Joachim Wehler

Modular Forms
and Elliptic Curves

DRAFT, Release 1.43

February 21, 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.

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

I thank all participants who pointed out some errors and proposed improvements. Please report to wehler@math.lmu.de any further errors or typos, adding the version of the lecture notes.

Release notes:

- **Release 1.43**: Chapter 5. Theorem 5.23 proof corrected.
- **Release 1.42**: Chapter 5. Theorem 5.23 corrected. Chapter 6 minor revisions.
- **Release 1.41**: Chapter 7. Section 7.2 added. Chapter 5. Theorem 5.21 expanded. Theorem 5.23 expanded and corollary integrated.
- **Release 1.40**: Chapter 7. Section 7.1 added.
- **Release 1.37**: Chapter 5. Section 5.2, Lemma 5.22 replaced by new version, subsequent Corollary added, Theorem 5.23 adapted, renumbering, Section 5.3 added.
- **Release 1.36**: Chapter 5. Section 5.2, Proposition 5.26 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 4.38 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 4.26 added, renumbering, minor revision. Section 4.3 added.
- **Release 1.30**: Chapter 4. Section 4.2, Example 4.35 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 ................................................................................. 1

PARI files .................................................................................. 3

Part I  General Theory

1  Elliptic functions ................................................................. 9
   1.1  The field of elliptic functions ........................................ 9
   1.2  The Weierstrass $\wp$-function .................................. 14
   1.3  Abel’s theorem ..................................................... 24

2  The modular group $\Gamma$ and its Hecke congruence subgroups $\Gamma_0(N)$ .................................. 31
   2.1  The moduli space of complex tori and group actions ..... 31
   2.2  Topology of the orbit space of the $\Gamma$-action .......... 46
   2.3  Modular curves $X(\Gamma_0(N))$ as compact Riemann surfaces .... 62

3  The algebra of modular forms .............................................. 79
   3.1  Modular forms and cusp forms .................................. 79
   3.2  Eisenstein series and the algebra of modular forms of $\Gamma$ .... 88
   3.3  Generalization to Hecke congruence subgroups $\Gamma_0(N)$ ...... 114

4  Elliptic curves ........................................................................ 123
   4.1  Embedding tori as plane cubic hypersurfaces ............. 123
   4.2  Elliptic curves over subfields of $\mathbb{C}$ ......................... 137
   4.3  Elliptic curves over finite fields .................................. 166

5  Introduction to Hecke theory and applications .................. 179
   5.1  Hecke operators of the modular group and their eigenforms .... 179
   5.2  The Petersson scalar product ................................... 196
   5.3  Numerology: Lagrange, Jacobi, Ramanujan, Mordell ........ 211

Part II  Advanced Theory
## Contents

6 Application to imaginary quadratic fields ............................................. 223  
  6.1 Imaginary quadratic fields and tori with complex multiplication ...... 223  
  6.2 Modular polynomials ................................................................. 230  
  6.3 Fractional ideals and the class number formula ......................... 243

7 Outlook: Modular elliptic curves, monstrous moonshine ................. 251  
  7.1 Modular elliptic curves ............................................................. 251  
  7.2 Monstrous moonshine ............................................................... 258

List of results and some outlooks ......................................................... 265

References ...................................................................................... 269

Index .............................................................................................. 273
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 unreveals 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

\[
\Gamma_0(N) \backslash \mathbb{H}
\]
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 unveil 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 are complex elliptic curves. They can be represented as non-singular cubic curves in the projective plane, defined as zero set of a Weierstrass polynomial, and vice versa. The main tool to represent a complex torus as an elliptic curve is the Weierstrass \( \wp \)-function and its differential equation. Choosing different fields for the coefficients 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. 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. And also a look at 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:

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_Hasse_estimate_05: Hasse estimate for number of $\mathbb{F}_p$-rational points, cf. Remark 4.41.
Chapter 5
- Congruence_subgroup_20: Oldforms and newforms for different $\Gamma_0(N)$, cf. Example 5.28.
- Modular_forms_theta_01: 4-square theorem and similar decompositions, cf. Example 5.37.

Chapter 6
- modular_polynomial_01: Modular polynomials of different levels, cf. Example 6.10.
- modular_polynomial_02: The polynomials $\Phi_m$ and their factorization, cf. Example 6.12.

Chapter 7
- Elliptic_curve_taniyama_10: Illustration of Wiles’ theorem by some numerical examples, cf. Example 7.9.
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 \( \text{SL}(2, \mathbb{Z}) \) 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 \( \mathbb{F}_p \) of \( \mathbb{Z} \). The Weierstrass \( \wp \)-function and its derivative \( \wp' \) from Chapter 1 embed 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 \( E(\mathbb{Q}) \) exists, then \( E \) is a rational elliptic curve. 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 \( (\text{card } E_p)_{p \text{ prime}} \) 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 \( \Gamma := \text{SL}(2, \mathbb{Z}) \) 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 \( \infty \). Due to their symmetry modular forms correspond bijectively to meromorphic sections of the line bundle \( \Omega^1 \) 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 \( M_{\ast}(\Gamma) = \bigoplus_k M_k(\Gamma) \). The grading is given by the weight of the modular forms. The algebra of modular forms \( M_{\ast}(\Gamma) \) contains the ideal of cusp forms \( S_{\ast}(\Gamma) = \bigoplus_k S_k(\Gamma) \). On \( M_{\ast}(\Gamma) \) acts the family of Hecke operators as an Abelian algebra of endomorphisms. The ideal \( S_{\ast}(\Gamma) \) 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 \( 2\pi \) and \( \pi \). 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

\[
\begin{align*}
f : G \setminus S &\to \mathbb{C}
\end{align*}
\]

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 \( z \in G \setminus P \)

\[
f(z + \omega) = f(z).
\]
Elliptic functions

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 \( z_0 \)

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

with coefficients

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

If \( f \) has the period \( \omega \) 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 \( \Gamma \) 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 \( \Gamma_f \) of all periods of \( f \) is a discrete subgroup of \( \mathbb{C} \). It is named the period group of \( f \).

Proof. i) Apparently \( \Gamma_f \) is a subgroup.

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

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 \( \Gamma \) 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 \((\omega_1, \omega_2)\) 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 \( \Gamma_f \).

- If \( \text{rank } \Gamma_f \geq 1 \) then \( f \) is named periodic.
• If \( \text{rank } \Gamma_f = 2 \) then \( f \) is named \textit{doubly periodic}. Its period group

\[
\Gamma_f = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2
\]

is also named the \textit{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 \textit{fundamental period parallelogram} of \( f \) with respect to the basis \((\omega_1, \omega_2)\).

A doubly periodic meromorphic function on \( \mathbb{C} \) is an \textit{elliptic function} with respect to a lattice \( \Lambda \) if

\[
\Lambda \subset \Gamma_f
\]

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

![Fig. 1.1 Period lattice \( \Lambda \)](image)

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

\[
\sum_{\zeta \in P} \text{res}_\zeta(f) = 0.
\]

**Proof.** The boundary \( \partial P \) 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

\[
\frac{1}{2\pi i} \int_{\partial P_a} f(z) \, dz = \sum_{\zeta \in P_a} \text{res}_\zeta(f) = \sum_{\zeta \in P} \text{res}_\zeta(f).
\]

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 \( \Gamma_f \) and no other pole mod \( \Gamma_f \).

2. There are no elliptic functions \( f \) with only one zero of order 1 modulo the period lattice \( \Gamma_f \) and no other zero mod \( \Gamma_f \).

**Proof.** 1. A pole of order 1 at \( a \in \mathbb{C} \) has \( \text{res}_a(f) \neq 0 \), 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 $\Lambda$ 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

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

Each residue evaluates to

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

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 $\Lambda$.

The $\wp$-function of $\Lambda$ is a distinguished elliptic function: All elliptic functions of the given lattice $\Lambda$ 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 $\Lambda$. 

1.2 The Weierstrass \( \wp \)-function

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

\[ \Lambda_n := \{ \mu \cdot \omega_1 + v \cdot \omega_2 \in \Lambda : |\mu|, |v| \leq n \text{ and } (|\mu| = n \text{ or } |v| = n) \}, \]

i.e.

\[ \Lambda = \bigcup_{n \in \mathbb{N}} \Lambda_n. \]

Then

\[ \text{card } \Lambda_n = 8n. \]

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

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

For \( k > 2 \)

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

Therefore the claim follows from

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

We will study elliptic functions with period lattice \( \Lambda \). According to Corollary 1.9 a candidate \( f \) for the most simple example would have only one pole mod \( \Lambda \), 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 \( \Lambda \) 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 \( \Lambda \), named the Weierstrass \( \wp \)-function of \( \Lambda \). The pole set of \( \wp \) is \( \Lambda \), 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 \( f_\nu \) has no pole in \( K \)
- the sequence \( (f_\nu)_{\nu > \nu_0} \) is uniformly convergent on \( K \).

i) **Meromorphic with pole set \( \Lambda \):** 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
\[
|z| \leq R \text{ and } 2R \leq |\omega|
\]
holds
\[
\frac{|\omega|}{2} - |z| \geq 0.
\]
The triangle inequality
\[
|z - \omega| = |\omega - z| \geq |||\omega| - |z|| = \left| \frac{|\omega|}{2} - |z| + \frac{|\omega|}{2} \right| \geq \frac{|\omega|}{2}
\]
implies the estimate
\[
\left| \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right| = \frac{\omega^2 - (z - \omega)^2}{\omega^2 \cdot (z - \omega)^2} \leq \frac{|-z^2 + 2z| |\omega|}{|\omega|^2 \cdot \left( \frac{|\omega|}{2} \right)^2} \leq 4 \cdot \frac{|z|^2 + 2 \cdot |z| \cdot |\omega|}{|\omega|^4}
\]
\[
\leq 4 \cdot \frac{|z|^2}{|\omega|^4} + 8 \cdot \frac{|z|}{|\omega|^3} \leq \frac{4 \cdot R^2}{2 \cdot R \cdot |\omega|^3} + 8 \cdot \frac{R}{|\omega|^3} = 10 \cdot \frac{R}{|\omega|^3}
\]
independent from \( |z| < R \).
1.2 The Weierstrass $\wp$-function

According to Lemma 1.11 the series

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

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

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

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 $\Lambda$.

ii) Even function with periods from $\Lambda$:

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

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

- $\wp$ has periods from $\Lambda$: 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 $\omega$ 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

\[
c_j = 0, \text{ q.e.d.}
\]

**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 \((\omega_1, \omega_2)\). The derivative \( \wp' \) of the Weierstrass function \( \wp \) of \( \Lambda \) has mod \( \Lambda \)

- 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 \( \Lambda \).

Moreover \( \wp' \) like \( \wp \) has a single pole at 0 \( \in \mathbb{C} \) mod \( \Lambda \). The pole of \( \wp' \) has order = 3. Corollary 1.10 implies that \( \wp' \) has exactly three zeros mod \( \Lambda \). 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 \( \Lambda \) 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 \( \Lambda \).
1.2 The Weierstrass $\wp$-function

- 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 $\Lambda$.

---

**Theorem 1.12** shows that the $\wp$-function of the lattice $\Lambda$ has all points from $\Lambda$ 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 $\Lambda$ and its derivative $\wp'$ have the period lattice $\Lambda$, i.e.

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

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

**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 \( \omega \in A \), q.e.d.

**Proposition 1.16 (Coefficients of the Laurent expansion of \( \wp \)).** The Weierstrass function \( \wp \) of \( \Lambda \) 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 \( \Lambda \)
\[ a_{2k} = (2k + 1) \cdot G_{\Lambda,2k+2}. \]

**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
\[ \frac{-1}{z - \omega} = \frac{1}{\omega - z} = \frac{1/\omega}{1 - (z/\omega)} = (1/\omega) \cdot \sum_{v=0}^{\infty} (1/\omega)^v \cdot z^v \]
shows
\[ \frac{1}{(z - \omega)^2} = (1/\omega) \cdot \sum_{v=1}^{\infty} v \cdot (1/\omega)^v \cdot z^{v-1} = \sum_{v=0}^{\infty} (v + 1) \cdot \frac{1}{\omega^{v+2}} \cdot z^v \]
and
\[ \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} = \sum_{v=1}^{\infty} (v + 1) \frac{1}{\omega^{v+2}} \cdot z^v. \]
Because \( \wp \) is even and the series converges absolutely, see Theorem 1.12, we obtain after rearrangement and using that \( \wp \) is even
\[
\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda'} \left( \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right) = \frac{1}{z^2} + \sum_{v=1}^{\infty} \left( \sum_{\omega \in \Lambda} \frac{1}{\omega^{v+2}} \right) z^v = \\
= \frac{1}{z^2} + \sum_{k=1}^{\infty} \frac{2k+1}{\omega_k} \left( \sum_{\omega \in \Lambda'} \frac{1}{\omega^{2k+2}} \right) z^{2k}, \text{ q.e.d.}
\]

**Theorem 1.17 (Differential equation of \( \wp \)).** The Weierstrass function \( \wp \) of the lattice \( \Lambda \) satisfies the differential equation
\[
\wp' \wp' = 4 \cdot \wp^3 - g_2 \cdot \wp - g_3
\]
with the constants
\[
g_2 := g_{\Lambda,2} := 60 \cdot G_{\Lambda,4}, \quad g_3 := g_{\Lambda,3} := 140 \cdot G_{\Lambda,6}
\]
derived from the lattice constants.

**Proof.** To simplify the notation we omit the index \( \Lambda \) from the lattice constants \( G_{\Lambda,k} \).
Due to Proposition 1.16 the Laurent expansions start
\[
\wp(z) = \frac{1}{z^2} + \sum_{k \geq 1} (2k+1) \cdot G_{2k+2} \cdot z^{2k} = \frac{1}{z^2} + 3 \cdot G_4 \cdot z^2 + 5 \cdot G_6 \cdot z^4 + O(6)
\]
\[
\wp'(z) = -\frac{2}{z^3} + 6 \cdot G_4 \cdot z + 20 \cdot G_6 \cdot z^3 + O(5)
\]
\[
\wp'(z)^2 = \frac{4}{z^6} - \frac{24 \cdot G_4}{z^2} - 80 \cdot G_6 + O(2)
\]
\[
\wp(z)^2 = \frac{1}{z^2} + 6 \cdot G_4 + 10 \cdot G_6 \cdot z^2 + O(4)
\]
\[
\wp(z)^3 = \frac{1}{z^6} + 6 \cdot G_4 + 10 \cdot G_6 + \frac{3 \cdot G_4}{z^2} + 5 \cdot G_6 + O(2) = \frac{1}{z^6} + \frac{9 \cdot G_4}{z^2} + 15 \cdot G_6 + O(2)
\]
Therefore all summands of order \( < 1 \) of the sum
\[
\wp' \wp' - 4 \cdot \wp^3 - g_2 \cdot \wp - g_3
\]
cancel and
\[
\wp' \wp' - 4 \cdot \wp^3 + g_2 \cdot \wp + g_3 = O(2).
\]
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 \( \mathcal{M}(\Lambda) \) of elliptic functions with respect to the lattice \( \Lambda \) is a field extension of \( \mathbb{C} \) of transcendence degree 1, more precisely

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

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

\[
g_2 := 60 \cdot G_{A,4}, \ g_3 := 140 \cdot G_{A,6}.
\]

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 \( \geq 2 \).

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

- We first consider the case that \( f \) has pole set \( \Lambda \).

The unique pole of \( f \mod \Lambda \) 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 \( \mod \Lambda \) 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

\[
f - c \cdot \wp^{m-1} \cdot \wp'
\]
1.2 The Weierstrass $\wp$-function

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 $\Lambda$ only finitely many poles $z_v \in P \setminus \Lambda$, $v = 1, \ldots, n$. The function $\wp$ is holomorphic in $P \setminus \Lambda$. Hence for suitable constants $k_1, \ldots, k_n \in \mathbb{N}$ the function

$$f(z) \cdot \prod_{v=1}^{n} (\wp(z) - \wp(z_v))^{k_v}$$

has poles at most in $\Lambda$. According to the first part

$$f(z) \cdot \prod_{v=1}^{n} (\wp(z) - \wp(z_v))^{k_v} \in \mathbb{C}(\wp, \wp').$$

Therefore

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

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

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

the cubic polynomial

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

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

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

As a consequence, the discriminant

$$\text{discr}(G_\Lambda) = \frac{1}{24} \cdot (g_2^3 - 27 \cdot g_3^2) \in \mathbb{C}$$

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
\[ \wp(\omega) = \wp(\omega') \] 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 \( \Lambda \) each value with multiplicity = 2. Hence
\[ \wp(\omega) \neq \wp(\omega'). \]

2. Discriminant: One checks the discriminant formula
\[ \text{discr}(G_\Lambda) = \frac{1}{24} \cdot (g_3^3 - 27 \cdot g_2^2) \in \mathbb{C}, \]
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 \( \Lambda \).

**Proposition 1.20 (Zero and pole divisor).** Consider an elliptic function and denote by \( A = (a_i)_{i=1,\ldots,n} \) its family of zeros in \( P \) and by \( B = (b_i)_{i=1,\ldots,n} \) its family of poles in \( P \). Then \( n \geq 2 \) and
\[ \sum_{i=1,\ldots,n} a_i - \sum_{i=1,\ldots,n} b_i \in \Lambda. \]
Note that each point \( p \) of \( \Lambda \) 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.
1.3 Abel's theorem

Proof. We consider a translation

\[ P_a := P + a \]

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

\[
\frac{1}{2\pi i} \int_{\partial P_a} z \cdot \frac{f'(z)}{f(z)} \, dz = \sum_{p \in P_a} \text{res}_p \left( z \cdot \frac{f'(z)}{f(z)} \right).
\]

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

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

In a neighbourhood of \( p \)

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

with \( f_1 \) holomorphic. 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 \( f_2 \) holomorphic. Therefore

\[
\text{res}_p \left( z \cdot \frac{f'(z)}{f(z)} \right) = p \cdot k
\]

and

\[
\sum_{p \in P_a} \text{res}_p \left( z \cdot \frac{f'(z)}{f(z)} \right) = \sum_{i=1}^{n} a_i - \sum_{i=1}^{n} b_i,
\]

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

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

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

\[
\int_{\overrightarrow{AB} + \overrightarrow{CD}} z \cdot \frac{f'(z)}{f(z)} \, dz = \omega_2 \cdot (\log f(A) - \log f(B)).
\]

Because
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

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

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

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

with \( A \) and \( B \) pairwise disjoint mod \( \Lambda \). Then are equivalent:

- There exists an elliptic function \( f \in \mathcal{M}(\Lambda) \) which has mod \( \Lambda \) 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 \( \Lambda \). 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
1.3 Abel’s theorem

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

Depending on the position relative to \( \Lambda \) 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 \( a_1 \neq a_2 \mod \Lambda \), and a zero of order = 2 at \( a_1 \equiv a_2 \mod \Lambda \) 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 \( \mod \Lambda \)

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

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 \( \mod \Lambda \)

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

and

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

Depending on the position of \( \tilde{a}_n \) relative to \( \Lambda \) we distinguish the following cases:
• $\tilde{a}_n \neq a_j$ 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

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

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

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

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

• $\tilde{a}_n \equiv a_n$: Then

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

By induction assumption two elliptic functions exist

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

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

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

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

• $\tilde{a}_n \neq a_n$, $\tilde{a}_n \equiv a_j$ 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

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

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

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

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

In all cases the elliptic function

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

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

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

$$a_1 + a_2 + a_3 = 0 \mod \Lambda.$$

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

The lengthy 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 periodicity 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 $\Gamma$ 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 $\Lambda$, 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

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

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

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

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

$$SL(2, \mathbb{Z}) \setminus M$$
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 \( \pm 1 \). 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 number \( a \in \mathbb{C} \) exists such that the following diagram commutes

Here \( \mu_a \) denotes the multiplication by \( a \) and \( \pi_i, i = 1, 2 \), 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 \( a \) satisfies \( a \cdot \Lambda_1 \subset \Lambda_2 \).

Proof. The composition \( F \circ \pi_1 : \mathbb{C} \to \mathbb{C}/\Lambda_2 \) starts from the simply-connected domain \( \mathbb{C} \). Therefore it lifts to the total space \( \mathbb{C} \) of the covering projection \( \pi_2 \). It provides a holomorphic map
\[ \tilde{F} : \mathbb{C} \to \mathbb{C}, \]
uniquely determined by the condition $F(0) = 0$. Commutativity of the lifting diagram shows: For all $z \in \mathbb{C}, \omega \in \Lambda_1$,

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

The lattice $\Lambda_2$ is discrete and $\tilde{F}$ is continuous. 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 $z \in \mathbb{C}$

$$\tilde{F}(z) = a \cdot z, \text{ q.e.d.}$$

**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 $\Lambda_1$ and $\Lambda_2$ are similar.

**Proof.** i) Assume the existence of a biholomorphic map

$$F : T_1 \rightarrow T_2$$

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

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

with $\mu_a$ 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 $\mu_b$ the unique lift of $F^{-1}$ fixing the origin. Then the map

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

is the unique lift of

$$id_{\mathbb{C}/\Lambda_1} = F^{-1} \circ F.$$
The modular group $\Gamma$ and its Hecke congruence subgroups $\Gamma_0(N)$ 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 $\tau$ 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
2.1 The moduli space of complex tori and group actions

\[ \tau := \frac{\omega_2}{\omega_1} \]

satisfies \( \text{Im } \tau > 0 \) and the lattice \( \Lambda \) 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

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

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 \( \Lambda_\tau \) 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.
\[
\tau' = \frac{a \cdot \alpha \tau + b \cdot \alpha}{c \cdot \alpha \tau + d \cdot \alpha} = \frac{a \cdot \tau + b}{c \cdot \tau + d}, \text{ q.e.d.}
\]

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
\[
\phi : G \times X \to X, \quad (g, x) \mapsto gx,
\]
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 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

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

**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

$$\text{Im} \, \gamma(\tau) = \det(\gamma) \cdot \text{Im} \, \frac{\tau}{|c\tau + d|^2}$$

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 $\Gamma$ on $\mathbb{H}^*$: We have

$z \in \mathbb{R} \implies \gamma(z) \in \mathbb{R} \cup \{\infty\}$ 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 $\gamma$ to the argument $\infty$ by setting

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

Set

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

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 congruence 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 $\Gamma$ 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. $\Gamma_\tau \supset \{\pm id\}$, are named *elliptic points* of $\Gamma_0(N)$. Half the order of the isotropy group

$$h_\tau := \frac{\text{ord } \Gamma_0(N)\tau}{2}$$
is named the *period* of $\tau$. 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 $\tau \in \mathbb{Q} \cup \{\infty\}$

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

**Remark 2.10 (Modular group and congruence subgroups).**

1. Apparently, $\Gamma = \Gamma_0(1)$

2. Corollary 2.18 will show that the isotropy groups of all elliptic points from Definition 2.9 are finite groups.

3. 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” $\overline{\mathbb{H}}$.

4. 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 $-id$.

**Example 2.11 (Cusps of $\Gamma$, $\Gamma_0(2)$, $\Gamma_0(4)$ and $\Gamma_0(11)$).** See [17, Sect. 3.8], and the PARI commands *mfcsps*, *mnfnumcusps*, *mfcspswidth*.
1. For \( N \in \mathbb{N} \) the number \( \varepsilon_{\infty}(\Gamma_0(N)) \) of cusps is
\[
\sum_{d \mid N} \phi(\gcd(d, N/d))
\]
with the sum extending over all positive divisors \( d \) of \( N \), and \( \phi \) denoting the Euler function defined as
\[
\Phi(n) := \text{card } (\mathbb{Z}/n\mathbb{Z})
\]
2. The group \( \Gamma \) has a single cusp
- *Orbit of the point 0:*
  \[\mathbb{Q} \cup \{\infty\}\]
  with \( \text{width} = 1 \). All rationals \( p/q \in \mathbb{Q} \) belong to the \( \Gamma \)-orbit of \( \infty \), 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 \( \text{width} = 2 \).
- *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 \( \text{width} = 1 \).

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 \( \text{width} = 4 \).
- *Orbit of the point 1/2:*
  \[
  \left\{ \frac{p}{q} \in \mathbb{Q} : (p, q) = 1, p \neq 0, q \text{ even, not divisible by 4} \right\}
  \]
2.1 The moduli space of complex tori and group actions

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 \( width = 1 \).

**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

\[ r := \prod_{p|c, p\neq a} p \]

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 \( q \mid r \) then \( q \mid b \). Therefore
  \[ \gcd(a, b, c, \ldots) \neq 1, \]
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

\[
1 \rightarrow \Gamma(N) \rightarrow \Gamma \xrightarrow{\pi} SL(2, \mathbb{Z}/N\mathbb{Z}) \rightarrow 1
\]

with

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

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

\( \pi : \Gamma \rightarrow SL(2, \mathbb{Z}/N\mathbb{Z}) \), \( A \mapsto \bar{A} \).

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

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

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

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

\[
\det \bar{A} = 1 \in \mathbb{Z}/N\mathbb{Z}
\]

implies

\[
\alpha \delta - \beta \gamma = 1 \mod N,
\]

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
\[ det \tilde{A} = (\alpha + xN) \cdot d - (\beta + yN) \cdot \gamma = 1 + sN + N(\alpha d - \beta \gamma) = 1, \]
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
\[
\begin{array}{cccccc}
1 & \longrightarrow & \Gamma(N) & \longrightarrow & \Gamma & \longrightarrow & SL(2, \mathbb{Z}/N\mathbb{Z}) & \longrightarrow & 1 \\
& & \downarrow{id} & & \uparrow{\pi} & & \uparrow{\psi} & & \\
1 & \longrightarrow & \Gamma(N) & \longrightarrow & \Gamma_0(N) & \longrightarrow & \Gamma_0(N)/\Gamma(N) & \longrightarrow & 1
\end{array}
\]
The induced map
\[ \psi : \Gamma_0(N)/\Gamma(N) \to SL(2, \mathbb{Z}/N\mathbb{Z}) \]
is injective with image
\[ \text{im } \psi = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{pmatrix} \right\} \subset SL(2, \mathbb{Z}/N\mathbb{Z}) \]

Apparently
\[ [\Gamma_0(N) : \Gamma(N)] = \text{card } \text{im } \psi = \phi(N) : N \]
with the Euler function \( \phi \).

The exact sequence of the first line of the diagram implies
\[ [\Gamma : \Gamma(N)] = \text{card } SL(2, \mathbb{Z}/N\mathbb{Z}). \]

The transititivity 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
\[ \phi(N) = \prod_{j=1}^{k} p_j^{e_j} \cdot \left( 1 - \frac{1}{p_j} \right) \]
with the Euler factors
\[ \phi(p^e) = p^e \cdot \left( 1 - \frac{1}{p} \right), \]
and the factorisation of the \( SL(2,\mathbb{Z}) \)-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
\[ \text{card } SL \left( 2, \mathbb{Z}/p_j^{e_j}\mathbb{Z} \right) = p_j^{3e_j} \cdot \left( 1 - \frac{1}{p_j^3} \right), \]
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
2.1 The moduli space of complex tori and group actions

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

see part i). It follows

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

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

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

Hence

\[ [\Gamma : \Gamma_0(N)] = \frac{[\Gamma : \Gamma(N)]}{[\Gamma_0(N) : \Gamma(N)]} = \frac{N^2 \cdot \phi(N) \cdot \prod_{j=1}^{k} \left( 1 + \frac{1}{p_j} \right)}{N \cdot \phi(N)} = N \cdot \prod_{p|N} \left( 1 + \frac{1}{p} \right), \text{ q.e.d.} \]

Example 2.15 (Right cosets of congruence subgroups). See the PARI-command \texttt{mfcosets}.

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

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

with the set of right coset representatives

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

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

\( \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \right\}. \)
2.2 Topology of the orbit space of the $\Gamma$-action

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

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

the continuous $\Gamma$-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 $\Phi$. We proceed along the following steps:

- Constructing a Hausdorff 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 $\Gamma$ contains the two distinguished elements

- **Reflection at the y-axis and dividing by squared absolute value:**
  $$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \Gamma, S(\tau) = -1/|\tau|^2$$

- **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 $\Gamma$-action).**

1. The modular group $\Gamma$ is generated by the two elements $S, T \in \Gamma$ which satisfy
   $$S^4 = id, (ST)^6 = id.$$
2.2 Topology of the orbit space of the $\Gamma$-action

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

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

the fundamental domain of $\Phi$.

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

- $\tau_0 = i$ with
  
  $$\Gamma_i = \langle S \rangle \subset \Gamma, \ \text{ord} \ \Gamma_i = 4,$$

- $\tau_0 = \rho := e^{2\pi i/3}$ with
  
  $$\Gamma_\rho = \langle ST \rangle \subset \Gamma, \ \text{ord} \ \Gamma_\rho = 6.$$

Figure 2.1 shows the fundamental domain $\mathcal{D}$ of the modular group $\Gamma$ shaded, from [29]

Figure 2.1 shows the fundamental domain $\mathcal{D}$ of the modular group. In order to exclude pairs of congruent points within $\mathcal{D}$ one has to exclude part of the boundary of $\mathcal{D}$. This convention is followed by [29] but not by all references. Most references name fundamental domain the closure $\overline{\mathcal{D}}$. 
Figure 2.2 shows some translates of the fundamental domain of $\Gamma$ 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

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

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

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

$$G := \langle S, T \rangle \subset \Gamma$$

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

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

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

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

$$-1/2 \leq \text{Re} \; \gamma_0(\tau) < 1/2.$$ 

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

$$\text{Im} \; (S \circ \gamma_0)(\tau) = \text{Im} \left( \frac{-\gamma_0(\tau)}{|\gamma_0(\tau)|^2} \right) > \text{Im} \; \gamma_0(\tau).$$
• If $|\gamma_0(\tau)| > 1$ then $\tau' := \gamma_0(\tau)$.
• If $|\gamma_0(\tau)| = 1$ but $0 < \text{Re} \gamma_0(\tau) \leq 1/2$ then
  $$\tau' := (S \circ \gamma_0)(\tau).$$
In both cases $\tau' \in \mathcal{D}$.

ii) Isotropy groups and fundamental domain: Consider two points $\tau, \tau' \in \mathcal{D}$ 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 $\text{Im} \tau' \geq \text{Im} \tau$. Then
  $$\text{Im} \tau' = \frac{\text{Im} \tau}{|c \cdot \tau + d|^2},$$
implies
  $$|c \cdot \tau + d| \leq 1.$$ 
Because $\text{Im} \tau \geq \sqrt{3}/2$ 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 $\text{Re} \tau' = (\text{Re} \tau) + b$ we obtain $b = 0$; i.e. $\tau = \tau'$ and
  $$\gamma = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \pm \text{id} \in \Gamma_\tau.$$
• Case 2, $c = 1$: Then $|\tau + d| \leq 1$, 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 $\tau \in \mathcal{D}$ the equation
  $$|c \cdot \tau + d| = |\tau| \leq 1$$
implies $|\tau| = 1$. Hence
  $$1/\tau = \overline{\tau} \text{ and } \tau' + \overline{\tau} = a \in \mathbb{Z}$$
which implies
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 \( \tau, \tau' \in \mathcal{D} \) 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
\[
ad - bc = a - b = 1 \quad \text{and} \quad \tau' = \frac{a \cdot \rho + b}{\rho + 1} = a + \rho,
\]
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
\[
\tau_0 := 2 \cdot i \in \mathcal{D}.
\]
Due to part i) an element \( \gamma_0 \in G \) exists with
\[
(\gamma_0 \circ \gamma)(\tau_0) \in \mathcal{D}.
\]
Due to part ii) the two points of \( \mathcal{D} \) coincide
\[
\tau_0 = (\gamma_0 \circ \gamma)(\tau_0) \in \mathcal{D},
\]
2.2 Topology of the orbit space of the \( \Gamma \)-action

i.e.

\[
\gamma_0 \circ \gamma \in \Gamma_0 = \{ \pm \text{id} \}
\]

which implies \( \gamma \in G \), q.e.d.

**Remark 2.17 (Presentation of \( SL(2, \mathbb{Z}) \)).**

1. Consider the element

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

which satisfies \( U^3 = \text{id} \). Apparently also

\[
G = \langle S, U \rangle.
\]

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

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

i.e. that

\[
SL(2, \mathbb{Z}) = \langle S, U; S^4, U^3, S^2U \cdot (US^2)^{-1} \rangle
\]

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

2. Denote by

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

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

\[
H_1 := \langle S \rangle \cong \mathbb{Z}/2\mathbb{Z} \quad \text{and} \quad H_2 := \langle U \rangle \cong \mathbb{Z}/3\mathbb{Z}.
\]

One can show

\[
PSL(2, \mathbb{Z}) = H_1 * H_2 = \langle S, U; S^2, U^3 \rangle
\]

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

**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 \( \Gamma \) has exactly two elliptic points \( i, \rho \in \mathcal{D} \), and both have finite isotropy groups. The index formula from Proposition 2.14 implies the finiteness of

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

Hence a finite coset decomposition exists

\[ \Gamma = \bigcup_{j=1}^{k} \gamma_j \cdot \Gamma_0(N) \]

with suitable elements \( \gamma_j \in \Gamma, \ j = 1, \ldots, k \). The set

\[ \mathcal{D}(\Gamma_0(N)) := \bigcup_{j=1}^{k} \gamma_j^{-1}(\mathcal{D}) \]

is a fundamental domain of \( \Gamma_0(N) \), e.g. see Figure 2.3. For each \( j = 1, \ldots, k \) and each point \( \tau \in \gamma_j^{-1}(\mathcal{D}) \) the group morphism

\[ \Gamma_0(N) \tau \rightarrow \Gamma_{\gamma_j(\tau)}, \ \gamma \mapsto \gamma_j \cdot \gamma \cdot \gamma_j^{-1}, \]

injects \( \Gamma_0(N) \tau \) into \( \Gamma_{\gamma_j(\tau)} \). Hence the elliptic points of \( \Gamma_0(N) \) contained in \( \mathcal{D}(\Gamma_0(N)) \) 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 \( \mathcal{D}(\Gamma_0(13)) \) splits into 14 disjoint translates of \( \mathcal{D} \) 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].
2.2 Topology of the orbit space of the $\Gamma$-action

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 $\Phi$ covers the main step for proving the Hausdorff property of the quotient topology 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 $\tau$. 
Figure 2.4 visualizes Lemma 2.19: If an element $\gamma \in \Gamma$ maps a point of the distinguished neighbourhood $U_1$ of $\tau_1$ to the distinguished neighbourhood $U_2$ of $\tau_2$, then $\gamma$ maps $\tau_1$ to $\tau_2$. The add-on states: If $\gamma \in \Gamma$ does not fix $\tau$, then $\gamma$ moves all points from $U$ to the complement of $U$.

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

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

and show: Only finitely many matrices $\gamma \in \Gamma$ exists with
2.2 Topology of the orbit space of the $\Gamma$-action

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

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

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

which provides a compact isotropy group of the point $i$

$SL(2, \mathbb{R}) \cdot i = SO(2, \mathbb{R})$.

One checks

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

hence

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

The action $\Phi$ 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

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

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

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

according to the following commutative diagram

$$\begin{array}{ccc}
\gamma_{e_1} & \downarrow \gamma & \gamma_{e_2} \\
\varepsilon_1 & \downarrow & \varepsilon_2 \\
i & \vdots & i \\
\end{array}$$

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
The modular group $\Gamma$ and its Hecke congruence subgroups $\Gamma_0(N)$

$$G := \{ \gamma \in SL(2, \mathbb{R}) : \gamma(V_1) \cap V_2 \neq \emptyset \} = \bigcup_{e_1 \in V_1, e_2 \in V_2} \gamma_{e_2} \cdot SO(2, \mathbb{R}) \cdot \gamma_{e_1}^{-1}.$$  

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

$$V_2 \times SO(2, \mathbb{R}) \times V_1$$

under the continuous map

$$V_2 \times SO(2, \mathbb{R}) \times V_1 \rightarrow SL(2, \mathbb{R}), \quad (e_2, \gamma, e_1) \mapsto \gamma_{e_2} \cdot \gamma \cdot \gamma_{e_1}^{-1},$$

and therefore compact itself. Its intersection

$$G \cap \Gamma$$

with the discrete group $\Gamma$ 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 $\tau_2$ 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 $\tau_1$ and $\tau_2$ in $\mathbb{H}$

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

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

$$\gamma(U_1) \cap U_2 = \emptyset.$$
2.2 Topology of the orbit space of the $\Gamma$-action

3. Isotropy group $\Gamma_\tau$: 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 $\zeta$. Because $z \neq \zeta$, 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
The modular group $\Gamma$ and its Hecke congruence subgroups $\Gamma_0(N)$

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

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 $\gamma^{-1}$

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

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 $j = 1, 2$ choose 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 $\tau_1$ and of $\tau_2$ 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 $\sigma$ 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

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

$$(\sigma(\gamma_v, \tau_v))_{v \in \mathbb{N}} = (\tau_v, \gamma_v(\tau_v))_{v \in \mathbb{N}}$$

is convergent. Set

$$x_1 := \lim_{v \to \infty} \tau_v, \quad x_2 := \lim_{v \to \infty} \gamma_v(\tau_v) \text{ (pointwise convergence).}$$

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

$$(\tau_v)_{v \in \mathbb{N}} \text{ and } (\gamma_v(\tau_v))_{v \in \mathbb{N}}$$

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

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 $v \in \mathbb{N}$ but finitely many indices

$$\tau_v \in U_1 \text{ and } \gamma_v(\tau_v) \in U_2,$$

hence

$$\gamma_v(U_1) \cap U_2 \neq \emptyset.$$ 

The lemma implies

$$\gamma_v(x_1) = x_2$$

The set

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

has the same cardinality as the isotropy group $\Gamma_{x_1}$. The latter is a finite group due to Theorem 2.16. A subsequence $(\gamma_v)_{v \in \mathbb{N}}$ 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
2.2 Topology of the orbit space of the $\Gamma$-action

- 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 neighbourhoods

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

of respectively $p(x)$ and $p(y)$ with

$$p(U) \cap p(V) = \emptyset, \text{ q.e.d.}$$

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

$$p^{-1}(y) \subset \mathbb{H}, \text{ } y \in Y,$$

of the $\Gamma$-action is closed.
2.3 Modular curves $X(Γ_0(N))$ 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 $τ ∈ ℍ$ with period $h_τ$ acts as the group of rotations of a disk around the origin with angles a multiple of $2π/h_τ$.

**Lemma 2.26 (Isotropy group acting as group of rotations).** For any point $τ ∈ ℍ$ exist

- a neighbourhood $U_τ ⊂ ℍ$ of $τ$ such that for all $γ ∈ Γ$
  \[ γ(U_τ) \cap U_τ \neq \emptyset \implies γ ∈ Γ_τ, \]
- and a fractional linear transformation $λ_τ ∈ GL(2, ℂ)$ satisfying
  \[ λ_τ : U_τ \xrightarrow{\sim} Δ_τ \]
  with a disc $Δ_τ = \{ z ∈ Δ : |z| < r_τ \}$ for a suitable radius $r_τ > 0$

such that: For all $γ ∈ Γ_τ$ the conjugate map
  \[ ˜γ_τ := λ_τ \circ γ \circ λ_τ^{-1} : Δ_τ \to Δ_τ \]
from the commutative diagram

\[
\begin{array}{ccc}
U_τ & \xrightarrow{γ} & γ(U_τ) \\
\downarrow {λ_τ} & & \downarrow {λ_τ} \\
Δ_τ & \xrightarrow{γ_τ} & Δ_τ \\
\end{array}
\]

is a rotation around $0 ∈ Δ_τ$. The angle of rotation is an integer multiple of $2π/h_τ$.

**Proof.** Due to Theorem 2.16 w.l.o.g.

\[ τ ∈ \{ i, \rho \}. \]

Denote by
2.3 Modular curves $X(G_0(N))$ as compact Riemann surfaces

\[
\lambda_\tau : \mathbb{P}^1 \to \mathbb{P}^1, \quad \lambda_\tau(z) := \frac{z - \tau}{z - \overline{\tau}}
\]

the fractional linear automorphism of $\mathbb{P}^1$ with $\lambda(\mathbb{H}) = \Delta$ and

\[
\lambda_\tau(\tau) = 0, \quad \lambda_\tau(\overline{\tau}) = \infty.
\]

The following diagram commutes for all $\gamma \in \Gamma_\tau$

\[
\begin{array}{ccc}
\mathbb{H} & \xrightarrow{\gamma} & \mathbb{H} \\
\downarrow \lambda_\tau & & \downarrow \lambda_\tau \\
\Delta & \xrightarrow{\tilde{\gamma}_\tau} & \Delta
\end{array}
\]

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

\[
\Gamma_i = \langle S \rangle \quad \text{and} \quad \Gamma_\rho = \langle ST \rangle.
\]

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

\[
\tilde{\gamma}_\tau(z) = e^{k(2\pi i/\tau)} \cdot z, \quad k \in \{0, 1, \ldots, h_\tau - 1\}
\]

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 diagram proves the claim, q.e.d.

In order to obtain a complex structure on the orbit space, the Hausdorff space

\[
Y = \Gamma \setminus \mathbb{H},
\]
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 $\Gamma_\tau$ as cyclic groups of rotations of a disk $\Delta_\tau$ due to Lemma 2.26. Assume

$$(1/2) \cdot \text{ord } \Gamma_\tau = h_\tau =: k.$$ 

Then in a neighbourhood $\Delta_\tau$ of $\lambda_\tau(\tau)$ the function

$$z \mapsto z^k$$

foliates the $k$ different segments of the disk $\Delta_\tau$, which are equivalent under the $\Gamma_\tau$-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 $\Delta_\tau$ 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.
2.3 Modular curves $X(\Gamma_0(N))$ as compact Riemann surfaces

**Proof.** i) *Homeomorphisms:* For each $\tau \in \mathbb{H}$ choose a neighbourhood $U_\tau \subset \mathbb{H}$ of $\tau$ with the properties from lemma 2.26. Using the notation from the lemma define

$$\text{pow}_\tau : \Delta_\tau \to \mathbb{C}, z \mapsto z^{\gamma_\tau},$$

and set

$$W_\tau := \text{pow}_\tau(\Delta_\tau)$$

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

\[
\begin{array}{ccc}
U_\tau & \xrightarrow{p|U_\tau} & p(U_\tau) \\
\downarrow{\lambda_\tau} & & \downarrow{\phi_\tau} \\
\Delta_\tau & \xrightarrow{\text{pow}_\tau} & W_\tau
\end{array}
\]

The map $\phi_\tau$ 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 $\text{pow}_\tau \circ \lambda_\tau$.

- continuous, because $p$ is open,

- open, because $\lambda_\tau$ and $\text{pow}_\tau$ are open.

As a consequence, $\phi_\tau$ 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

$$\phi_\tau : p(U_{\tau_1}) \to W_\tau$$

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

\[ U_i := U_{\tau_i}, \phi_i := \phi_{\tau_i}, \lambda_i := \lambda_{\tau_i}, h_i := h_{\tau_i}, W_i := W_i, \ i = 1, 2. \]

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 \( \phi \) 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. the case of an elliptic point \( \tau_1 \in \mathbb{H} \):

- 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 \( \tau_2 \) 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 \( \infty \) to \( \infty \). 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
\[ A \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^T = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^T, \ A \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^T. \]

As a consequence
\[ A = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \]
and
2.3 Modular curves $X(I_0(N))$ as compact Riemann surfaces

$$\phi_{2,1}(q) = \left( (\lambda_2 \circ \gamma \circ \lambda_1^{-1})(q^{1/h}) \right)^h = \left( A(q^{1/h}) \right)^h = ((a \cdot q^{1/h})/d)^h = (a/d)^h \cdot q.$$ 

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 $\tau_3 \in \mathcal{S}$ 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 $\lambda : \mathbb{H} \rightarrow \Delta$.

The upper half-plane has a canonical boundary point, the point $\infty$. 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

$$\{z \in \mathbb{C} : \text{Im } z > R \} \cup \{\infty\}, \ R > 0,$$

i.e. the complements of sets with bounded imaginary part. Secondly, one translates neighbourhoods of $\infty$ 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. The latter is finer than the topology induced 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]](image)

**Theorem 2.28 (The modular curve of the modular group).** Consider the action of the modular group $\Gamma$ 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

$$
\begin{array}{c}
\mathbb{H} \quad \xrightarrow{p} \quad \mathbb{H}^* \\
\downarrow \quad \downarrow \\
Y \quad \xrightarrow{p^*} \quad X
\end{array}
$$

2. The Riemann surface $X$ is biholomorphic equivalent to $\mathbb{P}^1$.

Proof. i) **Topology on $\mathbb{H}^*$**: Take as neighbourhood basis of $\infty$ for the topology on $\mathbb{H}^*$ the sets

$$U_R := \{ \tau \in \mathbb{H} : \text{Im} \tau > R \} \cup \{ \infty \}, \ R > 0,$$

and as neighbourhood basis of

$$q := a/c \in \mathbb{Q}, \ \text{gcd}(a, c) = 1,$$

the sets

$$\gamma(U_R), \ R > 0, \ \gamma = \left( \begin{array}{cc} a & * \\ c & * \end{array} \right) \in \Gamma,$$

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 $\Gamma$ 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 $\infty$ 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 $\Gamma \setminus \mathbb{H}^*$**: We provide the set

$$X := \Gamma \setminus \mathbb{H}^*$$

with the quotient topology with respect to the canonical projection

$$p^* : \mathbb{H}^* \rightarrow X.$$

Then $p^*$ is an open map: The proof is the same as the corresponding proof for Corollary 2.25. 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
\[
x_i = p^*(\tau_i) \in X, \quad \tau_i \in \mathbb{H}^+, i = 1, 2, \text{ and assume } x_1 \neq x_2.
\]
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
  \[
  \text{Im} \gamma(\tau) = \frac{\text{Im} \tau}{|c \cdot \tau + d|^2} = \frac{\text{Im} \tau}{(c \cdot \text{Re} \tau + d)^2 + c^2 \cdot (\text{Im} \tau)^2} \leq \frac{\text{Im} \tau}{\max \{1/\text{Im} \tau, 1/\text{Im} \tau\}}
  \]
  shows
  \[
  \text{Im} \gamma(\tau) \leq \max \{1/\text{Im} \tau, 1/\text{Im} \tau\},
  \]
  independently from \( \gamma \). Therefore a relatively compact neighbourhood
  \[
  U_1 \subset \mathbb{H}
  \]
of \( \tau_1 \) 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 \( \overline{\mathbb{H}} \subset \mathbb{H} \) the closure of \( \mathbb{H} \) with respect to \( \mathbb{H} \).
Then
  \[
  \overline{\mathbb{H}} := \mathbb{H} \cup \{\infty\} \subset \mathbb{H}^*
  \]
is compact with respect to \( \mathbb{H}^* \): Consider an open covering \((U_i)_{i \in I}\) of \( \overline{\mathbb{H}} \). If \( \infty \in U_{i_0} \)
then for suitable \( R > 0 \):
  \[
  \{ \tau \in \overline{\mathbb{H}} : \text{Im} \tau > R \} \cup \{\infty\} \subset U_{i_0}.
  \]
The remaining set
\[ \{ \tau \in \mathcal{D}^\mathbb{H} : \text{Im} \tau \leq R \} \]
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 \( \mathcal{D} \subset \mathbb{H}^* \).

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 \( \infty \in \mathbb{H}^* \)
\[ U_\infty := U_2 = \{ \tau \in \mathbb{H} : \text{Im} \tau > 2 \} \cup \{ \infty \} \]
We define
\[ \text{pow}_{\infty} : U_\infty \to \Delta, \quad \tau \mapsto \begin{cases} e^{2\pi i \tau} & \text{if } \tau \neq \infty \\ 0 & \text{if } \tau = \infty \end{cases} \]
and set
\[ W_\infty := \text{pow}_{\infty}(U_\infty) \subset \Delta. \]
For two points \( \tau_i \in U_\infty, i = 1, 2, \)
\[ \tau_2 = p^*(\tau_1) \iff \tau_2 = \gamma(\tau_1) \text{ for a suitable } \gamma \in \Gamma \]
\[ \iff \tau_2 = \tau_1 + m \text{ for a suitable } m \in \mathbb{Z}, \text{ due to Theorem 2.16}, \]
\[ \iff \text{pow}_{\infty}(\tau_2) = \text{pow}_{\infty}(\tau_1). \]
We define the chart \( \phi_\infty \) as the commutative completion of the diagram
One shows analogously to the proof of Proposition 2.27 that the map \( \phi_{\infty} \) is a homeomorphism.

Eventually we have to show that the charts of \( Y \) and the chart \( \phi_{\infty} \) 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 \( U_{\tau} \) 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

\[ Y = p(\mathcal{D}) \]

is homeomorphic to the plane \( \mathbb{C} \): Identify points on the left and right boundary of \( \mathcal{D} \) and equivalent points of \( \mathcal{D} \) on the unit circle. 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 \( \Gamma \)).** The compact Riemann surface from Theorem 2.28

\[ X(1) := X(\Gamma) := \Gamma \backslash \mathbb{H}^* \]

is named the **modular curve of \( \Gamma \)** 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

\[ X_0(N) := \Gamma_0(N) \backslash \mathbb{H}^* = (\Gamma_0(N) \backslash \mathbb{H}) \cup \text{Cusp}(\Gamma_0(N)), \]

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

\[ \deg f = [\Gamma : \Gamma_0(N)] = N \cdot \prod_{p \mid N} \left( 1 + \frac{1}{p} \right), \]

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

\[ f : X_0(N) \to X(1) \cong \mathbb{P}^1 \]

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
The modular group $\Gamma$ and its Hecke congruence subgroups $\Gamma_0(N)$

$$g(X_0(N)) = 1 + \frac{\deg f}{12} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3} - \frac{\varepsilon_\infty}{2}$$

with $\varepsilon_2$, $\varepsilon_3$ and $\varepsilon_\infty$ 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 $\varepsilon$-constants can be computed as

$$\varepsilon_\infty = \sum_{d|N} \Phi(gcd(d,N/d)),$$

see Example 2.11, and $\varepsilon_2$ and $\varepsilon_3$ 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
2.3 Modular curves $X(\Gamma_0(N))$ as compact Riemann surfaces

$$g(X_0(p)) = \begin{cases} \left\lfloor \frac{k}{12} \right\rfloor - 1 & \text{if } k \equiv 2 \text{ mod } 12 \\ \left\lfloor \frac{k}{12} \right\rfloor & \text{otherwise} \end{cases}$$

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 $p$:**
  $\text{kronecker}(a, p) := \left( \frac{a}{p} \right)$ for odd $p$

- **Even prime $p = 2$:**

  $$\text{kronecker}(a, 2) := \begin{cases} 0 & \text{if } a \text{ even} \\ (-1)^{\lfloor a^2 - 1 \rfloor / 8} & \text{otherwise} \end{cases}$$

The Kronecker symbol satisfies

- **Odd prime $p$:**

  $$\text{kronecker}(-4, p) = \left( \frac{-4}{p} \right) = \left( \frac{2}{p} \right)^2 \cdot \left( \frac{-1}{p} \right) = \left( \frac{-1}{p} \right)$$

- **Even prime $p = 2$:**

  $$\text{kronecker}(-4, 2) = 0 = \left( \frac{-1}{2} \right) \text{ and } \text{kronecker}(-3, 2) = -1 = \left( \frac{-3}{2} \right)$$

Hence

$$\varepsilon_2 = \begin{cases} \prod_{p \mid N} (1 + \text{kronecker}(-4, p)) & \text{if } 4 \nmid N \\ 0 & \text{otherwise} \end{cases}$$

and
The modular group $\Gamma$ and its Hecke congruence subgroups $\Gamma_0(N)$

$$\varepsilon_3 = \begin{cases} 
\prod_{p|N} (1 + \text{kronecker}(-3, p)) & \text{if } 9 \nmid N \\
0 & \text{otherwise}
\end{cases}$$

Figure 2.8 shows the invariants of the covering

$$X_0(p) \to X(1)$$

for all primes $p < 100$.

---

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 $\infty$ with rational Fourier coefficients after normalization.

The interplay of these two properties is coined “The magic of modular forms” [65]. Thence 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 $\Gamma$ 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 $\Gamma$, i.e. we introduce a $\Gamma$-action on certain vector spaces of holomorphic differential forms.

**Proposition 3.1 ($\Gamma$-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 $\Gamma$-right action. For

$$\gamma = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \Gamma, \ \omega = f \ d \tau \in W^1 \text{ and } \tau \in \mathbb{H}$$

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

$$\Omega^{k/2} := \Omega^{k/2}_{\mathbb{H}} \text{ and } W^{k/2} := H^0(\mathbb{H}, \Omega^{k/2})$$

and

$$\Phi^{k/2} : W^{k/2} \times \Gamma \to W^{k/2}, \ (\omega, \gamma) \mapsto \Phi^{k/2}(\omega, \gamma) := \gamma^* \omega.$$

For

$$\gamma = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \Gamma, \ \omega = f \ (d \tau)^{k/2} \in W^{k/2} \text{ and } \tau \in \mathbb{H}$$

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 $k \in \mathbb{N}$,

$$\gamma = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \Gamma \text{ and } \omega = f \ (d \tau)^{k/2} \in W^{k/2}$$
3.1 Modular forms and cusp forms

holds the equivalence

$$\gamma^*(\omega) = \omega \iff f(\tau) = (f \circ \gamma)(\tau) \frac{1}{(c\tau + d)^k} \text{ for all } \tau \in \mathbb{H}.$$ 

Note. In the context of modular forms $\Omega^{k/2}$ denotes the tensor product of $\Omega^1$ 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

$$(d\gamma)(\tau) \equiv d \left( \frac{a\tau + b}{c\tau + d} \right) = \frac{a(c\tau + d) - (a\tau + b)c}{(c\tau + d)^2} d\tau = \frac{1}{(c\tau + d)^2} d\tau$$

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 $k \in \mathbb{H}$ the invariant differential forms from the fixed space of the $\Gamma$-representation

$$f d\tau^{k/2} \in (W^{k/2})^\Gamma$$

are characterized by holomorphic coefficient functions $f \in \mathcal{O}(\mathbb{H})$ 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 coefficient 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
\[ T^*(f(d\tau)^{k/2}) = f(d\tau)^{k/2} \iff f(\tau + 1) = f(\tau) \quad \text{for all} \quad \tau \in \mathbb{H}, \]
and the latter equality means that the function \( f \) has the period \( = 1 \). Hence \( f \) expands into a convergent Fourier series
\[ f(\tau) = \hat{f}(q) = \sum_{n=-\infty}^{\infty} a_n \cdot q^n, \quad q = e^{2\pi i \tau}, \]
similar to the trigonometric function
\[ \cos(2\pi z) = \frac{1}{2} (e^{2\pi i z} + e^{-2\pi i z}). \]
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 \( \Delta^* \) according to the following diagram

Set
\[ \hat{f}(q) := f(\tau) = \sum_{n=-\infty}^{\infty} a_n \cdot q^n, \quad q = e^{2\pi i \tau}. \]
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 \( \Delta^* \) with
\[
\hat{f}(q) := \hat{f}(e^{2\pi i \tau}) := f(\tau).
\]
1. The function \( f \) is named \textit{meromorphic at} \( \infty \)
   
   • 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 \( \infty \) then the induced function \( \hat{f} \) has a Laurent expansion around 0
\[
\hat{f}(q) = \sum_{n=-n_0}^\infty a_n \cdot q^n, \quad q = e^{2\pi i \tau},
\]
with a suitable \( n_0 \in \mathbb{Z} \). The Laurent expansion is named the \textit{q-expansion} of \( f \), and the elements \( (a_n)_{n \geq n_0} \) are the \textit{Fourier coefficients} of \( f \).
3. A function \( f, \) meromorphic at \( \infty \), is named \textit{holomorphic at} \( \infty \) 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
\[
\Phi : \text{GL}(2, \mathbb{R})^+ \times \mathbb{H} \to \mathbb{H}, \quad (\gamma, \tau) \mapsto \gamma(\tau) := \frac{a \tau + b}{c \tau + d}, \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},
\]
which extends the group action of the modular group \( \Gamma \) to \( \text{GL}(2, \mathbb{R})^+ \). The map
\[
h : \text{GL}(2, \mathbb{R})^+ \times \mathbb{H} \to \mathbb{H}, \quad h(\gamma, \tau) := c \tau + d,
\]
is named the \textit{factor of automorphy} of \( \Phi \).

The translation \( T \in \text{SL}(2, \mathbb{Z}) \) 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

\[ h(B \cdot A, \tau) = h(B, A(\tau)) \cdot h(A, \tau); \quad A, B \in GL(2, \mathbb{R})^+, \quad \tau \in \mathbb{H}. \]

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

\[ V \times GL(2, \mathbb{R})^+ \to V, \quad (f, \gamma) \mapsto f[\gamma]_k, \]

with

\[ f[\gamma]_k(\tau) := f(\gamma(\tau)) \cdot h(\gamma, \tau)^{-k} \cdot (\det \gamma)^{k-1}, \quad \tau \in \mathbb{H}, \]

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 5.9.

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:

\[ B \cdot \begin{pmatrix} A \cdot \begin{pmatrix} \tau \\ 1 \end{pmatrix} \end{pmatrix} = B \cdot \begin{pmatrix} A(\tau) \\ 1 \end{pmatrix} \cdot h(A, \tau) = \begin{pmatrix} B(A(\tau)) \\ 1 \end{pmatrix} \cdot h(B,A(\tau)) \cdot h(A, \tau). \]

Equating with the right-hand side gives for the lower row

\[ h(B \cdot A, \tau) = h(B,A(\tau)) \cdot h(A, \tau), \]

\[ h(B \cdot A, \tau) = h(B,A(\tau)) \cdot h(A, \tau). \]
3.1 Modular forms and cusp forms

hence for the upper row

\[(B \cdot A)(\tau) = B(A(\tau))\).

2. Starting with the right-hand side we compute

\[
(f[B]_k[A]_k)(\tau) = (f[B]_k(A(\tau)) \cdot h(A, \tau)^{-k} \cdot (\text{det } A)^{k-1} =
\]

\[
= f(B(A(\tau)) \cdot h(B,A(\tau))^{-k} \cdot h(A, \tau)^{-k} \cdot (\text{det } B)^{k-1} \cdot (\text{det } A)^{k-1} =
\]

\[
= f((B \cdot A)(\tau)) \cdot h(B \cdot A, \tau)^{-k} \cdot (\text{det } (B \cdot A))^{k-1} = f[B \cdot A]_k(\tau).
\]

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

\[f[B \cdot A]_k = (f[B]_k[A]_k), \text{ q.e.d.}\]

**Remark 3.5 (Meromorphy and holomorphy at the cusps).** The Fourier expansion from Definition 3.2 is well-defined for holomorphic functions \(f : \mathbb{H} \rightarrow \mathbb{C}\) which are invariant with respect to the translation \(T\). The modular group \(\Gamma\) has only a single cusp, the orbit comprising \(\infty\) 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 \(q \in \mathbb{Q}\). How to extend a holomorphic function

\[f : \mathbb{H} \rightarrow \mathbb{C}\]

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?

The translation \(T \in \Gamma\) generates the isotropy group \(\Gamma_\infty:\)

\[\Gamma_\infty = \langle T^k : k \in \mathbb{Z} \rangle \simeq \mathbb{Z}.\]

If \(\alpha \in \Gamma\) with

\[q = \alpha(\infty)\]

then

\[\Gamma_0(N)_q \simeq \alpha^{-1} \cdot \Gamma_0(N)_q \cdot \alpha \subset \Gamma_\infty \simeq \Gamma_q\]

The width of the cusp passing through \(q\) is finite, i.e.

\[1 \leq h_q := [\Gamma_q : \Gamma_0(N)_q] < \infty,\]
86 3 The algebra of modular forms

see [17, Exerc. 2.4.4]. Therefore

\[
\alpha^{-1} \cdot \Gamma_0(N)_q \cdot \alpha = \left\{ (T^{h_q})^m : m \in \mathbb{Z} \right\},
\]

the unique subgroup of \( \Gamma_\infty \simeq \mathbb{Z} \) with index \( h_q \). We choose \( \gamma \in \Gamma_0(N)_q \) with

\[
\alpha^{-1} \cdot \gamma \cdot \alpha = T^{h_q}
\]

Lemma 3.4 shows

\[
(f[\alpha]_k)[T^{h_q}] = f[\alpha \cdot T^{h_q}] = f[\gamma \cdot \alpha]_k = (f[\gamma]_k)[\alpha]_k = f[\alpha]_k
\]

Hence \( f[\alpha]_k \) is invariant under \( T^{h_q} \) and has a Fourier series

\[
(f[\alpha]_k)(\tau) = \sum_{n=-\infty}^{\infty} a_n \cdot \hat{q}^n, \quad \hat{q} := e^{2\pi i \tau / h_q}
\]

The function \( f[\alpha]_k \) is named \textit{meromorphic} respectively \textit{holomorphic} at \( \infty \) iff \( f[\alpha]_k \) has at \( \hat{q} = 0 \) at most a pole respectively a removable singularity.

The fundamental object of the whole theory is the \textit{modular form}. We introduce modular forms of the modular group \( \Gamma \) 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 \textit{weakly modular of weight} \( k \) with respect to \( \Gamma \) if for all \( \gamma \in \Gamma \) and for all \( \tau \in \mathbb{H} \)
     \[
     f(\gamma(\tau)) \cdot \frac{1}{(c\tau + d)^k} = f(\tau), \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}
     \]
   - The function \( f \) is an \textit{automorphic form of weight} \( k \) with respect to \( \Gamma \) if \( f \) is weakly modular of weight \( k \) and meromorphic at \( \infty \).
   - The function \( f \) is a \textit{modular form of weight} \( k \) with respect to \( \Gamma \) if \( f \) is weakly modular of weight \( k \), holomorphic on \( \mathbb{H} \) and holomorphic at \( \infty \).
   - A modular form \( f \) of weight \( k \) vanishing at all points of the cusp of \( \Gamma \), i.e.
     \[
     f(\infty) = 0
     \]
3.1 Modular forms and cusp forms

is a cusp form of weight $k$ with respect to $\Gamma$.

- An automorphic function with respect to $\Gamma$ 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 $\Gamma$ 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
  \[ f(\gamma) = f, \]
  and for all $\alpha \in \Gamma$ the function $f(\alpha) = f$ is holomorphic at $\infty$ 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 $f(\alpha) = f$ is holomorphic at $\infty$, 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
  \[ f(\gamma) = f, \]
  and for all $\alpha \in \Gamma$ the function $f(\alpha) = f$ is meromorphic at $\infty$ 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 \( \Gamma \).

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 \( \Gamma \)

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 \( \Gamma \)-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
\[
q : \mathbb{H} \to \Delta^*, \quad \tau \mapsto q(\tau) := e^{2\pi i \tau},
\]
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
\[
q := e^{2\pi i \tau}.
\]
3.2 Eisenstein series and the algebra of modular forms of $\Gamma$

1. For $k \geq 2$ and $\text{Im } \tau \neq 0$

$$
\sum_{n \in \mathbb{Z}} \frac{1}{(\tau + n)^k} = \begin{cases} 
\sum_{r=1}^{\infty} r^{k-1} \cdot q^r & \text{Im } \tau > 0 \\
(-1)^k \cdot \sum_{r=1}^{\infty} r^{k-1} \cdot q^{-r} & \text{Im } \tau < 0
\end{cases}
$$

2. For $\text{Im } \tau > 0$ the double series

$$
\sum_{m=1}^{\infty} \left( \sum_{d=1}^{\infty} d \cdot q^{md} \right)
$$

is absolutely convergent.

3. For even $k \geq 2$, $\text{Im } \tau > 0$,

$$
\sum_{m \in \mathbb{Z}^*} \left( \sum_{n \in \mathbb{Z}} \frac{1}{(m\tau + n)^k} \right) = \frac{2 (2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n
$$

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 $\text{Im } \tau > 0$. 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
The algebra of modular forms

\[
\cot(\pi \tau) = i \cdot \frac{e^{i \pi \tau} + e^{-i \pi \tau}}{e^{i \pi \tau} - e^{-i \pi \tau}} = i \cdot \frac{q + 1}{q - 1} = (-i) \cdot \frac{1 + q}{1 - q}
\]

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 \(\tau\) shows

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

ii) For \(\text{Im } \tau < 0\) we first use

\[
\pi \cdot \cot(\pi \tau) = i \pi \cdot \frac{e^{i \pi \tau} + e^{-i \pi \tau}}{e^{i \pi \tau} - e^{-i \pi \tau}} = i \pi \cdot \frac{1 + (1/q)}{1 - (1/q)} = i \pi (1 + (1/q)) \cdot \sum_{m=1}^{\infty} q^{-m} = i \pi + 2\pi i \cdot \sum_{m=1}^{\infty} q^{-m}
\]

Equating the partial fraction expansion and the Fourier expansion 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 \(\tau\) shows

\[
\sum_{m \in \mathbb{Z}} \frac{1}{(\tau + m)^k} = (-1)^{1+(k-1)} \frac{(2\pi i)^k}{(k - 1)!} \sum_{m=1}^{\infty} m^{k-1} q^{-m} = \frac{(2\pi i)^k}{(k - 1)!} \sum_{m=1}^{\infty} m^{k-1} q^{-m}
\]

2. For any complex number \(x \in \mathbb{C}\) with \(|x| < 1\) the geometric series is absolutely convergent satisfying

\[
\sum_{d=0}^{\infty} x^d = \frac{1}{1-x}
\]

Taking the derivative and multiplying by \(x\) shows

\[
\sum_{d=1}^{\infty} d \cdot x^d = \frac{x}{(1-x)^2}.
\]

For \(m \geq 1\) set \(x = q^m\) with \(|q| = e^{-2\pi \text{Im } \tau} < 1\) gives
3.2 Eisenstein series and the algebra of modular forms of $\Gamma$

$$\sum_{m=1}^{\infty} \left( \sum_{d=1}^{\infty} d \cdot q^{md} \right) = \sum_{m=1}^{\infty} \left( \sum_{d=1}^{\infty} d \cdot (q^m)^d \right) = \sum_{m=1}^{\infty} \frac{q^m}{(1-q^m)^2}.$$ 

The last series is absolutely convergent because for fixed $q$

$$\lim_{m \to \infty} |1 - q^m|^2 = 1.$$

3. We split the summation $\sum_{m \in \mathbb{Z}^*}$ into

$$\sum_{m < 0 \text{ where } \text{Im}(m\tau) < 0}$$

and

$$\sum_{m > 0 \text{ where } \text{Im}(m\tau) > 0}.$$

Part 1) justifies the second equality sign, and note $k \geq 2$ even:

$$\sum_{m \in \mathbb{Z}^*} \left( \sum_{n \in \mathbb{Z}^*} \frac{1}{(m\tau + n)^k} \right) = \sum_{m < 0} \left( \sum_{n \in \mathbb{Z}} \frac{1}{(m\tau + n)^k} \right) + \sum_{m > 0} \left( \sum_{n \in \mathbb{Z}} \frac{1}{(m\tau + n)^k} \right) =$$

$$\frac{(2\pi i)^k}{(k-1)!} \left( \sum_{m < 0} \left( \sum_{r=1}^{\infty} r^{k-1} \cdot q^{-rm} \right) + \sum_{m > 0} \left( \sum_{r=1}^{\infty} r^{k-1} \cdot q^r \right) \right) =$$

$$= 2 \cdot \frac{(2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} \left( \sum_{r=1}^{\infty} r^{k-1} \cdot q^m \right).$$

For $k \geq 4$ any rearrangement is permitted. For $k = 2$ the last series is absolutely convergent according to part 2). We rearrange the series by changing the indices of summation from $(m,r)$ to $(n = rm, d|n)$:

$$\sum_{m=1}^{\infty} \left( \sum_{r=1}^{\infty} r^{k-1} \cdot q^m \right) = \sum_{n=1}^{\infty} \left( \sum_{d|n} d^{k-1} \cdot q^n \right) = \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n, \text{ q.e.d.}$$

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

$$\sum_{m=1}^{\infty} \left( \sum_{d=1}^{\infty} d \cdot q^{md} \right) = \sum_{m=1}^{\infty} \left( \sum_{d=1}^{\infty} d \cdot (q^m)^d \right) = \sum_{m=1}^{\infty} \frac{q^m}{(1-q^m)^2}.$$
The algebra of modular forms

\[ G_k(\tau) := \sum_{(c,d) \in \mathbb{Z}^2} \frac{1}{(c\tau + d)^k} \]

is absolutely and compactly convergent for \( \tau \in \mathbb{H} \).

The series defines a modular form \( G_k \) of \( \Gamma \) of weight \( k \) with

\[ G_k(\infty) = 2\zeta(k). \]

Here

\[ \zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \text{Re} \ s > 1, \]

denotes the Riemann \( \zeta \)-function.

2. The Eisenstein series \( G_k \in M_k(\Gamma) \) has the Fourier expansion

\[ G_k(\tau) = 2\zeta(k) + 2 \cdot \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_k-1(n) \cdot q^n, \quad q = e^{2\pi i \tau}. \]

**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 \( G_{\Lambda_\tau,k} \) is absolute convergent due to Lemma 1.11, hence allows arbitrary rearrangement. With respect to the translation

\[ T : \mathbb{H} \rightarrow \mathbb{H}, \ \tau \mapsto T(\tau) := \tau + 1, \]

we obtain

\[ G_k(\tau) = G_k(\tau + 1). \]

With respect to the reflection

\[ S : \mathbb{H} \rightarrow \mathbb{H}, \ \tau \mapsto S(\tau) := \frac{-1}{\tau} \]

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 \( \tau \in \mathbb{H} \)

\[ G_k(\tau) = G_k(\gamma(\tau)) \cdot h(\gamma, \tau)^{-k}, \quad \text{i.e.} \ G_k = G_k[\gamma]^k \]
ii) **Holomorphy:** The lattice constant 

\[ G_{\lambda, k} \lambda = e^{2\pi i/3}, \]

dominates the Eisenstein series and shows its compact convergence on \( \mathcal{D} \): We obtain for \( \tau \in \mathcal{D} \) and \( c, d \in \mathbb{Z} \) using \( |\tau| \geq 1 \) and \( |\text{Re} \ \tau| \leq 1/2 \)

\[ |c \cdot \tau + d|^2 = c^2|\tau|^2 + 2cd \cdot \text{Re} \ \tau + d^2 \geq \]

\[ \geq \begin{cases} 
  c^2 - cd + d^2 & cd \geq 0 \\
  c^2 + cd + d^2 & cd < 0 
\end{cases} \]

\[ = \begin{cases} 
  |c \cdot \rho + d|^2 & cd \geq 0 \\
  |c \cdot \rho - d|^2 & cd < 0 
\end{cases} \]

Therefore

\[ \sum_{(c,d) \in \mathbb{Z}^2} \frac{1}{|c \tau + d|^k} \leq \sum_{(c,d) \in \mathbb{Z}^2} \frac{1}{|c \rho + d|^k} + \sum_{(c,d) \in \mathbb{Z}^2} \frac{1}{|c \rho - d|^k} = \]

\[ = 2 \cdot \sum_{(c,d) \in \mathbb{Z}^2} \frac{1}{|c \rho + d|^k} < \infty \]

Hence the restriction \( G_k|\mathcal{D} \) is absolutely and uniformly convergent. Each summand of \( G_k \) is holomorphic in \( \mathbb{H} \). Therefore \( G_k|\mathcal{D} \) is holomorphic. For any \( \gamma \in \Gamma \) and \( \tau \in \gamma(\mathcal{D}) \)

\[ G_k(\tau) = G_k(\gamma^{-1}(\tau)) \cdot \text{h}(\gamma^{-1}, \tau)^{-k} \]

and

\[ \text{h}(\gamma^{-1}, \tau) \]

is holomorphic with respect to \( \tau \). As a consequence, the restriction \( G_k|\gamma(\mathcal{D}) \) is holomorphic. The representation

\[ \mathbb{H} = \bigcup_{\gamma \in \Gamma} \gamma(\mathcal{D}) \]

shows that \( G_k : \mathbb{H} \rightarrow \mathbb{C} \) is holomorphic.

iii) **Fourier expansion:** 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

\[ G_k(\tau) = \sum_{(c,d) \in \mathbb{Z}^2} \frac{1}{|c \tau + d|^k} = \sum_{d \in \mathbb{Z}^*} \frac{1}{d^k} + \sum_{c \in \mathbb{Z}, d \in \mathbb{Z}} \frac{1}{(c \tau + d)^k} = \]

\[ = 2\zeta(k) + 2 \left( \frac{2\pi i}{k-1} \right)^k \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n , \quad q = e^{2\pi i \tau}. \]
The Fourier expansion, a convergent power series, proves the holomorphy of \( G_k \) in \( \mathbb{H} \) and at the point \( \infty \), 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 \( \zeta \)-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

\[
E_k(\tau) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n \in M_k(\Gamma), \quad q = e^{2\pi i \cdot \tau}
\]

**Proof.**

1. **Euler relation of Bernoulli numbers**: See [20, Kap. VII, Satz 4.1]. We relate the cotangent function to the Bernoulli numbers. 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 \( \geq 3 \) and \( B_0 = 1, \ B_1 = -1/2 \)

\[
z \cdot \cot z = iz + \frac{2iz}{e^{2iz} - 1} = iz + 1 - \frac{2iz}{2} + \sum_{\mu=1}^{\infty} \frac{B_{2\mu}}{(2\mu)!} \cdot (2iz)^{2\mu} = 1 + \sum_{\mu=1}^{\infty} (-1)^{\mu} \cdot \frac{2\mu}{(2\mu)!} \cdot B_{2\mu} \cdot z^{2\mu}
\]

- On one hand from the definition of the Bernoulli numbers - replacing \( z \) by \( \pi z \) -

\[
\pi z \cdot \cot(\pi z) = 1 + \sum_{\mu=1}^{\infty} (-1)^{\mu} \cdot \frac{2\mu}{(2\mu)!} \cdot \pi^{2\mu} \cdot B_{2\mu} \cdot z^{2\mu}
\]

- On the other hand the partial fraction of the cotangent function

\[
\pi z \cdot \cot(\pi z) = 1 + z \sum_{v=1}^{\infty} \frac{2z}{\pi^2 - v^2}
\]
and the geometric series
\[
\frac{1}{z^2 - \nu^2} = \frac{1}{\nu^2} \sum_{\mu=0}^{\infty} \left( \frac{\nu^2}{\nu^2} \right)^\mu
\]
implies
\[
\pi z \cdot \cot(\pi z) = 1 + 2z^2 \sum_{v=1}^{\infty} \left( -\frac{1}{\nu^2} \sum_{\mu=0}^{\infty} \left( \frac{\nu^2}{\nu^2} \right)^\mu \right)
\]
\[
= 1 - 2 \sum_{\mu=1}^{\infty} \left( \sum_{v=1}^{\infty} \frac{1}{\nu^2 \mu} \right) z^{2\mu}
\]
Comparing the coefficients of both series representing
\[
\pi z \cdot \cot(\pi z)
\]
implies the Euler relation
\[
2 \cdot \zeta(2\mu) := 2 \sum_{v=1}^{\infty} \frac{1}{\nu^{2\mu}} = (-1)^{\mu+1} \frac{2^{2\mu}}{(2\mu)!} \cdot \pi^{2\mu} \cdot B_{2\mu}
\]
2. \emph{Rationality of the Fourier coefficients}: The Fourier expansion of the Eisenstein series \( G_k \) from Theorem 3.9 and Part 1) show
\[
E_k(\tau) := \frac{G_k(\tau)}{2\zeta(k)} = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) \cdot q^n \in M_k(\Gamma).
\]
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
\[
(2, \pi^2/6, 1/6, -24) \quad (4, \pi^4/(2 \cdot 3^2 \cdot 5), -1/30, 240)
\]
(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 \( k \geq 2 \) the Eisenstein series \( G_k \) relate to the lattice constants \( G_{A,k} \) 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

\[ G_{A,k} = \frac{1}{\omega_1^k} G_k(\tau). \]

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

\[ G_2(\tau) = 2 \cdot \zeta(2) - 8\pi^2 \sum_{n=1}^{\infty} \sigma_1(n) \cdot q^n, \quad q = e^{2\pi i \tau}. \]

The equality

\[ \zeta(2) = \frac{\pi^2}{6} \]

implies for the normalized Eisenstein series of weight \( k = 2 \)

\[ E_2(\tau) := G_2(\tau) \frac{1}{2\xi(2)} = 1 - 24 \sum_{n=1}^{\infty} \sigma_1(n) \cdot q^n, \quad q = e^{2\pi i \tau}. \]

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

\[ (G_2[\gamma]_2)(\tau) = G_2(\tau) - 2\pi ic \cdot h(\gamma, \tau)^{-1} \]

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 \( \Gamma \) of weight \( k = 12 \) defined as

\[ \Delta := g_2^3 - 27 \cdot g_3^2 : \mathbb{H} \rightarrow \mathbb{C} \]

derived from the Eisenstein series

\[ g_2 := 60 \cdot G_4, \quad g_3 := 140 \cdot G_6. \]

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 \( \tau \) of a given normalized lattice.
\[ \Lambda = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau. \]

**Proposition 3.14 (Fourier coefficients of the discriminant form).** All Fourier coefficients of the normalized discriminant form

\[ \Delta \in M_{12}(\Gamma) \]

are integers:

\[ \Delta(q) = \sum_{n=0}^{\infty} \tau_n \cdot q^n \in \mathbb{Z}\{q\}, \quad q = e^{2\pi i \cdot \tau}, \]

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 5.29.

**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

\[ g_2 = 60 \cdot G_4 = \frac{2^2}{3} \cdot \pi^4 \cdot E_4 \quad \text{and} \quad g_3 = 140 \cdot G_6 = \frac{2^3}{3^3} \cdot \pi^6 \cdot E_6. \]

Hence

\[ \Delta = g_2^3 - 3g_3^2 = \pi^{12} \cdot \frac{2^6}{3^3}(E_4^3 - E_6^2) = (2\pi)^{12} \cdot \frac{E^3_4 - E^2_6}{2^6 \cdot 3^3} = (2\pi)^{12} \cdot \frac{E^3_4 - E^2_6}{1728} \]

and eventually

\[ \Delta = \frac{E^3_4 - E^2_6}{2^6 \cdot 3^3} = \frac{E^3_4 - E^2_6}{1728}. \]

We set as shorthand

\[ X_k(q) := \sum_{n=1}^{\infty} \sigma_k(n) \cdot q^n \]

and obtain
3.2 Eisenstein series and the algebra of modular forms of $\Gamma$

\[
\Delta \frac{1}{(2\pi)^{12}} = \frac{(1 + 240 \cdot X_3)^3 - (1 - 504 \cdot X_3)^3}{2^6 \cdot 3^3}
\]

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
\[ d \in \{1, 2\} \subset \mathbb{Z}/3\mathbb{Z} = \{0, 1, 2\} \quad \text{and} \quad d \in \{1, 3\} \subset \mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}, \]
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

\[
j : X(1) \xrightarrow{\sim} \mathbb{P}^1
\]
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 \( \Delta \) 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 \( \infty \). Because \( j \) is even an automorphic function, it is a meromorphic function on the modular curve, i.e. a holomorphic map

\[
j : X(1) \xrightarrow{\sim} \mathbb{P}^1.
\]
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 \( D \in \text{Div}(X) \), and also Serre duality, see [63]:

\[
\dim H^0(X, \mathcal{O}_D) - \dim H^1(X, \mathcal{O}_D) = 1 - g(X) + \deg D.
\]

We will use also the notation

\[
\deg \mathcal{O}_D := \deg D.
\]

The canonical divisor \( K \in \text{Div}(X) \) has degree

\[
\deg K = 2g(X) - 2.
\]

Serre-duality allows to replace the cohomology group \( H^1 \) by the dual of a cohomology group \( H^0 \)

\[
H^1(X, \mathcal{O}_D) = H^0(X, \mathcal{O}_{K-D})^\vee.
\]

Moreover, for each divisor \( D \in \text{Div}(X) \) with \( \deg D < 0 \)

\[
\dim H^0(X, \mathcal{O}_D) = 0.
\]

• 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 4.27.

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

\[
\alpha : M_k(\Gamma) \to H^0\left(X, \mathcal{M} \otimes_{\mathcal{O}} \Omega^{\otimes k/2}\right), \ f \mapsto \omega_f,
\]

with \( \omega_f \) the well-defined meromorphic differential form on \( X \) induced by the \( \Gamma \)-invariant modular form on \( \mathbb{H} \).
2. The distinguished divisor: Consider the divisor

$$D_k := \left\lfloor \frac{k}{3} \right\rfloor \cdot \mathfrak{d} + \left\lfloor \frac{k}{3} \right\rfloor \cdot \mathfrak{p} + \frac{k}{2} \cdot \mathfrak{m} \in \text{Div}(X).$$

The attachment

$$U \mapsto \Omega_{\Gamma,k}(U), \ U \subset X \text{ open},$$

with

$$\Omega_{\Gamma,k}(U) := \left\{ \omega \in H^0(U, \mathcal{M} \otimes \mathcal{O}^{\otimes k/2}) : \omega \neq 0 \text{ and } \text{div } \omega \geq -D_k|U \right\} \cup \{0\}$$

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.
  $$\Omega_{\Gamma,k} \subset \mathcal{M} \otimes \mathcal{O}^{\otimes k/2}$$
- and is isomorphic to the line bundle

$$\mathcal{L}_{\Gamma,k} := \mathcal{O}(k/2) \cdot K + D_k \in \text{Pic}(X)$$

of multiples of the divisor $-(k/2) \cdot K + D_k \in \text{Div}(X)$ with $K \in \text{Div}(X)$ the canonical divisor of $X$.

3. Meromorphic differential forms on the modular curve: The image of the map $\alpha$ 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 $\mathcal{L}_{\Gamma,k}$.

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 $\alpha$: 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 $\omega_f$ on $X$ with pullback

$$f(\tau) \ (d\tau)^{k/2} := p^* \omega_f$$

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 $\omega_f$ at $[t] \in X$: 

$$\frac{k}{2} \cdot [t] \cdot \mathfrak{m} \in \text{Div}(X).$$
3.2 Eisenstein series and the algebra of modular forms of $\Gamma$

$$ord_t f = \begin{cases} 
ord_{\infty} \omega_f + k/2 & t = \infty \\
h_t \cdot ord_t \omega_f + (k/2) \cdot (h_t - 1) & t \in \mathbb{H} 
\end{cases}$$

Here $h_t$ denotes the period of $t$. The order of a meromorphic differential form

$$\omega \in H^0 \left( X, \mathcal{M} \otimes \Omega^{\otimes k/2} \right)$$

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 $\tau$ 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 $pow_\infty$ around $t$ and the chart $\phi_\infty$ around the cusp $[\infty]$ from the diagram

\[
\begin{array}{ccc}
U_\infty & \xrightarrow{p^*} & p^*(U_\infty) \\
\downarrow & & \downarrow \\
pow_\infty & \xrightarrow{} & \phi_\infty \\
\downarrow & & \downarrow \\
W_\infty & &
\end{array}
\]

For $\tau \in U_\infty$

$$q(\tau) := pow(\tau) := \begin{cases} 
eq \infty, \\
0 & \tau = \infty.
\end{cases}$$

Then

$$dq = 2\pi i q \ d\tau$$

and

$$\left( dq \right)^{k/2} = \left( 2\pi i \right)^{k/2} q^{k/2} \ (d\tau)^{k/2}$$

which implies

$$\left( d\tau \right)^{k/2} = \frac{1}{\left( 2\pi i \right)^{k/2}} \frac{(dq)^{k/2}}{q^{k/2}}$$

From
\begin{align*}
f(\tau) \cdot (d\tau)^{k/2} &= p^*(\omega_f)(\tau)\\
\text{one obtains by expressing } \omega_f \text{ in } \tau\text{-coordinates}\\
\omega_f(q(\tau)) &= f(q(\tau)) \cdot (d\tau)^{k/2}
\end{align*}

respectively in \( q \)-coordinates
\[
\omega_f(q) = \hat{f}(q) \cdot \frac{1}{(2\pi i)^{k/2}} \cdot \frac{(dq)^{k/2}}{q^{k/2}}
\]

It proves
\[
\operatorname{ord}_\infty \omega_f = \operatorname{ord}_0 \hat{f} - k/2 = \operatorname{ord}_\infty f - k/2
\]

using the definition
\[
\operatorname{ord}_\infty f := \operatorname{ord}_0 \hat{f}
\]

\begin{itemize}
  \item For \( t \in \{i, \rho\} \) we recall the chart \( \phi_t \) from the following diagram
\end{itemize}

\[
\begin{array}{cccc}
  U_t & \xrightarrow{p|U_t} & p(U_t) \\
  \downarrow \lambda_t & & \downarrow \phi_t \\
  \Delta_t & \xrightarrow{\text{pow}_t} & W_t
\end{array}
\]

The map
\[
\lambda_t : U_t \xrightarrow{\sim} \Delta_t
\]
is biholomorphic. For the order calculation we assume w.l.o.g.
\[
\lambda_t = \text{id} \text{ and } U_t = \Delta_t
\]
The isotropy group \( \Gamma_t \) acts on \( U_t \) by multiplication by an \( e \)-th root of unity with
\[
e := h_t
\]
For \( \tau \in U_t \)
\[
q(\tau) := \text{pow}_t(\tau) := \tau^e
\]
Therefore
\[
dq = e \cdot \tau^{e-1} d\tau \text{ and } (dq)^{k/2} = e^{k/2} \cdot \tau^{(k/2)(e-1)} (d\tau)^{k/2}
\]
If
\[
\omega_f(q) = g(q) \cdot (dq)^{k/2}
\]
then
\[ (p^* \omega_f)(\tau) = \omega_f(q(\tau)) = g(q(\tau)) \cdot e^{k/2} \cdot \tau^{(k/2) \cdot (e-1)} \cdot (d\tau)^{k/2} = f(\tau) \cdot (d\tau)^{k/2} \]

As a consequence
\[ f(\tau) = g(q(\tau)) \cdot \tau^{(k/2) \cdot (e-1)} \cdot e^{k/2} \]

By definition
\[ \text{ord}_{p|} \omega_f = \text{ord}_{p|} g \]

Hence
\[ \text{ord}_f \omega_f = e \cdot \text{ord}_{p|} g + (k/2) \cdot (e-1) = e \cdot \text{ord}_{p|} \omega_f + (k/2) \cdot (e-1) = h_1 \cdot \text{ord}_{p|} \omega_f + (k/2) \cdot (h_1 - 1) \]

Summing up
\[ \text{ord}_f \omega_f = \text{ord}_{p|} \omega_f \text{ if } t \in \mathcal{D} \setminus \{i, \rho, \infty\} \]
\[ \text{ord}_f = 2 \cdot \text{ord}_{p|} \omega_f + k/2 \]
\[ \text{ord}_f = 3 \cdot \text{ord}_{p|} \omega_f + k \]
\[ \text{ord}_f = \text{ord}_{\infty} \omega_f + k/2 \]

or, because for all \( t \in \mathbb{H}^* \) holds \( \text{ord}_f \geq 0 \):
\[ \text{ord}_{p|} \omega_f = \text{ord}_f \geq 0 \text{ if } t \in \mathcal{D} \setminus \{i, \rho, \infty\} \]
\[ \text{ord}_{p|} \omega_f = 1/2 \cdot \text{ord}_f - k/4 \geq -k/4, \text{ hence } \text{ord}_{p|} \omega_f \geq -|k/4| \]
\[ \text{ord}_{p|} \omega_f = 1/3 \cdot \text{ord}_f - k/3, \text{ hence } \text{ord}_{p|} \omega_f \geq -|k/3| \]
\[ \text{ord}_{\infty} \omega_f = \text{ord}_f - k/2, \text{ hence } \text{ord}_{\infty} \omega_f \geq -k/2 \]

which finishes the proof of the order relations. As a consequence
\[ \alpha(M_k(\Gamma)) = \left\{ \omega \in H^0 \left( X, \mathcal{M} \otimes \Omega^{\otimes k/2} \right) : \text{div} \ \omega \geq -\left[ \frac{k}{4} \cdot |i| - \left[ \frac{k}{3} \cdot |\rho| - \frac{k}{2} \cdot |\infty| \right] \right] \right\} \]

Conversely, each \( \omega \in H^0(X, \Omega_{\Gamma,k}) \) defines the modular form \( f \in M_k(\Gamma) \) with
\[ f(\tau) \cdot (d\tau)^{k/2} = p^* \omega \]

iii) Line bundle: It is well known that the sheaves of multiples of a divisor are line bundles, 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 \( \omega_f \) on the modular curve \( X \) may have poles. Actually, it is the divisor of \( \omega_f \) which encodes the information about \( f \).
In the language of line bundles, modular forms of weight $= k$ are the sections of the line bundle $\mathcal{L}_{\Gamma, k}$ on the modular curve:

$$M_k(\Gamma) \simeq \mathcal{H}^0(X, \mathcal{L}_{\Gamma, k})$$

**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

$$\text{ord}_\tau f \geq 0, \ \tau \in \mathbb{H}, \ \text{and} \ \text{ord}_\infty f \geq 1.$$

The order relations from Theorem 3.17 imply

$$\omega_f := \alpha(f) \in \mathcal{H}^0(X(1), \Omega_{\Gamma, 2})$$

satisfies for $\tau \in \mathcal{D} \setminus \{[i], [\rho], [\infty]\}$

$$\text{ord}_\tau \omega_f = \text{ord}_\tau f \geq 0$$

and for $k = 2$

$$\text{ord}_i \omega_f = (1/2)(\text{ord}_i f - 1) \geq -(1/2), \ \text{hence} \ \text{ord}_i \omega_f \geq 0$$

$$\text{ord}_\rho \omega_f = (1/3)(\text{ord}_\rho f - 2) \geq -(2/3), \ \text{hence} \ \text{ord}_\rho \omega_f \geq 0$$

$$\text{ord}_\infty \omega_f = \text{ord}_\infty f - 1 \geq 0$$

Therefore

$$\Omega_{\Gamma, 2} \simeq \Omega$$

and $\omega_f$ is holomorphic, i.e.

$$\omega_f \in \mathcal{H}^0(X, \Omega)$$

The group $\mathcal{H}^0(X, \Omega)$ vanishes because

$$\dim \mathcal{H}^0(X, \Omega) = g(X) = g(\mathbb{P}^1), \ q.e.d.$$

2. The formula generalizes to Hecke congruence subgroups as the isomorphy of vector spaces:

$$S_2(\Gamma_0(N)) \simeq \mathcal{H}^0(X_0(N), \Omega)$$
3.2 Eisenstein series and the algebra of modular forms of \( \Gamma \)

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:

\[
\dim M_k(\Gamma) = \begin{cases} 
  \lfloor k/12 \rfloor & k \equiv 2 \mod 12 \\
  \lfloor k/12 \rfloor + 1 & \text{otherwise}
\end{cases}
\]

For the dimension of the vector space \( S_k(\Gamma) \) of cusp forms see Lemma 3.23.

**Proof.** We have \( M_k(\Gamma) \cong H^0(X, \mathcal{L}_T)^k \).

For \( k = 0 \) we have on the compact Riemann surface \( X \cong \mathbb{P}^1 \)

\[
\dim M_0(\Gamma) = \dim H^0(X, \mathcal{O}) = 1.
\]

Therefore we are left with even \( k > 0 \):

i) **Serre duality and Riemann-Roch theorem:** By Serre-duality for each \( k > 0 \)

\[
\dim H^1(X, \mathcal{L}_T^\vee \otimes \mathcal{O}_K) = \dim H^0(X, \mathcal{O}(k/2) - D_k + K)
\]

Now

\[
\deg (- (k/2) \cdot K - D_k + K) = ((k/2) - 2) - [k/4] - [k/3] \leq ((k/2) - 2) - ((k/4) - 1) - ((k/3) - 1) = k/2 - k/4 - k/3 = k/2 - 1/4 - 1/3 < 0
\]

As a consequence

\[
0 = \dim H^0(X, \mathcal{L}_T^\vee \otimes \mathcal{O}_K) = \dim H^1(X, \mathcal{L}_T^\vee)
\]

The Riemann-Roch theorem implies for \( \mathcal{L}_{T,k} = \mathcal{O}_{(k/2)K + D_k} \)

\[
\dim M_k(\Gamma) = \dim H^0(X, \mathcal{L}_{T,k}) = 1 - g(X) + (k/2)(-2) + [k/4] + [k/3] + k/2 = 1 - k + [k/4] + [k/3] + k/2 = 1 - (k/2) + [k/3] + [k/4]
\]

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 \( \beta \)
$$1 - (k/2) + [k/3] + [k/4]$$

- **Residue $\beta = 0$:**
  $$1 - 6\alpha + 4\alpha + 3\alpha = 1 + \alpha = 1 + [k/12]$$

- **Residue $\beta = 2$:**
  $$1 - (6\alpha + 1) + [4\alpha + 2/3] + [3\alpha + 2/4] = 1 - (6\alpha + 1) + 4\alpha + 3\alpha = \alpha = [k/12]$$

- **Residue $\beta = 4$:**
  $$1 - (6\alpha + 2) + [4\alpha + 4/3] + [3\alpha + 1] = 1 - 2 + 1 + \alpha = \alpha + 1 = 1 + [k/12]$$

- **Residue $\beta = 6$:**
  $$1 - (6\alpha + 3) + [4\alpha + 6/3] + [3\alpha + 6/4] =$$
  $$= 1 - (6\alpha + 3) + (4\alpha + 2) + 3\alpha + 1 = 1 + \alpha = 1 + [k/12]$$

- **Residue $\beta = 8$:**
  $$= 1 - (6\alpha + 4) + [4\alpha + 8/3] + [3\alpha + 8/4] =$$
  $$= 1 - (6\alpha + 4) + (4\alpha + 2) + (3\alpha + 2) = 1 + \alpha = 1 + [k/12]$$

- **Residue $\beta = 10$:**
  $$1 - (6\alpha + 5) + [4\alpha + 10/3] + [3\alpha + 10/4] =$$
  $$= 1 - (6\alpha + 5) + (4\alpha + 4) + (3\alpha + 2) = 1 + \alpha = 1 + [k/12]$$

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 $\Delta$.

Apparently the numerical value $\dim H^0(X, \mathcal{L}_f, k)$ 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 $\mathcal{L}$ is determined by its degree $m$, and for $m \geq 0$

$$\dim H^0(\mathbb{P}^1, \mathcal{L}) = m + 1.$$
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:

\[
\text{ord}_\infty f + \frac{1}{2} \text{ord}_i f + \frac{1}{3} \text{ord}_\rho f + \sum' \text{ord}_\tau f = \frac{k}{12}
\]

Here the symbol \( \sum' \) denotes the summation over all points \( \tau \in \mathcal{D} \setminus \{i, \rho, \infty\} \).

**Proof.** We recall the relation between the order of \( f \in M_k(\Gamma) \) at a point \( \tau \) and the order of the differential form \( \omega_f \in H^0(X, \mathcal{M} \otimes \Omega^{\otimes k/2}) \) at the point \([\tau] \in X\) established during the proof of Theorem 3.17:

\[
\begin{align*}
\text{ord}_\infty f &= \text{ord}_{[\infty]} \omega_f + k/2 \\
\text{ord}_i f &= 2 \text{ord}_{[i]} \omega_f + k/2 \\
\text{ord}_\rho f &= 3 \text{ord}_{[\rho]} \omega_f + k \\
\text{ord}_\tau f &= \text{ord}_{[\tau]} \omega_f, \quad \tau \in \mathcal{D} \setminus \{i, \rho, \infty\}.
\end{align*}
\]

The modular curve \( X \) has genus \( g = 0 \) according to Corollary 3.16. The line bundle \( \Omega^{\otimes k/2} \) has degree

\[(2g - 2)(k/2) = -k.\]

Therefore

\[
\text{deg div } (\omega_f) = -k.
\]

\[
\text{ord}_\infty f + \frac{1}{2} \text{ord}_i f + \frac{1}{3} \text{ord}_\rho f + \sum' \text{ord}_\tau f = \left( \text{ord}_{[\infty]} \omega_f + \frac{k}{2} \right) + \left( \text{ord}_{[i]} \omega_f + \frac{k}{4} \right) + \left( \text{ord}_{[\rho]} \omega_f + \frac{k}{3} \right) + \sum' \text{ord}_{[\tau]} \omega_f = \text{deg div } (\omega) + \frac{k}{2} + \frac{k}{4} + \frac{k}{3} - k + \frac{k}{2} + \frac{k}{4} + \frac{k}{3} \quad \text{q.e.d.}
\]

**Corollary 3.21 (Specific values and Fourier coefficients of the modular invariant \( j \)).**

1. The modular invariant

\[
j : X(1) \to \mathbb{P}^1
\]

attains the distinguished values
The algebra of modular forms

\[ j([\bar{\rho}]) = 1728 \text{ and } j([\rho]) = 0. \]

2. All Fourier coefficients \((b_n)_{n \geq -1}\) 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 \(G_6(\rho) = 0\). The definition

\[ j = 1728 \cdot \frac{g_2^3}{g_2^3 - 27g_3^2} \]

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

\[ \frac{\Delta(\tau)}{(2\pi)^{12}} = \sum_{n=1}^{\infty} \tau_n \cdot q^n \in \mathbb{Z}[q], \quad q = e^{2\pi i \tau}. \]

We obtain

\[ j = \left(2^6 \cdot 3^3\right) \cdot \frac{g_2^3}{\Delta} = \left(2^6 \cdot 3^3\right) \cdot \left(\frac{2^6}{3^3} E_4^3 \cdot \pi^{12}\right) \cdot \frac{1}{\Delta} = \]

\[ = \frac{E_4^3}{\Delta / (2\pi)^{12}} = \sum_{n=1}^{\infty} \tau_n \cdot q^n = \frac{1}{q} \cdot \frac{E_4^3}{1 + \sum_{n=2}^{\infty} \tau_n \cdot q^{n-1}} = \]

\[ = \frac{1}{q} \cdot E_4^3 \cdot \sum_{m=0}^{\infty} \left((-1)^m \cdot \sum_{n=2}^{\infty} \tau_n \cdot q^{n-1}\right)^m \]

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 coefficients, q.e.d.
3.2 Eisenstein series and the algebra of modular forms of $\Gamma$

**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
   \[ f(\tau) = \sum_{n \geq -k} c_n \cdot q^n, \quad c_{-k} \neq 0, \]
   for a suitable $k \in \mathbb{N}$, then a polynomial $P(X) \in \mathbb{C}[X]$ 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 $k \rightarrow k$ consider the function
   \[ g := f - c_{-k} \cdot j^k. \]
   The function $g$ has at most a pole of order $= k - 1$ at $\infty$. Therefore the induction assumption applies to $g$.

2. Each automorphic function $f \in A_0(\Gamma)$ can be considered a meromorphic function $f \in \mathcal{M}(\mathbb{P}^1)$ on the projective space. Denote by
   \[ A := \{x_1, \ldots, x_n\} \subset \mathbb{H} \cup \{\infty\} \text{ and } B = \{y_1, \ldots, y_n\} \subset \mathbb{H} \cup \{\infty\} \]
   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
   \[ g := \prod_{v=1}^n \frac{j - f(x_v)}{j - f(y_v)} \in A_0(\Gamma) \]
   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
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 \( \Delta \) defines a vector space isomorphism
\[ \mu_\Delta : M_{k-12}(\Gamma) \xrightarrow{\cong} S_k(\Gamma). \]
• 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 \( \varepsilon \) 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 \( \Delta \) has no zero on \( \mathbb{H} \) due to Proposition 1.19. In addition \( g \) is holomorphic at the point \( \infty \) because \( \Delta \) has a zero of order 1 at \( \infty \) according to Proposition 3.14. Hence \( g \in M_{k-12}(\Gamma) \). In addition, the composition
\[ \varepsilon \circ \mu_\Delta = 0 \]
is obvious.
3.2 Eisenstein series and the algebra of modular forms of $\Gamma$

iii) Exactness on the left-hand side: Apparently the map $\mu_\Delta$ 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

$$M_\ast(\Gamma) := \left( \bigoplus_{k \geq 0} M_{2k}(\Gamma), +, \cdot \right)$$

of modular forms of the module group $\Gamma$ 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

$$S_\ast(\Gamma) := \bigoplus_{k \geq 0} S_{2k}(\Gamma) \subset M_\ast(\Gamma)$$

is a principal ideal generated by $\Delta \in S_{12}(\Gamma)$.

**Proof.** 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

$$G_4^\alpha \cdot G_6^\beta \in M_k \text{ and } e \left( G_4^\alpha \cdot G_6^\beta \right) \neq 0$$
Consider an arbitrary element \( f \in M_k \). For suitable \( \lambda \in \mathbb{C} \)
\[
e \left( f - \lambda \cdot G^\alpha_4 \cdot G^\beta_6 \right) = \left( f - \lambda \cdot G^\alpha_4 \cdot G^\beta_6 \right)(\infty) = 0.
\]
According to Lemma 3.23 an element \( g \in M_{k-12} \) exists with
\[
f - \lambda \cdot G^\alpha_4 \cdot G^\beta_6 = \Delta \cdot g.
\]
The claim follows by repeating the argument with \( g \in M_{k-12}(\Gamma) \), and using
\[
M_4(\Gamma) = \mathbb{C} \cdot G^4_4 \quad \text{and} \quad M_6(\Gamma) = \mathbb{C} \cdot G^6_6
\]
due to Corollary 3.19.

ii) \textit{Freely generated}: The generators \( G^4_4 \) and \( G^6_6 \) are even algebraically independent.
Assume the existence of a polynomial \( P \in \mathbb{C}[T_1, T_2] \) with
\[
P(G^4_4, G^6_6) = 0.
\]
We may assume that all monomials of \( P(G^4_4, G^6_6) \) have the same weight. The case
\[
P(G^4_4, G^6_6) = a \cdot G^m_4 + G^6_6 \cdot \hat{P}(G^4_4, G^6_6), \quad a \in \mathbb{C}^* \]
is excluded because \( G^4_4(i) \neq 0 \), but \( G^6_6(i) = 0 \). Analogously the case
\[
P(G^4_4, G^6_6) = b \cdot G^m_6 + G^4_4 \cdot \hat{P}(G^4_4, G^6_6), \quad b \in \mathbb{C}^* \]
is excluded because \( G^6_6(\rho) \neq 0 \), but \( G^4_4(\rho) = 0 \). Hence the product \( G^4_4 G^6_6 \) divides \( P(G^4_4, G^6_6) \), i.e.
\[
P(G^4_4, G^6_6) = G^4_4 G^6_6 \cdot \hat{P}(G^4_4, G^6_6) = 0.
\]
Iteration of the argument for
\[
\hat{P}(G^4_4, G^6_6) = 0 \quad \text{with} \quad \deg \hat{P} < \deg P
\]
proves \( P = 0 \) by descending induction.

iii) \textit{Ideal of cusp forms}: According to Lemma 3.23 any cusp form is a multiple of \( \Delta \), 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
3.3 Generalization to Hecke congruence subgroups $\Gamma_0(N)$

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

$$\deg f = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

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

$$D_k := \left\lfloor \frac{k}{4} \right\rfloor \cdot \sum_{x \in X_0(N), \ell_{x} = 2} x + \left\lfloor \frac{k}{3} \right\rfloor \cdot \sum_{x \in X_0(N), \ell_{x} = 3} x + \frac{k}{2} \cdot \sum_{x \in \text{Div}(X_0(N)), \text{cusp}} x \in \text{Div}(X_0(N)), \text{ even } k \geq 0.$$  

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

$$H^0\left(X_0(N), \mathcal{M} \otimes \Omega \otimes \mathcal{O}^{\otimes k/2}\right)$$

which arise from modular forms under the canonical injection

$$\alpha : M_k(\Gamma_0(N)) \to H^0\left(X_0(N), \mathcal{M} \otimes \mathcal{O} \otimes \Omega^{\otimes k/2}\right), \quad g \mapsto \omega_g,$$

with $\omega_g$ 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 $\alpha$: The map

$$\alpha : M_k(\Gamma_0(N)) \to H^0 \left( X_0(N), \mathcal{M} \otimes \Omega^{\otimes k/2} \right), \ g \mapsto \omega_g,$$

with $\omega_g$ 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

$$ord_{\tau} g = \begin{cases} 
\text{ord}_{\tau} \omega_g + k/2 & \text{[\tau] cusp} \\
\tau \cdot \text{ord}_{\tau} \omega_g + k/2 \cdot (\tau - 1) & \tau \in \mathbb{H} 
\end{cases}$$

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

$$\omega_g \in H^0 \left( Y_0(N), \mathcal{M} \otimes \Omega^{\otimes k/2} \right)$$

with singularities at most the finitely many orbits of elliptic points $\tau \in \mathbb{H}$.

Moreover $Y_0(N)$ has only finitely many cusps, see Example 2.11. For arbitrary $q \in \mathbb{Q}$ and $\beta \in \Gamma$ with $q = \beta(\infty)$ each modular form $g \in M_k(\Gamma_0(N))$ has a well-defined order

$$ord_q g := ord_{\tau} g[\beta]_k$$

independent from the choice of $\beta$. Hence $\omega_g$ extends as meromorphic differential form to the compactified modular curve.
3.3 Generalization to Hecke congruence subgroups $\Gamma_0(N)$

$$\omega_k \in H^0\left(X_0(N), \mathcal{M} \otimes \Omega^{\otimes k/2}_{X_0(N)}\right)$$

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 $\alpha$ is well-defined. The map $\alpha$ 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 $K \in \text{Div}(X_0(N))$ the line bundle

$$\mathcal{L}_{N,k} := \mathcal{O}_{(k/2)K+D_k} \in \text{Pic}(X_0(N))$$

with the divisor

$$D_k := \left\lfloor \frac{k}{4} \right\rfloor \cdot \sum_{x \in X_0(N), h_x = 2} x + \left\lfloor \frac{k}{3} \right\rfloor \cdot \sum_{x \in X_0(N), h_x = 3} x + \frac{k}{2} \cdot \sum_{x \in X_0(N), x \text{ cusp}} x \in \text{Div}(X_0(N))$$

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:

$$\mathcal{L}_{N,k} \simeq \Omega_{N,k}$$

with the subsheaf of meromorphic differential forms on $X_0(N)$

$$\Omega_{N,k} \subset \mathcal{M} \otimes \mathcal{O}^{\otimes k/2}$$

defined by

$$\Omega_{N,k}(U) := \{ \omega \in H^0(U, \mathcal{M} \otimes \mathcal{O}^{\otimes k/2}) : \omega \neq 0 \text{ and } \text{div} \omega \geq -D_k|U] \cup \{0\} \}$$

for each open $U \subset X_0(N)$.
Global sections: Consider the canonical map
\[ \alpha : M_k(\Gamma_0(N)) \rightarrow H^0(X_0(N), \mathcal{M} \otimes \Omega^\otimes k/2), \quad g \mapsto \omega_g, \]
with \( \omega_g \) the unique differential form with
\[ p^* \omega_g = g(\tau) (d\tau)^{k/2}. \]
Here \( p : \mathbb{H}^* \rightarrow X_0(N) \) denotes the canonical projection. Then
\[ H^0(X_0(N), \mathcal{L}_{N,k}) \simeq H^0(X_0(N), \Omega_{N,k}) = \]
\[ = \text{im} \left[ \alpha : M_k(\Gamma_0(N)) \rightarrow H^0 \left( X_0(N), \mathcal{M} \otimes \Omega^\otimes k/2 \right) \right] \]

Cohomology: For \( k \geq 2 \)
\[ H^1(X_0(N), \mathcal{L}_{N,k}) = 0 \]

Dimension of vector space of sections: For \( k \geq 2 \)
\[ \dim H^0(X_0(N), \mathcal{L}_{N,k}) = (g(X_0(N)) - 1) \cdot (k - 1) + \deg D_k, \]
and for \( k = 0 \)
\[ \mathcal{L}_{N,0} \simeq \mathcal{O}, \text{ hence } \dim H^0(X_0(N), \mathcal{L}_{N,0}) = 1. \]

Proof. We set
\[ g := g(X_0(N)) \]

1) Estimating the degree of \((k/2) \cdot K + D_k\): By definition
\[ \mathcal{L}_{N,k} \simeq \mathcal{O}_{(k/2)K + D_k}. \]
Using the estimates
\[ |k/4| \geq (k/4) - 1/2 \text{ and } |k/3| \geq (k/3) - 2/3 \]
and the genus formula for \( X_0(N) \) we obtain for the degree of the corresponding divisor for \( k \geq 2 \)
\[ \deg \left( (k/2) \cdot K + D_k \right) \geq \left( \frac{k}{2} (2g - 2) \right) + \left( \frac{k - 2}{4} \cdot \varepsilon_2 + \frac{k - 2}{3} \cdot \varepsilon_3 + \frac{k}{2} \cdot \varepsilon_{\infty} \right) = \]
\[ = (2g - 2) + \frac{k - 2}{2} \left( 2g - 2 + \frac{\varepsilon_2}{2} + \frac{2}{3} \cdot \varepsilon_3 + \varepsilon_{\infty} \right) + \varepsilon_{\infty} = \]
\[ = (2g - 2) + \frac{k - 2}{2} \cdot \left( \frac{\deg f}{6} \right) + \varepsilon_{\infty} > 2g - 2 \]
3.3 Generalization to Hecke congruence subgroups $\Gamma_0(N)$

ii) \textit{Vanishing of} $\dim H^1(\mathcal{X}_0(N), \mathcal{L}_{N,k})$: We apply Serre’s duality theorem in the form

$$H^1(\mathcal{X}_0(N), \mathcal{L}_{N,k}) = H^0(\mathcal{X}_0(N), \mathcal{L}_{N,k}^\vee \otimes \mathcal{O})^\vee$$

and estimate for even $k \geq 2$ due to part i)

$$\deg \left(-\left(\frac{k}{2}\right) \cdot K + D_k\right) + K < (2 - 2g) + (2g - 2) = 0$$

Hence

$$\dim H^1(\mathcal{X}_0(N), \mathcal{L}_{N,k}) = \dim H^0(\mathcal{X}_0(N), \mathcal{L}_{N,k}^\vee \otimes \mathcal{O}) = 0$$

iii) \textit{Riemann-Roch theorem for} $\mathcal{L}_{N,k}$: The Riemann-Roch theorem proves the dimension formula

$$\dim H^0(\mathcal{X}_0(N), \mathcal{L}_{N,k}) = 1 - g + \deg \left(\left(\frac{k}{2}\right) \cdot K + D_k\right) =$$

$$= 1 - g + \deg \left(\left(\frac{k}{2}\right) \cdot K\right) + \deg D_k = (k - 1)(g - 1) + \deg D_k, \text{ q.e.d.}$$

\textit{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

$$\dim H^0(X(\Gamma_0(N)), \mathcal{L}_{N,k})$$

computed by applying the Riemann-Roch theorem to the line bundle $\mathcal{L}_{N,k}$. 
Fig. 3.1 Dimension formulas for modular forms of weight $k = 4$ of $\Gamma_0(p^n)$

Apparently

$$M_0(\Gamma_0(N)) \cong \mathbb{C}, \ N \in \mathbb{N},$$

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 $= \varepsilon_n$, the number of cusps of $X_0(N)$. In particular, the codimension does not depend on the weight $k$. 
3.3 Generalization to Hecke congruence subgroups $\Gamma_0(N)$

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 $\varepsilon_\infty$ in the general case see Example 2.11.

Proof. Set

$$g := g(X_0(N))$$

and consider the divisor $D_k \in \text{Div}(X_0(N))$ from Theorem 3.26, and define the divisor

$$D_k^\circ := \sum_{x \in X_0(N)_{\text{cusp}}} (-1) \cdot x + D_k \in \text{Div}(X_0(N))$$

and the corresponding line bundle

$$L_{N,k}^\infty = \mathcal{O}(k/2) \cdot k + D_k^\circ \in \text{Pic}(X_0(N))$$

with

$$\deg L_{N,k}^\infty = -\varepsilon_\infty + \deg L_{N,k}. $$

The order relations imply for even $k \geq 2$

$$H^0(X_0(N), L_{N,k}^\infty) =$$

$$= \{ \omega_h \in H^0(X_0(N), \Omega_{N,k}) : \text{ord}_t \omega_h \geq (k/2) - 1 \text{ for all cusps } x \in X_0(N) \} =$$

$$= \{ h \in M_k(\Gamma_0(N)) : \text{ord}_t h \geq 1 \text{ for all } t \in \mathbb{H}^* \text{ with } [t] \text{ cusp} \} = S_k(\Gamma_0(N))$$

1. $k \geq 4$: The formula from the proof of Theorem 3.26 shows for even $k \geq 4$

$$\deg L_{N,k}^\infty \geq 2g - 2 + \frac{k - 2}{2} \cdot \deg f > 2g - 2$$

because $\deg f \geq 1$. Hence $H^1(X_0(N), L_{N,k}^\infty) = 0$ because

$$\deg (L_{N,k}^\infty)^\vee \otimes \omega_1 < -(2g - 2) + (2g - 2) = 0,$$

and the Riemann-Roch theorem implies

$$\dim S_k(\Gamma_0(N)) = \dim H^0(X_0(N), L_{N,k}^\infty) =$$

$$= \dim H^0(X_0(N), L_{N,k}) - \varepsilon_\infty = \dim M_k(\Gamma_0(N)) - \varepsilon_\infty.$$
2. $k = 2$: The explicit form of $D_2^\infty$ shows

$$D_2^\infty = 0 \in \text{Div}(X_0(N)),$$

which implies

$$\mathcal{L}_N^{\infty} = \mathcal{O}_K = \Omega^1$$

and

$$S_2(X_0(N)) = H^0(X_0(N), \Omega), \text{ q.e.d.}$$
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

\[
z = (z_0, \ldots, z_n) \sim w = (w_0, \ldots, w_n) : \iff \exists \lambda \in \mathbb{C}^*: w = \lambda \cdot z
\]

and with the canonical projection onto equivalence classes

\[
\pi : \mathbb{C}^{n+1} \setminus \{0\} \to \mathbb{P}^n, \ z \mapsto [z].
\]

For \( z = (z_0, \ldots, z_n) \in \mathbb{C}^{n+1} \setminus \{0\} \) the expression
Elliptic curves

\[(z_0 : ... : z_n) := \pi(z) \in \mathbb{P}^n\]

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 \(U_i := (U_i)_{i=0, \ldots, n}\) with the open sets

\[U_i := \{ (z_0 : ... : z_n) \in \mathbb{P}^n : z_i \neq 0 \}, \ i = 0, \ldots, n.\]

and for each \(i = 0, \ldots, n\) as \(i\)-th standard chart the homeomorphism

\[\phi_i : U_i \rightarrow \mathbb{C}^n, \ (z_0 : ... : z_n) \mapsto \left(\frac{z_0}{z_i}, ..., \frac{z_i}{z_i}, \frac{z_i}{z_i}, ..., \frac{z_n}{z_i}\right).\]

Here the “hat” indicates omission of the term. The transformation between two charts \(\phi_j\) and \(\phi_i\) with \(i < j\) is the map

\[\psi_{ij} := \phi_i \circ \phi_j^{-1} : \phi_j(U_i \cap U_j) \rightarrow \phi_i(U_i \cap U_j),\]

\[(w_0, w_1, ..., w_{j-1}, 1, w_{j+1}, ..., w_n) \mapsto \left(\frac{w_0}{w_i}, ..., \frac{w_{i-1}}{w_i}, 1, \frac{w_{i+1}}{w_i}, ..., \frac{w_{j-1}}{w_i}, \frac{1}{w_i}, \frac{w_{j+1}}{w_i}, ..., \frac{w_n}{w_i}\right).\]

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 \(\Lambda\). The map
4.1 Embedding tori as plane cubic hypersurfaces

\[ \phi : T \to \mathbb{P}^2, \ p \mapsto \begin{cases} (1 : \wp(p) : \wp'(p)) & \text{if } p \neq 0 \\ (0 : 0 : 1) & \text{if } p = 0 \end{cases} \]

maps the torus \( T \) biholomorphically onto the cubic hypersurface \( E \subset \mathbb{P}^2 \) defined by the cubic polynomial

\[ F_{\text{hom}}(X_0, X_1, X_2) = X_2^2X_0 - (4X_1^3 - g_2 \cdot X_1X_0^2 - g_3 \cdot X_0^3) \in \mathbb{C}[X_0, X_1, X_2], \]

which is the homogenization of

\[ F(X, Y) = Y^2 - (4X^3 - g_2X - g_3) \in \mathbb{C}[X, Y]. \]

**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

\[ \phi(T \setminus \{0\}) \subset E_{\text{aff}} := \{(x, y) \in \mathbb{C}^2 : y^2 = 4 \cdot x^3 - g_2 \cdot x - g_3\} \]

The closure of the affine algebraic set

\[ E_{\text{aff}} \subset \mathbb{C}^2 \subset \mathbb{P}^2 \]

is the projective algebraic variety \( E \subset \mathbb{P}^2 \), the zero set in \( \mathbb{P}^2 \) of

\[ F_{\text{hom}}(X_0, X_1, X_2), \]

see Figure 4.5.
ii) Holomorphy of $\phi$: To check holomorphy in a neighbourhood of $0 \in T$ we choose an open neighbourhood $U \subset T$ of the origin such that $\phi'$ has no zeros in $U$. On

$$U^* := U \setminus \{0\}$$

one obtains by diving the homogeneous coordinate by $\phi'$

$$\phi(U^*) = (1 : \phi : \phi') = \left(1/\phi' : \phi/\phi' : 1\right),$$

which converges with limit

$$\lim_{z \to 0} \phi(z) = (0 : 0 : 1) := O \in \mathbb{P}^2$$

because $\phi$ and $\phi'$ have poles at $0$ of order respectively $= 2$ and $3$. Hence $0 \in T$ is a removable singularity of $\phi$.

iii) Injectivity of $\phi$: The holomorphic map

$$\phi : T \to \mathbb{P}^1$$

is a branched covering of degree $= 2$, while the holomorphic map

$$\phi' : T \to \mathbb{P}^1$$

is a branched covering of degree $= 3$. To give an indirect proof of the injectivity of $\phi$ assume two distinct points
4.1 Embedding tori as plane cubic hypersurfaces

\[ z \neq w \in T \setminus \{0\} \]

with

\[ (\varphi(z), \varphi'(z)) = (\varphi(w), \varphi'(w)) \in \mathbb{C}^2. \]

Then \( \varphi(z) = \varphi(w) \) implies \( w = -z \)

and

\[ \varphi'(z) = \varphi'(w) = \varphi'(-z) = -\varphi'(z) \implies \varphi'(z) = 0. \]

Lemma 1.13 implies that

\[ z = \left\{ \omega / 2 \right\}, \ \omega \in \Lambda \text{ and } w = -z \in T \]

are two distinct classes of half-period points of \( \Lambda \). But \( \varphi \) attains at \( z \) the value \( \varphi(z) \) with multiplicity \( =2 \), hence \( \varphi \) assumes the value \( \varphi(z) = \varphi(w) \) with multiplicity \( =4 \), a contradiction.

iv) The image of \( \phi \): Consider a point

\[ (1 : x : y) \in E. \]

The \( \varphi \)-function is a non-constant holomorphic map

\[ \varphi : T \to \mathbb{P}^1, \]

in particular it is surjective: There exists \( z \in T \) with

\[ \varphi(z) = x. \]

The function \( \varphi \) is even, therefore also

\[ \varphi(-z) = x. \]

From

\[ y^2 = 4x^3 - g_2 \cdot x - g_3 = 4\varphi(z)^3 - g_2 \cdot \varphi(z) - g_3 = \varphi'(z)^2 \]

follows:

- Either

  \[ y = \varphi'(z) \text{ and } \phi(z) = (1 : x : y). \]

- Or

  \[ y = -\varphi'(z) = \varphi'(-z) \text{ and } \phi(-z) = (1 : x : y) \]

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

  \[ 0 = F(x_0, y_0) = y_0^2 - (4x_0^3 - Ax_0 - B) \]
\[
\frac{\partial F}{\partial y}(x_0, y_0) = 2y_0 = 0 \quad \text{and} \quad \frac{\partial F}{\partial x}(x_0, y_0) = -12x_0^2 + A = 0
\]

Introducing the cubic polynomial

\[f(x) := 4x^3 - Ax + B \in \mathbb{C}[x]\]

the condition is equivalent to

\[f(x_0) = 0 \quad \text{and} \quad f'(x_0) = 0.
\]

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 \(O\)

\[\phi_2 : U_2 \to \mathbb{C}^2, \ (z_0 : z_1 : z_2) \mapsto (u, v) := \left(\frac{z_0}{z_2}, \frac{z_1}{z_2}\right).
\]

We have

\[\phi_2(E \cap U_2) = \{(u, v) \in \mathbb{C}^2 : f(u, v) = 0\}
\]

with

\[f(u, v) := u - (4 \cdot v^3 - A \cdot u^2 \cdot v - B \cdot u^3).
\]

Then the partial derivatives are

\[\frac{\partial f}{\partial u}(u, v) = 1 - (2 \cdot A \cdot u \cdot v - 3 \cdot B \cdot u^2) \quad \text{and} \quad \frac{\partial f}{\partial v}(u, v) = -12 \cdot v^2 + A \cdot u^2
\]

hence

\[\nabla f(0, 0) = (1, 0) \neq 0.
\]

The non-singular projective algebraic curve \(E \subset \mathbb{P}^2\) is 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.
4.1 Embedding tori as plane cubic hypersurfaces

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 given tori $T = \mathbb{C}/\Lambda$, see Figure 4.2. Real values are approximated by rationals.

![Fig. 4.2 Embedding tori as plane cubics](image)

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

$$\mathcal{L} \in \text{Pic}(X).$$

Definition 4.5 (The twisted line bundle on $\mathbb{P}^n$). The twisted line bundle $\mathcal{O}(1)$ on $\mathbb{P}^n$ is defined with respect to the standard atlas of $\mathbb{P}^n$ by the cocycle

$$g = (g_{ij}) \in Z^1(\mathcal{M}, \mathcal{O}^*)$$

with
Elliptic curves

\[ g_{ij}(z_0 : \ldots : z_n) := \frac{z_j}{z_i}, \, 0 \leq i \neq j \leq n. \]

**Proposition 4.6 (Sections of \( O(1) \)).** The sections of \( O(1) \) on \( \mathbb{P}^n \) correspond bijectively to the linear polynomials \( HPol(1) \subset \mathbb{C}[z_0, \ldots, z_n] \), i.e. the map

\[ HPol(1) \to H^0(\mathbb{P}^n, O(1)), \, z_k \mapsto s_k, \, k = 0, \ldots, n. \]

Here \( s_k \in H^0(\mathbb{P}^n, O(1)) \) 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

\[ s_k := (s_{k,i})_{i=0,\ldots,n} \in H^0(\mathbb{P}^n, O(1)) \]

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

\[ O(k) := O(1)^{\otimes k}, \, k \in \mathbb{N}, \]

cf. also [63].

In order that a line bundle \( \mathcal{L} \) on a Riemann surface \( X \) defines a holomorphic map

\[ \phi_{\mathcal{L}} : X \to \mathbb{P}^n \]

to a projective space, the line bundle \( \mathcal{L} \) has to be globally generated.

**Definition 4.7 (Base-point, globally generated line bundle).** Consider a Riemann surface \( X \) and a line bundle \( \mathcal{L} \) on \( X \).

1. A point \( x \in X \) is a base-point of \( \mathcal{L} \) if each section \( \sigma \in H^0(X, \mathcal{L}) \) satisfies \( \sigma(x) = 0 \). Note

\[ \sigma(x) = 0 \iff \sigma_x \in m_x \mathcal{L}_x \]

with \( \mathcal{L}_x \) the stalk of \( \mathcal{L} \) at \( x \in X \) and

\[ m_x \subset \mathcal{O}_x \]

the maximal ideal of the stalk \( \mathcal{O}_x \) 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 \( \sigma \in H^0(X, \mathcal{L}) \) such that the germ \( \sigma_x \in \mathcal{L}_x \) generates the stalk \( \mathcal{L}_x \) as \( O_x \)-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 \( \mathcal{L} \) on \( X \). After choosing a basis \( (\sigma_i)_{i=0,...,n} \in H^0(X, \mathcal{L}) \)

the map

\[
\phi: X \to \mathbb{P}^n, \ x \mapsto (\sigma_0(x) : ... : \sigma_n(x)),
\]

is well-defined, independent from the chosen trivialization of \( \mathcal{L} \) in a neighbourhood of \( x \in X \). It induces an isomorphism

\[
\phi^*(\mathcal{O}(1)) \cong \mathcal{L}
\]

with \( \phi^*(\mathcal{O}(1)) \) the pull-back of the twisted line bundle.

**Proof.** We set

\[
\phi := \phi_{\mathcal{L}}.
\]

i) **Definition:** We consider the definition of \( \phi \) in a suitable open neighbourhood \( U \) of \( x \). On \( U \) we choose a trivialization to identify the line bundle \( \mathcal{L} \) with the structure sheaf \( \mathcal{O} \). Hence sections from \( H^0(U, \mathcal{L}) \) become holomorphic functions. Because \( \mathcal{L} \) is globally generated there is an index \( j \in \{0,...,n\} \) with

\[
\sigma_j(x) \neq 0.
\]

Hence the point

\[
(\sigma_0(x) : ... : \sigma_n(x)) \in \mathbb{P}^n
\]

is well-defined. It is independent of the choice of the chart and of the isomorphism

\[
\mathcal{L}|U \cong \mathcal{O}|U.
\]

Apparently the map \( \phi \) is holomorphic on \( U \).

ii) **Pullback of the twisted line bundle:** For each \( i = 0,...,n \) the sets

\[
X_i := \phi^{-1}(U_i) = \{x \in X : (\sigma_i)_x \notin \mathfrak{m}_x \mathcal{L}_x\}
\]

form an open covering \( (X_i)_{i=0,...,n} \) of \( X \) because \( \mathcal{L} \) is globally generated. For \( i = 0,...,n \) the canonical morphisms between the rings of local sections

\[
\mathcal{O}(1)(U_i) \to \phi_* (\mathcal{L})(U_i) = \mathcal{L}(X_i) \text{ induced by } s_i|U_i \mapsto \sigma_i|X_i
\]

define a canonical sheaf morphism on \( \mathbb{P}^n \).
\[ \mathcal{O}(1) \to \phi_* \mathcal{L} \]

The latter corresponds to a sheaf morphism on \( X \)

\[ \phi^*(\mathcal{O}(1)) \to \mathcal{L}, \]

because the two functors \( \phi^* \) and \( \phi_* \) are adjoint, see [29, Chap. II, § 5], i.e. there is a canonical group isomorphism

\[ \text{Hom}_{\mathcal{O}_X}(\phi^*(\mathcal{O}(1)), \mathcal{L}) \simeq \text{Hom}_{\mathcal{O}_{\mathbb{P}^n}}(\mathcal{O}(1), \phi_* \mathcal{L}) \]

The induced morphism

\[ \phi^*(\mathcal{O}(1)) \to \mathcal{L} \]

between the two line bundles is an isomorphism because it is an isomorphism on stalks: If for a given \( i \in \{0, ..., n\} \)

\( x \in X_i \subset X \) and \( y := \phi(x) \in U_i \subset \mathbb{P}^n \)

then

\( (\phi^* \mathcal{O}(1))_x = \mathcal{O}(1)_y \otimes \mathcal{O}_{\mathbb{P}^n, y} \mathcal{O}_{X,x} \to \mathcal{L}_x, \ (s)_y \otimes 1 \mapsto (\sigma)_x, \ q.e.d. \)

Theorem 4.9 provides a geometric criterion for the map provided by a globally generated line bundle \( \mathcal{L} \) 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 \( \mathcal{L} \) on \( X \). Then the induced map

\[ \phi_{\mathcal{L}} : X \to \mathbb{P}^n \]

is a holomorphic closed embedding iff \( \mathcal{L} \) satisfies both of the following properties:

1. **Separating points:** For any two distinct points \( p \neq q \in X \) exists a section

\[ \sigma \in H^0(X, \mathcal{L}) \text{ with } \sigma(p) \neq 0 \text{ but } \sigma(q) = 0 \]

or vice versa.

2. **Separating tangent vectors:** For all \( x \in X \) the map

\[ d_{\mathcal{L}, x} : \{ \sigma \in H^0(X, \mathcal{L}) : \sigma_x \in m_x \mathcal{L}_x \} \to m_x \mathcal{L}_x/m_x^2 \mathcal{L}_x, \ \sigma \mapsto [\sigma_x], \]

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 \( p \neq q \in X \)

\[
\phi_L(p) \neq \phi_L(q)
\]

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 isomorphism of \( \mathcal{O}_x \)-modules - respectively of complex vector spaces -

\[
m_x \mathcal{L}_x / m_x^2 \mathcal{L}_x \cong (m_x/m_x^2) \otimes \mathcal{O}_x \mathcal{L}_x = T^1_x \otimes \mathcal{O}_x \mathcal{L}_x
\]

with the cotangent space

\[
T^1_x := m_x/m_x^2
\]

of \( X \) at \( x \). Then the map

\[
d_{\mathcal{L},x}: \{ \sigma \in H^0(X, \mathcal{L}) : \sigma_x \in m_x \mathcal{L}_x \} \rightarrow T^1_x \otimes \mathcal{O}_x \mathcal{L}_x
\]

is induced by the total differential \( d_x \) of holomorphic functions: A section

\[
\sigma \in H^0(X, \mathcal{L}) \text{ with } \sigma_x \in m_x \mathcal{L}_x
\]

factorizes in a suitable neighbourhood \( U \) of \( x \) as

\[
\sigma = f \cdot \sigma_1
\]

with a holomorphic function \( f \in \mathcal{O}(U) \) satisfying \( f_x \in m_x \) and a holomorphic section \( \sigma_1 \in \mathcal{L}(U) \). Then

\[
d_{\mathcal{L},x}(\sigma) = d_x f \otimes \sigma_1 \in T^1_x \otimes \mathcal{O}_x \mathcal{L}_x
\]

independent from the decomposition of \( \sigma \).
\{ s \in H^0(\mathbb{P}^n, \mathcal{O}(1)) : s(y) = 0 \} \xrightarrow{\phi^* \circ d_{\mathcal{O}(1),y}} T_{\mathbb{P}^n,y} \otimes_{\mathcal{O}(1)} \mathcal{O}(1)
\{ \sigma \in H^0(X, \mathcal{L}) : \sigma(x) = 0 \} \xrightarrow{d_{\mathcal{L},x}} T_{X,x} \otimes_{\mathcal{O}_X} \mathcal{L}

Fig. 4.3 Separating tangent vectors

The commutative diagram from Figure 4.3 with

\( y := \phi(x) \)

and surjective maps

\( d_{\mathcal{O}(1),y} \) and \( \phi^* \)

shows: The pull-back \( \phi^* \) is surjective if and only if \( d_{\mathcal{L},x} \) is surjective.

**Definition 4.11 (Very ample line bundle).** A globally generated line bundle \( \mathcal{L} \) on a compact Riemann surface \( X \) is **very ample** if the induced map

\( \phi_{\mathcal{L}} : X \to \mathbb{P}^n \)

is an embedding.

A globally generated line bundle \( \mathcal{L} \) on \( X \) has enough sections to define a holomorphic map

\( \phi_{\mathcal{L}} : X \to \mathbb{P}^n \).

If \( \mathcal{L} \) is very ample then there are enough sections that \( \phi_{\mathcal{L}} \) 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 \( \mathcal{L} \) on a Riemann surface \( X \) and a divisor \( D \in \text{Div}(X) \) we denote by

\( \mathcal{L}_D := \mathcal{L} \otimes_{\mathcal{O}} \mathcal{O}_D \)

the sheaf of meromorphic sections of \( \mathcal{L} \) which are multiples of the divisor \(-D\). The sheaf \( \mathcal{L}_D \) is isomorphic to a line bundle.

Consider a line bundle \( \mathcal{L} \) on a compact Riemann surface \( X \). Theorem 4.13 states a numerical criterion for the dimension of the vector spaces.
4.1 Embedding tori as plane cubic hypersurfaces

\[ H^0(X, \mathcal{L}_D), \ D \in \text{Div}(X), \]

which ensures that the map
\[ \phi_{\mathcal{L}} : X \to \mathbb{P}^n \]
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 \( \mathcal{L} \) on \( X \) are equivalent:

- The line bundle \( \mathcal{L} \) is very ample.
- For two not necessarily distinct points \( p, q \in X \) the corresponding point divisors
  \[ P := 1 \cdot p, \ Q := 1 \cdot q \in \text{Div}(X) \]
satisfy
  \[ \dim H^0(X, \mathcal{L} - (P + Q)) = \dim H^0(X, \mathcal{L}) - 2. \]

**Proof.**

1) Assume the validity of the dimension formula: The formula implies for any two point divisors \( P, Q \in \text{Div}(X) \)
\[ H^0(X, \mathcal{L} - (P + Q)) \subseteq H^0(X, \mathcal{L} - P) \subseteq H^0(X, \mathcal{L}) \]
and each proper inclusion has codimension = 1 because it is defined by a single linear equation.
- The equation
  \[ h^0(X, \mathcal{L} - P) = h^0(X, \mathcal{L}) - 1. \]
states that the kernel of the evaluation
\[ H^0(X, \mathcal{L}) \to \mathcal{L}_P/m_p \mathcal{L}_P \simeq \mathbb{C}, \ \sigma \mapsto [\sigma_P], \]
has codimension = 1. Hence \( p \) is not a base-point of \( \mathcal{L} \). As a consequence, the line bundle \( \mathcal{L} \) is globally generated and
\[ \phi_{\mathcal{L}} : X \to \mathbb{P}^n \]
is well-defined.
- The equation
  \[ H^0(X, \mathcal{L} - (P + Q)) \subseteq H^0(X, \mathcal{L} - P) \]
implies that for any pair of distinct points \( p, q \in X \) there exists a section
\[ \sigma \in H^0(X, \mathcal{L} - P) \backslash H^0(X, \mathcal{L} - (P + Q)) \]
i.e. satisfying
\[ \sigma(p) = 0 \text{ but } \sigma(q) \neq 0. \]
Hence the sheaf \( \mathcal{L} \) separates points.

- The dimension formula shows for any point \( p \in X \) with point divisor \( P \in \text{Div}(X) \)
  \[ H^0(X, \mathcal{L} - 2P) \subseteq H^0(X, \mathcal{L} - P) \]
has codimension = 1. Hence there exists a section
\[ \sigma \in H^0(X, \mathcal{L} - P) \]
which implies the surjectivity of the composition of the canonical maps
\[ H^0(X, \mathcal{L} - p) \rightarrow m_{X,p} \mathcal{L}_p \rightarrow m_{X,p} \mathcal{L}_p / m^2_{X,p} \mathcal{L}_p \]
due to
\[ \dim_\mathbb{C}(m_{X,p}/m^2_{X,p}) = 1. \]
Therefore \( \mathcal{L} \) separates tangent vectors.

ii) **Assume \( \mathcal{L} \) very ample**: Theorem 4.9 implies that \( \mathcal{L} \) separates points and tangent vectors. Separating points implies for all point divisors \( P \neq Q \in \text{Div}(X) \)
\[ \dim H^0(X, \mathcal{L} - (P + Q)) = \dim H^0(X, \mathcal{L}) - 2. \]
Separating tangent vectors implies for each point divisor \( P \in \text{Div}(X) \)
\[ \dim H^0(X, \mathcal{L} - 2P) = \dim H^0(X, \mathcal{L}) - 2, \text{ q.e.d.} \]

**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 \( \Omega^{\otimes 3} \in \text{Pic}(X) \) is very ample, see [63].

2. For a complex torus \( X = \mathbb{C}/\Lambda \) holds \( \Omega \simeq \mathcal{O} \), hence
\[ g(X) := \dim H^0(X, \Omega) = 1 \]
Consider the divisor
\[ D := 3 \cdot 0 \in \text{Div}(X) \]
with the point \( 0 \in X \) being the origin. Then the line bundle
4.2 Elliptic curves over subfields of $\mathbb{C}$

Let $\mathcal{L} := \mathcal{O}_D \in \text{Pic}(X)$

is very ample according to Theorem 4.13: As a consequence of $\Omega \cong \mathcal{O}$, for two point divisors

$P = 1 \cdot p, \; Q = 1 \cdot q \in \text{Div}(X)$

holds

$$\dim H^1(X, \mathcal{L} - (P + Q)) = \dim H^0(X, \mathcal{O}_{-D + (P + Q)}) = 0$$

because

$$\deg (-D + (P + Q)) = -3 + 2 = -1 < 0$$

Hence

$$\dim H^0(X, \mathcal{L}_{-(P + Q)}) = 1 - g(X) + \deg \mathcal{L} - 2 = \dim H^0(X, \mathcal{L}) - 2$$

The line bundle $\mathcal{L}$ is isomorphic to the subsheaf of meromorphic functions

$$\mathcal{O}_D \subset \mathcal{M}$$

with a single pole at 0, having order at most $= 3$:

$$H^0(X, \mathcal{O}_D) = \{ f \in \mathcal{M}(X) : f \neq 0 \text{ and } \text{div } f \geq -D \} \cup \{0\}$$

The Riemann-Roch theorem implies

$$\dim H^0(X, \mathcal{O}_D) = \deg D = 3$$

Apparently, a basis of $H^0(X, \mathcal{O}_D)$ 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).**
<table>
<thead>
<tr>
<th>Complex Analytic Geometry</th>
<th>Algebraic Geometry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complex Manifold</td>
<td>Smooth variety</td>
</tr>
<tr>
<td>Euclidean topology</td>
<td>Zariski topology</td>
</tr>
<tr>
<td>Compact complex manifold</td>
<td>Smooth projective algebraic variety</td>
</tr>
<tr>
<td>Compact Riemann surface</td>
<td>Projective algebraic curve</td>
</tr>
<tr>
<td>Genus</td>
<td></td>
</tr>
<tr>
<td>Stein manifold</td>
<td>Smooth affine variety</td>
</tr>
<tr>
<td>Structure sheaf $\mathcal{O}_X$</td>
<td></td>
</tr>
<tr>
<td>Holomorphic function</td>
<td>Regular function</td>
</tr>
<tr>
<td>Meromorphic function</td>
<td>Rational function</td>
</tr>
<tr>
<td>Local ring $\mathcal{O}_{X,x}$</td>
<td></td>
</tr>
<tr>
<td>Line bundle</td>
<td></td>
</tr>
<tr>
<td>Very ampleness</td>
<td></td>
</tr>
<tr>
<td>Divisor</td>
<td></td>
</tr>
<tr>
<td>Sheaf $\Omega_X$ of differential forms</td>
<td></td>
</tr>
<tr>
<td>Cohomology</td>
<td></td>
</tr>
<tr>
<td>Riemann-Roch Theorem</td>
<td></td>
</tr>
<tr>
<td>Serre Duality</td>
<td></td>
</tr>
</tbody>
</table>

The table relates concepts from complex analytic 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 Kähler manifold has a counterpart in Algebraic Geometry. Hence not any instance of a concept on the left-hand side of the table induces a corresponding instance on the right-hand side. On both sides there are objects which cannot be studied by methods from the other side.
4.2 Elliptic curves over subfields of $\mathbb{C}$

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

$$X = V(a) \subset \mathbb{A}^n(\overline{k}) = \overline{k}^n$$

of a prime ideal $a \subset \overline{k}[X_1, \ldots, X_n]$, i.e.

$$X := \{ x \in \mathbb{A}^n(\overline{k}) : f(x) = 0 \text{ for all } f \in a \}.$$

The ring

$$R := \overline{k}[X_1, \ldots, X_n]/a$$

is the affine coordinate ring of $X$.

If $a$ can be generated by polynomials from $k[X_1, \ldots, X_n]$, 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

$$X = V(a) \subset \mathbb{P}^n(\overline{k})$$

of a prime ideal

$$a \subset \overline{k}[X_0, \ldots, X_n],$$
generated by homogeneous polynomials, i.e.

\[ X := \{ (x = (x_0 : \ldots : x_n) \in \mathbb{P}^n(\overline{k}) : f(x) = 0 \text{ for all homogeneous } f \in \mathfrak{a} \}. \]

3. Zariski topology: Closed sets of \( \mathbb{A}^n(\overline{k}) \) are the affine algebraic subvarieties. The Zariski topology on an affine algebraic variety \( X \subset \mathbb{A}^n(\overline{k}) \) is the subspace topology induced from the Zariski topology of \( \mathbb{A}^n(\overline{k}) \). 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 \( \mathbb{P}^n(\overline{k}) \) are the projective algebraic subvarieties. The Zariski topology on a projective algebraic variety \( X \subset \mathbb{P}^n(\overline{k}) \) is the subspace topology induced from the Zariski topology of \( \mathbb{P}^n(\overline{k}) \).

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

\[ f : U \rightarrow \overline{k} \]

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 \( \mathcal{O}_X \) of regular functions on an affine algebraic variety \( X \) is the contravariant functor

\[ U \mapsto \mathcal{O}_X(U) := \{ f : U \rightarrow \overline{k} \mid f \text{ regular } \}, \ U \subset X \text{ open}, \]

with the restriction of functions. The sheaf \( \mathcal{O}_X \) is named the structure sheaf of \( X \). Sections over a basis open set \( D_h \subset X \) form the ring

\[ \mathcal{O}(D_h) = \mathcal{R}_h := \{ g/h^n : g \in R, \ n \in \mathbb{N} \} \]

Because the ideal

\[ \mathfrak{a} \subset \overline{k}[X_1, \ldots, X_n] \]

is prime, the quotient \( R \) and all rings

\[ \mathcal{O}_X(U), \ U \subset X \text{ open}, \]

are integral domains. The sheaf \( \mathcal{M}_X \) of rational functions on \( X \) is the sheafification of the presheaf

\[ U \mapsto \mathcal{Q}(\mathcal{O}_X(U)), \ U \subset X \text{ open}, \]
4.2 Elliptic curves over subfields of \( \mathbb{C} \)

with \( Q(\mathcal{O}_X(U)) \) the quotient field of the integral domain \( \mathcal{O}_X(U) \). Sections of \( \mathcal{M}_X(U) \) are locally quotients

\[ g/h, \ g, \ h \in R, \ h \neq 0. \]

For a non-empty open set \( U \subset X \) holds

\[ \mathcal{M}(U) = Q(R) =: \overline{k}(X), \]

independent from \( U \). The field \( Q(R) \) is named the function field \( \overline{k}(X) \) of \( X \). The sheaf

\[ \mathcal{M}^* \subset \mathcal{M} \]

is the multiplicative subsheaf of non-zero rational functions.

The definitions carry over to projective algebraic varieties, because 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 \( \mathcal{O}_{X,x} \) 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 \( \mathcal{O}_{X,x} \) is a regular local ring, i.e. if \( \dim \mathcal{O}_{X,x} = \dim_{\kappa(x)} (m_x/m_x^2) \) (Dimension equals cotangent dimension).

Here

\[ \kappa(x) := \mathcal{O}_{X,x}/m_x \]

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

\[ X \subset k^n(\overline{k}), \]

the primary object is the ideal

\[ \mathfrak{a} \subset k[X_1, \ldots, X_n] \]
with minimal field of definition $k$, or its quotient, the ring

$$R := k[X_1, \ldots, X_n]/a$$

Due to Grothendieck’s reformulation of algebraic geometry, the basic concept is for arbitrary rings $R$ the affine scheme

$$(X := \text{Spec } R, \mathcal{O}_X)$$

Here $\text{Spec } R$ is a topological space with points the prime ideals of $R$. The structure sheaf $\mathcal{O}_X$ has as stalks the localizations

$$R_p, \ p \subset R \text{ prime ideal.}$$

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 of $X/k$).** 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

$$X(K) := X \cap \mathbb{P}^n(K) =$$
4.2 Elliptic curves over subfields of $\mathbb{C}$

$$= \{ x = (x_0 : \ldots : x_n) \in \mathbb{P}^n(K) : x \in X \text{ and } x_i \in K \text{ for all } i = 0,\ldots,n \}.$$ 

**Remark 4.18 (GAGA).**

1. **Chow’s theorem:** Historically, the first GAGA-result is Chow’s theorem: Any complex projective algebraic 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 $\text{An}_{\mathbb{C}}$ denote the category of complex spaces and holomorphic maps. On the other hand, let $\text{Al}_{\mathbb{C}}$ denote the category of schemes of finite type defined over $\mathbb{C}$ and regular maps. The first step attaches to a schema $X \in \text{Al}_{\mathbb{C}}$ a distinguished complex analytic space $X^{an} \in \text{An}_{\mathbb{C}}$. The latter is obtained via the functor:

$$\Phi : \text{An}_{\mathbb{C}} \to \text{Ens}$$

attaching to a complex analytic space $Y$ the set

$$\Phi(Y) := \text{Hom}_{\mathbb{C}}(Y, X)$$

of morphisms of ringed spaces. The functor $\Phi$ can be represented by a universal object $(X^{an}, \phi)$, 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

```
Y
```

```
<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
</table>
X
```

The analytification $\phi : X \to X^{an}$ from the analytification defines for each $x \in X^{an}$ a pull-back
\( \phi : \mathcal{O}_{X, \phi(x)} \to \mathcal{O}_{X^{an}, x} \)

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 \( \mathbb{A}^{n}_{\mathbb{C}} \) induces a unique holomorphic map
\[
f^{an} : X^{an} \to Y^{an}
\]
such that the following diagram commutes

\[
\begin{array}{ccc}
X^{an} & \xrightarrow{\phi_{X}} & X \\
\downarrow{f^{an}} & & \downarrow{f} \\
Y^{an} & \xrightarrow{\phi_{Y}} & Y
\end{array}
\]

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:
\[
\phi^{*} : \text{Sheaf}_{\mathcal{O}_{X}} \to \text{Sheaf}_{\mathcal{O}_{X^{an}}}, \mathcal{F} \mapsto \phi^{*} \mathcal{F}
\]

and
\[
f : \mathcal{F} \to \mathcal{G}, \mapsto \phi^{*} f : \phi^{*} \mathcal{F} \to \phi^{*} \mathcal{G}.
\]

The stalk at a point \( x \in X^{an} \) of the inverse image sheaf is easy to calculate
\[
(\phi^{*} \mathcal{F})_{x} = \mathcal{F}_{\phi(x)} \otimes_{\mathcal{O}_{X, \phi(x)}} \mathcal{O}_{X^{an}, x}
\]

Serre investigated in his GAGA-paper [49] for a projective schema \( X \in \mathbb{A}^{n}_{\mathbb{C}} \) and a coherent \( \mathcal{O}_{X} \)-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
\[
f : X \to Y
\]
4.2 Elliptic curves over subfields of \( \mathbb{C} \)

in \( \mathbb{A}^1_{\mathbb{C}} \) and a coherent \( \mathcal{O}_X \)-module sheaf \( \mathcal{F} \) the canonical morphisms in \( \mathbb{A}^n_{\mathbb{C}} \) between the corresponding direct image sheaves

\[
(R^j f_* \mathcal{F})^{an} \cong R^j f_!^{an} (\mathcal{F}^{an}), \quad j \in \mathbb{N},
\]

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 \( D \in \text{Div}(C) \) 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 \( \text{Div}(C) \), its subgroup \( \text{Div}_0(C) \subset \text{Div}(C) \) contains the classes of divisors of degree \( = 0 \).

2. A divisor \( D \in \text{Div}(C) \) is a **principal divisor** if \( D = 0 \) or

\[
D = \text{div} f
\]

for a rational function \( f \in \overline{k}(C) \). Two divisors \( D_1, D_2 \in \text{Div}(C) \) 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

\[
\deg (\text{div} f) = 0.
\]

Denote by

\[
\text{Prin}(C) \subset \text{Div}_0(C)
\]
the subgroup of principal divisors. The quotient
\[ Cl(C) := \text{Div}(C) / \text{Prin}(C) \]
is named the divisor class group of \( C \). Its subgroup
\[ Cl_0(C) := \text{Div}_0(C) / \text{Prin}(C) \subset Cl(C) \]
is the class group of degree zero divisors.

3. A divisor
\[ D = \sum_{x \in C} n_x \cdot x \in \text{Div}(C) \]
is defined over \( k \) if it is invariant under the action of the Galois group \( G_{\mathbb{K}/k} \), i.e. if for all \( \sigma \in G_{\mathbb{K}/k} \)
\[ D = D^\sigma := \sum_{x \in C} n_x \cdot x^\sigma \in \text{Div}(C) \]

4. For a divisor \( D \in \text{Div}(C) \) we denote by \( \mathcal{O}_D \) the sheaf of multiples of \( -D \), i.e.
\[ \mathcal{O}_D(U) := \{ f \in \mathcal{M}^*(U) : \text{div } f \geq -D|U \cup \{0\} \}, U \subset X \text{ open.} \]

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
\[ \dim H^0(C, \mathcal{O}) = 1 \]
hold literally in the same form as on compact Riemann surfaces. Also the canonical divisor \( K \in \text{Div}(C) \) has degree
\[ \deg K = 2g(C) - 2. \]
Hence we will apply these results also in the context of algebraic geometry 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
\[ O_\infty := 1 \cdot O \in \text{Div}(E) \]
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 $D \in \text{Div}(E)$. Then

$$\dim H^0(E, \mathcal{O}_D) = \begin{cases} 0 & \text{if } \deg D < 0 \\ 0 & \text{if } \deg D = 0, \text{ } D \text{ not principal} \\ 1 & \text{if } \deg D = 0, \text{ } D \text{ principal} \\ \deg D & \text{if } \deg D > 0 \end{cases}$$

**Proof.** The Riemann-Roch theorem together with Serre duality imply for any divisor $D \in \text{Div}(E)$

$$\dim H^0(E, \mathcal{O}_D) - \dim H^1(E, \mathcal{O}_D) = \dim H^0(E, \mathcal{O}_D) - \dim H^0(E, \mathcal{O}_{-D+K}) = 1 - g + \deg D = \deg D$$

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

$$\dim H^0(E, \mathcal{O}_D) = \begin{cases} \deg D & \text{if } \deg D > 0 \\ 0 & \text{if } \deg D < 0 \end{cases}$$

ii) **Case $\deg D = 0$:** We consider the sheaf $\mathcal{O}_D$ as a line bundle. Then

$D \text{ principal } \iff \mathcal{O}_D \simeq \mathcal{O}$
On one hand, $D$ principal implies
\[ H^0(E, \mathcal{O}_D) = \dim H^0(E, \mathcal{O}) = 1 \]

On the other hand, for non-principal $D$ the line bundle $\mathcal{O}_D$ is not trivial. Hence an regular section of $s \in H^0(E, \mathcal{O}_D)$ 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
\[ D = \sum_{x \in X} n_x \cdot x \in \text{Div}(C) \]

which is defined over $k$. Then the finite dimensional $\overline{k}$-vector space
\[ H^0(C, \mathcal{O}_D) = \{ f \in \overline{k}(C) : \text{div } f \geq -D \} \cup \{0\} \]

has a basis of rational functions from $k(C)$.

For the proof see [56, II, Prop. 5.8].

Elliptic curves are by definition subvarieties of a projective space $\mathbb{P}^n(k)$. Theorem 4.23 proves that they are even plane curves, i.e. that they embed as hypersurfaces into $\mathbb{P}^2(k)$.

**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
\[ \phi : E \to \mathbb{P}^2(\overline{k}), p \mapsto \begin{cases} (1 : x(p) : y(p)) & p \neq O \\ (0 : 0 : 1) & p = O \end{cases} \]

induces an isomorphism onto the plane cubic $C \subset \mathbb{P}^2(\overline{k})$, which is defined by a homogeneous polynomial $F_{\text{hom}} \in k[X_0, X_1, X_2]$ of the form
\[ F_{\text{hom}}(X_0, X_1, X_2) = X_0X_2^2 + a_1X_0X_1X_2 + a_3X_0^2X_2 - (X_1^3 + a_2X_0X_1^2 + a_4X_0^2X_1 + a_6X_0^3) \]

with five suitable constants $a_i \in k, i = 1, 2, 3, 4, 6$. In particular, $C$ is defined over $k$.

**Proof.** We construct a very ample line bundle $\mathcal{L} = \mathcal{O}_D$ on $E$ and define $\phi := \phi_{\mathcal{L}}$. Therefore consider the divisor
\[ D := 3 \cdot O_{\infty} \in \text{Div}(E). \]

The line bundle
4.2 Elliptic curves over subfields of $\mathbb{C}$

$satisfies the very ampleness criterion from Theorem 4.13: The proof follows from
the dimension formula in Lemma 4.21 because for all points $p, q \in E$
\[\dim H^0(E, \mathcal{O}_{D-p}) = \dim H^0(E, \mathcal{O}_D) - 1\]
and
\[\dim H^0(E, \mathcal{O}_{D-(p+q)}) = \dim H^0(E, \mathcal{O}_D) - 2.\]
For $n \geq 0$
\[H^0(E, \mathcal{O}_{nO}) = \{f \in \overline{k}(E) : f \text{ has at most a pole at } O \text{ of order } n\} \cup \{0\}\]
and the dimension formula implies the proper inclusion
\[H^0(E, \mathcal{O}_{3O}) \supset H^0(E, \mathcal{O}_{2O}) \supset H^0(E, \mathcal{O}_O) \cong H^0(E, \mathcal{O}) = \mathbb{C}\]}
Hence a basis $(1, x, y)$ of
\[H^0(E, \mathcal{L}) = H^0(E, \mathcal{O}_{3O})\]
exists with
- $y \in H^0(E, \mathcal{O}_{3O}) \subset \overline{k}(E)$ has a pole of order $3$ at $O$ and no other pole,
- $x \in H^0(E, \mathcal{O}_{2O}) \subset \overline{k}(E)$ has a pole of order $2$ at $O$ and no other pole,
- $1 \in H^0(E, \mathcal{O}) = H^0(E, \mathcal{O}_O) \subset \overline{k}(E)$ 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 $\mathcal{L}$ defines the closed embedding
\[\phi := \phi_\mathcal{L} : E \to \mathbb{P}^2(\overline{k}), \ p \mapsto (1 : x(p) : y(p)),\]
on to 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 $H^0(E, \mathcal{O}_{6O})$ 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
\[y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\]
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 \( F_{\text{hom}} \in k[X_0, X_1, X_2] \) with

\[ F_{\text{hom}}(X_0, X_1, X_2) := X_0X_1^3 + a_1X_0X_1X_2 + a_3X_2X_0^2 - (X_3^3 + a_2X_2^2X_0 + a_4X_1X_3^2 + a_6X_0^3). \]

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

\[ C := V(F_{\text{hom}}) \subset \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(k) : F_{\text{hom}}(x_0, x_1, x_2) = 0\}. \]

The cubic \( C \) intersects the line at infinity

\[ \mathbb{P}^1(k) \simeq \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(k) : x_0 = 0\} \]

in the single point \((0 : 0 : 1)\) with multiplicity = 3. Its affine part is the affine variety of the polynomial \( F(X, Y) \in k[X, Y] \)

\[ C_{\text{aff}} = \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(k) : F_{\text{hom}}((x_0 : x_1 : x_2)) = 0 \text{ and } x_0 \neq 0\} = \{(x, y) \in k^2(k) : F(x, y) = 0\} = V(F). \]

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 \( C_{\text{aff}} \) 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

\[ \phi(E) = C \text{ and } E \simeq C \text{ over } k, \text{ q.e.d.} \]

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).** A Weierstrass polynomial over a field \( k \) is a cubic polynomial

\[ F(X, Y) = Y^2 + a_1XY + a_3Y - (X^3 + a_2X^2 + a_4X + a_6) \in k[X, Y] \]
with coefficients
\[ a_1, a_2, a_3, a_4, a_6 \in k. \]
The corresponding equation
\[ F(X, Y) = 0, \]
i.e.
\[ Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \]
is named Weierstrass equation over \( k \).

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. Discriminant and \( j \)-invariant: The Weierstrass polynomial \( F \) has the discriminant
\[ \Delta_F = -b_2^2b_8 - 8b_4^4 + 27b_6^2 - 2b_2b_8 \]
with
\[ b_2 := a_1^2 + 4a_2, \quad b_4 := 2a_4 + a_1a_3, \quad b_6 := a_3^2 + 4a_6 \]
and
\[ b_8 := a_1^2a_6 + 4a_3a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \]
It has the \( j \)-invariant
\[ j_F = \frac{c_4^3}{\Delta_F}, \quad c_4 := b_2^2 - 24b_8. \]

2. Short form: If \( \text{char } k \neq 2, 3 \) 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
\[ r, s, t \in k, u \in k^\times \]
which transforms \( F(X, Y) \) to the Weierstrass polynomial in short form
\[ F'(X', Y') = Y'^2 - (X'^3 + A' \cdot X' + B'), \quad A', B' \in k \]
with discriminant
\[ \Delta_{F'} = -2^4 \cdot (4A^3 + 27B^2) \in k \]
and the same \( j \)-invariant.
3. 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

\[A = u^4 \cdot A', \ B = u^6 \cdot B', \ \Delta = u^{12} \cdot \Delta_F'.\]

retaining the $j$-invariant

\[j_F := 1728 \cdot \frac{(4A)^3}{\Delta_F} = 1728 \cdot \frac{(4A')^3}{\Delta_{F'}} =: j_{F'}.
\]

4. 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 $k$.

5. 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) and part 2) cf. Chap. III, §1; for part 3) cf. Chap. III, Rem. 1.3; for part 4) cf. Chap III, Prop. 1.4(b); for part 5) cf. Chap III, Prop. 1.4(c).

Remark 4.26 (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 4.27 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
4.2 Elliptic curves over subfields of $\mathbb{C}$

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 $e^{2\pi i t}$ on the parameter interval $[0, 1]$.

**Theorem 4.27 (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

$$\Phi : T \xrightarrow{\sim} E(\mathbb{C}).$$

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

$$\Delta_F = A^3 - 27 \cdot B^3$$

We search for a lattice

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

with lattice constants $G_{\Lambda, 4}$ and $G_{\Lambda, 6}$ satisfying

$$A = 60 \cdot G_{\Lambda, 4} \text{ and } B = 140 \cdot G_{\Lambda, 6}.$$  

The restriction of the modular invariant

$$j : \mathbb{H} \to \mathbb{C}, \ j(\tau) := 1728 \cdot \frac{g_2^3(\tau)}{g_3^3(\tau) - 27g_3^2(\tau)},$$

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
\[ j(\tau) = 1728 \cdot \frac{g_3^3(\tau)}{g_2^2(\tau) - 27g_3^2(\tau)} = 1728 \cdot \frac{A^3}{\Delta_F} \]
and
\[ \Delta_F = A^3 - 27B^2 \]
imply
\[ \frac{g_3^3(\tau)}{g_2^2(\tau) - 27g_3^2(\tau)} = \frac{A^3}{A^3 - 27B^2}. \]

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
\[ \frac{A}{g_2(\tau)} = \left( \frac{1}{\omega_1} \right)^4 \quad \text{and} \quad \frac{B}{g_3(\tau)} = \left( \frac{1}{\omega_1} \right)^6. \]

This choice is possible because we may replace \( \omega_1 \) by \( i\omega_1 \). In addition, we set
\[ \omega_2 := \tau \cdot \omega_1, \text{ i.e. } \tau = \omega_2 / \omega_1. \]

Then \( (\omega_1, \omega_2) \) is a positively oriented basis of the lattice
\[ \Lambda := \mathbb{Z} \omega_1 + \mathbb{Z} \omega_2. \]

Its lattice constants are
\[ G_{A,4} = \left( \frac{1}{\omega_1} \right)^4 \cdot G_4(\tau) = \left( \frac{1}{\omega_1} \right)^4 \cdot (1/60) \cdot g_2(\tau) = (1/60) \cdot A \]
and similarly
\[ G_{A,6} = (1/140) \cdot B, \]
i.e.
\[ A = g_{A,2} \text{ and } B = g_{A,3}. \]

The map
4.2 Elliptic curves over subfields of \( \mathbb{C} \)

\[ \phi : \mathbb{C} / \Lambda \to \mathbb{P}^2 \]

from Theorem 4.3 maps the torus \( \mathbb{C} / \Lambda \) biholomorphically to the cubic hypersurface with Weierstrass polynomial

\[ F(X,Y) = Y^2 - (4 \cdot X^3 - g_{A,2} \cdot X - g_{A,3}) = Y^2 - (4 \cdot X^3 - A \cdot X - B), \quad q.e.d. \]

The discriminant \( \Delta_F \in k \) of a Weierstrass polynomial \( F(X,Y) \in k[X,Y] \) indicates whether the projective algebraic variety

\[ C = V(F_{\text{hom}}) \subset \mathbb{P}^2(k) \]

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 4.28 (Singularities of cubics).** Assume \( \text{char } k \neq 2,3 \) and consider a plane cubic curve

\[ C := V(F_{\text{hom}}) \subset \mathbb{P}^2(k) \]

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 4.28 see [56, Chap. III, Prop. 1.4].

**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 4.39 later.

For the computation and the plots see the PARI files \texttt{Elliptic_curve_02} and \texttt{Elliptic_curve_plot_06}. 
<table>
<thead>
<tr>
<th>Figure</th>
<th>Weierstrass equation</th>
<th>$j$-invariant</th>
<th>discriminant</th>
<th>conductor</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.5</td>
<td>$Y^2 = X^3 - 3X + 3$</td>
<td>$-2^8 \cdot 3^3/5$</td>
<td>$-2^4 \cdot 3^3 \cdot 5$</td>
<td>$2^3 \cdot 3^3 \cdot 5$</td>
</tr>
<tr>
<td>4.6</td>
<td>$Y^2 = X^3 + X$</td>
<td>1728</td>
<td>$-2^6$</td>
<td>$2^6$</td>
</tr>
<tr>
<td>4.7</td>
<td>$Y^2 = X^3 - X$</td>
<td>1728</td>
<td>$2^6$</td>
<td>$2^5$</td>
</tr>
<tr>
<td>4.8</td>
<td>$Y^2 = X^3 + 3$</td>
<td>0</td>
<td>$-2^4 \cdot 3^5$</td>
<td>$2^4 \cdot 3^5$</td>
</tr>
<tr>
<td></td>
<td>$Y^2 = X^3 - X - 14$</td>
<td>$-2^5 \cdot 3^3/661$</td>
<td>$-2^7 \cdot 661$</td>
<td>$2^7 \cdot 661$</td>
</tr>
<tr>
<td></td>
<td>$Y^2 + 5XY + Y = X^3$</td>
<td>$5^3 \cdot 101^3/(2 \cdot 7^2)$</td>
<td>$2 \cdot 7^2$</td>
<td>$2 \cdot 7$</td>
</tr>
</tbody>
</table>

|          | Elliptic curve |
|          | 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
4.2 Elliptic curves over subfields of \( \mathbb{C} \)

**Fig. 4.5** \( Y^2 = X^3 - 3X + 3 \)

**Fig. 4.6** \( Y^2 = X^3 + X \)

**Fig. 4.7** \( Y^2 = X^3 - X \)
Fig. 4.8 $y^2 = x^3 + 3$

Fig. 4.9 $y^2 = x^3 + x^2$

Fig. 4.10 $y^2 = x^3$
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

$$D := P - Q \in \text{Div}(E)$$

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 rational function $f \in \mathbb{k}(E)^*$ with

$$\text{div } f = P - Q$$

with $P, Q \in \text{Div}(E)$ the elementary divisors of two distinct points $p \neq q \in E$.

**Proof.** Consider the point divisor

$$Q \in \text{Div}(E)$$

of degree $\deg Q = 1$.

Lemma 4.21 implies

$$\dim H^0(E, \mathcal{O}_Q) = 1.$$ 

Hence the inclusion

$$\mathbb{k} \subset H^0(E, \mathcal{O}_Q)$$

implies

$$\mathbb{k} = H^0(E, \mathcal{O}_Q).$$

Hence each $f \in H^0(E, \mathcal{O}_Q)$ is constant, and therefore $f = 0$ or

$$\text{div } f = 0 \in \text{Div}(E)$$

which implies $p = q$, a contradiction, q.e.d.

Lemma 4.30 shows: The obstructions for a divisor $D \in \text{Div}_0(E)$ to be a principal divisor are divisors of type $P - Q$ or even of type $P - O_\infty$. A divisor $D \in \text{Div}_0(E)$ 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.

**Theorem 4.31 (The class group of degree zero divisors on an elliptic curve).** Consider an elliptic curve $(E/k, O)$.

i) For any divisor $D \in \text{Div}_0(E)$ exists a unique point $p \in E$ with
Denote the corresponding map by
\[ \sigma : \text{Div}_0(E) \to E, \ D \mapsto p. \]

ii) The map \( \sigma \) is surjective. It induces a bijective map
\[ \sigma : \text{Cl}_0(E) \xrightarrow{\approx} E \]
with inverse
\[ E \xrightarrow{\approx} \text{Cl}_0(E), \ p \mapsto [P - O_\infty]. \]

Proof. i) Definition of \( \sigma \): 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
\[ \text{div } f \geq -(D + O_\infty). \]
Because \( \deg (\text{div } f) = 0 \) but \( \deg(-(D + O_\infty)) = -1 \),
there exists a point \( p \in E \) with
\[ \text{div } f = -(D + O_\infty) + P \]
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 \( g \in \overline{k}^*(E) \)
\[ P - Q = \text{div } g, \]
contradicting Lemma 4.30. Therefore
\[ \sigma(D) := p \in E \]
is well-defined.

ii) Bijectivity of \( \sigma \): First we show the surjectivity of \( \sigma \): Consider an arbitrary point \( p \in E \). Set

\[ D \sim P - O_\infty \] (Notation from Definition 4.19)
4.2 Elliptic curves over subfields of $\mathbb{C}$

Then $\sigma(D) = P$ by definition, which proves the surjectivity of $\sigma$.

Secondly, to show that $\sigma$ induces a bijective map $\sigma$ we have to show for each pair of divisors $D_1, D_2 \in \text{Div}_0(E)$:

$$\sigma(D_1) = \sigma(D_2) \iff [D_1] = [D_2] \in \text{Cl}_0(E)$$

We have

$$P := \sigma(D_1) = \sigma(D_2) \iff D_1 \sim P - O_\infty \sim D_2 \iff D_1 \sim D_2 \iff D_1 - D_2 \sim 0 \iff [D_1] = [D_2] \in \text{Cl}_0(E), \text{ q.e.d.}$$

**Definition 4.32 (Group structure of an elliptic curve).** Consider an elliptic curve $(E/k, O)$ and denote by $(\text{Cl}_0(E), +)$ the group of divisor classes of degree zero. The bijective map from Theorem 4.31

$$\sigma : \text{Cl}_0(E) \to E, [P - O_\infty] \mapsto p,$$

carries over the group structure from $(\text{Cl}_0(E), +)$ to $E$: The map

$$+ : E \times E \to E, p + q := \sigma([P - O_\infty] + [Q - O_\infty]),$$

defines an Abelian additive group $(E, +)$ 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

$$D = \sum_{p \in E} n_p \cdot P \in \text{Div}_0(E)$$

is a principal divisor iff

$$\bigoplus_{p \in E} n_p \cdot p = O \in E.$$ 

Here the last equation refers to the group structure $\oplus$ on $E$. The product $n_p \cdot p$ 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
\[ D = D - \sum_{p \in E} n_p \cdot O_\infty = \sum_{p \in E} n_p \cdot (P - O_\infty) \in \text{Div}_0(E) \]
Due to Theorem 4.31, part ii)
\[ D \text{ principal} \iff [D] = 0 \iff \overline{\sigma}([D]) = O \in E \iff \]
\[ \iff \overline{\sigma} \left( \sum_{p \in E} n_p \cdot [P - O_\infty] \right) = O \in E \iff \bigoplus_{p \in E} n_p \cdot \overline{\sigma}([P - O_\infty]) = O \in E \iff \]
\[ \iff \bigoplus_{p \in E} n_p \cdot p = 0 \in E, \ q.e.d. \]

Remark 4.34 (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].
2. **Mordell’s 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 $r < \infty$

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r.$$ 

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.
\[ \text{card } C(\mathbb{Q}) < \infty. \]

The Mordell-conjecture was proved by Faltings, see [58].

**Example 4.35 (Group structure).** 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 \( E(\mathbb{Q})_{\text{tors}} \) has a factor isomorphic to \( \mathbb{Z}/7\mathbb{Z} \). For more information, in particular for the equality

\[ E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/7\mathbb{Z} \]

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 \( E/\mathbb{Q} \).
4.2 Elliptic curves over subfields of $\mathbb{C}$

Fig. 4.12 The group $E(\mathbb{Q})_{\text{tor}}$

Elliptic_curve_torsion_group: Start.

Weierstrass polynom.: $Y^2 = X^3 + (-43X) + (166)$

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
4.3 Elliptic curves over finite fields

The present section starts the investigation of elliptic curves defined over \( \mathbb{Q} \). When multiplying a given Weierstrass polynomial with rational coefficients by the principal nominator of all coefficients one obtains a Weierstrass polynomial with integer coefficients. Hence elliptic curves over \( \mathbb{Q} \) are already defined over the ring \( \mathbb{Z} \).

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 \( \text{Spec} \, \mathbb{Z} \), and all 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 4.28 one has to find a unique minimal discriminant. The corresponding Weierstrass polynomial is named \textit{global minimal}.

**Definition 4.36 (Global minimal Weierstrass polynomial).** For an elliptic curve \( E/\mathbb{Q} \) a Weierstrass polynomial \( F \in \mathbb{Z}[X,Y] \) with integer coefficients is \textit{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 \( \Delta_F \) in the following sense: The elliptic curve \( E/\mathbb{Q} \) has no Weierstrass polynomial \( F_p(X,Y) \in \mathbb{Z}[X,Y] \) with discriminant \( \Delta_{F_p} \) satisfying

\[
\text{ord}_p(\Delta_{F_p}) < v(p).
\]

“Global minimality” is a global property because it refers to all primes of \( \Delta_F \).

**Remark 4.37 (Global minimal Weierstrass polynomial).**

1. **Non-uniqueness 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 4.36 implies for any prime factor \( p \neq 2, 3 \) of its discriminant \( \text{ord}_p(\Delta_F) < 12 \).

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 4.38 (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 discriminant

\[ \Delta_F = -2^4 \cdot 3^3 \cdot 5^{12} \]

is not minimal because \( 5^{12} | \Delta_F \).

The global minimal Weierstrass polynomial is

\[ F_{\text{min}}(X, Y) = Y^2 - (X^3 + 1) \]

with discriminant

\[ \Delta_{F_{\text{min}}} = -2^4 \cdot 3^3. \]
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 coefficient. To obtain a global minimal Weierstrass polynomial, we make the transformation

\[
\left( \begin{array}{c} X \\ Y \end{array} \right) = \left( \begin{array}{c} u^{-2} \cdot X' \\ u^{-3} \cdot Y' \end{array} \right) \quad \text{with} \quad u = 5
\]

and multiply by \( u^6 \). We obtain the Weierstrass equation

\[ Y'^2 = X'^3 + \frac{1}{u} \cdot u^{-2} \cdot u^6 \cdot X' + u^6 \quad \text{i.e.} \quad Y'^2 = X'^3 + 5^3 \cdot X' + 5^6 \]

Hence \( E/\mathbb{Q} \) is also defined by the Weierstrass polynomial

\[ F_{\text{min}}(X, Y) = Y^2 - (X^3 + 5^3 \cdot X + 5^6) \in \mathbb{Z}[X, Y] \]

which is global minimal because

\[ \Delta_{F_{\text{min}}} = -2^4 \cdot 5^9 \cdot 31 \cdot 109 \in \mathbb{Z}, \]
Definition 4.39 (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

$$F_{\text{hom}} \in \mathbb{Z}[X_0, X_1, X_2]$$

the homogenization of $F$. For each prime $p \in \mathbb{N}$ reducing mod $p$ the coefficients of $F_{\text{hom}}$ provides a Weierstrass polynomial

$$F_{\text{hom}, p} \in \mathbb{F}_p[X_0, X_1, X_2]$$

with coefficients from the finite field $\mathbb{F}_p$. The Weierstrass polynomial defines the projective variety

$$E_p := \text{Var}(F_{\text{hom}, p}) := \{(x_0 : x_1 : x_2) \in \mathbb{P}^2(\mathbb{F}_p) : F_{\text{hom}, p}(x_0, x_1, x_2) = 0\} \subset \mathbb{P}^2(\mathbb{F}_p),$$

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 $\text{cond}(E) \in \mathbb{N}^\times$ of $E/\mathbb{Q}$ distinguishes the primes $p$ with semistable reduction from those with unstable reduction: One has

$$\text{cond}(E) = \prod_p p^{e_p}$$

with the same prime factors $p$ as the discriminant $\Delta_F$. 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 4.28 the distinction between stable and not-stable at a prime \( p \) depends on the reduction of the minimal discriminant. The following example 4.40 shows why it is necessary to study elliptic curves by considering global minimal Weierstrass polynomials, not just arbitrary Weierstrass polynomials.

**Example 4.40 (Global minimal Weierstrass polynomial and reduction mod \( p \)).** Consider the elliptic curve \((E/\mathbb{Q}, O)\) from Example 4.38 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 \( \text{mod } p = 5 \) gives the Weierstrass polynomial in short form

\[
F_p(X, Y) = Y^2 - X^3 \in \mathbb{F}_p[X, Y]
\]

with discriminant

\[
\Delta_{F_p} = 0 \in \mathbb{F}_p.
\]

Hence the Weierstrass polynomial \( \mathbb{F}_p \) defines a singular cubic with a cusp. Note that the discriminant \( \Delta_F \) contains the prime factor \( 5^{12} \).

ii) The coordinate transformation with the matrix

\[
\begin{pmatrix}
1/u^2 & 0 \\
0 & 1/u^3
\end{pmatrix}
\]

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 \( F' \text{ mod } p = 5 \) creates the Weierstrass polynomial

\[
F'_p(X', Y') = Y'^2 - (X'^3 + 1)
\]

with discriminant

\[
\Delta_{F'_p} = 3 \in \mathbb{F}_5.
\]

The reduction of \( E \text{ mod } p = 5 \) defines an elliptic curve \( E_5 \) over \( \mathbb{F}_5 \).
Remark 4.41 (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 $E_p \subset \mathbb{P}^2(\mathbb{F}_p)$ with all coordinates in the finite fields $\mathbb{F}_p^n$.

We recall the following result of Hasse for the case $n = 1$:

$$|1 + p - \text{card } E_p(\mathbb{F}_p)| \leq 2 \cdot \sqrt{p}.$$ 

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

$$|\text{card } E_p(\mathbb{F}_p)| \leq (1 + 2p).$$

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 $\text{card } E_p(\mathbb{F}_p)$.

One defines for any prime $p$ the difference

$$a_p(E) := 1 + p - \text{card } E_p(\mathbb{F}_p)$$

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.
3. The sequence

\( (a_p(E))_{p \text{ prime}} \)

will turn out to be a fundamental characteristic of the elliptic curve \( E \), see Remark 4.44. These numbers determine also the cardinalities

\[ \text{card } E_p(F_{p^n}) \]

for \( n \geq 2 \). The latter will serve as the generators of the \( \zeta \)-function of \( E \), see Definition 4.43.
Historically, the first example of a $\zeta$-function is due to L. Euler. The function has later been named Riemann $\zeta$-function.

**Proposition 4.42 ($\zeta$-function and Euler product).** The Riemann $\zeta$-function

$$\zeta : \{s \in \mathbb{C} : \text{Re } s > 1\} \to \mathbb{C}, \quad \zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

is holomorphic. The $\zeta$-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 $s = \frac{1}{2}$

$$\pi^{-s/2} \cdot \Gamma(s/2) \cdot \zeta(s) = \pi^{-(1-s)/2} \cdot \Gamma((1-s)/2) \cdot \zeta(1-s)$$

with the $\Gamma$-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

$$\prod_{p < N} \frac{1}{1 - p^{-s}} = \prod_{p < N} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots\right) = \sum_{n} \frac{1}{n^s}$$

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 $\zeta$-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 $p$

$$\frac{1}{1 - p^{-s}} = \sum_{n=0}^{\infty} (1/p^{-s})^n$$

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 $p$

$$\text{card } E_p(\mathbb{F}_p^n), \ n \in \mathbb{N}^*.$$ 

**Definition 4.43 (Zeta-function of an elliptic curve over $\mathbb{F}_p$).** Consider an elliptic curve $E_p/\mathbb{F}_p$. The $\zeta$-function of $E_p$ is the formal power series with generator derived from the sequence $(\text{card } E_p(\mathbb{F}_p^n))_{n \in \mathbb{N}^*}$

$$Z(E_p, T) := \exp \left( \sum_{n=1}^{\infty} \frac{\text{card } E_p(\mathbb{F}_p^n) \cdot T^n}{n} \right) \in \mathbb{Q}[T].$$

One checks by formal derivation

$$T \cdot \frac{d}{dT} \log Z(E_p, T) = T \cdot \frac{Z'}{Z} = T \cdot \sum_{n=1}^{\infty} (\text{card } E_p(\mathbb{F}_p^n) \cdot T^{n-1}) = \sum_{n=1}^{\infty} (\text{card } E_p(\mathbb{F}_p^n) \cdot T^n)$$

**Remark 4.44 (Properties of the $\zeta$-function of an elliptic curve over $\mathbb{F}_p$).** The $\zeta$-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 $\zeta$-function is a rational function over the ring $\mathbb{Z}$, more precisely:

$$Z(E_p, T) = \frac{L(E_p, T)}{(1 - T) \cdot (1 - pT)} \in \mathbb{Z}(T)$$

with a quadratic polynomial with integer coefficients at the stable points

$$L(E_p, T) = \begin{cases} 1 - a_p(E) \cdot T + p \cdot T^2 & \text{if } E \text{ stable at } p \\ 1 - a_p(E) \cdot T & \text{if } E \text{ semistable or unstable at } p \end{cases}$$

Here

$$a_p(E) := 1 + p - \text{card } E_p(\mathbb{F}_p).$$

2. **Functional equation:** The $\zeta$-function satisfies the functional equation

$$Z(E_p, 1/pT) = Z(E_p, T).$$

3. **Analogue of the Riemann hypothesis:** For stable $E_p$ both complex zeros $\alpha, \beta \in \mathbb{C}$ of $L(E_p, T)$ have modulus

$$|\alpha| = |\beta| = \sqrt{p}.$$
4.3 Elliptic curves over finite fields

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 $\zeta$-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 4.45 (L-series of an elliptic curve over $\mathbb{Q}$).** The $L$-series of an elliptic curve $E/\mathbb{Q}$ is the function

$$L(E, s) : \{s \in \mathbb{C} : \text{Re } s > 3/2\} \to \mathbb{C}, \quad L(E, s) := \prod_p \frac{1}{Z(E_p, p^{-s})}$$

**Remark 4.46 (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 4.41 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

$$\text{rank } E(\mathbb{Q}) = r$$

with $r$ equal to the analytic rank defined as the order of the zero of the $L$-series at $s = 1$

$$r := \text{ord}(L(E); 1).$$

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 $\zeta$-function $Z(E_p, T)$ evaluate at $T = p^{-s}$ as values of the Riemann $\zeta$-function

$$\frac{1}{1 - p^{-s}} = \zeta(s)$$ 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 $\zeta$-function $\zeta(s)$ on the level of the two product representations

$$L(E, s) = \prod_{p} \frac{1}{Z(E_p, p^{-s})}$$ and $$\zeta(s) = \prod_{p} \frac{1}{1 - p^{-s}}$$

then for each given prime $p$ the local factor

$$Z(E_p, p^{-s})$$ corresponds to $$\frac{1}{1 - p^{-s}}$$

The geometric series on the right hand side depends only on the prime $p$, while the corresponding $\zeta$-function on the left-hand side depends on $p$ and on the reduction of the given elliptic curve $E/\mathbb{Q}$. 
Fig. 4.15 Analytic rank of several elliptic curves $E/\mathbb{Q}$
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 *multiplicative* 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
\[ \sigma_k : \mathbb{N}^* \to \mathbb{N}^*, \quad \sigma_k(n) := \sum_{d|n} d^k, \]
is multiplicative. It has the product representation
\[ \sigma_k(n) = \prod_{j=1}^{\nu(n)} \left( \frac{p_j^{(e_j+1)k} - 1}{p_j^k - 1} \right) \]

**Proof.** The prime decomposition
\[ n = \prod_{j=1}^{\nu(n)} p_j^{e_j}, \quad n \in \mathbb{N}^*, \]
and the formula for the finite geometric series imply the product formula
\[ \sigma_k(n) = \left( p_1^k + p_1^{k^2} + ... + p_1^{k^{e_1}} \right) \cdot ... \cdot \left( p_N^k + p_N^{k^2} + ... + p_N^{k^{e_N}} \right) = \]
Introduction to Hecke theory and applications

\[ N \prod_{j=1}^{\infty} \left( \sum_{\nu=0}^{p_j} \left( p_j^{\nu} \right) \right) = N \prod_{j=1}^{\infty} \frac{p_j^{(e_j+1)k} - 1}{p_j^k - 1} \]

And the product formula implies for coprime \( n, m \in \mathbb{N}^* \)

\[ \sigma_k(n) \cdot \sigma_k(m) = \sigma_k(n \cdot m), \text{ q.e.d.} \]

**Corollary 5.3 (Eisenstein series are multiplicative).** For each even \( k \geq 4 \) the Fourier coefficients of the Eisenstein series

\[ \frac{-B_k}{2k} \cdot E_k(\tau) = \sum_{\nu=0}^{\infty} c_{\nu} \cdot q^{\nu}, \quad q = e^{2\pi i \tau}, \]

are multiplicative.

**Proof.** We reduce the statement of the corollary to Proposition 5.2: Corollary 3.11 shows

\[ E_k(\tau) = 1 - \frac{2k}{B_k} \sum_{\nu=1}^{\infty} \sigma_{k-1}(\nu) \cdot q^{\nu}, \quad q = e^{2\pi i \tau} \]

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 coefficients

\[ c_{\nu} = \sigma_{k-1}(\nu), \quad \nu \geq 1, \text{ q.e.d.} \]

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 \( \tau \)-function.

Hecke operators are linear maps on modular forms, more precisely: For each even weight \( k \in \mathbb{N} \) the Hecke algebra

\[ \mathcal{H}_k(\Gamma) \subset \text{End}_k(M_k(\Gamma)) \]

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 \( \mathcal{H}_k(\Gamma) \) 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.

**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

\[ \Gamma_{m, \text{prim}} := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_m : (a, b, c, d) = 1 \right\} \]

of primitive matrices. We denote by

\[ \Phi_m : \Gamma \times \Gamma_m \rightarrow \Gamma_m, (A, M) \mapsto A \cdot M \]

the canonical \( \Gamma \)-left action, and by

\[ \Phi_{m, \text{prim}} := \Phi_m |_{\Gamma_{m, \text{prim}}} : \Gamma \times \Gamma_{m, \text{prim}} \rightarrow \Gamma_{m, \text{prim}} \]

its restriction. The respective orbits sets are denoted as the left quotients

\[ \Gamma \backslash \Gamma_m \] and \[ \Gamma \backslash \Gamma_{m, \text{prim}}. \]

**Remark 5.5 (Restriction of the \( \Gamma \)-action to the primitive matrices).** The subset

\[ \Gamma_{m, \text{prim}} \subset \Gamma_m \]

is stable under the \( \Gamma \)-left action \( \Phi_m \).

**Proof.** For the proof consider any

\[ A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma \text{ and } M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_{m, \text{prim}}. \]

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
which implies

\[(1) = I\]

Hence the coefficients of the product matrix \(A \cdot M\) are coprime, i.e.

\[\Phi_m(A, M) = A \cdot M \in \Gamma_{m, \text{prim}}, \text{ q.e.d.}\]

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

\[\Gamma \backslash \Gamma_m \xrightarrow{\sim} V(m) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Gamma_m : 0 \leq b < d \right\}\]

to a subset of upper triangular matrices. The orbit set of \(\Phi_m\) has cardinality \(\sigma_1(m)\).

2. A bijective map exists

\[\Gamma \backslash \Gamma_{m, \text{prim}} \xrightarrow{\sim} V(m, \text{prim}) := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in V(m) : (a, b, d) = 1 \right\}\]

The orbit set of \(\Phi_{m, \text{prim}}\) has cardinality

\[\psi(m) := m \cdot \prod_{p \mid m} (1 + (1/p))\]

**Proof.** 1. We define a map

\[p : \Gamma_m \rightarrow V(m),\]

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 \( \gamma \) and \( \delta \) 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
\[ A_{21} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad \text{and} \quad M_i := \begin{pmatrix} a_i & b_i \\ 0 & d_i \end{pmatrix}, \quad i = 1, 2. \]

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 \( b_1 + \beta \cdot d_1 = d_2 \).
- Because \( 0 \leq b_1, b_2 < d_1 = d_2 \) we get \( b_1 = b_2 \) and \( \beta = 0 \).

As a consequence
\[ A_{21} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \text{or} \quad A_1 = A_2. \]

iii) Part i) and ii) show that
\[ p : \Gamma_m \to V(m), \quad M \mapsto A \cdot M, \]
is well-defined, and \( p(M) \) belongs to the same orbit as \( M \).

iv) The map \( p \) is surjective 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
\[ \Gamma \setminus \Gamma_m \to V(m), \quad \overline{M} \mapsto p(M). \]

v) The equality
\[ \text{card } V(m) = \sigma_m(1) \]
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 \( \Gamma \setminus \Gamma_{m, \text{prim}} \) follows from part 1) by restriction.
For the cardinality of \( V(m, \text{prim}) \) 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 \( \Gamma \setminus \Gamma_m \), i.e. with respect to the canonical projection
\[ \Gamma_m \to \Gamma \setminus \Gamma_m, \ M \mapsto [M], \]
holds the equality of sets
\[ \Gamma \setminus \Gamma_m = \{ [M] : M \in V(m) \} = \{ [M \cdot \gamma] : M \in V(m) \}. \]

2. The set
\[ V(m, \text{prim}) \cdot \gamma \subset \Gamma_m, \text{prim} \]
is a complete set of representatives of the orbit set \( \Gamma \setminus \Gamma_m, \text{prim} \).

Proof. Consider a fixed, but arbitrary \( \gamma \in \Gamma \). 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 \( M \), 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
\[ \Phi_{\text{left}} : \Gamma \times \Gamma_p \to \Gamma_p, (\gamma, M) \mapsto \gamma \cdot M \]
1. Besides the set \( V(p) \) from Lemma 5.6 the set of symmetric matrices
\[ V_{\text{sym}} := \left\{ \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 1 \\ b \\ b^2 \end{pmatrix} : 0 \leq b < p \right\} \]
is a complete set of representatives of \( \Phi_{\text{left}} \) too.

2. Consider a complete set \( \mathcal{Y} \) of representatives of \( \Phi_{\text{left}} \) formed by symmetric matrices. Then also the system of adjoints
\[ \mathcal{Y}^\dagger := \{ M' : M \in \mathcal{Y} \}, \ M' := (\det M) \cdot M^{-1}, \]
is a complete systems of representatives of $\Phi_{left}$.

Proof. 1. For each $0 \leq b < p$

$$\begin{pmatrix} 1 & b \\ b & p+b^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix}$$

Hence the matrices

$$\begin{pmatrix} 1 & b \\ b & p+b^2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix}$$

belong to the same orbit of $\Phi_{left}$.

2. i) Let

$$\Phi_{right}: \Gamma_p \times \Gamma \to \Gamma_p, \quad (M, \gamma) \mapsto M \cdot \gamma,$$

be the corresponding right action of $\Gamma$. For each complete system $\mathcal{V}$ of representatives of $\Phi_{left}$ the set of transposed elements

$$\mathcal{V}^\top := \{v^\top : v \in \mathcal{V}\}$$

is a complete system of representatives of $\Phi_{right}$. Assume $v \in \Gamma_p$. Then also $v^\top \in \Gamma_p$ and

$$v^\top = A \cdot M$$

for suitable

$$A \in \Gamma \quad \text{and} \quad M \in \mathcal{V}.$$ 

Hence

$$v = M^\top \cdot A^\top$$

with $A^\top \in \Gamma^\top = \Gamma$.

As a consequence, if $\mathcal{V}$ is formed by symmetric matrices, then $\mathcal{V}$ is also a complete system of representatives for $\Phi_{right}$.

ii) For given $w \in \Gamma_p$ set

$$v := (\det w) \cdot w^{-1} \in \Gamma_p.$$ 

Then

$$\det v = (\det w)^2 \cdot \det w^{-1} = \det w \quad \text{and} \quad w = (\det v) \cdot v^{-1}$$

Due to part i) exist

$$A \in \Gamma \quad \text{and} \quad M \in \mathcal{V}$$

with

$$v = M \cdot A$$

Then

$$\det v = \det M$$
5.1 Hecke operators of the modular group and their eigenforms

and

\[ v^{-1} = A^{-1} \cdot M^{-1} \]

and

\[ w = v^{-1} \cdot \det v = A^{-1} \cdot ((\det M) \cdot M^{-1}) \]

with

\[ A^{-1} \in \Gamma^{-1} = \Gamma, \ q.e.d. \]

**Definition 5.9 (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

\[ T_m : M_k(\Gamma) \to M_k(\Gamma) \]

which is defined on \( M_k(\Gamma), k \in \mathbb{N} \), as

\[ M_k(\Gamma) \to M_k(\Gamma), f \mapsto T_m f := \sum_{\Gamma \setminus \Gamma_m} f[M]_k. \]

Here the summation extends over an arbitrary complete set of representatives \( M \in \Gamma_m \) of the orbit set \( \Gamma \setminus \Gamma_m \) 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 5.9 of the Hecke operator \( T_m \) may extend over the elements of \( V(m) \) or over the elements of \( V(m) \cdot \gamma, \gamma \in \Gamma \).

**Theorem 5.10 (Fourier coefficients of Hecke transforms).**

1. The Hecke operators from Definition 5.9 are well-defined, i.e. for each even weight \( k \) and for all \( m \geq 1 \)

\[ f \in M_k(\Gamma) \iff T_m f \in M_k(\Gamma). \]

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
\[
b_n = \begin{cases} 
a_0 \cdot \sigma_{k-1}(m) & \text{if } n = 0 \\
a_m & \text{if } n = 1 \\
\sum_{r > 0, r | (m, n)} r^{k-1} \cdot a_{mn/r^2} & \text{if } n > 1 \end{cases} \]

3. The ideal of cusp forms is stable under all Hecke operators, i.e. for each \(m \in \mathbb{N}^*\)
\[
T_m(S_\ast(\Gamma)) \subset S_\ast(\Gamma).
\]

Due to Theorem 5.10, 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:

- Apparentely \(T_m f\) 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 \(\infty\): 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) \(\exp(2\pi in \cdot M(\tau)) = \exp \left(2\pi in \cdot \frac{a\tau + b}{d}\right) = e^{2\pi in(\tau/d)} \cdot e^{2\pi in(b/d)}, \ n \in \mathbb{N}.\)
5.1 Hecke operators of the modular group and their eigenforms\[189\]

ii) \[
\sum_{0 \leq b < d} e^{2\pi i b (n/d)} = \begin{cases} 
    d & \text{if } d | n \\
    0 & \text{otherwise}
\end{cases}
\]

The first case follows from \[e^{2\pi i b (n/d)} = 1\] for each of the \(d\) summands with \(0 \leq b < d\). The second case follows from the formula of the finite geometric series with argument \[e^{2\pi i (n/d)}:\]
\[
\sum_{b=0}^{d-1} e^{2\pi i b (n/d)} = \frac{e^{2\pi i d (n/d)} - 1}{e^{2\pi i (n/d)} - 1} = 0
\]

iii) We have
\[
f(M(\tau)) = f(\alpha \tau + b) = \sum_{n=0}^{\infty} a_n \cdot \exp\left(2\pi i n \cdot \frac{\alpha \tau + b}{d}\right) = \\
= \sum_{n=0}^{\infty} a_n \cdot \exp\left(2\pi i n \cdot \frac{\alpha \tau}{d}\right) \cdot \exp\left(2\pi i n \cdot \frac{b}{d}\right)
\]

Hence
\[
\sum_{b=0}^{d-1} f(M(\tau)) = \sum_{n=0}^{\infty} d \cdot a_{nd} \cdot q^{n(m/d)}, \quad q = \exp(2\pi i n),
\]

because
\[
\sum_{b=0}^{d-1} f(M(\tau)) = \sum_{n=0}^{\infty} \left( \sum_{b=0}^{d-1} a_n \cdot e^{2\pi i n(\alpha \tau)/d} \cdot e^{2\pi i n(b/d)} \right) = \\
= \sum_{n=0}^{\infty} a_n \cdot e^{2\pi i n(\alpha \tau)/d} \cdot \sum_{b=0}^{d-1} e^{2\pi i n(b/d)} = \sum_{n=0}^{\infty} a_{nd} \cdot e^{2\pi in\alpha \tau} \cdot d = \\
= d \cdot \sum_{n=0}^{\infty} a_{nd} \cdot q^{nd} = d \cdot \sum_{n=0}^{\infty} a_{nd} \cdot q^{n(m/d)}
\]

Due to part ii) the two final sums retain only summands with index \(nd\).

We now use the representation of the orbit set \(\Gamma \setminus \mathcal{I}_m\) from Lemma 5.6 and insert the Fourier series of \(f\). We obtain due to the formula from part iii)
\[
(T_m f)(\tau) = \sum_{M \in \mathcal{V}(m)} f(M(\tau)) = m^{k-1} \cdot \sum_{M \in \mathcal{V}(m)} h(M, \tau)^{-k} \cdot f(M(\tau)) = \\
\]
\[ = m^{k-1} \sum_{d \mid m} \frac{1}{d^2} \sum_{n=0}^{\infty} a_{nd} \cdot q^{n(m/d)} \cdot d = \sum_{d>0} \left( \frac{m}{d} \right)^{k-1} \left( \sum_{n=0}^{\infty} a_{nd} \cdot q^{n(m/d)} \right) = \]

\[ \sum_{d>0} \left( \frac{m}{d} \right)^{k-1} \left( \sum_{n=0}^{\infty} a_{nd} \cdot q^{n(m/d)} \right) \]

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

\[(T_m f)(\tau) = \sum_{t=0}^{\infty} \left( \sum_{r>0} \left( \frac{r^{k-1} \cdot a_{(tm)/r^2}}{r} \right) \right) q^t \]

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 5.10. It gives the formula for the Fourier coefficients of the Hecke transform for prime indices.

**Corollary 5.11 (Fourier coefficients with prime index of Hecke transforms).**

Consider a modular form \( f \in \mathcal{M}_k(\Gamma) \) 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 \( p \)

\[ b_p = \begin{cases} a_{mp} & \text{if } p \nmid m \\ a_{mp} + p^{k-1} \cdot a_{m/p} & \text{if } p \mid m \end{cases} \]
**Proof.** The claim follows from the third formula for the general case in Theorem 5.10:

- If \( p \nmid m \) then \( r \mid (p, m) \) implies \( r = 1 \).
- If \( p \mid m \) then \( r \mid (p, m) \) implies \( r = 1 \) or \( r = p \); note \( n = p \), q.e.d.

**Corollary 5.12 (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. \( \Delta \) is an eigenvector of all Hecke operators

\[
T_m \in \text{End}(S_{12}(\Gamma)), \ m \geq 1.
\]

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 \( \Delta \) from Definition 3.13 as a basis. Hence \( \Delta \) 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 5.10 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 5.13 (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

\[ f_1 := \Delta \cdot E_4^4 \quad \text{and} \quad f_2 := \Delta^2 \cdot E_4 \]

are linearly independent because

\[ \text{ord}(f_1; \infty) = 1 \quad \text{and} \quad \text{ord}(f_2; \infty) = 2. \]

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 \((f_1, f_2)\)
5.1 Hecke operators of the modular group and their eigenforms

The result from Figure 5.1 has been computed by the PARI script `Hecke_matrix_02`.

It is not by chance that in Example 5.13 the Hecke endomorphism \( T_2 \in \text{End}(S_{28}(\Gamma)) \) can be diagonalized. Theorem 5.16 will show: The Hecke algebra of a given weight is commutative. And Theorem 5.24 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 5.14 (Hecke algebra of weight \( k \)).** The Hecke algebra of even weight \( k \in \mathbb{N} \)

\[
\text{Hecke}_k(\Gamma) \subset \text{End}(M_k(\Gamma))
\]

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 5.16 about the Hecke algebra we consider for two matrices
\[ M_j = \begin{pmatrix} a_j & b_j \\ 0 & d_j \end{pmatrix} \in V(n_j), \quad j = 1, 2 \]

the components of the product

\[ M_1 \cdot M_2 = \begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 d_2 \\ 0 & d_1 d_2 \end{pmatrix} \in \Gamma_{n_1 \cdot n_2} \]

We want to show that the products form a complete set of representatives of the \( \Gamma \)-left action on \( \Gamma_{n_1 \cdot n_2} \).

**Lemma 5.15 (Relaation system for \( V(n_1 \cdot n_2) \)).** For \( j = 1, 2 \) consider two coprime numbers

\[ n_j \in \mathbb{N}^*, \quad j = 1, 2. \]

1. For given positive numbers \( a_j, d_j \) with \( n_j = a_j \cdot d_j \) the map

\[ \phi : (\mathbb{Z}/d_1 \mathbb{Z}) \times (\mathbb{Z}/d_2 \mathbb{Z}) \to \mathbb{Z}/d_1 d_2 \mathbb{Z}, \quad (b_1, b_2) \mapsto a_1 \cdot b_2 + b_1 \cdot d_2 \]

is bijective.

2. The map of the product of complete systems of representatives

\[ V(n_1) \times V(n_2) \to V(n_1 \cdot n_2), \quad (M_1, M_2) \mapsto M_1 \cdot M_2, \]

is well-defined and bijective.

**Proof.**

1. It suffices to show that \( \phi \) 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
5.1 Hecke operators of the modular group and their eigenforms

\[ b_2 = \tilde{b}_2. \]

Analogously \( b_1 = \tilde{b}_1. \)

2. In addition to part 1) one uses the bijectivity of the maps of divisor sets

\[ \{ a_1 \in \mathbb{N}^* : a_1 | n_1 \} \times \{ a_2 \in \mathbb{N}^* : a_2 | n_2 \} \to \{ a \in \mathbb{N}^* : a | n_1 n_2 \}, (a_1, a_2) \mapsto a_1 a_2, \text{ q.e.d}. \]

**Theorem 5.16 (The Hecke algebras are commutative).** For each weight \( k \in \mathbb{N} \) the Hecke algebra \( \text{Hecke}_k(\Gamma) \) is commutative. It has the following properties:

1. For coprime \( n, m \in \mathbb{N}^* \) Hecke operators are multiplicative:

\[ T_m \circ T_n = T_{mn} \]

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 \( \text{Hecke}_k(\Gamma) \) is generated by the family \( T_p, p \text{ prime} \).

**Proof.** 1. For each \( f \in M_k(\Gamma) \) Lemma 5.15 and Lemma 3.4 imply

\[ (T_m \circ T_n)(f) = T_m(T_n f) = \sum_{M_2 \in V(m)} (T_n f)[M_2]k = \sum_{M_2 \in V(m)} \left( \sum_{M_1 \in V(n)} (f[M_1]k)[M_2]k \right) = \sum_{M_1 \in V(n) \atop M_2 \in V(m)} f[M_1 M_2]k = \sum_{M \in V(nm)} f[M]k = T_{nm} f \]

2. The proof is by induction. First one replaces Lemma 5.15 by two analogous results about restsystems. Secondly, one evaluates the formula for the Fourier coefficients of Hecke transforms from Theorem 5.10 and Corollary 5.11, 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 \( T_p \), 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 5.17 (Hyperbolic volume form).** The hyperbolic volume form on \( \mathbb{H} \) is the differential form

\[
d\mu(\tau) := \frac{dx \wedge dy}{\gamma^2}, \quad \tau = x + iy \in \mathbb{H}
\]

**Lemma 5.18 (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

\[
d\mu(\tau) = \frac{i}{2} \frac{d\tau \wedge d\overline{\tau}}{(Im \tau)^2}
\]

and

\[
(\gamma^* d\mu)(\tau) = \frac{i}{2} \frac{d\gamma(\tau) \wedge d\overline{\gamma(\tau)}}{(Im \gamma(\tau))^2}
\]

The proof of Proposition 3.1 and the formulas from Remark 2.8

\[
Im \gamma(\tau) = \frac{Im \tau}{|c\tau + d|^2} \text{ and } d\gamma(\tau) = \frac{d\tau}{(c\tau + d)^2}
\]

imply

\[
(\gamma^* d\mu)(\tau) = d\mu(\tau), \text{ q.e.d.}
\]
5.2 The Petersson scalar product

Proposition 5.19 (Volume of fundamental domains). The fundamental domain \( \mathcal{D} \) of \( \Gamma \) has the volume

\[
\text{vol} \mathcal{D} := \int_{\mathcal{D}} d\mu = \frac{\pi}{3}
\]

More general, for the congruence subgroup \( \Gamma_0(N) \)

\[
\text{vol} (\mathcal{D}(\Gamma_0(N))) = \frac{\pi}{3} N \cdot \prod_{p|N} (1 + (1/p)).
\]

Proof. From the geometrical description of \( \mathcal{D} \), see Figure 2.1:

\[
\int_{\mathcal{D}} d\mu = \int_{-1/2}^{1/2} \left( \int_{1 - 1/2}^{\infty} \frac{dy}{\sqrt{1 - x^2}} \right) dx = \int_{-1/2}^{1/2} \left( -1/y \right) \left|_{1 - 1/2}^{\infty} \right. = \arcsin x \left|_{-1/2}^{1/2} \right. = \frac{\pi}{2} \cdot (1/6) = \pi/3
\]

The general formula for

\[
\text{vol} (\mathcal{D}(\Gamma_0(N))) = [\Gamma : \Gamma_0(N)] \cdot \text{vol} \mathcal{D}
\]

follows from the index formula Proposition 2.14 and the representation of the fundamental domain as disjoint union

\[
\mathcal{D}(\Gamma_0(N)) = \bigcup_{j=1}^{[\Gamma : \Gamma_0(N)]} \gamma \cdot \mathcal{D}(\Gamma_0(N))
\]

in the proof of Corollary 2.18, q.e.d.

Definition 5.20 (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

\[
\langle -, - \rangle_{\Gamma_0(N)} : S_k(\Gamma_0(N)) \times S_k(\Gamma_0(N)) \rightarrow \mathbb{C},
\]

\[
\langle f, g \rangle_{\Gamma_0(N)} := \frac{1}{[\Gamma : \Gamma_0(N)]} \int_{\mathcal{D}(\Gamma_0(N))} f(\tau) \overline{g(\tau)} \cdot (\text{Im} \tau)^k \, d\mu(\tau)
\]

Theorem 5.21 (Petersson scalar product). The map from Definition 5.20

\[
\langle -, - \rangle_{\Gamma_0(N)}
\]

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 5.19 implies the estimate
\[
\frac{1}{|\Gamma : \Gamma_0(N)|} \int_{\mathcal{D}(\Gamma_0(N))} |\phi| \, d\mu \leq \text{vol}(\mathcal{D}) \cdot \|\phi\|_H < \infty
\]
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 \( \phi : \mathbb{H} \to \mathbb{C} \),
\[ \phi(\tau) := f(\tau) \cdot \overline{g(\tau)} \cdot (\text{Im} \, \tau)^k. \]
i) The function \( \phi \) is \( \Gamma_0(N) \)-invariant because for each \( \gamma \in \Gamma_0(N) \) and \( \tau \in \mathbb{H} \) according to Definition 3.6
\[
\phi(\gamma(\tau)) = f(\gamma(\tau)) \cdot \overline{g(\gamma(\tau))} \cdot (\text{Im} \, \gamma(\tau))^k =
\]
\[
f[\gamma]^k(\tau) \cdot h(\gamma, \tau)^k \cdot \overline{g[\gamma]^k(\tau)} \cdot \text{Im} \, \gamma(\tau)^k \cdot (\text{Im} \, \gamma \cdot |h(\gamma, \tau)|^{-2k}) =
\]
\[
f[\gamma]^k(\tau) \cdot \overline{g[\gamma]^k(\tau)} \cdot \text{Im} \, \gamma = f(\tau) \cdot \overline{g(\tau)} \cdot \text{Im} \, \tau = \phi(\tau)
\]
i) To prove the boundedness of \( \phi \) it suffices to prove for any \( \gamma \in \Gamma \) that the restriction
\[ (\phi \circ \gamma)|_{\mathcal{D}} \]
is bounded: Being continuous \( \phi \circ \gamma \) is bounded on each compact subset of \( \mathcal{D} \). Secondly, the Fourier expansions with \( q = e^{2\pi i \tau} \)
\[ f[\gamma]^k(\tau) = \sum_{n=1}^{\infty} \alpha_n \cdot q_n^k \quad \text{and} \quad g[\gamma]^k(\tau) = \sum_{n=1}^{\infty} \beta_n \cdot q_n^k, \quad q_n = e^{2\pi i \tau/h}, \]
for a suitable \( h \in \mathbb{N} \), show that both cusp forms are of type \( O(q_h) \) for \( \lim_{\tau \to \infty} \). Then
\[ |q_h| = |e^{2\pi i \tau/h}| = e^{-2\pi \cdot (\text{Im} \, \tau)/h} \quad \implies \quad O(q_h^2) \cdot (\text{Im} \, \tau)^k = o(q_h) \]
which finishes the proof, q.e.d.

Note. The proof of Theorem 5.21 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 5.22 (Petersson scalar product). Consider
5.2 The Petersson scalar product

- 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. Integrating an invariant integrand over different fundamental domains: Consider a continuous function
   \[ \Omega : \mathbb{H} \to \mathbb{C} \]
   with fixed group
   \[ \Gamma(\Omega) := \{ A \in \Gamma : \Omega \circ A = \Omega \}. \]
   For each subgroup \( K \subset \Gamma(\Omega) \) and for each pair \((\mathcal{F}_1, \mathcal{F}_2)\) of fundamental domains of the \( K \)-action
   \[ K \times \mathbb{H} \to \mathbb{H} \]
   holds:
   \[ \int_{\mathcal{F}_1} \Omega \, d\mu = \int_{\mathcal{F}_2} \Omega \, d\mu \]
   if at least one of the two integrals is finite.

2. Transformation formula for subgroups of finite index: Each subgroup \( K \subset \Gamma(\Omega) \)
   with finite index \([\Gamma(\Omega) : K] < \infty\) satisfies
   \[ \frac{1}{[\Gamma(\Omega) : K]} \int_{\mathcal{F}(K)} \Omega \, d\mu = \int_{\mathcal{F}(\Gamma(\Omega))} \Omega \, d\mu \]
   if at least one of the two integrals is finite.

3. Finiteness of the index under conjugation: The congruence subgroup of \( \Gamma \)
   \[ \Gamma(p) := \{ L \in \Gamma : L \equiv 1 \mod p \} \]
   has finite index. In addition, define for each pair of continuous functions
   \[ h_1, h_2 : \mathbb{H} \to \mathbb{C} \]
   the function
   \[ \Omega(h_1, h_2) : \mathbb{H} \to \mathbb{C}, \Omega(h_1, h_2)(\tau) := (h_1 \cdot h_2)(\tau) \cdot (Im \; \tau)^k \]
   Then with respect to the fixed groups holds the inclusion of subgroups
   \[ \Gamma(\Omega(f[M]_k, g)) \text{ and } \Gamma(\Omega(f, g[M']_k)) : \]
   \[ \Gamma(p) \subset \Gamma(\Omega(f[M]_k, g)) \text{ and } M^{-1}\Gamma(p)M \subset \Gamma(\Omega(f[M]_k, g)), \]
   and both subgroups have finite index. An analogous result holds for
   \[ \Gamma(p) \subset \Gamma(\Omega(f, g[M']_k)) \text{ and } M\Gamma(p)M^{-1} \subset \Gamma(\Omega(f, g[M']_k)). \]
4. Invariance of the index under conjugation:

\[ [\Gamma : \Gamma(p)] = [\Gamma : M^{-1}\Gamma(p)M] \]

**Proof.** Cf. [36, Kap. IV, §3.3]. Because \( k \) is fixed during the whole computation we simplify the notation \( \lbrack - \rbrack := \lbrack - \rbrack_k \).

1. 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 \( A(\mathcal{F}_2), A \in K \), and observes that \( \pm 1 \) act as identity on \( \mathbb{H} \), then

\[ \int_{\mathcal{F}_1} \Omega \, d\mu = (1/2) \cdot \sum_{A \in K} \int_{A(\mathcal{F}_2) \cap \mathcal{F}_1} \Omega \, d\mu = (1/2) \cdot \sum_{A \in K} \int_{\mathcal{F}_2} \Omega \, d\mu = \int_{\mathcal{F}_2} \Omega \, d\mu \]

2. Consider a fundamental domain \( \mathcal{F} \) of \( \Gamma(\Omega) \). Then each decomposition of \( \Gamma(\Omega) \) into the finite number \( [\Gamma(\Omega) : K] \) of residue classes with respect to \( K \)

\[ \Gamma(\Omega) = \bigcup_v K \cdot M_v \]

provides a fundamental domain of \( K \)

\[ \mathcal{G} = \bigcup_v M_v, \mathcal{F} \]

The previous part, applied to each pair \( (\mathcal{F}, M_v(\mathcal{F})) \) of fundamental domains of \( \Gamma(\Omega) \), implies

\[ \int_{M_v, \mathcal{F}} \Omega \, d\mu = \int_{\mathcal{F}} \Omega \, d\mu, \]

hence

\[ \int_{\mathcal{G}(K)} \Omega \, d\mu = \int_{\mathcal{G}} \Omega \, d\mu = \sum_v \int_{M_v, \mathcal{F}} \Omega \, d\mu = \]

\[ = \sum_v \int_{\mathcal{F}} \Omega \, d\mu = [\Gamma(\phi) : K] \cdot \int_{\mathcal{G}(\Gamma(\Omega))} \Omega \, d\mu \]

3. For each level \( N \in \mathbb{N}^\ast \) the canonical map

\[ SL(2,Z) \to SL(2,Z/NZ) \]

has as kernel the principal congruence subgroup

\[ \Gamma(N) := \{ \gamma \in \Gamma : \gamma \equiv \mathbb{I} \mod N \}. \]
Because the image of the canonical map is contained in the finite group $SL(2,\mathbb{Z}/N\mathbb{Z})$ the index

$$[\Gamma : \Gamma(N)]$$

is finite - one can even compute

$$[\Gamma : \Gamma(N)] = \text{card } SL(2,\mathbb{Z}/N\mathbb{Z}) = N^3 \prod_{p|N} (1 - (1/p^2)).$$

Each element $L \in \Gamma(p) \subset \Gamma$ with decomposition

$L = \pm \mathbb{1} + p \cdot A, \ A \in M(2 \times 2, \mathbb{Z})$.

has the conjugate

$L_0 := MLM^{-1} = M(\pm \mathbb{1} + p \cdot A)M^{-1} = \pm \mathbb{1} + M(pA)M^{-1} = \pm \mathbb{1} + MAM'$

Hence

$L_0 \in \Gamma$ and $L_0 M = ML$

which implies

$$(f[M])[L] = (f[L_0])[M]_k = f[M].$$

Because $\Gamma(p) \subset \Gamma$ also

$g[L] = g$.

The two $L$-invariant elements $f[M]$ and $g$

satisfy for $\tau \in \mathbb{H}$ the transformation formula

$$(f[M] \cdot g)(L(\tau)) = (f[M] \cdot g)(\tau) \cdot |h(L, \tau)|^{2k}:$$

We compute

$$(f[M] \cdot g)(L(\tau)) = f[M](L(\tau)) \cdot g(L(\tau)) = (f[M]|L)(\tau) \cdot h(L, \tau)^k \cdot g(L(\tau)) =$$

$$= f[M](\tau) \cdot h(L, \tau)^k \cdot g[L](\tau) \cdot |h(L, \tau)|^k = f[M](\tau) \cdot g(\tau) \cdot |h(L, \tau)|^{2k}$$

Multiplying by $(Im \ L(\tau))^k$ both sides of the transformation formula for

$f[M]$ 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

$$(f[M]|_k \cdot g)(L(\tau)) \cdot (Im \ L(\tau))^k = (f[M]|_k \cdot g)(\tau) \cdot (Im \ \tau)^k$$
or
\[ \Omega(f[M], g) \circ L = \Omega(f[M], g) \]
Because \( L \in \Gamma(p) \) is arbitrary we have shown
\[ \Gamma(p) \subset \Gamma(\Omega(f[M], g)) \]
The finiteness of \( \Gamma(p) \) and of its \( M \)-conjugate in the fixgroups follow from the finiteness
\[ [\Gamma : \Gamma(p)] < \infty \]
4. We consider the two subgroups of \( \Gamma \) from part 3)
\[ \Gamma(p) \subset \Gamma \text{ and } K := M^{-1}\Gamma(p)M. \]
Consider a fundamental domain \( \mathcal{F} \subset \mathbb{H} \) of \( \Gamma(p) \). Then \( M^{-1}\mathcal{F} \) is a fundamental domain of \( K \): For each \( x \in \mathbb{H} \) also \( M(x) \in \mathbb{H} \). Hence by assumption exists a unique \( \gamma \in \Gamma(p) \) with
\[ \gamma(M(x)) \in \mathcal{F}. \]
Then
\[ M^{-1}(\gamma(M(x))) = (M^{-1}\gamma M)(x) \in M^{-1}\mathcal{F}. \]
The uniqueness of \( \gamma \) 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 5.18
\[ [\Gamma : \Gamma(p)] \cdot \text{vol} \mathcal{D} = \text{vol} \mathcal{F} = \int_{\mathcal{F}} d\mu = \int_{M^{-1}\mathcal{F}} d\mu = \text{vol}(M^{-1}\mathcal{F}) = [\Gamma : K] \cdot \text{vol} \mathcal{D} \]
Hence
\[ [\Gamma : \Gamma(p)] = [\Gamma : K] = [\Gamma : M^{-1}\Gamma(p)M], \]
in particular independent from \( M \in \Gamma_p \), q.e.d.

**Theorem 5.23 (Selfadjointness of the Hecke operators).** For each even weight \( k \geq 0 \) the Hecke operators
\[ T_m \in \text{End}(S_k(\Gamma)), \quad m \in \mathbb{N}, \]
are self-adjoint with respect to the Petersson scalar product, i.e. for all \( f, g \in S_k(\Gamma) \)
\[ \langle T_m f, g \rangle = \langle f, T_m g \rangle \]
**Proof.** Due to Theorem 5.16 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 \( \Gamma \)-action
\[ \Phi_{\text{left}}: \Gamma \times \Gamma_p \to \Gamma_p \]
such that also \( V(p)^2 \), 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
\[ \Omega(h_1, h_2)(\tau) := (h_1 \cdot \overline{h_2})(\tau) \cdot (\text{Im } \tau)^k, \quad \tau \in \mathbb{H}, \]
which has been introduced in Lemma 5.22, part 3). To simplify the notations we set for \( M \in V(p) \)
\[ \Omega_M, \text{left} := \Omega(f[M]_k, g) \] and \( \Omega_M, \text{right} := \Omega(f, g[M']_k) \)
Explicit computation with the definition of the \([-]_k\)-operation on \( M_k(\Gamma) \) proves
\[ \Omega_M, \text{left} = \Omega_M, \text{right} \circ M \]

ii) **Existence of the integrals**: Denote by
\[ \mathcal{F} = \bigcup_{\gamma} \gamma(\mathcal{D}) \]
the fundamental domain of \( \Gamma(p) \) resulting from a finite coset representation of \( \Gamma \) with respect to the subgroup \( \Gamma(p) \subset \Gamma \). We show for \( M \in V(p) \)
\[ \int_{\mathcal{F}} \Omega_M, \text{left} \, d\mu < \infty \]
by proving for \( \gamma \in \Gamma \)
\[ \int_{\gamma(\mathcal{D})} \Omega_M, \text{left} \, d\mu < \infty \]
Similarly to the proof of Theorem 5.21, part i) one checks on \( \mathcal{D} \) an analogue of the transformation formula. First,
\[ \Omega_M, \text{left} \circ \gamma = \Omega(f[M]_k, g) \circ \gamma = \Omega((f[M]_k)[\gamma]_k, g[\gamma]_k) = \Omega(f[M \cdot \gamma]_k, g[\gamma]_k) \]
Due to Lemma 5.6 there exists a matrix \( A \in \Gamma \) with
\[ A \cdot (M \cdot \gamma) = L \]
with an upper triangular matrix \( L \in V(p) \)
Set
\[ \gamma_{\text{left}} := A^{-1} \in \Gamma, \]
then
\[ M \cdot \gamma = \gamma_{\text{left}} \cdot L. \]
Secondly, using that \( f \) and \( g \) are modular forms with respect to \( \Gamma \)
\[ \Omega(f[M \cdot \gamma]_k, g[\gamma]_k) = \Omega(f[\gamma_{\text{left}} \cdot L]_k, g[\gamma]_k) = \Omega((f[\gamma_{\text{left}}])L_\gamma, g[\gamma]_k) = \]
\[ \Omega(f[L], g) = \Omega_{L, \text{left}} \]

As a consequence

\[ \int_{\mathcal{D}} \Omega_{M, \text{left}} \, d\mu = \int_{\mathcal{D}} \Omega_{L, \text{left}} \circ \gamma \, d\mu = \int_{\mathcal{D}} \Omega_{L, \text{left}} \, d\mu \]

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 5.21, part ii) shows the boundedness of the integrand on \( \mathcal{D} \). Hence

\[ \int_{\mathcal{D}} \gamma(\mathcal{D}) \Omega_{M, \text{left}} \, d\mu = \int_{\mathcal{D}} \Omega_{L, \text{left}} \, d\mu < \infty \]

iii) Left-right switching of \([-k]: \) For given \( M \in V(p) \)

\[ \int_{\mathcal{D}} \Omega_{M, \text{left}} \, d\mu = [\Gamma(\Omega_{M, \text{left}}) : \Gamma(p)] \cdot \int_{\mathcal{D}(\Gamma(\Omega_{M, \text{left}}))} \Omega_{M, \text{left}} \, d\mu \]

because

\[ \Gamma(p) \subset \Gamma(\Omega_{M, \text{left}}) \]

has finite index according to Lemma 5.22, part 3). Concerning the indices Lemma 5.22, part 4) implies

\[ [\Gamma : \Gamma(p)] = [\Gamma : M^{-1} \Gamma(p)M] \]

hence also

\[ [\Gamma(\Omega_{M, \text{left}}) : \Gamma(p)] = [\Gamma(\Omega_{M, \text{left}}) : M^{-1} \Gamma(p)M] \]

Using the transformation formula from part i) and taking \( M^{-1} \mathcal{D} \) as a fundamental domain of \( M^{-1} \Gamma(p)M \) the calculation continues

\[ [\Gamma(\Omega_{M, \text{left}}) : \Gamma(p)] \cdot \int_{\mathcal{D}(\Gamma(\Omega_{M, \text{left}}))} \Omega_{M, \text{left}} \, d\mu = \]

\[ = [\Gamma(\Omega_{M, \text{left}}) : M^{-1} \Gamma(p)M] \cdot \int_{\mathcal{D}(\Gamma(\Omega_{M, \text{left}}))} \Omega_{M, \text{left}} \, d\mu = \]

\[ \int_{M^{-1} \mathcal{D}} \Omega_{M, \text{left}} \, d\mu = \int_{M^{-1} \mathcal{D}} \Omega_{M', \text{right}} \circ M \, d\mu = \int_{\mathcal{D}} \Omega_{M', \text{right}} \, d\mu \]

iv) Left-right switching of the Hecke operator:

\[ < T_p f, g > = \int_{\mathcal{D}} (T_p f \cdot \overline{g})(\tau) \cdot (\text{Im} \, \tau)^{k} \, d\mu = \int_{\mathcal{D}} \Omega(T_p f, g) \, d\mu \]

For any pair of cusp forms \( T_p f \) and \( g \) the integrand is invariant under the action of \( \Gamma \) as checked during the proof of Theorem 5.21, part i). In particular it is invariant under the action of the subgroup \( \Gamma(p) \subset \Gamma \). Hence continuing
\[ \int_{\mathcal{D}} \Omega(T_p f, g) \, d\mu = \frac{1}{[\Gamma : \Gamma(p)]} \int_{\mathcal{F}} \Omega(T_p f, g) \, d\mu = \]
\[ = \frac{1}{[\Gamma : \Gamma(p)]} \sum_{M \in V(p)} \Omega_{M, \text{left}} \, d\mu = \frac{1}{[\Gamma : \Gamma(p)]} \sum_{M \in V(p)} \int_{\mathcal{F}} \Omega_{M, \text{left}} \, d\mu \]

Using the result from part iii) and the property of \( V(p) \), the calculation continues
\[ \frac{1}{[\Gamma : \Gamma(p)]} \sum_{M \in V(p)} \int_{\mathcal{F}} \Omega_{M, \text{left}} \, d\mu = \frac{1}{[\Gamma : \Gamma(p)]} \sum_{M \in V(p)} \int_{\mathcal{F}} \Omega_{M, \text{right}} \, d\mu = \]
\[ = \int_{\mathcal{D}} \Omega(f, T_p g) \, d\mu = \int_{\mathcal{D}} (f \cdot T_{p \mathcal{G}}(\tau) \cdot (\text{Im } \tau)^k \, d\mu = < f, T_p g >, \text{ q.e.d.} \]

**Theorem 5.24 (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 \( \text{Hecke}_k(\Gamma) \).

**Proof.** First, Theorem 5.16 implies that \( \text{Hecke}_k(\Gamma) \) is commutative. Secondly, Theorem 5.23 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 5.25 (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 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 5.26 (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
\[
j : M_k(\Gamma_0(M)) \to M_k(\Gamma_0(m \cdot M)), \quad f \mapsto f[\mu_m],
\]
is a well-defined injection and restricts to an inclusion of cusp forms.

**Proof.** 1. **Conjugation of \( \Gamma_0(M) \):** Denote by
\[
\Gamma' := \mu_m^{-1} \cdot \Gamma_0(M) \cdot \mu_m := \{ \mu_m^{-1} \cdot \gamma : \mu_m \cdot \gamma \in \Gamma_0(M) \} \subset GL(2, \mathbb{Q})^+
\]
the \( \mu_m \)-conjugate of \( \Gamma_0(M) \). If
\[
\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(M)
\]
then
\[
\mu_m^{-1} \cdot \gamma \cdot \mu_m = \frac{1}{m} \begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix} \cdot \gamma \cdot \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b/m \\ cm & d \end{pmatrix} \in GL(2, \mathbb{Q})^+
\]

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
\[
M | c \implies m \cdot M | c \cdot m, \text{ i.e. } N | c \cdot m
\]
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
\[
\beta = \mu_N^{-1} \cdot \gamma \cdot \mu_N \text{ with } \gamma := \begin{pmatrix} a & mb \\ cM & d \end{pmatrix}.
\]
Here
\[ \det \gamma = \det \beta = 1 \] and \( \Gamma_0(N) \subset \Gamma_0(M) \)

Hence
\[ \gamma \in \Gamma_0(M) \]

As a consequence
\[ \Gamma_0(N) \subset (\Gamma' \cap \Gamma_0(M)) \]

2. Changing right-multiplication to left-multiplication: Claim: For each \( \alpha \in \Gamma \)
exists \( \alpha_{\text{left}} \in \Gamma \) such that
\[ \mu_m \cdot \alpha = \alpha_{\text{left}} \cdot \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in M(2 \times 2, \mathbb{Z}) \cap GL(2, \mathbb{Q})^+. \]

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
\[ \alpha_{\text{left}} := A^{-1} \in \Gamma \]

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
\[ \alpha_{\text{left}} \in \Gamma \]

such that
\[ \mu_m \cdot \alpha = \alpha_{efl} \cdot \theta \]

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

\[ g(\alpha)_k = f[\mu_n \cdot \alpha]_k = f[\alpha_{efl} \cdot \theta] = (f[\alpha_{efl}])_k[\theta]_k \]

From the Fourier expansion

\[ f[\alpha_{efl}]_k = \sum_{n=0}^{\infty} a_n \cdot \hat{q}^n, \quad \hat{q} = e^{2\pi i \tau/h} \]

for a suitable \( h \in \mathbb{N} \) one obtains as a consequence

\[ g(\alpha)_k(\tau) = f[\alpha_{efl}][\theta]_k(\tau) = m^{k-1} \cdot d^{-k} \cdot \sum_{n=0}^{\infty} a_n \cdot e^{2\pi i (b/n) \cdot d} \cdot \hat{q}^n, \quad \hat{q} = e^{2\pi i (\tau/h) - (a/d)}. \]

Hence \( g(\alpha)_k \) is holomorphic at \( \infty \). 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 \( \mathcal{M}_k(\Gamma_0(N)) \) generated by the images of the maps

\[ j_{p,(N/p),k} : S_k(\Gamma_0(N/p)) \times S_k(\Gamma_0(N/p)) \rightarrow S_k(\Gamma_0(N)), \quad (f, g) \mapsto f + g[\mu_p]_k, \]

for all prime factors \( p | N \) is named the oldspace, see Definition 5.27.

**Definition 5.27 (Oldform and newform of cusp forms).** Consider a level \( N \in \mathbb{N}^* \) and a weight \( k \).

1. The image

\[ \left( \sum_{p | N} \text{im } j_{p,(N/p),k} \right) \subset S_k(\Gamma_0(N)) \]

is named the subspace

\[ S^\text{old}_k(\Gamma_0(N)) \subset S_k(\Gamma_0(N)) \]

of oldforms. The summation is indexed by the primes \( p \) dividing \( N \).

2. The orthogonal complement of \( S^\text{old}_k(\Gamma_0(N)) \) with respect to the Petersson scalar product is named the subspace
5.2 The Petersson scalar product

\[ S^\text{new}_k(I_0(N)) := S^\text{old}_k(I_0(N)) \perp \subset S_k(I_0(N)) \]

of newforms.

Apparently, by the same mappings one can also define the oldspace of modular forms as a subspace \( M_k(I_0(N)) \). 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 5.28 (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 \( k = 0, \ldots, 12 \) into oldforms and newforms.

According to Definition 5.27 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

\[ \Delta_2 : \mathbb{H} \to \mathbb{C}, \quad \tau \mapsto \Delta(2 \cdot \tau) \]

belongs to \( S_{12}(\Gamma_0(2)) \). The computation shows

\[ S_{12}(\Gamma_0(2)) = \text{span}_\mathbb{C} \langle \Delta, \Delta_2 \rangle, \]

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 \( \Delta \) and \( \Delta_{11} \).
210 5  Introduction to Hecke theory and applications

---

### Fig. 5.2 \( \Gamma_0(2) \) oldforms and newforms

```plaintext
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)
8: (3, 0, 1)
12: (4, 2, 0)
Congruence subgroups_20, End
```

---

### Fig. 5.3 \( \Gamma_0(4) \) oldforms and newforms

```plaintext
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: (5, 0, 1)
8: (5, 1, 0)
10: (6, 2, 1)
12: (7, 3, 1)
Congruence subgroups_20, End
```

---
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 \( \tau \)-function is encoded by the modular discriminant, the cusp form \( \Delta \in S_{12}(\Gamma) \).

**Definition 5.29 (Ramanujan \( \tau \)-function).** The Fourier coefficients \( (\tau_n)_{n \in \mathbb{N}} \) of the normalized discriminant form

\[
\frac{\Delta(\tau)}{(2\pi)^6} = \sum_{n=1}^{\infty} \tau_n \cdot q^n, \quad q = e^{2\pi i \tau},
\]

define the Ramanujan \( \tau \)-function

\[
\tau : \mathbb{N} \rightarrow \mathbb{Z}, \quad n \mapsto \tau(n) := \tau_n.
\]
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

\[
|\tau(p)| \leq 2 \cdot p^{11/2}
\]

The conjecture was proved inter alia one year later by Mordell [42]. Figure 5.6 shows Mordell’s introduction from his paper.
5.3 Numerology: Lagrange, Jacobi, Ramanujan, Mordell

the form \( o(n^{\frac{3}{2}}) \). For it appears that

\[
\sum_{n=1}^{\infty} \frac{\tau(n)}{n^t} = \prod_p \frac{1}{1 - \tau(p)p^{-t} + p^{11-2t}}. \tag{101}
\]

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

\[n^{-\frac{1}{2}} \tau(n) = \frac{\sin(1 + a_1)\theta_{p_1} \sin(1 + a_2)\theta_{p_2} \cdots \sin(1 + a_r)\theta_{p_r}}{\sin \theta_{p_1} \sin \theta_{p_2} \cdots \sin \theta_{p_r}}, \tag{102}\]

where

\[\cos \theta_p = \frac{1}{2} p^{-\frac{11}{2}} \tau(p).\]

It would follow that, if \( n \) and \( n' \) are prime to each other, we must have

\[\tau(nn') = \tau(n)\tau(n'). \tag{103}\]

Let us suppose that (102) is true, and also that (as appears to be highly probable)

\[\{2\tau(p)\}^2 \leq p^{11}, \tag{104}\]

---

Fig. 5.5 Ramanujan’s conjecture on \( \tau(n) \) from [45]

---

Mr Mordell, On Mr Ramanujan’s Empirical Expansions, etc.

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

\[
\left(\frac{\omega_2}{2\pi}\right)^2 \Delta(\omega_1, \omega_2) = r \left( (1 - r)(1 - r^2)(1 - r^3) \cdots \right)^2 = \sum_{n=1}^{\infty} T(n) r^n,
\]

he finds that

\[T(mn) = T(m)T(n) \] \hspace{1cm} \text{(1)}

if \( m \) and \( n \) are prime to each other; and also that

\[\sum_{n=1}^{\infty} \frac{T(n)}{n^s} = \Pi \frac{1}{1 - T(p)p^{-s} + p^{11-2s}} \] \hspace{1cm} \text{(2)},

where the product refers to the primes 2, 3, 5, 7 \ldots. 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

\[\Delta(\omega_1, \omega_2) = (r = e^{2\pi i \omega}, \omega = \omega_1/\omega_2), \]

is the well-known modular invariant of dimensions -12 in \( \omega_1, \omega_2 \), which is unaltered by the substitutions of the homogeneous modular group defined by
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 5.30 (Product and recursion formula of the Ramanujan \( \tau \)-function).**

The Ramanujan \( \tau \)-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 \( k > 1 \)
   \[
   \tau(p) \cdot \tau(p^k) = \tau(p^{k+1}) + p^{11} \cdot \tau(p^{k-1}).
   \]

**Proof.** 1. Consider an arbitrary, but fixed \( m \in \mathbb{N} \). Corollary 5.12 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 coefficient formula from Theorem 5.10 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

   \[
   \tau(p^k) \cdot \tau(p) = \tau(p^{k+1}) + p^{11} \cdot \tau(p^{k-1}), \text{ q.e.d.}
   \]
Remark 5.31 (Growth estimation of the Ramanujan $\tau$-function). The final conjecture of Ramanujan about the $\tau$-function is the growth estimation

$$|\tau(p)| \leq 2 \cdot p^{11/2}, \text{ p prime},$$

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 $\tau$-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 5.36 is due to Jacobi in 1834. For the history of these issues see [47].

Definition 5.32 (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

$$r(n,k) := \text{card} \left\{ v = (v_1, \ldots, v_k) \in \mathbb{Z}^k : n = v_1^2 + \cdots + v_k^2 \right\}.$$

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 5.33 (Generating function $\vartheta$). The series

$$\vartheta (\tau, k) := \sum_{n=0}^\infty r(n,k) \cdot q^n, \text{ } q := e^{2\pi i \tau},$$

which is generated by the sequence $r(n,k)_{n\in\mathbb{N}}$, is named a $\vartheta$-series.
Proposition 5.34 (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. Sketch, see cf. [17, Chap.1, §2], [36].

i) The congruence subgroup $\Gamma_0(4)$ is generated as

$$\Gamma_0(4) = \text{span} < T, \gamma >$$

with

$$\gamma = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} \in \Gamma_0(4)$$

ii) The translation $T$ apparently satisfies

$$\vartheta(-,4)[T]_4 = \vartheta(-,4)$$

The product formula

$$\vartheta(\tau,4) = \vartheta(\tau)^4$$

with

$$\vartheta(\tau) = \sum_{d=0}^{\infty} r(n,1) \cdot q^n$$

reduces the weak modularity

$$\vartheta(-,4)[\gamma]_4 = \vartheta(-,4)$$

to the transformation formula for $\vartheta$.

iii) The difficult part is to prove

$$\vartheta(-1/(4\tau) = \sqrt{-2i\tau} \cdot \vartheta(\tau).$$

iv) The Fourier series

$$\vartheta(\tau) = 1 + r(1,1) \cdot q + O(q^2) = 1 + 2 \cdot q + O(q^2)$$

shows

$$\vartheta(\tau,4) = (1 + 2 \cdot q)^4 + O(2) = 1 + 8 \cdot q + O(2), \ q.e.d.$$
5.3 Numerology: Lagrange, Jacobi, Ramanujan, Mordell

**Theorem 5.35 (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

\[
(G_2[\mu_N]_2)(\tau) := G_2(\mu_N(\tau)) \cdot \det \mu_N \cdot j(\mu_N, \tau)^{-1} = N \cdot G_2(N\tau)
\]

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

\[
G_2[\gamma]_2(\tau) = G_2(\tau) - 2\pi i \cdot c \cdot h(\gamma, \tau)^{-1} \text{ for } \gamma := \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma
\]

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

  \[
  G_2[\alpha]_2(\tau) = G_2(\tau) - 2\pi i \cdot c \cdot h(\alpha, \tau)^{-1}
  \]

- **\( (G_2[\mu_N]_2)[\alpha]_2 \):** Then

  \[
  \mu_N \cdot \alpha = \beta \cdot \mu_N \text{ with } \beta := \begin{pmatrix} a \cdot N b \\ c/N \cdot d \end{pmatrix}
  \]

  Here \( \beta \in \Gamma \) because

  \[
  c \equiv 0 \text{ mod } N \implies c/N \in \mathbb{Z}
  \]

  Then

  \[
  (G_2[\beta]_2)(z) = G_2(z) - 2\pi i \cdot (c/N) \cdot h(\beta, z)^{-1}
  \]

  Hence with the argument \( z = \mu_N(\tau) = N\tau \)

  \[
  (G_2[\beta]_2)(\mu_N(\tau)) = G_2(\mu_N(\tau)) - 2\pi i \cdot (c/N) \cdot h(\beta, \mu_N(\tau))^{-1}
  \]
Then
\[(G_2[\mu_N]|_2)\alpha_2)(\tau) = (G_2[\mu_N \cdot \alpha_2])(\tau) = (G_2[\beta \cdot \mu_N]|_2)(\tau) =\]
\[= (G_2[\beta]|_2)(\mu_N(\tau)) \cdot h(\mu_N, \tau)^{-1} \cdot N =\]
\[= (G_2[\mu_N(\tau)] - 2\pi i \cdot (c/N) \cdot h(\beta, \mu_N(\tau))^{-1}) \cdot h(\mu_N, \tau)^{-1} \cdot N =\]
\[= G_2(\mu_N(\tau)) \cdot h(\mu_N, \tau)^{-1} \cdot N - 2\pi i ((c/N) \cdot h(\beta, \mu_N(\tau))) \cdot h(\mu_N, \tau)^{-1} =\]
\[= G_2[\mu_N]|_2(\tau) - 2\pi i ((c/N) \cdot h(\beta, \mu_N(\tau))) \cdot h(\mu_N, \tau)^{-1}\]

Now
\[h(\beta, \mu_N(\tau)) = h(\beta, N\tau) = (c/N) \cdot N \tau + d = c\tau + d\] and \(h(\mu_N, \tau) = 1\)

and
\[h(\alpha, \tau) = c\tau + d\]

which implies
\[h(\beta, \mu_N(\tau)) = h(\alpha, \tau)\]

Hence
\[(G_2[\mu_N]|_2\alpha_2)(\tau) = (G_2[\mu_N]|_2)(\tau) - 2\pi i \cdot c \cdot h(\alpha, \tau)^{-1}\]

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 5.36 (Four squares theorem).** For any \(n \in \mathbb{N}, n \geq 1\), there are
\[r(n, 4) = 8 \cdot \sum_{d \mid n, 4 \mid d} d\]
possibilities to represent the non-negative integer \(n\) as the sum of 4 integer squares. In particular for \(4 \nmid n\)
\[r(n, 4) = 8 \cdot \sigma_1(n) = 8 \cdot \sum_{d \mid n} d.\]

**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 5.35 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

$$G_{2,2}(\tau) = -\frac{\pi^2}{3} \left( 1 + 24 \cdot \sum_{n=1}^{\infty} \left( \sum_{d|n, d \text{ odd}} d \right) q^n \right) = -\frac{\pi^2}{3} (1 + 24q + O(2))$$

and

$$G_{2,4}(\tau) = -\pi^2 \left( 1 + 8 \cdot \sum_{n=1}^{\infty} \left( \sum_{d|n, 4|n} d \right) q^n \right) = -\pi^2 (1 + 8q + O(2)).$$

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 5.34 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

$$r(n, 4) = 8 \cdot \sum_{d|n, 4|d} d \cdot q.e.d.$$

Example 5.37 (Modular forms via $\vartheta$-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 5.36. The figure shows the output of the PARI-script `Modular_forms_theta_01`. 
Modular functions to compute $r(-,k,e)$
Chapter 6
Application to imaginary quadratic fields

The modular $j$-invariant parametrizes the set of complex 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 $j(\alpha(\tau))$, $\alpha \in \Gamma_{m, \text{prim}}$, $m \in \mathbb{N}^*$?

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 6.7.

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

$$\mathbb{Q} \subset K \subset \mathbb{C}$$

with degree $\deg K := [K : \mathbb{Q}] < \infty$.

If $\deg K = 2$ then $K$ is a **quadratic field**.

2. The **Galois group** $\text{Gal}(K/\mathbb{Q})$ of a number field $K$ is the group of all $\mathbb{Q}$-linear automorphisms of the $\mathbb{Q}$-vector space $K$.

**Remark 6.2 (Discriminant and algebraic integers).** Consider a number field $K$ of degree

$$n = [K : \mathbb{Q}]$$

and denote by

$$(\alpha_j)_{j=1,...,n}$$

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

$$\mu_\alpha(a_j) = \sum_{k=1,...,n} \alpha_{j_k} \alpha_k, \ j = 1,...,n.$$

1. For $\alpha \in K$ norm and trace are respectively defined as

$$N_K(\alpha) := \det(\alpha_{j_k}) \in \mathbb{Q}$$

and

$$\text{tr}_K(\alpha) := \sum_{j=1,...,n} \alpha_{j,j} \in \mathbb{Q}.$$

2. The discriminant of $K$ is defined as

$$\Delta_K := \det(\text{tr}_K(\alpha_{j} \cdot \alpha_k)) \in \mathbb{Q}.$$

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 lattice of rank $k$.

5. The number field $K$ has a $\mathbb{Q}$-basis $(\alpha_j)_{j=1,...,n}$ by algebraic integers $\alpha_j \in \mathcal{O}_K$.

Each element $\alpha \in K$ has a unique representation

$$\alpha = \frac{\mathbb{Z} \alpha_1 + \ldots + \mathbb{Z} \alpha_n}{\Delta_K}$$
6.1 Imaginary quadratic fields and tori with complex multiplication

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

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \equiv 2, 3 \mod 4 \\ \mathbb{Z} \left[ \frac{1 + \sqrt{D}}{2} \right] & \text{if } D \equiv 1 \mod 4 \end{cases}$$

Note. Due to historical reasons the symbol $\mathcal{O}$ has two different meanings. In the context of complex analysis $\mathcal{O}$ also denotes the complex structure sheaf.

Remark 6.3 (Number field).

1. 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

$$P(\alpha) = 0 \text{ with } P(X) \in \mathbb{Q}[X] \text{ and } \deg P = \deg K.$$  

2. Each quadratic number field has the form $K = \mathbb{Q}(\sqrt{d})$ with $d \in \mathbb{Z}$ squarefree.

If $d < 0$ then $K$ is named imaginary quadratic, if $d > 0$ then $K$ is named real quadratic.

3. 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

$$\sigma_1(z) = \begin{cases} -z & d > 0 \\ z & d < 0 \end{cases}$$

Set

$$\sigma_0 := id_{Gal(K/\mathbb{Q})}.$$  

Then norm and trace of an element $z \in K$ are defined by the elementary symmetric functions

$$N(z) := \sigma_0(z) \cdot \sigma_1(z) \text{ and } Tr(z) := \sigma_0(z) + \sigma_1(z)$$
Definition 6.4 (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

$$
\begin{array}{ccc}
\mathbb{C} & \xrightarrow{\mu_\alpha} & \mathbb{C} \\
\downarrow{p} & & \downarrow{p} \\
\mathbb{C}/\Lambda & \xrightarrow{f} & \mathbb{C}/\Lambda
\end{array}
$$

with a unique multiplication map $\mu_\alpha$ determined by an element $\alpha = \alpha_f \in \mathbb{C}$: For all $z \in \mathbb{C}$

$$\mu_\alpha(z) = \alpha \cdot z$$

Proposition 6.5 (Endomorphism ring). The set of endomorphisms of a torus

$$T = \mathbb{C}/\Lambda$$

constitutes with respect to addition and composition a ring $\text{End}(T)$, the endomorphism ring of $T$. The map

$$\text{End}(T) \to \{ \alpha \in \mathbb{C} : \mu_\alpha(\Lambda) \subset \Lambda \}, \ f \mapsto \alpha_f,$$

is an isomorphism of rings.

If not stated otherwise by the above ring isomorphism we identify the endomorphism ring $\text{End}(T)$ with a subring of $\mathbb{C}$. Because each torus $T$ is an Abelian group its endomorphism ring $\text{End}(T)$ comprises at least the group $\mathbb{Z}$:

$$\mathbb{Z} \subset \text{End}(T) \subset \mathbb{C}.$$ 

Which intermediate rings are possible? The case

$$\text{End}(T) = \mathbb{Z}$$

is the general case, justifying a specific name for tori with additional endomorphisms.
6.1 Imaginary quadratic fields and tori with complex multiplication

Definition 6.6 (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

\[
T = \mathbb{C}/\Lambda, \quad \Lambda = \mathbb{Z} \oplus \mathbb{Z} \cdot \tau,
\]

satisfies

\[
\mathbb{Z} \subseteq \text{End}(T)
\]

2. The values \( j(\tau) \subset \mathbb{C} \) at CM-points \( \tau \in \mathbb{H} \) are named singular moduli.

Theorem 6.7 states a remarkable relation between tori and number fields. It reveals the arithmetic structure encoded in a complex torus with complex multiplication.

Theorem 6.7 (Complex multiplication and imaginary quadratic fields). The complex number \( \tau \in \mathbb{H} \) is a CM-point iff \( \tau \) belongs to an imaginary quadratic number field \( K \).

If \( \tau \in \mathbb{H} \) is a CM-point with torus \( T := \mathbb{C}/\Lambda_\tau \) then

\[
\text{End}(T) \subset \mathcal{O}_K
\]

is an order.

Proof. 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

\[
\alpha = a + b \cdot \tau, \quad \alpha \cdot \tau = c + d \cdot \tau,
\]

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 \( a \tau \in \text{End}(T) \), \( a \tau \notin \mathbb{Z} \), and \( T \) has complex multiplication, iii) Assume that \( T \) has complex multiplication and consider an endomorphism \( f \in \text{End}(T) \) operating as multiplication \( \mu_\alpha \) with a complex number \( \alpha \). Alike to the proof of part 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 \( \alpha \) is an eigenvalue of \( \gamma \) and satisfies the eigenvalue equation, which is an integral equation:
\[
\alpha^2 - (d + a) \cdot \alpha + ab - cd = 0.
\]
As a consequence \( \alpha \in \mathcal{O}_K \). As a \( \mathbb{Z} \)-submodule of the lattice \( \mathcal{O}_K \) the ring \( \text{End}(T) \) is a lattice too. Because
\[
\mathbb{Z} \subseteq \text{End}(T)
\]
the lattice \( \text{End}(T) \) has rank = 2. Hence the ring \( \text{End}(T) \) is an order of \( \mathcal{O}_K \), q.e.d.

We consider in detail the two elliptic points of the modular group \( \Gamma \), see Theorem 2.16:

**Example 6.8 (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
\[
\text{End}(T) = \Lambda_i
\]
The endomorphism ring
\[
\text{End}(T) = \Lambda_i
\]
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

\[
\text{End}(T) = \Lambda_\rho
\]

The result is similar to the first example: The endomorphism ring

\[
\text{End}(T) = \Lambda_\rho
\]

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

\[
\text{End}(T) = \mathcal{O}
\]

with

\[
\mathcal{O} = \Lambda_{2\rho} \subset \mathcal{O}_K
\]

is a proper order of \( K \). Note

\[
j(2\rho) = 54000 \in \mathbb{Z}, \quad j(\rho) = 0 \in \mathbb{Z}.
\]
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 6.15 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 6.9.

We take up the investigation of the integral matrices \( \Gamma_m \) from Section 5.1, in particular Definition 5.4 of the set \( \Gamma_{m,prim} \) of primitive matrices and its set \( V(m, prim) \) of representatives with respect to the canonical left \( \Gamma \)-operation. The set \( V(m, prim) \) has cardinality

\[
\psi(m) := m \cdot \prod_{\substack{p | m \text{ prime} \not \pmod{m}}} (1 + (1/p))
\]

Definition 6.9 (Modular polynomials). Consider a level \( m \in \mathbb{N} \) and the complete set of representatives of \( \Gamma \setminus \Gamma_{m,prim} \)

\[
V(m, prim) = \{ M_1, ..., M_{\psi(m)} \}.
\]

1. Each matrix \( M_\mu \in V(m, prim) \) induces the automorphism of the upper half-plane

\[
M_\mu : \mathbb{H} \to \mathbb{H}, \ \tau \mapsto M_\mu(\tau).
\]

The functions

\[
 j_\mu := j \circ M_\mu \in \mathscr{M}(\mathbb{H}), \ \mu = 1, ..., \psi(m),
\]

are the class invariants of \( \Gamma \setminus \Gamma_m \).

2. The modular polynomial of level \( m \) is the polynomial

\[
F_m(X) := \prod_{\mu=1}^{\psi(m)} (X - j_\mu) \in \mathscr{M}(\mathbb{H})[X].
\]

Note. The modular invariant is constant along the orbits of the action of the modular group \( \Gamma \). Therefore the value of \( j_\mu \) in Definition 6.9 does not depend on representing a coset from \( \Gamma \setminus \Gamma_{m,prim} \) by the matrix \( M \in V(N, prim) \) or by the matrix \( \gamma \cdot M, \gamma \in \Gamma \).

Example 6.10 (Modular polynomials). The PARI-script `modular_polynomial_01` computes for several levels \( N \) the modular polynomials, see Figure 6.1.
Fig. 6.1 Modular polynomials

1. \( m = 2 \):

\[
\psi_2 = 3
\]
and

\[
F_2(X, j) = X^3 + (\psi_2^2 - 1488 * j - 162000) * X^2 + (1488 * \psi_2^2 + 40773375 * j + 87480000) * X + (j^3 - 162000 * j^2 + 8748000000 * j - 157464000000000)
\]

2. \( m = 3 \):

\[
\psi_3 = 4
\]
and

\[
F_3(X, j) = X^4 + (\psi_3^3 + 2232 * j^2 - 1069956 * j + 36864000) * X^3 + (2232 * j^3 + 2587918086 * j^2 + 8900222976000 * j + 452984832000000) * X^2 + (1069956 * j^3 + 8900222976000 * j^2 - 77084596636000000 * j + 185542587187200000000000) * X + (j^4 + 36864000 * j^3 + 452984832000000 * j^2 + 185542587187200000000000 * j)
\]

Apparently, the roots of the modular polynomials from \( \mathcal{M}(\mathbb{H})[X] \) are exactly the class invariants

\[
f_\mu, \mu = 1, ..., \psi(m),
\]
corresponding to the \( \Gamma \)-left operation on \( \Gamma_{m, \text{prim}} \). For \( \mu = 1, ..., \psi(m) \) denote by \( s_\mu \) the \( \mu \)-th elementary symmetric function in \( \psi(m) \) variables, then up to sign the functions

\[
s_\mu(j_1, ..., j_{\psi(m)}) \in \mathcal{M}(\mathbb{H})
\]
are the coefficients of the modular polynomial \( F_m(X) \). E.g.,
\((-1)^{\psi(m)} s_{\psi}(m) = j_1 \cdots j_{\psi(m)}\)

is the constant term and
\[\begin{align*}
(-1) \cdot \sigma_1(j_1, \ldots, j_{\psi(m)}) &= -(j_1 + \ldots + j_{\psi(m)})
\end{align*}\]
is the coefficient of the term \(X^{\psi(m) - 1}\).

The modular polynomial \(F_m(X)\) is a polynomial in the variable \(X\) with coefficients from the field of meromorphic functions \(\mathcal{M}(\mathbb{H})\). Theorem 6.11 takes a closer look on the coefficients. As the theorem shows they are polynomials in the modular \(j\)-invariant with integer coefficients, i.e. they belong to the subring
\[\mathbb{Z}[j] \subset \mathcal{M}(\mathbb{H}).\]

See also Example 6.10.

**Theorem 6.11 (Coefficients of the modular polynomials).** For each level \(m \in \mathbb{N}^*\)
\[F_m(X) = \prod_{\mu=1}^{\psi(m)} (X - j_\mu) \in \mathbb{Z}[j][X] = \mathbb{Z}[j, X].\]

**Proof.** For arbitrary but fixed index \(\mu = 1, \ldots, \psi(m)\) we consider the coefficient
\[c := c_\mu := \sigma_\mu(j_1, \ldots, j_{\psi(m)}) \in \mathcal{M}(\mathbb{H})\]
of the modular polynomial
\[F_m(X) \in \mathcal{M}(\mathbb{H})[X].\]

We prove step by step the following properties of the coefficients
\[c \in \mathbb{Z}[j].\]

i) **Weakly modular:** According to Corollary 5.7 right multiplication with an element \(\gamma \in \Gamma\) permutes the orbits of the \(\Gamma\)-left operation \(\Phi_m\)
\[\{[M_1], \ldots, [M_{\psi(m)}]\} = \{[M_1 \cdot \gamma], \ldots, [M_{\psi(m)} \cdot \gamma]\}.\]
Hence right multiplication does not change the value of the elementary symmetric functions: For all \(j = 1, \ldots, \psi(m)\)
\[\sigma_\mu(j_1, \ldots, j_{\psi(m)}) = \sigma_\mu(j_1 \circ \gamma, \ldots, j_{\psi(m)} \circ \gamma)).\]
Therefore \(c\) is weakly modular.

ii) **Holomorphic on \(\mathbb{H}\):** The modular \(j\)-invariant is holomorphic on \(\mathbb{H}\) according to Corollary 3.16. Therefore also the coefficient \(c\) is holomorphic.
iii) **Meromorphic at \( \infty \):** The coefficient \( c \) is weakly modular according to part i). Hence \( c \) has a Fourier expansion

\[
c(\tau) = \sum_{\nu \in \mathbb{Z}} a_{\nu} \cdot q^\nu, \quad q = e^{2\pi i \tau}.
\]

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 3.16 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 a 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

\[
e^{2\pi i (b/(d)) \cdot q^{(a/d)}} = \zeta_m^{ab} \cdot (q^{1/m})^d.
\]

Here

\[
\zeta_m := e^{2\pi i / m},
\]

denotes a primitive \( m \)-th root of unity. Therefore

\[
|(j \circ \alpha)(\tau)| \leq \frac{1}{|q|^{a/d}} + O(1)
\]

for a single class invariant, and a constant \( M \) exists with

\[
|c(\tau)| \leq M \cdot \frac{1}{|q|^{a/d}}
\]

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 the substitution of \( q \) by
\[ \zeta_{m}^{ab} \cdot (q^{1/m})^2. \]

As a consequence the class invariant \( j \circ \alpha \) has a Fourier expansion with respect to \( q^{1/m} \), namely

\[ j(\alpha(\tau)) = \frac{1}{(q^{1/m})^2} \cdot \zeta_{m}^{ab} + P(q^{a/d} \cdot \zeta_{m}^{ab}), \]

which shows that the Fourier coefficients 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 algebraic integers from

\[ \mathbb{Z} + \mathbb{Z} \cdot \zeta_{m} = \mathcal{O}_K. \]

v) **Integrality** \( c \in \mathbb{Z}[j] \): The operation of the Galois group

\[ \text{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*. \]

extends to an operation on the set \( \{ j_1, \ldots, j_{\psi(m)} \} \) of class invariants

\[ \text{Gal}(K/\mathbb{Q}) \times \{ j_1, \ldots, j_{\psi(m)} \} \to \{ j_1, \ldots, j_{\psi(m)} \}, \ (\chi, j_\mu) \mapsto j_\mu^X, \]

which is defined as follows: Assume \( \chi \in \text{Gal}(K/\mathbb{Q}) \) maps \( \chi(\zeta_m) = \zeta_m^e \) with \( (e, m) = 1 \). If \( j_\mu \) is the class invariant of the matrix

\[ M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \]

then we define \( j_\mu^X \) as the class invariant of the matrix

\[ M^\chi = \begin{pmatrix} a & b^X \\ 0 & d \end{pmatrix} \]

with

\[ 0 \leq b^X < d \text{ and } b^X \equiv e \cdot b \mod d. \]

Because the function \( c \) is fixed under the operation of \( \text{Gal}(K/\mathbb{Q}) \), its Fourier coefficients belong to the fixed field \( \mathbb{Q} \). Due to part iv) the Fourier coefficients even belong to

\[ \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}, \text{ q.e.d.} \]

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 \( j \).
$\Phi_m(j) := F_m(j, j) = \prod_{\mu=1}^{\psi(m)} (j - j_\mu) \in \mathbb{Z}[j].$

**Example 6.12 (The polynomials $\Phi_m(j) \in \mathbb{Z}[j]$).** We take up Example 6.10 with Figure 6.2, which shows some polynomials $\Phi_m$.

The PARI script `Modular_polynomial_02` computes their factorization:

1. $m = 2$:

   $\Phi_2(j) = F_2(j, j) = -j^4 + 2978 * j^3 + 40449375 * j^2 + 174696000000 * j - 157454000000000$

   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 $j - 54000, (j - 8000)^2, j, (j + 32768)^2$
Lemma 6.13 (Leading coefficient of the modular polynomials). For squarefree \( m \geq 2 \) the polynomial
\[
\Phi_m(j) \in \mathbb{Z}[j]
\]
has leading coefficient \( \pm 1 \).

Example 6.10 illustrates Lemma 6.13 by
\[
\Phi_2(j) = -j^4 + O(3) \text{ and } \Phi_3(j) = -j^6 + O(5).
\]

Proof. The function
\[
\Phi_m(j) : \mathbb{H} \rightarrow \mathbb{C}
\]
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 \( F_m \) as polynomial in \( j \). The coefficient is the product of the highest negative coefficients of the factors
\[
j - j_\mu, \; \mu = 1, \ldots, \psi(m).
\]
For arbitrary but fixed \( \mu \) the representation
\[
j(\tau) = \frac{1}{q} + P(q)
\]
implies
\[
j_\mu(\tau) = j \left( \frac{a\tau + b}{d} \right) = \frac{e^{-2\pi i (b/d)}}{q^{a/d}} + P \left( q^{a/d} e^{2\pi i (b/d)} \right)
\]
with \( j_\mu \) corresponding to the matrix
\[
\begin{pmatrix}
a & b \\
0 & d
\end{pmatrix} \in V(m, \text{prim}).
\]
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 coefficient of
\[
j - j_\mu
\]
is a root of unity, and the same holds for the coefficient \( c_k \) of the product.
\[ \Phi = \prod_{\mu=1}^{\psi(m)} (j - j_\mu). \]

Because \( c_k \in \mathbb{Z} \) we have \( c_k = \pm 1 \), q.e.d.

According to Theorem 6.11 the modular polynomial

\[ F_m(j, X) = \prod_{\mu=1}^{\psi(m)} (X - j_\mu) \in \mathbb{Z}[j, X] \]

is a polynomial in the two variables \( j \) and \( X \) with integer coefficients. It expands as

\[ F_m(j, X) = \sum_{n=0}^{N} \left( \sum_{r+s=n} c_{rs} \cdot j^r \cdot X^s \right), \quad c_{rs} \in \mathbb{Z}. \]

Proposition 6.14 shows that \( F_m(t, X) \) 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 6.14 (Symmetry of the modular polynomials).** The modular polynomials

\[ F_m(j, X) \in \mathbb{Z}[j, X] \]

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

\[ K := \mathbb{Q}(R) = \mathbb{Q}(j). \]

i) **Irreducibility of \( F_m(X) \in R[X] \) over the base field \( K \):** The polynomial

\[ F_m(X) = \prod_{\mu=1}^{\psi(m)} (X - j_\mu(\tau)) \in R[X] \]

has the roots

\[ j_\mu, \quad \mu = 1, \ldots, \psi(m). \]

To prove that \( F_m \) is irreducible, we show that the Galois group

\[ \text{Gal}(L/K) \]

of the splitting field \( L = K(j_1, \ldots, j_{\psi(m)}) \) of \( F_m(X) \) acts transitively on the roots. Then no root belongs to the fixed field \( K \). For the proof set
$j_\mu = j \circ \alpha_\mu$

with matrices

$\alpha_\mu \in V(m, \text{prim}), \mu = 1, ..., \psi(m)$,

a complete set of representatives of $\Gamma \backslash I_{m, \text{prim}}$. According to Corollary 5.7 for any $\gamma \in \Gamma$ the same holds for the set

$\{ \alpha_\mu \cdot \gamma : \mu = 1, ..., \psi(m) \} \subset \Gamma_m$.

Hence the $\Gamma$-orbit of any matrix $(\alpha_\mu \cdot \gamma)$ equals the $\Gamma$-orbit of a suitable matrix $\alpha_\mu'$. Therefore the functions

$(j \circ (\alpha_\mu \cdot \gamma))_{\mu = 1, ..., \psi(m)}$

are a permutation of the functions

$(j \circ \alpha_\mu)_{\mu = 1, ..., \psi(m)}$.

As a consequence, for any $\gamma \in \Gamma$ the map

$L \rightarrow L, f \mapsto f \circ \gamma$

is an element of the Galois group $\text{Gal}(L/K)$. For each pair $(\nu, \mu)$ exist elements $\gamma', \gamma \in \Gamma$ with

$\alpha_\mu = \gamma' \cdot \alpha_\nu \cdot \gamma$.

Therefore $\text{Gal}(L/K)$ 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 set

$f(X) := F_m(j, X)$ and $g(X) := F_m(X, j)$.

For any matrix $\alpha \in V(m, \text{prim})$ the function

$x_\alpha := j \circ \alpha$

is a root of the polynomial $f(X)$. In particular,

$\alpha := \begin{pmatrix} 1 & 0 \\ 0 & m \end{pmatrix} \in V(m, \text{prim})$

satisfies for all $\tau \in \mathbb{H}$

$f(x_\alpha)(\tau) = F_m(j(\tau), (j \circ \alpha)(\tau)) = F_m(j(\tau), j(\tau/m)) = 0$.

The latter equation can be also interpreted: For all $\tau \in \mathbb{H}$

$0 = F_m(j(m \cdot \tau), j(\tau)) = F_m((j \circ \beta)(\tau), j(\tau)) = g(x_\beta)(\tau)$
with the matrix
\[
\beta := \begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix} \in V(m, \text{prim}).
\]
But \( j \circ \beta \) is also a zero of \( f(X) \) because \( \beta = \alpha_\mu \) for a suitable \( \mu \in \{1, \ldots, \psi(m)\} \).

We now apply the basic fact about the minimal polynomial of algebraic field extensions: Both polynomials
\[
f(X), g(X) \in K[X]
\]
have the common zero
\[
x_\beta := j \circ \beta.
\]
The polynomial \( f(X) \) is irreducible, see part i), with leading coefficient \( = 1 \). Therefore \( f(X) \) is the minimal polynomial of the field extension \( k \subset K[x_\beta] \), and a polynomial \( h(X) \in K[X] \) exists with
\[
g(X) = h(X) \cdot f(X).
\]
According to Theorem 6.11 both polynomials \( f(X) \) and \( g(X) \) have their coefficients already in the ring \( R \). 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 \( R \). Set
\[
H(j, X) := h(X) \in R[X] = \mathbb{Z}[j][X].
\]
Then
\[
F_m(X, j) = H(j, X) \cdot F_m(j, X) \in \mathbb{Z}[j, X].
\]
iii) Invariance: The last equation from part ii), considered as an equation of polynomials in two variables, is invariant when interchanging the role of \( j \) and \( X \).

Hence also
\[
F_m(j, X) = H(X, j) \cdot F_m(X, j).
\]
Therefore
\[
F_m(j, X) = H(X, j) \cdot H(j, X) \cdot F_m(j, X),
\]
\[
H(X, j) \cdot H(j, X) = 1,
\]
and
\[
H(X, j) = H(j, X) = \pm 1.
\]
The case \( H(X, j) = -1 \) would imply \( H(j, j) = -H(j, j) \) and
\[
H(j, j) = 0,
\]
contradicting the fact that \( \Phi_m(j) = F_m(j, j) \) has leading coefficient \( \pm 1 \) according to Lemma 6.13. Therefore \( H(X, j) = 1 \) and
We now apply the results about the modular polynomials to show that the modular $j$-function provides a necessary condition for a class $[\tau] \in X(\Gamma)$ to be a CM-class.

**Theorem 6.15 (Integral values of the modular $j$-invariant).** For each CM-class $[\tau] \in X(\Gamma)$ the value $j(\tau) \in \mathbb{C}$ is an algebraic integer.

The proof will show: For each CM-point $\tau \in \mathbb{H}$ exists a level $m \in \mathbb{N}$ such that the normalized polynomial $\Phi_m \in \mathbb{Z}[j]$ annihilates $j(\tau) \in \mathbb{C}$.

**Proof.** The complex number $\tau \in \mathbb{H}$ is not rational. Theorem 6.7 implies that $\tau$ 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 $(1, z)$, $z \in \mathbb{H}$. For admissible values of $z$ see Remark 6.2.

i) **Determine a matrix $1 \neq \alpha \in \Gamma_{m, {\text{prim}}}$ which fixes $z$:** The element $\xi \in K$

$$\xi := \begin{cases} 
\sqrt{-d} & D > 1 \\
1 + i & D = 1 
\end{cases}$$

is an algebraic integer. Its norm

$$N(\xi) = \bar{\xi}\xi \in \mathbb{Z}$$

is squarefree. Multiplication with $\xi \in \mathcal{O}_K$ defines a $\mathbb{Z}$-linear endomorphism

$$\mathcal{O}_K \to \mathcal{O}_K, \; x \mapsto \xi \cdot x.$$ 

Denote by

$$\alpha = \begin{pmatrix} a & b \\
c & d \end{pmatrix} \in \text{M}(2 \times 2, \mathbb{Z}) \cap \text{GL}(2, \mathbb{R})^+$$

its matrix with respect to the basis $(1, z)$. Then

$$\xi \cdot \begin{pmatrix} z \\
1 \end{pmatrix} = \alpha \cdot \begin{pmatrix} z \\
1 \end{pmatrix}$$
or in components
\[
\begin{pmatrix}
\xi \cdot z \\
\xi \cdot 1
\end{pmatrix} =
\begin{pmatrix}
a z + b \\
c z + d
\end{pmatrix}
\]

- The first form shows: Representing the \(\mathbb{Z}\)-linear multiplication the matrix
\[\alpha \in M(2 \times 2, \mathbb{Z})\]
has the eigenvalue \(\xi\) and by conjugation \(\alpha = \bar{\alpha}\) also the eigenvalue \(\overline{\xi}\). Hence
\[m := \det \alpha = \xi \overline{\xi} = N(\xi) \in \mathbb{Z}\]
is squarefree which implies
\[(a, b, c, d) = 1\]
According to Definition 5.4
\[\alpha \in \Gamma_{m, \text{prim}}.\]

- 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: The value of \(j\) is constant along each orbit of the \(\Gamma\)-operation. Lemma 5.6 implies the existence of a matrix
\[\alpha_\mu \in V(m, \text{prim}), \ \mu \in \{1, \ldots, \psi(m)\},\]
with the same \(\Gamma\)-orbit as \(\alpha\) with respect to the left action
\[\Phi_{m, \text{prim}} : \Gamma \times \Gamma_{m, \text{prim}} \to \Gamma_{m, \text{prim}}, \ (A, M) \mapsto A \cdot M,\]
w.l.o.g. \(\mu = 1\). Due to part i)
\[j(z) = j(\alpha(z)) = j(\alpha_1(z)) = j_1(z),\]
which implies: The function
\[\Phi_m(j) = \prod_{\mu=1}^{\psi(m)} (j - j_\mu) \in \mathbb{Z}[j]\]
vanishes at \(z \in \mathbb{H}\):
\[\Phi_m(j)(z) = \Phi_m(j(z)) = 0.\]
The polynomial
\[ \Phi_m \in \mathbb{Z}[j] \]
has integer coefficients, and leading coefficient \( \pm 1 \) due to Lemma 6.13. Hence
\[ 0 = \Phi_m(j(z)) \]
proves that \( j(z) \) is an algebraic integer.

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
\[ \beta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Gamma_{m,\text{prim}}, \ m := a \cdot d. \]

Alike to the argument from part ii) the \( \Gamma \)-orbit of \( \beta \) passes through a matrix \( \alpha_\mu \in V(m, \text{prim}) \)
which proves
\[ j(\tau) = j(\beta(z)) = j(\alpha_\mu(z)) = j_\mu(z). \]
Theorem 6.11 implies that \( j_\mu \) 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 ii) and part iii) the
transitivity of integral dependence proves the integrality of \( j(\tau) \) over \( \mathbb{Z} \), i.e. \( \tau \) is an
algebraic integer, q.e.d.

\textit{Example 6.16 (Singular values of the modular \( j \)-function).} Continuing Example 6.12
we consider a CM-class \([\tau] \in X(\Gamma)\) and choose the level
\[ m = 2. \]

1. According to Example 6.12 the modular polynomial
\[ \Phi_2(j) \in \mathbb{Z}[j] \]
has degree = 4 and the zeros
\[ j - 8000, \ j - 1728, \ (j + 3375)^2 \]
The three matrices from $\Gamma_{2, \text{prim}}$

\[
\begin{align*}
M_1 &= \begin{pmatrix} 1 & -2 \\ 1 & 0 \end{pmatrix}, & M_2 &= \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, & M_3 &= \begin{pmatrix} 0 & -1 \\ 2 & 0 \end{pmatrix}
\end{align*}
\]

have respectively the fixed points in $\mathbb{H}$

\[
z_1 = \frac{1 + i\sqrt{7}}{2}, \quad z_2 = i, \quad z_3 = i\sqrt{2}
\]

One computes

\[
j(z_1) = -3375, \quad j(z_2) = 0, \quad j(z_3) = 8000
\]

Note. The corresponding imaginary quadratic fields

\[
\mathbb{Z}[z_1] = \mathcal{O}_K, \quad K = \mathbb{Q}(\sqrt{-7}); \quad \mathbb{Z}[z_2] = \mathcal{O}_K, \quad K = \mathbb{Q}(\sqrt{-1}); \quad \mathbb{Z}[z_3] = \mathcal{O}_K, \quad K = \mathbb{Q}(\sqrt{-2})
\]

have class number $h_K = 1$. In accordance with Corollary 6.23 the $j$-invariant attains integer values

\[
j(z_\mu) \in \mathbb{Z}, \quad \mu = 1, 2, 3.
\]

2. The number field

\[
K := \mathbb{Q}(i\sqrt{2})
\]

has the ring of integers

\[
\mathcal{O}_K = \mathbb{Z}[z_3]
\]

We consider the $CM$-point

\[
\tau = \frac{i}{\sqrt{2}}
\]

It is obtained as

\[
\tau = \alpha(z_3) \text{ with } \alpha = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in V(2, \text{prim})
\]

Hence

\[
j\left(\frac{i}{\sqrt{2}}\right) = j(\tau) = j(z_3) = 8000
\]

6.3 Fractional ideals and the class number formula

A further application of the modular $j$-invariant to arithmetic is the class number formula for imaginary quadratic fields.
We first recall the divisor sequence of a Riemann surface, e.g., cf. [63].

**Remark 6.17 (Class group of a compact Riemann surface).** The divisor sequence on a compact Riemann surface $X$

$$1 \to O^* \to M^* \to D \to 0$$

provides the exact sequence of Abelian groups

$$1 \to \mathbb{C}^+ \to M^*(X) \to \text{Div}(X) \to \text{Cl}(X) \to 0.$$ 

because

$$H^0(X, O^*) = \mathbb{C}^+, \quad H^0(X, D) = \text{Div}(X), \quad \text{Cl}(X) := \frac{\text{Div}(X)}{\text{im}[M^*(X) \to \text{Div}(X)]}.$$

The vanishing $H^1(X, M^*) = 0$ is a result from the theory of compact Riemann surfaces. It implies the isomorphism

$$\text{Cl}(X) \cong H^1(X, O^*) = \text{Pic}(X)$$

between the group of divisor classes and the Picard group of isomorphism classes of holomorphic line bundles on $X$. Moreover, the Picard group

$$\text{Pic}(X)$$

is finitely generated.

For number fields an analogue of divisors are fractional ideals, see [4, Chap. 9].

**Definition 6.18 (Fractional ideal).** Consider a number field $K$.

1. A **fractional ideal** of $K$ is defined as an $O_K$-submodule $a \subset K$ for which there exists an element $d \in O_K$, $d \neq 0$, with

$$d \cdot a \subset O_K.$$

Hence a fractional ideal is a subset of the form

$$a = \frac{\tilde{a}}{d} \subset K$$

with an ideal $\tilde{a} \subset O_K$. The element $d$ is named a **common denominator** of $a$.

2. Fractional ideals generated by a single element $\alpha \in K$

$$a = (\alpha) := O_K \cdot \alpha$$
are named *principal* fractional ideals.

3. For two fractionals ideals $a, b \subset K$ the *product*

$$a \cdot b$$

is the fractional ideal generated by all products $a \cdot b$, $a \in a$, $b \in b$.

4. For a fractional ideal $a \neq \{0\}$ the set

$$a^{-1} := \{x \in K : x \cdot a \subset \mathcal{O}_K\}$$

is named the *inverse* of $a$.

**Remark 6.19 (Fractional ideals).** Consider a number field $K$ with number ring $\mathcal{O}_K$.

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 $K$. As a consequence: Any fractional ideal of $K$ is a lattice of rank $= n$.

2. Because $\mathcal{O}_K$ is a Dedekind ring for a fractional ideal

$$a \neq \{0\} \subset K$$

the inverse $a^{-1}$ is also a fractional ideal, see [4, Theor. 9.8]. It satisfies

$$a \cdot a^{-1} = (1)$$

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 $K$

$$Cl(K) := J(K)/\text{im}[K^* \to J(K)]$$

The canonical map is

$$K^* \to J(K), \, x \mapsto (x).$$

Hence two fractional ideals

$$a_1, \, a_2 \in J(K)$$

define the same class in $Cl(K)$ iff

$$a_2 = a \cdot a_1 \text{ for a suitable } a \in K^*. $$

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

$$h_K := \text{ord} \ Cl(K)$$

see [40, Chap. 5, Cor. 2], [32, Chap. 12, §2]. The result is an analogue to the fact that the Picard group 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 6.17 one easily observes the analogy between corresponding objects:

<table>
<thead>
<tr>
<th>Compact Riemann surface $X$</th>
<th>Number field $K$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathcal{O}_X^*$</td>
<td>$\mathcal{O}_K^*$</td>
</tr>
<tr>
<td>$\mathcal{M}_X^*$</td>
<td>$K^*$</td>
</tr>
<tr>
<td>$\text{Div}(X)$</td>
<td>$J(K)$</td>
</tr>
<tr>
<td>$\text{Cl}(X)$</td>
<td>$\text{Cl}(K)$</td>
</tr>
</tbody>
</table>

Example 6.20 (Class number).

1. The imaginary quadratic field

$$K = \mathbb{Q}(i)$$

has class number $h_K = 1$.

2. There are exactly 9 imaginary quadratic fields

$$K = \mathbb{Q}(\sqrt{-D}), \ D > 0 \text{ squarefree integer},$$

with $h_K = 1$. They belong to the values

$$D \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}.$$  

3. The imaginary quadratic field

$$K = \mathbb{Q}(\sqrt{-5})$$

has class number $h_K = 2$. The class of the ideal

$$(2, 1 + \sqrt{-5}) \subset \mathcal{O}_K$$

is not principal. It generates $\text{Cl}(K)$, see [40, Chap. 5].
Proposition 6.21 shows for tori with complex multiplication: The endomorphism ring does not characterize the isomorphism class of the torus. Tori from different classes of biholomorphy may have the same endomorphism ring. Instead it is the class ring of the number field of the endomorphism ring, which is in bijective correspondence with the different isomorphism classes of tori. In particular, there are only finitely many isomorphism classes of tori with given endomorphism ring.

**Proposition 6.21 (Ideal classes and endomorphisms of complex tori).** Consider an arbitrary, but fixed imaginary quadratic field $K$ with ring of integers $O_K$. There exists a bijection

$$Cl(K) \cong \{[T] : T \text{ torus with } End(T) \simeq O_K\}$$

between the ideal class group $Cl(K)$ and the set of classes of biholomorphically equivalent complex tori with ring of endomorphisms $O_K$. The bijection is induced by the attachment

$$\Lambda \in J(K) \mapsto T = \mathbb{C}/\Lambda \text{ with } End(T) \simeq O_K.$$

Its inverse is induced by the attachment

$$T = \mathbb{C}/\Lambda \text{ with } End(T) = O_K \mapsto \Lambda \in J(K).$$

**Proof.** Assume

$$O_K = \mathbb{Z} + \mathbb{Z}\omega, \ \omega \in \mathbb{H}.$$

i) **Well-definedness of the map:** Starting with a fractional ideal

$$\Lambda \subset K \subset \mathbb{C}$$

Due to Remark 6.19 the ideal is a lattice and defines a torus $T = \mathbb{C}/\Lambda$. According to Corollary 2.4 the isomorphism class of $T$ depends only on the ideal class $[\Lambda] \in Cl(K)$. Proposition 6.5 implies

$$End(T) = \{\alpha \in \mathbb{C} : \alpha \cdot \Lambda \subset \Lambda\}.$$

As a consequence $O_K \subset End(T)$.

For the opposite inclusion consider a number $\alpha \in End(T)$. We may assume that the lattice is normalized

$$\Lambda = \mathbb{Z} + \Lambda \cdot \tau$$

In particular

$$\alpha = \alpha \cdot 1 \subset \mathbb{Z} + \mathbb{Z}\tau \subset O_K$$

ii) **Well-definedness of the inverse map:** Starting with a torus $T = \mathbb{C}/\Lambda$ we have to show that $\Lambda \subset K$ is a fractional ideal. W.l.o.g. the lattice $\Lambda$ is normalized
\[ \Lambda = \mathbb{Z} + \mathbb{Z} \tau. \]

By assumption

\[ \text{End}(T) = \mathcal{O}_K \]

If \( \mathcal{O}_K = \mathbb{Z} + \mathbb{Z} \omega \) then

\[ \omega \cdot \begin{pmatrix} 1 \\ \tau \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 \\ \tau \end{pmatrix}. \]

Hence

\[ \omega = \omega \cdot 1 = a + b \cdot \tau. \]

It implies

\[ \tau \in \mathbb{Q}(\omega) = K \]

and hence

\[ \Lambda \subset K. \]

The assumption

\[ \text{End}(T) = \{ \alpha \in \mathbb{C} : \alpha \Lambda \subset \Lambda \} = \mathcal{O}_K \]

implies that \( \Lambda \) is even a fractional ideal of \( K \).

iii) The two constructions from part i) and ii) are inverse to each other, q.e.d.

The class number \( h_K \) of an imaginary quadratic number field \( K \) relates to the singular value of the modular function \( j \) at a generator \( \tau \in \mathbb{H} \) of its ring \( \mathcal{O}_K \) of integers. We show that \( h_K \) is bounded from below by the degree

\[ [\mathbb{Q}(j(\tau)) : \mathbb{Q}] \]

of the singular value of the torus \( T = \mathbb{C}/\mathcal{O}_K \) attached to \( K \).

**Theorem 6.22 (Lower bound of the class number).** Consider a given imaginary quadratic field \( K \) and denote by

\[ \mathcal{O}_K = \mathbb{Z} + \mathbb{Z} \cdot \tau, \quad \tau \in \mathbb{H}, \]

its number ring. Then the class number \( h_K \) satisfies the estimate

\[ [\mathbb{Q}(j(\tau)) : \mathbb{Q}] \leq h_K. \]

Note that \( j(\tau) \in \mathbb{C} \) is an algebraic integer due to Theorem 6.15. 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] which uses the notation

\[ ELL(\mathcal{O}_K) := \{ [T] : T \text{ torus with } \text{End}(T) \simeq \mathcal{O}_K \} \]
with $[T]$ the biholomorphy class of the torus $T$. Then Proposition 6.21 states that the group action

$$CL(K) \times ELL(\mathcal{O}_K) \to ELL(\mathcal{O}_K), \ ([a], [\mathbb{C}/\Lambda]) \mapsto [\mathbb{C}/a \cdot \Lambda]$$

is transitive without fixpoints.

**Proof.** During the proof we will often switch between tori and elliptic curves, using implicitly Theorem 4.3 and Theorem 4.27. The proof will deal with two number fields:

- The given number field $K$ which defines by its number ring $\mathcal{O}_K$ an element $\tau \in \mathbb{H}$ which determines an algebraic integer $j(\tau) \subset \mathbb{Q}$.

- and the number field
  
  $$L := \mathbb{Q}[j(\tau)]$$
  
  which defines an elliptic curve $E/L$ with $j$-invariant
  
  $$j(E/L) = j(\tau)$$
  
  and for $\sigma \in \text{Gal}(L/\mathbb{Q})$ a series of conjugate elliptic curves
  
  $$(E/L)^\sigma \text{ with } j((E/L)^\sigma) = \sigma(j(\tau)).$$

The class number of the first number field $K$ turns out to be an upper bound for the degree of the second number field $L$. In the following we will use that the endomorphism ring of a complex torus $T$ does not depend on the field of definition of the different elliptic curves $E/k$ having $T$ as set of complex points, i.e. with

$$(E/k)(\mathbb{C}) = T.$$

i) The number field $L := \mathbb{Q}[j(\tau)]$: Theorem 6.15 shows that $j(\tau)$ is an algebraic integer. Hence the extension field

$$L := \mathbb{Q}(j(\tau))$$

is a number field. Set

$$m := [L : \mathbb{Q}]$$

Then $m$ automorphisms exist

$$id = \sigma_1, \sigma_2, \ldots, \sigma_m \in \text{Gal}(L/\mathbb{Q})$$

such that the conjugates

$$\sigma_1(j(\tau)), \ldots, \sigma_m(j(\tau)) \in \mathbb{C}$$

are pairwise distinct.
ii) Extending $\sigma \in \text{Gal}(L/\mathbb{Q})$ to $\tilde{\sigma} \in \text{Gal}(\mathbb{C}/L)$: The extension can be achieved in two steps:

- Extending from $\text{Gal}(L/\mathbb{Q})$ to $\text{Gal}(\mathbb{C}/L)$
- and from $\text{Gal}(\mathbb{C}/L)$ to $\text{Gal}(\mathbb{C}/\tilde{L})$

The first field extension

$$L \subset \tilde{L}$$

is an infinite tower of algebraic extensions, while the second

$$\tilde{L} \subset \mathbb{C}$$

is a pure transcendental extension with a transcendence basis $(X_i)_{i \in I}$. Hence for each $\sigma \in \text{Gal}(L/\mathbb{Q})$

$$\text{End}(E/L) \cong \text{End}((E/L)^{\tilde{\sigma}})$$

iii) Elliptic curves arising from the action of the Galois group:

Because the elements of the family $(\sigma_\mu(j(\tau)))_{\mu = 1, \ldots, m}$ are pairwise distinct, the elliptic curves

$$((E/L)^{\sigma_\mu})_{\mu = 1, \ldots, m}$$

with these $j$-invariants are pairwise non-biholomorphic. Proposition 6.21 implies that the corresponding ideal classes in $\text{Cl}(K)$ are pairwise distinct. Their number is bounded by the class number

$$h_K = \text{card } \text{Cl}(K).$$

Hence

$$[\mathbb{Q}(j(\tau)) : \mathbb{Q}] = m \leq h_K,$$

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 6.15 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

$$a_p(E) := 1 + p - \text{card } E_p(\mathbb{F}_p), \text{ } p \text{ prime},$$

to the eigenvalues of Hecke operators acting on a suitable cusp form as common eigenform. For the meaning of the numbers $a_p(E)$, the deviation of the numbers of $\mathbb{F}_p$-valued points of the reduction $E(\mathbb{F}_p)$ from the average value, see Remark 4.41.

As an introduction we start with an analogue - not for the cubics of elliptic curves but for quadrics.

Corollary 5.12 represents the discriminant modular form $\Delta$ 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 $\Delta$. We translate the law of quadratic reciprocity from algebraic number theory into a similar shape, following the preface from [17].

Remark 7.1 (Law of quadratic reciprocity). 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
\[
\left( \frac{d}{p} \right) := \begin{cases} 
+1 & d \neq 0 \mod p \text{ and } d \text{ quadratic rest } \mod p \\
-1 & d \neq 0 \mod p \text{ and } d \text{ not quadratic rest } \mod p \\
0 & d \equiv 0 \mod p 
\end{cases}
\]

The law of quadratic reciprocity relates the Legendre symbol of two primes \( p \neq q \) according to the formula
\[
\left( \frac{p}{q} \right) = \begin{cases} 
\left( \frac{q}{p} \right) & p \equiv 1 \mod 4 \text{ or } q \equiv 1 \mod 4 \\
-\left( \frac{q}{p} \right) & p \equiv 3 \mod 4 \text{ and } q \equiv 3 \mod 4
\end{cases}
\]

**Remark 7.2 (Reduction of quadrics modulo primes).**

1. 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 4.41 for elliptic curves we define

\[
a_p(Q) := \text{card } Q(\mathbb{F}_p) - 1.
\]

The value 1 in the definition is the average number of solutions \( \mod p \). Apparently, \( a_p(Q) \) equals the Legendre symbol

\[
a_p(Q) = \left( \frac{d}{p} \right).
\]

The values extend to \( a_n(Q) \), \( n \in \mathbb{N} \), and satisfy the product rule

\[
a_{nm}(Q) = a_n(Q) \cdot a_m(Q).
\]

Due to the Law of Quadratic Reciprocity the Legendre symbol depends only on the residue class \( p \mod 4d \).
2. 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

\[ (T_p f)(n) := \begin{cases} 
 f(p \cdot n) & p \nmid N \\
 0 & p \nmid N 
\end{cases} \]

for \(n \in G\). We claim: All endomorphisms \((T_p)_{p \text{ prime}}\) have a simultaneous eigenvector, namely the distinguished function

\[ f_Q : G \to \mathbb{C}, \quad f(n) := a_n(Q). \]

Note that \(f_Q\) is well-defined on the residue classes of \(G\) because the Legendre symbol depends on the residue class \(p \mod 4d\). 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 \(p \in \mathbb{Z}\)

\[ T_p(f_Q) = a_p(Q) \cdot f_Q. \]

A first version of the relation between rational elliptic curves and the theory of modular forms is Conjecture 7.6.

**Conjecture 7.3 (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 7.4 (Wiles’ modularity theorem). The Shimura-Taniyama-Weil conjecture is correct.

For the proof of the modularity theorem, Theorem 7.4, 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 4.43 and 4.45, and also Remark 4.44.

For the cusp form $f$ see Definition 7.5.

Definition 7.5 ($L$-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

$$f(\tau) = \sum_{n=1}^{\infty} c_n \cdot q^n, \quad q := e^{2\pi i \tau},$$

one defines its $L$-series

$$L(f,-): \{s \in \mathbb{C} : \text{Re } s > 1 + (k/2)\} \rightarrow \mathbb{C}, \quad L(f,s) := \sum_{n=1}^{\infty} \frac{c_n}{n^s}.$$

Remark 7.6 ($L$-series of a cusp form).

1. The $L$-series $L(f,-)$ from Definition 7.5 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 7.4. 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 7.7 (Versions of the modularity theorem).

1. Complex elliptic curve: Each elliptic curve $E/\mathbb{C}$ with rational modular invariant
   \[ j_E = \frac{1728 \cdot g_3^3}{g_3^3 - 27 \cdot g_3^2} \in \mathbb{Q} \]
   is uniformized by a modular curve, i.e. there exists an integer $N \in \mathbb{N}$ and a surjective holomorphic map
   \[ X_0(N) \rightarrow E/\mathbb{C}, \]
   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 $\mathbb{Q}$
   \[ X_0(N)_{\mathbb{Q}} \rightarrow E/\mathbb{Q}, \]
   see [17, Theor. 7.7.2].

3. Jacobi torus: For each elliptic curve $E/\mathbb{C}$ with rational modular invariant
   \[ j_E = \frac{1728 \cdot g_3^3}{g_3^3 - 27 \cdot g_3^2} \in \mathbb{Q} \]
   exists an integer $N \in \mathbb{N}$ and a surjective holomorphic map
   \[ \text{Jac}(X_0(N)) \rightarrow E, \]
   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 4.39 for an elliptic curve $E/\mathbb{Q}$ with global minimal Weierstrass polynomial $F \in \mathbb{Z}[X,Y]$ the conductor
\[ \text{cond } E = \prod_p p^{e_p} \in \mathbb{Z}, \]
having the same prime factors \( p \) as the discriminant \( \Delta_F \) 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 7.8 (Forerunner of the Shimura-Taniyama-Weil Conjecture 7.3).

1. It is known that a non-constant holomorphic map

\[ X_0(N) \to E(\mathbb{C}) \]

as required in Conjecture 7.3 would be defined by two automorphic functions, see Definition 3.6,

\[ u, v \in \mathcal{A}_0(\Gamma_0(N)) \]

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 \( f \in S_2^{\text{new}}(\Gamma_0(N)) \).

3. If the new form \( f \in S_2^{\text{new}}(\Gamma_0(N)) \) 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

\[ X^n + Y^n = Z^n, \quad n \in \mathbb{N}, \quad n \geq 3, \]

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-Hellegouarche 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

\[j = \frac{c^3}{\Delta}\] 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 7.4, 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 7.9 (Modularity theorem).** Figure 7.1 shows different elliptic curves \(E/\mathbb{Q}\) defined by a minimal Weierstrass polynomial, their conductor \(N\), the coefficients of their \(L\)-series, and the Fourier coefficients of the new-forms in

\[S_2(I_0(N)) = H^0(X_0(N), \Omega)\]

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.
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 7.10 (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 7.11 generalizes this construction. It formalizes in which sense simple groups are the building blocks of all finite groups.
Proposition 7.11 (Jordan-Hölder theorem). Each finite group $G$ has a finite, strictly increasing sequence of subgroups, a composition series,

$$G_0 = \{e\} \subset G_1 \subset \ldots \subset G_n = G$$

such that for each $i = 1, \ldots, n$

$$G_{i-1} \subset G_i$$

is a normal subgroup with simple quotient group

$$Q_i := G_i / G_{i-1}$$

All composition series of $G$ have the same length. 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 7.12 (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 7.13 (Group representation). Consider a group $G$.

1. A group representation is a pair $(V, \rho)$ 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

$$G \times V \to V, (g, v) \mapsto g \cdot v := \rho(g)(v).$$

2. For a group representation

$$\rho : G \to V$$

with finite dimensional $V$ the trace of linear endomorphisms defines a map

$$\text{trace } \rho : G \to \mathbb{C}, \chi_\rho(g) := \text{trace } \rho(g),$$

which is named the trace of $\rho$.
The representation $V^g$ 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 permutation shows for $g_0, g \in G$

$$\text{trace } \rho(g \cdot g_0 \cdot g^{-1}) = \text{trace}(\rho(g) \cdot \rho(g_0) \cdot \rho(g)^{-1}) =$$

$$= (\text{trace}(\rho(g_0) \cdot \rho(g)^{-1} \cdot \rho(g)) = \text{trace } \rho(g_0)$$

Apparently the trace of the neutral element equals the dimension of the representation

$$\text{trace } \rho(e) = \dim V \in \mathbb{N}.$$
4. The largest sporadic is the *monster* $M$ with

$$\text{ord } M = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^3 \cdot 13^2 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 \sim 8 \cdot 10^{53}$$

The monster has 194 conjugacy classes and therefore exactly 194 irreducible representations.

**Example 7.16 (Monstrous Moonshine).** Figure 7.2 shows

- on the right-hand side the dimensions $a(n)$ of the first irreducible complex modules $V_n$, $n \leq 18$, of the monster $M$, ordered by dimension.

- and on the left-hand side the Fourier coefficients $c(n)$ of the $q$-expansion of the modular $j$-invariant.

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
relating two coefficients of the \( q \)-expansion of the modular \( j \)-invariant to the dimensions of the two lowest irreducible \( M \)-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 7.17 (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 \( \mathbb{H}^* \)
   \[
   \phi : G \times \mathbb{H}^* \rightarrow \mathbb{H}^*
   \]
   is a compact Riemann surface \( X(G) \), the modular curve of \( G \). For \( G \) with
   \[
   \text{genus } X(G) = 0
   \]
   the unique meromorphic function \( J_G \in \mathcal{M}(X(G)) \) with Fourier expansion normalized as
   \[
   J_G(\tau) = \frac{1}{q} + \sum_{n=1}^{m} a_n \cdot q^n, \quad q = e^{2\pi i \cdot \tau},
   \]
   is the Hauptmodul of \( G \).

Moonshine groups \( G \subset SL(2, \mathbb{R}) \) are congruent to the modular group \( \Gamma \) in the following sense: The intersection
\[
H := G \cap \Gamma
\]
satisfies the equality of indices
\[
\]
In particular, the index is finite because
\[
[\Gamma : H] \leq [\Gamma : \Gamma_0(N)] < \infty.
\]
7.2 Monstrous moonshine

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

$$\mathcal{M}(X(G)) = \mathbb{C}(J_G).$$

Example 7.18 (Hauptmodul).

- The Hauptmodul of the modular group $\Gamma$ 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 $\text{SL}(2, \mathbb{R})$, the moonshine group

$$\Gamma_0(2) + \subset \text{SL}(2, \mathbb{R})$$

has the Hauptmodul

$$J_{\Gamma_0(2)+} = \frac{1}{q} + 4'372 \cdot q + 96'256 \cdot q^2 + O(3)$$

Remark 7.19 (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**

$$T_{[g]}(\tau) = \sum_{n \in \mathbb{N}} \text{trace}(g|V_n^\natural) \cdot q^n, \ g \in \mathbb{M},$$

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 according to increasing dimension then the first summands of the representation from Remark 7.19 are
\[ (V_0, \rho_1), (V_1 = \{0\}), (V_2, \rho_1 \oplus \rho_{196'883}), (V_3, \rho_1 \oplus \rho_{196'883} \oplus \rho_{21'493'760} \oplus \rho_{21'493'760}) \]
The series generated by the dimensions \( (\dim V_n)_{n \in \mathbb{N}} \) has the Fourier expansion
\[
\sum_{n=-1}^{\infty} (\dim V_{n+1}) \cdot q^n = J(\tau) = 1 + 196'884 \cdot q + 21'493'760 \cdot q^2 + 21'493'760 \cdot q^3 + O(4), \quad q = e^{2\pi i \tau}.
\]
The open problem was to find explicitly a representation with the properties from the Conway-Norton conjecture, see Remark 7.19. Borcherds proved in 1992 Theorem 7.20, see [6].

**Theorem 7.20 (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 $\Gamma$ 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)
List of results and some outlooks

Group action (Def. 2.6)
Modular group and Hecke congruence subgroups (Def. 2.9)
Fundamental domain of the $\Gamma$-action (Theor. 2.16)
Proper discontinuity of the $\Gamma$-action (Lem. 2.19)
Hausdorff topology of the orbit space of the $\Gamma$-action (Theor. 2.21, Cor. 2.25)
Analytic structure of the orbit space of the $\Gamma$-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

$\Gamma$-invariant differential forms (Prop. 3.1)
Modular forms and cusp forms (Def. 3.6)
Eisenstein series (Theor. 3.9)
Discriminant form $\Delta$ (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. 4.27)
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. 4.39)
The $\zeta$-function of an elliptic curve $E/\mathbb{F}_p$ (Def. 4.43)
The $L$-series of an elliptic curve $E/\mathbb{Q}$ (Def. 4.45)

Chapter 5. Introduction to Hecke theory and applications

Focus: Analysis, number theory

Hecke operators of the modular group (Def. 5.9)
Fourier coefficients of Hecke transforms (Theor. 5.10)
The discriminant $\Delta$ as simultaneous eigenform (Cor. 5.12)
Commutativity of the Hecke algebra (Theor. 5.16)
Petersson scalar product (Theor. 5.21)
Self-adjointness of the Hecke operators of the modular group (Theor. 5.23)
Eigenforms of the Hecke algebra of the modular group (Theor. 5.24)
Oldforms and newforms (Def. 5.27)
Properties of the Ramanujan $\tau$-function (Prop. 5.30)

The modular forms $G_2N \in M_2(\Gamma_0(N))$ (Theor. 5.35)

The 4-squares theorem (Theor. 5.36)

Chapter 6. Application to imaginary quadratic fields

Focus: Analysis, algebraic number theory

Complex multiplication (Def. 6.6)

Complex multiplication and imaginary quadratic fields (Theor. 6.7)

Modular polynomials of a given level (Def. 6.9)

Coefficients of the modular polynomials from $\mathbb{Z}[j]$ (Theor. 6.11)

For CM-points $\tau \in \mathbb{H}$ the $j$-values $j(\tau) \in \mathbb{C}$ are algebraic integers (Theor. 6.15)

The ideal class group and tori with complex multiplication (Prop. 6.21)

The class number formula and the $j$-invariant (Theor. 6.22)

Chapter 7. Modular elliptic curves, monstrous moonshine

Focus: Analysis, algebraic geometry, group theory

Rational elliptic curves are modular (Theor. 7.4)

The Monstrous Moonshine theorem (Theor. 7.20)
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 platform: [57] (textbook level), [41] (research level)

The basic textbook is [17], for an elementary survey see [2].

41. mathoverflow. https://mathoverflow.net/
References

48. Schultz, Dan: Notes on Modular Forms. https://faculty.math.illinois.edu/~schult25/ModFormNotes.pdf Call 27.10.2020
57. stackexchange. https://math.stackexchange.com/
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>orbit set of $\Gamma$-action</td>
<td>182</td>
</tr>
<tr>
<td>meromorphic at $\infty$</td>
<td>83</td>
</tr>
<tr>
<td>modular curve</td>
<td></td>
</tr>
<tr>
<td>as Riemann surface</td>
<td>70</td>
</tr>
<tr>
<td>modular form</td>
<td></td>
</tr>
<tr>
<td>algebra of modular forms</td>
<td>113</td>
</tr>
<tr>
<td>as differential form on the modular curve</td>
<td>101</td>
</tr>
<tr>
<td>dimension formula</td>
<td>107</td>
</tr>
<tr>
<td>weight formula</td>
<td>109</td>
</tr>
<tr>
<td>modular function</td>
<td>87</td>
</tr>
<tr>
<td>modular group</td>
<td></td>
</tr>
<tr>
<td>action of isotropy groups</td>
<td>62</td>
</tr>
<tr>
<td>fundamental domain</td>
<td>46</td>
</tr>
<tr>
<td>orbit space</td>
<td>64</td>
</tr>
<tr>
<td>modular invariant</td>
<td></td>
</tr>
<tr>
<td>definition</td>
<td>100</td>
</tr>
<tr>
<td>evaluates to an algebraic integer</td>
<td>240</td>
</tr>
<tr>
<td>generates field of automorphic functions</td>
<td>111</td>
</tr>
<tr>
<td>modular polynomial</td>
<td></td>
</tr>
<tr>
<td>definition</td>
<td>230</td>
</tr>
<tr>
<td>representation</td>
<td>232</td>
</tr>
<tr>
<td>moduli space</td>
<td>64</td>
</tr>
<tr>
<td>number field</td>
<td></td>
</tr>
<tr>
<td>class number</td>
<td>246</td>
</tr>
<tr>
<td>period</td>
<td></td>
</tr>
<tr>
<td>definition</td>
<td>9</td>
</tr>
<tr>
<td>period group</td>
<td>10</td>
</tr>
<tr>
<td>period parallelogram</td>
<td>11</td>
</tr>
<tr>
<td>plane projective algebraic curve</td>
<td>139</td>
</tr>
<tr>
<td>positively oriented basis</td>
<td>31</td>
</tr>
<tr>
<td>projective algebraic curve</td>
<td>139</td>
</tr>
<tr>
<td>projective algebraic variety</td>
<td>139</td>
</tr>
<tr>
<td>projective space</td>
<td></td>
</tr>
<tr>
<td>higher dimensional</td>
<td>123</td>
</tr>
<tr>
<td>standard atlas</td>
<td>124</td>
</tr>
<tr>
<td>proper group action</td>
<td>59</td>
</tr>
<tr>
<td>Ramanujan $\tau$-function</td>
<td></td>
</tr>
<tr>
<td>definition</td>
<td>211</td>
</tr>
<tr>
<td>growth estimate</td>
<td>215</td>
</tr>
<tr>
<td>product and recursion formula</td>
<td>214</td>
</tr>
<tr>
<td>regular function</td>
<td>139</td>
</tr>
<tr>
<td>regular local ring</td>
<td>139</td>
</tr>
<tr>
<td>Riemann $\zeta$-function</td>
<td></td>
</tr>
<tr>
<td>sheaf</td>
<td></td>
</tr>
<tr>
<td>base-point free</td>
<td>130</td>
</tr>
<tr>
<td>globally generated</td>
<td>130</td>
</tr>
<tr>
<td>very ample</td>
<td>134</td>
</tr>
<tr>
<td>smooth point</td>
<td>139</td>
</tr>
<tr>
<td>torus</td>
<td></td>
</tr>
<tr>
<td>holomorphic map</td>
<td>32</td>
</tr>
<tr>
<td>is an elliptic curve</td>
<td>124</td>
</tr>
<tr>
<td>ring of endomorphisms</td>
<td>226</td>
</tr>
<tr>
<td>very ampleness criterion</td>
<td>135</td>
</tr>
<tr>
<td>Weierstrass $\wp$-function</td>
<td></td>
</tr>
<tr>
<td>definition</td>
<td>15</td>
</tr>
<tr>
<td>differential equation</td>
<td>21</td>
</tr>
<tr>
<td>Laurent expansion</td>
<td>20</td>
</tr>
<tr>
<td>Weierstrass polynomial</td>
<td></td>
</tr>
<tr>
<td>minimal</td>
<td>166</td>
</tr>
<tr>
<td>Zariski topology</td>
<td>139</td>
</tr>
</tbody>
</table>