Modular Forms mod p and Galois Representations of Weight One

Gabor Wiese

9th February 2012

Abstract

This is a sketch of the content of my four lectures during the Workshop on Modular Forms and Related Topics, 6 – 10 February 2012, in Beirut. Thanks Wissam and Kamal for the nice organisation!

Note that the title does not really reflect the content of these lectures.

Some words of motivation

All speakers at this workshop are interested in Fourier coefficients of modular forms. Why? For their number theoretic significance!

- The Fourier coefficients of the Eisenstein series E_k (see Kohnen's lecture) are $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$; the function σ_{k-1} has an obvious number theoretic significance!
- The Fourier coefficients of (certain) theta-series are representation numbers of quadratic forms. The nicest example is maybe the following: the number of times, a given positive integer n can be represented as a sum of four squares, i.e. $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$, is the coefficient of a modular form. This allows one to write down a formula for this number (see Kohnen's lecture).
- In Kohnen's next lectures an analytic property of the coefficients will be studied: their growth. In my lectures, however, I will focus on algebraic properties: we will prove, for instance, that the Fourier coefficients of normalised Hecke eigenforms (to be defined below) are algebraic integers. This will be a consequence of the existence of an integral structure, by which we start the lectures. The very deep connection that will be stated towards the end of the third or the fourth lecture is that are actually related to Galois representations in a very precise way; this is an essential ingredient, for instance, for the proof of Fermat's Last Theorem.

I should maybe add a word about 'integral structures'. The first aim of these lectures, and maybe a good example to explain the concept, is the following: The $\mathbb{Z}$-module (i.e. abelian group) consisting of those modular forms, all of whose Fourier coefficients (except possibly the 0-th one) are integers

(we will denote this by $M_k(N)(\mathbb{Z})$) forms an integral structure in the $\mathbb{C}$-vector space of all modular forms. We formalise the statement like this: The natural map (multiplying together)

$$\mathbb{C} \otimes_{\mathbb{Z}} M_k(N)(\mathbb{Z}) \to M_k(N)$$

is an isomorphism of $\mathbb{C}$-vector spaces.

To illustrate this notion now in an elementary way, we give some simple examples: $\mathbb{Z} \subset \mathbb{C}$ is an integral structure, as is $\mathbb{Z}\pi \subset \mathbb{C}$, but $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z} \subset \mathbb{C}$ is not (because the left hand side is a free $\mathbb{Z}$-module of rank 2 so that $\mathbb{C} \otimes_{\mathbb{Z}} (\mathbb{Z} + \mathbb{Z}[i]) \cong \mathbb{C} \oplus \mathbb{C}$ and not $\mathbb{C}$!). In dimension 2, $\mathbb{Z} \oplus \mathbb{Z} \subset \mathbb{C} \oplus \mathbb{C} = \mathbb{C}^2$ is an integral structure, as is $\mathbb{Z} \oplus i\mathbb{Z} \subset \mathbb{C}^2$, but $\mathbb{Z} \oplus (\mathbb{Z} + i\mathbb{Z}) \subset \mathbb{C}^2$ is not.

1 Hecke algebras and q-expansions

We start by fixing notation. By $M_k(N)$ we denote the $\mathbb{C}$-vector space of modular forms on $\Gamma_1(N)$ and weight k. The cuspidal subspace will be referred to as $S_k(N)$.

Hecke algebras play an essential role in most of the lectures. We will be careful and define two sorts of Hecke algebras, one over the complex numbers, the other over the integers. In the first lecture we will see how they are related.

Let $\mathcal{H}_k(N)$ be the $\mathbb{C}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(M_k(N))$ generated by all Hecke operators T_n for $n \in \mathbb{N}$. By $\mathbb{T}_k(N)$ we deonote the $\mathbb{Z}$-subalgebra (i.e. subring) of $\mathrm{End}_{\mathbb{C}}(M_k(N))$ generated by all Hecke operators T_n for $n \in \mathbb{N}$. Of course, $\mathbb{T}_k(N) \subset \mathcal{H}_k(N) \subseteq \mathrm{End}_{\mathbb{C}}(M_k(N))$. Both are called *Hecke algebra of weight k on $\Gamma_1(N)$*. If we choose a $\mathbb{C}$-basis of $M_k(N)$, then the T_n are matrices with complex entries. The algebra $\mathcal{H}_k(N)$ consists of all $\mathbb{C}$-linear combinations of those, and $\mathbb{T}_k(N)$ of all integral linear combinations, both inside the complex matrix ring.

Let me point out that we could have made the same definitions with $S_k(N)$ instead of $M_k(N)$ (or, any other modular forms space that is stable under the Hecke action). In later talks, we shall start using the Hecke algebras for cusp forms.

Aim: Our first objective is to show that there is a basis of $M_k(N)$ such that all T_n have integral matrix entries.

We start with some facts, which are easy to prove.

Fact 1.1. *(a) The Hecke algebras $\mathcal{H}_k(N)$ and $\mathbb{T}_k(N)$ are commutative.*

(b) There are $0 \neq f \in M_k(N)$ and $\lambda_n \in \mathbb{C}$ (in fact, another **aim** *is to show that the λ_n are algebraic integers) such that $T_n f = \lambda_n f$ for all $n \in \mathbb{N}$, i.e. f is an eigenform for all Hecke operators. We call f a* (Hecke) eigenform. *If, moreover, $a_1(f) = 1$, then we call f* normalised. *Here, and everywhere later, $a_n(f)$ is the n-th Fourier coefficient of the Fourier series of f at ∞, i.e. $f(z) = \sum_{n=0}^{\infty} a_n(f) e^{2\pi i n z}$.*

The following assertions are very simple to prove (which we will partly do!), but, are astonishingly powerful.

Lemma 1.2 (Key Lemma)**.** *Let $f = \sum_{n=0}^{\infty} a_n(f) e^{2\pi i n z} \in M_k(N)$. Then for all $n \in \mathbb{N}$ one has*

$$a_1(T_n f) = a_n(f).$$

Proof. This follows immediately from the formula describing T_n on the Fourier expansion of f. See any introductory course to modular forms, or, Kohnen's lecture. □

We assume from now on that the weight satisfies $k \geq 1$ (later, we will impose $k \geq 2$ and come back to $k = 1$ in the last lecture).

Corollary 1.3 (Key Corollary)**.** *The* complex q-pairing

$$\mathcal{H}_k(N) \times M_k(N) \to \mathbb{C}, \quad (T, f) \mapsto a_1(Tf)$$

is non-degenerate and, hence by linear algebra, gives rise to the isomorphism of $\mathbb{C}$-vector spaces

$$\Phi : M_k(N) \to \mathrm{Hom}_{\mathbb{C}}(\mathcal{H}_k(N), \mathbb{C}), \quad f \mapsto \big(T_n \mapsto a_1(T_n f) = a_n(f)\big).$$

The inverse Ψ of Φ is given by $\phi \mapsto a_0 + \sum_{n=1}^{\infty} \phi(T_n) q^n$, where a_0 is a uniquely defined complex number.

Proof. This follows from the Key Lemma 1.2 like this. If for all n we have $0 = a_1(T_n f) = a_n(f)$, then $f = 0$ (this is immediately clear for cusp forms; for general modular forms at the first place we can only conclude that f is a constant, but since $k \geq 1$, non-zero constants are not modular forms). Conversely, if $a_1(Tf) = 0$ for all f, then $a_1(T(T_n f)) = a_1(T_n T f) = a_n(Tf) = 0$ for all f and all n, whence $Tf = 0$ for all f. As the Hecke algebra is defined as a subring in the endomorphism of $M_k(N)$, we find $T = 0$, proving the non-degeneracy.

Let $\phi \in \mathrm{Hom}_{\mathbb{C}}(\mathcal{H}_k(N), \mathbb{C})$. It is obvious that $\Psi(\phi)$ is a modular form f such that $a_n(f) = \phi(T_n)$ for all $n \geq 1$. Note that the coefficients $a_n(f)$ for $n \geq 1$ uniquely determine $a_0(f)$, as the difference of two forms having the same $a_n(f)$ for $n \geq 1$ would be a constant modular form of the same weight and so is the 0-function by the assumption $k > 0$. However, I do not know a general formula how to write down $a_0(f)$ (but, it can be computed in all cases). □

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

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

So, from the knowledge of the Hecke algebra we can recover the modular forms via their q-expansions as the $\mathbb{C}$-linear maps $\mathcal{H}_k(N) \to \mathbb{C}$. It is this point of view that will generalise well (in view of our aim of studying mod p modular forms)!

But, more is true: We can identify normalised eigenforms as the $\mathbb{C}$-algebra homomorphisms among the $\mathcal{H}_k(N) \to \mathbb{C}$:

Corollary 1.4. *Let f in $M_k(N)$ be a normalised eigenform.*

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

(b) $\Phi(f)$ *is a ring homomorphism* $\Leftrightarrow$ f *is a normalised eigenform.*

Proof. (a) Let λ_n be the eigenvalue of T_n on a normalised eigenform f. Then:

$$a_n(f) = a_1(T_n f) = a_1(\lambda_n f) = \lambda_n a_1(f) = \lambda_n,$$

proving (a).

(b) '$\Leftarrow$': We have:

$$\Phi(f)(T_n T_m) = a_1(T_n T_m f) = a_1(T_n a_m(f) f) = a_m(f) a_n(f) = \Phi(f)(T_n)\Phi(f)(T_m),$$

as well as (using that T_1 is the identity of $\mathcal{H}_k(N)$):

$$\Phi(f)(T_1) = a_1(f) = 1.$$

This proves that $\Phi(f)$ is a ring homomorphism (note that it suffices to check the multiplicativity on a set of generators – given the additivity).

'$\Rightarrow$': If $\Phi(f)$ is a ring homomorphism, then

$$a_n(Tf) = \Phi(Tf)(T_n) = a_1(TT_n f) = \Phi(f)(TT_n) = \Phi(f)(T)\Phi(f)(T_n) = \Phi(f)(T) a_n(f)$$

for all $n \geq 1$ showing that $Tf = \lambda f$ with $\lambda = \Phi(f)(T)$ (note that we again have to worry about the 0-th coefficient, but, as before, it suffices that the other coefficients agree to conclude that the 0-th one does as well). □

2 Integral structures in Hecke algebras

The **aim** of this section is to prove that $\mathbb{T}_k(N)$ is an integral structure in $\mathcal{H}_k(N)$. For $N = 1$ there is an elementary proof requiring ony Eisenstein series and Ramanujan's Δ-function. For computations, this is also very handy, since it uses the Victor-Miller basis. See William Stein's book and the appendix to this section.

Let R be any commutative ring and $n \geq 0$. We denote by $R[X,Y]_n$ the R-module consisting of the homogeneous polynomials of degree n in the two variables X, Y. It carries a left $\mathrm{SL}_2(\mathbb{Z})$-action:

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

This part actually requires the knowledge of some group cohomology. We will just give an ad hoc definition of H^1.

Definition 2.1. *Let* G *be a group and* M *an* $R[G]$*-module. Define the* R*-module of* 1-cocycles *as*

$$Z^1(G,M) := \{f : G \to M \text{ map} \mid f(gh) = g.f(h) + f(g)\}$$

and the R-module of 1-coboundaries *as*

$$B^1(G,M) := \{f : G \to M \text{ map} \mid \exists m \in M \text{ s.t. } f(g) = (g-1).m \text{ for all } g \in G\}.$$

One checks immediately that $B^1(G,M)$ is an R-submodule of $Z^1(G,M)$. The first group cohomology of G and M *is defined as the R-module*

$$H^1(G,M) := Z^1(G,M)/B^1(G,M).$$

We will now assume $k \geq 2$ and obtain the required integral structure from the following theorem of Eichler and Shimura. In order to be able to state it, we need a fact (see Peter Bruin's lectures?):

Fact 2.2. *Let $k \geq 2$. We have that $H^1(\Gamma_1(N), \mathbb{C}[X,Y]_{k-2})$ is a finite dimensional $\mathbb{C}$-vector space, which is equipped with Hecke operators T_n for $n \in \mathbb{N}$ (coming from the correspondences on modular curves that can also be used to define Hecke operators on modular forms).*

Theorem 2.3 (Eichler-Shimura)**.** *Let $k \geq 2$ and fix $z_0 \in \mathbb{H}$, the upper half plane. Then the map*

$$M_k(N) \oplus \overline{S_k(N)} \to H^1(\Gamma_1(N), \mathbb{C}[X,Y]_{k-2})$$

given by

$$(f, \overline{g}) \mapsto (\gamma \mapsto \int_{z_0}^{\gamma z_0} f(z)(Xz+Y)^{k-1}dz + \int_{z_0}^{\gamma z_0} \overline{g}(z)(X\overline{z}+Y)^{k-1}d\overline{z})$$

is an isomorphism of $\mathbb{C}$-vector spaces, which is compatible with the Hecke operators T_n for $n \in \mathbb{N}$.

By $\overline{S_k(N)}$ we denote the space of anti-holomorphic cusp forms, i.e. the complex conjugates of the usual cusp forms.

Corollary 2.4. *The Hecke algebras $\mathcal{H}_k(N)$ (and $\mathbb{T}_k(N)$) coincide with the $\mathbb{C}$-subalgebra (the $\mathbb{Z}$-subalgebra) of $\mathrm{End}_{\mathbb{C}}(H^1(\Gamma_1(N), \mathbb{C}[X,Y]_{k-2}))$ generated by the T_n for $n \in \mathbb{N}$.*

Proof. This follows immediately from the compatibility of the isomorphism of Theorem 2.3 for the Hecke action. □

Since we are at some point going to switch from $M_k(N)$ to $S_k(N)$ we mention that there is a natural $\mathbb{C}$-subspace $H^1_{\text{par}}(\Gamma_1(N), \mathbb{C}[X,Y]_{k-2})$ of $H^1(\Gamma_1(N), \mathbb{C}[X,Y]_{k-2})$ such that the isomorphism from Eichler-Shimura restricts to an isomorphism

$$S_k(N) \oplus \overline{S_k(N)} \to H^1_{\text{par}}(\Gamma_1(N), \mathbb{C}[X,Y]_{k-2}).$$

This allows us to obtain the same results, which we will show below, for the cusp spaces, too.

We need one more (rather easy) fact.

Fact 2.5. *We have*

$$H^1(\Gamma_1(N), \mathbb{Z}[X,Y]_{k-2})/\text{torsion} \otimes_{\mathbb{Z}} \mathbb{C} \cong H^1(\Gamma_1(N), \mathbb{C}[X,Y]_{k-2})$$

and the Hecke operators T_n for $n \in \mathbb{N}$ can already be defined on the left hand side,

In fact, for $N \geq 4$, there is no torsion. The torsion elements have order only divisible by 2 and/or 3 and come from non-trivial stabilisers for the action of $\Gamma_1(N)$ on the upper half plane.

Corollary 2.6. *The $\mathbb{C}$-vector space $H^1(\Gamma_1(N), \mathbb{C}[X,Y]_{k-2})$ has a basis with respect to which all Hecke operators T_n for $n \in \mathbb{N}$ have integral matrix entries.*

Proof. Any $\mathbb{Z}$-basis of $H^1(\Gamma_1(N), \mathbb{Z}[X,Y]_{k-2})/\text{torsion}$ is automatically a $\mathbb{C}$-basis of the $\mathbb{C}$-vector space $H^1(\Gamma_1(N), \mathbb{C}[X,Y]_{k-2})$ and, of course, the matrix entries for this basis are integral. □

Now consider the following injection:

$$\mathcal{H}_k(N) \hookrightarrow \text{End}_{\mathbb{C}}(H^1(\Gamma_1(N), \mathbb{C}[X,Y]_{k-2})) \cong \text{Mat}_{m\times m}(\mathbb{C}),$$

where we make the last identification with respect to the above basis, guaranteeing that the Hecke operators T_n have integral matrix entries. Under this injection, $\mathbb{T}_k(N)$ is hence sent into $\text{Mat}_{m\times m}(\mathbb{Z})$, i.e. we have the injection

$$\mathbb{T}_k(N) \hookrightarrow \text{Mat}_{m\times m}(\mathbb{Z}).$$

Now we draw our conclusions:

Corollary 2.7. *The natural map $\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{T}_k(N) \to \mathcal{H}_k(N)$ is an isomorphism. In particular, $\mathbb{T}_k(N)$ is free as $\mathbb{Z}$-module (i.e. abelian group) of rank equal to the $\mathbb{C}$-dimension of $\mathcal{H}_k(N)$.*

Hence, $\mathbb{T}_k(N)$ is an integral structure in $\mathcal{H}_k(N)$.

Proof. We have seen that $\mathbb{T}_k(1)$ lies in $\text{Mat}_{m\times m}(\mathbb{Z})$, which we write more formally as a (ring) injection

$$\iota : \mathbb{T}_k(N) \hookrightarrow \text{Mat}_{m\times m}(\mathbb{Z}).$$

Recall that $\mathbb{C}$ is a flat $\mathbb{Z}$-module, hence, tensoring with $\mathbb{C}$ over $\mathbb{Z}$ preserves injections, yielding

$$\text{id} \otimes \iota : \mathbb{C} \otimes_{\mathbb{Z}} \mathbb{T}_k(N) \hookrightarrow \mathbb{C} \otimes_{\mathbb{Z}} \text{Mat}_{m\times m}(\mathbb{Z}) \cong \text{Mat}_{m\times m}(\mathbb{C}),$$

where the last isomorphism can be seen as $\mathbb{C} \otimes_{\mathbb{Z}} (\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}) \cong (\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{Z}) \oplus (\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{Z}) \oplus (\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{Z}) \oplus (\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{Z}) \cong \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$. The image of $\text{id} \otimes \iota$ lies in $\mathcal{H}_k(N)$ and contains all T_m, whence the image is $\mathcal{H}_k(N)$, proving the isomorphism $\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{T}_k \cong \mathcal{H}_k(N)$.

It follows immediately that $\mathbb{T}_k(N)$ is a free $\mathbb{Z}$-module of rank equal to the dimension of $\mathcal{H}_k(N)$. □

Appendix: Proof in level 1 using Eisenstein series

The input to this proof are the following standard facts from modular forms courses:

Lemma 2.8. *(a) The Eisenstein series $E_4 \in M_4(1)$ and $E_6 \in M_6(1)$ have a Fourier expansion with integral coefficients and 0-th coefficient equal to 1. Ramanujan's $\Delta \in M_{12}(1)$ is a cusp form with integral Fourier expansion and 1-st coeffient equal to 1.*

(b) Let $f \in M_k(N)$ be a modular form with an integral Fourier expansion. Then $T_n(f)$ also has an integral Fourier expansion.

(c) For any k, we have $M_{k+12} = \Delta \cdot M_k \oplus \mathbb{C}E_4^\alpha E_6^\beta$, where $\alpha, \beta \in \mathbb{N}_0$ are any elements such that $k+12 = 4\alpha+6\beta$ (which always exist since k is even – otherwise we're dealing with the 0-space).

This can be used to construct a Victor-Miller basis of $M_k(1)$ (say, its dimension is n), that is any basis of the $\mathbb{C}$-vector space $M_k(1)$ consisting of modular forms $f_0, f_2, \ldots, f_{n-1}$ with integral Fourier coefficients such that

$$a_i(f_j) = \delta_{i,j}$$

for all $0 \leq i, j \leq n-1$.

How to construct such a basis? We do it inductively. For $k = 4, 6, 8, 10, 14$ the existence is obvious, since the space $M_k(1)$ is 1-dimensional and the Eisenstein series does the job. For $k = 12$, we start with $E_6^2 = 1 - 1008q + \ldots$ and $\Delta = q + \ldots$, so that we can take $f_0 = E_6^2 + 1008\Delta$ and $f_1 = \Delta$.

Suppose now that we have a Victor-Miller basis $f_0, \ldots, f_{n-1}$ of $M_k(N)$. For $i = 0, \ldots, n-1$, let $g_{i+1} := \Delta f_i$ and $g_0 := E_4^\alpha E_6^\beta$. This is not a Victor-Miller basis, in general, but can be made into one. Note first that $a_i(g_i) = 1$ for all $0 \leq i \leq n$ and that $a_j(g_i) = 0$ for all $0 \leq i \leq n$ and all $0 \leq j < i$. Graphically, it looks like this:

$$\begin{array}{rccccc}
g_0 = 1+ & \bullet q+ & \bullet q^2 + \ldots & \ldots+ & \bullet q^{n-1}+ & \bullet q^n \\
g_1 = & q+ & \bullet q^2 + \ldots & \ldots+ & \bullet q^{n-1}+ & \bullet q^n \\
g_2 = & & q^2 + \ldots & \ldots+ & \bullet q^{n-1}+ & \bullet q^n \\
\vdots & & & & & \\
g_{n-1} = & & & & q^{n-1}+ & \bullet q^n \\
g_n = & & & & & q^n
\end{array}$$

I think that it is now obvious how to make this basis into a Victor-Miller one.

Proposition 2.9. *Let $\{f_0, \ldots, f_{n-1}\}$ be a Victor-Miller basis of $M_k(1)$. Then the Hecke operators T_m, written as matrices with respect to the Victor-Miller basis, have integral entries.*

Proof. In order to write down the matrix, we must determine $T_m f_i$ for all $0 \leq i \leq n-1$ in terms of the basis. But, this is trivial: If

$$T_m f_i = a_{i,0} + a_{i,1} q + a_{i,2} q^2 + \cdots + a_{i,n-1} q^{n-1} + \ldots,$$

then $T_m f_i = \sum_{j=0}^{n-1} a_{i,j} f_j$, so the $a_{i,j}$ are just the entries of the matrix. They are integral, as $T_m f_i$ has integral Fourier coefficients (using here that all the f_i do). □

3 Integral structures on modular forms

In this section we are going to use the statements derived from the Key Corollary to deduce from the integral structure on the Hecke algebras the promised integral structure on modular forms.

We first recall the important isomorphism

$$\Phi : M_k(N) \to \mathrm{Hom}_{\mathbb{C}}(\mathcal{H}_k(N), \mathbb{C}), \quad f \mapsto (T_n \mapsto a_1(T_n f) = a_n(f)).$$

Its inverse is the following

$$\Psi : \mathrm{Hom}_{\mathbb{C}}(\mathcal{H}_k(N), \mathbb{C}) \to M_k(N), \quad \varphi \mapsto a_0(\varphi) + \sum_{n=1}^{\infty} \varphi(T_n) e^{2\pi i z}.$$

Here, $a_0(\varphi)$ is uniquely determined, but, I do not know of a simple way to write down what it actually is (except for $N = 1$).

Corollary 3.1. *(a) $\mathbb{T}_k(N)$ is a $\mathbb{Z}$-algebra that is finite and free as a $\mathbb{Z}$-module of $\mathbb{Z}$-rank equal to* $\dim_{\mathbb{C}} M_k(N)$.

(b) We have isomorphisms of $\mathbb{C}$-vector spaces (we will also call it Ψ)

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_k(N), \mathbb{C}) \cong \mathrm{Hom}_{\mathbb{C}}(\mathcal{H}_k(N), \mathbb{C}) \overset{\psi}{\cong} M_k(N).$$

(c) Under the isomorphism from (b), the ring homomorphisms $\mathbb{T}_k(N) \to \mathbb{C}$ correspond bijectively to the normalised Hecke eigenforms.

Proof. All three statements become immediately clear if one chooses some identification of $\mathbb{T}_k(N)$ with $\mathbb{Z}^r$, where r is the $\mathbb{Z}$-rank of $\mathbb{T}_k(N)$, which by the integral structure and the duality between Hecke algebras and modular forms is equal to the $\mathbb{C}$-dimension of $M_k(N)$. □

Very explicitly, we now have the $\mathbb{C}$-linear isomorphism

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_k(N), \mathbb{C}) \to M_k(N), \quad f \mapsto (T_n \mapsto a_1(T_n f) = a_n(f)).$$

Definition 3.2. *Let R be any ring. We let*

$$M_k(N)(R) := \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_k(N), R)$$

and call this the modular forms of weight k and level N with coefficients in R.

In particular, $M_k(N)(\mathbb{Z})$ is the subset of $M_k(N)$ consisting of such f such that all $a_n(f)$ are integers for all $n \geq 1$. Note, however, that $a_0(f)$ may nevertheless not be an integer (see, for instance, the slightly differently normalised Eisenstein series $\frac{2k}{B_k}E_k = \frac{2k}{B_k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n)e^{2\pi inz}$ (it actually is a normalised eigenform in the sense that we defined above).

Lemma 3.3. *Let $R \to S$ be a ring homomorphism. Then we have*

$$S \otimes_R M_k(N)(R) \cong M_k(N)(S).$$

Proof. $S \otimes_R M_k(N)(R) = S \otimes_R \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_k(N), R) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_k(N), S) \cong M_k(N)(S)$. □

In particular, we have

$$\mathbb{C} \otimes_{\mathbb{Z}} M_k(N)(\mathbb{Z}) = M_k(N)(\mathbb{C}) \cong M_k(N),$$

where the final isomorphism comes from the above corollary.

4 Coefficients of normalised Hecke eigenforms

Let us recall from the previous section that we have the isomorphism

$$\Phi : M_k(N) \to M_k(N)(\mathbb{C}) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_k(N), \mathbb{C}),$$

given by sending f to the map defined by $T_n \mapsto a_1(T_n f) = a_n(f)$. Recall further that we showed in Corollary 1.4 that under this isomorphism normalised Hecke eigenforms correspond bijectively to the ring homomorphisms in $\mathrm{Hom}_{\mathbb{C}}(\mathcal{H}_k(N), \mathbb{C}) \cong \mathrm{Hom}_{\mathbb{C}}(\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{T}_k(N), \mathbb{C}) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_k(N), \mathbb{C})$.

Let now $f \in M_k(N)$ be a normalised Hecke eigenform and consider $\varphi := \Phi(f)$, which is thus a ring homomorphism

$$\varphi : \mathbb{T}_k(N) \to \mathbb{C}.$$

Its kernel $\ker(\varphi)$ is a prime ideal of $\mathbb{T}_k(N)$ (since factoring it out yields a subring of $\mathbb{C}$ and thus an integral domain). The image of φ is the smallest subring of $\mathbb{C}$ containing all $\varphi(T_n) = a_n(f)$, i.e. $\mathrm{im}(\varphi) = \mathbb{Z}[a_n(f) \mid n \in \mathbb{N}] =: \mathbb{Z}_f$. Its field of fractions is denoted by $\mathbb{Q}_f$ and called the *coefficient field of f*. It is explicitly given as $\mathbb{Q}(a_n(f) \mid n \in \mathbb{N})$.

Now we use that $\mathbb{T}_k(N)$ is of finite $\mathbb{Z}$-rank. Then, of course, so is $\mathbb{T}_k(N)/\ker(\varphi) \cong \mathbb{Z}_f$. Consequently, also $\mathbb{Q}_f$ is of finite $\mathbb{Q}$-dimension. That means that $\mathbb{Q}_f$ is a number field and $\mathbb{Z}_f$ is an order in it. This is a highly non-trivial result! Recall that $\mathbb{Q}_f$ is generated over $\mathbb{Q}$ by infinitely many numbers, namely, the $a_n(f)$; nevertheless, all of them are contained in a finite extensions! This is a consequence of the existence of the integral structure (on Hecke algebras: $\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{T}_k(N) \cong \mathcal{H}_k(N)$, which we derived from the Eichler-Shimura isomorphism).

Moreover, as $\mathbb{Z}_f$ is of finite $\mathbb{Z}$-rank, every element of $\mathbb{Z}_f$ is integral over $\mathbb{Z}$, i.e. an *algebraic integer*. By definition an element $x \in \mathbb{C}$ is an algebraic integer if there is a nonzero monic (leading coefficient equal to 1 – if we leave out this assumption, then we only finite algebraic numbers and not

algebraic integers) polynomial $q \in \mathbb{Z}[X]$ such that $q(x) = 0$. For later use, we denote the set of all algebraic integers by $\overline{\mathbb{Z}}$ and the set of all algebraic numbers by $\overline{\mathbb{Q}}$ (which is also the algebraic closure of $\mathbb{Q}$ inside $\mathbb{C}$).

Let us summarise:

Corollary 4.1. *Let $f \in M_k(N)$ be a normalised Hecke eigenform. Then its Fourier coefficients $a_n(f)$ for $n \in \mathbb{N}$ are algebraic integers. Moreover, $\mathbb{Z}_f$ is an order in the number field $\mathbb{Q}_f$.*

5 Background on Galois theory

Let L/K be a field extension, that is, L is a field and K is a subfield of L. By restricting the multiplication map $L \times L \to L$ to $K \times L \to L$, we obtain a K-scalar multiplication on L, making L into a K-vector space. The *degree* of the field extension L/K is the K-dimension of L, notation:

$$[L : K] := \dim_K L.$$

A field extension is called *finite* if its degree is finite.

Let us look at some examples:

(a) $\mathbb{C}/\mathbb{R}$ is a field extension of degree 2 and an $\mathbb{R}$-basis of $\mathbb{C}$ is given by 1 and i.

(b) $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a field extension of degree n.

(c) $\mathbb{C}/\mathbb{Q}$ is a field extension of infinite (even uncountable) degree.

(d) $\overline{\mathbb{F}}_p/\mathbb{F}_p$ is an infinite field extension.

Here I take a shortcut and deviate from the standard definition of Galois extensions, by giving the following equivalent one: We denote by $\mathrm{Aut}_K(L)$ the group of field automorphisms $\sigma : L \to L$ such that their restriction to K is the identity (note that any field homomorphism is automatically injective).

Let us first assume that $[L : K] < \infty$. Then one can show that one always has:

$$\#\,\mathrm{Aut}_K(L) \leq [L : K].$$

(This is not so difficult to show: One can always write $L = K[X]/(f)$, where f is an irreducible polynomial of degree $[L : K]$. Let us fix one root α (in $\overline{K}$) of f. Then every field automorphism $L \to L$ is uniquely determined by the image of α. But, this image must be another root of f, hence, there are at most $[L : K]$ different choices, proving the claim.)

A finite field extension L/K is called *Galois* if we actually have equality, i.e.

$$\#\,\mathrm{Aut}_K(L) = [L : K].$$

In that case we write $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ and call this the *Galois group of* L/K.

We again look at some examples:

(a) $\mathbb{C}/\mathbb{R}$ is Galois and its Galois group has order 2 and consists of the identity and complex conjugation.

(b) $\mathbb{F}_{p^n}/\mathbb{F}_p$: Since we are in characteristic p, the *Frobenius* map $\mathrm{Frob}_p : x \mapsto x^p$ is a field automorphism of $\mathbb{F}_{p^n}$ (the point is that it is additive! That clearly fails over $\mathbb{C}$, for instance). Using that $\mathbb{F}_{p^n}^\times$ is a cyclic group of order $p^n - 1$, one immediately gets that $x^{p^n} = x$ in $\mathbb{F}_{p^n}$. This shows that $(\mathrm{Frob}_p)^n$ is the identity. But, it also shows that there is $x \in \mathbb{F}_{p^n}$ such that $(\mathrm{Frob}_p)^i(x) = x^{p^i} \neq x$ for all $i = 1, \ldots, n-1$. This shows that Frob_p has order n. Consequently, we have found n field automorphisms, namely, the powers of Frob_p. Thus, $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension and its Galois group is cyclic of order n generated by Frob_p.

(c) Let ζ be a primitive ℓ^n-th root of unity inside $\overline{\mathbb{Q}}$ (where ℓ is a prime number). Explicitly, we can take $\zeta = e^{2\pi i/\ell^n}$. We consider the field extension $\mathbb{Q}(\zeta)/\mathbb{Q}$. Here $\mathbb{Q}(\zeta)$ is the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and ζ. It is not so difficult to show that one has

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(\ell^n) = (\ell - 1)\ell^{n-1}.$$

Let $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta))$. Then we have

$$1 = \sigma(1) = \sigma(\zeta^{\ell^n}) = (\sigma(\zeta))^{\ell^n},$$

showing that $\sigma(\zeta)$ is another ℓ^n-th root of 1. As σ is invertible, $\sigma(\zeta)$ must also be primitive (i.e. have order ℓ^n). This means that there is an element $\overline{\chi}_{\ell^n}(\sigma) \in (\mathbb{Z}/(\ell^n))^\times$ such that $\sigma(\zeta) = \zeta^{\overline{\chi}_{\ell^n}(\sigma)}$ (the complicated notation becomes clear below). Let us write this as a map:

$$\overline{\chi}_{\ell^n} : \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) \to (\mathbb{Z}/(\ell^n))^\times.$$

Note that this map is surjective (for any $i \in (\mathbb{Z}/(\ell^n))^\times$ define a field automorphism uniquely by sending ζ to ζ^i). Thus, $\mathbb{Q}(\zeta)/\mathbb{Q}$ is also a Galois extension. In fact, it is trivially checked that χ_{ℓ^n} is a group homomorphism. Thus, $\overline{\chi}_{\ell^n}$ is a group isomorphism between the Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ and $(\mathbb{Z}/(\ell^n))^\times$.

We still have to mention the case of infinite L/K. Also, here I take a shortcut and give a non-standard but equivalent definition. A (possibly infinite degree) field extension L/K is *Galois* if L is the union of all finite Galois subextensions M/K, i.e.

$$L = \bigcup_{K \subseteq M \subseteq L,\ M/K \text{ finite Galois}} M.$$

In that case, we also write $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$. In fact, one has

$$\mathrm{Gal}(L/K) = \varprojlim_{K \subseteq M \subseteq L,\ M/K \text{ finite Galois}} \mathrm{Gal}(M/K).$$

Then, $\mathrm{Gal}(L/K)$ is in fact a topological group, more precisely, it is a profinite group. A topological group is called *profinite* if it is compact, Hausdorff and totally disconnected (that is, the connected component containing some x is equal to $\{x\}$). We must always keep this topology in mind!

As an example we now look at $\overline{\mathbb{F}}_p/\mathbb{F}_p$. We clearly have

$$\overline{\mathbb{F}}_p = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n},$$

since any element in $\overline{\mathbb{F}}_p$ is contained in some finite extension $\mathbb{F}_{p^n}$. Hence, this is a Galois extension (in fact, for any field F the extension $\overline{F}/F$, where $\overline{F}$ is an algebraic closure of F, is a Galois extension, by the properties of an algebraic closure). We thus have

$$\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \varprojlim_{n\in\mathbb{N}} \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/(n) =: \hat{\mathbb{Z}} = \langle \mathrm{Frob}_p \rangle_{\text{top. gp.}}.$$

This means that the Galois group is a pro-cyclic group (by definition, this is the projective limit of cyclic groups), and, equivalently, that it is topologically generated by a single element, namely the Frobenius.

6 Background on the ℓ-adic numbers

Recall from your Analysis class that $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the usual absolute value: it can be defined as the quotient of all Cauchy sequences modulo those sequences that tend to 0. In this way, one 'adds' to $\mathbb{Q}$ all the 'limits' of all Cauchy sequences.

There is nothing that prevents one to make the same construction for another absolute value. It may seem astonishing that there are other (signifiacantly different) absolute values than the usual one: Let ℓ be a prime number. For $a \in \mathbb{Z}$, write $a = \ell^r a'$ with $\gcd(a', \ell) = 1$, let

$$|a|_\ell := \ell^{-r};$$

and for $\frac{a}{b} \in \mathbb{Q}$, let

$$|\frac{a}{b}|_\ell := \frac{|a|_\ell}{|b|_\ell}.$$

One easily checks that this definition satisfies all properties of an absolute value on $\mathbb{Q}$.

The completion of $\mathbb{Q}$ with respect to $|\cdot|_\ell$ is called the field of *ℓ-adic numbers* and denoted as $\mathbb{Q}_\ell$. For us, the following subring is important:

$$\mathbb{Z}_\ell := \{x \in \mathbb{Q}_\ell \mid |x|_\ell \leq 1\}.$$

There are more explicit ways of seeing $\mathbb{Q}_\ell$ and $\mathbb{Z}_\ell$, for instance, in terms of ℓ-adic expansions. I am not going into that here (see, for instance, the wikipedia page). But, I want to mention the following abstract alternative:

$$\mathbb{Z}_\ell = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/(\ell^n).$$

Then $\mathbb{Q}_\ell$ is the field of fractions of $\mathbb{Z}_\ell$.

7 Background on Galois representations

Let K be a (topological) field and $F/\mathbb{Q}$ a number field. A continous group homomorphism

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(K)$$

is called an *n-dimensional Galois representation*. More precisely, if

- $K = \mathbb{C}$, then ρ is called an *Artin representation*,
- $K/\mathbb{Q}_\ell$, then ρ is called an *ℓ-adic Galois representation*,
- $K/\mathbb{F}_\ell$, then ρ is called a *(residual) mod ℓ Galois representation*. In this case, K is equipped with the discrete topology.

Proposition 7.1. *(a) Any Artin and any mod-ℓ Galois representation has a finite image.*

(b) Let $K/\mathbb{Q}_\ell$ be a finite extension. Any $\rho : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(K)$ is equivalent (i.e. conjugate) to a representation of the form $\mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\mathcal{O}_K)$, where $\mathcal{O}_K$ is the valuation ring of K (i.e. the integral closure of $\mathbb{Z}_\ell$ in K, sometimes also called the ring of integers of K). Consequently, by composing with $\mathcal{O}_K \twoheadrightarrow \mathcal{O}_K/(\pi_K) \cong \mathbb{F}_{\ell^d}$, where π_K is a uniformiser of $\mathcal{O}_K$ (for some $d \in \mathbb{N}$), we obtain a mod ℓ Galois representation

$$\overline{\rho} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_n(\mathbb{F}_{\ell^d}),$$

called the residual representation of ρ.

Proof. (a) The image of the compact group $\mathrm{Gal}(\overline{F}/F)$ under the continuous map ρ is compact. As it is also discrete (that's trivial for mod ℓ representations, for Artin representations one has to work a bit), it is finite.

(b) For short, we write $\mathcal{O} := \mathcal{O}_K$ and $G := \mathrm{Gal}(\overline{F}/F)$. Define

$$U := \{g \in G \mid \rho(g)\mathcal{O}^n \subseteq \mathcal{O}^n\}.$$

It is clearly a subgroup of G. We want to show that it is open.

For $i = 1, \dots, n$ consider the map $\alpha_i : G \to K^n$ given by $g \mapsto \rho(g)e_i$, where e_i is the i-th standard basis vector. By the continuity of ρ, the α_i are continuous maps. Note that $\alpha_i^{-1}(\mathcal{O}^n)$ is the set of $g \in G$ such that the i-th column of $\rho(g)$ has entries lying in $\mathcal{O}$ (instead of only in K). Consequently, we find

$$U = \bigcap_{i=1}^{n} \alpha_i^{-1}(\mathcal{O}^n),$$

which is clearly open as the intersection of finitely many open sets.

Since $U \leq G$ is an open subgroup and G is compact, the index of U in G is finite. Let $G = \bigsqcup_{i=1}^{m} g_i U$ be a coset decomposition. Then $L := \sum_{i=1}^{m} \rho(g_i)\mathcal{O}^n \subset K^n$ is a finitely generated $\mathcal{O}$-submodule such that its K-span is all of K^n (in other words, L is an $\mathcal{O}$-lattice in K). The point about L is that it is stable under the G-action, i.e. ρ factors as

$$\rho : G \to \mathrm{Aut}_{\mathcal{O}}(L) \subset \mathrm{Aut}_K(K^n) \cong \mathrm{GL}_n(K).$$

Choosing any $\mathcal{O}$-basis of L, we identify $\mathrm{Aut}_{\mathcal{O}}(L)$ with $\mathrm{GL}_n(\mathcal{O})$, finishing the proof. □

The residual representation defined in (b) above depends on the choice of lattice! But, if we take the semi-simplification of the residual representation, then the Brauer-Nesbitt theorem implies that there is no such dependence (Reason: The Brauer-Nesbitt theorem states that a semi-simple representation is uniquely (up to isomorphism) determined by its character, which is just the mod π_K reduction of the character of ρ.).

From now on we take $F = \mathbb{Q}$ for simplicity. We now give a very important example in dimension 1: the *ℓ-adic cyclotomic character*. Recall from above that we found the group isomorphism:

$$\overline{\chi}_{\ell^n} : \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) \to (\mathbb{Z}/(\ell^n))^{\times}.$$

Let us rewrite this, using the group surjection $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$:

$$\overline{\chi}_{\ell^n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_1(\mathbb{Z}/(\ell^n)).$$

We can now take the projective limit to obtain the *ℓ-adic cyclotomic character*

$$\chi_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{Z}_\ell^{\times} \cong \mathrm{GL}_1(\mathbb{Z}_\ell).$$

Recall that the construction of $\mathbb{Q}_\ell$ was very analogous to the construction of $\mathbb{R}$. This leads us to consider the Galois extensions $\mathbb{C}/\mathbb{R}$ and $\overline{\mathbb{Q}}_p/\mathbb{Q}_p$ in as analogous a way as possible. We start with the first one, which is easier.

Recall that $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is a group of order 2 consisting of the identity and complex conjugaction, denoted by c. By restricting these elements to $\overline{\mathbb{Q}}$ (note that the complex conjugate of an algebraic number is another algebraic number), we obtain an injection

$$\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

We will still denote the image of complex conjugation in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ by c.

A 2-dimensional Galois representation

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

is called *odd* if $\det(\rho(c)) = -1$.

I should point out that there is actually a choice that we made: we see $\overline{\mathbb{Q}}$ inside $\mathbb{C}$ in the 'natural way'. But, there are infinitely many other embeddings of $\overline{\mathbb{Q}}$ into $\mathbb{C}$ and we could have restricted to $\overline{\mathbb{Q}}$

via these embeddings. This would have led to a conjugate embedding of $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. But, as the determinant is independent of conjugation, the notion of oddness does not depend on any choice!

Now we proceed analogously with $\overline{\mathbb{Q}}_p/\mathbb{Q}_p$. We choose an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. Restricting field automorphisms to $\overline{\mathbb{Q}}$ via this embedding we obtain as above an embedding

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \hookrightarrow \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}).$$

Another embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_p$ would have led to a conjugate embedding of the Galois group. We must always keep this in mind!

Whereas $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ is a very simple group (order 2), the group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ is much more complicated (it is uncountable). It turns out to be very useful to identify a certain normal subgroup in it, the inertia group, which we define now. It is not so difficult to show that one can let any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ act on $\overline{\mathbb{F}}_p$ (since σ respects $\overline{\mathbb{Z}}_p$, that is, the elements that are integral over $\mathbb{Z}_p$, we can let σ act on $\overline{\mathbb{F}}_p$ by reduction modulo p, by which I mean the image of a fixed ring surjection $\overline{\mathbb{Z}}_p \twoheadrightarrow \overline{\mathbb{F}}_p$), and that the resulting group homomorphism $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is surjective. We let I_p be the kernel of this homomorphism; this is the *inertia group at* p.

We say that a Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(K)$ is *unramified at* p if I_p is in its kernel.

Recall that $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is topologically generated by the Frobenius Frob_p. Let $\widetilde{\mathrm{Frob}}_p$ be any preimage of Frob_p in $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. If ρ is unramified at p, then $\rho(\widetilde{\mathrm{Frob}}_p)$ does not depend on the choice of preimage and we simple write $\rho(\mathrm{Frob}_p)$ (note that this expression does not make sense at all if ρ is not unramified at p).

Now recall further that the embedding of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ into $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is only well-defined up to conjugation. Hence, one must be very careful when speaking about Frob_p as an element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. It would be much better to only speak of its conjugacy class. However, the important role is actually played by the characteristic polynomial of $\rho(\mathrm{Frob}_p)$, which by linear algebra only depends on the conjugacy class. Hence, and this is the conclusion to remember from this discussion, one can without any ambiguity speak of the characteristic polynomial of $\rho(\mathrm{Frob}_p)$ for any prime p at which ρ is unramified.

8 The Galois representation attached to a modular form

In this section, I only state the main theorem about Galois representations attached to modular forms and try to illustrate its significance in a toy example. For every prime ℓ we fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$.

Theorem 8.1 (Eichler, Shimura, Igusa, Deligne, Serre)**.** *Let $f \in S_k(N)$ be a normalised Hecke eigenform ($k \geq 1$). Then for every prime number ℓ there is an irreducible Galois representation*

$$\rho_{f,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$$

such that

- *$\rho_{f,\ell}$ is unramified at all primes $p \nmid N\ell$ and*
- *the characteristic polynomial of $\rho_{f,\ell}(\mathrm{Frob}_p)$ for any $p \nmid N\ell$ is equal to*

$$X^2 - a_p(f)X + p^{k-1} \in \overline{\mathbb{Q}}_\ell[X],$$

where $a_p(f) \in \overline{\mathbb{Q}}$ is considered inside $\overline{\mathbb{Q}}_\ell$ via the fixed embedding.

The content of the theorem is the deep arithmetic meaning of the Fourier coefficients of a Hecke eigenform which was alluded to in the beginning of this lecture series. The coefficient a_p knows about the Frobenius at p! This may sound very abstract and it might not at all be evident why this is number theory. So, I just want to give a very brief sketch of a toy example.

Question: Let $Q \in \mathbb{Z}[X]$ be a polynomial. How does this polynomial factor modulo p?

Let us first look at $Q(X) = X^2 + 1$. Of course, it quickly turn out that Q has two distinct factors modulo p if and only if $p \equiv 1 \pmod 4$. If $p \equiv 3 \pmod 4$, the polynomial remains irreducible modulo p, and $p = 2$ plays a special role (a double factor: $X^2 + 1 \equiv (X + 1)^2 \pmod 2$).

Now, take a more complicated example (still a toy one!!): $Q(X) = X^6 - 6X^4 + 9X^2 + 23$. Compute factorisations modulo p for some small p with the computer and try to find a pattern! It won't be easy at all (I'd be astonished if you found one without reading on)! But, there is one: There is a unique Hecke eigenform f in $S_1(23)(\mathbb{F}_7)$ (this is with a certain quadratic Dirichlet character); you can also see it in weight 7 or in weight 2 for level $7 \cdot 23$. The pattern is the following. Let p be a prime. Then (with finitely many exceptions):

- Q has 2 factors modulo $p \Leftrightarrow a_p(f) = 6$.
- Q has 3 factors modulo $p \Leftrightarrow a_p(f) = 0$.
- Q has 6 factors modulo $p \Leftrightarrow a_p(f) = 2$.

This comes from the attached Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_7)$. There are only the following matrices in the image of ρ:

$$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right), \quad \left(\begin{smallmatrix}2&0\\0&4\end{smallmatrix}\right), \quad \left(\begin{smallmatrix}4&0\\0&2\end{smallmatrix}\right), \quad \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \quad \left(\begin{smallmatrix}0&2\\4&0\end{smallmatrix}\right), \quad \left(\begin{smallmatrix}0&4\\2&0\end{smallmatrix}\right).$$

The first one has order 1 and trace 2, the second and third have order 3 and trace 6, and the final ones have order 2 and trace 0.

The polynomial Q is Galois over $\mathbb{Q}$. For a given p, $\rho(\mathrm{Frob}_p)$ must be one of these matrices. If the trace is 2, then $\rho(\mathrm{Frob}_p)$ must be the identity and thus have order 1. That means that Q factors completely modulo p (there's a small issue with primes dividing the index of the equation order generated by Q in the maximal order – these primes are next to 7 and 23 the finitely many exceptions mentioned above). If the trace is 0, then the order has to be 2, leading to a factorisation of Q into three fractors modulo p. In the remaining case the trace is 6 and the order is 3, so that Q has three factors modulo p.

9 Galois representations and Hecke algebras of weight one

The last part of my lecture was devoted to my preprint *On Galois Representations of Weight One*, which can be found on arXiv. There is no need to reproduce it here.