

Computational Arithmetic of Modular Forms

Gabor Wiese

Abstract

These course notes are about computing modular forms and some of their arithmetic properties. Their aim is to explain and prove the modular symbols algorithm in as elementary and as explicit terms as possible, and to enable the devoted student to implement it over any ring (such that a sufficient linear algebra theory is available in the chosen computer algebra system). The chosen approach is based on group cohomology and along the way the needed tools from homological algebra are provided.

MSC (2010): 11-01, 11F11, 11F25, 11F67, 11Y16

Contents

1	Motivation and Survey	3
1.1	Theory: Brief review of modular forms and Hecke operators	3
1.2	Theory: The modular symbols formalism	7
1.3	Theory: The modular symbols algorithm	12
1.4	Theory: Number theoretic applications	14
1.5	Theory: Exercises	17
1.6	Computer exercises	18
2	Hecke algebras	19
2.1	Theory: Hecke algebras and modular forms over rings	20
2.1.1	Some commutative algebra	23
2.1.2	Commutative algebra of Hecke algebras	26
2.2	Algorithms and Implementations: Localisation Algorithms	28
2.2.1	Primary spaces	28
2.2.2	Algorithm for computing common primary spaces	29
2.2.3	Algorithm for computing idempotents	30
2.3	Theoretical exercises	30
2.4	Computer exercises	31
3	Homological algebra	32
3.1	Theory: Categories and Functors	32
3.2	Theory: Complexes and Cohomology	34
3.3	Theory: Cohomological Techniques	37
3.4	Theory: Generalities on Group Cohomology	41
3.5	Theoretical exercises	43
4	Cohomology of $\mathrm{PSL}_2(\mathbb{Z})$	44
4.1	Theory: The standard fundamental domain for $\mathrm{PSL}_2(\mathbb{Z})$	44
4.2	Theory: $\mathrm{PSL}_2(\mathbb{Z})$ as a free product	46
4.3	Theory: Mayer-Vietoris for $\mathrm{PSL}_2(\mathbb{Z})$	47
4.4	Theory: Parabolic group cohomology	50

4.5	Theory: Dimension computations	51
4.6	Theoretical exercises	53
4.7	Computer exercises	54
5	Modular symbols and Manin symbols	54
5.1	Theory: Manin symbols	54
5.2	Theory: Manin symbols and group cohomology	57
5.3	Algorithms and Implementations: Conversion between Manin and modular symbols	58
5.4	Theoretical exercises	59
5.5	Computer exercises	59
6	Eichler-Shimura	59
6.1	Theory: Petersson scalar product	59
6.2	Theory: The Eichler-Shimura map	63
6.3	Theory: Cup product and Petersson scalar product	66
6.4	Theory: The Eichler-Shimura theorem	70
6.5	Theoretical exercises	71
7	Hecke operators	71
7.1	Theory: Hecke rings	72
7.2	Theory: Hecke operators on modular forms	74
7.3	Theory: Hecke operators on group cohomology	76
7.4	Theory: Hecke operators and Shapiro's lemma	77
7.5	Theory: Eichler-Shimura revisited	78
7.6	Theoretical exercises	80
7.7	Computer exercises	81

Preface

All sections of this course are either labelled as ‘Theory’ or as ‘Algorithms and Implementations’. It is possible to study only the theory parts. However, the algorithmic parts depend heavily on the developed theory. Of course, if one is principally interested in implementations, one need not understand each and every proof. Accordingly, theoretical and computer exercises are provided.

The conception of this course is different from every treatment I know, in particular, from William Stein’s excellent book ‘Modular Forms: A Computational Approach’ ([21]) and from [6]. We emphasize the central role of Hecke algebras and focus on the use of group cohomology since on the one hand it can be described in very explicit and elementary terms and on the other hand already allows the application of the strong machinery of homological algebra. We shall not discuss any geometric approaches.

The treatment of the (group cohomological) modular symbols algorithm given in this course is complete. However, we did not include any treatment of Heilbronn matrices describing Hecke operators on Manin symbols, which allow a speed-up of Hecke operators.

This course was originally held at the Universität Duisburg-Essen in 2008 and its notes have been slightly reworked for publication in this volume.

Acknowledgements. I would like to thank the anonymous referees for a huge number of helpful suggestions and corrections that surely improved the text. Thanks are also due to the students who followed the original course, among them Maite Aranés, Adam Mohamed and Ralf Butenuth, for their helpful feedback. I would also like to thank Mariagiulia De Maria, Daniel Berhanu Mamo, Atin Modi, Luca Notarnicola and Emiliano Torti for useful corrections.

1 Motivation and Survey

This section serves as an introduction to the topics of the course. We will briefly review the theory of modular forms and Hecke operators. Then we will define the modular symbols formalism and state a theorem by Eichler and Shimura establishing a link between modular forms and modular symbols. This link is the central ingredient since the modular symbols algorithm for the computation of modular forms is entirely based on it. In this introduction, we shall also be able to give an outline of this algorithm.

1.1 Theory: Brief review of modular forms and Hecke operators

Congruence subgroups

We first recall the standard congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. By N we shall always denote a positive integer.

Consider the group homomorphism

$$\mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

By Exercise 1.22 it is surjective. Its kernel is called the principal congruence subgroup of level N and denoted $\Gamma(N)$.

The group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts naturally on $(\mathbb{Z}/N\mathbb{Z})^2$ (by multiplying the matrix with a vector). We look at the orbit and the stabiliser of $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. The orbit is

$$\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \left\{ \begin{pmatrix} a \\ c \end{pmatrix} \mid a, c \text{ generate } \mathbb{Z}/N\mathbb{Z} \right\}$$

because the determinant is 1. We also point out that the orbit of $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ can and should be viewed as the set of elements in $(\mathbb{Z}/N\mathbb{Z})^2$ which are of precise (additive) order N . We now consider the stabiliser of $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and define the group $\Gamma_1(N)$ as the preimage of that stabiliser group in $\mathrm{SL}_2(\mathbb{Z})$. Explicitly, this means that $\Gamma_1(N)$ consists of those matrices in $\mathrm{SL}_2(\mathbb{Z})$ whose reduction modulo N is of the form $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

The group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ also acts on $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$, the projective line over $\mathbb{Z}/N\mathbb{Z}$, which one can define as the tuples $(a : c)$ with $a, c \in \mathbb{Z}/N\mathbb{Z}$ such that $\langle a, c \rangle = \mathbb{Z}/N\mathbb{Z}$ modulo the equivalence relation given by multiplication by an element of $(\mathbb{Z}/N\mathbb{Z})^\times$. The action is the natural one (we should actually view $(a : c)$ as a column vector, as above). The orbit of $(1 : 0)$ for this action is $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. The preimage in $\mathrm{SL}_2(\mathbb{Z})$ of the stabiliser group of $(1 : 0)$ is called $\Gamma_0(N)$. Explicitly, it consists of those matrices in $\mathrm{SL}_2(\mathbb{Z})$ whose reduction is of the form $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. We also point out that the quotient of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ modulo the stabiliser of $(1 : 0)$ corresponds to the set of cyclic subgroups of precise order N in $(\mathbb{Z}/N\mathbb{Z})^2$. These observations are at the base of defining level structures for elliptic curves.

It is clear that $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$ and that the map

$$\Gamma_0(N)/\Gamma_1(N) \xrightarrow{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a \pmod N} (\mathbb{Z}/N\mathbb{Z})^\times$$

is a group isomorphism.

The quotient $\Gamma_0(N)/\Gamma_1(N)$ will be important in the sequel because it will act on modular forms and modular symbols for $\Gamma_1(N)$. For that purpose, we shall often consider characters (i.e. group homomorphisms) of the form

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times.$$

We shall also often extend χ to a map $(\mathbb{Z}/N\mathbb{Z}) \rightarrow \mathbb{C}$ by imposing $\chi(r) = 0$ if $(r, N) \neq 1$.

On the number theory side, the group $(\mathbb{Z}/N\mathbb{Z})^\times$ enters as the Galois group of a cyclotomic extension. More precisely, by class field theory or Exercise 1.23 we have the isomorphism

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\mathrm{Frob}_\ell \mapsto \ell} (\mathbb{Z}/N\mathbb{Z})^\times$$

for all primes $\ell \nmid N$. By Frob_ℓ we denote (a lift of) the Frobenius endomorphism $x \mapsto x^\ell$, and by ζ_N we denote any primitive N -th root of unity. We shall, thus, later on also consider χ as a character of $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. The name *Dirichlet character* (here of *modulus* N) is common usage for both.

Modular forms

We now recall the definitions of modular forms. Standard references are [10] and [5], but I still vividly recommend [9], which gives a concise and yet rather complete introduction. We denote by

$$\mathbb{H} = \{z \in \mathbb{C} \mid \text{im}(z) > 0\}$$

the upper half plane. The set of cusps is by definition $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$. The group $\text{PSL}_2(\mathbb{Z})$ acts on \mathbb{H} by Möbius transforms; more explicitly, for $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ and $z \in \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ one sets

$$M.z = \frac{az + b}{cz + d}. \quad (1.1)$$

For $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ an integer matrix with non-zero determinant, an integer k and a function $f : \mathbb{H} \rightarrow \mathbb{C}$, we put

$$(f|_k M)(z) = (f|M)(z) := f(M.z) \frac{\det(M)^{k-1}}{(cz + d)^k}.$$

Fix integers $k \geq 1$ and $N \geq 1$. A function

$$f : \mathbb{H} \rightarrow \mathbb{C}$$

given by a convergent power series (the $a_n(f)$ are complex numbers)

$$f(z) = \sum_{n=0}^{\infty} a_n(f) (e^{2\pi iz})^n = \sum_{n=0}^{\infty} a_n(f) q^n \quad \text{with } q(z) = e^{2\pi iz}$$

is called a *modular form of weight k for $\Gamma_1(N)$* if

- (i) $(f|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix})(z) = f(\frac{az+b}{cz+d})(cz+d)^{-k} = f(z)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$, and
- (ii) the function $(f|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix})(z) = f(\frac{az+b}{cz+d})(cz+d)^{-k}$ admits a limit when z tends to $i\infty$ (we often just write ∞) for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ (this condition is called *f is holomorphic at the cusp a/c*).

We use the notation $M_k(\Gamma_1(N); \mathbb{C})$. If we replace (ii) by

- (ii)' the function $(f|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix})(z) = f(\frac{az+b}{cz+d})(cz+d)^{-k}$ is holomorphic and the limit $f(\frac{az+b}{cz+d})(cz+d)^{-k}$ is 0 when z tends to $i\infty$,

then f is called a *cusp form*. For these, we introduce the notation $S_k(\Gamma_1(N); \mathbb{C})$.

Let us now suppose that we are given a Dirichlet character χ of modulus N as above. Then we replace (i) as follows:

- (i)' $f(\frac{az+b}{cz+d})(cz+d)^{-k} = \chi(d)f(z)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

Functions satisfying this condition are called *modular forms* (respectively, *cusp forms* if they satisfy (ii)') *of weight k , character χ and level N* . The notation $M_k(N, \chi; \mathbb{C})$ (respectively, $S_k(N, \chi; \mathbb{C})$) will be used.

All these are finite dimensional \mathbb{C} -vector spaces. For $k \geq 2$, there are dimension formulae, which one can look up in [21]. We, however, point the reader to the fact that for $k = 1$ nearly nothing about the dimension is known (except that it is smaller than the respective dimension for $k = 2$; it is believed to be much smaller, but only very weak results are known to date).

Hecke operators

At the base of everything that we will do with modular forms are the Hecke operators and the diamond operators. One should really define them more conceptually (e.g. geometrically), but this takes some time. Here is a definition by formulae.

If a is an integer coprime to N , by Exercise 1.24 we may let σ_a be a matrix in $\Gamma_0(N)$ such that

$$\sigma_a \equiv \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \pmod{N}. \quad (1.2)$$

We define the *diamond operator* $\langle a \rangle$ (you see the diamond in the notation, with some phantasy) by the formula

$$\langle a \rangle f = f|_k \sigma_a.$$

If $f \in M_k(N, \chi; \mathbb{C})$, then we have by definition $\langle a \rangle f = \chi(a)f$. The diamond operators give a group action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $M_k(\Gamma_1(N); \mathbb{C})$ and on $S_k(\Gamma_1(N); \mathbb{C})$, and the $M_k(N, \chi; \mathbb{C})$ and $S_k(N, \chi; \mathbb{C})$ are the χ -eigenspaces for this action. We thus have the isomorphism

$$M_k(\Gamma_1(N); \mathbb{C}) \cong \bigoplus_{\chi} M_k(N, \chi; \mathbb{C})$$

for χ running through the characters of $(\mathbb{Z}/N\mathbb{Z})^\times$ (and similarly for the cuspidal spaces).

Let ℓ be a prime. We let

$$\mathcal{R}_\ell := \left\{ \begin{pmatrix} 1 & r \\ 0 & \ell \end{pmatrix} \mid 0 \leq r \leq \ell - 1 \right\} \cup \left\{ \sigma_\ell \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \right\}, \quad \text{if } \ell \nmid N \quad (1.3)$$

$$\mathcal{R}_\ell := \left\{ \begin{pmatrix} 1 & r \\ 0 & \ell \end{pmatrix} \mid 0 \leq r \leq \ell - 1 \right\}, \quad \text{if } \ell \mid N \quad (1.4)$$

We use these sets to define the *Hecke operator* T_ℓ acting on f as above as follows:

$$f|_k T_\ell := T_\ell f := \sum_{\delta \in \mathcal{R}_\ell} f|_k \delta.$$

Lemma 1.1. *Suppose $f \in M_k(N, \chi; \mathbb{C})$. Recall that we have extended χ so that $\chi(\ell) = 0$ if ℓ divides N . We have the formula*

$$a_n(T_\ell f) = a_{\ell n}(f) + \ell^{k-1} \chi(\ell) a_{n/\ell}(f).$$

In the formula, $a_{n/\ell}(f)$ is to be read as 0 if ℓ does not divide n .

Proof. Exercise 1.25. □

The Hecke operators for composite n can be defined as follows (we put T_1 to be the identity):

$$\begin{aligned} T_{\ell^{r+1}} &= T_\ell \circ T_{\ell^r} - \ell^{k-1} \langle \ell \rangle T_{\ell^{r-1}} && \text{for all primes } \ell \text{ and } r \geq 1, \\ T_{uv} &= T_u \circ T_v && \text{for coprime positive integers } u, v. \end{aligned} \quad (1.5)$$

We derive the very important formula (valid for every n)

$$a_1(T_n f) = a_n(f). \quad (1.6)$$

It is the only formula that we will really need.

From Lemma 1.1 and the above formulae it is also evident that the Hecke operators commute among one another. By Exercise 1.26 eigenspaces for a collection of operators (i.e. each element of a given set of Hecke operators acts by scalar multiplication) are respected by all Hecke operators. Hence, it makes sense to consider modular forms which are eigenvectors for every Hecke operator. These are called *Hecke eigenforms*, or often just *eigenforms*. Such an eigenform f is called *normalised* if $a_1(f) = 1$. We shall consider eigenforms in more detail in the following section.

Finally, let us point out the formula (for ℓ prime and $\ell \equiv d \pmod{N}$)

$$\ell^{k-1} \langle d \rangle = T_\ell^2 - T_{\ell^2}. \quad (1.7)$$

Hence, the diamond operators can be expressed as \mathbb{Z} -linear combinations of Hecke operators. Note that divisibility is no trouble since we may choose ℓ_1, ℓ_2 , both congruent to d modulo N satisfying an equation $1 = \ell_1^{k-1} r + \ell_2^{k-1} s$ for appropriate $r, s \in \mathbb{Z}$.

Hecke algebras and the q -pairing

We now quickly introduce the concept of Hecke algebras. It will be treated in more detail in later sections. In fact, *when we claim to compute modular forms with the modular symbols algorithm, we are really computing Hecke algebras*. In the couple of lines to follow, we show that the Hecke algebra is the dual of modular forms, and hence all knowledge about modular forms can - in principle - be derived from the Hecke algebra.

For the moment, we define the *Hecke algebra* of $M_k(\Gamma_1(N); \mathbb{C})$ as the sub- \mathbb{C} -algebra inside the endomorphism ring of the \mathbb{C} -vector space $M_k(\Gamma_1(N); \mathbb{C})$ generated by all Hecke operators and all diamond operators. We make similar definitions for $S_k(\Gamma_1(N); \mathbb{C})$, $M_k(N, \chi; \mathbb{C})$ and $S_k(N, \chi; \mathbb{C})$. Let us introduce the pieces of notation

$$\mathbb{T}_{\mathbb{C}}(M_k(\Gamma_1(N); \mathbb{C})), \mathbb{T}_{\mathbb{C}}(S_k(\Gamma_1(N); \mathbb{C})), \mathbb{T}_{\mathbb{C}}(M_k(N, \chi; \mathbb{C})) \text{ and } \mathbb{T}_{\mathbb{C}}(S_k(N, \chi; \mathbb{C})),$$

respectively. We now define a bilinear pairing, which we call the (*complex*) q -pairing, as

$$M_k(N, \chi; \mathbb{C}) \times \mathbb{T}_{\mathbb{C}}(M_k(N, \chi; \mathbb{C})) \rightarrow \mathbb{C}, \quad (f, T) \mapsto a_1(Tf)$$

(compare with Equation 1.6).

Lemma 1.2. *Suppose $k \geq 1$. The complex q -pairing is perfect, as is the analogous pairing for $S_k(N, \chi; \mathbb{C})$. In particular,*

$$M_k(N, \chi; \mathbb{C}) \cong \text{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}(M_k(N, \chi; \mathbb{C})), \mathbb{C}), \quad f \mapsto (T \mapsto a_1(Tf))$$

and similarly for $S_k(N, \chi; \mathbb{C})$. For $S_k(N, \chi; \mathbb{C})$, the inverse is given by sending ϕ to $\sum_{n=1}^{\infty} \phi(T_n)q^n$.

Proof. Let us first recall that a pairing over a field is perfect if and only if it is non-degenerate. That is what we are going to check. It follows from Equation 1.6 like this. If for all n we have $0 = a_1(T_n f) = a_n(f)$, then $f = 0$ (this is immediately clear for cusp forms; for general modular forms at the first place we can only conclude that f is a constant, but since $k \geq 1$, non-zero constants are not modular forms). Conversely, if $a_1(Tf) = 0$ for all f , then $a_1(T(T_n f)) = a_1(T_n Tf) = a_n(Tf) = 0$ for all f and all n , whence $Tf = 0$ for all f . As the Hecke algebra is defined as a subring in the endomorphism of $M_k(N, \chi; \mathbb{C})$ (resp. the cusp forms), we find $T = 0$, proving the non-degeneracy. \square

The perfectness of the q -pairing is also called the *existence of a q -expansion principle*. Due to its central role for this course, we repeat and emphasize that the Hecke algebra is the linear dual of the space of modular forms.

Lemma 1.3. *Let f in $M_k(\Gamma_1(N); \mathbb{C})$ be a normalised eigenform. Then*

$$T_n f = a_n(f) f \quad \text{for all } n \in \mathbb{N}.$$

Moreover, the natural map from the above duality gives a bijection

$$\{\text{Normalised eigenforms in } M_k(\Gamma_1(N); \mathbb{C})\} \leftrightarrow \text{Hom}_{\mathbb{C}\text{-algebra}}(\mathbb{T}_{\mathbb{C}}(M_k(\Gamma_1(N); \mathbb{C})), \mathbb{C}).$$

Similar results hold, of course, also in the presence of χ .

Proof. Exercise 1.27. \square

1.2 Theory: The modular symbols formalism

In this section we give a definition of formal modular symbols, as implemented in MAGMA and like the one in [16], [6] and [21], except that we do not factor out torsion, but intend a common treatment for all rings.

Contrary to the texts just mentioned, we prefer to work with the group

$$\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}) / \langle -1 \rangle,$$

since it will make some of the algebra much simpler and since it has a very simple description as a free product (see later). The definitions of modular forms could have been formulated using $\mathrm{PSL}_2(\mathbb{Z})$ instead of $\mathrm{SL}_2(\mathbb{Z})$, too (Exercise 1.28).

We introduce some definitions and pieces of notation to be used in all the course.

Definition 1.4. *Let R be a ring, Γ a group and V a left $R[\Gamma]$ -module. The Γ -invariants of V are by definition*

$$V^\Gamma = \{v \in V \mid g.v = v \ \forall g \in \Gamma\} \subseteq V.$$

The Γ -coinvariants of V are by definition

$$V_\Gamma = V / \langle v - g.v \mid g \in \Gamma, v \in V \rangle.$$

If $H \leq \Gamma$ is a finite subgroup, we define the norm of H as

$$N_H = \sum_{h \in H} h \in R[\Gamma].$$

Similarly, if $g \in \Gamma$ is an element of finite order n , we define the norm of g as

$$N_g = N_{\langle g \rangle} = \sum_{i=0}^{n-1} g^i \in R[\Gamma].$$

Please look at the important Exercise 1.29 for some properties of these definitions. We shall make use of the results of this exercise in the section on group cohomology.

For the rest of this section, we let R be a commutative ring with unit and Γ be a subgroup of finite index in $\mathrm{PSL}_2(\mathbb{Z})$. For the time being we allow general modules; so we let V be a left $R[\Gamma]$ -module. Recall that $\mathrm{PSL}_2(\mathbb{Z})$ acts on $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ by Möbius transformations, as defined earlier. A generalised version of the definition below appeared in [24].

Definition 1.5. *We define the R -modules*

$$\mathcal{M}_R := R[\{\alpha, \beta\} \mid \alpha, \beta \in \mathbb{P}^1(\mathbb{Q})] / \langle \{\alpha, \alpha\}, \{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\} \mid \alpha, \beta, \gamma \in \mathbb{P}^1(\mathbb{Q}) \rangle$$

and

$$\mathcal{B}_R := R[\mathbb{P}^1(\mathbb{Q})].$$

We equip both with the natural left Γ -action. Furthermore, we let

$$\mathcal{M}_R(V) := \mathcal{M}_R \otimes_R V \quad \text{and} \quad \mathcal{B}_R(V) := \mathcal{B}_R \otimes_R V$$

for the left diagonal Γ -action.

(a) We call the Γ -coinvariants

$$\mathcal{M}_R(\Gamma, V) := \mathcal{M}_R(V)_\Gamma = \mathcal{M}_R(V) / \langle (x - gx) \mid g \in \Gamma, x \in \mathcal{M}_R(V) \rangle$$

the space of (Γ, V) -modular symbols.

(b) We call the Γ -coinvariants

$$\mathcal{B}_R(\Gamma, V) := \mathcal{B}_R(V)_\Gamma = \mathcal{B}_R(V) / \langle (x - gx) | g \in \Gamma, x \in \mathcal{B}_R(V) \rangle$$

the space of (Γ, V) -boundary symbols.

(c) We define the boundary map as the map

$$\mathcal{M}_R(\Gamma, V) \rightarrow \mathcal{B}_R(\Gamma, V)$$

which is induced from the map $\mathcal{M}_R \rightarrow \mathcal{B}_R$ sending $\{\alpha, \beta\}$ to $\{\beta\} - \{\alpha\}$.

(d) The kernel of the boundary map is denoted by $\mathcal{CM}_R(\Gamma, V)$ and is called the space of cuspidal (Γ, V) -modular symbols.

(e) The image of the boundary map inside $\mathcal{B}_R(\Gamma, V)$ is denoted by $\mathcal{E}_R(\Gamma, V)$ and is called the space of (Γ, V) -Eisenstein symbols.

The reader is now invited to prove that the definition of $\mathcal{M}_R(\Gamma, V)$ behaves well with respect to base change (Exercise 1.30).

The modules $V_n(R)$ and $V_n^X(R)$

Let R be a ring. We put $V_n(R) = R[X, Y]_n \cong \text{Sym}^n(R^2)$ (see Exercise 1.31). By $R[X, Y]_n$ we mean the homogeneous polynomials of degree n in two variables with coefficients in the ring R . By $\text{Mat}_2(\mathbb{Z})_{\det \neq 0}$ we denote the monoid of integral 2×2 -matrices with non-zero determinant (for matrix multiplication), i.e., $\text{Mat}_2(\mathbb{Z})_{\det \neq 0} = \text{GL}_2(\mathbb{Q}) \cap \mathbb{Z}^{2 \times 2}$. Then $V_n(R)$ is a $\text{Mat}_2(\mathbb{Z})_{\det \neq 0}$ -module in several natural ways.

One can give it the structure of a left $\text{Mat}_2(\mathbb{Z})_{\det \neq 0}$ -module via the polynomials by putting

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f \right)(X, Y) = f\left((X, Y) \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) = f((aX + cY, bX + dY)).$$

Merel and Stein, however, consider a different one, and that is the one implemented in MAGMA, namely

$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot f \right)(X, Y) = f\left(\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right)^\iota \begin{pmatrix} X \\ Y \end{pmatrix} \right) = f\left(\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \right) = f\left(\begin{pmatrix} dX - bY \\ -cX + aY \end{pmatrix} \right).$$

Here, ι denotes Shimura's main involution whose definition can be read off from the line above (note that M^ι is the inverse of M if M has determinant 1). Fortunately, both actions are isomorphic due to the fact that the transpose of $\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right)^\iota \begin{pmatrix} X \\ Y \end{pmatrix}$ is equal to $(X, Y)\sigma^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \sigma$, where $\sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. More precisely, we have the isomorphism $V_n(R) \xrightarrow{f \mapsto \sigma^{-1} \cdot f} V_n(R)$, where the left hand side module carries "our" action and the right hand side module carries the other one. By $\sigma^{-1} \cdot f$ we mean "our" $\sigma^{-1} \cdot f$.

Of course, there is also a natural right action by $\text{Mat}_2(\mathbb{Z})_{\det \neq 0}$, namely

$$(f \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}) \left(\begin{pmatrix} X \\ Y \end{pmatrix} \right) = f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \right) = f\left(\begin{pmatrix} aX + bY \\ cX + dY \end{pmatrix} \right).$$

By the standard inversion trick, also both left actions described above can be turned into right ones.

Let now $(\mathbb{Z}/N\mathbb{Z})^\times \rightarrow R^\times$ be a Dirichlet character, which we shall also consider as a character $\chi : \Gamma_0(N) \xrightarrow{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a} (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\chi} R^\times$. By R^χ we denote the $R[\Gamma_0(N)]$ -module which is defined to be R with the $\Gamma_0(N)$ -action through χ , i.e. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot r = \chi(a)r = \chi^{-1}(d)r$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ and $r \in R$.

For use with Hecke operators, we extend this action to matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2 \times 2}$ which are congruent to an upper triangular matrix modulo N (but not necessarily of determinant 1). Concretely, we also put $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot r = \chi(a)r$ for $r \in R$ in this situation. Sometimes, however, we want to use the coefficient d in the action. In order to do so, we let $R^{\chi, X}$ be R with the action $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot r = \chi(d)r$ for matrices as above. In particular, the $\Gamma_0(N)$ -actions on $R^{\chi, X}$ and $R^{\chi^{-1}}$ coincide.

Note that due to $(\mathbb{Z}/N\mathbb{Z})^\times$ being an abelian group, the same formulae as above make R^χ also into a right $R[\Gamma_0(N)]$ -module. Hence, putting

$$(f \otimes r) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (f|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix}) \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix} r$$

makes $M_k(\Gamma_1(N); \mathbb{C}) \otimes_{\mathbb{C}} \mathbb{C}^\times$ into a right $\Gamma_0(N)$ -module and we have the description (Exercise 1.32)

$$M_k(N, \chi; \mathbb{C}) = (M_k(\Gamma_1(N); \mathbb{C}) \otimes_{\mathbb{C}} \mathbb{C}^\times)^{(\mathbb{Z}/N\mathbb{Z})^\times} \quad (1.8)$$

and similarly for $S_k(N, \chi; \mathbb{C})$.

We let

$$V_n^\chi(R) := V_n(R) \otimes_R R^\times \text{ and } V_n^{\iota, \chi}(R) := V_n(R) \otimes_R R^{\iota, \chi}$$

equipped with the natural diagonal left $\Gamma_0(N)$ -actions. Note that unfortunately these modules are in general not $\mathrm{SL}_2(\mathbb{Z})$ -modules, but we will not need that. Note, moreover, that if $\chi(-1) = (-1)^n$, then minus the identity acts trivially on $V_n^\chi(R)$ and $V_n^{\iota, \chi}(R)$, whence we consider these modules also as $\Gamma_0(N)/\{\pm 1\}$ -modules.

The modular symbols formalism for standard congruence subgroups

We now specialise the general set-up on modular symbols that we have used so far to the precise situation needed for establishing relations with modular forms.

So we let $N \geq 1$, $k \geq 2$ be integers and fix a character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow R^\times$, which we also sometimes view as a group homomorphism $\Gamma_0(N) \rightarrow R^\times$ as above. We impose that $\chi(-1) = (-1)^k$.

We define

$$\begin{aligned} \mathcal{M}_k(N, \chi; R) &:= \mathcal{M}_R(\Gamma_0(N)/\{\pm 1\}, V_{k-2}^\chi(R)), \\ \mathcal{CM}_k(N, \chi; R) &:= \mathcal{CM}_R(\Gamma_0(N)/\{\pm 1\}, V_{k-2}^\chi(R)), \\ \mathcal{B}_k(N, \chi; R) &:= \mathcal{B}_R(\Gamma_0(N)/\{\pm 1\}, V_{k-2}^\chi(R)) \end{aligned}$$

and

$$\mathcal{E}_k(N, \chi; R) := \mathcal{E}_R(\Gamma_0(N)/\{\pm 1\}, V_{k-2}^\chi(R)).$$

We make the obvious analogous definitions for $\mathcal{M}_k(\Gamma_1(N); R)$ etc.

Let

$$\eta := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}. \quad (1.9)$$

Because of

$$\eta \begin{pmatrix} a & b \\ c & d \end{pmatrix} \eta = \begin{pmatrix} a & -b \\ -c & d \end{pmatrix}$$

we have

$$\eta \Gamma_1(N) \eta = \Gamma_1(N) \quad \text{and} \quad \eta \Gamma_0(N) \eta = \Gamma_0(N).$$

We can use the matrix η to define an involution (also denoted by η) on the various modular symbols spaces. We just use the diagonal action on $\mathcal{M}_R(V) := \mathcal{M}_R \otimes_R V$, provided, of course, that η acts on V . On $V_{k-2}(R)$ we use the usual $\mathrm{Mat}_2(\mathbb{Z})_{\det \neq 0}$ -action, and on $V_{k-2}^\chi(R) = V_{k-2}(R) \otimes R^\times$ we let η only act on the first factor. We will denote by the superscript $+$ the subspace invariant under this involution, and by the superscript $-$ the anti-invariant one. We point out that there are other very good definitions of $+$ -spaces and $-$ -spaces. For instance, in many applications it can be of advantage to define the $+$ -space as the η -coinvariants, rather than the η -invariants. In particular, for modular symbols, where we are using quotients and coinvariants all the time, this alternative definition is more suitable. The reader should just think about the differences between these two definitions. Note that here we are not following the conventions of [21], p. 141. Our action just seems more natural than adding an extra minus sign.

Hecke operators

The aim of this part is to state the definition of Hecke operators and diamond operators on formal modular symbols $\mathcal{M}_k(N, \chi; R)$ and $\mathcal{CM}_k(N, \chi; R)$. One immediately sees that it is very similar to the one on modular forms. One can get a different insight in the defining formulae by seeing how they are derived from a double coset formulation in section 7.

The definition given here is also explained in detail in [21]. We should also mention the very important fact that one can transfer Hecke operators in an explicit way to Manin symbols using Heilbronn matrices. We shall not do this explicitly in this course. This point is discussed in detail in [21] and [16].

We now give the definition only for T_ℓ for a prime ℓ and the diamond operators. The T_n for composite n can be computed from those by the formulae already stated in (1.5). Notice that the $R[\Gamma_0(N)]$ -action on $V_{k-2}^\chi(R)$ (for the usual conventions, in particular, $\chi(-1) = (-1)^k$) extends naturally to an action of the semi-group generated by $\Gamma_0(N)$ and \mathcal{R}_ℓ (see Equation 1.3). Thus, this semi-group acts on $\mathcal{M}_k(N, \chi; R)$ (and the cusp space) by the diagonal action on the tensor product. Let $x \in \mathcal{M}_k(\Gamma_1(N); R)$ or $x \in \mathcal{M}_k(N, \chi; R)$. We put

$$T_\ell x = \sum_{\delta \in \mathcal{R}_\ell} \delta.x.$$

If a is an integer coprime to N , we define the diamond operator as

$$\langle a \rangle x = \sigma_a x$$

with σ_a as in equation (1.2). When $x = (m \otimes v \otimes 1)_{\Gamma_0(N)/\{\pm 1\}} \in \mathcal{M}_k(N, \chi; R)$ for $m \in \mathcal{M}_R$ and $v \in V_{k-2}$, we have $\langle a \rangle x = (\sigma_a m \otimes \sigma_a v) \otimes \chi(a^{-1})_{\Gamma_0(N)/\{\pm 1\}} = x$, thus $(\sigma_a(m \otimes v) \otimes 1)_{\Gamma_0(N)/\{\pm 1\}} = \chi(a)(m \otimes v \otimes 1)_{\Gamma_0(N)/\{\pm 1\}}$.

As in the section on Hecke operators on modular forms, we define Hecke algebras on modular symbols in a very similar way. We will take the freedom of taking arbitrary base rings (we will do that for modular forms in the next section, too).

Thus for any ring R we let $\mathbb{T}_R(\mathcal{M}_k(\Gamma_1(n); R))$ be the R -subalgebra of the R -endomorphism algebra of the R -module $\mathcal{M}_k(\Gamma_1(n); R)$ generated by the Hecke operators T_n . For a character $\chi : \mathbb{Z}/N\mathbb{Z} \rightarrow R^\times$, we make a similar definition. We also make a similar definition for the cuspidal subspace and the $+$ - and $-$ -spaces.

The following fact will be obvious from the description of modular symbols as Manin symbols (see Theorem 5.7), which will be derived in a later chapter. Here, we already want to use it.

Proposition 1.6. *The R -modules $\mathcal{M}_k(\Gamma_1(N); R)$, $\mathcal{CM}_k(\Gamma_1(N); R)$, $\mathcal{M}_k(N, \chi; R)$, $\mathcal{CM}_k(N, \chi; R)$ are finitely presented.*

Corollary 1.7. *Let R be Noetherian. The Hecke algebras $\mathbb{T}_R(\mathcal{M}_k(\Gamma_1(N); R))$, $\mathbb{T}_R(\mathcal{CM}_k(\Gamma_1(N); R))$, $\mathbb{T}_R(\mathcal{M}_k(N, \chi; R))$ and $\mathbb{T}_R(\mathcal{CM}_k(N, \chi; R))$ are finitely presented R -modules.*

Proof. This follows from Proposition 1.6 since the endomorphism ring of a finitely generated module is finitely generated and submodules of finitely generated modules over Noetherian rings are finitely generated. Furthermore, over a Noetherian ring, finitely generated implies finitely presented. \square

This very innocent looking corollary will give - together with the Eichler-Shimura isomorphism - that coefficient fields of normalised eigenforms are number fields. We next prove that the formation of Hecke algebras for modular symbols behaves well with respect to flat base change. We should have in mind the example $R = \mathbb{Z}$ or $R = \mathbb{Z}[\chi] := \mathbb{Z}[\chi(n) : n \in \mathbb{N}]$ (i.e., the ring of integers of the cyclotomic extension of \mathbb{Q} generated by the values of χ or, equivalently, $\mathbb{Z}[e^{2\pi i/r}]$ where r is the order of χ) and $S = \mathbb{C}$.

Proposition 1.8. *Let R be a Noetherian ring and $R \rightarrow S$ a flat ring homomorphism.*

(a) The natural map

$$\mathbb{T}_R(\mathcal{M}_k(\Gamma_1(N); R)) \otimes_R S \cong \mathbb{T}_S(\mathcal{M}_k(\Gamma_1(N); S))$$

is an isomorphism of S -algebras.

(b) The natural map

$$\mathrm{Hom}_R(\mathbb{T}_R(\mathcal{M}_k(\Gamma_1(N); R)), R) \otimes_R S \cong \mathrm{Hom}_S(\mathbb{T}_S(\mathcal{M}_k(\Gamma_1(N); S)), S)$$

is an isomorphism of S -modules.

(c) The map

$$\mathrm{Hom}_R(\mathbb{T}_R(\mathcal{M}_k(\Gamma_1(N); R)), S) \xrightarrow{\phi \mapsto (T \otimes s \mapsto \phi(T)s)} \mathrm{Hom}_S(\mathbb{T}_R(\mathcal{M}_k(\Gamma_1(N); R)) \otimes_R S, S)$$

is also an isomorphism of S -modules.

(d) Suppose in addition that R is an integral domain and S a field extension of the field of fractions of R . Then the natural map

$$\mathbb{T}_R(\mathcal{M}_k(\Gamma_1(N); R)) \otimes_R S \rightarrow \mathbb{T}_R(\mathcal{M}_k(\Gamma_1(N); S)) \otimes_R S$$

is an isomorphism of S -algebras.

For a character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow R^\times$, similar results hold. Similar statements also hold for the cuspidal subspace.

Proof. We only prove the proposition for $M := \mathcal{M}_k(\Gamma_1(N); R)$. The arguments are exactly the same in the other cases.

(a) By Exercise 1.30 it suffices to prove

$$\mathbb{T}_R(M) \otimes_R S \cong \mathbb{T}_S(M \otimes_R S).$$

Due to flatness and the finite presentation of M the natural homomorphism

$$\mathrm{End}_R(M) \otimes_R S \rightarrow \mathrm{End}_S(M \otimes_R S)$$

is an isomorphism (see [13], Prop. 2.10). By definition, the Hecke algebra $\mathbb{T}_R(M)$ is an R -submodule of $\mathrm{End}_R(M)$. As injections are preserved by flat morphisms, we obtain the injection

$$\mathbb{T}_R(M) \otimes_R S \hookrightarrow \mathrm{End}_R(M) \otimes_R S \cong \mathrm{End}_S(M \otimes_R S).$$

The image is equal to $\mathbb{T}_S(M \otimes_R S)$, since all Hecke operators are hit, establishing (a).

(b) follows from the same citation from [13] as above.

(c) Suppose that under the map from Statement (c) $\phi \in \mathrm{Hom}_R(\mathbb{T}_R(M), S)$ is mapped to the zero map. Then $\phi(T)s = 0$ for all T and all $s \in S$. In particular with $s = 1$ we get $\phi(T) = 0$ for all T , whence ϕ is the zero map, showing injectivity. Suppose now that $\psi \in \mathrm{Hom}_S(\mathbb{T}_R(M) \otimes_R S, S)$ is given. Call ϕ the composite $\mathbb{T}_R(M) \rightarrow \mathbb{T}_R(M) \otimes_R S \xrightarrow{\psi} S$. Then ψ is the image of ϕ , showing surjectivity.

(d) We first define

$$N := \ker \left(M \xrightarrow{\pi: m \mapsto m \otimes 1} M \otimes_R S \right).$$

We claim that N consists only of R -torsion elements. Let $x \in N$. Then $x \otimes 1 = 0$. If $rx \neq 0$ for all $r \in R - \{0\}$, then the map $R \xrightarrow{r \mapsto rx} N$ is injective. We call F the image to indicate that it is a free R -module. Consider the exact sequence of R -modules:

$$0 \rightarrow F \rightarrow M \rightarrow M/F \rightarrow 0.$$

From flatness we get the exact sequence

$$0 \rightarrow F \otimes_R S \rightarrow M \otimes_R S \rightarrow M/F \otimes_R S \rightarrow 0.$$

But, $F \otimes_R S$ is 0, since it is generated by $x \otimes 1 \in M \otimes_R S$. However, F is free, whence $F \otimes_R S$ is also S . This contradiction shows that there is some $r \in R - \{0\}$ with $rx = 0$.

As N is finitely generated, there is some $r \in R - \{0\}$ such that $rN = 0$. Moreover, N is characterised as the set of elements $x \in M$ such that $rx = 0$. For, we already know that $x \in N$ satisfies $rx = 0$. If, conversely, $rx = 0$ with $x \in M$, then $0 = rx \otimes 1/r = x \otimes 1 \in M \otimes_R S$.

Every R -linear (Hecke) operator T on M clearly restricts to N , since $rTn = Trn = T0 = 0$. Suppose now that T acts as 0 on $M \otimes_R S$. We claim that then $rT = 0$ on all of M . Let $m \in M$. We have $0 = T\pi m = \pi Tm$. Thus $Tm \in N$ and, so, $rTm = 0$, as claimed. In other words, the kernel of the homomorphism $\mathbb{T}_R(M) \rightarrow \mathbb{T}_R(M \otimes_R S)$ is killed by r . This homomorphism is surjective, since by definition $\mathbb{T}_R(M \otimes_R S)$ is generated by all Hecke operators acting on $M \otimes_R S$. Tensoring with S kills the torsion and the statement follows. \square

Some words of warning are necessary. It is essential that $R \rightarrow S$ is a flat homomorphism. A similar result for $\mathbb{Z} \rightarrow \mathbb{F}_p$ is not true in general. I call this a "faithfulness problem", since then $\mathcal{M}_k(\Gamma_1(N); \mathbb{F}_p)$ is not a faithful module for $\mathbb{T}_{\mathbb{Z}}(\mathcal{M}_k(\Gamma_1(N); \mathbb{C})) \otimes_{\mathbb{Z}} \mathbb{F}_p$. Some effort goes into finding k and N , where this module is faithful. See, for instance, [23]. Moreover, $\mathcal{M}_k(\Gamma_1(N); R)$ need not be a free R -module and can contain torsion. Please have a look at Exercise 1.33 now to find out whether one can use the $+$ - and the $-$ -space in the proposition.

1.3 Theory: The modular symbols algorithm

The Eichler-Shimura theorem

At the basis of the modular symbols algorithm is the following theorem by Eichler, which was extended by Shimura. One of our aims in this lecture is to provide a proof for it. In this introduction, however, we only state it and indicate how the modular symbols algorithm can be derived from it.

Theorem 1.9 (Eichler-Shimura). *There are isomorphisms respecting the Hecke operators*

- (a) $M_k(N, \chi; \mathbb{C}) \oplus S_k(N, \chi; \mathbb{C})^\vee \cong \mathcal{M}_k(N, \chi; \mathbb{C})$,
- (b) $S_k(N, \chi; \mathbb{C}) \oplus S_k(N, \chi; \mathbb{C})^\vee \cong \mathcal{C}\mathcal{M}_k(N, \chi; \mathbb{C})$,
- (c) $S_k(N, \chi; \mathbb{C}) \cong \mathcal{C}\mathcal{M}_k(N, \chi; \mathbb{C})^+$.

Similar isomorphisms hold for modular forms and modular symbols on $\Gamma_1(N)$ and $\Gamma_0(N)$.

Proof. Later in this lecture (Theorems 5.9 and 6.15, Corollary 7.30). \square

Corollary 1.10. *Let R be a subring of \mathbb{C} and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow R^\times$ a character. Then there is the natural isomorphism*

$$\mathbb{T}_R(M_k(N, \chi; \mathbb{C})) \cong \mathbb{T}_R(\mathcal{M}_k(N, \chi; \mathbb{C})).$$

A similar result holds cusp forms, and also for $\Gamma_1(N)$ without a character as well as for $\Gamma_0(N)$.

Proof. We only prove this for the full space of modular forms. The arguments in the other cases are very similar. Theorem 1.9 tells us that the R -algebra generated by the Hecke operators inside the endomorphism ring of $M_k(N, \chi; \mathbb{C})$ equals the R -algebra generated by the Hecke operators inside the endomorphism ring of $\mathcal{M}_k(N, \chi; \mathbb{C})$, *i.e.* the assertion to be proved. To see this, one just needs to see that the algebra generated by all Hecke operators on $M_k(N, \chi; \mathbb{C}) \oplus S_k(N, \chi; \mathbb{C})^\vee$ is the same as the one generated by all Hecke operators on $M_k(N, \chi; \mathbb{C})$, which follows from the fact that if some Hecke operator T annihilates the full space of modular forms, then it also annihilates the dual of the cusp space. \square

The following corollary of the Eichler-Shimura theorem is of utmost importance for the theory of modular forms. It says that Hecke algebras of modular forms have an integral structure (take $R = \mathbb{Z}$ or $R = \mathbb{Z}[\chi]$). We will say more on this topic in the next section.

Corollary 1.11. *Let R be a subring of \mathbb{C} and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow R^\times$ a character. Then the natural map*

$$\mathbb{T}_R(\mathcal{M}_k(N, \chi; \mathbb{C})) \otimes_R \mathbb{C} \cong \mathbb{T}_{\mathbb{C}}(\mathcal{M}_k(N, \chi; \mathbb{C}))$$

is an isomorphism. A similar result holds cusp forms, and also for $\Gamma_1(N)$ without a character as well as for $\Gamma_0(N)$.

Proof. We again stick to the full space of modular forms. Tensoring the isomorphism from Corollary 1.10 with \mathbb{C} we get

$$\mathbb{T}_R(\mathcal{M}_k(N, \chi; \mathbb{C})) \otimes_R \mathbb{C} \cong \mathbb{T}_R(\mathcal{M}_k(N, \chi; \mathbb{C})) \otimes_R \mathbb{C} \cong \mathbb{T}_{\mathbb{C}}(\mathcal{M}_k(N, \chi; \mathbb{C})) \cong \mathbb{T}_{\mathbb{C}}(\mathcal{M}_k(N, \chi; \mathbb{C})),$$

using Proposition 1.8 (d) and again Theorem 1.9. \square

The next corollary is at the base of the modular symbols algorithm, since it describes modular forms in linear algebra terms involving only modular symbols.

Corollary 1.12. *Let R be a subring of \mathbb{C} and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow R^\times$ a character. Then we have the isomorphisms*

$$\begin{aligned} \mathcal{M}_k(N, \chi; \mathbb{C}) &\cong \text{Hom}_R(\mathbb{T}_R(\mathcal{M}_k(N, \chi; R)), R) \otimes_R \mathbb{C} \\ &\cong \text{Hom}_R(\mathbb{T}_R(\mathcal{M}_k(N, \chi; R)), \mathbb{C}) && \text{and} \\ \mathcal{S}_k(N, \chi; \mathbb{C}) &\cong \text{Hom}_R(\mathbb{T}_R(\mathcal{C}\mathcal{M}_k(N, \chi; R)), R) \otimes_R \mathbb{C} \\ &\cong \text{Hom}_R(\mathbb{T}_R(\mathcal{C}\mathcal{M}_k(N, \chi; R)), \mathbb{C}). \end{aligned}$$

Similar results hold for $\Gamma_1(N)$ without a character and also for $\Gamma_0(N)$.

Proof. This follows from Corollaries 1.10, 1.11, Proposition 1.8 and Lemma 1.2. \square

Please look at Exercise 1.34 to find out which statement should be included into this corollary concerning the $+$ -spaces. Here is another important consequence of the Eichler-Shimura theorem.

Corollary 1.13. *Let $f = \sum_{n=1}^{\infty} a_n(f)q^n \in \mathcal{S}_k(\Gamma_1(N); \mathbb{C})$ be a normalised Hecke eigenform. Then $\mathbb{Q}_f := \mathbb{Q}(a_n(f) | n \in \mathbb{N})$ is a number field of degree less than or equal to $\dim_{\mathbb{C}} \mathcal{S}_k(\Gamma_1(N); \mathbb{C})$.*

If f has Dirichlet character χ , then \mathbb{Q}_f is a finite field extension of $\mathbb{Q}(\chi)$ of degree less than or equal to $\dim_{\mathbb{C}} \mathcal{S}_k(N, \chi; \mathbb{C})$. Here $\mathbb{Q}(\chi)$ is the extension of \mathbb{Q} generated by all the values of χ .

Proof. It suffices to apply the previous corollaries with $R = \mathbb{Q}$ or $R = \mathbb{Q}(\chi)$ and to remember that normalised Hecke eigenforms correspond to algebra homomorphisms from the Hecke algebra into \mathbb{C} . \square

Sketch of the modular symbols algorithm

It may now already be quite clear how the modular symbols algorithm for computing cusp forms proceeds. We give a very short sketch.

Algorithm 1.14. *Input:* A field $K \subset \mathbb{C}$, integers $N \geq 1$, $k \geq 2$, P , a character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow K^\times$. *Output:* A basis of the space of cusp forms $\mathcal{S}_k(N, \chi; \mathbb{C})$; each form is given by its standard q -expansion with precision P .

- (1) create $M := \mathcal{C}\mathcal{M}_k(N, \chi; K)$.
- (2) $L \leftarrow []$ (empty list), $n \leftarrow 1$.
- (3) repeat
- (4) compute T_n on M .
- (5) join T_n to the list L .

- (6) $\mathbb{T} \leftarrow$ the K -algebra generated by all $T \in L$.
- (7) $n \leftarrow n + 1$
- (8) until $\dim_K(\mathbb{T}) = \dim_{\mathbb{C}} S_k(N, \chi; \mathbb{C})$
- (9) compute a K -basis B of \mathbb{T} .
- (10) compute the basis B^\vee of \mathbb{T}^\vee dual to B .
- (11) for ϕ in B^\vee do
- (12) output $\sum_{n=1}^P \phi(T_n)q^n \in K[q]$.
- (13) end for.

We should make a couple of remarks concerning this algorithm. Please remember that there are dimension formulae for $S_k(N, \chi; \mathbb{C})$, which can be looked up in [21]. It is clear that the repeat-until loop will stop, due to Corollary 1.12. We can even give an upper bound as to when it stops at the latest. That is the so-called Sturm bound, which is the content of the following proposition.

Proposition 1.15 (Sturm). *Let $f \in M_k(N, \chi; \mathbb{C})$ such that $a_n(f) = 0$ for all $n \leq \frac{k\mu}{12}$, where $\mu = N \prod_{l|N} (1 + \frac{1}{l})$. Then $f = 0$.*

Proof. Apply Corollary 9.20 of [21] with $\mathfrak{m} = (0)$. □

Corollary 1.16. *Let K, N, χ etc. as in the algorithm. Then $\mathbb{T}_K(\mathcal{CM}_k(N, \chi; K))$ can be generated as a K -vector space by the operators T_n for $1 \leq n \leq \frac{k\mu}{12}$.*

Proof. Exercise 1.35. □

We shall see later how to compute eigenforms and how to decompose the space of modular forms in a "sensible" way.

1.4 Theory: Number theoretic applications

We close this survey and motivation section by sketching some number theoretic applications.

Galois representations attached to eigenforms

We mention the sad fact that until 2006 only the one-dimensional representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ were well understood. In the case of finite image one can use the Kronecker-Weber theorem, which asserts that any cyclic extension of \mathbb{Q} is contained in a cyclotomic field. This is generalised by global class field theory to one-dimensional representations of $\text{Gal}(\overline{\mathbb{Q}}/K)$ for each number field K . Since we now have a proof of Serre's modularity conjecture [18] (a theorem by Khare, Wintenberger [15]), we also know a little bit about 2-dimensional representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, but, replacing \mathbb{Q} by any other number field, all one has is conjectures.

The great importance of modular forms for modern number theory is due to the fact that one may attach a 2-dimensional representation of the Galois group of the rationals to each normalised cuspidal eigenform. The following theorem is due to Shimura for $k = 2$ and due to Deligne for $k \geq 2$.

Until the end of this section, we shall use the language of Galois representations (e.g. irreducible, unramified, Frobenius element, cyclotomic character) without introducing it. It will not be used elsewhere. The meanwhile quite old lectures by Darmon, Diamond and Taylor are still an excellent introduction to the subject [7].

Theorem 1.17. *Let $k \geq 2$, $N \geq 1$, p a prime, and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ a character.*

Then to any normalised eigenform $f \in S_k(N, \chi; \mathbb{C})$ with $f = \sum_{n \geq 1} a_n(f)q^n$ one can attach a Galois representation, i.e. a continuous group homomorphism,

$$\rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\overline{\mathbb{Q}}_p)$$

such that

- (i) ρ_f is irreducible,
- (ii) $\det(\rho_f(c)) = -1$ for any complex conjugation $c \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (one says that ρ_f is odd),
- (iii) for all primes $\ell \nmid Np$ the representation ρ_f is unramified at ℓ ,

$$\text{tr}(\rho_f(\text{Frob}_\ell)) = a_\ell(f) \quad \text{and} \quad \det(\rho_f(\text{Frob}_\ell)) = \ell^{k-1}\chi(\ell).$$

In the statement, Frob_ℓ denotes a Frobenius element at ℓ .

By choosing a $\rho(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ -stable lattice in $\overline{\mathbb{Q}}_p^2$ and applying reduction and semi-simplification one obtains the following consequence.

Theorem 1.18. *Let $k \geq 2$, $N \geq 1$, p a prime, and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ a character.*

Then to any normalised eigenform $f \in S_k(N, \chi; \mathbb{C})$ with $f = \sum_{n \geq 1} a_n(f)q^n$ and to any prime ideal \mathfrak{P} of the ring of integers \mathcal{O}_f of $\mathbb{Q}_f = \mathbb{Q}(a_n(f) : n \in \mathbb{N})$ with residue characteristic p (and silently a fixed embedding $\mathcal{O}_f/\mathfrak{P} \hookrightarrow \overline{\mathbb{F}}_p$), one can attach a Galois representation, i.e. a continuous group homomorphism (for the discrete topology on $\text{GL}_2(\overline{\mathbb{F}}_p)$),

$$\rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\overline{\mathbb{F}}_p)$$

such that

- (i) ρ_f is semi-simple,
- (ii) $\det(\rho_f(c)) = -1$ for any complex conjugation $c \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (one says that ρ_f is odd),
- (iii) for all primes $\ell \nmid Np$ the representation ρ_f is unramified at ℓ ,

$$\text{tr}(\rho_f(\text{Frob}_\ell)) \equiv a_\ell(f) \pmod{\mathfrak{P}} \quad \text{and} \quad \det(\rho_f(\text{Frob}_\ell)) \equiv \ell^{k-1}\overline{\chi}(\ell) \pmod{\mathfrak{P}}.$$

Translation to number fields

Proposition 1.19. *Let f , \mathbb{Q}_f , \mathfrak{P} and ρ_f be as in Theorem 1.18. Then the following hold:*

- (a) *The image of ρ_f is finite and its image is contained in $\text{GL}_2(\mathbb{F}_{p^r})$ for some r .*
- (b) *The kernel of ρ_f is an open subgroup of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and is hence of the form $\text{Gal}(\overline{\mathbb{Q}}/K)$ for some Galois number field K . Thus, we can and do consider $\text{Gal}(K/\mathbb{Q})$ as a subgroup of $\text{GL}_2(\mathbb{F}_{p^r})$.*
- (c) *The characteristic polynomial of Frob_ℓ (more precisely, of $\text{Frob}_{\Lambda/\ell}$ for any prime Λ of K dividing ℓ) is equal to $X^2 - a_\ell(f)X + \chi(\ell)\ell^{k-1} \pmod{\mathfrak{P}}$ for all primes $\ell \nmid Np$.*

Proof. Exercise 1.36. □

To appreciate the information obtained from the $a_\ell(f) \pmod{\mathfrak{P}}$, the reader is invited to do Exercise 1.37 now.

Images of Galois representations

One can also often tell what the Galois group $\text{Gal}(K/\mathbb{Q})$ is as an abstract group. There are not so many possibilities, as we see from the following theorem.

Theorem 1.20 (Dickson). *Let p be a prime and H a finite subgroup of $\text{PGL}_2(\overline{\mathbb{F}}_p)$. Then a conjugate of H is isomorphic to one of the following groups:*

- finite subgroups of the upper triangular matrices,
- $\text{PSL}_2(\mathbb{F}_{p^r})$ or $\text{PGL}_2(\mathbb{F}_{p^r})$ for $r \in \mathbb{N}$,
- dihedral groups D_r for $r \in \mathbb{N}$ not divisible by p ,
- A_4 , A_5 or S_4 .

For modular forms there are several results mostly by Ribet concerning the groups that occur as images [19]. Roughly speaking, they say that the image is ‘as big as possible’ for almost all \mathfrak{P} (for a given f). For modular forms without CM and inner twists (we do not define these notions in this course) this means that if G is the image, then G modulo scalars is equal to $\text{PSL}_2(\mathbb{F}_{p^r})$ or $\text{PGL}_2(\mathbb{F}_{p^r})$, where \mathbb{F}_{p^r} is the extension of \mathbb{F}_p generated by the $a_n(f) \pmod{\mathfrak{P}}$.

An interesting question is to study which groups (i.e. which $\text{PSL}_2(\mathbb{F}_{p^r})$) actually occur. It would be nice to prove that all of them do, since - surprisingly - the simple groups $\text{PSL}_2(\mathbb{F}_{p^r})$ are still resisting a lot to all efforts to realise them as Galois groups over \mathbb{Q} in the context of inverse Galois theory.

Serre’s modularity conjecture

Serre’s modularity conjecture is the following. Let p be a prime and $\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\overline{\mathbb{F}}_p)$ be a continuous, odd, irreducible representation.

- Let N_ρ be the (outside of p) conductor of ρ (defined by a formula analogous to the formula for the Artin conductor, except that the local factor for p is dropped).
- Let k_ρ be the integer defined by [18].
- Let χ_ρ be the prime-to- p part of $\det \circ \rho$ considered as a character $(\mathbb{Z}/N_\rho\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \overline{\mathbb{F}}_p^\times$.

Theorem 1.21 (Khare, Wintenberger, Kisin: Serre’s Modularity Conjecture). *Let p be a prime and $\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\overline{\mathbb{F}}_p)$ be a continuous, odd, irreducible representation.*

Then there exists a normalised eigenform

$$f \in S_{k_\rho}(N_\rho, \chi_\rho; \mathbb{C})$$

such that ρ is isomorphic to the Galois representation

$$\rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\overline{\mathbb{F}}_p)$$

attached to f by Theorem 1.18.

Serre’s modularity conjecture implies that we can compute (in principle, at least) arithmetic properties of all Galois representations of the type in Serre’s conjecture by computing the mod p Hecke eigenforms they come from. Conceptually, Serre’s modularity conjecture gives an explicit description of all irreducible, odd and continuous ‘mod p ’ representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and, thus, in a sense generalises class field theory.

Edixhoven et al. [12] have succeeded in giving an algorithm which computes the actual Galois representation attached to a mod p modular form. Hence, with Serre’s conjecture we have a way of - in principle - obtaining all information on 2-dimensional irreducible, odd continuous representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

1.5 Theory: Exercises

Exercise 1.22. (a) The group homomorphism

$$\mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

given by reducing the matrices modulo N is surjective.

(b) Check the bijections

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma_1(N) = \left\{ \begin{pmatrix} a & \\ & c \end{pmatrix} \mid \langle a, c \rangle = \mathbb{Z}/N\mathbb{Z} \right\}$$

and

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma_0(N) = \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}),$$

which were given in the beginning.

Exercise 1.23. Let N be an integer and $\zeta_N \in \mathbb{C}$ any primitive N -th root of unity. Prove that the map

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \xrightarrow{\mathrm{Frob}_\ell \mapsto \ell} (\mathbb{Z}/N\mathbb{Z})^\times$$

(for all primes $\ell \nmid N$) is an isomorphism.

Exercise 1.24. Prove that a matrix σ_a as in Equation 1.2 exists.

Exercise 1.25. Prove Lemma 1.1. See also [10, Proposition 5.2.2].

Exercise 1.26. (a) Let K be a field, V a vector space and T_1, T_2 two commuting endomorphisms of V , i.e. $T_1T_2 = T_2T_1$. Let $\lambda_1 \in K$ and consider the λ_1 -eigenspace of T_1 , i.e. $V_1 = \{v \mid T_1v = \lambda_1v\}$. Prove that $T_2V_1 \subseteq V_1$.

(b) Suppose that $M_N(\Gamma_1(k); \mathbb{C})$ is non-zero. Prove that it contains a Hecke eigenform.

Exercise 1.27. Prove Lemma 1.3.

Hint: use the action of Hecke operators explicitly described on q -expansions.

Exercise 1.28. Check that it makes sense to replace $\mathrm{SL}_2(\mathbb{Z})$ by $\mathrm{PSL}_2(\mathbb{Z})$ in the definition of modular forms.

Hint: for the transformation rule: if -1 is not in the congruence subgroup in question, there is nothing to show; if -1 is in it, one has to verify that it acts trivially. Moreover convince yourself that the holomorphy at the cusps does not depend on replacing a matrix by its negative.

Exercise 1.29. Let R be a ring, Γ a group and V a left $R[\Gamma]$ -module.

(a) Define the augmentation ideal I_Γ by the exact sequence

$$0 \rightarrow I_\Gamma \rightarrow R[\Gamma] \xrightarrow{\gamma \mapsto 1} R \rightarrow 1.$$

Prove that I_Γ is the ideal in $R[\Gamma]$ generated by the elements $1 - g$ for $g \in \Gamma$.

(b) Conclude that $V_\Gamma = V/I_\Gamma V$.

(c) Conclude that $V_\Gamma \cong R \otimes_{R[\Gamma]} V$.

(d) Suppose that $\Gamma = \langle T \rangle$ is a cyclic group (either finite or infinite (isomorphic to $(\mathbb{Z}, +)$)). Prove that I_Γ is the ideal generated by $(1 - T)$.

(e) Prove that $V^\Gamma \cong \mathrm{Hom}_{R[\Gamma]}(R, V)$.

Exercise 1.30. Let R, Γ and V as in Definition 1.5 and let $R \rightarrow S$ be a ring homomorphism.

(a) Prove that

$$\mathcal{M}_R(\Gamma, V) \otimes_R S \cong \mathcal{M}_S(\Gamma, V \otimes_R S).$$

(b) Suppose $R \rightarrow S$ is flat. Prove a similar statement for the cuspidal subspace.

- (c) Are similar statements true for the boundary or the Eisenstein space? What about the $+$ - and the $-$ -spaces?

Exercise 1.31. Prove that the map

$$\mathrm{Sym}^n(R^2) \rightarrow R[X, Y]_n, \quad \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} a_n \\ b_n \end{pmatrix} \mapsto (a_1X + b_1Y) \cdots (a_nX + b_nY)$$

is an isomorphism, where $\mathrm{Sym}^n(R^2)$ is the n -th symmetric power of R^2 , which is defined as the quotient of $\underbrace{R^2 \otimes_R \cdots \otimes_R R^2}_{n\text{-times}}$ by the span of all elements $v_1 \otimes \cdots \otimes v_n - v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}$ for all σ in the symmetric group on the letters $\{1, 2, \dots, n\}$.

Exercise 1.32. Prove Equation 1.8.

Exercise 1.33. Can one use $+$ - or $-$ -spaces in Proposition 1.8? What could we say if we defined the $+$ -space as $M/(1 - \eta)M$ with M standing for some space of modular symbols?

Exercise 1.34. Which statements in the spirit of Corollary 1.12 (b) are true for the $+$ -spaces?

Exercise 1.35. Prove Corollary 1.16.

Exercise 1.36. Prove Proposition 1.19.

Exercise 1.37. In how far is a conjugacy class in $\mathrm{GL}_2(\mathbb{F}_{p^r})$ determined by its characteristic polynomial? Same question as above for a subgroup $G \subset \mathrm{GL}_2(\mathbb{F}_{p^r})$.

1.6 Computer exercises

Computer Exercise 1.38. (a) Create a list L of all primes in between 234325 and 3479854? How many are there?

- (b) For $n = 2, 3, 4, 5, 6, 7, 997$ compute for each $a \in \mathbb{Z}/n\mathbb{Z}$ how often it appears as a residue in the list L .

Computer Exercise 1.39. In this exercise you verify the validity of the prime number theorem.

- (a) Write a function `NumberOfPrimes` with the following specifications. Input: Positive integers a, b with $a \leq b$. Output: The number of primes in $[a, b]$.
- (b) Write a function `TotalNumberOfPrimes` with the following specifications. Input: Positive integers x, s . Output: A list $[n_1, n_2, n_3, \dots, n_m]$ such that n_i is the number of primes between 1 and $i \cdot s$ and m is the largest integer smaller than or equal to x/s .
- (c) Compare the output of `TotalNumberOfPrimes` with the predictions of the prime number theorem: Make a function that returns the list $[r_1, r_2, \dots, r_m]$ with $r_i = \frac{si}{\log si}$. Make a function that computes the quotient of two lists of "numbers".
- (d) Play with these functions. What do you observe?

Computer Exercise 1.40. Write a function `ValuesInField` with: Input: a unitary polynomial f with integer coefficients and K a finite field. Output: the set of values of f in K .

Computer Exercise 1.41. (a) Write a function `BinaryExpansion` that computes the binary expansion of a positive integer. Input: positive integer n . Output: list of 0's and 1's representing the binary expansion.

- (b) Write a function `Expo` with: Input: two positive integers a, b . Output a^b . You must not use the in-built function a^b , but write a sensible algorithm making use of the binary expansion of b . The only arithmetic operations allowed are multiplications.
- (c) Write similar functions using the expansion with respect to a general base d .

Computer Exercise 1.42. *In order to contemplate recursive algorithms, the monks in Hanoi used to play the following game. First they choose a degree of contemplation, i.e. a positive integer n . Then they create three lists:*

$$L_1 := [n, n-1, \dots, 2, 1]; L_2 := []; L_3 := [];$$

The aim is to exchange L_1 and L_2 . However, the monks may only perform the following step: Remove the last element from one of the lists and append it to one of the other lists, subject to the important condition that in all steps all three lists must be descending.

Contemplate how the monks can achieve their goal. Write a procedure with input n that plays the game. After each step, print the number of the step, the three lists and test whether all lists are still descending.

[Hint: For recursive procedures, i.e. procedures calling themselves, in MAGMA one must put the command forward `my_procedure` in front of the definition of `my_procedure`.]

Computer Exercise 1.43. *This exercise concerns the normalised cuspidal eigenforms in weight 2 and level 23.*

- (a) *What is the number field K generated by the coefficients of each of the two forms?*
- (b) *Compute the characteristic polynomials of the first 100 Fourier coefficients of each of the two forms.*
- (c) *Write a function that for a given prime p computes the reduction modulo p of the characteristic polynomials from the previous point and their factorisation.*
- (d) *Now use modular symbols over \mathbb{F}_p for a given p . Compare the results.*
- (e) *Now do the same for weight 2 and level 37. In particular, try $p = 2$. What do you observe? What could be the reason for this behaviour?*

Computer Exercise 1.44. *Implement Algorithm 1.14.*

2 Hecke algebras

An important point made in the previous section is that for computing modular forms, one computes Hecke algebras. This perspective puts Hecke algebras in its centre. The present section is written from that point of view. Starting from Hecke algebras, we define modular forms with coefficients in arbitrary rings, we study integrality properties and also present results on the structure of Hecke algebras, which are very useful for studying the arithmetic of modular forms.

It is essential for studying arithmetic properties of modular forms to have some flexibility for the coefficient rings. For instance, when studying mod p Galois representations attached to modular forms, it is often easier and sometimes necessary to work with modular forms whose q -expansions already lie in a finite field. Moreover, the concept of congruences of modular forms only gets its seemingly correct framework when working over rings such as extensions of finite fields or rings like $\mathbb{Z}/p^n\mathbb{Z}$.

There is a very strong theory of modular forms over a general ring R that uses algebraic geometry over R . One can, however, already get very far if one just defines modular forms over R as the R -linear dual of the \mathbb{Z} -Hecke algebra of the holomorphic modular forms, i.e. by taking q -expansions with coefficients in R . In this course we shall only use this. Precise definitions will be given in a moment. A priori it is maybe not clear whether non-trivial modular forms with q -expansions in the integers exist at all. The situation is as good as it could possibly be: the modular forms with q -expansion in the integers form a lattice in the space of all modular forms (at least for $\Gamma_1(N)$ and $\Gamma_0(N)$; if we are working with a Dirichlet character, the situation is slightly more involved). This is an extremely useful and important fact, which we shall derive from the corollaries of the Eichler-Shimura isomorphism given in the previous section.

Hecke algebras of modular forms over R are finitely generated R -modules. This leads us to a study, belonging to the theory of Commutative Algebra, of finite R -algebras, that is, R -algebras that are finitely generated as R -modules. We shall prove structure theorems when R is a discrete valuation ring or a finite field. Establishing back the connection with modular forms, we will for example see that the maximal ideals of Hecke algebras correspond to Galois conjugacy classes of normalised eigenforms, and, for instance, the notion of a congruence can be expressed as a maximal prime containing two minimal ones.

2.1 Theory: Hecke algebras and modular forms over rings

We start by recalling and slightly extending the concept of Hecke algebras of modular forms. It is of utmost importance for our treatment of modular forms over general rings and their computation. In fact, as pointed out a couple of times, we will compute Hecke algebras and not modular forms. We shall assume that $k \geq 1$ and $N \geq 1$.

As in the introduction, we define the *Hecke algebra* of $M_k(\Gamma_1(N); \mathbb{C})$ as the subring (i.e. the \mathbb{Z} -algebra) inside the endomorphism ring of the \mathbb{C} -vector space $M_k(\Gamma_1(N); \mathbb{C})$ generated by all Hecke operators. Remember that due to Formula 1.7 all diamond operators are contained in the Hecke algebra. Of course, we make similar definitions for $S_k(\Gamma_1(N); \mathbb{C})$ and use the notations $\mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C}))$ and $\mathbb{T}_{\mathbb{Z}}(S_k(\Gamma_1(N); \mathbb{C}))$.

If we are working with modular forms with a character, we essentially have two possibilities for defining the Hecke algebra, namely, firstly as above as the \mathbb{Z} -algebra generated by all Hecke operators inside the endomorphism ring of the \mathbb{C} -vector space $M_k(N, \chi; \mathbb{C})$ (notation $\mathbb{T}_{\mathbb{Z}}(M_k(N, \chi; \mathbb{C}))$) or, secondly, as the $\mathbb{Z}[\chi]$ -algebra generated by the Hecke operators inside $\text{End}_{\mathbb{C}}(M_k(N, \chi; \mathbb{C}))$ (notation $\mathbb{T}_{\mathbb{Z}[\chi]}(M_k(N, \chi; \mathbb{C}))$); similarly for the cusp forms. Here $\mathbb{Z}[\chi]$ is the ring extension of \mathbb{Z} generated by all values of χ , it is the integer ring of $\mathbb{Q}(\chi)$. For two reasons we prefer the second variant. The first reason is that we needed to work over $\mathbb{Z}[\chi]$ (or its extensions) for modular symbols. The second reason is that on the natural \mathbb{Z} -structure inside $M_k(\Gamma_1(N); \mathbb{C})$ the decomposition into $(\mathbb{Z}/N\mathbb{Z})^\times$ -eigenspaces can only be made after a base change to $\mathbb{Z}[\chi]$. So, the \mathbb{C} -dimension of $M_k(N, \chi; \mathbb{C})$ equals the $\mathbb{Q}[\chi]$ -dimension of $\mathbb{T}_{\mathbb{Q}[\chi]}(M_k(N, \chi; \mathbb{C}))$ and not the \mathbb{Q} -dimension of $\mathbb{T}_{\mathbb{Q}}(M_k(N, \chi; \mathbb{C}))$.

Lemma 2.1. (a) *The \mathbb{Z} -algebras $\mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C}))$ and $\mathbb{T}_{\mathbb{Z}}(M_k(N, \chi; \mathbb{C}))$ are free \mathbb{Z} -modules of finite rank; the same holds for the cuspidal Hecke algebras.*

(b) *The $\mathbb{Z}[\chi]$ -algebra $\mathbb{T}_{\mathbb{Z}[\chi]}(M_k(N, \chi; \mathbb{C}))$ is a torsion-free finitely generated $\mathbb{Z}[\chi]$ -module; the same holds for the cuspidal Hecke algebra.*

Proof. (a) Due to the corollaries of the Eichler-Shimura theorem (Corollary 1.11) we know that these algebras are finitely generated as \mathbb{Z} -modules. As they lie inside a vector space, they are free (using the structure theory of finitely generated modules over principal ideal domains).

(b) This is like (a), except that $\mathbb{Z}[\chi]$ need not be a principal ideal domain, so that we can only conclude torsion-freeness, but not freeness. \square

Modular forms over rings

Let $k \geq 1$ and $N \geq 1$. Let R be any \mathbb{Z} -algebra (ring). We now use the q -pairing to define modular (cusp) forms over R . We let

$$\begin{aligned} M_k(\Gamma_1(N); R) &:= \text{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C})), R) \\ &\cong \text{Hom}_R(\mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C})) \otimes_{\mathbb{Z}} R, R). \end{aligned}$$

We stress the fact that Hom_R denotes the homomorphisms as R -modules (and not as R -algebras; those will appear later). The isomorphism is proved precisely as in Proposition 1.8 (c), where we did not use

the flatness assumption. Every element f of $M_k(\Gamma_1(N); R)$ thus corresponds to a \mathbb{Z} -linear function $\Phi : \mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C})) \rightarrow R$ and is uniquely identified by its *formal q -expansion*

$$f = \sum_n \Phi(T_n)q^n = \sum_n a_n(f)q^n \in R[[q]].$$

We note that $\mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C}))$ acts naturally on $\text{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C})), R)$, namely by

$$(T \cdot \Phi)(S) = \Phi(TS) = \Phi(ST). \quad (2.10)$$

This means that the action of $\mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C}))$ on $M_k(\Gamma_1(N); R)$ gives the same formulae as usual on formal q -expansions. For cusp forms we make the obvious analogous definition, i.e.

$$\begin{aligned} S_k(\Gamma_1(N); R) &:= \text{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(S_k(\Gamma_1(N); \mathbb{C})), R) \\ &\cong \text{Hom}_R(\mathbb{T}_{\mathbb{Z}}(S_k(\Gamma_1(N); \mathbb{C})) \otimes_{\mathbb{Z}} R, R). \end{aligned}$$

We caution the reader that for modular forms which are not cusp forms there also ought to be some 0th coefficient in the formal q -expansion, for example, for recovering the classical holomorphic q -expansion. Of course, for cusp forms we do not need to worry.

Now we turn our attention to modular forms with a character. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^{\times} \rightarrow \mathbb{C}^{\times}$ be a Dirichlet character and $\mathbb{Z}[\chi] \rightarrow R$ a ring homomorphism. We now proceed analogously to the treatment of modular symbols for a Dirichlet character. We work with $\mathbb{Z}[\chi]$ as the base ring (and not \mathbb{Z}). We let

$$\begin{aligned} M_k(N, \chi; R) &:= \text{Hom}_{\mathbb{Z}[\chi]}(\mathbb{T}_{\mathbb{Z}[\chi]}(M_k(N, \chi; \mathbb{C})), R) \\ &\cong \text{Hom}_R(\mathbb{T}_{\mathbb{Z}[\chi]}(M_k(N, \chi; \mathbb{C})) \otimes_{\mathbb{Z}[\chi]} R, R) \end{aligned}$$

and similarly for the cusp forms.

We remark that these definitions of $M_k(\Gamma_1(N); \mathbb{C})$, $M_k(N, \chi; \mathbb{C})$ etc. agree with those from section 1; thus, it is justified to use the same pieces of notation. As a special case, we get that $M_k(\Gamma_1(N); \mathbb{Z})$ precisely consists of those holomorphic modular forms in $M_k(\Gamma_1(N); \mathbb{C})$ whose q -expansions take values in \mathbb{Z} .

If $\mathbb{Z}[\chi] \xrightarrow{\pi} R = \mathbb{F}$ with \mathbb{F} a finite field of characteristic p or $\overline{\mathbb{F}}_p$, we call $M_k(N, \chi; \mathbb{F})$ the space of *mod p modular forms of weight k , level N and character χ* . Of course, for the cuspidal space similar statements are made and we use similar notation.

We furthermore extend the notation for Hecke algebras introduced in section 1 as follows. If S is an R -algebra and M is an S -module admitting the action of Hecke operators T_n for $n \in \mathbb{N}$, then we let $\mathbb{T}_R(M)$ be the R -subalgebra of $\text{End}_S(M)$ generated by all T_n for $n \in \mathbb{N}$.

We now study base change properties of modular forms over R .

Proposition 2.2. (a) *Let $\mathbb{Z} \rightarrow R \rightarrow S$ be ring homomorphisms. Then the following statements hold.*

(i) *The natural map*

$$M_k(\Gamma_1(N); R) \otimes_R S \rightarrow M_k(\Gamma_1(N); S)$$

is an isomorphism.

(ii) *The evaluation pairing*

$$M_k(\Gamma_1(N); R) \times \mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C})) \otimes_{\mathbb{Z}} R \rightarrow R$$

is the q -pairing and it is perfect.

(iii) *The Hecke algebra $\mathbb{T}_R(M_k(\Gamma_1(N); R))$ is naturally isomorphic to $\mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C})) \otimes_{\mathbb{Z}} R$.*

(b) If $\mathbb{Z}[\chi] \rightarrow R \rightarrow S$ are flat, then Statement (i) holds for $M_k(N, \chi; R)$.

(c) If $\mathbb{T}_{\mathbb{Z}[\chi]}(M_k(N, \chi; \mathbb{C}))$ is a free $\mathbb{Z}[\chi]$ -module and $\mathbb{Z}[\chi] \rightarrow R \rightarrow S$ are ring homomorphisms, statements (i)-(iii) hold for $M_k(N, \chi; R)$.

Proof. (a) We use the following general statement, in which M is assumed to be a free finitely generated R -module and N, T are R -modules:

$$\mathrm{Hom}_R(M, N) \otimes_R T \cong \mathrm{Hom}_R(M, N \otimes_R T).$$

To see this, just see M as $\bigoplus R$ and pull the direct sum out of the Hom, do the tensor product, and put the direct sum back into the Hom.

(i) Write $\mathbb{T}_{\mathbb{Z}}$ for $\mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C}))$. It is a free \mathbb{Z} -module by Lemma 2.1. We have

$$M_k(\Gamma_1(N); R) \otimes_R S = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, R) \otimes_R S,$$

which by the above is isomorphic to $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, R \otimes_R S)$ and hence to $M_k(\Gamma_1(N); S)$.

(ii) The evaluation pairing $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathbb{Z}) \times \mathbb{T}_{\mathbb{Z}} \rightarrow \mathbb{Z}$ is perfect, since $\mathbb{T}_{\mathbb{Z}}$ is free as a \mathbb{Z} -module. The result follows from (i) by tensoring with R .

(iii) We consider the natural map

$$\mathbb{T}_{\mathbb{Z}} \otimes_{\mathbb{Z}} R \rightarrow \mathrm{End}_R(\mathrm{Hom}_R(\mathbb{T}_{\mathbb{Z}} \otimes_{\mathbb{Z}} R, R))$$

and show that it is injective. Its image is by definition $\mathbb{T}_R(M_k(\Gamma_1(N); R))$. Let T be in the kernel. Then $\phi(T) = 0$ for all $\phi \in \mathrm{Hom}_R(\mathbb{T}_{\mathbb{Z}} \otimes_{\mathbb{Z}} R, R)$. As the pairing in (ii) is perfect and, in particular, non-degenerate, $T = 0$ follows.

(b) Due to flatness we have

$$\mathrm{Hom}_R(\mathbb{T}_{\mathbb{Z}[\chi]} \otimes_{\mathbb{Z}[\chi]} R, R) \otimes_R S \cong \mathrm{Hom}_S(\mathbb{T}_{\mathbb{Z}[\chi]} \otimes_{\mathbb{Z}[\chi]} S, S),$$

as desired.

(c) The same arguments as in (a) work. □

Galois conjugacy classes

By the definition of the Hecke action in equation (2.10), the normalised Hecke eigenforms in the R -module $M_k(\Gamma_1(N); R)$ are precisely the \mathbb{Z} -algebra homomorphisms in $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C})), R)$, where the normalisation means that the identity operator T_1 is sent to 1. Such an algebra homomorphism Φ is often referred to as a *system of eigenvalues*, since the image of each T_n corresponds to an eigenvalue of T_n , namely to $\Phi(T_n) = a_n(f)$ (if f corresponds to Φ).

Let us now consider a perfect field K (if we are working with a Dirichlet character, we also want that K admits a ring homomorphism $\mathbb{Z}[\chi] \rightarrow K$). Denote by \overline{K} an algebraic closure, so that we have

$$\begin{aligned} M_k(\Gamma_1(N); \overline{K}) &= \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C})), \overline{K}) \\ &\cong \mathrm{Hom}_K(\mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C})) \otimes_{\mathbb{Z}} K, \overline{K}). \end{aligned}$$

We can compose any $\Phi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C})), \overline{K})$ by any field automorphism $\sigma : \overline{K} \rightarrow \overline{K}$ fixing K . Thus, we obtain an action of the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ on $M_k(\Gamma_1(N); \overline{K})$ (on formal q -expansions, we only need to apply σ to the coefficients). All this works similarly for the cuspidal subspace, too.

Like this, we also obtain a $\mathrm{Gal}(\overline{K}/K)$ -action on the normalised eigenforms, and can hence speak about *Galois conjugacy classes of eigenforms*.

Proposition 2.3. *We have the following bijective correspondences:*

$$\begin{aligned} \text{Spec}(\mathbb{T}_K(\cdot)) &\stackrel{1\leftrightarrow 1}{\longleftrightarrow} \text{Hom}_{K\text{-alg}}(\mathbb{T}_K(\cdot), \overline{K}) / \text{Gal}(\overline{K}/K) \\ &\stackrel{1\leftrightarrow 1}{\longleftrightarrow} \{ \text{normalised eigenf. in } \cdot \} / \text{Gal}(\overline{K}/K) \end{aligned}$$

and with $K = \overline{K}$

$$\text{Spec}(\mathbb{T}_{\overline{K}}(\cdot)) \stackrel{1\leftrightarrow 1}{\longleftrightarrow} \text{Hom}_{\overline{K}\text{-alg}}(\mathbb{T}_{\overline{K}}(\cdot), \overline{K}) \stackrel{1\leftrightarrow 1}{\longleftrightarrow} \{ \text{normalised eigenforms in } \cdot \}.$$

Here, \cdot stands for either $M_k(\Gamma_1(N); \overline{K})$, $S_k(\Gamma_1(N); \overline{K})$ or the respective spaces with a Dirichlet character.

We recall that Spec of a ring is the set of prime ideals. In the next section we will see that in $\mathbb{T}_K(\cdot)$ and $\mathbb{T}_{\overline{K}}(\cdot)$ all prime ideals are already maximal (it is an easy consequence of the finite dimensionality).

Proof. Exercise 2.19. □

We repeat that the coefficients of any eigenform f in $M_k(N, \chi; \overline{K})$ lie in a finite extension of K , namely in $\mathbb{T}_K(M_k(N, \chi; K))/\mathfrak{m}$, when \mathfrak{m} is the maximal ideal corresponding to the conjugacy class of f .

Let us note that the above discussion applies to $\overline{K} = \mathbb{C}$, $\overline{K} = \overline{\mathbb{Q}}$, $\overline{K} = \overline{\mathbb{Q}}_p$, as well as to $\overline{K} = \overline{\mathbb{F}}_p$. In the next sections we will also take into account the finer structure of Hecke algebras over \mathcal{O} , or rather over the completion of \mathcal{O} at one prime.

2.1.1 Some commutative algebra

In this section we leave the special context of modular forms for a moment and provide quite useful results from commutative algebra that will be applied to Hecke algebras in the sequel.

We start with a simple case which we will prove directly. Let \mathbb{T} be an *Artinian* algebra, i.e. an algebra in which every descending chain of ideals becomes stationary. Our main example will be finite dimensional algebras over a field. That those are Artinian is obvious, since in every proper inclusion of ideals the dimension diminishes.

For any ideal \mathfrak{a} of \mathbb{T} the sequence \mathfrak{a}^n becomes stationary, i.e. $\mathfrak{a}^n = \mathfrak{a}^{n+1}$ for all n “big enough”. Then we will use the notation \mathfrak{a}^∞ for \mathfrak{a}^n .

Proposition 2.4. *Let \mathbb{T} be an Artinian ring.*

- (a) *Every prime ideal of \mathbb{T} is maximal.*
- (b) *There are only finitely many maximal ideals in \mathbb{T} .*
- (c) *Let \mathfrak{m} be a maximal ideal of \mathbb{T} . It is the only maximal ideal containing \mathfrak{m}^∞ .*
- (d) *Let $\mathfrak{m} \neq \mathfrak{n}$ be two maximal ideals. For any $k \in \mathbb{N}$ and $k = \infty$ the ideals \mathfrak{m}^k and \mathfrak{n}^k are coprime.*
- (e) *The Jacobson radical $\bigcap_{\mathfrak{m} \in \text{Spec}(\mathbb{T})} \mathfrak{m}$ is equal to the nilradical and consists of the nilpotent elements.*
- (f) *We have $\bigcap_{\mathfrak{m} \in \text{Spec}(\mathbb{T})} \mathfrak{m}^\infty = (0)$.*
- (g) *(Chinese Remainder Theorem) The natural map*

$$\mathbb{T} \xrightarrow{a \mapsto (\dots, a + \mathfrak{m}^\infty, \dots)} \prod_{\mathfrak{m} \in \text{Spec}(\mathbb{T})} \mathbb{T}/\mathfrak{m}^\infty$$

is an isomorphism.

- (h) *For every maximal ideal \mathfrak{m} , the ring $\mathbb{T}/\mathfrak{m}^\infty$ is local with maximal ideal \mathfrak{m} and is hence isomorphic to $\mathbb{T}_{\mathfrak{m}}$, the localisation of \mathbb{T} at \mathfrak{m} .*

Proof. (a) Let \mathfrak{p} be a prime ideal of \mathbb{T} . The quotient $\mathbb{T} \rightarrow \mathbb{T}/\mathfrak{p}$ is an Artinian integral domain, since ideal chains in \mathbb{T}/\mathfrak{p} lift to ideal chains in \mathbb{T} . Let $0 \neq x \in \mathbb{T}/\mathfrak{p}$. We have $(x)^n = (x)^{n+1} = (x)^\infty$ for some n big enough. Hence, $x^n = yx^{n+1}$ with some $y \in \mathbb{T}/\mathfrak{p}$ and so $xy = 1$, as \mathbb{T}/\mathfrak{p} is an integral domain.

(b) Assume there are infinitely many maximal ideals, number a countable subset of them by $\mathfrak{m}_1, \mathfrak{m}_2, \dots$. Form the descending ideal chain

$$\mathfrak{m}_1 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \supset \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \mathfrak{m}_3 \supset \dots$$

This chain becomes stationary, so that for some n we have

$$\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n = \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n \cap \mathfrak{m}_{n+1}.$$

Consequently, $\mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n \subset \mathfrak{m}_{n+1}$. We claim that there is $i \in \{1, 2, \dots, n\}$ with $\mathfrak{m}_i \subset \mathfrak{m}_{n+1}$. Due to the maximality of \mathfrak{m}_i we obtain the desired contradiction. To prove the claim we assume that $\mathfrak{m}_i \not\subset \mathfrak{m}_{n+1}$ for all i . Let $x_i \in \mathfrak{m}_i - \mathfrak{m}_{n+1}$ and $y = x_1 \cdot x_2 \cdots x_n$. Then $y \in \mathfrak{m}_1 \cap \dots \cap \mathfrak{m}_n$, but $y \notin \mathfrak{m}_{n+1}$ due to the primality of \mathfrak{m}_{n+1} , giving a contradiction.

(c) Let $\mathfrak{m} \in \text{Spec}(\mathbb{T})$ be a maximal ideal. Assume that \mathfrak{n} is a different maximal ideal with $\mathfrak{m}^\infty \subset \mathfrak{n}$. Choose $x \in \mathfrak{m}$. Some power $x^r \in \mathfrak{m}^\infty$ and, thus, $x^r \in \mathfrak{n}$. As \mathfrak{n} is prime, $x \in \mathfrak{n}$ follows, implying $\mathfrak{m} \subseteq \mathfrak{n}$, contradicting the maximality of \mathfrak{m} .

(d) Assume that $I := \mathfrak{m}^k + \mathfrak{n}^k \neq \mathbb{T}$. Then I is contained in some maximal ideal \mathfrak{p} . Hence, \mathfrak{m}^∞ and \mathfrak{n}^∞ are contained in \mathfrak{p} , whence by (c), $\mathfrak{m} = \mathfrak{n} = \mathfrak{p}$; contradiction.

(e) It is a standard fact from Commutative Algebra that the nilradical (the ideal of nilpotent elements) is the intersection of the minimal prime ideals.

(f) For $k \in \mathbb{N}$ and $k = \infty$, (d) implies

$$\bigcap_{\mathfrak{m} \in \text{Spec}(\mathbb{T})} \mathfrak{m}^k = \prod_{\mathfrak{m} \in \text{Spec}(\mathbb{T})} \mathfrak{m}^k = \left(\prod_{\mathfrak{m} \in \text{Spec}(\mathbb{T})} \mathfrak{m} \right)^k = \left(\bigcap_{\mathfrak{m} \in \text{Spec}(\mathbb{T})} \mathfrak{m} \right)^k.$$

By (e) we know that $\bigcap_{\mathfrak{m} \in \text{Spec}(\mathbb{T})} \mathfrak{m}$ is the nilradical. It can be generated by finitely many elements a_1, \dots, a_n all of which are nilpotent. So a high enough power of $\bigcap_{\mathfrak{m} \in \text{Spec}(\mathbb{T})} \mathfrak{m}$ is zero.

(g) The injectivity follows from (f). It suffices to show that the elements $(0, \dots, 0, 1, 0, \dots, 0)$ are in the image of the map. Suppose the 1 is at the place belonging to \mathfrak{m} . Due to coprimeness (d) for any maximal ideal $\mathfrak{n} \neq \mathfrak{m}$ we can find $a_n \in \mathfrak{n}^\infty$ and $a_m \in \mathfrak{m}^\infty$ such that $1 = a_m + a_n$. Let $x := \prod_{\mathfrak{n} \in \text{Spec}(\mathbb{T}), \mathfrak{n} \neq \mathfrak{m}} a_n$. We have $x \in \prod_{\mathfrak{n} \in \text{Spec}(\mathbb{T}), \mathfrak{n} \neq \mathfrak{m}} \mathfrak{n}^\infty$ and $x = \prod_{\mathfrak{n} \in \text{Spec}(\mathbb{T}), \mathfrak{n} \neq \mathfrak{m}} (1 - a_m) \equiv 1 \pmod{\mathfrak{m}}$. Hence, the map sends x to $(0, \dots, 0, 1, 0, \dots, 0)$, proving the surjectivity.

(h) By (c), the only maximal ideal of \mathbb{T} containing \mathfrak{m}^∞ is \mathfrak{m} . Consequently, $\mathbb{T}/\mathfrak{m}^\infty$ is a local ring with maximal ideal the image of \mathfrak{m} . Let $s \in \mathbb{T} - \mathfrak{m}$. As $s + \mathfrak{m}^\infty \notin \mathfrak{m}/\mathfrak{m}^\infty$, the element $s + \mathfrak{m}^\infty$ is a unit in $\mathbb{T}/\mathfrak{m}^\infty$. Thus, the map

$$\mathbb{T}_\mathfrak{m} \xrightarrow{\frac{y}{s} \mapsto ys^{-1} + \mathfrak{m}^\infty} \mathbb{T}/\mathfrak{m}^\infty$$

is well-defined. It is clearly surjective. Suppose $\frac{y}{s}$ maps to 0. Since the image of s is a unit, $y \in \mathfrak{m}^\infty$ follows. The element x constructed in (g) is in $\prod_{\mathfrak{n} \in \text{Spec}(\mathbb{T}), \mathfrak{n} \neq \mathfrak{m}} \mathfrak{n}^\infty$, but not in \mathfrak{m} . By (f) and (d), $(0) = \prod_{\mathfrak{m} \in \text{Spec}(\mathbb{T})} \mathfrak{m}^\infty$. Thus, $y \cdot x = 0$ and also $\frac{y}{s} = \frac{yx}{sx} = 0$, proving the injectivity. \square

A useful and simple way to rephrase a product decomposition as in (g) is to use idempotents. In concrete terms, the idempotents of \mathbb{T} (as in the proposition) are precisely the elements of the form (\dots, x_m, \dots) with $x_m \in \{0, 1\} \subseteq \mathbb{T}/\mathfrak{m}^\infty$.

Definition 2.5. Let \mathbb{T} be a ring. An idempotent of \mathbb{T} is an element e that satisfies $e^2 = e$. Two idempotents e, f are orthogonal if $ef = 0$. An idempotent e is primitive if $e\mathbb{T}$ is a local ring. A set of idempotents $\{e_1, \dots, e_n\}$ is said to be complete if $1 = \sum_{i=1}^n e_i$.

In concrete terms for $\mathbb{T} = \prod_{\mathfrak{m} \in \text{Spec}(\mathbb{T})} \mathbb{T}/\mathfrak{m}^\infty$, a complete set of primitive pairwise orthogonal idempotents is given by

$$(1, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, \dots, 0, 1, 0), (0, \dots, 0, 1).$$

In Exercise 2.20, you are asked (among other things) to prove that in the above case \mathfrak{m}^∞ is a principal ideal generated by an idempotent.

Below we will present an algorithm for computing a complete set of primitive pairwise orthogonal idempotents for an Artinian ring.

We now come to a more general setting, namely working with a finite algebra \mathbb{T} over a complete local ring instead of a field. We will lift the idempotents of the reduction of \mathbb{T} (for the maximal ideal of the complete local ring) to idempotents of \mathbb{T} by Hensel's lemma. This gives us a proposition very similar to Proposition 2.4.

Proposition 2.6 (Hensel's lemma). *Let R be a ring that is complete with respect to the ideal \mathfrak{m} and let $f \in R[X]$ be a polynomial. If*

$$f(a) \equiv 0 \pmod{(f'(a))^2 \mathfrak{m}}$$

for some $a \in R$, then there is $b \in R$ such that

$$f(b) = 0 \text{ and } b \equiv a \pmod{f'(a)\mathfrak{m}}.$$

If $f'(a)$ is not a zero-divisor, then b is unique with these properties.

Proof. [13], Theorem 7.3. □

Recall that the *height* of a prime ideal \mathfrak{p} in a ring R is the supremum among all $n \in \mathbb{N}$ such that there are inclusions of prime ideals $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_{n-1} \subsetneq \mathfrak{p}$. The *Krull dimension* of R is the supremum of the heights of the prime ideals of R .

Proposition 2.7. *Let \mathcal{O} be an integral domain of characteristic zero which is a finitely generated \mathbb{Z} -module. Write $\widehat{\mathcal{O}}$ for the completion of \mathcal{O} at a maximal prime of \mathcal{O} and denote by \mathbb{F} the residue field and by \widehat{K} the fraction field of $\widehat{\mathcal{O}}$. Let furthermore \mathbb{T} be a commutative \mathcal{O} -algebra which is finitely generated as an \mathcal{O} -module. For any ring homomorphism $\mathcal{O} \rightarrow S$ write \mathbb{T}_S for $\mathbb{T} \otimes_{\mathcal{O}} S$. Then the following statements hold.*

- (a) *The Krull dimension of $\mathbb{T}_{\widehat{\mathcal{O}}}$ is less than or equal to 1, i.e. between any prime ideal and any maximal ideal $\mathfrak{p} \subset \mathfrak{m}$ there is no other prime ideal. The maximal ideals of $\mathbb{T}_{\widehat{\mathcal{O}}}$ correspond bijectively under taking pre-images to the maximal ideals of $\mathbb{T}_{\mathbb{F}}$. Primes \mathfrak{p} of height 0 (i.e. those that do not contain any other prime ideal) which are properly contained in a prime of height 1 (i.e. a maximal prime) of $\mathbb{T}_{\widehat{\mathcal{O}}}$ are in bijection with primes of $\mathbb{T}_{\widehat{K}}$ under extension (i.e. $\mathfrak{p}\mathbb{T}_{\widehat{K}}$), for which the notation \mathfrak{p}^e will be used.*

Under the correspondences, one has

$$\mathbb{T}_{\mathbb{F}, \mathfrak{m}} \cong \mathbb{T}_{\widehat{\mathcal{O}}, \mathfrak{m}} \otimes_{\widehat{\mathcal{O}}} \mathbb{F}$$

and

$$\mathbb{T}_{\widehat{\mathcal{O}}, \mathfrak{p}} \cong \mathbb{T}_{\widehat{K}, \mathfrak{p}^e}.$$

- (b) *The algebra $\mathbb{T}_{\widehat{\mathcal{O}}}$ decomposes as*

$$\mathbb{T}_{\widehat{\mathcal{O}}} \cong \prod_{\mathfrak{m}} \mathbb{T}_{\widehat{\mathcal{O}}, \mathfrak{m}},$$

where the product runs over the maximal ideals \mathfrak{m} of $\mathbb{T}_{\widehat{\mathcal{O}}}$.

(c) The algebra $\mathbb{T}_{\mathbb{F}}$ decomposes as

$$\mathbb{T}_{\mathbb{F}} \cong \prod_{\mathfrak{m}} \mathbb{T}_{\mathbb{F}, \mathfrak{m}},$$

where the product runs over the maximal ideals \mathfrak{m} of $\mathbb{T}_{\mathbb{F}}$.

(d) The algebra $\mathbb{T}_{\widehat{K}}$ decomposes as

$$\mathbb{T}_{\widehat{K}} \cong \prod_{\mathfrak{p}} \mathbb{T}_{\widehat{K}, \mathfrak{p}^e} \cong \prod_{\mathfrak{p}} \mathbb{T}_{\widehat{\mathcal{O}}, \mathfrak{p}},$$

where the products run over the minimal prime ideals \mathfrak{p} of $\mathbb{T}_{\widehat{\mathcal{O}}}$ which are contained in a prime ideal of height 1.

Proof. We first need that $\widehat{\mathcal{O}}$ has Krull dimension 1. This, however, follows from the fact that \mathcal{O} has Krull dimension 1, as it is an integral extension of \mathbb{Z} , and the correspondence between the prime ideals of a ring and its completion. As $\mathbb{T}_{\widehat{\mathcal{O}}}$ is a finitely generated $\widehat{\mathcal{O}}$ -module, $\mathbb{T}_{\widehat{\mathcal{O}}}/\mathfrak{p}$ with a prime \mathfrak{p} is an integral domain which is a finitely generated $\widehat{\mathcal{O}}/(\mathfrak{p} \cap \widehat{\mathcal{O}})$ -module. Hence, it is either a finite field (when the prime ideal $\mathfrak{p} \cap \widehat{\mathcal{O}}$ is the unique maximal ideal of $\widehat{\mathcal{O}}$) or a finite extension of $\widehat{\mathcal{O}}$ (when $\mathfrak{p} \cap \widehat{\mathcal{O}} = 0$ so that the structure map $\widehat{\mathcal{O}} \rightarrow \mathbb{T}_{\widehat{\mathcal{O}}}/\mathfrak{p}$ is injective). This proves that the height of \mathfrak{p} is less than or equal to 1. The correspondences and the isomorphisms of Part (a) are the subject of Exercise 2.21.

We have already seen Parts (c) and (d) in Lemma 2.4. Part (b) follows from (c) by applying Hensel's lemma (Proposition 2.6) to the idempotents of the decomposition of (c). We follow [13], Corollary 7.5, for the details. Since $\widehat{\mathcal{O}}$ is complete with respect to some ideal \mathfrak{p} , so is $\mathbb{T}_{\widehat{\mathcal{O}}}$ as it is a finitely generated $\widehat{\mathcal{O}}$ -module. Hence, we may use Hensel's lemma in $\mathbb{T}_{\widehat{\mathcal{O}}}$. Given an idempotent \bar{e} of $\mathbb{T}_{\mathbb{F}}$, we will first show that it lifts to a unique idempotent of $\mathbb{T}_{\widehat{\mathcal{O}}}$. Let e be any lift of \bar{e} and let $f(X) = X^2 - X$ be a polynomial annihilating \bar{e} . We have that $f'(e) = 2e - 1$ is a unit since $(2e - 1)^2 = 4e^2 - 4e + 1 \equiv 1 \pmod{\mathfrak{p}}$. Hensel's lemma now gives us a unique root $e_1 \in \mathbb{T}_{\widehat{\mathcal{O}}}$ of f , i.e. an idempotent, lifting \bar{e} .

We now lift every element of a set of pairwise orthogonal idempotents of $\mathbb{T}_{\mathbb{F}}$. It now suffices to show that the lifted idempotents are also pairwise orthogonal (their sum is 1; otherwise we would get a contradiction in the correspondences in (a): there cannot be more idempotents in $\mathbb{T}_{\widehat{\mathcal{O}}}$ than in $\mathbb{T}_{\mathbb{F}}$). As their reductions are orthogonal, a product $e_i e_j$ of lifted idempotents is in \mathfrak{p} . Hence, $e_i e_j = e_i^d e_j^d \in \mathfrak{p}^d$ for all d , whence $e_i e_j = 0$, as desired. \square

2.1.2 Commutative algebra of Hecke algebras

Let $k \geq 1$, $N \geq 1$ and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$. Moreover, let p be a prime, $\mathcal{O} := \mathbb{Z}[\chi]$, \mathfrak{P} a maximal prime of \mathcal{O} above p , and let \mathbb{F} be the residue field of \mathcal{O} modulo \mathfrak{P} . We let $\widehat{\mathcal{O}}$ denote the completion of \mathcal{O} at \mathfrak{P} . Moreover, the field of fractions of $\widehat{\mathcal{O}}$ will be denoted by \widehat{K} and an algebraic closure by $\overline{\widehat{K}}$. For $\mathbb{T}_{\mathcal{O}}(M_k(N, \chi; \mathbb{C}))$ we only write $\mathbb{T}_{\mathcal{O}}$ for short, and similarly over other rings. We keep using the fact that $\mathbb{T}_{\mathcal{O}}$ is finitely generated as an \mathcal{O} -module. We shall now apply Proposition 2.7 to $\mathbb{T}_{\widehat{\mathcal{O}}}$.

Proposition 2.8. *The Hecke algebras $\mathbb{T}_{\mathcal{O}}$ and $\mathbb{T}_{\widehat{\mathcal{O}}}$ are pure of Krull dimension 1, i.e. every maximal prime contains some minimal prime ideal.*

Proof. It suffices to prove that $\mathbb{T}_{\widehat{\mathcal{O}}}$ is pure of Krull dimension 1 because completion of $\mathbb{T}_{\mathcal{O}}$ at a maximal ideal of \mathcal{O} does not change the Krull dimension. First note that $\widehat{\mathcal{O}}$ is pure of Krull dimension 1 as it is an integral extension of \mathbb{Z}_p (and the Krull dimension is an invariant in integral extensions). With the same reasoning, $\mathbb{T}_{\widehat{\mathcal{O}}}$ is of Krull dimension 1; we have to see that it is pure. According to proposition 2.7, $\mathbb{T}_{\widehat{\mathcal{O}}}$ is the direct product of finite local $\widehat{\mathcal{O}}$ -algebras \mathbb{T}_i . As each \mathbb{T}_i embeds into a finite dimensional matrix algebra over \widehat{K} , it admits a simultaneous eigenvector (after possibly a finite extension of \widehat{K}) for the standard action of the matrix algebra on the corresponding \widehat{K} -vector space and the map φ sending an element of \mathbb{T}_i to its eigenvalue is non-trivial and its kernel is a prime ideal strictly contained in the maximal ideal of \mathbb{T}_i . To see this, notice that the eigenvalues are integral, i.e. lie in the valuation ring of

a finite extension of \widehat{K} , and can hence be reduced modulo the maximal ideal. The kernel of φ followed by the reduction map is the required maximal ideal. This proves that the height of the maximal ideal is 1. \square

By Proposition 2.7, minimal primes of $\mathbb{T}_{\mathcal{O}}$ correspond to the maximal primes of $\mathbb{T}_{\widehat{K}}$ and hence to $\text{Gal}(\widehat{K}/\widehat{K})$ -conjugacy classes of eigenforms in $M_k(N, \chi; \widehat{K})$. By a brute force identification of $\widehat{K} = \overline{\mathbb{Q}}_p$ with \mathbb{C} we may still think about these eigenforms as the usual holomorphic ones (the Galois conjugacy can then still be seen as conjugacy by a decomposition group above p inside the absolute Galois group of the field of fractions of \mathcal{O}).

Again by Proposition 2.7, maximal prime ideals of $\mathbb{T}_{\mathcal{O}}$ correspond to the maximal prime ideals of $\mathbb{T}_{\mathbb{F}}$ and hence to $\text{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ -conjugacy classes of eigenforms in $M_k(N, \chi; \overline{\mathbb{F}})$.

The spectrum of $\mathbb{T}_{\mathcal{O}}$ allows one to phrase very elegantly when conjugacy classes of eigenforms are congruent modulo a prime above p . Let us first explain what that means. Normalised eigenforms f take their coefficients $a_n(f)$ in rings of integers of number fields ($\mathbb{T}_{\mathcal{O}}/\mathfrak{m}$, when \mathfrak{m} is the kernel of the \mathcal{O} -algebra homomorphism $\mathbb{T}_{\mathcal{O}} \rightarrow \mathbb{C}$, given by $T_n \mapsto a_n(f)$), so they can be reduced modulo primes above p (for which we will often just say ‘‘reduced modulo p ’’). The reduction modulo a prime above p of the q -expansion of a modular form f in $M_k(N, \chi; \mathbb{C})$ is the formal q -expansion of an eigenform in $M_k(N, \chi; \overline{\mathbb{F}})$.

If two normalised eigenforms f, g in $M_k(N, \chi; \mathbb{C})$ or $M_k(N, \chi; \widehat{K})$ reduce to the same element in $M_k(N, \chi; \overline{\mathbb{F}})$, we say that they are *congruent modulo p* .

Due to Exercise 2.22, we may speak about *reductions modulo p* of $\text{Gal}(\widehat{K}/\widehat{K})$ -conjugacy classes of normalised eigenforms to $\text{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ -conjugacy classes. We hence say that two $\text{Gal}(\widehat{K}/\widehat{K})$ -conjugacy classes, say corresponding to normalised eigenforms f, g , respectively, minimal ideals \mathfrak{p}_1 and \mathfrak{p}_2 of $\mathbb{T}_{\mathcal{O}}$, are *congruent modulo p* , if they reduce to the same $\text{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ -conjugacy class.

Proposition 2.9. *The $\text{Gal}(\widehat{K}/\widehat{K})$ -conjugacy classes belonging to minimal primes \mathfrak{p}_1 and \mathfrak{p}_2 of $\mathbb{T}_{\mathcal{O}}$ are congruent modulo p if and only if they are contained in a common maximal prime \mathfrak{m} of $\mathbb{T}_{\mathcal{O}}$.*

Proof. Exercise 2.23. \square

We mention the fact that if f is a newform belonging to the maximal ideal \mathfrak{m} of the Hecke algebra $\mathbb{T} := \mathbb{T}_{\mathbb{Q}}(S_k(\Gamma_1(N), \mathbb{C}))$, then $\mathbb{T}_{\mathfrak{m}}$ is isomorphic to $\mathbb{Q}_f = \mathbb{Q}(a_n | n \in \mathbb{N})$. This follows from newform (Atkin-Lehner) theory (see [10, §5.6-5.8]), which implies that the Hecke algebra on the newspace is diagonalisable, so that it is the direct product of the coefficient fields.

We include here the famous Deligne-Serre lifting lemma [8, Lemme 6.11], which we can easily prove with the tools developed so far.

Proposition 2.10 (Deligne-Serre lifting lemma). *Any normalised eigenform $\bar{f} \in S_k(\Gamma_1(N); \overline{\mathbb{F}}_p)$ is the reduction of a normalised eigenform $f \in S_k(\Gamma_1(N); \mathbb{C})$.*

Proof. Let $\mathbb{T}_{\mathbb{Z}} = \mathbb{T}_{\mathbb{Z}}(S_k(\Gamma_1(N); \mathbb{C}))$. By definition, \bar{f} is a ring homomorphism $\mathbb{T}_{\mathbb{Z}} \rightarrow \overline{\mathbb{F}}_p$ and its kernel is a maximal ideal \mathfrak{m} of $\mathbb{T}_{\mathbb{Z}}$. According to Proposition 2.8, the Hecke algebra is pure of Krull dimension one, hence \mathfrak{m} is of height 1, meaning that it strictly contains a minimal prime ideal $\mathfrak{p} \subset \mathbb{T}_{\mathbb{Z}}$. Let f be the composition of the maps in the first line of the diagram:

$$\begin{array}{ccccccc}
 \mathbb{T}_{\mathbb{Z}} & \longrightarrow & \mathbb{T}_{\mathbb{Z}}/\mathfrak{p} & \hookrightarrow & \overline{\mathbb{Z}}^{\mathbb{C}} & \longrightarrow & \mathbb{C} \\
 & \searrow & \downarrow & & \downarrow & & \\
 & & \mathbb{T}_{\mathbb{Z}}/\mathfrak{m} & \hookrightarrow & \overline{\mathbb{F}}_p & & \\
 & & & & \uparrow \bar{f} & &
 \end{array}$$

where all surjections and all injections are the natural ones, and the map $\overline{\mathbb{Z}} \rightarrow \overline{\mathbb{F}}_p$ is chosen in order to make the diagram commutative. Note that \bar{f} is a ring homomorphism and thus a normalised eigenform in $S_k(\Gamma_1(N); \mathbb{C})$. By the diagram, its reduction is \bar{f} . \square

2.2 Algorithms and Implementations: Localisation Algorithms

Let K be a perfect field, \overline{K} an algebraic closure and A a finite dimensional commutative K -algebra. In the context of Hecke algebras we would like to compute a local decomposition of A as in Proposition 2.7.

2.2.1 Primary spaces

Definition 2.11. *An A -module V which is finite dimensional as K -vector space is called a primary space for A if the minimal polynomial for all $a \in A$ is a prime power in $K[X]$.*

Lemma 2.12. (a) *A is local if and only if the minimal polynomial of a (in $K[X]$) is a prime power for all $a \in A$.*

(b) *Let V be an A -module which is finite dimensional as K -vector space and which is a primary space for A . Then the image of A in $\text{End}_K(V)$ is a local algebra.*

(c) *Let V be an A -module which is finite dimensional as K -vector space and let a_1, \dots, a_n be generators of the algebra A . Suppose that for $i \in \{1, \dots, n\}$ the minimal polynomial a_i on V is a power of $(X - \lambda_i)$ in $K[X]$ for some $\lambda_i \in K$ (e.g. if $K = \overline{K}$). Then the image of A in $\text{End}_K(V)$ is a local algebra.*

Proof. (a) Suppose first that A is local and take $a \in A$. Let $\phi_a : K[X] \rightarrow A$ be the homomorphism of K -algebras defined by sending X to a . Let (f) be the kernel with f monic, so that by definition f is the minimal polynomial of a . Hence, $K[X]/(f) \hookrightarrow A$, whence $K[X]/(f)$ is local, as it does not contain any non-trivial idempotent. Thus, f cannot have two different prime factors.

Conversely, if A were not local, we would have an idempotent $e \notin \{0, 1\}$. The minimal polynomial of e is $X(X - 1)$, which is not a prime power.

(b) follows directly. For (c) one can use the following. Suppose that $(a - \lambda)^r V = 0$ and $(b - \mu)^s V = 0$. Then $((a + b) - (\lambda + \mu))^{r+s} V = 0$, as one sees by rewriting $((a + b) - (\lambda + \mu)) = (a - \lambda) + (b - \mu)$ and expanding out. From this it also follows that $(ab - \lambda\mu)^{2(r+s)} V = 0$ by rewriting $ab - \lambda\mu = (a - \lambda)(b - \mu) + \lambda(b - \mu) + \mu(a - \lambda)$. \square

We warn the reader that algebras such that a set of generators acts primarily need not be local, unless they are defined over an algebraically closed field, as we have seen in Part (c) above. In Exercise 2.24 you are asked to find an example.

The next proposition, however, tells us that an algebra over a field having a basis consisting of primary elements is local. I found the idea for that proof in [11].

Proposition 2.13. *Let K be a field of characteristic 0 or a finite field. Let A be a finite dimensional commutative algebra over K and let a_1, \dots, a_n be a K -basis of A with the property that the minimal polynomial of each a_i is a power of a prime polynomial $p_i \in K[X]$.*

Then A is local.

Proof. We assume that A is not local and take a decomposition $\alpha : A \xrightarrow{\sim} \prod_{j=1}^r A_j$ with $r \geq 2$. Let K_j be the residue field of A_j and consider the finite dimensional K -algebra $\overline{A} := \prod_{j=1}^r K_j$. Write $\overline{a}_1, \dots, \overline{a}_n$ for the images of the a_i in \overline{A} . They form a K -basis. In order to have access to the components, also write $\overline{a}_i = (\overline{a}_{i,1}, \dots, \overline{a}_{i,r})$. Since the minimal polynomial of an element in a product is the lowest common multiple of the minimal polynomials of the components, the assumption implies that, for each $i = 1, \dots, r$, the minimal polynomial of $a_{i,j}$ is independent of j ; call it $p_i \in K[X]$. Let N/K be the splitting field of the polynomials p_1, \dots, p_r . This means that N is the normal closure of K_j over K for any j . As a particular case, note that $N = K_j$ for all j if K is a finite field since finite extensions of finite fields are automatically normal. Now consider the trace $\text{Tr}_{N/K}$ and note that $\text{Tr}_{N/K}(\overline{a}_i)$ is a diagonal element in \overline{A} for all $i = 1, \dots, r$ since the components $\overline{a}_{i,j}$ are roots of the same minimal

polynomial. Consequently, $\text{Tr}_{N/K}(\bar{a})$ is a diagonal element for all $\bar{a} \in \bar{A}$ since the \bar{a}_i form a K -basis of \bar{A} .

In order to come to a contradiction, it now suffices to produce an element the trace of which is not diagonal. By Exercise 2.25 there is $x \in K_1$ such that $\text{Tr}_{N/K}(x) \neq 0$. Then the element $(x, 0, \dots, 0) \in \bar{A}$ clearly provides an example of an element with non-diagonal trace. \square

Lemma 2.14. *Let A be a local finite dimensional commutative algebra over a perfect field K . Let a_1, \dots, a_n be a set of K -algebra generators of A such that the minimal polynomial of each a_i is a prime polynomial. Then A is a field.*

Proof. As the a_i are simultaneously diagonalisable over a separable closure (considering the algebra as a matrix algebra) due to their minimal polynomials being squarefree (using here the perfectness of K), so are sums and products of the a_i . Hence, 0 is the only nilpotent element in A . As the maximal ideal in an Artinian local algebra is the set of nilpotent elements, the lemma follows. \square

Proposition 2.15. *Let A be a local finite dimensional commutative algebra over a perfect field K . Let a_1, \dots, a_n be a set of K -algebra generators of A . Let $p_i^{e_i}$ be the minimal polynomial of a_i (see Lemma 2.12).*

Then the maximal ideal \mathfrak{m} of A is generated by $\{p_1(a_1), \dots, p_n(a_n)\}$.

Proof. Let \mathfrak{a} be the ideal generated by $\{p_1(a_1), \dots, p_n(a_n)\}$. The quotient A/\mathfrak{a} is generated by the images of the a_i , call them \bar{a}_i . As $p_i(a_i) \in \mathfrak{a}$, it follows $p_i(\bar{a}_i) = 0$, whence the minimal polynomial of \bar{a}_i equals the prime polynomial p_i . By Lemma 2.14, we know that A/\mathfrak{a} is a field, whence \mathfrak{a} is the maximal ideal. \square

2.2.2 Algorithm for computing common primary spaces

It may help to think about finite dimensional commutative algebras over a field as algebras of matrices. Then the localisation statements of this section just mean choosing a basis such that one obtains block matrices.

By a *common primary space* for commuting matrices we mean a direct summand of the underlying vector space on which the minimal polynomials of the given matrices are prime powers. By Proposition 2.13, a common primary space of a basis of a matrix algebra is a local factor of the algebra.

By a *generalised eigenspace* for commuting matrices we mean a vector subspace of the underlying vector space on which the minimal polynomial of the given matrices are irreducible. Allowing base changes to extension fields, the matrices restricted to the generalised eigenspace are diagonalisable.

In this section we present a straight forward algorithm for computing common primary spaces and common generalised eigenspaces.

Algorithm 2.16. *Input: list **ops** of commuting operators acting on the K -vector space V .*

*Output: list of the common primary spaces inside V for all operators in **ops**.*

- (1) $List := [V]$;
- (2) for T in **ops** do
- (3) $newList := []$;
- (4) for W in $List$ do
- (5) compute the minimal polynomial $f \in K[X]$ of T restricted to W .
- (6) factor f over K into its prime powers $f(X) = \prod_{i=1}^n p_i(X)^{e_i}$.
- (7) if n equals 1, then
- (8) append W to $newList$,
- (9) else for $i := 1$ to n do

- (10) compute \widetilde{W} as the kernel of $p_i(T|_W)^\alpha$ with $\alpha = e_i$ for common primary spaces or $\alpha = 1$ for common generalised eigenspaces.
- (11) append \widetilde{W} to *newList*.
- (12) end for; end if;
- (13) end for;
- (14) *List* := *newList*;
- (15) end for;
- (16) return *List* and stop.

2.2.3 Algorithm for computing idempotents

Using Algorithm 2.16 it is possible to compute a complete set of orthogonal primitive idempotents for A . We now sketch a direct algorithm.

Algorithm 2.17. *Input:* matrix M .

Output: complete set of orthogonal primitive idempotents for the matrix algebra generated by M and 1.

- (1) compute the minimal polynomial f of M .
- (2) factor it $f = (\prod_{i=1}^n p_i^{e_i})X^e$ over K with p_i distinct irreducible polynomials different from X .
- (3) *List* := [];
- (4) for $i = 1$ to n do
- (5) $g := f/p_i^{e_i}$;
- (6) $M_1 := g(M)$. If we think about M_1 in block form, then there is only one non-empty block on the diagonal, the rest is zero. In the next steps this block is replaced by the identity.
- (7) compute the minimal polynomial h of M_1 .
- (8) strip possible factors X from h and normalise h so that $h(0) = 1$.
- (9) append $1 - h(M_1)$ to *List*. Note that $h(M_1)$ is the identity matrix except at the block corresponding to p_i , which is zero. Thus $1 - h(M_1)$ is the idempotent being zero everywhere and being the identity in the block corresponding to p_i .
- (10) end for;
- (11) if $e > 0$ then
- (12) append $1 - \sum_{e \in \text{List}} e$ to *List*.
- (13) end if;
- (14) return *List* and stop.

The algorithm for computing a complete set of orthogonal primitive idempotents for a commutative matrix algebra consists of multiplying together the idempotents of every matrix in a basis. See Computer Exercise 2.31.

2.3 Theoretical exercises

Exercise 2.18. Use your knowledge on modular forms to prove that a modular form $f = \sum_{n=0}^{\infty} a_n(f)q^n$ of weight $k \geq 1$ and level N (and Dirichlet character χ) is uniquely determined by $\sum_{n=1}^{\infty} a_n(f)q^n$.

Exercise 2.19. Prove Proposition 2.3.

Hint: use that the kernel of a ring homomorphism into an integral domain is a prime ideal; moreover, use that all prime ideals in the Hecke algebra in the exercise are maximal; finally, use that field homomorphisms can be extended to separable extensions (using here that K is perfect).

Exercise 2.20. Let \mathbb{T} be an Artinian ring.

- (a) Let \mathfrak{m} be a maximal ideal of \mathbb{T} . Prove that \mathfrak{m}^∞ is a principal ideal generated by an idempotent. Call it $e_{\mathfrak{m}}$.
- (b) Prove that the idempotents $1 - e_{\mathfrak{m}}$ and $1 - e_{\mathfrak{n}}$ for different maximal ideals \mathfrak{m} and \mathfrak{n} are orthogonal.
- (c) Prove that the set $\{1 - e_{\mathfrak{m}} \mid \mathfrak{m} \in \text{Spec}(\mathbb{T})\}$ forms a complete set of pairwise orthogonal idempotents.

Hint: see [2, §8].

Exercise 2.21. Prove the correspondences and the isomorphisms from Part (a) of Proposition 2.7.

Hint: you only need basic reasonings from commutative algebra.

Exercise 2.22. Let $f, g \in M_k(N, \chi; \overline{K})$ be normalised eigenforms that we assume to be $\text{Gal}(\overline{K}/\overline{K})$ -conjugate. Prove that their reductions modulo p are $\text{Gal}(\overline{\mathbb{F}}/\mathbb{F})$ -conjugate.

Exercise 2.23. Prove Proposition 2.9.

Hint: it suffices to write out the definitions.

Exercise 2.24. Find a non-local algebra A over a field K (of your choice) such that A is generated as a K -algebra by a_1, \dots, a_n having the property that the minimal polynomial of each a_i is a power of an irreducible polynomial in $K[X]$.

Exercise 2.25. Let K be a field of characteristic 0 or a finite field. Let L be a finite extension of K with Galois closure N over K . Show that there is an element $x \in L$ with $\text{Tr}_{N/K}(x) \neq 0$.

Exercise 2.26. Let A be a commutative matrix algebra over a perfect field K . Suppose that the minimal polynomial of each element of a generating set is the power of a prime polynomial (i.e. it is primary).

Show that there exist base change matrices such that the base changed algebra consists only of lower triangular matrices. You may and you may have to extend scalars to a finite extension of K . In Computer Exercise 2.33 you are asked to find and implement an algorithm computing such base change matrices.

2.4 Computer exercises

Computer Exercise 2.27. Change Algorithm 1.14 (see Computer Exercise 1.44) so that it works for modular forms over a given ring R .

Computer Exercise 2.28. Let A be a commutative matrix algebra over a perfect field K .

- (a) Write an algorithm to test whether A is local.
- (b) Suppose A is local. Write an algorithm to compute its maximal ideal.

Computer Exercise 2.29. Let A be a commutative algebra over a field K . The regular representation is defined as the image of the injection

$$A \rightarrow \text{End}_K(A), \quad a \mapsto (b \mapsto a \cdot b).$$

Write a function computing the regular representation.

Computer Exercise 2.30. Implement Algorithm 2.16. Also write a function that returns the local factors as matrix algebras (possibly using regular representations).

Computer Exercise 2.31. (a) Implement Algorithm 2.17.

- (b) Let S be a set of idempotents. Write a function selecting a subset of S consisting of pairwise orthogonal idempotents such that the subset spans S (all idempotents in S can be obtained as sums of elements in the subset).

- (c) Write a function computing a complete set of pairwise orthogonal idempotents for a commutative matrix algebra A over a field by multiplying together the idempotents of the matrices in a basis and selecting a subset as in (b).
- (d) Use Computer Exercise 2.28 to compute the maximal ideals of A .

Computer Exercise 2.32. Let A be a commutative matrix algebra over a perfect field K . Suppose that A is a field (for instance obtained as the quotient of a local A by its maximal ideal computed in Computer Exercise 2.28). Write a function returning an irreducible polynomial p such that A is $K[X]/(p)$.

If possible, the algorithm should not use factorisations of polynomials. It is a practical realisation of Kronecker's primitive element theorem.

Computer Exercise 2.33. Let A be a commutative matrix algebra over a perfect field K . Suppose that the minimal polynomial of each element of a generating set is the power of a prime polynomial (i.e. it is primary).

Write a function computing base change matrices such that the base changed algebra consists only of lower triangular matrices (cf. Exercise 2.26).

3 Homological algebra

In this section we provide the tools from homological algebra that will be necessary for the modular symbols algorithm (in its group cohomological version). A good reference is [22].

We will be sloppy about categories. When we write category below, we really mean abelian category, since we obviously need the existence of kernels, images, quotients etc. For what we have in mind, we should really understand the word category not in its precise mathematical sense but as a placeholder for R -modules, or (co-)chain complexes of R -modules and other categories from everyday life.

3.1 Theory: Categories and Functors

Definition 3.1. A category \mathcal{C} consists of the following data:

- a class $\text{obj}(\mathcal{C})$ of objects,
- a set $\text{Hom}_{\mathcal{C}}(A, B)$ of morphisms for every ordered pair (A, B) of objects,
- an identity morphism $\text{id}_A \in \text{Hom}_{\mathcal{C}}(A, A)$ for every object A , and
- a composition function

$$\text{Hom}_{\mathcal{C}}(A, B) \times \text{Hom}_{\mathcal{C}}(B, C) \rightarrow \text{Hom}_{\mathcal{C}}(A, C), \quad (f, g) \mapsto g \circ f$$

for every ordered triple (A, B, C) of objects

such that

- (Associativity) $(h \circ g) \circ f = h \circ (g \circ f)$ for all $f \in \text{Hom}_{\mathcal{C}}(A, B)$, $g \in \text{Hom}_{\mathcal{C}}(B, C)$, $h \in \text{Hom}_{\mathcal{C}}(C, D)$ and
- (Unit Axiom) $\text{id}_B \circ f = f = f \circ \text{id}_A$ for $f \in \text{Hom}_{\mathcal{C}}(A, B)$.

Example 3.2. Examples of categories are

- Sets: objects are sets, morphisms are maps.
- Let R be a not necessarily commutative ring. Left R -modules (R -modules): objects are R -modules, morphisms are R -module homomorphisms. This is the category we are going to work with most of the time. Note that the category of \mathbb{Z} -modules is the category of abelian groups.
- Right R -modules (modules $- R$): as above.

Definition 3.3. Let \mathcal{C} and \mathcal{D} be categories. A covariant/contravariant functor $F : \mathcal{C} \rightarrow \mathcal{D}$ is

- a rule $\text{obj}(\mathcal{C}) \rightarrow \text{obj}(\mathcal{D})$, $C \mapsto F(C)$ and
- a rule $\begin{cases} \text{covariant:} & \text{Hom}_{\mathcal{C}}(C_1, C_2) \rightarrow \text{Hom}_{\mathcal{D}}(F(C_1), F(C_2)), f \mapsto F(f) \\ \text{contravariant:} & \text{Hom}_{\mathcal{C}}(C_1, C_2) \rightarrow \text{Hom}_{\mathcal{D}}(F(C_2), F(C_1)), f \mapsto F(f) \end{cases}$

such that

- $F(\text{id}_{\mathcal{C}}) = \text{id}_{F(\mathcal{C})}$ and
- $\begin{cases} \text{covariant:} & F(g \circ f) = F(g) \circ F(f) \\ \text{contravariant:} & F(g \circ f) = F(f) \circ F(g) \end{cases}$

Example 3.4. • Let $M \in \text{obj}(R\text{-modules})$. Define

$$\text{Hom}_R(M, \cdot) : R\text{-modules} \rightarrow \mathbb{Z}\text{-modules}, \quad A \mapsto \text{Hom}_R(M, A).$$

This is a covariant functor.

- Let $M \in \text{obj}(R\text{-modules})$. Define

$$\text{Hom}_R(\cdot, M) : R\text{-modules} \rightarrow \mathbb{Z}\text{-modules}, \quad A \mapsto \text{Hom}_R(A, M).$$

This is a contravariant functor.

- Let $M \in \text{obj}(R\text{-modules})$. Define

$$\cdot \otimes_R M : \text{modules} - R \rightarrow \mathbb{Z}\text{-modules}, \quad A \mapsto A \otimes_R M.$$

This is a covariant functor.

- Let $M \in \text{obj}(\text{modules} - R)$. Define

$$M \otimes_R \cdot : R\text{-modules} \rightarrow \mathbb{Z}\text{-modules}, \quad A \mapsto M \otimes_R A.$$

This is a covariant functor.

Definition 3.5. Let \mathcal{C} and \mathcal{D} be categories and $F, G : \mathcal{C} \rightarrow \mathcal{D}$ be both covariant or both contravariant functors. A natural transformation $\alpha : F \Rightarrow G$ is a collection of morphisms $\alpha = (\alpha_C)_{C \in \mathcal{C}} : F(C) \rightarrow G(C)$ in \mathcal{D} for $C \in \mathcal{C}$ such that for all morphisms $f : C_1 \rightarrow C_2$ in \mathcal{C} the following diagram commutes:

$$\begin{array}{ccc} \text{covariant:} & & \text{contravariant:} \\ F(C_1) & \xrightarrow{F(f)} & F(C_2) & F(C_1) & \xleftarrow{F(f)} & F(C_2) \\ \alpha_{C_1} \downarrow & & \downarrow \alpha_{C_2} & \alpha_{C_1} \downarrow & & \downarrow \alpha_{C_2} \\ G(C_1) & \xrightarrow{G(f)} & G(C_2) & G(C_1) & \xleftarrow{G(f)} & G(C_2). \end{array}$$

Example 3.6. Let R be a not necessarily commutative ring and let $A, B \in \text{obj}(R\text{-modules})$ together with a morphism $A \rightarrow B$. Then there are natural transformations $\text{Hom}_R(B, \cdot) \Rightarrow \text{Hom}_R(A, \cdot)$ and $\text{Hom}_R(\cdot, A) \Rightarrow \text{Hom}_R(\cdot, B)$ as well as $\cdot \otimes_R A \Rightarrow \cdot \otimes_R B$ and $A \otimes_R \cdot \Rightarrow B \otimes_R \cdot$.

Proof. Exercise 3.31. □

Definition 3.7. • A covariant functor $F : \mathcal{C} \rightarrow \mathcal{D}$ is called left-exact, if for every exact sequence

$$0 \rightarrow A \rightarrow B \rightarrow C$$

the sequence

$$0 \rightarrow F(A) \rightarrow F(B) \rightarrow F(C)$$

is also exact.

- A contravariant functor $F : \mathcal{C} \rightarrow \mathcal{D}$ is called *left-exact*, if for every exact sequence

$$A \rightarrow B \rightarrow C \rightarrow 0$$

the sequence

$$0 \rightarrow F(C) \rightarrow F(B) \rightarrow F(A)$$

is also exact.

- A covariant functor $F : \mathcal{C} \rightarrow \mathcal{D}$ is called *right-exact*, if for every exact sequence

$$A \rightarrow B \rightarrow C \rightarrow 0$$

the sequence

$$F(A) \rightarrow F(B) \rightarrow F(C) \rightarrow 0$$

is also exact.

- A contravariant functor $F : \mathcal{C} \rightarrow \mathcal{D}$ is called *right-exact*, if for every exact sequence

$$0 \rightarrow A \rightarrow B \rightarrow C$$

the sequence

$$F(C) \rightarrow F(B) \rightarrow F(A) \rightarrow 0$$

is also exact.

- A covariant or contravariant functor is *exact* if it is both left-exact and right-exact.

Example 3.8. Both functors $\text{Hom}_R(\cdot, M)$ and $\text{Hom}_R(M, \cdot)$ for $M \in \text{obj}(R\text{-modules})$ are left-exact. Both functors $\cdot \otimes_R M$ for $M \in \text{obj}(R\text{-modules})$ and $M \otimes_R \cdot$ for $M \in \text{obj}(\text{modules} - R)$ are right-exact.

Proof. Exercise 3.32. □

Definition 3.9. Let R be a not necessarily commutative ring. A left R -module P is called *projective* if the functor $\text{Hom}_R(P, \cdot)$ is exact. A left R -module I is called *injective* if the functor $\text{Hom}_R(\cdot, I)$ is exact.

Lemma 3.10. Let R be a not necessarily commutative ring and let P be a left R -module. Then P is projective if and only if P is a direct summand of some free R -module. In particular, free modules are projective.

Proof. Exercise 3.33. □

3.2 Theory: Complexes and Cohomology

Definition 3.11. A (right) chain complex C_\bullet in the category $R\text{-modules}$ is a collection of objects $C_n \in \text{obj}(R\text{-modules})$ for $n \geq m$ for some $m \in \mathbb{Z}$ together with homomorphisms $C_{n+1} \xrightarrow{\partial_{n+1}} C_n$, i.e.

$$\cdots \rightarrow C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \rightarrow \cdots \rightarrow C_{m+2} \xrightarrow{\partial_{m+2}} C_{m+1} \xrightarrow{\partial_{m+1}} C_m \xrightarrow{\partial_m} 0,$$

such that

$$\partial_n \circ \partial_{n+1} = 0$$

for all $n \geq m$. The group of n -cycles of this chain complex is defined as

$$Z_n(C_\bullet) = \ker(\partial_n).$$

The group of n -boundaries of this chain complex is defined as

$$B_n(C_\bullet) = \text{im}(\partial_{n+1}).$$

The n -th homology group of this chain complex is defined as

$$H_n(C_\bullet) = \ker(\partial_n) / \text{im}(\partial_{n+1}).$$

The chain complex C_\bullet is exact if $H_n(C_\bullet) = 0$ for all n . If C_\bullet is exact and $m = -1$, one often says that C_\bullet is a resolution of C_{-1} .

A morphism of right chain complexes $\phi_\bullet : C_\bullet \rightarrow D_\bullet$ is a collection of homomorphisms $\phi_n : C_n \rightarrow D_n$ for $n \in \mathbb{N}_0$ such that all the diagrams

$$\begin{array}{ccc} C_{n+1} & \xrightarrow{\partial_{n+1}} & C_n \\ \phi_{n+1} \downarrow & & \downarrow \phi_n \\ D_{n+1} & \xrightarrow{\partial_{n+1}} & D_n \end{array}$$

are commutative.

If all ϕ_n are injective, we regard C_\bullet as a sub-chain complex of D_\bullet . If all ϕ_n are surjective, we regard D_\bullet as a quotient complex of C_\bullet .

Definition 3.12. A (right) cochain complex C^\bullet in the category R -modules is a collection of objects $C^n \in \text{obj}(R\text{-modules})$ for $n \geq m$ for some $m \in \mathbb{Z}$ together with homomorphisms $C^n \xrightarrow{\partial^{n+1}} C^{n+1}$, i.e.

$$0 \xrightarrow{\partial^m} C^m \xrightarrow{\partial^{m+1}} C^{m+1} \xrightarrow{\partial^{m+2}} C^{m+2} \rightarrow \dots \rightarrow C^{n-1} \xrightarrow{\partial^n} C^n \xrightarrow{\partial^{n+1}} C^{n+1} \rightarrow \dots,$$

such that

$$\partial^{n+1} \circ \partial^n = 0$$

for all $n \geq m$. The group of n -cocycles of this cochain complex is defined as

$$Z^n(C_\bullet) = \ker(\partial^{n+1}).$$

The group of n -coboundaries of this cochain complex is defined as

$$B^n(C_\bullet) = \text{im}(\partial_n).$$

The n -th cohomology group of this cochain complex is defined as

$$H^n(C^\bullet) = \ker(\partial^{n+1}) / \text{im}(\partial^n).$$

The cochain complex C^\bullet is exact if $H^n(C_\bullet) = 0$ for all n . If C^\bullet is exact and $m = -1$, one often says that C^\bullet is a resolution of C^{-1} .

A morphism of right cochain complexes $\phi^\bullet : C^\bullet \rightarrow D^\bullet$ is a collection of homomorphisms $\phi^n : C^n \rightarrow D^n$ for $n \in \mathbb{N}_0$ such that all the diagrams

$$\begin{array}{ccc} C^n & \xrightarrow{\partial^{n+1}} & C^{n+1} \\ \phi^n \downarrow & & \downarrow \phi^{n+1} \\ D^n & \xrightarrow{\partial^{n+1}} & D^{n+1} \end{array}$$

are commutative.

If all ϕ^n are injective, we regard C^\bullet as a sub-chain complex of D^\bullet . If all ϕ^n are surjective, we regard D^\bullet as a quotient complex of C^\bullet .

In Exercise 3.34 you are asked to define kernels, cokernels and images of morphisms of cochain complexes and to show that morphisms of cochain complexes induce natural maps on the cohomology groups. In fact, cochain complexes of R -modules form an abelian category.

Example: standard resolution of a group

Let G be a group and R a commutative ring. Write G^n for the n -fold direct product $G \times \dots \times G$ and equip $R[G^n]$ with the diagonal $R[G]$ -action. We describe the *standard resolution* $F(G)_\bullet$ of R by free $R[G]$ -modules:

$$0 \xleftarrow{\partial_0} R \xleftarrow{\epsilon} F(G)_0 := R[G] \xleftarrow{\partial_1} F(G)_1 := R[G^2] \xleftarrow{\partial_2} \dots,$$

where we put (the ‘‘hat’’ means that we leave out that element):

$$\partial_n := \sum_{i=0}^n (-1)^i d_i \quad \text{and} \quad d_i(g_0, \dots, g_n) := (g_0, \dots, \hat{g}_i, \dots, g_n).$$

The map ϵ is the usual augmentation map defined by sending $g \in G$ to $1 \in R$. By ‘standard resolution’ we refer to the straight maps. We have included the bended arrow ∂_0 , which is 0 by definition, because it will be needed in the definition of group cohomology (Definition 3.13). In Exercise 3.35 you are asked to check that the standard resolution is indeed a resolution, i.e. that the above complex is exact.

Example: bar resolution of a group

We continue to treat the standard resolution R by $R[G]$ -modules, but we will write it differently. [22] calls the following the *unnormalised bar resolution* of G . We shall simply say *bar resolution*. If we let $h_r := g_{r-1}^{-1}g_r$, then we get the identity

$$(g_0, g_1, g_2, \dots, g_n) = g_0 \cdot (1, h_1, h_1h_2, \dots, h_1h_2 \dots h_n) =: g_0 \cdot [h_1|h_2| \dots |h_n].$$

The symbols $[h_1|h_2| \dots |h_n]$ with arbitrary $h_i \in G$ hence form an $R[G]$ -basis of $F(G)_n$, and one has $F(G)_n = R[G] \otimes_R$ (free R -module on $[h_1|h_2| \dots |h_n]$). One computes the action of ∂_n on this basis and gets $\partial_n = \sum_{i=0}^n (-1)^i d_i$ where

$$d_i([h_1| \dots |h_n]) = \begin{cases} [h_1|h_2| \dots |h_n] & i = 0 \\ [h_1| \dots |h_i h_{i+1}| \dots |h_n] & 0 < i < n \\ [h_1| \dots |h_{n-1}] & i = n. \end{cases}$$

We will from now on, if confusion is unlikely, simply write (h_1, \dots, h_n) instead of $[h_1| \dots |h_n]$.

Example: resolution of a cyclic group

Let $G = \langle T \rangle$ be an infinite cyclic group (i.e. a group isomorphic to $(\mathbb{Z}, +)$). Here is a very simple resolution of R by free $R[G]$ -modules:

$$0 \rightarrow R[G] \xrightarrow{T-1} R[G] \xrightarrow{\epsilon} R \rightarrow 0. \tag{3.11}$$

Let now $G = \langle \sigma \rangle$ be a finite cyclic group of order n and let $N_\sigma := \sum_{i=0}^{n-1} \sigma^i$. Here is a resolution of R by free $R[G]$ -modules:

$$\dots \rightarrow R[G] \xrightarrow{N_\sigma} R[G] \xrightarrow{1-\sigma} R[G] \xrightarrow{N_\sigma} R[G] \xrightarrow{1-\sigma} R[G] \xrightarrow{\epsilon} R \rightarrow 0. \tag{3.12}$$

In Exercise 3.36 you are asked to verify the exactness of these two sequences.

Group cohomology

A standard reference for group cohomology is [4].

Definition 3.13. Let R be a ring, G a group and M a left $R[G]$ -module. Recall that $F(G)_\bullet$ denotes the standard resolution of R by free $R[G]$ -modules.

(a) Let M be a left $R[G]$ -module. When we apply the functor $\text{Hom}_{R[G]}(\cdot, M)$ to the standard resolution $F(G)_\bullet$ cut off at 0 (i.e. $F(G)_1 \xrightarrow{\partial_1} F(G)_0 \xrightarrow{\partial_0} 0$), we get the cochain complex $\text{Hom}_{R[G]}(F(G)_\bullet, M)$:

$$\cdots \rightarrow \text{Hom}_{R[G]}(F(G)_{n-1}, M) \xrightarrow{\partial^n} \text{Hom}_{R[G]}(F(G)_n, M) \xrightarrow{\partial^{n+1}} \text{Hom}_{R[G]}(F(G)_{n+1}, M) \rightarrow \cdots$$

Define the n -th cohomology group of G with values in the G -module M as

$$H^n(G, M) := H^n(\text{Hom}_{R[G]}(F(G)_\bullet, M)).$$

(b) Let M be a right $R[G]$ -module. When we apply the functor $M \otimes_{R[G]} \cdot$ to the standard resolution $F(G)_\bullet$ cut off at 0 we get the chain complex $M \otimes_{R[G]} F(G)_\bullet$:

$$\cdots \rightarrow M \otimes_{R[G]} F(G)_{n+1} \xrightarrow{\partial_{n+1}} M \otimes_{R[G]} F(G)_n \xrightarrow{\partial_n} M \otimes_{R[G]} F(G)_{n-1} \rightarrow \cdots$$

Define the n -th homology group of G with values in the G -module M as

$$H_n(G, M) := H_n(M \otimes_{R[G]} F(G)_\bullet).$$

In this lecture we shall only use group cohomology. As a motivation for looking at group cohomology in this lecture, we can already point out that

$$H^1(\Gamma_1(N), V_{k-2}(R)) \cong \mathcal{M}_k(\Gamma_1(N), R),$$

provided that 6 is invertible in R (see Theorem 5.9). The reader is invited to compute explicit descriptions of H^0 , H_0 and H^1 in Exercise 3.37.

3.3 Theory: Cohomological Techniques

The cohomology of groups fits into a general machinery, namely that of derived functor cohomology. Derived functors are universal cohomological δ -functors and many properties of them can be derived in a purely formal way from the universality. What this means will be explained in this section. We omit all proofs.

Definition 3.14. Let \mathcal{C} and \mathcal{D} be (abelian) categories (for instance, \mathcal{C} the right cochain complexes of R -modules and $\mathcal{D} = R$ -modules). A positive covariant cohomological δ -functor between \mathcal{C} and \mathcal{D} is a collection of functors $H^n : \mathcal{C} \rightarrow \mathcal{D}$ for $n \geq 0$ together with connecting morphisms

$$\delta^n : H^n(C) \rightarrow H^{n+1}(A)$$

which are defined for every short exact sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ in \mathcal{C} such that the following hold:

- (a) (Positivity) H^n is the zero functor if $n < 0$.
- (b) For every short exact sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ in \mathcal{C} there is the long exact sequence in \mathcal{D} :

$$\cdots \rightarrow H^{n-1}(C) \xrightarrow{\delta^{n-1}} H^n(A) \rightarrow H^n(B) \rightarrow H^n(C) \xrightarrow{\delta^n} H^{n+1}(A) \rightarrow \cdots,$$

where the maps $H^n(A) \rightarrow H^n(B) \rightarrow H^n(C)$ are those that are induced from the homomorphisms in the exact sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$.

(c) For every commutative diagram in \mathcal{C}

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & & & f \downarrow & & g \downarrow & & h \downarrow \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \end{array}$$

with exact rows the following diagram in \mathcal{D} commutes, too:

$$\begin{array}{ccccccccc} H^{n-1}(C) & \xrightarrow{\delta^{n-1}} & H^n(A) & \longrightarrow & H^n(B) & \longrightarrow & H^n(C) & \xrightarrow{\delta^n} & H^{n+1}(A) \\ H^{n-1}(h) \downarrow & & H^n(f) \downarrow & & H^n(g) \downarrow & & H^n(h) \downarrow & & H^{n+1}(f) \downarrow \\ H^{n-1}(C') & \xrightarrow{\delta^{n-1}} & H^n(A') & \longrightarrow & H^n(B') & \longrightarrow & H^n(C') & \xrightarrow{\delta^n} & H^{n+1}(A') \end{array}$$

Theorem 3.15. Let R be a ring (not necessarily commutative). Let \mathcal{C} stand for the category of cochain complexes of left R -modules. Then the cohomology functors

$$H^n : \mathcal{C} \rightarrow R\text{-modules}, \quad C^\bullet \mapsto H^n(C^\bullet)$$

form a cohomological δ -functor.

Proof. This theorem is proved by some 'diagram chasing' starting from the snake lemma. See Chapter 1 of [22] for details. \square

It is not difficult to conclude that group cohomology also forms a cohomological δ -functor.

Proposition 3.16. Let R be a commutative ring and G a group.

(a) The functor from $R[G]$ -modules to cochain complexes of $R[G]$ -modules which associates to a left $R[G]$ -module M the cochain complex $\text{Hom}_{R[G]}(F(G)_\bullet, M)$ with $F(G)_\bullet$ the bar resolution of R by free $R[G]$ -modules is exact, i.e. it takes an exact sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ of $R[G]$ -modules to the exact sequence

$$0 \rightarrow \text{Hom}_{R[G]}(F(G)_\bullet, A) \rightarrow \text{Hom}_{R[G]}(F(G)_\bullet, B) \rightarrow \text{Hom}_{R[G]}(F(G)_\bullet, C) \rightarrow 0$$

of cochain complexes.

(b) The functors

$$H^n(G, \cdot) : R[G]\text{-modules} \rightarrow R\text{-modules}, \quad M \mapsto H^n(G, M)$$

form a positive cohomological δ -functor.

Proof. Exercise 3.38. \square

We will now come to universal δ -functors. Important examples of such (among them group cohomology) are obtained from injective resolutions. Although the following discussion is valid in any abelian category (with enough injectives), we restrict to R -modules for a not necessarily commutative ring R .

Definition 3.17. Let R be a not necessarily commutative ring and let $M \in \text{obj}(R\text{-modules})$.

A projective resolution of M is a resolution

$$\cdots \rightarrow P_2 \xrightarrow{\partial_2} P_1 \xrightarrow{\partial_1} P_0 \rightarrow M \rightarrow 0,$$

i.e. an exact chain complex, in which all the P_n for $n \geq 0$ are projective R -modules.

An injective resolution of M is a resolution

$$0 \rightarrow M \rightarrow I^0 \xrightarrow{\partial^1} I^1 \xrightarrow{\partial^2} I^2 \rightarrow \cdots,$$

i.e. an exact cochain complex, in which all the I^n for $n \geq 0$ are injective R -modules.

We state the following lemma as a fact. It is easy for projective resolutions and requires work for injective ones (see e.g. [13]).

Lemma 3.18. *Injective and projective resolutions exist in the category of R -modules, where R is any ring (not necessarily commutative).*

Note that applying a left exact covariant functor \mathcal{F} to an injective resolution

$$0 \rightarrow M \rightarrow I^0 \rightarrow I^1 \rightarrow I^2 \rightarrow \dots$$

of M gives rise to a cochain complex

$$0 \rightarrow \mathcal{F}(M) \rightarrow \mathcal{F}(I^0) \rightarrow \mathcal{F}(I^1) \rightarrow \mathcal{F}(I^2) \rightarrow \dots,$$

of which only the part $0 \rightarrow \mathcal{F}(M) \rightarrow \mathcal{F}(I^0) \rightarrow \mathcal{F}(I^1)$ need be exact. This means that the H^0 of the (cut off at 0) cochain complex $\mathcal{F}(I^0) \rightarrow \mathcal{F}(I^1) \rightarrow \mathcal{F}(I^2) \rightarrow \dots$ is equal to $\mathcal{F}(M)$.

Definition 3.19. *Let R be a not necessarily commutative ring.*

(a) *Let \mathcal{F} be a left exact covariant functor on the category of R -modules (mapping for instance to \mathbb{Z} -modules).*

The right derived functors $R^n\mathcal{F}(\cdot)$ of \mathcal{F} are the functors on the category of R -modules defined as follows. For $M \in \text{obj}(R\text{-modules})$ choose an injective resolution $0 \rightarrow M \rightarrow I^0 \rightarrow I^1 \rightarrow \dots$ and let

$$R^n\mathcal{F}(M) := H^n(\mathcal{F}(I^0) \rightarrow \mathcal{F}(I^1) \rightarrow \mathcal{F}(I^2) \rightarrow \dots).$$

(b) *Let \mathcal{G} be a left exact contravariant functor on the category of R -modules.*

The right derived functors $R^n\mathcal{G}(\cdot)$ of \mathcal{G} are the functors on the category of R -modules defined as follows. For $M \in \text{obj}(R\text{-modules})$ choose a projective resolution $\dots \rightarrow P_1 \rightarrow P_0 \rightarrow M \rightarrow 0$ and let

$$R^n\mathcal{G}(M) := H^n(\mathcal{G}(P_0) \rightarrow \mathcal{G}(P_1) \rightarrow \mathcal{G}(P_2) \rightarrow \dots).$$

We state the following lemma without a proof. It is a simple consequence of the injectivity respectively projectivity of the modules in the resolution.

Lemma 3.20. *The right derived functors do not depend on the choice of the resolution and they form a cohomological δ -functor.*

Of course, one can also define left derived functors of right exact functors. An important example is the Tor-functor which is obtained by deriving the tensor product functor in a way dual to Ext (see below). As already mentioned, the importance of right and left derived functors comes from their universality.

Definition 3.21. (a) *Let $(H^n)_n$ and $(T^n)_n$ be cohomological δ -functors. A morphism of cohomological δ -functors is a collection of natural transformations $\eta^n : H^n \Rightarrow T^n$ that commute with the connecting homomorphisms δ , i.e. for every short exact sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ and every n the diagram*

$$\begin{array}{ccc} H^n(C) & \xrightarrow{\delta} & H^{n+1}(A) \\ \eta_C^n \downarrow & & \eta_A^{n+1} \downarrow \\ T^n(C) & \xrightarrow{\delta} & T^{n+1}(A) \end{array}$$

commutes.

(b) *The cohomological δ -functor $(H^n)_n$ is universal if for every cohomological δ -functor $(T^n)_n$ and every natural transformation $\eta^0 : H^0(\cdot) \Rightarrow T^0(\cdot)$ there is a unique natural transformation $\eta^n : H^n(\cdot) \Rightarrow T^n(\cdot)$ for all $n \geq 1$ such that the η^n form a morphism of cohomological δ -functors between $(H^n)_n$ and $(T^n)_n$.*

For the proof of the following central result we refer to [22], Chapter 2.

Theorem 3.22. *Let R be a not necessarily commutative ring and let \mathcal{F} be a left exact covariant or contravariant functor on the category of R -modules (mapping for instance to \mathbb{Z} -modules).*

The right derived functors $(R^n\mathcal{F}(\cdot))_n$ of \mathcal{F} form a universal cohomological δ -functor.

Example 3.23. (a) *Let R be a commutative ring and G a group. The functor*

$$(\cdot)^G : R[G] - \text{modules} \rightarrow R - \text{modules}, \quad M \mapsto M^G$$

is left exact and covariant, hence we can form its right derived functors $R^n(\cdot)^G$. Since we have the special case $(R^0(\cdot)^G)(M) = M^G$, universality gives a morphism of cohomological δ -functors $R^n(\cdot)^G \Rightarrow H^n(G, \cdot)$. We shall see that this is an isomorphism.

(b) *Let R be a not necessarily commutative ring. We have seen that the functors $\text{Hom}_R(\cdot, M)$ and $\text{Hom}_R(M, \cdot)$ are left exact. We write*

$$\text{Ext}_R^n(\cdot, M) := R^n\text{Hom}_R(\cdot, M) \quad \text{and} \quad \text{Ext}_R^n(M, \cdot) := R^n\text{Hom}_R(M, \cdot).$$

See Theorem 3.24 below.

(c) *Many cohomology theories in (algebraic) geometry are also of a right derived functor nature. For instance, let X be a topological space and consider the category of sheaves of abelian groups on X . The global sections functor $\mathcal{F} \mapsto \mathcal{F}(X) = H^0(X, \mathcal{F})$ is left exact and its right derived functors $R^n(H^0(X, \cdot))$ can be formed. They are usually denoted by $H^n(X, \cdot)$ and they define 'sheaf cohomology' on X . Etale cohomology is an elaboration of this based on a generalisation of topological spaces.*

Universal properties of group cohomology

Theorem 3.24. *Let R be a not necessarily commutative ring. The Ext-functor is balanced. This means that for any two R -modules M, N there are isomorphisms*

$$(\text{Ext}_R^n(\cdot, N))(M) \cong (\text{Ext}_R^n(M, \cdot))(N) =: \text{Ext}_R^n(M, N).$$

Proof. [22], Theorem 2.7.6. □

Corollary 3.25. *Let R be a commutative ring and G a group. For every $R[G]$ -module M there are isomorphisms*

$$H^n(G, M) \cong \text{Ext}_{R[G]}^n(R, M) \cong (R^n(\cdot)^G)(M)$$

and the functors $(H^n(G, \cdot))_n$ form a universal cohomological δ -functor. Moreover, apart from the standard resolution of R by free $R[G]$ -modules, any resolution of R by projective $R[G]$ -modules may be used to compute $H^n(G, M)$.

Proof. We may compute $\text{Ext}_{R[G]}^n(\cdot, M)(R)$ by any resolution of R by projective $R[G]$ -modules. Our standard resolution is such a resolution, since any free module is projective. Hence, $H^n(G, M) \cong \text{Ext}_{R[G]}^n(\cdot, M)(R)$. The key is now that Ext is balanced (Theorem 3.24), since it gives $H^n(G, M) \cong \text{Ext}_{R[G]}^n(R, \cdot)(M) \cong R^n(\cdot)^G(M) \cong \text{Ext}_{R[G]}^n(R, M)$. As the Ext-functor is universal (being a right derived functor), also $H^n(G, \cdot)$ is universal. For the last statement we recall that right derived functors do not depend on the chosen projective respectively injective resolution. □

You are invited to look at Exercise 3.39 now.

3.4 Theory: Generalities on Group Cohomology

We now apply the universality of the δ -functor of group cohomology. Let $\phi : H \rightarrow G$ be a group homomorphism and A an $R[G]$ -module. Via ϕ we may consider A also as an $R[H]$ -module and $\text{res}^0 : H^0(G, \cdot) \rightarrow H^0(H, \cdot)$ is a natural transformation. By the universality of $H^\bullet(G, \cdot)$ we get natural transformations

$$\text{res}^n : H^n(G, \cdot) \rightarrow H^n(H, \cdot).$$

These maps are called *restrictions*. See Exercise 3.40 for a description in terms of cochains. Very often ϕ is just the embedding map of a subgroup.

Assume now that H is a normal subgroup of G and A is an $R[G]$ -module. Then we can consider $\phi : G \rightarrow G/H$ and the restriction above gives natural transformations $\text{res}^n : H^n(G/H, (\cdot)^H) \rightarrow H^n(G, (\cdot)^H)$. We define the *inflation maps* to be

$$\text{infl}^n : H^n(G/H, A^H) \xrightarrow{\text{res}^n} H^n(G, A^H) \longrightarrow H^n(G, A)$$

where the last arrow is induced from the natural inclusion $A^H \hookrightarrow A$.

Under the same assumptions, conjugation by $g \in G$ preserves H and we have the isomorphism $H^0(H, A) = A^H \xrightarrow{a \mapsto ga} A^H = H^0(H, A)$. Hence by universality we obtain natural maps $H^n(H, A) \rightarrow H^n(H, A)$ for every $g \in G$. One even gets an $R[G]$ -action on $H^n(H, A)$. As $h \in H$ is clearly the identity on $H^0(H, A)$, the above action is in fact also an $R[G/H]$ -action.

Let now $H \leq G$ be a subgroup of finite index. Then the norm $N_{G/H} := \sum_{\{g_i\}} \in R[G]$ with $\{g_i\}$ a system of representatives of G/H gives a natural transformation $\text{cores}^0 : H^0(H, \cdot) \rightarrow H^0(G, \cdot)$ where \cdot is an $R[G]$ -module. By universality we obtain

$$\text{cores}^n : H^n(H, \cdot) \rightarrow H^n(G, \cdot),$$

the *corestriction (transfer)* maps.

The inflation map, the $R[G/H]$ -action and the corestriction can be explicitly described in terms of cochains of the bar resolution (see Exercise 3.40).

It is clear that $\text{cores}^0 \circ \text{res}^0$ is multiplication by the index $(G : H)$. By universality, also $\text{cores}^n \circ \text{res}^n$ is multiplication by the index $(G : H)$. Hence we have proved the first part of the following proposition.

Proposition 3.26. (a) *Let $H < G$ be a subgroup of finite index $(G : H)$. For all i and all $R[G]$ -modules M one has the equality*

$$\text{cores}_H^G \circ \text{res}_H^G = (G : H)$$

on all $H^i(G, M)$.

(b) *Let G be a finite group of order n and R a ring in which n is invertible. Then $H^i(G, M) = 0$ for all $i \geq 1$ and all $R[G]$ -modules M .*

Proof. Part (b) is an easy consequence with $H = 1$, since

$$H^i(G, M) \xrightarrow{\text{res}_H^G} H^i(1, M) \xrightarrow{\text{cores}_H^G} H^i(G, M)$$

is the zero map (as $H^i(1, M) = 0$ for $i \geq 1$), but it also is multiplication by n . \square

The following exact sequence turns out to be very important for our purposes.

Theorem 3.27 (Hochschild-Serre). *Let $H \leq G$ be a normal subgroup and A an $R[G]$ -module. There is the exact sequence:*

$$0 \rightarrow H^1(G/H, A^H) \xrightarrow{\text{infl}} H^1(G, A) \xrightarrow{\text{res}} H^1(G, A)^{G/H} \rightarrow H^2(G/H, A^H) \xrightarrow{\text{infl}} H^2(G, A).$$

Proof. We only sketch the proof for those who know spectral sequences. It is, however, possible to verify the exactness on cochains explicitly (after having defined the missing map appropriately). Grothendieck's theorem on spectral sequences ([22], 6.8.2) associates to the composition of functors

$$(A \mapsto A^H \mapsto (A^H)^{G/H}) = (A \mapsto A^G)$$

the spectral sequence

$$E_2^{p,q} : H^p(G/H, H^q(H, A)) \Rightarrow H^{p+q}(G, A).$$

The statement of the theorem is then just the 5-term sequence that one can associate with every spectral sequence of this type. \square

Coinduced modules and Shapiro's Lemma

Let $H < G$ be a subgroup and A be a left $R[H]$ -module. The $R[G]$ -module

$$\text{Coind}_H^G(A) := \text{Hom}_{R[H]}(R[G], A)$$

is called the *coinduction* or the *coinduced module* from H to G of A . We make $\text{Coind}_H^G(A)$ into a left $R[G]$ -module by

$$(g \cdot \phi)(g') = \phi(g'g) \quad \forall g, g' \in G, \phi \in \text{Hom}_{R[H]}(R[G], A).$$

Proposition 3.28 (Shapiro's Lemma). *For all $n \geq 0$, the map*

$$\text{Sh} : H^n(G, \text{Coind}_H^G(A)) \rightarrow H^n(H, A)$$

given on cochains is given by

$$c \mapsto ((h_1, \dots, h_n) \rightarrow (c(h_1, \dots, h_n))(1_G))$$

is an isomorphism.

Proof. Exercise 3.41. \square

Mackey's formula and stabilisers

If $H \leq G$ are groups and V is an $R[G]$ -module, we denote by $\text{Res}_H^G(V)$ the module V considered as an $R[H]$ -module if we want to stress that the module is obtained by restriction. In later sections, we will often silently restrict modules to subgroups.

Proposition 3.29. *Let R be a ring, G be a group and H, K subgroups of G . Let furthermore V be an $R[H]$ -module. Mackey's formula is the isomorphism*

$$\text{Res}_K^G \text{Coind}_H^G V \cong \prod_{g \in H \backslash G / K} \text{Coind}_{K \cap g^{-1}Hg}^K {}^g(\text{Res}_{H \cap gKg^{-1}}^H V).$$

Here ${}^g(\text{Res}_{H \cap gKg^{-1}}^H V)$ denotes the $R[K \cap g^{-1}Hg]$ -module obtained from V via the conjugated action $g^{-1}hg \cdot v := h \cdot v$ for $v \in V$ and $h \in H$ such that $g^{-1}hg \in K$.

Proof. We consider the commutative diagram

$$\begin{array}{ccc} \text{Res}_K^G \text{Hom}_{R[H]}(R[G], V) & \longrightarrow & \prod_{g \in H \backslash G / K} \text{Hom}_{R[K \cap g^{-1}Hg]}(R[K], {}^g(\text{Res}_{H \cap gKg^{-1}}^H V)) \\ & \searrow & \downarrow \sim \\ & & \prod_{g \in H \backslash G / K} \text{Hom}_{R[H \cap gKg^{-1}]}(R[gKg^{-1}], \text{Res}_{H \cap gKg^{-1}}^H V). \end{array}$$

The vertical arrow is just given by conjugation and is clearly an isomorphism. The diagonal map is the product of the natural restrictions. From the bijection

$$(H \cap gKg^{-1}) \backslash gKg^{-1} \xrightarrow{gkg^{-1} \mapsto Hgk} H \backslash HgK$$

it is clear that also the diagonal map is an isomorphism, proving the proposition. \square

From Shapiro's Lemma 3.28 we directly get the following.

Corollary 3.30. *In the situation of Proposition 3.29 one has*

$$\begin{aligned} \mathrm{H}^i(K, \mathrm{Coind}_H^G V) &\cong \prod_{g \in H \backslash G / K} \mathrm{H}^i(K \cap g^{-1} H g, {}^g(\mathrm{Res}_{H \cap g K g^{-1}}^H V)) \\ &\cong \prod_{g \in H \backslash G / K} \mathrm{H}^i(H \cap g K g^{-1}, \mathrm{Res}_{H \cap g K g^{-1}}^H V) \end{aligned}$$

for all $i \in \mathbb{N}$.

3.5 Theoretical exercises

Exercise 3.31. *Check the statements made in Example 3.6.*

Exercise 3.32. *Verify the statements of Example 3.8.*

Exercise 3.33. *Prove Lemma 3.10.*

Hint: take a free R -module F which surjects onto P , i.e. $\pi : F \rightarrow P$, and use the definition of P being projective to show that the surjection admits a split $s : P \rightarrow F$, meaning that $\pi \circ s$ is the identity on P . This is then equivalent to the assertion.

Exercise 3.34. *Let $\phi^\bullet : C^\bullet \rightarrow D^\bullet$ be a morphism of cochain complexes.*

- Show that $\ker(\phi^\bullet)$ is a cochain complex and is a subcomplex of C^\bullet in a natural way.
- Show that $\mathrm{im}(\phi^\bullet)$ is a cochain complex and is a subcomplex of D^\bullet in a natural way.
- Show that $\mathrm{coker}(\phi^\bullet)$ is a cochain complex and is a quotient of D^\bullet in a natural way.
- Show that ϕ^\bullet induces homomorphisms $\mathrm{H}^n(C^\bullet) \xrightarrow{\mathrm{H}^n(\phi^\bullet)} \mathrm{H}^n(D^\bullet)$ for all $n \in \mathbb{N}$.

Exercise 3.35. *Check the exactness of the standard resolution of a group G .*

Exercise 3.36. *Check the exactness of the resolutions (3.11) and (3.12) for an infinite and a finite cyclic group, respectively.*

Exercise 3.37. *Let R, G, M be as in the definition of group (co-)homology.*

- Prove $\mathrm{H}^0(G, M) \cong M^G$, the G -invariants of M .
- Prove $\mathrm{H}_0(G, M) \cong M_G$, the G -coinvariants of M .
- Prove the explicit descriptions:

$$\begin{aligned} Z^1(G, M) &= \{f : G \rightarrow M \text{ map} \mid f(gh) = g.f(h) + f(g) \forall g, h \in G\}, \\ B^1(G, M) &= \{f : G \rightarrow M \text{ map} \mid \exists m \in M : f(g) = (1 - g)m \forall g \in G\}, \\ \mathrm{H}^1(G, M) &= Z^1(G, M) / B^1(G, M). \end{aligned}$$

In particular, if the action of G on M is trivial, the boundaries $B^1(G, M)$ are zero, and one has:

$$\mathrm{H}^1(G, M) = \mathrm{Hom}_{\mathrm{group}}(G, M).$$

Exercise 3.38. *Prove Proposition 3.16.*

Hint: for (a), use that free modules are projective. (b) follows from (a) together with Theorem 3.15 or, alternatively, by direct calculation. See also [4, III.6.1].

Exercise 3.39. *Let R be a commutative ring.*

- Let $G = \langle T \rangle$ be a free cyclic group and M any $R[G]$ -module. Prove

$$\mathrm{H}^0(G, M) = M^G, \quad \mathrm{H}^1(G, M) = M / (1 - T)M \quad \text{and} \quad \mathrm{H}^i(G, M) = 0$$

for all $i \geq 2$.

(b) For a finite cyclic group $G = \langle \sigma \rangle$ of order n and any $R[G]$ -module M prove that

$$\begin{aligned} \mathrm{H}^0(G, M) &\cong M^G, & \mathrm{H}^1(G, M) &\cong \{m \in M \mid N_\sigma m = 0\} / (1 - \sigma)M, \\ \mathrm{H}^2(G, M) &\cong M^G / N_\sigma M, & \mathrm{H}^i(G, M) &\cong \mathrm{H}^{i+2}(G, M) \text{ for all } i \geq 1. \end{aligned}$$

Exercise 3.40. Let R be a commutative ring.

- (a) Let $\phi : H \rightarrow G$ be a group homomorphism and A an $R[G]$ -module. Prove that the restriction maps $\mathrm{res}^n : H^n(G, A) \rightarrow H^n(H, A)$ are given in terms of cochains of the bar resolution by composing the cochains by ϕ .
- (b) Let H be a normal subgroup of G . Describe the inflation maps in terms of cochains of the bar resolution.
- (c) Let H be a normal subgroup of G and A an $R[G]$ -module. Describe the $R[G/H]$ -action on $H^n(H, A)$ in terms of cochains of the bar resolution.
- (d) Let now $H \leq G$ be a subgroup of finite index. Describe the corestriction maps in terms of cochains of the bar resolution.

Exercise 3.41. Prove Shapiro's lemma, i.e. Proposition 3.28.

Hint: see [22, (6.3.2)] for an abstract proof; see also [4, III.6.2] for the underlying map.

4 Cohomology of $\mathrm{PSL}_2(\mathbb{Z})$

In this section, we shall calculate the cohomology of the group $\mathrm{PSL}_2(\mathbb{Z})$ and important properties thereof. This will be at the basis of our treatment of Manin symbols in the following section. The key in this is the description of $\mathrm{PSL}_2(\mathbb{Z})$ as a free product of two cyclic groups.

4.1 Theory: The standard fundamental domain for $\mathrm{PSL}_2(\mathbb{Z})$

We define the matrices of $\mathrm{SL}_2(\mathbb{Z})$

$$\sigma := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \tau := \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \tau\sigma.$$

By the definition of the action of $\mathrm{SL}_2(\mathbb{Z})$ on \mathbb{H} in equation 1.1, we have for all $z \in \mathbb{H}$:

$$\sigma.z = \frac{-1}{z}, \quad \tau.z := 1 - \frac{1}{z}, \quad T.z = z + 1.$$

These matrices have the following conceptual meaning:

$$\langle \pm\sigma \rangle = \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(i), \quad \langle \pm\tau \rangle = \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\zeta_6) \quad \text{and} \quad \langle \pm T \rangle = \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{Z})}(\infty)$$

with $\zeta_6 = e^{2\pi i/6}$. From now on we will often represent classes of matrices in $\mathrm{PSL}_2(\mathbb{Z})$ by matrices in $\mathrm{SL}_2(\mathbb{Z})$. The orders of σ and τ in $\mathrm{PSL}_2(\mathbb{Z})$ are 2 and 3, respectively. These statements are checked by calculation. Exercise 4.19 is recommended at this point.

Even though in this section our interest concerns the full group $\mathrm{SL}_2(\mathbb{Z})$, we give the definition of fundamental domain for general subgroups of $\mathrm{SL}_2(\mathbb{Z})$ of finite index.

Definition 4.1. Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a subgroup of finite index. A fundamental domain for the action of Γ on \mathbb{H} is a subset $\mathcal{F} \subset \mathbb{H}$ such that the following hold:

- (i) \mathcal{F} is open.
- (ii) For every $z \in \mathbb{H}$, there is $\gamma \in \Gamma$ such that $\gamma.z \in \overline{\mathcal{F}}$.
- (iii) If $\gamma.z \in \mathcal{F}$ for $z \in \mathcal{F}$ and $\gamma \in \Gamma$, then one has $\gamma = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

In other words, a fundamental domain is an open set, which is small enough not to contain any two points that are equivalent under the operation by Γ , and which is big enough that every point in the upper half plane is equivalent to some point in the closure of the fundamental domain.

Proposition 4.2. *The set*

$$\mathcal{F} := \left\{ z \in \mathbb{H} \mid |z| > 1 \text{ and } -\frac{1}{2} < \operatorname{Re}(z) < \frac{1}{2} \right\}$$

is a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on \mathbb{H} .

It is clear that \mathcal{F} is open. For (ii), we use the following lemma.

Lemma 4.3. *Let $z \in \mathbb{H}$. The orbit $\mathrm{SL}_2(\mathbb{Z}).z$ contains a point $\gamma.z$ with maximal imaginary part (geometrically also called ‘height’), i.e.*

$$\operatorname{Im}(\gamma.z) \geq \operatorname{Im}(g.z) \quad \forall g \in \mathrm{SL}_2(\mathbb{Z}).$$

A point $z \in \mathbb{H}$ is of maximal height if $|cz + d| \geq 1$ for all coprime $c, d \in \mathbb{Z}$.

Proof. We have the simple formula $\operatorname{Im}(\gamma.z) = \frac{\operatorname{Im}(z)}{|cz+d|^2}$. It implies

$$\operatorname{Im}(z) \leq \operatorname{Im}(\gamma.z) \Leftrightarrow |cz + d| \leq 1.$$

For fixed $z = x + iy$ with $x, y \in \mathbb{R}$, consider the inequality

$$1 \geq |cz + d|^2 = (cx + d)^2 + c^2y^2.$$

This expression admits only finitely many solutions $c, d \in \mathbb{Z}$. Among these finitely many, we may choose a coprime pair (c, d) with minimal $|cz + d|$. Due to the coprimeness, there are $a, b \in \mathbb{Z}$ such that the matrix $M := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ belongs to $\mathrm{SL}_2(\mathbb{Z})$. It is now clear that $M.z$ has maximal height. \square

We next use a simple trick to show (ii) in Definition 4.1 for \mathcal{F} . Let $z \in \mathbb{H}$. By Lemma 4.3, we choose $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma.z$ has maximal height. We now ‘transport’ $\gamma.z$ via an appropriate translation T^n in such a way that $-1/2 \leq \operatorname{Re}(T^n\gamma.z) < 1/2$. The height is obviously left invariant. Now we have $|T^n\gamma.z| \geq 1$ because otherwise the height of $T^n\gamma.z$ would not be maximal. For, if $|T^n\gamma.z + 0| < 1$ then applying σ (corresponding to reflection on the unit circle) would make the height strictly bigger. More precisely, we have the following result.

Lemma 4.4. *Every point of maximal height in \mathbb{H} can be translated into the closure of the fundamental domain $\overline{\mathcal{F}}$. Conversely, $\overline{\mathcal{F}}$ only contains points of maximal height.*

Proof. The first part was proved in the preceding discussion. The second one follows from the calculation

$$\begin{aligned} |cz + d|^2 &= (cx + d)^2 + c^2y^2 = c^2|z|^2 + 2cdx + d^2 \\ &\geq c^2|z|^2 - |cd| + d^2 \geq c^2 - |cd| + d^2 \geq (|c| - |d|)^2 + |cd| \geq 1 \end{aligned} \quad (4.13)$$

for all coprime integers c, d and $z = x + iy \in \mathbb{H}$ with $x, y \in \mathbb{R}$. \square

End of the proof of Proposition 4.2. Let $z \in \mathcal{F}$ and $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma.z \in \mathcal{F}$. By Lemma 4.4, z and $\gamma.z$ both have maximal height, whence $|cz + d| = 1$. Hence the inequalities in equation 4.13 are equalities, implying $c = 0$. Thus, $\gamma = \pm T^n$ for some $n \in \mathbb{Z}$. But only $n = 0$ is compatible with the assumption $\gamma.z \in \mathcal{F}$. This proves (iii) in Definition 4.1 for \mathcal{F} . \square

Proposition 4.5. *The group $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices σ and τ .*

Proof. Let $\Gamma := \langle \sigma, \tau \rangle$ be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by σ and T .

We prove that for any $z \in \mathbb{H}$ there is $\gamma \in \Gamma$ such that $\gamma.z \in \overline{\mathcal{F}}$. For that, note that the orbit $\Gamma.z$ contains a point $\gamma.z$ for $\gamma \in \Gamma$ of maximal height as it is a subset of $\mathrm{SL}_2(\mathbb{Z}).z$, for which we have seen that statement. As Γ contains $T = \tau\sigma$, we can translate $\gamma.z$ so as to have real part in between $-\frac{1}{2}$ and $\frac{1}{2}$. As Γ also contains σ , the absolute value of the new point has to be at least 1 because otherwise σ would make the height bigger.

In order to conclude, choose any point $z \in \mathcal{F}$ and let $M \in \mathrm{SL}_2(\mathbb{Z})$. We consider the point $M.z$ and ‘transport’ it back into \mathcal{F} via a matrix $\gamma \in \Gamma$. We thus have $(\gamma M).z \in \mathcal{F}$. As \mathcal{F} is a fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$, it follows $\gamma M = \pm 1$, showing $M \in \Gamma$. \square

An alternative algorithmic proof is provided in Algorithm 5.10 below.

4.2 Theory: $\mathrm{PSL}_2(\mathbb{Z})$ as a free product

We now apply the knowledge about the (existence of the) fundamental domain for $\mathrm{PSL}_2(\mathbb{Z})$ to derive that $\mathrm{PSL}_2(\mathbb{Z})$ is a free product.

Definition 4.6. Let G and H be two groups. The free product $G * H$ of G and H is the group having as elements all the possible words, i.e. sequences of symbols, $a_1 a_2 \dots a_n$ with $a_i \in G - \{1\}$ or $a_i \in H - \{1\}$ such that elements from G and H alternate (i.e. if $a_i \in G$, then $a_{i+1} \in H$ and vice versa) together with the empty word, which we denote by 1. The integer n is called the length of the group element (word) $w = a_1 a_2 \dots a_n$ and denoted by $l(w)$. We put $l(1) = 0$ for the empty word.

The group operation in $G * H$ is concatenation of words followed by ‘reduction’ (in order to obtain a new word obeying to the rules). The reduction rules are: for all words v, w , all $g_1, g_2 \in G$ and all $h_1, h_2 \in H$:

- $v1w = vw$,
- $vg_1g_2w = v(g_1g_2)w$ (i.e. the multiplication of g_1 and g_2 in G is carried out),
- $vh_1h_2w = v(h_1h_2)w$ (i.e. the multiplication of h_1 and h_2 in H is carried out).

In Exercise 4.18 you are asked to verify that $G * H$ is indeed a group and to prove a universal property. Alternatively, if G is given by the set of generators \mathcal{G}_G together with relations \mathcal{R}_G and similarly for the group H , then the free product $G * H$ can be described as the group generated by $\mathcal{G}_G \cup \mathcal{G}_H$ with relations $\mathcal{R}_G \cup \mathcal{R}_H$.

Theorem 4.7. Let \mathcal{P} be the free product $\langle \sigma \rangle * \langle \tau \rangle$ of the cyclic groups $\langle \sigma \rangle$ of order 2 and $\langle \tau \rangle$ of order 3.

Then \mathcal{P} is isomorphic to $\mathrm{PSL}_2(\mathbb{Z})$. In particular, as an abstract group, $\mathrm{PSL}_2(\mathbb{Z})$ can be represented by generators and relations as $\langle \sigma, \tau \mid \sigma^2 = \tau^3 = 1 \rangle$.

In the proof, we will need the following statement, which we separate because it is entirely computational.

Lemma 4.8. Let $\gamma \in \mathcal{P}$ be 1 or any word starting in σ on the left, i.e. $\sigma\tau^{e_1}\sigma\tau^{e_2}\dots$. Then $\mathrm{Im}(\tau^2\gamma.i) < 1$.

Proof. For $\gamma = 1$, the statement is clear. Suppose $\gamma = \sigma\tau^{e_1}\sigma\tau^{e_2}\sigma\dots\tau^{e_{r-1}}\sigma\tau^{e_r}$ with $r \geq 0$, $e_i \in \{1, 2\}$ for $i = 1, \dots, r$. We prove more generally

$$\mathrm{Im}(\tau^2\gamma.i) = \mathrm{Im}(\tau^2(\gamma\sigma).i) > \mathrm{Im}(\tau^2(\gamma\sigma)\tau^e.i) = \mathrm{Im}(\tau^2(\gamma\sigma)\tau^e\sigma.i)$$

for any $e = 1, 2$. This means that extending the word to the right by $\sigma\tau^e$, the imaginary part goes strictly down for both $e = 1, 2$.

We first do some matrix calculations. Let us say that an integer matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfies (*) if $(c+d)^2 > \max(c^2, d^2)$. The matrix $\tau^2\sigma = \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}$ clearly satisfies (*). Let us assume that $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

satisfies (*). We show that $\gamma\tau\sigma = \begin{pmatrix} * & * \\ c & c+d \end{pmatrix}$ and $\gamma\tau^2\sigma = \begin{pmatrix} * & * \\ -c-d & -d \end{pmatrix}$ also satisfy (*). The first one follows once we know $(2c+d)^2 > \max(c^2, (c+d)^2)$. This can be seen like this:

$$(2c+d)^2 = (c^2 + 2cd) + 2c^2 + (c+d)^2 > 2c^2 + (c+d)^2 \geq \max(c^2, (c+d)^2),$$

where we used that (*) implies $(c+d)^2 > d^2$ and, thus, $c^2 + 2cd > 0$. The second inequality is obtained by exchanging the roles of c and d .

We thus see that $\tau^2\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfies (*) for all words γ starting and ending in σ . Finally, we have for all such γ :

$$\begin{aligned} \mathrm{Im}(\tau^2\gamma i) &= \frac{1}{|ci + d|^2} &&= \frac{1}{c^2 + d^2}, \\ \mathrm{Im}(\tau^2\gamma\tau i) &= \mathrm{Im}(\tau^2\gamma(i+1)) = \frac{1}{|c(i+1) + d|^2} &&= \frac{1}{(c+d)^2 + c^2}, \\ \mathrm{Im}(\tau^2\gamma\tau^2 i) &= \mathrm{Im}(\tau^2\gamma \frac{1+i}{2}) = \frac{1/2}{|c(i/2 + 1/2) + d|^2} &&= \frac{2}{(c+2d)^2 + c^2}. \end{aligned}$$

Now (*) implies the desired inequalities of the imaginary parts. \square

Proof of Theorem 4.7. As $\mathrm{SL}_2(\mathbb{Z})$ is generated by σ and τ due to Proposition 4.5, the universal property of the free product gives us a surjection of groups $\mathcal{P} \twoheadrightarrow \mathrm{PSL}_2(\mathbb{Z})$.

Let B be the geodesic path from ζ_6 to i , i.e. the arc between ζ_6 and i in positive orientation (counter clockwise) on the circle of radius 1 around the origin, lying entirely on the closure $\overline{\mathcal{F}}$ of the standard fundamental domain from Proposition 4.2. Define the map

$$\mathrm{PSL}_2(\mathbb{Z}) \xrightarrow{\phi} \{\text{Paths in } \mathbb{H}\}$$

which sends $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$ to $\gamma.B$, i.e. the image of B under γ . The proof of the theorem is finished by showing that the composite

$$\mathcal{P} \twoheadrightarrow \mathrm{PSL}_2(\mathbb{Z}) \xrightarrow{\phi} \{\text{Paths in } \mathbb{H}\}$$

is injective, as then the first map must be an isomorphism.

This composition is injective because its image is a tree, that is, a graph without circles. By drawing it, one convinces oneself very quickly hereof. We, however, give a formal argument, which can also be nicely visualised on the geometric realisation of the graph as going down further and further in every step.

In order to prepare for the proof, let us first suppose that $\gamma_1.B$ and $\gamma_2.B$ for some $\gamma_1, \gamma_2 \in \mathrm{PSL}_2(\mathbb{Z})$ meet in a point which is not the endpoint of either of the two paths. Then $\gamma.B$ intersects B in some interior point for $\gamma := \gamma_1^{-1}\gamma_2$. This intersection point lies on the boundary of the fundamental domain \mathcal{F} . Consequently, by (iii) in Definition 4.1, $\gamma = \pm 1$ and $\gamma_1.B = \gamma_2.B$. This implies that if $\mathrm{Im}(\gamma_1.i) \neq \mathrm{Im}(\gamma_2.i)$ where $i = \sqrt{-1}$, then $\gamma_1.B$ and $\gamma_2.B$ do not meet in any interior point and are thus distinct paths.

It is obvious that $B, \sigma.B, \tau.B$ are distinct paths. They share the property that their point that is conjugate to i has imaginary part 1 (in fact, the points conjugate to i in the paths are $i, i, i+1$, respectively).

By Lemma 4.8, for γ equal to 1 or any word in \mathcal{P} starting with σ on the left, we obtain that $\tau^2\gamma.B$ is distinct from $B, \sigma.B, \tau.B$ because it lies 'lower'. In particular, $\tau^2\gamma.B \neq B$. As $\tau^2\gamma.B \neq \tau.B$, we also find $\tau\gamma.B \neq B$. Finally, if $\gamma.B = B$ and $\gamma = \sigma\tau^e\gamma'$ with $e \in \{1, 2\}$ and γ' starting in σ or $\gamma' = 1$, then $\tau^e\gamma'.B = \sigma.B$, which has already been excluded. We have thus found that for any non-trivial word $\gamma \in \mathcal{P}$, the conjugate $\gamma.B$ is distinct from B . This proves the desired injectivity. \square

4.3 Theory: Mayer-Vietoris for $\mathrm{PSL}_2(\mathbb{Z})$

Motivated by the description $\mathrm{PSL}_2(\mathbb{Z}) = C_2 * C_3$, we now consider the cohomology of a group G which is the free product of two finite groups G_1 and G_2 , i.e. $G = G_1 * G_2$.

Proposition 4.9. *Let R be a commutative ring. The sequence*

$$0 \rightarrow R[G] \xrightarrow{\alpha} R[G/G_1] \oplus R[G/G_2] \xrightarrow{\epsilon} R \rightarrow 0$$

with $\alpha(g) = (gG_1, -gG_2)$ and $\epsilon(gG_1, 0) = 1 = \epsilon(0, gG_2)$ is exact.

Proof. This proof is an even more elementary version of an elementary proof that I found in [3]. Clearly, ϵ is surjective and also $\epsilon \circ \alpha = 0$.

Next we compute exactness at the centre. We first claim that for every element $g \in G$ we have

$$g - 1 = \sum_j \alpha_j g_j (h_j - 1) \in R[G/G_1]$$

for certain $\alpha_j \in R$ and certain $g_j \in G$, $h_j \in G_2$ and analogously with the roles of G_1 and G_2 exchanged. To see this, we write $g = a_1 a_2 \dots a_n$ with a_i alternatingly in G_1 and G_2 (we do not need the uniqueness of this expression). If $n = 1$, there is nothing to do. If $n > 1$, we have

$$a_1 a_2 \dots a_n - 1 = a_1 a_2 \dots a_{n-1} (a_n - 1) + (a_1 a_2 \dots a_{n-1} - 1)$$

and we obtain the claim by induction. Consequently, we have for all $\lambda = \sum_i r_i g_i G_1$ and all $\mu = \sum_k \tilde{r}_k \tilde{g}_k G_2$ with $r_i, \tilde{r}_k \in R$ and $g_i, \tilde{g}_k \in G$

$$\lambda - \sum_i r_i 1_G G_1 = \sum_j \alpha_j g_j (h_j - 1) \in R[G/G_1]$$

and

$$\mu - \sum_k \tilde{r}_k 1_G G_2 = \sum_l \tilde{\alpha}_l \tilde{g}_l (\tilde{h}_l - 1) \in R[G/G_2]$$

for certain $\alpha_j, \tilde{\alpha}_l \in R$, certain $g_j, \tilde{g}_l \in G$ and certain $h_j \in G_2$, $\tilde{h}_l \in G_1$. Suppose now that with λ and μ as above we have

$$\epsilon(\lambda, \mu) = \sum_i r_i + \sum_k \tilde{r}_k = 0.$$

Then we directly get

$$\alpha\left(\sum_j \alpha_j g_j (h_j - 1) - \sum_l \tilde{\alpha}_l \tilde{g}_l (\tilde{h}_l - 1) + \sum_i r_i 1_G\right) = (\lambda, \mu)$$

and hence the exactness at the centre.

It remains to prove that α is injective. Now we use the freeness of the product. Let $\lambda = \sum_w a_w w \in R[G]$ be an element in the kernel of α . Hence, $\sum_w a_w w G_1 = 0$ and $\sum_w a_w w G_2 = 0$. Let us assume that $\lambda \neq 0$. It is clear that λ cannot just be a multiple of $1 \in G$, as otherwise it would not be in the kernel of α . Now pick the $g \in G$ with $a_g \neq 0$ having maximal length $l(g)$ (among all the $l(w)$ with $a_w \neq 0$). It follows that $l(g) > 0$. Assume without loss of generality that the representation of g ends in a non-zero element of G_1 . Further, since $a_g \neq 0$ and $0 = \sum_w a_w w G_2$, there must be an $h \in G$ with $g \neq h$, $gG_2 = hG_2$ and $a_h \neq 0$. As g does not end in G_2 , we must have $h = gy$ for some $0 \neq y \in G_2$. Thus, $l(h) > l(g)$, contradicting the maximality and proving the proposition. \square

Recall that we usually denote the restriction of a module to a subgroup by the same symbol. For example, in the next proposition we will write $H^1(G_1, M)$ instead of $H^1(G_1, \mathrm{Res}_{G_1}^G(M))$.

Proposition 4.10 (Mayer-Vietoris). *Let $G = G_1 * G_2$ be a free product. Let M be a left $R[G]$ -module. Then the Mayer-Vietoris sequence gives the exact sequences*

$$0 \rightarrow M^G \rightarrow M^{G_1} \oplus M^{G_2} \rightarrow M \rightarrow H^1(G, M) \xrightarrow{\mathrm{res}} H^1(G_1, M) \oplus H^1(G_2, M) \rightarrow 0.$$

and for all $i \geq 2$ an isomorphism

$$H^i(G, M) \cong H^i(G_1, M) \oplus H^i(G_2, M).$$

Proof. We see that all terms in the exact sequence of Proposition 4.9 are free R -modules. We now apply the functor $\mathrm{Hom}_R(\cdot, M)$ to this exact sequence and obtain the exact sequence of $R[G]$ -modules

$$0 \rightarrow M \rightarrow \underbrace{\mathrm{Hom}_{R[G_1]}(R[G], M)}_{\cong \mathrm{Coind}_{G_1}^G(M)} \oplus \underbrace{\mathrm{Hom}_{R[G_2]}(R[G], M)}_{\cong \mathrm{Coind}_{G_2}^G(M)} \rightarrow \underbrace{\mathrm{Hom}_R(R[G], M)}_{\cong \mathrm{Coind}_\Gamma^G(M)} \rightarrow 0.$$

The central terms, as well as the term on the right, can be identified with coinduced modules. Hence, the statements on cohomology follow by taking the long exact sequence of cohomology and invoking Shapiro's Lemma 3.28. \square

We now apply the Mayer-Vietoris sequence (Prop. 4.10) to $\mathrm{PSL}_2(\mathbb{Z})$ and get that for any ring R and any left $R[\mathrm{PSL}_2(\mathbb{Z})]$ -module M the sequence

$$0 \rightarrow M^{\mathrm{PSL}_2(\mathbb{Z})} \rightarrow M^{(\sigma)} \oplus M^{(\tau)} \rightarrow M \xrightarrow{m \mapsto f_m} \mathrm{H}^1(\mathrm{PSL}_2(\mathbb{Z}), M) \xrightarrow{\mathrm{res}} \mathrm{H}^1(\langle \sigma \rangle, M) \oplus \mathrm{H}^1(\langle \tau \rangle, M) \rightarrow 0 \quad (4.14)$$

is exact and for all $i \geq 2$ one has isomorphisms

$$\mathrm{H}^i(\mathrm{PSL}_2(\mathbb{Z}), M) \cong \mathrm{H}^i(\langle \sigma \rangle, M) \oplus \mathrm{H}^i(\langle \tau \rangle, M). \quad (4.15)$$

The 1-cocycle f_m can be explicitly described as the cocycle given by $f_m(\sigma) = (1 - \sigma)m$ and $f_m(\tau) = 0$ (see Exercise 4.21).

Lemma 4.11. *Let $\Gamma \leq \mathrm{PSL}_2(\mathbb{Z})$ be a subgroup of finite index and let $x \in \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ be any point. Recall that $\mathrm{PSL}_2(\mathbb{Z})_x$ denotes the stabiliser of x for the $\mathrm{PSL}_2(\mathbb{Z})$ -action.*

(a) *The map*

$$\Gamma \backslash \mathrm{PSL}_2(\mathbb{Z}) / \mathrm{PSL}_2(\mathbb{Z})_x \xrightarrow{g \mapsto gx} \Gamma \backslash \mathrm{PSL}_2(\mathbb{Z}) x$$

is a bijection.

(b) *For $g \in \mathrm{PSL}_2(\mathbb{Z})$ the stabiliser of gx for the Γ -action is*

$$\Gamma_{gx} = \Gamma \cap g\mathrm{PSL}_2(\mathbb{Z})_x g^{-1}.$$

(c) *For all $i \in \mathbb{N}$, and all $R[\Gamma]$ -modules, Mackey's formula (Prop. 3.29) gives an isomorphism*

$$\mathrm{H}^i(\mathrm{PSL}_2(\mathbb{Z})_x, \mathrm{Coind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})} V) \cong \prod_{y \in \Gamma \backslash \mathrm{PSL}_2(\mathbb{Z}) x} \mathrm{H}^i(\Gamma_y, V).$$

Proof. (a) and (b) are clear and (c) follows directly from Mackey's formula. \square

Corollary 4.12. *Let R be a ring and $\Gamma \leq \mathrm{PSL}_2(\mathbb{Z})$ be a subgroup of finite index such that all the orders of all stabiliser groups Γ_x for $x \in \mathbb{H}$ are invertible in R . Then for all $R[\Gamma]$ -modules V one has*

$$\mathrm{H}^1(\Gamma, V) \cong M / (M^{(\sigma)} + M^{(\tau)})$$

with $M = \mathrm{Coind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V)$ and

$$\mathrm{H}^i(\Gamma, V) = 0$$

for all $i \geq 2$.

Proof. By Lemma 4.11 (b), all non-trivial stabiliser groups for the action of Γ on \mathbb{H} are of the form $g\langle \sigma \rangle g^{-1} \cap \Gamma$ or $g\langle \tau \rangle g^{-1} \cap \Gamma$ for some $g \in \mathrm{PSL}_2(\mathbb{Z})$. Due to the invertibility assumption we get from Prop. 3.26 that the groups on the right in the equation in Lemma 4.11 (c) are zero. Hence, by Shapiro's lemma (Prop. 3.28) we have

$$\mathrm{H}^i(\Gamma, V) \cong \mathrm{H}^i(\mathrm{PSL}_2(\mathbb{Z}), M)$$

for all $i \geq 0$, so that by Equations (4.14) and (4.15) we obtain the proposition. \square

By Exercise 4.19, the assumptions of the proposition are for instance always satisfied if R is a field of characteristic not 2 or 3. Look at Exercise 4.20 to see for which N the assumptions hold for $\Gamma_1(N)$ and $\Gamma_0(N)$ over an arbitrary ring (e.g. the integers).

4.4 Theory: Parabolic group cohomology

Before going on, we include a description of the cusps as $\mathrm{PSL}_2(\mathbb{Z})$ -orbits that is very useful for the sequel.

Lemma 4.13. *The cusps $\mathbb{P}^1(\mathbb{Q})$ lie in a single $\mathrm{PSL}_2(\mathbb{Z})$ -orbit. The stabiliser group of ∞ for the $\mathrm{PSL}_2(\mathbb{Z})$ -action is $\langle T \rangle$ and the map*

$$\mathrm{PSL}_2(\mathbb{Z})/\langle T \rangle \xrightarrow{g\langle T \rangle \mapsto g\infty} \mathbb{P}^1(\mathbb{Q})$$

is a $\mathrm{PSL}_2(\mathbb{Z})$ -equivariant bijection.

Proof. The claim on the stabiliser follows from a simple direct computation. This makes the map well-defined and injective. The surjectivity is equivalent to the claim that the cusps lie in a single $\mathrm{PSL}_2(\mathbb{Z})$ -orbit and simply follows from the fact that any pair of coprime integers (a, c) appears as the first column of a matrix in $\mathrm{SL}_2(\mathbb{Z})$. \square

Let R be a ring, $\Gamma \leq \mathrm{PSL}_2(\mathbb{Z})$ a subgroup of finite index. One defines the *parabolic cohomology group for the left $R[\Gamma]$ -module V* as the kernel of the restriction map in

$$0 \rightarrow H_{\mathrm{par}}^1(\Gamma, V) \rightarrow H^1(\Gamma, V) \xrightarrow{\mathrm{res}} \prod_{g \in \Gamma \backslash \mathrm{PSL}_2(\mathbb{Z})/\langle T \rangle} H^1(\Gamma \cap \langle gTg^{-1} \rangle, V). \quad (4.16)$$

Proposition 4.14. *Let R be a ring and $\Gamma \leq \mathrm{PSL}_2(\mathbb{Z})$ be a subgroup of finite index such that all the orders of all stabiliser groups Γ_x for $x \in \mathbb{H}$ are invertible in R . Let V be a left $R[\Gamma]$ -module. Write for short $G = \mathrm{PSL}_2(\mathbb{Z})$ and $M = \mathrm{Hom}_{R[\Gamma]}(R[G], V)$. Then the following diagram is commutative, its vertical maps are isomorphisms and its rows are exact:*

$$\begin{array}{ccccccc} 0 \rightarrow & H_{\mathrm{par}}^1(\Gamma, V) & \longrightarrow & H^1(\Gamma, V) & \xrightarrow{\mathrm{res}} & \prod_{g \in \Gamma \backslash \mathrm{PSL}_2(\mathbb{Z})/\langle T \rangle} H^1(\Gamma \cap \langle gTg^{-1} \rangle, V) & \rightarrow V_{\Gamma} \rightarrow 0 \\ & \uparrow \text{Shapiro} & & \uparrow \text{Shapiro} & & \uparrow \text{Mackey} & \parallel \\ 0 \rightarrow & H_{\mathrm{par}}^1(G, M) & \longrightarrow & H^1(G, M) & \xrightarrow{\mathrm{res}} & H^1(\langle T \rangle, M) & \rightarrow V_{\Gamma} \rightarrow 0 \\ & \parallel & & \uparrow m \mapsto f_m & & \downarrow c \mapsto c(T) & \uparrow \phi \\ 0 \rightarrow & H_{\mathrm{par}}^1(G, M) & \rightarrow & M/(M^{(\sigma)} + M^{(\tau)}) & \xrightarrow{m \mapsto (1-\sigma)m} & M/(1-T)M & \rightarrow M_G \rightarrow 0 \end{array}$$

The map $\phi : M_G \rightarrow V_{\Gamma}$ is given as $f \mapsto \sum_{g \in \Gamma \backslash G} f(g)$.

Proof. The commutativity of the diagram is checked in Exercise 4.22. By Exercise 3.39 we have $H^1(\langle T \rangle, M) \cong M/(1-T)M$. Due to the assumptions we may apply Corollary 4.12. The cokernel of $M/(M^{(\sigma)} + M^{(\tau)}) \xrightarrow{m \mapsto (1-\sigma)m} M/(1-T)M$ is immediately seen to be $M/((1-\sigma)M + (1-T)M)$, which is equal to M_G , as T and σ generate $\mathrm{PSL}_2(\mathbb{Z})$. Hence, the lower row is an exact sequence.

We now check that the map ϕ is well-defined. For this we verify that the image of $f(g)$ in V_{Γ} only depends on the coset $\Gamma \backslash G$:

$$f(g) - f(\gamma g) = f(g) - \gamma f(g) = (1 - \gamma)f(g) = 0 \in V_{\Gamma}.$$

Hence, for any $h \in G$ we get

$$\phi((1-h).f) = \sum_{g \in \Gamma \backslash \mathrm{PSL}_2(\mathbb{Z})} (f(g) - f(gh)) = 0,$$

as gh runs over all cosets. Thus, ϕ is well-defined. To show that ϕ is an isomorphism, we give an inverse ψ to ϕ by

$$\psi : V_{\Gamma} \rightarrow \mathrm{Hom}_{R[\Gamma]}(R[G], V)_G, \quad v \mapsto e_v \text{ with } e_v(g) = \begin{cases} gv, & \text{for } g \in \Gamma \\ 0, & \text{for } g \notin \Gamma. \end{cases}$$

It is clear that $\phi \circ \psi$ is the identity. The map ϕ is an isomorphism, as ψ is surjective. In order to see this, fix a system of representatives $\{1 = g_1, g_2, \dots, g_n\}$ for $\Gamma \backslash \mathrm{PSL}_2(\mathbb{Z})$. We first have $f = \sum_{i=1}^n g_i^{-1} \cdot e_{f(g_i)}$ because for all $h \in G$ we find

$$f(h) = g_j^{-1} \cdot e_{f(g_j)}(h) = e_{f(g_j)}(hg_j^{-1}) = hg_j^{-1} \cdot f(g_j) = \cdot f(hg_j^{-1}g_j) = f(h),$$

where $1 \leq j \leq n$ is the unique index such that $h \in \Gamma g_j$. Thus

$$f = \sum_{i=1}^n e_{f(g_i)} - \sum_{i=2}^n (1 - g_i^{-1}) \cdot e_{f(g_i)} \in \mathrm{im}(\psi),$$

as needed.

More conceptually, one can first identify the coinduced module $\mathrm{Coind}_{\Gamma}^{\mathrm{PSL}_2(\mathbb{Z})}(V)$ with the induced one $\mathrm{Ind}_{\Gamma}^{\mathrm{PSL}_2(\mathbb{Z})}(V) = R[G] \otimes_{R[\Gamma]} V$. We claim that the G -coinvariants are isomorphic to $R \otimes_{R[\Gamma]} V \cong V_{\Gamma}$. As R -modules we have $R[G] = I_G \oplus R1_G$ since $r \mapsto r1_G$ defines a splitting of the augmentation map. Here I_G is the augmentation ideal defined in Exercise 1.29. Consequently, $R[G] \otimes_{R[\Gamma]} V \cong (I_G \otimes_{R[\Gamma]} V) \oplus R \otimes_{R[\Gamma]} V$. The claim follows, since $I_G(R[G] \otimes_{R[\Gamma]} V) \cong I_G \otimes_{R[\Gamma]} V$.

Since all the terms in the upper and the middle row are isomorphic to the respective terms in the lower row, all rows are exact. \square

4.5 Theory: Dimension computations

This seems to be a good place to compute the dimension of $H^1(\Gamma, V_{k-2}(K))$ and $H_{\mathrm{par}}^1(\Gamma, V_{k-2}(K))$ over a field K under certain conditions. The results will be important for the proof of the Eichler-Shimura theorem.

Lemma 4.15. *Let R be a ring and let $n \geq 1$ be an integer, $t = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$ and $t' = \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix}$.*

(a) *If $n!N$ is not a zero divisor in R , then for the t -invariants we have*

$$V_n(R)^{\langle t \rangle} = \langle X^n \rangle$$

and for the t' -invariants

$$V_n(R)^{\langle t' \rangle} = \langle Y^n \rangle.$$

(b) *If $n!N$ is invertible in R , then the coinvariants are given by*

$$V_n(R)_{\langle t \rangle} = V_n(R) / \langle Y^n, XY^{n-1}, \dots, X^{n-1}Y \rangle$$

respectively

$$V_n(R)_{\langle t' \rangle} = V_n(R) / \langle X^n, X^{n-1}Y, \dots, XY^{n-1} \rangle.$$

(c) *If $n!N$ is not a zero divisor in R , then the R -module of $\Gamma(N)$ -invariants $V_n(R)^{\Gamma(N)}$ is zero. In particular, if R is a field of characteristic 0 and Γ is any congruence subgroup, then $V_n(R)^{\Gamma}$ is zero.*

(d) *If $n!N$ is invertible in R , then the R -module of $\Gamma(N)$ -coinvariants $V_n(R)_{\Gamma(N)}$ is zero. In particular, if R is a field of characteristic 0 and Γ is any congruence subgroup, then $V_n(R)_{\Gamma}$ is zero.*

Proof. (a) The action of t is $t \cdot (X^{n-i}Y^i) = X^{n-i}(NX + Y)^i$ and consequently

$$(t-1) \cdot (X^{n-i}Y^i) = \left(\sum_{j=0}^i \binom{i}{j} N^{i-j} X^{i-j} Y^j \right) X^{n-i} - X^{n-i} Y^i = \sum_{j=0}^{i-1} r_{i,j} X^{n-j} Y^j$$

with $r_{i,j} = N^{i-j} \binom{i}{j}$, which is not a zero divisor, respectively invertible, by assumption. For $x = \sum_{i=0}^n a_i X^{n-i} Y^i$ we have

$$\begin{aligned} (t-1).x &= \sum_{i=0}^n a_i \sum_{j=0}^{i-1} r_{i,j} X^{n-j} Y^j = \sum_{j=0}^{n-1} X^{n-j} Y^j \left(\sum_{i=j+1}^n a_i r_{i,j} \right) \\ &= XY^{n-1} a_n r_{n,n-1} + X^2 Y^{n-2} (a_n r_{n,n-2} + a_{n-1} r_{n-1,n-2}) + \dots \end{aligned}$$

If $(t-1).x = 0$, we conclude for $j = n-1$ that $a_n = 0$. Next, for $j = n-2$ it follows that $a_{n-1} = 0$, and so on, until $a_1 = 0$. This proves the statement on the t -invariants. The one on the t' -invariants follows from symmetry.

(b) The claims on the coinvariants are proved in a very similar and straightforward way.

(c) and (d) As $\Gamma(N)$ contains the matrices t and t' , this follows from Parts (a) and (b). \square

Proposition 4.16. *Let K be a field of characteristic 0 and $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup of finite index μ such that $\Gamma_y = \{1\}$ for all $y \in \mathbb{H}$ (e.g. $\Gamma = \Gamma_1(N)$ with $N \geq 4$). We can and do consider Γ as a subgroup of $\mathrm{PSL}_2(\mathbb{Z})$.*

Then

$$\dim_K \mathrm{H}^1(\Gamma, V_{k-2}(K)) = (k-1) \frac{\mu}{6} + \delta_{k,2}$$

and

$$\dim_K \mathrm{H}_{\mathrm{par}}^1(\Gamma, V_{k-2}(K)) = (k-1) \frac{\mu}{6} - \nu_\infty + 2\delta_{k,2},$$

where ν_∞ is the number of cusps of Γ , i.e. the cardinality of $\Gamma \backslash \mathbb{P}^1(\mathbb{Q})$, and $\delta_{k,2} = \begin{cases} 1 & \text{if } k = 2 \\ 0 & \text{otherwise.} \end{cases}$

Proof. Let $M = \mathrm{Coind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V_{k-2}(K))$. This module has dimension $(k-1)\mu$. From the Mayer-Vietoris exact sequence

$$0 \rightarrow M^{\mathrm{PSL}_2(\mathbb{Z})} \rightarrow M^{\langle \sigma \rangle} \oplus M^{\langle \tau \rangle} \rightarrow M \rightarrow \mathrm{H}^1(\mathrm{PSL}_2(\mathbb{Z}), M) \rightarrow 0,$$

we obtain

$$\dim \mathrm{H}^1(\Gamma, V_{k-2}(K)) = \dim M + \dim M^{\mathrm{PSL}_2(\mathbb{Z})} - \dim \mathrm{H}^0(\langle \sigma \rangle, M) - \dim \mathrm{H}^0(\langle \tau \rangle, M).$$

Recall the left $\mathrm{PSL}_2(\mathbb{Z})$ -action on $\mathrm{Hom}_K[\Gamma](K[\mathrm{PSL}_2(\mathbb{Z})], V_{k-2}(K))$, which is given by $(g.\phi)(h) = \phi(hg)$. It follows directly that every function in the K -vector space $\mathrm{Hom}_K[\Gamma](K[\mathrm{PSL}_2(\mathbb{Z})], V_{k-2}(K))^{\mathrm{PSL}_2(\mathbb{Z})}$ is constant and equal to its value at 1. The Γ -invariance, however, imposes additionally that this constant lies in $V_{k-2}(K)^\Gamma$. Hence, by Lemma 4.15, $\dim M^{\mathrm{PSL}_2(\mathbb{Z})} = \delta_{k,2}$. The term $\mathrm{H}^0(\langle \sigma \rangle, M)$ is handled by Mackey's formula:

$$\dim \mathrm{H}^0(\langle \sigma \rangle, M) = \sum_{x \in \Gamma \backslash \mathrm{PSL}_2(\mathbb{Z}).i} \dim V_{k-2}(K)^{\Gamma_x} = (k-1) \#(\Gamma \backslash \mathrm{PSL}_2(\mathbb{Z}).i) = (k-1) \frac{\mu}{2},$$

since all Γ_x are trivial by assumption and there are hence precisely $\mu/2$ points in Y_Γ lying over i in $Y_{\mathrm{SL}_2(\mathbb{Z})}$. By the same argument we get

$$\dim \mathrm{H}^0(\langle \tau \rangle, M) = \frac{\mu}{3}.$$

Putting these together gives the first formula:

$$\dim_K \mathrm{H}^1(\Gamma, V_{k-2}(K)) = (k-1) \left(\mu - \frac{\mu}{2} - \frac{\mu}{3} \right) + \delta_{k,2} = (k-1) \frac{\mu}{6} + \delta_{k,2}.$$

The second formula can be read off from the diagram in Proposition 4.14. It gives directly

$$\begin{aligned} \dim \mathrm{H}_{\mathrm{par}}^1(\Gamma, V_{k-2}(K)) &= \dim \mathrm{H}^1(\Gamma, V_{k-2}(K)) + \dim V_{k-2}(K)_\Gamma \\ &\quad - \sum_{g \in \Gamma \backslash \mathrm{PSL}_2(\mathbb{Z}) / \langle T \rangle} \dim \mathrm{H}^1(\Gamma \cap \langle gTg^{-1} \rangle, V_{k-2}(K)). \end{aligned}$$

All the groups $\Gamma \cap \langle gTg^{-1} \rangle$ are of the form $\langle T^n \rangle$ for some $n \geq 1$. Since they are cyclic, we have

$$\dim H^1(\Gamma \cap \langle gTg^{-1} \rangle, V_{k-2}(K)) = \dim V_{k-2}(K)_{\langle T^n \rangle} = 1$$

by Lemma 4.15. As the set $\Gamma \backslash \mathrm{PSL}_2(\mathbb{Z}) / \langle T \rangle$ is the set of cusps of Γ , we conclude

$$\sum_{g \in \Gamma \backslash \mathrm{PSL}_2(\mathbb{Z}) / \langle T \rangle} \dim H^1(\Gamma \cap \langle gTg^{-1} \rangle, V_{k-2}(K)) = \nu_\infty.$$

Moreover, also by Lemma 4.15, $\dim V_{k-2}(K)_\Gamma = \delta_{k,2}$. Putting everything together yields the formula

$$\dim H_{\mathrm{par}}^1(\Gamma, V_{k-2}(K)) = (k-1) \frac{\mu}{6} + 2\delta_{k,2} - \nu_\infty,$$

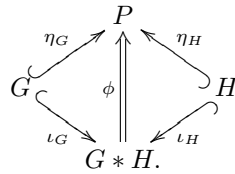
as claimed. □

Remark 4.17. One can derive a formula for the dimension even if Γ is not torsion-free. One only needs to compute the dimensions $V_{k-2}(K)^{\langle \sigma \rangle}$ and $V_{k-2}(K)^{\langle \tau \rangle}$ and to modify the above proof slightly.

4.6 Theoretical exercises

Exercise 4.18. (a) Verify that $G * H$ is a group.

(b) Prove the universal property represented by the commutative diagram



More precisely, let $\iota_G : G \rightarrow G * H$ and $\iota_H : H \rightarrow G * H$ be the natural inclusions. Let P be any group together with group injections $\eta_G : G \rightarrow P$ and $\eta_H : H \rightarrow P$, then there is a unique group homomorphism $\phi : G * H \rightarrow P$ such that $\eta_G = \phi \circ \iota_G$ and $\eta_H = \phi \circ \iota_H$.

Exercise 4.19. (a) Let $M \in \mathrm{SL}_n(\mathbb{Z})$ be an element of finite order m . Determine the primes that may divide m . [Hint: Look at the characteristic polynomial of M .]

(b) Determine all conjugacy classes of elements of finite order in $\mathrm{PSL}_2(\mathbb{Z})$.

Exercise 4.20. (a) Determine the $N \geq 1$ for which $\Gamma_1(N)$ has no element of finite order apart from the identity. [Hint: You should get $N \geq 4$.]

(b) Determine the $N \geq 1$ for which $\Gamma_0(N)$ has no element of order 4. Also determine the cases in which there is no element of order 6.

Exercise 4.21. (a) Prove that the explicit description of f_m in the Mayer-Vietoris sequence (Equation 4.14) satisfies the properties required for the 0-th connecting homomorphism in Definition 3.21.

Hint: Prove that if f_m is a boundary, then $m \in M^{\langle \sigma \rangle} + M^{\langle \tau \rangle}$. Moreover, prove that a 1-cocycle in $H^1(\mathrm{PSL}_2(\mathbb{Z}), M)$ which becomes a coboundary when restricted to either $\langle \sigma \rangle$ or $\langle \tau \rangle$ can be changed by a coboundary to be of the form f_m for some $m \in M$.

(b) Let $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ be an exact sequence of G -modules for some group G . Let $c \in C^G$ and write it as a class $b + A \in B/A \cong C$. As it is G -invariant, we have $0 = (1-g)c = (1-g)(b+A)$, whence $(1-g)b \in A$ for all $g \in G$. Define the 1-cocycle $\delta^0(c)$ as the map $G \rightarrow A$ sending g to $(1-g)b \in A$.

Prove that δ^0 satisfies the properties required for the 0-th connecting homomorphism in Definition 3.21.

Note that the connecting homomorphisms are not unique (one can, e.g. replace them by their negatives).

(c) As an alternative approach to (a), you may apply (b) to the exact sequence from which the Mayer-Vietoris sequence is derived as the associated long cohomology sequence in Proposition 4.10.

Exercise 4.22. Verify the commutativity of the diagram in Proposition 4.14.

4.7 Computer exercises

Computer Exercise 4.23. Let $N \geq 1$. Compute a list of the elements of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. Compute a list of the cusps of $\Gamma_0(N)$ and $\Gamma_1(N)$ (cf. [21], p. 60). I recommend to use the decomposition of $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ into $\mathbb{P}^1(\mathbb{Z}/p^n\mathbb{Z})$.

Computer Exercise 4.24. Let K be some field. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow K^\times$ be a Dirichlet character of modulus N . For given N and K , compute the group of all Dirichlet characters. Every Dirichlet character should be implemented as a map $\phi : \mathbb{Z} \rightarrow K^\times$ such that $\phi(a) = 0$ for all $a \in \mathbb{Z}$ with $(a, N) \neq 1$ and $\phi(a) = \chi(a \bmod N)$ otherwise.

5 Modular symbols and Manin symbols

5.1 Theory: Manin symbols

This section is an extended version of a specialisation of parts of my article [24] to the group $\mathrm{PSL}_2(\mathbb{Z})$. Manin symbols provide an alternative description of modular symbols. See Definition 5.6 below. We shall use this description for the comparison with group cohomology and for implementing the modular symbols formalism. We stay in the general setting over a ring R .

Proposition 5.1. *The sequence of R -modules*

$$0 \rightarrow R[\mathrm{PSL}_2(\mathbb{Z})]N_\sigma + R[\mathrm{PSL}_2(\mathbb{Z})]N_\tau \rightarrow R[\mathrm{PSL}_2(\mathbb{Z})] \xrightarrow{g \mapsto g(1-\sigma)^\infty} R[\mathbb{P}^1(\mathbb{Q})] \xrightarrow{g^\infty \mapsto 1} R \rightarrow 0$$

is exact. Here we are considering $R[\mathrm{PSL}_2(\mathbb{Z})]$ as a right $R[\mathrm{PSL}_2(\mathbb{Z})]$ -module.

Proof. Let H be a finite subgroup of a group G and let $H \backslash G = \{g_i \mid i \in I\}$ stand for a fixed system of representatives of the cosets. We write $R[H \backslash G]$ for the free R -module on the set of representatives. The map

$$\mathrm{Hom}_R(R[H], R[H \backslash G]) \rightarrow R[G], \quad f \mapsto \sum_{h \in H} h \cdot f(h)$$

is an isomorphism. Indeed, suppose that for $f \in \mathrm{Hom}_R(R[H], R[H \backslash G])$ we have

$$0 = \sum_{h \in H} h \cdot (f(h)) = \sum_{h \in H} h \cdot \left(\sum_{i \in I} a_{h,i} g_i \right) = \sum_{h \in H} \left(\sum_{i \in I} a_{h,i} h g_i \right),$$

then $a_{h,i} = 0$ for all $h \in H$ and all $i \in I$ (since the elements $h g_i$ are all distinct), whence $f = 0$. For the surjectivity, note that all elements in $R[G]$ can be written as (finite) sums of the form $\sum_{h \in H} \sum_{i \in I} a_{h,i} h g_i$ because any element in G is of the form $h g_i$ for a unique $h \in H$ and a unique $i \in I$.

This yields via Shapiro's lemma that

$$H^i(\langle \sigma \rangle, R[\mathrm{PSL}_2(\mathbb{Z})]) = H^i(\langle 1 \rangle, R[\langle \sigma \rangle \backslash \mathrm{PSL}_2(\mathbb{Z})]) = 0$$

for all $i \geq 1$, and similarly for $\langle \tau \rangle$. The resolution for a finite cyclic group (3.12) gives

$$\begin{aligned} R[\mathrm{PSL}_2(\mathbb{Z})]N_\sigma &= \ker_{R[\mathrm{PSL}_2(\mathbb{Z})]}(1 - \sigma) = R[\mathrm{PSL}_2(\mathbb{Z})]^{\langle \sigma \rangle}, \\ R[\mathrm{PSL}_2(\mathbb{Z})]N_\tau &= \ker_{R[\mathrm{PSL}_2(\mathbb{Z})]}(1 - \tau) = R[\mathrm{PSL}_2(\mathbb{Z})]^{\langle \tau \rangle}, \\ R[\mathrm{PSL}_2(\mathbb{Z})](1 - \sigma) &= \ker_{R[\mathrm{PSL}_2(\mathbb{Z})]} N_\sigma \quad \text{and} \\ R[\mathrm{PSL}_2(\mathbb{Z})](1 - \tau) &= \ker_{R[\mathrm{PSL}_2(\mathbb{Z})]} N_\tau. \end{aligned}$$

By Proposition 4.9, we have the exact sequence

$$0 \rightarrow R[\mathrm{PSL}_2(\mathbb{Z})] \rightarrow R[\mathrm{PSL}_2(\mathbb{Z})]_{\langle\sigma\rangle} \oplus R[\mathrm{PSL}_2(\mathbb{Z})]_{\langle\tau\rangle} \rightarrow R \rightarrow 0.$$

The injectivity of the first map in the exact sequence (which we recall is a consequence of $\mathrm{PSL}_2(\mathbb{Z}) = \langle\sigma\rangle * \langle\tau\rangle$) leads to

$$R[\mathrm{PSL}_2(\mathbb{Z})](1 - \sigma) \cap R[\mathrm{PSL}_2(\mathbb{Z})](1 - \tau) = 0.$$

Sending g to $g\infty$ yields a bijection between $R[\mathrm{PSL}_2(\mathbb{Z})]/R[\mathrm{PSL}_2(\mathbb{Z})](1 - T)$ and $R[\mathbb{P}^1(\mathbb{Q})]$. In order to prove the exactness at $R[\mathrm{PSL}_2(\mathbb{Z})]$, we show that the equality $x(1 - \sigma) = y(1 - T)$ for $x, y \in R[\mathrm{PSL}_2(\mathbb{Z})]$ yields that x belongs to $R[\mathrm{PSL}_2(\mathbb{Z})]_{\langle\sigma\rangle} + R[\mathrm{PSL}_2(\mathbb{Z})]_{\langle\tau\rangle}$.

Note that $x(1 - \sigma) = y(1 - T) = y(1 - \tau) - yT(1 - \sigma)$ because of the equality $\tau = T\sigma$. This yields $x(1 - \sigma) + yT(1 - \sigma) = y(1 - \tau)$. This expression, however, is equal to zero. Hence, there exists a $z \in R[\mathrm{PSL}_2(\mathbb{Z})]$ satisfying $y = zN_\tau$. We have $N_\tau T = N_\tau\sigma$ because of $T = \tau\sigma$. Consequently, we get

$$y(1 - T) = zN_\tau(1 - T) = zN_\tau(1 - \sigma) = y(1 - \sigma).$$

The equality $x(1 - \sigma) = y(1 - \sigma)$ implies that $x - y$ belongs to $R[\mathrm{PSL}_2(\mathbb{Z})]_{\langle\sigma\rangle}$. Since $y \in R[\mathrm{PSL}_2(\mathbb{Z})]_{\langle\tau\rangle}$, we see get that $x = (x - y) + y$ lies in $R[\mathrm{PSL}_2(\mathbb{Z})]_{\langle\sigma\rangle} + R[\mathrm{PSL}_2(\mathbb{Z})]_{\langle\tau\rangle}$, as required.

It remains to prove the exactness at $R[\mathbb{P}^1(\mathbb{Q})]$. The kernel of $R[\mathrm{PSL}_2(\mathbb{Z})] \xrightarrow{g \mapsto 1} R$ is the augmentation ideal, which is generated by all elements of the form $1 - g$ for $g \in \mathrm{PSL}_2(\mathbb{Z})$. Noticing further that we can write

$$1 - \alpha\beta = \alpha(1 - \beta) + (1 - \alpha)$$

for $\alpha, \beta \in \mathrm{PSL}_2(\mathbb{Z})$, the fact that σ and $T = \tau\sigma$ generate $\mathrm{PSL}_2(\mathbb{Z})$ implies that the kernel of $R[\mathrm{PSL}_2(\mathbb{Z})] \xrightarrow{g \mapsto 1} R$ equals

$$R[\mathrm{PSL}_2(\mathbb{Z})](1 - \sigma) + R[\mathrm{PSL}_2(\mathbb{Z})](1 - T)$$

inside $R[\mathrm{PSL}_2(\mathbb{Z})]$. It suffices to take the quotient by $R[\mathrm{PSL}_2(\mathbb{Z})](1 - T)$ to obtain the desired exactness. \square

Lemma 5.2. *The sequence of R -modules*

$$0 \rightarrow \mathcal{M}_R \xrightarrow{\{\alpha, \beta\} \mapsto \beta - \alpha} R[\mathbb{P}^1(\mathbb{Q})] \xrightarrow{\alpha \mapsto 1} R \rightarrow 0$$

is exact.

Proof. Note that, using the relations defining \mathcal{M}_R , any element in \mathcal{M}_R can be written $\sum_{\alpha \neq \infty} r_\alpha \{\infty, \alpha\}$ with $r_\alpha \in R$. This element is mapped to $\sum_{\alpha \neq \infty} r_\alpha \alpha - (\sum_{\alpha \neq \infty} r_\alpha) \infty$. If this expression equals zero, all coefficients r_α have to be zero. This shows the injectivity of the first map.

Let $\sum_\alpha r_\alpha \alpha \in R[\mathbb{P}^1(\mathbb{Q})]$ be an element in the kernel of the second map. Then $\sum_\alpha r_\alpha = 0$, so that we can write

$$\sum_\alpha r_\alpha \alpha = \sum_{\alpha \neq \infty} r_\alpha \alpha - \left(\sum_{\alpha \neq \infty} r_\alpha \right) \infty$$

to obtain an element in the image of the first map. \square

Proposition 5.3. *The homomorphism of R -modules*

$$R[\mathrm{PSL}_2(\mathbb{Z})] \xrightarrow{\phi} \mathcal{M}_R, \quad g \mapsto \{g \cdot 0, g \cdot \infty\}$$

is surjective with kernel $R[\mathrm{PSL}_2(\mathbb{Z})]N_\sigma + R[\mathrm{PSL}_2(\mathbb{Z})]N_\tau$.

Proof. This follows from Proposition 5.1 and Lemma 5.2. \square

We have now provided all the input required to prove the description of modular symbols in terms of Manin symbols. For this we need the notion of an induced module. In homology it plays the role that the coinduced module plays in cohomology.

Definition 5.4. *Let R be a ring, G a group, $H \leq G$ a subgroup and V a left $R[H]$ -module. The induced module of V from H to G is defined as*

$$\mathrm{Ind}_H^G(V) := R[G] \otimes_{R[H]} V,$$

where we view $R[G]$ as a right $R[H]$ -module via the natural action. The induced module is a left $R[G]$ -module via the natural left action of G on $R[G]$.

In case of H having a finite index in G (as in our standard example $\Gamma_1(N) \leq \mathrm{PSL}_2(\mathbb{Z})$), the induced module is isomorphic to the coinduced one:

Lemma 5.5. *Let R be a ring, G a group, $H \leq G$ a subgroup of finite index and V a left $R[H]$ -module.*

- (a) $\mathrm{Ind}_H^G(V)$ and $\mathrm{Coind}_H^G(V)$ are isomorphic as left $R[G]$ -modules.
- (b) Equip $(R[G] \otimes_R V)$ with the diagonal left H -action $h.(g \otimes v) = hg \otimes h.v$ and the right G -action $(g \otimes v).\tilde{g} = g\tilde{g} \otimes v$. Consider the induced module $\mathrm{Ind}_H^G(V)$ as a right $R[G]$ -module by inverting the left action in the definition. Then

$$\mathrm{Ind}_H^G(V) \rightarrow (R[G] \otimes_R V)_H, \quad g \otimes v \mapsto g^{-1} \otimes v$$

is an isomorphism of right $R[G]$ -modules.

Proof. Exercise 5.11. □

Definition 5.6. *Let $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ be a finite index subgroup, V a left $R[\Gamma]$ -module and consider $M = \mathrm{Ind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V)$, which we identify with the right $R[\mathrm{PSL}_2(\mathbb{Z})]$ -module $(R[\mathrm{PSL}_2(\mathbb{Z})] \otimes_R V)_\Gamma$ as in Lemma 5.5 (b).*

Elements in $M/(MN_\sigma + MN_\tau)$ are called Manin symbols over R (for the subgroup $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ and the left $R[\Gamma]$ -module V).

Theorem 5.7. *In the setting of Definition 5.6, the following statements hold:*

- (a) *The homomorphism ϕ from Proposition 5.3 induces the exact sequence of R -modules*

$$0 \rightarrow MN_\sigma + MN_\tau \rightarrow M \rightarrow \mathcal{M}_R(\Gamma, V) \rightarrow 0,$$

and the homomorphism $M \rightarrow \mathcal{M}_R(\Gamma, V)$ is given by $g \otimes v \mapsto \{g.0, g.\infty\} \otimes v$.

In other words, this map induces an isomorphism between Manin symbols over R (for the subgroup $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ and the left $R[\Gamma]$ -module V) and the modular symbols module $\mathcal{M}_R(\Gamma, V)$.

- (b) *The homomorphism $R[\mathrm{PSL}_2(\mathbb{Z})] \rightarrow R[\mathbb{P}^1(\mathbb{Q})]$ sending g to $g.\infty$ induces the exact sequence of R -modules*

$$0 \rightarrow M(1-T) \rightarrow M \rightarrow \mathcal{B}_R(\Gamma, V) \rightarrow 0.$$

- (c) *The identifications of (a) and (b) imply the isomorphism*

$$\mathcal{C}\mathcal{M}_R(\Gamma, V) \cong \ker \left(M/(MN_\sigma + MN_\tau) \xrightarrow{m \mapsto m(1-\sigma)} M/M(1-T) \right).$$

Proof. (a) Proposition 5.3 gives the exact sequence

$$0 \rightarrow R[\mathrm{PSL}_2(\mathbb{Z})]N_\sigma + R[\mathrm{PSL}_2(\mathbb{Z})]N_\tau \rightarrow R[\mathrm{PSL}_2(\mathbb{Z})] \rightarrow \mathcal{M}_R \rightarrow 0,$$

which we tensor with V over R , yielding the exact sequence of left $R[\Gamma]$ -modules

$$0 \rightarrow (R[\mathrm{PSL}_2(\mathbb{Z})] \otimes_R V)N_\sigma + (R[\mathrm{PSL}_2(\mathbb{Z})] \otimes_R V)N_\tau \rightarrow (R[\mathrm{PSL}_2(\mathbb{Z})] \otimes_R V) \rightarrow \mathcal{M}_R(V) \rightarrow 0.$$

Passing to left Γ -coinvariants yields (a) because MN_σ and MN_τ are the images of $(R[\mathrm{PSL}_2(\mathbb{Z})] \otimes_R V)N_\sigma$ and $(R[\mathrm{PSL}_2(\mathbb{Z})] \otimes_R V)N_\tau$ inside M , respectively. (b) is clear from the definition and (c) has already been observed in the proof of Proposition 5.1. \square

In the literature on Manin symbols one usually finds a more explicit version of the induced module. This is the contents of the following proposition. It establishes the link with the main theorem on Manin symbols in [21], namely Theorem 8.4.

Since in the following proposition left and right actions are involved, we sometimes indicate left (co-)invariants by using left subscripts (resp. superscripts) and right (co-)invariants by right ones.

Proposition 5.8. *Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow R^\times$ be a character such that $\chi(-1) = (-1)^k$. Consider the R -module*

$$X := R[\Gamma_1(N) \backslash \mathrm{SL}_2(\mathbb{Z})] \otimes_R V_{k-2}(R) \otimes_R R^\chi$$

equipped with the right $\mathrm{SL}_2(\mathbb{Z})$ -action $(\Gamma_1(N)h \otimes V \otimes r)g = (\Gamma_1(N)hg \otimes g^{-1}v \otimes r)$ and with the left $\Gamma_1(N) \backslash \Gamma_0(N)$ -action $g(\Gamma_1(N)h \otimes v \otimes r) = (\Gamma_1(N)gh \otimes v \otimes \chi(g)r)$.

Then

$$X \cong \mathrm{Ind}_{\Gamma_1(N)}^{\mathrm{SL}_2(\mathbb{Z})}(V_k^\chi(R))$$

as a right $R[\mathrm{SL}_2(\mathbb{Z})]$ -module and a left $R[\Gamma_1(N) \backslash \Gamma_0(N)]$ -module. Moreover,

$$\Gamma_1(N) \backslash \Gamma_0(N) X \cong \mathrm{Ind}_{\Gamma_0(N)}^{\mathrm{SL}_2(\mathbb{Z})}(V_k^\chi(R)).$$

If $N \geq 3$, then the latter module is isomorphic to $\mathrm{Ind}_{\Gamma_0(N)/\{\pm 1\}}^{\mathrm{PSL}_2(\mathbb{Z})}(V_k^\chi(R))$.

Proof. Mapping $g \otimes v \otimes r$ to $g \otimes g^{-1}v \otimes r$ defines an isomorphism of right $R[\mathrm{SL}_2(\mathbb{Z})]$ -modules and of left $R[\Gamma_1(N) \backslash \Gamma_0(N)]$ -modules

$$\Gamma_1(N)(R[\mathrm{SL}_2(\mathbb{Z})] \otimes_R V_{k-2}(R) \otimes_R R^\chi) \rightarrow X.$$

As we have seen above, the left hand side module is naturally isomorphic to the induced module $\mathrm{Ind}_{\Gamma_1(N)}^{\mathrm{SL}_2(\mathbb{Z})}(V_k^\chi(R))$ (equipped with its right $R[\mathrm{SL}_2(\mathbb{Z})]$ -action described before). This establishes the first statement. The second one follows from $\Gamma_1(N) \backslash \Gamma_0(N)(\Gamma_1(N)M) = \Gamma_0(N)M$ for any $\Gamma_0(N)$ -module M . The third statement is due to the fact that $\langle -1 \rangle (R[\mathrm{SL}_2(\mathbb{Z})] \otimes_R V_{k-2}^\chi(R))$ is naturally isomorphic to $R[\mathrm{PSL}_2(\mathbb{Z})] \otimes_R V_{k-2}^\chi(R)$, since -1 acts trivially on the second factor, as the assumption assures that $-1 \in \Gamma_0(N)$ but $-1 \notin \Gamma_1(N)$. \square

For one more description of the induced module $\mathrm{Ind}_{\Gamma_0(N)/\{\pm 1\}}^{\mathrm{PSL}_2(\mathbb{Z})}(V_k^\chi(R))$ see Exercise 5.12. It is this description that uses up the least memory in an implementation. Now all the prerequisites have been provided for implementing Manin symbols (say for $\Gamma_0(N)$ and a character). This is the task of Computer Exercise 5.14.

5.2 Theory: Manin symbols and group cohomology

Let $\Gamma \leq \mathrm{PSL}_2(\mathbb{Z})$ be a subgroup of finite index, and V a left $R[\Gamma]$ -module for a ring R .

Theorem 5.9. *Suppose that the orders of all stabiliser subgroups of Γ for the action on \mathbb{H} are invertible in R . Then we have isomorphisms:*

$$H^1(\Gamma, V) \cong \mathcal{M}_R(\Gamma, V)$$

and

$$H_{\mathrm{par}}^1(\Gamma, V) \cong \mathcal{CM}_R(\Gamma, V).$$

Proof. As before, set $M = \text{Ind}_{\Gamma}^{\text{PSL}_2(\mathbb{Z})}(V)$ and recall that this module is isomorphic to $\text{Coind}_{\Gamma}^{\text{PSL}_2(\mathbb{Z})}(V)$. To see the first statement, in view of Theorem 5.7 and the corollary of the Mayer-Vietoris exact sequence (Corollary 4.12), it suffices to show $M^{(\sigma)} = MN_{\sigma}$ and $M^{(\tau)} = MN_{\tau}$. By the resolution of R for a cyclic group in (3.12), the quotient $M^{(\sigma)}/MN_{\sigma}$ is equal to $H^2(\langle\sigma\rangle, M)$, but this one is zero by the application of Mackey's formula done in Lemma 4.11 (c). The same argument works with τ instead of σ .

The passage to the parabolic/cuspidal subspaces is immediate because the boundary map with source M has the same explicit description in both cases (see Theorem 5.7 (c) and Proposition 4.14). \square

5.3 Algorithms and Implementations: Conversion between Manin and modular symbols

We now use the Euclidean Algorithm to represent any element $g \in \text{PSL}_2(\mathbb{Z})$ in terms of σ and T .

Algorithm 5.10. *Input:* A matrix $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with integer entries and determinant 1.

Output: A list of matrices $[A_1, A_2, \dots, A_n]$ where all $A_i \in \{T^n | n \in \mathbb{Z}\} \cup \{\sigma\}$ and σ and T^n alternate.

- (1) create an empty list output.
- (2) if $|c| > |a|$ then
- (3) append σ to output.
- (4) $M := \sigma M$.
- (5) end if;
- (6) while $c \neq 0$ do
- (7) $q := a \text{ div } c$.
- (8) append T^q to output.
- (9) append σ to output.
- (10) $M := \sigma T^{-q} M$.
- (11) end while;
- (12) if $M \notin \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$ then [At this point $M \in \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & * \\ 0 & -1 \end{pmatrix} \right\}$.]
- (13) append M to output.
- (14) end if;
- (15) return output.

This algorithm gives a constructive proof of the fact (Proposition 4.5) that $\text{PSL}_2(\mathbb{Z})$ is generated by σ and T , and hence also by σ and τ . Note, however, that the algorithm does not necessarily give the shortest such representation. See Exercise 5.13 for a relation to continued fractions.

We can use the algorithm to make a conversion between modular symbols and Manin symbols, as follows. Suppose we are given the modular symbols $\{\alpha, \infty\}$ (this is no loss of generality, as we can represent $\{\alpha, \beta\} = \{\alpha, \infty\} - \{\beta, \infty\}$). Suppose α is given as $g\infty$ with some $g \in \text{SL}_2(\mathbb{Z})$ (i.e. representing the cusp as a fraction $\frac{a}{c}$ with $(a, c) = 1$, then we can find b, d by the Euclidean Algorithm such that $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ satisfies the requirements). We now use Algorithm 5.10 to represent g as $\sigma T^{a_1} \sigma T^{a_2} \sigma \dots T^{a_n} \sigma$ (for example). Then we have

$$\{\alpha, \infty\} = \sigma T^{a_1} \sigma T^{a_2} \sigma \dots T^{a_n} \{0, \infty\} + \sigma T^{a_1} \sigma T^{a_2} \sigma \dots T^{a_{n-1}} \{0, \infty\} + \dots + \sigma T^{a_1} \{0, \infty\} + \{0, \infty\}.$$

If g does not end in σ but T^{a_n} , then we must drop T^{a_n} from the above formula (since T stabilises ∞). If g starts in T^{a_1} (instead of σ), then we must drop the last summand.

Since we are in weight 2 (i.e. trivial module V), the space of Manin symbols is a quotient of $R[\mathrm{PSL}_2(\mathbb{Z})]/\Gamma$ (see Definition 5.6). The Manin symbol corresponding to the above example chosen for the modular symbol $\{\alpha, \infty\}$ is then simply represented by the formal sum

$$\sigma T^{a_1} \sigma T^{a_2} \sigma \dots T^{a_n} + \sigma T^{a_1} \sigma T^{a_2} \sigma \dots T^{a_{n-1}} + \dots + \sigma T^{a_1} + 1. \quad (5.17)$$

If the module V is not trivial, a modular symbol would typically look like $\{\alpha, \infty\} \otimes v$ for $v \in V$ and the corresponding Manin symbol would be the formal sum in (5.17) tensored with v .

In Computer Exercise 5.15 you are asked to implement a conversion between Manin and modular symbols.

5.4 Theoretical exercises

Exercise 5.11. *Prove Lemma 5.5.*

Exercise 5.12. *Assume the set-up of Proposition 5.8. Describe a right $\mathrm{PSL}_2(\mathbb{Z})$ -action on*

$$Y := R[\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})] \otimes_R V_{k-2}(R) \otimes_R R^x$$

and an isomorphism

$$\Gamma_1(N) \backslash \Gamma_0(N) X \rightarrow Y$$

of right $\mathrm{PSL}_2(\mathbb{Z})$ -modules.

Exercise 5.13. *Provide a relationship between Algorithm 5.10 and continued fractions.*

5.5 Computer exercises

Computer Exercise 5.14. *Use the description of Exercise 5.12 and your results from Computer Exercises 4.23 and 4.24 to implement Manin symbols for $\Gamma_0(N)$ and a character over a field. As a first approach you may use the trivial character only.*

Computer Exercise 5.15. (a) *Write an algorithm to represent any element of the group $\mathrm{PSL}_2(\mathbb{Z})$ in terms of σ and T .*

(b) *Write an algorithm that represents any modular symbol $\{\alpha, \beta\}$ as a Manin symbol (inside the vector space created in Computer Exercise 5.14).*

6 Eichler-Shimura

This section is devoted to proving the theorem by Eichler and Shimura that is at the basis of the modular symbols algorithm and its group cohomological variant. The standard reference for the Eichler-Shimura theorem is [20, §8.2]. In the entire section, let $k \geq 2$ be an integer.

6.1 Theory: Petersson scalar product

Recall the standard fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$

$$\mathcal{F} = \{z = x + iy \in \mathbb{H} \mid |z| > 1, |x| < \frac{1}{2}\}$$

from Proposition 4.2. Every subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index has a fundamental domain, for example, $\bigcup_{\gamma \in \bar{\Gamma} \backslash \mathrm{PSL}_2(\mathbb{Z})} \gamma \mathcal{F}$ for any choice of system of representatives of the cosets $\bar{\Gamma} \backslash \mathrm{PSL}_2(\mathbb{Z})$, where we put $\bar{\Gamma} = \Gamma / (\langle \pm 1 \rangle \cap \Gamma)$.

Lemma 6.1. (a) Let $\gamma \in \mathrm{GL}_2(\mathbb{R})^+$ be a real matrix with positive determinant. Let $f \in \mathcal{M}_k(\Gamma; \mathbb{C})$ and $g \in \mathcal{S}_k(\Gamma; \mathbb{C})$. We have with $z \in \mathbb{H}$

$$f(\gamma z) \overline{g(\gamma z)} (\gamma z - \gamma \bar{z})^k = \det(\gamma)^{2-k} f|_{\gamma}(z) \overline{g|_{\gamma}(z)} (z - \bar{z})^k$$

for all $\gamma \in \mathrm{SL}_2(\mathbb{R})$. The function $G(z) := f(z) \overline{g(z)} (z - \bar{z})^k$ is bounded on \mathbb{H} .

(b) We have $d\gamma z = \frac{\det(\gamma)}{(cz+d)^2} dz$ for all $\gamma \in \mathrm{GL}_2(\mathbb{R})^+$.

(c) The differential form $\frac{dz \wedge d\bar{z}}{(z-\bar{z})^2}$ is $\mathrm{GL}_2(\mathbb{R})^+$ -invariant. In terms of $z = x + iy$ we have $\frac{dz \wedge d\bar{z}}{(z-\bar{z})^2} = \frac{i}{2} \frac{dx \wedge dy}{y^2}$.

(d) Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a subgroup with finite index $\mu = (\mathrm{PSL}_2(\mathbb{Z}) : \bar{\Gamma})$. The volume of any fundamental domain \mathcal{F}_{Γ} for Γ with respect to the differential form $\frac{2dz \wedge d\bar{z}}{i(z-\bar{z})^2}$, i.e.

$$\mathrm{vol}(\mathcal{F}_{\Gamma}) = \int_{\mathcal{F}_{\Gamma}} \frac{2dz \wedge d\bar{z}}{i(z-\bar{z})^2},$$

is equal to $\mu \frac{\pi}{3}$.

Proof. (a) The first statement is computed as follows:

$$\begin{aligned} & f(\gamma z) \overline{g(\gamma z)} (\gamma z - \gamma \bar{z})^k \\ &= \det(\gamma)^{2(1-k)} (f|_{\gamma}(z) (cz+d)^k) \overline{(g|_{\gamma}(z) (cz+d)^k)} \left(\frac{az+b}{cz+d} - \frac{a\bar{z}+b}{c\bar{z}+d} \right)^k \\ &= \det(\gamma)^{2-2k} f|_{\gamma}(z) \overline{g|_{\gamma}(z)} ((az+b)(c\bar{z}+d) - (a\bar{z}+b)(cz+d))^k \\ &= \det(\gamma)^{2-k} f|_{\gamma}(z) \overline{g|_{\gamma}(z)} (z - \bar{z})^k, \end{aligned}$$

where we write $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. By the preceding computation, the function $G(z)$ is invariant under $\gamma \in \Gamma$. Hence, it suffices to check that $|G(z)|$ is bounded on the closure of any fundamental domain \mathcal{F}_{Γ} for Γ . For this, it is enough to verify for every γ in a system of representatives of $\Gamma \backslash \mathrm{SL}_2(\mathbb{Z})$ that any of the functions $G(\gamma z)$ is bounded on the closure of the standard fundamental domain \mathcal{F} . By the preceding computation, we also have $G(\gamma z) = f|_{\gamma}(z) \overline{g|_{\gamma}(z)} (z - \bar{z})^k$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Note that $f(z)g(z)$ is a cusp form in $\mathcal{S}_{2k}(\Gamma; \mathbb{C})$, in particular, for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ the function $f|_{\gamma}(z)g|_{\gamma}(z)$ has a Fourier expansion in ∞ of the form $\sum_{n=1}^{\infty} a_n e^{2\pi i z n}$. This series converges absolutely and uniformly on compact subsets of \mathbb{H} , in particular, for any $C > 1$

$$K_{\gamma} := \sum_{n=1}^{\infty} |a_n e^{2\pi i(x+iC)n}| = \sum_{n=1}^{\infty} |a_n| e^{-2\pi C n}$$

is a positive real number, depending on γ (in a system of representatives $\Gamma \backslash \mathrm{SL}_2(\mathbb{Z})$). We have with $z = x + iy$ and $y \geq C$

$$\begin{aligned} |G(\gamma z)| &\leq (2y)^k \sum_{n=1}^{\infty} |a_n| e^{-2\pi y n} = (2y)^k e^{-2\pi y} \sum_{n=1}^{\infty} |a_n| e^{-2\pi y(n-1)} \\ &\leq (2y)^k e^{-2\pi y} \sum_{n=1}^{\infty} |a_n| e^{-2\pi C(n-1)} \\ &\leq (2y)^k e^{-2\pi y} K_{\gamma} e^{2\pi C}. \end{aligned}$$

This tends to 0 if y tends to ∞ . Consequently, the function $G(\gamma z)$ is bounded on the closure of the standard fundamental domain, as desired.

(b) Again writing $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we have

$$\frac{d\gamma z}{dz} = \frac{d \frac{az+b}{cz+d}}{dz} = \frac{1}{(cz+d)^2} (a(cz+d) - (az+b)c) = \frac{\det(\gamma)}{(cz+d)^2},$$

which gives the claim.

(c) This is again a simple computation:

$$\begin{aligned} (\gamma z - \gamma \bar{z})^{-2} d\gamma z \wedge d\gamma \bar{z} &= \det(\gamma)^2 \left(\frac{az+b}{cz+d} - \frac{a\bar{z}+b}{c\bar{z}+d} \right)^{-2} (cz+d)^{-2} (c\bar{z}+d)^{-2} dz \wedge d\bar{z} \\ &= (z - \bar{z})^{-2} dz \wedge d\bar{z}, \end{aligned}$$

using (b). The last statement is

$$\frac{dz \wedge d\bar{z}}{(z - \bar{z})^2} = \frac{(dx + idy) \wedge (dx - idy)}{(2iy)^2} = \frac{-2idx \wedge dy}{-4y^2} = \frac{idx \wedge dy}{2y^2}.$$

(d) Due to the Γ -invariance, it suffices to show

$$\int_{\mathcal{F}} \frac{dz \wedge d\bar{z}}{(z - \bar{z})^2} = \frac{i\pi}{6}.$$

Let $\omega = -\frac{dz}{z - \bar{z}}$. The total derivative of ω is

$$d\omega = ((z - \bar{z})^{-2} dz - (z - \bar{z})^{-2} d\bar{z}) \wedge dz = \frac{dz \wedge d\bar{z}}{(z - \bar{z})^2}.$$

Hence, Stokes' theorem yields

$$\int_{\mathcal{F}} \frac{dz \wedge d\bar{z}}{(z - \bar{z})^2} = - \int_{\partial\mathcal{F}} \frac{dz}{z - \bar{z}},$$

where $\partial\mathcal{F}$ is the positively oriented border of \mathcal{F} , which we describe concretely as the path A from ∞ to ζ_3 on the vertical line, followed by the path C from ζ_3 to ζ_6 on the unit circle and finally followed by $-TA$. Hence with $z = x + iy$ we have

$$\int_{\mathcal{F}} \frac{dz \wedge d\bar{z}}{(z - \bar{z})^2} = -\frac{1}{2i} \left(\int_A \frac{dz}{y} - \int_{TA} \frac{dz}{y} + \int_C \frac{dz}{y} \right) = -\frac{1}{2i} \int_C \frac{dz}{y},$$

since $dz = dTz$. Using the obvious parametrisation of C we obtain

$$\begin{aligned} -\frac{1}{2i} \int_C \frac{dz}{y} &= -\frac{1}{2i} \int_{2\pi/3}^{2\pi/6} \frac{1}{\operatorname{Im}(e^{i\phi})} \frac{de^{i\phi}}{d\phi} d\phi = -\frac{1}{2} \int_{2\pi/3}^{2\pi/6} \frac{e^{i\phi}}{\operatorname{Im}(e^{i\phi})} d\phi \\ &= -\frac{1}{2} \int_{2\pi/3}^{2\pi/6} \left(\frac{\cos(\phi)}{\sin(\phi)} + i \right) d\phi = -\frac{i}{2} \left(\frac{2\pi}{6} - \frac{2\pi}{3} \right) = \frac{i\pi}{6}, \end{aligned}$$

since \sin is symmetric around $\pi/2$ and \cos is antisymmetric, so that the integral over $\frac{\cos(\phi)}{\sin(\phi)}$ cancels. \square

Definition 6.2. Let $\Gamma \leq \operatorname{SL}_2(\mathbb{Z})$ be a subgroup of finite index and $\mu := (\operatorname{PSL}_2(\mathbb{Z}) : \bar{\Gamma})$ be the index of $\bar{\Gamma} = \Gamma / (\langle \pm 1 \rangle \cap \Gamma)$ in $\operatorname{PSL}_2(\mathbb{Z})$. We define the Petersson pairing as

$$\begin{aligned} \operatorname{M}_k(\Gamma; \mathbb{C}) \times \operatorname{S}_k(\Gamma; \mathbb{C}) &\rightarrow \mathbb{C} \\ (f, g) &\mapsto \frac{-1}{(2i)^{k-1} \mu} \int_{\mathcal{F}_\Gamma} f(z) \overline{g(z)} (z - \bar{z})^k \frac{dz \wedge d\bar{z}}{(z - \bar{z})^2} \\ &= \frac{1}{\mu} \int_{\mathcal{F}_\Gamma} f(z) \overline{g(z)} y^{k-2} dx \wedge dy =: (f, g), \end{aligned}$$

where \mathcal{F}_Γ is any fundamental domain for Γ .

Proposition 6.3. (a) The integral in the Petersson pairing converges. It does not depend on the choice of the fundamental domain \mathcal{F}_Γ .

(b) The Petersson pairing is a sesqui-linear pairing (linear in the first and anti-linear in the second variable).

(c) The restriction of the Petersson pairing to $\operatorname{S}_k(\Gamma; \mathbb{C})$ is a positive definite scalar product (the Petersson scalar product).

- (d) If f, g are modular (cusp) forms for the group Γ and $\Gamma' \leq \Gamma$ is a subgroup of finite index, then the Petersson pairing of f and g with respect to Γ gives the same value as the one with respect to Γ' .

Proof. (a) By Lemma 6.1 the integral converges, since the function

$$G(z) := f(z)\overline{g(z)}(z - \bar{z})^k$$

is bounded on \mathcal{F}_Γ and the volume of \mathcal{F}_Γ for the measure in question is finite. The integral does not depend on the choice of the fundamental domain by the invariance of $G(z)$ under Γ .

(b) is clear.

(c) We have

$$(f, f) = \frac{1}{\mu} \int_{\mathcal{F}_\Gamma} |f(z)|^2 y^{k-2} dx \wedge dy,$$

which is clearly non-negative. It is 0 if and only if f is the zero function, showing that the product is positive definite.

(d) If \mathcal{F}_Γ is a fundamental domain for Γ , then $\bigcup_{\gamma \in \Gamma' \setminus \Gamma} \gamma \mathcal{F}_\Gamma$ is a fundamental domain for Γ' (for any choice of representatives of $\Gamma' \setminus \Gamma$). But on every $\gamma \mathcal{F}_\Gamma$ the integral takes the same value. \square

Proposition 6.4. *Let $f, g \in S_k(\Gamma; \mathbb{C})$. We have*

$$(f, g) = \frac{-1}{(2i)^{k-1}\mu} \sum_{\gamma \in \bar{\Gamma} \setminus \text{PSL}_2(\mathbb{Z})} \int_{\zeta_3}^i \int_{-\infty}^0 f|_\gamma(z)\overline{g|_\gamma(z)}(z - \bar{z})^{k-2} dz d\bar{z}.$$

Proof. Let us write for short $G_\gamma(z, \bar{z}) = f|_\gamma(z)\overline{g|_\gamma(z)}(z - \bar{z})^k$ for $\gamma \in \text{SL}_2(\mathbb{Z})$. Then

$$-(2i)^{k-1}\mu(f, g) = \int_{\bigcup_\gamma \gamma \mathcal{F}} G_\gamma(z, \bar{z}) \frac{dz \wedge d\bar{z}}{(z - \bar{z})^2} = \sum_\gamma \int_{\mathcal{F}} G_\gamma(z, \bar{z}) \frac{dz \wedge d\bar{z}}{(z - \bar{z})^2}$$

by Lemma 6.1, where the union resp. sum runs over a fixed system of coset representatives of $\bar{\Gamma} \setminus \text{PSL}_2(\mathbb{Z})$; by our observations, everything is independent of this choice. Consider the differential form

$$\omega_\gamma := \left(\int_{-\infty}^z f|_\gamma(u)(u - \bar{z})^{k-2} du \right) \overline{g|_\gamma(z)} d\bar{z}.$$

Note that the integral converges since f is a cusp form. The total derivative of ω_γ is $d\omega_\gamma = G_\gamma(z, \bar{z}) \frac{dz \wedge d\bar{z}}{(z - \bar{z})^2}$. Consequently, Stokes' theorem gives

$$\sum_\gamma \int_{\mathcal{F}} G_\gamma(z, \bar{z}) \frac{dz \wedge d\bar{z}}{(z - \bar{z})^2} = \sum_\gamma \int_{\partial \mathcal{F}} \left(\int_{-\infty}^z f|_\gamma(u)(u - \bar{z})^{k-2} du \right) \overline{g|_\gamma(z)} d\bar{z},$$

where as above $\partial \mathcal{F}$ is the positively oriented border of the standard fundamental domain \mathcal{F} , which we describe as the path A along the vertical line from ∞ to ζ_3 , followed by the path B from ζ_3 to i along the unit circle, followed by $-\sigma B$ and by $-TA$.

We now make a small calculation. Let for this C be any (piecewise continuously differentiable) path in \mathbb{H} and $M \in \text{SL}_2(\mathbb{Z})$:

$$\begin{aligned} & \int_{MC} \int_{-\infty}^z f|_\gamma(u)\overline{g|_\gamma(z)}(u - \bar{z})^{k-2} dud\bar{z} \\ &= \int_C \int_{-\infty}^{Mz} f|_\gamma(u)\overline{g|_\gamma(Mz)}(u - M\bar{z})^{k-2} du \frac{dM\bar{z}}{d\bar{z}} d\bar{z} \\ &= \int_C \int_{M^{-1}\infty}^z f|_{\gamma M}(u)\overline{g|_{\gamma M}(z)}(u - \bar{z})^{k-2} dud\bar{z} \\ &= \int_C \int_{-\infty}^z f|_{\gamma M}(u)\overline{g|_{\gamma M}(z)}(u - \bar{z})^{k-2} dud\bar{z} - \int_C \int_{-\infty}^{M^{-1}\infty} f|_{\gamma M}(u)\overline{g|_{\gamma M}(z)}(u - \bar{z})^{k-2} dud\bar{z}. \end{aligned}$$

This gives

$$\int_{C-MC} \int_{\infty}^z f|_{\gamma}(u)\overline{g|_{\gamma}(z)}(u-\bar{z})^{k-2}dud\bar{z} = \int_C \int_{\infty}^z (G_{\gamma}(u, \bar{z}) - G_{\gamma M}(u, \bar{z}))dud\bar{z} + \int_C \int_{\infty}^{M^{-1}\infty} G_{\gamma M}(u, \bar{z})dud\bar{z}.$$

Continuing with the main calculation, we have

$$\begin{aligned} & - (2i)^{k-1}\mu(f, g) \\ &= \sum_{\gamma} \left[\int_A \int_{\infty}^z (G_{\gamma}(u, \bar{z}) - G_{\gamma T}(u, \bar{z}))dud\bar{z} + \int_A \int_{\infty}^{T^{-1}\infty} G_{\gamma T}(u, \bar{z})dud\bar{z} \right] \\ &+ \sum_{\gamma} \left[\int_B \int_{\infty}^z (G_{\gamma}(u, \bar{z}) - G_{\gamma\sigma}(u, \bar{z}))dud\bar{z} + \int_B \int_{\infty}^{\sigma^{-1}\infty} G_{\gamma\sigma}(u, \bar{z})dud\bar{z} \right] \\ &= \sum_{\gamma} \int_B \int_{\infty}^0 G_{\gamma\sigma}(u, \bar{z})dud\bar{z}, \end{aligned}$$

using $T^{-1}\infty = \infty$, $\sigma^{-1}\infty = 0$ and the fact that the γT and $\gamma\sigma$ are just permutations of the cosets. \square

6.2 Theory: The Eichler-Shimura map

Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a subgroup of finite index. We fix some $z_0 \in \mathbb{H}$. For $f \in M_k(\Gamma; \mathbb{C})$ with $k \geq 2$ and γ, δ in $\mathbb{Z}^{2 \times 2}$ with positive determinant, let

$$I_f(\gamma z_0, \delta z_0) := \int_{\gamma z_0}^{\delta z_0} f(z)(Xz + Y)^{k-2}dz \in V_{k-2}(\mathbb{C}).$$

The integral is to be taken coefficient wise. Note that it is independent of the chosen path since we are integrating holomorphic functions.

Lemma 6.5. *For any $z_0 \in \mathbb{H}$ and any matrices $\gamma, \delta \in \mathbb{Z}^{2 \times 2}$ with positive determinant we have*

$$I_f(z_0, \gamma\delta z_0) = I_f(z_0, \gamma z_0) + I_f(\gamma z_0, \gamma\delta z_0)$$

and

$$I_f(\gamma z_0, \gamma\delta z_0) = \det(\gamma)^{2-k}(\gamma \cdot (I_{f|_{\gamma}}(z_0, \delta z_0))) = (\det(\gamma)^{-1}\gamma) \cdot (I_{f|_{\gamma}}(z_0, \delta z_0)).$$

Proof. The first statement is clear. Write $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Recall that by Lemma 6.1 (b), we have $d\gamma z = \frac{\det(\gamma)}{(cz+d)^2}dz$. We compute further

$$\begin{aligned} I_f(\gamma z_0, \gamma\delta z_0) &= \int_{\gamma z_0}^{\gamma\delta z_0} f(z)(Xz + Y)^{k-2}dz \\ &= \int_{z_0}^{\delta z_0} f(\gamma z)(X\gamma z + Y)^{k-2}\frac{d\gamma z}{dz}dz \\ &= \det(\gamma)^{2-k} \int_{z_0}^{\delta z_0} f|_{\gamma}(z)(cz + d)^{k-2}\left(X\frac{az + b}{cz + d} + Y\right)^{k-2}dz \\ &= \det(\gamma)^{2-k} \int_{z_0}^{\delta z_0} f|_{\gamma}(z)(X(az + b) + Y(cz + d))^{k-2}dz \\ &= \det(\gamma)^{2-k} \int_{z_0}^{\delta z_0} f|_{\gamma}(z)((Xa + Yc)z + (Xb + Yd))^{k-2}dz \\ &= \det(\gamma)^{2-k} \int_{z_0}^{\delta z_0} f|_{\gamma}(z)(\gamma \cdot (Xz + Y))^{k-2}dz \\ &= \det(\gamma)^{2-k} \cdot \gamma \cdot \left(\int_{z_0}^{\delta z_0} f|_{\gamma}(z)(Xz + Y)^{k-2}dz \right) \\ &= \det(\gamma)^{2-k} \cdot \gamma \cdot (I_{f|_{\gamma}}(z_0, \delta z_0)). \end{aligned}$$

We recall that for a polynomial $P(X, Y)$ we have the action

$$(g.P)(X, Y) = P((X, Y) \begin{pmatrix} a & b \\ c & d \end{pmatrix}) = P(Xa + Yc, Xb + Yd).$$

□

Definition 6.6. *The space of antiholomorphic cusp forms $\overline{S_k(\Gamma; \mathbb{C})}$ consists of the functions $z \mapsto \overline{f(z)} := \overline{f(z)}$ with $f \in S_k(\Gamma; \mathbb{C})$.*

We can consider an antiholomorphic cusp form as a power series in \bar{z} . For instance, if $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$, then $\overline{f(z)} = \sum_{n=1}^{\infty} \overline{a_n} e^{2\pi i n (-\bar{z})} = \tilde{f}(-\bar{z})$, where $\tilde{f}(z) = \sum_{n=1}^{\infty} \overline{a_n} e^{2\pi i n z}$. Note that

$$\int_{\alpha} \overline{F(z)} d\bar{z} = \int_0^1 \overline{F(\alpha(t))} \frac{d\bar{\alpha}}{dt} dt = \int_0^1 \overline{F(\alpha(t))} \frac{d\bar{\alpha}}{dt} dt = \overline{\int_0^1 F(\alpha(t)) \frac{d\alpha}{dt} dt} = \overline{\int_{\alpha} F(z) dz} \quad (6.18)$$

for any piecewise analytic path $\alpha : [0, 1] \rightarrow \mathbb{C}$ and any integrable complex valued function F . This means for $f \in S_k(\Gamma; \mathbb{C})$:

$$\overline{I_f(\gamma z_0, \delta z_0)} = \int_{\gamma z_0}^{\delta z_0} \overline{f(z)} (X\bar{z} + Y)^{k-2} d\bar{z} \in V_{k-2}(\mathbb{C}).$$

Proposition 6.7. *Let $k \geq 2$ and $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a subgroup of finite index and fix $z_0, z_1 \in \mathbb{H}$.*

(a) *The Eichler-Shimura map*

$$\begin{aligned} M_k(\Gamma; \mathbb{C}) \oplus \overline{S_k(\Gamma; \mathbb{C})} &\rightarrow H^1(\Gamma, V_{k-2}(\mathbb{C})), \\ (f, \bar{g}) &\mapsto (\gamma \mapsto I_f(z_0, \gamma z_0) + \overline{I_g(z_1, \gamma z_1)}) \end{aligned}$$

is a well-defined homomorphism of \mathbb{C} -vector spaces. It does not depend on the choice of z_0 and z_1 .

(b) *The induced Eichler-Shimura map*

$$\begin{aligned} M_k(\Gamma; \mathbb{C}) \oplus \overline{S_k(\Gamma; \mathbb{C})} &\rightarrow H^1(\mathrm{SL}_2(\mathbb{Z}), \mathrm{Hom}_{\mathbb{C}[\Gamma]}(\mathbb{C}[\mathrm{SL}_2(\mathbb{Z})], V_{k-2}(\mathbb{C}))), \\ (f, \bar{g}) &\mapsto (a \mapsto (b \mapsto I_f(bz_0, baz_0) + \overline{I_g(bz_1, baz_1)})) \end{aligned}$$

is a well-defined homomorphism of \mathbb{C} -vector spaces. It does not depend on the choice of z_0 and z_1 .

Via the map from Shapiro's lemma, this homomorphism coincides with the one from (a).

Proof. (a) For checking that the map is well-defined, it suffices to compute that $\gamma \mapsto I_f(z_0, \gamma z_0)$ is a 1-cocycle:

$$I_f(z_0, \gamma \delta z_0) = I_f(z_0, \gamma z_0) + I_f(\gamma z_0, \gamma \delta z_0) = I_f(z_0, \gamma z_0) + \gamma \cdot I_f(z_0, \delta z_0),$$

using Lemma 6.5 and $f|_{\gamma} = f$ since $\gamma \in \Gamma$.

The independence of the base point is seen as follows. Let \tilde{z}_0 be any base point.

$$I_f(\tilde{z}_0, \gamma \tilde{z}_0) = I_f(\tilde{z}_0, z_0) + I_f(z_0, \gamma z_0) + I_f(\gamma z_0, \gamma \tilde{z}_0) = I_f(z_0, \gamma z_0) + (1 - \gamma) I_f(\tilde{z}_0, z_0).$$

The difference of the cocycles $(\gamma \mapsto I_f(\tilde{z}_0, \gamma \tilde{z}_0))$ and $(\gamma \mapsto I_f(z_0, \gamma z_0))$ is hence the coboundary $(\gamma \mapsto (1 - \gamma) I_f(\tilde{z}_0, z_0))$.

(b) We first check that the map $(b \mapsto I_f(bz_0, baz_0) + \overline{I_g(bz_1, baz_1)})$ is indeed in the coinduced module $\mathrm{Hom}_{\mathbb{C}[\Gamma]}(\mathbb{C}[\mathrm{SL}_2(\mathbb{Z})], V_{k-2}(\mathbb{C}))$. For that let $\gamma \in \Gamma$. We have

$$I_f(\gamma bz_0, \gamma baz_0) = \gamma \cdot (I_f(bz_0, baz_0))$$

by Lemma 6.5, as desired. The map $\phi(a) := (b \mapsto I_f(bz_0, baz_0) + \overline{I_g(bz_1, baz_1)})$ is a cocycle:

$$\begin{aligned} \phi(a_1 a_2)(b) &= I_f(bz_0, ba_1 a_2 z_0) + \overline{I_g(bz_1, ba_1 a_2 z_1)} \\ &= I_f(bz_0, ba_1 z_0) + I_f(ba_1 z_0, ba_1 a_2 z_0) + \overline{I_g(bz_1, ba_1 z_1)} + \overline{I_g(ba_1 z_1, ba_1 a_2 z_1)} \\ &= \phi(a_1)(b) + \phi(a_2)(ba_1) = \phi(a_1)(b) + (a_1 \cdot \phi(a_2))(b), \end{aligned}$$

by the definition of the left action of $\mathrm{SL}_2(\mathbb{Z})$ on the coinduced module. Note that the map in Shapiro's lemma in our situation is given by

$$\phi \mapsto (\gamma \mapsto \phi(\gamma)(1) = I_f(z_0, \gamma z_0) + \overline{I_g(z_1, \gamma z_1)}),$$

which shows that the maps from (a) and (b) coincide. The independence from the base point in (b) now follows from the independence in (a). \square

Next we identify the cohomology of $\mathrm{SL}_2(\mathbb{Z})$ with the one of $\mathrm{PSL}_2(\mathbb{Z})$.

Proposition 6.8. *Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a subgroup of finite index and let R be a ring in which 2 is invertible. Let V be a left $R[\Gamma]$ -module. Assume that either $-1 \notin \Gamma$ or $-1 \in \Gamma$ acts trivially on V . Then the inflation map*

$$\mathrm{H}^1(\mathrm{PSL}_2(\mathbb{Z}), \mathrm{Hom}_{R[\overline{\Gamma}]}(R[\mathrm{PSL}_2(\mathbb{Z})], V)) \xrightarrow{\mathrm{infl}} \mathrm{H}^1(\mathrm{SL}_2(\mathbb{Z}), \mathrm{Hom}_{R[\Gamma]}(R[\mathrm{SL}_2(\mathbb{Z})], V))$$

is an isomorphism. We shall identify these two R -modules from now on.

Proof. If $-1 \notin \Gamma$, then $\Gamma \cong \overline{\Gamma}$ and $\mathrm{Hom}_{R[\Gamma]}(R[\mathrm{SL}_2(\mathbb{Z})], V)^{\langle -1 \rangle}$ consists of all the functions satisfying $f(g) = f(-g)$ for all $g \in \mathrm{SL}_2(\mathbb{Z})$, which are precisely the functions in $\mathrm{Hom}_{R[\overline{\Gamma}]}(R[\mathrm{PSL}_2(\mathbb{Z})], V)$.

If $-1 \in \Gamma$ and -1 acts trivially on V , then $f(-g) = (-1).f(g) = f(g)$ and so -1 already acts trivially on $\mathrm{Hom}_{R[\Gamma]}(R[\mathrm{SL}_2(\mathbb{Z})], V)$. This $R[\mathrm{SL}_2(\mathbb{Z})]$ -module is then naturally isomorphic to $\mathrm{Hom}_{R[\overline{\Gamma}]}(R[\mathrm{PSL}_2(\mathbb{Z})], V)$ since any function is uniquely determined on its classes modulo $\langle -1 \rangle$.

Due to the invertibility of 2, the Hochschild-Serre exact sequence (Theorem 3.27) shows that inflation indeed gives the desired isomorphism because the third term $\mathrm{H}^1(\langle \pm 1 \rangle, \mathrm{Hom}_{R[\Gamma]}(R[\mathrm{SL}_2(\mathbb{Z})], V))$ in the inflation-restriction sequence is zero (see Proposition 3.26). \square

Proposition 6.9. *The kernel of the Eichler-Shimura map composed with the restriction*

$$\mathrm{M}_k(\Gamma; \mathbb{C}) \oplus \overline{\mathrm{S}_k(\Gamma; \mathbb{C})} \rightarrow \mathrm{H}^1(\Gamma, V_{k-2}(\mathbb{C})) \rightarrow \prod_{c \in \Gamma \backslash \mathbb{P}^1(\mathbb{Q})} \mathrm{H}^1(\Gamma_c, V_{k-2}(\mathbb{C}))$$

is equal to $\mathrm{S}_k(\Gamma; \mathbb{C}) \oplus \overline{\mathrm{S}_k(\Gamma; \mathbb{C})}$. In particular, the image of $\mathrm{S}_k(\Gamma; \mathbb{C}) \oplus \overline{\mathrm{S}_k(\Gamma; \mathbb{C})}$ under the Eichler-Shimura map lies in the parabolic cohomology $\mathrm{H}_{\mathrm{par}}^1(\Gamma, V_{k-2}(\mathbb{C}))$.

Proof. In order to simplify the notation of the proof, we shall only prove the case of a modular form $f \in \mathrm{M}_k(\Gamma; \mathbb{C})$. The statement for anti-holomorphic forms is proved in the same way. The composition maps the modular form f to the 1-cocycle (for $\gamma \in \Gamma_c$)

$$\gamma \mapsto \int_{z_0}^{\gamma z_0} f(z)(Xz + Y)^{k-2} dz$$

with a fixed base point $z_0 \in \mathbb{H}$. The aim is now to move the base point to the cusps. We cannot just replace z_0 by ∞ , as then the integral might not converge any more (it converges on cusp forms). Let $c = M\infty$ be any cusp with $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. We then have $\Gamma_c = \langle MTM^{-1} \rangle \cap \Gamma = \langle MT^r M^{-1} \rangle$ for some $r \geq 1$. Since f is holomorphic in the cusps, we have

$$f|_M(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n/rz} = a_0 + g(z)$$

and thus

$$f(z) = a_0|_{M^{-1}}(z) + g|_{M^{-1}}(z) = \frac{a_0}{(-cz + a)^k} + g|_{M^{-1}}(z).$$

Now we compute the cocycle evaluated at $\gamma = MT^r M^{-1}$:

$$\int_{z_0}^{\gamma z_0} f(z)(Xz + Y)^{k-2} dz = a_0 \int_{z_0}^{\gamma z_0} \frac{(Xz + Y)^{k-2}}{(-cz + a)^k} dz + \int_{z_0}^{\gamma z_0} g|_{M^{-1}}(z)(Xz + Y)^{k-2} dz.$$

Before we continue by evaluating the right summand, we remark that the integral

$$I_{g|_{M^{-1}}}(z_0, M^\infty) = \int_{z_0}^{M^\infty} g|_{M^{-1}}(z)(Xz + Y)^{k-2} dz = M \cdot \int_{M^{-1}z_0}^{\infty} g(z)(Xz + Y)^{k-2} dz$$

converges. We have

$$\begin{aligned} \int_{z_0}^{\gamma z_0} g|_{M^{-1}}(z)(Xz + Y)^{k-2} dz &= \left(\int_{z_0}^{M^\infty} + \int_{\gamma M^\infty}^{\gamma z_0} \right) g|_{M^{-1}}(z)(Xz + Y)^{k-2} dz \\ &= (1 - \gamma) \cdot \int_{z_0}^{M^\infty} g|_{M^{-1}}(z)(Xz + Y)^{k-2} dz \end{aligned}$$

since $g|_{M^{-1}\gamma}(z) = g|_{T^r M^{-1}}(z) = g|_{M^{-1}}(z)$. The 1-cocycle $\gamma \mapsto \int_{z_0}^{\gamma z_0} g|_{M^{-1}}(z)(Xz + Y)^{k-2} dz$ is thus a 1-coboundary. Consequently, the class of the image of f is equal to the class of the 1-cocycle

$$\gamma \mapsto a_0 \int_{z_0}^{\gamma z_0} \frac{(Xz + Y)^{k-2}}{(-cz + a)^k} dz.$$

We have the isomorphism (as always for cyclic groups)

$$H^1(\Gamma_c, V_{k-2}(\mathbb{C})) \xrightarrow{\phi \mapsto \phi(MT^r M^{-1})} V_{k-2}(\mathbb{C})_{\Gamma_c}.$$

Furthermore, we have the isomorphism

$$V_{k-2}(\mathbb{C})_{\Gamma_c} \xrightarrow{P \mapsto M^{-1}P} V_{k-2}(\mathbb{C})_{\langle T^r \rangle} \xrightarrow{P \mapsto P(0,1)} \mathbb{C}$$

with polynomials $P(X, Y)$. Note that the last map is an isomorphism by the explicit description of $V_{k-2}(\mathbb{C})_{\langle T^r \rangle}$. Under the composition the image of the cocycle coming from the modular form f is

$$\begin{aligned} a_0 M^{-1} \cdot \int_{z_0}^{\gamma z_0} \frac{(Xz + Y)^{k-2}}{(-cz + a)^k} dz(0, 1) &= a_0 \int_{z_0}^{\gamma z_0} \frac{(Xz + Y)^{k-2}}{(-cz + a)^k} dz(-c, a) \\ &= a_0 \int_{z_0}^{\gamma z_0} \frac{1}{(-cz + a)^2} dz = a_0 \int_{M^{-1}z_0}^{T^r M^{-1}z_0} dz = a_0(M^{-1}z_0 + r - M^{-1}z_0) = ra_0, \end{aligned}$$

as $(0, 1)M^{-1} = (0, 1) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = (-c, a)$. This expression is zero if and only if $a_0 = 0$, i.e. if and only if f vanishes at the cusp c .

A similar argument works for anti-holomorphic cusp forms. □

6.3 Theory: Cup product and Petersson scalar product

This part owes much to the treatment of the Petersson scalar product by Haberland in [14] (see also [5, §12]).

Definition 6.10. *Let G be a group and M and N be two left $R[G]$ -modules. We equip $M \otimes_R N$ with the diagonal left $R[G]$ -action. Let $m, n \geq 0$. Then we define the cup product*

$$\cup : H^n(G, M) \otimes_R H^m(G, N) \rightarrow H^{n+m}(G, M \otimes_R N)$$

by

$$\phi \cup \psi := ((g_1, \dots, g_n, g_{n+1}, \dots, g_{n+m}) \mapsto \phi(g_1, \dots, g_n) \otimes (g_1 \cdots g_n) \cdot \psi(g_{n+1}, \dots, g_{n+m}))$$

on cochains of the bar resolution.

This description can be derived easily from the natural one on the standard resolution. For instance, [4, §5.3] gives the above formula up to a sign (which does not matter in our application anyway because we work in fixed degree). In Exercise 6.17 it is checked that the cup product is well-defined.

Lemma 6.11. *Keep the notation of Definition 6.10 and let $\phi \in H^n(G, M)$ and $\psi \in H^m(G, N)$. Then*

$$\phi \cup \psi = (-1)^{mn} \psi \cup \phi$$

via the natural isomorphism $M \otimes_R N \cong N \otimes_R M$.

Proof. Exercise 6.18. □

We are now going to formulate a pairing on cohomology, which will turn out to be a version of the Petersson scalar product. We could introduce compactly supported cohomology for writing it in more conceptual terms, but have decided not to do this in order not to increase the amount of new material even more.

Definition 6.12. *Let M be an $R[\mathrm{PSL}_2(\mathbb{Z})]$ -module. The parabolic 1-cocycles are defined as*

$$Z_{\mathrm{par}}^1(\Gamma, M) = \ker(Z^1(\Gamma, M) \xrightarrow{\mathrm{res}} \prod_{g \in \Gamma \backslash \mathrm{PSL}_2(\mathbb{Z}) / \langle T \rangle} Z^1(\Gamma \cap \langle gTg^{-1} \rangle, M)).$$

Proposition 6.13. *Let R be a ring in which 6 is invertible. Let M and N be left $R[\mathrm{PSL}_2(\mathbb{Z})]$ -modules together with a $R[\mathrm{PSL}_2(\mathbb{Z})]$ -module homomorphism $\pi : M \otimes_R N \rightarrow R$ where we equip $M \otimes_R N$ with the diagonal action. Write G for $\mathrm{PSL}_2(\mathbb{Z})$. We define a pairing*

$$\langle \cdot, \cdot \rangle : Z^1(G, M) \times Z^1(G, N) \rightarrow R$$

as follows: Let (ϕ, ψ) be a pair of 1-cocycles. Form their cup product $\rho := \pi_*(\phi \cup \psi)$ in $Z^2(G, R)$ via $Z^2(G, M \otimes_R N) \xrightarrow{\pi_*} Z^2(G, R)$. As $H^2(G, R)$ is zero (Corollary 4.12), ρ must be a 2-coboundary, i.e. there is $a : G \rightarrow R$ (depending on (ϕ, ψ)) such that

$$\rho(g, h) = \pi(\phi(g) \otimes g.\psi(h)) = a(h) - a(gh) + a(g).$$

We define the pairing by

$$\langle \phi, \psi \rangle := a(T).$$

(a) *The pairing is well-defined and bilinear. It can be expressed as*

$$\langle \phi, \psi \rangle = -\rho(\tau, \sigma) + \frac{1}{2}\rho(\sigma, \sigma) + \frac{1}{3}(\rho(\tau, \tau) + \rho(\tau, \tau^2)).$$

(b) *If $\phi \in Z_{\mathrm{par}}^1(G, M)$, then $\rho(\tau, \sigma) = \rho(\sigma, \sigma)$ and*

$$\langle \phi, \psi \rangle = -\frac{1}{2}\rho(\sigma, \sigma) + \frac{1}{3}(\rho(\tau, \tau) + \rho(\tau, \tau^2)).$$

Moreover, $\langle \phi, \psi \rangle$ only depends on the class of ψ in $H^1(G, N)$.

(c) *If $\psi \in Z_{\mathrm{par}}^1(G, N)$, then $\rho(\tau, \sigma) = \rho(\tau, \tau^2)$ and*

$$\langle \phi, \psi \rangle = \frac{1}{2}\rho(\sigma, \sigma) + \frac{1}{3}\rho(\tau, \tau) - \frac{2}{3}\rho(\tau, \tau^2).$$

Moreover, $\langle \phi, \psi \rangle$ only depends on the class of ϕ in $H^1(G, M)$.

(d) *If $\phi \in Z_{\mathrm{par}}^1(G, M)$ and $\psi \in Z_{\mathrm{par}}^1(G, N)$, then $\rho(\sigma, \sigma) = \rho(\tau, \tau^2)$ and*

$$\langle \phi, \psi \rangle = -\frac{1}{6}\rho(\sigma, \sigma) + \frac{1}{3}\rho(\tau, \tau).$$

Proof. (a) We first have

$$0 = \pi(\phi(1) \otimes \psi(1)) = \rho(1, 1) = a(1) - a(1) + a(1) = a(1),$$

since ϕ and ψ are 1-cocycles. Recall that the value of a 1-cocycle at 1 is always 0 due to $\phi(1) = \phi(1 \cdot 1) = \phi(1) + \phi(1)$. Furthermore, we have

$$\begin{aligned}\rho(\tau, \sigma) &= a(\sigma) - a(T) + a(\tau) \\ \rho(\sigma, \sigma) &= a(\sigma) - a(1) + a(\sigma) = 2a(\sigma) \\ \rho(\tau, \tau^2) &= a(\tau^2) - a(1) + a(\tau) = a(\tau) + a(\tau^2) \\ \rho(\tau, \tau) &= a(\tau) - a(\tau^2) + a(\tau) = 2a(\tau) - a(\tau^2)\end{aligned}$$

Hence, we get $a(T) = -\rho(\tau, \sigma) + a(\sigma) + a(\tau)$ and $a(\sigma) = \frac{1}{2}\rho(\sigma, \sigma)$ as well as $a(\tau) = \frac{1}{3}(\rho(\tau, \tau) + \rho(\tau, \tau^2))$, from which the claimed formula follows. The formula also shows the independence of the choice of a and the bilinearity.

(b) Now assume $\phi(T) = 0$. Using $T = \tau\sigma$ we obtain

$$\begin{aligned}\rho(\tau, \sigma) &= \pi(\phi(\tau) \otimes \tau\psi(\sigma)) = -\pi(\tau.\phi(\sigma) \otimes \tau\psi(\sigma)) \\ &= -\pi(\phi(\sigma) \otimes \psi(\sigma)) = \pi((\phi(\sigma) \otimes \sigma\psi(\sigma))) = \rho(\sigma, \sigma)\end{aligned}$$

because $0 = \phi(T) = \phi(\tau\sigma) = \tau.\phi(\sigma) + \phi(\tau)$ and $0 = \psi(1) = \psi(\sigma^2) = \sigma.\psi(\sigma) + \psi(\sigma)$. This yields the formula.

We now show that the pairing does not depend on the choice of 1-cocycle in the class of ψ . To see this, let $\psi(g) = (g-1)n$ with $n \in N$ be a 1-coboundary. Put $b(g) := \pi(-\phi(g) \otimes gn)$. Then, using $\phi(gh) = g(\phi(h)) + \phi(g)$, one immediately checks the equality

$$\rho(g, h) = \pi(\phi(g) \otimes g(h-1)n) = g.b(h) - b(gh) + b(g).$$

Hence, (ϕ, ψ) is mapped to $b(T) = \pi(-\phi(T) \otimes Tn) = \pi(0 \otimes Tn) = 0$.

(c) Let now $\psi(T) = 0$. Then $0 = \psi(T) = \psi(\tau\sigma) = \tau\psi(\sigma) + \psi(\tau)$ and $0 = \psi(\tau^3) = \tau\psi(\tau^2) + \psi(\tau)$, whence $\tau\psi(\tau^2) = \tau\psi(\sigma)$. Consequently,

$$\rho(\tau, \sigma) = \pi(\phi(\tau) \otimes \tau\psi(\sigma)) = \pi(\phi(\tau) \otimes \tau\psi(\tau^2)) = \rho(\tau, \tau^2),$$

implying the formula.

The pairing does not depend on the choice of 1-cocycle in the class of ϕ . Let $\phi(g) = (g-1)m$ be a 1-coboundary and put $c(g) := \pi(m \otimes \psi(g))$. Then the equality

$$\rho(g, h) = \pi((g-1)m \otimes g\psi(h)) = g.c(h) - c(gh) + c(g)$$

holds. Hence, (ϕ, ψ) is mapped to $c(T) = \pi(m \otimes \psi(T)) = \pi(m \otimes 0) = 0$.

(d) Suppose now that $\phi(T) = 0 = \psi(T)$, then by what we have just seen

$$\rho(\tau, \sigma) = \rho(\sigma, \sigma) = \rho(\tau, \tau^2).$$

This implies the claimed formula. □

Our next aim is to specialise this pairing to the cocycles coming from modular forms under the Eichler-Shimura map. We must first define a pairing on the modules used in the cohomology groups.

On the modules $\text{Sym}^{k-2}(R^2)$ we now define the *symplectic pairing* over any ring R in which $(k-2)!$ is invertible. Let $n = k-2$ for simplicity. The pairing for $n = 0$ is just the multiplication on R . We now define the pairing for $n = 1$ as

$$R^2 \times R^2 \rightarrow R, \quad \begin{pmatrix} a \\ c \end{pmatrix} \bullet \begin{pmatrix} b \\ d \end{pmatrix} := \det \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

For any $g \in \text{SL}_2(\mathbb{Z})$ we have

$$g \begin{pmatrix} a \\ c \end{pmatrix} \bullet g \begin{pmatrix} b \\ d \end{pmatrix} = \det g \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix} \bullet \begin{pmatrix} b \\ d \end{pmatrix}.$$

As the next step, we define a pairing on the n -th tensor power of R^2

$$(R^2 \otimes_R \cdots \otimes_R R^2) \times (R^2 \otimes_R \cdots \otimes_R R^2) \rightarrow R$$

by

$$\left(\begin{pmatrix} a_1 \\ c_1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} a_n \\ c_n \end{pmatrix} \right) \bullet \left(\begin{pmatrix} b_1 \\ d_1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} b_n \\ d_n \end{pmatrix} \right) := \prod_{i=1}^n \begin{pmatrix} a_i \\ c_i \end{pmatrix} \bullet \begin{pmatrix} b_i \\ d_i \end{pmatrix}.$$

This pairing is still invariant under the $\mathrm{SL}_2(\mathbb{Z})$ -action.

Now we use the assumption on the invertibility of $n!$ in order to embed $\mathrm{Sym}^n(R^2)$ as an $R[S_n]$ -module in the n -th tensor power, where the action of the symmetric group S_n is on the indices. We have that the map (in fact, $1/n!$ times the norm)

$$\mathrm{Sym}^n(R^2) \rightarrow R^2 \otimes_R \cdots \otimes_R R^2, \quad \left[\begin{pmatrix} a_1 \\ c_1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} a_n \\ c_n \end{pmatrix} \right] \mapsto \frac{1}{n!} \sum_{\sigma \in S_n} \begin{pmatrix} a_{\sigma(1)} \\ c_{\sigma(1)} \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} a_{\sigma(n)} \\ c_{\sigma(n)} \end{pmatrix}$$

is injective (one can use Tate cohomology groups to see this) as the order of S_n is invertible in the ring.

Finally, we define the pairing on $\mathrm{Sym}^n(R^2)$ as the restriction of the pairing on the n -th tensor power to the image of $\mathrm{Sym}^n(R^2)$ under the embedding that we just described. This pairing is, of course, still $\mathrm{SL}_2(\mathbb{Z})$ -invariant.

We point to the important special case

$$\begin{pmatrix} a \\ c \end{pmatrix}^{\otimes(k-2)} \bullet \begin{pmatrix} b \\ d \end{pmatrix}^{\otimes(k-2)} = (ad - bc)^{k-2}.$$

Hence, after the identification $\mathrm{Sym}^{k-2}(R^2) \cong V_{k-2}(R)$ from Exercise 1.31, the resulting pairing on $V_{k-2}(R)$ has the property

$$(aX + cY)^{k-2} \bullet (bX + dY)^{k-2} \mapsto (ad - bc)^{k-2}.$$

This pairing extends to a pairing on coinduced modules

$$\pi : \mathrm{Hom}_{R[\Gamma]}(R[\mathrm{PSL}_2(\mathbb{Z})], V_{k-2}(R)) \otimes_R \mathrm{Hom}_{R[\Gamma]}(R[\mathrm{PSL}_2(\mathbb{Z})], V_{k-2}(R)) \rightarrow R \quad (6.19)$$

by mapping (α, β) to $\sum_{\gamma \in \Gamma \backslash \mathrm{PSL}_2(\mathbb{Z})} \alpha(\gamma) \bullet \beta(\gamma)$.

Proposition 6.14. *Let $k \geq 2$. Assume $-1 \notin \Gamma$ (whence we view Γ as a subgroup of $\mathrm{PSL}_2(\mathbb{Z})$). Let $f, g \in S_k(\Gamma; \mathbb{C})$ be cusp forms. Denote by ϕ_f the 1-cocycle associated with f under the Eichler-Shimura map for the base point $z_0 = \infty$, i.e.*

$$\phi_f(a) = (b \mapsto I_f(b\infty, ba\infty)) \in Z^1(\mathrm{PSL}_2(\mathbb{Z}), \mathrm{Coind}_{\Gamma}^{\mathrm{PSL}_2(\mathbb{Z})}(V_{k-2}(\mathbb{C}))).$$

Further denote

$$\overline{\phi_f}(a) = (b \mapsto \overline{I_f(b\infty, ba\infty)}) \in Z^1(\mathrm{PSL}_2(\mathbb{Z}), \mathrm{Coind}_{\Gamma}^{\mathrm{PSL}_2(\mathbb{Z})}(V_{k-2}(\mathbb{C}))).$$

Similarly, denote by ψ_g the 1-cocycle associated with g for the base point $z_1 = \zeta_6$. Define a bilinear pairing as in Proposition 6.13

$$\langle \cdot, \cdot \rangle : (Z^1(\mathrm{PSL}_2(\mathbb{Z}), \mathrm{Coind}_{\Gamma}^{\mathrm{PSL}_2(\mathbb{Z})}(V_{k-2}(\mathbb{C}))))^2 \rightarrow \mathbb{C}$$

with the product on the coinduced modules described in (6.19). Then the equation

$$\langle \phi_f, \overline{\psi_g} \rangle = (2i)^{k-1} \mu(f, g)$$

holds where (f, g) denotes the Petersson scalar product and μ the index of Γ in $\mathrm{PSL}_2(\mathbb{Z})$.

Proof. Note that the choice of base point ∞ is on the one hand well-defined (the integral converges, as it is taken over a cusp form) and on the other hand it ensures that $\phi_f(T) = \overline{\phi_f}(T) = 0$. But note that ψ_g is not a parabolic cocycle in general since the chosen base point is not ∞ even though g is also a cusp form.

Now consider $\langle \phi_f, \overline{\psi_g} \rangle$. Let $\rho(a, b) := \pi(\phi_f(a) \otimes a\overline{\psi_g}(b))$, where π is from (6.19). We describe $\rho(a, b)$:

$$\begin{aligned} \rho(a, b) &= \sum_{\gamma} \left(\int_{\gamma\infty}^{\gamma a\infty} f(z)(Xz + Y)^{k-2} dz \right) \bullet \left(\int_{\gamma a\zeta_6}^{\gamma ab\zeta_6} \overline{g(z)}(X\bar{z} + Y)^{k-2} d\bar{z} \right) \\ &= \sum_{\gamma} \int_{\gamma a\zeta_6}^{\gamma ab\zeta_6} \int_{\gamma\infty}^{\gamma a\infty} f(z)\overline{g(z)}((Xz + Y)^{k-2} \bullet (X\bar{z} + Y)^{k-2}) dz d\bar{z} \\ &= \sum_{\gamma} \int_{\gamma a\zeta_6}^{\gamma ab\zeta_6} \int_{\gamma\infty}^{\gamma a\infty} f(z)\overline{g(z)}(z - \bar{z})^{k-2} dz d\bar{z} \\ &= \sum_{\gamma} \int_{a\zeta_6}^{ab\zeta_6} \int_{\infty}^{a\infty} f|_{\gamma}(z)\overline{g|_{\gamma}(z)}(z - \bar{z})^{k-2} dz d\bar{z}. \end{aligned}$$

where the sums run over a system of representatives of $\Gamma \backslash \mathrm{PSL}_2(\mathbb{Z})$. We obtain

$$\begin{aligned} &\rho(\sigma, \sigma) \\ &= \sum_{\gamma} \int_{\sigma\zeta_6}^{\sigma^2\zeta_6} \int_{\infty}^{\sigma\infty} f|_{\gamma}(z)\overline{g|_{\gamma}(z)}(z - \bar{z})^{k-2} dz d\bar{z} \\ &= \sum_{\gamma} \int_{\zeta_3}^{\zeta_6} \int_{\infty}^0 f|_{\gamma}(z)\overline{g|_{\gamma}(z)}(z - \bar{z})^{k-2} dz d\bar{z}, \\ &= \sum_{\gamma} \left[\int_{\zeta_3}^i \int_{\infty}^0 f|_{\gamma}(z)\overline{g|_{\gamma}(z)}(z - \bar{z})^{k-2} dz d\bar{z} + \int_{\sigma\zeta_3}^{\sigma i} \int_{\sigma\infty}^{\sigma 0} f|_{\gamma}(z)\overline{g|_{\gamma}(z)}(z - \bar{z})^{k-2} dz d\bar{z} \right] \\ &= \sum_{\gamma} \left[\int_{\zeta_3}^i \int_{\infty}^0 f|_{\gamma}(z)\overline{g|_{\gamma}(z)}(z - \bar{z})^{k-2} dz d\bar{z} + \int_{\zeta_3}^i \int_{\infty}^0 f|_{\gamma\sigma}(z)\overline{g|_{\gamma\sigma}(z)}(z - \bar{z})^{k-2} dz d\bar{z} \right] \\ &= 2 \sum_{\gamma} \int_{\zeta_3}^i \int_{\infty}^0 f|_{\gamma}(z)\overline{g|_{\gamma}(z)}(z - \bar{z})^{k-2} dz d\bar{z}, \end{aligned}$$

and

$$\begin{aligned} \rho(\tau, \tau) &= \sum_{\gamma} \int_{\tau\zeta_6}^{\tau^2\zeta_6} \int_{\infty}^{\tau\infty} f|_{\gamma}(z)\overline{g|_{\gamma}(z)}(z - \bar{z})^{k-2} dz d\bar{z} = 0 \\ \rho(\tau, \tau^2) &= \sum_{\gamma} \int_{\tau\zeta_6}^{\tau^3\zeta_6} \int_{\infty}^{\tau\infty} f|_{\gamma}(z)\overline{g|_{\gamma}(z)}(z - \bar{z})^{k-2} dz d\bar{z} = 0, \end{aligned}$$

since τ stabilises ζ_6 . It now suffices to compare with the formulas computed before (Propositions 6.13 and 6.4) to obtain the claimed formula. \square

6.4 Theory: The Eichler-Shimura theorem

We can now, finally, prove that the Eichler-Shimura map is an isomorphism. It should be pointed out again that the cohomology groups can be replaced by modular symbols according to Theorem 5.9.

Theorem 6.15 (Eichler-Shimura). *Let $N \geq 4$ and $k \geq 2$. The Eichler-Shimura map and the induced Eichler-Shimura map (Proposition 6.7) are isomorphisms for $\Gamma = \Gamma_1(N)$. The image of $S_k(\Gamma_1(N); \mathbb{C}) \oplus \overline{S_k(\Gamma_1(N); \mathbb{C})}$ is isomorphic to the parabolic subspace.*

Proof. We first assert that the dimensions of both sides of the Eichler-Shimura map agree and also that twice the dimension of the space of cusp forms equals the dimension of the parabolic subspace.

The dimension of the cohomology group and its parabolic subspace was computed in Proposition 4.16. For the dimension of the left-hand side we refer to [21, §6.2].

Suppose that (f, g) are in the kernel of the Eichler-Shimura map. Then by Proposition 6.9 it follows that f and g are both cuspidal. Hence, it suffices to prove that the restriction of the Eichler-Shimura map to $S_k(\Gamma_1(N); \mathbb{C}) \oplus \overline{S_k(\Gamma_1(N); \mathbb{C})}$ is injective. In order to do this we choose $z_0 = z_1 = \infty$ as base points for the Eichler-Shimura map, which is possible as the integrals converge on cusp forms (as in Proposition 6.7 one sees that this choice of base point does not change the cohomology class). As in Proposition 6.14, we write ϕ_f for the 1-cocycle associated with a cusp form f for the base point ∞ .

We now make use of the pairing from Proposition 6.14 on

$$Z^1(\mathrm{PSL}_2(\mathbb{Z}), \mathrm{Coind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V_{k-2}(\mathbb{C}))),$$

where we put $\Gamma := \Gamma_1(N)$ for short. This pairing induces a \mathbb{C} -valued pairing $\langle \cdot, \cdot \rangle$ on

$$H_{\mathrm{par}}^1(\mathrm{PSL}_2(\mathbb{Z}), \mathrm{Coind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V_{k-2}(\mathbb{C}))).$$

Next observe that the map

$$S_k(\Gamma_1(N); \mathbb{C}) \oplus \overline{S_k(\Gamma_1(N); \mathbb{C})} \xrightarrow{(f, \bar{g}) \mapsto (f+g, \bar{f}-\bar{g})} S_k(\Gamma_1(N); \mathbb{C}) \oplus \overline{S_k(\Gamma_1(N); \mathbb{C})}$$

is an isomorphism. Let $f, g \in S_k(\Gamma_1(N); \mathbb{C})$ be cusp forms and assume now that $(f + g, \bar{f} - \bar{g})$ is sent to the zero-class in $H_{\mathrm{par}}^1(\mathrm{PSL}_2(\mathbb{Z}), \mathrm{Coind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V_{k-2}(\mathbb{C})))$. In that cohomology space, we thus have

$$0 = \phi_f + \phi_g + \bar{\phi}_f - \bar{\phi}_g = (\phi_f + \bar{\phi}_f) + (\phi_g - \bar{\phi}_g) = 2 \operatorname{Re}(\phi_f) + 2i \operatorname{Im}(\phi_g).$$

We conclude that the cohomology classes of $\phi_f + \bar{\phi}_f$ and $\phi_g - \bar{\phi}_g$ are both zero.

Now we apply the pairing as follows:

$$0 = \langle \phi_f, \phi_f + \bar{\phi}_f \rangle = \langle \phi_f, \phi_f \rangle + \langle \phi_f, \bar{\phi}_f \rangle = (2i)^{k-1} \mu(f, f)$$

where we used $\langle \phi_f, \phi_f \rangle = 0$ because of Lemma 6.11 (since the pairing is given by the cup product), as well as Proposition 6.14. Hence, $(f, f) = 0$ and, thus, $f = 0$ since the Petersson scalar product is positive definite. Similar arguments with $0 = \langle \phi_g, \phi_g - \bar{\phi}_g \rangle$ show $g = 0$. This proves the injectivity. \square

Remark 6.16. *The Eichler-Shimura map is in fact an isomorphism for all subgroups Γ of $\mathrm{SL}_2(\mathbb{Z})$ of finite index. The proof is the same, but must use more involved dimension formulae for the cohomology group (see Remark 4.17) and modular forms.*

In Corollary 7.30 we will see that there also is an Eichler-Shimura isomorphism with a Dirichlet character.

6.5 Theoretical exercises

Exercise 6.17. *Check that the cup product is well-defined.*

Hint: this is a standard exercise that can be found in many textbooks (e.g. [4]).

Exercise 6.18. *Prove Lemma 6.11.*

Hint: [4, (5.3.6)].

7 Hecke operators

In this section we introduce Hecke operators on group cohomology using the double cosets approach and we prove that the Eichler-Shimura isomorphism is compatible with the Hecke action on group cohomology and modular forms.

7.1 Theory: Hecke rings

Definition 7.1. Let $N, n \in \mathbb{N}$. We define

$$\begin{aligned}\Delta_0^n(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N}, (a, N) = 1, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = n \right\}, \\ \Delta_1^n(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \pmod{N}, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = n \right\}, \\ \Delta_0(N) &= \bigcup_{n \in \mathbb{N}} \Delta_0^n(N), \\ \Delta_1(N) &= \bigcup_{n \in \mathbb{N}} \Delta_1^n(N).\end{aligned}$$

From now on, let $(\Delta, \Gamma) = (\Delta_1(N), \Gamma_1(N))$ or $(\Delta, \Gamma) = (\Delta_0(N), \Gamma_0(N))$.

Lemma 7.2. Let $\alpha \in \Delta$. We put

$$\Gamma_\alpha = \Gamma \cap \alpha^{-1}\Gamma\alpha \text{ and } \Gamma^\alpha = \Gamma \cap \alpha\Gamma\alpha^{-1}.$$

Then Γ_α has finite index in Γ and $\alpha^{-1}\Gamma\alpha$ (one says that Γ and $\alpha^{-1}\Gamma\alpha$ are commensurable), and also Γ^α has finite index in Γ and $\alpha\Gamma\alpha^{-1}$ (hence, Γ and $\alpha\Gamma\alpha^{-1}$ are commensurable).

Proof. Let $n = \det \alpha$. One checks by matrix calculation that

$$\alpha^{-1}\Gamma(Nn)\alpha \subset \Gamma(N).$$

Thus,

$$\Gamma(Nn) \subset \alpha^{-1}\Gamma(N)\alpha \subset \alpha^{-1}\Gamma\alpha.$$

Hence, we have $\Gamma(Nn) \subset \Gamma_\alpha$ and the first claim follows. For the second claim, one proceeds similarly. \square

Example 7.3. Let $\Gamma = \Gamma_0(N)$ and p a prime. The most important case for the sequel is $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. An elementary calculation shows $\Gamma^\alpha = \Gamma_0(Np)$.

Definition 7.4. Let $\alpha \in \Delta$. We consider the diagram

$$\begin{array}{ccc} \Gamma_\alpha \backslash \mathbb{H} & \xrightarrow[\tau \mapsto \alpha\tau]{\alpha} & \Gamma^\alpha \backslash \mathbb{H} \\ \downarrow \pi_\alpha & & \downarrow \pi^\alpha \\ \Gamma \backslash \mathbb{H} & & \Gamma \backslash \mathbb{H}, \end{array}$$

in which π^α and π_α are the natural projections. One checks that this is well defined by using $\alpha\Gamma_\alpha\alpha^{-1} = \Gamma^\alpha$.

The group of divisors $\text{Div}(S)$ on a Riemann surface S consists of all formal \mathbb{Z} -linear combinations of points of S . For a morphism $\pi : S \rightarrow T$ of Riemann surfaces, define the pull-back $\pi^* : \text{Div}(T) \rightarrow \text{Div}(S)$ and the push-forward $\pi_* : \text{Div}(S) \rightarrow \text{Div}(T)$ uniquely by the rules $\pi^*(t) = \sum_{s \in S: \pi(s)=t} s$ and $\pi_*(s) = \pi(s)$ for points $t \in T$ and $s \in S$.

The modular correspondence or Hecke correspondence τ_α is defined as

$$\tau_\alpha : \text{Div}(Y_\Gamma) \xrightarrow{\pi_\alpha^*} \text{Div}(Y_{\Gamma_\alpha}) \xrightarrow{\alpha_*} \text{Div}(Y_{\Gamma^\alpha}) \xrightarrow{\pi_*^\alpha} \text{Div}(Y_\Gamma).$$

These modular correspondences will be described more explicitly in a moment. First a lemma:

Lemma 7.5. Let $\alpha_i \in \Gamma$ for $i \in I$ with some index set I . Then we have

$$\Gamma = \bigsqcup_{i \in I} \Gamma_\alpha \alpha_i \Leftrightarrow \Gamma \alpha \Gamma = \bigsqcup_{i \in I} \Gamma \alpha \alpha_i.$$

Proof. This is proved by quite a straight forward calculation. \square

Corollary 7.6. *Let $\alpha \in \Delta$ and $\Gamma\alpha\Gamma = \bigsqcup_{i \in I} \Gamma\alpha_i$. Then the Hecke correspondence $\tau_\alpha : \text{Div}(Y_\Gamma) \rightarrow \text{Div}(Y_\Gamma)$ is given by $\tau \mapsto \sum_{i \in I} \alpha_i \tau$ for representatives $\tau \in \mathbb{H}$.*

Proof. It suffices to check the definition using Lemma 7.5. □

Remark 7.7. *We have $\Delta^n = \bigcup_{\alpha \in \Delta, \det \alpha = n} \Gamma\alpha\Gamma$ and one can choose finitely many α_i for $i \in I$ such that $\Delta^n = \bigsqcup_{i \in I} \Gamma\alpha_i\Gamma$.*

Definition 7.8. *Let $\Delta^n = \bigsqcup_{i \in I} \Gamma\alpha_i\Gamma$. The Hecke operator T_n on $\text{Div}(Y_\Gamma)$ is defined as*

$$T_n = \sum_{i \in I} \tau_{\alpha_i}.$$

Let us recall from equation (1.2) the matrix $\sigma_a \in \Gamma_0(N)$ (for $(a, N) = 1$) which satisfies

$$\sigma_a \equiv \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \pmod{N}.$$

Proposition 7.9. (a) *We have the decomposition*

$$\Delta_0^n(N) = \bigsqcup_a \bigsqcup_b \Gamma_0(N) \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

where a runs through the positive integers with $a \mid n$ and $(a, N) = 1$ and b runs through the integers such that $0 \leq b < d := n/a$.

(b) *We have the decomposition*

$$\Delta_1^n(N) = \bigsqcup_a \bigsqcup_b \Gamma_1(N) \sigma_a \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

with a, b, d as in (a).

Proof. This proof is elementary. □

Note that due to $\sigma_a \in \Gamma_0(N)$, the matrices $\sigma_a \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ used in part (b) also work in part (a). One can thus use the same representatives regardless if one works with $\Gamma_0(N)$ or $\Gamma_1(N)$. Note also that for $n = \ell$ a prime, these representatives are exactly the elements of \mathcal{R}_ℓ from equation (1.3).

Next, we turn to the important description of the Hecke algebra as a double coset algebra.

Definition 7.10. *The Hecke ring $R(\Delta, \Gamma)$ is the free abelian group on the double cosets $\Gamma\alpha\Gamma$ for $\alpha \in \Delta$.*

As our next aim we would like to define a multiplication, which then also justifies the name "ring". First let $\Gamma\alpha\Gamma = \bigsqcup_{i=1}^n \Gamma\alpha_i$ and $\Gamma\beta\Gamma = \bigsqcup_{j=1}^m \Gamma\beta_j$. We just start computing.

$$\Gamma\alpha\Gamma \cdot \Gamma\beta\Gamma = \bigcup_j \Gamma\alpha\Gamma\beta_j = \bigcup_{i,j} \Gamma\alpha_i\beta_j.$$

This union is not necessarily disjoint. The left hand side can be written as a disjoint union of double cosets $\bigsqcup_{k=1}^r \Gamma\gamma_k\Gamma$. Each of these double cosets is again of the form

$$\Gamma\gamma_k\Gamma = \bigsqcup_{l=1}^{n_k} \Gamma\gamma_{k,l}.$$

We obtain in summary

$$\Gamma\alpha\Gamma \cdot \Gamma\beta\Gamma = \bigcup_{i,j} \Gamma\alpha_i\beta_j = \bigsqcup_k \bigsqcup_l \Gamma\gamma_{k,l}.$$

We will now introduce a piece of notation for the multiplicity with which every coset on the right appears in the centre of the above equality. For fixed k we define for every l

$$m_{k,l} = \#\{(i, j) \mid \Gamma\gamma_{k,l} = \Gamma\alpha_i\beta_j\}.$$

The important point is the following lemma.

Lemma 7.11. *The number $m_{k,l}$ is independent of l . We put $m_k := m_{k,l}$.*

Proof. The proof is combinatorial and quite straight forward. □

Definition 7.12. *We define the multiplication on $R(\Delta, \Gamma)$ by*

$$\Gamma\alpha\Gamma \cdot \Gamma\beta\Gamma = \sum_{k=1}^n m_k \Gamma\gamma_k\Gamma,$$

using the preceding notation.

In Exercise 7.34 you are asked to check that the Hecke ring is indeed a ring. The definition of the multiplication makes sense, as it gives for Hecke correspondences:

$$\tau_\alpha \circ \tau_\beta = \sum_{k=1}^n m_k \tau_{\gamma_k}.$$

Definition 7.13. *For $\alpha \in \Delta$ let $\tau_\alpha = \Gamma\alpha\Gamma$. We define (as above)*

$$T_n = \sum_{\alpha} \tau_\alpha \in R(\Delta, \Gamma),$$

where the sum runs over a set of α such that $\Delta^n = \bigsqcup_{\alpha} \Gamma\alpha\Gamma$. For $a \mid d$ and $(d, N) = 1$ we let

$$T(a, d) = \Gamma\sigma_a \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \Gamma \in R(\Delta, \Gamma).$$

From Exercise 7.35, we obtain the the following important corollary.

Corollary 7.14. *We have $T_m T_n = T_n T_m$ and hence $R(\Delta, \Gamma)$ is a commutative ring.*

7.2 Theory: Hecke operators on modular forms

In this section we again let $(\Delta, \Gamma) = (\Delta_0(N), \Gamma_0(N))$ or $(\Delta_1(N), \Gamma_1(N))$. We now define an action of the Hecke ring $R(\Delta, \Gamma)$ on modular forms.

Definition 7.15. *Let $\alpha \in \Delta$. Suppose $\Gamma\alpha\Gamma = \bigsqcup_{i=1}^n \Gamma\alpha_i$ and let $f \in M_k(\Gamma)$. We put*

$$f \cdot \tau_\alpha := \sum_{i=1}^n f|_{\alpha_i}.$$

Lemma 7.16. *The function $f \cdot \tau_\alpha$ again lies in $M_k(\Gamma)$.*

Proof. For $\gamma \in \Gamma$ we check the transformation rule:

$$\sum_i f|_{\alpha_i}|_\gamma = \sum_i f|_{\alpha_i\gamma} = \sum_i f|_{\alpha_i},$$

since the cosets $\Gamma(\alpha_i\gamma)$ are a permutation of the cosets $\Gamma\alpha_i$. The holomorphicity of $f \cdot \tau_\alpha$ is clear and the holomorphicity in the cusps is not difficult. □

This thus gives the desired operation of $R(\Delta, \Gamma)$ on $M_k(\Gamma)$.

Proposition 7.17. *Let $(\Delta, \Gamma) = (\Delta_0(N), \Gamma_0(N))$ and $f \in M_k(\Gamma)$. The following formulae hold:*

- (a) $(f \cdot T_m)(\tau) = \frac{1}{m} \sum_{a \mid m, (a, N)=1} \sum_{b=0}^{m-1} a^k f\left(\frac{a\tau+b}{m/a}\right),$
- (b) $a_n(f \cdot T_m) = \sum_{a \mid (m, n), (a, N)=1} a^{k-1} a \frac{m}{a^2}.$

Similar formulae hold for $(\Delta_1(N), \Gamma_1(N))$, if one includes a Dirichlet character at the right places.

Proof. (a) follows directly from Proposition 7.9.

$$(b) \text{ is a simple calculation using } \sum_{b=0}^{d-1} e^{2\pi i \frac{b}{d}n} = \begin{cases} 0, & \text{if } d \nmid n \\ d, & \text{if } d \mid n. \end{cases} \quad \square$$

Remark 7.18. The Hecke ring $R(\Delta, \Gamma)$ also acts on $S_k(\Gamma)$.

Corollary 7.19. Let $(\Delta, \Gamma) = (\Delta_0(N), \Gamma_0(N))$. For the action of the Hecke operators on $M_k(\Gamma)$ and $S_k(\Gamma)$ the following formulae hold:

- (a) $T_n T_m = T_{nm}$ for $(n, m) = 1$,
- (b) $T_{p^{r+1}} = T_p T_{p^r} - p^{k-1} T_{p^{r-1}}$, if $p \nmid N$, and
- (c) $T_{p^{r+1}} = T_p T_{p^r}$, if $p \mid N$.

Here, p always denotes a prime number. Similar formulae hold for $(\Delta_1(N), \Gamma_1(N))$, if one includes a Dirichlet character at the right places.

Proof. These formulae follow from Exercise 7.35 and the definition of the action. \square

Even though it is not directly relevant for our purposes, we include Euler products, which allow us to express the formulae from the corollary in a very elegant way.

Proposition 7.20 (Euler product). The action of the Hecke operators T_n on modular forms satisfies the formal identity:

$$\sum_{n=1}^{\infty} T_n n^{-s} = \prod_{p \nmid N} (1 - T_p p^{-s} + p^{k-1-2s})^{-1} \cdot \prod_{p \mid N} (1 - T_p p^{-s})^{-1}.$$

That the identity is formal means that we can arbitrarily permute terms in sums and products without considering questions of convergence.

Proof. The proof is carried out in three steps.

1st step: Let $g : \mathbb{Z} \rightarrow \mathbb{C}$ be any function. Then we have the formal identity

$$\prod_p \sum_{r=0}^{\infty} g(p^r) = \sum_{n=1}^{\infty} \prod_{p^r \parallel n} g(p^r).$$

For its proof, let first S be a finite set of prime numbers. Then we have the formal identity:

$$\prod_{p \in S} \sum_{r=0}^{\infty} g(p^r) = \sum_{n=1, n \text{ only has prime factors in } S}^{\infty} \prod_{p^r \parallel n} g(p^r),$$

which one proves by multiplying out the left hand side (Attention! Here one permutes the terms!). We finish the first step by letting S run through arbitrarily large sets.

2nd step: For $p \nmid N$ we have

$$\left(\sum_{r=0}^{\infty} T_{p^r} p^{-rs} \right) (1 - T_p p^{-s} + p^{k-1-2s}) = 1$$

and for $p \mid N$:

$$\left(\sum_{r=0}^{\infty} T_{p^r} p^{-rs} \right) (1 - T_p p^{-s}) = 1.$$

The proof of the second step consists of multiplying out these expressions and to identify a “telescope”.

3rd step: The proposition now follows by using the first step with $g(p^r) = T_{p^r} p^{-rs}$ and plugging in the formulae from the second step. \square

7.3 Theory: Hecke operators on group cohomology

In this section we again let $(\Delta, \Gamma) = (\Delta_0(N), \Gamma_0(N))$ or $(\Delta_1(N), \Gamma_1(N))$. Let R be a ring and V a left $R[\Gamma]$ -module which extends to a semi-group action by the semi-group consisting of all α^ι for $\alpha \in \Delta^n$ for all n . Recall that $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^\iota = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

We now give the definition of the Hecke operator τ_α on $\text{Div}(\Gamma \backslash \mathbb{H})$ (see, for instance, [9] or [23]).

Definition 7.21. *Let $\alpha \in \Delta$. The Hecke operator τ_α acting on group cohomology is the composite*

$$H^1(\Gamma, V) \xrightarrow{\text{res}} H^1(\Gamma^\alpha, V) \xrightarrow{\text{conj}_\alpha} H^1(\Gamma_\alpha, V) \xrightarrow{\text{cores}} H^1(\Gamma, V).$$

The first map is the restriction, and the third one is the corestriction. We explicitly describe the second map on cocycles:

$$\text{conj}_\alpha : H^1(\Gamma^\alpha, V) \rightarrow H^1(\Gamma_\alpha, V), \quad c \mapsto (g_\alpha \mapsto \alpha^\iota \cdot c(\alpha g_\alpha \alpha^{-1})).$$

There is a similar description on the parabolic subspace and the two are compatible, see Exercise 7.36.

Proposition 7.22. *Let $\alpha \in \Delta$. Suppose that $\Gamma \alpha \Gamma = \bigcup_{i=1}^n \Gamma \delta_i$ is a disjoint union. Then the Hecke operator τ_α acts on $H^1(\Gamma, V)$ and $H_{\text{par}}^1(\Gamma, V)$ by sending the cocycle c to $\tau_\alpha c$ defined by*

$$(\tau_\alpha c)(g) = \sum_{i=1}^n \delta_i^\iota c(\delta_i g \delta_{\sigma_g(i)}^{-1})$$

for $g \in \Gamma$. Here $\sigma_g(i)$ is the index such that $\delta_i g \delta_{\sigma_g(i)}^{-1} \in \Gamma$.

Proof. We only have to describe the corestriction explicitly. For that we use that $\Gamma = \bigcup_{i=1}^n \Gamma_\alpha g_i$ with $\alpha g_i = \delta_i$. Furthermore, by Exercise 7.37 the corestriction of a cocycle $u \in H^1(\Gamma_\alpha, V)$ is the cocycle $\text{cores}(u)$ uniquely given by

$$\text{cores}(u)(g) = \sum_{i=1}^n g_i^{-1} u(g_i g g_{\sigma_g(i)}^{-1}) \quad (7.20)$$

for $g \in \Gamma$. Combining with the explicit description of the map conj_α yields the result. \square

Definition 7.23. *For a positive integer n , the Hecke operator T_n is defined as $\sum_\alpha \tau_\alpha$, where the sum runs through a system of representatives of the double cosets $\Gamma \backslash \Delta^n / \Gamma$.*

Let a be an integer coprime to N . The diamond operator $\langle a \rangle$ is defined as τ_α for the matrix $\sigma_a \in \Gamma_0(N)$, defined in Equation 1.2 (if the Γ -action on V extends to an action of the semi-group generated by Γ and α^ι ; note that $\alpha \in \Delta_0^1$, but in general not in Δ_1^1).

It is clear that the Hecke and diamond operators satisfy the ‘‘usual’’ Euler product.

Proposition 7.24. *The Eichler-Shimura isomorphism is compatible with the Hecke operators.*

Proof. We recall the definition of Shimura’s main involution: $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^\iota = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. In other words, for matrices with a non-zero determinant, we have

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^\iota = (\det \begin{pmatrix} a & b \\ c & d \end{pmatrix}) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1}.$$

Let now $f \in M_k(\Gamma; \mathbb{C})$ be a modular form, $\gamma \in \Gamma$ and $z_0 \in \mathbb{H}$. For any matrix g with non-zero determinant, Lemma 6.5 yields

$$I_{f|_g}(z_0, \gamma z_0) = g^\iota I_f(g z_0, g \gamma z_0).$$

Let $\alpha \in \Delta$. We show the compatibility of the Hecke operator τ_α with the map

$$f \mapsto (\gamma \mapsto I_f(z_0, \gamma z_0))$$

between $M_k(\Gamma; \mathbb{C})$ and $H^1(\Gamma, V_{k-2}(\mathbb{C}))$. The same arguments will also work, when $I_f(z_0, \gamma z_0)$ is replaced by $J_{\bar{g}}(z_1, \gamma z_1)$ with anti-holomorphic cusp forms \bar{g} .

Consider a coset decomposition $\Gamma\alpha\Gamma = \bigsqcup_i \Gamma\delta_i$. We use notation as in Proposition 7.22 and compute:

$$\begin{aligned} & I_{\tau_\alpha f}(z_0, \gamma z_0) \\ &= I_{\sum_i f|_{\delta_i}}(z_0, \gamma z_0) = \sum_i I_{f|_{\delta_i}}(z_0, \gamma z_0) = \sum_i \delta_i^\iota I_f(\delta_i z_0, \delta_i \gamma z_0) \\ &= \sum_i \delta_i^\iota (I_f(\delta_i z_0, z_0) + I_f(z_0, \delta_i \gamma \delta_{\sigma_\gamma(i)}^{-1} z_0) + I_f(\delta_i \gamma \delta_{\sigma_\gamma(i)}^{-1} z_0, \delta_i \gamma \delta_{\sigma_\gamma(i)}^{-1} \delta_{\sigma_\gamma(i)} z_0)) \\ &= \sum_i \delta_i^\iota I_f(z_0, \delta_i \gamma \delta_{\sigma_\gamma(i)}^{-1} z_0) + \sum_i \delta_i^\iota I_f(\delta_i z_0, z_0) - \sum_i \delta_i^\iota \delta_i \gamma \delta_{\sigma_\gamma(i)}^{-1} I_f(\delta_{\sigma_\gamma(i)} z_0, z_0) \\ &= \sum_i \delta_i^\iota I_f(z_0, \delta_i \gamma \delta_{\sigma_\gamma(i)}^{-1} z_0) + (1 - \gamma) \sum_i \delta_i^\iota I_f(\delta_i z_0, z_0), \end{aligned}$$

since $\delta_i^\iota \delta_i \gamma \delta_{\sigma_\gamma(i)}^{-1} = \gamma \delta_{\sigma_\gamma(i)}^\iota$. Up to coboundaries, the cocycle $\gamma \mapsto I_{\tau_\alpha f}(z_0, \gamma z_0)$ is thus equal to the cocycle $\gamma \mapsto \sum_i \delta_i^\iota I_f(z_0, \delta_i \gamma \delta_{\sigma_\gamma(i)}^{-1} z_0)$, which by Proposition 7.22 is equal to τ_α applied to the cocycle $\gamma \mapsto I_f(z_0, \gamma z_0)$, as required. \square

Remark 7.25. *The conceptual reason why the above proposition is correct, is, of course, that the Hecke operators come from Hecke correspondences.*

7.4 Theory: Hecke operators and Shapiro's lemma

We now prove that the Hecke operators are compatible with Shapiro's lemma. This was first proved by Ash and Stevens [1]. We need to say what the action of $\alpha \in \Delta$ on the coinduced module $\text{Hom}_{R[\Gamma]}(R[\text{SL}_2(\mathbb{Z})], V)$ should be. Here we are assuming that V carries an action by the semi-group Δ^ι (that is, ι applied to all elements of Δ).

Let U_N be the image of Δ^ι in $\text{Mat}_2(\mathbb{Z}/N\mathbb{Z})$. The natural map

$$\Gamma \backslash \text{SL}_2(\mathbb{Z}) \rightarrow U_N \backslash \text{Mat}_2(\mathbb{Z}/N\mathbb{Z})$$

is injective. Its image consists of those $U_N g$ such that

$$(0, 1)g = (u, v) \text{ with } \langle u, v \rangle = \mathbb{Z}/N\mathbb{Z}. \quad (7.21)$$

If that is so, then we say for short that g satisfies (7.21). Note that this condition does not depend on the choice of g in $U_N g$. Define the $R[\Delta^\iota]$ -module $\mathcal{C}(N, V)$ as

$$\{f \in \text{Hom}_R(R[U_N \backslash \text{Mat}_2(\mathbb{Z}/N\mathbb{Z})], V) \mid f(g) = 0 \text{ if } g \text{ does not satisfy (7.21)}\}$$

with the action of $\delta \in \Delta^\iota$ given by $(\delta.f)(g) = \delta.(f(g\delta))$. The module $\mathcal{C}(N, V)$ is isomorphic to the coinduced module $\text{Hom}_{R[\Gamma]}(R[\text{SL}_2(\mathbb{Z})], V)$ as an $R[\Gamma]$ -module by

$$\begin{aligned} & \text{Hom}_{R[\Gamma]}(R[\text{SL}_2(\mathbb{Z})], V) \rightarrow \mathcal{C}(N, V), \\ & f \mapsto \begin{cases} (g \mapsto gf(g^{-1})) & \text{for any } g \in \text{SL}_2(\mathbb{Z}), \\ 0 & \text{if } g \text{ does not satisfy (7.21)}. \end{cases} \end{aligned}$$

One might wonder why we introduce the new module $\mathcal{C}(N, V)$ instead of working directly with $\text{Hom}_{R[\Gamma]}(R[\text{SL}_2(\mathbb{Z})], V)$. The point is that we cannot directly act on the latter with a matrix of determinant different from 1. Hence we need a way to naturally extend the action. We do this by embedding $\Gamma \backslash \text{SL}_2(\mathbb{Z})$ into $U_N \backslash \text{Mat}_2(\mathbb{Z}/N\mathbb{Z})$. Of course, we then want to work on the image of this embedding, which is exactly described by (7.21). The module $\mathcal{C}(N, V)$ is then immediately written down in view of the identification between $\text{Hom}_{R[\Gamma]}(R[\text{SL}_2(\mathbb{Z})], V)$ and $\text{Hom}_R(R[\Gamma \backslash \text{SL}_2(\mathbb{Z})], V)$ given by sending f to $(g \mapsto g.f(g^{-1}))$ (which is clearly independent of the choice of g in the coset Γg).

Proposition 7.26. *The Hecke operators are compatible with Shapiro's Lemma. More precisely, for all $n \in \mathbb{N}$ the following diagram commutes:*

$$\begin{array}{ccc} \mathrm{H}^1(\Gamma, V) & \xrightarrow{T_n} & \mathrm{H}^1(\Gamma, V) \\ \text{Shapiro} \uparrow & & \text{Shapiro} \uparrow \\ \mathrm{H}^1(\mathrm{SL}_2(\mathbb{Z}), \mathcal{C}(N, V)) & \xrightarrow{T_n} & \mathrm{H}^1(\mathrm{SL}_2(\mathbb{Z}), \mathcal{C}(N, V)). \end{array}$$

Proof. Let $j \in \{0, 1\}$ indicate whether we work with Γ_0 or Γ_1 . Let δ_i , for $i = 1, \dots, r$ be the representatives of $\mathrm{SL}_2(\mathbb{Z}) \backslash \Delta_j^n(1)$ provided by Proposition 7.9. Say, that they are ordered such that δ_i for $i = 1, \dots, s$ with $s \leq r$ are representatives for $\Gamma \backslash \Delta_j^n(N)$. This explicitly means that the lower row of δ_i^t is $(0, a)$ with $(a, N) = 1$ (or even $(0, 1)$ if $j = 1$) for $i = 1, \dots, s$. If $s < i \leq r$, then the lower row is (u, v) with $\langle u, v \rangle \not\leq \mathbb{Z}/N\mathbb{Z}$.

Let $c \in \mathrm{H}^1(\mathrm{SL}_2(\mathbb{Z}), \mathcal{C}(N, V))$ be a 1-cochain. Then, as required, we find

$$\begin{aligned} \text{Shapiro}(T_n(c))(\gamma) &= \sum_{i=1}^r (\delta_i^t \cdot c(\delta^i \gamma \delta_{\sigma_\gamma(i)}^{-1})) \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) = \sum_{i=1}^r \delta_i^t (c(\delta^i \gamma \delta_{\sigma_\gamma(i)}^{-1})(\delta_i^t)) \\ &= \sum_{i=1}^s (\delta_i^t \cdot c(\delta^i \gamma \delta_{\sigma_\gamma(i)}^{-1})) \left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) = T_n(\text{Shapiro}(c))(\gamma), \end{aligned}$$

where the second equality is due to the definition of the action and the third one holds since $c(\delta^i \gamma \delta_{\sigma_\gamma(i)}^{-1})$ lies in $\mathcal{C}(N, V)$ and thus evaluates to 0 on δ_i^t for $i > s$. \square

Remark 7.27. *A very similar description exists involving $\mathrm{PSL}_2(\mathbb{Z})$.*

Remark 7.28. *It is possible to give an explicit description of Hecke operators on Manin symbols from Theorem 5.7 by using Heilbronn matrices and variations as, for instance, done in [16].*

Remark 7.29. *One can show that the isomorphisms from Theorem 5.9 are compatible with Hecke operators.*

7.5 Theory: Eichler-Shimura revisited

In this section we present some corollaries and extensions of the Eichler-Shimura theorem. We first come to modular symbols with a character and, thus, also to modular symbols for $\Gamma_0(N)$.

Corollary 7.30 (Eichler-Shimura). *Let $N \geq 1$, $k \geq 2$ and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ be a Dirichlet character. Then the Eichler-Shimura map gives isomorphisms*

$$\mathrm{M}_k(N, \chi; \mathbb{C}) \oplus \overline{\mathrm{S}_k(N, \chi; \mathbb{C})} \rightarrow \mathrm{H}^1(\Gamma_0(N), V_{k-2}^{\chi}(\mathbb{C})),$$

and

$$\mathrm{S}_k(N, \chi; \mathbb{C}) \oplus \overline{\mathrm{M}_k(N, \chi; \mathbb{C})} \rightarrow \mathrm{H}_{\text{par}}^1(\Gamma_0(N), V_{k-2}^{\chi}(\mathbb{C})),$$

which are compatible with the Hecke operators.

Proof. Recall that the σ_a form a system of coset representatives for $\Gamma_0(N)/\Gamma_1(N) =: \Delta$ and that the group Δ acts on $\mathrm{H}^1(\Gamma_0(N), V)$ by sending a cocycle c to the cocycle δc (for $\delta \in \Delta$) which is defined by

$$\gamma \mapsto \delta \cdot c(\delta^{-1} \gamma \delta).$$

With $\delta = \sigma_a^{-1} = \sigma_a^t$, this reads

$$\gamma \mapsto \sigma_a^t \cdot c(\sigma_a \gamma \sigma_a^{-1}) = \tau_{\sigma_a} c = \langle a \rangle c.$$

Hence, $\sigma_a \in \Delta$ -action acts through the inverse of the diamond operators.

We now appeal to the Hochschild-Serre exact sequence, using that the cohomology groups (from index 1 onwards) vanish if the group order is finite and invertible. We get the isomorphism

$$H^1(\Gamma_0(N), V_{k-2}^{\ell, \chi}(\mathbb{C})) \xrightarrow{\text{res}} H^1(\Gamma_1(N), V_{k-2}^{\ell, \chi}(\mathbb{C}))^\Delta.$$

Moreover, the Eichler-Shimura isomorphism is an isomorphism of Hecke modules

$$M_k(\Gamma_1(N); \mathbb{C}) \oplus \overline{S_k(\Gamma_1(N); \mathbb{C})} \rightarrow H^1(\Gamma_1(N), V_{k-2}^{\ell, \chi}(\mathbb{C})),$$

since for matrices in $\Delta_1(N)$ acting through the Shimura main involution the modules $V_{k-2}^{\ell, \chi}(\mathbb{C})$ and $V_{k-2}(\mathbb{C})$ coincide. Note that it is necessary to take $V_{k-2}^{\ell, \chi}(\mathbb{C})$ because the action on group cohomology involves the Shimura main involution. Moreover, with this choice, the Eichler-Shimura isomorphism is Δ -equivariant.

To finish the proof, it suffices to take Δ -invariants on both sides, i.e. to take invariants for the action of the diamond operators. The result on the parabolic subspace is proved in the same way.

Since Hecke and diamond operators commute, the Hecke action is compatible with the decomposition into χ -isotypical components. \square

Next we consider the action of complex conjugation.

Corollary 7.31. *Let $\Gamma = \Gamma_1(N)$. The maps*

$$S_k(\Gamma; \mathbb{C}) \rightarrow H_{\text{par}}^1(\Gamma, V_{k-2}(\mathbb{R})), \quad f \mapsto (\gamma \mapsto \text{Re}(I_f(z_0, \gamma z_0)))$$

and

$$S_k(\Gamma; \mathbb{C}) \rightarrow H_{\text{par}}^1(\Gamma, V_{k-2}(\mathbb{R})), \quad f \mapsto (\gamma \mapsto \text{Im}(I_f(z_0, \gamma z_0)))$$

are isomorphisms (of real vector spaces) compatible with the Hecke operators. A similar result holds in the presence of a Dirichlet character.

Proof. We consider the composite

$$S_k(\Gamma; \mathbb{C}) \xrightarrow{f \mapsto \frac{1}{2}(f + \bar{f})} S_k(\Gamma; \mathbb{C}) \oplus \overline{S_k(\Gamma; \mathbb{C})} \xrightarrow{\text{Eichler-Shimura}} H_{\text{par}}^1(\Gamma, V_{k-2}(\mathbb{C})).$$

It is clearly injective. As $J_{\bar{f}}(z_0, \gamma z_0) = \overline{I_f(z_0, \gamma z_0)}$, the composite map coincides with the first map in the statement. Its image is thus already contained in the real vector space $H_{\text{par}}^1(\Gamma, V_{k-2}(\mathbb{R}))$. Since the real dimensions coincide, the map is an isomorphism. In order to prove the second isomorphism, we use $f \mapsto \frac{1}{2i}(f - \bar{f})$ and proceed as before. \square

We now treat the $+$ and the $-$ -space for the involution attached to the matrix $\eta = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ from equation (1.9). The action of η on $H^1(\Gamma, V)$ is the action of the Hecke operator τ_η ; strictly speaking, this operator is not defined because the determinant is negative, however we use the same definition. To be precise we have

$$\tau_\eta : H^1(\Gamma, V) \rightarrow H^1(\Gamma, V), \quad c \mapsto (\gamma \mapsto \eta^t \cdot c(\eta\gamma\eta)),$$

provided, of course, that η^t acts on V (compatibly with the Γ -action).

We also want to define an involution τ_η on $S_k(\Gamma; \mathbb{C}) \oplus \overline{S_k(\Gamma; \mathbb{C})}$. For that recall that if $f(z) = \sum a_n e^{2\pi i n z}$, then $\tilde{f}(z) := \sum \bar{a}_n e^{2\pi i n z}$ is again a cusp form in $S_k(\Gamma; \mathbb{C})$ since we only applied a field automorphism (complex conjugation) to the coefficients (think of cusp forms as maps from the Hecke algebra over \mathbb{Q} to \mathbb{C}). We define τ_η as the composite

$$\tau_\eta : S_k(\Gamma; \mathbb{C}) \xrightarrow{f \mapsto (-1)^{k-1} \tilde{f}} S_k(\Gamma; \mathbb{C}) \xrightarrow{\tilde{f} \mapsto \bar{\tilde{f}}} \overline{S_k(\Gamma; \mathbb{C})}.$$

Similarly, we also define $\tau_\eta : \overline{S_k(\Gamma; \mathbb{C})} \rightarrow S_k(\Gamma; \mathbb{C})$ and obtain in consequence an involution τ_η on $S_k(\Gamma; \mathbb{C}) \oplus \overline{S_k(\Gamma; \mathbb{C})}$. We consider the function $(-1)^{k-1} \overline{f(z)}$ as a function of \bar{z} . We have

$$\begin{aligned} \tau_\eta(f)(\bar{z}) &= (-1)^{k-1} \overline{f(z)} = (-1)^{k-1} \overline{\sum_n \bar{a}_n e^{2\pi i n z}} = (-1)^{k-1} \sum_n a_n e^{2\pi i n(-\bar{z})} \\ &= (-1)^{k-1} f(-\bar{z}) = f|_\eta(\bar{z}). \end{aligned}$$

Proposition 7.32. *The Eichler-Shimura map commutes with τ_η .*

Proof. Let $f \in S_k(\Gamma; \mathbb{C})$ (for simplicity). We have to check whether τ_η of the cocycle attached to f is the same as the cocycle attached to $\tau_\eta(f)$. We evaluate the latter at a general $\gamma \in \Gamma$ and compute:

$$\begin{aligned} J_{(-1)^{k-1} \bar{f}}(\infty, \gamma\infty) &= (-1)^{k-1} \int_\infty^{\gamma\infty} f(-\bar{z})(X\bar{z} + Y)^{k-2} d\bar{z} \\ &= - \int_\infty^{\gamma\infty} f(-\bar{z})(X(-\bar{z}) - Y)^{k-2} d\bar{z} \\ &= \int_{\gamma\infty}^\infty f(-\bar{z})(X(-\bar{z}) - Y)^{k-2} d\bar{z} \\ &= \int_0^\infty f(-(\gamma\infty + it))(X(-(\gamma\infty + it)) - Y)^{k-2} (-i) dt \\ &= - \int_0^\infty f(-\gamma\infty + it)(X(-\gamma\infty + it) - Y)^{k-2} i dt \\ &= \int_\infty^{-\gamma\infty} f(z)(Xz - Y)^{k-2} dz \\ &= \eta^t . I_f(\infty, -\gamma\infty) = \eta^t . I_f(\infty, \eta\gamma\eta\infty). \end{aligned}$$

This proves the claim. □

Corollary 7.33. *Let $\Gamma = \Gamma_1(N)$. The maps*

$$S_k(\Gamma; \mathbb{C}) \rightarrow H_{\text{par}}^1(\Gamma, V_{k-2}(\mathbb{C}))^+, \quad f \mapsto (1 + \tau_\eta).(\gamma \mapsto I_f(z_0, \gamma z_0))$$

and

$$S_k(\Gamma; \mathbb{C}) \rightarrow H_{\text{par}}^1(\Gamma, V_{k-2}(\mathbb{C}))^-, \quad f \mapsto (1 - \tau_\eta).(\gamma \mapsto I_f(z_0, \gamma z_0))$$

are isomorphisms compatible with the Hecke operators, where the $+$ (respectively the $-$) indicate the subspace invariant (respectively anti-invariant) for the involution τ_η . A similar result holds in the presence of a Dirichlet character.

Proof. Both maps are clearly injective (consider them as being given by $f \mapsto f + \tau_\eta f$ followed by the Eichler-Shimura map) and so dimension considerations show that they are isomorphisms. □

7.6 Theoretical exercises

Exercise 7.34. *Check that $R(\Delta, \Gamma)$ is a ring (associativity and distributivity).*

Exercise 7.35. *Show the formula*

$$T_m T_n = \sum_{d|(m,n), (d,N)=1} dT(d, d) T_{\frac{mn}{d^2}}.$$

Also show that $R(\Delta, \Gamma)$ is generated by T_p and $T(p, p)$ for p running through all prime numbers.

Exercise 7.36. *Check that the Hecke operator τ_α from Definition 7.21 restricts to $H_{\text{par}}^1(\Gamma, V)$.*

Exercise 7.37. *Prove Equation 7.20.*

7.7 Computer exercises

Computer Exercise 7.38. *Implement Hecke operators.*

References

- [1] A. Ash and G. Stevens. *Modular forms in characteristic l and special values of their L -functions*, Duke Math. J. **53** (1986), no. 3, 849–868.
- [2] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969 ix+128 pp.
- [3] R. Bieri. *Homological dimension of discrete groups*. Queen Mary College Mathematics Notes, London, 1976.
- [4] K. S. Brown. *Cohomology of groups*, Springer, New York, 1982.
- [5] H. Cohen, F. Strömberg. *Modular forms. A classical approach*. Graduate Studies in Mathematics, 179. American Mathematical Society, Providence, RI, 2017. xii+700 pp.
- [6] J. E. Cremona. *Algorithms for modular elliptic curves*. Second edition. Cambridge University Press, Cambridge, 1997.
- [7] H. Darmon, F. Diamond, R. Taylor. *Fermat’s last theorem*. Elliptic curves, modular forms & Fermat’s last theorem (Hong Kong, 1993), 2–140, Int. Press, Cambridge, MA, 1997.
- [8] P. Deligne, J. P. Serre. *Formes modulaires de poids 1*. Ann. Sci. Ecole Norm. Sup. (4) **7** (1974), 507–530.
- [9] F. Diamond and J. Im. *Modular forms and modular curves*, in *Seminar on Fermat’s Last Theorem (Toronto, ON, 1993–1994)*, 39–133, Amer. Math. Soc., Providence, RI, 1995.
- [10] Diamond, Fred; Shurman, Jerry: *A first course in modular forms*. Graduate Text in Mathematics, 228. Springer-Verlag, 2005.
- [11] W. Eberly: *Decomposition of algebras over finite fields and number fields*. Comput. Complexity **1** (1991), no. 2, 183–210.
- [12] B. Edixhoven, J.-M. Couveignes. *Computational aspects of modular forms and Galois representations*. Ann. of Math. Stud., 176, Princeton Univ. Press, Princeton, NJ, 2011.
- [13] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics, **150**, Springer-Verlag, New York, 1995.
- [14] K. Haberland. *Perioden von Modulformen einer Variablen and Gruppencohomologie. I, II, III*. Math. Nachr. **112** (1983), 245–282, 283–295, 297–315.
- [15] C. Khare, J. P. Wintenberger. *Serre’s modularity conjecture. I*. Invent. Math. **178** (2009), no. 3, 485–504
- [16] L. Merel. *Universal Fourier expansions of modular forms*, in *On Artin’s conjecture for odd 2-dimensional representations*, 59–94, Lecture Notes in Math., 1585, Springer, Berlin, 1994.
- [17] J.-P. Serre. *A course in arithmetic*. Translated from the French. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973. viii+115 pp.
- [18] J.-P. Serre. *Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* . Duke Mathematical Journal **54**, No. 1 (1987), 179–230.
- [19] K. Ribet. *On l -adic representations attached to modular forms. II*. Glasgow Math. J. **27** (1985), 185–194.
- [20] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Forms*. Princeton University Press, 1994.

- [21] W. A. Stein *Modular forms, a computational approach*. With an appendix by Paul E. Gunnells. Graduate Studies in Mathematics, 79. American Mathematical Society, Providence, RI, 2007.
- [22] C. A. Weibel. *An introduction to homological algebra*, Cambridge Univ. Press, Cambridge, 1994.
- [23] G. Wiese. *On the faithfulness of parabolic cohomology as a Hecke module over a finite field*. J. Reine Angew. Math. 606 (2007), 79–103.
- [24] G. Wiese. *On modular symbols and the cohomology of Hecke triangle surfaces*. Int. J. Number Theory 5 (2009), no. 1, 89–108.

Gabor Wiese
University of Luxembourg
Mathematics Research Unit
Maison du nombre
6, avenue de la Fonte
L-4364 Esch-sur-Alzette
Grand-Duchy of Luxembourg
gabor.wiese@uni.lu