Computational Arithmetic of Modular Forms

(Modulformen II)

Wintersemester 2007/2008

Universität Duisburg-Essen

Gabor Wiese
gabor.wiese@uni-due.de

Version of 4th February 2008

Preface

This lecture is about computing modular forms and some of their arithmetic properties.

We set the following challenging objectives:

- We explain and completely prove the *modular symbols algorithm* in as elementary and as explicit terms as possible. The chosen approach is based on group cohomology.
- The devoted student shall be enabled to implement the (group cohomological) modular symbols algorithm over any ring (such that a sufficient linear algebra theory is available in the chosen computer algebra system).
- We introduce the theory of Galois representations attached to modular forms in as explicit terms as possible. We explain some of its number theoretic significance and some computational approaches.
- The devoted student shall be enabled to compute important properties of Galois representations attached to modular forms explicitly.

According to these objectives the lecture consists of two main parts:

I. Computing Modular Forms

II. Computational Galois Representations

Due to the diversity of the audience, ranging from students up to PhD students intending to generalise the presented algorithms in different directions, and due to the dual aims, theoretic and algorithmic, the lecture is conceived in *parallel layers*. Not all layers need be followed by all students and all layers can be reduced individually. The layers are the following:

- Theory. Roughly in 3 of the 4h per week the lecture will introduce theoretical results. All students are expected to attend the lectures. The lectures will be accompanied by exercises concerning the theory presented. Exercises can be handed in and will be corrected. Some time will be devoted to discussing possible solutions.
- Algorithms and implementations. In a lecture in the beginning, programming in some standard computer algebra systems is introduced. In some lectures during the term, algorithms and possibly concrete implementations are presented. Much emphasis is laid on practical issues and students will also be asked to find and implement algorithms. Possible solutions will be discussed.
- Self-learn modules. For the devoted student to gain a more complete picture of the theory than can be presented during the lecture, complementary reading is suggested.

The parallel layers will not necessarily be on a single subject all the time, as it is often necessary to introduce theory first. The lecture is divided up into stages, instead of chapters, in order to emphasize the possible variety of subjects in each stage.

The conception of this lecture is different from every treatment I know, in particular, from William Stein's excellent book "Modular Forms: A Computational Approach" ([Stein]). Parts will, however, be similar to notes of a series of 4 lectures that I gave at the MSRI Graduate Workshop in Computational Number Theory "Computing With Modular Forms" ([MSRI]). 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 mention geometric approaches only in passing.

Organisational issues will be discussed with all participants and decided together in order to suit everybody.

Contents

Stage 1

Motivation and Survey

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

In the second part of the introduction, we will state and explain the theorems by Shimura, Deligne and Serre attaching a Galois representation to a Hecke eigenform. The modern number theoretic significance of modular forms arises from these theorems (e.g. the role of modular forms in the proof of Fermat's Last Theorem). We will also sketch which number theoretic information can be obtained from computing modular forms.

In the practically oriented part of the lecture, we shall introduce the computer algebra systems MAGMA and SAGE and also show how to use the modular forms and modular symbols packages that are already provided by these systems.

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

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

By Exercise 1 it is surjective. Its kernel is called $\Gamma(N)$. 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). In particular, the map $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \to (\mathbb{Z}/N\mathbb{Z})^2$ given by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$ takes all $\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right) \in (\mathbb{Z}/N\mathbb{Z})^2$ as image such that a, c generate $\mathbb{Z}/N\mathbb{Z}$ (that's due to the determinant being 1). We also point out that the image 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 consider the stabiliser of $\left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)$. We 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 $\left(\begin{smallmatrix}1&*\\0&1\end{smallmatrix}\right)$.

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 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 $\left(\begin{smallmatrix}*&*\\0&*\end{smallmatrix}\right)$. 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 $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. These observations are at the base of defining level structures for elliptic curves (see [MF]).

It is clear that

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

is a group isomorphism. We also let

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

denote a character, i.e. a group homomorphism. We shall extend χ to a map $(\mathbb{Z}/N\mathbb{Z}) \to \mathbb{C}$ by imposing $\chi(r) = 0$ if $(r, N) \neq 1$.

By class field theory or Exercise 2 we have the isomorphism

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

for all primes $l \nmid N$. By ζ_N we denote any primitive N-th root of unity. We shall, thus, later on also consider χ as a character of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. The name *Dirichlet character* (here of *modulus* N) is common usage for both.

Modular forms

We now recall the definitions of modular forms. We denote by $\mathbb{H}$ the upper half plane, i.e. the set $\{z \in \mathbb{C} | \mathrm{Im}(z) > 0\}$. The set of cusps is by definition $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$.

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

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

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

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

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

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

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

(i) the function $(f|_k \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))(z) = f(\frac{az+b}{cz+d})(cz+d)^{-k}$ is a holomorphic function (still from $\mathbb{H}$ to $\mathbb{C}$) for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ (this condition is called *f is holomorphic at the cusp a/c*), and

(ii) $(f|_k \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))(z) = f(\frac{az+b}{cz+d})(cz+d)^{-k} = f(z)$ for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$.

We use the notation $\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})$. If we replace (i) by

(i)' the function $(f|_k \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))(z) = f(\frac{az+b}{cz+d})(cz+d)^{-k}$ is a holomorphic function and the limit $f(\frac{az+b}{cz+d})(cz+d)^{-k}$ is 0 when z tends to $i\infty$ (we often just write ∞),

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

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

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

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

All these are finite dimensional $\mathbb{C}$-vector space and for $k \geq 2$, there are dimension formulae, which one can look up in [Stein]. 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 conceptually, as we have done in [MF]. Here is a definition by formulae.

If a is an integer coprime to N, by Exercise 3 we may let σ_a be a matrix in $\Gamma_0(N)$ such that

$$\sigma_a \equiv \left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right) \mod N. \tag{1.1.1}$$

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 $f \in \mathrm{M}_k(N, \chi\,;\,\mathbb{C})$, 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 $\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})$ and on $\mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{C})$, and the $\mathrm{M}_k(N, \chi\,;\,\mathbb{C})$ and $\mathrm{S}_k(N, \chi\,;\,\mathbb{C})$ are the χ-eigenspaces for this action.

Let l be a prime. We let

$$\mathcal{R}_l := \{\left(\begin{smallmatrix} 1 & r \\ 0 & l \end{smallmatrix}\right) | 0 \leq r \leq l-1\} \cup \{\sigma_l \left(\begin{smallmatrix} l & 0 \\ 0 & 1 \end{smallmatrix}\right)\}, \qquad \text{if } l \nmid N \tag{1.1.2}$$

$$\mathcal{R}_l := \{\left(\begin{smallmatrix} 1 & r \\ 0 & l \end{smallmatrix}\right) | 0 \leq r \leq l-1\}, \qquad \text{if } l \mid N \tag{1.1.3}$$

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

$$f|_k T_l = T_l f = \sum_{\delta \in \mathcal{R}_l} f|_k \delta.$$

Lemma 1.1.1 *Suppose $f \in \mathrm{M}_k(N, \chi\,; \mathbb{C})$. Recall that we have extended χ so that $\chi(l) = 0$ if l divides N. We have the formula*

$$a_n(T_l f) = a_{ln}(f) + l^{k-1}\chi(l) a_{n/l}(f).$$

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

Proof. Exercise 4. □

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

- $T_{l^{r+1}} = T_l \circ T_{l^r} - l^{k-1}\langle l \rangle T_{l^{r-1}}$ for all primes l and $r \geq 1$,
- $T_{uv} = T_u \circ T_v$ for coprime positive integers u, v.

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

$$a_1(T_n f) = a_n(f). \tag{1.1.4}$$

It is the only formula that we will really need.

From the above formulae it is also evident that the Hecke operators commute among one another. By Exercise 5 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 stage.

Finally, let us point out the formula (for l prime and $l \equiv d \mod N$)

$$l^{k-1}\langle d \rangle = T_l^2 - T_{l^2}. \tag{1.1.5}$$

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 $1 = l_1^{k-1} r + l_2^{k-1} s$.

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, however, show that the Hecke algebra is the dual of modular forms, and hence all knowledge about modular forms can - in principal - be derived from the Hecke algebra.

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

$$\mathbb{T}_{\mathbb{C}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})), \mathbb{T}_{\mathbb{C}}(\mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{C})), \mathbb{T}_{\mathbb{C}}(\mathrm{M}_k(N,\chi\,;\,\mathbb{C})) \text{ and } \mathbb{T}_{\mathbb{C}}(\mathrm{S}_k(N,\chi\,;\,\mathbb{C})),$$

respectively.

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

$$\mathrm{M}_k(N,\chi\,;\,\mathbb{C}) \times \mathbb{T}_{\mathbb{C}}(\mathrm{M}_k(N,\chi\,;\,\mathbb{C})) \to \mathbb{C}, \quad (f,T) \mapsto a_1(Tf)$$

(compare with Equation 1.1.4).

Lemma 1.1.2 *Suppose $k \geq 1$. The complex q-pairing is perfect, as is the analogous pairing for $\mathrm{S}_k(N,\chi\,;\,\mathbb{C})$. In particular,*

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

and similarly for $\mathrm{S}_k(N,\chi\,;\,\mathbb{C})$. For $\mathrm{S}_k(N,\chi\,;\,\mathbb{C})$, the inverse is given by $\phi \mapsto \sum_{n=1}^{\infty} \phi(T_n)q^n$.

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 1.1.4 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 $a_1(T(T_n f)) = a_1(T_n T f) = a_n(Tf) = 0$ 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 $\mathrm{M}_k(N,\chi\,;\,\mathbb{C})$ (resp. the cusp forms), we find $T = 0$, proving the non-degeneracy. □

The perfectness of the q-pairing is also called the *existence of a q-expansion principle*.

The Hecke algebra is the linear dual of the space of modular forms.

Lemma 1.1.3 *Let f in $\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})$ be a normalised eigenform. Then*

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

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

$$\{\text{Normalised eigenforms in } \mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})\} \leftrightarrow \mathrm{Hom}_{\mathbb{C}-\text{alg}}(\mathbb{T}_{\mathbb{C}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})),\mathbb{C}).$$

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

Proof. Exercise 6. □

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 [MerelUniversal], [Cremona] and [Stein], 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 7).

We introduce some definitions and notations to be used in all the lecture.

Definition 1.2.1 *Let R be a ring, Γ a group and V a left $R[\Gamma]$-module. The Γ-invariants of V are by definition*

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

The Γ-coinvariants of V are by definition

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

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 8 for some properties of these definitions. We shall make use of the results of this exercise in the section on group cohomology and probably also at other places.

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.

Definition 1.2.2 *We define the R-modules*

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

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*

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

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*

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

which is induced from the map $\mathcal{M}_R \to \mathcal{B}_R$ *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 9).

The modules $V_n(R)$ and $V_n^\chi(R)$

Let R be a ring. We put $V_n(R) = R[X, Y]_n \cong \mathrm{Sym}^n(R^2)$ (see Exercise 10). By $R[X, Y]_n$ we mean the homogeneous polynomials of degree n in two variables with coefficients in the ring R. By $\mathrm{Mat}_2(\mathbb{Z})_{\neq 0}$ we denote the $\mathbb{Z}$-module of integral 2×2-matrices with non-zero determinant. Then $V_n(R)$ is a $\mathrm{Mat}_2(\mathbb{Z})_{\neq 0}$-module in several natural ways.

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

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

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

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

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 $\Big(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\Big)^\iota \left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right)$ is equal to $(X, Y)\sigma^{-1}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\sigma$. More precisely, we have

the ismorphism $V_n(R) \xrightarrow{f\mapsto\sigma^{-1}.f} V_n(R)$, where the left hand side module carries "our" action and the right hand side module carries the other one. By $\sigma^{-1}.f$ we mean "our" $\sigma^{-1}.f$.

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

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

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

Let now $(\mathbb{Z}/N\mathbb{Z})^\times \to R^\times$ be a Dirichlet character, which we shall also consider as a character $\chi : \Gamma_0(N) \xrightarrow{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\mapsto a} (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\chi} R^\times$. 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. $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).r = \chi(a)r = \chi^{-1}(d)r$ for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$.

Note that due to $(\mathbb{Z}/N\mathbb{Z})^\times$ being an abelian group, the same formula makes R^χ also into a right $R[\Gamma_0(N)]$-module. Hence, putting $(f\otimes r).\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = (f|_k\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))\otimes\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) r$ makes $\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})\otimes_{\mathbb{C}} \mathbb{C}^\chi$ into a right $\Gamma_0(N)$-module and we have the description (Exercise 11)

$$\mathrm{M}_k(N,\chi\,;\,\mathbb{C}) = (\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})\otimes_{\mathbb{C}}\mathbb{C}^\chi)^{(\mathbb{Z}/N\mathbb{Z})^\times} \tag{1.2.6}$$

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

We let

$$V_n^\chi(R) := V_n(R)\otimes_R R^\chi$$

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

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 $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to R^\times$, which we also sometimes view as a group homomorphism $\Gamma_0(N) \to R^\times$ as above. We impose that $\chi(-1) = (-1)^k$.

We define

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

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

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

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 $\eta := \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Because of

$$\eta\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\eta = \left(\begin{smallmatrix} a & -b \\ -c & d \end{smallmatrix}\right)$$

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 $\mathrm{Mat}_2(\mathbb{Z})_{\neq 0}$-action, and on $V_{k-2}^{\chi}(R) = V_{k-2}(R) \otimes R^{\chi}$ 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 adavantage 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 [Stein], 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 "Hecke correspondence like" formulation in the section on Hecke operators on group cohomology.

The definition given here is also explained in detail in [Stein]. We should also mention the very important fact that one can transfer Hecke operators in an explicit way to Manin symbols. Also that point is discussed in detail in [Stein].

We now give the definition only for T_l for a prime l and diamond operators. The T_n for composite n can be computed from those by the formulae already stated in the beginning. 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 1.1.2). 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

$$T_p x = \sum_{\delta \in \mathcal{R}_l} \delta.x.$$

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 1.1.1. When $x \in \mathcal{M}_k(N, \chi\,;\, R)$, we have $\langle a \rangle x = \chi(a)x$.

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 stage, 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 $\mathcal{M}_k(\Gamma_1(n)\,;\,R)$ generated by the Hecke operators T_n. For a character $\chi : \mathbb{Z}/N\mathbb{Z} \to R^\times$, 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, which will be derived in a later chapter. Here, we already want to use it.

Fact 1.2.3 *The R-modules $\mathcal{M}_k(\Gamma_1(N)\,;\,R)$, $\mathcal{CM}_k(\Gamma_1(N)\,;\,R)$, $\mathcal{M}_k(N,\chi\,;\,R)$ and $\mathcal{CM}_k(N,\chi\,;\,R)$ are finitely presented R-modules.*

Corollary 1.2.4 *Let R be a Noetherian ring. The Hecke algebras*

$$\mathbb{T}_R(\mathcal{M}_k(\Gamma_1(N)\,;\,R)), \mathbb{T}_R(\mathcal{CM}_k(\Gamma_1(N)\,;\,R)), \mathbb{T}_R(\mathcal{M}_k(N,\chi\,;\,R)) \text{ and } \mathbb{T}_R(\mathcal{CM}_k(N,\chi\,;\,R))$$

are finitely presented R-modules.

Proof. This follows from Fact 1.2.3, since the endomorphism ring of a finitely presented module is finitely presented and submodules of finitely presented modules over Noetherian rings are finitely presented. □

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 $R = \mathbb{Z}[\chi]$ and $S = \mathbb{C}$.

Proposition 1.2.5 *Let R be a Noetherian ring and $R \to S$ 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.

(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.

(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.

(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

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

is an isomorphism.

For a character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to R^\times$, 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 9 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

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

is an isomorphism (see [Eisenbud], 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 [Eisenbud] 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 $\mathbb{T}_R(M) \to \mathbb{T}_R(M) \otimes_R S \xrightarrow{\psi} S$. 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:

$$0 \to F \to M \to M/F \to 0.$$

From flatness we get the exact sequence

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

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 $0 = T\pi m = \pi T m$. Thus $Tm \in N$ and, so, $rTm = 0$, as claimed. In other words, the kernel of the homomorphism $\mathbb{T}_R(M) \to \mathbb{T}_R(M \otimes_R S)$ 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. □

Some words of warning are necessary. It is essential that $R \to S$ is a flat homomorphism. A similar result for $\mathbb{Z} \to \mathbb{F}_p$ 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.

Moreover, $\mathcal{M}_k(\Gamma_1(N)\,;\,R)$ need not be a free R-module and can contain torsion. We will later in the lecture calculate this torsion, at least for certain rings R.

Please have a look at Exercise 12 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 1.3.1 (Eichler-Shimura) *There are isomorphisms respecting the Hecke operators*

(a) $\mathrm{M}_k(N,\chi\,;\,\mathbb{C})) \oplus \mathrm{S}_k(N,\chi\,;\,\mathbb{C})^\vee \cong \mathcal{M}_k(N,\chi\,;\,\mathbb{C})$,

(b) $\mathrm{S}_k(N,\chi\,;\,\mathbb{C})) \oplus \mathrm{S}_k(N,\chi\,;\,\mathbb{C})^\vee \cong \mathcal{CM}_k(N,\chi\,;\,\mathbb{C})$,

(c) $\mathrm{S}_k(N,\chi\,;\,\mathbb{C}) \cong \mathcal{CM}_k(N,\chi\,;\,\mathbb{C})^+$.

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

Proof. Later in this lecture. Those who already want to have an indication about the proof are referred to [Diamond-Im], Theorem 12.2.2. There the language of group cohomology is used, as we will do in this lecture. So, the reader should believe the fact - to be proved later this lecture, too - that the group cohomology in [Diamond-Im] coincides with the modular symbols. □

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 stage.

Corollary 1.3.2 *Let R be a subring of $\mathbb{C}$ and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to R^\times$ a character. Then the natural map*

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

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

Proof. We only prove this for the full space of modular forms. The arguments for cusp forms are very similar. Theorem 1.3.1 tells us that the R-algebra generated by the Hecke operators inside the endomorphism ring of $\mathrm{M}_k(N, \chi\,;\, \mathbb{C})$ equals the R-algebra generated by the Hecke operators inside the endomorphism ring of $\mathcal{M}_k(N, \chi\,;\, \mathbb{C})$. i.e.

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

To see this, one just need to see that the algebra generated on $\mathrm{M}_k(N, \chi\,;\, \mathbb{C})) \oplus \mathrm{S}_k(N, \chi\,;\, \mathbb{C})^\vee$ is the same as the one generated on $\mathrm{M}_k(N, \chi\,;\, \mathbb{C}))$, which follows from the fact that if some T annihilates the full space of modular forms, then it also annihilates the dual of the cusp space.

Tensoring with $\mathbb{C}$ we get

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

using Proposition 1.2.5 (d) and again Theorem 1.3.1. □

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 1.3.3 *Let R be a subring of $\mathbb{C}$ and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to R^\times$ a character. Then*

(a) $\mathrm{M}_k(N, \chi\,;\, \mathbb{C}) \cong \mathrm{Hom}_R(\mathbb{T}_R(\mathcal{M}_k(N, \chi\,;\, R)), R) \otimes_R \mathbb{C} \cong \mathrm{Hom}_R(\mathbb{T}_R(\mathcal{M}_k(N, \chi\,;\, R)), \mathbb{C})$ *and*

(b) $\mathrm{S}_k(N, \chi\,;\, \mathbb{C}) \cong \mathrm{Hom}_R(\mathbb{T}_R(\mathcal{CM}_k(N, \chi\,;\, R)), R) \otimes_R \mathbb{C} \cong \mathrm{Hom}_R(\mathbb{T}_R(\mathcal{CM}_k(N, \chi\,;\, R)), \mathbb{C})$.

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

Proof. This follows from Corollary 1.3.2, Proposition 1.2.5 and Lemma 1.1.2. □

Please look at Exercise 13 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 1.3.4 *Let $f = \sum_{n=1}^{\infty} a_n(f) q^n \in \mathrm{S}_k(\Gamma_1(N)\,;\, \mathbb{C})$ 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 $\dim_{\mathbb{C}} \mathrm{S}_k(\Gamma_1(N)\,;\, \mathbb{C})$.*

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 $\dim_{\mathbb{C}} \mathrm{S}_k(N, \chi\,;\, \mathbb{C})$. 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 $\mathbb{C}$. □

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

(1) Create $M := \mathcal{CM}_k(N, \chi\,; K)$.

(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 $\dim_K(\mathbb{T}) = \dim_{\mathbb{C}} \mathrm{S}_k(N, \chi\,; \mathbb{C})$

(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 $\mathrm{S}_k(N, \chi\,; \mathbb{C})$. In last term's lecture [MF] we gave some of them. The general case can be looked up in [Stein].

It is clear that the repeat-until loop will stop, due to Corollary 1.3.3. We can even give an upper bound as to when it stops at the latest. That is the so-called Sturm bound, which we also treated in last term's course [MF] in some cases (even weights, no character; to get the formulation here, one should plug in the formula used in the proof of Lemma 3.3.33 into the Sturm bound of Satz 3.3.37).

Proposition 1.3.6 (Sturm) *Let $f \in \mathrm{M}_k(N, \chi\,;\, \mathbb{C})$ such that $a_n(f) = 0$ for all $n \leq \frac{k\mu}{12}$, where $\mu = N \prod_{l|N \text{ prime}}(1 + \frac{1}{l})$.*

Then $f = 0$.

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

Corollary 1.3.7 *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 $T_1, T_2, \ldots, T_{\frac{k\mu}{12}}$.*

Proof. Exercise 14. □

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

Galois representations attached to eigenforms

We mention the sad fact that until 2006 only the one-dimensional representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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 $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for each number field K. Since we now have Serre's conjecture (a theorem by Khare, Wintenberger and Kisin), we also know a little bit about 2-dimensional representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, but, replacing $\mathbb{Q}$ by any other number field, all one has is conjectures.

[Added an explanation of the p-cyclotomic character, the notion of unramified primes of Galois representations and Frobenius elements.]

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 $k \geq 2$.

Theorem 1.4.1 *Let $k \geq 2$, $N \geq 1$, p a prime not dividing N, and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ a character.*

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

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

such that

(i) *ρ_f is irreducible,*

(ii) *$\rho_f(c) = -1$ for any complex conjugation $c \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (one says that ρ_f is* odd*),*

(iii) for all primes $l \nmid Np$ the representation ρ_f is unramified at l,

$$\mathrm{Tr}(\rho_f(\mathrm{Frob}_l)) = a_l(f) \quad \textit{and} \quad \det(\rho_f(\mathrm{Frob}_l)) = \epsilon_p(l)^{k-1}\chi(l).$$

In the statement, Frob_l denotes a Frobenius element at l, and ϵ_p is the p-cyclotomic character.

By choosing a lattice in $\mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ containing $\rho(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, and applying reduction and semi-simplification one obtains the following consequence.

Theorem 1.4.2 *Let $k \geq 2$, $N \geq 1$, p a prime not dividing N, and $\overline{\chi} : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$ a character.*

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

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

such that

(i) ρ_f is semi-simple,

(ii) $\rho_f(c) = -1$ for any complex conjugation $c \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (one says that ρ_f is odd*),*

(iii) for all primes $l \nmid Np$ the representation ρ_f is unramified at l,

$$\mathrm{Tr}(\rho_f(\mathrm{Frob}_l)) \equiv a_l(f) \mod \mathfrak{P} \quad \textit{and} \quad \det(\rho_f(\mathrm{Frob}_l)) \equiv l^{k-1}\overline{\chi}(l) \mod \mathfrak{P}.$$

Translation to number fields

Proposition 1.4.3 *Let f, $\mathbb{Q}_f$, $\mathfrak{P}$ and ρ_f be as in Theorem 1.4.2. Then the following hold:*

(a) The image of ρ_f is finite and its image is contained in $\mathrm{GL}_2(\mathbb{F}_{p^r})$ for some r.

(b) The kernel of ρ_f is an open subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and is hence of the form $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for some Galois number field K. Thus, we can and do consider $\mathrm{Gal}(K/\mathbb{Q})$ as a subgroup of $\mathrm{GL}_2(\mathbb{F}_{p^r})$.

(c) The characteristic polynomial of Frob_l (more precisely, of $\mathrm{Frob}_{\Lambda/l}$ for any prime Λ of K dividing l) is equal to $X^2 - a_l(f)X + \chi(l)l^{k-1} \mod \mathfrak{P}$ for all primes $l \nmid Np$.

Proof. Exercise 15. □

To appreciate the information obtained from the $a_l(f) \mod \mathfrak{P}$, the reader is invited to do Exercise 16 now.

Images of Galois representations

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

Theorem 1.4.4 (Dickson) *Let p be a prime and H a finite subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_p)$. Then a conjugate of H is isomorphic to one of the following groups:*

- *finite subgroups of the upper triangular matrices,*
- $\mathrm{PSL}_2(\mathbb{F}_{p^r})$ *or* $\mathrm{PGL}_2(\mathbb{F}_{p^r})$ *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. 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 (to be defined later) this means that if G is the image, then G modulo scalars is equal to $\mathrm{PSL}_2(\mathbb{F}_{p^r})$ or $\mathrm{PGL}_2(\mathbb{F}_{p^r})$, where $\mathbb{F}_{p^r}$ is the extension of $\mathbb{F}_p$ generated by the $a_n(f) \mod \mathfrak{P}$. More precise results will be given later.

An interesting question is to study which groups (i.e. which $\mathrm{PSL}_2(\mathbb{F}_{p^r})$) occur in practice. It would be nice to prove that all of them do, since - surprisingly - the simple groups $\mathrm{PSL}_2(\mathbb{F}_{p^r})$ 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 conjecture

If time allows, we plan to explain this topic in more detail in the second part of this lecture.

Serre's conjecture is the following. Let p be a prime and $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ 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 [Serre].
- Let χ_ρ be the prime-to-p part of $\det \circ \rho$ considered as a character $(\mathbb{Z}/N_\rho\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$.

Conjecture 1.4.5 (Serre) *Let p be a prime and $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be a continuous, odd, irreducible representation. Define N_ρ, $k(\rho)$, k_ρ and χ_ρ as above.*

- *(Strong form) There exists a normalised eigenform $f \in \mathrm{S}_{k_\rho}(N_\rho, \chi_\rho\,; \overline{\mathbb{F}}_p)$*

- *(Weak form) There exist N, k, χ and a normalised eigenform $f \in \mathrm{S}_k(N, \chi\,; \overline{\mathbb{F}}_p)$*

such that ρ is isomorphic to the Galois representation

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

attached to f by Theorem 1.4.2.

It is known that the weak form implies the strong form. However, there is a "strongest" form with a slightly different definition of weight. There is still an open case for $p = 2$ for the strongest form.

As mentioned above, Serre's conjecture is now a theorem by Khare, Wintenberger and Kisin.

Serre's 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 eigenform it comes from. Conceptually, Serre's conjecture gives an explicit description of all irreducible, odd and continuous "mod p" representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and, thus, in a sense generalises class field theory.

Edixhoven and coworkers have recently 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 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

1.5 Theory: Exercises

Exercise 1 *(a) The group homomorphism*

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

given by reducing the matrices modulo N is surjective.

(b) Check the bijections

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

and

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

which were given in the beginning.

Exercise 2 *Let N be an integer and $\zeta_N \in \mathbb{C}$ any primitive n-th root of unity. Prove that the map*

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

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

Exercise 3 *Prove that a matrix σ_a as in Equation 1.1.1 exists.*

Exercise 4 *Proof Lemma 1.1.1.*

Exercise 5 *(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. $V_1 = \{v | T_1 v = \lambda_1 v\}$. Prove that $T_2V_1 \subseteq V_1$.*

(b) Suppose that $\mathrm{M}_N(\Gamma_1(k)\,;\,\mathbb{C})$ is non-empty. Prove that it contains a Hecke eigenform.

Exercise 6 *Prove Lemma 1.1.3.*

Exercise 7 *Check that it makes sense to replace $\mathrm{SL}_2(\mathbb{Z})$ by $\mathrm{PSL}_2(\mathbb{Z})$ in the definition of modular forms.*

Exercise 8 *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

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

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 9 *Let R, Γ and V as in Definition 1.2.2 and let $R \to S$ 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 $R \to S$ 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 10 *Prove that the map*

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

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 $\{1, 2, \ldots, n\}$.

Exercise 11 *Prove Equation 1.2.6.*

Exercise 12 *Can one use $+$- or $-$-spaces in Proposition 1.2.5? What could we say if we defined the $+$-space as $M/(1-\eta)M$ with M standing for some space of modular symbols?*

Exercise 13 *Which statements in the spirit of Corollary 1.3.3 (b) are true for the $+$-spaces?*

Exercise 14 *Prove Corollary 1.3.7.*

Exercise 15 *Prove Propsition 1.4.3.*

Exercise 16 *In how far is a conjugacy class in $\mathrm{GL}_2(\mathbb{F}_{p^r})$ determined by its characteristic polynomial?*

Let $G \subset \mathrm{GL}_2(\mathbb{F}_{p^r})$ be a subgroup. Same question as above for G.

1.6 Algorithms and Implementations: MAGMA and SAGE

Introduction to MAGMA

Please download the example file "MagmaIntro" from the web page. It will be explained during the lecture.

Introduction to SAGE

We shall not have time to present SAGE in detail. Please try to find the analogues of the topics presented for MAGMA yourself. The web pages for SAGE are:
http://sage.apcocoa.org/
http://www.sagemath.org/

1.7 Algorithms and Implementations: Modular symbols in MAGMA

Please download the example file "ModularSymbols" from the web page. It will be explained during the lecture.

1.8 Computer exercises

Computer exercise 1 *(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 2 *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*. Outut: A list* $[n_1, n_2, n_3, \ldots, n_m]$ *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* $[r_1, r_2, \ldots, r_m]$ *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 3 *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 4 *(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 5 *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:*

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

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 `PlayHanoi` *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, one must put the command `forward my_procedure` *in front of the definition of* `my_procedure`*.]*

Computer exercise 6 *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 7 *Try to implement Algorithm 1.3.5.*
If it is still too difficult, don't worry. We will be getting there.

1.9 Self-learn module:

Those not familiar enough with the theory of modular forms are invited to read the basics on modular forms.

Part I

Computing Modular Forms

Stage 2

Hecke algebras

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 lecture 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 stage.

Hecke algebras of modular forms over R are finitely generated as 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 $\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})$ as the subring (i.e. the $\mathbb{Z}$-algebra) inside the endomorphism ring of the $\mathbb{C}$-vector space $\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})$ generated by all Hecke operators. Remember that due to Formula 1.1.5 all diamond operators are contained in the Hecke algebra. Of course, we make similar definitions for $\mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{C})$ and use the notations $\mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C}))$ and $\mathbb{T}_{\mathbb{Z}}(\mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{C}))$.

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 $\mathrm{M}_k(N,\chi\,;\,\mathbb{C})$ (notation $\mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(N,\chi\,;\,\mathbb{C}))$) or, secondly, as the $\mathbb{Z}[\chi]$-algebra generated by the Hecke operators inside $\mathrm{End}_{\mathbb{C}}(\mathrm{M}_k(N,\chi\,;\,\mathbb{C}))$ (notation $\mathbb{T}_{\mathbb{Z}[\chi]}(\mathrm{M}_k(N,\chi\,;\,\mathbb{C}))$); 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 $\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})$ 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 $\mathrm{M}_k(N,\chi\,;\,\mathbb{C})$ equals the $\mathbb{Q}[\chi]$-dimension of $\mathbb{T}_{\mathbb{Q}[\chi]}(\mathrm{M}_k(N,\chi\,;\,\mathbb{C}))$ and not the $\mathbb{Q}$-dimension of $\mathbb{T}_{\mathbb{Q}}(\mathrm{M}_k(N,\chi\,;\,\mathbb{C}))$.

Lemma 2.1.1 *(a) The $\mathbb{Z}$-algebras $\mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C}))$ and $\mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(N,\chi\,;\,\mathbb{C}))$ are free $\mathbb{Z}$-modules of finite rank; the same holds for the cuspidal Hecke algebras.*

(b) The $\mathbb{Z}[\chi]$-algebra $\mathbb{T}_{\mathbb{Z}[\chi]}(\mathrm{M}_k(N,\chi\,;\,\mathbb{C}))$ 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 1.3.2) 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. □

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

$$\mathrm{M}_k(\Gamma_1(N)\,;\,R) := \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})), R) \cong \mathrm{Hom}_R(\mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})) \otimes_{\mathbb{Z}} R, R).$$

The isomorphism is proved precisely as in Proposition 1.2.5 (c), where we did not use the flatness assumption. Every element f of $\mathrm{M}_k(\Gamma_1(N)\,;\,R)$ thus corresponds to a $\mathbb{Z}$-linear function $\Phi : \mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})) \to R$ 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 $\mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C}))$ acts naturally on $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})), R)$, namely by

$$(T.\Phi)(S) = \Phi(TS) = \Phi(ST).$$

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

$$\mathrm{S}_k(\Gamma_1(N)\,;\,R) := \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(\mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{C})), R) \cong \mathrm{Hom}_R(\mathbb{T}_{\mathbb{Z}}(\mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{C})) \otimes_{\mathbb{Z}} R, R).$$

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 $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character and $\mathbb{Z}[\chi] \to R$ 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

$$\mathrm{M}_k(N, \chi\,;\,R) := \mathrm{Hom}_{\mathbb{Z}[\chi]}(\mathbb{T}_{\mathbb{Z}[\chi]}(\mathrm{M}_k(N, \chi\,;\,\mathbb{C})), R) \cong \mathrm{Hom}_R(\mathbb{T}_{\mathbb{Z}[\chi]}(\mathrm{M}_k(N, \chi\,;\,\mathbb{C})) \otimes_{\mathbb{Z}[\chi]} R, R)$$

and similarly for the cusp forms.

We remark that the two definitions of $\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})$, $\mathrm{M}_k(N, \chi\,;\,\mathbb{C})$ etc. agree. As a special case, we get that $\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{Z})$ precisely consists of those holomorphic forms 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 $\mathrm{M}_k(N, \overline{\chi}\,;\,\mathbb{F})$ the space of *mod p modular forms of weight k, level N and character $\overline{\chi}$ (over $\mathbb{F}$)*. By $\overline{\chi}$ we mean $\pi \circ \chi$, which we write to point out that the definition of $\mathrm{M}_k(N, \overline{\chi}\,;\,\mathbb{F})$ only depends on $\pi \circ \chi$. Of course, for the cuspidal space similar statements hold and we use similar notations.

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

Proposition 2.1.2 *(a) Let $\mathbb{Z} \to R \to S$ be ring homomorphisms. Then the following statements hold.*

(i) The natural map

$$\mathrm{M}_k(\Gamma_1(N)\,;\,R) \otimes_R S \to \mathrm{M}_k(\Gamma_1(N)\,;\,S)$$

is an isomorphism.

(ii) The evaluation pairing

$$\mathrm{M}_k(\Gamma_1(N)\,;\,R) \times \mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})) \otimes_{\mathbb{Z}} R \to R$$

is the q-pairing and it is perfect.

(iii) The algebra $\mathbb{T}_R(\mathrm{M}_k(\Gamma_1(N)\,;\,R))$ is naturally isomorphic to $\mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})) \otimes_{\mathbb{Z}} R$.

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

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

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 $\mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C}))$. It is a free $\mathbb{Z}$-module by Lemma 2.1.1. We have

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

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

(ii) The evaluation pairing $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}, \mathbb{Z}) \times \mathbb{T}_{\mathbb{Z}} \to \mathbb{Z}$ 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

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

and show that it is injective. Its image is by definition $\mathbb{T}_R(\mathrm{M}_k(\Gamma_1(N)\,;\,R))$. 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

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

as desired.

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

Galois conjugacy classes

Recall that the normalised eigenforms in $\mathrm{M}_k(\Gamma_1(N)\,;\,R)$ are precisely the set of $\mathbb{Z}$-algebra homomorphisms inside $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})), R)$. 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 field K (if we are working with a Dirichlet character, we also want that K admits a ring homomorphism $\mathbb{Z}[\chi] \to K$). Denote by $\overline{K}$ a separable closure, so that we have

$$\mathrm{M}_k(\Gamma_1(N)\,;\,\overline{K}) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})),\overline{K}) \cong \mathrm{Hom}_K(\mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C}))\otimes_{\mathbb{Z}} K,\overline{K}).$$

We can compose any $\Phi \in \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})),\overline{K})$ by any Galois automorphism $\sigma : \overline{K} \to \overline{K}$ fixing K. Thus, we obtain an action of the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$ on $\mathrm{M}_k(\Gamma_1(N)\,;\,\overline{K})$ (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 2.1.3 *We have the following bijective correspondences.*

$$\mathrm{Spec}(\mathbb{T}_K(\cdot)) \overset{1-1}{\leftrightarrow} \mathrm{Hom}_{K\text{-alg}}(\mathbb{T}_K(\cdot),\overline{K})/\,\mathrm{Gal}(\overline{K}/K) \overset{1-1}{\leftrightarrow} \{\text{ normalised eigenf. in } \cdot\,\}/\,\mathrm{Gal}(\overline{K}/K)$$

and with $K = \overline{K}$

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

Here, $\cdot$ *stands for either* $\mathrm{M}_k(\Gamma_1(N)\,;\,\overline{K})$, $\mathrm{S}_k(\Gamma_1(N)\,;\,\overline{K})$ *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 18. □

We repeat that the coefficients of any eigenform f in $\mathrm{M}_k(N,\chi\,;\,\overline{K})$ lie in a finite extension of K, namely in $\mathbb{T}_K(\mathrm{M}_k(N,\chi\,;\,K))/\mathfrak{m}$, 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 $\mathfrak{a}^\infty$ for $\mathfrak{a}^n$.

Proposition 2.1.4 *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 $\mathfrak{m}^\infty$.

(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 $\bigcap_{\mathfrak{m}\in \mathrm{Spec}(\mathbb{T})} \mathfrak{m}$ is equal to the nilradical and consists of the nilpotent elements.

(f) We have $\bigcap_{\mathfrak{m}\in \mathrm{Spec}(\mathbb{T})} \mathfrak{m}^\infty = (0)$.

(g) (Chinese Remainder Theorem) The natural map

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

is an isomorphism.

(h) For every maxmimal 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 $\mathbb{T} \twoheadrightarrow \mathbb{T}/\mathfrak{p}$ 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 $\mathfrak{m}_i \not\subseteq \mathfrak{m}_{n+1}$ 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 $\mathfrak{m} \in \mathrm{Spec}(\mathbb{T})$ 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, $\mathfrak{m}^\infty$ and $\mathfrak{n}^\infty$ 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

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

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

(g) The injectivity follows from (f). It suffices to show that the elements $(0, \ldots, 0, 1, 0, \ldots, 0)$ 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 $a_\mathfrak{n} \in \mathfrak{n}^\infty$ and $a_\mathfrak{m} \in \mathfrak{m}^\infty$ such that $1 = a_\mathfrak{m} + a_\mathfrak{n}$. Let $x := \prod_{\mathfrak{n}\in\mathrm{Spec}(\mathbb{T}),\mathfrak{n}\neq\mathfrak{m}} a_\mathfrak{n}$. We have $x \in \prod_{\mathfrak{n}\in\mathrm{Spec}(\mathbb{T}),\mathfrak{n}\neq\mathfrak{m}} \mathfrak{n}^\infty$ and $x = \prod_{\mathfrak{n}\in\mathrm{Spec}(\mathbb{T}),\mathfrak{n}\neq\mathfrak{m}}(1 - a_\mathfrak{m}) \equiv 1 \mod \mathfrak{m}$. Hence, the map sends x to $(0, \ldots, 0, 1, 0, \ldots, 0)$, proving the surjectivity.

(h) By (c), the only maximal ideal of $\mathbb{T}$ containing $\mathfrak{m}^\infty$ 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 $\prod_{\mathfrak{n}\in\mathrm{Spec}(\mathbb{T}),\mathfrak{n}\neq\mathfrak{m}} \mathfrak{n}^\infty$, but not it $\mathfrak{m}$. By (f) and (d), $(0) = \prod_{\mathfrak{m}\in\mathrm{Spec}(\mathbb{T})} \mathfrak{m}^\infty$. Thus, $y \cdot x = 0$ and also $\frac{y}{s} = \frac{yx}{sx} = 0$, proving the injectivity. □

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 $(\ldots, x_\mathfrak{m}, \ldots)$ with $x_\mathfrak{m} \in \{0, 1\} \subseteq \mathbb{T}/\mathfrak{m}^\infty$.

Definition 2.1.5 *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 $\{e_1, \ldots, e_n\}$ is said to be* complete *if $1 = \sum_{i=1}^n e_i$.*

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

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

In Exercise 19, you are asked (among other things) to prove that in the above case $\mathfrak{m}^\infty$ 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 2.1.4.

Proposition 2.1.6 (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*

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

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

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

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

Proof. [Eisenbud], Theorem 7.3. □

[Recall the term *Krull dimension* and *height* of a prime ideal.]

Proposition 2.1.7 *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 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 $\mathcal{O} \to S$ 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 $\mathbb{T}_K$ under extension (i.e. $\mathfrak{p}\mathbb{T}_K$), 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

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

(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 $\mathbb{T}_K$ decomposes as

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

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 by the correspondence of prime ideals between 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 $\widehat{\mathcal{O}}$-module. Hence, it is either a finite field or a finite extension of $\widehat{\mathcal{O}}$. 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 20. [This part could be explained with a bit more detail.]

We have already seen Parts (c) and (d) in Lemma 2.1.4. Part (b) follows from (c) by applying Hensel's lemma (Proposition 2.1.6) to the idempotents of the decomposition of (c). We follow [Eisenbud], Corollary 7.5, for the details. Since $\widehat{\mathcal{O}}$ is complete with respect to some ideal $\mathfrak{p}$, so is $\mathbb{T}_{\widehat{\mathcal{O}}}$. Hence, we may use Hensel's lemma in $\mathbb{T}_{\widehat{\mathcal{O}}}$.

Given an idempotent $\overline{e}$ 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 $\overline{e}$ and let $f(X) = X^2 - X$ be a polynomial annihilating $\overline{e}$. We have that $f'(e) = 2e - 1$ is a unit, since $(2e-1)^2 \equiv 1 \mod \mathfrak{p}$. Hensel's lemma now gives us a unique root $e_1 \in \mathbb{T}_{\widehat{\mathcal{O}}}$ of f, i.e. an idempotent, lifting $\overline{e}$.

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. □

2.1.2 Commutative algebra of Hecke algebras

Let $k \geq 1$, $N \geq 1$ and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. 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 K. For $\mathbb{T}_{\mathcal{O}}(\mathrm{M}_k(N,\chi\,;\mathbb{C}))$ 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 2.1.7 to $\mathbb{T}_{\widehat{\mathcal{O}}}$. It is a free $\widehat{\mathcal{O}}$-module of finite rank (as it is torsion-free), which has Krull dimension 1, i.e. every maximal prime contains at least one minimal prime.

By Proposition 2.1.7, minimal primes of $\mathbb{T}_{\widehat{\mathcal{O}}}$ correspond to the maximal primes of $\mathbb{T}_K$ and hence to $\mathrm{Gal}(\overline{K}/K)$-conjugacy classes of eigenforms in $\mathrm{M}_k(N,\chi\,;\,\overline{K})$. By a brute force identification of $\overline{K}=\overline{\mathbb{Q}}_p$ 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 2.1.7, maximal primes of $\mathbb{T}_{\widehat{\mathcal{O}}}$ correspond to the maximal primes of $\mathbb{T}_{\mathbb{F}}$ and hence to $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$-conjugacy classes of eigenforms in $\mathrm{M}_k(N,\chi\,;\,\overline{\mathbb{F}})$.

The spectrum of $\mathbb{T}_{\widehat{\mathcal{O}}}$ 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 $\mathbb{T}_{\mathcal{O}}\to\mathbb{C}$, 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 $\mathrm{M}_k(N,\chi\,;\,\mathbb{C})$ is the formal q-expansion of an eigenform in $\mathrm{M}_k(N,\chi\,;\,\overline{\mathbb{F}})$.

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

Due to Exercise 21, we may speak about *reductions modulo* p of $\mathrm{Gal}(\overline{K}/K)$-conjugacy classes of normalised eigenforms to $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$-conjugacy classes. We hence say that two $\mathrm{Gal}(\overline{K}/K)$-conjugacy classes, say corresponding to normalised eigenforms f,g, respectively, minimal ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of $\mathbb{T}_{\widehat{\mathcal{O}}}$, are *congruent modulo* p, if they reduce to the same $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$-conjugacy class.

Proposition 2.1.8 *The $\mathrm{Gal}(\overline{K}/K)$-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 22. □

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 $\mathbb{Q}_f=\mathbb{Q}(a_n|n\in\mathbb{N})$.

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.

2.2.1 Primary spaces

Lemma 2.2.1 *(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 such that for all $a\in A$ the minimal polynomial of a on V is a prime power in $K[X]$, i.e. V is a primary space for all $a\in A$. Then the image of A in $\mathrm{End}(V)$ is a local algebra.

(c) Let V be an A-module and let $a_1, \ldots, a_n$ be generators of the algebra A. Suppose that for $i \in \{1, \ldots, n\}$ the minimal polynomial of $\overline{a_i}$ 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_K in $\mathrm{End}(V)$ is a local algebra.

Proof. (a) Suppose first that A is local and take $a \in A$. Let $\phi_a : K[X] \to A$ 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 a 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 $ab - \lambda\mu = (a-\lambda)(b-\mu) + \lambda(b-\mu) + \mu(a-\lambda)$. □

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 23 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 a paper by Wayne Eberly.

Proposition 2.2.2 *Let K be a field of characteristic 0 or a finite field. Let A be a finite dimensional algebra over K and let $a_1, \ldots, a_n$ 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

$$A \xrightarrow{\sim\ \alpha} \prod_{j=1}^{r} A_j$$

with $r \geq 2$. Let K_j be the residue field of A_j. The assumption on the basis means that the minimal polynomial of $a_i|_{A_j} = p_i^{r_{i,j}}$ with p_i irreducible and certain $r_{i,j}$. The normal closure N of K_j over K is equal to the splitting field of the polynomials p_i for $i = 1, \ldots, n$ and is hence independent of j. Moreover, $\mathrm{Tr}_{N/K}(\pi \circ \alpha(a_i)|_{K_j})$ is also independent of j with $\pi : \prod_{j=1}^r A_j \twoheadrightarrow \prod_{j=1}^r K_j$, since the minimal polynomial of $\pi \circ \alpha(a_i)|_{K_j}$ is independent of j.

We now use the assumptions on K. By Exercise 24 there is $x \in K_1$ such that $\mathrm{Tr}_{N/K}(x) \neq 0$. In A we take an element $y = \sum_{i=1}^r s_i a_i$ which maps to $(x, 0, \ldots, 0) \in \prod_{j=1}^r K_j$ under $\pi \circ \alpha$, i.e.

$$x = \sum_{i=1}^{n} s_i \cdot (\pi \circ \alpha(a_i)|_{K_1}) \text{ and}$$
$$0 = \sum_{i=1}^{n} s_i \cdot (\pi \circ \alpha(a_i)|_{K_2}).$$

The traces for N/K of the right hand side of the two equations are equal; on the left hand side they are not. This contradiction proves the proposition. □

Lemma 2.2.3 *Let A be a local finite dimensional algebra over a perfect field K. Let $a_1, \ldots, a_n$ 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 diagonalisable (over a separable closure - considering the algebra as a matrix algebra), 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. □

Proposition 2.2.4 *Let A be a local finite dimensional algebra over a perfect field K. Let $a_1, \ldots, a_n$ be a set of K-algebra generators of A. Let $p_i^{e_i}$ be the minimal polynomial of a_i (see Lemma 2.2.1).*

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

Proof. Let $\mathfrak{a}$ be the ideal generated by $\{p_1(a_1), \ldots, p_n(a_n)\}$. The quotient $\mathbb{T}/\mathfrak{a}$ is generated by the images of the a_i, call them $\overline{a_i}$. We claim that either $\overline{a_i} = 0$ or the minimal polynomial of $\overline{a_i}$ is equal to p_i. For, as $p_i(a_i) \in \mathfrak{a}$, it follows $p_i(\overline{a_i}) = 0$, whence the minimal polynomial of $\overline{a_i}$ divides the prime polynomial p_i, so that they are equal if $\overline{a_i} \neq 0$. By Lemma 2.2.3, we know that $\mathbb{T}/\mathfrak{a}$ is a field, whence $\mathfrak{a}$ is the maximal ideal. □

2.2.2 Algorithm for computing common primary spaces

[Recalled that one can think about finite dimensional algebras over a field as algebras of matrices and that the localisation statements of this section just mean writing the matrices as blocks.]

By a *common primary space* for commuting matrices we mean a subvector space of the underlying vector space on which the minimal polynomials of the given matrices are prime powers. By Proposition 2.2.2, 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 subvector space 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 2.2.5 Input: A list ops of operators acting on the K-vector space V.

Output: A 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 2.2.5 it is possible to compute a complete set of orthogonal idempotents for A. We now sketch a direct algorithm.

Algorithm 2.2.6 Input: A matrix M.

Output: A complete set of orthogonal 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) $g := f$ div $p_i^{e_i}$;

(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 idempotents for a commutative matrix algebra consists of multiplying together the idempotents of every matrix in a basis and to select an orthogonal subset from these products. See Computer Exercise 12.

2.3 Algorithms and Implementations: More of MAGMA

- Linear algebra in MAGMA.
- Functions and procedures and comments revisited.
- Packages and intrinsics.

2.4 Theoretical exercises

Exercise 17 *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 18 *Prove Proposition 2.1.3.*

Exercise 19 *Let $\mathbb{T}$ be an Artinian ring.*

(a) Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}$. Prove that $\mathfrak{m}^\infty$ 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 $\{1 - e_{\mathfrak{m}} | \mathfrak{m} \in \mathrm{Spec}(\mathbb{T})\}$ forms a complete set of pairwise orthogonal idempotents.

Exercise 20 *Prove the correspondences and the isomorphisms from Part (a) of Proposition 2.1.7.*

Exercise 21 *Let $f, g \in \mathrm{M}_k(N, \chi\,; \overline{K})$ be normalised eigenforms that are $\mathrm{Gal}(\overline{K}/K)$-conjugate. Prove that their reductions modulo p are $\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F})$-conjugate.*

Exercise 22 *Prove Proposition 2.1.8.*

Exercise 23 *Find a non-local algebra A over a field K (of your choice) such that A is generated as a K-algebra by $a_1, \ldots, a_n$ having the property that the minimal polynomial of each a_i is a power of an irreducible polynomial in $K[X]$.*

Exercise 24 *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 $\mathrm{Tr}_{N/K}(x) \neq 0$.*

Exercise 25 *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 14 you are asked to find and implement an algorithm computing such base change matrices.

2.5 Computer exercises

Computer exercise 8 *Change Algorithm 1.3.5 (see Computer Exercise 7) so that it works for modular forms over a given ring R.*

Computer exercise 9 *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 10 *Let A be a commutative algebra over a field K. The regular representation is defined as the image of the injection*

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

Write a function computing the regular representation.

Computer exercise 11 *Implement Algorithm 2.2.5. Also write a function that returns the local factors as matrix algebras (possibly using regular representations).*

Computer exercise 12 *(a) Implement Algorithm 2.2.6.*

(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 9 to compute the maximal ideals of A.

Computer exercise 13 *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 9). 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 14 *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 25).

Stage 3

Homological algebra

3.1 Theory: Categories and Functors

Definition 3.1.1 *A* category $\mathcal{C}$ *consists of the following data:*

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

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

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

such that

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

Example 3.1.2 *Examples of categories are*

- *Sets: objects are sets, morphisms are maps.*
- *Let* R *be a not necessarily commutative ring. Left* R*-modules (*$R - \mathrm{modules}$*): 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 (*$\mathrm{modules} - R$*): as above.*
- *Etc.*

Definition 3.1.3 *Let $\mathcal{C}$ and $\mathcal{D}$ be categories. A* covariant/contravariant functor $F : \mathcal{C} \to \mathcal{D}$ *is*

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

such that

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

Example 3.1.4

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

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

This is a covariant functor.

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

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

This is a contravariant functor.

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

$$\cdot \otimes_R M : \mathrm{modules} - R \to \mathbb{Z} - \mathrm{modules},\ \ A \mapsto A \otimes_R M.$$

This is a covariant functor.

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

$$M \otimes_R \cdot : R - \mathrm{modules} \to \mathbb{Z} - \mathrm{modules},\ \ A \mapsto M \otimes_R A.$$

This is a covariant functor.

Definition 3.1.5

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

$$0 \to A \to B \to C$$

the sequence

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

is also exact.

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

$$A \to B \to C \to 0$$

the sequence

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

is also exact.

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

$$A \to B \to C \to 0$$

the sequence

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

is also exact.

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

$$0 \to A \to B \to C$$

the sequence

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

is also exact.

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

Example 3.1.6 *Both functors $\mathrm{Hom}_R(\cdot, M)$ and $\mathrm{Hom}_R(M, \cdot)$ for $M \in \mathrm{obj}(R - \mathrm{modules})$ are left-exact. Both functors $\cdot \otimes_R M$ for $M \in \mathrm{obj}(R - \mathrm{modules})$ and $M \otimes_R \cdot$ for $M \in \mathrm{obj}(\mathrm{modules} - R)$ are right-exact.*

Proof. Exercise 26. □

Definition 3.1.7 *Let R be a not necessarily commutative ring. A left R-module P is called* projective *if the functor $\mathrm{Hom}_R(P, \cdot)$ is exact. A left R-module I is called* injective *if the functor $\mathrm{Hom}_R(\cdot, I)$ is exact.*

Lemma 3.1.8 *Let R be a not necessarily commutative ring and let P be a left R-module.*

Show that 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 27. □

3.2 Theory: Complexes and Cohomology

Definition 3.2.1 *A* (right) chain complex $C_\bullet$ *in the category* $R-\mathrm{modules}$ *is a collection of objects* $C_n \in \mathrm{obj}(R-\mathrm{modules})$ *for* $n \geq m$ *for some* $m \in \mathbb{Z}$ *together with homomorphisms* $C_{n+1} \xrightarrow{\partial_{n+1}} C_n$*, i.e.*

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

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*

$$\mathrm{Z}_n(C_\bullet) = \ker(\partial_n).$$

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

$$\mathrm{B}_n(C_\bullet) = \mathrm{im}(\partial_{n+1}).$$

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

$$\mathrm{H}_n(C_\bullet) = \ker(\partial_n)/\,\mathrm{im}(\partial_{n+1}).$$

The chain complex $C_\bullet$ *is* exact *if* $\mathrm{H}_n(C_\bullet) = 0$ *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 $\phi_\bullet : C_\bullet \to D_\bullet$ *is a collection of homomorphisms* $\phi_n : C_n \to D_n$ *for* $n \in \mathbb{N}_0$ *such that all the diagrams*

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

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

$$0 \xrightarrow{\partial^m} C^m \xrightarrow{\partial^{m+1}} C^{m+1} \xrightarrow{\partial^{m+2}} C^{m+2} \to \cdots \to C^{n-1} \xrightarrow{\partial^n} C^n \xrightarrow{\partial^{n+1}} C^{n+1} \to \ldots,$$

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*

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

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

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

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

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

The cochain complex $C^\bullet$ *is* exact *if* $\mathrm{H}^n(C_\bullet) = 0$ *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 $\phi^\bullet : C^\bullet \to D^\bullet$ *is a collection of homomorphisms* $\phi^n : C^n \to D^n$ *for* $n \in \mathbb{N}_0$ *such that all the diagrams*

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

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 28 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. We describe the *standard resolution* $F(G)_\bullet$ of R by free $R[G]$-modules:

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

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 $1 \in R$. We have $\partial_0 = 0$ by definition.

In Exercise 29 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. [Weibel] 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

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

The symbols $[h_1|h_2| \ldots |h_n]$ 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 $[h_1|h_2| \ldots |h_n]$). One computes the action of d_i on this basis and gets

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

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

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:

$$0 \to R[G] \xrightarrow{T-1} R[G] \xrightarrow{\epsilon} R \to 0.$$

Let now $G = \langle \sigma \rangle$ be a finite cyclic group of order n. Here is a resolution of R by free $R[G]$-modules:

$$\cdots \to R[G] \xrightarrow{N_\sigma} R[G] \xrightarrow{1-\sigma} R[G] \xrightarrow{N_\sigma} R[G] \xrightarrow{1-\sigma} R[G] \to \cdots \to R[G] \xrightarrow{1-\sigma} R[G] \xrightarrow{\epsilon} R \to 0.$$

In Exercise 30 you are asked to verify the exactness of these two sequences.

Example: simplicial cohomology

Please have a look at the definition of simplicial cohomology in any textbook on Algebraic Topology.

Group cohomology

Definition 3.2.3 *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 $\mathrm{Hom}_{R[G]}(\cdot, M)$ 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 $\mathrm{Hom}_{R[G]}(F(G)_\bullet, M)$:

$$\to \mathrm{Hom}_{R[G]}(F(G)_{n-1}, M) \xrightarrow{\partial^n} \mathrm{Hom}_{R[G]}(F(G)_n, M) \xrightarrow{\partial^{n+1}} \mathrm{Hom}_{R[G]}(F(G)_{n+1}, M) \to .$$

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

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

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

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

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

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

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

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

provided that 6 is invertible in R. We shall prove this later in this lecture.

The reader is invited to compute explicit descriptions of H^0, H_0 and H^1 in Exercise 31.

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. We will also 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. Here we should really understand the word category not in its precise mathematical sense but as a placeholder for $R-\mathrm{modules}$, or (co-)chain complexes of $R-\mathrm{modules}$ and other categories from everyday life.

Definition 3.3.1 *Let $\mathcal{C}$ and $\mathcal{D}$ be (abelian) categories (for instance, $\mathcal{C}$ the right cochain complexes of $R-\mathrm{modules}$ and $\mathcal{D} = R-\mathrm{modules}$). A* positive covariant cohomological δ-functor *between $\mathcal{C}$ and $\mathcal{D}$ is a collection of functors $\mathrm{H}^n : \mathcal{C} \to \mathcal{D}$ for $n \geq 0$ together with* connecting morphisms

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

which are defined for every short exact sequence $0 \to A \to B \to C \to 0$ 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 $0 \to A \to B \to C \to 0$ *in* $\mathcal{C}$ *there is the* long exact sequence *in* $\mathcal{D}$*:*

$$\ldots \mathrm{H}^{n-1}(C) \xrightarrow{\delta^{n-1}} \mathrm{H}^n(A) \to \mathrm{H}^n(B) \to \mathrm{H}^n(C) \xrightarrow{\delta^n} \mathrm{H}^{n+1}(A) \to \ldots,$$

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

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

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

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

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

Theorem 3.3.2 *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*

$$\mathrm{H}^n : \mathcal{C} \to \mathbb{Z} - \mathrm{modules}, \quad C^\bullet \mapsto \mathrm{H}^n(C^\bullet)$$

form a cohomological δ*-functor.*

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

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

Proposition 3.3.3 *Let* R *be a commutative ring and* G *a group.*

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

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

of cochain complexes.

(b) The functors

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

form a cohomological δ*-functor.*

Proof. Exercise 32. □

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 $R-\mathrm{modules}$ for a not necessarily commutative ring R.

Definition 3.3.4 *Let R be a not necessarily commutative ring and let $M \in \mathrm{obj}(R-\mathrm{modules})$.*

A projective resolution *of M is a resolution*

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

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*

$$0 \to M \to I^0 \xrightarrow{\partial^1} I^1 \xrightarrow{\partial^2} I^2 \to \ldots,$$

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.

Lemma 3.3.5 *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 functor $\mathcal{F}$ to an injective resolution

$$0 \to M \to I^0 \to I^1 \to I^2 \to \ldots$$

of M gives rise to a cochain complex

$$0 \to \mathcal{F}(M) \to \mathcal{F}(I^0) \to \mathcal{F}(I^1) \to \mathcal{F}(I^2) \to \ldots,$$

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

Definition 3.3.6 *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 $\mathbb{Z}-\mathrm{modules}$).

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

$$R^n\mathcal{F}(M) := \mathrm{H}^n\left(\mathcal{F}(I^0) \to \mathcal{F}(I^1) \to \mathcal{F}(I^2) \to \ldots\right).$$

(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 $R-\mathrm{modules}$ defined as follows. For $M \in \mathrm{obj}(R-\mathrm{modules})$ choose a projective resolution $\cdots \to P_1 \to P_0 \to M \to 0$ and let*

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

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 3.3.7 *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 3.3.8 *Let $\mathcal{C}$ and $\mathcal{D}$ be two categories and F and G two covariant functors between $\mathcal{C}$ and $\mathcal{D}$. A* natural transformation $\eta : F \Rightarrow G$ *is a rule that associates a morphism*

$$\eta_C : F(C) \to G(C)$$

for every $C \in \mathrm{obj}(\mathcal{C})$ such that to every $f : C \to C'$ in $\mathrm{Hom}_{\mathcal{C}}(C, C')$ the diagram

$$\begin{array}{ccc} F(C) & \xrightarrow{F(f)} & F(C') \\ {\scriptstyle \eta_C}\downarrow & & {\scriptstyle \eta_{C'}}\downarrow \\ G(C) & \xrightarrow{G(f)} & G(C') \end{array}$$

commutes. For contravariant functors we make the same definition with the horizontal arrows in the diagram reversed.

Example 3.3.9 *Let R be a not necessarily commutative ring and let $A, B \in \mathrm{obj}(R-\mathrm{modules})$ as well as $C, D \in \mathrm{obj}(\mathrm{modules}-R)$ with morphisms $A \to B$ and $C \to D$. Then there are natural transformations $\mathrm{Hom}_R(B,\cdot) \Rightarrow \mathrm{Hom}_R(A,\cdot)$ and $\mathrm{Hom}_R(\cdot, A) \Rightarrow \mathrm{Hom}_R(\cdot, B)$ as well as $\cdot \otimes_R A \Rightarrow \cdot \otimes_R B$ and $A \otimes_R \cdot \Rightarrow B \otimes_R \cdot$.*

Proof. Exercise 33. □

Definition 3.3.10 *(a) Let $(\mathrm{H}^n)_n$ and $(T^n)_n$ be cohomological δ-functors. A* morphism of cohomological δ-functors *is a collection of natural transformations $\eta^n : \mathrm{H}^n \Rightarrow T^n$ that commute with the*

connecting homomorphisms δ, i.e. for every short exact sequence $0 \to A \to B \to C \to 0$ and every n the diagram

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

commutes.

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

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

Theorem 3.3.11 *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 $\mathbb{Z} - \mathrm{modules}$).*

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

Example 3.3.12 *(a) Let R be a commutative ring and G a group. The functor*

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

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 in a moment.

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

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

By definition we have $\mathrm{H}^n(G, M) \cong \mathrm{Ext}_R^n(\cdot, M)(R)$.

(c) If R is again commutative and G a group, then due to the universality and $\mathrm{Hom}_{R[G]}(R, M) = M^G$ we have that $R^n(\cdot)^G$ is isomorphic to $\mathrm{Ext}_R^n(R, \cdot)$.

(d) 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 $\mathcal{F} \mapsto \mathcal{F}(X) = \mathrm{H}^0(X, \mathcal{F})$ is left exact and its right derived functors $R^n(\mathrm{H}^0(X, \cdot))$ can be formed. They are usually denoted by $\mathrm{H}^n(X, \cdot)$ 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 3.3.13 *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*

$$(\mathrm{Ext}^n_R(\cdot, N))(M) \cong (\mathrm{Ext}^n_R(M, \cdot)(N) =: \mathrm{Ext}^n_R(M, N).$$

Proof. [Weibel],Theorem 2.7.6. □

Corollary 3.3.14 *Let R be a commutative ring and G a group. For every $R[G]$-module M there are isomorphisms*

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

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

Proof. We may compute $\mathrm{Ext}^n_{R[G}(\cdot, M)(R)$ by any resolution of R by projective $R[G]$-modules. Our standard resolution is such a resolution, since any free module is projective. Hence, $H^n(G, M) \cong \mathrm{Ext}^n_{R[G]}(\cdot, M)(R)$. The key is now that Ext is balanced (Theorem 3.3.13), since it gives $H^n(G, M) \cong \mathrm{Ext}^n_{R[G]}(R, \cdot)(M) = R^n(\cdot)^G(M) \cong \mathrm{Ext}^n_{R[G]}(R, M)$. 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 34 now.

3.4 Theory: Generalities on Group Cohomology

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

$$\mathrm{res}^n : \mathrm{H}^n(G, \cdot) \to \mathrm{H}^n(H, \cdot).$$

These maps are called *restrictions*. See Exercise 35 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 $\phi : G \to G/H$ and the restriction above gives natural transformations $\mathrm{res}^n : \mathrm{H}^n(G/H, (\cdot)^H) \to \mathrm{H}^n(G, (\cdot)^H)$. We define the *inflation maps* to be

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

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 $H^n(H,A) \to H^n(H,A)$ for every $g \in G$. One even gets an $R[G]$-action on $\mathrm{H}^n(H,A)$. As $h \in H$ is clearly the identity on $\mathrm{H}^0(H,A)$, 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 $\mathrm{cores}^0 : \mathrm{H}^0(H,\cdot) \to \mathrm{H}^0(G,\cdot)$ where $\cdot$ is an $R[G]$-module. By universality we obtain

$$\mathrm{cores}^n : \mathrm{H}^n(H,\cdot) \to \mathrm{H}^n(G,\cdot),$$

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 35).

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

Proposition 3.4.1 *(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*

$$\mathrm{cores}^G_H \circ \mathrm{res}^G_H = (G : H)$$

on all $\mathrm{H}^i(G,M)$.

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

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

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

is trivially the zero map, but it also is multiplication by n. □

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

Theorem 3.4.2 (Hochschild-Serre) *Let $H \leq G$ be a normal subgroup and A an $R[G]$-module. There is the exact sequence:*

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

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 ([Weibel], 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. □

Coinduced modules and Shapiro's Lemma

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

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

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

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

Proposition 3.4.3 (Shapiro's Lemma) *For all $n \geq 0$, the map*

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

given on cochains is given by

$$c \mapsto ((h_1, \ldots, h_n) \to (c(h_1, \ldots, h_n))(1_G))$$

is an isomorphism.

Proof. Exercise 36. □

Mackey's formula and stabilisers

If $H \leq G$ are groups and V is an $R[G]$-module, we denote by $\mathrm{Res}_H^K(V)$ the module V considered as an $R[H]$-module.

Proposition 3.4.4 *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*

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

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

Proof. We consider the commutative diagram

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

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

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

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

From Shapiro's Lemma we directly get the following.

Corollary 3.4.5 *In the situation of Proposition 3.4.4 one has*

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

for all $i \in \mathbb{N}$. □

3.5 Theoretical exercises

Exercise 26 *Verify the statements of Example 3.1.6.*

Exercise 27 *Prove Lemma 3.1.8.*

Exercise 28 *Let* $\phi^\bullet : C^\bullet \to D^\bullet$ *be a morphism of cochain complexes.*

(a) Show that $\ker(\phi^\bullet)$ *is a cochain complex and is a subcomplex of* $C^\bullet$ *in a natural way.*

(b) Show that $\mathrm{im}(\phi^\bullet)$ *is a cochain complex and is a subcomplex of* $D^\bullet$ *in a natural way.*

(c) Show that $\mathrm{coker}(\phi^\bullet)$ *is a cochain complex and is a quotient of* $D^\bullet$ *in a natural way.*

(d) Show that $\phi^\bullet$ *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 29 *Check the exactness of the standard resolution of a group* G.

Exercise 30 *Check the exactness of the resolutions given for an infinite and a finite cyclic group on page 50.*

Exercise 31 *Let R, G, M be as in the definition of group (co-)homology.*

(a) Prove $\mathrm{H}^0(G,M) \cong M^G$, the G-invariants of M.

(b) Prove $\mathrm{H}_0(G,M) \cong M_G$, the G-coinvariants of M.

(c) Prove the explicit descriptions:

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

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

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

Exercise 32 *Prove Proposition 3.3.3.*

Exercise 33 *Check the statements made in Example 3.3.9.*

Exercise 34 *Let R be a commutative ring.*

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

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

for all $i \geq 2$.

(b) For a finite cyclic group G and any $R[G]$-module M prove that

$$\mathrm{H}^i(G,M) \cong \mathrm{H}^{i+2}(G,M)$$

for all $i \geq 1$.

Exercise 35 *Let R be a commutative ring.*

(a) Let $\phi : H \to G$ be a group homomorphism and A an $R[G]$-module. Prove that the restriction maps $\mathrm{res}^n : H^n(G,A) \to H^n(H,A)$ 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 36 *Prove Shapiro's lemma, i.e. Prop. 3.4.3.*

Stage 4

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

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

As already done for the modular symbols formalism, we shall also base our group cohomological treatment of modular symbols on the group $\mathrm{PSL}_2(\mathbb{Z})$, rather than $\mathrm{SL}_2(\mathbb{Z})$, which simplifies the treatment, since $\mathrm{PSL}_2(\mathbb{Z})$ has a very simple structure, namely as a free product of two cyclic groups. That is what we are going to treat first.

Definition 4.1.1 *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 group operation in $G * H$ is concatenation of words, possibly multiplying the two symbols that meet at the concatenation point.*

The integer n is called the length *of the group element (word) $g = a_1 a_2 \dots a_n$ and denoted by $l(g)$. We put $l(1) = 0$ for the empty word.*

In Exercise 37 you are asked to verify the $G * H$ is indeed a group and to prove a universal property.

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

$$\sigma := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right), \quad \tau := \left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right), \quad T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) = \tau\sigma.$$

They have the following conceptual meaning:

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

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 38 is recommended at this point.

Theorem 4.1.2 *The group $\mathrm{PSL}_2(\mathbb{Z})$ is the free product of the cyclic groups $\langle\sigma\rangle$ of order 2 and $\langle\tau\rangle$ of order 3. In particular, as an abstract group, $\mathrm{PSL}_2(\mathbb{Z})$ can be represented by generators and relations as $\langle\sigma,\tau \mid \sigma^2=\tau^3=1\rangle$.*

Proof. Let $\mathcal{P}=\langle\sigma\rangle * \langle\tau\rangle$. In last term's course we proved that $\mathrm{SL}_2(\mathbb{Z})$ is generated by σ and τ, hence 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. Define the map ('graph')

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

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 now 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.

Why this composition is injective, is easily seen and explained by looking at the tessellation of the upper half plane by the standard fundamental domain and by marking the image of ϕ, i.e. all the $\gamma.B$. Neighbouring edges of the edge $\gamma.B$ are $\gamma\sigma.B, \gamma\tau.B, \gamma\tau^2.B$ and the three neighbouring edges are distinct. Just by looking at the image of ϕ, one sees that it forms a tree, i.e. a graph without circles. Hence, applying any word $a_1a_2\ldots a_n$ of positive length $n \geq 1$ as in the definition of the free product, one never has $B = a_1a_2\ldots a_n.B$, as desired. [Show some picture.] □

4.2 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 4.2.1 *The sequence*

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

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 [Bieri]. 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 $g = a_1 a_2 \dots a_n$ (we do not need the uniqueness of this expression). If $n = 1$, there is nothing to do. If $n \geq 1$, 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

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

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, $\sum_w a_w w G_1 = 0 = \sum_w a_w w G_2$. 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. □

Proposition 4.2.2 (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*

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

and for all $i \geq 2$ an isomorphism

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

Proof. We see that all terms in the exact sequence of Proposition 4.2.1 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

$$0 \to M \to \mathrm{Hom}_{R[G_1]}(R[G], M) \oplus \mathrm{Hom}_{R[G_2]}(R[G], M) \to \mathrm{Hom}_R(R[G], M) \to 0.$$

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 3.4.3. □

We now apply the Mayer-Vietoris sequence (Prop. 4.2.2) 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

$$0 \to M^{\mathrm{PSL}_2(\mathbb{Z})} \to M^{\langle\sigma\rangle} \oplus M^{\langle\tau\rangle} \to M \xrightarrow{m \mapsto f_m} \mathrm{H}^1(\mathrm{PSL}_2(\mathbb{Z}), M) \xrightarrow{\mathrm{res}} \mathrm{H}^1(\langle\sigma\rangle, M) \oplus \mathrm{H}^1(\langle\tau\rangle, M) \to 0 \quad (4.2.1)$$

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

$$\mathrm{H}^i(\mathrm{PSL}_2(\mathbb{Z}), M) \cong \mathrm{H}^i(\langle\sigma\rangle, M) \oplus \mathrm{H}^i(\langle\tau\rangle, M). \quad (4.2.2)$$

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 40).

Lemma 4.2.3 *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.*

(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) Recall that $\mathrm{PSL}_2(\mathbb{Z})_x$ denotes the stabiliser of x for the $\mathrm{PSL}_2(\mathbb{Z})$-action. 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 $i \in \mathbb{N}$, Mackey's formula (Prop. 3.4.4) 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. □

Corollary 4.2.4 *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 $\mathrm{H}^1(\Gamma, V) = M/(M^{\langle\sigma\rangle} + M^{\langle\tau\rangle})$ 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 Exercise 38, 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. 3.4.1 that the groups on the right in the equation in Lemma 4.2.3 (c) are zero. Hence, by Shapiro's lemma (Prop. 3.4.3) and Equations (4.2.1) and (4.2.2) we obtain the proposition. □

By Exercise 38, the assumptions of the proposition are for instance always satisfied if R is a field of characteristic not 2 or 3. Look at Exercise 39 to see for which N the assumptions hold for $\Gamma_1(N)$ and $\Gamma_0(N)$ over an arbitrary ring (e.g. the integers).

4.3 Theory: Parabolic group cohomology

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

$$0 \to \mathrm{H}^1_{\mathrm{par}}(\Gamma, V) \to \mathrm{H}^1(\Gamma, V) \xrightarrow{\mathrm{res}} \prod_{g \in \Gamma\backslash \mathrm{PSL}_2(\mathbb{Z})/\langle T\rangle} \mathrm{H}^1(\Gamma \cap \langle gTg^{-1}\rangle, V). \tag{4.3.3}$$

Proposition 4.3.1 *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:*

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

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

Proof. The commutativity of the diagram is checked in Exercise 41. By Exercise 34 we have $\mathrm{H}^1(\langle T\rangle, M) \cong M/(1-T)M$. Due to the assumptions we may apply Corollary 4.2.4. The cokernel of $M/(M^{\langle\sigma\rangle} + M^{\langle\tau\rangle}) \xrightarrow{m \mapsto (1-\sigma)m} M/(1-T)M$ 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

$$\psi : V_\Gamma \to \mathrm{Hom}_{R[\Gamma]}(R[G], V)_G, \quad v \mapsto e_v \text{ with } e_v(g) = \begin{cases} gv, & \text{for } g \in \Gamma \\ 0, & \text{for } g \notin \Gamma. \end{cases}$$

It is clear that $\phi \circ \psi$ is the identity. The map ϕ is an isomorphism, as ψ is surjective. Fix a system of representatives $\{1 = g_1, g_2, \ldots, g_n\}$ for $\Gamma\backslash\mathrm{PSL}_2(\mathbb{Z})$. We have

$$f = \sum_{i=1}^{n} g_i.e_{f(g_i)} = \sum_{i=2}^{n} e_{f(g_i)} + \sum_{i=2}^{n} (1 - g_i).e_{f(g_i)} \in \mathrm{im}(\psi),$$

as needed. [Actually, a more conceptual proof would be to first identify non-canonically the coinduced module $\mathrm{Coind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V)$ with the induced one $\mathrm{Ind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V) = R[G] \otimes_{R[\Gamma]} V$ (see later). We claim that the G-coinvariants are isomorphic to $R \otimes_{R[\Gamma]} V \cong V_\Gamma$. As R-modules we have $R[G] = IG \oplus R1_G$, since $r \mapsto r1_G$ defines a splitting of the augmentation map. Consequently, $R[G] \otimes_{R[\Gamma]} V \cong (IG \otimes_{R[\Gamma]} V) \oplus R \otimes_{R[\Gamma]} V$. The claim follows, since $IG(R[G] \otimes_{R[\Gamma]} V) \cong IG \otimes_{R[\Gamma]} V$.]

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. □

4.4 Theory: Dimension computations

This seems to be a good place to compute the dimension of $\mathrm{H}^1(\Gamma, V_{k-2}(K))$ and $\mathrm{H}^1_{\mathrm{par}}(\Gamma, V_{k-2}(K))$ over a field K under certain conditions. The results will be important for the proof of the Eichler-Shimura theorem.

Lemma 4.4.1 *Let R be a ring and let $n \geq 1$ be an integer, $t = \left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right)$ and $t' = \left(\begin{smallmatrix} 1 & 0 \\ N & 1 \end{smallmatrix}\right)$.*

(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

$$V_n(R)_{\langle t \rangle} = V_n(R)/\langle Y^n, XY^{n-1}, \ldots, X^{n-1}Y \rangle$$

respectively

$$V_n(R)_{\langle t' \rangle} = V_n(R)/\langle X^n, X^{n-1}Y, \ldots, XY^{n-1} \rangle.$$

(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 $t.(X^{n-i}Y^i) = X^{n-i}(NX+Y)^i$ and consequently

$$(t-1).(X^{n-i}Y^i) = (\sum_{j=0}^{i} \binom{i}{j} N^{i-j}X^{i-j}Y^j)X^{n-i} - X^{n-i}Y^i = \sum_{j=0}^{i-1} r_{i,j}X^{n-j}Y^j$$

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

$$\begin{aligned}(t-1).x = \sum_{i=0}^{n} a_i \sum_{j=0}^{i-1} X^{n-j}Y^j &= \sum_{j=0}^{n-1} X^{n-j}Y^j(\sum_{i=j+1}^{n} a_i r_{i,j}) \\ &= XY^{n-1}a_n r_{n,n-1} + X^2Y^{n-2}(a_n r_{n,n-2} + a_{n-1}r_{n-1,n-2}) + \dots.\end{aligned}$$

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). □

Proposition 4.4.2 *Let K be a field of characteristic 0 and $\Gamma \leq \mathrm{PSL}_2(\mathbb{Z})$ 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 $N \geq 4$).*

Then

$$\dim_K \mathrm{H}^1(\Gamma, V_{k-2}(K)) = (k-1)\frac{\mu}{6} + \delta_{k,2}$$

and

$$\dim_K \mathrm{H}^1_{\mathrm{par}}(\Gamma, V_{k-2}(K)) = (k-1)\frac{\mu}{6} - \nu_\infty + 2\delta_{k,2},$$

where ν_∞ is the number of cusps of Γ.

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

$$0 \to M^{\mathrm{PSL}_2(\mathbb{Z})} \to M^{\langle\sigma\rangle} \oplus M^{\langle\tau\rangle} \to M \to \mathrm{H}^1(\mathrm{PSL}_2(\mathbb{Z}), M) \to 0,$$

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 is clear that every function in $\mathrm{Hom}_{K[\Gamma]}(K[\mathrm{PSL}_2(\mathbb{Z})], V_{k-2}(K))^{\mathrm{PSL}_2(\mathbb{Z})}$ is constant and equal to its value at 1. The Γ-invariance, however, imposes additionally that this contant lies in

$V_{k-2}(K)^\Gamma$. Hence, by Lemma 4.4.1 $\dim M^{\mathrm{PSL}_2(\mathbb{Z})} = \delta_{k,2}$. 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:

$$\dim_K \mathrm{H}^1(\Gamma, V_{k-2}(K)) = (k-1)(\mu - \frac{\mu}{2} - \frac{\mu}{3}) + \delta_{k,2} = (k-1)\frac{\mu}{6} + \delta_{k,2}.$$

The second formula can be read off from the diagram in Proposition 4.3.1. It gives directly

$$\dim \mathrm{H}^1_{\mathrm{par}}(\Gamma, V_{k-2}(K)) = \\ \dim \mathrm{H}^1(\Gamma, V_{k-2}(K)) + \dim V_{k-2}(K)_\Gamma - \sum_{g\in\Gamma\backslash\mathrm{PSL}_2(\mathbb{Z})/\langle T\rangle} \dim \mathrm{H}^1(\Gamma\cap\langle gTg^{-1}\rangle, V_{k-2}(K)).$$

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

$$\dim \mathrm{H}^1(\Gamma\cap\langle gTg^{-1}\rangle, V_{k-2}(K)) = \dim V_{k-2}(K)_{\langle T^n\rangle} = 1$$

by Lemma 4.4.1. As the set $\Gamma\backslash\mathrm{PSL}_2(\mathbb{Z})/\langle T\rangle$ is the set of cusps of Γ, we conclude

$$\sum_{g\in\Gamma\backslash\mathrm{PSL}_2(\mathbb{Z})/\langle T\rangle} \dim \mathrm{H}^1(\Gamma\cap\langle gTg^{-1}\rangle, V_{k-2}(K)) = \nu_\infty.$$

Moreover, also by Lemma 4.4.1 $\dim V_{k-2}(K)_\Gamma = \delta_{k,2}$. Putting everything together yields the formula

$$\dim \mathrm{H}^1_{\mathrm{par}}(\Gamma, V_{k-2}(K)) = (k-1)\frac{\mu}{6} + 2\delta_{k,2} - \nu_\infty,$$

as claimed. □

Remark 4.4.3 *It is easy to 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.*

4.5 Theoretical exercises

Exercise 37 *(a) Verify that $G * H$ is a group.*

(b) Prove the following universal property. Let $\iota_G : G \to G*H$ and $\iota_H : H \to G*H$ be the natural inclusions. Let P be any group together with group injections $\eta_G : G \to P$ and $\eta_H : H \to P$, then there is a unique group homomorphism $\phi : G * H \to P$ such that $\eta_G = \phi\circ\iota_G$ and $\eta_H = \phi\circ\iota_H$.

Exercise 38 *(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 39 *(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 40 *Prove the explicit description of f_m in the Mayer-Vietoris sequence (Equation 4.2.1).*

Exercise 41 *Verify the commutativity of the diagram in Proposition 4.3.1.*

4.6 Computer exercises

Computer exercise 15 *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 $\Gamma_1(N)$ (vgl. [Stein], 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 16 *Let K be some field. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to K^\times$ 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 $\phi : \mathbb{Z} \to K^\times$ such that $\phi(a) = 0$ for all $a \in \mathbb{Z}$ with $(a, N) \neq 1$ and $\phi(a) = \chi(a \mod N)$ otherwise.*

Stage 5

Modular symbols and Manin symbols

5.1 Theory: Manin symbols

Manin symbols provide an alternative description of modular symbols. We shall use this description for the comparison with group cohomology and for implementating the modular symbols formalism. We stay in the general setting over a ring R.

Proposition 5.1.1 *The sequence of R-modules*

$$0 \to R[\mathrm{PSL}_2(\mathbb{Z})]N_\sigma + R[\mathrm{PSL}_2(\mathbb{Z})]N_\tau \to R[\mathrm{PSL}_2(\mathbb{Z})] \xrightarrow{g \mapsto g(1-\sigma)\infty} R[\mathbb{P}^1(\mathbb{Q})] \xrightarrow{g\infty \mapsto 1} R \to 0$$

is exact. (We are considering $R[\mathrm{PSL}_2(\mathbb{Z})]$ as a right $R[\mathrm{PSL}_2(\mathbb{Z})]$-module.)

Proof. For a finite subgroup H of a group G, one easily checks that the map

$$\mathrm{Hom}_R(R[H], R[H\backslash G]) \to R[G], \quad f \mapsto \sum_{h \in H} h.f(h),$$

where $H\backslash G$ stands for a fixed system of representatives of the cosets, is an isomorphism. 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 cyclic group on page 50 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 4.2.1, we have the exact sequence

$$0 \to R[\mathrm{PSL}_2(\mathbb{Z})] \to R[\mathrm{PSL}_2(\mathbb{Z})]_{\langle\sigma\rangle} \oplus R[\mathrm{PSL}_2(\mathbb{Z})]_{\langle\tau\rangle} \to R \to 0.$$

The injectivity of the first map in the exact sequence (which we recall is a consequence of $\mathrm{PSL}_2(\mathbb{Z}) = \langle\sigma\rangle * \langle\tau\rangle$) means

$$R[\mathrm{PSL}_2(\mathbb{Z})](1-\sigma) \cap R[\mathrm{PSL}_2(\mathbb{Z})](1-\tau) = 0.$$

We identify $R[\mathrm{PSL}_2(\mathbb{Z})]/R[\mathrm{PSL}_2(\mathbb{Z})](1-T)$ with $R[\mathbb{P}^1(\mathbb{Q})]$ by sending g to $g\infty$. Now we show the exactness at $R[\mathrm{PSL}_2(\mathbb{Z})]$, which comes down to proving that the equation $x(1-\sigma) = y(1-T)$ for $x, y \in R[\mathrm{PSL}_2(\mathbb{Z})]$ implies that x is in $R[\mathrm{PSL}_2(\mathbb{Z})]^{\langle\sigma\rangle} + R[\mathrm{PSL}_2(\mathbb{Z})]^{\langle\tau\rangle}$.

Using the formula $\tau = T\sigma$ we obtain that $x(1-\sigma) = y(1-T) = y(1-\tau) - yT(1-\sigma)$. This yields $x(1-\sigma) + yT(1-\sigma) = y(1-\tau)$. This expression, however, is zero. Consequently, there is a $z \in R[\mathrm{PSL}_2(\mathbb{Z})]$ such that $y = zN_\tau$. Hence, using $T = \tau\sigma$ and consequently $N_\tau T = N_\tau\sigma$, we get

$$y(1-T) = zN_\tau(1-T) = zN_\tau(1-\sigma) = y(1-\sigma).$$

The equation $x(1-\sigma) = y(1-\sigma)$ means that $x - y$ is in $R[\mathrm{PSL}_2(\mathbb{Z})]^{\langle\sigma\rangle}$. As we know that $y \in R[\mathrm{PSL}_2(\mathbb{Z})]^{\langle\tau\rangle}$, we see that $x = (x-y) + y$ is in $R[\mathrm{PSL}_2(\mathbb{Z})]^{\langle\sigma\rangle} + R[\mathrm{PSL}_2(\mathbb{Z})]^{\langle\tau\rangle}$, as required.

The exactness at $R[\mathbb{P}^1(\mathbb{Q})]$ can be seen as follows (we avoid here the traditional continued fractions argument). Since σ and $T = \tau\sigma$ generate $\mathrm{PSL}_2(\mathbb{Z})$, the kernel of $R[\mathrm{PSL}_2(\mathbb{Z})] \xrightarrow{g\mapsto 1} R$ is $R[\mathrm{PSL}_2(\mathbb{Z})](1-\sigma) + R[\mathrm{PSL}_2(\mathbb{Z})](1-T)$. Taking the quotient by $R[\mathrm{PSL}_2(\mathbb{Z})](1-T)$ gives the desired exactness. □

Lemma 5.1.2 *The sequence of R-modules*

$$0 \to \mathcal{M}_R \xrightarrow{\{\alpha,\beta\}\mapsto\beta-\alpha} R[\mathbb{P}^1(\mathbb{Q})] \xrightarrow{\alpha\mapsto 1} R \to 0$$

is exact.

Proof. The injectivity of the first arrow is clear, since we can write any element in $\mathcal{M}_R$ as $\sum_{\alpha\neq\infty} r_\alpha\{\infty,\alpha\}$ with $r_\alpha \in R$, using the relations defining $\mathcal{M}_R$. The image of this element under the first arrow is $\sum_{\alpha\neq\infty} r_\alpha\alpha - (\sum_{\alpha\neq\infty} r_\alpha)\infty$. If this is zero, clearly all r_α are zero, proving the injectivity of the first arrow.

Suppose now we are given $\sum_\alpha r_\alpha\alpha \in R[\mathbb{P}^1(\mathbb{Q})]$ in the kernel of the second arrow. Then $\sum_\alpha r_\alpha = 0$ and consequently we have

$$\sum_\alpha r_\alpha\alpha = \sum_{\alpha\neq\infty} r_\alpha\alpha - (\sum_{\alpha\neq\infty} r_\alpha)\infty$$

which is in the image of the first arrow, as noticed before. □

Proposition 5.1.3 *The homomorphism of R-modules*

$$R[\mathrm{PSL}_2(\mathbb{Z})] \xrightarrow{\phi} \mathcal{M}_R, \quad g \mapsto \{g.0, g.\infty\}$$

is surjective and its kernel is given by $R[\mathrm{PSL}_2(\mathbb{Z})]N_\sigma + R[\mathrm{PSL}_2(\mathbb{Z})]N_\tau$.

Proof. This is a direct consequence of Proposition 5.1.1 and Lemma 5.1.2. □

We are now ready 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 5.1.4 *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 non-canonically isomorphic to the coinduced one:

Lemma 5.1.5 *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 (non-canonically) 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

$$\mathrm{Ind}_H^G(V) \to (R[G] \otimes_R V)_H, \quad g \otimes v \mapsto g^{-1} \otimes v$$

is an isomorphism of right $R[G]$-modules.

Proof. Exercise 42. □

Theorem 5.1.6 *Let $M = \mathrm{Ind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V)$, 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 5.1.5 (b). The following statements hold:*

(a) The homomorphism ϕ from Proposition 5.1.3 induces the exact sequence of R-modules

$$0 \to MN_\sigma + MN_\tau \to M \to \mathcal{M}_R(\Gamma, V) \to 0.$$

The homomorphism $M \to \mathcal{M}_R(\Gamma, V)$ is given by $g \otimes v \mapsto \{g.0, g.\infty\} \otimes v$.

Elements in $M/(MN_\sigma + MN_\tau)$ are called Manin symbols.

(b) The homomorphism $R[\mathrm{PSL}_2(\mathbb{Z})] \to R[\mathbb{P}^1(\mathbb{Q})]$ sending g to $g.\infty$ induces the exact sequence of R-modules

$$0 \to M(1-T) \to M \to \mathcal{B}_R(\Gamma, V) \to 0.$$

(c) The identifications of (a) and (b) imply the isomorphism

$$\mathcal{CM}_R(\Gamma, V) \cong \ker\big(M/(MN_\sigma + MN_\tau) \xrightarrow{m\mapsto m(1-\sigma)} M/M(1-T)\big).$$

Proof. (a) We derive this from Proposition 5.1.3, which gives the exact sequence

$$0 \to R[\mathrm{PSL}_2(\mathbb{Z})]N_\sigma + R[\mathrm{PSL}_2(\mathbb{Z})]N_\tau \to R[\mathrm{PSL}_2(\mathbb{Z})] \to \mathcal{M}_2(R) \to 0.$$

Tensoring with V over R, we obtain the exact sequence of left $R[\Gamma]$-modules

$$0 \to (R[\mathrm{PSL}_2(\mathbb{Z})] \otimes_R V)N_\sigma + (R[\mathrm{PSL}_2(\mathbb{Z})] \otimes_R V)N_\tau \to (R[\mathrm{PSL}_2(\mathbb{Z})] \otimes_R V) \to \mathcal{M}_R(V) \to 0.$$

Passing to left Γ-coinvariants yields (a). Part (b) is clear from the definition and Part (c) has already been noticed in the proof of Proposition 5.1.1. □

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 [Stein], 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 5.1.7 *Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to R^\times$ 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 is isomorphic as a right $R[\mathrm{SL}_2(\mathbb{Z})]$-module and a left $R[\Gamma_1(N)\backslash\Gamma_0(N)]$-module to $\mathrm{Ind}_{\Gamma_1(N)}^{\mathrm{SL}_2(\mathbb{Z})}(V_k^\chi(R))$, and, moreover, ${}_{\Gamma_1(N)\backslash\Gamma_0(N)}X$ is isomorphic to $\mathrm{Ind}_{\Gamma_0(N)}^{\mathrm{SL}_2(\mathbb{Z})}(V_k^\chi(R))$. If $N \geq 3$, then the latter module is isomorphic to $\mathrm{Ind}_{\Gamma_0(N)/\{\pm1\}}^{\mathrm{PSL}_2(\mathbb{Z})}(V_k^\chi(R))$.

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

$${}_{\Gamma_1(N)}(R[\mathrm{SL}_2(\mathbb{Z})] \otimes_R V_{k-2}(R) \otimes_R R^\chi) \to X.$$

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 ${}_{\Gamma_1(N)\backslash\Gamma_0(N)}\big({}_{\Gamma_1(N)}M\big) = {}_{\Gamma_0(N)}M$ 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 $-1 \notin \Gamma_1(N)$. □

For one more description of the induced module $\mathrm{Ind}_{\Gamma_0(N)/\{\pm1\}}^{\mathrm{PSL}_2(\mathbb{Z})}(V_k^\chi(R))$ see Exercise 43. 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 17.

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 5.2.1 *Suppose that the orders of all stabliser subgroups of Γ for the action on $\mathbb{H}$ are invertible in R. Then we have isomorphisms:*

$$\mathrm{H}^1(\Gamma, V) \cong \mathcal{M}_R(\Gamma, V)$$

and

$$\mathrm{H}^1_{\mathrm{par}}(\Gamma, V) \cong \mathcal{CM}_R(\Gamma, V)$$

Proof. This follows immediately from comparing the Manin symbols description of modular symbols (Theorem 5.1.6) with the corollary of the Mayer-Vietoris exact sequence (Corollary 4.2.4), using Mackey's formula as in Lemma 4.2.3 (c) and the resolution of R for a free group on page 50. □

5.3 Algorithms and Implementations: Conversion between Manin and modular symbols

We now use the Euclidean Algorithm to represent any element $g \in \mathrm{PSL}_2(\mathbb{Z})$ in terms of σ and T.

Algorithm 5.3.1 Input: A matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with integer entries and determinant 1.

Output: A list of matrices $[A_1, A_2, \ldots, A_n]$ 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) $q := a$ div c.

(8) Append T^q to `output`.

(9) Append σ to `output`.

(10) $M := \sigma T^{-q} M$.

(11) end while;

(12) if $M \notin \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\}$ then [At this point $M \in \{\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & * \\ 0 & -1 \end{smallmatrix}\right)\}$.]

(13) Append M to `output`.

(14) end if;

(15) return `output`.

This algorithm gives a constructive proof of the fact that $\mathrm{PSL}_2(\mathbb{Z})$ 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 44 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 $g \in \mathrm{SL}_2(\mathbb{Z})$ (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 $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ satisfies the requirements). We now use Algorithm 5.3.1 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.

In Computer Exercise 18 you are asked to implement a conversion between Manin and modular symbols.

5.4 Theoretical exercises

Exercise 42 *Prove Lemma 5.1.5.*

Exercise 43 *Assume the set-up of Proposition 5.1.7. Describe a right* $\mathrm{PSL}_2(\mathbb{Z})$*-action on*

$$Y := R[\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})] \otimes_R V_{k-2}(R) \otimes_R R^\chi$$

and an isomorphism

$$_{\Gamma_1(N)\backslash\Gamma_0(N)}X \to Y$$

of right $\mathrm{PSL}_2(\mathbb{Z})$*-modules.*

Exercise 44 *Provide a relationship between Algorithm 5.3.1 and continued fractions.*

5.5 Computer exercises

Computer exercise 17 *Use the description of Exercise 43 and your results from Computer Exercises 15 and 16 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 18 *(a) Write an algorithm to represent any element of* $\mathrm{PSL}_2(\mathbb{Z})$ *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 17).*

Stage 6

Eichler-Shimura

6.1 Theory: Petersson scalar product

Recall the (closed) standard fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$ (from last term's course)

$$\mathcal{F} = \{z = x + iy \in \mathbb{H} \,|\, |z| \geq 1, |x| \leq \frac{1}{2}\}.$$

Every subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ of finite index has a fundamental domain, e.g. $\bigcup_{\gamma \in \overline{\Gamma}\backslash \mathrm{PSL}_2(\mathbb{Z})} \gamma\mathcal{F}$ for any choice of system of representatives of the cosets $\overline{\Gamma}\backslash\mathrm{PSL}_2(\mathbb{Z})$, where we put $\overline{\Gamma} = \Gamma/(\langle \pm 1\rangle \cap \Gamma)$.

Lemma 6.1.1 *(a) Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a subgroup of finite index. Let $f \in \mathrm{M}_k(\Gamma\,;\mathbb{C})$ and $g \in \mathrm{S}_k(\Gamma\,;\mathbb{C})$. We have with $z \in \mathbb{H}$*

$$f(\gamma z)\overline{g(\gamma z)}(\gamma z - \gamma\overline{z})^k = f|_\gamma(z)\overline{g|_\gamma(z)}(z-\overline{z})^k$$

for all $\gamma \in \mathrm{SL}_2(\mathbb{R})$. The function $G(z) := f(z)\overline{g(z)}(z-\overline{z})^k$ is bounded on $\mathbb{H}$.

(b) We have $d\gamma z = \frac{1}{(cz+d)^2}dz$ for all $\gamma \in \mathrm{SL}_2(\mathbb{R})$.

(c) The differential form $\frac{dz\wedge d\overline{z}}{(z-\overline{z})^2}$ is $\mathrm{SL}_2(\mathbb{R})$-invariant. In terms of $z = x + iy$ we have $\frac{dz\wedge d\overline{z}}{(z-\overline{z})^2} = \frac{i}{2}\frac{dx\wedge dy}{y^2}$.

(d) Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a subgroup with finite index $\mu = (\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma})$. The volume of any fundamental domain $\mathcal{F}_\Gamma$ for Γ with respect to the differential form $\frac{2dz\wedge d\overline{z}}{i(z-\overline{z})^2}$, i.e.

$$\mathrm{vol}(\mathcal{F}_\Gamma) = \int_{\mathcal{F}_\Gamma} \frac{2dz\wedge d\overline{z}}{i(z-\overline{z})^2},$$

is equal to $\mu\frac{\pi}{3}$.

Proof. (a) The first statement is computed as follows:

$$\begin{aligned} f(\gamma z)\overline{g(\gamma z)}(\gamma z - \gamma\overline{z})^k &= (f|_\gamma(z)(cz+d)^k)\overline{(g|_\gamma(z)(cz+d)^k)}(\frac{az+b}{cz+d} + \frac{a\overline{z}+b}{c\overline{z}+d})^k \\ &= f|_\gamma(z)\overline{g|_\gamma(z)}((az+b)(c\overline{z}+d) - (a\overline{z}+b)(cz+d))^k \\ &= f|_\gamma(z)\overline{g|_\gamma(z)}(z-\overline{z})^k, \end{aligned}$$

where we write $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. 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 any closed fundamental domain $\mathcal{F}_\Gamma$ 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 $G(\gamma z) = f|_\gamma(z)\overline{g|_\gamma(z)}(z-\overline{z})^k$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Note that $f(z)g(z)$ is a cusp form in $\mathrm{S}_{2k}(\Gamma\,;\mathbb{C})$, 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 goes to 0 if y tends to ∞. Consequently, the function $G(\gamma z)$ is bounded on all of the standard fundamental domain, as desired.

(b) Again writing $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ we have

$$\frac{d\gamma z}{dz} = \frac{d\frac{az+b}{cz+d}}{dz} = \frac{1}{(cz+d)^2}(a(cz+d) - (az+b)c) = \frac{1}{(cz+d)^2},$$

which gives the claim.

(c) This is again a simple computation:

$$\begin{aligned} (\gamma z - \gamma\overline{z})^{-2} d\gamma z \wedge d\gamma\overline{z} &= \left(\frac{az+b}{cz+d} + \frac{a\overline{z}+b}{c\overline{z}+d}\right)^{-2} (cz+d)^{-2}(c\overline{z}+d)^{-2} dz \wedge d\overline{z} \\ &= (z-\overline{z})^{-2} dz \wedge d\overline{z}, \end{aligned}$$

using (b). The last statement is

$$\frac{dz \wedge d\overline{z}}{(z-\overline{z})^2} = \frac{(dx+idy)\wedge(dx-idy)}{(2iy)^2} = \frac{-2idx\wedge dy}{-4y^2} = \frac{idx\wedge dy}{2y^2}.$$

(d) Due to the Γ-invariance, it suffices to show

$$\int_{\mathcal{F}} \frac{dz \wedge d\overline{z}}{(z-\overline{z})^2} = \frac{i\pi}{6}.$$

Let $\omega = -\frac{dz}{z-\overline{z}}$. The total derivative of ω is

$$d\omega = ((z-\overline{z})^{-2} dz - (z-\overline{z})^{-2} d\overline{z}) \wedge dz = \frac{dz \wedge d\overline{z}}{(z-\overline{z})^2}.$$

Hence, Stokes' theorem yields

$$\int_{\mathcal{F}} \frac{dz \wedge d\overline{z}}{(z-\overline{z})^2} = -\int_{\partial\mathcal{F}} \frac{dz}{z-\overline{z}},$$

where $\partial\mathcal{F}$ is the positively oriented border of $\mathcal{F}$, which we desribe 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

$$\int_{\mathcal{F}} \frac{dz \wedge d\overline{z}}{(z-\overline{z})^2} = -\frac{1}{2i}\Big(\int_A \frac{dz}{y} - \int_{TA} \frac{dz}{y} + \int_C \frac{dz}{y}\Big) = -\frac{1}{2i}\int_C \frac{dz}{y},$$

since $dz = dTz$. Using the obvious parametrisation of C we obtain

$$\begin{aligned} -\frac{1}{2i}\int_C \frac{dz}{y} = -\frac{1}{2i}\int_{2\pi/3}^{2\pi/6} \frac{1}{\mathrm{Im}(e^{i\phi})}\frac{de^{i\phi}}{d\phi}d\phi = -\frac{1}{2}\int_{2\pi/3}^{2\pi/6} \frac{e^{i\phi}}{\mathrm{Im}(e^{i\phi})}d\phi \\ = -\frac{1}{2}\int_{2\pi/3}^{2\pi/6} \Big(\frac{\cos(\phi)}{\sin(\phi)} + i\Big)d\phi = -\frac{i}{2}\Big(\frac{2\pi}{6} - \frac{2\pi}{3}\Big) = \frac{i\pi}{6}, \end{aligned}$$

since $\sin$ is symmetric around $\pi/2$ and $\cos$ is antisymmetric, so that the integral over $\frac{\cos(\phi)}{\sin(\phi)}$ cancels. □

Definition 6.1.2 *Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a subgroup of finite index and let $\mu := (\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma})$ be the index of $\overline{\Gamma} = \Gamma/(\langle \pm 1\rangle \cap \Gamma)$ in $\mathrm{PSL}_2(\mathbb{Z})$. We define the* Petersson pairing *as*

$$\mathrm{M}_k(\Gamma\,;\mathbb{C}) \times \mathrm{S}_k(\Gamma\,;\mathbb{C}) \to \mathbb{C}, \quad (f,g) \mapsto \frac{1}{\mu}\int_{\mathcal{F}_\Gamma} f(z)\overline{g(z)}(z-\overline{z})^k \frac{2dz \wedge d\overline{z}}{i(z-\overline{z})^2} =: (f,g),$$

where $\mathcal{F}_\Gamma$ is any fundamental domain for Γ.

Proposition 6.1.3 *(a) The integral in the Petersson pairing converges. It does not depend on the choice of the fundamental domain $\mathcal{F}_\Gamma$.*

(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 $\mathrm{S}_k(\Gamma\,;\mathbb{C})$ 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 6.1.1 the integral converges, since the function $G(z) := f(z)\overline{g(z)}(z-\overline{z})^k$ is bounded on $\mathcal{F}_\Gamma$ and the volume of $\mathcal{F}_\Gamma$ 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) The product to (f,f) is $\frac{1}{\mu}\int_{\mathcal{F}} |f(z)|^2 y^{k-2} dx \wedge dy$, 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 $\mathcal{F}_\Gamma$ is a fundamental domain for Γ, then $\bigcup_{\gamma\in\Gamma'\backslash\Gamma}\gamma\mathcal{F}_\Gamma$ is a fundamental domain for Γ' (for any choice of representatives of $\Gamma'\backslash\Gamma$). But on every $\gamma\mathcal{F}_\Gamma$ the integral takes the same value. □

Proposition 6.1.4 *Let $f,g\in \mathrm{S}_k(\Gamma\,;\mathbb{C})$. We have*

$$(f,g)=\frac{2}{i\mu}\sum_{\gamma\in\overline{\Gamma}\backslash\mathrm{PSL}_2(\mathbb{Z})}\int_{\zeta_3}^{i}\int_{\infty}^{0} f|_\gamma(z)\overline{g|_\gamma(z)}(z-\overline{z})^{k-2}dzd\overline{z}.$$

Proof. Let us write for short $G_\gamma(z,\overline{z})=f|_\gamma(z)\overline{g|_\gamma(z)}(z-\overline{z})^k$ for $\gamma\in\mathrm{SL}_2(\mathbb{Z})$. Then

$$\frac{i\mu}{2}(f,g)=\int_{\bigcup_\gamma\gamma\mathcal{F}}G(z,\overline{z})\frac{dz\wedge d\overline{z}}{(z-\overline{z})^2}=\sum_\gamma\int_{\mathcal{F}}G_\gamma(z,\overline{z})\frac{dz\wedge d\overline{z}}{(z-\overline{z})^2}$$

by Lemma 6.1.1, where the union resp. sum runs over a fixed system of coset representatives of $\overline{\Gamma}\backslash\mathrm{PSL}_2(\mathbb{Z})$; by our observations everything is independent of this choice. Consider the differential form

$$\omega_\gamma:=\big(\int_\infty^z f|_\gamma(u)(u-\overline{z})^{k-2}du\big)\overline{g|_\gamma(z)}d\overline{z}.$$

Note that the integral converges, since f is a cusp form. The total derivative of ω_γ is $d\omega_\gamma=G_\gamma(z,\overline{z})\frac{dz\wedge d\overline{z}}{(z-\overline{z})^2}$. Consequently, Stokes' theorem gives

$$\sum_\gamma\int_{\mathcal{F}}G_\gamma(z,\overline{z})\frac{dz\wedge d\overline{z}}{(z-\overline{z})^2}=\sum_\gamma\int_{\partial\mathcal{F}}\big(\int_\infty^z f|_\gamma(u)(u-\overline{z})^{k-2}du\big)\overline{g|_\gamma(z)}d\overline{z},$$

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 $M\in\mathrm{SL}_2(\mathbb{Z})$:

$$\begin{aligned}
&\int_{MC}\int_\infty^z f|_\gamma(u)\overline{g|_\gamma(z)}(u-\overline{z})^{k-2}dud\overline{z}\\
&=\int_C\int_\infty^{Mz} f|_\gamma(u)\overline{g|_\gamma(Mz)}(u-M\overline{z})^{k-2}du\frac{dM\overline{z}}{d\overline{z}}d\overline{z}\\
&=\int_C\int_{M^{-1}\infty}^z f|_{\gamma M}(u)\overline{g|_{\gamma M}(z)}(u-\overline{z})^{k-2}dud\overline{z}\\
&=\int_C\int_\infty^z f|_{\gamma M}(u)\overline{g|_{\gamma M}(z)}(u-\overline{z})^{k-2}dud\overline{z}-\int_C\int_\infty^{M^{-1}\infty} f|_{\gamma M}(u)\overline{g|_{\gamma M}(z)}(u-\overline{z})^{k-2}dud\overline{z}.
\end{aligned}$$

This gives

$$\begin{aligned}
\int_{C-MC}\int_\infty^z f|_\gamma(u)\overline{g|_\gamma(z)}(u-\overline{z})^{k-2}dud\overline{z}=&\\
&\int_C\int_\infty^z(G_\gamma(u,\overline{z})-G_{\gamma M}(u,\overline{z}))dud\overline{z}+\int_C\int_\infty^{M^{-1}\infty}G_{\gamma M}(u,\overline{z})dud\overline{z}.
\end{aligned}$$

Continuing with the main calculation, we have

$$\begin{aligned}\frac{i\mu}{2}(f,g) &= \sum_\gamma \Big[\int_A \int_\infty^z (G_\gamma(u,\overline{z}) - G_{\gamma T}(u,\overline{z}))dud\overline{z} + \int_A \int_\infty^{T^{-1}\infty} G_{\gamma T}(u,\overline{z})dud\overline{z}\Big] \\ &+ \sum_\gamma \Big[\int_B \int_\infty^z (G_\gamma(u,\overline{z}) - G_{\gamma\sigma}(u,\overline{z}))dud\overline{z} + \int_B \int_\infty^{\sigma^{-1}\infty} G_{\gamma\sigma}(u,\overline{z})dud\overline{z}\Big] \\ &= \sum_\gamma \int_B \int_\infty^0 G_{\gamma\sigma}(u,\overline{z})dud\overline{z},\end{aligned}$$

using $T^{-1}\infty = \infty$, $\sigma^{-1}\infty = 0$ and the fact that the γT and $\gamma\sigma$ are just permutations of the cosets. □

6.2 Theory: The Eichler-Shimura map

Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a subgroup of finite index.

Definition 6.2.1 *The space of* antiholomorphic cusp forms $\overline{\mathrm{S}_k(\Gamma\,;\,\mathbb{C})}$ *consists of the functions* $z \mapsto \overline{f}(z) := \overline{f(z)}$ *with* $f \in \mathrm{S}_k(\Gamma\,;\,\mathbb{C})$.

We fix some $z_0, z_1 \in \mathbb{H}$. For $f \in \mathrm{M}_k(\Gamma\,;\,\mathbb{C})$ with $k \geq 2$ and g, h in $\mathrm{SL}_2(\mathbb{Z})$ let

$$I_f(gz_0, hz_0) := \int_{gz_0}^{hz_0} f(z)(Xz+Y)^{k-2}dz \in V_{k-2}(\mathbb{C})$$

and

$$I_{\overline{f}}(gz_1, hz_1) := \int_{gz_1}^{hz_1} \overline{f(z)}(X\overline{z}+Y)^{k-2}d\overline{z} \in V_{k-2}(\mathbb{C}).$$

The integral is to be taken coefficient wise. Note that it is independent of the chosen path, since we are integrating a holomorphic respectively anti-holomorphic function.

Lemma 6.2.2 *For any* $z_0 \in \mathbb{H}$ *and any matrices* $g, h \in \mathbb{Z}^{2\times 2}$ *with positive determinant we have*

$$I_f(z_0, ghz_0) = I_f(z_0, gz_0) + I_f(gz_0, ghz_0)$$

and

$$I_f(gz_0, ghz_0) = det(g)^{2-k} g.\big(I_{f|_g}(z_0, hz_0)\big)$$

and similarly for $\overline{f}$.

Proof. The first statement is clear. Write $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Recall that by Lemma 6.1.1 (b), we have $dgz = \frac{\det(g)}{(cz+d)^2}dz$. We compute further

$$\begin{aligned}
I_f(gz_0, ghz_0) &= \int_{gz_0}^{ghz_0} f(z)(Xz+Y)^{k-2}dz \\
&= \int_{z_0}^{hz_0} f(gz)(Xgz+Y)^{k-2}\frac{dgz}{dz}dz \\
&= \det(g)^{2-k}\int_{z_0}^{hz_0} f|_g(z)(cz+d)^{k-2}(X\frac{az+b}{cz+d}+Y)^{k-2}dz \\
&= \det(g)^{2-k}\int_{z_0}^{hz_0} f|_g(z)(X(az+b)+Y(cz+d))^{k-2}dz \\
&= \det(g)^{2-k}\int_{z_0}^{hz_0} f|_g(z)((Xa+Yc)z+(Xb+Yd))^{k-2}dz \\
&= \det(g)^{2-k}\int_{z_0}^{hz_0} f|_g(z)(g.(Xz+Y)^{k-2})dz \\
&= \det(g)^{2-k}g.\big(\int_{z_0}^{hz_0} f|_g(z)(Xz+Y)^{k-2}dz\big) \\
&= \det(g)^{2-k}g.\big(I_{f|_g}(z_0, hz_0)\big).
\end{aligned}$$

We recall that for a polynomial $P(X,Y)$ we have the action $(g.P)(X,Y) = P((X,Y)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) = P(Xa+Yc, Xb+Yd)$. The statement on $I_{\overline{f}}$ is proved in exactly the same way. □

Proposition 6.2.3 *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

$$\begin{aligned}
\mathrm{M}_k(\Gamma\,;\mathbb{C}) \oplus \overline{\mathrm{S}_k(\Gamma\,;\mathbb{C})} &\to \mathrm{H}^1(\Gamma, V_{k-2}(\mathbb{C})), \\
(f,\overline{g}) &\mapsto (\gamma \mapsto I_f(z_0,\gamma z_0) + I_{\overline{g}}(z_1,\gamma z_1))
\end{aligned}$$

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

$$\begin{aligned}
\mathrm{M}_k(\Gamma\,;\mathbb{C}) \oplus \overline{\mathrm{S}_k(\Gamma\,;\mathbb{C})} &\to \mathrm{H}^1(\mathrm{SL}_2(\mathbb{Z}), \mathrm{Hom}_{\mathbb{C}[\Gamma]}(\mathbb{C}[\mathrm{SL}_2(\mathbb{Z})], V_{k-2}(\mathbb{C}))), \\
(f,\overline{g}) &\mapsto (a \mapsto (b \mapsto I_f(bz_0, baz_0) + I_{\overline{g}}(bz_1, baz_1)))
\end{aligned}$$

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:

$$I_f(z_0, \gamma\delta z_0) = I_f(z_0, \gamma z_0) + I_f(\gamma z_0, \gamma\delta z_0) = I_f(z_0, \gamma z_0) + \gamma.I_f(z_0, \delta z_0),$$

using Lemma 6.2.2 and $f|_\gamma = f$, since $\gamma \in \Gamma$.

The independence of the base point is seen as follows. Let $\tilde{z}_0$ be another 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 $(b \mapsto I_f(bz_0, baz_0) + I_{\overline{g}}(bz_0, baz_0))$ 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

$$I_f(\gamma bz_0, \gamma baz_0) = \gamma.(I_f(bz_0, baz_0))$$

by Lemma 6.2.2, as desired. The map $\phi(a) := (b \mapsto I_f(bz_0, baz_0) + I_{\overline{g}}(bz_1, baz_1))$ is a cocycle:

$$\begin{aligned}\phi(a_1a_2)(b) = I_f(bz_0, ba_1a_2z_0) &= I_f(bz_0, ba_1z_0) + I_f(ba_1z_0, ba_1a_2z_0) \\ &= \phi(a_1)(b) + \phi(a_2)(ba_1) = \phi(a_1)(b) + (a_1.(\phi(a_2)))(b),\end{aligned}$$

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

$$\phi \mapsto (\gamma \mapsto \phi(\gamma)(1) = I_f(z_0, \gamma z_0)),$$

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). □

Proposition 6.2.4 *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 $\mathrm{H}^1(\mathrm{SL}_2(\mathbb{Z}), \mathrm{Hom}_{R[\Gamma]}(R[\mathrm{SL}_2(\mathbb{Z})], V))$ and $\mathrm{H}^1(\mathrm{PSL}_2(\mathbb{Z}), \mathrm{Hom}_{R[\overline{\Gamma}]}(R[\mathrm{PSL}_2(\mathbb{Z})], V))$ are naturally isomorphic. We shall make this identification from now on.

Proof. Due to the invertibility of 2, the Hochschild-Serre exact sequence gives an isomorphism

$$\mathrm{H}^1(\mathrm{PSL}_2(\mathbb{Z}), \mathrm{Hom}_{R[\Gamma]}(R[\mathrm{SL}_2(\mathbb{Z})], V)^{\langle -1\rangle}) \xrightarrow{\mathrm{infl}} \mathrm{H}^1(\mathrm{SL}_2(\mathbb{Z}), \mathrm{Hom}_{R[\Gamma]}(R[\mathrm{SL}_2(\mathbb{Z})], V)).$$

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 $\mathrm{Hom}_{R[\Gamma]}(R[\mathrm{PSL}_2(\mathbb{Z})], V)$.

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 $\langle -1\rangle$. □

Proposition 6.2.5 *The kernel of the Eichler-Shimura map composed with the restriction*

$$\mathrm{M}_k(\Gamma\,;\,\mathbb{C}) \oplus \overline{\mathrm{S}_k(\Gamma\,;\,\mathbb{C})} \to \mathrm{H}^1(\Gamma, V_{k-2}(\mathbb{C})) \to \prod_{c\in\Gamma\backslash\mathbb{P}^1(\mathbb{Q})} \mathrm{H}^1(\Gamma_c, V_{k-2}(\mathbb{C}))$$

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* $\mathrm{H}^1_{\mathrm{par}}(\Gamma, V_{k-2}(\mathbb{C}))$*.*

Proof. The composition maps a 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 $M = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. We then have $\Gamma_c = \langle MTM^{-1}\rangle \cap \Gamma = \langle MT^rM^{-1}\rangle$ for some $r \geq 1$. Since f is holomorphic in the cusps, we have

$$f|_M(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z} = a_0 + g(z)$$

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 $\gamma = MT^sM^{-1}$:

$$\int_{z_0}^{\gamma z_0} f(z)(Xz+Y)^{k-2}dz = a_0\int_{z_0}^{\gamma z_0} \frac{(Xz+Y)^{k-2}}{(-cz+a)^k}dz + \int_{z_0}^{\gamma z_0} g|_{M^{-1}}(z)(Xz+Y)^{k-2}dz.$$

Before we continue by evaluating the right summand, we remark that the integral

$$I_{g|_{M^{-1}}}(z_0, M\infty) = \int_{z_0}^{M\infty} g|_{M^{-1}}(z)(Xz+Y)^{k-2}dz = M.\int_{M^{-1}z_0}^{\infty} g(z)(Xz+Y)^{k-2}dz$$

converges. We have

$$\begin{aligned}\int_{z_0}^{\gamma z_0} g|_{M^{-1}}(z)(Xz+Y)^{k-2}dz &= \Big(\int_{z_0}^{M\infty} + \int_{\gamma M\infty}^{\gamma z_0}\Big) g|_{M^{-1}}(z)(Xz+Y)^{k-2}dz \\ &= (1-\gamma).\int_{z_0}^{M\infty} g|_{M^{-1}}(z)(Xz+Y)^{k-2}dz\end{aligned}$$

since $g|_{M^{-1}\gamma}(z) = g|_{T^sM^{-1}}(z) = g|_{M^{-1}}(z)$. 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)

$$\mathrm{H}^1(\Gamma_c, V_{k-2}(\mathbb{C})) \xrightarrow{\phi\mapsto\phi(MT^rM^{-1})} V_{k-2}(\mathbb{C})_{\Gamma_c}.$$

Furthermore, we have the isomorphism

$$V_{k-2}(\mathbb{C})_{\Gamma_c} \xrightarrow{P\mapsto M^{-1}P} V_{k-2}(\mathbb{C})_{\langle T^s\rangle} \xrightarrow{P\mapsto P(0,1)} \mathbb{C}$$

with polyomials $P(X,Y)$. Note that the last map is an isomorphism by the explicit description of $V_{k-2}(\mathbb{C})_{\langle T^s\rangle}$. Under the composition the image of the cocycle coming from the modular form f is

$$\begin{aligned} a_0M^{-1}.\int_{z_0}^{\gamma z_0}\frac{(Xz+Y)^{k-2}}{(-cz+a)^k}dz(0,1) &= a_0\int_{z_0}^{\gamma z_0}\frac{(Xz+Y)^{k-2}}{(-cz+a)^k}dz(-c,a)\\ &= a_0\int_{z_0}^{\gamma z_0}\frac{1}{(-cz+a)^2}dz = a_0\int_{M^{-1}z_0}^{T^rM^{-1}z_0}dz = a_0(M^{-1}z_0+r-M^{-1}z_0) = ra_0, \end{aligned}$$

as $(0,1)M^{-1} = (0,1)\left(\begin{smallmatrix} d & -b\\ -c & a\end{smallmatrix}\right) = (-c,a)$. 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.

Definition 6.3.1 *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

$$\cup : \mathrm{H}^n(G,M)\otimes_R \mathrm{H}^m(G,N)\to \mathrm{H}^{n+m}(G, M\otimes_R N)$$

by

$$(\phi,\psi)\mapsto((g_1,\dots,g_n,g_{n+1},\dots,g_{n+m})\mapsto \phi(g_1,\dots,g_n)\otimes g_n.\psi(g_{n+1},\dots,g_{n+m})$$

on cochains of the bar resolution.

In Exercise 45 it is checked that the cup product is well-defined. 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 6.3.2 *Let M be an $R[\mathrm{PSL}_2(\mathbb{Z})]$-module. The* parabolic 1-cocycles *are defined as*

$$\mathrm{Z}^1_{\mathrm{par}}(\Gamma,M) = \ker(\mathrm{Z}^1(\Gamma,M)\xrightarrow{\mathrm{res}}\prod_{g\in\Gamma\backslash\mathrm{PSL}_2(\mathbb{Z})/\langle T\rangle}\mathrm{Z}^1(\Gamma\cap\langle gTg^{-1}\rangle,V)).$$

Proposition 6.3.3 *Let R be a ring in which 6 is invertible. Let M,N be left $R[\mathrm{PSL}_2(\mathbb{Z})]$-modules together with a homomorphism $\pi : M\otimes_R N\to R$ of $R[\mathrm{PSL}_2(\mathbb{Z})]$-modules, where we equiv $M\otimes_R N$ with the diagonal action. Write G for $\mathrm{PSL}_2(\mathbb{Z})$. We define a pairing*

$$\langle,\rangle : \mathrm{Z}^1(G,M)\times\mathrm{Z}^1(G,N)\to R$$

as follows: Let (ϕ, ψ) be a pair of 1-cocycles. Form their cup product $\rho := \pi_*(\phi \cup \psi)$ in $\mathrm{Z}^2(G, R)$ via $\mathrm{Z}^2(G, M \otimes_R N) \xrightarrow{\pi_*} \mathrm{Z}^2(G, R)$. As $\mathrm{H}^2(G, R)$ is zero (Corollary 4.2.4), ρ must be a 2-coboundary, i.e. there is $a : G \to R$ such that

$$\rho(g, h) = \pi(\phi(g) \otimes g.\psi(h)) = g.a(h) - a(gh) + a(g).$$

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 $\phi \in \mathrm{Z}^1_{\mathrm{par}}(G, M)$, 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 $\mathrm{H}^1(G, N)$.

(c) If $\psi \in \mathrm{Z}^1_{\mathrm{par}}(G, N)$, 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 $\mathrm{H}^1(G, M)$.

(d) If $\phi \in \mathrm{Z}^1_{\mathrm{par}}(G, M)$ and $\psi \in \mathrm{Z}^1_{\mathrm{par}}(G, N)$, 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

$$\begin{aligned}
\rho(\tau, \sigma) &= a(\tau) - a(T) + a(\sigma) \\
\rho(\sigma, \sigma) &= a(\sigma) - a(1) + a(\sigma) = 2a(\sigma) \\
\rho(\tau, \tau^2) &= a(\tau^2) - a(1) + a(\tau) = a(\tau) + a(\tau^2) \\
\rho(\tau, \tau) &= a(\tau) - a(\tau^2) + a(\tau) = 2a(\tau) - a(\tau^2)
\end{aligned}$$

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

$$\rho(\tau,\sigma) = \pi(\phi(\tau) \otimes \tau\psi(\sigma)) = -\pi(\tau.\phi(\sigma) \otimes \tau\psi(\sigma)) \\ = -\pi(\phi(\sigma) \otimes \psi(\sigma)) = \pi((\phi(\sigma) \otimes \sigma\psi(\sigma))) = \rho(\sigma,\sigma)$$

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 $\psi(g) = (g-1)n$ be a 1-coboundary. Put $b(g) := -\phi(g) \otimes gn$. Then one immediately checks the equality

$$\rho(g,h) = \phi(g) \otimes g(h-1)n = g.b(h) - b(gh) + b(g).$$

Hence, (ϕ,ψ) is mapped to $b(T) = -\phi(T) \otimes Tn = 0 \otimes Tn = 0$.

(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 $c(g) := m \otimes \psi(g)$. Then the equality

$$\rho(g,h) = (g-1)m \otimes g\psi(h) = g.c(h) - c(gh) + c(g)$$

holds. Hence, (ϕ,ψ) is mapped to $c(T) = m \otimes \psi(T) = m \otimes 0 = 0$.

(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 $\mathrm{Sym}^{k-2}(R^2)$ 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

$$R^2 \times R^2 \to R^2, \quad \left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right) \bullet \left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right) := \det \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).$$

For any $g \in \mathrm{SL}_2(\mathbb{Z})$ we have

$$g\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right) \bullet g\left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right) = \det g \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \det \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right) \bullet \left(\begin{smallmatrix} b \\ d \end{smallmatrix}\right).$$

As the next step, we define a pairing on the n-th tensor power of R^2

$$(R^2 \otimes_R \cdots \otimes_R R^2) \times (R^2 \otimes_R \cdots \otimes_R R^2) \to R$$

by

$$(\left(\begin{smallmatrix} a_1 \\ c_1 \end{smallmatrix}\right) \otimes \cdots \otimes \left(\begin{smallmatrix} a_n \\ c_n \end{smallmatrix}\right)) \bullet (\begin{pmatrix} b_1 \\ d_1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} b_n \\ d_n \end{pmatrix}) := \prod_{i=1}^{n} \left(\begin{smallmatrix} a_i \\ c_i \end{smallmatrix}\right) \bullet \begin{pmatrix} b_i \\ d_i \end{pmatrix}.$$

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 n is on the indices. We have that the map (in fact, $1/n!$ times the norm)

$$\mathrm{Sym}^n(R^2) \to R^2 \otimes_R \cdots \otimes_R R^2, \quad [\left(\begin{smallmatrix} a_1 \\ c_1 \end{smallmatrix}\right) \otimes \cdots \otimes \left(\begin{smallmatrix} a_n \\ c_n \end{smallmatrix}\right)] \mapsto \frac{1}{n!} \sum_{\sigma \in S_n} \begin{pmatrix} a_{\sigma(1)} \\ c_{\sigma(1)} \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} a_{\sigma(n)} \\ c_{\sigma(n)} \end{pmatrix}$$

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

$$\left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)^{\otimes(k-2)} \bullet \begin{pmatrix} b \\ d \end{pmatrix}^{\otimes(k-2)} = (ad - bc)^{k-2}.$$

Hence, after the identification $\mathrm{Sym}^{k-2}(R^2) \cong V_{k-2}(R)$ from Exercise 10, 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 paring on induced modules

$$\pi : \mathrm{Hom}_{R[\Gamma]}(R[\mathrm{PSL}_2(\mathbb{Z})], V_{k-2}(R)) \otimes_R \mathrm{Hom}_{R[\Gamma]}(R[\mathrm{PSL}_2(\mathbb{Z})], V_{k-2}(R)) \to R$$

by mapping (α, β) to $\sum_{\gamma \in \Gamma \backslash \mathrm{PSL}_2(\mathbb{Z})} \alpha(\gamma) \bullet \beta(\gamma)$.

Proposition 6.3.4 *Let $k \geq 2$. Let $f, g \in \mathrm{S}_k(\Gamma\,; \mathbb{C})$ be cusp forms. Denote by ϕ_f and $\phi_{\overline{f}}$ the 1-cocycles associated with f and $\overline{f}$ under the Eichler-Shimura map for the base points $z_0 = \infty$, i.e.*

$$\phi_f(a) = (b \mapsto I_f(b\infty, ba\infty)) \in \mathrm{Z}^1(\mathrm{PSL}_2(\mathbb{Z}), \mathrm{Coind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V_{k-2}(\mathbb{C})))$$

and

$$\phi_{\overline{f}}(a) = (b \mapsto I_{\overline{f}}(b\infty, ba\infty)) \in \mathrm{Z}^1(\mathrm{PSL}_2(\mathbb{Z}), \mathrm{Coind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V_{k-2}(\mathbb{C}))).$$

Similarly, denote by ψ_g and $\psi_{\overline{g}}$ the 1-cocycles associated with g and $\overline{g}$ for the base point $z_1 = \zeta_6$. Define a bilinear pairing as in Proposition 6.3.3

$$\langle , \rangle : \mathrm{Z}^1(\mathrm{PSL}_2(\mathbb{Z}), \mathrm{Coind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V_{k-2}(\mathbb{C}))) \times \mathrm{Z}^1(\mathrm{PSL}_2(\mathbb{Z}), \mathrm{Coind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V_{k-2}(\mathbb{C}))) \to \mathbb{C}$$

with the product on the coinduced modules described above.

Then the equations

$$\begin{aligned}\langle \phi_f, \psi_{\overline{g}} \rangle &= \frac{\mu}{2i}(f,g)\\ \langle \psi_{\overline{g}}, \phi_f \rangle &= (-1)^{k-1}\langle \phi_f, \psi_{\overline{g}} \rangle \text{ and}\\ \langle \phi_{\overline{f}}, \psi_{\overline{g}} \rangle &= (-1)^{k-1}\overline{\langle \psi_g, \phi_f \rangle}\end{aligned}$$

hold, where (f,g) *denotes the Petersson scalar product and* μ *the index of* $\overline{\Gamma}$ *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 $\phi_f(T) = \phi_{\overline{f}}(T) = 0$.

Now consider $\langle \phi_f, \psi_{\overline{g}} \rangle$. Let $\rho(a,b) := \pi(\phi_f(a) \otimes a\psi_{\overline{g}}(b))$. We first describe $\rho(a,b)$:

$$\begin{aligned}\rho(a,b) &= \sum_\gamma \Big(\int_{\gamma\infty}^{\gamma a\infty} f(z)(Xz+Y)^{k-2}dz \Big) \bullet \Big(\int_{\gamma a\zeta_6}^{\gamma ab\zeta_6} \overline{g(z)}(X\overline{z}+Y)^{k-2}d\overline{z} \Big)\\ &= \sum_\gamma \int_{\gamma a\zeta_6}^{\gamma ab\zeta_6} \int_{\gamma\infty}^{\gamma a\infty} f(z)\overline{g(z)}\big((Xz+Y)^{k-2} \bullet (X\overline{z}+Y)^{k-2}\big)dzd\overline{z}\\ &= \sum_\gamma \int_{\gamma a\zeta_6}^{\gamma ab\zeta_6} \int_{\gamma\infty}^{\gamma a\infty} f(z)\overline{g(z)}(z-\overline{z})^{k-2}dzd\overline{z}\\ &= \sum_\gamma \int_{a\zeta_6}^{ab\zeta_6} \int_{\infty}^{a\infty} f|_\gamma(z)\overline{g|_\gamma(z)}(z-\overline{z})^{k-2}dzd\overline{z}.\end{aligned}$$

where the sums run over a system of representatives of $\Gamma\backslash\mathrm{PSL}_2(\mathbb{Z})$. We obtain

$$\begin{aligned}\rho(\sigma,\sigma) &= \sum_\gamma \int_{\sigma\zeta_6}^{\sigma^2\zeta_6} \int_{\infty}^{\sigma\infty} f|_\gamma(z)\overline{g|_\gamma(z)}(z-\overline{z})^{k-2}dzd\overline{z}\\ &= \sum_\gamma \int_{\zeta_3}^{\zeta_6} \int_{\infty}^{0} f|_\gamma(z)\overline{g|_\gamma(z)}(z-\overline{z})^{k-2}dzd\overline{z},\\ &= \sum_\gamma \Big[\int_{\zeta_3}^{i} \int_{\infty}^{0} f|_\gamma(z)\overline{g|_\gamma(z)}(z-\overline{z})^{k-2}dzd\overline{z} + \int_{\sigma\zeta_3}^{\sigma i} \int_{\sigma\infty}^{\sigma 0} f|_\gamma(z)\overline{g|_\gamma(z)}(z-\overline{z})^{k-2}dzd\overline{z}\Big]\\ &= \sum_\gamma \Big[\int_{\zeta_3}^{i} \int_{\infty}^{0} f|_\gamma(z)\overline{g|_\gamma(z)}(z-\overline{z})^{k-2}dzd\overline{z} + \int_{\zeta_3}^{i} \int_{\infty}^{0} f|_{\gamma\sigma}(z)\overline{g|_{\gamma\sigma}(z)}(z-\overline{z})^{k-2}dzd\overline{z}\Big]\\ &= 2\sum_\gamma \int_{\zeta_3}^{i} \int_{\infty}^{0} f|_\gamma(z)\overline{g|_\gamma(z)}(z-\overline{z})^{k-2}dzd\overline{z},\\ \rho(\tau,\tau) &= \sum_\gamma \int_{\tau\zeta_6}^{\tau^2\zeta_6} \int_{\infty}^{\tau\infty} f|_\gamma(z)\overline{g|_\gamma(z)}(z-\overline{z})^{k-2}dzd\overline{z} = 0 \text{ and}\\ \rho(\tau,\tau^2) &= \sum_\gamma \int_{\tau\zeta_6}^{\tau^3\zeta_6} \int_{\infty}^{\tau\infty} f|_\gamma(z)\overline{g|_\gamma(z)}(z-\overline{z})^{k-2}dzd\overline{z} = 0,\end{aligned}$$

since τ stabilises ζ_6. It now suffices to compare with the formulas computed before (Propositions 6.3.3 and 6.1.4) to obtain $\langle \phi_f, \psi_{\overline{g}} \rangle = \frac{\mu}{2i}(f,g)$.

Now consider $\langle \psi_{\overline{g}}, \phi_f \rangle$. Let $\lambda(a,b) := \pi(\psi_{\overline{g}}(a) \otimes a\phi_f(b))$. We now describe $\lambda(a,b)$:

$$\begin{aligned}\lambda(a,b) &= \sum_\gamma \Big(\int_{\gamma\zeta_6}^{\gamma a\zeta_6} \overline{g(z)}(X\overline{z}+Y)^{k-2}d\overline{z}\Big) \bullet \Big(\int_{\gamma a\infty}^{\gamma ab\infty} f(z)(Xz+Y)^{k-2}dz\Big) \\ &= \sum_\gamma \int_{\zeta_6}^{a\zeta_6} \int_{a\infty}^{ab\infty} f|_\gamma(z)\overline{g|_\gamma(z)}(\overline{z}-z)^{k-2}dzd\overline{z}.\end{aligned}$$

where again the sums run over a system of representatives of $\Gamma\backslash \mathrm{PSL}_2(\mathbb{Z})$. We find further

$$\begin{aligned}\lambda(\sigma,\sigma) &= (-1)^k \sum_\gamma \int_{\zeta_6}^{\sigma\zeta_6} \int_{\sigma\infty}^{\sigma^2\infty} f|_\gamma(z)\overline{g|_\gamma(z)}(z-\overline{z})^{k-2}dzd\overline{z} \\ &= (-1)^k \sum_\gamma \int_{\zeta_3}^{\zeta_6} \int_{\infty}^{0} f|_\gamma(z)\overline{g|_\gamma(z)}(z-\overline{z})^{k-2}dzd\overline{z} = \rho(\sigma,\sigma), \\ \lambda(\tau,\tau) &= \sum_\gamma \int_{\zeta_6}^{\tau\zeta_6} \int_{\tau\infty}^{\tau^2\infty} f|_\gamma(z)\overline{g|_\gamma(z)}(\overline{z}-z)^{k-2}dzd\overline{z} = 0 \text{ and} \\ \lambda(\tau,\tau^2) &= \sum_\gamma \int_{\zeta_6}^{\tau\zeta_6} \int_{\tau\infty}^{\tau^3\infty} f|_\gamma(z)\overline{g|_\gamma(z)}(\overline{z}-z)^{k-2}dzd\overline{z} = 0.\end{aligned}$$

We can again appeal to Propositions 6.3.3 and 6.1.4 to obtain $\langle \psi_{\overline{g}}, \phi_f \rangle = (-1)^{k-1}\frac{\mu}{2i}(f,g)$.

To prove the final equation we proceed precisely as in the preceding calculations and obtains $\langle \phi_{\overline{f}}, \psi_{\overline{g}} \rangle = (-1)^{k-1}\langle \psi_{\overline{g}}, \phi_{\overline{f}} \rangle$. To conclude, one uses

$$\int_\alpha \overline{F(z)}d\overline{z} = \int_0^1 \overline{F(\alpha(t))}\frac{d\overline{\alpha}}{dt}dt = \int_0^1 \overline{F(\alpha(t))}\overline{\frac{d\alpha}{dt}}dt = \overline{\int_0^1 F(\alpha(t))\frac{d\alpha}{dt}dt} = \overline{\int_\alpha F(z)dz}$$

for any piecewise analytic path $\alpha : [0,1] \to \mathbb{C}$ and any integrable complex valued function F. □

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 5.2.1.

Theorem 6.4.1 (Eichler-Shimura) *Let $N \geq 4$ and $k \geq 2$. The Eichler-Shimura map and the induced Eichler-Shimura map (Proposition 6.2.3) are isomorphisms for $\Gamma = \Gamma_1(N)$. The image of $\mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{C}) \oplus \overline{\mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{C})}$ 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 4.4.2. For the dimension of the left-hand side we refer to last terms course (for even weights) or to [Stein].

Due to Proposition 6.2.5 it suffices to prove that the restriction of the Eichler-Shimura map to $\mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{C}) \oplus \overline{\mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{C})}$ 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 6.2.3 one sees that this choice of base point does not change the cohomology class). As in Proposition 6.3.4, we write ϕ_f and $\phi_{\overline{f}}$ for the 1-cocycles associated with a cusp form f for the base point ∞ and also ψ_f and $\psi_{\overline{f}}$ for the base point ζ_6.

We now make use of the pairing from Proposition 6.3.4 on $\mathrm{Z}^1(\mathrm{PSL}_2(\mathbb{Z}), \mathrm{Coind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V_{k-2}))$, where we put $\Gamma := \Gamma_1(N)$ for short. This pairing induces a pairing

$$\langle , \rangle : \mathrm{Z}^1_{\mathrm{par}}(\mathrm{PSL}_2(\mathbb{Z}), \mathrm{Coind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V_{k-2})) \times \mathrm{H}^1(\mathrm{PSL}_2(\mathbb{Z}), \mathrm{Coind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V_{k-2})) \to R.$$

Let $f, g \in \mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{C})$ be cusp forms and assume that $[\phi_f] + [\phi_{\overline{g}}] = 0$. By $[\cdot]$ we denote cohomology classes. We must make a distinction between odd and even weights. Assume first that k is even. Then the formulae from Proposition 6.3.4 give

$$\begin{aligned}
0 &= \langle -\phi_{\overline{f}} + \phi_g, [\phi_f] + [\phi_{\overline{g}}] \rangle = -\langle \phi_{\overline{f}}, [\phi_f] \rangle + \langle \phi_g, [\phi_{\overline{g}}] \rangle - \langle \phi_{\overline{f}}, [\phi_{\overline{g}}] \rangle + \langle \phi_g, [\phi_f] \rangle \\
&= -\langle \phi_{\overline{f}}, \phi_f \rangle + \langle \phi_g, \phi_{\overline{g}} \rangle - \langle \phi_{\overline{f}}, \phi_{\overline{g}} \rangle + \langle \phi_g, \phi_f \rangle = -\langle \psi_{\overline{f}}, \phi_f \rangle + \langle \phi_g, \psi_{\overline{g}} \rangle - \langle \phi_{\overline{f}}, \psi_{\overline{g}} \rangle + \langle \psi_g, \phi_f \rangle \\
&= \langle \phi_f, \psi_{\overline{f}} \rangle + \langle \phi_g, \psi_{\overline{g}} \rangle + \overline{\langle \psi_g, \phi_f \rangle} + \langle \psi_g, \phi_f \rangle \\
&= \frac{\mu}{2i}\big((f,f) + (g,g)\big) + 2\,\mathrm{Re}(\langle \psi_g, \phi_f \rangle).
\end{aligned}$$

Hence, $(f,f) = 0 = (g,g)$ and, thus, $f = g = 0$, since the Petersson scalar product is positive definite. If k is odd, we conclude similarly:

$$\begin{aligned}
0 &= \langle \phi_{\overline{f}} + \phi_g, [\phi_f] + [\phi_{\overline{g}}] \rangle = \langle \phi_{\overline{f}}, [\phi_f] \rangle + \langle \phi_g, [\phi_{\overline{g}}] \rangle + \langle \phi_{\overline{f}}, [\phi_{\overline{g}}] \rangle + \langle \phi_g, [\phi_f] \rangle \\
&= \langle \phi_{\overline{f}}, \phi_f \rangle + \langle \phi_g, \phi_{\overline{g}} \rangle + \langle \phi_{\overline{f}}, \phi_{\overline{g}} \rangle + \langle \phi_g, \phi_f \rangle = \langle \psi_{\overline{f}}, \phi_f \rangle + \langle \phi_g, \psi_{\overline{g}} \rangle + \langle \phi_{\overline{f}}, \psi_{\overline{g}} \rangle + \langle \psi_g, \phi_f \rangle \\
&= \langle \phi_f, \psi_{\overline{f}} \rangle + \langle \phi_g, \psi_{\overline{g}} \rangle + \overline{\langle \psi_g, \phi_f \rangle} + \langle \psi_g, \phi_f \rangle \\
&= \frac{\mu}{2i}\big((f,f) + (g,g)\big) + 2\,\mathrm{Re}(\langle \psi_g, \phi_f \rangle).
\end{aligned}$$

Hence, again $f = g = 0$. This proves the injectivity. □

Remark 6.4.2 *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 4.4.3) and modular forms.*

In Corollary 7.4.1 we will see that there also is an Eichler-Shimura isomorphism with a Dirichlet character.

6.5 Theoretical exercises

Exercise 45 *Check that the cup product is well-defined.*

Stage 7

Hecke operators

7.1 Hecke rings

Definition 7.1.1 *Let $N, n \in \mathbb{N}$. We define*

$$\begin{aligned}
\Delta_0^n(N) &= \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) | \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \mod N, (a, N) = 1, \det \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = n\}, \\
\Delta_1^n(N) &= \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) | \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \mod N, \det \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = n\}, \\
\Delta_0(N) &= \bigcup_{n \in \mathbb{N}} \Delta_0^n(N), \\
\Delta_1(N) &= \bigcup_{n \in \mathbb{N}} \Delta_1^n(N).
\end{aligned}$$

In the following we always let $(\Delta, \Gamma) = (\Delta_1(N), \Gamma_1(N))$ oder $(\Delta, \Gamma) = (\Delta_0(N), \Gamma_0(N))$, unless we state something different explicitly.

Lemma 7.1.2 *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 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. □

Example 7.1.3 *Let $\Gamma = \Gamma_0(N)$ and p a prime. The most important case for the sequel is $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$. An elementary calculation shows*

$$\Gamma^\alpha = \Gamma_0(Np).$$

Definition 7.1.4 *Let $\alpha \in \Delta$. We consider the diagram*

$$\begin{array}{ccc} \Gamma_\alpha\backslash\mathbb{H} & \xrightarrow[\sim]{\tau\mapsto\alpha\tau} & \Gamma^\alpha\backslash\mathbb{H} \\ \downarrow{\scriptstyle \pi_\alpha} & & \downarrow{\scriptstyle \pi^\alpha} \\ \Gamma\backslash\mathbb{H} & & \Gamma\backslash\mathbb{H}, \end{array}$$

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 modular correspondence *or* Hecke correspondence *τ_α is defined as*

$$\tau_\alpha : \mathrm{Div}(Y_\Gamma) \xrightarrow{\pi_\alpha^*} \mathrm{Div}(Y_{\Gamma_\alpha}) \xrightarrow{\alpha_*} \mathrm{Div}(Y_{\Gamma^\alpha}) \xrightarrow{\pi_*^\alpha} \mathrm{Div}(Y_\Gamma).$$

Here, π^* is the pull-back of divisors and π_α^* and π_*^α are the maps which one obtains by applying α and π^α to the points of the divisor.

These modular correspondences will be described more explicitly in a moment. First a lemma:

Lemma 7.1.5 *Let $\alpha_i \in \Gamma$ for $i \in I$ with some index set I. Then we have*

$$\Gamma = \bigsqcup_{i\in I} \Gamma\alpha_i\alpha_i \;\Leftrightarrow\; \Gamma\alpha\Gamma = \bigsqcup_{i\in I} \Gamma\alpha\alpha_i.$$

Proof. Last term's course. A simple calculation. □

Corollary 7.1.6 *Let $\alpha \in \Delta$ and $\Gamma\alpha\Gamma = \bigsqcup_{i\in I} \Gamma\alpha\alpha_i$. Then the Hecke corresondence $\tau_\alpha : \mathrm{Div}(Y_\Gamma) \to \mathrm{Div}(Y_\Gamma)$ is given by $\tau \mapsto \sum_{i\in I} \alpha\alpha_i\tau$ for representatives $\tau \in \mathbb{H}$.*

Proof. It suffices to check the definition using the Lemma. □

Remark 7.1.7 *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 7.1.8 *Let $\Delta^n = \bigsqcup_{i\in I} \Gamma\alpha_i\Gamma$. The Hecke operator T_n on $\mathrm{Div}(Y_\Gamma)$ is defined as*

$$T_n = \sum_{i\in I} \tau_{\alpha_i}.$$

We have already seen in the beginning:

Lemma 7.1.9 *For $(a,N)=1$ there is a matrix $\sigma_a \in \Gamma_0(N)$ with $\sigma_a \equiv \left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right) \mod N$.*

Proof. From $(a,N)=1$ we conclude the existence of r,s with $1 = ar - Ns$. Hence the matrix $\left(\begin{smallmatrix} r & s \\ N & a \end{smallmatrix}\right)$ is in $\Gamma_0(N)$ and further $\left(\begin{smallmatrix} r & s \\ N & a \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} a^{-1} & s \\ 0 & a \end{smallmatrix}\right) \mod N$. Now it suffices to clear the top right corner in order to find the desired matrix. We put $\sigma_a = \left(\begin{smallmatrix} r & s \\ N & a \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -as \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(N)$. A short matrix calculation shows that σ_a satisfies the demands. □

Proposition 7.1.10 *(a) We have the decomposition*

$$\Delta_0^n(N) = \bigsqcup_a \bigsqcup_b \Gamma_0(N) \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right),$$

where a runs through the positive integers with $a \mid n$ and $(a,N)=1$ and b runs through the integers such that $0 \le b < d =: n/a$.

(b) For $(a,N)=1$ we choose a matrix σ_a as in the Lemma. Then we have the decomposition

$$\Delta_1^n(N) = \bigsqcup_a \bigsqcup_b \Gamma_1(N)\sigma_a \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$$

with a,b,d as in (a).

Proof. Last term's lecture. This proof is elementary. □

For completeness we give an interpretation of the Hecke operator T_p in terms of the moduli interpretation of the modular curve $Y_{\Gamma_0(N)}$.

Proposition 7.1.11 *On $Y_{\Gamma_0(N)}$ the Hecke operator T_p for a prime number p is given by*

$$T_p : \tau \mapsto \begin{cases} \sum_{b=0}^{p-1} \frac{\tau+b}{p} + p\tau, & \text{if } p \nmid N, \\ \sum_{b=0}^{p-1} \frac{\tau+b}{p}, & \text{if } p \mid N. \end{cases}$$

Under the identifications

$$\Gamma_0(N)\backslash\mathbb{H} \to \{(E,C)\}/\cong, \quad \tau \mapsto (\mathbb{C}/\Lambda_\tau, \langle \frac{1}{N} \rangle$$

and $\mathrm{Div}(Y_{\Gamma_0(N)}) \cong \mathrm{Div}(\{(E,C)\}/\cong)$ *we have*

$$T_p : (E,C) \mapsto \sum_{(E',C')} (E',C'),$$

where the sum is taken over all p-isogenies $E \to E'$ and C' denotes the image of C.

Proof. The first statement follows from the preceding proposition. For the second one only has to convince oneself what p-isogenies for the elliptic curve $\mathbb{C}/\Lambda_\tau$ look like. The details of this simple calculation were presented in last term's course. □

Next, we turn to the important description of the Hecke algebra as a double coset algebra.

Definition 7.1.12 *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 $\Gamma\alpha\Gamma = \bigsqcup_{i=1}^{n} \Gamma\alpha_i$ und $\Gamma\beta\Gamma = \bigsqcup_{j=1}^{m} \Gamma\beta_j$. 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 disjoing. 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 notation for the multiplicity with which every coset on the right appears in the centre. For fixed k we define for every l

$$m_{k,l} = \#\{(i,j) | \Gamma\gamma_{k,l} = \Gamma\alpha_i\beta_j\}.$$

The important point is the following lemma.

Lemma 7.1.13 *The number* $m_{k,l}$ *is independent of* l*. We put* $m_k := m_{k,l}$.

Proof. See last term's course. The proof is combinatorial and quite straight forward. □

In conclusion, Lemma 7.1.13 tells us that the coset $\Gamma\gamma_{k,l}$ appears precisely m_k times in

$$\bigcup_{i,j} \Gamma\alpha_i\beta_j = \Gamma\alpha\Gamma \cdot \Gamma\beta\Gamma = \bigsqcup_k \Gamma\gamma_k\Gamma = \bigsqcup_k \bigsqcup_l \Gamma\gamma_{k,l}.$$

Definition 7.1.14 *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 notations.

In Exercise 46 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 7.1.15 *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

$$T(a, d) = \Gamma\sigma_a \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \Gamma \in R(\Delta, \Gamma).$$

From Exercise 47, we obtain the the following important corollary.

Corollary 7.1.16 *We have $T_m T_n = T_n T_m$ and hence $R(\Delta, \Gamma)$ is a commutative ring.* □

7.2 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 7.2.1 *Let $\alpha \in \Delta$. Suppose $\Gamma\alpha\Gamma = \bigsqcup_{i=1}^n \Gamma\alpha_i$ and let $f \in M_k(\Gamma)$. We put*

$$f.\tau_\alpha := \sum_{i=1}^n f|_{\alpha_i}.$$

Lemma 7.2.2 *The function $f.\tau_\alpha$ 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 $f.\tau$ 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 7.2.3 *Let $(\Delta, \Gamma) = (\Delta_0(N), \Gamma_0(N))$ and $f \in M_k(\Gamma)$. The following formulae hold:*

(a) $(f.T_m)(\tau) = \frac{1}{m} \sum_{a \mid m, (a,N)=1} \sum_{b=0}^{\frac{m}{a}-1} a^k f(\frac{a\tau+b}{m/a})$,

(b) $a_n(f.T_m) = \sum_{a \mid (m,n), (a,N)=1} a^{k-1} a_{\frac{mn}{a^2}}$.

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 7.1.10.

(b) is a simple calculation using

$$\sum_{b=0}^{d-1} e^{2\pi i \frac{b}{d} n} = \begin{cases} 0, & \text{if } d \nmid n \\ d, & \text{if } d \mid n. \end{cases}$$

For details, see last term's course. □

Remark 7.2.4 *The Hecke ring $R(\Delta,\Gamma)$ also acts on $S_k(\Gamma)$.*

Corollary 7.2.5 *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) $T_nT_m = T_{nm}$ *for* $(n,m)=1$,

(b) $T_{p^{r+1}} = T_pT_{p^r} - p^{k-1}T_{p^{r-1}}$, *if* $p \nmid N$, *and*

(c) $T_{p^{r+1}} = T_pT_{p^r}$, *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 47 and the definition of the action. □

The formulae from the corollary can be expressed very elegantly like this:

Proposition 7.2.6 (Euler product) *The action of the Hecke operators T_n on modular forms satisfies the formal identity:*

$$\sum_{n=1}^{\infty} T_n n^{-s} = \prod_{p\nmid N}(1 - T_pp^{-s} + p^{k-1-2s})^{-1} \cdot \prod_{p|N}(1 - T_pp^{-s})^{-1}.$$

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 $g : \mathbb{Z} \to \mathbb{C}$ be any function. Then we have the formal identity

$$\prod_{p \text{ prime}} \sum_{r=0}^{\infty} g(p^r) = \sum_{n=1}^{\infty} \prod_{p^r \| n} g(p^r).$$

For its proof, let first S be a finite set of prime numbers. Then we have the formal identity:

$$\prod_{p\in S} \sum_{r=0}^{\infty} g(p^r) = \sum_{n=1, n \text{ only has prime factors in } S}^{\infty} \prod_{p^r \| n} g(p^r),$$

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

$$(\sum_{r=0}^{\infty} T_{p^r}p^{-rs})(1 - T_pp^{-s} + p^{k-1-2s}) = 1$$

and for $p \mid N$:

$$(\sum_{r=0}^{\infty} T_{p^r}p^{-rs})(1 - T_pp^{-s}) = 1.$$

The proof of the second step consists of multiplying out these expressions and to identify a "telescope". For details see last term's course.

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. □

7.3 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 $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^\iota = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$.

Recall the definition of the Hecke operator τ_α on $\mathrm{Div}(\Gamma\backslash\mathbb{H})$.

Definition 7.3.1 *Let $\alpha \in \Delta$. The* Hecke operator τ_α *acting on group cohomology is the composite*

$$\mathrm{H}^1(\Gamma, V) \xrightarrow{\mathrm{res}} \mathrm{H}^1(\Gamma^\alpha, V) \xrightarrow{\mathrm{conj}_\alpha} \mathrm{H}^1(\Gamma_\alpha, V) \xrightarrow{\mathrm{cores}} \mathrm{H}^1(\Gamma, V).$$

The first map is the restriction*, and the third one is the* corestriction*. We explicitly describe the second map on cocycles:*

$$\mathrm{conj}_\alpha : \mathrm{H}^1(\Gamma^\alpha, V) \to \mathrm{H}^1(\Gamma_\alpha, V), \quad c \mapsto \big(g_\alpha \mapsto \alpha^\iota . c(\alpha g_\alpha \alpha^{-1})\big).$$

There is a similar description on the parabolic subspace and the two are compatible, see Exercise 48.

Proposition 7.3.2 *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 $\mathrm{H}^1(\Gamma, V)$ and $\mathrm{H}^1_{\mathrm{par}}(\Gamma, V)$ by sending the non-homogeneous cocyle c to $T_\alpha c$ 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 49 the corestriction of a non-homogeneous cocycle $u \in \mathrm{H}^1(\Gamma_\alpha, V)$ is the cocycle $\mathrm{cores}(u)$ uniquely given by

$$\mathrm{cores}(u)(g) = \sum_{i=1}^n g_i^{-1} u(g_i g g_{\sigma_g(i)}^{-1}) \tag{7.3.1}$$

for $g \in \Gamma$. Combining with the explicit description of the map conj_α yields the result. □

Definition 7.3.3 *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 1.1.1 (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 7.3.4 *The Eichler-Shimura isomorphism is compatible with the Hecke operators.*

Proof. We recall the definition of Shimura's main involution: $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^\iota = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$. In other words, for matrices with a non-zero determinant, we have

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^\iota = (\det \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) \cdot \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^{-1}.$$

Let now $f \in \mathrm{M}_k(\Gamma\,;\mathbb{C})$ be a modular form, $\gamma \in \Gamma$ and $z_0 \in \mathbb{H}$. For any matrix g with non-zero determinant, Lemma 6.2.2 yields

$$I_{f|_g}(z_0, \gamma z_0) = g^\iota I_f(gz_0, g\gamma z_0).$$

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 $\mathrm{M}_k(\Gamma\,;\mathbb{C})$ and $\mathrm{H}^1(\Gamma, V_{k-2}(\mathbb{C}))$. The same arguments will also hold for anti-holomorphic cusp forms.

Consider a coset decomposition $\Gamma\alpha\Gamma = \bigsqcup_i \Gamma\delta_i$. We use the notations as in Proposition 7.3.2. We compute:

$$\begin{aligned} I_{\tau_\alpha f}(z_0, \gamma z_0) = I_{\sum_i f|_{\delta_i}}(z_0, \gamma z_0) &= \sum_i I_{f|_{\delta_i}}(z_0, \gamma z_0) = \sum_i \delta_i^\iota I_f(\delta_i z_0, \delta_i \gamma z_0) \\ &= \sum_i \delta_i^\iota \big(I_f(\delta_i z_0, z_0) + I_f(z_0, \delta_i\gamma\delta_{\sigma_\gamma(i)}^{-1} z_0) + I_f(\delta_i\gamma\delta_{\sigma_\gamma(i)}^{-1} z_0, \delta_i\gamma\delta_{\sigma_\gamma(i)}^{-1}\delta_{\sigma_\gamma(i)} z_0)\big) \\ &= \sum_i \delta_i^\iota I_f(z_0, \delta_i\gamma\delta_{\sigma_\gamma(i)}^{-1} z_0) + \sum_i \delta_i^\iota I_f(\delta_i z_0, z_0) - \sum_i \delta_i^\iota\delta_i\gamma\delta_{\sigma_\gamma(i)}^{-1} I_f(\delta_{\sigma_\gamma(i)} z_0, z_0) \\ &= \sum_i \delta_i^\iota I_f(z_0, \delta_i\gamma\delta_{\sigma_\gamma(i)}^{-1} z_0) + (1-\gamma)\sum_i \delta_i^\iota I_f(\delta_i z_0, z_0), \end{aligned}$$

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 7.3.2 is equal to τ_α applied to the cocycle $\gamma \mapsto I_f(z_0, \gamma z_0)$, as required. □

Remark 7.3.5 *The conceptual reason why the above proposition is correct, is, of course, that the Hecke operators come from Hecke correspondences. Formulating the proof using the definition of Hecke operators rather than Proposition 7.3.2 makes it more lengthy, but maybe also less mysterious.*

7.4 Theory: Eichler-Shimura revisited

In this sections 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 7.4.1 (Eichler-Shimura) *Let $N \geq 1$, $k \geq 2$ and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character. Then the Eichler-Shimura map gives isomorphisms*

$$\mathrm{M}_k(N, \chi\,;\, \mathbb{C}) \oplus \overline{\mathrm{S}_k(N, \chi\,;\, \mathbb{C})} \to \mathrm{H}^1(\Gamma_0(N), V_{k-2}^\chi(\mathbb{C})),$$

and

$$\mathrm{S}_k(N, \chi\,;\, \mathbb{C}) \oplus \overline{\mathrm{S}_k(N, \chi\,;\, \mathbb{C})} \to \mathrm{H}^1_{\mathrm{par}}(\Gamma_0(N), V_{k-2}^\chi(\mathbb{C})).$$

Proof. Recall that the σ_a are 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

$$\gamma \mapsto \delta.c(\delta^{-1}\gamma\delta).$$

With $\delta = \sigma_a^{-1} = \sigma_a^\iota$, this reads

$$\gamma \mapsto \sigma_a^\iota.c(\sigma_a^{-1}\gamma\sigma_a) = \sigma_a^\iota c(\sigma_a^{-1}\gamma\sigma_a) = \tau_{\sigma_a} c = \langle a \rangle c.$$

Hence, the Δ-action is through 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

$$\mathrm{H}^1(\Gamma_0(N), V_{k-2}^\chi(\mathbb{C})) \xrightarrow{\mathrm{res}} \mathrm{H}^1(\Gamma_1(N), V_{k-2}^\chi(\mathbb{C}))^\Delta.$$

The Eichler-Shimura theorem we proved further gives us an isomorphism of Hecke modules

$$\mathrm{M}_k(\Gamma_1(N)\,;\, \mathbb{C}) \oplus \overline{\mathrm{S}_k(\Gamma_1(N)\,;\, \mathbb{C})} \to \mathrm{H}^1(\Gamma_1(N), V_{k-2}^\chi(\mathbb{C})),$$

since as a $\Gamma_1(N)$-module $V_{k-2}^\chi(\mathbb{C}) \cong V_{k-2}(\mathbb{C})$. 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. □

Corollary 7.4.2 *Let $\Gamma = \Gamma_1(N)$. The maps*

$$\mathrm{S}_k(\Gamma\,;\, \mathbb{C}) \to \mathrm{H}^1_{\mathrm{par}}(\Gamma, V_{k-2}(\mathbb{R})), \quad f \mapsto (\gamma \mapsto \mathrm{Re}(I_f(z_0, \gamma z_0)))$$

and

$$\mathrm{S}_k(\Gamma\,;\, \mathbb{C}) \to \mathrm{H}^1_{\mathrm{par}}(\Gamma, V_{k-2}(\mathbb{R})), \quad f \mapsto (\gamma \mapsto \mathrm{Im}(I_f(z_0, \gamma z_0)))$$

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

$$\mathrm{S}_k(\Gamma\,;\, \mathbb{C}) \xrightarrow{f \mapsto \frac{1}{2}(f+\overline{f})} \mathrm{S}_k(\Gamma\,;\, \mathbb{C}) \oplus \overline{\mathrm{S}_k(\Gamma\,;\, \mathbb{C})} \xrightarrow{\text{Eichler-Shimura}} \mathrm{H}^1_{\mathrm{par}}(\Gamma, V_{k-2}(\mathbb{C})).$$

It is clearly injective. Note that $I_{\overline{f}}(z_0, \gamma z_0) = \overline{I_f(z_0, \gamma z_0)}$. Hence, the composite map coincides with the first map in the statement. Its image is thus already contained in $\mathrm{H}^1_{\mathrm{par}}(\Gamma, V_{k-2}(\mathbb{R}))$. Since the real

dimensions coincide, the map is an isomorphism. In order to prove the second isomorphism, we use $f \mapsto \frac{1}{2}(f - \overline{f})$ and proceed as before. □

We now treat the $+$ and the $-$-space for the involution attached to the matrix $\eta = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ (see p. 13). The action of η on $\mathrm{H}^1(\Gamma, V)$ 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

$$\tau_\eta : \mathrm{H}^1(\Gamma, V) \to \mathrm{H}^1(\Gamma, V), \quad c \mapsto (\gamma \mapsto \eta^\iota.c(\eta\gamma\eta)),$$

provided, of course, that η^ι acts on V (compatibly with the Γ-action).

We also want to define an involution τ_η on $\mathrm{S}_k(\Gamma\,;\mathbb{C}) \oplus \overline{\mathrm{S}_k(\Gamma\,;\mathbb{C})}$. For that recall that if $f(z) = \sum a_n e^{2\pi i n z}$, then $\tilde{f}(z) := \sum \overline{a_n} e^{2\pi i n z}$ is again a cusp form in $\mathrm{S}_k(\Gamma\,;\mathbb{C})$, 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

$$\tau_\eta : \mathrm{S}_k(\Gamma\,;\mathbb{C}) \xrightarrow{f \mapsto (-1)^{k-1}\tilde{f}} \mathrm{S}_k(\Gamma\,;\mathbb{C}) \xrightarrow{\tilde{f} \mapsto \overline{\tilde{f}}} \overline{\mathrm{S}_k(\Gamma\,;\mathbb{C})}.$$

Similarly, we also define $\tau_\eta : \overline{\mathrm{S}_k(\Gamma\,;\mathbb{C})} \to \mathrm{S}_k(\Gamma\,;\mathbb{C})$ and obtain in consequence an involution τ_η on $\mathrm{S}_k(\Gamma\,;\mathbb{C}) \oplus \overline{\mathrm{S}_k(\Gamma\,;\mathbb{C})}$.

Let us consider the function $(-1)^{k-1}\overline{\tilde{f}(z)}$ as a function of $\overline{z}$:

$$(-1)^{k-1}\overline{\tilde{f}(z)} = (-1)^{k-1}\overline{\sum_n \overline{a_n} e^{2\pi i n z}} = (-1)^{k-1}\sum_n a_n e^{2\pi i n(-\overline{z})} = (-1)^{k-1} f(-\overline{z}) = f|_\eta(\overline{z}).$$

Proposition 7.4.3 *The Eichler-Shimura map commutes with τ_η.*

Proof. Let $f \in \mathrm{S}_k(\Gamma\,;\mathbb{C})$ (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:

$$\begin{aligned} I_{(-1)^{k-1}\overline{\tilde{f}}}(z_0, \gamma z_0) &= (-1)^{k-1}\int_{z_0}^{\gamma z_0} \overline{\tilde{f}(z)}(X\overline{z} + Y)^{k-2} d\overline{z} \\ &= (-1)^{k-1}\int_{z_0}^{\gamma z_0} f(-\overline{z})(X\overline{z} + Y)^{k-2} d\overline{z} \\ &= (-1)^{k-2}\int_{-\overline{z_0}}^{-\gamma\overline{z_0}} f(z)(X(-z) + Y)^{k-2} dz \\ &= \eta^\iota \int_{-\overline{z_0}}^{\eta\gamma\eta(-\overline{z_0})} f(z)(Xz + Y)^{k-2} dz. \end{aligned}$$

If we change the last expression by a suitable coboundary, then it is equal to

$$\eta^\iota \int_{z_0}^{\eta\gamma\eta z_0} f(z)(Xz + Y)^{k-2} dz,$$

which is τ_η of the cocycle attached to f, as required. □

Corollary 7.4.4 *Let $\Gamma = \Gamma_1(N)$. The maps*

$$\mathrm{S}_k(\Gamma\,;\mathbb{C}) \to \mathrm{H}^1_{\mathrm{par}}(\Gamma, V_{k-2}(\mathbb{C}))^+, \quad f \mapsto (1+\tau_\eta).(\gamma \mapsto I_f(z_0, \gamma z_0))$$

and

$$\mathrm{S}_k(\Gamma\,;\mathbb{C}) \to \mathrm{H}^1_{\mathrm{par}}(\Gamma, V_{k-2}(\mathbb{C}))^-, \quad f \mapsto (1-\tau_\eta).(\gamma \mapsto I_f(z_0, \gamma z_0))$$

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. □

Note that if the coefficients of f are real, then $\tilde{f} = f$ and the image of f under the maps from the two preceding corollaries is the same (possibly up to a sign). You are invited to take a look at Exercise 50.

7.5 Theory: Transfer of Hecke operators to Manin symbols

We first prove that the Hecke operators are compatible with Shapiro's lemma. This was first proved by Ash and Stevens. We first need to say what the action of $\alpha \in \Delta$ on the coinduced module $\mathrm{Hom}_{R[\Gamma]}(R[\mathrm{SL}_2(\mathbb{Z})], V)$ 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 $\mathrm{Mat}_2(\mathbb{Z}/N\mathbb{Z})$. The natural map

$$\Gamma\backslash\mathrm{SL}_2(\mathbb{Z}) \to U_N\backslash\,\mathrm{Mat}_2(\mathbb{Z}/N\mathbb{Z})$$

is injective. Its image consists of those $U_N g$ such that

$$(*) \qquad (0,1)g = (u,v) \text{ with } \langle u, v\rangle = \mathbb{Z}/N\mathbb{Z}.$$

If that is so, then we say for short that g is $(*)$. Note that this condition does not depend on the choice of g in $U_N g$. Define the $R[\Delta^\iota]$-module $\mathcal{C}(N,V)$ by

$$\mathcal{C}(N,V) = \{f \in \mathrm{Hom}_R(R[U_N\backslash\,\mathrm{Mat}_2(\mathbb{Z}/N\mathbb{Z})] \mid f(g) = 0 \text{ if } g \text{ is not } (*)\}$$

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 $\mathrm{Hom}_{R[\Gamma]}(R[\mathrm{SL}_2(\mathbb{Z})], V)$ as an $R[\Gamma]$-module by

$$\mathrm{Hom}_{R[\Gamma]}(R[\mathrm{SL}_2(\mathbb{Z})], V) \to \mathcal{C}(N,V), \quad f \mapsto \begin{cases} (g \mapsto gf(g^{-1})) & \text{for any } g \in \mathrm{SL}_2(\mathbb{Z}) \\ 0 & \text{if } g \text{ is not } (*). \end{cases}$$

Note that

Proposition 7.5.1 *The Hecke operators are compatible with Shapiro's Lemma. More precisely, for all $n \in \mathbb{N}$ the following diagram commutes:*

$$\begin{array}{ccc} \mathrm{H}^1(\Gamma, V) & \xrightarrow{T_n} & \mathrm{H}^1(\Gamma, V) \\ \text{Shapiro}\uparrow & & \uparrow\text{Shapiro} \\ \mathrm{H}^1(\mathrm{SL}_2(\mathbb{Z}), \mathcal{C}(N, V)) & \xrightarrow{T_n} & \mathrm{H}^1(\mathrm{SL}_2(\mathbb{Z}), \mathcal{C}(N, V)). \end{array}$$

Proof. Let δ_i, for $i = 1, \ldots, r$ be the representatives of $\mathrm{SL}_2(\mathbb{Z})\backslash\Delta(1)^n$ provided by Proposition 7.1.10. Say, that they are ordered such that δ_i for $i = 1, \ldots, s$ with $s \leq r$ are representatives for $\Gamma\backslash\Delta$. This explicitly means that the lower row of δ_i^ι is $(0, a)$ with $(a, N) = 1$ (or even $(0, 1)$ if we are in the $\Gamma_1(N)$-situation) for $i = 1, \ldots, s$. If $s < i \leq r$, then the lower row is (u, v) with $\langle u, v\rangle \lneq \mathbb{Z}/N\mathbb{Z}$.

Let $c \in \mathrm{H}^1(\mathrm{SL}_2(\mathbb{Z}), \mathcal{C}(N, V))$ be a 1-cochain. Then

$$\begin{aligned} \text{Shapiro}(T_n(c))(\gamma) &= \sum_{i=1}^{r} (\delta_i^\iota . c(\delta^i \gamma \delta_{\sigma_\gamma(i)}^{-1}))(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)) = \sum_{i=1}^{r} \delta_i^\iota (c(\delta^i \gamma \delta_{\sigma_\gamma(i)}^{-1})(\delta_i^\iota)) \\ &= \sum_{i=1}^{s} \delta_i^\iota (c(\delta^i \gamma \delta_{\sigma_\gamma(i)}^{-1})(\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right))) = T_n(\text{Shapiro}(c))(\gamma), \end{aligned}$$

as required. □

Remark 7.5.2 *A very similar description exists involving* $\mathrm{PSL}_2(\mathbb{Z})$.

[For the rest of this section only hand-written notes exist presently. They will be typed once the author is more satisfied with the presentation than he currently is.]

7.6 Theoretical exercises

Exercise 46 *Check that that $R(\Delta, \Gamma)$ is a ring (associativity and distributivity).*

Exercise 47 *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 48 *Check that the Hecke operator τ_α from Definition 7.3.1 restricts to $\mathrm{H}^1_{\mathrm{par}}(\Gamma, V)$.*

Exercise 49 *Prove Equation 7.3.1.*

Exercise 50 *Does the Eichler-Shimura map send the subspace of Eisenstein series to the $+$-space $\mathrm{H}^1(\Gamma, V_{k-2}(\mathbb{C}))^+$, to the $-$-space or to none of them (in general)?*

7.7 Computer exercises

Computer exercise 19 *Implement Hecke operators.*

Part II

Computational Galois Representations

Stage 8

Images of Galois Representations

As time is running short, we shall only treat images of Galois representations without actually speaking about Galois representations. This will be done in next term's lecture in detail.

The main theorem in this context is due to Deligne and Shimura.

Theorem 8.0.1 (Shimura, Deligne) *Let $f \in \mathrm{S}_k(N, \chi\,; \mathbb{C})$ be a normalised Hecke eigenform. Denote by $\mathbb{Q}_f$ the coefficient field of $\mathbb{Q}$, i.e. $\mathbb{Q}(a_n | (n, N) = 1)$, where the a_n are the coefficients of f in the q-expansion at infinity.*

For any prime ideal $\mathfrak{P}$ of (the ring of integers of) $\mathbb{Q}_f$, there exists a Galois number field K with Galois group $\mathrm{Gal}(K/\mathbb{Q}) =: G$ such that

- *K is unramified outside Np, where p is the residue characteristic of $\mathfrak{P}$;*
- *there is a group injection $G := \mathrm{Gal}(K/\mathbb{Q}) \overset{\rho}{\hookrightarrow} \mathrm{GL}_2(\mathbb{F}_q)$, where q is the cardinality of the residue field of $\mathfrak{P}$;*
- *for all maximal ideals Λ of (the ring of integers of) $\mathbb{Q}_f$ coprime to pN we have*

$$\mathrm{charpoly}(\rho(\mathrm{Frob}_\Lambda)) = X^2 - \overline{a_p} X + l^{k-1}\overline{\chi(l)},$$

  where l is the residue characteristic of Λ and $\bar{\cdot}$ denotes the reduction modulo $\mathfrak{P}$;

- *K is totally imaginary if $p \neq 2$.*

We quickly explain the notion of Frobenius elements: Frob_Λ. The decomposition group D_Λ is a subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ and, since Λ is unramified, reduction modulo Λ gives an isomorphism between D_Λ and $\mathrm{Gal}((\mathcal{O}_{\mathbb{Q}_f}/\Lambda)/\mathbb{F}_l)$. The latter Galois group is cyclic and generated by the Frobenius automorphism $x \mapsto x^l$. By Frob_Λ we denote the unique element of $\mathrm{Gal}(K/\mathbb{Q})$ lying in D_Λ whose reduction modulo Λ gives the Frobenius automorphism of the finite field.

One often writes Frob_l instead of Frob_Λ. If one does this, one has to keep in mind that the actual element Frob_Λ depends on the choice of a prime Λ above l. Another choice, say Λ' would give $\mathrm{Frob}_{\Lambda'}$

and Frob_Λ and $\mathrm{Frob}_{\Lambda'}$ are conjugate by some element in $\mathrm{Gal}(K/\mathbb{Q})$ (namely the $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\Lambda' = \sigma\Lambda$).

The above theorem, however, only makes statements about characteristic polynomials of images of Frobenius elements. Characteristic polynomials only depend on the conjugacy class. Thus, for the above purpose, it is enough to write Frob_l.

In the lecture so far we have explained how one computes coefficients of modular forms, i.e. the a_n. Now we ask the question what we can determine about the number field K from Deligne's and Shimura's theorem. In this final lecture we shall show that we can determine (in most cases) the group G. Calculating a polynomial whose splitting field is K is much much more difficult; but the question has been solved in principle by Edixhoven et al. last year. We will not be able to treat the answer here.

The determination of the group G is very much simplified by the fact that the subgroup structure of $\mathrm{GL}_2(\mathbb{F}_q)$ is very simple. This is a fact that goes back into the 19th century (see also the introduction).

Theorem 8.0.2 (Dickson) *Let p be a prime and H a subgroup of $\mathrm{PGL}_2(\mathbb{F}_q)$. Then a conjugate of H is isomorphic to one of the following groups:*

- *finite subgroups of the upper triangular matrices (order dividing $q(q-1)$)*
- $\mathrm{PSL}_2(\mathbb{F}_{p^r})$ *or* $\mathrm{PGL}_2(\mathbb{F}_{p^r})$ *with* $\mathbb{F}_{p^r} \subseteq \mathbb{F}_q$,
- *dihedral groups D_r of order $2r$ with $r \mid q-1$ or $r \mid q+1$,*
- *cyclic groups D_r of order $2r$ with $r \mid q-1$ or $r \mid q+1$,*
- A_4, A_5 *or* S_4.

Corollary 8.0.3 *Let $H \subseteq \mathrm{GL}_2(\mathbb{F}_q)$ be a subgroup containing x, y, z such that*

- $\mathrm{ord}(x) \neq 2 \neq \mathrm{ord}(y)$ *and* $\mathrm{ord}(z) > 5$
- $\mathrm{charpoly}(x) = (X-a)(X-b)$ *with* $a, b \in \mathbb{F}_q[X]$ *and* $a \neq b$,
- $\mathrm{charpoly}(y)$ *is irreducible over* $\mathbb{F}_q$,
- $\mathrm{charpoly}(z) \neq (X-c)^2$ *for any* $c \in \overline{\mathbb{F}}_p$.

Then H modulo scalars is $\mathrm{PSL}_2(\mathbb{F}_{p^r})$ *or* $\mathrm{PGL}_2(\mathbb{F}_{p^r})$ *for some* $\mathbb{F}_{p^r} \hookrightarrow \mathbb{F}_q$.

If furthermore s is the minimum such that $\mathbb{F}_{p^s}$ contains a and b and $\mathbb{F}_{p^{2s}}$ contains the roots of $\mathrm{charpoly}(y)$, *then $s \mid r$.*

Proof. The order of x divides $q-1$ and the order of y divides $q+1$. Since the greatest common divisor of $q-1$ and $q+1$ is 2, the dihedral, cyclic and upper triangular groups appearing in Dickson's theorem are excluded. The presence of a non-scalar element of order bigger than 5 excludes A_4, S_4 and A_5. □

Proposition 8.0.4 *The set of subgroups* $\{H \subseteq \mathrm{GL}_2(\mathbb{F}_q) | \mathrm{SL}_2(\mathbb{F}_q) \subseteq H\}$ *is in bijection with the set of subgroups* $\{R \subseteq \mathbb{F}_q^\times\}$.

The bijection associates with an H *the group* $R := \{\det(h) | h \in H\}$ *and with an* R *the group* $H := \{g \in \mathrm{GL}_2(\mathbb{F}_q) | \det(g) \in R\}$.

Proof. Just notice that the determinant gives a group isomorphism $\mathrm{GL}_2(\mathbb{F}_q)/\mathrm{SL}_2(\mathbb{F}_q) \to \mathbb{F}_q^\times$. The statement is then a well-known result from algebra. □

Proposition 8.0.5 *Assume the situation of Deligne's theorem and suppose that* $\mathrm{SL}_2(\mathbb{F}_q) \subseteq G$. *Then*

$$\{\det(g) | g \in G\} = \langle W, \mathbb{F}_l^{\times(k-1)} \rangle \subseteq \mathbb{F}_q^\times,$$

where $W = \{\overline{\chi(n)} | (n, N) = 1\} \subseteq \mathbb{F}_q^\times$.

Proof. The number field cut out by χ, i.e. the number field L such that $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ is the kernel of $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^\times$, is unramified at l. Hence, its intersection with the at l totally ramified field $\mathbb{Q}(\zeta_l)$ is $\mathbb{Q}$. Hence, the Galois group $\mathrm{Gal}(M/\mathbb{Q})$ of the composite $M = L\mathbb{Q}(\zeta_l)$ is the direct product of $\mathrm{Gal}(L/\mathbb{Q}) \cong W$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_l)/\mathbb{Q} \cong \mathbb{F}_l^\times$. The isomorphisms are given by $\mathrm{Frob}_r \mapsto \overline{\chi(r)}$ and $\mathrm{Frob}_r \mapsto r \mod l$. Chebotarev's density theorem hence tells us that for a given $w \in W$ and a given residue class $a \mod l$ there exist infinitely many primes r such that $\chi(r) = w$ and $r \equiv a \mod l$. Consequently, every element of the form wa^{k-1} lies in the left hand side group. The other inclusion is trivial. □

Now we dispose of the necessary tools for writing down an algorithm that determines the Galois group of the extension $K/\mathbb{Q}$ from Deligne's and Shimura's theorem. More precisely, the algorithm will return a minimal s as in Corollary 8.0.3, or it will return the answer that the algorithm was not conclusive. If $\mathbb{F}_{p^s} = \mathbb{F}_q$, then by Propositions 8.0.4 and 8.0.5 the Galois group can be determined precisely.

Algorithm 8.0.6 Input: A field $\mathbb{F}$ and a list `CharPolyList` of $< a, b >$, where a is the trace and b is the determinant of a 2×2-matrix over $\mathbb{F}$, where $\mathbb{F}$ is some extension of $\mathbb{F}_l$.

Output: A boolean value `conclusive` and an integer `s`. If `conclusive` is false, the algorithm was not conclusive. If `conclusive` is true, then any matrix algebra containing matrices with trace and determinant given in the input contains the group $\mathrm{SL}_2(\mathbb{F}_l^s)$.

(1) `divplus := false; divmin := false; bigorder := false; s := 1;`

(2) `for t in CharPolyList do`

(3) $f := X^2 - t[1]X + t[2] \in \mathbb{F}[X]$ *[This is the characteristic polynomial of any matrix with the given trace and determinant.]*

(4) Factor f over $\mathbb{F}[X]$.

(5) `if` $f \neq (X - c)^2$`, then` *[This excludes that the matrix is scalar.]*

(6) `if` $((x^5-1 \mod f) \neq 0)$ and $((x^4-1 \mod f) \neq 0)$ and $((x^3-1 \mod f) \neq 0)$ `then`

(7) `bigorder := true;`

(8) `end if;` *[If the condition is true, then the order of any matrix with the given polynomial is bigger than* 5*.]*

(9) `if` f is irreducible over $\mathbb{F}[X]$, `then`

(10) Factor f over the quadratic extension of $\mathbb{F}$.

(11) Let a be $1/2$ times the degree of the first zero of f in the quadratic extension of $\mathbb{F}$.

(12) Let s be the lowest common multiple of a and s.

(13) `divplus := true;` *[the charpoly is irreducible over* $\mathbb{F}$*, hence, the order divides* $q+1$ *with* $q = |\mathbb{F}|$*.]*

(14) `else`

(15) Let a be the degree of the first zero of f in $\mathbb{F}$.

(16) Let b be the degree of the second zero of f in $\mathbb{F}$.

(17) Let s be the lowest common multiple of a, b and s.

(18) `divmin := true;` *[the charpoly is reducible over* $\mathbb{F}$*, hence, the order divides* $q-1$*.]*

(19) `end if;`

(20) `end if;`

(21) `end for;`

(22) `return divplus and divmin and bigorder, s;`

Bibliography

[AshStevens] 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.

[Bieri] R. Bieri. *Homological dimension of discrete groups.* Queen Mary College Mathematics Notes, London, 1976.

[Brown] K. S. Brown. *Cohomology of groups*, Springer, New York, 1982.

[Cremona] J. E. Cremona. *Algorithms for modular elliptic curves.* Second edition. Cambridge University Press, Cambridge, 1997.

[Diamond-Im] 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.

[DS] Diamond, Fred; Shurman, Jerry: *A first course in modular forms.* Graduate Text in Mathematics, 228. Springer-Verlag, 2005.

[Eisenbud] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics, **150**, Springer-Verlag, New York, 1995.

[MerelUniversal] 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.

[M] Milne, James: *Modular functions and modular forms.* http://www.jmilne.org/math/index.html

[Serre] J.-P. Serre. *Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*. Duke Mathematical Journal **54**, No. 1 (1987), 179–230.

[Weibel] C. A. Weibel. *An introduction to homological algebra*, Cambridge Univ. Press, Cambridge, 1994.

[Shimura] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Forms*. Princeton University Press, 1994.

[Stein] Stein, W. A. *Modular Forms. A Computational Approach.* AMS, 2007.

[MF] Wiese, G. *Vorlesung über Modulformen.* Lecture notes, Universität Duisburg-Essen, Sommersemester 2007, http://maths.pratum.net

[MSRI] Wiese, G. *Mod p Modular Forms.* Lecture notes from the MSRI Summer Graduate Workshop "Computing With Modular Forms", http://maths.pratum.net