3. *Zariski topology*: Closed sets of $\mathbb{A}^n(\bar{k})$ are the affine algebraic subvarieties and their finite unions. The *Zariski topology* on an affine algebraic variety $X \subset \mathbb{A}^n(\bar{k})$ is the subspace topology induced from the Zariski topology of $\mathbb{A}^n(\bar{k})$. A basis of the Zariski topology of X are the sets

$$D_h := \{x \in X : \ h(x) \neq 0\}, \ h \in R.$$

Closed sets of $\mathbb{P}^n(\bar{k})$ are the projective algebraic subvarieties. The *Zariski topology* on a projective algebraic variety $X \subset \mathbb{P}^n(\bar{k})$ is the subspace topology induced from the Zariski topology of $\mathbb{P}^n(\bar{k})$.

Non-empty open subsets of an irreducible space are irreducible itself, and are also dense.

4. *Structure sheaf and sheaf of rational functions*: Consider an affine algebraic variety X and an open set $U \subset X$. A function

$$f : U \to \bar{k}$$

is *regular* if it has locally the form

$$f = \frac{g}{h} \text{ with } g, h \in R, \ h \text{ locally without zeros in } X.$$

Note that the quotient representation of f is only required to hold locally. The sheaf $\mathscr{O}_X$ of *regular functions* on an affine algebraic variety X is the contravariant functor

$$U \mapsto \mathscr{O}_X(U) := \{f : U \to \bar{k} | \ f \text{ regular } \}, \ U \subset X \text{ open},$$

with the restriction of functions. The sheaf $\mathscr{O}_X$ is named the *structure sheaf* of X. Sections over a basis open set $D_h \subset X$ form the ring

$$\mathscr{O}(D_h) = R_h := \{g/h^n : \ g \in R, \ n \in \mathbb{N}\}$$

Because the ideal

$$\mathfrak{a} \subset \bar{k}[X_1, ..., X_n]$$

is prime, the quotient R and all rings

$$\mathscr{O}_X(U), \ U \subset X \text{ open},$$

are integral domains. The sheaf $\mathscr{M}_X$ of *rational functions* on X is the sheafification of the presheaf

$$U \mapsto Q(\mathscr{O}_X(U)), \ U \subset X \text{ open},$$

with $Q(\mathscr{O}_X(U))$ the quotient field of the integral domain $\mathscr{O}_X(U)$. Sections of $\mathscr{M}_X(U)$ are locally quotients

$$g/h,\ g,\ h \in R,\ h \neq 0.$$

For a non-empty open set $U \subset X$ holds

$$\mathscr{M}(U) = Q(R) =: \overline{k}(X),$$

independent from U. The field $Q(R)$ is named the *function field* $\overline{k}(X)$ of X. The sheaf

$$\mathscr{M}^* \subset \mathscr{M}$$

is the multiplicative subsheaf of non-zero rational functions.

The definitions carry over to projective algebraic varieties, beaucse the latter have an atlas of affine algebraic varieties.

5. *Non-singularity*: Consider an algebraic variety X and a point $x \in X$. The local ring $\mathscr{O}_{X,x}$ at $x \in X$ is the ring of germs of regular functions defined in a neighbourhood of $x \in X$. Its dimension defines the dimension of X at $x \in X$.

   The variety X is *non-singular* or *smooth* at $x \in X$ if $\mathscr{O}_{X,x}$ is a *regular* local ring, i.e. if

   $$dim\ \mathscr{O}_{X,x} = dim_{\kappa(x)}\ (\mathfrak{m}_x/\mathfrak{m}_x{}^2)$$ (Dimension equals cotangent dimension).

   Here

   $$\kappa(x) := \mathscr{O}_{X,x}/\mathfrak{m}_x$$

   denotes the residue field of X at x.

6. *Curve over k*: A projective algebraic *curve* C/k is a 1-dimensional, non-singular projective algebraic variety defined over the field k. If

   $$C \subset \mathbb{P}^2(\overline{k})$$

   then C/k is a *plane projective algebraic curve*. Its *genus* is defined as

   $$g(C) = dim_{\overline{k}}\, H^0(C, \Omega),$$

   the dimension of the $\overline{k}$-vector space of *regular differential forms*.

7. *Affine schemes*: From a modern viewpoint the primary property of a variety is not the point set

   $$X \subset \mathbb{A}^n(\overline{k}),$$

   the primary object is the ideal

   $$\mathfrak{a} \subset k[X_1, ..., X_n]$$

with minimal field of definition k, or its quotient, the ring

$$R := k[X_1, ..., X_n]/\mathfrak{a}$$

Due to Grothendieck's reformulation of algebraic geometry, the basic concept is for arbitrary rings R the *affine scheme*

$$(X := Spec\ R, \mathscr{O}_X)$$

Here $Spec\ R$ is a topological space with points the prime ideals of R. The structure sheaf $\mathscr{O}_X$ has as stalks the localizations

$$R_{\mathfrak{p}},\ \mathfrak{p} \subset R \text{ prime ideal.}$$

We have included the requirement of non-singularity into our definition of a projective algebraic curve because all curves under consideration will be assumed smooth if not stated otherwise. Note that any plane projective algebraic curve is defined by a single homogeneous polynomial. Its degree is the *degree* of C/k.

Remark 4.16 for X/k involves two fields:

- First, the field of definition k is not necessarily algebraically closed. It is the minimal field where the coefficients of a set of generators of $I(X)$ may be taken from.
- Secondly, the algebraically closed field $\bar{k}$, used to visualize K/k as a point set X from a geometrical view point. Also the condition on smoothness refers to $\bar{k}$.

But the set $X \subset \mathbb{A}^n(\bar{k})$ respectively $X \subset \mathbb{P}^n(\bar{k})$ is not the only point set attached to K/k. Definition 4.17 introduces point sets $X(K)$ attached to all intermediate fields $k \subset K \subset \bar{k}$.

Definition 4.17 (K-valued point pf X/k). Consider a projective algebraic variety X/k with

$$X \subset \mathbb{P}^n(\bar{k}).$$

Then for any field

$$k \subset K$$

the set of *K-valued points* of X is defined as

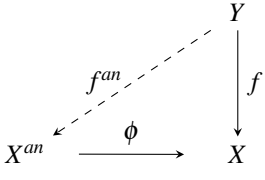
$$X(K) := X \cap \mathbb{P}^n(K) =$$

$$= \{x = (x_0 : ... : x_n) \in \mathbb{P}^n(\overline{k}) : x \in X \text{ and } x_i \in K \text{ for all } i = 0, ..., n\}.$$

Remark 4.18 (GAGA).

1. *Chow's theorem*: Historically, the first GAGA-result is Chow's theorem: Any projective complex analytic manifold $X \subset \mathbb{P}^n$ is the variety of homogeneous polynomials, i.e. if $X \subset \mathbb{P}^n$ is locally defined as the zero set of holomorphic functions, then X can be globally defined by homogenous polynomials.

2. *Analytification of schemes*: To formalize the analogy between complex analytic geometry and complex algebraic geometry Grothendieck uses the language of category theory. On one hand, let $\underline{An}_{\mathbb{C}}$ denote the category of complex spaces and holomorphic maps. On the other hand, let $\underline{Al}_{\mathbb{C}}$ denote the category of schemes of finite type defined over $\mathbb{C}$ and regular maps. The first step attaches to a schema $X \in \underline{Al}_{\mathbb{C}}$ a distinguished complex analytic space $X^{an} \in \underline{An}_{\mathbb{C}}$. The latter is obtained via the functor:
$$\Phi : \underline{An}_{\mathbb{C}} \to \underline{Ens}$$
attaching to a complex analytic space Y the set
$$\Phi(Y) := Hom_{\mathbb{C}}(Y, X)$$
of morphisms of ringed spaces. The functor Φ can be represented by a universal object (X^{an}, ϕ), named the *analytification* of X. The pair comprises a complex analytic space X^{an} and a morphism
$$\phi : X^{an} \to X,$$
see [46]. As a consequence: For a given complex analytic space Y each morphism
$$f : Y \to X$$
of ringed spaces induces a unique holomorphic map
$$f^{an} : Y \to X^{an},$$
such that the following diagram commutes



The analytification $\phi : X^{an} \to X$ from the analytification defines for each $x \in X^{an}$ a pull-back

$$\phi_x : \mathscr{O}_{X,\phi(x)} \to \mathscr{O}_{X^{an},x}$$

which allows to compare the local ring of *regular* functions on X and the local ring of *holomorphic* functions on X^{an}. As a consequence one obtains comparison theorems between the algebraic properties of the local rings of the structure sheaves of X and X^{an}, see [46, Chap. 2].

In addition, any morphism $f : X \to Y$ in $\underline{An}_{\mathbb{C}}$ induces a unique holomorphic map

$$f^{an} : X^{an} \to Y^{an}$$

such that the following diagram commutes

$$\begin{array}{ccc} X^{an} & \xrightarrow{\phi_X} & X \\ {\scriptstyle f^{an}}\big\downarrow & & \big\downarrow{\scriptstyle f} \\ Y^{an} & \xrightarrow{\phi_Y} & Y \end{array}$$

Again, one obtains comparison theorems between the algebraic properties of the morphisms

$$f : X \to Y \text{ and } f^{an} : X^{an} \to Y^{an},$$

see [46, Chap. 3].

3. *Coherent sheaves and proper maps*: The morphism

$$\phi : X \to X^{an}$$

from the analytification of X defines the functor *analytical inverse image* as the pull-back of module sheaves over the structure sheaf:

$$\phi^* : \underline{Sheaf}_{\mathscr{O}_X} \to \underline{Sheaf}_{\mathscr{O}_{X^{an}}},\ \mathscr{F} \mapsto \phi^*\mathscr{F}$$

and

$$f : \mathscr{F} \to \mathscr{G}, \mapsto \phi^* f : \phi^* F \to \phi^* \mathscr{G}.$$

The stalk at a point $x \in X^{an}$ of the inverse image sheaf is easy to calculate

$$(\phi^*\mathscr{F})_x = \mathscr{F}_{\phi(x)} \otimes_{\mathscr{O}_{X,\phi(x)}} \mathscr{O}_{X^{an},x}$$

Serre investigated in his GAGA-paper [49] for a projective schema $X \in \underline{Al}_{\mathbb{C}}$ and a coherent $\mathscr{O}_X$-module the relation between the cohomology in the algebraic and the analytic category. Subsequently his results have been generalized to the relative case: For a proper morphism

$$f : X \to Y$$

in $\underline{Al}_{\mathbb{C}}$ and a coherent $\mathscr{O}_X$-module sheaf $\mathscr{F}$ the canonical morphisms in $\underline{An}_{\mathbb{C}}$ between the corresponding direct image sheaves

$$(R^j f_* \mathscr{F})^{an} \xrightarrow{\simeq} R^j f_*^{an}(\mathscr{F}^{an}),\ j \in \mathbb{N},$$

are isomorphisms, see [46, Chap. 4].

The literal analogue of divisors on compact Riemann surfaces are divisors on a projective algebraic curve C/k. A priori, these divisors refer to the points of the curve $C \subset \mathbb{P}^n(\overline{k})$ with coordinates in $\overline{k}$. In a second step we will consider those divisors which are defined over k.

Definition 4.19 (Divisors on projective algebraic curves). Consider a projective algebraic curve C/k with $C \subset \mathbb{P}^n(\overline{k})$.

1. A *divisor* on C/k is formal sum

$$D = \sum_{x \in C} n_x \cdot x$$

with integers $n_x \in \mathbb{Z}$ satisfying $n_x = 0$ for all but finitely many indices. For a point $p \in C$ the corresponding point divisor is denoted

$$P := 1 \cdot p$$

Each divisor $D \in Div(C)$ has a well-defined degree

$$deg\ D := \sum_{x \in C} n_x \in \mathbb{Z}$$

The additive group of divisors on C/k is denoted $Div(C)$, its subgroup $Div_0(C) \subset Div(C)$ contains the classes of divisors of degree $= 0$.

2. A divisor $D \in Div(C)$ is a *principal divisor* if $D = 0$ or

$$D = div\ f$$

for a rational function $f \in \overline{k}(C)$. Two divisors $D_1, D_2 \in Div(C)$ are *equivalent*, annotated

$$D_1 \sim D_2,$$

if their difference is a principal divisor. The divisor of a rational function $f \in \overline{k}^*$ has degree

$$deg\ (div\ f) = 0.$$

Denote by

$$Prin(C) \subset Div_0(C)$$

the subgroup of principal divisors. The quotient

$$Cl(C) := Div(C)/Prin(C)$$

is named the *divisor class group* of C. Its subgroup

$$Cl_0(C) := Div_0(C)/Prin(C) \subset Cl(C)$$

is the *class group of degree zero divisors*.

3. A divisor
$$D = \sum_{x \in C} n_x \cdot x \in Div(C)$$
is *defined over k* if it is invariant under the action of the Galois group $G_{\overline{k}/k}$, i.e. if for all $\sigma \in G_{\overline{k}/k}$
$$D = D^\sigma := \sum_{x \in C} n_x \cdot x^\sigma \in Div(C)$$

4. For a divisor $D \in Div(C)$ we denote by $\mathscr{O}_D$ the sheaf of multiples of $-D$, i.e.

$$\mathscr{O}_D(U) := \{f \in \mathscr{M}^*(U) : \ div\ f \geq -D|U\} \cup \{0\},\ U \subset X \text{ open.}$$

For projective-algebraic curves C/k the theorems of Riemann-Roch, Serre duality, the very-ampleness criterion from Theorem 4.13 and the dimension formula

$$dim\ H^0(C, \mathscr{O}) = 1$$

hold literally in the same form as on compact Riemann surfaces. Also the canonical divisor $K \in Div(C)$ has degree

$$deg\ K = 2g(C) - 2.$$

Hence we will apply these results also in the context of algebraic geoemtery without further mentioning.

Definition 4.20 (Elliptic curve over k). An *elliptic curve defined over k* is a pair (E, O) with

- a projective algebraic curve E/k of genus $g = 1$
- and a k-valued point $O \in E$

Note. In Definition 4.20 “O” denotes the upper-case letter O, not the digit 0. We denote by

$$O_\infty := 1 \cdot O \in Div(E)$$

the distinguished point divisor. It is defined over k.

If the base field k and the k-valued point O are not relevant for the context, we will often denote an elliptic curve just by E.

Note that there exist smooth projective algebraic curves $C/\mathbb{Q}$ of genus $g = 1$ without rational points, i.e. with $C(\mathbb{Q}) = \emptyset$. An example is the *Selmer* curve $C \in \mathbb{P}^2(\mathbb{C})$ defined by the homogeneous cubic equation

$$3X^3 + 4Y^3 + 5Z^3 = 0.$$

The fact $g = 1$ for an elliptic curve E allows a simple application of the Riemann-Roch theorem to compute the vector spaces of multiples of a divisor on E.

Lemma 4.21 (Divisors on an elliptic curve). *Consider an elliptic curve E and a divisor $D \in Div(E)$. Then*

$$dim\ H^0(E, \mathscr{O}_D) = \begin{cases} 0 & \text{if } deg\ D < 0 \\ 0 & \text{if } deg\ D = 0,\ D \text{ not principal} \\ 1 & \text{if } deg\ D = 0,\ D \text{ principal} \\ deg\ D & \text{if } deg\ D > 0 \end{cases}$$

Proof. The Riemann-Roch theorem together with Serre duality imply for any divisor $D \in Div(E)$

$$dim\ H^0(E, \mathscr{O}_D) - dim\ H^1(E, \mathscr{O}_D) = dim\ H^0(E, \mathscr{O}_D) - dim\ H^0(E, \mathscr{O}_{-D+K}) =$$

$$= 1 - g + deg\ D = deg\ D$$

Because an elliptic curve E has genus $g = 1$, its canonical divisor has degree

$$deg\ K = 2g - 2 = 0.$$

As a consequence

$$deg\ (-D + K) = deg\ (-D) = -deg\ D$$

i) *Case* $deg\ D \neq 0$: If $deg\ D > 0$ then $deg\ (-D) < 0$. As a consequence

$$dim\ H^0(E, \mathscr{O}_D) = \begin{cases} deg\ D & \text{if } deg\ D > 0 \\ 0 & \text{if } deg\ D < 0 \end{cases}$$

ii) *Case* $deg\ D = 0$: We consider the sheaf $\mathscr{O}_D$ as a line bundle. Then

$$D \text{ principal} \iff \mathscr{O}_D \simeq \mathscr{O}$$

On one hand, D principal implies

$$H^0(E,\mathscr{O}_D) = dim\, H^0(E,\mathscr{O}) = 1$$

On the other hand, for non-principal D the line bundle $\mathscr{O}_D$ is not trivial. Hence each regular section of $s \in H^0(E,\mathscr{O}_D)$ has a zero. If $s \neq 0$, then $deg\ D = 0$ implies that s has also at least a pole, contradicting the regularity of s. Therefore $s = 0$, q.e.d.

The following Lemma 4.22 will be used in the proof of Theorem 4.23. It indicates why the existence of a k-valued point is requested for an elliptic curve defined over k.

Lemma 4.22 (Divisors defined over a subfield). *Consider a projective algebraic curve C/k and a divisor*

$$D = \sum_{x\in X} n_x \cdot x \in Div(C)$$

which is defined over k. Then the finite dimensional $\bar{k}$-vector space

$$H^0(C,\mathscr{O}_D) = \{f \in \bar{k}^*(C) :\ div\ f \geq -D\} \cup \{0\}$$

has a basis of rational functions from $k(C)$, more precisely

$$H^0(C,\mathscr{O}_D) = \bar{k} \otimes_k \{f \in k^*(C) :\ div\ f \geq -D\} \cup \{0\}$$

For the proof see [56, II, Prop. 5.8].

Elliptic curves are by definition subvarieties of a projective space $\mathbb{P}^n(\bar{k})$. Theorem 4.23 proves that they are even plane curves, i.e. that they embed as hypersurfaces into $\mathbb{P}^2(\bar{k})$.

Theorem 4.23 (Elliptic curves are plane cubics). *For an elliptic curve $(E/k, O)$ exist two rational functions $x, y \in k(E)$ with poles only at O such that the map*

$$\phi : E \to \mathbb{P}^2(\bar{k}), p \mapsto \begin{cases} (1 : x(p) : y(p)) & p \neq O \\ (0:0:1) & p = O \end{cases}$$

induces an isomorphism onto the plane cubic $C \subset \mathbb{P}^2(\bar{k})$, which is defined by a homogeneous polynomial $F_{hom} \in k[X_0, X_1, X_2]$ of the form

$$F_{hom}(X_0,X_1,X_2) = X_0X_2^2 + a_1X_0X_1X_2 + a_3X_0^2X_2 - (X_1^3 + a_2X_0X_1^2 + a_4X_0^2X_1 + a_6X_0^3)$$

with five suitable constants $a_i \in k, i = 1,2,3,4,6$. In particular, C is defined over k and non-singular.

Proof. We construct a very ample line bundle $\mathscr{L} = \mathscr{O}_D$ on E and define $\phi := \phi_{\mathscr{L}}$. Therefore consider the divisor

$$D := 3 \cdot O_\infty \in Div(E).$$

The line bundle

$$\mathscr{L} := \mathscr{O}_D \in Pic(E)$$

satisfies the very ampleness criterion from Theorem 4.13: The proof follows from the dimension formula in Lemma 4.21 because for all points $p, q \in E$

$$dim\, H^0(E, \mathscr{O}_{D-P}) = dim\, H^0(E, \mathscr{O}_D) - 1$$

and

$$dim\, H^0(E, \mathscr{O}_{D-(P+Q)}) = dim\, H^0(E, \mathscr{O}_D) - 2.$$

For $n \geq 0$

$$H^0(E, \mathscr{O}_{n \cdot O_\infty}) = \{f \in \overline{k}^*(E) : \ f \text{ has at most a pole at } O \text{ of order } = n\} \cup \{0\}$$

and the dimension formula implies the proper inclusion

$$H^0(E, \mathscr{O}_{3 \cdot O_\infty}) \supsetneq H^0(E, \mathscr{O}_{2 \cdot O_\infty}) \supsetneq H^0(E, \mathscr{O}_{O_\infty}) \simeq H^0(E, \mathscr{O}) = \mathbb{C}.$$

Hence a basis $(1, x, y)$ of

$$H^0(E, \mathscr{L}) = H^0(E, \mathscr{O}_{3 \cdot O_\infty})$$

exists with

- $y \in H^0(E, \mathscr{O}_{3 \cdot O_\infty}) \subset \overline{k}(E)$ has a pole of order $= 3$ at O and no other pole,
- $x \in H^0(E, \mathscr{O}_{2 \cdot O_\infty}) \subset \overline{k}(E)$ has a pole of order $= 2$ at O and no other pole,
- $1 \in H^0(E, \mathscr{O}) = H^0(E, \mathscr{O}_{1 \cdot O_\infty}) \subset \overline{k}(E)$ has no poles.

By assumption $O \in E(k)$. Therefore the divisor D is defined over k. According to Lemma 4.22 we may choose even $x, y \in k(E)$. With respect to the basis $(1, x, y)$ the line bundle $\mathscr{L}$ defines the closed embedding

$$\phi := \phi_{\mathscr{L}} : E \to \mathbb{P}^2(\overline{k}), \ p \mapsto (1 : x(p) : y(p)),$$

onto a curve C/k in $\mathbb{P}^2(\overline{k})$. The family

$$(1,\ x,\ y,\ x^2,\ xy,\ x^3,\ y^2)$$

of seven rational functions from the 6-dimensional vector space $H^0(E, \mathscr{O}_{6 \cdot O_\infty})$ is linearly dependent. Therefore the functions satisfy a linear relation with coefficients from k. Among them the two functions x^3 and y^2 are the only ones having a pole at $O \in E$ of order $= 6$. Hence their coefficients in the linear relation are not zero. After division we may assume that their coefficients are $= \pm 1$ and

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

with coefficients $a_i \in k$. This relation defines the inhomogeneous polynomial

$$F(X,Y) := Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6) \in k[X,Y]$$

and its homogenization, the polynomial $F_{hom} \in k[X_0,X_1,X_2]$ with

$$F_{hom}(X_0,X_1,X_2) := X_0X_1^2 + a_1X_0X_1X_2 + a_3X_2X_0^2 - (X_1^3 + a_2X_1^2X_0 + a_4X_1X_0^2 + a_6X_0^3).$$

The inhomogeneous variables (X,Y) relate to the homogeneous variables (X_0,X_1,X_2) according to

$$X = \frac{X_1}{X_0} \text{ and } Y = \frac{X_2}{X_0}.$$

The curve $\phi(E)$ is a subvariety of the 1-dimensional cubic hypersurface

$$C := V(F_{hom}) \subset \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(\bar{k}) : \ F_{hom}(x_0,x_1,x_2) = 0\}.$$

The cubic C intersects the line at infinity

$$\mathbb{P}^1(\bar{k}) \simeq \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(\bar{k}) : x_0 = 0\}$$

in the single point $(0:0:1)$ with multiplicity $= 3$. Its affine part is the affine variety of the polynomial $F(X,Y) \in k[X,Y]$

$$C_{\text{aff}} = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(\bar{k}) : \ F_{hom}((x_0 : x_1 : x_2)) = 0 \text{ and } x_0 \neq 0\} =$$

$$= \{(x,y) \in \mathbb{A}^2(\bar{k}) : \ F(x,y) = 0\} = V(F).$$

The polynomial $F \in k[X][Y]$, considered as polynomial in Y with coefficients from the ring $k[X]$, is irreducible: It does not split as

$$F(X,Y) = (Y + b_1)(Y + b_2)$$

with polynomials $b_1, b_2 \in k[X]$. Therefore C_{aff} and also C are irreducible. Hence the non-constant regular map

$$\phi : E \to C$$

is surjective, cf. [29, Chap. II, Prop. 6.8], an analogue of the theorem about non-constant proper holomorphic maps between Riemann surfaces. As a consequence

$$\phi(E) = C \text{ and } E \simeq C \text{ over } k$$

and C is non-singular, q.e.d.

In the following we will identify an abstract elliptic curve $(E/k,O)$ with the plane cubic from Theorem 4.23. We say that $(E/k,O)$, more precisely its affine part, is defined over k by the *Weierstrass equation* $F(X,Y) = 0$.

Definition 4.24 (Weierstrass polynomial and Weierstrass equation, its discriminant and j-invariant). A *Weierstrass polynomial* over a field k is a cubic poynomial

$$F(X,Y) = Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6) \in k[X,Y]$$

with coefficients

$$a_1,\ a_2,\ a_3,\ a_4,\ a_6 \in k.$$

1. The equation

$$F(X,Y) = 0,$$

i.e.

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

is named the *Weierstrass equation* over k defined by F.

2. The *discriminant* of F is

$$\Delta_F := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

with

$$b_2 := a_1^2 + 4a_2,\ b_4 := 2a_4 + a_1a_3,\ b_6 := a_3^2 + 4a_6$$

and

$$b_8 := a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

3. The *j-invariant* of F is

$$j_F := \frac{c_4^3}{\Delta_F},\ c_4 := b_2^2 - 24b_b.$$

Starting from an elliptic curve over a field k the resulting Weierstrass polynomial is not unique. There exist coordinate transformations defined over k which transform a Weierstrass polynomial over k to a different form, in particular to a more simple form.

Proposition 4.25 (Weierstrass equation in short form, discriminant and j-invariant). *Consider a Weierstrass polynomial*

$$F(X,Y) = Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6) \in k[X,Y]$$

1. Short form*: If char $k \neq 2,3$ then there exists a linear coordinate change*

$$\begin{pmatrix} X \\ Y \end{pmatrix} \mapsto \begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} u^2 \cdot X + r \\ u^3 \cdot Y + s \cdot u^2 \cdot X + t \end{pmatrix}$$

with constants

$$r,s,t \in k, u \in k^*$$

which transforms $F(X,Y)$ *to the* Weierstrass polynomial in short form

$$F'(X',Y') = Y'^2 - (X'^3 + A \cdot X' + B),\ A,\ B \in k$$

with discriminant

$$\Delta_{F'} = -2^4 \cdot (4A^3 + 27B^2) \in k$$

and the same j*-invariant*

$$j_{F'} = j_F$$

2. Transforming Weierstrass polynomials in short form*: Each linear coordinate transformation over* k

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} \mapsto \begin{pmatrix} X \\ Y \end{pmatrix} := \begin{pmatrix} u^2 & 0 \\ 0 & u^3 \end{pmatrix} \cdot \begin{pmatrix} X' \\ Y' \end{pmatrix}.$$

with $u \in k^*$ *transforms a Weierstrass polynomial in short form*

$$F'(X',Y') = Y'^2 - (X'^3 + A' \cdot X' + B') \in k[X',Y']$$

to the Weierstrass polynomial in short form

$$F(X,Y) = Y^2 - (X^3 + A \cdot X + B) \in k[X,Y].$$

such that the numerical constants relate as

$$A = u^4 \cdot A',\ B = u^6 \cdot B',\ \Delta_F = u^{12} \cdot \Delta_{F'}.$$

retaining the j*-invariant*

$$j_F := 1728 \cdot \frac{(4A)^3}{\Delta_F} = 1728 \cdot \frac{(4A')^3}{\Delta_{F'}} =: j_{F'}$$

3. The j-invariant*: Two Weierstrass polynomials in short form have the same* j*-invariant if and only if they are related by an isomorphism as in part 3) defined over* $\overline{k}$ *- not necessarily over* k*.*

4. *For each algebraic number* $j_0 \in \overline{k}$ *exists an elliptic curve* $E/k(j_0)$ *with* j*-invariant equal to* j_0*.*

For the proof of Proposition 4.25 see [56]: For part 1) cf. Chap. III, §1; for part 2) cf. Chap. III, Rem. 1.3; for part 3) cf. Chap. III, Prop. 1.4(b); for part 4) cf. Chap. III, Prop. 1.4(c).

The discriminant $\Delta_F \in k$ of a Weierstrass polynomial $F(X,Y) \in k[X,Y]$ indicates whether the projective algebraic variety

$$C = V(F_{hom}) \subset \mathbb{P}^2(\bar{k})$$

is non-singular or not. If $\Delta_F \neq 0$ then $(C/k, (0:0:1))$ is non-singular, i.e. an elliptic curve.

Proposition 4.26 (Singularities of cubics). *Assume char $k \neq 2,3$ and consider a plane cubic curve*

$$C := V(F_{hom}) = \subset \mathbb{P}^2(\bar{k})$$

defined by the homogenization of a Weierstrass polynomial in short form

$$F(X,Y) = Y^2 - (X^3 + AX + B) \in k[X,Y]$$

with $A,\ B \in k$ and discriminant

$$\Delta_F = -16 \cdot (4A^3 + 27B^2).$$

The curve C has at most one singular point. The curve

- *is* non-singular *iff* $\Delta_F \neq 0$
- *has a* node *iff* $\Delta_F = 0$ *and* $A \neq 0$
- *has a* cusp *iff* $\Delta_F = A = 0$.

For a proof of Proposition 4.26 see [56, Chap. III, Prop. 1.4].

Remark 4.27 (Cubic projective-algebraic curves and elliptic curves). The *adjunction formula* for non-singular hypersurfaces implies: Any projective algebraic cubic curve $C \subset \mathbb{P}^2$ has genus $= 1$. Hence C/k is an elliptic curve if C has at least one k-valued point, see [29, Chap. V, Example. 1.5.1].

Theorem 4.28 is the converse of Theorem 4.3. it shows that the complex points of an elliptic curve, defined over a subfield of $\mathbb{C}$, can be parametrized by the Weierstrass function $\wp$ and its derivative $\wp'$ of a suitable torus. The proof relies on the result of Theorem 4.23 that elliptic curves are plane cubics which satisfy a Weierstrass equation.
A very coarse analogue of the uniformization is the parametrization of the points of the unit circle by the values of the exponential function $e^{2\pi i \cdot t}$ on the parameter interval $[0,1]$.

Theorem 4.28 (Uniformization of elliptic curves $E/\mathbb{C}$ by tori). *For any elliptic curve E defined over $\mathbb{C}$ exists a torus $T = \mathbb{C}/\Lambda$ and a biholomorphic map*

$$\Phi : T \xrightarrow{\simeq} E(\mathbb{C}).$$

Here $E(\mathbb{C}) \subset \mathbb{P}^n(\mathbb{C})$ is provided with the induced Euclidean topology and analytic structure from the complex manifold $\mathbb{P}^n(\mathbb{C}) = \mathbb{P}^n$.

Proof. Due to Theorem 4.23 we may assume that E is defined as a plane curve, defined by the homogenization of a Weierstrass polynomial in short form

$$F(X,Y') := Y'^2 - (X^3 + a_4 \cdot X + a_6) \in \mathbb{C}[X,Y'].$$

The substitution

$$Y' = (1/2) \cdot Y$$

shows that E can also be defined by the Weierstrass polynomial

$$F(X,Y) = Y^2 - (4 \cdot X^3 - A \cdot X - B)$$

with suitable constants $A,\ B \in \mathbb{C}$ and discriminant

$$\Delta_F = A^3 - 27 \cdot B^3$$

due to Proposition 4.26. We search for a lattice

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$$

with lattice constants $G_{\Lambda,4}$ and $G_{\Lambda,6}$ satisfiying

$$A = 60 \cdot G_{\Lambda,\,4} \text{ and } B = 140 \cdot G_{\Lambda,\,6}.$$

The restriction of the modular invariant

$$j|\mathbb{H} : \mathbb{H} \to \mathbb{C},\ j(\tau) := 1728 \cdot \frac{g_2^3(\tau)}{g_2^3(\tau) - 27 g_3^2(\tau)},$$

is surjective according to Corollary 3.16. Hence a number $\tau \in \mathbb{H}$ exists with

$$j(\tau) = 1728 \cdot \frac{A^3}{\Delta_F}.$$

If $g_2(\tau) = 0$ then $\tau = \rho$ according to Corollary 3.20. We choose

$$\Lambda := \Lambda_\rho.$$

Similarly, if $g_3(\tau) = 0$ then $\tau = i$, and we choose

$$\Lambda := \Lambda_i.$$

Otherwise, the two equations

$$j(\tau) = 1728 \cdot \frac{g_2^3(\tau)}{g_2^3(\tau) - 27 g_3^2(\tau)} = 1728 \cdot \frac{A^3}{\Delta_F}$$

and

$$\Delta_F = A^3 - 27B^2$$

imply

$$\frac{g_2^3(\tau)}{g_2^3(\tau)-27g_3^2(\tau)} = \frac{A^3}{A^3-27\cdot B^2}.$$

Clearing the denominators by crosswise multiplication implies

$$\left(\frac{A}{g_2(\tau)}\right)^3 = \left(\frac{B}{g_3(\tau)}\right)^2$$

We choose $\omega_1 \in \mathbb{C}$ with

$$\frac{A}{g_2(\tau)} = \left(\frac{1}{\omega_1}\right)^4 \text{ and } \frac{B}{g_3(\tau)} = \left(\frac{1}{\omega_1}\right)^6.$$

This choice is possible because we may replace ω_1 by $i\omega_1$. In addition, we set

$$\omega_2 := \tau\cdot\omega_1, \text{ i.e. } \tau = \omega_2/\omega_1.$$

Then (ω_1,ω_2) is a positively oriented basis of the lattice

$$\Lambda := \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2.$$

Its lattice constants are

$$G_{\Lambda,4} = \left(\frac{1}{\omega_1}\right)^4 \cdot G_4(\tau) = \left(\frac{1}{\omega_1}\right)^4 \cdot (1/60)\cdot g_2(\tau) = (1/60)\cdot A$$

and similarly

$$G_{\Lambda,6} = (1/140)\cdot B,$$

i.e.

$$A = g_{\Lambda,2} \text{ and } B = g_{\Lambda,3}.$$

The map

$$\phi : \mathbb{C}/\Lambda \to \mathbb{P}^2$$

from Theorem 4.3 maps the torus $\mathbb{C}/\Lambda$ biholomorphically to the cubic hypersurface with Weierstrass polynomial

$$F(X,Y) = Y^2 - (4\cdot X^3 - g_{\Lambda,2}\cdot X - g_{\Lambda,3}) = Y^2 - (4\cdot X^3 - A\cdot X - B),\ q.e.d.$$

Example 4.29 (Elliptic curves and cubics with a singularity). The following Figures 4.5 - 4.8 show some elliptic curves.

While Figure 4.9 and Figure 4.10 show the singular cubics *node* and the *Neil parabola*. They have a single singularity, namely at the origin respectively a node and a cusp. The corresponding table from Figure 4.4 shows the invariants. The role of the *conductor* will be explained in Definition 4.40 later.

For the computation and the plots see the PARI files `Elliptic_curve_02` and `Elliptic_curve_plot_06`.

Figure	Weierstrass equation	j-invariant	discriminant	conductor
Elliptic curve				
4.5	$Y^2 = X^3 - 3X + 3$	$-2^8 \cdot 3^3/5$	$-2^4 \cdot 3^3 \cdot 5$	$2^3 \cdot 3^3 \cdot 5$
4.6	$Y^2 = X^3 + X$	1728	-2^6	2^6
4.7	$Y^2 = X^3 - X$	1728	2^6	2^5
4.8	$Y^2 = X^3 + 3$	0	$-2^4 \cdot 3^5$	$2^4 \cdot 3^5$
	$Y^2 = X^3 - X - 14$	$-2^5 \cdot 3^3/661$	$-2^7 \cdot 661$	$2^7 \cdot 661$
	$Y^2 + 5XY + Y = X^3$	$5^3 \cdot 101^3/(2 \cdot 7^2)$	$2 \cdot 7^2$	$2 \cdot 7$
Singular cubic				
4.9	$Y^2 = X^3 + X^2$	–	0	–
4.10	$Y^2 = X^3$	–	0	–

Fig. 4.4 Numerical values of some cubic curves

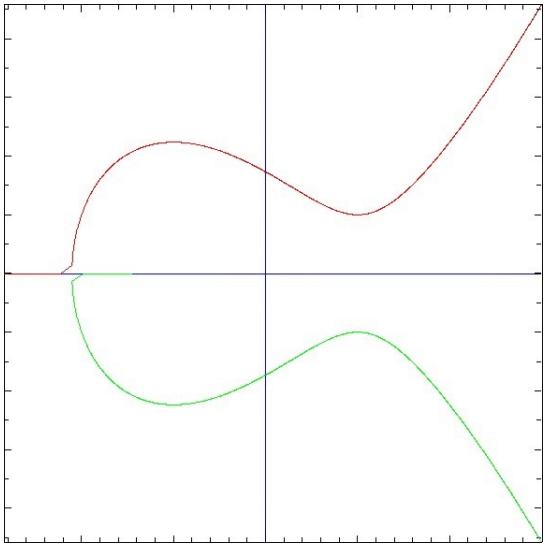


Fig. 4.5 $Y^2 = X^3 - 3X + 3$

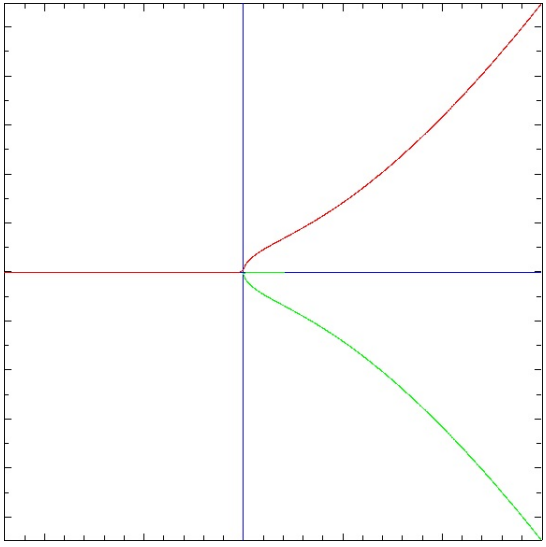
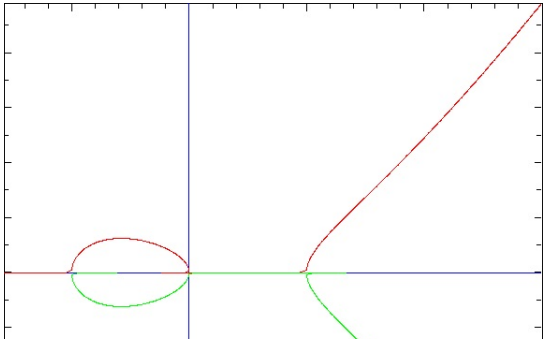


Fig. 4.6 $Y^2 = X^3 + X$



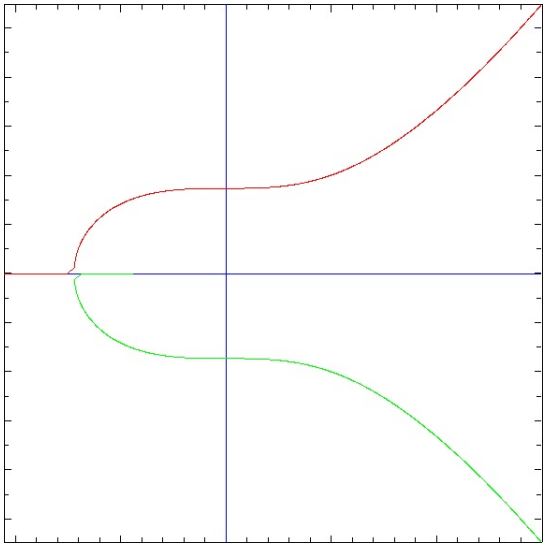


Fig. 4.8 $Y^2 = X^3 + 3$

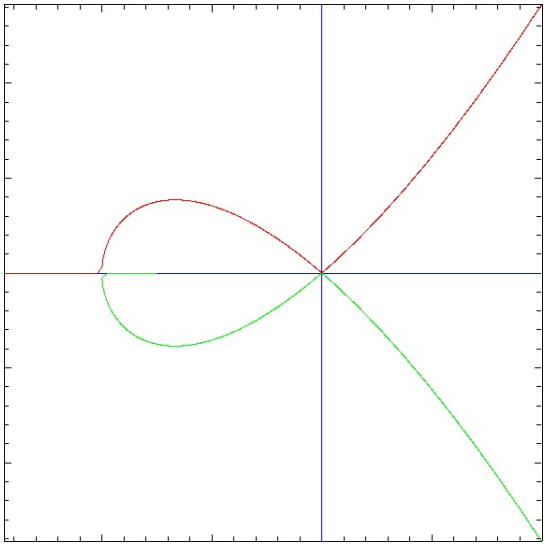
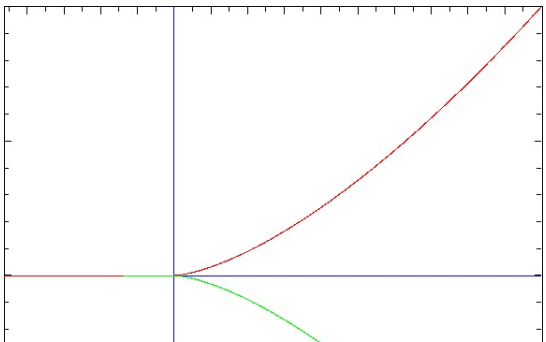


Fig. 4.9 $Y^2 = X^3 + X^2$



Lemma 4.30 prepares the proof of Theorem 4.31 and the Definition 4.32 of the group structure of an elliptic curve $(E/k, O)$. The lemma shows that for a pair (p,q) of distinct points from E the divisor

$$D := P - Q \in Div(E)$$

cannot be a principal divisor. Note that the lemma gives also a second proof of Corollary 1.9.

Lemma 4.30 (No single pole of order one). *Consider an elliptic curve $(E/k, O)$ defined over a field k. There is no ratiomal function $f \in \overline{k}(E)^*$ with*

$$div\ f = P - Q$$

with P, $Q \in Div(E)$ the elementary divisors of two distinct points $p \neq q \in E$.

Proof. Consider the point divisor

$$Q \in Div(E) \text{ of degree } deg\ Q = 1.$$

Lemma 4.21 implies

$$dim\ H^0(E, \mathcal{O}_Q) = 1.$$

Hence the inclusion

$$\overline{k} \subset H^0(E, \mathcal{O}_Q)$$

implies

$$\overline{k} = H^0(E, \mathcal{O}_Q).$$

Hence each $f \in H^0(E, \mathcal{O}_Q)$ is constant, and therefore $f = 0$ or

$$div\ f = 0 \in Div(E)$$

which implies $p = q$, a contradiction, q.e.d.

Lemma 4.30 shows: The obstructions for a divisor $D \in Div_0(E)$ to be a principal divisor are divisors of type $P - Q$ or even of type $P - O_\infty$. A divisor $D \in Div_0(E)$ is the divisor of a rational function up to a divisor of type

$$P - O_\infty.$$

Because the point $P \in E$ is uniquely determined by D, the obstruction is expressed by P alone.

We use the notation from Definition 4.19).

Theorem 4.31 (The class group of degree zero divisors on an elliptic curve). *Consider an elliptic curve $(E/k, O)$.*

1. *For any divisor $D \in Div_0(E)$ exists a unique point $p \in E$ with*

$$D \sim P - O_\infty$$

Denote the corresponding map by

$$\sigma : Div_0(E) \to E,\ D \mapsto p.$$

2. *The map σ is surjective. It induces a bijective map from the group of divisor classes of degree $= 0$*

$$\overline{\sigma} : Cl_0(E) \xrightarrow{\simeq} E$$

with inverse

$$E \xrightarrow{\simeq} Cl_0(E),\ p \mapsto [P - O_\infty].$$

Proof. 1. *Definition of σ*: The divisor $D + O_\infty$ has degree $= 1$. Lemma 4.21 implies

$$dim\, H^0(E, \mathcal{O}_{D+O_\infty}) = 1.$$

We choose a non-zero rational function $f \in \overline{k}(E)^*$ with divisor satisfying

$$div\, f \geq -(D + O_\infty).$$

Because

$$deg\ (div\, f) = 0 \text{ but } deg(-(D + O_\infty)) = -1,$$

there exists a point $p \in E$ with

$$div\, f = -(D + O_\infty) + P$$

Then

$$0 \sim -(D + O_\infty) + P \text{ i.e. } D \sim P - O_\infty.$$

If for a different point

$$q \in E,\ q \neq p,$$

also

$$D \sim Q - O_\infty$$

then

$$0 = D - D \sim P - Q.$$

Hence for a suitable rational function $g \in \overline{k}^*(E)$

$$P - Q = div\, g,$$

contradicting Lemma 4.30. Therefore

$$\sigma(D) := p \in E$$

is well-defined.

2. i) *Surjectivity of* σ: Consider an arbitrary point $p \in E$. Set

$$D := P - O_\infty \in Div_0(E).$$

Then $\sigma(D) = P$ by definition, which proves the surjectivity of σ.

ii) *Induced map* $\overline{\sigma}$:

$$[D_1] = [D_2] \implies P_1 - O_\infty \sim P_2 - O_\infty \implies P_1 \sim P_2 \implies \sigma(D_1) = \sigma(D_2)$$

iii) *Injectivity of* $\overline{\sigma}$:

$$\overline{\sigma}([D_1]) = \overline{\sigma}([D_2]) \implies \sigma(D_1) = \sigma(D_2) \implies$$

$$\implies \exists p \in E : D_1 \sim P - O_\infty \text{ and } D_2 \sim P - O_\infty \implies D_1 \sim D_2 \implies [D_1] = [D_2],\ q.e.d.$$

Definition 4.32 (Group structure of an elliptic curve). Consider an elliptic curve $(E/k, O)$ and denote by $(Cl_0(E), +)$ the group of divisor classes of degree zero. The bijective map from Theorem 4.31

$$\overline{\sigma} : Cl_0(E) \to E,\ [P - O_\infty] \mapsto p,$$

carries over the group structure from $(Cl_0(E), +)$ to E: The map

$$\oplus : E \times E \to E,\ p \oplus q := \overline{\sigma}([P - O_\infty] + [Q - O_\infty]),$$

defines an Abelian *additive group* $(E, \oplus)$ with neutral element the k-valued point $O \in E(k)$.

Corollary 4.33 (Abel's Theorem for elliptic curves). *Consider an elliptic curve* $(E/k, O)$. *A divisor*

$$D = \sum_{p \in E} n_p \cdot P \in Div_0(E)$$

is a principal divisor iff

$$\bigoplus_{p \in E} n_p * p = O \in E.$$

Here the last equation refers to the group structure $\oplus$ on E. The product $n_p * p$ means:

- Taking n_p-times the sum of a point $p \in E$ if $n_p \geq 0$, and
- taking $(-n_p)$-times the sum of $\ominus p \in E$ if $n_p \leq 0$. Here the symbol $\ominus p \in E$ denotes the negative of p with respect to the group structure.

Proof. Because

$$0 = deg\ D = \sum_{p \in E} n_p$$

we have

$$D = D - \sum_{p \in E} n_P \cdot O_\infty = \sum_{p \in E} n_p \cdot (P - O_\infty) \in Div_0(E)$$

Due to Theorem 4.31, part ii)

$$D\ principal \iff [D] = 0 \iff \overline{\sigma}([D]) = O \in E \iff$$

$$\iff \overline{\sigma}\left(\sum_{p \in E} n_p \cdot [P - O_\infty]\right) = O \in E \iff \bigoplus_{p \in E} n_p * \overline{\sigma}([P - O_\infty]) = O \in E \iff$$

$$\iff \bigoplus_{p \in E} n_p * p = 0 \in E,\ q.e.d.$$

Proposition 4.34 (Group structure of tori and elliptic curves). *For a complex torus $T = \mathbb{C}/\Lambda$ the biholomorphic map from Theorem 4.3*

$$\phi : T \to E(\mathbb{C})$$

onto the complex points of a plane elliptic curve E is an isomorphism of groups.

Proof. 1. i) Denote by $0_T \in T$ the neutral element of the group $(T, \oplus)$. The canonical morphism

$$\rho : (T, \oplus) \to (Div_0(T), +),\ p \mapsto 1 \cdot p - 1 \cdot 0_T,$$

is a group morphism: For $j = 1, 2$ and two points $p_j \in T$ and divisors from $Div_0(T)$

$$D_j := 1 \cdot p_j - 1 \cdot 0_T \text{ and } D := 1 \cdot (p_1 \oplus p_2) - 1 \cdot 0_T$$

the difference

$$D_1 + D_2 - D = 1 \cdot p_1 + 1 \cdot p_2 - 1 \cdot (p_1 \oplus p_2) - 1 \cdot 0_T \in Div_0(T)$$

is a principal divisor according to Abel's Theorem 1.21 because

$$p_1 \oplus p_2 \ominus (p_1 \oplus p_2) \ominus 0_T = 0_T \in \Lambda$$

ii) For a point $p \in T$ the image

$$\rho(p) = 1 \cdot p - 1 \cdot 0_T \in Div_0(T)$$

is a principal divisor iff $p = 0_T$, again due to Abel's Theorem. If we denote by

$$\overline{\rho} : T \to Cl_0(T)$$

the composition of ρ with the canonical map $Div_0(T) \to Cl_0(T)$ then

$$\overline{\rho} : T \to Cl_0(T)$$

is injective.

iii) Each divisor

$$D = \sum_{a \in A} n_a \cdot a - \sum_{b \in B} n_b \cdot b \in Div_0(T),\ A,\ B \subset T, A \cap B = \emptyset, n_a, n_b > 0,$$

defines a point

$$p := \left(\bigoplus_{a \in A} n_a \cdot a \right) \ominus \left(\bigoplus_{b \in B} n_b \cdot b \right) \in T$$

Then

$$\rho(p) = 1 \cdot p - 1 \cdot 0_T \in Div_0(T)$$

Due to Abel's Theorem the difference

$$\rho(p) - D = 1 \left(\left(\bigoplus_{a \in A} n_a \cdot a \right) \ominus \left(\bigoplus_{b \in B} n_b \cdot b \right) \right) - 1 \cdot 0_T - \left(\sum_{a \in A} n_a \cdot a - \sum_{b \in B} n_b \cdot b \right) \in Div_0(T)$$

is a principal divisor because $\ominus 0_T = 0_T \in \Lambda$. Hence ρ is surjective.

iv) Part ii) and iii) imply that ρ is an isomorphism of groups.

2. Due to part 1) and Definition 4.32 the group structures respectively on domain and codomain of

$$\phi : T \to E(\mathbb{C})$$

are determined by the divisor class groups. Because ϕ is an analytical isomorphism it is a group isomorphism, q.e.d.

Remark 4.35 (Group structure of an elliptic curve).

1. *Geometric version*: The group structure from Definition 4.32 of an elliptic curve $(E/k, O)$ can also be obtained by a geometric construction. It relies on the fact that a cubic and a line in $\mathbb{P}^2$ intersect in exactly three points, counted with multiplicity.

   See Figure 4.11: Two add two points $p, q \in E \setminus \{O\}$ consider the line $L(p,q)$ passing through p and q. The line intersects E in a third point $r \in E$. The second line $L(r, O)$ intersects E in a third point, which is $p \oplus q$. For more details see [63].

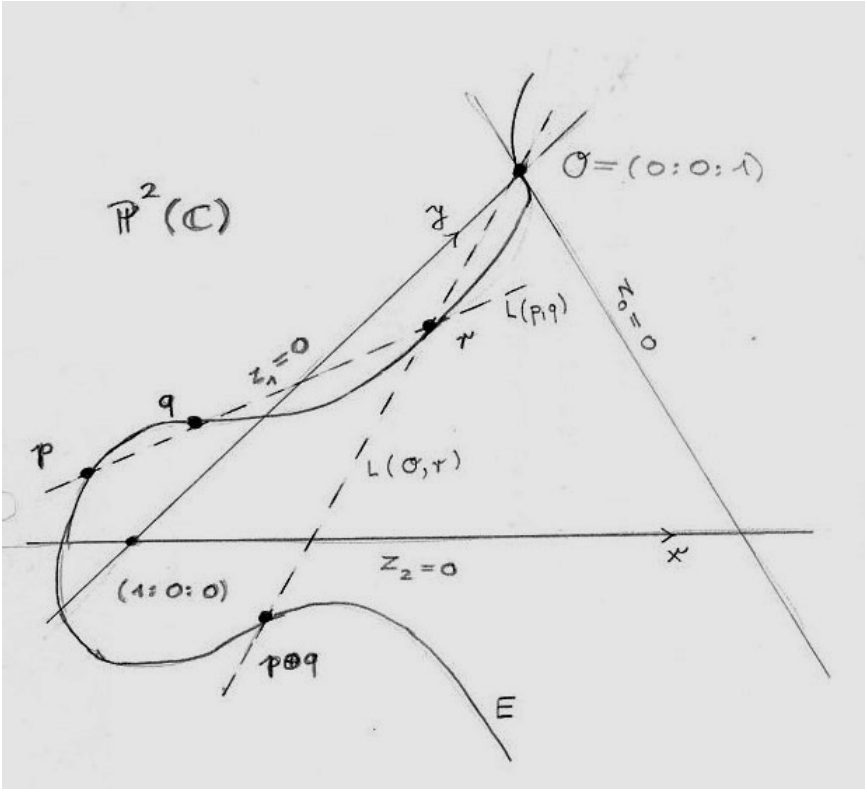


Fig. 4.11 Group law on an elliptic curve (Geometric construction)

2. *Mordells theorem*: The group structure on $E(\overline{\mathbb{Q}})$ provides also the set $E(K)$ of K-valued points with a group structure for any intermediate field

$$\mathbb{Q} \subset K \subset \overline{\mathbb{Q}}.$$

Mordell proved: The Abelian group $E(\mathbb{Q})$ of $\mathbb{Q}$-valued points of E is finitely generated, [56, Chap. VIII, Theor. 4.1]. As a consequence, $E(\mathbb{Q})$, today names the *Mordell-Weil group* of $E/\mathbb{Q}$, decomposes as the product of an Abelian torsion group and a free Abelian group of finite rank $r < \infty$

$$E(\mathbb{Q}) = E(\mathbb{Q})_{tors} \times \mathbb{Z}^r.$$

Many open questions are related to the rank r.

3. *Falting's theorem*: Elliptic curves have genus $g = 1$. Curves of genus $g > 1$ do no longer carry a group structure. Mordell conjectured: Projective algebraic curves $C/\mathbb{Q}$ with genus $g > 1$ have only finitely many points with rational coordinates, i.e.

$$card\, C(\mathbb{Q}) < \infty.$$

The Mordell-conjecture was proved by Faltings, see [58].

Example 4.36 (Group structure of an elliptic curve). Consider an elliptic curve $E/\mathbb{Q}$. The PARI file `Elliptic_curve_torsion_group` investigates the torsion group of $E(\mathbb{Q})$ for the elliptic curve $E/\mathbb{Q}$ with Weierstrass polynomial

$$y^2 = x^3 - 43x + 166$$

see Figure 4.12. It shows that the torsion group $E(\mathbb{Q})_{tors}$ has a factor isomorphic to $\mathbb{Z}/7\mathbb{Z}$. For more information, in particular for the equality

$$E(\mathbb{Q})_{tors} = \mathbb{Z}/7\mathbb{Z}$$

see [54, Chap. VII, Theor. 7.5]. It is conjectured that the rank r of the free part of the group $E(\mathbb{Q})$ equals the analytic rank of $E/\mathbb{Q}$.

```
=====================================================
Elliptic_curve_torsion_group: Start.

Weierstrass polynom.: Y^2 = X^3 + (-43*X) + (166)
j-invar.: [-1, 1; 2, -7; 3, 3; 13, -1; 43, 3]
discr.: [-1, 1; 2, 19; 13, 1], analytic. rank: 0

[3, 8] is on curve? 1
[3, 8] is torsion point of order 7
2 * [3, 8]: [-5, -16]
---------------------------------
[3, -8] is on curve? 1
[3, -8] is torsion point of order 7
2 * [3, -8]: [-5, 16]
---------------------------------
[-5, 16] is on curve? 1
[-5, 16] is torsion point of order 7
2 * [-5, 16]: [11, -32]
---------------------------------
[-5, -16] is on curve? 1
[-5, -16] is torsion point of order 7
2 * [-5, -16]: [11, 32]
---------------------------------
[11, 32] is on curve? 1
[11, 32] is torsion point of order 7
2 * [11, 32]: [3, 8]
---------------------------------
[11, -32] is on curve? 1
[11, -32] is torsion point of order 7
2 * [11, -32]: [3, -8]
---------------------------------
Elliptic_curve_torsion_group: End
```

Fig. 4.12 The group $E(\mathbb{Q})_{tors}$

4.3 Elliptic curves over finite fields

The present section starts the investigation of elliptic curves defined over $\mathbb{Q}$. Each elliptiv curve $E/\mathbb{Q}$ can also be defined by a distinguished Weierstrass polynomial with integer coefficients, called a *global minimal polynomial*, see Definition 4.37 and Remark 4.38.

Entering into the field of arithmetic geometry one may reduce the integer equation modulo any prime $p \in \mathbb{Z}$, each time obtaining an elliptic curve defined over a finite field $\mathbb{F}_p$. Considered from a general point of view: An elliptic curve defined over $\mathbb{Q}$ is a family of not necessarily smooth curves defined over all prime fields of prime characteristic. Or even more general, it is a map to *Spec* $\mathbb{Z}$, and all but but finitely many fibres are elliptic curves over prime fields. Reduction modulo p is a powerful tool to investigate the arithmetic information encoded in an elliptic curve defined over $\mathbb{Q}$.

Before investigating the family of elliptic curves one has to eliminate redundant prime powers of the discriminant which otherwise would distort the result. The discriminants of the different Weierstrass polynomials of an elliptic curve differ by a non-zero rational. After multiplying with a principal nominator they differ by a non-zero integer. Hence the reduction of the discriminants modulo a prime $p \in \mathbb{Z}$ may differ. To generalize the discriminant criterion from Proposition 4.26 one has to find a unique minimal discriminant. The corresponding Weierstrass polynomial is named *global minimal*.

Definition 4.37 (Global minimal Weierstrass polynomial). For an elliptic curve $E/\mathbb{Q}$ a Weierstrass polynomial $F \in \mathbb{Z}[X,Y]$ with integer coefficients is *global minimal* if its discriminant

$$\Delta_F = \pm \prod_{p \text{ prime}} p^{v(p)},\ v(p) \in \mathbb{N}^*,$$

is minimal for each given prime factor p of Δ_F in the following sense: The elliptic curve $E/\mathbb{Q}$ cannot be defined by a Weierstrass polynomial $F_p(X,Y) \in \mathbb{Z}[X,Y]$ with discriminant Δ_{F_p} satisfying

$$ord_p(\Delta_{F_p}) < v(p).$$

"Global minimality" is a global property because it refers to all primes of Δ_F

Remark 4.38 (Global minimal Weierstrass polynomial).

1. *Non-uniqeness of the discriminant*: The Weierstrass polynomial of an elliptic curve, even if is in short form, is not uniquely determined. In general, an elliptic curve does not have a unique discriminant. It is not the discriminant, but the j-invariant which characterizes the elliptic curve.

2. *Global minimal Weierstrass polynomial*: The discriminant of a global minimal Weierstrass polynomial
$$F(X,Y) \in \mathbb{Z}[X,Y]$$
is uniquely determined. The last condition from Definition 4.37 implies for any prime factor $p \neq 2,3$ of its discriminant
$$ord_p(\Delta_F) < 12.$$
Each elliptic curve over $k = \mathbb{Q}$ has a global minimal Weierstrass polynomial. The result generalizes to elliptic curves over arbitrary number fields with class number $= 1$, see [56, Chap. VIII, Cor. 8.3] and more specific [33, Theor. 10.3]. A global minimal Weierstrass polynomial is not necessarily in short form.

3. *PARI command*: The Pari command *ellminimalmodel* provides the global minimal model for elliptic curves over number fields k with class number $= 1$.

Example 4.39 (Global minimal Weierstrass polynomial).

1. See PARI-file `Elliptic_curve_weierstrass_equation_12`. Figure 4.13, upper example, considers the Weierstrass polynomial
$$F(X,Y) = Y^2 - (X^3 + 15.625)$$
Its discrimant
$$\Delta_F = -2^4 \cdot 3^3 \cdot 5^{12}$$
is not minimal because
$$5^{12} | \Delta_F$$
The global minimal Weierstrass polynomial is
$$F_{\min}(X,Y) = Y^2 - (X^3 + 1)$$
with discriminant
$$\Delta_{F_{min}} = -2^4 \cdot 3^3.$$

```
================================================
Elliptic curve weierstrass_equation_12 = Start.

Elliptic curve parameter = [0, 0, 0, 0, 15625]
Elliptic curve, Weierstrass equation: Y^2 + 0*XY + 0*Y = X^3 + 0*X^2 + 0*X + 15625
Discriminant = -105468750000 = [-1, 1; 2, 4; 3, 3; 5, 12]

Elliptic curve, global minimal Weierstrass equation: Y^2 + 0*XY + 0*Y = X^3 + 0*X^2 + 0*X + 1
Discriminant = -432 = [-1, 1; 2, 4; 3, 3]
------------------------------------------------
Elliptic curve parameter = [0, 0, 0, 1/5, 1]
Elliptic curve, Weierstrass equation: Y^2 + 0*XY + 0*Y = X^3 + 0*X^2 + 1/5*X + 1
Discriminant = -54064/125 = [-1, 1; 2, 4; 5, -3; 31, 1; 109, 1]

Elliptic curve, global minimal Weierstrass equation: Y^2 + 0*XY + 0*Y = X^3 + 0*X^2 + 125*X + 15625
Discriminant = -105593750000 = [-1, 1; 2, 4; 5, 9; 31, 1; 109, 1]
------------------------------------------------
Elliptic curve weierstrass_equation_12 = End.
================================================
```

Fig. 4.13 Global minimal Weierstrass polynomial

2. The Weierstrass polynomial

$$F(X,Y) = Y^2 - (X^3 - 595 \cdot X + 5.586) \in \mathbb{Z}[X,Y]$$

with discriminant

$$\Delta_F = 2^{12} \cdot 7^3$$

is global minimal, despite of the exponent 12 of the particular prime factor $p = 2$.

3. Consider the elliptic curve $E/\mathbb{Q}$ with Weierstrass polynomial in short form

$$F(X,Y) = Y^2 - (X^3 + \frac{1}{5} \cdot X + 1) \in \mathbb{Q}[X,Y]$$

which is not global minimal because it has a non-integer cefficient. To obtain a global minimal Weierstrass polynomial, we make the transformation

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} u^{-2} \cdot X' \\ u^{-3} \cdot Y' \end{pmatrix} \text{ with } u := 5$$

and multiply by u^6. We obtain the Weierstrass equation

$$Y'^2 = X'^3 + \frac{1}{u} \cdot u^{-2} \cdot u^6 \cdot X' + u^6 \text{ i.e. } Y'^2 = X'^3 + 5^3 \cdot X' + 5^6$$

Hence $E/\mathbb{Q}$ is also defined by the Weierstrass polynomial

$$F_{min}(X,Y) = Y^2 - (X^3 + 5^3 \cdot X + 5^6) \in \mathbb{Z}[X,Y]$$

which is global minimal because

$$\Delta_{F_{min}} = -2^4 \cdot 5^9 \cdot 31 \cdot 109 \in \mathbb{Z},$$

see Figure 4.13, lower example.

Definition 4.40 (Reduction mod p). Consider an elliptic curve

$$E = (E/\mathbb{Q}, O)$$

with global minimal Weierstrass polynomial $F(X,Y) \in \mathbb{Z}[X,Y]$.

1. Denote by
$$F_{hom} \in \mathbb{Z}[X_0, X_1, X_2]$$
the homogeniziation of F. For each prime $p \in \mathbb{N}$ reducing mod p the coefficients of F_{hom} provides a Weierstrass polynomial
$$F_{hom,p} \in \mathbb{F}_p[X_0, X_1, X_2]$$
with coefficients from the finite field $\mathbb{F}_p$. The Weierstrass polynomial defines the projective variety
$$E_p := Var(F_{hom,p}) := \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(\overline{\mathbb{F}}_p) : \ F_{hom,p}(x_0, x_1, x_2) = 0\} \subset \mathbb{P}^2(\overline{\mathbb{F}}_p),$$
which is named the *reduction mod p of E* .

2. At a prime $p \in \mathbb{Z}$ the elliptic curve E is
   - *stable* if (E_p, O) is non-singular, i.e. an elliptic curve over $\mathbb{F}_p$.
   - *semistable* if (E_p, O) is singular with a node.
   - *unstable* if (E_p, O) is singular with a cusp.
3. The *conductor* $cond(E) \in \mathbb{N}^*$ of $E/\mathbb{Q}$ distinguishes the primes p with semistable reduction from those with unstable reduction: One has
$$cond(E) = \prod_p p^{e_p}$$
with the same prime factors p as the discriminant Δ_F. The exponents of the prime factors satisfy
$$e_p := 1 \iff E \text{ is semistable at } p$$
and for $p > 3$
$$e_p := 2 \iff E \text{ is unstable at } p,$$
For $p = 2,\ 3$ see also [54, App. C, §16].

According to Proposition 4.26 the distinction between stable and not-stable at a prime p depends on the reduction of the minimal discriminant. The following example 4.41 shows why it is necessary to study elliptic curves by considering global minimal Weierstrass polynomials, not just arbitrary Weierstrass polynomials.

Example 4.41 (Reduction mod p of a global minimal Weierstrass polynomial). Consider the elliptic curve $(E/\mathbb{Q}, O)$ from Example 4.39 defined by the inhomogeneous Weierstrass polynomial

$$F(X,Y) = Y^2 - (X^3 + 15.625) \in \mathbb{Q}[X,Y]$$

with discriminant

$$\Delta_F = -2^4 \cdot 3^3 \cdot 5^{12} \in \mathbb{Z}.$$

Note $15.625 = 5^6$.

i) The Weierstrass polynomial $F \in \mathbb{Z}[X,Y]$ is in short form but it is not global minimal. Reducing its coefficients *mod* $p = 5$ gives the Weierstrass polynomial in short form

$$F_5(X,Y) = Y^2 - X^3 \in \mathbb{F}_5[X,Y]$$

with discriminant

$$\Delta_{F_5} = 0 \in \mathbb{F}_5.$$

Hence the Weierstrass polynomial F_5 defines a singular cubic over $\mathbb{F}_5$ with a cusp. Note that the discriminant Δ_F contains the prime factor 5^{12}.

ii) Therefore we have to apply first the coordinate transformation with the matrix

$$\begin{pmatrix} 1/u^2 & 0 \\ 0 & 1/u^3 \end{pmatrix},\ u := 5,$$

which transforms $F(X,Y)$ to the global minimal Weierstrass polynomial

$$F'(X',Y') = Y'^2 - (X'^3 + 1)$$

with discriminant

$$\Delta_{F'} = -2^4 \cdot 3^3 \in \mathbb{Z}.$$

Reducing the coefficients of F' *mod* $p = 5$ creates the Weierstrass polynomial

$$F'_5(X',Y') = Y'^2 - (X'^3 + 1) \in \mathbb{F}_5[X',Y']$$

with discriminant

$$\Delta_{F'_5} = 3 \in \mathbb{F}_5.$$

The reduction of E *mod* $p = 5$ defines an elliptic curve E_5 over $\mathbb{F}_5$.

Remark 4.42 (Hasse estimate).

1. Important properties of an elliptic curve $E/\mathbb{Q}$ are encoded in the function, which attaches to each prime p with stable E_p the family

$$E_p(\mathbb{F}_{p^n}),\ n \in \mathbb{N}^*,$$

of orders of the groups of $\mathbb{F}_{p^n}$-valued points of the elliptic curve E_p. These groups collect those points from $E_p \subset \mathbb{P}^2(\overline{F}_p)$ with all coordinates in the finite fields $\mathbb{F}_{p^n}$.

We recall the following result of Hasse for the case $n = 1$:

$$\left|1 + p - card\ E_p(\mathbb{F}_p)\right| \leq 2 \cdot \sqrt{p}.$$

For a proof see [33, Theor. 10.5].

Hasse's result was conjectured by Artin. The value

$$1 + p$$

for comparison is motivated as follows: The field $\mathbb{F}_p$ has p elements. A Weierstrass equation

$$Y^2 = X^3 + AX + B$$

is quadratic in Y. Hence for each $x \in \mathbb{F}_p$ there exist at most two solutions $(x, y) \in \mathbb{A}^2(\mathbb{F}_p)$. Taking into account the point at infinity $O \in E_p(\mathbb{F}_p)$ gives the estimate

$$card\ E_p(\mathbb{F}_p) \leq (1 + 2p).$$

In the average, i.e. by choosing the Weierstrass polynomial at random, one could expect a 50% chance to find a solution (x, y) at all. Therefore $1 + p$ is a plausible average for $card\ E_p(\mathbb{F}_p)$.

One defines for any prime p the difference

$$a_p(E) := 1 + p - card\ E_p(\mathbb{F}_p)$$

between the average number and the actual number of $\mathbb{F}_p$-valued points of E.

2. See the PARI-file `Elliptic_curve_Hasse_estimate_05` for the numerical example of the Hasse inequality displayed in Figure 4.14.

```
==================================================
Elliptic curve: y^2 = x^3 + 0*x + (-17)
Discriminant: -124848 = [-1, 1; 2, 4; 3, 3; 17, 2]
j(E): 0
Number of points in E[F_p]:
--------------------------------
card E[F_2] = 2, |a_p| = 1, 2 * sqrt(2) = 2.828427125
card E[F_3] = 3, |a_p| = 1, 2 * sqrt(3) = 3.464101615
card E[F_5] = 6, |a_p| = 0, 2 * sqrt(5) = 4.472135955
card E[F_7] = 3, |a_p| = 5, 2 * sqrt(7) = 5.291502622
card E[F_11] = 12, |a_p| = 0, 2 * sqrt(11) = 6.633249581
card E[F_13] = 21, |a_p| = 7, 2 * sqrt(13) = 7.211102551
card E[F_17] = 17, |a_p| = 1, 2 * sqrt(17) = 8.246211251
card E[F_19] = 13, |a_p| = 7, 2 * sqrt(19) = 8.717797887
card E[F_23] = 24, |a_p| = 0, 2 * sqrt(23) = 9.591663047
card E[F_29] = 30, |a_p| = 0, 2 * sqrt(29) = 10.77032961
card E[F_31] = 21, |a_p| = 11, 2 * sqrt(31) = 11.13552873
card E[F_37] = 49, |a_p| = 11, 2 * sqrt(37) = 12.16552506
card E[F_41] = 42, |a_p| = 0, 2 * sqrt(41) = 12.80624847
card E[F_43] = 31, |a_p| = 13, 2 * sqrt(43) = 13.11487705
card E[F_47] = 48, |a_p| = 0, 2 * sqrt(47) = 13.71130920
card E[F_53] = 54, |a_p| = 0, 2 * sqrt(53) = 14.56021978
card E[F_59] = 60, |a_p| = 0, 2 * sqrt(59) = 15.36229150
card E[F_61] = 49, |a_p| = 13, 2 * sqrt(61) = 15.62049935
card E[F_67] = 73, |a_p| = 5, 2 * sqrt(67) = 16.37070554
card E[F_71] = 72, |a_p| = 0, 2 * sqrt(71) = 16.85229955
card E[F_73] = 64, |a_p| = 10, 2 * sqrt(73) = 17.08800749
card E[F_79] = 84, |a_p| = 4, 2 * sqrt(79) = 17.77638883
card E[F_83] = 84, |a_p| = 0, 2 * sqrt(83) = 18.22086716
card E[F_89] = 90, |a_p| = 0, 2 * sqrt(89) = 18.86796226
card E[F_97] = 103, |a_p| = 5, 2 * sqrt(97) = 19.69771560
card E[F_101] = 102, |a_p| = 0, 2 * sqrt(101) = 20.09975124
```

Fig. 4.14 The Hasse estimate

3. The sequence

$$(a_p(E))_{p\ prime}$$

will turn out to be a fundamental characteristic of the elliptic curve E, see Remark 4.45. These numbers determine also the cardinalities

$$card\ E_p(\mathbb{F}_{p^n})$$

for $n \geq 2$. The latter will serve as the generators of the ζ-function of E, see Definition 4.44.

Historically, the first example of a ζ-function is due to by L. Euler. The function has later be named *Riemann ζ-function*

Proposition 4.43 (ζ-function and Euler product). *The* Riemann ζ-function

$$\zeta : \{s \in \mathbb{C} : Re\ s > 1\} \to \mathbb{C},\ \zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

is holomorphic. The ζ-function

1. *extends to a meromorphic function on $\mathbb{C}$ with a single pole at $s = 1$. The pole has order $= 1$ and residue $= 1$.*

2. *It satisfies the functional equation with respect to reflection at the point $s = 1$*

$$\pi^{-s/2} \cdot \Gamma(s/2) \cdot \zeta(s) = \pi^{-(1-s)/2} \cdot \Gamma((1-s)/2) \cdot \zeta(1-s)$$

   with the Γ-function,

3. *and it has the product representation*

$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}}$$

   with the product taken over all primes p.

Proof. 1. See [64, Teil I, § 4].

2. See reference from part 1).

3. For each $N \in \mathbb{N}$ expand the finite product by using the geometric series and the unique prime factor decomposition of integers

$$\prod_{p<N} \frac{1}{1-p^{-s}} = \prod_{p<N} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots\right) = \sum{}' \frac{1}{n^s}$$

   with the sum on the right-hand side taken over all positive integers with all prime factors less than N. The limit $N \to \infty$ proves the claim, q.e.d.

From the viewpoint of the ring $\mathbb{Z}$ the Riemann ζ-function is a global object. Because it considers all primes $p \in \mathbb{Z}$ and collects as a product the local information encoded in the geometric series of p

$$\frac{1}{1-p^{-s}} = \sum_{n=0}^{\infty} \left(1/p^{-s}\right)^n$$

Apparently, all information about a prime p is just its value.

We now switch from the primes p of $\mathbb{Z}$ to the elliptic curves $E_p/\mathbb{F}_p$, which are the fibres of a given elliptic curve $E/\mathbb{Q}$ over its stable primes p. First we study the local information, i.e. the information encoded in $E_p/\mathbb{F}_p$. The curve E_p contributes as local information at the prime p the sequence of cardinalities of points with values in the finite fields of characteristic p

$$card\ E_p(\mathbb{F}_{p^n}),\ n \in \mathbb{N}^*.$$

Definition 4.44 (Zeta-function of an elliptic curve over $\mathbb{F}_p$). Consider an elliptic curve $E_p/\mathbb{F}_p$. The *ζ-function of E_p* is the formal power series with generator derived from the sequence $(card\ E_p(\mathbb{F}_{p^n}))_{n\in\mathbb{N}^*}$

$$Z(E_p,T) := exp\left(\sum_{n=1}^{\infty} card\ E_p(\mathbb{F}_{p^n}) \cdot \frac{T^n}{n}\right) \in \mathbb{Q}[[T]].$$

One checks by formal derivation

$$T \cdot \frac{d}{dT} log\, Z(E_p,T) = T \cdot \frac{Z'}{Z} = T \cdot \sum_{n=1}^{\infty} \left(card\ E_p(\mathbb{F}_p^n) \cdot T^{n-1}\right) = \sum_{n=1}^{\infty} \left(card\ E_p(\mathbb{F}_p^n) \cdot T^n\right)$$

Remark 4.45 (Properties of the ζ-function of an elliptic curve over $\mathbb{F}_p$). The ζ-function of an elliptic curve $E_p/\mathbb{F}_p$

$$Z(E_p,T) \in \mathbb{Q}[[T]]$$

has the following properties:

1. *Rationality*: The ζ-function is a rational function over the ring $\mathbb{Z}$, more precisely:

$$Z(E_p,T) = \frac{L(E_p,T)}{(1-T)\cdot(1-p\cdot T)} \in \mathbb{Z}(T)$$

with the quadratic polynomial

$$L(E_p,T) = 1 - a_p(E)\cdot T + p\cdot T^2,\ a_p(E) := 1 + p - card\ E_p(\mathbb{F}_p).$$

2. *Functional equation*: The ζ-function satisfies the functional equation

$$Z(E_p, 1/pT) = Z(E_p,T).$$

3. *Analogue of the Riemann hypothesis*: Both complex zeros $\alpha,\ \beta \in \mathbb{C}$ of $L(E_p,T)$ have modulus

$$|\alpha| = |\beta| = \sqrt{p}.$$

The proof of these properties is due to Weil, [56, Chap. V, Theor. 2.2].

Weil also stated and proved a generalization for projective algebraic curves curves $C_p/\mathbb{F}_p$ of arbitrary genus. If the curve C_p is the reduction mod p of a curve

$$C/\mathbb{Q}$$

then Weil's theorem shows the neat relation between the curve C_p and the complex curve $X(C) \subset \mathbb{P}^n$: The dimension of the polynomial in the numerator of the ζ-function of C_p is the first Betti number of the compact Riemann surface $X/\mathbb{C}$.

Moreover, Weil made a conjecture for the general case of higher-dimensional smooth projective algebraic varieties. Deligne proved the Weil conjecture. For an excellent introduction to the whole subject see [29, Appendix C].

The L-series $L(E)$ of an elliptic curve $E/\mathbb{Q}$ collects for each prime $p \in \mathbb{Z}$ the local information about the reduction E_p. Hence the L-series is a global object.

Definition 4.46 (L-series of an elliptic curve over $\mathbb{Q}$). The *L-series* of an elliptic curve $E/\mathbb{Q}$ is the function

$$L(E,-) : \{s \in \mathbb{C} : \ Re\ s > 3/2\} \to \mathbb{C},\ L(E,s) := \prod_p \frac{1}{Z(E_p, p^{-s})}$$

Remark 4.47 (L-series of an elliptic curve $E/\mathbb{Q}$).

1. The convergence of the L-series and its representation as an absolut convergent Dirichlet series with respect to the variable s follows from Hasse's estimate in Remark 4.42 and the theory of Euler products, see [33, Chap. X, Cor. 10.6]. Hence $L(E)$ is a holomorphic function.
   Due to the proof of the Shimura-Taniyama-Weil conjecture the L-series of an elliptic curve extends holomorphically to the whole complex plane. There are several unsolved conjectures about the arithmetic information encoded by the L-series of an elliptic curve. E.g. Birch and Swinnerton-Dyer conjectured

   $$rank\ E(\mathbb{Q}) = r$$

   with r equal to the *analytic rank* defined as the order of the zero of the L-series at $s = 1$

   $$r := ord(L(E);\ 1).$$

   The PARI script `Elliptic_curve_04_2` computes the analytic rank for some elliptic curves $E/\mathbb{Q}$ of higher analytic rank, see Figure 4.15.

   For more results and conjectures see [56, App. C, § 16].

2. The two polynomials in the denominator of the ζ-function $Z(E_p,T)$ evaluate at $T = p^{-s}$ as values of the Riemann ζ-function

$$\frac{1}{1-p^{-s}} = \zeta(s) \text{ and } \frac{1}{1-p^{1-s}} = \zeta(s-1)$$

They do not provide new information about the elliptic curve.

3. If one compares the L-series $L(E,s)$ of an elliptic curve $E/\mathbb{Q}$ with the Riemann ζ-function $\zeta(s)$ on the level of the two product representations

$$L(E,s) = \prod_p \frac{1}{Z(E_p,p^{-s})} \text{ and } \zeta(s) = \prod_p \frac{1}{1-p^{-s}}$$

then for each given prime p the local factor

$$Z(E_p,p^{-s}) \text{ corresponds to } \frac{1}{1-p^{-s}}$$

The geometric series on the right hand side depends only on the prime p, while the corresponding ζ-function on the left-hand side depends on p and on the reduction of the given elliptic curve $E/\mathbb{Q}$.

```
================================================
Elliptic_curve_04: Start.

Min. Weierstrass polynom.: Y^2 = X^3 + (7*X)
Analytic rank: 0

Min. Weierstrass polynom.: Y^2 = X^3 + (3*X)
Analytic rank: 1

Min. Weierstrass polynom.: Y^2 = X^3 + (73*X)
Analytic rank: 2

Min. Weierstrass polynom.: Y^2 = X^3 + (89*X)
Analytic rank: 2

Min. Weierstrass polynom.: Y^2 = X^3 + (-82*X)
Analytic rank: 3

Min. Weierstrass polynom.: Y^2 = X^3 + (-X^2) + (-24649*X) + (1355209)
Analytic rank: 4

Min. Weierstrass polynom.: Y^2 = X^3 + (-856967076*X)
Analytic rank: 4

Min. Weierstrass polynom.: Y^2 = X^3 + (-X^2) + (-2069247973*X) + (36191779888342)
Analytic rank: 6

Elliptic_curve_04: End
================================================
```

Fig. 4.15 Analytic rank of several elliptic curves $E/\mathbb{Q}$

Chapter 5
Introduction to Hecke theory and applications

5.1 Hecke operators of the modular group and their eigenforms

Definition 5.1 (Multiplicative function). A function

$$f : \mathbb{N}^* \to \mathbb{N}^*$$

is *muliplicative* if for each pair of coprime integers $m,\ n \in \mathbb{N}^*$ holds

$$f(n \cdot m) = f(n) \cdot f(m)$$

Proposition 5.2 (Multiplicativeness of the power sum function). *For each $k \in \mathbb{N}$ the function*

$$\sigma_k : \mathbb{N}^* \to \mathbb{N}^*,\ \sigma_k(n) := \sum_{d|n} d^k,$$

is multiplicative. It has the product representation

$$\sigma_k(n) = \prod_{j=1}^{N} \frac{p_j^{(e_j+1)k} - 1}{p_j^k - 1}$$

Proof. The prime decomposition

$$n = \prod_{j=1}^{N} p_j^{e_j},\ n \in \mathbb{N}^*,$$

and the formula for the finite geometric series imply the product formula

$$\sigma_k(n) = \left(p_1^k + p_1^{k\cdot 2} + \ldots + p_1^{k\cdot e_1}\right) \cdot \ldots \cdot \left(p_N^k + p_N^{k\cdot 2} + \ldots + p_N^{k\cdot e_N}\right) =$$

$$= \prod_{j=1}^{N} \left(\sum_{\nu=1}^{e_j} \left(p_j^k\right)^\nu \right) = \prod_{j=1}^{N} \frac{p_j^{(e_j+1)k} - 1}{p_j^k - 1}$$

And the product formula implies for coprime $n, m \in \mathbb{N}^*$

$$\sigma_k(n) \cdot \sigma_k(m) = \sigma_k(n \cdot m),\ q.e.d.$$

Corollary 5.3 (Eisenstein series are multiplicative). *For each even $k \geq 4$ the Fourier coefficents of the Eisenstein series*

$$\frac{-B_k}{2k} \cdot E_k(\tau) = \sum_{\nu=0}^{\infty} c_\nu \cdot q^\nu,\ q = e^{2\pi i \cdot \tau},$$

are multiplicative for $\nu \geq 1$.

Proof. We reduce the statement of the corollary to Proposition 5.2: Corollary 3.11 shows

$$E_k(\tau) = 1 - \frac{2k}{B_k} \cdot \sum_{\nu=1}^{\infty} \sigma_{k-1}(\nu)\ \cdot q^\nu,\ q = e^{2\pi i \cdot \tau}$$

and

$$\frac{-B_k}{2k} \cdot E_k(\tau) = \frac{-B_k}{2k} + \sum_{\nu=1}^{\infty} \sigma_{k-1}(\nu) \cdot q^\nu,$$

with Fourier coefficents

$$c_\nu = \sigma_{k-1}(\nu),\ \nu \geq 1,\ q.e.d.$$

Corollary 5.3 starts with the multiplicativeness of a well-known arithmetic function and derives the multiplicativeness of the Fourier coefficients of certain modular forms. Hecke theory goes the way in the opposite direction: Hecke operators single out certain modular forms and derive the multiplicativeness of their Fourier coefficients. Historically the first example is the normalized discriminant form

$$\frac{\Delta}{(2\pi)^{12}}$$

which gives the multiplicativeness of Ramanujan's τ-function.

Hecke operators are linear maps on modular forms, more precisely: For each even weight $k \in \mathbb{N}$ the Hecke algebra

$$\mathscr{H}_k(\Gamma) \subset End(M_k(\Gamma))$$

is a commutative subalgebra of endomorphisms, which restrict to endomorphisms of the vector spaces of cusp forms $S_k(\Gamma) \subset M_k(\Gamma)$. For fixed weight the Hecke algebra $\mathscr{H}_k(\Gamma)$ is generated by a family of Hecke operators $(T_m)_{m \in \mathbb{N}}$. They average

the transformation behaviour of modular forms with respect to certain equivalence classes of matrices

$$\Gamma_m \subset GL(2,\mathbb{R})^+$$

The equivalence classes are the orbits of a left action of the modular group on these matrices, which we have to study first.

Besides the two sequences of levels $N \in \mathbb{N}^*$ from Definition 2.9 and weights $k \in \mathbb{Z}$ from Definition 3.6 we now introduce a third sequence $m \in \mathbb{N}^*$. It is the sequence of the sets of integral matrices with determinant $= m$, see Definition 5.4. These matrices generalize the modular group Γ with respect to the determinant. They serve to define the Hecke operators which average the values of modular forms of a given weight and level. In addition, these integral matrices will serve in Section 6.2 to average as class invariants distinguished values of the j-invariant.

Definition 5.4 (Integral matrices with positive determinant). For any $m \in \mathbb{N}^*$ consider the set of matrices

$$\Gamma_m := \{M \in M(2\times 2,\mathbb{Z}) : det\ M = m\} \subset GL(2,\mathbb{Q})^+$$

and its subset

$$\Gamma_{m,prim} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_m :\ (a,b,c,d) = 1 \right\}$$

of *primitive* matrices. We denote by

$$\Phi_m : \Gamma \times \Gamma_m \to \Gamma_m, (A,M) \mapsto A \cdot M$$

the canonical Γ-left action, and by

$$\Phi_{m,prim} := \Phi_m | \Gamma_{m,prim} : \Gamma \times \Gamma_{m,prim} \to \Gamma_{m,prim}$$

its restriction. The respective orbits sets are denoted as the left quotients

$$\Gamma\backslash\Gamma_m \text{ and } \Gamma\backslash\Gamma_{m,prim}.$$

Remark 5.5 (Restriction of the Γ-action to the primitive matrices). The subset

$$\Gamma_{m,prim} \subset \Gamma_m$$

is stable under the Γ-left action Φ_m.

Proof. For the proof consider any

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma \text{ and } M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_{m,prim}.$$

The ideal generated by the coefficients of the product matrix $A \cdot M$

$$I := (\alpha a + \beta c, \alpha b + \beta d, \gamma a + \delta c, \gamma b + \delta d) \subset \mathbb{Z}$$

contains the element

$$\delta \cdot (\alpha a + \beta c) + (-\beta) \cdot (\gamma a + \delta c) = (\alpha\delta - \beta\gamma)a + (\delta\beta - \beta\delta)c = a$$

and similar for b, c, d with the other generators of I. Therefore

$$(1) = (a, b, c, d) \subset I$$

which implies

$$(1) = I$$

Hence the coefficients of the product matrix $A \cdot M$ are coprime, i.e.

$$\Phi_m(A, M) = A \cdot M \in \Gamma_{m,prim},\ q.e.d.$$

Lemma 5.6 shows that each orbit of the group action can be represented by a triangular matrix which facilitates many calculations.

Lemma 5.6 (Orbit sets of the left action). *Consider a positive integer $m \in \mathbb{N}^*$.*

1. A bijective map exists

$$\Gamma \backslash \Gamma_m \xrightarrow{\simeq} V(m) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Gamma_m : 0 \le b < d \right\}$$

to a subset of upper triangular matrices. The orbit set of Φ_m has cardinality $\sigma_1(m)$.

2. A bijective map exists

$$\Gamma \backslash \Gamma_{m,prim} \xrightarrow{\simeq} V(m, prim) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in V(m) :\ (a, b, d) = 1 \right\}.$$

The orbit set of $\Phi_{m,prim}$ has cardinality

$$\psi(m) := m \cdot \prod_{\substack{p \mid m \\ p\ prime}} (1 + (1/p))$$

Proof. 1. We define a map

$$p : \Gamma_m \to V(m),$$

which attaches to each $M \in \Gamma_m$ a distinguished triangular matrix $p(M)$ belonging to the same orbit. And we show that the matrix $p(M)$ depends only on the orbit of M:

i) Consider a fixed but arbitrary element

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_m.$$

We construct a matrix

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma$$

such that

$$A \cdot M = \begin{pmatrix} \alpha a + \beta c & \alpha b + \beta d \\ \gamma a + \delta c & \gamma b + \delta d \end{pmatrix} \in V(m) :$$

First, in order to remove the entry c of M we choose coprime integers $\gamma, \delta \in \mathbb{Z}$ with

$$\gamma \cdot a + \delta \cdot c = 0.$$

In order to obtain a matrix with $det\ = 1$ we choose integers $\alpha, \beta \in \mathbb{Z}$ with

$$\alpha \cdot \delta - \beta \cdot \gamma = 1.$$

Such a choice is possible because γ and δ are coprime. Set

$$A_1 := \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma.$$

Then

$$A_1 \cdot M = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$$

and

$$det\ (A_1 \cdot M) = det\ M = a' \cdot d' = m.$$

In particular $d' \neq 0$ and possibly after replacing A_1 by $-A_1$ even $a',\ d' > 0$.

Secondly, because $T \in \Gamma$, for any $k \in \mathbb{Z}$ also

$$A_2(k) := T^k \cdot A_1 \in \Gamma.$$

Then

$$A_2(k) \cdot M = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} a' & b' + k \cdot d' \\ 0 & d' \end{pmatrix}.$$

We choose $k_0 \in \mathbb{Z}$ such that

$$0 \leq b' + k_0 \cdot d' < d'$$

and set

$$A := A_2(k_0).$$

ii) The construction from part i) determines uniquely the element

$$A \cdot M \in V(m) :$$

Assume two matrices $A_i \in \Gamma$ such that

$$A_i \cdot M =: M_i \in V(m),\ i = 1,2.$$

Then

$$M = A_1^{-1} \cdot M_1 = A_2^{-1} \cdot M_2 \text{ or } A_{21} \cdot M_1 = M_2,\ A_{21} := A_2 \cdot A_1^{-1}.$$

Set

$$A_{21} =: \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \text{ and } M_i := \begin{pmatrix} a_i & b_i \\ 0 & d_i \end{pmatrix},\ i = 1,2.$$

From

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$$

follows:

- $\gamma \cdot a_1 = 0$, hence $\gamma = 0$.
- From $d_2 = \delta \cdot d_1$ follows $\delta > 0$. Together with $\alpha \cdot \delta = 1$ it implies $\alpha = \delta = 1$.
- As a consequence $a_1 = a_2$, $d_1 = d_2$, and $b_1 + \beta \cdot d_1 = b_2$.
- Because $0 \leq b_1, b_2 < d_1 = d_2$ we get $b_1 = b_2$ and $\beta = 0$.

As a consequence

$$A_{21} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } A_1 = A_2.$$

iii) Part i) and ii) show that

$$p : \Gamma_m \to V(m),\ M \mapsto A \cdot M,$$

is well-defined, and $p(M)$ belongs to the same orbit as M.

iv) The map p is surjectice because $V(m) \subset \Gamma_m$. In addition,

$$p(M_1) = p(M_2) \iff \exists\, A \in \Gamma \text{ with } A \cdot M_1 = M_2$$

$$\iff M_1 \text{ and } M_2 \text{ on the same orbit of } \Phi_m.$$

As a consequence p induces the bijective map

$$\Gamma \backslash \Gamma_m \xrightarrow{\simeq} V(m),\ \overline{M} \mapsto p(M).$$

v) The equality

$$card\ V(m) = \sigma_m(1)$$

follows at once from the explicit representation of the elements of $V(m)$: Each coefficient $d \geq 0$ satisfies $d|m$ and allows d different coefficients b.

2. The representation of the orbit set $\Gamma\backslash\Gamma_{m,prim}$ follows from part 1) by restriction. For the cardinality of $V(m,prim)$ see [38, Chap. 5, §1].

Corollary 5.7 (Complete representatives of the orbit set). *For each $\gamma \in \Gamma$:*

1. The set

$$V(m)\cdot\gamma \subset \Gamma_m$$

is a complete set of representatives of the orbit set $\Gamma\backslash\Gamma_m$, i.e. with respect to the canonical projection

$$\Gamma_m \to \Gamma\backslash\Gamma_m,\ M \mapsto [M],$$

holds the equality of sets

$$\Gamma\backslash\Gamma_m = \{[M] :\ M \in V(m)\} = \{[M\cdot\gamma] : M \in V(m)\}.$$

2. The set

$$V(m,prim)\cdot\gamma \subset \Gamma_{m,prim}$$

is a complete set of representatives of the orbit set $\Gamma\backslash\Gamma_{m,prim}$.

Proof. 1. Consider a given $\gamma \in \Gamma$. We show: For arbitrary but fixed $M \in V(m)$ exist an element

$$M_1 \in V(m)$$

and a unique matrix $A \in \Gamma$ such that

$$A\cdot M = M_1\cdot\gamma.$$

According to Lemma 5.6, applied to $M\cdot\gamma^{-1} \in \Gamma_m$, a unique element $A \in \Gamma$ exists with

$$M_1 := A\cdot(M\cdot\gamma^{-1}) \in V(m).$$

Then

$$M_1\cdot\gamma = A\cdot M.$$

Hence $M_1\cdot\gamma$ lies on the same orbit as M. As a consequence, the map

$$V(m) \to V(m),\ [M] \mapsto [M\cdot\gamma],$$

is well-defined and injective.

2. Analogously, q.e.d.

Lemma 5.8 (Complete sets of common representatives for left/right-action). *Consider an arbitrary but fixed prime p, and the left action*

$$\Phi_{left} : \Gamma \times \Gamma_p \to \Gamma_p, (\gamma, M) \mapsto \gamma\cdot M$$

1. *Besides the set $V(p)$ from Lemma 5.6 the set of symmetric matrices*

$$V_{sym} := \left\{ \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 1 & b \\ b & p+b^2 \end{pmatrix} : \ 0 \le b < p \right\}$$

is a complete set of representatives of Φ_{left} too.

2. *Consider a complete set $\mathscr{V}$ of representatives of Φ_{left} formed by symmetric matrices. Then also the system of adjoints*

$$\mathscr{V}^\sharp := \{M^\sharp : \ M \in \mathscr{V}\}, \ M^\sharp := (det\ M) \cdot M^{-1},$$

is a complete systems of representatives of Φ_{left}.

Proof. 1. For each $0 \le b < p$

$$\begin{pmatrix} 1 & b \\ b & p+b^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix}$$

Hence the matrices

$$\begin{pmatrix} 1 & b \\ b & p+b^2 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix}$$

belong to the same orbit of Φ_{left}.

2. i) Let

$$\Phi_{right} : \Gamma_p \times \Gamma \to \Gamma_p, \ (M, \gamma) \mapsto M \cdot \gamma,$$

be the corresponding right action of Γ. For each complete system $\mathscr{V}$ of representatives of Φ_{left} the set of transposed elements

$$\mathscr{V}^\top := \{\mathrm{v}^\top : \ \mathrm{v} \in \mathscr{V}\}$$

is a complete system of representatives of Φ_{right}: Assume $\mathrm{v} \in \Gamma_p$. Then also $\mathrm{v}^\top \in \Gamma_p$ and

$$\mathrm{v}^\top = A \cdot M$$

for suitable

$$A \in \Gamma \text{ and } \ M \in \mathscr{V}.$$

Hence

$$\mathrm{v} = M^\top \cdot A^\top$$

with $A^\top \in \Gamma^\top = \Gamma$.

As a consequence, if $\mathscr{V}$ is formed by symmetric matrices, then $\mathscr{V}$ is also a complete system of representatives for Φ_{right}.

ii) For given $w \in \Gamma_p$ set

$$\mathrm{v} := (det\ w) \cdot w^{-1} \in \Gamma_p.$$

Then

$$\mathrm{v} = w^{\sharp} \text{ and } det\ \mathrm{v} = (det\ w)^2 \cdot det\ w^{-1} = det\ w \text{ and } w = (det\ \mathrm{v}) \cdot \mathrm{v}^{-1}$$

Due to part i) exist

$$A \in \Gamma \text{ and } M \in \mathscr{V}$$

with

$$\mathrm{v} = M \cdot A$$

Then

$$det\ \mathrm{v} = det\ M$$

and

$$\mathrm{v}^{-1} = A^{-1} \cdot M^{-1}$$

and

$$w = \mathrm{v}^{-1} \cdot det\ \mathrm{v} = A^{-1} \cdot ((det\ M) \cdot M^{-1})$$

with

$$A^{-1} \in \Gamma^{-1} = \Gamma,\ q.e.d.$$

We recall a simple version of the elementary divisor theorem.

Proposition 5.9 (Elementary divisor theorem).

1. *For each matrix*

$$A \in \Gamma_m,\ m \in \mathbb{N}^*,$$

exist two matrices $\gamma_1, \gamma_2 \in \Gamma$ *with*

$$\gamma_1 \cdot A \cdot \gamma_2 = \begin{pmatrix} e_1 & 0 \\ 0 & e_2 \end{pmatrix} \text{ satisfying the divisor relation } e_1 | e_2.$$

2. *For each pair of primitive matrices*

$$A_1, A_2 \in \Gamma_{m,prim},\ m \in \mathbb{N}^*,$$

exist two matrices $\gamma_1, \gamma_2 \in \Gamma$ *with*

$$A_2 = \gamma_1 \cdot A_1 \cdot \gamma_2.$$

Proposition 5.9 is a special case of the *Smith normal form*, a result which holds for matrices over principal ideal domains.

Definition 5.10 (Hecke operators of the modular group). For any positive integer $m \geq 1$ the m-th *Hecke operator* is the $\mathbb{C}$-linear endomorphism of the algebra of modular forms

$$T_m : M_*(\Gamma) \to M_*(\Gamma)$$

which is defined on $M_k(\Gamma),\ k \in \mathbb{N}$, as

$$M_k(\Gamma) \to M_k(\Gamma), f \mapsto T_m f := \sum_{\Gamma \backslash \Gamma_m} f[M]_k.$$

Here the summation extends over an arbitrary complete set of representatives $M \in \Gamma_m$ of the orbit set $\Gamma \backslash \Gamma_m$ of the left action

$$\Gamma \times \Gamma_m \to \Gamma_m.$$

The value $f[M]_k$ does not depend on the choice of a representative from the orbit $\Gamma \cdot M$ because due to Lemma 3.4: For all $\alpha \in \Gamma$

$$f[\alpha \cdot M]_k = (f[\alpha]_k)[M]_k = f[M]_k$$

E.g., the summation in Definition 5.10 of the Hecke operator T_m may extend over the elements of $V(m)$ or over the elements of $V(m) \cdot \gamma, \gamma \in \Gamma$. Note $T_1 = id$.

Theorem 5.11 (Fourier coefficients of Hecke transforms).

1. *The Hecke operators from Definition 5.10 are well-defined, i.e. for each even weight k and for all* $m \geq 1$

$$f \in M_k(\Gamma) \implies T_m f \in M_k(\Gamma).$$

2. *For a modular form* $f \in M_k(\Gamma)$ *with Fourier expansion*

$$f(\tau) = \sum_{n=0}^{\infty} a_n \cdot q^n,\ q = e^{2\pi i \cdot \tau},$$

its Hecke transform $T_m f \in M_k(\Gamma)$ *has the Fourier expansion*

$$(T_m f)(\tau) = \sum_{n=0}^{\infty} b_n \cdot q^n$$

with Fourier coefficients

$$b_n = \sum_{\substack{r>0 \\ r \in (m,n)}} r^{k-1} \cdot a_{mn/r^2},\ n \in \mathbb{N},$$

in particular

$$b_0 = a_0 \cdot \sigma_{k-1}(m) \text{ and } b_1 = a_m$$

3. *The ideal of cusp forms is stable under all Hecke operators, i.e. for each* $m \in \mathbb{N}^*$

$$T_m(S_*(\Gamma)) \subset S_*(\Gamma).$$

Due to Theorem 5.11, part 1) we will use the same notation T_m for a Hecke operator and its restriction to a single modular space of fixed weight.

Proof. 1. To prove that $T_m f$ is a modular form of the same weight as f we have to verify the properties from Definition 3.6:

- Appararently $T_m f$ is holomorphic on $\mathbb{H}$.

- Weakly modularity: Consider a fixed but arbitrary matrix $\gamma \in \Gamma$. We replace the summation over the orbit set $V(m)$ by the summation over the complete set of representatives $V(m) \cdot \gamma$, see Corollary 5.7:

$$(T_m f)[\gamma]_k = \sum_{M \in V(m)} (f[M]_k)[\gamma]_k = \sum_{M \in V(m)} (f[M \cdot \gamma]_k) =$$

$$= \sum_{N \in V(m) \cdot \gamma} f[N]_k = \sum_{M \in V(m)} f[M]_k = T_m f.$$

- Holomorphy of $T_m f$ at the point ∞: To compute the Fourier series of $T_m f$ we use the summation with

$$M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in V(m)$$

For the computation of

$$(f[M]_k)(\tau) = f(M(\tau)) \cdot h(M, \tau)^{-k} \cdot (det\ M)^{k-1}$$

we employ the following intermediate results:

i)

$$\exp(2\pi i n \cdot M(\tau)) = \exp\left(2\pi i n \cdot \frac{a\tau + b}{d}\right) = e^{2\pi i n \cdot (a\tau/d)} \cdot e^{2\pi i n \cdot (b/d)},\ n \in \mathbb{N}.$$

ii)

$$\sum_{0 \le b < d} e^{2\pi i b \cdot (n/d)} = \begin{cases} d & \text{if } d|n \\ 0 & \text{otherwise} \end{cases}$$

The first case follows from

$$e^{2\pi i b \cdot (n/d)} = 1$$

for each of the d summands with $0 \le b < d$. The second case follows from the formula of the finite geometric series with argument $e^{2\pi i \cdot (n/d)}$:

$$\sum_{b=0}^{d-1} e^{2\pi i b \cdot (n/d)} = \frac{e^{2\pi i \cdot d \cdot (n/d)} - 1}{e^{2\pi i \cdot (n/d)} - 1} = 0$$

iii) We have

$$f(M(\tau)) = f\left(\frac{a\tau+b}{d}\right) = \sum_{n=0}^{\infty} a_n \cdot exp\left(2\pi in \cdot \frac{a\tau+b}{d}\right) =$$

$$= \sum_{n=0}^{\infty} a_n \cdot exp\left(2\pi in \cdot \frac{a\tau}{d}\right) \cdot exp\left(2\pi in \cdot \frac{b}{d}\right)$$

Hence

$$\sum_{b=0}^{d-1} f(M(\tau)) = \sum_{n=0}^{\infty} d \cdot a_{nd} \cdot q^{n(m/d)},\ q = exp(2\pi in\tau),$$

because

$$\sum_{b=0}^{d-1} f(M(\tau)) = \sum_{b=0}^{d-1} \left(\sum_{n=0}^{\infty} a_n \cdot e^{2\pi in(a\tau)/d} \cdot e^{2\pi in(b/d)} \right) =$$

$$= \sum_{n=0}^{\infty} \left(a_n \cdot e^{2\pi in(a\tau)/d} \cdot \sum_{b=0}^{d-1} e^{2\pi in(b/d)} \right) = \sum_{n=0}^{\infty} a_{nd} \cdot e^{2\pi ina\tau} \cdot d =$$

$$= d \cdot \sum_{n=0}^{\infty} a_{nd} \cdot q^{na} = d \cdot \sum_{n=0}^{\infty} a_{nd} \cdot q^{n(m/d)}$$

Due to part ii) the third last sum retains only summands with index $= nd$.

We now use the representation of the orbit set $\Gamma\backslash\Gamma_m$ from Lemma 5.6 and insert the Fourier series of f. We obtain due to the formula from part iii)

$$(T_m f)(\tau) = \sum_{M \in V(m)} f[M]_k(\tau) = m^{k-1} \cdot \sum_{M \in V(m)} h(M,\tau)^{-k} \cdot f(M(\tau)) =$$

$$= m^{k-1} \sum_{\substack{d>0 \\ d|m}} \frac{1}{d^k} \cdot \sum_{n=0}^{\infty} a_{nd} \cdot q^{n(m/d)} \cdot d = \sum_{\substack{d>0 \\ d|m}} \left(\frac{m}{d}\right)^{k-1} \left(\sum_{n=0}^{\infty} a_{nd} \cdot q^{n(m/d)} \right) =$$

$$= \sum_{\substack{d>0 \\ d \in (m,n)}} \left(\frac{m}{d}\right)^{k-1} \left(\sum_{n=0}^{\infty} a_n \cdot q^{(n/d)\cdot(m/d)} \right)$$

The substitution

$$(d,n) \mapsto (t = (n/d)\cdot(m/d),\ r = m/d)$$

provides

$$n = \frac{d^2 \cdot t}{m} = \left(\frac{d}{m}\right)^2 tm = \frac{tm}{r^2}.$$

Hence

$$(T_m f)(\tau) = \sum_{t=0}^{\infty} \left(\sum_{\substack{r>0 \\ r|(m,t)}} r^{k-1} \cdot a_{(tm)/r^2} \right) q^t$$

with the inner sum being finite. Apparently, the Fourier series has no coefficients with negative index. Hence $T_m f$ is holomorphic at $\infty \in \mathbb{H}^*$.

2. For the proof see the Fourier series from the previous part.

3. A cusp form satisfies $a_0 = 0$. The formula for the Fourier coefficients of $T_m f$ from part 2) shows that $T_m f$ is a cusp form again, q.e.d.

The following corollary specializes the general formula from Theorem 5.11. It gives the formula for the Fourier coefficients of the Hecke transform for prime indices.

Corollary 5.12 (Fourier coefficients with prime index of Hecke transforms). *Consider a modular form $f \in M_k(\Gamma)$ with Fourier coefficients $(a_n)_{n\in\mathbb{N}}$. Then the Fourier coefficients $(b_n)_{n\in\mathbb{N}}$ of its Hecke transform $T_m f$ satisfy for each prime index p*

$$b_p = \begin{cases} a_{mp} & \text{if } p \nmid m \\ a_{mp} + p^{k-1} \cdot a_{m/p} & \text{if } p|m \end{cases}$$

Proof. The claim follows from the third formula for the general case in Theorem 5.11:

- If $p \nmid m$ then $r|(p,m)$ implies $r = 1$.
- If $p|m$ then $r|(p,m)$ implies $r = 1$ or $r = p$; note $n = p$, q.e.d.

Corollary 5.13 (Simultaneous eigenvector of all Hecke operators). *The discriminant modular form*

$$\Delta \in S_{12}(\Gamma)$$

is a simultaneous eigenform of all Hecke operators, i.e. Δ is an eigenvector of all Hecke operators

$$T_m \in End(S_{12}(\Gamma)),\ m \geq 1.$$

The Fourier coefficients of the normalized discriminant modular form

$$\frac{\Delta}{(2\pi)^{12}} = \sum_{m=1}^{\infty} \tau_m \cdot q^m$$

are the corresponding eigenvalues, i.e. for all $m \in \mathbb{N}^*$

$$T_m(\Delta) = \tau_m \cdot \Delta.$$

Proof. According to Corollary 3.19 and Lemma 3.23 the vector space $S_{12}(\Gamma)$ of cusp forms of weight $k = 12$ is 1-dimensional. It has the discriminant modular form Δ from Definition 3.13 as a basis. Hence Δ is an eigenvector of each Hecke operator T_m, $m \geq 1$. To calculate the corresponding eigenvalue we recall the Fourier expansion of the normalized discriminant modular form from Proposition 3.14:

$$\frac{\Delta(\tau)}{(2\pi)^{12}} = \sum_{n=1}^{\infty} \tau_n \cdot q^n, \ \tau_1 = 1.$$

Theorem 5.11 provides the Fourier expansion

$$T_m\left(\frac{1}{(2\pi)^{12}} \cdot \Delta\right)(\tau) = \tau_m \cdot q + O(2).$$

Hence by comparing the linear term of the Fourier series on both sides

$$T_m(\Delta) = \tau_m \cdot \Delta, \ q.e.d.$$

Example 5.14 (Hecke operators). Consider the vector space of cusp forms $S_{28}(\Gamma)$. Due to Theorem 3.19 and Lemma 3.23

$$dim\ S_{28}(\Gamma) = 2.$$

The two cuspforms of weight 28

$$f_1 := \Delta \cdot E_4^4 \text{ and } f_2 := \Delta^2 \cdot E_4$$

are linearly independent because

$$ord(f_1;\infty) = 1 \text{ and } ord(f_2;\infty) = 2.$$

Hence (f_1, f_2) is a basis of $S_{28}(\Gamma)$. We consider the Hecke operator

$$T_2 : S_{28}(\Gamma) \to S_{28}(\Gamma).$$

The endomorphism has two distinct eigenvalues, hence it can be diagonalized. Figure 5.1 shows

- the Fourier series of f_1 and f_2

- the Fourier series of $T_2 f_1$ and $T_2 f_2$
- the Hecke matrix of T_2 with respect to the basis (f_1, f_2)
- the eigenvalues of T_2
- the Fourier coefficients of two corresponding eigenvectors (v_1, v_2) of T_2, normalized with linear Fourier coefficient $= 1$,
- the representation of the eigenvectors with respect to (f_1, f_2)

```
====================================================
Hecke_matrix_02, Start

Hecke operator T_2: S_28(Gamma_0(1)) ---> S_28(Gamma_0(1))

Basis of S_28(Gamma_0(1)): f1 = Delta * E_4^4, f2 = Delta^2 * E_4 with Fourier series:

f1_ser: q + 936*q^2 + 331452*q^3 + 53282368*q^4 + O(q^5)

f2_ser: q^2 + 192*q^3 - 8280*q^4 + O(q^5)
----------------------------------

heck_2_f1_ser: 936*q + 187500096*q^2 + 36142047072*q^3 + O(q^4)

heck_2_f2_ser: q - 8280*q^2 - 1438020*q^3 + O(q^4)
----------------------------------

Matrix of Hecke operator T_2 with respect to basis (f1,f2): [936, 1; 186624000, -9216]
----------------------------------

Eigenvalues: -18713.59859, 10433.59859
----------------------------------

v_1: 1.000000000*q - 18713.59859*q^2 - 3441270.930*q^3 + 215981044.4*q^4 + O(q^5)

v_2: 1.000000000*q + 10433.59859*q^2 + 2154990.930*q^3 - 25357748.36*q^4 + O(q^5)
----------------------------------

v_1 = 1.000000000 * f1 + -19649.59859 * f2

v_2 = 1.000000000 * f1 + 9497.598595 * f2
----------------------------------
```

Fig. 5.1 Hecke operator $T_2 \in End(S_{28}(\Gamma))$

The result from Figure 5.1 has been computed by the PARI script `Hecke_matrix_02`.

We give an analogue to the Hecke operators from the theory of quadrics. The preface of the textbook [17] chooses the analogue as an introduction to the theory of modular forms. Corollary 5.13 represents the discriminant modular form Δ as simultaneous eigenform of all Hecke operators $(T_m)_{m \geq 1}$ acting on the complex vector space

$$V := S_{12}(\Gamma).$$

The corresponding eigenvalues are the Fourier coefficients of Δ. Remark 5.15 translates the law of quadratic reciprocity from algebraic number theory into a similar shape.

Remark 5.15 (Reduction of quadrics mod p).

1. The *Legendre symbol* considers an odd prime $p \in \mathbb{Z}$, and determines for each integer $d \in \mathbb{Z}$ whether d is a square mod p. The Legendre symbol is defined as

$$\left(\frac{d}{p}\right) := \begin{cases} +1 & d \not\equiv 0 \ mod\ p \text{ and } d \text{ quadratic rest } mod\ p \\ -1 & d \not\equiv 0 \ mod\ p \text{ and } d \text{ not quadratic rest } mod\ p \\ 0 & d \equiv 0 \ mod\ p \end{cases}$$

   The law of quadratic reciprocity relates the Legendre symbol of two odd primes $p \neq q$ according to the formula

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & p \equiv 1 \mod 4 \text{ or } q \equiv 1 \mod 4 \\ -\left(\frac{q}{p}\right) & p \equiv 3 \mod 4 \text{ and } q \equiv 3 \mod 4 \end{cases}$$

2. Consider an arbitrary, but fixed integer $d \neq 0$ and the quadratic polynomial

$$F(X) := X^2 - d \in \mathbb{Z}[X]$$

   which defines the affine quadric $Q/\mathbb{Q}$

$$\{x \in \mathbb{C} : \ F(x) = 0\}.$$

   For each prime p we consider the reduction *mod p*

$$F_p(X) := X^2 - d_p \in \mathbb{F}_p[X]$$

   and the set $Q(\mathbb{F}_p)$ of points of Q with coordinates from $\mathbb{F}_p$.

   Analogously to Remark 4.42 for elliptic curves we define

$$a_p(Q) := card\ Q(\mathbb{F}_p) - 1.$$

   The number 1 in the definition is the average number of solutions *mod p*. The values $a_p(Q)$ extend from prime indices to $a_n(Q)$, $n \in \mathbb{N}$, and satisfy the product rule

$$a_{nm}(Q) = a_n(Q) \cdot a_m(Q),\ n,m \in \mathbb{N}^*.$$

   For odd prime p the number $a_p(Q)$ equals the *Legendre symbol*

$$a_p(Q) = \left(\frac{d}{p}\right).$$

Due to the Law of Quadratic Reciprocity and its two supplements the Legendre symbol depends only on the residue class $p \bmod 4d$.

3. We now represent the sequence $(a_p(Q))_{p \text{ prime}}$ as a sequence of eigenvalues of a simultaneous eigenvector for a suitable sequence of linear endomorphisms $(T_p)_{p \text{ prime}}$. Our aim is to formulate an analogue of the modular group, of modular functions and of Hecke operators:

   Set
   $$N = N_Q := 4|d|,$$
   and consider the multiplicative group
   $$G := (\mathbb{Z}/N\mathbb{Z})^*,$$
   and the complex vector space of functions defined on G
   $$V := \{f : G \to \mathbb{C}\}.$$
   Eventually, as an analogue to the Hecke operators we introduce the family of linear endomorphisms $(T_p)_{p \text{ prime}}$ of V defined as
   $$(T_p f)(n) := \begin{cases} f(p \cdot n) & p \nmid N \\ 0 & p \mid N \end{cases}$$
   for $n \in G$. We claim: All endomorphism $(T_p)_{p \text{ prime}}$ have a simultaneous eigenvector, namely the distinguished function
   $$f_Q : G \to \mathbb{C},\ f(n) := a_n(Q).$$
   Note that f_Q is well-defined on the residue classes of G because the Legendre symbol depends only on the residue class $p \bmod 4d$. Computing the eigenvalues we get for all $n \in G$
   $$T_p(f_Q)(n) = \begin{cases} f_Q(p \cdot n) = a_{pn}(Q) = a_p(Q) \cdot a_n(Q) & p \nmid N \\ 0 & p \mid N \end{cases}$$
   As a consequence, for all primes $p \in \mathbb{Z}$
   $$T_p(f_Q) = a_p(Q) \cdot f_Q.$$

It is not by chance that in Example 5.14 the Hecke endomorphism $T_2 \in End(S_{28}(\Gamma))$ can be diagonalized. Theorem 5.18 will show: The Hecke algebra of a given weight

is commutative. And Theorem 5.26 will show that the Hecke operators are selfadjoint with respect to a certain Hermitian scalar product on the cusp forms. Hence all Hecke operators on cusp forms can be simultaneously diagonalized.

Definition 5.16 (Hecke algebra of weight k). The *Hecke algebra* of even weight $k \in \mathbb{N}$

$$Hecke_k(\Gamma) \subset End(M_k(\Gamma))$$

is the subalgebra spanned by the family $(T_m|M_k(\Gamma))_{m\in\mathbb{N}}$ of Hecke operators.

To prepare the proof of Theorem 5.18 about the Hecke algebra we consider for two matrices

$$M_j = \begin{pmatrix} a_j & b_j \\ & \\ 0 & d_j \end{pmatrix} \in V(n_j),\ j = 1,2$$

the components of the product

$$M_1 \cdot M_2 = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1d_2 \\ & \\ 0 & d_1d_2 \end{pmatrix} \in \Gamma_{n_1\cdot n_2}$$

We want to show that the products form a complete set of representatives of the Γ-left action on $\Gamma_{n_1\cdot n_2}$

Lemma 5.17 (Restsystem for $V(n_1 \cdot n_2)$). *For $j = 1,2$ consider two coprime numbers*

$$n_j \in \mathbb{N}^*, j = 1,2.$$

1. *For given positive numbers a_j, d_j with $n_j = a_j \cdot d_j$ the map of restsystems*

   $$\phi : \{0,...,d_1-1\} \times \{0,...,d_2-1\} \to \{0,...,d_1 \cdot d_2\},\ (b_1,b_2) \mapsto a_1 \cdot b_2 + b_1 \cdot d_2,$$

   is bijective.

2. *The map on the product of complete systems of representatives*

   $$V(n_1) \times V(n_2) \to \Gamma_{n_1\cdot n_2},\ (M_1,M_2) \mapsto M_1 \cdot M_2,$$

   maps injectively onto a complete system of representatives of $\Gamma\backslash\Gamma_{n_1\cdot n_2}$.

Proof. 1. It suffices to show that ϕ is injective because its domain and codomain have the same finite cardinality. Therefore assume

$$(\tilde{b}_1,\tilde{b}_2) \in (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}) \text{ with } \phi((b_1,b_2)) = \phi((\tilde{b}_1,\tilde{b}_2))$$

i.e.

$$a_1 \cdot b_2 + b_1 \cdot d_2 \equiv a_1 \cdot \tilde{b}_2 + \tilde{b}_1 \cdot d_2 \mod d_1 d_2$$

Then

$$a_1(b_2 - \tilde{b}_2) \equiv (\tilde{b}_1 - b_1)d_2 \mod d_1 d_2$$

which implies

$$a_1(b_2 - \tilde{b}_2) \equiv 0 \mod d_2$$

Because

$$gcd(n_1, n_2) = 1 \implies gcd(a_1, d_2) = 1$$

therefore

$$b_1 - \tilde{b}_1 \equiv 0 \mod d_1, \text{ i.e. } b_1 \equiv \tilde{1}_2 \mod d_1$$

which implies

$$b_2 = \tilde{b}_2.$$

Analogously $b_1 = \tilde{b}_1$.

2. In addition to part 1) one uses the bijectivity of the maps of divisor sets

$$\{a_1 \in \mathbb{N}^* : a_1 | n_1\} \times \{a_2 \in \mathbb{N}^* : a_2 | n_2\} \to \{a \in \mathbb{N}^* : a | n_1 n_2\},\ (a_1, a_2) \mapsto a_1 a_2,\ q.e.d.$$

Theorem 5.18 (The Hecke algebras are commutative). *For each weight $k \in \mathbb{N}$ the Hecke algebra $Hecke_k(\Gamma)$ is commutative. It has the following properties:*

1. *For coprime $n, m \in \mathbb{N}^*$ Hecke operators are multiplicative:*

$$T_m \circ T_n = T_{m \cdot n}$$

2. *For a prime power $p^r,\ r \geq 1$, holds*

$$T_{p^r} \circ T_p = T_{p^{r+1}} + p^{k-1} \cdot T_{p^{r-1}}$$

In particular

$$T_{p^r} \in \mathbb{Z}[T_p]$$

3. *The algebra $Hecke_k(\Gamma)$ is generated by the family $T_p,\ p$ prime.*

Proof. 1. For each $f \in M_k(\Gamma)$ Lemma 5.17 and Lemma 3.4 imply

$$(T_m \circ T_n)(f) = T_m(T_n f) = \sum_{M_2 \in V(m)} (T_n f)[M_2]_k = \sum_{M_2 \in V(m)} \left(\sum_{M_1 \in V(n)} (f[M_1]_k)[M_2]_k \right) =$$

$$= \sum_{\substack{M_1 \in V(n) \\ M_2 \in V(m)}} f[M_1 \cdot M_2]_k = \sum_{M \in V(n \cdot m)} f[M]_k = T_{nm} f$$

2. The proof is by induction. First one replaces Lemma 5.17 by two analogous results about restsystems. Secondly, one evaluates the formula for the Fourier coefficients of Hecke transforms from Theorem 5.11 and Corollary 5.12, cf. [36, Kap. IV, §2.2].

3. Due to part 1) the family $(T_m)_{m\in\mathbb{N}}$ of all Hecke operators generates the same algebra as the family of Hecke operators with all prime power indices

$$T_{p^r},\ p \text{ prime },\ r \in \mathbb{N}.$$

Due to part 2) for each fixed prime p the family $T_{p^r},\ r \in \mathbb{N}$, generates the same algebra as the single Hecke operator T_p.

The commutativity of the Hecke algebras follows from the parts 1) and 3) , q.e.d.

5.2 The Petersson scalar product

Next we introduce a Hermitian scalar product on the vector space of cusp forms of a given congruence subgroup $\Gamma_0(N)$.

Definition 5.19 (Hyperbolic volume form). The *hyperbolic volume form* on $\mathbb{H}$ is the differential form

$$d\mu(\tau) := \frac{dx\wedge dy}{y^2},\ \tau = x+iy \in \mathbb{H}$$

Lemma 5.20 (Invariance of the hyperbolic volume form). *The hyperbolic volume form is $GL(2,\mathbb{R})^+$-invariant, i.e. for each $\gamma \in GL(2,\mathbb{R})^+$ holds*

$$\gamma^* d\mu = d\mu$$

Proof. For each

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2,\mathbb{R})^+$$

we have to show: For all $\tau \in \mathbb{H}$

$$(\gamma^* d\mu)(\tau) = d\mu(\tau):$$

For the proof one uses the usual coordinate transformation

$$dx\wedge dy = \frac{i}{2}\, d\tau \wedge d\overline{\tau}$$

which implies

$$d\mu(\tau) = \frac{i}{2} \cdot \frac{d\tau \wedge d\overline{\tau}}{(Im\ \tau)^2}$$

and

$$(\gamma^* d\mu)(\tau) = \frac{i}{2} \cdot \frac{d\gamma(\tau) \wedge d\gamma(\overline{\tau})}{(Im\ \gamma(\tau))^2}$$

The proof of Proposition 3.1 and the formulas from Remark 2.8

$$Im\ \gamma(\tau) = det(\gamma) \cdot \frac{Im\ \tau}{|c\tau + d|^2} \text{ and } d\gamma(\tau) = det(\gamma) \cdot \frac{d\tau}{(c\tau + d)^2}$$

imply

$$(\gamma^* d\mu)(\tau) = d\mu(\tau),\ q.e.d.$$

Proposition 5.21 (Integration over fundamental domains).

1. *The standard fundamental domain $\mathscr{D}$ of Γ has the volume*

$$vol\ \mathscr{D} := \int_{\mathscr{D}} d\mu = \frac{\pi}{3}$$

2. *The fundamental domain of a congruence subgroup $\Gamma_0(N)$ has the volume*

$$vol\ \mathscr{D}(\Gamma_0(N)) := \int_{\mathscr{D}(\Gamma_0(N))} d\mu = [\Gamma : \Gamma_0(N)] \cdot vol\ \mathscr{D} = \frac{\pi}{3} \cdot N \cdot \prod_{p|N} (1 + (1/p)),$$

   independent from the chosen left coset decomposition of Γ with respect to $\Gamma_0(N)$.

3. *Consider a continuous function*

$$\Omega : \mathbb{H} \to \mathbb{C}$$

   with fixed group

$$\Gamma(\Omega) := \{A \in \Gamma :\ \Omega \circ A = \Omega\}.$$

   Then for each subgroup $K \subset \Gamma(\Omega)$ with $\pm\mathbb{1} \in K$ and for each pair$(\mathscr{F}_1, \mathscr{F}_2)$ of fundamental domains of K:

$$\int_{\mathscr{F}_1} \Omega\ d\mu = \int_{\mathscr{F}_2} \Omega\ d\mu$$

   if at least one of the two integrals is finite.

Apparently, part 2) of Proposition 5.21 is a special case of part 3).

Proof. 1. From the geometrical description of $\mathscr{D}$, see Figure 2.1:

$$\int_{\mathscr{D}} d\mu = \int_{-1/2}^{1/2} \left(\int_{\sqrt{1-x^2}}^{\infty} \frac{dy}{y^2} \right) dx = \int_{-1/2}^{1/2} \left((-1/y) \Big|_{\sqrt{1-x^2}}^{\infty} \right) dx =$$

$$= \int_{-1/2}^{1/2} \frac{dx}{\sqrt{1-x^2}} = arcsin\, x \Big|_{-1/2}^{1/2} = \pi/6 - (-\pi/6) = \pi/3$$

2. The general formula for

$$vol\ (\mathscr{D}(\Gamma_0(N))) = [\Gamma : \Gamma_0(N)] \cdot vol\ \mathscr{D}$$

follows from

- the index formula Proposition 2.14,
- the representation of the fundamental domain as disjoint union

$$\mathscr{D}(\Gamma_0(N)) = \bigcup_{j=1}^{[\Gamma:\Gamma_0(N)]} \gamma_j^{-1}(\mathscr{D})$$

see Remark 2.17,

- and the invariance of the volume form $d\mu$ according to Lemma 5.20.

3. For $A \in \Gamma(\phi)$ the usual transformation formula for integrals and the invariance of the hyperbolic volume form $d\mu$ imply for each measurable set $B \subset \mathbb{H}$

$$\int_B \Omega\, d\mu = \int_{A(B)} \Omega\, d\mu$$

If one splits $\mathbb{H}$ as the disjoint union of the sets $A(\mathscr{F}_2)$, $A \in K$, and observes that $\pm\mathbb{1}$ act as identity on $\mathbb{H}$, which introduces the factor $= 1/2$, then

$$\int_{\mathscr{F}_1} \Omega\, d\mu = (1/2) \cdot \sum_{A \in K} \int_{A(\mathscr{F}_2) \cap \mathscr{F}_1} \Omega\, d\mu = (1/2) \cdot \sum_{A \in K} \int_{\mathscr{F}_2 \cap A^{-1}(\mathscr{F}_1)} \Omega\, d\mu =$$

$$= (1/2) \cdot \sum_{A \in K} \int_{A(\mathscr{F}_1) \cap \mathscr{F}_2} \Omega\, d\mu = \int_{\mathscr{F}_2} \Omega\, d\mu,\ q.e.d.$$

Definition 5.22 (Petersson scalar product). For each level $N \in \mathbb{N}$ and each even weight $k \in \mathbb{N}$, $k \geq 0$, the *Petersson scalar product* on the cusp space $S_k(\Gamma_0(N))$ is the $\mathbb{C}$-sesquilinear map

$$< -, - >_{\Gamma_0(N)} : S_k(\Gamma_0(N)) \times S_k(\Gamma_0(N)) \to \mathbb{C},$$

$$< f,g >_{\Gamma_0(N)} := \frac{1}{vol\ \mathscr{D}(\Gamma_0(N))} \cdot \int_{\mathscr{D}(\Gamma_0(N))} f(\tau) \cdot \overline{g(\tau)} \cdot (Im\ \tau)^k\ d\mu(\tau)$$

Note

$$vol\ \mathscr{D}(\Gamma_0(N)) < \infty \text{ because } [\Gamma : \Gamma_0(N)] < \infty.$$

Definition 5.22, see [17, Chap. 5, Def. 5.4.1], implies: If

$$\Gamma_1 := \Gamma_0(N_1) \subset \Gamma_2 := \Gamma_0(N_2) \text{ and } f,\ g \in S_k(\Gamma_2)$$

then

$$< f,g >_{\Gamma_1} = < f,g >_{\Gamma_2}$$

While [36, Kap. IV, 3.2], which considers only the modular group Γ, employs in Definition 5.22 instead before the integral the factor $= 1$.

Theorem 5.23 (Petersson scalar product). *The map from Definition 5.22*

$$< -,- >_{\Gamma_0(N)}$$

is well-defined. It is a Hermitian scalar product on the vector space $S_k(\Gamma_0(N))$ of cusp forms.

Proof. For each continuous and bounded function

$$\phi : \mathbb{H} \to \mathbb{C}$$

Proposition 5.21 implies the estimate

$$\int_{\mathscr{D}(\Gamma_0(N))} |\phi|\ d\mu \leq vol(\mathscr{D}(\Gamma_0(N))) \cdot \|\phi\|_{\mathbb{H}} < \infty$$

To prove that the Petersson scalar product of two modular forms $f,g \in S_k(\Gamma_0(N))$ is well-defined, consider the continuous function

$$\phi : \mathbb{H} \to \mathbb{C},\ \phi(\tau) := f(\tau) \cdot \overline{g(\tau)} \cdot (Im\ \tau)^k.$$

i) To prove the boundedness of ϕ it suffices to prove for any $\gamma \in \Gamma$ that the restriction

$$(\phi \circ \gamma)|\mathscr{D}$$

is bounded: Being continuous $\phi \circ \gamma$ is bounded on each compact subset of $\overline{\mathscr{D}}$. Secondly, the Fourier expansions

$$f[\gamma]_k(\tau) = \sum_{n=1}^{\infty} \alpha_n \cdot q_h^n \text{ and } g[\gamma]_k(\tau) = \sum_{n=1}^{\infty} \beta_n \cdot q_h^n,\ q_h = e^{2\pi i \tau/h},$$

for a suitable $h \in \mathbb{N}$, show that both cusp forms are of type $O(q_h)$ in the limit $Im\ \tau \to \infty$. Then

$$|q_h| = |e^{2\pi i\tau/h}| = e^{-2\pi\cdot(Im\ \tau)/h} \implies O(q_h^2)\cdot(Im\ \tau)^k = o(q_h)$$

ii) The function ϕ is Γ-invariant because for each $\gamma \in \Gamma$ and $\tau \in \mathbb{H}$ according to Definition 3.6

$$\phi(\gamma(\tau)) = f(\gamma(\tau))\cdot\overline{g(\gamma(\tau))}\cdot(Im\ \gamma(\tau))^k =$$
$$= f[\gamma]_k(\tau)\cdot h(\gamma,\tau)^k\cdot\overline{g[\gamma]_k(\tau)}\cdot\overline{h(\gamma,\tau)}^k\cdot(Im\ \tau)^k\cdot|h(\gamma,\tau)|^{-2k} =$$
$$= f[\gamma]_k(\tau)\cdot\overline{g[\gamma]_k(\tau)}\cdot(Im\ \tau)^k = f(\tau)\cdot\overline{g(\tau)}\cdot(Im\ \tau)^k = \phi(\tau)$$

Hence part i) and Proposition 5.21, part 3) imply that the Petersson scalar product is independent from the choice of a fundamental domain, which finishes the proof, q.e.d.

Note. The proof of Theorem 5.23 shows that the Hermitian scalar product $< f,g >_{\Gamma_0(N)}$ is also defined for two modular forms $f,\ g \in M_k(\Gamma_0(N))$ if at least one of them is a cusp form.

Recall from Remark 2.8 the operation of $GL(2,\mathbb{Q})^+$ and its subgroups on $\mathbb{H}$

Lemma 5.24 (Petersson scalar product). *Consider*

- *a weight $k \in \mathbb{N}$ and two cusp forms $f,\ g \in S_k(\Gamma)$*
- *together with a prime p and a matrix $M \in \Gamma_p$.*

Then:

1. Transformation formula for subgroups of finite index*: Each subgroup $K \subset \Gamma(\Omega)$ with finite index $[\Gamma(\Omega) : K] < \infty$ satisfies*

$$\frac{1}{[\Gamma(\Omega) : K]}\cdot\int_{\mathscr{D}(K)} \Omega\ d\mu = \int_{\mathscr{D}(\Gamma(\Omega))} \Omega\ d\mu$$

   if at least one of the two integrals is finite.

2. Finiteness of the index under conjugation*: The extended principal congruence subgroup of Γ of level p*

$$\tilde{\Gamma}(p) := \{L \in \Gamma :\ L \equiv \pm\mathbb{1}\ mod\ p\}$$

   has finite index. In addition, define for each pair of continuous functions

$$h_1, h_2 : \mathbb{H} \to \mathbb{C}$$

the function

$$\Omega(h_1,h_2):\mathbb{H}\to\mathbb{C},\ \Omega(h_1,h_2)(\tau):=(h_1\cdot\overline{h}_2)(\tau)\cdot(Im\ \tau)^k$$

Then with respect to the fixed groups

$$\Gamma(\Omega(f[M]_k,g))\ and\ \Gamma(\Omega(f,g[M^\sharp]_k))$$

holds the inclusion of subgroups:

$$\tilde{\Gamma}(p)\subset\Gamma(\Omega(f[M]_k,g))\ \ and\ \ M^{-1}\tilde{\Gamma}(p)M\subset\Gamma(\Omega(f[M]_k,g)),$$

and both subgroups have finite index, and analogously for

$$\tilde{\Gamma}(p)\subset\Gamma(\Omega(f,g[M^\sharp]_k))\ \ and\ \ M\tilde{\Gamma}(p)M^{-1}\subset\Gamma(\Omega(f,g[M^\sharp]_k)).$$

3. Invariance of the index under conjugation*:*

$$[\Gamma:\tilde{\Gamma}(p)]=[\Gamma:M^{-1}\tilde{\Gamma}(p)M]$$

Proof. Cf. [36, Kap. IV, §3.3]. Because k is fixed during the whole computation we simplify the notation $[-]:=[-]_k$.

1. Consider a fundamental domain $\mathscr{F}$ of $\Gamma(\Omega)$. Then each decomposition of $\Gamma(\Omega)$ into the finite number $[\Gamma(\Omega):K]$ of left classes with respect to K

$$\Gamma(\Omega)=\dot{\bigcup}_\nu M_\nu^{-1}\cdot K$$

provides a fundamental domain of K

$$\mathscr{G}=\dot{\bigcup}_\nu M_\nu(\mathscr{F})$$

Proposition 5.21, part 3), applied to each pair $(\mathscr{F},M_\nu(\mathscr{F}))$ of fundamental domains of $\Gamma(\Omega)$, implies

$$\int_{M_\nu\mathscr{F}}\Omega\ d\mu=\int_{\mathscr{F}}\Omega\ d\mu,$$

hence

$$\int_{\mathscr{D}(K)}\Omega\ d\mu=\int_{\mathscr{G}}\Omega\ d\mu=\sum_\nu\int_{M_\nu(\mathscr{F})}\Omega\ d\mu=$$

$$=\sum_\nu\int_{\mathscr{F}}\Omega\ d\mu=[\Gamma(\phi):K]\cdot\int_{\mathscr{D}(\Gamma(\Omega))}\Omega\ d\mu$$

2. i) According to Proposition 2.14

$$[\Gamma:\Gamma(p)]<\infty\ \text{hence also}\ [\Gamma:\tilde{\Gamma}(p)]<\infty.$$

Each element $L \in \tilde{\Gamma}(p) \subset \Gamma$ with decomposition

$$L = \pm\mathbb{1} + p \cdot A,\ A \in M(2 \times 2, \mathbb{Z}).$$

has the conjugate

$$L_0 := MLM^{-1} = M(\pm\mathbb{1} + p \cdot A)M^{-1} = \pm\mathbb{1} + M(pA)M^{-1} = \pm\mathbb{1} + MAM^{\sharp}$$

Hence

$$L_0 M = ML \text{ and } L_0 \in \Gamma$$

which implies

$$(f[M])[L] = (f[L_0])[M] = f[M].$$

Because $\tilde{\Gamma}(p) \subset \Gamma$ also

$$g[L] = g.$$

The two L-invariant elements

$$f[M] \text{ and } g$$

satisfy for $\tau \in \mathbb{H}$ the transformation formula

$$(f[M] \cdot \overline{g})(L(\tau)) = (f[M] \cdot \overline{g})(\tau) \cdot |h(L,\tau)|^{2k} :$$

We compute

$$(f[M] \cdot \overline{g})(L(\tau)) = f[M](L(\tau)) \cdot \overline{g}(L(\tau)) = (f[M][L])(\tau) \cdot h(L,\tau)^k \cdot \overline{g}(L(\tau)) =$$

$$= f[M](\tau) \cdot h(L,\tau)^k \cdot \overline{g}[L](\tau)\ \cdot \overline{h(L,\tau)^k} = f[M](\tau) \cdot \overline{g}(\tau) \cdot |h(L,\tau)|^{2k}$$

Multiplying by $(Im\ L(\tau))^k$ both sides of the transformation formula for

$$f[M] \text{ and } g$$

and using the transformation formula for the imaginary part of the argument

$$Im\ L(\tau) = (Im\ \tau) \cdot h(L,\tau)^{-2}$$

shows

$$(f[M] \cdot \overline{g})(L(\tau)) \cdot (Im\ L(\tau))^k = (f[M] \cdot \overline{g})(\tau) \cdot (Im\ \tau)^k$$

or

$$\Omega(f[M], g) \circ L = \Omega(f[M], g)$$

Because $L \in \tilde{\Gamma}(p)$ is arbitrary we have shown

$$\tilde{\Gamma}(p) \subset \Gamma(\Omega(f[M], g))$$

The finiteness of the index of $\tilde{\Gamma}(p)$ in the fixgroups follow from the finiteness

$$[\Gamma : \tilde{\Gamma}(p)] < \infty$$

ii) For arbitrary $k \in \mathbb{N}$ holds

$$M\tilde{\Gamma}(kp)M^{-1} \subset \tilde{\Gamma}(k) :$$

If $L \in \tilde{\Gamma}(kp)$ then

$$M \cdot L \cdot M^{\sharp} \equiv \pm M \cdot \mathbb{1} \cdot M^{\sharp} \; mod \; kp = \pm \, p \cdot \mathbb{1} \; mod \; kp$$

$$M \cdot L \cdot \frac{1}{det \; M} \cdot M^{\sharp} \equiv \pm \; \mathbb{1} \; mod \; k \;\; \text{i.e.} \; M \cdot L \cdot M^{-1} \in \tilde{\Gamma}(k).$$

Now setting $k = 1$ shows

$$M\tilde{\Gamma}(p)M^{-1} \subset \tilde{\Gamma},$$

while setting $k = p$ shows

$$M\tilde{\Gamma}(p^2)M^{-1} \subset \tilde{\Gamma}(p) \;\; \text{or} \; \tilde{\Gamma}(p^2) \subset M^{-1}\tilde{\Gamma}(p)M$$

As a consequence

$$[\Gamma : M^{-1}\tilde{\Gamma}(p)M] \leq [\Gamma : \tilde{\Gamma}(p^2)] < \infty$$

Finally one checks

$$M^{-1}\tilde{\Gamma}(p)M \subset \Gamma(\Omega(f[M], g)).$$

iii) The claim about the subgroups related to $M^{\sharp}$ follows from part i) and ii) by interchanging the role of f and g and the role of M and $M^{\sharp}$.

3. We consider the two subgroups of Γ from part 2)

$$\tilde{\Gamma}(p) \subset \Gamma \text{ and } K := M^{-1}\tilde{\Gamma}(p)M.$$

Consider a fundamental domain $\mathscr{F} \subset \mathbb{H}$ of $\tilde{\Gamma}(p)$. Then $M^{-1}\mathscr{F}$ is a fundamental domain of K: For each $x \in \mathbb{H}$ also $M(x) \in \mathbb{H}$. Hence by assumption exists a unique $\gamma \in \tilde{\Gamma}(p)$ with

$$\gamma(M(x)) \in \mathscr{F}.$$

Then

$$M^{-1}(\gamma(M(x)) = (M^{-1}\gamma M)(x) \in M^{-1}\mathscr{F}$$

The uniqueness of γ implies the uniqueness of $M^{-1}\gamma M$.

We compute the volume of both fundamental domains, hereby using the $GL(2,\mathbb{Q})^{+}$-invariance of the hyperbolic volume form $d\mu$ according to Lemma 5.20

$$[\Gamma : \tilde{\Gamma}(p)] \cdot vol \; \mathscr{D} = vol \; \mathscr{F} = \int_{\mathscr{F}} d\mu =$$

$$= \int_{M^{-1}\mathscr{F}} d\mu = vol(M^{-1}\mathscr{F}) = [\Gamma : K] \cdot vol \; \mathscr{D}$$

Hence

$$[\Gamma : \tilde{\Gamma}(p)] = [\Gamma : K] = [\Gamma : M^{-1}\tilde{\Gamma}(p)M],$$

in particular independent from $M \in \Gamma_p$, q.e.d.

Theorem 5.25 (Selfadjointness of the Hecke operators). *For each even weight $k \geq 0$ the Hecke operators*

$$T_m \in End(S_k(\Gamma)),\ m \in \mathbb{N},$$

are self-adjoint with respect to the Petersson scalar product, i.e. for all $f,\ g \in S_k(\Gamma)$

$$< T_m f, g > = < f, T_m g >$$

Proof. Due to Theorem 5.18 it suffices to prove the claim for $m = p$ prime. Due to Lemma 5.8 there exists a complete set $V(p)$ of representatives of the Γ-action

$$\Phi_{left} : \Gamma \times \Gamma_p \to \Gamma_p$$

such that also $V(p)^{\sharp}$, the set of adjoints of the matrices from $V(p)$, is a complete set of representatives.

i) *Transformation formula for the integrand*: We consider the function $\Omega(h_1, h_2)$ defined as

$$\Omega(h_1, h_2)(\tau) := (h_1 \cdot \overline{h}_2)(\tau) \cdot (Im\ \tau)^k,\ \tau \in \mathbb{H},$$

which has been introduced in Lemma 5.24, part 3). To simplify the notations we set for $M \in V(p)$

$$\Omega_{M,left} := \Omega(f[M]_k, g) \text{ and } \Omega_{M',right} := \Omega(f, g[M']_k)$$

Explicit computation with the definition of the $[-]_k$-operation on $M_k(\Gamma)$ proves

$$\Omega_{M,left} = \Omega_{M',right} \circ M$$

ii) *Existence of the integrals*: Denote by

$$\mathscr{F} = \dot{\bigcup}_{\gamma}\, \gamma(\mathscr{D})$$

the fundamental domain of $\tilde{\Gamma}(p)$ resulting from a finite coset representation of Γ with respect to the subgroup $\tilde{\Gamma}(p) \subset \Gamma$. We show for $M \in V(p)$

$$\int_{\mathscr{F}} \Omega_{M,left}\, d\mu \text{ exists}$$

by proving for $\gamma \in \Gamma$

$$\int_{\gamma(\mathscr{D})} \Omega_{M,left}\, d\mu \text{ exists :}$$

Similarly to the proof of Theorem 5.23, part ii) one checks on $\mathscr{D}$ an analogue of the transformation formula. First,

$$\Omega_{M,left} \circ \gamma = \Omega(f[M]_k, g) \circ \gamma = \Omega((f[M]_k)[\gamma]_k, g[\gamma]_k) = \Omega(f[M \cdot \gamma]_k, g[\gamma]_k)$$

Due to Lemma 5.6 there exists a matrix $A \in \Gamma$ with

$$A \cdot (M \cdot \gamma) = L \text{ with an upper triangular matrix } L \in V(p)$$

Set

$$\gamma_{left} := A^{-1} \in \Gamma,$$

then

$$M \cdot \gamma = \gamma_{left} \cdot L.$$

Secondly, using that f and g are modular forms with respect to Γ

$$\Omega(f[M \cdot \gamma]_k, g[\gamma]_k) = \Omega(f[\gamma_{left} \cdot L]_k, g[\gamma]_k) = \Omega((f[\gamma_{left}])[L]_k, g[\gamma]_k) =$$

$$= \Omega(f[L]_k, g) = \Omega_{L,left}$$

As a consequence

$$\int_{\gamma(\mathscr{D})} \Omega_{M,left}\, d\mu = \int_{\mathscr{D}} \Omega_{M,left} \circ \gamma\, d\mu = \int_{\mathscr{D}} \Omega_{L,left}\, d\mu$$

Because L is an upper triangular matrix the Fourier series of the cusp form f can easily be evaluated at $L(\tau),\ \tau \in \mathbb{H}$, while the automophy factor $h(L,-)$ is a constant and $det\ L = p$. An analogous estimate as in the proof of Theorem 5.23, part ii) shows the boundedness of the integrand on $\mathscr{D}$. Hence

$$\int_{\gamma(\mathscr{D})} \Omega_{M,left}\, d\mu = \int_{\mathscr{D}} \Omega_{L,left}\, d\mu < \infty$$

iii) *Left-right switching of* $[-]_k$: For given $M \in V(p)$

$$\int_{\mathscr{F}} \Omega_{M,left}\, d\mu = \left[\Gamma(\Omega_{M,left}) : \tilde{\Gamma}(p)\right] \cdot \int_{\mathscr{D}(\Gamma(\Omega_{M,left}))} \Omega_{M,left}\, d\mu$$

because

$$\tilde{\Gamma}(p) \subset \Gamma(\Omega_{M,left})$$

has finite index according to Lemma 5.24, part 2). Concerning the indices Lemma 5.24, part 3) implies

$$[\Gamma : \tilde{\Gamma}(p)] = [\Gamma : M^{-1}\tilde{\Gamma}(p)M]$$

hence also

$$\left[\Gamma(\Omega_{M,left}) : \tilde{\Gamma}(p)\right] = \left[\Gamma(\Omega_{M,left}) : M^{-1}\tilde{\Gamma}(p)M\right]$$

Using the transformation formula from part i) and taking $M^{-1}\mathscr{F}$ as a fundamental domain of $M^{-1}\tilde{\Gamma}(p)M$ the calculation continues

$$\left[\Gamma(\Omega_{M,left}):\tilde{\Gamma}(p)\right]\cdot\int_{\mathscr{D}(\Gamma(\Omega_{M,left}))}\Omega_{M,left}\,d\mu=$$

$$=\left[\Gamma(\Omega_{M,left}):M^{-1}\tilde{\Gamma}(p)M\right]\cdot\int_{\mathscr{D}(\Gamma(\Omega_{M,left}))}\Omega_{M,left}\,d\mu=$$

$$\int_{M^{-1}\mathscr{F}}\Omega_{M,left}\,d\mu=\int_{M^{-1}\mathscr{F}}\Omega_{M',right}\circ M\,d\mu=\int_{\mathscr{F}}\Omega_{M',right}\,d\mu$$

iv) *Left-right switching of the Hecke operator*:

$$<T_pf,g>=\int_{\mathscr{D}}(T_pf\cdot\overline{g})(\tau)\cdot(Im\ \tau)^k\,d\mu=\int_{\mathscr{D}}\Omega(T_pf,g)\,d\mu$$

For any pair of cusp forms T_pf and g the integrand is invariant under the action of Γ as checked during the proof of Theorem 5.23, part i). Hence continuing

$$\int_{\mathscr{D}}\Omega(T_pf,g)\,d\mu=\frac{1}{[\Gamma:\tilde{\Gamma}(p)]}\cdot\int_{\mathscr{F}}\Omega(T_pf,g)d\mu=$$

$$=\frac{1}{[\Gamma:\tilde{\Gamma}(p)]}\cdot\int_{\mathscr{F}}\sum_{M\in V(p)}\Omega_{M,left}\,d\mu=\frac{1}{[\Gamma:\tilde{\Gamma}(p)]}\cdot\sum_{M\in V(p)}\int_{\mathscr{F}}\Omega_{M,left}\,d\mu$$

Using the result from part iii) and the property of $V(p)^\sharp$ the calculation continues

$$\frac{1}{[\Gamma:\tilde{\Gamma}(p)]}\cdot\sum_{M\in V(p)}\int_{\mathscr{F}}\Omega_{M,left}\,d\mu=\frac{1}{[\Gamma:\tilde{\Gamma}(p)]}\cdot\sum_{M\in V(p)}\int_{\mathscr{F}}\Omega_{M',right}\,d\mu=$$

$$\frac{1}{[\Gamma:\tilde{\Gamma}(p)]}\cdot\int_{\mathscr{F}}\sum_{M\in V(p)}\Omega_{M',right}\,d\mu=\frac{1}{[\Gamma:\tilde{\Gamma}(p)]}\cdot\int_{\mathscr{F}}\Omega(f,T_pg)\,d\mu=$$

$$=\int_{\mathscr{D}}\Omega(f,T_pg)\,d\mu=\int_{\mathscr{D}}(f\cdot\overline{T_pg})(\tau)\cdot(Im\ \tau)^k\,d\mu=<f,T_pg>,\ q.e.d.$$

Theorem 5.26 (Eigenforms of the Hecke algebra of the modular group). *For each even weight $k\geq 0$ the cusp space $S_k(\Gamma)$ has a basis of eigenforms of the Hecke algebra $Hecke_k(\Gamma)$.*

Proof. First, Theorem 5.18 implies that $Hecke_k(\Gamma)$ is commutative. Secondly, Theorem 5.25 implies that all Hecke operators T_m, $m\in\mathbb{N}$, are selfadjoint endomorphisms of the unitary vector space $(S_k(\Gamma),<-,->)$. Hence the claim follows due to a result from linear algebra about simultaneous diagonalizability of a family of pairwise commuting, self-adjoint endomorphisms, q.e.d.

Remark 5.27 (Hecke theory of congruence subgroups). For each level $N \in \mathbb{N}$ and even weight $k \geq 0$ one can define Hecke operators on modular forms of $M_k(\Gamma_0(N))$. The corresponding Hecke algebras are commutative, and each vector space of cusp forms of fixed weight has an eigenbasis with respect to the family

$$T_m,\ m \in \mathbb{N} \text{ and } gcd(N,m) = 1.$$

For a proof see [34, Chap. 4, Theor. 4.22], [17], [33, Chap. IX, §6].

One should not consider a Hecke congruence subgroup $\Gamma_0(N)$ as an isolated object of a fixed level N. Instead one should focus on the whole family of Hecke congruence subgroups

$$\Gamma_0(N),\ N \in \mathbb{N}$$

For each weight $k \in \mathbb{N}$ and positive integer $m \in \mathbb{N}$ the modular spaces of different levels

$$M_k(\Gamma_0(M)) \text{ and } M_k(\Gamma_0(m \cdot M))$$

are related.

Proposition 5.28 (Changing levels $(N/m) \mapsto N$). *Consider a weight $k \in \mathbb{N}$, a level $M \in \mathbb{N}$ and a positive integer $m \in \mathbb{N}$. Set*

$$\mu_m := \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma_m$$

The map

$$j : M_k(\Gamma_0(M)) \to M_k(\Gamma_0(m \cdot M)),\ f \mapsto f[\mu_m]_k,$$

is a well-defined injection and restricts to an inclusion of cusp forms.

Under the assumptions of Proposition 5.28 one has apparently also the injection

$$M_k(\Gamma_0(N)) \hookrightarrow M_k(\Gamma_0(m \cdot N)).$$

Proof. 1. *Conjugation of $\Gamma_0(M)$*: Denote by

$$\Gamma' := \mu_m^{-1} \cdot \Gamma_0(M) \cdot \mu_m := \{\mu_m^{-1} \cdot \gamma \cdot \mu_m :\ \gamma \in \Gamma_0(M)\} \subset GL(2,\mathbb{Q})^+$$

the μ_m-conjugate of $\Gamma_0(M)$. If

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(M)$$

then

$$\mu_m^{-1} \cdot \gamma \cdot \mu_m = \frac{1}{m} \cdot \begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix} \cdot \gamma \cdot \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b/m \\ cm & d \end{pmatrix} \in GL(2,\mathbb{Q})^+$$

Claim: For $N := m \cdot M$

$$\Gamma' \cap \Gamma_0(M) = \Gamma_0(N).$$

The inclusion

$$\Gamma' \cap \Gamma_0(M) \subset \Gamma_0(N)$$

is obvious because

$$M|c \implies m \cdot M|c \cdot m, \ i.e. \ N|c \cdot m$$

To prove the opposite inclusion

$$\Gamma_0(N) \subset \Gamma' \cap \Gamma_0(M) :$$

Each matrix

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

has the form

$$\beta = \mu_m^{-1} \cdot \gamma \cdot \mu_m \text{ with } \gamma := \begin{pmatrix} a & mb \\ cM & d \end{pmatrix}.$$

Here

$$det \ \gamma = det \ \beta = 1, \text{ hence } \gamma \in \Gamma_0(M).$$

As a consequence

$$\Gamma_0(N) \subset \Gamma' \text{ and even } \Gamma_0(N) \subset (\Gamma' \cap \Gamma_0(M))$$

2. *Changing right-multiplication to left-multiplication*: Claim: For each $\alpha \in \Gamma$ exists $\alpha_{left} \in \Gamma$ such that

$$\mu_m \cdot \alpha = \alpha_{left} \cdot \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in M(2 \times 2, \mathbb{Z}) \cap GL(2, \mathbb{Q})^+.$$

For the proof set

$$M := \mu_m \cdot \alpha \in \Gamma_m$$

By Lemma 5.6 exists a matrix $A \in \Gamma$ such that

$$A \cdot M \in \Gamma_m$$

is triangular. Set

$$\alpha_{left} := A^{-1} \in \Gamma$$

3. *Weak modularity*: Assume $f \in M_k(\Gamma_0(M))$ and set

$$g := f[\mu_m]_k.$$

Due to part 1) a given $\beta \in \Gamma_0(N)$ has the form

$$\beta = \mu_m^{-1} \cdot \gamma \cdot \mu_m$$

with a suitable $\gamma \in \Gamma_0(M)$. Then

$$g[\beta]_k = (f[\mu_m]_k)[\beta]_k = f[\mu_m \cdot \beta]_k = f[\mu_m \cdot \mu_m^{-1} \cdot \gamma \cdot \mu_m]_k =$$

$$= f[\gamma \cdot \mu_m]_k = (f[\gamma]_k)[\mu_m]_k = f[\mu_m]_k = g$$

Hence $f[\mu_m]_k$ is weakly modular with respect to $\Gamma_0(N)$.

4. *Holomorphy at the cusps*: According to the definition one has to show: For each

$$g := f[\mu_m]_k, f \in M_k(\Gamma_0(M)),$$

and each $\alpha \in \Gamma$ the function $g[\alpha]_k$ is holomorphic at $\infty \in \mathbb{H}^*$ according to the definition of $M_k(\Gamma_0(N))$. Due part 2) there exists a matrix

$$\alpha_{left} \in \Gamma$$

such that

$$\mu_m \cdot \alpha = \alpha_{left} \cdot \theta$$

with a triangular matrix

$$\theta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M(2 \times 2, \mathbb{Z}) \cap GL(2, \mathbb{Q})^+$$

Hence

$$g[\alpha]_k = f[\mu_m \cdot \alpha]_k = f[\alpha_{left} \cdot \theta] = (f[\alpha_{left}]_k)[\theta]_k$$

From the Fourier expansion

$$f[\alpha_{left}]_k = \sum_{n=0}^{\infty} a_n \cdot \hat{q}^n,\ \hat{q} = e^{2\pi i \cdot \tau/h}$$

for a suitable $h \in \mathbb{N}$ one obtains as a consequence

$$g[\alpha]_k(\tau) = f[\alpha_{left}]_k[\theta]_k(\tau) = m^{k-1} \cdot d^{-k} \cdot \sum_{n=0}^{\infty} a_n \cdot e^{2\pi i n \cdot (b/(dh))} \cdot \tilde{q}^n,\ \tilde{q} = e^{2\pi i (\tau/h) \cdot (a/d)}.$$

Hence $g[\alpha]_k$ is holomorphic at ∞. And the last Fourier series shows that j maps cusp forms to cusp forms.

If we fix the level N then each prime factor $p|N$ defines a level changing

$$(N/p) \mapsto N, \text{using } \mu_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma_p.$$

The subspace of $M_k(\Gamma_0(N))$ generated by the images of the maps

$$j_{p,(N/p),k} : S_k(\Gamma_0(N/p)) \times S_k(\Gamma_0(N/p)) \to S_k(\Gamma_0(N)),\ (f,g) \mapsto f + g[\mu_p]_k,$$

for all prime factors $p|N$ is named the *oldspace*, see Definition 5.29.

Definition 5.29 (Oldform and newform of cusp forms). Consider a level $N \in \mathbb{N}^*$ and a weight k.

1. The image
$$\left(\sum_{p|N} im\ j_{p,(N/p),k} \right) \subset S_k(\Gamma_0(N))$$
is named the subspace
$$S_k^{old}(\Gamma_0(N)) \subset S_k(\Gamma_0(N))$$
of *oldforms*. The summation is indexed by the primes p dividing N.

2. The orthogonal complement of $S_k^{old}(\Gamma_0(N)$ with respect to the Petersson scalar product is named the subspace
$$S_k^{new}(\Gamma_0(N)) := S_k^{old}(\Gamma_0(N)^{\perp} \subset S_k(\Gamma_0(N))$$
of *newforms*.

Apparently, by the same mappings one can also define the oldspace of modular forms as a subspace fo $M_k(\Gamma_0(N))$. But unfortunately the Petersson scalar product does not extend from the cusp forms to all modular forms. Hence there is no orthogonal complement of subspace of old forms.

Example 5.30 (Oldforms and newforms). See PARI-file `Congruence_subgroup_20`.

- *Congruence subgroup* $\Gamma_0(2)$: Figure 5.2 displays for the Hecke congruence subgroup $\Gamma_0(2)$ of level $N = 2$ the splitting of the cusp space for the first even weights $k = 0, ..., 12$ into oldforms and newforms.

  According to Definition 5.29 one has to consider for the splitting the single prime factor $p = 2$ and the cusp forms $S_k(\Gamma_0(1))$, i.e. the cusp forms of the full modular group $\Gamma = \Gamma_0(1)$.

  For weight $k = 12$ one has the 1-dimensional subspace
  $$S_{12}(\Gamma) = \mathbb{C} \cdot \Delta \subset S_{12}(\Gamma_0(2))$$
  In addition also the modular form
  $$\Delta_2 : \mathbb{H} \to \mathbb{C},\ \tau \mapsto \Delta(2 \cdot \tau)$$
  belongs to $S_{12}(\Gamma_0(2))$. The computation shows

$$S_{12}(\Gamma_0(2)) = span_{\mathbb{C}} < \Delta, \Delta_2 >,$$

all cusp forms in $S_{12}(\Gamma_0(2))$ are old forms induced by $S_{12}(\Gamma)$.

- *Congruence subgroup* $\Gamma_0(4)$: Similarly Figure 5.3 considers the modular group $\Gamma_0(4)$ of level $N = 4$. For the splitting one has to consider $S_k(\Gamma_0(2))$ and the level change $2 \mapsto 4$. As expected the oldforms of $\Gamma_0(4)$ contain all cusp forms induced from the cusp forms of $\Gamma_0(2)$.

- *Congruence subgroup* $\Gamma_0(11)$: The final Figure 5.4 considers the modular group $\Gamma_0(11)$ of level $N = 11$. For the splitting one has to consider the level change $1 \mapsto 11$. The old forms of $\Gamma_0(11)$ derive from the modular forms Δ and $j(\Delta)$.

```
==================================================
Congruence subgroups_20, Start

Modular forms, cusp forms, newforms,

Congruence subgroup Gamma_0(2): Modular forms, oldforms, newforms

Index [Gamma:Gamma_0(2)] = 3

Right cosets: [[0, -1; 1, 0], [1, 0; 1, 1], [1, 0; 2, 1]]

Cusps of Gamma_0(2): [0, 1/2]

Weight k: (dim M_k(Gamma_0(2), dim S_k_old(Gamma_0(2), dim S_k_new(Gamma_0(2)))

0: (1, 0, 0)
2: (1, 0, 0)
4: (2, 0, 0)
6: (2, 0, 0)
8: (3, 0, 1)
10: (3, 0, 1)
12: (4, 2, 0)

Congruence subgroups_20, End
==================================================
```

Fig. 5.2 $\Gamma_0(2)$ oldforms and newforms

```
==================================================
Congruence subgroups_20, Start

Modular forms, cusp forms, newforms,

Congruence subgroup Gamma_0(4): Modular forms, oldforms, newforms

Index [Gamma:Gamma_0(4)] = 6

Right cosets: [[0, -1; 1, 0], [1, 0; 1, 1], [0, -1; 1, 2], [0, -1; 1, 3], [1, 0; 2, 1], [1, 0; 4, 1]]

Cusps of Gamma_0(4): [0, 1/2, 1/4]

Weight k: (dim M_k(Gamma_0(4), dim S_k_old(Gamma_0(4), dim S_k_new(Gamma_0(4)))

0: (1, 0, 0)
2: (2, 0, 0)
4: (3, 0, 0)
6: (4, 0, 1)
8: (5, 2, 0)
10: (6, 2, 1)
12: (7, 3, 1)

Congruence subgroups_20, End
==================================================
```

Fig. 5.3 $\Gamma_0(4)$ oldforms and newforms

```
==================================================
Congruence subgroups_20, Start

Modular forms, cusp forms, newforms,

Congruence subgroup Gamma_0(11): Modular forms, oldforms, newforms

Index [Gamma:Gamma_0(11)] = 12

Right cosets: [[0, -1; 1, 0], [1, 0; 1, 1], [0, -1; 1, 2], [0, -1; 1, 3], [0, -1; 1, 4], [0, -1; 1, 5], [0, -1; 1, 6], [0, -1; 1, 7], [
0, -1; 1, 8], [0, -1; 1, 9], [0, -1; 1, 10], [1, 0; 11, 1]]

Cusps of Gamma_0(11): [0, 1/11]

Weight k: (dim M_k(Gamma_0(11), dim S_k_old(Gamma_0(11), dim S_k_new(Gamma_0(11)))

0: (1, 0, 0)
2: (2, 0, 1)
4: (4, 0, 2)
6: (6, 0, 4)
8: (8, 0, 6)
10: (10, 0, 8)
12: (12, 2, 8)

Congruence subgroups_20, End
==================================================
```

Fig. 5.4 $\Gamma_0(11)$ oldforms and newforms

5.3 Numerology: Lagrange, Jacobi, Ramanujan, Mordell

The present section draws some conclusion from the existence of simultaneous eigenforms of the Hecke operators. First we prove a conjecture of Ramanujan concerning a certain numerical function. Secondly, we derive the four squares theorem.

Information about the Ramanujan τ-function is encoded by the modular discriminant, the cusp form $\Delta \in S_{12}(\Gamma)$.

Definition 5.31 (Ramanujan τ-function). The Fourier coefficients $(\tau_n)_{n\in\mathbb{N}}$ of the normalized discriminant form

$$\frac{\Delta(\tau)}{(2\pi)^{12}} = \sum_{n=1}^{\infty} \tau_n \cdot q^n,\ q = e^{2\pi i\cdot\tau},$$

define the *Ramanujan τ-function*

$$\tau : \mathbb{N} \to \mathbb{Z},\ n \mapsto \tau(n) := \tau_n.$$

According to Proposition 3.14 all Fourier coefficients are integers $\tau(n) \in \mathbb{Z}$.

Computing the first coefficients $\tau(n)$ up to $n = 6$ gives

$$\frac{\Delta(\tau)}{(2\pi)^{12}} = q - 24q^2 + 252q^3 - 1.472q^4 + 4.830q^5 - 6.048q^6 + O(7)$$

From these values one verifies at once the product formula

$$\tau(2)\cdot\tau(3) = -24\cdot 252 = -6.048 = \tau(6),$$

and as a particular case of the recursion formula

$$\tau(p^2) = \tau(p)^2 - p^{11}\cdot\tau(p^0)$$

the formula for $p = 2$

$$\tau(2^2) = -1.472 = \tau(2)^2 - 2^{11} = (-24)^2 - 2.048.$$

From explicit computation of the first 30 values of $\tau(n)$ Ramanujan [45] conjectured in 1916 several generalizations. Figure 5.5 shows equations (103) and (104) from the original paper with two of Ramanujan's conjectures.

Note. There is a typo in equation (104) referring to the factor 2. It should read

$$|\tau(p)| \le 2\cdot p^{11/2}$$

the form $o(n^{\frac{11}{2}})$. For it appears that

$$\sum_{1}^{\infty} \frac{\tau(n)}{n^t} = \prod_{p} \frac{1}{1 - \tau(p)p^{-t} + p^{11-2t}}. \tag{10}$$

This assertion is equivalent to the assertion that, if

$$n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_r^{a_r},$$

where $p_1, p_2, \ldots, p_r$ are the prime divisors of n, then

$$n^{-\frac{11}{2}}\tau(n) = \frac{\sin(1+a_1)\theta_{p_1}}{\sin\theta_{p_1}} \frac{\sin(1+a_2)\theta_{p_2}}{\sin\theta_{p_2}} \cdots \frac{\sin(1+a_r)\theta_{p_r}}{\sin\theta_{p_r}}, \tag{10}$$

where

$$\cos\theta_p = \tfrac{1}{2}p^{-\frac{11}{2}}\tau(p).$$

It would follow that, if n and n' are prime to each other, we must have

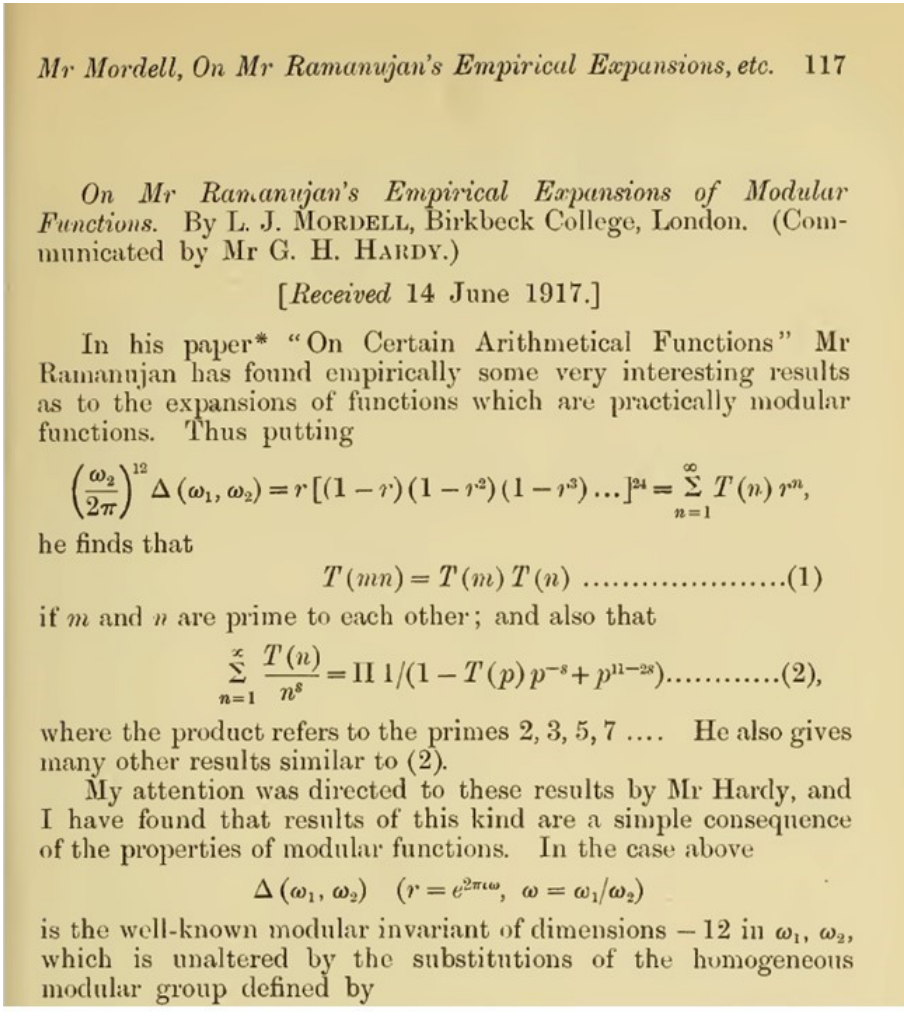
$$\tau(nn') = \tau(n)\tau(n'). \tag{10}$$

Let us suppose that (102) is true, and also that (as appears to be highly probable)

$$\{2\tau(p)\}^2 \leq p^{11}, \tag{10}$$

Fig. 5.5 Ramanujan's conjecture on $\tau(n)$ from [45]

The conjecture was proved inter alia one year later by Mordell [42]. Figure 5.6 shows Mordell's introduction from his paper.



Mr Mordell, On Mr Ramanujan's Empirical Expansions, etc. 117

On Mr Ramanujan's Empirical Expansions of Modular Functions. By L. J. MORDELL, Birkbeck College, London. (Communicated by Mr G. H. HARDY.)

[*Received* 14 June 1917.]

In his paper* "On Certain Arithmetical Functions" Mr Ramanujan has found empirically some very interesting results as to the expansions of functions which are practically modular functions. Thus putting

$$\left(\frac{\omega_2}{2\pi}\right)^{12}\Delta(\omega_1,\omega_2)=r[(1-r)(1-r^2)(1-r^3)\ldots]^{24}=\sum_{n=1}^{\infty}T(n)\,r^n,$$

he finds that

$$T(mn)=T(m)\,T(n)\quad\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

if m and n are prime to each other; and also that

$$\sum_{n=1}^{\infty}\frac{T(n)}{n^s}=\Pi\,1/(1-T(p)\,p^{-s}+p^{11-2s})\ldots\ldots\ldots\ldots(2),$$

where the product refers to the primes 2, 3, 5, 7 .... He also gives many other results similar to (2).

My attention was directed to these results by Mr Hardy, and I have found that results of this kind are a simple consequence of the properties of modular functions. In the case above

$$\Delta(\omega_1,\omega_2)\quad(r=e^{2\pi i\omega},\ \omega=\omega_1/\omega_2)$$

is the well-known modular invariant of dimensions -12 in ω_1, ω_2, which is unaltered by the substitutions of the homogeneous modular group defined by

Fig. 5.6 Mordell's introduction to [42]

A film about Ramanujan is to be recommended, named "The man who knew infinity" (Deutsch: Die Poesie des Unendlichen).

Today Ramanujan's product formula and recursion formula can be obtained as a first application of Hecke theory:

Proposition 5.32 (Product and recursion formula of the Ramanujan τ-function). *The Ramanujan τ-function satisfies:*

1. Product formula*: For all integers* $m,n \geq 1$

$$\tau(m) \cdot \tau(n) = \sum_{r|(m,n)} r^{11} \cdot \tau(mn/r^2).$$

In particular, for coprime m and n:

$$\tau(m) \cdot \tau(n) = \tau(m \cdot n).$$

2. Recursion formula*: For all primes p and integers* $k \geq 1$

$$\tau(p) \cdot \tau(p^k) = \tau(p^{k+1}) + p^{11} \cdot \tau(p^{k-1}).$$

Proof. 1. Consider an arbitrary, but fixed $m \in \mathbb{N}$. Corollary 5.13 from Hecke theory derives the eigenvalue equation

$$T_m \left(\frac{\Delta}{(2\pi)^{12}} \right) = \tau(m) \cdot \frac{\Delta}{(2\pi)^{12}}$$

When equating for each fixed $n \in \mathbb{N}$ the terms of order n on both sides of the equation the coefficent formula from Theorem 5.11 implies:

$$\sum_{r|(m,n)} r^{11} \cdot \tau(mn/r^2) = \tau(m) \cdot \tau(n).$$

For coprime integers m,n we have $(m,n) = 1$ and the summation reduces to the single term for $r = 1$:

$$\tau(m) \cdot \tau(n) = \tau(m \cdot n)$$

2. We set $m = p^k$ and $n = p$ in the product formula from part 1). Due to

$$(p^k, p) = p$$

we now have two summands, referring to the indices $r = 1$ and $r = p$. We obtain

$$\tau(p^k) \cdot \tau(p) = \tau(p^{k+1}) + p^{11} \cdot \tau(p^{k-1}),\ q.e.d.$$

Remark 5.33 (Growth estimation of the Ramanujan τ-function). The final conjecture of Ramanujan about the τ-function is the growth estimation

$$|\tau(p)| \leq 2 \cdot p^{11/2},\ p \text{ prime},$$

see Figure 5.5 equation (104) (after correction). This conjecture lies much deeper than Ramanujan's other conjectures. Deligne proved the growth condition of the τ-function as a consequence of his proof of the Weil conjectures in 1974.

The next application uses information encoded by modular forms from $M_2(\Gamma_0(4))$. The "Four squares theorem" answers the question: How many possibilities exist to represent a positive integer as the sum of four integer squares?

Fermat recalls in a letter to a friend from 1659 those results from arithmetic which he considers his most important contribution to this field. One of these results is the claim that any natural number can be written as the sum of four squares. The first proof of this theorem has been given by Lagrange in 1770. The more refined version of Theorem 5.38 is due to Jacobi in 1834. For the history of these issues see [47].

Definition 5.34 (Representing integers as sum of squares). The number of possibilities to represent a non-negative integer n as the sum of k integer squares defines the arithmetic function

$$r : \mathbb{N}^* \times \mathbb{N}^* \to \mathbb{N}$$

with

$$r(n,k) := card\ \left\{ v = (v_1, ..., v_k) \in \mathbb{Z}^k : n = v_1^2 + ... + v_k^2 \right\}.$$

Note that $r(n,k)$ counts k-tuples with positive and negative components as different, and distinguishes also k-tuples with the same components, but in different order.

We will see that the representation of integers as sum of squares is related to the congruence subgroup $\Gamma_0(4)$, the relevant space of modular forms is $M_2(\Gamma_0(4))$.

Definition 5.35 (Generating function ϑ). The series

$$\vartheta(\tau,k) := \sum_{n=0}^{\infty} r(n,k) \cdot q^n,\ q := e^{2\pi i \tau},$$

which is generated by the sequence $r(n,k)_{n\in\mathbb{N}}$, is named a *ϑ-series*.

Proposition 5.36 (Generating function as modular form). *The generating function $\theta(-,4)$ is a modular form of weight 2 of the congruence subgroup $\Gamma_0(4)$, i.e.*

$$\theta(-,4) \in M_2(\Gamma_0(4)).$$

Its Fourier series starts

$$\theta(\tau,4) = 1 + 8q + O(2),\ q = e^{2\pi i \tau}.$$

Proof. Scetch, see cf. [17, Chap.1, §2; Chap. 4, §9], [36].

i) The congruence subgroup $\Gamma_0(4)$ is generated as

$$\Gamma_0(4) =< T, \gamma >$$

with

$$\gamma = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \in \Gamma_0(4)$$

ii) The translation T apparently satisfies

$$\vartheta(-,4)[T]_2 = \vartheta(-,4)$$

The product formula

$$\vartheta(\tau,4) = \vartheta(\tau)^4$$

with

$$\vartheta(\tau) = \sum_{n=0}^{\infty} r(n,1) \cdot q^n$$

reduces the weak modularity

$$\vartheta(-,4)[\gamma]_2 = \vartheta(-,4)$$

to the transformation formula for ϑ: The difficult part is to prove

$$\vartheta(-1/(4\tau)) = \sqrt{-2i\tau} \cdot \vartheta(\tau).$$

Then follows

$$\vartheta\left(\frac{\tau}{4\tau+1}\right) = \vartheta\left(\frac{-1}{4(-1/(4\tau)-1)}\right) = \sqrt{2i\left(\frac{1}{4\tau}+1\right)} \cdot \vartheta\left(-\frac{1}{4\tau}-1\right) =$$

$$= \sqrt{2i\left(\frac{1}{4\tau}+1\right)} \cdot \vartheta\left(-\frac{1}{4\tau}\right) = \sqrt{2i\left(\frac{1}{4\tau}+1\right) \cdot (-2i\tau)} \cdot \vartheta(\tau) = \sqrt{4\tau+1} \cdot \vartheta(\tau),$$

and exponention

$$\vartheta(-,4) = \vartheta^4$$

shows the transformation formula

$$\vartheta\left(\frac{\tau}{4\tau+1},4\right) = (4\tau+1)^2 \cdot \vartheta(\tau,4) \text{ i.e. } \vartheta(-,4)[\gamma]_2 = \vartheta(-,4)$$

iv) The Fourier series

$$\vartheta(\tau) = 1 + r(1,1) \cdot q + O(q^2) = 1 + 2 \cdot q + O(q^2)$$

shows

$$\vartheta(\tau,4) = (1+2\cdot q)^4 + O(2) = 1+8\cdot q + O(2),\ q.e.d.$$

Theorem 5.37 (The modular form $G_{2,N} \in M_2(\Gamma_0(N))$). *Denote by G_2 the Eisenstein series from Remark 3.12. For each level $N \geq 1$ set*

$$\mu_N := \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \in M(2\times 2,\mathbb{Z}) \cap GL(2,\mathbb{Q})^+$$

The function

$$G_{2,N} := G_2 - G_2[\mu_N]_2 : \mathbb{H} \to \mathbb{C}$$

is a modular function

$$G_{2,N} \in M_2(\Gamma_0(N))$$

Proof. By definition

$$(G_2[\mu_N]_2)(\tau) := G_2(\mu_2(\tau)) \cdot \det\ \mu_N \cdot h(\mu_N,\tau)^{-2} = N \cdot G_2(N\tau)$$

i) *Holomorphy*: Due to Remark 3.12 the functions G_2 and hence also $G_{2,N}$ are holomorphic in $\mathbb{H} \cup \{\infty\}$.

ii) *Weak modularity*: We have to show for all $\alpha \in \Gamma_0(N)$:

$$G_{2,N}[\alpha]_2 = G_{2,N}.$$

We recall the formula from Remark 3.12

$$G_2[\gamma]_2(\tau) = G_2(\tau) - 2\pi i \cdot c \cdot h(\gamma,\tau)^{-2} \text{ for } \gamma := \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$$

We have to compute the transforms of the two summands of $G_{2,N}$.

- $G_2[\alpha]_2$: Set

  $$\gamma := \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \subset \Gamma.$$

  Then

  $$G_2[\alpha]_2(\tau) = G_2(\tau) - 2\pi i \cdot c \cdot h(\alpha,\tau)^{-2}$$

- $(G_2[\mu_N]_2)[\alpha]_2$: Then

  $$\mu_N \cdot \alpha = \beta \cdot \mu_N \text{ with } \beta := \begin{pmatrix} a & Nb \\ c/N & d \end{pmatrix}$$

  Here $\beta \in \Gamma$ because

  $$c \equiv 0 \bmod \mathrm{N} \implies c/N \in \mathbb{Z}$$

  Then

$$(G_2[\beta]_2)(z) = G_2(z) - 2\pi i \cdot (c/N) \cdot h(\beta, z)^{-2}$$

Hence with the argument $z = \mu_N(\tau) = N\tau$

$$(G_2[\beta]_2)(\mu_N(\tau)) = G_2(\mu_N(\tau)) - 2\pi i \cdot (c/N) \cdot h(\beta, \mu_N(\tau))^{-2}$$

Then

$$((G_2[\mu_N]_2)[\alpha]_2)(\tau) = (G_2[\mu_N \cdot \alpha]_2)(\tau) = (G_2[\beta \cdot \mu_N]_2)(\tau) =$$

$$= ((G_2[\beta]_2)[\mu_N]_2)(\tau) = (G_2[\beta]_2)(\mu_N(\tau)) \cdot h(\mu_N, \tau)^{-2} \cdot N =$$

$$= \left(G_2(\mu_N(\tau)) - 2\pi i \cdot (c/N) \cdot h(\beta, \mu_N(\tau))^{-2}\right) \cdot h(\mu_N, \tau)^{-2} \cdot N =$$

$$= G_2(\mu_N(\tau)) \cdot h(\mu_N, \tau)^{-1} \cdot N - 2\pi i((c/N) \cdot N) \cdot (h(\beta, \mu_N(\tau)) \cdot h(\mu_N, \tau))^{-2} =$$

$$= (G_2[\mu_N]_2)(\tau) - 2\pi i((c/N) \cdot N) \cdot (h(\beta, \mu_N(\tau)) \cdot h(\mu_N, \tau))^{-2}$$

Now

$$h(\beta, \mu_N(\tau)) = h(\beta, N\tau) = (c/N) \cdot N\tau + d = c\tau + d \text{ and } h(\mu_N, \tau) = 1$$

and

$$h(\alpha, \tau) = c\tau + d$$

which implies

$$h(\beta, \mu_N(\tau)) = h(\alpha, \tau)$$

Hence

$$((G_2[\mu_N]_2)[\alpha]_2)(\tau) = (G_2[\mu_N]_2)(\tau) - 2\pi i \cdot c \cdot h(\alpha, \tau)^{-2}$$

As a consequence, the transformation formulas for both summands imply:

$$G_{2,N}[\alpha]_2 = G_2[\alpha]_2 - ((G_2[\mu_N]_2)[\alpha]_2) = G_2 - (G_2[\mu_N]_2) = G_{2,N}$$

iv) Finally one checks the Fourier expansion at the cusps using the Fourier expansion of G_2 from Remark 3.12, see [17, Chap. I, Exerc. 1.2.8.e] and [33, Chap. IX, §3, Example 4], q.e.d.

Theorem 5.38 (Four squares theorem). *For any $n \in \mathbb{N},\ n \geq 1$, there are*

$$r(n,4) = 8 \cdot \sum_{d|n,\ 4\nmid d} d$$

possibilities to represent the non-negative integer n as the sum of 4 *integer squares. In particular for* $4 \nmid n$

$$r(n,4) = 8 \cdot \sigma_1(n) = 8 \cdot \sum_{d|n} d.$$

Proof. Computation within $M_2(\Gamma_0(4))$:

i) *Dimension*: $dim\, M_2(\Gamma_0(4)) = 2$ according to Theorem 3.26, see also Figure 5.3.

ii) *Basis*: According to Theorem 5.37 for each $N \geq 2$ the Eisenstein series

$$G_{2,N}(\tau) := G_2(\tau) - N \cdot G_2(N\tau)$$

is a modular form of the congruence subgroup $\Gamma_0(N)$ of weight 2, i.e.

$$G_{2,N}(\tau) \in M_2(\Gamma_0(N)).$$

The Fourier expansion of G_2 from Remark 3.12 provides for the two Eisenstein series $G_{2,2}$ and $G_{2,4}$ the Fourier expansions

$$G_{2,2}(\tau) = -\frac{\pi^2}{3}\left(1 + 24 \cdot \sum_{n=1}^{\infty}\left(\sum_{\substack{d|n \\ d\ odd}} d\right) q^n\right) = -\frac{\pi^2}{3}(1 + 24q + O(2))$$

and

$$G_{2,4}(\tau) = -\pi^2\left(1 + 8 \cdot \sum_{n=1}^{\infty}\left(\sum_{d|n,\ 4\nmid n} d\right) q^n\right) = -\pi^2(1 + 8q + O(2)).$$

Comparing terms of order 0 and 1 in the Fourier expansions shows that both Eisenstein series are linearly independent. Hence the family $(G_{2,2}, G_{2,4})$ is a basis of $M_2(\Gamma_0(4))$. In particular, it generates $\theta(-,4)$.

Proposition 5.36 implies by comparing Fourier coefficients of order 0 and 1

$$\theta(-,4) = -\frac{1}{\pi^2}\, G_{2,4}.$$

Equating on both sides the Fourier coefficients of order $n \in \mathbb{N}^*$ shows

$$r(n,4) = 8 \cdot \sum_{d|n,\ 4\nmid d} d,\ q.e.d.$$

Example 5.39 (Modular forms via ϑ-functions). Figure 5.7 shows for some pairs (k,e) the numbers

$$r(n,k,e).$$

Here $r(n,k,e) \in \mathbb{N}$ is the number of different representations of n as a sum of k summands, each an e-power. These numbers are the Fourier coefficients of suitable modular forms. The case

$$r(n,4,2) =: r(n,4)$$

has been investigated in Theorem 5.38. The figure shows the output of the PARI-script `Modular_forms_theta_01`.

```
==================================================
Modular_forms_theta_01: Start.
Modular_forms_theta_01: Fourier coefficients of r(-,k,e) with r(n,k,e) the number,
of different representations of n as a sum of k summands, each an e-power

parameter: (k,e) = (1,2)
Underlying modular space: M_1/2(G_0(4, 1))
Generating modular form: 1 + 2*q + 2*q^4 + 2*q^9 + O(q^10)
--------------------------------------
parameter: (k,e) = (2,2)
Underlying modular space: M_1(G_0(4, -4))
Generating modular form: 1 + 4*q + 4*q^2 + 4*q^4 + 8*q^5 + 4*q^8 + 4*q^9 + O(q^10)
--------------------------------------
parameter: (k,e) = (3,2)
Underlying modular space: M_3/2(G_0(4, 1))
Generating modular form: 1 + 6*q + 12*q^2 + 8*q^3 + 6*q^4 + 24*q^5 + 24*q^6 + 12*q^8 + 30*q^9 + O(q^10)
--------------------------------------
parameter: (k,e) = (4,2)
Underlying modular space: M_2(G_0(4, 1))
Generating modular form: 1 + 8*q + 24*q^2 + 32*q^3 + 24*q^4 + 48*q^5 + 96*q^6 + 64*q^7 + 24*q^8 + 104*q^9 + O(q^10)
--------------------------------------
parameter: (k,e) = (8,2)
Underlying modular space: M_4(G_0(4, 1))
Generating modular form: 1 + 16*q + 112*q^2 + 448*q^3 + 1136*q^4 + 2016*q^5 + 3136*q^6 + 5504*q^7 + 9328*q^8 + 12112*q^9 + O(q^10)
--------------------------------------
Modular_forms_theta_01: End
------------------------------------------------------
```

Fig. 5.7 Modular functions to compute $r(-,k,e)$

Part II
Advanced Theory

Chapter 6
Application to imaginary quadratic fields

The modular j-invariant parametrizes the set of compex tori by the values of the affine part of the modular curve $X(\Gamma) \simeq \mathbb{P}$. All complex analytic properties of a given torus with normalized period lattice $(1,\tau)$ are encoded in the value $j(\tau) \in \mathbb{C}$ of the modular j-invariant. But $j(\tau)$ is too coarse to discriminate between the arithmetic properties of the members of a class of biholomorphic equivalent tori.

Section 6.2 will investigate for tori with complex multiplication: Which arithmetic information can be obtained when considering besides $j(\tau)$ also the values

$$j(\alpha(\tau)),\ \alpha \in \Gamma_{m,prim},\ m \in \mathbb{N}^*?$$

References for the present chapter are [66, Chap. 6.1] and [50].

6.1 Imaginary quadratic fields and tori with complex multiplication

As a first arithmetic property of complex tori and elliptic curves we observe: Complex tori with normalized lattice generated by $(1,\tau)$ relate for certain numbers $\tau \in \mathbb{H}$ to an imaginary quadratic field. How to characterize tori with those arithmetic properties? The answer is given by Theorem 6.6.

As a general reference for number fields we recommend [22], [40], [32].

Definition 6.1 (Number field).

1. A field K is a *number field* if

$$\mathbb{Q} \subset K \subset \mathbb{C} \text{ with degree } deg\ K := [K : \mathbb{Q}] < \infty.$$

If $deg\ K = 2$ then K is a *quadratic field*.

2. The *Galois group* $Gal(K/\mathbb{Q})$ of a number field K is the group of all field automorphism of K which pointwise fix the elements of $\mathbb{Q}$.

Remark 6.2 (Number field). Consider a number field K of degree

$$n = [K : \mathbb{Q}]$$

1. Denote by

$$(\alpha_j)_{j=1,\dots,n}$$

a $\mathbb{Q}$-basis of K. For each $\alpha \in K$ the multiplication

$$\mu_\alpha : K \to K,\ x \mapsto \alpha \cdot x,$$

is determined by the values

$$\mu_\alpha(\alpha_j) = \sum_{k=1,\dots,n} \alpha_{jk} \cdot \alpha_k,\ j = 1, \dots, n.$$

For $\alpha \in K$ norm and trace are respectively defined as

$$N_K(\alpha) := det(\alpha_{jk}) \in \mathbb{Q} \text{ and } tr_K(\alpha) := \sum_{j=1,\dots,n} \alpha_{jj} \in \mathbb{Q}$$

2. The discriminant of K with respect to the basis $(\alpha_j)_{j=1,\dots,n}$ is defined as

$$\Delta_K := det(tr_K(\alpha_j \cdot \alpha_k)) \in \mathbb{Q}$$

The discriminant depends on the choice of the basis: It transforms with the square of the determinant of the base change matrix.

3. The ring of *algebraic integers* in K, the *number ring* of K, is the ring

$$\mathcal{O}_K := \{x \in K :\ x \text{ integral over } \mathbb{Z}\}$$

It is a lattice in K, and K is the quotient field of $\mathcal{O}_K$ of integers. The ring $\mathcal{O}_K$ is the prototype of a *Dedekind ring*, i.e. $\mathcal{O}_K$ is a Noetherian, 1-dimensional integral domain, integrally closed in its quotient field.

4. An *order* of K is a subring $\Lambda \subset \mathcal{O}_K$ which is a free $\mathbb{Z}$-module of rank n.

5. The number field K has a $\mathbb{Q}$-basis $(\alpha_j)_{j=1,\ldots,n}$ by algebraic integers $\alpha_j \in \mathcal{O}_K$. Each element $\alpha \in K$ has a unique representation

$$\alpha = \frac{\mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n}{\Delta_K}$$

6. For a quadratic field $K = \mathbb{Q}(\sqrt{d})$ with a squarefree integer $d \in \mathbb{Z}$ one has

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

and

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{\Delta_K + \sqrt{\Delta_K}}{2}\right]$$

7. Each number field K has a *primitive element*, i.e.

$$K = \mathbb{Q}(\alpha)$$

with a suitable $\alpha \in K$. Each primitive element satisfies a polynomial equation

$$P(\alpha) = 0 \text{ with } P(X) \in \mathbb{Q}[X] \text{ and } deg\ P = deg\ K.$$

8. Each quadratic number field has the form

$$K = \mathbb{Q}(\sqrt{d}) \text{ with } d \in \mathbb{Z} \text{ squarefree.}$$

If $d < 0$ then K is named *imaginary quadratic*, if $d > 0$ then K is named *real quadratic*.

9. The Galois group $Gal(K/\mathbb{Q})$ of a quadratic number field $K = \mathbb{Q}(\sqrt{d})$ equals the group $\mathbb{Z}_2$. Its generator

$$\sigma_1 : K \to K,\ z \mapsto \sigma_1(z),$$

satisfies

$$\sigma_1(z) = \begin{cases} -z & d > 0 \\ \bar{z} & d < 0 \end{cases}$$

Set

$$\sigma_0 := id_{Gal(K/\mathbb{Q})}.$$

Then *norm* and *trace* of an element $z \in K$ can be computed by using the elementary symmetric functions:

$$N(z) = \sigma_0(z) \cdot \sigma_1(z) \text{ and } Tr(z) = \sigma_0(z) + \sigma_1(z)$$

Note. Due to historical reasons the symbol $\mathscr{O}$ has two different meanings. In the context of complex analysis $\mathscr{O}$ also denotes the complex structure sheaf.

Definition 6.3 (Endomorphisms of a torus). An *endomorphism* f of a torus

$$(T,0) = \mathbb{C}/\Lambda$$

is a holomorphic map

$$f : (T,0) \to (T,0)$$

with $f(0) = 0$.

Recall from Proposition 2.3 that each endomorphism f of a torus fits into a commutative diagram

$$\begin{array}{ccc} \mathbb{C} & \overset{\mu_\alpha}{\dashrightarrow} & \mathbb{C} \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle p} \\ \mathbb{C}/\Lambda & \xrightarrow{f} & \mathbb{C}/\Lambda \end{array}$$

with a unique multiplication map μ_α determined by an element $\alpha = \alpha_f \in \mathbb{C}$: For all $z \in \mathbb{C}$

$$\mu_\alpha(z) = \alpha \cdot z$$

Proposition 6.4 (Endomorphism ring). *The set of endomorphisms of a torus*

$$T = \mathbb{C}/\Lambda$$

constitutes with respect to addition and composition a ring $End(T)$, the endomorphism ring *of T. The map*

$$End(T) \to \{\alpha \in \mathbb{C} : \alpha \cdot \Lambda \subset \Lambda\},\ f \mapsto \alpha_f,$$

is an isomorphism of rings.

If not stated otherwise by the above ring isomorphism we identify the endomorphism ring $End(T)$ with a subring of $\mathbb{C}$. Because each torus T is an Abelian group its endomorphism ring $End(T)$ comprises at least the group $\mathbb{Z}$:

$$\mathbb{Z} \subset End(T) \subset \mathbb{C}.$$

Which intermediate rings are possible? The case

$$End(T) = \mathbb{Z}$$

is the general case, justifying a specific name for tori with additional endomorphisms.

Definition 6.5 (Complex multiplication (*CM*)).

1. A complex number $\tau \in \mathbb{H}$ is a *CM-point* and its class $[\tau] \in X(\Gamma)$ in the modular curve is a *CM-class*, if the corresponding torus

$$T = \mathbb{C}/\Lambda,\ \Lambda = \mathbb{Z} \oplus \mathbb{Z} \cdot \tau,$$

satisfies

$$\mathbb{Z} \subsetneq End(T)$$

2. The values $j(\tau) \subset \mathbb{C}$ at *CM*-points $\tau \in \mathbb{H}$ are named *singular moduli* or *singular values* of the modular invariant j.

Theorem 6.6 states a remarkable relation between tori and number fields. It reveals the arithmetic structure encoded in a complex torus with complex multiplication.

Theorem 6.6 (Complex multiplication and imaginary quadratic fields). *Consider a point $\tau \in \mathbb{H}$.*

1. *Then: τ is a CM-point $\iff$ $\mathbb{Q}(\tau)$ is an imaginary quadratic number field.*

2. *If τ is a CM-point with $K := \mathbb{Q}(\tau)$, then the torus*

$$T := \mathbb{C}/\Lambda_\tau,\ \Lambda_\tau := \mathbb{Z} + \mathbb{Z} \cdot \tau,$$

has as ring of endomorphisms

$$End(T) \subset \mathbb{C}$$

an order of K.

Note that any order of an imaginary quadratic number field is a lattice.

Proof. 1. i) Consider a CM-point $\tau \in \mathbb{H}$. By definition exists $\alpha \in \mathbb{C} \setminus \mathbb{Z}$ with

$$\alpha \cdot \Lambda_\tau \subset \Lambda_\tau.$$

We obtain a matrix

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2 \times 2, \mathbb{Z})$$

with

$$\alpha \cdot \begin{pmatrix} 1 \\ \tau \end{pmatrix} = \gamma \cdot \begin{pmatrix} 1 \\ \tau \end{pmatrix}.$$

We obtain

$$\alpha = a + b \cdot \tau,\ \alpha \cdot \tau = c + d \cdot \tau,$$

which implies $b \neq 0$, because $\alpha \notin \mathbb{Z}$, and

$$b \cdot \tau^2 + (a - d) \cdot \tau - c = 0.$$

Because $\tau \in \mathbb{H}$ is not a real number, the number field $\mathbb{Q}(\tau)$ is imaginary quadratic.

ii) Assume that $\tau \in \mathbb{H}$ belongs to an imaginary quadratic number field. Then for suitable integers $a, b, c \in \mathbb{Z}$ with $a \neq 0$ because $\tau \in \mathbb{H}$

$$a \cdot \tau^2 + b \cdot \tau + c = 0.$$

From

$$(a\tau) \cdot \begin{pmatrix} 1 \\ \tau \end{pmatrix} = \begin{pmatrix} 0 & a \\ -c & -b \end{pmatrix} \cdot \begin{pmatrix} 1 \\ \tau \end{pmatrix}$$

follows $a\tau \in End(T),\ \alpha\tau \notin \mathbb{Z}$, and T has complex multiplication,

2. Assume that T has complex multiplication and consider an endomorphism $f \in End(T)$ operating as multiplication μ_α with a complex number α. Alike to the proof of part 1, i) we obtain a matrix

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2 \times 2, \mathbb{Z})$$

with

$$\alpha \cdot \begin{pmatrix} 1 \\ \tau \end{pmatrix} = \gamma \cdot \begin{pmatrix} 1 \\ \tau \end{pmatrix}$$

Therefore α is an eigenvalue of γ and satisfies the eigenvalue equation, which is an integral equation:

$$\alpha^2 - (d + a) \cdot \alpha + ab - cd = 0.$$

As a consequence $\alpha \in \mathcal{O}_K$, which implies

$$\mathbb{Z} \subsetneq End(T) \subset \mathcal{O}_K$$

Because $\mathcal{O}_K$ is free of rank $= 2$ the same holds true for $End(T)$, and the subring $End(T)$ is a sublattice of $\mathcal{O}_K$, i.e. an order, q.e.d.

We consider in detail the two elliptic points of the modular group Γ, see Theorem 2.16:

Example 6.7 (CM-points).

1. *Elliptic point i*: The point $i \in \mathbb{H}$ determines the normalized lattice of *Gaussian integers*

$$\Lambda_i = \mathbb{Z} + \mathbb{Z} \cdot i$$

The torus $T = \mathbb{C}/\Lambda_i$ has the endomorphism ring

$$End(T) = \Lambda_i$$

The endomorphism ring

$$End(T) = \Lambda_i$$

equals the ring

$$\mathcal{O}_K \subset K := \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$$

of algebraic integers from K. Recall from Corollary 3.21

$$j(i) = 1728 = 2^6 \cdot 3^3 \in \mathbb{Z}.$$

2. *Elliptic point* $\rho = e^{2\pi i/3}$: The point $\rho \in \mathbb{H}$ determines the normalized lattice

$$\Lambda_\rho = \mathbb{Z} + \mathbb{Z} \cdot \rho$$

The torus $T = \mathbb{C}/\Lambda_\rho$ has the endomorphism ring

$$End(T) = \Lambda_\rho$$

The result is similar to the first example: The endomorphism ring

$$End(T) = \Lambda_\rho$$

equals the ring

$$\mathcal{O}_K \subset K := \mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{-3})$$

of algebraic integers from K. Recall from Corollary 3.21

$$j(\rho) = 0 \in \mathbb{Z}.$$

Also the element $2\rho \in \mathbb{H}$ belongs to K. The torus

$$T = \mathbb{C}/\Lambda_{2\rho}$$

with the normalized lattice

$$\Lambda_{2\rho} = \mathbb{Z} + \mathbb{Z} \cdot 2\rho$$

has as endomorphisms the multiplication with arbitrary elements

$$\alpha \in \Lambda_{2\rho}.$$

For the proof one uses the equation

$$\rho^2 + \rho + 1 = 0.$$

The endomorphism ring is

$$End(T) = \mathscr{O}$$

with

$$\mathscr{O} = \Lambda_{2\rho} \subsetneq \mathscr{O}_K$$

is a proper order of K. Note $j(\rho) = 0 \in \mathbb{Z}$. A PARI-calculation shows

$$j(2\rho) = 54000 \in \mathbb{Z}.$$

6.2 Modular polynomials

The present section takes up the study of imaginary quadratic fields K from the viewpoint of modular forms. We relate complex multiplication to the value attainment of the modular j-function: Theorem 6.14 proves that the value $j(\tau) \in \mathbb{C}$ is an algebraic integer for any CM-class $[\tau] \in X(\Gamma)$. The main tool to derive the necessary properties of the modular j-invariant are the modular polynomials from Definition 6.8.

The *modular polynomials* are a family of polynomials $(F_m(X))_{m\in\mathbb{N}^*}$ which extract the properties of the j-invariant $j \in \mathscr{M}(\mathbb{H})$ from its transformation behaviour with respect to the operation of the modular group Γ

$$\Gamma \times \Gamma_{m,prim} \to \Gamma_{m,prim}$$

on the set of primitive matrices $\Gamma_{m,prim}$.

There is the following analogy to the family of Hecke operators $(T_m)_{m\in\mathbb{N}^*}$: The latter extract the Fourier coefficients of a given modular $f \in M_k(\Gamma)$ from the transformation behaviour of f with respect to the operation of the modular group Γ

$$\Gamma \times \Gamma_m \to \Gamma_m$$

on the set of matrices Γ_m. The Hecke operators are the family of linear maps with

$$T_m(f) := \sum_{M\in V(m)} f[M]_k$$

defined as the weighted sum of over a complete system $V(m)$ of representatives.

Similarly the modular polynomials are the family

$$F_m(X) = \prod_{M\in V(m,prim)} (X - j\circ M) \in \mathscr{M}(\mathbb{H})[X]$$

defined as the product over a complete set $V(m, prim)$ of representatives. Note the similarity between the definition $f[M]_k$ for modular forms from Definition 3.4 and the expression $j \circ M$ for the automorphic function j.

We take up the investigation of the integral matrices Γ_m from Section 5.1, in particular Definition 5.4 of the set $\Gamma_{m,prim}$ of primitive matrices and its complete set $V(m, prim)$ of representatives with respect to the canonical left Γ-operation. The set $V(m, prim)$ has cardinality

$$\psi(m) := m \cdot \prod_{\substack{p|m \\ \text{p prime}}} (1 + (1/p))$$

Definition 6.8 (Modular polynomials). Consider $m \in \mathbb{N}^*$ and the complete set $V(m, prim)$ of representatives of $\Gamma \backslash \Gamma_{m,prim}$.

1. Each matrix $M \in V(m, prim)$ induces the automorphism of the upper half-plane

$$M : \mathbb{H} \to \mathbb{H},\ \tau \mapsto M_\mu(\tau).$$

   The $\psi(m)$ functions

$$j_M := j \circ M \in V(m, prim)$$

   are the *class invariants* of $\Gamma \backslash \Gamma_m$.

2. The *m-th modular polynomial* is the polynomial

$$F_m(X) := \prod_{M \in V(m,prim)} (X - j_M) \in \mathscr{M}(\mathbb{H})[X].$$

Note. The modular invariant is constant along the orbits of the action of the modular group Γ. Therefore the value of j_M in Definition 6.8 does not depend on representing a coset from $\Gamma \backslash \Gamma_{m,prim}$ by the matrix $M \in V(m, prim)$ or by the matrix $\gamma \cdot M, \gamma \in \Gamma$.

Example 6.9 (Modular polynomials). The PARI-script `modular_polynomial_01` computes for several m the modular polynomials F_m, see Figure 6.1.

```
============================================================
modular_polynomial_01: Start

Modular polynomial F_2 : x^3 + (-j^2 + 1488*j - 162000)*x^2 + (1488*j^2 + 40773375*j + 8748000
000)*x + (j^3 - 162000*j^2 + 8748000000*j - 157464000000000)
------------------------------------------------
Modular polynomial F_3 : x^4 + (-j^3 + 2232*j^2 - 1069956*j + 36864000)*x^3 + (2232*j^3 + 2587
918086*j^2 + 8900222976000*j + 452984832000000)*x^2 + (-1069956*j^3 + 8900222976000*j^2 - 7708
45966336000000*j + 185542587187200000000)*x + (j^4 + 36864000*j^3 + 452984832000000*j^2 + 185
542587187200000000*j)
------------------------------------------------
modular_polynomial_01: End
============================================================
```

Fig. 6.1 Modular polynomials

1. $m = 2$:

$$\psi(2) = 3$$

and

$$F_2(X, j) = X^3 +$$
$$+(-j^2 + 1488 * j - 162000) * X^2 +$$
$$+(1488 * j^2 + 40773375 * j + 8748000000) * X +$$
$$+(j^3 - 162000 * j^2 + 8748000000 * j - 157464000000000)$$

2. $m = 3$:

$$\psi(3) = 4$$

and

$$F_3(X, j) = X^4 +$$
$$+(-j^3 + 2232 * j^2 - 1069956 * j + 36864000) * X^3 +$$
$$+(2232 * j^3 + 2587918086 * j^2 + 8900222976000 * j + 452984832000000) * X^2 +$$
$$+(-1069956 * j^3 + 8900222976000 * j^2 - 770845966336000000 * j + 185542587187200000000)$$
$$+(j^4 + 36864000 * j^3 + 452984832000000 * j^2 + 185542587187200000000 * j)$$

The roots of the modular polynomial $F_m(X) \in \mathscr{M}(\mathbb{H})[X]$ are exactly the class invariants $j_M \in V(m, prim)$ of the operation

$$\Gamma \times \Gamma_{m,prim} \to \Gamma_{m,prim}$$

We denote by $s_\mu,\ j = 1, ..., \psi(m)$, the elementary symmetric functions in $\psi(m)$ variables. Then up to sign the functions

$$s_\mu(j_1, ..., j_{\psi(m)}) \in \mathscr{M}(\mathbb{H}),\ j = 1, ..., \psi(m),$$

are the coefficients of the modular polynomial $F_m(X)$. E.g.,

$$(-1)^{\psi(m)} s_{\psi(m)}(j_1,...,j_{\psi(m)}) = (-1)^{\psi(m)} \cdot j_1 \cdot ... \cdot j_{\psi(m)}$$

is the constant term and

$$(-1) \cdot \sigma_1(j_1,...,j_{\psi(m)}) = -(j_1 + ... + j_{\psi(m)})$$

is the coefficient of the term $X^{\psi(m)-1}$. Theorem 6.10 now takes a closer look on these coefficients and proves: They are polynomials in the modular j-invariant with integer coeffcients, i.e. the coefficients belong to the subring

$$\mathbb{Z}[j] \subset \mathscr{M}(\mathbb{H}).$$

See also Example 6.9.

Theorem 6.10 (Coefficients of the modular polynomials). *For each* $m \in \mathbb{N}^*$

$$F_m(X) = \prod_{M \in V(m,prim)} (X - j_M) \in \mathbb{Z}[j][X] = \mathbb{Z}[j,X].$$

Proof. For arbitrary but fixed index $\mu = 1,...,\psi(m)$ we consider the coefficient

$$c := c_\mu := \sigma_\mu(j_1,...,j_{\psi(m)}) \in \mathscr{M}(\mathbb{H})$$

of the modular polynomial

$$F_m(X) \in \mathscr{M}(\mathbb{H})[X].$$

We prove step by step the following properties of the coefficient $c \in \mathscr{M}(\mathbb{H})$ until arriving at $c \in \mathbb{Z}$:

i) *Weakly modular*: According to Corollary 5.7 right multiplication with an element $\gamma \in \Gamma$ permutes the orbits of the Γ-left operation Φ_m

$$\{[M_1],...,[M_{\psi(m)}]\} = \{[M_1 \cdot \gamma],...,[M_{\psi(m)} \cdot \gamma]\}.$$

Hence right multiplication does not change the value of the elementary symmetric functions: For all $j = 1,...,\psi(m)$

$$\sigma_\mu(j_1,...,j_{\psi(m)}) = \sigma_\mu(j_1 \circ \gamma,...,j_{\psi(m)} \circ \gamma).$$

Therefore c is weakly modular.

ii) *Holomorphic on* $\mathbb{H}$: The j-invariant is holomorphic on $\mathbb{H}$ according to Corollary 3.16. Therefore also the coefficient c is holomorphic.

iii) *Meromorphic at* ∞: The coefficient c is weakly modular according to part i). Hence c has a Fourier expansion

$$c(\tau) = \sum_{\nu \in \mathbb{Z}} a_\nu \cdot q^\nu,\ q = e^{2\pi i \tau}.$$

We have to show that the singularity $q = 0$ is a pole of c. For the proof we estimate the growth of c: According to Corollary 3.21 the modular invariant has the Fourier expansion

$$j(\tau) = \frac{1}{q} + P(q)$$

with $P \in \mathbb{Z}\{q\}$ a convergent power series with integer coefficients. For an upper triangular matrix

$$\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in V(m, prim)$$

the Fourier series of the class invariant $j \circ \alpha$ derives from the Fourier series of j by substituting the variable $q = e^{2\pi i \tau}$ by

$$e^{2\pi i \alpha(\tau)} = e^{2\pi i (b/d)} \cdot q^{(a/d)}$$

The equality

$$ad = m$$

implies

$$e^{2\pi i \alpha(\tau)} = \zeta_m^{ab} \cdot (q^{1/m})^{a^2} \text{ with } \zeta_m := e^{2\pi i/m}$$

a primitive m-th root of unity. In particular

$$|(j \circ \alpha)(\tau)| \leq \frac{1}{|q|^{a/d}} + O(1)$$

for a single class invariant. Hence for suitable constants k, M

$$|c(\tau)| \leq M \cdot \frac{1}{|q|^k}$$

for small $q \in \Delta \setminus \{0\}$.

iv) *Integrality* $c \in \mathcal{O}_K[j]$: Due to the part already proved, Corollary 3.22 implies that c is a polynomial with complex coefficients in the modular invariant, i.e.

$$c \in \mathbb{C}[j].$$

We show that even

$$c \in \mathcal{O}_K[j]$$

with

$$K := \mathbb{Q}(\zeta_m)$$

the m-th cyclotomic number field. For the proof we recall from part iii) the substitution of q by

$$\zeta_m{}^{ab} \cdot (q^{1/m})^{a^2}.$$

As a consequence the class invariant $j \circ \alpha$ has a Fourier expansion with respect to $q^{1/m}$, namely

$$j(\alpha(\tau)) = \frac{1}{(q^{1/m})^{a^2} \cdot \zeta_m{}^{ab}} + P\left((q^{1/m})^{a^2} \cdot \zeta_m{}^{ab}\right),$$

which shows that the Fourier coefficents of c belong to K. According to Corollary 3.22 the coefficients of the polynomial $c \in \mathbb{C}[j]$ are $\mathbb{Z}$-linear combinations of the Fourier coefficients of c. Hence the coefficients are $\mathbb{Z}$-linear combinations of the m-th roots of unity. Therefore the coefficients of $c \in \mathbb{C}[j]$ are algebraic integers from $\mathcal{O}_K$, i.e. $c \in \mathcal{O}_K[j]$.

v) *Integrality* $c \in \mathbb{Z}[j]$: The operation of the Galois group

$$Gal(K/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^*.$$

extends to an operation on the set $\{j_1, ..., j_{\psi(m)}\}$ of class invariants

$$Gal(K/\mathbb{Q}) \times \{j_1, ..., j_{\psi(m)}\} \to \{j_1, ..., j_{\psi(m)}\},\ (\chi, j_\mu) \mapsto j_\mu{}^\chi,$$

which is defined as follows: Assume $\chi \in Gal(K/\mathbb{Q})$ maps $\chi(\zeta_m) = \zeta_m{}^e$ with $(e,m) = 1$. If j_μ is the class invariant of the matrix

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

then we define $j_\mu{}^\chi$ as the class invariant of the matrix

$$M^\chi = \begin{pmatrix} a & b^\chi \\ 0 & d \end{pmatrix}$$

with

$$0 \le b^\chi < d \text{ and } b^\chi \equiv e \cdot b \mod d.$$

Because the function c is fixed under the operation of $Gal(K/\mathbb{Q})$, its Fourier coefficients belong to the fixed field $\mathbb{Q}$. Due to part iv) the Fourier coefficients even belong to

$$\mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z},\ q.e.d.$$

We now evaluate the modular polynomials

$$F_m(X) \in \mathbb{Z}[j][X]$$

on the diagonal $\{X = j\}$, i.e. we consider the polynomials of the single variable j

$$\Phi_m(j) := F_m(j,j) = \prod_{M \in V(m,prim)} (j - j_M) \in \mathbb{Z}[j].$$

Example 6.11 (The polynomials $\Phi_m(j) \in \mathbb{Z}[j]$). We take up Example 6.9 with Figure 6.2, which shows some polynomials Φ_m. The PARI script `Modular_polynomial_02` computes their factorization:

1. $m = 2$:

   $$\Phi_2(j) = F_2(j,j) = -j^4 + 2978 * j^3 + 40449375 * j^2 + 17496000000 * j - 157464000000000$$

   splits into the factors

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

2. $m = 3$:

   $$\Phi_3(j) = F_3(j,j) = -j^6 + 4464 * j^5 + 2585778176 * j^4 + 17800519680000 * j^3$$
   $$-769939996672000000 * j^2 + 3710851743744000000000 * j$$

   splits into the factors

   $$j - 54000,\ (j - 8000)^2,\ j,\ (j + 32768)^2$$

3. The example $\Phi_5(j)$ shows: In general $\Phi_m(j)$, *m prime*, does not split into linear factors over $\mathbb{Z}$.

```
modular_polynomial_02: Start

Polynomial Phi_2 : -j^4 + 2978*j^3 + 40449375*j^2 + 17496000000*j - 157464000000000
factor 1 = [j - 8000, 1]
factor 2 = [j - 1728, 1]
factor 3 = [j + 3375, 2]
-----------------------------------------------
Polynomial Phi_3 : -j^6 + 4464*j^5 + 2585778176*j^4 + 17800519680000*j^3 - 769939996672000000*j^2 + 3710851743744000000000*j
factor 1 = [j - 54000, 1]
factor 2 = [j - 8000, 2]
factor 3 = [j, 1]
factor 4 = [j + 32768, 2]
-----------------------------------------------
Polynomial Phi_5 : -j^10 + 7440*j^9 + 1665990262720*j^8 + 215757860427776000*j^7 - 44044079829384857963724 8*j^6 + 53797234800359280738891202560*j^5 + 472602591088402774948339764953088 0*j^4 + 736699627235561376470215877959090176 00*j^3 - 250688456991364600842741491417948646014976*j^2 + 10654866160684885090084032054671301830246400 0*j + 14135994715472135869775347469107136275100467 2000
factor 1 = [j - 287496, 2]
factor 2 = [j - 1728, 2]
factor 3 = [j + 32768, 2]
factor 4 = [j + 884736, 2]
factor 5 = [j^2 - 1264000*j - 681472000, 1]
-----------------------------------------------
modular_polynomial_02: End
```

Fig. 6.2 Some polynomials Φ_m and their factorization

Lemma 6.12 (Leading coefficient of the modular polynomials). *For squarefree $m \geq 2$ the polynomial*

$$\Phi_m(j) \in \mathbb{Z}[j]$$

has leading coefficient ± 1.

Example 6.9 illustrates Lemma 6.12 by

$$\Phi_2(j) = -j^4 + O(3),\ \Phi_3(j) = -j^6 + O(5) \text{ and } \Phi_7(j) = -j^{10} + O(9).$$

Proof. The function

$$\Phi_m(j) : \mathbb{H} \to \mathbb{C}$$

is an automorphic function. Consider its Fourier expansion

$$\Phi_m(j)(\tau) = \frac{c_k}{q^k} + \frac{c_{k-1}}{q^{k-1}} + \text{ higher terms}$$

Because j has a pole at $\tau = \infty$ of order $= 1$, the coefficient c_k of the Fourier series is also the leading coefficient of Φ_m as polynomial in j. The coefficient is the product of the highest negative coefficients of the factors

$$j - j_\mu,\ \mu = 1, ..., \psi(m).$$

For arbitrary but fixed μ the representation

$$j(\tau) = \frac{1}{q} + P(q)$$

implies

$$j_\mu(\tau) = j\left(\frac{a\tau + b}{d}\right) = \frac{e^{-2\pi i(b/d)}}{q^{a/d}} + P\left(q^{a/d} \cdot e^{2\pi i(b/d)}\right)$$

with j_μ corresponding to the matrix

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in V(m, prim).$$

Hence the highest negative coefficient in the Fourier expansion of $j - j_\mu$ is

$$\begin{cases} 1 & a < d \\ e^{-2\pi i(b/d)} & a > d \end{cases}$$

Note that the case $a = d$ is excluded because $m = a \cdot d$ is squarefree. In any case the highest negative coefficent of

$$j - j_\mu$$

is a root of unity, and the same holds for the coefficient c_k of the product

$$\Phi = \prod_{M \in V(m,prim)} (j - j_M).$$

Because $c_k \in \mathbb{Z}$ we have $c_k = \pm 1$, q.e.d.

According to Theorem 6.10 the modular polynomial

$$F_m(j,X) := F_m(X) = \prod_{\mu=1}^{\psi(m)} (X - j_\mu) \in \mathbb{Z}[j,X]$$

is a polynomial in the two variables j and X with integer coefficients. It expands as

$$F_m(j,X) = \sum_{n=0}^{N} \left(\sum_{r+s=n} c_{rs} \cdot j^r \cdot X^s \right), \; c_{rs} \in \mathbb{Z}.$$

Proposition 6.13 will show that $F_m(j,X)$ is symmetric in both variables, i.e. the coefficients satisfy

$$c_{rs} = c_{sr}.$$

As a consequence, the highest exponent of j in $F_m(j,X)$ is $\psi(m)$.

Proposition 6.13 (Symmetry of the modular polynomials). *The modular polynomials*

$$F_m(j,X) \in \mathbb{Z}[j,X], \; m \in \mathbb{N}^*,$$

are symmetric with respect to j and X, i.e.

$$F_m(j,X) = F_m(X,j).$$

Proof. We set $R = \mathbb{Z}[j]$ with quotient field

$$K := Q(R) = \mathbb{Q}(j).$$

i) *Irreducibility of $F_m(X) \in R[X]$ over K*: The modular polynomial

$$F_m(X) = \prod_{M \in V(m,prim)} (X - j_M) \in R[X]$$

has as roots the class invariants

$$j_M \in V(m,prim) = \{j_1, ..., j_{\psi(m)}\}.$$

They are pairwise distinct which can be shown by comparing their Fourier coefficients. To prove that $F_m(X)$ is an irreducible polynomial we show that the Galois group

$$Gal(L/K)$$

of the splitting field

$$L = K(j_1, ..., j_{\psi(m)})$$

of the polynomial $F_m(X) \in R[X]$ acts transitively on the roots. Then no root belongs to the fixed field K.

Elements of the Galois group can be obtained as follows: Any matrix $\gamma \in \Gamma$ defines the automorphism

$$L = K(j_1, ..., j_{\psi(m)}) \to L,\ f \mapsto f \circ \gamma.$$

Consider two class invariants

$$j_\mu, j_\nu,\ 1 \le \mu, \nu \le \psi(m)$$

corresponding to the matrices

$$M_\mu, M_\nu \in V(m, prim)$$

One has to find $\gamma \in \Gamma$ such that

$$j_\nu = j_\mu \circ \gamma$$

i.e. one has to find $\gamma, \gamma' \in \Gamma$ such that

$$\gamma' \cdot M_\nu = M_\mu \cdot \gamma,$$

which is achieved by Proposition 5.9, part 2). Therefore $Gal(L/K)$ operates transitively on the roots of $F_m(X)$, and the latter polynomial is irreducible over K.

ii) *Common root of* $F_m(j,X)$ *and* $F_m(X,j)$: We consider the two polynomials

$$f(X) := F_m(j,X) \in R[X] \text{ and } g(X) := F_m(X,j) \in R[X]$$

For any matrix $M \in V(m, prim)$ the class invariant

$$j_M := j \circ M$$

is a root of the modular polynomial $f(X) \in R[X]$. In particular for

$$\alpha := \begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix} \in V_{m,prim}$$

holds for all $\tau \in \mathbb{H}$

$$0 = f(j_\alpha(\tau)) = F_m(j(\tau), j_\alpha(\tau)) = F_m\left(j(\tau), j\left(\frac{\tau}{m}\right)\right)$$

Replacing the argument τ by $\tau \cdot m$ shows for all $\tau \in \mathbb{H}$

$$0 = F_m(j(\tau \cdot m), j(\tau)) = F_m(j_\beta(\tau), j(\tau)) = g(j_\beta(\tau)) \text{ i.e. } g(j_\beta) = 0$$

with

$$\beta := \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} \in V_{m,prim}$$

Also $f(j_\beta) = 0$ because $\beta \in V_{m,prim}$. Hence both polynomials $f(X), g(X) \in R[X]$ have the common root j_β.

iii) *Symmetry*: Due to Lemma 6.12 and part i) the polynomial $f(X) \in K[X]$ is irreducible with leading coefficient ± 1. Hence $f(X)$ is the minimal polynomial of the field extension $K \subset K[j_\beta]$, and $g(X)$ is a multiple of $f(X)$, i.e.

$$g(X) = h(X) \cdot f(X)$$

with a polynomial $h(X) \in K[X]$. According to Theorem 6.10 both polynomials $f(X)$ and $g(X)$ have their coefficients already in the ring $R = \mathbb{Z}[j]$. The ring R is factorial as a ring of polynomials over the factorial ring $\mathbb{Z}$. The Lemma of Gauss implies that also the polynomial $h[X]$ has all coefficients from R, and the equation

$$g(X) = h(X) \cdot f(X)$$

holds in $R[X]$. Set

$$H(j,X) := h(X) \in R[X] = \mathbb{Z}[j][X].$$

Then

$$F_m(X,j) = H(j,X) \cdot F_m(j,X) \in \mathbb{Z}[j,X].$$

Considered as an equation in the ring $\mathbb{Z}[j,X]$ of polynomials in two variables the last equation is invariant when interchanging the role of j and X. Hence also

$$F_m(j,X) = H(X,j) \cdot F_m(X,j) \in \mathbb{Z}[j,X].$$

As a consequence

$$F_m(j,X) = H(X,j) \cdot H(j,X) \cdot F_m(j,X),$$

$$H(X,j) \cdot H(j,X) = 1,$$

and

$$H(X,j) = H(j,X) = \pm 1.$$

In case $H(X,j) = -1$ the previous equation

$$F_m(j,X) = H(X,j) \cdot F_m(X,j)$$

would imply

$$F_m(X,j) = -F_m(j,X) \text{ and } F_m(j,j) = -F_m(j,j).$$

Then

$$F_m(j,j) = 0$$

which contradicts the fact that $\Phi_m(j) = F_m(j,j)$ has leading coefficient ± 1 according to Lemma 6.12. Therefore

$$H(X,j) = 1$$

and

$$F_m(j,X) = F_m(X,j),\ q.e.d.$$

We now derive from the theory of modular polynomials that all singular values $j(\tau)$ are algebraic integers.

Theorem 6.14 (Singular values of the modular j-invariant). *For each CM-point $\tau \in \mathbb{H}$ the j-value $j(\tau) \in \mathbb{C}$ is an algebraic integer. More precisely: There exists $m \in \mathbb{N}^*$ such that $j(\tau)$ is a root of the polynomial $\Phi_m(X) \in \mathbb{Z}[X]$.*

Proof. Consider a CM-point $\tau \in \mathbb{H}$. Theorem 6.6 implies that τ belongs to an imaginary quadratic field

$$K = \mathbb{Q}(\sqrt{d})$$

with $d \in \mathbb{Z},\ d < 0$ squarefree. The subring

$$\mathcal{O}_K \subset K$$

of algebraic integers of K is a free $\mathbb{Z}$-module of rank $= 2$

$$\mathcal{O}_K = \mathbb{Z} \oplus \mathbb{Z} \cdot z$$

with a $\mathbb{Z}$-basis $(z,1)$, $z \in \mathbb{H}$. For admissible values of z see Remark 6.2.

i) *A matrix $\alpha \in \Gamma_{m,prim}$ which fixes z*: If a matrix $\alpha \in \Gamma_{m,prim}$ fixes a point $\tau \in \mathbb{H}$, i.e. if

$$\alpha(\tau) = \tau,$$

then

$$j(\tau) = j(\alpha(\tau))$$

and vice versa. Hence the fixed points of the matrices $\alpha \in \Gamma_{m,prim}$ correspond to the roots of the polynomial $\Phi_m(X) \in \mathbb{Z}[X]$. We determine a matrix $\alpha \in \Gamma_{m,prim}$ which fixes z: The element

$$\xi := \begin{cases} \sqrt{d} & d < -1 \\ \\ 1+i & d = -1 \end{cases}$$

is an algebraic integer. Its norm

$$N(\xi) = \xi\overline{\xi} \in \mathbb{Z}$$

is squarefree. Multiplication with $\xi \in \mathscr{O}_K$ defines a $\mathbb{Z}$-linear endomorphism

$$\mathscr{O}_K \to \mathscr{O}_K,\ x \mapsto \xi \cdot x.$$

Denote by

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2\times 2,\mathbb{Z}) \cap GL(2,\mathbb{R})^+$$

its matrix with respect to the basis $(z,1)$ of $\mathscr{O}_K$. Then

$$\xi \cdot \begin{pmatrix} z \\ 1 \end{pmatrix} = \alpha \cdot \begin{pmatrix} z \\ 1 \end{pmatrix}$$

or in components

$$\begin{pmatrix} \xi \cdot z \\ \xi \cdot 1 \end{pmatrix} = \begin{pmatrix} az+b \\ cz+d \end{pmatrix}$$

- The first form shows: The matrix

  $$\alpha \in M(2\times 2,\mathbb{Z})$$

  which represents the $\mathbb{Z}$-linear multiplication by ξ has the eigenvalue ξ and by conjugation $\alpha = \overline{\alpha}$ also the eigenvalue $\overline{\xi}$. Hence

  $$m := det\ \alpha = \xi\overline{\xi} = N(\xi) \in \mathbb{Z}$$

  is squarefree which implies

  $$(a,b,c,d) = 1$$

  and therefore

  $$\alpha \in \Gamma_{m,prim}$$

  due to Definition 5.4.

- The component form shows: Considered as a fractional linear transformation

  $$\mathbb{H} \to \mathbb{H},\ w \mapsto \alpha(w) := \frac{a\cdot w+b}{c\cdot w+d}$$

  the matrix matrix $\alpha \in GL(2,\mathbb{R})^+$ satisfies

  $$\alpha(z) = \frac{a\cdot z+b}{c\cdot z+d} = \frac{\xi\cdot z}{\xi\cdot 1} = z$$

ii) $j(z)$ *is an algebraic integer*: Lemma 5.6 implies the existence of a matrix

$$\alpha_\mu \in V(m,prim),\ \mu \in \{1,...,\psi(m)\},$$

with the same Γ-orbit as α with respect to the left action

$$\Phi_{m,prim} : \Gamma \times \Gamma_{m,prim} \to \Gamma_{m,prim},\ (A,M) \mapsto A \cdot M,$$

w.l.o.g. $\mu = 1$. Then

$$j \circ \alpha = j \circ \alpha_1$$

because the value of j is constant along each orbit of the Γ-operation. Due to part i)

$$j(z) = j(\alpha(z)) = j(\alpha_1(z)) = j_1(z),$$

which implies: The function

$$\Phi_m(j) = \prod_{M \in V(m,prim)} (j - j_M) \in \mathbb{Z}[j]$$

vanishes at $z \in \mathbb{H}$:

$$\Phi_m(j)(z) = \Phi_m(j(z)) = 0.$$

The polynomial

$$\Phi_m(j) \in \mathbb{Z}[j]$$

has integer coefficients, and leading coefficient ± 1 due to Lemma 6.12. Hence

$$0 = \Phi_m(j(z))$$

proves that $j(z)$ is an algebraic integer. Hence the subring

$$\mathbb{Z}[j(z)] \subset \mathbb{C}$$

is integral over the ring $\mathbb{Z}$.

iii) $j(\tau)$ *is integral over* $\mathbb{Z}[j(z)]$: The given element

$$\tau \in K = \mathbb{Q} + \mathbb{Q} \cdot z$$

has a representation

$$\tau = \beta(z) := \frac{az+b}{d}$$

with a primitive matrix

$$\beta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Gamma_{m,prim},\ m := a \cdot d.$$

Alike to the argument from part ii) the Γ-orbit of β passes through a matrix $\alpha_\mu \in V(m, prim)$ which proves

$$j(\tau) = j(\beta(z)) = j(\alpha_\mu(z)) = j_\mu(z).$$

Theorem 6.10 implies that j_μ is integral over the ring $\mathbb{Z}[j]$. Hence

$$j(\tau) = j_\mu(z)$$

is integral over $\mathbb{Z}[j(z)]$.

iv) $j(\tau)$ *is an algebraic integer*: When combining part iii) and part ii) the transitivity of integral dependence proves the integrality of $j(\tau)$ over $\mathbb{Z}$, i.e. τ is an algebraic integer, q.e.d.

Example 6.15 (Singular values of the modular j-function). Continuing Example 6.11 we consider a *CM*-class $[\tau] \in X(\Gamma)$ and choose the level

$$m = 2.$$

1. According to Example 6.11 the polynomial

$$\Phi_2(j) \in \mathbb{Z}[j]$$

has degree $= 4$ and factorizes as

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

Which property is expressed by the three factors, why are the values $j \in \{8000,\ 1728,\ -3375\}$ related?

According to Theorem 6.14 we determine a complete set of representatives

$$\alpha_j \in \Gamma_{2,prim},\ j = 1,2,3,$$

with fixed points $\alpha_j(z_j) = z_j,\ z_j \in \mathbb{H}$:

- $$\alpha_1 = \begin{pmatrix} 1 & -2 \\ 1 & 0 \end{pmatrix} \text{ has fixed point } z_1 = \frac{1 + i\sqrt{7}}{2}$$

  which defines the lattice

$$\Lambda_1 := < 1, \frac{1 + \sqrt{-7}}{2} > = \mathcal{O}_{K_1} \subset K_1 := \mathbb{Q}(\sqrt{-7})$$

  of the torus $T_1 := \mathbb{C}/\Lambda_1$.

- $$\alpha_2 = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \text{ has fixed point } z_2 = i$$

  which defines the lattice

$$\Lambda_2 := < 1, i > = \mathscr{O}_{K_2} \subset K_2 := \mathbb{Q}(\sqrt{-1})$$

of the torus $T_2 := \mathbb{C}/\Lambda_2$.

- $$\alpha_3 = \begin{pmatrix} 0 & -1 \\ 2 & 0 \end{pmatrix} \text{ has fixed point } z_3 = i\sqrt{2}$$

  which defines the lattice

$$\Lambda_3 := < 1, i\sqrt{2} > = \mathscr{O}_{K_3} \subset K_3 := \mathbb{Q}(\sqrt{-2})$$

of the torus $T_3 := \mathbb{C}/\Lambda_3$.

Hence the three resulting fields $K_j,\ j = 1,2,3$ are imaginary quadratic. Due to Theorem 6.6 each of the three fields relates to a torus with complex multiplication. In addition Theorem 6.14 shows that the tori have their j-values from

$$\{8000, 1728, -3375\}$$

We already know $j(z_2) = j(i) = 1728$. A PARI-computation completes at once the remaining values

$$j(z_1) = -3375 \text{ and } j(z_3) = 8000.$$

One knows that all three fields have class number $h_K = 1$, which will confirm Corollary 6.23.

6.3 Fractional ideals and the class number formula

A further application of the modular j-invariant to number theory is the class number formula for imaginary quadratic fields.

We first recall the divisor sequence of a Riemann surface, e.g., cf. [63].

Remark 6.16 (Class group of a compact Riemann surface). The divisor sequence on a compact Riemann surface X

$$1 \to \mathscr{O}^* \to \mathscr{M}^* \to \mathscr{D} \to 0$$

provides the exact sequence of Abelian groups

$$1 \to \mathbb{C}^* \to \mathscr{M}^*(X) \to Div(X) \to Cl(X) \to 0.$$

because

$$H^0(X,\mathscr{O}^*)=\mathbb{C}^*,\ H^0(X,\mathscr{D})=Div(X),\ Cl(X):=\frac{Div(X)}{im[\mathscr{M}^*(X)\to Div(X)]}\ \text{and}\ H^1(X,\mathscr{M}^*)=0$$

The vanishing $H^1(X,\mathscr{M}^*)=0$ is a result from the theory of compact Riemann surfaces. It implies the isomorphy

$$Cl(X)\xrightarrow{\simeq}H^1(X,\mathscr{O}^*)=Pic(X)$$

between the group of divisor classes and the Picard group of isomorphism classes of holomorphic line bundles on X.

For number fields an analogue of divisors are fractional ideals, see [4, Chap. 9].

Definition 6.17 (Fractional ideal). Consider a number field K of degree.

1. A *fractional ideal* of K is defined as an $\mathscr{O}_K$-submodule $\mathfrak{a}\subset K$ for which there exists an element $d\in\mathscr{O}_K,\ d\neq 0$, with

   $$d\cdot\mathfrak{a}\subset\mathscr{O}_K.$$

   Hence a fractional ideal is a subset of the form

   $$\mathfrak{a}=\frac{\tilde{a}}{d}\subset K$$

   with an ideal $\tilde{a}\subset\mathscr{O}_K$. The element d is named a *common denominator* of $\mathfrak{a}$.

2. Fractional ideals generated by a single element $\alpha\in K$

   $$\mathfrak{a}=(\alpha):=\mathscr{O}_K\cdot\alpha$$

   are named *principal* fractional ideals.

3. For two fractionals ideals $\mathfrak{a},\ \mathfrak{b}\subset K$ the *product*

   $$\mathfrak{a}\cdot\mathfrak{b}$$

   is the fractional ideal generated by all products $a\cdot b,\ a\in\mathfrak{a},\ b\in\mathfrak{b}$.

4. For a fractional ideal $\mathfrak{a}\neq\{0\}$ the set

   $$\mathfrak{a}^{-1}:=\{x\in K:\ x\cdot\mathfrak{a}\subset\mathscr{O}_K\}$$

   is named the *inverse* of $\mathfrak{a}$.

Remark 6.18 (Fractional ideals). Consider a number field K with number ring $\mathscr{O}_K$.

1. Each non-zero ideal of $\mathcal{O}_K$ and each non-zero fractional ideal of K is a lattice of rank $= deg\ K$. The fractional ideals of K are the finitely generated $\mathcal{O}_K$-submodules of K.

2. Because $\mathcal{O}_K$ is a Dedekind ring for a fractional ideal

$$\mathfrak{a} \neq \{0\} \subset K$$

the inverse $\mathfrak{a}^{-1}$ is also a fractional ideal, see [4, Theor. 9.8]. It satisfies

$$\mathfrak{a} \cdot \mathfrak{a}^{-1} = (1)$$

3. With respect to multiplication the set of fractional ideals is an Abelian group $J(K)$. Its quotient by the subgroup of principal fractional ideals is named the *ideal class group* or simply *class group* of K

$$Cl(K) := J(K)/im[K^* \to J(K)]$$

The canonical map is

$$K^* \to J(K),\ x \mapsto (x).$$

Hence two fractional ideals

$$\mathfrak{a}_1,\ \mathfrak{a}_2 \in J(K)$$

define the same class in $Cl(K)$ iff

$$\mathfrak{a}_2 = a \cdot \mathfrak{a}_1 \text{ for a suitable } a \in K^*.$$

As a consequence there is an exact sequence of multiplicative Abelian groups

$$1 \to \mathcal{O}_K^* \to K^* \to J(K) \to Cl(K) \to 1$$

4. A number ring $\mathcal{O}_K$ is a principal ideal domain iff

$$h_K = 1$$

A theorem from algebraic number theory states the finiteness of the *class number*

$$h_K := ord\ Cl(K)$$

see [40, Chap. 5, Cor. 2], [32, Chap. 12, §2]. The result is an analogue to the fact that the Neron-Severi group

$$NS(X) := Pic(X)/Pic_0(X)$$

of a compact Riemann surface is finitely generated. This similarity strongly validates the analogy between the function fields of compact Riemann surfaces and number fields.

5. Comparing the exact sequence of a number field with the exact divisor sequence of a Riemann surface from Remark 6.16 one easily observes the analogy between corresponding objects:

Compact Riemann surface X	Number field K
$\mathscr{O}_X^*$	$\mathscr{O}_K^*$
$\mathscr{M}_X^*$	K^*
$Div(X)$	$J(K)$
$Cl(X)$	$Cl(K)$

Example 6.19 (Class number).

1. There are exactly 9 imaginary quadratic fields

$$K = \mathbb{Q}(\sqrt{-D}),\ D > 0 \text{ squarefree integer},$$

with class number $h_K = 1$. They belong to the values

$$D \in \{1,2,3,7,11,19,43,67,163\}.$$

2. The imaginary quadratic field

$$K = \mathbb{Q}(\sqrt{-5})$$

has class number $h_K = 2$. The class of the ideal

$$(2, 1+\sqrt{-5}) \subset \mathscr{O}_K$$

is not principal. It generates $Cl(K)$, see [40, Chap. 5].

We now consider isomorphism classes of tori with complex multiplication and a given number ring $\mathscr{O}_K$. How many isomorphism classes have $\mathscr{O}_K$ as ring of endomorphisms? Proposition 6.20 shows that their number equals the class number h_K. In particular, there are only finitely many isomorphism classes of tori with endomorphism ring $\mathscr{O}_K$.

Proposition 6.20 (Class group and tori with given endomorphism ring). *Consider an arbitrary, but fixed imaginary quadratic field K with ring of integers $\mathscr{O}_K$. There exists a bijection*

$$Cl(K) \xrightarrow{\simeq} \{[T] :\ T \text{ torus with } End(T) = \mathscr{O}_K\}$$

between the ideal class group $Cl(K)$ and the set of classes of biholomorphically equivalent complex tori with ring of endomorphisms $\mathscr{O}_K$. The bijection is induced by the attachement

$$\textit{normalized lattice } \Lambda \in J(K) \mapsto T = \mathbb{C}/\Lambda \textit{ with } End(T) = \mathscr{O}_K.$$

Its inverse is induced by the attachement

$$\textit{normalized torus } T = \mathbb{C}/\Lambda \textit{ with } End(T) = \mathscr{O}_K \mapsto \Lambda \in J(K).$$

Proof. i) *Well-definedness of the map*: Starting with a fractional ideal

$$\Lambda \subset K \subset \mathbb{C}$$

we may assume

$$\Lambda = \mathbb{Z} + \mathbb{Z} \cdot \omega$$

a normalized lattice because the ideal class is determined up to an element of K. Due to Proposition 6.4 the torus

$$T := \mathbb{C}/\Lambda$$

has the endomorphism ring

$$End(T) = \{\alpha \in \mathbb{C} : \ \alpha \cdot \Lambda \subset \Lambda\}$$

Because Λ is an $\mathscr{O}_K$-module one obtains

$$\mathscr{O}_K \subset End(T).$$

For the opposite inclusion consider a number $\alpha \in End(T)$, i.e. $\alpha \cdot \Lambda \subset \Lambda$. The normalization $\mathbb{Z} + \mathbb{Z} \cdot \tau = \Lambda$ implies

$$\alpha \cdot 1 = \alpha \in \Lambda.$$

ii) *Well-definedness of the inverse map*: Starting with a normalized torus

$$T = \mathbb{C}/\Lambda_\tau, \ \Lambda_\tau = \mathbb{Z} + \mathbb{Z} \cdot \tau, \text{ with } End(T) = \mathscr{O}_K$$

we have to show that $\Lambda_\tau \subset K$ is a fractional ideal. After choosing a $\mathbb{Z}$-basis $(1, \omega)$ of $\mathscr{O}_K$ the assumption

$$\mathscr{O}_K = End(T) = \{\alpha \in \mathbb{C} : \ \alpha \cdot \Lambda_\tau \subset \Lambda_\tau\}$$

provides a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(2 \times 2, \mathbb{Z})$$

with

$$\omega \cdot \begin{pmatrix} 1 \\ \tau \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 \\ \tau \end{pmatrix}.$$

Hence

$$\omega = a + b \cdot \tau \text{ and } \omega \cdot \tau = c + d \cdot \tau$$

- The second equation implies
$$\tau = \frac{c}{\omega - \alpha},$$
hence $\Lambda_\tau \subset Q(\mathscr{O}_K) = K$.

- The lattice $\Lambda_\tau \subset K$ is an $\mathscr{O}_K$-module because both equations taken together imply
$$1, \omega, \tau, \tau \cdot \omega \in \Lambda_\tau$$

- Finally the first equation implies
$$b \cdot \Lambda_\tau \subset \mathbb{Z} + \mathbb{Z} \cdot b \cdot \tau \subset \mathbb{Z} + \mathbb{Z} \cdot \omega = \mathscr{O}_K$$

As a consequence $\Lambda_\tau \subset K$ is a fractional ideal of K.

iii) The two constructions from part i) and ii) are inverse to each other, q.e.d.

Lemma 6.21 (Rigidness of orders). *Consider an imaginary quadratic number field K, an order $\Lambda \subset \mathscr{O}_K$ and a subring $R \subset K$. If $\Lambda \cong R$ as ring isomorphism then $\Lambda = R$.*

Proof. For the proof assume $\Lambda = \mathbb{Z} + \mathbb{Z} \cdot \tau$ and consider a ring isomorphism
$$f : \Lambda \to R$$
For suitable $a, b \in \mathbb{Z}$ holds
$$\tau^2 = a \cdot \tau + b.$$
Then
$$f(\tau)^2 = f(a \cdot \tau + b) = a \cdot f(\tau) + b \implies$$
$$\implies (f(\tau) - \tau) \cdot (f(\tau) + \tau) = f(\tau)^2 - \tau^2 = a \cdot f(\tau) + b - \tau^2 =$$
$$= a \cdot f(\tau) + b - a \cdot \tau - b = a \cdot (f(\tau) - \tau)$$
Hence
$$f(\tau) = \tau \text{ or } f(\tau) = a - \tau$$
In both cases
$$R = f(\mathbb{Z} + \mathbb{Z} \cdot \tau) = \mathbb{Z} + \mathbb{Z} \cdot f(\tau) = \mathbb{Z} + \mathbb{Z} \cdot \tau, \ q.e.d.$$

The class number h_K of an imaginary quadratic number field K with number ring $\mathscr{O}_K$ relates to the singular value $j(\tau)$ of the j-invariant at an element $\tau \in \mathbb{H}$ with

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z} \cdot \tau$$

The complex number $j(\tau) \in \mathbb{C}$ is an algebraic integer due to Theorem 6.14. Hence $\mathbb{Q}(j(\tau))$ is a number field. We show the estimate

$$[\mathbb{Q}(j(\tau)) : \mathbb{Q}] \leq h_K.$$

Theorem 6.22 holds even in the strong form

$$[\mathbb{Q}(j(\tau)) : \mathbb{Q}] = h_K$$

See also [55, Chap. II, Theor. 4.3]. The book uses the notation

$$ELL(\mathcal{O}_K) := \{[T] : \ T \text{ torus with } End(T) \cong \mathcal{O}_K\}$$

with $[T]$ the biholomorphy class of the torus T.

Theorem 6.22 (Estimate of the class number). *Consider a given imaginary quadratic field K and denote by*

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z} \cdot \tau, \ \tau \in \mathbb{H},$$

its number ring. Then the class number h_K satisfies the estimate

$$[\mathbb{Q}(j(\tau)) : \mathbb{Q}] \leq h_K.$$

Proof. i) *Construction of a distinguished torus*: Consider the given number field K and its number ring

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z} \cdot \tau, \ \tau \in \mathbb{H}.$$

Proposition 6.20 provides a normalized ideal $\Lambda \subset J(K)$ such that the torus

$$T := \mathbb{C}/\Lambda$$

has endomorphism ring

$$End(T) = \mathcal{O}_K$$

Due to Theorem 4.3 the torus T embeds into $\mathbb{P}^2$ as a smooth cubic hypersurface, i.e. as the set $E = E(\mathbb{C})$ of complex points of a plane elliptic curve defined over $\mathbb{C}$.

ii) *The number field* $\mathbb{Q}(j(\tau))$: Theorem 6.6 implies that the complex number $\tau \in \mathbb{H}$ from part i) is a *CM*-point, and Theorem 6.14 concludes that $j(\tau) \in \mathbb{C}$ is an algebraic integer. Define the number field

$$L := \mathbb{Q}(j(\tau))$$

and denote by

$$m := [L : \mathbb{Q}]$$

its degree. There exist m field morphisms over $\mathbb{Q}$

$$\phi_i : L \to \mathbb{C},\ i = 1,...,m,$$

with pairwise distinct values $\phi_i(j(\tau))$. Each extends to an element of the Galois group $Gal(\mathbb{C}/\mathbb{Q})$. That's made possible by extending elements from the Galois group over $\mathbb{Q}$ along algebraic field extensions and along a pure transcendental field extension: A given element

$$\phi \in \{\phi_i :\ i = 1,...,m\}$$

can be considered an element

$$\phi^1 \in Gal(L_{sp}/\mathbb{Q})$$

with $L_{sp} \subset \mathbb{C}$ the splitting field of L over $\mathbb{Q}$. The element ϕ^1 extends to an element

$$\phi^2 \in Gal(\overline{\mathbb{Q}}/\mathbb{Q})$$

along the algebraic extension $[\overline{\mathbb{Q}} : L_{sp}]$. Choose a trancendence basis S of $\mathbb{C}$ over $\overline{\mathbb{Q}}$ and consider the field

$$K := \overline{\mathbb{Q}}(S),$$

and the pure transcendental extension $[K : \overline{\mathbb{Q}}]$. Then ϕ^2 extends to an element

$$\phi^3 \in Gal(K/\mathbb{Q}).$$

Finally ϕ^3 extends to an element

$$\sigma \in Gal(\mathbb{C}/\mathbb{Q})$$

along the algebraic exension $[\mathbb{C} : K]$. The resulting elements

$$\sigma_i \in Gal(\mathbb{C}/\mathbb{Q}),\ i = 1,...,m,$$

have pairwise distinct values $\sigma_i(j(\tau))$.

iii) *Functorial action of the Galois group*: For the elliptic curve

$$E = Var(f),\ f(X_0,X_1,X_2) = \sum_I a_I \cdot X^I \in \mathbb{C}[X_0,X_1,X_2]$$

and an element $\sigma \in Gal(\mathbb{C}/\mathbb{Q})$ the curve

$$E^\sigma := Var(f^\sigma),\ f^\sigma(X_0,X_1,X_2) := \sum_I \sigma(a_I) \cdot X^I,$$

defines again a plane elliptic curve. The attachment

$$E \mapsto E^\sigma$$

from part ii) extends to a functor, i.e. each morphism $\Phi : E \to E'$ defines a canonical morphism

$$\Phi^\sigma : E^\sigma \to E'^\sigma$$

with

$$id^\sigma = id \text{ and } (\Phi \circ \Psi)^\sigma = \Phi^\sigma \circ \Psi^\sigma$$

For the proof represent a given holomorphic map

$$\Phi : E \to E', \Phi(O) = O,$$

by its induced multiplication map

$$F := \mu_a : \mathbb{C} \to \mathbb{C},\ z \mapsto a \cdot z,$$

via the corresponding uniformization of the elliptic curves by complex tori $\mathbb{C}/\Gamma$ and $\mathbb{C}/\Gamma'$ from Theorem 4.28.

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{F} & \mathbb{C} \\ \downarrow & & \downarrow \\ E & \overset{\Phi}{\dashrightarrow} & E' \end{array} \qquad \begin{array}{ccc} z \neq 0 & \longrightarrow & a \cdot z,\ z \neq 0 \\ \downarrow & & \downarrow \\ (1 : \wp_\Gamma(z) : \wp'_\Gamma(z)) & \dashrightarrow & (1 : \wp_{\Gamma'}(a \cdot z) : \wp'_{\Gamma'}(a \cdot z)) \end{array}$$

The diagrams induce a unique commutative completion

$$\Phi : E \to E'$$

because

$$a \cdot \Gamma \subset \Gamma'$$

and the functions $\wp_{\Gamma'}$ and its derivative have the period Γ'. The morphism Φ is locally represented by a pair of rational maps

$$\left(\frac{p_1}{q_1}, \frac{p_2}{q_2} \right)$$

defined as quotient of polynomials. Eventually apply $\sigma \in Gal(\mathbb{C}/\mathbb{Q})$ to the coefficients of these polynomials to obtain a representative of Φ^σ.

As a consequence, for each $\sigma \in Gal(\mathbb{C}/\mathbb{Q})$ the map

$$End(E) \to End(E^\sigma),\ \Phi \mapsto \Phi^\sigma,$$

is a ring isomorphisms, i.e. $End(E^\sigma) \cong End(E)$. Lemma 6.21 implies

$$End(E^\sigma) = End(E).$$

iv) *The classes* $[E^\sigma]$: The elliptic curve E with affine polynomial

$$F(X,Y) = Y^2 - (4 \cdot X^3 - g_2 \cdot X - g_3)$$

has the j-invariant

$$j(E) = 1728 \cdot \frac{g_2^3}{g_2^3 - 27 \cdot g_3^2} = j(\tau).$$

Hence the elliptic curve E^σ has the affine polynomial

$$F^\sigma(X,Y) = Y^2 - (4 \cdot X^3 - \sigma(g_2) \cdot X - \sigma(g_3))$$

and the j-invariant

$$j(E^\sigma) = 1728 \cdot \frac{\sigma(g_2)^3}{\sigma(g_2)^3 - 27 \cdot \sigma(g_3)^2} = \sigma(j(\tau))$$

The biholomorphy classes of elliptic curves are determined by the j-invariants of the curves. The elements of the family

$$(j(E^{\sigma_i}) = \sigma_i(j(\tau))_{i=1,\ldots,m}$$

are pairwise distinct. Hence the elliptic curves

$$(E^{\sigma_i})_{i=1,\ldots,m}$$

with these j-invariants are pairwise not biholomorphic equivalent. For $i = 1,\ldots,m$ holds

$$End(E^{\sigma_i}) = \mathcal{O}_K$$

due to part iii). Proposition 6.20 implies that the corresponding ideal classes in $Cl(K)$ are pairwise distinct. Their number m is bounded by the class number

$$h_K = card\ Cl(K).$$

Hence

$$m = [L : \mathbb{Q}] \leq h_K,\ q.e.d.$$

Corollary 6.23 (Integer values of the modular invariant). *Consider an imaginary quadratic number field K with class number $h_K = 1$ and number ring*

$$\mathcal{O}_K = \mathbb{Z} + \mathbb{Z} \cdot \tau$$

Then $j(\tau) \in \mathbb{Z}$.

Proof. The proof follows from Theorem 6.14 and Theorem 6.22, q.e.d.

Chapter 7
Outlook: Modular elliptic curves, monstrous moonshine

7.1 Modular elliptic curves

The relation between elliptic curves $E/\mathbb{Q}$ and modular forms is given by Wiles' theorem, the proof of the Shimura-Taniyama-Weil conjecture for semistable elliptic curves. Wiles's modularity theorem has been subsequently extended to all elliptic curves $E/\mathbb{Q}$ by Breuil, Conrad, Diamond and Taylor. The modularity theorem relates for each elliptic curve $E/\mathbb{Q}$ the numbers

$$a_p(E) := 1 + p - card\ E_p(\mathbb{F}_p),\ p \text{ prime},$$

to the eigenvalues of Hecke operators acting on a suitable cusp form as common eigenform. The numbers $a_p(E)$ measure the deviation of the numbers of $\mathbb{F}_p$-valued points of the reduction $E(\mathbb{F}_p)$ from the average value, see Remark 4.42.

A first version of the relation between rational elliptic curves and the theory of modular forms is Conjecture 7.4.

Conjecture 7.1 (Shimura-Taniyama-Weil). For each elliptic curve $E/\mathbb{Q}$ exists a level $N \in \mathbb{N}$ and a non-constant holomorphic map from a modular curve

$$X_0(N) \to E(\mathbb{C})$$

Theorem 7.2 (Wiles' modularity theorem). *The Shimura-Taniyama-Weil conjecture is true.*

For the proof of the modularity theorem, Theorem 7.2, by Wiles in the stable and semistable case see the symposion [15]. Concerning the remaining cases subsequently proved by several authors see the announcement [16] and the proof in [10].

When comparing rational elliptic curves $E/\mathbb{Q}$ and cusp forms $f \in S_k(\Gamma_0(N))$ one compares the L-series of both mathematical objects. For the elliptic curve $E/\mathbb{Q}$ recall the L-series $L(E,-)$ arising from the numbers $(a_p(E))_{p \text{ prime}}$, see Definitions 4.44 and 4.46, and also Remark 4.45.

For the cusp form f see Definition 7.3.

Definition 7.3 (L-series of a cusp form). Consider a level $N \in \mathbb{N}^*$ and a weight $k \in \mathbb{N}$. For a cusp form $f \in S_k(\Gamma_0(N))$ with Fourier series

$$f(\tau) = \sum_{n=1}^{\infty} c_n \cdot q^n,\ q := e^{2\pi i \cdot \tau},$$

one defines its *L-series*

$$L(f,-) : \{s \in \mathbb{C} :\ Re\ s > 1 + (k/2)\} \to \mathbb{C},\ L(f,s) := \sum_{n=1}^{\infty} \frac{c_n}{n^s}$$

Remark 7.4 (L-series of a cusp form).

1. The L-series $L(f,-)$ from Definition 7.3 is well-defined. One obtains $L(f,-)$ from the Mellin transform of f, see [33, Chap. VIII, §5].

2. The L-series $L(f,-)$ extends to a holomorphic function on $\mathbb{C}$ and satisfies the functional equation with respect to the reflection at k

$$\frac{1}{(2\pi)^s} \cdot \Gamma(s) \cdot L(f,s) = (-1)^{k/2} \cdot \frac{1}{(2\pi)^{k-s}} \cdot \Gamma(k-s) \cdot L(f,k-s)$$

   see [33, Chap. VIII, Theor. 8.1]

The textbook [17] does not prove Theorem 7.2. But it gives an excellent introduction to the problem and it highlights different views onto the theorem. In joint work with his coworkers, one of the authors of [17] proved in [10] the final step of the modularity theorem.

Theorem 7.5 (Versions of the modularity theorem).

1. Complex elliptic curve*: Each elliptic curve $E/\mathbb{C}$ with rational modular invariant*

$$j_E = \frac{1728 \cdot g_2^3}{g_2^3 - 27 \cdot g_3^2} \in \mathbb{Q}$$

is uniformized by a modular curve, i.e. there exists an integer $N \in \mathbb{N}$ and a surjective holomorphic map

$$X_0(N) \to E/\mathbb{C},$$

see [17, Theor. 2.5.1].

2. Rational elliptic curve*: Each elliptic curve $E/\mathbb{Q}$ is uniformized by a modular curve, i.e. there exists an integer $N \in \mathbb{N}$ and a surjective regular map over $\mathbb{Q}$*

$$X_0(N)_{\mathbb{Q}} \to E/\mathbb{Q},$$

see [17, Theor. 7.7.2].

3. Jacobi torus*: For each elliptic curve $E/\mathbb{C}$ with rational modular invariant*

$$j_E = \frac{1728 \cdot g_2^3}{g_2^3 - 27 \cdot g_3^2} \in \mathbb{Q}$$

exists an integer $N \in \mathbb{N}$ and a surjective holomorphic map

$$Jac(X_0(N)) \to E,$$

from the Jacobi torus of a modular curve $X_0(N)$, $N \in \mathbb{N}$, which is a group homomorphism, see [17, Theor. 6.1.3].

4. Cusp form, version with coefficients*: For each elliptic curve $E/\mathbb{Q}$ with conductor $N_E \in \mathbb{N}$ exists a new form*

$$f(q) = \sum_{n=1}^{\infty} a_n(f) \cdot q^n \in S_2(\Gamma_0(N_E))$$

satisfying for all primes $p \in \mathbb{N}$

$$a_p(f) = a_p(E),$$

see [17, Theor. 8.8.1].

Recall from Definition 4.40 for an elliptic curve $E/\mathbb{Q}$ with global minimal Weierstrass polynomial $F \in \mathbb{Z}[X,Y]$ the conductor

$$cond\ E = \prod_p p^{e_p} \in \mathbb{Z},$$

having the same prime factors p as the discriminant Δ_F and exponents $e_p \in \mathbb{N}^*$ deriving from the type of singularity of the reduction $E(\mathbb{F}_p)$.

5. Cusp form, version with L-series*: For each elliptic curve $E/\mathbb{Q}$ with conductor $N_E \in \mathbb{N}$ exists a new form*

$$f(q) = \sum_{n=1}^{\infty} a_n(f) \cdot q^n \in S_2(\Gamma_0(N_E))$$

with

$$L(f,-) = L(E,-),$$

see [17, Theor. 8.8.3]

Remark 7.6 (Forerunner of the Shimura-Taniyama-Weil Conjecture).

1. It is known that a non-constant holomorphic map

   $$X_0(N) \to E(\mathbb{C})$$

   as required in Conjecture 7.1 would be defined by two automorphic functions, see Definition 3.6,

   $$u, \mathrm{v} \in A_0(\Gamma_0(N))$$

   which satisfy a Weierstrass equation of $E/\mathbb{Q}$.

2. If the level N is minimal such that a non-constant holomorphic map

   $$X_0(N) \to E(\mathbb{C})$$

   exists, then the map is induced by a new form $f \in S_2^{new}(\Gamma_0(N))$.

3. If the new form $f \in S_2^{new}(\Gamma_0(N))$ from the previous step has integer-valued Fourier coefficients then

   $$L(f,-) = L(E,-)$$

   and N is the conductor of E.

4. The Fermat conjecture once stated that the Fermat equation

   $$X^n + Y^n = Z^n,\ n \in \mathbb{N},\ n \geq 3,$$

   has no non-trivial integer solutions.

   For the particular exponents $n = 3, 4$ the Fermat conjecture was proved by Euler. In addition it was known: The general case follows from the case of prime exponents $n = l \geq 5$. Before 1995 the conjecture was open for general primes $l \geq 5$.

   Assuming for an indirect proof of the Fermat conjecture the existence of a non-trivial solution

   $$(a,b,c) \in \mathbb{Z},\ gcd(a,b,c) = 1,$$

   of the Fermat equation with prime exponent $l \geq 5$ Frey proposed to study the elliptic curve $E_{FH}/\mathbb{Q}$ with Weierstrass equation

$$Y^2 = X \cdot (X - a^l) \cdot (X - c^l),$$

today named the *Frey-Hellegouarch* curve. The relation between non-trivial solutions of the Fermat equation and points on elliptic curves had already been considered by Hellegouarch, see [30]. The curve E_{FH} has discriminant

$$\Delta = 2^4 \cdot (abc)^{2l}$$

and modular j-invariant

$$j = \frac{c_4^3}{\Delta} \text{ with } c_4 = 2^4 \cdot (a^{2l} - (ac)^l + c^{2l})$$

The global minimal Weierstrass polynomial of E_{FH} has conductor

$$N = \prod_{p|abc} p$$

Serre and Ribet proved that the existence of E_{FH} would contradict the validity of the Shimura-Taniyama-Weil conjecture. Hence Wiles' modularity theorem, Theorem 7.2, implies that the Frey-Hellegouarche curve E_{FH} does not exist. Hence the Fermat conjecture is true.

A reference for all issues of this remark is [33, Chap. XII, § 1 and 4].

Example 7.7 (Modularity theorem). Figure 7.1 shows different elliptic curves $E/\mathbb{Q}$ defined by a minimal Weierstrass polynomial, their conductor N, and a sample of coefficients of their L-series and of the Fourier coefficients of the new-forms in

$$S_2(\Gamma_0(N)) = H^0(X_0(N), \Omega),$$

see Corollary 3.28. The numerical result from the PARI script `Elliptic_curve_taniyama_10` confirms the Modularity Theorem that a rational elliptic curves arises from a modular form.

```
Case 1: Global minimal model: Y^2 + (Y) = X^3 + (-X)
j(E) = 110592/37, minimal discr.: 37 = Mat([37, 1]), conductor: 37 = Mat([37, 1])
Genus X_0(37) = dim S_2(Gamma_0(37)): 2
L-series: q - 2*q^2 - 3*q^3 + 2*q^4 - 2*q^5 + 6*q^6 - q^7 + 6*q^9 + 4*q^10 - 5*q^11 - 6*q^12 - 2*q^13 + O(q^14)

Old forms: S^old_2(Gamma_0(37)) has dimension: 0
New forms: S^new_2(Gamma_0(37)) has dimension: 2
basis_1:  q + q^3 - 2*q^4 - q^7 - 2*q^9 + 3*q^11 - 2*q^12 - 4*q^13 + O(q^14)
basis_2:  q - 2*q^2 - 3*q^3 + 2*q^4 - 2*q^5 + 6*q^6 - q^7 + 6*q^9 + 4*q^10 - 5*q^11 - 6*q^12 - 2*q^13 + O(q^14)

-------------------------------------------
Case 2: Global minimal model: Y^2 + (YX) + (Y) = X^3 + (-X)
j(E) = -15625/28, minimal discr.: -28 = [-1, 1; 2, 2; 7, 1], conductor: 14 = [2, 1; 7, 1]
Genus X_0(14) = dim S_2(Gamma_0(14)): 1
L-series: q - q^2 - 2*q^3 + q^4 + 2*q^6 + q^7 - q^8 + q^9 - 2*q^12 - 4*q^13 + O(q^14)
Old forms: S^old_2(Gamma_0(14)) has dimension: 0
New forms: S^new_2(Gamma_0(14)) has dimension: 1
basis_1:  q - q^2 - 2*q^3 + q^4 + 2*q^6 + q^7 - q^8 + q^9 - 2*q^12 - 4*q^13 + O(q^14)
-------------------------------------------
Case 3: Global minimal model: Y^2 + (YX) + (Y) = X^3 + (-11*X) + (12)
j(E) = 128787625/98, minimal discr.: 98 = [2, 1; 7, 2], conductor: 14 = [2, 1; 7, 1]
Genus X_0(14) = dim S_2(Gamma_0(14)): 1
L-series: q - q^2 - 2*q^3 + q^4 + 2*q^6 + q^7 - q^8 + q^9 - 2*q^12 - 4*q^13 + O(q^14)
Old forms: S^old_2(Gamma_0(14)) has dimension: 0
New forms: S^new_2(Gamma_0(14)) has dimension: 1
basis_1:  q - q^2 - 2*q^3 + q^4 + 2*q^6 + q^7 - q^8 + q^9 - 2*q^12 - 4*q^13 + O(q^14)
```

Fig. 7.1 Relation between rational elliptic curves and new forms

7.2 Monstrous moonshine

What is "monstrous moonshine"? Monstrous moonshine is a synonym for the relation between modular forms on one side and finite simple groups on the other side.

That type of moonshine was detected in 1979, then formalized as a conjecture, proved by Borcherds in 1992, and finally honored by a Fields Medal awarded to him in 1998.

For an introduction see [8] and [59], on a more advanced level see [24] and [25].

Definition 7.8 (Simple group). A group G is *simple* if it has no normal, proper subgroup $H \subset G$, i.e. satisfying

$$H \neq \{e\} \text{ and } H \neq G$$

If a finite group G has a proper normal subgroup $H \subsetneq G$ then one will try to investigate G by studying the smaller groups H and G/H. Proposition 7.9 generalizes this construction. It formalizes in which sense simple groups are the building blocks of all finite groups.

Proposition 7.9 (Jordan-Hölder theorem). *Each finite group G has a finite, strictly increasing sequence of subgroups, a* composition series*,*

$$G_0 = \{e\} \subset G_1 \subset ... \subset G_n = G$$

such that for each $i = 1, ..., n$

$$G_{i-1} \subset G_i$$

is a normal subgroup with simple quotient group

$$Q_i := G_i / G_{i-1}$$

All composition series of G have the same lenght. Each two composition series of G have - up to permutation - the same simple quotients counted with multiplicity.

For a proof see [38, Chap. IV, §4].

Example 7.10 (Composition series). The cyclic groups C_{12} has the following different composition series

$$\{0\} \subset C_3 \subset C_6 \subset C_{12}$$

$$\{0\} \subset C_2 \subset C_6 \subset C_{12}$$

$$\{0\} \subset C_2 \subset C_4 \subset C_{12}$$

Each composition series of C_{12} has the same family of simple quotients (C_2, C_2, C_3) up to permutation.

Definition 7.11 (Group representation). Consider a group G.

1. A *group representation* is a pair (V, ρ) with a vector space V and group morphism

   $$\rho : G \to GL(V)$$

   to the group of linear automorphisms of V. As a shorthand one calls the vector space a *G-module* using the notation

   $$G \times V \to V,\ (g, \mathrm{v}) \mapsto g \cdot \mathrm{v} := \rho(g)(\mathrm{v}).$$

2. For a group representation

   $$\rho : G \to V$$

   with finite dimensional V the trace of linear endomorphisms defines a map

   $$trace\ \rho : G \to \mathbb{C},\ \chi_\rho(g) := trace\ \rho(g),$$

   which is named the *trace* of ρ

The representation $V^\natural$ for monstrous moonshine is infinite-dimensional. But it splits as the direct sum of finite-dimensional representations. For a finite-dimensional representation the trace of an element $g \in G$ only depends on the conjugacy class of g_0

$$[g_0] := \{g \cdot g_0 \cdot g^{-1} : \ g \in G\}$$

because invariance of the trace under cyclic permuation shows for $g_0,\ g \in G$

$$trace\ \rho(g \cdot g_0 \cdot g^{-1}) = trace(\rho(g) \cdot \rho(g_0) \cdot \rho(g)^{-1}) =$$

$$= (trace(\rho(g_0) \cdot \rho(g)^{-1} \cdot \rho(g)) = trace\ \rho(g_0)$$

Apparently the trace of the neutral element equals the dimension of the representation

$$trace\ \rho(e) = dim\ V \in \mathbb{N}.$$

Theorem 7.12 (Complete reducibility). *Consider a finite group G.*

1. Any G-module is completely reducible, i.e.

$$V = \bigoplus_{i \in I} V_i$$

with irreducible G-modules $V_i,\ i \in I$.

2. The irreducible G-modules correspond bijectively to the conjugacy classes of G.

Proof. See [51, §2, Theor. 7].

Remark 7.13 (Classification of finite simple groups).

1. Each finite simple group falls into exactly one of the following classes
   - a set of 18 infinite sequences of groups
   - a set of 26 groups, named the *sporadics*.
2. To the first class belongs the sequence $(A_n)_{n \geq 5}$ of the group of alternating permutations of n elements, the sequence $C(p)_{p\ \text{prime}}$ of cyclic groups with p elements, and a series of Lie type groups like $(PSL(n, \mathbb{F}_{p^k}))_n$.
3. The sporadics can be distinguished by their order. The next-to-biggest sporadic is Fischer's *baby monster* $\mathbb{B}$ with

$$ord\ \mathbb{B} = 2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47 \sim 4 \cdot 10^{33}$$

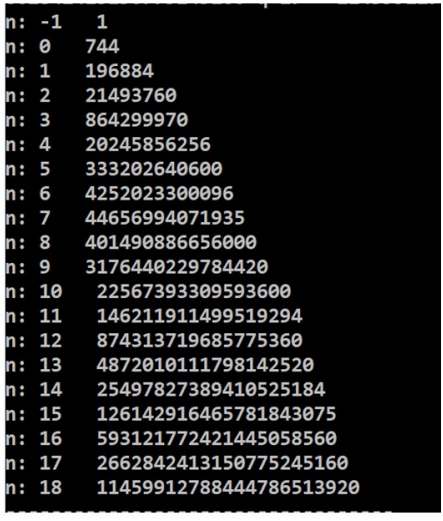
4. The largest sporadic is the *monster* $\mathbb{M}$ with

$$ord\ \mathbb{M} = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \sim 8 \cdot 10^{53}$$

The monster has 194 conjugacy classes and therefore exactly 194 irreducible representations.

Example 7.14 (Monstrous Moonshine). Figure 7.2 shows

- on the right-hand side for the monster $\mathbb{M}$ the dimensions $a(n)$ of the first irreducible, complex $\mathbb{M}$-modules V_n, $n \leq 18$, ordered by dimension,
- and on the left-hand side the Fourier coefficients $c(n)$ of the q-expansion of the modular j-invariant.



Coeff. of q-expansion of modular j-invariant

n	a (n)
1	1
2	196883
3	21296876
4	842609326
5	18538750076
6	19360062527
7	293553734298
8	3879214937598
9	36173193327999
10	125510727015275
11	190292345709543
12	222879856734249
13	1044868466775133
14	1109944460516150
15	2374124840062976
16	8980616927734375
17	8980616927734375
18	15178147608537368

Dimension of irred. represent. of monster M

Fig. 7.2 Monstrous Moonshine

What later was named "monstrous moonshine" started with the observations from Figure 7.2

$$1 = 1 \text{ and } 196.884 = 1 + 196.883$$

by McKay in 1978. The formula states

$$c(-1) = a(1) \text{ and } c(1) = a(1) + a(2)$$

relating two coefficients of the q-expansion of the modular j-invariant to the dimensions of the two lowest irreducible $\mathbb{M}$-modules. As Borcherds remarks "*moonshine* is not a poetic term referring to light from the moon. It means foolish or crazy idea (Quatsch in German)."

Definition 7.15 (Some generalizations of the modular theory).

1. *Moonshine group*: A discrete subgroup $G \subset SL(2,\mathbb{R})$ is a group *of moonshine type* if for a suitable level $N \in \mathbb{N}^*$

$$\Gamma_0(N) \subset G$$

and for a translation

$$\gamma = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in G \iff b \in \mathbb{Z},$$

i.e. G contains all integer-valued translations and no other translations.

2. *Hauptmodul*: The orbit space of the canonical action of a group G of moonshine type on the extended upper half plane $\mathbb{H}^*$

$$\phi : G \times \mathbb{H}^* \to \mathbb{H}^*$$

is a compact Riemann surface $X(G)$, the *modular curve* of G. For G with

$$genus\, X(G) = 0$$

the unique meromorphic function $J_G \in \mathscr{M}(X(G))$ with Fourier expansion normalized as

$$J_G(\tau) = \frac{1}{q} + \sum_{n=1}^{\infty} a_n \cdot q^n,\ q = e^{2\pi i \cdot \tau},$$

is the *Hauptmodul* of G.

Moonshine groups $G \subset SL(2,\mathbb{R})$ are *congruent* to the modular group Γ in the following sense: The intersection

$$H := G \cap \Gamma$$

satisfies the equality of indices

$$[G : H] = [\Gamma : H].$$

In particular, the index is finite because

$$[\Gamma : H] \leq [\Gamma : \Gamma_0(N)] < \infty.$$

For a moonshine group G of *genus* $X(G) = 0$ the modular curve $X(G)$ is $\mathbb{P}^1$, and J_G is a distinguished generator of the field of meromorphic functions

$$\mathscr{M}(X(G)) = \mathbb{C}(J_G).$$

Example 7.16 (Hauptmodul).

- The Hauptmodul of the modular group Γ is the normalized modular j-invariant

$$J_\Gamma(q) = j(q) - 744 = \frac{1}{q} + 196'884 \cdot q + 21'493'760 \cdot q^2 + 864'299'970 \cdot q^3 + O(4)$$

- The Hecke congruence subgroup $\Gamma_0(2)$ has the Hauptmodul

$$J_{\Gamma_0(2)} = \frac{1}{q} + 276 \cdot q - 2'048 \cdot q^2 + 11'202 \cdot q^3 + O(4)$$

- The normalizer of $\Gamma_0(2)$ in $SL(2,\mathbb{R})$, the moonshine group

$$\Gamma_0(2)+ \subset SL(2,\mathbb{R})$$

  has the Hauptmodul

$$J_{\Gamma_0(2)+} = \frac{1}{q} + 4'372 \cdot q + 96'256 \cdot q^2 + O(3)$$

Remark 7.17 (Forerunner of the Monstrous Moonshine Theorem).

1. *McKay-Thompson conjecture*: McKay and Thompson conjectured the existence of a graded, infinite-dimensional $\mathbb{M}$-module

$$V^\natural = \bigoplus_{n\in\mathbb{N}} V_n^\natural$$

   satisfying: The graded components $V_n^\natural$ split as the direct sum of irreducible $\mathbb{M}$-modules with a certain multiplicity. The $\mathbb{M}$-module $V^\natural$ is characterized by the family of series, later named *McKay-Thompson series*

$$T_{[g]}(\tau) = \sum_{n\in\mathbb{N}} trace(g|V_n^\natural) \cdot q^n,\ g \in \mathbb{M},$$

   see [60].

2. *Conway-Norton conjecture*: Each McKay-Thompson series $T_{[g]}$ is the Hauptmodul of a moonshine group $\Gamma_{[g]}$ with modular curve of genus $= 0$.

Thompson decoded the data from Figure 7.2 as follows:

$$c(2) = 21'493'760 = a(1) + a(2) + a(3)$$

and subsequently

$$c(3) = 2 \cdot a(1) + 2 \cdot a(2) + a(3) + a(4)$$

$$c(4) = 3 \cdot a(1) + 3 \cdot a(2) + a(3) + 2 \cdot a(4) + a(5)$$

$$c(5) = 4 \cdot a(1) + 5 \cdot a(2) + 3 \cdot a(3) + 2 \cdot a(4) + a(5) + a(6) + a(7)$$

If the irreducible representations $\rho_i,\ i \in \mathbb{N}$, of $\mathbb{M}$ are ordered acccording to increasing dimension then the first summands of the representation from Remark 7.17 are

$$(V_0, \rho_1),\ (V_1 = \{0\}),\ (V_2, \rho_1 \oplus \rho_{196'883}),\ (V_3, \rho_1 \oplus \rho_{196'883} \oplus \rho_{21'296'876})$$

The series generated by the dimensions $(dim\, V_n)_{n\in\mathbb{N}}$ has the Fourier expansion

$$\sum_{n=-1}^{\infty} (dim\, V_{n+1}) \cdot q^n =$$

$$= J(\tau) = \frac{1}{q} + 196'884 \cdot q + 21'493'760 \cdot q^2 + 21'493'760 \cdot q^3 + O(4),\ q = e^{2\pi i \cdot \tau}.$$

The open problem was to find explicitly a representation with the properties from the Conway-Norton conjecture, see Remark 7.17. Borcherds proved in 1992 Theorem 7.18, see [6].

Theorem 7.18 (Monstrous Moonshine). *The monster group $\mathbb{M}$ has a representation as automorphism group of the monster vertex algebra $V^\natural$. The representation satisfies the properties of the Conway-Norton conjecture.*

List of results and some outlooks

Part I. General Theory

Chapter 1. Elliptic functions

Focus: Analysis

Holomorphic elliptic functions are constant (Prop. 1.7)

Sum of residues vanishes for elliptic functions (Prop. 1.8)

Elliptic functions attain each value with equal multiplicity (Cor. 1.10)

Weierstrass function $\wp$ of a lattice (Theor. 1.12)

Differential equation of $\wp$ (Theor. 1.17)

Field of elliptic functions equals $\mathbb{C}(\wp)[\wp']$ (Theor. 1.18)

Elliptic functions with prescribed zeros and poles (Theor. 1.21)

Chapter 2. The modular group Γ and its Hecke congruence subgroups $\Gamma_0(N)$

Focus: Analysis, Topology

Holomorphic maps between complex tori (Prop. 2.3)

Moduli space of complex tori (Theor. 2.5)

Group action (Def. 2.6)

Modular group and Hecke congruence subgroups (Def. 2.9)

Fundamental domain of the Γ-action (Theor. 2.16)

Proper discontinuity of the Γ-action (Lem. 2.19)

Hausdorff topologyy of the orbit space of the Γ-action (Theor. 2.21, Cor. 2.25)

Analytic structure of the orbit space of the Γ-action (Prop. 2.27)

The modular curve as compact Riemann surface (Theor. 2.28)

The modular curves of the Hecke congruence subgroups (Rem. 2.30)

Chapter 3. The algebra of modular forms

Focus: Analysis

Γ-invariant differential forms (Prop. 3.1)

Modular forms and cusp forms (Def. 3.6)

Eisenstein series (Theor. 3.9)

Discriminant form Δ (Def. 3.13)

Modular invariant j (Def. 3.15)

Modular curve and modular invariant j (Cor. 3.16)

Modular forms as meromorphic diff. forms on the modular curve (Theor. 3.17)

The field $\mathbb{C}(j)$ of automorphic functions (Cor. 3.22)

The algebra of modular forms and the ideal of cusp forms (Theor. 3.24)

The line bundle of modular forms (Theor. 3.26)

The codimension of cusp forms (Cor. 3.28)

Chapter 4. Elliptic curves

Focus: Analysis, algebraic geometry, arithmetic geometry

Embedding tori (Theor. 4.3, Rem. 4.14)

Globally generated line bundle (Def. 4.7)

Very-ampleness criterion (Theor. 4.13)

Elliptic curve over k (Def. 4.20)

Elliptic curves are plane cubics (Theor. 4.23)

Weierstrass polynomial (Def. 4.24)

Elliptic curves over $\mathbb{C}$ are tori (Theor. 4.28)

The group of classes of degree zero divisors of an elliptic curve (Theor. 4.31)

Abel's theorem for elliptic curves (Theor. 4.33)

Reduction of an elliptic curve $E/\mathbb{Q}$ mod p (Def. 4.40)

The ζ-function of an elliptic curve $E/\mathbb{F}_p$ (Def. 4.44)

The L-series of an elliptic curve $E/\mathbb{Q}$ (Def. 4.46)

Chapter 5. Introduction to Hecke theory and applications

Focus: Analysis, number theory

Hecke operators of the modular group (Def. 5.10)

Fourier coefficients of Hecke transforms (Theor. 5.11)

The discriminant Δ as simultaneous eigenform (Cor. 5.13)

Commutativity of the Hecke algebra (Theor. 5.18)

Petersson scalar product (Theor. 5.23)

Self-adjointness of the Hecke operators of the modular group (Theor. 5.25)

Eigenforms of the Hecke algebra of the modular group (Theor. 5.26)

Oldforms and newforms (Def. 5.29)

Properties of the Ramanujan τ-function (Prop. 5.32)

The modular forms $G_2N \in M_2(\Gamma_0(N))$ (Theor. 5.37)

The 4-squares theorem (Theor. 5.38)

Chapter 6. Application to imaginary quadratic fields

Focus: Analysis, algebraic number theory

Complex multiplication (Def. 6.5)

Complex multiplication and imaginary quadratic fields (Theor. 6.6)

Modular polynomials of a given level (Def. 6.8)

Coefficients of the modular polynomials from $\mathbb{Z}[j]$ (Theor. 6.10)

For *CM*-points $\tau \in \mathbb{H}$ the singular values $j(\tau) \in \mathbb{C}$ are algebraic integers (Theor. 6.14)

The ideal class group and tori with complex multiplication (Prop. 6.20)

The class number formula and the modular j-invariant (Theor. 6.22)

Chapter 7. Modular elliptic curves, monstrous moonshine

Focus: Analysis, algebraic geometry, group theory

Rational elliptic curves are modular (Theor. 7.2)

The Monstrous Moonshine theorem (Theor. 7.18)

References

References for these notes are grouped as

- Modular Forms: [9], [11] [15] [16] [19] [34] [36] [39] [42] [43] [44] [45] [50] [52] [53] [65]
- Complex Analysis: [1] [5] [21] [27]
- Algebraic Geometry: [23] [29] [49] [54] [56]
- Number Theory: [13] [22] [26] [32] [40] [47]
- Online plattform: [57] (textbook level), [41] (research level)

The basic textbook is [17], for an elementary survey see [2].

1. Ahlfors, Lars: Complex Analysis. 2nd edition, McGraw-Hill, Tokyo (1966)
2. Alfes-Neumann, Claudia: Modulformen. Fundamentale Werkzeuge der Mathematik. Springer, Wiesbaden (2020)
3. Alperin, Roger C.: $PSL_2(\mathbb{Z}) = \mathbb{Z}_2 * \mathbb{Z}_3$. The American Mathematical Monthly. Vol. 100 (1993), 385-386
4. Atiyah, M. F.; Macdonald, I. G.: Introduction to Commutative Algebra. Addison Wesley (1969)
5. Ben-Zvi, David, D.: Moduli Spaces. https://www.ma.utexas.edu/users/benzvi/math/pcm0178.pdf
6. Borcherds, Richard E.: Monstrous Moonshine and Monstrous Lie Superalgebras. Invent. Math. 109, (1992), p. 405-444
7. Borcherds, Richard E.: Proceedings of the I.C.M., Vol. I (Berlin, 1998). Doc. Math. 1998, Extra Vol. I, 607-615, `http://math.berkeley.edu/~reb/papers/icm98/icm98.pdf` Call 8.7.2020
8. Borcherds, Richard E.: What is ... The Monster? Notices of the AMS, 49,7 (2002), p. 1076-1077
9. Borel, A.; Chowla, S.; Herz, C.; Iwasawa, K.; Serre, J-P.: Seminar on Complex Multiplication. Lecture Notes in Mathematics 21. Springer, Berlin (1966)
10. Breuil, Christophe; Conrad, Brian; Diamond, Fred; Taylor, Richard: On the Modularity of Elliptic Curves over $\mathbb{Q}$: Wild 3-adic exercises. Journal of the American Mathematical Society. 14(4), p. 843-939 (2001)

11. Chenevier, Gaëtan: Introduction aux Formes Modulaires. Internet (2015)
12. Cheng, Miranda: Moonshine-I. https://www.youtube.com/watch?v=HB5dCXQIWqM Call 8.7.2020
13. Cohen, Henri: A Course in Computational Algebraic Number Theory. Springer, Berlin (1993)
14. Conway, J.H.; Norton, S.P.: Monstrous Moonshine. Bull. London. Math. Scoc 11, (1979), 308-339
15. Cornell, Gary; Silvermann, Joseph H.; Stevens, Glenn (Eds.): Modular Forms and Fermat's Last Theorem. Springer, New York (1997)
16. Darmon, Henri: A proof of the full Shimura-Taniyama-Weil conjecture is announced. Notices Americ. Math. Soc. 46,11 (1999), p. 1397-1401
17. Diamond, Fred; Shurman, Jerry: A First Course in Modular Forms. Springer, New York (2005)
18. Dugundji, James: Topology. Allyn and Bacon, Boston (1966)
19. Eichler, Martin; Zagier, Don: On the Zeros of the Weierstrass $\wp$-Function. Mathematische Annalen 258, (1982), p. 399-407
20. Fischer, Wolfgang; Lieb, Ingo: Funktionentheorie. Vieweg, Braunschweig (1980)
21. Forster, Otto: Riemannsche Flächen. Springer, Berlin (1977)
22. Forster, Otto: Algorithmische Zahlentheorie. 2. Auflage Springer Spektrum (2015)
23. Fulton, William: Algebraic Curves. An Introduction to Algebraic Geometry. The Benjamin/Cummings Publishing Company (1969)
24. Gannon, Terry: Monstrous Moonshine: The first twenty-five years. Bull. London Math. Soc. 38, p. 1-33 (2006)
25. Gannon, Terry: Moonshine beyond the Monster. The bridge connecting Algebra, Modular Forms and Physics, Cambridge University Press, Cambridge (2006)
26. Gross, Benedict: The arithmetic of elliptic curves - An update. Arabian Journal of Science and Engineering 1 (2009), p. 95-103 http://www.math.harvard.edu/~gross/preprints/ell2.pdf
27. Gunning, Robert C.: Lectures on Riemann Surfaces. Princeton University Press (1966)
28. Han, Juncheol: The general linear group over a ring. Bull. Korean Math. Soc. 43 (2006), No. 3, pp. 619-626
29. Hartshorne, Robin: Algebraic Geometry. Springer, New York (1977)
30. Y. Hellegouarch: Points d'order $2p^h$ sur les courbes elliptiques. Acta Arithmetica 26 (1972), 253-263
31. Huybrechts, Daniel: The geometry of cubic hypersurfaces. (2020) http://www.math.uni-bonn.de/people/huybrech/Notes.pdf Call 15.9.2020
32. Ireland, Kenneth; Rosen, Michael: A Classical Introduction to Modern Number Theory. Springer, New York (1982)
33. Knapp, Anthony: Elliptic Curves. Princeton University Press. Princeton (1992)
34. Kilford, Lloyd James: Modular forms: a classical and computational introduction. Imperial College Press, 2nd ed. (2015)
35. Koblitz, Neal: Introduction to Elliptic Curves and Modular Forms. Springer, New York, 2nd ed. (1993)
36. Koecher, Max; Krieg, Aloys: Elliptische Funktionen und Modulformen. 2. Aufl. Springer, Berlin (2007)
37. Lang, Serge: Algebra. Addison-Wesley, Reading, 7th ed. (1977)
38. Lang, Serge: Elliptic Functions. 2nd edition Springer, Berlin (1987)
39. Lang, Serge: Introduction to Modular Forms. Springer, Berlin (1995)
40. Marcus, Daniel A.: Number Fields. Springer, New York (1977)
41. mathoverflow. https://mathoverflow.net/
42. Mordell, Louis Joel: On Mr. Ramanujan's empirical expansion of modular functions. Proc. Cambridge Philosophical Society, 19 (1917), p. 117-124
43. Ono, Ken: The last words of a genius. Notices Americ. Math. Soc. 57, 11 (2010), p.1410-1419
44. Pantchichkine, Alexeï: Formes Modulaire et Courbes Elliptiques. https://www-fourier.ujf-grenoble.fr/ panchish/06ensl.pdf

45. Ramanujan, Srinivasa: On certain arithmetical functions. Trans. Cambridge Philosophical Society. 22(9) (1916), p. 159-184
46. Raynaud, Michèle: Géometrie Algébrique et Géometrie Analytique. Séminaire de Géometrie Algébrique du Bois Marie 1960-61, Exposé XII. https://arxiv.org/pdf/math/0206203.pdf Call June 2020
47. Scharlau, Winfried; Opolka Hans: Von Fermat bis Minkowski. Eine Vorlesung über Zahlentheorie. Springer, Berlin (1980)
48. Schultz, Dan: Notes on Modular Forms. https://faculty.math.illinois.edu/\%7eschult25/ModFormNotes.pdf Call 27.10.2020
49. Serre, Jean-Pierre: Géométrie Algébrique et Géométrie Analytique. Annales de l'Institut Fourier. IV (1955-56), p. 1-42
50. Serre, Jean-Pierre: II Modular Forms. (1957/58). In: [9].
51. Serre, Jean-Pierre: Représentations linéaires des groupes finis. Herman, Paris (1967)
52. Serre, Jean-Pierre: A Course in Arithmetic. Springer, New York (1973)
53. Shimura, Goto: Introduction to the Arithmetic Theory of Automorphic Functions. Iwanami Shoten and Princeton University Press, o.O. (1971)
54. Silverman, Joseph: The Arithmetic of Elliptic Curves. Springer, New York (1986)
55. Silverman, Joseph: Advanced Topics in the Arithmetic of Elliptic Curves. Springer, New York (1994)
56. Silverman, Joseph; Tate, John: Rational points on Elliptic Curves. Springer, New York (1992)
57. stackexchange. https://math.stackexchange.com/
58. Szpiro, Lucien: Séminaire sur les pinceaux arithmétiques: La conjecture de Mordell. Astérisque 127. Société Mathématiques de France, Paris (1985)
59. Tatitscheff, Valdo: A short introduction to Monstrous Moonshine. Preprint (2019) https://www.researchgate.net/publication/331008545_A_short_introduction_to_Monstrous_Moonshine
60. Thompson, J. G.: Some Numerology between the Fischer-Griess monster and the Elliptic Modular Function. Bull. Lond. Math. Soc. 11 (1979), 352-353
61. van der Geer, Gerard: Siegel Modular Forms. arXiv:math/0605346 [math.AG]
62. Wehler, Joachim: Complex Analysis. Lecture Notes (2019) http://www.mathematik.uni-muenchen.de/\%7ewehler/20181218_Funktionentheorie_Script.pdf
63. Wehler, Joachim: Riemann Surfaces. Lecture Notes (2020) http://www.mathematik.uni-muenchen.de/\%7ewehler/20190530_RiemannSurfacesScript.pdf
64. Zagier, Don: Zetafunktionen und quadratische Körper. Eine Einführung in die höhere Zahlentheorie. Springer, Berlin (1981)
65. Zagier, Don: https://www.youtube.com/watch?v=zKt5L0ggZ3o (2015)
66. Zagier, Don: Elliptic Modular Forms and Their Applications. https://people.mpim-bonn.mpg.de/zagier/files/doi/10.1007/978-3-540-74119-0_1/fulltext.pdf Call 16.7.2020

Index