

Computational Arithmetic of Modular Forms

(Modulformen II)

Wintersemester 2007/2008

Universität Duisburg-Essen

Gabor Wiese

`gabor.wiese@uni-due.de`

Version of 13th October 2007

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

1	Motivation and Survey	5
1.1	Theory: Brief review of modular forms and Hecke operators	5
1.2	Theory: The modular symbols formalism	10
1.3	Theory: The modular symbols algorithm	14
1.4	Theory: Number theoretic applications	16
1.5	Theory: Exercises	19
1.6	Algorithms and Implementations: MAGMA and SAGE	21
1.7	Algorithms and Implementations: Modular symbols in MAGMA	21
1.8	Computer exercises	21
1.9	Self-learn module:	23

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 $SL_2(\mathbb{Z})$. By N we shall always denote a positive integer.

Consider the group homomorphism

$$SL_2(\mathbb{Z}) \rightarrow SL_2(\mathbb{Z}/N\mathbb{Z}).$$

By Exercise 1 it is surjective. Its kernel is called $\Gamma(N)$. The group $SL_2(\mathbb{Z}/N\mathbb{Z})$ acts naturally on $(\mathbb{Z}/N\mathbb{Z})^2$ (by multiplying the matrix with a vector). In particular, the homomorphism $SL_2(\mathbb{Z}/N\mathbb{Z}) \rightarrow (\mathbb{Z}/N\mathbb{Z})^2$ given by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix}$ takes all $\begin{pmatrix} a \\ c \end{pmatrix} \in (\mathbb{Z}/N\mathbb{Z})^2$ 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 . The kernel is the stabiliser of $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. 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 $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

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

It is clear that

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

is a group isomorphism. We also let

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

denote a character, i.e. a group homomorphism. We shall extend χ to a map $(\mathbb{Z}/N\mathbb{Z}) \rightarrow \mathbb{C}$ 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 $\{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$. The set of cusps is by definition $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$.

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

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

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

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

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

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

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

- (i) the function $(f|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix})(z) = f(\frac{az+b}{cz+d})(cz+d)^{-k}$ is a holomorphic function (still from \mathbb{H} to \mathbb{C}) for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ (this condition is called *f is holomorphic at the cusp a/c*), and
- (ii) $(f|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix})(z) = f(\frac{az+b}{cz+d})(cz+d)^{-k} = f(z)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$.

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

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

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

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

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

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

All these are finite dimensional \mathbb{C} -vector 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

$$\sigma_a \equiv \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \pmod{N}. \quad (1.1.1)$$

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

Let l be a prime. We let

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

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

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

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

Lemma 1.1.1 *Suppose $f \in M_k(N, \chi; \mathbb{C})$. 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):

- $T_{lr+1} = T_l \circ T_{lr} - l^{k-1} \langle l \rangle T_{lr-1}$ 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 section.

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

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

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

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

respectively.

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

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

(compare with Equation 1.1.4).

Lemma 1.1.2 *The complex q -pairing is perfect, as is the analogous pairing for $S_k(N, \chi; \mathbb{C})$. In particular,*

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

and similarly for $S_k(N, \chi; \mathbb{C})$. For $M_k(N, \chi; \mathbb{C})$, 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 $M_k(N, \chi; \mathbb{C})$ (resp. the cusp forms), we find $T = 0$, proving the non-degeneracy. \square

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

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

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

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

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

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

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

Proof. Exercise 6. \square

1.2 Theory: The modular symbols formalism

In this section we give a definition of formal modular symbols, as implemented in MAGMA and like the one in [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*

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

The Γ -coinvariants of V are by definition

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

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*

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

and

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

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

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

for the left diagonal Γ -action.

(a) We call the Γ -coinvariants

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

the space of (Γ, V) -modular symbols.

(b) We call the Γ -boundary symbols

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

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

(c) We define the boundary map as the map

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

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

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

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

The reader is now invited to prove that the definition of $\mathcal{M}_R(\Gamma, V)$ behaves well with respect to base change (Exercise 9).

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

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

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

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

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

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

Here, ι denotes Shimura's main involution whose definition can be read off from the line above (note that M^ι is the inverse of M if M has determinant 1). Fortunately, both actions are isomorphic due to the fact that the transpose of $\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right)^\iota \begin{pmatrix} X \\ Y \end{pmatrix}$ is equal to $(X, Y) \sigma^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \sigma$ (the isomorphism is given by $v \mapsto \sigma v$).

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

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

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

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

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 $(f \otimes r) \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (f|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix}) \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix} r$ makes $M_k(\Gamma_1(N); \mathbb{C})$ into a right $\Gamma_0(N)$ -module and we have the description (Exercise 11)

$$M_k(N, \chi; \mathbb{C}) = (M_k(\Gamma_1(N); \mathbb{C}))^{(\mathbb{Z}/N\mathbb{Z})^\times} \quad (1.2.6)$$

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

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 $\text{SL}_2(\mathbb{Z})$ -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 $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow R^\times$, which we also sometimes view as a group homomorphism $\Gamma_0(N) \rightarrow R^\times$ as above. We impose that $\chi(-1) = (-1)^k$.

We define

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

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

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

and

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

Let $\eta := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Because of

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

we have

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

We can use the matrix η to define an involution (also denoted by η) on the various modular symbols spaces. We just use the diagonal action on $\mathcal{M}_R(V) := \mathcal{M}_R \otimes_R V$, provided, of course, that η acts on V . On $V_{k-2}(R)$ we use the usual $\text{Mat}_2(\mathbb{Z})_{\neq 0}$ -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.

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). To be precise, we make that statement for the action discussed by Stein and Merel (see the section on $V_n(R)$). 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 $x \in \mathcal{M}_k(N, \chi; R)$. 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

$$\langle a \rangle x = \sigma_a x = \chi(a)x$$

with σ_a as in Equation 1.1.1.

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

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

Proposition 1.2.3 *Let R be \mathbb{Z} or a subfield of \mathbb{C} . Then we have*

$$\mathbb{T}_R(\mathcal{M}_k(\Gamma_1(n); R)) \otimes_R \mathbb{C} \cong \mathbb{T}_{\mathbb{C}}(\mathcal{M}_k(\Gamma_1(n); \mathbb{C}))$$

and similarly for the cuspidal subspace and the $+$ and $-$ -spaces. Moreover,

$$\mathrm{Hom}_R(\mathbb{T}_R(\mathcal{M}_k(\Gamma_1(n); R)), \mathbb{C}) \cong \mathrm{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}(\mathcal{M}_k(\Gamma_1(n); R)), \mathbb{C}).$$

For a character $\chi : \mathbb{Z}/N\mathbb{Z} \rightarrow R^\times$, similar results hold.

Proof. Exercise 12. □

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*

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

$$(b) \ S_k(N, \chi; \mathbb{C}) \oplus S_k(N, \chi; \mathbb{C})^\vee \cong \mathcal{C}\mathcal{M}_k(N, \chi; \mathbb{C}),$$

$$(c) \ S_k(N, \chi; \mathbb{C}) \cong \mathcal{C}\mathcal{M}_k(N, \chi; \mathbb{C})^+.$$

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. □

We may rephrase the Eichler-Shimura theorem as follows.

Corollary 1.3.2 *Let K be a subfield of \mathbb{C} and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow K^\times$ a character. Then*

$$(a) \ M_k(N, \chi; \mathbb{C}) \cong \mathrm{Hom}_K(\mathbb{T}_K(\mathcal{M}_k(N, \chi; K)), \mathbb{C}),$$

$$(b) \ S_k(N, \chi; \mathbb{C}) \cong \mathrm{Hom}_K(\mathbb{T}_K(\mathcal{C}\mathcal{M}_k(N, \chi; K)), \mathbb{C}) \text{ and}$$

$$(c) \ S_k(N, \chi; \mathbb{C}) \cong \mathrm{Hom}_K(\mathbb{T}_K(\mathcal{C}\mathcal{M}_k(N, \chi; K)^+), \mathbb{C}).$$

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

Proof. We only prove (a), as the others are very similar. Theorem 1.3.1 first of all tells us that the \mathbb{C} -algebra generated by the Hecke operators inside the endomorphism ring of $M_k(N, \chi; \mathbb{C})$ equals the \mathbb{C} -algebra generated by the Hecke operators inside the endomorphism ring of $\mathcal{M}_k(N, \chi; \mathbb{C})$. i.e.

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

To see this, one just need to see that the algebra generated on $M_k(N, \chi; \mathbb{C}) \oplus S_k(N, \chi; \mathbb{C})^{\vee}$ is the same as the one generated on $M_k(N, \chi; \mathbb{C})$, 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.

The claim now follows from Proposition 1.2.3 and Lemma 1.1.2. \square

Sketch of the modular symbols algorithm

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

Algorithm 1.3.3 Input: A field $K \subset \mathbb{C}$, integers $N \geq 1$, $k \geq 2$, P , a character $\chi : (\mathbb{Z}/N\mathbb{Z})^{\times} \rightarrow K^{\times}$.

Output: A basis of the space of cusp forms $S_k(N, \chi; \mathbb{C})$; each form is given by its standard q -expansion with precision P .

- (1) Create $M := \mathcal{C}\mathcal{M}_k(N, \chi; K)$.
- (2) $L \leftarrow []$ (empty list), $n \leftarrow 1$.
- (3) repeat
- (4) Compute T_n on M .
- (5) Join T_n to the list L .
- (6) $\mathbb{T} \leftarrow$ the K -algebra generated by all $T \in L$.
- (7) $n \leftarrow n + 1$
- (8) until $\dim_K(\mathbb{T}) = \dim_{\mathbb{C}} S_k(N, \chi; \mathbb{C})$
- (9) Compute a K -basis B of \mathbb{T} .
- (10) Compute the basis B^{\vee} of \mathbb{T}^{\vee} dual to B .
- (11) for ϕ in B^{\vee} do
- (12) Output $\sum_{n=1}^P \phi(T_n)q^n \in K[q]$.
- (13) end for.

We should make a couple of remarks concerning this algorithm. Please remember that there are dimension formulae for $S_k(N, \chi; \mathbb{C})$. 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 1.3.2. 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 1.3.4 (Sturm) *Let $f \in M_k(N, \chi; \mathbb{C})$ such that $a_n(f) = 0$ for all $n \leq \frac{k\mu}{12}$, where $\mu = N \prod_{l|N} (1 + \frac{1}{l})$.*

Then $f = 0$.

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

Corollary 1.3.5 *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 $T_1, T_2, \dots, T_{\frac{k\mu}{12}}$.*

Proof. Exercise 13. □

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

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

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

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

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

such that

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

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

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

By choosing a lattice in $\text{GL}_2(\overline{\mathbb{Q}}_p)$ containing $\rho(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, 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 $\overline{\chi} : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \overline{\mathbb{F}}_p^\times$ a character.*

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

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

such that

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

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

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

Proof. Exercise 14. □

To appreciate the information obtained from the $a_l(f) \pmod{\mathfrak{P}}$, the reader is invited to do Exercise 15 now.

Images of Galois representations

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

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

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

For modular forms there are several results mostly by Ribet concerning the groups that occur as images. 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 $\text{PSL}_2(\mathbb{F}_{p^r})$ or $\text{PGL}_2(\mathbb{F}_{p^r})$, where \mathbb{F}_{p^r} is the extension of \mathbb{F}_p generated by the $a_n(f) \pmod{\mathfrak{P}}$. More precise results will be given later.

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

Serre's 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 $\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\overline{\mathbb{F}}_p)$ be a continuous, odd, irreducible representation.

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

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

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

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

such that ρ is isomorphic to the Galois representation

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

attached to f by Theorem 1.4.2.

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 $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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 $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

1.5 Theory: Exercises

Exercise 1 *The group homomorphism*

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

given by reducing the matrices modulo N is surjective.

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

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

(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. $V_1 = \{v | T_1v = \lambda_1v\}$. Prove that $T_2V_1 \subseteq V_1$.*

(b) Suppose that $M_N(\Gamma_1(k); \mathbb{C})$ 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 $SL_2(\mathbb{Z})$ by $PSL_2(\mathbb{Z})$ 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

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

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

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

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

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

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

Exercise 9 Let R, Γ and V as in Definition 1.2.2 and let $R \rightarrow S$ be a ring homomorphism.

(a) Prove that

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

(b) Is a similar statement true for the cuspidal, the boundary or the Eisenstein space?

Exercise 10 Prove that the map

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

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

Exercise 11 Prove Equation 1.2.6.

Exercise 12 Prove Proposition 1.2.3. In which generality does the proposition hold? Can we replace R by any subring of \mathbb{C} ?

Exercise 13 Prove Corollary 1.3.5.

Exercise 14 Prove Proposition 1.4.3.

Exercise 15 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 . Output: A list $[n_1, n_2, n_3, \dots, n_m]$ such that n_i is the number of primes between 1 and $i \cdot s$ and m is the largest integer smaller than or equal to x/s .

- (c) Compare the output of `TotalNumberOfPrimes` with the predictions of the prime number theorem: Make a function that returns the list $[r_1, r_2, \dots, r_m]$ with $r_i = \frac{s_i}{\log s_i}$. 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:

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

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

Contemplate how the monks can achieve their goal. Write a procedure `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 1.3.3.

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.

Bibliography

- [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 $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* . 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>