Mod p Modular Forms

Gabor Wiese

7th August 2006

Abstract

These are notes and background information for my lectures at the MSRI Summer Graduate Workshop in Computational Number Theory, 31st July to 11th August 2006.

The lectures will, of course, only cover part of what is presented here, but may also contain additional material. The presentation in the workshop will not follow the notes chronologically.

Contents

1 Modular Forms and Hecke Algebras mod p

In this first section we will first recall some facts on congruence subgroups and holomorphic modular forms. We will then define the concept of Hecke algebras which on which we will base our treatment of mod p modular forms. Commutative algebra properties of Hecke algebras will also be studied in some detail, which will enable us to prove some theorems which are useful for computations later on. This section also contains a short discussion of modular curves, as well as a definition of Katz modular forms with a particular emphasis on the weight one case. As our principal motivation for the study of mod p modular forms, we shall present their important role in the theory of Galois representations. In that context, we shall mention Serre's conjecture.

1.1 Holomorphic 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.

1.1.1 Exercise. *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.

The kernel of $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ 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 homomorphism $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \to (\mathbb{Z}/N\mathbb{Z})^2$ 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. The kernel is 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, which may seem unimportant at this point, are at the base of defining level structures for elliptic curves (see the section on modular curves).

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 $(r, N) \neq 1$. The simplest instance of class field theory (here a simple exercise; by ζ_N we mean any primitive N-th root of unity) tells us that

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

(for all primes $l \nmid N$) is an isomorphism. We shall 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 $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$. 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)

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

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

(i) the function $f(\frac{az+b}{cz+d})(cz+d)^{-k}$ 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) $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ 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 $f(\frac{az+b}{cz+d})(cz+d)^{-k}$ 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 *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)' $f(\frac{az+b}{cz+d}) = \chi(d)(cz+d)^k f(z)$ 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 [SteinBook]. 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. We should really define them conceptually (see the section on Hecke correspondences). Here is a definition by formulae.

For $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ an integer matrix with non-zero determinant, we put

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

for a modular form $f \in \mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})$ or $f \in \mathrm{M}_k(N, \chi\,;\,\mathbb{C})$.

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

$$\sigma_a \equiv \left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right) \mod N. \tag{1.1}$$

1.1.2 Exercise. *Prove that such a matrix σ_a exists.*

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

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

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

$$\mathcal{R}_l := \{\left(\begin{smallmatrix}1 & r\\ 0 & l\end{smallmatrix}\right) | 0 \le r \le l-1\} \cup \{\sigma_l \left(\begin{smallmatrix}l & 0\\ 0 & 1\end{smallmatrix}\right)\}, \qquad \text{if } l \nmid N \tag{1.2}$$

$$\mathcal{R}_l := \{\left(\begin{smallmatrix}1 & r\\ 0 & l\end{smallmatrix}\right) | 0 \le r \le l-1\}, \qquad \text{if } l \mid N \tag{1.3}$$

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

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

1.1.3 Exercise. *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. Prove 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.

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 $r \ge 1$,
- $T_{uv} = T_u \circ T_v$ for coprime positive integers u, v.

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

$$a_1(T_n f) = a_n(f). \tag{1.4}$$

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. Hence, 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 $l \equiv d \mod N$)

$$l^{k-1}\langle d\rangle = T_l^2 - T_{l^2}. \tag{1.5}$$

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

1.2 Hecke algebra of holomorphic modular forms and modular forms mod p

In this section we shall define the concept of Hecke algebras. It will be of utmost importance to our treatment of mod p modular forms and their computation (in fact, we will compute the Hecke algebra and not the modular forms). We shall assume that $k \geq 1$ and $N \geq 1$.

We define the *Hecke algebra* of $\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})$ as the subring 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 $\mathrm{S}_k(N,\chi\,;\,\mathbb{C})$. In the latter two cases, we can alternatively take the $\mathcal{O}$-subalgebra in the respective complex endomorphism ring which is generated by the Hecke operators. Here $\mathcal{O}$ denotes the ring $\mathbb{Z}[\chi]$ (i.e. $\mathbb{Z}$ and all values of χ adjoint (they are roots of unity); it is the maximal order (i.e. the ring of integers) of $\mathbb{Q}(\chi)$ ($\mathbb{Q}$ adjoined all values of χ)). It is this description that we shall use in the sequel. Note that the Hecke algebras are free $\mathbb{Z}$-modules (respectively, also free $\mathcal{O}$-modules), since they are defined as submodules of a complex vector space.

Let us introduce the notations $\mathbb{T}_{\mathbb{Z}}(\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C}))$ respectively $\mathbb{T}_{\mathbb{Z}}(\mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{C}))$, as well as $\mathbb{T}_{\mathcal{O}}(\mathrm{M}_k(N,\chi\,;\,\mathbb{C}))$ respectively $\mathbb{T}_{\mathcal{O}}(\mathrm{S}_k(N,\chi\,;\,\mathbb{C}))$. If $\mathcal{O} \to R$ is an $\mathcal{O}$-algebra, we write

$$\mathbb{T}_R(\cdot) := \mathbb{T}_{\mathcal{O}}(\cdot) \otimes_{\mathcal{O}} R.$$

The q-pairing

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 1.4).

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

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

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

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 1.4 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 $k \geq 1$, 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*.

Modular forms over rings and mod p

We now use the q-pairing to define modular (cusp) forms over any $\mathcal{O}$-algebra $\pi : \mathcal{O} \to R$ as follows. We let

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

Every element f of $\mathrm{M}_k(N, \chi\,;\, R)$ thus corresponds to a linear function $\Phi : \mathbb{T}_{\mathcal{O}}(\mathrm{M}_k(N, \chi\,;\, \mathbb{C})) \to R$ and is uniquely identified by its *formal q-expansion* $f = \sum_n \Phi(T_n)q^n = \sum_n a_n(f)q^n$. We note that $\mathbb{T}_{\mathcal{O}}(\mathrm{M}_k(N, \chi\,;\, \mathbb{C}))$ acts naturally on $\mathrm{Hom}_{\mathcal{O}}(\mathbb{T}_{\mathcal{O}}(\mathrm{M}_k(N, \chi\,;\, \mathbb{C})), R)$, namely by $(T.\Phi)(S) = \Phi(TS) = \Phi(ST)$. This means that the action of $\mathbb{T}_{\mathcal{O}}(\mathrm{M}_k(N, \chi\,;\, \mathbb{C}))$ on $\mathrm{M}_k(N, \chi\,;\, R)$ gives the same formulae as above on formal q-expansions. We make a similar definition for the cusp space, namely

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

It is well known (see e.g. [SteinBook]) that the space of holomorphic modular forms (for given $k \geq 1$, $N \geq 1$ and character χ) is the orthogonal direct sum with respect to the Petersson inner product of the cuspidal modular forms and the *space of Eisenstein series*:

$$\mathrm{M}_k(N, \chi\,;\, \mathbb{C}) = \mathrm{Eis}_k(N, \chi\,;\, \mathbb{C}) \oplus \mathrm{S}_k(N, \chi\,;\, \mathbb{C}).$$

The Hecke operators respect this decomposition. As before, we let

$$\mathrm{Eis}_k(N, \chi\,;\, R) \cong \mathrm{Hom}_{\mathcal{O}}(\mathbb{T}_{\mathcal{O}}(\mathrm{Eis}_k(N, \chi\,;\, \mathbb{C})), R) \cong \mathrm{Hom}_R(\mathbb{T}_R(\mathrm{Eis}_k(N, \chi\,;\, \mathbb{C})), R).$$

Let us notice that the two definitions of $\mathrm{M}_k(N, \chi\,;\, \mathbb{C})$ agree. As a special case, we get that $\mathrm{M}_k(N, \chi\,;\, \mathcal{O})$ precisely consists of those holomorphic forms whose q-expansions take values in $\mathcal{O}$. If $R = \mathbb{F}$ is 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 and the Eisenstein spaces similar statements hold and we use similar notations.

Note that the normalised eigenforms in $\mathrm{M}_k(N, \chi\,;\, R)$ are precisely the set of $\mathcal{O}$-algebra homomorphisms inside $\mathrm{Hom}_{\mathcal{O}}(\mathbb{T}_{\mathcal{O}}(\mathrm{M}_k(N, \chi\,;\, \mathbb{C})), R)$. 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).

Galois conjugacy classes

Let us now consider a field K which admits a ring homomorphism $\mathcal{O} \to K$. Denote by $\overline{K}$ a separable closure, so that we have

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

We can compose any $\Phi \in \mathrm{Hom}_K(\mathbb{T}_K(\mathrm{M}_k(N, \chi\,;\, \mathbb{C})), \overline{K})$ 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 $\mathrm{M}_k(N, \chi\,;\, \overline{K})$ (on

formal q-expansions, we only need to apply σ to the coefficients). All this works similarly for the cuspidal and the Eisenstein spaces, 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*. We have the following bijective correspondences.

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

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 $\mathrm{M}_k(N, \chi\,;\, \overline{K})$ or $\mathrm{S}_k(N, \chi\,;\, \overline{K})$. 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).

1.2.2 Exercise. *Prove these correspondences.*

Let us not fail to record 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.

1.3 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.

Let us start with a simple case which we will prove directly. It would, however, also follow from the more general approach adopted below.

Let $\mathbb{T}$ be a finite dimensional algebra over a field K. Such an algebra is *Artinian*, i.e. every descending chain of ideals becomes stationary. That is obvious, since in every proper inclusion of ideals the dimension diminishes. In particular, 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 $\mathfrak{a}^n$. If $\mathfrak{m}$ is a prime ideal, then $\mathbb{T}/\mathfrak{m}$ is an integral domain (since $\mathfrak{m}$ is a prime ideal) which is a finite extension of a field, so it is a field itself, whence the ideal is maximal. Moreover, for dimension reasons there can only be finitely many maximal ideals in $\mathbb{T}$.

1.3.1 Lemma. *The Chinese Remainder Theorem gives*

$$\mathbb{T} \cong \prod_{\mathfrak{m} \in \mathrm{Spec}(\mathbb{T})} \mathbb{T}/\mathfrak{m}^\infty \cong \prod_{\mathfrak{m} \in \mathrm{Spec}(\mathbb{T})} \mathbb{T}_\mathfrak{m},$$

where $\mathbb{T}_\mathfrak{m}$ denotes the localisation at $\mathfrak{m}$.

Proof. The intersection of all prime ideals $\bigcap_{\mathfrak{m}\in\mathrm{Spec}(\mathbb{T})}\mathfrak{m}$ contains only nilpotent elements, whence $\bigcap_{\mathfrak{m}\in\mathrm{Spec}(\mathbb{T})}\mathfrak{m}^\infty = (0)$ (alternatively, one can look at the primary decomposition of (0)). So, if $\mathbb{T}$ is local, we are done. Hence, suppose there are at least two different prime ideals in $\mathbb{T}$.

Put $I := \sum_{\mathfrak{m}\in\mathrm{Spec}(\mathbb{T})}\mathfrak{m}^\infty$. We have $I = A$. For, let us suppose the contrary. As I is an ideal, it is contained in a maximal one, say $\mathfrak{m}_1$. In particular, every $\mathfrak{m}^\infty \subseteq \mathfrak{m}_1$. Let $x \in \mathfrak{m}_2 - \mathfrak{m}_1$ (for a prime ideal $\mathfrak{m}_2 \neq \mathfrak{m}_1$). The element x^n is in $\mathfrak{m}_2^\infty$ if n is big enough. As $\mathfrak{m}_2^\infty$ is a subset of $\mathfrak{m}_1$, the primality of $\mathfrak{m}_1$ implies that x is in $\mathfrak{m}_1$, contradicting the fact that it is not.

It is clear that $\mathbb{T}_{\mathfrak{m}^\infty}$ is a local ring. In fact, every element $s \in \mathbb{T} - \mathfrak{m}$ is invertible in $\mathbb{T}_{\mathfrak{m}^\infty}$ since it clearly does not lie in the unique maximal ideal $\mathfrak{m}/\mathfrak{m}^\infty$. This establishes the second isomorphism. □

Let us now come to a more general setting.

1.3.2 Proposition. *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 dimension of $\mathbb{T}_{\widehat{\mathcal{O}}}$ is less than or equal to 1. 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 which are contained in a prime of height 1 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. 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 the following exercise.

We have already seen Parts (c) and (d) in Lemma 1.3.1. Part (b) follows from (c) by applying Hensel's lifting lemma to the idempotents of the decomposition of (c) (see also [Eisenbud], Corollary 7.6). □

1.3.3 Exercise. *Prove the correspondences and the isomorphisms from Part (a) of Proposition 1.3.2.*

Similar decompositions for $\mathbb{T}$-modules are derived by applying the idempotents of the decompositions of Part (b). More precisely, I mean the following. Any direct product decomposition is given by idempotents. So, in the case of $\mathbb{T}_{\widehat{\mathcal{O}}}$ there exist elements $e_{\mathfrak{m}}$ for each prime in $\mathrm{Spec}(\mathbb{T}_{\widehat{\mathcal{O}}})$ such that $e_{\mathfrak{m}}\mathbb{T}_{\widehat{\mathcal{O}}} = \mathbb{T}_{\widehat{\mathcal{O}},\mathfrak{m}}$. Explicitly, under the decomposition we have $e_{\mathfrak{m}} = (0,\dots,0,1,0,\dots,0)$. If now V is any $\mathbb{T}_{\widehat{\mathcal{O}}}$-module, then we have the natural isomorphism

$$V \cong \bigoplus_{\mathfrak{m}} e_{\mathfrak{m}} V$$

of $\mathbb{T}_{\widehat{\mathcal{O}}}$-modules.

1.4 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 shall now apply Proposition 1.3.2 to $\mathbb{T}_{\widehat{\mathcal{O}}}$. It is a free $\widehat{\mathcal{O}}$-module of finite rank which has dimension 1, i.e. every maximal prime contains at least one minimal prime.

By Proposition 1.3.2, 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 1.3.2, 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").

1.4.1 Exercise. *Prove that 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*.

1.4.2 Exercise. *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.*

Due to Exercise 1.4.2, 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.

1.4.3 Proposition. *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 $\mathbb{T}_{\mathcal{O}}$.*

1.4.4 Exercise. *Prove Proposition 1.4.3.*

1.5 Eisenstein primes

Let integers $k \geq 1$, $N \geq 1$ and a character χ be given. Recall the decomposition

$$\mathrm{M}_k(N, \chi\,;\, \mathbb{C}) = \mathrm{Eis}_k(N, \chi\,;\, \mathbb{C}) \oplus \mathrm{S}_k(N, \chi\,;\, \mathbb{C}).$$

We return to the notations of the previous section. A minimal ideal $\mathfrak{p}$ of $\mathbb{T}_{\widehat{\mathcal{O}}}$ is called an *Eisenstein (minimal) ideal* if the corresponding normalised eigenform lies in $\mathrm{Eis}_k(N, \chi\,;\, \mathbb{C})$ (via an identification of $\overline{K}$ with $\mathbb{C}$).

A maximal ideal $\mathfrak{m}$ of $\mathbb{T}_{\widehat{\mathcal{O}}}$ is called an *Eisenstein (maximal) ideal* if it contains an Eisenstein minimal ideal, i.e. if the eigenforms mod p belonging to $\mathfrak{m}$ are reductions of Eisenstein series. Let us remark that it can happen that an Eisenstein maximal ideal contains both an Eisenstein minimal ideal and a non-Eisenstein minimal ideal. In that case one has hence a congruence between a cusp form and an Eisenstein series.

1.6 Geometry of modular curves

Complex modular curves

We will use the following matrices

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

The order of σ is 4 and the order of τ is 3. Considered as elements of $\mathrm{PSL}_2(\mathbb{Z})$, the respective orders are 2 and 3.

We recall that by *cusps* we understand the set $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$. To make the following completely explicit, we also recall that we will consider ∞ as the element $(1:0)\ \mathbb{P}^1(\mathbb{Q})$ and also as $1/0$. We write $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$.

The group $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathbb{H}$ by fractional linear transformations, i.e. by

$$z \mapsto \frac{az+b}{cz+d} \quad \text{for } z \in \mathbb{H} \text{ and } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{R}).$$

Note that the same formula also makes sense for the action of $\mathrm{GL}_2(\mathbb{Q})$ on $\mathbb{P}^1(\mathbb{Q})$, whence overall we obtain a $\mathrm{SL}_2(\mathbb{Q})$-action on $\overline{\mathbb{H}}$. Obviously, the matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ acts trivially, so that the action passes to an action of $\mathrm{PSL}_2(\mathbb{Q})$.

1.6.1 Exercise. *(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 $\mathrm{PSL}_2(\mathbb{Z})$. [Hint: One might find it helpful to look at the standard fundamental domain.]

1.6.2 Exercise. *Determine the $N \geq 1$ for which $\Gamma_1(N)$ has no element of finite order apart from the identity. [Hint: You should get $N \geq 4$.]*

1.6.3 Exercise. *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.*

Let $\Gamma \leq \mathrm{PSL}_2(\mathbb{Z})$ be a subgroup of finite index, for example (the projective image of) $\Gamma_0(N)$ or $\Gamma_1(N)$. We let

$$Y_\Gamma := \Gamma\backslash\mathbb{H} \quad \text{and} \quad X_\Gamma := Y_\Gamma \cup \Gamma\backslash\mathbb{P}^1(\mathbb{Q}).$$

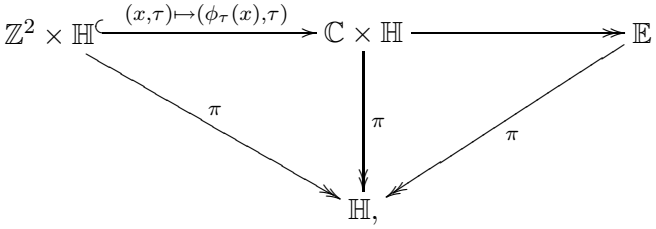
One can equip Y_Γ and X_Γ with the structure of a Riemann surface (which is compact in the case of X_Γ).

Let us denote by π the (open) quotient map $\mathbb{H} \twoheadrightarrow Y_\Gamma$. Via the associated fractional linear transformation, every $\gamma \in \Gamma$ gives a map $\mathbb{H} \xrightarrow{\gamma} \mathbb{H}$, which is trivial on the quotient Y_Γ. The fibre of a point $y \in Y_\Gamma$ is the Γ-orbit Γx (if $\pi(x) = y$). If the stabiliser subgroup Γ_x is trivial for all x, then the quotient map π is a Galois covering and the fractional transformations are covering maps (deck transformations, Galois covering maps). One sees that $\mathbb{H}$ is the universal covering space (since it is simply connected). The group Γ is hence the universal covering group of the Galois covering given by π and can thus be identified with the fundamental group of Y_Γ.

Complex modular curves as moduli spaces

The following discussion is based on lecture notes and explanations by Bas Edixhoven. These things are discussed in [KM] and [Deligne-Rapoport] (see also [Diamond-Im] and [DDT]).

Let us consider the following commutative diagram



(1.6)

where the map ϕ_τ is defined by $\binom{n}{m} \mapsto \binom{n}{m}^T \binom{\tau}{1} = n\tau + m$ and π denotes the obvious projection maps. We shall consider this diagram in the category of complex manifolds.

Let us look at the fibre of a point $\tau \in \mathbb{H}$ under π, it is

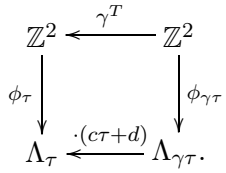
$$0 \to \mathbb{Z}^2 \xrightarrow{\phi_\tau} \mathbb{C} \to E_\tau \to 0,$$

where $E_\tau = \mathbb{C}/\Lambda_\tau$ with $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$. I.e. the fibre is an elliptic curve over $\mathbb{C}$, and we have kept track of the lattice, in a standard form, that gives rise to the curve.

Next we bring natural actions of the group $\mathrm{SL}_2(\mathbb{Z})$ into play. Recall its action on the upper half plane $\mathbb{H}$ by fractional linear transformations. We want to relate this action to the standard one on $\mathbb{Z}^2$. First we note the obvious formula

$$(c\tau + d)\binom{\gamma.\tau}{1} = \gamma\binom{\tau}{1}.$$

Furthermore, one immediately finds the commutative diagram



(1.7)

We will put these relations to two different uses. First, we define actions by the group $\mathrm{SL}_2(\mathbb{Z})$ on Diagram 1.6. So let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be a matrix in $\mathrm{SL}_2(\mathbb{Z})$. We make γ act on $\mathbb{Z}^2 \times \mathbb{H}$ by $\gamma.(\binom{n}{m}, \tau) := (\gamma^{-1,T}\binom{n}{m}, \gamma.\tau)$ and on $\mathbb{C} \times \mathbb{H}$ by $\gamma.(z,\tau) := (\frac{z}{c\tau+d}, \gamma.\tau)$.

It is immediate to check, e.g. using the relations exhibitied above, that the left hand side of Diagram 1.6 is $\mathrm{SL}_2(\mathbb{Z})$-equivariant. We transport the action to the right hand side, and could consequently pass to the quotient for any subgroup $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ of finite index. The quotient maps would also be analytic again. However, we avoid the use of quotients at this stage. Instead of speaking of a fibre of $\Gamma\tau$ for the quotients, we can look at the family of exact sequences

$$0 \to \mathbb{Z}^2 \xrightarrow{\phi_{\gamma\tau}} \mathbb{C} \to E_{\gamma\tau} \to 0 \qquad \text{for } \gamma \in \Gamma.$$

We next want to see the use of the standard congruence subgroups $\Gamma(N)$, $\Gamma_1(N)$ and $\Gamma_0(N)$ in this context. They will give rise to families of elliptic curves having some common property related to their torsion groups.

For that it is convenient to consider such an exact sequence as a pair (E_τ, ϕ_τ) (here, of course, the second component determines the first one). We interpret ϕ_τ as the choice of a lattice basis.

Let $N > 0$ be an integer. The N-torsion group $E_\tau[N]$ of the elliptic curve E_τ is defined as the first term in the exact sequence

$$0 \to \frac{1}{N}\Lambda_\tau/\Lambda_\tau \to E_\tau \xrightarrow{\cdot N} E_\tau.$$

The "choice of basis" isomorphism ϕ_τ descends to give the isomorphism

$$\overline{\phi_\tau} : (\mathbb{Z}/N\mathbb{Z})^2 \to E_\tau[N], \quad x \mapsto \frac{1}{N}\phi_\tau(x),$$

which should also be interpreted as a choice of basis of the torsion group. $\overline{\phi_\tau}$ is called a *level structure*.

Let us now compare the exact sequence of τ with the one of $\gamma\tau$ for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ as above, i.e. we want to relate the pair (E_τ, ϕ_τ) to $(E_{\gamma\tau}, \phi_{\gamma\tau})$. From Diagram 1.7, we immediately obtain the commutative diagram

$$\begin{array}{ccc} (\mathbb{Z}/N\mathbb{Z})^2 & \xleftarrow{\overline{\gamma^T}} & (\mathbb{Z}/N\mathbb{Z})^2 \\ \downarrow{\scriptstyle \overline{\phi_\tau}} & & \downarrow{\scriptstyle \overline{\phi_{\gamma\tau}}} \\ E_\tau[N] & \xleftarrow{\cdot(c\tau+d)} & E_{\gamma\tau}[N], \end{array}$$

in which all maps are isomorphism.

We fix a $\tau \in \mathbb{H}$.

- Recall the group $\Gamma(N) = \ker\big(\mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\big)$. It gives rise to the family of the exact sequences represented by the pairs $(E_{\gamma\tau}, \phi_{\gamma\tau})$ for $\gamma \in \Gamma(N)$, which precisely have in common that the choice of basis of their torsion groups are the same (for the natural ismorphism between E_τ and $E_{\gamma\tau}$).

  Hence the family $\Gamma(N)\tau$ corresponds to the isomorphism class of a pair $(E_\tau, \overline{\phi_\tau})$. By isomorphism of pairs we mean an isomorphism between the curves respecting the level structure, i.e. sitting in the commutative diagram

$$\begin{array}{ccccc} & & (\mathbb{Z}/N\mathbb{Z})^2 & & \\ & \swarrow{\scriptstyle \overline{\phi_\tau}} & & \searrow{\scriptstyle \overline{\phi_{\gamma\tau}}} & \\ E_\tau[N] & & \xleftarrow{\cdot(c\tau+d)} & & E_{\gamma\tau}[N]. \end{array}$$

- Next consider the group $\Gamma_1(N)$. It gives rise to the family, where $\overline{\phi_\tau}(\binom{0}{1}) = \overline{\phi_{\gamma\tau}}(\binom{0}{1})$. That means that the natural isomorphism maps the point $\frac{1}{N}$ of E_τ to the point $\frac{1}{N}$ of $E_{\gamma\tau}$.

  This family thus corresponds to the isomorphism class of the pair $(E_\tau, \overline{\phi_\tau}) = (E_\tau, 1/N)$.

- Finally, we consider the group $\Gamma_0(N)$. The family corresponding to it can be characterised by saying that the subgroup of $E_\tau[N]$ generated by $\frac{1}{N}$ is mapped isomorphically into the corresponding one of $E_{\gamma\tau}[N]$.

  Thus, we have the interpretation as the isomorphism class of a pair $(E_\tau, < 1/N >)$.

We have been quite restrictive considering only elliptic curves of the form E_τ. More generally one ought to regard pairs (E, ϕ), where E is an elliptic curve over $\mathbb{C}$ and $\phi : \mathbb{Z}^2 \to H_1(E(\mathbb{C}), \mathbb{Z})$ is a group isomorphism, in which case $E = H_1(E(\mathbb{C}), \mathbb{R})/H_1(E(\mathbb{C}), \mathbb{Z})$. Since, however, scaling the lattice by a non-zero complex number results in an isomorphic elliptic curve, the isomorphism class of (E, ϕ) always contains an element of the form (E_τ, ϕ_τ). In particular, there is an obvious way to broaden the definition of the pairs in the three points above, while the isomorphism classes stay the same.

The $\Gamma_1(N)$-moduli problem over a ring R

Motivated by the $\Gamma_1(N)$-case in the discussion on complex modular curves, we define the category $[\Gamma_1(N)]_R$ of *elliptic curves with a given torsion point* for a ring R as follows:

- Objects: Pairs $(E/S/R, \phi)$. Here $E/S/R$ is an elliptic curve, i.e. E/S a proper smooth scheme over $\mathrm{Spec}(R)$, whose geometric fibres are connected smooth curves of genus 1, and there is an S-valued point 0 of E. And $\phi : (\mathbb{Z}/N\mathbb{Z})_S \hookrightarrow E[N]$ is an embedding of group schemes. We briefly recall that $E[N]$ is the S-group scheme obtained from the cartesian diagram

$$\begin{array}{ccc} E & \xrightarrow{\cdot N} & E \\ \uparrow & \square & \uparrow{\scriptstyle 0} \\ E[N] & \longrightarrow & S, \end{array}$$

  i.e. it is the kernel of the multiplication by N map, which results from E/S being an abelian group scheme.

- Morphisms: Cartesian diagrams

$$\begin{array}{ccc} E' & \xrightarrow{h} & E \\ \downarrow & \square & \downarrow \\ S' & \xrightarrow{g} & S, \end{array}$$

  such that the diagram

$$\begin{array}{ccc} E' & \xrightarrow{h} & E \\ \uparrow{\scriptstyle 0} & & \uparrow{\scriptstyle 0} \\ S' & \xrightarrow{g} & S \end{array}$$

  is commutative, and the embedding

$$\phi' : (\mathbb{Z}/N\mathbb{Z})_{S'} \hookrightarrow E'[N]$$

  is obtained by base change from

$$\phi : (\mathbb{Z}/N\mathbb{Z})_S \hookrightarrow E[N].$$

1.6.4 Theorem. (Igusa) *If $N \geq 5$ and R is a ring in which N is invertible, then $[\Gamma_1(N)]_R$ is representable by a smooth affine scheme $Y_1(N)_R$ which is of finite type over R.*

In fact, a suitable extension of the category to the "cusps" (by using generalised elliptic curves) is representable by a proper smooth scheme $X_1(N)_R$ which is of finite type over R.

Hecke correspondences on the moduli problem

We first describe Hecke correspondences on complex modular curves. We will only work with the $\Gamma_1(N)$-moduli problem.

Let $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$ and set for abbreviation $\Gamma := \Gamma_1(N)$. Then the groups

$$\Gamma_\alpha := \alpha^{-1}\Gamma\alpha \cap \Gamma \quad \text{and} \quad \Gamma^\alpha := \alpha\Gamma\alpha^{-1} \cap \Gamma$$

have finite index in Γ. We consider the commutative diagram

$$\begin{array}{ccc} \Gamma_\alpha\backslash\mathbb{H} & \xrightarrow[\sim]{\alpha} & \Gamma^\alpha\backslash\mathbb{H} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \Gamma\backslash\mathbb{H} & & \Gamma\backslash\mathbb{H}, \end{array} \tag{1.8}$$

where π denotes the natural projections. Diagram 1.8 is to be seen as a correspondence on $Y_\Gamma = \Gamma\backslash\mathbb{H}$. On divisors (formal finite sums of points), it gives rise to the map

$$\mathrm{Div}(Y_\Gamma) \to \mathrm{Div}(Y_\Gamma), \quad \tau \mapsto \sum_{x \in (\pi\alpha)^{-1}(\tau)} \pi(x).$$

Note that we may use Diagram 1.8 to obtain the commutative diagram on group cohomology:

$$\begin{array}{ccc} H^1(\Gamma_\alpha, M) & \xrightarrow[\sim]{\text{conj. by } \alpha} & H^1(\Gamma^\alpha, M) \\ \downarrow{\scriptstyle \text{cores}} & & \uparrow{\scriptstyle \text{res}} \\ H^1(\Gamma, M) & \xleftarrow{T_\alpha} & H^1(\Gamma, M), \end{array}$$

where M is a Γ-module. One sees immediately that it is precisely the definition of a Hecke operator on group cohomology which is given later on.

Now we apply this abstract situation to two cases, in both of which we will give an equivalent description on the moduli spaces.

- Diamond correspondences:

  Let a be an integer coprime to N and choose a matrix $\alpha = \sigma_a \in \Gamma_0(N)$ as in Equation 1.1. As $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$, the groups Γ_α and Γ^α are equal to Γ and the maps π are the identity. The operator corresponding to α is called the *diamond operator* and denoted $\langle a \rangle$. It will become apparent that it indeed only depends on a and not on the choice of α.

Under α, the elliptic curve with given torsion point $(\mathbb{C}/\mathbb{Z}\tau+\mathbb{Z}, 1/N)$ is mapped to $(\mathbb{C}/\mathbb{Z}\alpha\tau+\mathbb{Z}, 1/N)$, which is isomorphic to $(\mathbb{C}/\mathbb{Z}\tau+\mathbb{Z}, a/N)$.

More generally, we can define the functor $\langle a\rangle$ on $[\Gamma_1(N)]_R$ which sends an object $(E/S/R, \phi)$ to the object $(E/S/R, \phi\circ a)$, where we interpret a as multiplication by a on $(\mathbb{Z}/N\mathbb{Z})_S$.

- Hecke correspondences:

  For simplicity, we again give the definition of Hecke correspondences only for primes l. So let l be a prime. The l-th Hecke correspondence T_l is defined by the matrix $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & l \end{smallmatrix}\right)$.

  Straightforward calculations yield (whether l divides N or not)

  $$\Gamma^\alpha = \Gamma_1(N)\cap\Gamma_0(l) \text{ and } \Gamma_\alpha = \Gamma_1(N)\cap(\Gamma_0(l))^T,$$

  where the superscript T stands for transpose. By identifying $\tau \mapsto (\mathbb{C}/\mathbb{Z}\tau+\mathbb{Z}, 1/N, <\tau/l>)$, one gets a one-to-one correspondence between $\Gamma_\alpha\backslash\mathbb{H}$ and triples (E, P, H) (up to isomorphism), where E is an elliptic curve with N-torsion point P and $H \leq E$ a (cyclic) subgroup of order l that does not contain the point P. For Γ^α one can proceed similarly (the third component must be replaced by $<1/l>$). Direct inspection shows that on the moduli spaces the map α corresponds to

  $$(E, P, H) \mapsto (E/H, P \bmod H, E[l]/H).$$

  Of course, the maps π just mean dropping the third component. The H correspond precisely to the isogenies $E \to E'$ of degree l (for some E'; for given H, of course, $E' = E/H$) with P not in the kernel.

  For $[\Gamma_1(N)]_R$ we interpret the Hecke correspondence T_l as assigning to an object $(E/S/R, \phi)$ the set of objects $(\psi(E)/S/R, \psi\circ\phi)$, where ψ runs through the isogenies $\psi : E \to E'$ of degree l such that $\psi\circ\phi$ is still a $\Gamma_1(N)$-level structure.

1.6.5 Exercise. *Check the above calculations. (I'm not so sure whether I have not messed them up a bit when I did them a long time ago, so don't worry if you find the need to correct some statements.)*

1.7 Katz modular forms

The purpose of the present section is to give an informal introduction to Katz modular forms. We let R be a ring in which $N \geq 1$ is invertible.

For every elliptic curve $E/S/R$ in $[\Gamma_1(N)]_R$, we let $\underline{\omega}_{E/S} = 0^*\underline{\Omega}_{E/S}$. Given any morphism $h : E'/S'/R \to E/S/R$, the induced map $\underline{\omega}_{E'/S'} \to h^*\underline{\omega}_{E/S}$ is an isomorphism. Indeed, it is a well-known fact ([Hartshorne], II.8.10) that the sheaf of relative differentials is stable under base change: $h^*\underline{\Omega}_{E/S} \cong \underline{\Omega}_{E'/S'}$. Thus, we get (with g as above)

$$g^*\underline{\omega}_{E/S} = (g^*\circ 0^*)\underline{\Omega}_{E/S} = (0\circ g)^*\underline{\Omega}_{E/S} = (h\circ 0)^*\underline{\Omega}_{E/S} \cong 0^*\underline{\Omega}_{E'/S'} = \underline{\omega}_{E'/S'}.$$

A *Katz modular form (cusp) form* $f \in \mathrm{M}_k(\Gamma_1(N)\,;\,R)_{\text{Katz}}$ (respectively, $f \in \mathrm{S}_k(\Gamma_1(N)\,;\,R)_{\text{Katz}}$) assigns to every object $(E/S/R, \alpha)$ of $[\Gamma_1(N)]_R$ an element $f(E/S/R,\alpha) \in \underline{\omega}_{E/S}^{\otimes k}(S)$, compatibly for the morphisms in the category, subject to the condition that all q-expansions (which one obtains by adjoining all N-th roots of unity and plugging in a suitable Tate curve) have no negative terms (respectively, only have positive terms).

Hecke operators

The discussion of Hecke correspondences above, makes the following definition appear quite suggestive. For $(a, N) = 1$, we define the diamond operator $\langle a\rangle$ by

$$\langle a\rangle : \mathrm{M}_k(\Gamma_1(N)\,;\,R)_{\text{Katz}} \to \mathrm{M}_k(\Gamma_1(N)\,;\,R)_{\text{Katz}},$$

$$(\langle a\rangle f)(E/S/R,\phi) = f(E/S/R, \phi\circ a).$$

One thus gets again an action of the group $(\mathbb{Z}/N)^* \cong \Gamma_0(N)/\Gamma_1(N)$ on the space of Katz modular forms (cusp forms). Let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to R^*$ be a character. Then we let $\mathrm{M}_k(N,\chi\,;\,R)_{\text{Katz}}$ be the χ-eigenspace, and similarly for the cusp space.

Next, we give an idea of the definition of the Hecke operator T_l (for a prime l) on Katz modular forms.

$$T_l : \mathrm{M}_k(\Gamma_1(N)\,;\,R)_{\text{Katz}} \to \mathrm{M}_k(\Gamma_1(N)\,;\,R)_{\text{Katz}},$$

$$(T_l F)(E/S/R, P) = \frac{1}{l}\sum_{\psi} F(\psi(E)/S/R, \psi\circ\phi),$$

where the sum runs over all isogenies $\psi : E \to E'$ of degree l such that $\psi\circ\phi$ is a $\Gamma_1(N)$-level structure.

Note that we divide by l which need not always make sense. However, there are ways to get around that problem. We refer to the discussion in Sections 3 and 4 of [Gross]. In that article, Gross proves also that the Hecke operators defined like this give the very same action on the q-expansions as we have seen for holomorphic modular forms. To mention another complication we must point out that the moduli problem considered by Gross is slightly different from ours (the differences are not at all serious, but must not be forgotten).

Comparison of Katz forms over $\mathbb{F}_p$ and modular forms mod p

One can compute explicitly (see [Diamond-Im], Section 12.3) that

$$\mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C}) \cong \mathrm{M}_k(\Gamma_1(N)\,;\,\mathbb{C})_{\text{Katz}} \quad\text{and}\quad \mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{C}) \cong \mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{C})_{\text{Katz}}.$$

1.7.1 Theorem. *Let S be an R-algebra with R a $\mathbb{Z}[1/N]$-algebra for some integer $N \geq 5$. Let $k \in \mathbb{N}$ and suppose that one of the following holds:*

(i) $k \geq 2$

(ii) $R \to S$ *is flat.*

Then the following natural maps are isomorphisms:

$$\mathrm{M}_k(\Gamma_1(N)\,;\,R)_{\textit{Katz}} \otimes_R S \cong \mathrm{M}_k(\Gamma_1(N)\,;\,S)_{\textit{Katz}} \quad \textit{and}$$
$$\mathrm{S}_k(\Gamma_1(N)\,;\,R)_{\textit{Katz}} \otimes_R S \cong \mathrm{S}_k(\Gamma_1(N)\,;\,S)_{\textit{Katz}}$$

Proof. This is [Diamond-Im], Theorem 12.3.2. □

In the case of a character, the statements of the theorem do in general not stay correct. For a precise statement see [EdixSerre].

One knows (that follows from [EdixSerre], Lemma 1.9) for $k \geq 2$, $N \geq 1$ over the ring $R = \mathbb{F}_p$ with $p > 3$ and $p \nmid N$ that

$$\mathrm{M}_k(N, \overline{\chi}\,;\,\mathbb{F}_p)_{\text{Katz}} \cong \mathrm{M}_k(N, \overline{\chi}\,;\,\mathbb{F}_p).$$

Hence, in most cases for weights $k \geq 2$ we may just think about Katz modular forms over $\mathbb{F}_p$ as mod p modular forms. A similar statement holds for the cusp spaces (since the q-expansions coincide).

1.8 Katz modular forms over $\overline{\mathbb{F}_p}$ of weight one

Edixhoven explains in [EdixJussieu], Section 4, how weight one cuspidal Katz modular forms over finite fields of characteristic p can be computed from the knowledge of the Hecke algebra of weight p cusp forms over the same field. In this section we shall recall this.

Let $\mathbb{F}$ be a finite field of prime characteristic p or $\overline{\mathbb{F}_p}$ and fix a level $N \geq 1$ with $p \nmid N$ and a character $\overline{\chi} : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{F}^*$ with $\overline{\chi}(-1) = (-1)^k$. We have two injections of $\mathbb{F}$-vector spaces

$$F, A : \mathrm{S}_1(N, \overline{\chi}\,;\,\mathbb{F})_{\text{Katz}} \to \mathrm{S}_p(N, \overline{\chi}\,;\,\mathbb{F})_{\text{Katz}},$$

given on q-expansions by $a_n(Ag) = a_n(g)$ and $a_n(Fg) = a_{n/p}(g)$ (with $a_n(Fg) = 0$ if $p \nmid n$), which are compatible with all Hecke operators T_l for primes $l \neq p$. The former comes from the *Frobenius* and the latter is multiplication by the *Hasse invariant*. One has $T_p^{(p)} F = A$ and $AT_p^{(1)} = T_p^{(p)} A + \overline{\chi}(p)F$, where we have indicated the weight as a superscript (see e.g. [EdixJussieu], Equation (4.1.2)). At this point, we should remark that there is a subtlety concerning two different definitions of Katz modular forms. For the Frobenius on q-expansions to be given as indicated one has to use Gross' definition, instead of the one sketched before. This point is discussed in [EdixJussieu] (in that paper, the space we should be using is called $S_k(\cdot)'_{\text{Katz}}$).

Let us write $\mathbb{T}^{(k)}$ for $\mathbb{T}_{\mathbb{F}}(\mathrm{S}_k(N, \overline{\chi}\,;\,\mathbb{F})_{\text{Katz}})$, the Hecke algebra over $\mathbb{F}$ of weight k for a fixed level N and a fixed character $\overline{\chi}$. We will also indicate the weight of Hecke operators by superscripts. We denote by $A^{(p)}$ the $\mathbb{F}_p$-subalgebra of $\mathbb{T}^{(p)}$ generated by all Hecke operators $T_n^{(p)}$ for $p \nmid n$.

1.8.1 Proposition. *(a) There is a homomorphism* Θ*, called a* derivation*, which on* q*-expansions is given by* $a_n(\Theta f) = n a_n(f)$ *such that the sequence*

$$0 \to \mathrm{S}_1(N, \overline{\chi}\,;\,\mathbb{F})_{\textit{Katz}} \xrightarrow{F} \mathrm{S}_p(N, \overline{\chi}\,;\,\mathbb{F})_{\textit{Katz}} \xrightarrow{\Theta} \mathrm{S}_{p+2}(N, \overline{\chi}\,;\,\mathbb{F})_{\textit{Katz}}$$

is exact.

(b) Suppose $f \in \mathrm{S}_1(N, \overline{\chi}\,; \mathbb{F})_{\textit{Katz}}$ *such that* $a_n(f) = 0$ *for all* n *with* $p \nmid n$. *Then* $f = 0$. *In particular* $A\mathrm{S}_1(N, \overline{\chi}\,; \mathbb{F})_{\textit{Katz}} \cap F\mathrm{S}_1(N, \overline{\chi}\,; \mathbb{F})_{\textit{Katz}} = 0$.

(c) The Hecke algebra $\mathbb{T}^{(1)}$ *in weight one can be generated by all* $T_l^{(1)}$, *where* l *runs through the primes different from* p.

(d) The weight one Hecke algebra $\mathbb{T}^{(1)}$ *is the algebra generated by the* $A^{(p)}$*-action on the module* $\mathbb{T}^{(p)}/A^{(p)}$.

Proof. (a) The main theorem of [KatzDerivation] gives the exact sequence

$$0 \to \mathrm{S}_1(N, \overline{\chi}\,; \mathbb{F})_{\mathrm{Katz}} \xrightarrow{F} \mathrm{S}_p(N, \overline{\chi}\,; \mathbb{F})_{\mathrm{Katz}} \xrightarrow{A\Theta} \mathrm{S}_{2p+1}(N, \overline{\chi}\,; \mathbb{F})_{\mathrm{Katz}}$$

by taking Galois invariants. As explained in [EdixJussieu], Section 4, the image $A\Theta\mathrm{S}_p(N, \overline{\chi}\,; \mathbb{F})_{\mathrm{Katz}}$ in weight $2p+1$ can be divided by the Hasse invariant, whence the weight is as claimed.

(b) The condition implies by looking at q-expansions that $A\Theta f = 0$, whence by Part (3) of Katz' theorem cited above f comes from a lower weight than 1, but below there is just the 0-form (see also [EdixJussieu], Proposition 4.4).

(c) It is enough to show that $T_p^{(1)}$ is linearly dependent on the span of all $T_n^{(1)}$ for $p \nmid n$. If it were not, then there would be a modular cusp form of weight 1 satisfying $a_n(f) = 0$ for $p \nmid n$, but $a_p(f) \neq 0$, contradicting (b).

(d) Dualising the exact sequence in (a) yields that $\mathbb{T}^{(p)}/A^{(p)}$ and $\mathbb{T}^{(1)}$ are isomorphic as $A^{(p)}$-modules, which implies the claim. □

1.8.2 Proposition. *Set* $B = \frac{N}{12}\prod_{l|N, l\ \textit{prime}}(1 + \frac{1}{l})$. *The* $\mathbb{F}$*-algebra* $A^{(p)}$ *can be generated as an* $\mathbb{F}$*-vector space by the set*

$$\{\ T_n^{(p)}\ \mid\ p \nmid n,\ n \leq (p+2)B\ \}.$$

Proof. Assume that some $T_m^{(p)}$ for $m > (p+2)B$ and $p \nmid m$ is linearly independent of the operators in the set of the assertion. This means that there is a cusp form $f \in \mathrm{S}_p(N, \overline{\chi}\,; \mathbb{F})_{\mathrm{Katz}}$ satisfying $a_n(f) = 0$ for all $n \leq (p+2)B$ with $p \nmid n$, but $a_m(f) \neq 0$. One gets $a_n(\Theta f) = 0$ for all $n \leq (p+2)B$, but $a_m(\Theta f) \neq 0$. This contradicts the Sturm bound of Proposition 3.3.1 (which also applies to Katz modular forms). □

1.8.3 Remark. *If we work with* $\Gamma_1(N)$ *and no character, the number* B *above has to be replaced by*

$$B' = \frac{N^2}{24}\prod_{l|N, l\ \textit{prime}}(1 - \frac{1}{l^2}).$$

Part of the following proposition is [EdixJussieu], Proposition 6.2. We are particularly interested in its last part which states that weight p eigenforms which live in the span of Ag and Fg for a weight 1 eigenform g are ordinary, i.e. $a_p(f) \neq 0$.

1.8.4 Proposition. *Let $V \subset \mathrm{S}_p(N, \overline{\chi}\,; \mathbb{F})_{Katz}$ be the eigenspace of a system of eigenvalues for the operators $T_l^{(p)}$ for all primes $l \neq p$*

If the system of eigenvalues does not come from a weight one form, then V is at most of dimension one. Conversely, if there is a normalised weight one eigenform g with that system of eigenvalues for $T_l^{(1)}$ for all primes $l \neq p$, then $V = \langle Ag, Fg \rangle$ and that space is 2-dimensional. On it $T_p^{(p)}$ acts with eigenvalues u and $\overline{\chi}(p)u^{-1}$ satisfying $u + \overline{\chi}(p)u^{-1} = a_p(g)$. In particular, the eigenforms in weight p which come from weight one are ordinary.

Proof. We choose a normalised eigenform f for all operators. If V is at least 2-dimensional, then we have $V = \mathbb{F}f \oplus \{h \mid a_n(h) = 0 \ \forall p \nmid n\}$. As a form h in the right summand is annihilated by Θ, it is equal to Fg for some form g of weight one by Proposition 1.8.1 (a). By Part (b) of that proposition we know that $\langle Ag, Fg \rangle$ is 2-dimensional. If V were more than 2-dimensional, then there would be two different cusp forms in weight 1, which are eigenforms for all $T_l^{(1)}$ with $l \neq p$. This, however, contradicts Part (c).

Assume now that V is 2-dimensional. Any normalised eigenform $f \in V$ for all Hecke operators in weight p has to be of the form $Ag + \mu Fg$ for some $\mu \in \overline{\mathbb{F}}$. The eigenvalue of $T_p^{(p)}$ on f is the p-th coefficient, hence $u = a_p(g) + \mu$, as $a_p(Fg) = a_1(g) = 1$. Now we have

$$\begin{aligned}(a_p(g) + \mu)(Ag + \mu Fg) &= T_p^{(p)}(Ag + \mu Fg) = T_p^{(p)}Ag + \mu Ag \\ &= AT_p^{(1)}g - \overline{\chi}(p)Fg + \mu Ag = (a_p(g) + \mu)Ag - \overline{\chi}(p)Fg,\end{aligned}$$

which implies $-\overline{\chi}(p) = (a_p(g) + \mu)\mu = u^2 - ua_p(g)$ by looking at the p-th coefficient. From this one obtains the claim on u. □

1.9 Galois representations attached to eigenforms

We mention the sad fact that only the one-dimensional representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ are 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.

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 $k \geq 2$.

1.9.1 Theorem. *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.

1.9.2 Theorem. *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 $f \in \mathrm{S}_k(N, \overline{\chi}\,; \overline{\mathbb{F}_p})$ *with* $f = \sum_{n\geq 1} a_n(f)q^n$ *one can attach a Galois representation, i.e. a continuous group homomorphism (for the trivial 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*,*

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

1.9.3 Exercise. *A continuous group homomorphism from a profinite group* G *to any* $\mathrm{GL}_2(\overline{\mathbb{F}_p})$ *(with the discrete topology) has a finite image. [Hint: Image of a compact set under a continuous map is compact.]*

Each normalised eigenform mod p hence gives us a 2-dimensional odd Galois representation. Its kernel is by Galois theory of the form $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ for some number field K. Hence, we can also say that K is attached to f. But even more is true. The arithmetic of K can (at least partially) be read off from the coefficients of f, since we know the traces of the Frobenius elements.

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.

1.9.4 Theorem. (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*.*

1.10 Galois representations of weight one Katz modular forms over $\mathbb{F}_p$

We have just seen that a normalised eigenform $f \in \mathrm{S}_1(N, \overline{\chi}\,; \overline{\mathbb{F}_p})_{\text{Katz}}$ can be embedded into weight p in two different ways, via the Hasse invariant and the Frobenius. On the subspace $V := \langle Af, Ff \rangle$ of $\mathrm{S}_p(N, \overline{\chi}\,; \overline{\mathbb{F}_p})_{\text{Katz}}$ all Hecke operators T_l for $l \neq p$ act as multiplication by $a_l(f)$ and there is a modular forms $g \in V$ which is also an eigenform for T_p.

We define ρ_f to be the Galois representation

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

attached to g by Theorem 1.9.2. Note that $l^{p-1} = l^{1-1} = 1$, so that we could have formulated Theorem 1.9.2 to include weight one forms from the beginning.

1.10.1 Theorem. (Edixhoven, Coleman-Voloch, Gross) *Let $f \in \mathrm{S}_1(N, \overline{\chi}\,; \overline{\mathbb{F}_p})_{\text{Katz}}$ be a normalised eigenform, and suppose $p > 2$. Then ρ_f is unramified at p.*

Proof. That is [EdixWeight], Theorem 4.5. □

1.11 Serre's conjecture

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 $k(\rho)$ be the integer defined by [EdixWeight] or k_ρ be the integer defined by [Serre]. In particular, one has $k(\rho) = 1$ if and only if ρ is unramified at p (in that case $k_\rho = p$).
- Let χ_ρ be the prime-to-p part of $\det \circ \rho$, which we consider as a character $(\mathbb{Z}/N_\rho\mathbb{Z})^\times \times (\mathbb{Z}/p\mathbb{Z})^\times \to \overline{\mathbb{F}_p}^\times$.

1.11.1 Conjecture. (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.*

- *(Strongest form) There exists a normalised eigenform $f \in \mathrm{S}_{k(\rho)}(N_\rho, \chi_\rho\,; \overline{\mathbb{F}_p})$*
- *(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 1.9.2.

It is known that for $p > 2$, the weak form implies the strong and the strongest form ([EdixWeight], Theorem 4.5). For $p = 2$, this implication is not known in the so-called exceptional cases, in general. Very recently, Khare and Wintenberger announced a proof of the strong form of Serre's conjecture for all ρ whose N_ρ is odd. Let us mention that N_ρ is odd if and only if $p = 2$ or ρ is unramified at 2.

Serre's conjecture implies, if true, 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. That's the purpose of these notes.

Edixhoven and coworkers have recently succeeded in giving an algorithm which computes the actual Galois representation attached to a mod p modular form!

1.12 Images of Galois representations

With a view towards the problems, we quote two results of Ribet showing that the images of Galois representations attached to modular forms are in general not solvable.

A normalised eigenform f is said to have *complex multiplications (CM)* by a non-trivial quadratic character $\epsilon : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$, if

$$a_p(f) = \epsilon(p) a_p(f)$$

for all primes p in a set of density 1.

1.12.1 Proposition. (Ribet) *Let $f \in \mathrm{S}_2(N, \chi\,; \mathbb{C})$ be an eigenform of level N and some character χ which is not a CM-form. Then for almost all primes p, the image of the representation*

$$\overline{\rho}_p : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$$

attached to f restricted to a suitable open subgroup $H \leq G_{\mathbb{Q}}$ is $\{g \in \mathrm{GL}_2(\mathbb{F}) | \det(g) \in \mathbb{F}_p^*\}$ for some finite extension $\mathbb{F}$ of $\mathbb{F}_p$.

Proof. Reducing modulo a suitable prime above p, this follows from Theorem 3.1 of [R1], where the statement is proved for the p-adic representation attached to f. □

1.12.2 Proposition. (Ribet) *Let N be a square-free integer and $f \in \mathrm{S}_2(\Gamma_0(N)\,; \mathbb{C})$ a newform for the trivial character. Then for all primes $p > 2$, the image of the Galois representation*

$$\overline{\rho}_p : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$$

attached to f contains the group $\mathrm{SL}_2(\mathbb{F}_p)$ if $\overline{\rho}_p$ is irreducible.

Proof. The representation $\overline{\rho}_p$ is semi-stable (see [R2], p. 278). As it is assumed to be irreducible, the proposition is just a restatement of [R2], Corollary 2.3. □

2 Modular Symbols mod p

We distinguish different kinds of modular symbols which we name as follows:

(I) Formal modular symbols: the *modular symbols formalism*.

(II) Group (cohomological) modular symbols.

(III) Geometric homological modular symbols

(IV) Geometric cohomological modular symbols.

The historically first notion of modular symbols was that of geometric homological modular symbols (Birch, Manin, Šokurov, Merel). Group (cohomological) modular symbols were prominently used by Shimura in his proof of the Eichler-Shimura theorem (Theorem 3.1.1). The modular symbols formalism was discussed by Cremona, Merel and Stein, and it is the way MAGMA and SAGE understand modular symbols. Geometric cohomological modular symbols are useful for applying cohomological methods in (algebraic) geometry.

We shall describe in some detail group modular symbols and the modular symbols formalism. Their relation to geometric cohomological modular symbols will be stated without proofs. The geometric homological modular symbols will only be mentioned as a motivation in the weight two case, but will otherwise be disregarded in the present treatment. [SteinBook] is based on them, but unfortunately does not give all the proofs.

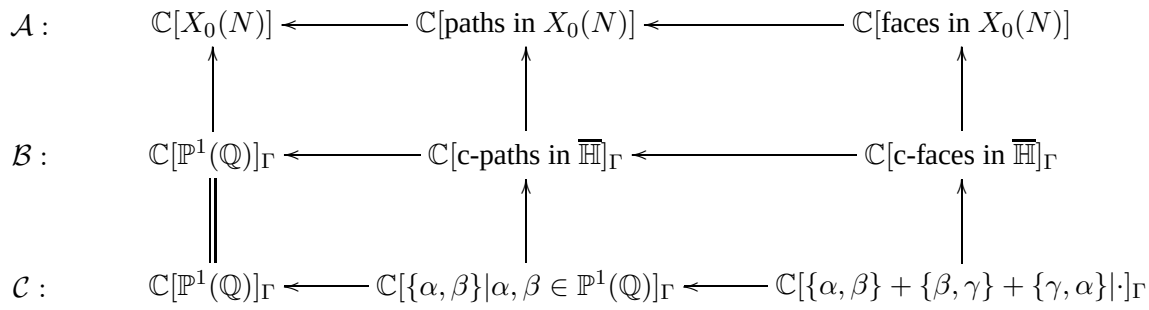
Each of the four types mentioned has its own virtues: The modular symbols formalism is purely in terms of linear algebra and can hence easily be implemented on a computer. The group cohomological description has the advantage of allowing the use of cohomological tools (long exact sequences etc.), while staying in a rather explicit environment. Obviously, the geometric modular symbols have their virtues in all geometric treatments. We only point out that modern definitions of modular forms are very often geometric ones (as one may see if the section on Katz modular forms is written).

2.1 Motivation for weight 2

This part only serves as a motivation for what is going to come. We present geometric homological modular symbols and relate them to the modular symbols formalism, in the case of weight two.

Geometric homological modular symbols should be thought of as a presentation (in terms of generators) of the homology of modular curves. In the following we shall establish a link to the modular symbols formalism. As the base field we choose the complex numbers $\mathbb{C}$.

Consider the following commutative diagram for $\Gamma = \Gamma_0(N)$



One must read "path" as "1-simplex" and "face" as "2-simplex". As we are only motivating a definition, we are not really precise. By c-paths we mean paths that have both their endpoints in the set of cusps. A c-face is a face whose boundary consists of c-paths. The boundary maps are the natural ones for the complexes $\mathcal{A}$ and $\mathcal{B}$. The left map in $\mathcal{C}$ is given by $\{\alpha,\beta\} \mapsto \beta - \alpha$. The right hand side one is the natural map. We have by definition $H_1(\mathcal{A}) = H_1(X_0(N), \mathbb{C})$. Moreover,

$$H_1(\mathcal{C}) \cong \ker\big((\mathbb{C}[\{\alpha,\beta\}|\alpha,\beta \in \mathbb{P}^1(\mathbb{Q})]/\langle\{\alpha,\beta\}+\{\beta,\gamma\}+\{\gamma,\alpha\}\rangle)_\Gamma \to \mathbb{C}[\Gamma\backslash\mathbb{P}^1(\mathbb{Q})]\big).$$

We denote this space by $\mathcal{CM}_2(\Gamma_0(N)\,;\,\mathbb{C})$ and call it the space of *cuspidal modular symbols for* $\Gamma_0(N)$.

The vertical maps from $\mathcal{B}$ to $\mathcal{A}$ are the natural ones. The map from $\mathcal{C}_1$ to $\mathcal{B}_1$ sends $\{\alpha,\beta\}$ to the geodesic path from α to β, which is a semi-circle with α and β on the diameter. Thus, the element $\{\alpha,\beta\}+\{\beta,\gamma\}+\{\gamma,\alpha\}$ in $\mathcal{C}_2$ is sent to the face whose boundaries are the geodesics from α to β, from β to γ and from γ to α. In order to see that this is well defined, one must verify that $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ sends a geodesic to another geodesic, which is true.

2.1.1 Proposition. *We have $H_1(\mathcal{C}) \cong H_1(\mathcal{B}) \cong H_1(\mathcal{A})$. In particular, this gives*

$$\mathcal{CM}_2(\Gamma_0(N)\,;\,\mathbb{C}) \cong H_1(X_0(N), \mathbb{C}).$$

We shall not give a proof in this section. However, it is easy to derive one from the general comparison result to be established later on (Theorem 2.5.1). One can try to compute this isomorphism directly, but one has to watch out, since with $\mathbb{Z}$ instead of $\mathbb{C}$, one only has surjections $H_1(\mathcal{C}) \twoheadrightarrow H_1(\mathcal{B}) \twoheadrightarrow H_1(\mathcal{A})$ whose kernels are torsion. That torsion is due to the existence of non-trivial stabilisers for the actions of $\Gamma_0(N)$ on $\mathbb{H}$.

2.1.2 Remark. *We have $H_1(\mathcal{B}) \twoheadrightarrow H_1(\mathcal{A})$ by a direct argument.*

Proof. The idea is that the elements in the kernel of $\mathcal{A}_1 \to \mathcal{A}_0$ are loops and that one can always compose a loop with another one which meets a cusp and is contractible.

Let $x = \sum_\phi z_\phi \phi$ be in the kernel of the boundary map (the ϕ are paths). Hence, one has $0 = \sum_\phi z_\phi(\phi(0) - \phi(1))$ from which it follows that for any $a \in X_0(N)$ the equality

$$0 = \sum_{\phi,\phi(0)=a} z_\phi - \sum_{\psi,\psi(1)=a} z_\psi$$

holds. This implies

$$0 = \sum_{\phi,\phi(0)=a} z_\phi\{\infty,a\} - \sum_{\psi,\psi(1)=a} z_\psi\{\infty,a\} = \sum_{\phi,\phi(0)=a} z_\phi\{\infty,a\} + \sum_{\psi,\psi(1)=a} z_\psi\{a,\infty\},$$

where $\{\infty,a\}$ means a path from ∞ (as a cusp of $X_0(N)$) to a. One concludes:

$$\begin{aligned} x &= \sum_{a\in X_0(N)} \Big(\sum_{\phi,\phi(0)=a} z_\phi\phi + \sum_{\psi,\psi(1)=a} z_\psi\psi - \sum_{\eta,\eta(0)=\eta(1)=a} z_\eta\eta\Big) \\ &= \sum_{a\in X_0(N)} \Big(\sum_{\phi,\phi(0)=a} z_\phi(\phi+\{\infty,a\}) + \sum_{\psi,\psi(1)=a} z_\psi(\psi+\{a,\infty\}) \\ &- \sum_{\eta,\eta(0)=\eta(1)=a} z_\eta(\eta+\{\infty,a\}+\{a,\infty\})\Big). \end{aligned}$$

By composing the paths, one sees that all paths used have the endpoints in the cusps (in fact, equal to the image of ∞). If one lifts these paths to $\overline{\mathbb{H}}$, one obtains the desired surjectivity. □

Why are we computing $H_1(X_0(N),\mathbb{C})$? Because one has an isomorphism, the *Eichler-Shimura isomorphism*, of its dual to the holomorphic and anti-holomorphic modular forms!

2.1.3 Proposition. *The map*

$$\mathrm{S}_2(\Gamma_0(N)\,;\,\mathbb{C}) \oplus \overline{\mathrm{S}_2(\Gamma_0(N)\,;\,\mathbb{C})} \to H_1(X_0(N),\mathbb{C})^\vee,\ \ (f,g) \mapsto \big(\gamma \mapsto \int_\gamma f(z)dz + \int_\gamma g(z)d\overline{z}\big)$$

is an isomorphism. Under the identifications explained above, one may replace $H_1(X_0(N),\mathbb{C})^\vee$ by $\mathcal{CM}_2(\Gamma_0(N)\,;\,\mathbb{C})^\vee$. The map then becomes

$$(f,g) \mapsto \big(\{\alpha,\beta\} \mapsto \int_\alpha^\beta f(z)dz + \int_\alpha^\beta g(z)d\overline{z}\big)$$

where the integration path is along the geodesic from α to β.

Proof. This is a special case of the Eichler-Shimura isomorphism to be discussed later. The modern proof uses cohomology and the Hodge decomposition:

$$H_1(X_0(N),\mathbb{C})^\vee \cong H^1(X_0(N),\mathbb{C}) \cong H^1_{\mathrm{dR}}(X_0(N)) \cong H^0(X_0(N),\Omega^{\text{hol}}_{X_0(N)} \oplus \Omega^{\text{anti-hol}}_{X_0(N)}).$$

A proof in the language of Riemann surfaces can be found in several books. □

Let us recall that for $f \in \mathrm{S}_2(\Gamma_0(N)\,;\,\mathbb{C})$ and $M = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \mathrm{PGL}_2(\mathbb{Q})$ one puts $(f|M)(z) = f(Mz)\frac{\det(M)}{(cz+d)^2}$.

2.1.4 Definition. *Let p be a prime. Recall the set $\mathcal{R}_p$ from Equation 1.2. Recall also that the Hecke operator T_p for $f \in \mathrm{S}_2(\Gamma_0(N)\,;\,\mathbb{C})$ is*

$$(T_p f)(z) = \sum_{M\in\mathcal{R}_p} (f|M)(z).$$

We now define T_p on $\mathcal{CM}_2(\Gamma_0(N)\,;\,\mathbb{C})$ by

$$T_p\{\alpha,\beta\} = \sum_{M\in\mathcal{R}_p} M\{\alpha,\beta\} = \sum_{M\in\mathcal{R}_p} \{M\alpha, M\beta\}$$

which we extend linearly.

2.1.5 Proposition. *The Hecke operators are compatible with the isomorphism of Proposition 2.1.3.*

Proof. Let γ be a geodesic path from α to β. For $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ we have

$$\int_{M\gamma} f(z)dz = \int_\gamma f(Mz)d(Mz) = \int_\gamma f(Mz)\frac{\det(M)}{(cz+d)^2}dz = \int_\gamma (f|M)(z)dz,$$

whence the result. □

The idea of the modular symbols algorithm is to compute the Hecke algebra on modular symbols, which we have described explicitly above and which is suitable for an implementation on the computer. By the compatibility of the Eichler-Shimura isomorphism with the Hecke operators the Hecke algebra on modular symbols agrees with the one on modular forms! We have seen above that its knowledge is equivalent to the knowledge of the modular forms.

2.2 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's textbook [SteinBook], except that we do not factor out torsion, but intend a common treatment for all rings.

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. If $g \in \mathrm{PSL}_2(\mathbb{Z})$ is some element of finite order m, we denote by N_g the element $1 + g + \cdots + g^{m-1}$ of the group ring $R[\mathrm{PSL}_2(\mathbb{Z})]$. Similarly, if $H \leq \mathrm{PSL}_2(\mathbb{Z})$ is a finite subgroup, we write $N_H = \sum_{h\in H} h \in R[\mathrm{PSL}_2(\mathbb{Z})]$.

2.2.1 Definition. *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

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

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.

2.2.2 Exercise. *Let* R*,* Γ *and* V *as above and let* $R \to S$ *be a ring homomorphism. Then*

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

[Hint: Use that tensoring and taking coinvariants are both right exact.]

Manin symbols

Manin symbols provide an alternative description of formal modular symbols. We shall use this description for the comparison with the other kinds of modular symbols. We should also point out that Manin symbols are important for the implementations of the modular symbols formalism.

We stay in the general setting over a ring R.

As $\mathrm{PSL}_2(\mathbb{Z})$ is infinite, the induced module $R[\mathrm{PSL}_2(\mathbb{Z})]$ is not isomorphic to the coinduced one $\mathrm{Hom}_R(R[\mathrm{PSL}_2(\mathbb{Z})], R)$ and $R[\mathrm{PSL}_2(\mathbb{Z})]$ is not cohomologically trivial. However, the R-module $H^1_{\mathrm{par}}(\mathrm{PSL}_2(\mathbb{Z}), R[\mathrm{PSL}_2(\mathbb{Z})])$ is zero. This is the essence of the following proposition. (One need not understand that sentence at this point.)

2.2.3 Proposition. *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. We first use that $R[\mathrm{PSL}_2(\mathbb{Z})]$ is a cohomologically trivial module for both $\langle\sigma\rangle$ and $\langle\tau\rangle$. This gives

$$R[\mathrm{PSL}_2(\mathbb{Z})]N_\sigma = \ker_{R[\mathrm{PSL}_2(\mathbb{Z})]}(1-\sigma) = R[\mathrm{PSL}_2(\mathbb{Z})]^{\langle\sigma\rangle},$$

$$R[\mathrm{PSL}_2(\mathbb{Z})]N_\tau = \ker_{R[\mathrm{PSL}_2(\mathbb{Z})]}(1-\tau) = R[\mathrm{PSL}_2(\mathbb{Z})]^{\langle\tau\rangle},$$

$$R[\mathrm{PSL}_2(\mathbb{Z})](1-\sigma) = \ker_{R[\mathrm{PSL}_2(\mathbb{Z})]} N_\sigma \quad \text{and} \quad R[\mathrm{PSL}_2(\mathbb{Z})](1-\tau) = \ker_{R[\mathrm{PSL}_2(\mathbb{Z})]} N_\tau.$$

By Proposition B.6.1, 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 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. Note that instead of this explicit calculation we could also have appealed to Proposition 2.3.6.

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. □

2.2.4 Lemma. *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. □

2.2.5 Proposition. *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 2.2.3 and Lemma 2.2.4. □

We are now ready to prove the description of modular symbols in terms of Manin symbols.

2.2.6 Theorem. *Let $M = \mathrm{Ind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V)$, which we identify with $(R[\mathrm{PSL}_2(\mathbb{Z})] \otimes_R V)_\Gamma$. That module carries the right $R[\mathrm{PSL}_2(\mathbb{Z})]$-action $(h \otimes v)g = (hg \otimes v)$, and the Γ-coinvariants are taken for the diagonal left Γ-action. The following statements hold:*

(a) The homomorphism ϕ from Proposition 2.2.5 induces the exact sequence of R-modules

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

(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 2.2.5, 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 2.2.3. □

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

Let R be a ring. We put $V_n(R) = \mathrm{Sym}^n(R^2) \cong R[X,Y]_n$. By the latter 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

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

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

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

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 $(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right))^\iota \left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right)$ is equal to $(X,Y)\sigma^{-1}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\sigma$ (the isomorphism is given by $v \mapsto \sigma v$).

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.

2.2.7 Proposition. *Suppose that $n!$ is invertible in R. Then there is a perfect pairing*

$$V_n(R) \times V_n(R) \to R$$

of R-modules. It hence induces an isomorphism $V_n(R) \to V_n(R)^\vee$ of R-modules respecting the $\mathrm{Mat}_2(\mathbb{Z})_{\neq 0}$-action which is given on $V_n(R)^\vee$ by $(M.\phi)(w) = \phi(M^\iota w)$ for $M \in \mathrm{Mat}_2(\mathbb{Z})_{\neq 0}$, $\phi \in V_n(R)^\vee$ and $w \in V_n(R)$.

Proof. One defines the perfect pairing on $V_n(R)$ by first constructing a perfect pairing on R^2, which we consider as column vectors. One sets

$$R^2 \times R^2 \to R, \quad \langle v, w\rangle := \det(v|w) = v_1w_2 - v_2w_1.$$

If M is a matrix in $\mathrm{Mat}_2(\mathbb{Z})_{\neq 0}$, one checks easily that $\langle Mv, w\rangle = \langle v, M^\iota w\rangle$. This pairing extends naturally to a pairing on the n-th tensor power of R^2. Due to the assumption on the invertibility of $n!$, we may view $\mathrm{Sym}^n(R^2)$ as a submodule in the n-th tensor power, and hence obtain the desired pairing and the isomorphism of the statement. □

2.2.8 Lemma. *Let $n \geq 1$ be an integer, $t = \left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right)$ and $t' = \left(\begin{smallmatrix} 1 & 0 \\ N & 1 \end{smallmatrix}\right)$. 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 $V_n(R)^{\langle t'\rangle} = \langle Y^n\rangle$. 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 $V_n(R)_{\langle t'\rangle} = V_n(R)/\langle X^n, X^{n-1}Y, \ldots, XY^{n-1}\rangle$.*

Proof. The action of t is $t.(X^{n-i}Y^i) = X^{n-i}(NX+Y)^i$ and consequently $(t-1).(X^{n-i}Y^i) = \sum_{j=0}^{i-1} r_{i,j}X^{n-j}Y^j$ 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 $(t-1).x = \sum_{j=0}^{n-1} X^{n-j}Y^j(\sum_{i=j+1}^{n} a_i r_{i,j})$. 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. The claims on the coinvariants are proved in a very similar and straightforward way. □

2.2.9 Proposition. *Let $n \geq 1$ be an integer.*

(a) 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.

(b) If $n!N$ is invertible in R, then the R-module of $\Gamma(N)$-coinvariants $V_n(R)_{\Gamma(N)}$ is zero.

(c) Suppose that Γ is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ such that reduction modulo p defines a surjection $\Gamma \twoheadrightarrow \mathrm{SL}_2(\mathbb{F}_p)$ (e.g. $\Gamma(N)$, $\Gamma_1(N)$, $\Gamma_0(N)$ for $p \nmid N$). Suppose moreover that $1 \leq n \leq p$ if $p > 2$, and $n = 1$ if $p = 2$. Then one has $V_n(\mathbb{F}_p)^{\Gamma} = 0 = V_n(\mathbb{F}_p)_{\Gamma}$.

Proof. As $\Gamma(N)$ contains the matrices t and t', Lemma 2.2.8 already finishes Parts (a) and (b). The only part of (c) that is not yet covered is when the degree is $n = p > 2$. One has the exact sequence of Γ-modules $0 \to V_1(\mathbb{F}_p) \to V_p(\mathbb{F}_p) \to V_{p-2}(\mathbb{F}_p) \to 0$. Hence, it suffices to take invariants respectively coinvariants to obtain the result. □

Let now $\chi : \Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times \to R^\times$ be a character. By R^χ we denote the $R[\Gamma_0(N)]$-module which is defined to be R with $\Gamma_0(N)$-action through χ^{-1} (taking the inverse is not some amusement in making formulae more difficult, but arises from the fact that we want our modular symbols with character χ to match the definition in [SteinBook] (at least in most cases)).

We further let

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

equipped with the diagonal $\Gamma_0(N)$-action. Note that unfortunately this module is not an $\mathrm{SL}_2(\mathbb{Z})$-module any more, but we will not need that.

Since as $\Gamma_1(N)$-modules $V_n^\chi(R)$ and $V_n(R)$ are isomorphic, Proposition 2.2.9 also applies to $V_n^\chi(R)$. 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 $\Gamma_0(N) \to R^\times$. We impose that $\chi(-1) = (-1)^k$.

We define

$$\mathcal{M}_k(N,\chi\,;\,R) := \mathcal{M}_R(\Gamma_0(N)/\{\pm1\}, V_{k-2}^{\chi}(R)),$$

as well as similarly for the boundary and the cuspidal spaces. The natural action of the matrix $\eta = \left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$ gives an involution on all of these spaces. We will denote by the superscript $^+$ the subspace invariant under this involution, and by the superscript $^-$ the anti-invariant one.

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 [SteinBook], namely Theorem 8.2.2 (in the last version of [SteinBook] that I printed).

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.

2.2.10 Proposition. *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 $-1 \notin \Gamma_1(N)$. □

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 [SteinBook]. 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 [SteinBook].

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 1.2). 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.

I had wondered for a long time why Merel and Stein use their action on $V_n(R)$ (i.e. applying the Shimura main involution) and not the maybe more straight forward one. The answer becomes clear in the discussion of Hecke operators on group cohomology, where the main involution comes in quite naturally.

2.3 Group cohomological modular symbols

As in the section on the modular symbols formalism, we shall also base our group cohomological modular symbols on the group $\mathrm{PSL}_2(\mathbb{Z})$, rather than $\mathrm{SL}_2(\mathbb{Z})$, which simplifies the treatment, since $\mathrm{SL}_2(\mathbb{Z})$ has a very simple structure, namely as a free product of two cyclic groups.

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

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

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

One knows that $\mathrm{PSL}_2(\mathbb{Z})$ is the free product of the cyclic groups $\langle\sigma\rangle$ of order 2 and $\langle\tau\rangle$ of order 3. In other words, $\mathrm{PSL}_2(\mathbb{Z})$ has the presentation $\langle \sigma, \tau | \sigma^2 = \tau^3 = 1 \rangle$ as an abstract group.

In the following we will exploit the simplicity of this description. In fact, we have already used a consequence of the freeness (namely Proposition B.6.1) in our proof of the Manin symbols theorem.

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

We now apply the Mayer-Vietoris sequence (Prop. B.6.2) to our situation to get that for any ring R and any left $R[\mathrm{PSL}_2(\mathbb{Z})]$-module M the sequence

$$\begin{aligned} 0 \to M^{\mathrm{PSL}_2(\mathbb{Z})} \to M^{\langle\sigma\rangle} \oplus M^{\langle\tau\rangle} \to M \\ \to H^1(\mathrm{PSL}_2(\mathbb{Z}), M) \to H^1(\langle\sigma\rangle, M) \oplus H^1(\langle\tau\rangle, M) \to 0 \end{aligned} \quad (2.9)$$

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

$$H^i(\mathrm{PSL}_2(\mathbb{Z}), M) \cong H^i(\langle\sigma\rangle, M) \oplus H^i(\langle\tau\rangle, M). \tag{2.10}$$

2.3.1 Corollary. *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 $H^1(\Gamma, V) = M/(M^{\langle\sigma\rangle} + M^{\langle\tau\rangle})$ with $M = \mathrm{Coind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})}(V)$ and $H^i(\Gamma, V) = 0$ for all $i \geq 2$.*

Proof. For $x \in \mathbb{H}$ we denote by $\mathrm{PSL}_2(\mathbb{Z})_x$ the stabiliser subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ of the point x. The image of the $\mathrm{PSL}_2(\mathbb{Z})$-orbit of x in $\Gamma\backslash\mathbb{H}$ is in bijection with the double cosets $\Gamma\backslash\mathrm{PSL}_2(\mathbb{Z})/\mathrm{PSL}_2(\mathbb{Z})_x$ as follows

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

Moreover, the group $\Gamma \cap g\mathrm{PSL}_2(\mathbb{Z})_x g^{-1}$ equals Γ_{gx}, the stabiliser subgroup of Γ of the point gx. Thus, for all $i \in \mathbb{N}$, Mackey's formula (Prop. B.5.1) gives an isomorphism

$$H^i(\mathrm{PSL}_2(\mathbb{Z})_x, \mathrm{Coind}_\Gamma^{\mathrm{PSL}_2(\mathbb{Z})} V) \cong \prod_{y\in\Gamma\backslash\mathrm{PSL}_2(\mathbb{Z})x} H^i(\Gamma_y, V). \tag{2.11}$$

By Exercise 1.6.1, all non-trivial stabiliser groups for the action of $\mathrm{PSL}_2(\mathbb{Z})$ 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. B.3.1 that the groups in Equation 2.11 are zero. Hence, by Shapiro's lemma (Prop. B.4.1) and Equations (2.9) and (2.10) we obtain the proposition. □

By Exercise 1.6.1, the assumptions of the proposition are for instance always satisfied if R is a field of characteristic not 2 or 3. They also hold for $\Gamma_1(N)$ with $N \geq 4$ over any ring.

Definition of 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

$$0 \to H^1_{\mathrm{par}}(\Gamma, V) \to H^1(\Gamma, V) \xrightarrow{\mathrm{res}} \prod_{g\in\Gamma\backslash\mathrm{PSL}_2(\mathbb{Z})/\langle T\rangle} H^1(\Gamma \cap \langle gTg^{-1}\rangle, V). \tag{2.12}$$

2.3.2 Exercise. *Use Mackey's formula as in the proof of Corollary 2.3.1 to show that the definition of parabolic cohomology is compatible with Shapiro's lemma, i.e. that Equation (2.12) is isomorphic to*

$$0 \to H^1_{\mathrm{par}}(\mathrm{PSL}_2(\mathbb{Z}), M) \to H^1(\mathrm{PSL}_2(\mathbb{Z}), M) \xrightarrow{\mathrm{res}} H^1(\langle T\rangle, M) \tag{2.13}$$

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

2.3.3 Proposition. *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 left $R[\Gamma]$-modules V the sequence*

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

is exact.

Proof. Due to the assumptions we may apply Corollary 2.3.1. The restriction map in Equation (2.13) thus becomes

$$M/(M^{\langle\sigma\rangle} + M^{\langle\tau\rangle}) \xrightarrow{m\mapsto(1-\sigma)m} M/(1-T)M,$$

since $H^1(\langle T\rangle, M) \cong M/(1-T)M$ by Exercise B.2.1. Seeing M as $\mathrm{Hom}_\Gamma(R[\mathrm{PSL}_2(\mathbb{Z})], V)$ gives that the cokernel of this map, which one directly obtains as M_G (the G-coinvariants), are the constant functions to V^Γ, which are clearly isomorphic to V^Γ. □

Exact computation of cohomology of subgroups of $\mathrm{PSL}_2(\mathbb{Z})$

We have already seen how to use the Mayer-Vietoris sequence (Proposition 2.9) to compute the cohomology of subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ of finite index, if we allow some rather weak conditions on the invertiblity of stabiliser orders in the base ring.

For the course we will not need the present section, but it is included since it gives an explicit description of the cohomology of $\mathrm{PSL}_2(\mathbb{Z})$ over any ring, even in the presence of non-trivial stabilisers. Moreover, it illustrates that already from the definition of group cohomology in terms of cochains, one can get a Manin symbols like statement.

Let us recall some notation. We let R be a ring. If $g \in \mathrm{PSL}_2(\mathbb{Z})$ is some element of finite order m, we denote by N_g the element $1 + g + \cdots + g^{m-1}$ of the group ring $R[\mathrm{PSL}_2(\mathbb{Z})]$. Similarly, if $H \leq \mathrm{PSL}_2(\mathbb{Z})$ is a finite subgroup, we write $N_H = \sum_{h\in H} h \in R[\mathrm{PSL}_2(\mathbb{Z})]$.

2.3.4 Proposition. *Let M be a left $R[\mathrm{PSL}_2(\mathbb{Z})]$-module. Then the sequence of R-modules*

$$0 \to M^{\mathrm{PSL}_2(\mathbb{Z})} \to M \to \ker_M N_\sigma \times \ker_M N_\tau \to H^1(\mathrm{PSL}_2(\mathbb{Z}), M) \to 0$$

is exact.

Proof. We determine the 1-cocycles of M. Apart from $f(1) = 0$, they must satisfy

$$0 = f(\sigma^2) = \sigma f(\sigma) + f(\sigma) = N_\sigma f(\sigma) \text{ and}$$

$$0 = f(\tau^n) = \cdots = N_\tau f(\tau).$$

Since these are the only relations in $\mathrm{PSL}_2(\mathbb{Z})$, a cocycle is uniquely given by the choices

$$f(\sigma) \in \ker_M N_\sigma \text{ and } f(\tau) \in \ker_M N_\tau.$$

The 1-coboundaries are precisely the cocycles f which satisfy $f(\sigma) = (1-\sigma)m$ and $f(\tau) = (1-\tau)m$ for some $m \in M$. This proves

$$H^1(\mathrm{PSL}_2(\mathbb{Z}), M) \cong (\ker_M N_\sigma \times \ker_M N_\tau)/\big(((1-\sigma)m, (1-\tau)m) \mid m \in M\big).$$

Rewriting yields the proposition. □

2.3.5 Remark. *As* $\mathrm{PSL}_2(\mathbb{Z})_\infty = \langle T\rangle < \mathrm{PSL}_2(\mathbb{Z})$ *is infinite cyclic, one has by Exercise B.2.1 that* $H^1(\mathrm{PSL}_2(\mathbb{Z})_\infty, \mathrm{Res}^{\mathrm{PSL}_2(\mathbb{Z})_\infty}_{\mathrm{PSL}_2(\mathbb{Z})} M) \cong M/(1-T)M$.

An explicit presentation of the parabolic group cohomology is the following.

2.3.6 Proposition. *The parabolic group cohomology group sits in the exact sequence*

$$0 \to M^{\langle T\rangle}/M^{\mathrm{PSL}_2(\mathbb{Z})} \to \ker_M N_\sigma \cap \ker_M N_\tau \xrightarrow{\phi} H^1_{\mathrm{par}}(\mathrm{PSL}_2(\mathbb{Z}), M) \to 0,$$

where ϕ *maps an element* m *to the* 1*-cocycle* f *uniquely determined by* $f(\sigma) = f(\tau) = m$.

Proof. Using Proposition 2.3.4, we have the exact commutative diagram

$$\begin{array}{ccccc}
M^{\langle T\rangle}/M^{\mathrm{PSL}_2(\mathbb{Z})} & \xrightarrow{(\sigma^{-1}-1)} & \ker N_\sigma \cap \ker N_\tau & \longrightarrow & H^1_{\mathrm{par}}(\mathrm{PSL}_2(\mathbb{Z}), M) \\
\downarrow{\scriptstyle \sigma^{-1}} & & \downarrow & & \downarrow \\
M/M^{\mathrm{PSL}_2(\mathbb{Z})} & \xrightarrow{(1-\sigma, 1-\tau)} & \ker N_\sigma \times \ker N_\tau & \twoheadrightarrow & H^1(\mathrm{PSL}_2(\mathbb{Z}), M) \\
\downarrow{\scriptstyle (1-T)\sigma} & & \downarrow{\scriptstyle (a,b)\mapsto b-a} & & \downarrow \\
(1-T)M & \hookrightarrow & M & \twoheadrightarrow & H^1(\mathrm{PSL}_2(\mathbb{Z})_\infty, M).
\end{array}$$

As the bottom left vertical arrow is surjective, the claim follows from the snake lemma. □

Hecke operators

Hecke operators conceptually come from Hecke correspondences on modular curves. It is quite easily checked that the treatment of Hecke operators on group cohomology to be given here, coincides with the one coming from the Hecke correspondences on complex modular curves (at least, when there are no non-trivial stabilisers, i.e. for the group $\Gamma_1(N)$ with $N \geq 5$), see e.g. [Diamond-Im], 3.2 and 7.3. For the description here, we follow [Diamond-Im] 12.4.

Let $N \geq 1$. We define the following two sets (for $n \neq 0$):

$$\Delta_0^n(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) | a, b, c, d \in \mathbb{Z}, (a, N) = 1, c \equiv 0 \bmod N, \det \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = n\} \tag{2.14}$$

$$\Delta_1^n(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) | a, b, c, d \in \mathbb{Z}, a \equiv 1 \bmod N, c \equiv 0 \bmod N, \det \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = n\} \tag{2.15}$$

We now let $\Gamma := \Gamma_1(N)$ and $\Delta^p := \Delta_1^p(N)$ or $\Gamma := \Gamma_0(N)$ and $\Delta^p := \Delta_0^p(N)$. We also 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 $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^\iota = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$.

Let $\alpha \in \Delta$. We use the notations $\Gamma_\alpha := \Gamma \cap \alpha^{-1}\Gamma\alpha$ and $\Gamma^\alpha := \Gamma \cap \alpha\Gamma\alpha^{-1}$, where we consider α^{-1} as an element of $\mathrm{GL}_2(\mathbb{Q})$. Both groups are commensurable with Γ.

The *Hecke operator* T_α acting on group cohomology is the composite

$$H^1(\Gamma, V) \xrightarrow{\mathrm{res}} H^1(\Gamma^\alpha, V) \xrightarrow{\mathrm{conj}_\alpha} H^1(\Gamma_\alpha, V) \xrightarrow{\mathrm{cores}} H^1(\Gamma, V).$$

The first map is the usual *restriction*, and the third one is the so-called *corestriction*, which one also finds in the literature under the name *transfer*. We explicitly describe the second map on non-homogeneous cocycles (cf. [Diamond-Im], p. 116):

$$\mathrm{conj}_\alpha : H^1(\Gamma^\alpha, V) \to H^1(\Gamma_\alpha, V), \;\; c \mapsto \big(g_\alpha \mapsto \alpha^\iota.c(\alpha g_\alpha \alpha^{-1})\big).$$

There is a similar description on the parabolic subspace and the two are compatible. The following formula can also be found in [Diamond-Im], p. 116, and [Shimura], Section 8.3.

2.3.7 Proposition. *Suppose that $\Gamma\alpha\Gamma = \bigcup_{i=1}^n \Gamma\delta_i$ is a disjoint union. Then the Hecke operator T_α acts on $H^1(\Gamma, V)$ and $H^1_{\mathrm{par}}(\Gamma, V)$ by sending the non-homogeneous cocyle c to $T_\alpha c$ defined by*

$$(T_\alpha c)(g) = \sum_{i=1}^n \delta_i^\iota c(\delta_i g \delta_{j(i)}^{-1})$$

for $g \in \Gamma$. Here $j(i)$ is the index such that $\delta_i g \delta_{j(i)}^{-1} \in \Gamma$.

Proof. We only have to describe the corestriction explicitly. For that we notice that one has $\Gamma = \bigcup_{i=1}^n \Gamma_\alpha g_i$ with $\alpha g_i = \delta_i$. Furthermore the corestriction of a non-homogeneous cocycle $u \in H^1(\Gamma_\alpha, V)$ is the cocycle $\mathrm{cores}(u)$ uniquely given by

$$\mathrm{cores}(u)(g) = \sum_{i=1}^n g_i^{-1} u(g_i g g_{j(i)}^{-1})$$

for $g \in \Gamma$. Combining with the explicit description of the map conj_α yields the result. □

For a positive integer n, the *Hecke operator* T_n is defined as $\sum_\alpha T_\alpha$, where the sum runs through a system of representatives of the double cosets $\Gamma\backslash\Delta^n/\Gamma$.

2.3.8 Exercise. *Let p be a prime. Prove that $\Delta^p = \Gamma \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma$ and that $\mathcal{R}_p$ is a system of representatives of $\Gamma\backslash\Delta^p$. ($\mathcal{R}_p$ was defined in Equation 1.2.)*

Let a be an integer coprime to N. The *diamond operator* $\langle a \rangle$ is defined as T_α for the matrix $\sigma_a \in \Gamma_0(N)$, defined in Equation 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 can be checked that the Hecke and diamond operators satisfy the "usual" Euler product and one has the formulae $T_n T_m = T_{nm}$ for any pair of coprime integers n, m and $T_{p^{r+1}} = T_{p^r} T_p - p^{k-1}\langle p \rangle T_{p^{r-1}}$ if $p \nmid N$, and $T_{p^{r+1}} = T_{p^r} T_p$ if $p \mid N$.

Finally, we should mention that the definition of Hecke operators is compatible under Shapiro's Lemma. This was first proved by [AshStevens].

Group cohomological modular symbols

The group cohomological modular symbols that we will be interested in are, of course, those arising in the Eichler-Shimura theorem (see Theorem 3.1.1).

Let R be a ring, $k \geq 2$, $N \geq 1$ integers, $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to R^\times$ a character.

The *group cohomological modular symbols of weight k, level N for the character χ over the ring R* are defined to be

$$H^1(\Gamma_0(N), V_{k-2}^\chi(R)).$$

Their *cusp space* is defined to be

$$H^1_{\mathrm{par}}(\Gamma_0(N), V_{k-2}^\chi(R)).$$

For our treatment of Hecke operators to make sense, we must still say how we see $V_{k-2}^\chi(R)$ as a $\Delta_0^n(N)$-module. We just extend the alternative description of the character $\chi : \Gamma_0(N)/\Gamma_1(N) \to R$ given by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \chi(a)$ to $\chi : \Delta_0^n(N) \to R$ given by the same formula. Accordingly, we extend the $\Gamma_0(N)$ action on R^χ to a $\Delta_0^n(N)$-action, so that $V_{k-2}^\chi(R) = V_{k-2}(R) \otimes_R R^\chi$ is also a $\Delta_0^n(N)$-module.

Torsion in group cohomological modular symbols

Herremans has computed a torsion-freeness result like the following proposition in [Herremans], Proposition 9. Here we give a short and conceptual proof of a slightly more general statement. The way of approach was suggested by Bas Edixhoven. This is one of the poitns where the cohomological machinery becomes really handy. Herremans worked with formal modular symbols, so his proof is much more difficult (to my mind).

2.3.9 Proposition. *Let R be an integral domain of characteristic 0 having a principal maximal ideal $\mathfrak{m} = (\pi)$ with residue field $\mathbb{F}$ of characteristic p. Let $N \geq 1$ and $k \geq 2$ be integers such that the orders of the stabiliser subgroups of $\Gamma_0(N)$ for $x \in \mathbb{H}$ have order coprime to p (see Exercise 1.6.3). We also let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to R^\times$ be a character with $\chi(-1) = (-1)^k$. We denote by $\overline{\chi}$ the composition of χ with the natural projection $R \to \mathbb{F}$. Then the following statements hold:*

(a) $H^1(\Gamma_0(N), V_{k-2}^\chi(R)) \otimes_R \mathbb{F} \cong H^1(\Gamma_0(N), V_{k-2}^{\overline{\chi}}(\mathbb{F}))$.

(b) If $k = 2$, then $H^1(\Gamma_0(N), V_{k-2}^\chi(R))[\pi] = 0$. If $k \geq 3$, then

$$H^1(\Gamma_0(N), V_{k-2}^\chi(R))[\pi] = V_{k-2}^{\overline{\chi}}(\mathbb{F})^{\Gamma_0(N)}.$$

In particular, if $p \nmid N$, then $H^1(\Gamma_0(N), V_{k-2}^\chi(R))[\pi] = 0$ for all $k \in \{2, \ldots, p+2\}$.

(c) If $k = 2$, or if $k \in \{3, \ldots, p+2\}$ and $p \nmid N$, then

$$H^1_{\mathrm{par}}(\Gamma_0(N), V_{k-2}^\chi(R)) \otimes_R \mathbb{F} \cong H^1_{\mathrm{par}}(\Gamma_0(N), V_{k-2}^{\overline{\chi}}(\mathbb{F})).$$

Proof. Let us first notice that the sequence

$$0 \to V_{k-2}^\chi(R) \xrightarrow{\cdot\pi} V_{k-2}^\chi(R) \to V_{k-2}^{\overline{\chi}}(\mathbb{F}) \to 0$$

of $R[\Gamma_0(N)]$-modules is exact. The associated long exact sequence gives rise to the short exact sequence

$$0 \to H^i(\Gamma_0(N), V_{k-2}^{\chi}(R)) \otimes \mathbb{F} \to H^i(\Gamma_0(N), V_{k-2}^{\overline{\chi}}(\mathbb{F})) \to H^{i+1}(\Gamma_0(N), V_{k-2}^{\chi}(R))[\pi] \to 0$$

for every $i \geq 0$. Exploiting this sequence for $i = 1$ immediately yields Part (a), since any H^2 of $\Gamma_0(N)$ is zero by Corollary 2.3.1. Part (b) is a direct consequence of the case $i = 0$ and Proposition 2.2.9.

We have the exact commutative diagram

$$\begin{array}{ccccccc}
0 & \to & H^1(\Gamma_0(N), V_{k-2}^{\chi}(R)) & \xrightarrow{\cdot\pi} & H^1(\Gamma_0(N), V_{k-2}^{\chi}(R)) & \to & H^1(\Gamma_0(N), V_{k-2}^{\overline{\chi}}(\mathbb{F})) \to 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \prod_g H^1(D_g, V_{k-2}^{\chi}(R)) & \xrightarrow{\cdot\pi} & \prod_g H^1(D_g, V_{k-2}^{\chi}(R)) & \to & \prod_g H^1(D_g, V_{k-2}^{\overline{\chi}}(\mathbb{F})) \to 0 \\
 & & \downarrow & & \downarrow & & \\
 & & (V_{k-2}^{\chi}(R))^{\Gamma_0(N)} & \xrightarrow{\cdot\pi} & (V_{k-2}^{\chi}(R))^{\Gamma_0(N)} & & \\
 & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & &
\end{array}$$

where the products are taken over $g \in \Gamma_0(N)\backslash \mathrm{PSL}_2(\mathbb{Z})/\langle T \rangle$, and $D_g = \Gamma_0(N) \cap \langle gTg^{-1} \rangle$. The exactness of the first row is the contents of Parts (a) and (b). That the columns are exact follows from Proposition 2.3.3. The zero on the right of the second row is due to the fact that D_g is free on one generator (see Exercise B.1.1). That generator is of the form $g \left(\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right) g^{-1}$ with $r \mid N$, so that r is invertible in $\mathbb{F}$. The zero on the left is trivial for $k = 2$ and for $3 \leq k \leq p + 2$ it is a consequence of Lemma 2.2.8. Part (c) now follows from the snake lemma, since by Proposition 2.2.9 the lower row is zero. □

2.4 Geometric cohomological modular symbols

In this section we give a brief introduction to "geometric cohomological modular symbols", without proving any results.

We 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. Denote by $\mathcal{C}$ either $\mathbb{H}$ or $\overline{\mathbb{H}}$, by X the quotient space Y_Γ respectively X_Γ, and by π the quotient map $\mathcal{C} \to X$.

Let $\underline{V}$ be the constant sheaf on $\mathcal{C}$ associated to V together with its natural Γ-action, i.e. for an open set $U \subset \mathcal{C}$ we let $\underline{V}(U) = \mathrm{Hom}_{\mathrm{cts}}(U, V)$ (equipping V with the discrete topology) together with isomorphisms $\phi_g : \underline{V} \to g_*\underline{V}$ for each $g \in \Gamma$ which on U are given by

$$\mathrm{Hom}_{\mathrm{cts}}(U, V) \to \mathrm{Hom}_{\mathrm{cts}}(gU, V), \quad f \mapsto (gu \mapsto gf(u)\ \forall u \in U).$$

We have that $\pi_*\underline{V}$ is a sheaf on X of $R[\Gamma]$-modules and the Γ-action from geometry agrees with the one on the module. We let $(\pi_*\underline{V})^\Gamma$ to be the sheaf

$$U \mapsto (\pi_*\underline{V}(U))^\Gamma = \left(\underline{V}(\pi^{-1}(U))\right)^\Gamma.$$

Suppose now that there is no non-trivially stabilised point of $\mathcal{C}$ for the action of Γ. In that case, the sheaf $\pi_*\underline{V}$ is easily seen to be locally constant. In that case, one can check that

$$H^i(\Gamma, V) \cong H^i(Y_\Gamma, (\pi_*\underline{V})^\Gamma). \tag{2.16}$$

In the general setting, the following theorem is proved in [W2], Theorems 5.7 and 5.9, using methods from homological algebra.

2.4.1 Theorem. *Let M denote the coinduced module $\mathrm{Coind}_\Gamma^G(V)$. We have the two exact sequence:*

$$0 \to H^1(Y_\Gamma, (\pi_* \underline{V})^\Gamma) \to H^1(\Gamma, V) \to H^1(\langle\sigma\rangle, M) \oplus H^1(\langle\tau\rangle, M)$$

and

$$0 \to H^1(X_\Gamma, (\pi_* \underline{V})^\Gamma) \to H^1(\Gamma, V) \to H^1(\langle\sigma\rangle, M) \oplus H^1(\langle\tau\rangle, M) \oplus H^1(\langle T\rangle, M).$$

2.4.2 Corollary. *We have the explicit descriptions:*

$$H^1(Y_\Gamma, (\pi_* \underline{V})^\Gamma) \cong M/\big(M^{\langle\sigma\rangle} + M^{\langle\tau\rangle}\big)$$

and

$$H^1_{\mathrm{par}}(Y_\Gamma, (\pi_* \underline{V})^\Gamma) \cong \ker\big(M/(M^{\langle\sigma\rangle} + M^{\langle\tau\rangle}) \xrightarrow{1-\sigma} M/(1-T)M\big).$$

Proof. It suffices to compare the exact sequences of Theorem 2.4.1 with the Mayer-Vietoris exact sequence (Equation 2.9). □

2.5 Comparing the different types of modular symbols

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.

2.5.1 Theorem. *Suppose that the orders of all stabliser subgroups of Γ for the action on $\mathbb{H}$ are invertible in R. Then we have isomorphisms (which respect the Hecke operators in the cases for which we defined them):*

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

and

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

Proof. This follows immediately from comparing the Manin symbols description of modular symbols (Theorem 2.2.6) with the Mayer-Vietoris exact sequence (Equation 2.9) and Shapiro's Lemma. □

The precise differences between the spaces of modular symbols are computed in the following theorem. We assume the notations from the previous section.

2.5.2 Theorem. *The following sequences are exact:*

(a) $0 \to H^1(Y_\Gamma, (\pi_* \underline{V})^\Gamma) \to H^1(\Gamma, V) \to \prod_{x \in Y_\Gamma} H^1(\Gamma_{y_x}, V)$,

(b) $0 \to H^1_{\mathrm{par}}(Y_\Gamma, (\pi_* \underline{V})^\Gamma) \to H^1_{\mathrm{par}}(\Gamma, V) \to \prod_{x \in Y_\Gamma} H^1(\Gamma_{y_x}, V)$,

(c) $\prod_{x\in Y_\Gamma}\left(V^{\Gamma_{y_x}}/N_{\Gamma_{y_x}}V\right)\to\mathcal{M}_R(\Gamma,V)\to H^1(Y_\Gamma,(\pi_*\underline{V})^\Gamma)\to 0$,

(d) $\prod_{x\in Y_\Gamma}\left(V^{\Gamma_{y_x}}/N_{\Gamma_{y_x}}V\right)\to\mathcal{CM}_R(\Gamma,V)\to H^1_{\mathrm{par}}(Y_\Gamma,(\pi_*\underline{V})^\Gamma)\to 0$,

where for all $x\in Y_\Gamma$ *we have chosen* $y_x\in\mathbb{H}$ *such that* $\pi(y_x)=x$.

Proof. Via an identification between the induced and the coinduced module, this follows from Corollary 2.4.2 and Theorems 2.4.1 and 2.2.6 together with Mackey's formula and Shapiro's Lemma. □

2.5.3 Corollary. *Let* $R=\mathbb{Z}$. *The* $\mathbb{Z}$*-modules* $H^1(\Gamma,V)$, $H^1(Y_\Gamma,(\pi_*\underline{V})^\Gamma)$ *and* $\mathcal{M}_\mathbb{Z}(\Gamma,V)$ *only differ by torsion. The same statement holds for the* $\mathbb{Z}$*-modules* $H^1_{\mathrm{par}}(\Gamma,V)$, $H^1_{\mathrm{par}}(Y_\Gamma,(\pi_*\underline{V})^\Gamma)$ *and* $\mathcal{CM}_\mathbb{Z}(\Gamma,V)$. □

2.5.4 Corollary. *We now suppose that the order of* Γ_x *is invertible in* R *for all* $x\in\mathbb{H}$. *Then there are isomorphisms*

$$H^1(\Gamma,V)\cong H^1(Y_\Gamma,(\pi_*\underline{V})^\Gamma)\cong\mathcal{M}_R(\Gamma,V)$$

and

$$H^1_{\mathrm{par}}(\Gamma,V)\cong H^1_{\mathrm{par}}(Y_\Gamma,(\pi_*\underline{V})^\Gamma)\cong\mathcal{CM}_R(\Gamma,V).$$

The statements hold, in particular, for the group $\Gamma_1(N)$ *with* $N\geq 4$.

Proof. This follows from Theorem 2.5.2. We have already seen part of it in Theorem 2.5.1. For the last part we use that under the condition $N\geq 4$ all $\Gamma_1(N)_x$ are trivial by Exercise 1.6.2. □

We point the reader to Exercises 1.6.3. in order to see in which cases the assumptions of the previous corollary hold for the group $\Gamma_0(N)$.

3 Computing Modular Forms mod p

Throughout this section, we let, as before, $k\geq 2$, $N\geq 1$, p a prime, and $\chi:(\mathbb{Z}/N\mathbb{Z})^\times\to\mathbb{C}^\times$ a character. Further we let $\mathcal{O}=\mathbb{Z}[\chi]$, $\mathfrak{P}$ a prime of $\mathcal{O}$ above p, $\mathbb{F}$ the residue field, $\widehat{\mathcal{O}}$ the completion of $\mathcal{O}$ at $\mathfrak{P}$, as well as K the field of fractions of $\widehat{\mathcal{O}}$.

Notation for Hecke algebras

Let R be a ring, $S\subset R$ a subring and M an R-module on which Hecke operators and diamond operators act. We denote by $\mathbb{T}_S(M)$ the sub-S-algebra of the endomorphism ring $\mathrm{End}_R(M)$ generated by the Hecke and the diamond operators. If $S\to S'$ is a ring homomorphism, we use the notation $\mathbb{T}_{S'}(M)=\mathbb{T}_S(M)\otimes_S S'$.

This notation agrees with the previous one used for modular forms.

3.1 The Eichler-Shimura theorem

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

(a) $\mathrm{M}_k(N,\chi\,;\,\mathbb{C}))\oplus \mathrm{S}_k(N,\chi\,;\,\mathbb{C})^\vee \cong H^1(\Gamma_0(N),V_{k-2}^\chi(\mathbb{C}))\cong \mathcal{M}_k(N,\chi\,;\,\mathbb{C})$,

(b) $\mathrm{S}_k(N,\chi\,;\,\mathbb{C}))\oplus \mathrm{S}_k(N,\chi\,;\,\mathbb{C})^\vee \cong H^1_{\mathrm{par}}(\Gamma_0(N),V_{k-2}^\chi(\mathbb{C}))\cong \mathcal{CM}_k(N,\chi\,;\,\mathbb{C})$,

(c) $\mathrm{S}_k(N,\chi\,;\,\mathbb{C})\cong H^1_{\mathrm{par}}(\Gamma_0(N),V_{k-2}^\chi(\mathbb{C}))^+\cong \mathcal{CM}_k(N,\chi\,;\,\mathbb{C})^+$.

Proof. The first isomorphisms of Parts (a) and (b) are [Diamond-Im], Theorem 12.2.2. Via the comparison, Theorem 2.5.1, we obtain the second isomorphisms. As the space of anti-holomorphic cusp forms is dual to the space of holomorphic cusp forms, Part (c) is a direct consequence of (b). □

We may rephrase the Eichler-Shimura theorem as follows.

3.1.2 Corollary. *(a) The Hecke algebras* $\mathbb{T}_{\mathcal{O}}(\mathrm{M}_k(N,\chi\,;\,\mathbb{C}))$, $\mathbb{T}_{\mathcal{O}}(\mathcal{M}_k(N,\chi\,;\,\mathbb{C}))$ *are isomorphic.*

(b) The Hecke algebras $\mathbb{T}_{\mathcal{O}}(\mathrm{S}_k(N,\chi\,;\,\mathbb{C}))$, $\mathbb{T}_{\mathcal{O}}(\mathcal{CM}_k(N,\chi\,;\,\mathbb{C}))$ *and* $\mathbb{T}_{\mathcal{O}}(\mathcal{CM}_k(N,\chi\,;\,\mathbb{C})^+)$ *are isomorphic.* □

3.2 Comparing Hecke algebras over $\mathbb{F}$

From Exercise 2.2.2 one deduces a natural surjection

$$\mathbb{T}_{\mathcal{O}}(\mathcal{M}_k(N,\chi\,;\,\mathcal{O}))\otimes_{\mathcal{O}}\mathbb{F}\twoheadrightarrow \mathbb{T}_{\mathbb{F}}(\mathcal{M}_k(N,\chi\,;\,\mathbb{F})). \tag{3.17}$$

One way to think about this map is as reducing matrices with entries in $\mathcal{O}$ modulo $\mathfrak{P}$. In the same way, one also obtains from Corollary 3.1.2

$$\mathbb{T}_{\mathcal{O}}(\mathcal{M}_k(N,\chi\,;\,\mathcal{O}))\twoheadrightarrow \mathbb{T}_{\mathcal{O}}(\mathcal{M}_k(N,\chi\,;\,\mathcal{O})/\text{torsion})\cong \mathbb{T}_{\mathcal{O}}(\mathrm{M}_k(N,\chi\,;\,\mathbb{C})). \tag{3.18}$$

Similar statements hold for the cuspidal subspace.

Later on, we shall give a criterion to determine during the calculation of $\mathbb{T}_{\mathbb{F}}(\mathcal{CM}_k(N,\chi\,;\,\mathbb{F}))$ whether Equation 3.17 is an isomorphism, from which one then deduces via Equation 3.18 a relation to the Hecke algebra of cusp forms modulo p.

We call a maximal prime $\mathfrak{m}$ of $\mathbb{T}_{\mathcal{O}}(\mathcal{M}_k(N,\chi\,;\,\mathcal{O}))\otimes_{\mathcal{O}}\widehat{\mathcal{O}}$ (respectively the corresponding prime of $\mathbb{T}_{\mathcal{O}}(\mathcal{M}_k(N,\chi\,;\,\mathcal{O}))\otimes_{\mathcal{O}}\mathbb{F}$) *non-torsion* if

$$\mathcal{M}_k(N,\chi\,;\,\widehat{\mathcal{O}}))_{\mathfrak{m}}\cong(\mathcal{M}_k(N,\chi\,;\,\widehat{\mathcal{O}})/\text{torsion})_{\mathfrak{m}}.$$

Equivalently, we have that Equation 3.18 becomes

$$\mathbb{T}_{\mathcal{O}}(\mathcal{M}_k(N,\chi\,;\,\mathcal{O}))_{\mathfrak{m}}\twoheadrightarrow \mathbb{T}_{\mathcal{O}}(\mathcal{M}_k(N,\chi\,;\,\mathcal{O})/\text{torsion})_{\mathfrak{m}}\cong \mathbb{T}_{\mathcal{O}}(\mathrm{M}_k(N,\chi\,;\,\mathbb{C}))_{\mathfrak{m}}. \tag{3.19}$$

Another equivalent condition is that the height of $\mathfrak{m}$ is 1.

We recall that we have listed cases of the absence of torsion in the discussion of group cohomological modular symbols. Via the comparison (Theorem 2.5.1) we see that in many cases all primes are non-torsion.

Even if Equation 3.17 is not an isomorphism, we can still use $\mathcal{M}_k(N, \chi\,;\, \mathbb{F})$ for the computation of the coefficients of all eigenforms mod p.

3.2.1 Proposition. *(a) Let $f \in \mathrm{M}_k(N, \overline{\chi}\,;\, \overline{\mathbb{F}})$ be a normalised eigenform. Then there exists an $x \neq 0$ in $\mathcal{M}_k(N, \overline{\chi}\,;\, \mathbb{F})$ such that $T_n x = a_n(f)x$ for all n.*

(b) Let $\mathfrak{m}$ be a non-torsion maximal ideal of $\mathbb{T}_{\mathbb{F}}(\mathcal{M}_k(N, \overline{\chi}\,;\, \mathbb{F}))$ and $0 \neq x \in \mathcal{M}_k(N, \overline{\chi}\,;\, \overline{\mathbb{F}})$ such that $T_n x = a_n(f)x$ for all n and certain $\lambda_n \in \overline{\mathbb{F}}$. Then there exists a normalised eigenform $f \in \mathrm{M}_k(N, \overline{\chi}\,;\, \overline{\mathbb{F}})$ such that $a_n(f) = \lambda_n$ for all n.

Proof. The systems of eigenvalues for the action of the Hecke operators T_n on the non-torsion part of $\mathcal{M}_k(N, \chi\,;\, \mathbb{C})_{\mathfrak{m}}$ agree by Equation 3.18 with the systems of eigenvalues on $\mathrm{M}_k(N, \chi\,;\, \mathbb{C})_{\mathfrak{m}}$. Due to

$$\mathcal{M}_k(N, \chi\,;\, \mathcal{O})_{\mathfrak{m}} \otimes_{\mathcal{O}} \mathbb{F} \cong \mathcal{M}_k(N, \overline{\chi}\,;\, \mathbb{F})_{\mathfrak{m}}$$

(see Exercise 2.2.2) both parts follow. □

3.3 The Sturm bound

In this section we state the so called *Sturm bound* (also called *Hecke bound*), which gives the best known a priori upper bound for how many Hecke operators are needed to generate all the Hecke algebra. We only need it in our algorithm in cases in which it is theoretically not known that the stop criterion which we will discuss below is always reached. This will enable the algorithm to detect if the Hecke algebra on modular symbols is not isomorphic to the corresponding one on cuspidal modular forms.

3.3.1 Proposition. (Sturm bound) *The Hecke algebra $\mathbb{T}_{\mathbb{C}}(S_k(N, \chi\,;\, \mathbb{C}))$ can be generated as an algebra by the Hecke operators T_p for all primes p smaller than or equal to $\frac{kN}{12} \prod_{l|N, l \text{ prime}}(1 + \frac{1}{l})$.*

Proof. This is discussed in detail in Chapter 11 of [SteinBook]. □

3.4 The stop criterion

This section is based on the preprint [KW], which is joint work with Lloyd Kilford.

Algebraic preparation

3.4.1 Proposition. *Assume the set-up of Proposition 1.3.2 and let M, N be $\mathbb{T}$-modules which as $\mathcal{O}$-modules are free of finite rank. Suppose that*

(a) $M \otimes_{\mathcal{O}} \mathbb{C} \cong N \otimes_{\mathcal{O}} \mathbb{C}$ *as* $\mathbb{T} \otimes_{\mathcal{O}} \mathbb{C}$*-modules, or*

(b) $M \otimes_{\mathcal{O}} \bar{K} \cong N \otimes_{\mathcal{O}} \bar{K}$ *as* $\mathbb{T} \otimes_{\mathcal{O}} \bar{K}$*-modules.*

Then for all prime ideals $\mathfrak{m}$ *of* $\mathbb{T}_{\mathbb{F}}$ *corresponding to height* 1 *primes of* $\mathbb{T}_{\widehat{\mathcal{O}}}$ *the equality*

$$\dim_{\mathbb{F}}(M \otimes_{\mathcal{O}} \mathbb{F})_{\mathfrak{m}} = \dim_{\mathbb{F}}(N \otimes_{\mathcal{O}} \mathbb{F})_{\mathfrak{m}}$$

holds.

Proof. As for $\mathbb{T}$, we also write M_K for $M \otimes_{\mathcal{O}} K$ and similarly for N and $\widehat{\mathcal{O}}$, $\mathbb{F}$, etc. By choosing an isomorphism $\mathbb{C} \cong \bar{K}$, it suffices to prove Part (b). Using Proposition 1.3.2, Part (d), the isomorphism $M \otimes_{\mathcal{O}} \bar{K} \cong N \otimes_{\mathcal{O}} \bar{K}$ can be rewritten as

$$\bigoplus_{\mathfrak{p}} (M_{K,\mathfrak{p}^e} \otimes_K \bar{K}) \cong \bigoplus_{\mathfrak{p}} (N_{K,\mathfrak{p}^e} \otimes_K \bar{K}),$$

where the sums run over the minimal primes $\mathfrak{p}$ of $\mathbb{T}_{\widehat{\mathcal{O}}}$ which are properly contained in a maximal prime. Hence, an isomorphism $M_{K,\mathfrak{p}^e} \otimes_K \bar{K} \cong N_{K,\mathfrak{p}^e} \otimes_K \bar{K}$ exists for each $\mathfrak{p}$. Since for each maximal ideal $\mathfrak{m}$ of $\mathbb{T}_{\widehat{\mathcal{O}}}$ of height 1 we have by Proposition 1.3.2

$$M_{\widehat{\mathcal{O}},\mathfrak{m}} \otimes_{\widehat{\mathcal{O}}} K \cong \bigoplus_{\mathfrak{p} \subseteq \mathfrak{m} \text{ min.}} M_{K,\mathfrak{p}^e}$$

and similarly for N, we get

$$\begin{aligned} \dim_{\mathbb{F}} M_{\mathbb{F},\mathfrak{m}} = & \operatorname{rk}_{\widehat{\mathcal{O}}} M_{\widehat{\mathcal{O}},\mathfrak{m}} = \sum_{\mathfrak{p} \subseteq \mathfrak{m} \text{ min.}} \dim_K M_{K,\mathfrak{p}^e} \\ & = \sum_{\mathfrak{p} \subseteq \mathfrak{m} \text{ min.}} \dim_K N_{K,\mathfrak{p}^e} = \operatorname{rk}_{\widehat{\mathcal{O}}} N_{\widehat{\mathcal{O}},\mathfrak{m}} = \dim_{\mathbb{F}} N_{\mathbb{F},\mathfrak{m}}. \end{aligned}$$

This proves the proposition. □

Comparing dimensions

We use the algebraic preparation in order to compare the $\mathbb{F}$-dimensions of local factors of mod p modular forms with $\mathbb{F}$-dimensions of the corresponding local factors of mod p modular symbols.

3.4.2 Proposition. *Let* $\mathfrak{m}$ *be a maximal ideal of* $\mathbb{T}_{\mathcal{O}}(\mathcal{M}_k(N, \chi\,;\, \mathcal{O})) \otimes_{\mathcal{O}} \mathbb{F}$ *which is non-torsion and non-Eisenstein. Then the following statements hold:*

(a) $\mathcal{CM}_k(N, \overline{\chi}\,;\, \mathbb{F})_{\mathfrak{m}} \cong \mathcal{M}_k(N, \overline{\chi}\,;\, \mathbb{F})_{\mathfrak{m}}$.

(b) $2 \cdot \dim_{\mathbb{F}} \mathrm{S}_k(N, \overline{\chi}\,;\, \mathbb{F})_{\mathfrak{m}} = \dim_{\mathbb{F}} \mathcal{CM}_k(N, \overline{\chi}\,;\, \mathbb{F})_{\mathfrak{m}}$.

(c) If $p \neq 2$*, then* $\dim_{\mathbb{F}} \mathrm{S}_k(N, \overline{\chi}\,;\, \mathbb{F})_{\mathfrak{m}} = \dim_{\mathbb{F}} \mathcal{CM}_k(N, \overline{\chi}\,;\, \mathbb{F})^{+}_{\mathfrak{m}}$.

Proof. Part (c) follows directly from Part (b) by decomposing $\mathcal{CM}_k(N,\overline{\chi}\,;\,\mathbb{F})$ into a direct sum of its plus- and its minus-part. Statements (a) and (b) will be concluded from Proposition 3.4.1. More precisely, it allows us to derive from Theorem 3.1.1 that

$$\begin{aligned}&\dim_{\mathbb{F}}\big((\mathcal{M}_k(N,\chi\,;\,\mathcal{O}))/\text{torsion}\otimes_{\mathcal{O}}\mathbb{F}\big)_{\mathfrak{m}}\\ =&\dim_{\mathbb{F}}\big(\mathrm{Eis}_k(N,\overline{\chi}\,;\,\mathbb{F})\oplus\mathrm{S}_k(N,\overline{\chi}\,;\,\mathbb{F})\oplus\mathrm{S}_k(N,\overline{\chi}\,;\,\mathbb{F})^{\vee}\big)_{\mathfrak{m}}\end{aligned}$$

and

$$\dim_{\mathbb{F}}\big((\mathcal{CM}_k(N,\chi\,;\,\mathcal{O})/\text{torsion}\otimes_{\mathcal{O}}\mathbb{F}\big)_{\mathfrak{m}}=2\cdot\dim_{\mathbb{F}}\mathrm{S}_k(N,\overline{\chi}\,;\,\mathbb{F})_{\mathfrak{m}}.$$

The latter proves Part (b), since $\mathfrak{m}$ is non-torsion. As by the definition of a non-Eisenstein prime $\mathrm{Eis}_k(N,\overline{\chi}\,;\,\mathbb{F})_{\mathfrak{m}}=0$ and again since $\mathfrak{m}$ is non-torsion, it follows that

$$\dim_{\mathbb{F}}\mathcal{CM}_k(N,\overline{\chi}\,;\,\mathbb{F})_{\mathfrak{m}}=\dim_{\mathbb{F}}\mathcal{M}_k(N,\overline{\chi}\,;\,\mathbb{F})_{\mathfrak{m}},$$

which implies Part (a). □

We will henceforth often regard non-Eisenstein non-torsion primes as in the proposition as maximal primes of $\mathbb{T}_{\mathbb{F}}(\mathrm{S}_k(N,\overline{\chi}\,;\,\mathbb{F}))$.

The stop equality

Although it is impossible to determine a priori the dimension of the local factor of the Hecke algebra associated with a given modular form mod p, the following corollary implies that the computation of Hecke operators can be stopped when the algebra generated has reached a certain dimension that is computed along the way. This criterion has turned out to be extremely useful.

3.4.3 Corollary. (Stop Criterion) *Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}_{\mathbb{F}}(\mathrm{S}_k(N,\overline{\chi}\,;\,\mathbb{F}))$ which is non-Eisenstein and non-torsion.*

(a) One has $\dim_{\mathbb{F}}\mathcal{M}_k(N,\overline{\chi}\,;\,\mathbb{F})_{\mathfrak{m}}=2\cdot\dim_{\mathbb{F}}\mathbb{T}_{\mathbb{F}}\big(\mathcal{M}_k(N,\overline{\chi}\,;\,\mathbb{F})\big)_{\mathfrak{m}}$ if and only if

$$\mathbb{T}_{\mathbb{F}}\big(\mathrm{S}_k(N,\overline{\chi}\,;\,\mathbb{F})\big)_{\mathfrak{m}}\cong\mathbb{T}_{\mathbb{F}}\big(\mathcal{CM}_k(N,\overline{\chi}\,;\,\mathbb{F})\big)_{\mathfrak{m}}.$$

(b) One has $\dim_{\mathbb{F}}\mathcal{CM}_k(N,\overline{\chi}\,;\,\mathbb{F})_{\mathfrak{m}}=2\cdot\dim_{\mathbb{F}}\mathbb{T}_{\mathbb{F}}\big(\mathcal{CM}_k(N,\overline{\chi}\,;\,\mathbb{F})\big)_{\mathfrak{m}}$ if and only if

$$\mathbb{T}_{\mathbb{F}}\big(\mathrm{S}_k(N,\overline{\chi}\,;\,\mathbb{F})\big)_{\mathfrak{m}}\cong\mathbb{T}_{\mathbb{F}}\big(\mathcal{CM}_k(N,\overline{\chi}\,;\,\mathbb{F})\big)_{\mathfrak{m}}.$$

(c) Assume $p\neq 2$. One has $\dim_{\mathbb{F}}\mathcal{CM}_k(N,\overline{\chi}\,;\,\mathbb{F})^{+}_{\mathfrak{m}}=\dim_{\mathbb{F}}\mathbb{T}_{\mathbb{F}}\big(\mathcal{CM}_k(N,\overline{\chi}\,;\,\mathbb{F})\big)_{\mathfrak{m}}$ if and only if

$$\mathbb{T}_{\mathbb{F}}\big(\mathrm{S}_k(N,\overline{\chi}\,;\,\mathbb{F})\big)_{\mathfrak{m}}\cong\mathbb{T}_{\mathbb{F}}\big(\mathcal{CM}_k(N,\overline{\chi}\,;\,\mathbb{F})^{+}\big)_{\mathfrak{m}}.$$

Proof. We only prove (a), as (b) and (c) are similar. From Part (b) of Proposition 3.4.2 and the fact that the $\mathbb{F}$-dimension of the algebra $\mathbb{T}_{\mathbb{F}}\big(\mathrm{S}_k(N,\overline{\chi}\,;\,\mathbb{F})\big)_{\mathfrak{m}}$ is equal to the one of $\mathrm{S}_k(N,\overline{\chi}\,;\,\mathbb{F})_{\mathfrak{m}}$, as they are dual to each other, it follows that

$$2\cdot\dim_{\mathbb{F}}\mathbb{T}_{\mathbb{F}}\big(\mathrm{S}_k(N,\overline{\chi}\,;\,\mathbb{F})\big)_{\mathfrak{m}}=\dim_{\mathbb{F}}\mathcal{CM}_k(N,\overline{\chi}\,;\,\mathbb{F})_{\mathfrak{m}}.$$

The result is now a direct consequence of Equations 3.17 and 3.19. □

Note that the first line of each statement only uses modular symbols and not modular forms, but it allows us to make statements involving modular forms. Moreover, the maximal ideal $\mathfrak{m}$ can a posteriori be taken as a maximal ideal of $\mathbb{T}_{\mathbb{F}}\big(\mathcal{M}_k(N,\overline{\chi}\,;\,\mathbb{F})\big)$, respectively, for the cuspidal version.

3.5 The algorithm

In this section we present a sketch of a rather efficient mod p modular symbols algorithm for computing Hecke algebras of mod p modular forms.

Input: Integers $N\geq 1$, $k\geq 2$, a finite field $\mathbb{F}$, a character $\chi:(\mathbb{Z}/N\mathbb{Z})^\times\to\mathbb{F}^\times$ and for each prime p less than or equal to the Sturm bound an irreducible polynomial $f_p\in\mathbb{F}[X]$.
Output: An $\mathbb{F}$-algebra.

- $M\leftarrow\mathcal{CM}_k(N,\chi\,;\,\mathbb{F})$, $f\leftarrow 2$, $p\leftarrow 1$, $L\leftarrow$ empty list.
- repeat
  - $p\leftarrow$ next prime after p.
  - Compute T_p on M and append it to the list L.
  - $M\leftarrow$ the restriction of M to the f_p-primary subspace for T_p, i.e. to the biggest subspace of M on which the minimal polynomial of T_p is a power of f_p.
  - $A\leftarrow$ the $\mathbb{F}$-algebra generated by the restrictions to M of $T_2,T_3,\ldots,T_p$.
- until $f\cdot\dim(A)=\dim(M)$ or $p>$ Sturm bound.
- return A.

The f_p should, of course, be chosen as the minimal polynomials of the coefficients $a_p(f)$ of the normalised eigenform $f\in\mathrm{S}_k(N,\chi\,;\,\overline{\mathbb{F}})$ whose local Hecke algebra one wants to compute. Suppose the algorithm stops at the prime p. If p is bigger than the Sturm bound, the equivalent conditions of Corollary 3.4.3 do not hold. In that case the output should be disregarded. Otherwise, A is isomorphic to a direct product of the form $\prod_{\mathfrak{m}}\mathbb{T}_{\mathbb{F}}(\mathrm{S}_k(N,\chi\,;\,\mathbb{F}))_{\mathfrak{m}}$ where the $\mathfrak{m}$ are those maximal ideals such that the minimal polynomials of $T_2,T_3,\ldots,T_p$ on $\mathbb{T}(\mathrm{S}_k(N,\chi\,;\,\mathbb{F}))_{\mathfrak{m}}$ are equal to $f_2,f_3,\ldots,f_p$. It can happen that A consists of more than one factor. Hence, one should still decompose A into its local factors. Alternatively, one can also replace the last line but one in the algorithm by

- until $\big((\dim(A) = f \cdot \dim(M))$ and A is local$\big)$ or $p >$ Sturm bound,

which ensures that the output is a local algebra. In practice, one modifies the algorithm such that not for every prime p a polynomial f_p need be given, but that the algorithm takes each irreducible factor of the minimal polynomial of T_p if no f_p is known.

3.6 Eichler-Shimura like statements over $\mathbb{F}_p$

In this section we present an analog of the Eichler-Shimura isomorphism, formulated in terms of p-adic Hodge theory. This was already used in [EdixJussieu], Theorem 5.2, to derive an algorithm for computing modular forms. However, p-adic Hodge theory always has the restriction that the weight be smaller than p.

3.6.1 Theorem. (Fontaine, Messing, Faltings) *Let p be a prime and $N \geq 5$, $2 \leq k < p$ be integers s.t. $p \nmid N$. Then the Galois representation $H^1_{\text{ét, par}}(Y_1(N)_{\overline{\mathbb{Q}_p}}, \mathrm{Sym}^{k-2}(\mathbb{V}))^\vee$ is crystalline, where $\mathbb{V} = R^1\pi_*\mathbb{F}_p$ with $\pi : \mathbb{E} \to Y_1(N)$ the universal elliptic curve. The corresponding ϕ-module D sits in the exact sequence*

$$0 \to \mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{F}_p) \to D \to \mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{F}_p)^\vee \to 0,$$

which is equivariant for the action of the Hecke operators.

This can be compared to Theorem 1.1 and Theorem 1.2 of [FJ]. Part (a) of the following corollary is part of [EdixJussieu], Theorem 5.2.

3.6.2 Corollary. *Let $N \geq 5$, $p \nmid N$ and $2 \leq k < p$. Then the parabolic cohomology group $H^1_{\mathrm{par}}(\Gamma_1(N), V_{k-2}(\mathbb{F}_p))$ is a faithful module for $\mathbb{T}_{\mathbb{F}_p}\big(\mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{F}_p)\big)$.*

Proof. From Theorem 3.6.1 we know that D is a faithful Hecke module. Hence, so is the cohomology $H^1_{\text{ét, par}}(Y_{\Gamma_1(N)}, \mathrm{Sym}^{k-2}(\mathbb{V}))$. This module can be identified with its analog in analytic cohomology which is isomorphic to $H^1_{\mathrm{par}}(\Gamma_1(N), V_{k-2}(\mathbb{F}_p))$. □

A weaker statement holds for $k = p$ and $k = p + 1$. For our computations this is good enough.

3.6.3 Theorem. *Let $2 < k \leq p + 1$, $N \geq 5$ such that $p \nmid N$. Let $\mathfrak{P}$ be a maximal ideal of $\mathbb{T}_{\mathbb{F}_p}\big(\mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{F}_p)\big)$ corresponding to a normalised eigenform $f \in \mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{F}_p)$ which is* ordinary, *i.e. $a_p(f) \neq 0$. Then we have an isomorphism*

$$\mathbb{T}_{\mathbb{F}_p}\big(\mathrm{S}_k(\Gamma_1(N)\,;\,\mathbb{F}_p)_{\mathfrak{P}}\big) \cong \mathbb{T}_{\mathbb{F}_p}\big(H^1_{\mathrm{par}}(\Gamma_1(N), V_{k-2}(\mathbb{F}_p))_{\mathfrak{P}}\big).$$

We have seen before that the embedding of weight one forms into weight p results in ordinary modular forms. As a consequence, the weight one forms land in the part of weight p which can be computed via parabolic group cohomology.

4 Problems

1. **Big images.** To every mod p eigenform Deligne attaches a 2-dimensional odd "mod p" Galois representation, i.e. a continuous group homomorphism

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

   (See Theorem 1.9.2). The trace of a Frobenius element at a prime l is for almost all l given by the l-th coefficient of the (normalised) eigenform. By continuity, the image of such a representation is a finite group.

   Find group theoretic criteria that allow one (in some cases) to determine the image computationally. Carry out systematic computations of mod p modular forms in order to find "big" images. Like this one can certainly realise some groups as Galois groups over $\mathbb{Q}$ that were not known to occur before!

2. **Non-liftable weight one modular forms over $\mathbb{F}_p$.** This problem is closely connected to the "big images" challenge, and could/should be treated in collaboration. Modular forms of weight 1 over $\mathbb{F}_p$ behave completely differently from forms of higher weights. One feature is that they are very often NOT reductions of holomorphic modular forms. In the course it will be explained how to compute modular forms of weight one. By looking at the image of a weight one form, one can often prove that it is such a non-liftable form. So far, there are many examples over $\mathbb{F}_2$, but only one example for an odd prime, namely for $p = 199$. Find examples in small odd characteristics!

A Computing local decompositions

Let K be a perfect field, $\overline{K}$ an algebraic closure and A a finite dimensional commutative K-algebra. We will write A_L for $A \otimes_K L$, where $L|K$ is an extension inside $\overline{K}$. The image of $a \in A$ in $A_{\overline{K}}$ is denoted as $\overline{a}$.

In the context of Hecke algebras we would like to

(1) compute a local decomposition of A, resp.

(2) compute a local decomposition of $A_{\overline{K}}$ keeping track of the $G(\overline{K}|K)$-conjugacy.

In this section we present an algorithms for both points.

A.1 Primary spaces

A.1.1 Lemma. *(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 $A_{\overline{K}}$-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 $\overline{K}[X]$ for some $\lambda_i \in \overline{K}$. Then the image of $A_{\overline{K}}$ 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, implying that 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 $ab - \lambda\mu = (a - \lambda)(b - \mu) + \lambda(b - \mu) + \mu(a - \lambda)$. □

Let us remark 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.

A.2 Algorithm for computing common primary spaces

In this section we present a straight forward algorithm for computing common eigenspaces.

A.2.1 Algorithm. *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`*.*

- *List := [V];*
- *for T in* `ops` *do*
  - *newList := [];*
  - *for W in List do*
    - *Compute the minimal polynomial $f \in K[X]$ of T restricted to W.*
    - *Factor f over K into its prime powers $f(X) = \prod_{i=1}^{n} p_i(X)^{e_i}$.*
    - *If n equals 1, then*
      - *Append W to newList,*
    - *else for i := 1 to n do*
      - *Compute $\widetilde{W}$ as the kernel of $p_i(T|_W)^{e_i}$.*
      - *Append $\widetilde{W}$ to newList.*
    - *end for; end if;*
  - *end for;*
  - *List := newList;*

- *end for;*
- *Return List and stop.*

A.3 Algorithm for computing local factors up to Galois conjugacy

Let us call a pair (V, L) consisting of a finite extension $L|K$ with $L \subset \overline{K}$ and an A_L-module V an *a-pair* for $a \in A$ if the coefficients of the minimal polynomial of $\overline{a}$ acting on $V \otimes_L \overline{K}$ generate L over K.

Let us furthermore call a set $\{(V_1, L_1), \dots (V_n, L_n)\}$ consisting of a-pairs an *a-decomposition* of an a-pair (V, L) if

(i) $V \otimes_L \overline{K} \cong \bigoplus_{i=1}^n \widetilde{V_i}$ with $\widetilde{V_i} \cong \bigoplus_{\sigma \in G_L/G_{L_i}} \sigma(V_i \otimes_{L_i} \overline{K})$ and

(ii) the minimal polynomial of $\overline{a}$ restricted to V_i is a power of $(X - \lambda_i)$ for some $\lambda_i \in L_i$ for all i and

(iii) the minimal polynomial of $\overline{a}$ restricted to $\widetilde{V_i}$ is coprime to the minimal polynomial of $\overline{a}$ restricted to $\widetilde{V_j}$ whenever $i \neq j$.

The $\widetilde{V_i}$ correspond to the local factors of the L-algebra $\langle a \rangle$ and the $\sigma(V_i \otimes_{L_i} \overline{K})$ to the local factors of the $\overline{K}$-algebra $\langle \overline{a} \rangle$. So the (V_i, L_i) are a choice out of a $G(L_i|L)$-conjugacy class. The third condition above assures that for $i \neq j$ no $(\sigma V_i, \sigma L_i)$ for $\sigma \in G(L_i|L)$ is conjugate to a $(\tau V_j, \tau L_j)$ for any $\tau \in G(L_j|L)$.

An a-decomposition of an a-pair can be computed by the following algorithm.

A.3.1 Algorithm. *We define the function* `DecomposePair` *as follows.*
Input: $(V, L), a$, where (V, L) is an a-pair.
Output: A list `output` *$[(V_1, L_1), \dots, (V_n, L_n)]$ containing an a-decomposition of (V, L).*

1. *Create an empty list* `output`*, which after the running will contain an a-decomposition.*
2. *Compute $f \in L[X]$, the minimal polynomial of $\overline{a}$ restricted to V.*
3. *Factor $f = \prod_{i=1}^n p_i^{e_i}$ with $p_i \in L[X]$ pairwise coprime.*
4. *For all i in $\{1, \dots, n\}$ do*
   1. *Compute $\widetilde{V_i}$ as the kernel of $p_i(\overline{a}|_V)^{e_i}$.*
   2. *Compute L_i, the splitting field over L of p_i.*
   3. *Factor $p_i(X) = \prod_{\sigma \in G_L/G_{L_i}} (X - \sigma\lambda_i)$, for some $\lambda_i \in L_i$.*
   4. *Compute V_i as the kernel of $(\overline{a}|_{\widetilde{V_i}} - \lambda_i)^{e_i}$.*
   5. *Join (V_i, L_i) to the list* `output`*.*
5. *Return* `output` *and stop.*

The decomposition of an A_K-module V corresponding to the local factors of $A_{\overline{K}}$ and keeping track of conjugacy can be computed by the following algorithm, when the $a_1, \ldots, a_n$ in the input generate A.

A.3.2 Algorithm. *We define the function* `Decompose` *as follows.*

Input: $(V, K), [a_1, \ldots, a_n]$ *with* $[a_1, \ldots, a_n]$ *a list of elements of* A *and* (V, K) *an* a_i*-pair for all* $i = 1, \ldots, n$.

Output: A list `output` $= [(V_1, K_1), \ldots, (V_n, K_n)]$ *consisting of pairs with* K_i *a finite extension of* K *and* V_i *an* A_{K_i}*-module. See Proposition A.3.3 for an interpretation.*

1. *Compute* `dec` *as* `DecomposePair(`(V, K)`,` a_1`)`.
2. *If* $n = 1$*, then return* `dec`.
3. *Create the empty list* `output`.
4. *For all* d *in* `dec` *do*
   1. *Compute* `dec1` *as* `Decompose(`d`,` $[a_2, \ldots, a_n]$`)`.
   2. *Join* `dec1` *to the list* `output`.
5. *Return the list* `output` *and stop.*

From Lemma A.1.1 the following is clear.

A.3.3 Proposition. *Let* A *be a commutative finite dimensional* K*-algebra with generators* $a_1, \ldots, a_n$. *Let* V *be an* A*-module. Suppose that* $\{(V_1, K_1), \ldots, (V_m, K_m)\}$ *is the output of the function call* `Decompose(`(V, K)`,` $[a_1, \ldots, a_n]$`)`.

Then $V \otimes_K \overline{K} = \bigoplus_{i=1}^{m} \widetilde{V}_i$ *with* $\widetilde{V}_i = \bigoplus_{\sigma \in G_k/G_{K_i}} \sigma V_i$. *The* $\widetilde{V}_i$ *correspond to the local factors of* A *and the* σV_i *correspond to the local factors of* $A_{\overline{K}}$. □

A.3.4 Corollary. *We keep the notation from Proposition A.3.3. If* V *is a faithful* A*-module, then the local factors of* A *are isomorphic to the images of* A *in* $\mathrm{End}(\widetilde{V}_i)$. *Moreover the local factors of* $A_{\overline{K}}$ *correspond to the images of* $A_{\overline{K}}$ *in* $\mathrm{End}(\sigma V_i)$.

B Group cohomology - an introduction

B.1 The derived functor definition

Those, not knowing group cohomology, but being comfortably acquainted with derived functor cohomology (e.g. with sheaf cohomology as in [Hartshorne]) might want to think about group cohomology in the following way.

We fix a ring R and a group G. By a G-module, we usually mean a left $R[G]$-module. The functor

$$\mathcal{F} : R[G]\text{-modules} \to R\text{-modules}, \quad M \mapsto M^G = \mathrm{Hom}_{R[G]}(R, M)$$

taking G-invariants is left exact. We define

$$H^i(G,M) := R^i(\mathcal{F})(M)$$

as the right derived functors of the G-invariants functor. Alternatively, we have by definition (of the Ext-functor)

$$H^i(G,M) := \mathrm{Ext}^i_{R[G]}(R,M).$$

Since Ext is balanced, i.e.

$$\mathrm{Ext}^i_{R[G]}(R,M) \cong R^n\mathrm{Hom}_{R[G]}(R,\cdot)(M) \cong R^n\mathrm{Hom}_{R[G]}(\cdot,M)(R)$$

([Weibel],Theorem 2.7.6), we may also compute $H^i(G,M)$ by applying the functor $\mathrm{Hom}_{R[G]}(\cdot,M)$ to any resolution of R by projective $R[G]$-modules. This shows the equivalence with the definition of group cohomology using the normalised standard resolution to be given later on.

B.1.1 Exercise. *Let G be a free group and M any $R[G]$-module. Prove that $H^i(G,M) = 0$ for all $i \geq 2$. Hint: Choose a suitable free resolution of R by $R[G]$-modules. Hint for the hint: Show that the augmentation ideal is free.*

B.2 Group cohomology via the standard resolution

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

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

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

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

If we let $h_r := g_{r-1}^{-1}g_r$, then we get the identity

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

The symbols $[h_1|h_2|\dots|h_n]$ with arbitrary $h_i \in G$ hence form an $R[G]$-basis of $F(G)_n$, and one has $F(G)_n = R[G] \otimes_R$ (free abelian group on $[h_1|h_2|\dots|h_n]$). One computes the action of d_i on this basis and gets

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

One checks that the standard resolution is a complex and is exact (i.e. is a resolution).

As mentioned above, $H^i(G,M)$ for an $R[G]$-module M can be calculated as the i-th cohomology group of the complex obtained by applying the functor $\mathrm{Hom}_{R[G]}(\cdot, M)$ to the standard resolution. Let us point out the following special case:

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

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

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

B.2.1 Exercise. *Let $\langle g\rangle$ be a free group on one generator. Show $H^1(\langle g\rangle, M) = M/(1-g)M$ (either using the normalised standard resolution, or the resolution of Exercise B.1.1, or any other trick).*

B.3 Functorial properties

The functor $H^n(G,\cdot)$ is a *positive cohomological δ-functor* for $R[G]$-modules, by which we mean the following: For every short exact sequence $0 \to A \to B \to C \to 0$ of $R[G]$-modules there is for every n a so-called *connecting homomorphism* $\delta^n : H^n(G,C) \to H^{n+1}(G,A)$ such that the following hold:

(i) For every commutative diagram

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

with exact rows, the following diagram commutes, too:

$$\begin{array}{ccc} H^n(G,C) & \xrightarrow{\delta^n} & H^{n+1}(G,A)\\ \downarrow{\scriptstyle H^n(h)} & & \downarrow{\scriptstyle H^{n+1}(f)}\\ H^n(G,C') & \xrightarrow{\delta^n} & H^{n+1}(G,A') \end{array}$$

(ii) The so-called *long exact sequence* is exact for all n:

$$H^n(G,A) \to H^n(G,B) \to H^n(G,C) \xrightarrow{\delta^n} H^{n+1}(G,A) \to H^{n+1}(G,B).$$

By *positive* we mean that the groups $H^n(G,A)$ are zero for all $n < 0$.

The functor $H^n(G,\cdot)$ is also *coeffaçable* with respect to the injective $R[G]$-modules, i.e. every $R[G]$-module A can be embedded into an injective module I. Injective modules are cohomologically trivial.

It is known that coeffaçable cohomological δ functors are *universal*. This means by definition that if S is another cohomological δ-functor and $f^0 : H^0(G,\cdot) \to S^0(\cdot)$ is a natural transformation, then there is a unique natural transformation $f^n : H^n(G,\cdot) \to S^n(\cdot)$ for all n extending f^0 such that all properties of δ-functors are preserved (all diagrams one would want to be commutative are). A shorter way to phrase this is that f^0 extends to a morphism of cohomological δ-functors $H^\bullet(G,\cdot) \to S^\bullet$.

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

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

These maps are called *restrictions*. On cochains of the standard resolution they can be seen as composing maps $G \to A$ by ϕ. Note that 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 us natural transformations $\mathrm{res}^n : H^n(G/H,(\cdot)^H) \to H^n(G,(\cdot)^H)$. We define the *inflation maps* to be

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

Under the same assumptions, note that by a similar argument applied to the conjugation by g map $H \to H$, one obtains an $R[G]$-action on $H^n(H,A)$. As conjugation by $h \in H$ is clearly the identity on $H^0(G,A)$, the above action is in fact also an $R[G/H]$-action.

Let now $H < G$ 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 $\mathrm{cores}^0 : H^0(H,\cdot) \to H^0(G,\cdot)$ where $\cdot$ is an $R[G]$-module. By universality, we obtain

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

the *corestriction (transfer)* maps. It is clear that $\mathrm{cores}^0 \circ \mathrm{res}^0$ is multiplication by the index $(G:H)$, which also extends to all n. Hence we have proved the first part of the following proposition.

B.3.1 Proposition. *(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 $H^i(G,M)$.

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

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

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

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

Let $H \leq G$ be a normal subgroup and A an $R[G]$-module. Grothendieck's theorem on spectral sequences associates to the composition of functors

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

a spectral sequence. This is the contents of the following theorem (see [Weibel], 6.8.2).

B.3.2 Theorem. (Hochschild-Serre) *There is a convergent first quadrant spectral sequence*

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

In particular, one has the exact sequence:

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

B.4 Coinduced modules and Shapiro's Lemma

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

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

is called the *coinduction from H to G of A*.

B.4.1 Proposition. (Shapiro's Lemma) *We have*

$$H^n(G, \mathrm{Coind}_H^G(A)) \cong H^n(H, A)$$

for all $n \geq 0$.

B.5 Mackey's formula and stabilisers

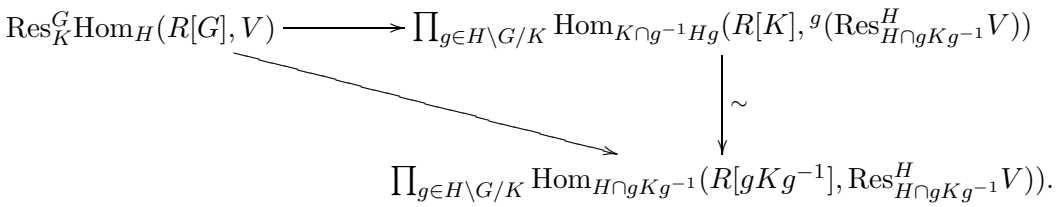
We now prove Mackey's formula for coinduced modules. If $H \leq G$ are groups and V is an $R[H]$-module, the coinduced module $\mathrm{Coind}_H^G V$ can be described as $\mathrm{Hom}_{R[H]}(R[G], V)$.

B.5.1 Proposition. *Let R be a ring, G be a group and H, K subgroups of G. Let furthermore V be an $R[H]$-module. Then* Mackey's formula

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

holds. 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



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.

B.5.2 Corollary. *In the situation of Proposition B.5.1 one has*

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

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

B.6 Free products and the Mayer-Vietoris exact sequence

Let us that the group G is the free product of two finite groups G_1 and G_2, for which we use the notation $G = G_1 * G_2$.

B.6.1 Proposition. *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.*

For the proof, which is completely elementary, we follow [Bieri]. Let G be a group and M an $R[G]$-module. Recall that a map $d : G \to M$ is called a *derivation* if

$$d(xy) = d(x) + xd(y)$$

(these are precisely the 1-cochains of the standard resolution!). Denote by ϵ the map $R[G] \to R$ given by $g \mapsto 1$. Then it is easy to check that d extends to an R-linear map

$$d : R[G] \to M, \text{ satisfying } d(ab) = d(a)\epsilon(b) + ad(b).$$

Let F be a free group on generators $\{f_i\}$. Since there are no relations, it is clear that the assignment

$$\frac{\partial}{\partial f_i}(f_j) = \delta_{i,j}$$

extends to a derivation $F \to R[F]$ (we define $\delta_{i,j} = 1$ if $i = j$ and $\delta_{i,j} = 0$ if $i \neq j$). Next, for any derivation $d : F \to M$ one puts

$$\tilde{d} : F \to M, \;\; \tilde{d}(w) = \sum_i \frac{\partial w}{\partial f_i} d(f_i).$$

A short calculation shows that $\tilde{d}$ is also a derivation. Moreover, $\tilde{d}(f_i) = d(f_i)$, whence $\tilde{d} = d$. In other words,

$$d(w) = \sum_i \frac{\partial w}{\partial f_i} d(f_i).$$

We now specialise to the derivation $d : F \to R[F]$ given by $d(w) = w - 1$. Moreover, we also suppose that $\pi : F \twoheadrightarrow G$ is a free presentation of the group G by the free group F discussed so far. We denote $\pi(f_i)$ by g_i and extend π linearly to $\pi : R[F] \to R[G]$. From the above, we immediately get the formula

$$\lambda - \epsilon(\lambda) = \sum_i \pi(\frac{\partial \Lambda}{\partial f_i})(g_i - 1) \tag{2.20}$$

for $\Lambda \in R[F]$ with $\pi(\Lambda) = \lambda$. It will be the main input in the following proof.

Proof of Proposition B.6.1. Suppose that G_1 is generated by the (minimal) set $\{\overline{x_i}\}$ and G_2 by $\{\overline{y_j}\}$. Let F be the free group on symbols $\{x_i, y_j\}$ so that $\pi : F \twoheadrightarrow G$ is given by $x_i \mapsto \overline{x_i}$ and $y_i \mapsto \overline{y_i}$.

Clearly, ϵ is surjective and also $\epsilon \circ \alpha = 0$. Next we compute exactness at the centre. The image of Equation 2.20 in $R[G/G_1] = R[G]/(R[G](1-h)|h \in G_1)$ is

$$\lambda G_1 - \epsilon(\lambda G_1) = \sum_j (\pi(\frac{\partial \Lambda}{\partial y_j})(\overline{y_j} - 1)G_1$$

for $\Lambda \in R[F]$ with $\pi(\Lambda) = \lambda$. In the same way we have

$$\lambda G_2 - \epsilon(\lambda G_2) = \sum_i (\pi(\frac{\partial \Lambda}{\partial x_i})(\overline{x_i} - 1)G_2.$$

Suppose now that

$$\epsilon(\lambda G_1, \mu G_2) = \epsilon(\lambda G_1) + \epsilon(\mu G_2) = 0$$

and choose $\Lambda, M \in R[F]$ with $\pi(\Lambda) = \lambda$ and $\pi(M) = \mu$. We directly get

$$\alpha(\sum_j (\pi(\frac{\partial \Lambda}{\partial y_j})(\overline{y_j} - 1) - \sum_i (\pi(\frac{\partial M}{\partial x_i})(\overline{x_i} - 1) + \epsilon(\lambda)) = (\lambda G_1, \mu G_2)$$

and hence the exactness at the centre.

It remains to prove that α is injective. Note that we have not yet used the freeness of the product; the discussion above would remain valid if there were additional relations in G. Now we do use the freeness, namely as follows. Every element $1 \neq g \in G$ has a unique representation as products of the form $g = a_1b_2a_3b_4 \cdots a_{k-1}b_k$, or $g = a_1b_2a_3b_4 \cdots b_{k-1}a_k$ where either all the $a_i \in G_1 - \{1\}$ and all $b_j \in G_2 - \{1\}$ or all the $a_i \in G_2 - \{1\}$ and all $b_j \in G_1 - \{1\}$. The integer k is defined to be the length of g, denoted by $l(g)$. We let $l(1) = 0$. For cosets $gG_1 \in G/G_1$ we let $l(gG_1) := l(g)$ when g is represented by a product as above ending in an element of G_2. We define $l(gG_2)$ similarly.

Let $\lambda = \sum_w a_w w \in R[G]$ be an element in the kernel of α. Hence, $\sum_w a_w wG_1 = 0 = \sum_w a_w wG_2$. 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. Then $l(gG_2) = l(g)$. Further, since $a_g \neq 0$ and $0 = \sum_w a_w wG_2$, 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. □

B.6.2 Proposition. (Mayer-Vietoris) *Let M be a left $R[G]$-module. Then the Mayer-Vietoris sequence gives the exact sequences*

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

and for all $i \geq 2$ an isomorphism

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

Proof. We see that all terms in the exact sequence of Proposition B.6.1 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 B.4.1. □

References

[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.

[DDT] H. Darmon, F. Diamond, R. Taylor. *Fermat's Last Theorem*.

[Deligne-Rapoport] P. Deligne and M. Rapoport. *Les schémas de modules de courbes elliptiques*, in *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, 143–316. Lecture Notes in Math. **349**, Springer, Berlin, 1973.

[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.

[EdixSerre] S. J. Edixhoven. *Serre's Conjecture*, in *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, 209–242, Springer, New York, 1997.

[EdixJussieu] S. J. Edixhoven. *Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod* 2 *of weight one*. Journal of the Inst. of Math. Jussieu **5** (2006), no. 1, 1–34.

[EdixWeight] S. J. Edixhoven. *The weight in Serre's conjectures on modular forms*, Invent. math. **109** (1992), no. 3, 563–594.

[Eisenbud] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics, **150**, Springer-Verlag, New York, 1995.

[FJ] G. Faltings, B. W. Jordan. *Crystalline Cohomology and* $\mathrm{GL}_2(\mathbb{Q})$, Israel J. Math. **90** (1995), no. 1–3, 1–66.

[Gross] B. H. Gross. *A tameness criterion for Galois representations associated to modular forms (mod* p*)*, Duke Math. J. **61** (1990), no. 2, 445–517.

[Hartshorne] R. Hartshorne. *Algebraic geometry*, Springer, New York, 1977.

[Herremans] A. Herremans. *A combinatorial interpretation of Serre's conjecture on modular Galois representations*, Ann. Inst. Fourier (Grenoble) **53** (2003), no. 5, 1287–1321.

[Katz] N. M. Katz. p*-adic properties of modular schemes and modular forms.* Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972). Lecture Notes in Mathematics, Vol. 350, Springer, Berlin, 1973, 69–190.

[KatzDerivation] N. M. Katz. *A result on modular forms in characteristic* p. Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), 53–61. Lecture Notes in Math., Vol. **601**, Springer, Berlin, 1977.

[KM] N. M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*, Ann. of Math. Stud. **108**, Princeton Univ. Press, Princeton, NJ, 1985.

[KW] L. J. P. Kilford, G. Wiese. *On the failure of the Gorenstein property for Hecke algebras of prime weight.* Preprint.

[Manin] Manin, Ju. I. *Parabolic points and zeta functions of modular curves.* Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66.

[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.

[R1] K. A. Ribet. *On l-adic representations attached to modular forms II*. Glasgow Math. J. **27** (1985), 185–194.

[R2] K. A. Ribet. *Images of semistable Galois representations*. Pacific Journal of Mathematics **181** No. 3 (1997), 277–297.

[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.

[Šokurov] V. V. Šokurov. *Shimura integrals of cusp forms.* Izv. Akad. Nauk SSSR Ser. Mat. **44** (1980), no. 3, 670–718, 720.

[SteinBook] W. A. Stein. *Explicitly Computing Modular Forms*, textbook to appear.

[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.

[W1] G. Wiese. *On the faithfulness of parabolic cohomology as a Hecke module over a finite field.* Accepted for publication in J. für die reine und angewandte Mathematik. `arXiv:math.NT/0511115`.

[W2] G. Wiese. *On modular symbols and the cohomology of Hecke triangle surfaces.* Preprint. `arXiv:math.NT/0511113`.

Gabor Wiese
NWF I - Mathematik
Universität Regensburg
D-93040 Regensburg
Germany
E-mail: `gabor@pratum.net`
Webpage: `http://maths.pratum.net/`