Lectures on
Modular Galois Representations Modulo Prime Powers

Gabor Wiese

9th December 2011

Abstract

This is a sketch of the content of my three lectures during the PhD School *Modular Galois Representations Modulo Prime Powers*, held in Copenhagen from 6/12/2011 until 9/12/2011, organised by Ian Kiming. Thanks Ian!

1 Modular Forms Modulo Prime Powers

Modular forms, in their classical appearance (19th century! Eisenstein, Weierstraß, Jacobi, Poincaré, etc.) and in the way one usually gets to know them during one's studies, are objects of Complex Analysis: holomorphic functions satisfying a certain transformation rule. Many have an evident number theoretic significance (they were studied because of this!), like the n-th Fourier coefficient of the Eisenstein series E_k being $\sigma_{k-1}(n) = \sum_{0<d|n} d^{k-1}$. But, it is a highly non-trivial step to 'transport' modular forms from Analysis to Algebra, i.e. to identify an algebraic structure, or, even stronger, an integral structure, on the complex vector space of modular forms. This was achieved by Hecke, Eichler and Shimura. Without that we would not be able to do anything of what we are doing this week, and it is probably fair to say that without that Fermat's last theorem would not have been proved. So, this first lecture is mainly concerned with integral structures on modular forms. Finally, it will be used to introduce modular forms modulo prime powers, as an application.

A reference where most of the content of this lecture is worked out are my lecture notes [4].

1.1 Hecke algebras and general q-expansions

Definition 1.1. *Let $M_k(N)$ be the $\mathbb{C}$-vector space of modular forms of weight k and level N (either $\Gamma_1(N)$ or $\Gamma_0(N)$ – doesn't matter for us). By $S_k(N)$ we denote the cuspidal subspace.*

Let $\mathcal{H}_k(N)$ be the $\mathbb{C}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(M_k(N))$ generated (as $\mathbb{C}$-algebra) by the Hecke operators T_n for $n \in \mathbb{N}$.

Let $\mathbb{T}_k(N)$ be the subring of $\mathrm{End}_{\mathbb{C}}(M_k(N))$ generated (as a ring, i.e. as a $\mathbb{Z}$-algebra) by the Hecke operators T_n for $n \in \mathbb{N}$.

Both $\mathcal{H}_k(N)$ and $\mathbb{T}_k(N)$ are called Hecke algebra of weight k and level N.

It is well-known that the Hecke algebra $\mathcal{H}_k(N)$ (and thus also $\mathbb{T}_k(N)$) is commutative. As it is commutative, in $M_k(N)$ there are modular forms that are eigenvectors for all Hecke operators T_n: These are called *(Hecke) eigenforms*. Let $f = \sum_{n=0}^{\infty} a_n(f)q^n$ be such an eigenform (we write $q = q(z) = e^{2\pi iz}$). We say that it is *normalised* if $a_1(f) = 1$.

One can compute directly that the level one Eisenstein series E_k are Hecke eigenforms (for all k). One also trivially gets an eigenform if the space of modular (cuspidal) forms is 1-dimensional. This proves that the Ramanujan $\Delta \in S_{12}(1)$ is a Hecke eigenform.

The following simple lemma, which is a direct consequence of the description of Hecke operators on Fourier expansions of modular forms, turns out to be the key to everything that follows.

Lemma 1.2. *Suppose $f = \sum_{n=0}^{\infty} a_n(f)q^n \in M_k(N)$ be a modular form of weight k and level N. Then for all $n \geq 1$ we have $a_1(T_n f) = a_n(f)$.*

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

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

Proposition 1.3. *Suppose $k \geq 1$. The complex q-pairing is non-degenerate. In particular, we have the isomorphism*

$$\Phi : M_k(N) \cong \mathrm{Hom}_{\mathbb{C}}(\mathcal{H}_k(N), \mathbb{C}), \quad f \mapsto \Phi(f), \text{ where } \Phi(f)(T) = a_1(Tf).$$

It is useful to point out that $\Phi(f)$ maps T_n to $a_1(T_n f) = a_n(f)$.

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 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 $a_1(T(T_n f)) = a_1(T_n Tf) = a_n(Tf) = 0$ for all f and all n, whence $Tf = 0$ for all f. As the Hecke algebra is defined as a subring in the endomorphism of $M_k(N)$, 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!

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. Then*

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

Moreover, Φ from Proposition 1.3 gives a bijection

$$\{\text{Normalised eigenforms in } M_k(N)\} \leftrightarrow \mathrm{Hom}_{\mathbb{C}-\text{alg}}(\mathcal{H}_k(N), \mathbb{C}).$$

Proof. 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 the first statement. Furthermore:

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

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).

Conversely, 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). □

1.2 Existence of integral structures on Hecke algebras

Note that by definition $\mathbb{T}_k(N)$ is a subring of $\mathcal{H}_k(N)$. The main point is to see that $\mathbb{T}_k(N)$ is an integral structure of $\mathcal{H}_k(N)$. We first prove this in the level 1 case, which requires least machinery. Then, we prove it in general by citing the Eichler-Shimura theorem, as well as facts on modular symbols.

1.2.1 Proof in level 1 using Eisenstein series

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

Lemma 1.5. *(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 1.6. *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). □

Now we draw our conclusions:

Corollary 1.7. *The natural map $\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{T}_k(1) \to \mathcal{H}_k(1)$ is an isomorphism. In particular, $\mathbb{T}_k(1)$ is free as $\mathbb{Z}$-module (i.e. abelian group) of rank equal to the $\mathbb{C}$-dimension of $\mathcal{H}_k(1)$.*

We say that $\mathbb{T}_k(1)$ is an integral structure in $\mathcal{H}_k(1)$.

Proof. Let us identify $\mathrm{End}_{\mathbb{C}}(M_k(1))$ with $\mathrm{Mat}_n(\mathbb{C})$ (with n the dimension of $M_k(1)$) by writing down the Hecke operators with respect to a Victor-Miller basis.

By Proposition 1.6, we have that $\mathbb{T}_k(1)$ lies in $\mathrm{Mat}_n(\mathbb{Z})$. Let us write this more formally as a (ring) injection

$$\iota : \mathbb{T}_k(1) \hookrightarrow \mathrm{Mat}_n(\mathbb{Z}).$$

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

$$\mathrm{id} \otimes \iota : \mathbb{C} \otimes_{\mathbb{Z}} \mathbb{T}_k \hookrightarrow \mathbb{C} \otimes_{\mathbb{Z}} \mathrm{Mat}_n(\mathbb{Z}) \cong \mathrm{Mat}_n(\mathbb{C}),$$

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 $\mathrm{id} \otimes \iota$ lies in $\mathcal{H}_k(1)$ and contains all T_m, whence the image is $\mathcal{H}_k(1)$, proving the isomorphism $\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{T}_k \cong \mathcal{H}_k(1)$.

It follows immediately that $\mathbb{T}_k(1)$ is a free $\mathbb{Z}$-module of rank equal to the dimension of $\mathcal{H}_k(1)$. □

What happened? The only non-trivial thing we used is that we could write down our Hecke operators as matrices with integral entries. For higher levels this also works, but, I do not know of a proof as easy as this one. We'll derive it from the Eichler-Shimura isomorphism.

1.2.2 General proof using Eichler-Shimura

In the level 1 situation we obtained Hecke operators with integral matrix entries by proving the existence of a 'good basis' consisting of modular forms with integral Fourier coefficients and exploiting the fact that Hecke operators preserve the subset of modular forms with integral Fourier coefficients. In the general level case, it is easier to obtain an integral structure not in the space of modular forms directly, but, in an other $\mathbb{C}$-vector space, a certain group cohomology space (or, a modular symbols space – see below).

We do not define group cohomology here. An account is given in my lecture notes [4].

The group $\mathrm{SL}_2(\mathbb{Z})$ acts on a polynomial $f(X,Y)$ (in two variables) from the left as follows:

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

By $R[X,Y]_{k-2}$ we denote the R-module of polynomials in two variables which are homogeneous of degree $k-2$ (for $k \geq 2$) with coefficients in any commutative ring R. It is possible to define Hecke operators T_n for $n \in \mathbb{N}$ on the group cohomology space $\mathrm{H}^1(\Gamma_1(N), R[X,Y]_{k-2})$ (also for $\Gamma_0(N)$) and on the parabolic subspace $\mathrm{H}^1_{\mathrm{par}}(\Gamma_1(N), R[X,Y]_{k-2})$.

Theorem 1.8 (Eichler-Shimura)**.** *Let $k \geq 2$. Then there are natural isomorphisms*

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

and

$$S_k(N) \oplus S_k(N) \cong \mathrm{H}^1_{\mathrm{par}}(\Gamma, \mathbb{C}[X,Y]_{k-2}),$$

which are compatible with the Hecke operators, where Γ is $\Gamma_1(N)$ or $\Gamma_0(N)$ (just as before).

The 'natural isomorphism' is actually given by integration (not so difficult!). The lecture notes [4] contain a description and a proof (which is probably not the most elegant one).

Corollary 1.9. *The Hecke algebra $\mathcal{H}_k(N)$ (resp. $\mathbb{T}_k(N)$) is isomorphic to the $\mathbb{C}$-subalgebra (resp. the subring) of $\mathrm{End}_{\mathbb{C}}(\mathrm{H}^1(\Gamma, \mathbb{C}[X,Y]_{k-2}))$ generated by T_n for $n \in \mathbb{N}$.*

Proof. A Hecke operator on $M_k(N) \oplus S_k(N)$ can be written as a block matrix (T, T') where T' is the restriction of T to $S_k(N)$. Sending (T, T') to T defines a homomorphism from the Hecke algebra on $\mathrm{H}^1(\Gamma, \mathbb{C}[X,Y]_{k-2})$ to the one on $M_k(N)$, which is clearly surjective as all generators (the T_n) are hit. It is injective, because if T is zero, then so is T'. □

From the standard resolution for definining group cohomology it is very easy to deduce that $\mathrm{H}^1(\Gamma, \mathbb{Z}[X,Y]_{k-2})_{\mathrm{free}}$ is an integral structure of $\mathrm{H}^1(\Gamma, \mathbb{C}[X,Y]_{k-2})$ in the sense that it is a subgroup and

$$\mathbb{C} \otimes_{\mathbb{Z}} \mathrm{H}^1(\Gamma, \mathbb{Z}[X,Y]_{k-2})_{\mathrm{free}} \cong \mathrm{H}^1(\Gamma, \mathbb{C}[X,Y]_{k-2}).$$

If M is any finitely generated $\mathbb{Z}$-module, then it is the direct sum of a free $\mathbb{Z}$-module and the torsion submodule: $M \cong M_{\mathrm{free}} \oplus M_{\mathrm{torsion}}$, where $M_{\mathrm{free}} = M/M_{\mathrm{torsion}}$. Note that the Hecke operators on $\mathrm{H}^1(\Gamma, \mathbb{Z}[X,Y]_{k-2})$ send torsion elements to torsion elements, and, thus give rise to Hecke operators on $\mathrm{H}^1(\Gamma, \mathbb{Z}[X,Y]_{k-2})_{\mathrm{free}}$ by modding out the torsion submodule.

Now, we can draw the same conclusion as in the level 1 case: The Hecke operators T_n can be written as matrices with integral entries, hence, $\mathbb{T}_k(N) \leq \mathrm{Mat}_n(\mathbb{Z})$, where n is the $\mathbb{C}$-dimension of $\mathrm{H}^1(\Gamma, \mathbb{C}[X,Y]_{k-2})$, which is equal to the $\mathbb{Z}$-rank of $\mathrm{H}^1(\Gamma, \mathbb{Z}[X,Y]_{k-2})$.

So, again by the flatness of $\mathbb{C}$ as $\mathbb{Z}$-module, we obtain, precisely as earlier:

Theorem 1.10 (Shimura??)**.** $\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{T}_k(N) \cong \mathcal{H}_k(N)$.

Note that our proof requires $k \geq 2$. For $k = 1$, I am not aware of a proof along the above lines. However, it is known that the result of the theorem is true nevertheless. This one proves using the algebraic geometric description of modular forms due to Katz, which is beyond the scope of this lecture.

1.2.3 General proof using modular symbols

Personally, I like group cohomology much better than modular symbols (at least, if one defines modular symbols in the way I am going to do in this section, namely, as an abstract formalism) because working with group cohomology one has all the tools from that theory at one's disposal.

However, modular symbols (the formalism) is precisely what is implemented in Magma and Sage (by William Stein, principally). Moreover, the definitions are so short that they easily fit into this lecture (at least the typed version), whereas a good definition of group cohomology doesn't.

Recall that the projective line over $\mathbb{Q}$ can be seen as $\mathbb{Q} \cup \{\infty\}$ and that it carries the natural left $\mathrm{SL}_2(\mathbb{Z})$-action by fractional linear combinations: $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \frac{x}{y} = \frac{ax+by}{cx+dy}$, where ∞ is treated in the obvious way, namely, as $\frac{1}{0}$.

Definition 1.11. *Let R be a commutative ring and write Γ for Γ or $\Gamma_0(N)$, as well as $V = R[X,Y]_{k-2}$ for some $k \geq 2$. We define the R-modules*

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

and

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

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

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

for the left diagonal Γ-action.

(a) We call the Γ-coinvariants

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

the space of modular symbols of level N and weight k.

(b) We call the Γ-coinvariants

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

the space of boundary symbols of level N and weight k.

(c) We define the boundary map *as the map*

$$\mathcal{M}_k(N;R) \to \mathcal{B}_k(N;R)$$

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 $\mathcal{CM}_k(N;R)$ and is called the space of cuspidal modular symbols of level N and weight k.

We now give the definition of the Hecke operator T_ℓ for a prime ℓ on $\Gamma_0(N)$ (the definition on $\Gamma_1(N)$ is slightly more involved). The T_n for composite n can be computed from those by the usual formulae. A matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Mat}_2(\mathbb{Z})$ with non-zero determinant acts on $\mathcal{M}_k(N;R)$ by the diagonal action on the tensor product. Let $x \in \mathcal{M}_k(N;R)$. We put

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

where

$$\begin{aligned} \mathcal{R}_\ell &:= \{\left(\begin{smallmatrix} 1 & r \\ 0 & \ell \end{smallmatrix}\right) | 0 \le r \le \ell - 1\} \cup \{\left(\begin{smallmatrix} \ell & 0 \\ 0 & 1 \end{smallmatrix}\right)\}, && \text{if } \ell \nmid N \\ \mathcal{R}_\ell &:= \{\left(\begin{smallmatrix} 1 & r \\ 0 & \ell \end{smallmatrix}\right) | 0 \le r \le \ell - 1\}, && \text{if } \ell \mid N. \end{aligned}$$

It is very easy to see that $\mathcal{M}_k(N;\mathbb{Z})_{\mathrm{free}} = \mathcal{M}_k(N;\mathbb{Z})/\mathcal{M}_k(N;\mathbb{Z})_{\mathrm{torsion}}$ is an integral structure in $\mathcal{M}_k(N;\mathbb{C})$, so Hecke operators on $\mathcal{M}_k(N;\mathbb{C})$ can be written as matrices with integral entries.

Modular symbols (over $\mathbb{C}$) describe the first homology of Γ for the module $\mathbb{C}[X,Y]_{k-2}$ (or the first homology of the modular curve Y_Γ – this comes with a caveat because we must pay attention whether we should not use compactly supported cohomology at some places; if we work with X_Γ and cuspidal modular symbols, everything is simpler). As homology and cohomology are dual to each other (at least in good situations), we have:

Proposition 1.12. *There is a non-degenerate pairing*

$$\mathrm{H}^1(\Gamma, \mathbb{C}[X,Y]_{k-2}) \times \mathcal{M}_k(N;\mathbb{C}) \to \mathbb{C}.$$

It follows that the Hecke algebra on $\mathrm{H}^1(\Gamma, \mathbb{C}[X,Y]_{k-2})$ is isomorphic to the one on $\mathcal{M}_k(N;\mathbb{C})$, where the isomorphism is simply given by transposing the matrices (wrt. to a fixed basis, say, of $\mathcal{M}_k(N;R)$) because the two spaces are dual to each other by the virtue of the pairing.

Consequently, we can again prove the isomorphism $\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{T}_k(N) \cong \mathcal{H}_k(N)$ by using the Hecke operators on $\mathcal{M}_k(N;\mathbb{Z})_{\mathrm{free}}$ (which, of course, can be represented by matrices with integral entries), again for $k \ge 2$.

1.3 Exploiting integral structures on Hecke algebras

We are now exploiting consequences of $\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{T}_k(N) \cong \mathcal{H}_k(N)$.

Corollary 1.13. *(a)* $\mathbb{T}_k(N)$ *is a free* $\mathbb{Z}$*-module of rank equal to the* $\mathbb{C}$*-dimension of* $\mathcal{H}_k(N)$*, which is equal to the* $\mathbb{C}$*-dimension of* $M_k(N)$ *by Proposition 1.3.*

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

(c) The $\mathbb{Z}$*-algebra homomorphisms in* $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_k(N), \mathbb{C})$ *correspond bijectively (under the mapping of the previous item) to the normalised Hecke eigenforms of* $M_k(N)$.

Proof. That the natural maps are isomorphisms is immediately clear if we write $\mathbb{T}_k(N) = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$. □

Now, we do not need $\mathcal{H}_k(N)$ anymore. We will only work with $\mathbb{T}_k(N)$.

The modular forms in $M_k(N)$ correspond to the group homomorphisms $\mathbb{T}_k(N) \to \mathbb{C}$.
The normalised eigenforms in $M_k(N)$ correspond to the ring homomorphisms $\mathbb{T}_k(N) \to \mathbb{C}$.

We include a short interlude on commutative algebra(s). Recall that a ring is called Artinian if every descending ideal chain becomes stationary. This is the case for $\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{T}_k(N)$ because it is a finite dimensional $\mathbb{F}_p$-vector space, so that ideals are subspaces, and, of course, chains of subspaces thus have to become stationary for dimension reasons. For the same reason, also $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{T}_k(N)$ is Artinian, but $\mathbb{T}_k(N)$, of course, is not!

Proposition 1.14. *Let R be an Artinian ring.*

(a) Every prime ideal of R is maximal.

(b) There are only finitely many maximal ideals in R.

(c) Let $\mathfrak{m}$ be a maximal ideal of R. It is the only maximal ideal containing $\mathfrak{m}^\infty$.

(d) Let $\mathfrak{m} \neq \mathfrak{n}$ be two maximal ideals. For any $k \in \mathbb{N}$ and $k = \infty$ the ideals $\mathfrak{m}^k$ and $\mathfrak{n}^k$ are coprime.

(e) The Jacobson radical $\bigcap_{\mathfrak{m} \in \mathrm{Spec}(R)} \mathfrak{m}$ is equal to the nilradical and consists of the nilpotent elements.

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

(g) (Chinese Remainder Theorem) The natural map

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

is an isomorphism.

(h) For every maxmimal ideal $\mathfrak{m}$, the ring $R/\mathfrak{m}^\infty$ is local with maximal ideal $\mathfrak{m}$ and is hence isomorphic to $R_{\mathfrak{m}}$, the localisation of R at $\mathfrak{m}$.

The Hecke algebra $\mathbb{T}_k(N)$ satisfies the assumptions (and hence the conclusions) of the following proposition.

Proposition 1.15. *Let $\mathbb{T}$ be a $\mathbb{Z}$-algebra which is free of finite rank r as a $\mathbb{Z}$-module. Let $\mathbb{T}_{\mathbb{Q}} := \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{T}$.*

(a) $\mathbb{Z} \subseteq \mathbb{T}$ is an integral ring extension.

(b) $\mathbb{T}$ *is equidimensional of Krull dimension* 1*, meaning that every maximal ideal* $\mathfrak{m}$ *of* $\mathbb{T}$ *contains at least one minimal prime ideal* $\mathfrak{p}$ *and there is no prime ideal strictly included between* $\mathfrak{p}$ *and* $\mathfrak{m}$*.*

(c) $\mathbb{T}/\mathfrak{m}$ *is a finite field of degree at most* r *over the prime field,* $\mathbb{T}/\mathfrak{p}$ *is an order in a number field of degree at most* r *over* $\mathbb{Q}$*.*

(d) $\mathbb{T}_{\mathbb{Q}}$ *is an Artin* $\mathbb{Q}$*-algebra of dimension* r*. As such it satisfies:* $\mathbb{T}_{\mathbb{Q}} \cong \prod_{\mathfrak{p} \lhd \mathbb{T}_{\mathbb{Q}} \text{ prime}} (\mathbb{T}_{\mathbb{Q}})_{\mathfrak{p}}$ *(localisation at* $\mathfrak{p}$*).*

(e) The embedding $\iota : \mathbb{T} \hookrightarrow \mathbb{T}_{\mathbb{Q}}$ *induces a bijection (via preimages) between the (finitely many) prime ideals of* $\mathbb{T}_{\mathbb{Q}}$ *(which are all maximal) and the minimal prime ideals of* $\mathbb{T}$*. The inverse is given by extension.*

The proofs of the two propositions are not difficult. We will now exploit them for our purposes. Let us write $\mathbb{T}_k(N)_{\mathbb{Q}} := \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{T}_k(N)$ (similarly to the use in the previous proposition).

We now consider ring homomorphisms $f : \mathbb{T}_k(N) \to \mathbb{C}$ in more detail.

Proposition 1.16. *Let* $f : \mathbb{T}_k(N) \to \mathbb{C}$ *be a ring homomorphism and let* $\mathfrak{p}_f$ *be its kernel.*

(a) $\mathfrak{p}_f$ *is a minimal prime ideal of* $\mathbb{T}_k(N)$*.*

(b) The image of f *is an order* $\mathbb{Z}_f$ *(the* coefficient ring of f*) in a number field* $\mathbb{Q}_f$ *(the* coefficient field of f*), which can be explicitly described as* $\mathbb{Z}_f = \mathbb{Z}[f(T_n) \mid n \geq 1]$ *and* $\mathbb{Q}_f = \mathbb{Q}(f(T_n) \mid n \geq 1)$*. Moreover,* $[\mathbb{Q}_f : \mathbb{Q}] \leq \dim_{\mathbb{C}} M_k(N)$*.*

(c) $f : \mathbb{T}_k(N) \to \mathbb{C}$ *extends to a* $\mathbb{Q}$*-linear map* $\mathbb{T}_k(N)_{\mathbb{Q}} \to \mathbb{C}$*, whose kernel is the maximal ideal which is the extension of* $\mathfrak{p}_f$ *(in accordance to the correspondence in Proposition 1.15). Conversely, every* $f : \mathbb{T}_k(N) \to \mathbb{C}$ *arises by restriction from a* $\mathbb{Q}$*-algebra homomorphism* $\mathbb{T}_k(N)_{\mathbb{Q}} \to \mathbb{C}$*.*

(d) Let $f : \mathbb{T}_k(N)_{\mathbb{Q}} \to \mathbb{C}$ *be a normalised Hecke eigenform and* $\phi \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$ *be a field automorphism. Then* $g := \phi \circ f$ *is another normalised Hecke eigenform, having the same kernel. In this case, we say that* f *and* g *are* $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$*-conjugated.*

Conversely, suppose that $f, g : \mathbb{T}_k(N)_{\mathbb{Q}} \to \mathbb{C}$ *have the same kernel. Then they are* $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$*-conjugated. Hence, the* $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$*-conjugacy classes are in bijection with the maximal ideals of* $\mathbb{T}_k(N)_{\mathbb{Q}}$*.*

(e) The local factors in $\mathbb{T}_k(N)_{\mathbb{Q}} \cong \prod_{\mathfrak{p} \lhd \mathbb{T}_k(N)_{\mathbb{Q}} \text{ prime}} (\mathbb{T}_k(N)_{\mathbb{Q}})_{\mathfrak{p}}$ *correspond to the* $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$*-conjugacy classes.*

Proof. A rough sketch only. Nothing is difficult and everything can be done as an exercise! Of course, the kernel $\mathfrak{p}$ is an ideal. It is prime because $\mathbb{T}_k(N)/\mathfrak{p}_f$ is a subring of $\mathbb{C}$ (hence, an integral domain), which is equal to the image of f. As $\mathbb{T}_k(N)$ is generated by the T_n, the image is generated by the values $f(T_n)$, i.e. is equal to $\mathbb{Z}_f$. By Proposition 1.15, $\mathbb{Z}_f$ is an order in the integers of a number field,

which is, of course, the fraction field of $\mathbb{Z}_f$, i.e. $\mathbb{Q}_f$. We can also see $\mathbb{Q}_f$ as the image of the induced homomorphism of $\mathbb{Q}$-algebras: $\mathbb{T}_k(N)_{\mathbb{Q}} \to \mathbb{C}$, showing that the $\mathbb{Q}$-dimension of $\mathbb{Q}_f$ can be at most the $\mathbb{Q}$-dimension of $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{T}_k(N)$, which is equal to the $\mathbb{Z}$-rank of $\mathbb{T}_k(N)$, which in turn is equal to the $\mathbb{C}$-dimension of $M_k(N)$, as already pointed out.

If $f, g : \mathbb{T}_k(N)_{\mathbb{Q}} \to \mathbb{C}$ have the same kernel, then $\mathbb{Q}_f$ and $\mathbb{Q}_g$ are isomorphic as field extensions of $\mathbb{Q}$. To see that f and g are conjugate, it suffices to lift this field isomorphism to an automorphism of $\mathbb{C}$, which can be done by a standard result from Galois theory. □

Note the obvious corollary for a normalised eigenform $f \in M_k(N)$: $\mathbb{Z}_f = \mathbb{Z}[a_n(f) \mid n \geq 1]$ is an order in the number field $\mathbb{Q}_f = \mathbb{Q}(a_n(f) \mid n \geq 1)$. This is much less trivial than it might look!

The coefficients $a_n(f)$ (for $n \geq 1$) of a normalised eigenform f are algebraic integers. Adjoining the infinitely many $a_n(f)$ (for $n \geq 1$), one only gets a finite extension of $\mathbb{Q}$.

Warning: This does not say anything about $a_0(f)$ and the same conclusion is wrong, in general! For instance, $E_{12} = \frac{691}{65520} + 1 + \sum_{n \geq 2} \sigma_{11}(n) q^n$ is a normalised eigenform, but a_0 is not an integer!

So, we are on the safe side working with cusp forms (all the above holds for cusp forms!). Or, we just disregard a_0, since it is uniquely determined anyway (as long as $k \geq 1$, what we are assuming).

1.4 Modular forms with coefficients in a ring

Let R be a commutative ring.

Definition 1.17. *A* modular form of weight k and level N with coefficients in R *is a group homomorphism:*

$$f : \mathbb{T}_k(N) \to R.$$

We use the notation $M_k(N)(R) := \mathrm{Hom}(\mathbb{T}_k(N), R)$ *for these.*

A weak Hecke eigenform of weight k and level N with coefficients in R *is a ring homomorphism:*

$$f : \mathbb{T}_k(N) \to R.$$

A weak Hecke eigenform $f : \mathbb{T}_k(N) \to R$ *is called* strong *if there is a normalised Hecke eigenform* $g \in M_k(N)$ *and a ring homomorphism* $\alpha : \mathbb{Z}_g \to R$ *such that* $f = \alpha \circ \Phi(g)$. *In this case, we have* $a_n(f) = \alpha(a_n(g))$ *for all* $n \geq 1$.

In analogy to normalised eigenforms in $M_k(N)$, we should actually always insert the word 'normalised' also in this definition, but, I prefer not to do it. It may even happen that I drop the word 'Hecke' form 'Hecke eigenform'. Hopefully, no confusion will arise.

We shall occasionally write $a_n(f)$ for $f(T_n)$ (as we already did in the definition) and think of f as the formal q-expansion $\sum_{n=1}^{\infty} a_n(f) q^n \in R[[q]]$ (note: we disregard a_0 due to the problems pointed out above).

Lemma 1.18. *Let* $R \to S$ *be a ring homomorphism. Then* $S \otimes_R M_k(N)(R) \cong M_k(N)(S)$.

Proof. We know that $\mathbb{T}_k(N)$ is a free $\mathbb{Z}$-module of some finite rank d. Hence: $S \otimes_R M_k(N)(R) \otimes_R S = S \otimes_R \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_k(N), R) \cong S \otimes_R \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^d, R) \cong S \otimes_R R^d \cong S^d \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^d, S) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_k(N), S) = M_k(N)$. □

Corollary 1.19. *We have $M_k(N)(\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C} \cong M_k(N)(\mathbb{C}) \cong M_k(N)$.*

Hence, $M_k(N)(\mathbb{Z})$, the modular forms with integral Fourier expansion, form an integral structure in the $\mathbb{C}$-vector space of modular forms $M_k(N)$.

1.5 Mod p modular forms

We now specialise to 'mod p' modular forms. Let p be a prime. We fix an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$.

Definition 1.20. *A modular form of weight k and level N with coefficients in $\overline{\mathbb{F}}_p$ is also called a* mod p modular form of weight k and level N. *Similarly, we define* weak mod p Hecke eigenforms.

Put $\mathbb{T}_k(N)_{\mathbb{F}_p} := \mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{T}_k(N) = \mathbb{T}_k(N)/p\mathbb{T}_k(N)$.

We continue with an abstract statement from commutative algebra (complementing Proposition 1.15), now focussing on mod p reductions. Its proof is not difficult and can be done as an exercise.

Proposition 1.21. *Let $\mathbb{T}$ be a $\mathbb{Z}$-algebra which is free of finite rank r as a $\mathbb{Z}$-module. Let $\mathbb{T}_{\mathbb{F}_p} := \mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{T}$.*

(a) $\mathbb{T}_{\mathbb{F}_p}$ is an Artin $\mathbb{F}_p$-algebra of dimension r. As such it satisfies: $\mathbb{T}_{\mathbb{F}_p} \cong \prod_{\mathfrak{m} \lhd \mathbb{T}_{\mathbb{F}_p} \text{ prime}} (\mathbb{T}_{\mathbb{F}_p})_{\mathfrak{m}}$ (localisation at $\mathfrak{m}$).

(b) The projection $\pi : \mathbb{T} \twoheadrightarrow \mathbb{T}_{\mathbb{F}_p}$ induces a bijection (via preimages) between the (finitely many) prime ideals of $\mathbb{T}_{\mathbb{F}_p}$ (which are all maximal) and the maximal prime ideals of $\mathbb{T}_{\mathbb{F}_p}$ of residue characteristic p. The inverse is given by the image under π.

Let us study this definition in a way similar to Proposition 1.16.

Proposition 1.22. *Let $f : \mathbb{T}_k(N) \to \overline{\mathbb{F}}_p$ be a weak Hecke eigenform of level N and weight k. Let $\mathfrak{m}_f := \ker(f)$ be the kernel of f.*

(a) $\mathfrak{m}_f$ is a maximal ideal of $\mathbb{T}_k(N)$. It has height 1.

(b) The image of f is the finite extension $\mathbb{F}_{p,f}$ of $\mathbb{F}_p$ (inside $\overline{\mathbb{F}}_p$) generated by the $a_n(f) = f(T_n)$ for $n \geq 1$. The degree $[\mathbb{F}_{p,f} : \mathbb{F}_p]$ is at most $\dim_{\mathbb{C}} M_k(N)$.

(c) f factors through to give an $\mathbb{F}_p$-algebra homomorphism $\mathbb{T}_k(N)_{\mathbb{F}_p} \to \overline{\mathbb{F}}_p$, whose kernel is the maximal ideal which is the image of $\mathfrak{m}_f$ (in accordance to the correspondence in Proposition 1.21). Conversely, every $f : \mathbb{T}_k(N) \to \overline{\mathbb{F}}_p$ arises by restriction from an $\mathbb{F}_p$-algebra homomorphism $\mathbb{T}_k(N)_{\mathbb{F}_p} \to \overline{\mathbb{F}}_p$.

(d) Let $f : \mathbb{T}_k(N)_{\mathbb{F}_p} \to \overline{\mathbb{F}}_p$ be a normalised Hecke eigenform and $\phi \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ be a field automorphism. Then $g := \phi \circ f$ is another weak Hecke eigenform, having the same kernel. In this case, we say that f and g are $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-conjugated.

Conversely, suppose that $f, g : \mathbb{T}_k(N)_{\mathbb{F}_p} \to \overline{\mathbb{F}}_p$ have the same kernel. Then they are $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-conjugated. Hence, the $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-conjugacy classes are in bijection with the maximal ideals of $\mathbb{T}_k(N)_{\mathbb{F}_p}$.

(e) The local factors in $\mathbb{T}_k(N)_{\mathbb{F}_p} \cong \prod_{\mathfrak{m} \lhd \mathbb{T}_k(N)_{\mathbb{F}_p} \text{ prime}} (\mathbb{T}_k(N)_{\mathbb{F}_p})_{\mathfrak{m}}$ correspond to the $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-conjugacy classes.

Proof. The image of f is clearly the subfield generated by the $f(T_n)$. As $\mathbb{T}_k(N)$ is free as a $\mathbb{Z}$-module of rank $\dim_{\mathbb{C}} M_k(N)$, it is clear that the degree of $\mathbb{F}_{p,f}$ is bounded by this number. Hence, $\mathbb{T}_k(N)/\mathfrak{m}_f$ is a finite field, whence $\mathfrak{m}_f$ is maximal.

The rest is very similar to the proof of Proposition 1.16, using Proposition 1.21). □

Proposition 1.23 (Deligne-Serre lifting lemma)**.** *Every weak mod p Hecke eigenform is strong.*

Proof. Let $f : \mathbb{T}_k(N) \to \overline{\mathbb{F}}_p$ be a weak Hecke eigenform with kernel $\mathfrak{m}$. As the height of $\mathfrak{m}$ is 1, it contains a minimal prime ideal $\mathfrak{p}$. So, we have

$$f : \mathbb{T}_k(N) \twoheadrightarrow \mathbb{T}_k(N)/\mathfrak{p} \twoheadrightarrow \mathbb{T}_k(N)/\mathfrak{m} \subseteq \overline{\mathbb{F}}_p.$$

Recall that $\mathcal{O} := \mathbb{T}_k(N)/\mathfrak{p}$ is an order in a number field (being an integral domain that is integral over $\mathbb{Z}$ and of finite $\mathbb{Z}$-rank), so that we can view it as a subring of $\mathbb{C}$. Consequently, we obtain

$$g : \mathbb{T}_k(N) \twoheadrightarrow \mathbb{T}_k(N)/\mathfrak{p} \hookrightarrow \mathbb{C},$$

a normalised holomorphic eigenform with $\mathbb{Z}_g = \mathbb{T}_k(N)/\mathfrak{p}$, so that we may take α to be $\mathbb{T}_k(N)/\mathfrak{p} \twoheadrightarrow \mathbb{T}_k(N)/\mathfrak{m} \hookrightarrow \overline{\mathbb{F}}_p$. □

Next we study congruences mod p in terms of prime ideals.

Definition 1.24. *Let $f_1, f_2 \in M_k(N)$ be normalised Hecke eigenforms. We know $a_n(f_1), a_n(f_2) \in \overline{\mathbb{Z}}$ for all $n \geq 1$. We say that $f_1 \equiv f_2 \pmod{p}$ if $\overline{a_n(f_1)} = \overline{a_n(f_2)}$ for all $n \geq 1$, where we denote by $\bar{\cdot}$ the reduction homomorphism $\overline{\mathbb{Z}} \twoheadrightarrow \overline{\mathbb{F}}_p$.*

Proposition 1.25. *(a) If $f_1 \equiv f_2 \pmod{p}$, then there is a maximal ideal $\mathfrak{m}$ of $\mathbb{T}_k(N)$ containing both the minimal prime ideals $\mathfrak{p}_{f_1}$ and $\mathfrak{p}_{f_2}$.*

(b) Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}_k(N)$ which contains minimal prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$. Then there are normalised Hecke eigenforms $f_1, f_2 \in M_k(N)$ such that $f_1 \equiv f_2 \pmod{p}$ and $\mathfrak{p}_1 = \mathfrak{p}_{f_1}$ and $\mathfrak{p}_2 = \mathfrak{p}_{f_2}$.

Proof. (a) We look at the ring homomorphisms

$$f_i : \mathbb{T}_k(N) \to \mathbb{T}_k(N)/\mathfrak{p}_{f_i} = \mathbb{Z}_{f_i} \hookrightarrow \overline{\mathbb{Z}} \hookrightarrow \mathbb{C}$$

for $i = 1, 2$. We obtain the ring homomorphisms

$$\overline{f}_i : \mathbb{T}_k(N) \to \mathbb{T}_k(N)/\mathfrak{p}_{f_i} = \mathbb{Z}_{f_i} \hookrightarrow \overline{\mathbb{Z}} \twoheadrightarrow \overline{\mathbb{F}}_p$$

for $i = 1, 2$, satisfying $\overline{f}_1(T_n) = \overline{a_n(f_1)} = \overline{a_n(f_2)} = \overline{f}_2(T_n)$ for all $n \geq 1$. So, $\overline{f}_1 = \overline{f}_2$ (they agree on a set of generators). Consequently, their kernel is a maximal ideal (factoring it out, we get a finite field), which contains $\mathfrak{p}_{f_1}$ and $\mathfrak{p}_{f_2}$ (that is evident from the two previous displayed formula).

(b) We just turn the argumentation in (a) around. Given $\mathfrak{m}$ we can write the same ring homomorphism in two different ways:

$$\mathbb{T}_k(N) \twoheadrightarrow \mathbb{T}_k(N)/\mathfrak{p}_i \twoheadrightarrow \mathbb{T}_k(N)/\mathfrak{m} \hookrightarrow \overline{\mathbb{F}}_p$$

for $i = 1, 2$. By *choosing* an embedding $\mathbb{T}_k(N)/\mathfrak{p}_i \hookrightarrow \mathbb{C}$, we obtain normalised Hecke eigenforms $f_i : \mathbb{T}_k(N) \twoheadrightarrow \mathbb{T}_k(N)/\mathfrak{p}_i \hookrightarrow \mathbb{C}$ for $i = 1, 2$, which are congruent mod p. □

One can do the same argumentation with congruences 'outside D', where D is any integer. Then one should consider the Hecke algebra generated by all T_n with $(n, D) = 1$, whose structure theory works in the same way. For the sake of not making the exposition too complicated, I did not do this. It is an instructive exercise to check it.

An important point, however, is to note that $\mathbb{T}_k^{(D)}(N) \subseteq \mathbb{T}_k(N)$ is an integral ring extension, whence prime ideals of $\mathbb{T}_k^{(D)}(N)$ (corresponding to 'partial' q-expansions) can be lifted to prime ideals of $\mathbb{T}_k(N)$ (corresponding to 'complete' q-expansion) by 'going up' (a theorem from commutative algebra). (I note this here because it doesn't seem so trivial to establish a similar statement mod p^n.)

1.6 Classical modular forms with p-adic coefficients

This section is not about p-adic modular forms (in any sense). Ian and Panos will say something about them. It just treats modular forms with p-adic coefficients according to our definition of such.

Let R be a $\mathbb{Z}_p$-algebra, e.g. R could be (the integers of) a p-adic field (i.e. a finite field extension of $\mathbb{Q}_p$), $\overline{\mathbb{Q}}_p$, $\mathbb{C}_p$ or a finite extension of $\mathbb{F}_p$ or $\overline{\mathbb{F}}_p$. This is also case, in which we are mainly interested this week, for modular forms mod p^n (see below).

It is common practice to view holomorphic modular forms as modular forms with coefficients in $\mathbb{Q}_p$ by choosing (and fixing!) a field isomorphism $\mathbb{C} \cong \mathbb{Q}_p$ (which, of course, does not at all respect the topology!).

Put $\mathbb{T}_k(N)_{\mathbb{Z}_p} := \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{T}_k(N)$.

We continue with some general statements about finite free $\mathbb{Z}$-algebras, as in Propositions 1.15 and 1.21. Its proof is again a good exercise.

Proposition 1.26. *Let $\mathbb{T}$ be a $\mathbb{Z}$-algebra that is free of finite rank r as $\mathbb{Z}$-module. Write $\mathbb{T}_{\mathbb{Z}_p} := \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{T}$ and $\mathbb{T}_{\mathbb{Q}_p} := \mathbb{Q}_p \otimes_{\mathbb{Z}} \mathbb{T} = \mathbb{Q}_p \otimes_{\mathbb{Q}} \mathbb{T}_{\mathbb{Q}}$.*

(a) $\mathbb{T}_{\mathbb{F}_p} = \mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{T} = \mathbb{F}_p \otimes_{\mathbb{Z}_p} \mathbb{T}_{\mathbb{Z}_p}$.

(b) The embedding $\iota : \mathbb{T} \hookrightarrow \mathbb{T}_{\mathbb{Z}_p}$ *induces (by taking preimages) a bijection between the maximal prime ideals of* $\mathbb{T}_{\mathbb{Z}_p}$ *and the maximal ideals of* $\mathbb{T}$ *of residue characteristic* p*. The inverse is given by extension.*

(c) Consider the embedding $\iota : \mathbb{T}_{\mathbb{Q}} \hookrightarrow \mathbb{T}_{\mathbb{Q}_p}$*, which makes* $\mathbb{T}_{\mathbb{Q}_p}$ *into a* $\mathbb{T}_{\mathbb{Q}}$*-algebra, whence we have*

$$\mathbb{T}_{\mathbb{Q}_p} \cong \prod_{\mathfrak{p} \lhd \mathbb{T}_{\mathbb{Q}} \text{ prime}} (\mathbb{T}_{\mathbb{Q}_p})_{\mathfrak{p}},$$

by localising at the primes of $\mathbb{T}_{\mathbb{Q}}$*. Letting* $K = \mathbb{T}_{\mathbb{Q}}/\mathfrak{p}$ *and considering* $\mathbb{Q}_p \otimes_{\mathbb{Q}} K = \prod_{\mathfrak{P}} K_{\mathfrak{P}}$*, where the product runs through all prime ideals* $\mathfrak{P}$ *of* K *dividing* p*, it follows that*

$$(\mathbb{T}_{\mathbb{Q}_p})_{\mathfrak{p}} \cong \prod_{\mathfrak{P}} (\mathbb{T}_{\mathbb{Q}_p})_{\mathfrak{Q}},$$

where $\mathfrak{Q}$ *is the kernel of* $\mathbb{T}_{\mathbb{Q}_p} \to (\mathbb{T}_{\mathbb{Q}_p})_{\mathfrak{p}} \twoheadrightarrow \mathbb{T}_{\mathbb{Q}_p}/\mathfrak{p} = K \twoheadrightarrow K_{\mathfrak{P}}$*.*

So, a $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{C})$*-conjugacy class breaks into* $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$*-conjugacy classes according to the decomposition of* p *in* $\mathbb{T}_{\mathbb{Q}}/\mathfrak{p}$*.*

We now pass from finite free $\mathbb{Z}$-algebras to finite free $\mathbb{Z}_p$-algebras. The latter have an even nicer structure theory, very close to the Artinian case. The following proposition applies, in particular, with $\widehat{\mathbb{T}}_k(N) := \mathbb{T}_k(N)_{\mathbb{Z}_p}$.

Proposition 1.27. *Let* $\widehat{\mathbb{T}}$ *be a* $\mathbb{Z}_p$*-algebra that is free of finite rank* r *as* $\mathbb{Z}_p$*-module. Write* $\widehat{\mathbb{T}}_{\mathbb{Q}_p} := \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \widehat{\mathbb{T}}$ *and* $\widehat{\mathbb{T}}_{\mathbb{F}_p} := \mathbb{F}_p \otimes_{\mathbb{Z}_p} \widehat{\mathbb{T}}$*.*

(a) $\mathbb{Z}_p \subseteq \widehat{\mathbb{T}}$ *is an integral ring extension.*

(b) $\widehat{\mathbb{T}}$ *is equidimensional of Krull dimension* 1*.*

(c) The natural projection $\pi : \widehat{\mathbb{T}} \to \widehat{\mathbb{T}}_{\mathbb{F}_p}$ *induces (by taking preimages) a bijection between the finitely many prime ideals of* $\widehat{\mathbb{T}}_{\mathbb{F}_p}$ *(which are all maximal) and the maximal ideals of* $\widehat{\mathbb{T}}$*. The inverse is given by taking the image. Moreover,* $\mathbb{F}_p \otimes_{\mathbb{Z}_p} \widehat{\mathbb{T}}_{\mathfrak{m}} \cong (\widehat{\mathbb{T}}_{\mathbb{F}_p})_{\mathfrak{m}}$*,*

(d) $\widehat{\mathbb{T}}_{\mathbb{F}_p}$ *is an Artin* $\mathbb{F}_p$*-algebra of dimension* r*. As such it satisfies:* $\widehat{\mathbb{T}}_{\mathbb{F}_p} \cong \prod_{\mathfrak{m} \lhd \widehat{\mathbb{T}}_{\mathbb{F}_p} \text{ prime}} (\widehat{\mathbb{T}}_{\mathbb{F}_p})_{\mathfrak{m}}$*.*

(e) $\widehat{\mathbb{T}}/\mathfrak{m}$ *is a finite field of degree at most* r *over* $\mathbb{F}_p$*,* $\widehat{\mathbb{T}}/\mathfrak{p}$ *is an order in a* p*-adic field of degree at most* r *over* $\mathbb{Q}_p$*.*

(f) $\widehat{\mathbb{T}} \cong \prod_{\mathfrak{m}} \widehat{\mathbb{T}}_{\mathfrak{m}}$*, where the product runs over all maximal ideals of* $\widehat{\mathbb{T}}$ *and* $\widehat{\mathbb{T}}_{\mathfrak{m}}$ *denotes the localisation of* $\widehat{\mathbb{T}}$ *at* $\mathfrak{m}$*.*

(g) $\widehat{\mathbb{T}}_{\mathbb{Q}_p}$ *is an Artin* $\mathbb{Q}_p$*-algebra of dimension* r*. As such it satisfies:* $\widehat{\mathbb{T}}_{\mathbb{Q}_p} \cong \prod_{\mathfrak{p} \lhd \widehat{\mathbb{T}}_{\mathbb{Q}_p} \text{ prime}} (\widehat{\mathbb{T}}_{\mathbb{Q}_p})_{\mathfrak{p}}$*.*

(h) The embedding $\iota : \widehat{\mathbb{T}} \hookrightarrow \widehat{\mathbb{T}}_{\mathbb{Q}_p}$ induces a bijection (via preimages) between the (finitely many) prime ideals of $\widehat{\mathbb{T}}_{\mathbb{Q}_p}$ (which are all maximal) and the minimal prime ideals of $\widehat{\mathbb{T}}$. The inverse is given by extension.

The proof of this proposition is precisely the same as what was done earlier, with the exception of (f). This, one obtains, by Hensel lifting the idempotents of the decompositon in (d).

Now we apply this to modular forms with coefficients in a $\mathbb{Z}_p$-algebra. The proof of the following proposition is again an instructive exercise without any greater difficulties.

Proposition 1.28. *Let R be a $\mathbb{Z}_p$-algebra and $f : \mathbb{T}_k(N) \to R$ a weak Hecke eigenform.*

(a) f extends to $f : \widehat{\mathbb{T}}_k(N) := \mathbb{T}_k(N)_{\mathbb{Z}_p} \to R$, by multiplying with the scalar. Let $\mathfrak{a} := \ker(f)$ be the kernel of f.

(b) By choosing a maximal ideal $\mathfrak{m} \lhd \widehat{\mathbb{T}}_k(N)$ containing $\mathfrak{a}$, we obtain a $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-conjugacy class of weak (and, hence, even strong) mod p eigenforms by $\widehat{\mathbb{T}}_k(N) \twoheadrightarrow \widehat{\mathbb{T}}_k(N)/\mathfrak{a} \twoheadrightarrow \widehat{\mathbb{T}}_k(N)/\mathfrak{m} \hookrightarrow \overline{\mathbb{F}}_p$.

(c) If R is local, then the $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-conjugacy class from (b) is unique and we denote a member of it by $\overline{f}$.

(d) The decomposition $\widehat{\mathbb{T}}_k(N) \cong \prod_{\mathfrak{m} \lhd \widehat{\mathbb{T}}_k(N) \text{ maximal}} \mathbb{T}_k(N)_{\mathfrak{m}}$ corresponds to the distinct residual $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$-conjugacy classes.

(e) $\widehat{\mathbb{T}}_k(N)_{\mathbb{Q}_p} \cong \prod_{\mathfrak{m} \lhd \widehat{\mathbb{T}}_k(N) \text{ maximal}} \big(\prod_{\mathfrak{p} \subset \mathfrak{m} \text{ minimal}} (\widehat{\mathbb{T}}_k(N)_{\mathbb{Q}_p})_{\mathfrak{p}} \big)$, is the decomposition of $\widehat{\mathbb{T}}_k(N)_{\mathbb{Q}_p}$ into $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-conjugacy classes, grouped together by being congruent mod p.

Note that the ideal $\mathfrak{a}$ need not contain a minimal prime ideal. In other words, a weak f as in the proposition need not be strong.

1.7 Interlude: Integers mod p^n

We want to define congruences mod p^n of two elements $\alpha \in \mathcal{O}_{K_1}$ and $\beta \in \mathcal{O}_{K_2}$, where K_1 and K_2 are finite extensions of $\mathbb{Q}_p$. Of course, in order to do so, one chooses a p-adic field K containing both K_1 and K_2. However, we want our definition to be independent of any such choice.

For this reason, it is useful, following [3], to define $\gamma_K(m) := (m-1)e_{K/\mathbb{Q}_p} + 1$, with $e_{K/\mathbb{Q}_p}$ the ramification index of $K/\mathbb{Q}_p$. This definition is made precisely so that the natural maps below yield injections of rings, i.e. ring extensions of $\mathbb{Z}/p^m\mathbb{Z}$,

$$\mathbb{Z}/p^m\mathbb{Z} \hookrightarrow \mathcal{O}_K/\mathfrak{p}_K^{\gamma_K(m)} \hookrightarrow \mathcal{O}_L/\mathfrak{p}_L^{\gamma_L(m)}$$

for any finite extension L/K (with $\mathfrak{p}_L$ the prime of L over $\mathfrak{p}_K$ in K). We can thus form the ring

$$\overline{\mathbb{Z}/p^m\mathbb{Z}} := \varinjlim_K \mathcal{O}_K/\mathfrak{p}_K^{\gamma_K(m)},$$

which we also consider as a topological ring with the discrete topology. When we speak of $\alpha \pmod{p^m}$ for $\alpha \in \overline{\mathbb{Z}}_p$, we mean its image in $\overline{\mathbb{Z}/p^m\mathbb{Z}}$. In particular, for $\alpha, \beta \in \overline{\mathbb{Z}}_p$, we define $\alpha \equiv \beta \pmod{p^m}$ as an equality in $\overline{\mathbb{Z}/p^m\mathbb{Z}}$, or equivalently, by $\alpha - \beta \in \mathfrak{p}_K^{\gamma_K(m)}$, where $K/\mathbb{Q}_p$ is any finite extension containing α and β.

Here is a different point of view on this, which was pointed out to me be Khuri-Makdisi. Let v the normalised valuation on $\overline{\mathbb{Z}}_p$, i.e. $v(p) = 1$. Define the ideal $\mathfrak{a}_n = \{x \in \overline{\mathbb{Z}}_p \mid v(x) > n - 1\}$. Then $\overline{\mathbb{Z}/p^n\mathbb{Z}} \cong \overline{\mathbb{Z}}_p/\mathfrak{a}_n$.

1.8 Modular forms mod p^n

Definition 1.29. *A* modular form mod p^n of weight k and level N *is a modular form of weight k and level N with coefficients in $\overline{\mathbb{Z}/p^n\mathbb{Z}}$.*

As before we define strong and weak eigenforms mod p^n as such having coefficients in $\overline{\mathbb{Z}/p^n\mathbb{Z}}$.

As seen above, if f is a modular form mod p^n of weight k and level N, then it can be seen as a $\mathbb{Z}_p$-linear map

$$f : \widehat{\mathbb{T}}_k(N) \to \overline{\mathbb{Z}/p^n\mathbb{Z}},$$

and as $\mathbb{Z}_p$-algebra homomorphism if it is a weak eigenform.

Contrary to the case $n = 1$, weak eigenforms mod p^n need not strong for $n > 1$! See, for example, [3], 4.2.

Later in the lecture we shall introduce one more kind of mod p modular form, namely, dc-weak modular forms (there we 'mix' weights).

2 Galois Representations Modulo Prime Powers

In this talk we study Galois representations mod p^n, without focussing on modular ones yet.

2.1 Some general representation theory

Proposition 2.1. *Let K be a p-adic field with $\mathcal{O}$ its ring of integers. Let G be a profinite group and V an n-dimensional K-vector space with a continous K-linear G-action, so that we have the continuous representation*

$$\rho : G \to \mathrm{Aut}_K(V) \cong \mathrm{GL}_n(K).$$

Then there is an $\mathcal{O}$-lattice L in V which is stabilised by ρ, so that ρ is equivalent to

$$\rho_L : G \to \mathrm{Aut}_{\mathcal{O}}(L) \cong \mathrm{GL}_n(\mathcal{O}).$$

Proposition 2.2. *Let R be a local ring and let $\rho_i : G \to \mathrm{GL}_n(R)$ be a continuous representation of a group G for $i = 1, 2$ such that ρ_1 is residually absolutely irreducible. Assume that all traces are equal: $\mathrm{Tr}(\rho_1(g)) = \mathrm{Tr}(\rho_2(g))$ for all $g \in G$.*

Then ρ_1 and ρ_2 are equivalent.

Corollary 2.3. *Let K be a p-adic field with $\mathcal{O}$ its ring of integers. Let G be a profinite group and*

$$\rho : G \to \mathrm{GL}_n(K)$$

be a continuous representation. Let ρ_{L_1} ρ_{L_2} be two lifts to $\mathrm{GL}_n(\mathcal{O})$.

If the residual representations $\overline{\rho}_{L_1} : G \to \mathrm{GL}_n(\mathcal{O}) \twoheadrightarrow \mathrm{GL}_n(\mathbb{F})$ is absolutely irreducible, then ρ_{L_1} is equivalent to ρ_{L_1}.

We will just write ρ for ρ_L and $\overline{\rho}$ for the reduction.

Warning: If $\overline{\rho}$ is not absolutely irreducible, it makes no sense to speak of the reduction of a representation taking values in $\overline{\mathbb{Q}}_p$! Note that the semi-simplification of $\overline{\rho}_L$ for any lattice L is independent of L. That is what people in modular forms normally do. But, we will see that in general we cannot define semi-simplifications in the mod p^n set-up.

[Could recall the definition of the conductor of a Galois representation in order to show that fixed spaces play an essential role, which are not free, in general, when we work mod p^n.]

2.2 Two dimensional representations mod p^n

Let G be a finite group and $\mathcal{O}$ be the ring of integers of a p-adic field K. Here we study representations:

$$\rho : G \to \mathrm{GL}_2(\mathcal{O}/\mathfrak{p}_K^{\gamma_K(n)}) \hookrightarrow \mathrm{GL}_2(\overline{\mathbb{Z}/p^n\mathbb{Z}}).$$

Fixed vectors

The definition of the conductor of a Galois representation (over a field) involves the dimension of the fixed spaces V^{G_i}, where G_i are the higher ramification groups.

Note that an analogous definition mod p^n leads into trouble. Look at the matrix $\left(\begin{smallmatrix} 1+p & 1 \\ 0 & 2 \end{smallmatrix}\right)$ (assuming $2 \neq p$). As a matrix in $\mathbb{Z}_p$ it fixes only the zero vector:

$$\left(\begin{smallmatrix} 1+p & 1 \\ 0 & 2 \end{smallmatrix}\right)\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) = \left(\begin{smallmatrix} x(1+p)+y \\ 2y \end{smallmatrix}\right)$$

(note that $y = 0$ follows immediately, and $x(1+p) = x$ implies $x = 0$). But, over $\mathbb{Z}/(p^2)$, we have a non-zero fixed vector, namely $\left(\begin{smallmatrix} p \\ 0 \end{smallmatrix}\right)$!!! But this fixed vector does not span a free submodule.

Let's change the previous example a bit and consider the matrix $\left(\begin{smallmatrix} 1+p & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Its fixed space is the span of $\left(\begin{smallmatrix} 1 \\ -p \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} p \\ 0 \end{smallmatrix}\right)$, which is also not free.

So, we would not be able to simply replace 'dimension' by 'rank' in the definition of the conductor.

Reducible representations

Let $K/\mathbb{Q}_p$ be $\mathbb{Q}_p(\pi)$ where π is such that $\pi^2 = p$. This is a totally ramified extension of degree 2, so that $\gamma_K(2) = e(n-1)+1 = 3$. We make some computations modulo p^2 (i.e. mod π^3). Consider the matrix $M := \left(\begin{smallmatrix} 1+p & 1 \\ p & 1-p \end{smallmatrix}\right)$. Its characteristic polynomial is $X^2 - 2X + 1 - p - p^2$, i.e. viewing it modulo π^3, it is just $X^2 - 2X + 1 - p$.

Let us suppose that α is an eigenvalue with an eigenvector that spans a free rank 1 submodule of $\mathcal{O}^2/(\pi^3)$; this just means that not both entries in the eigenvector are divisible by π. Then we can form a base change matrix by putting the eigenvector into the first column, and choosing any other second column which makes the determinant (i.e. the matrix) invertible. For this new basis, the matrix will then have upper triangular form.

Let $a \in \{0, \dots, p-1\}$ and consider $\alpha = 1 + \pi + a\pi^2$ and $\beta = 1 - \pi - a\pi^2$. These are all elements such that $\alpha + \beta = 2$ (the trace) and $\alpha\beta = 1 - p$ (the determinant), i.e. $X^2 - 2X + 1 - p = (X - \alpha)(X - \beta)$. Note that this means that the polynomial as $2p$ zeros (instead of 2). [Maybe, I should have put a as a subscript of α and β to recall the dependence.]

Let's compute the eigenvectors for α and β:

$$\begin{pmatrix} 1+p & 1 \\ p & 1-p \end{pmatrix} \begin{pmatrix} 1 \\ \pi+\pi^2(a-1) \end{pmatrix} = \begin{pmatrix} 1+\pi+a\pi^2 \\ \pi+a\pi^2 \end{pmatrix} = \alpha \begin{pmatrix} 1 \\ \pi+\pi^2(a-1) \end{pmatrix}$$
$$\begin{pmatrix} 1+p & 1 \\ p & 1-p \end{pmatrix} \begin{pmatrix} 1 \\ -\pi+\pi^2(-a-1) \end{pmatrix} = \begin{pmatrix} 1-\pi-a\pi^2 \\ -\pi-a\pi^2 \end{pmatrix} = \beta \begin{pmatrix} 1 \\ -\pi+\pi^2(-a-1) \end{pmatrix}$$

The computation shows that $\begin{pmatrix} 1 \\ \pi+\pi^2(a-1) \end{pmatrix}$ is an eigenvector for the eigenvalue α and $\begin{pmatrix} 1 \\ -\pi+\pi^2(-a-1) \end{pmatrix}$ is an eigenvector for the eigenvalue β.

The first conclusion is that the matrix $\begin{pmatrix} 1+p & 1 \\ p & 1-p \end{pmatrix}$ cannot be brought into diagonal form (α and β on the diagonal) by conjugation because the base change matrix would be $\begin{pmatrix} 1 & 1 \\ \pi+\pi^2(a-1) & -\pi+\pi^2(-a-1) \end{pmatrix}$, which is not invertible in the ring.

But, we can use the base change matrix $C := \begin{pmatrix} 1 & 0 \\ \pi+\pi^2(a-1) & 1 \end{pmatrix}$. Conjugation gives:

$$C^{-1}MC = \begin{pmatrix} \alpha & 1 \\ 0 & \beta \end{pmatrix}.$$

Now we interpret this in terms of representations. Let χ_α be the character that multiplies an entry by α. Then our representation is equivalent is equivalent to

$$1 \to \chi_\alpha \to V \to \chi_\beta \to 1,$$

and this extension is non-split. But, now recall that α depends on the choice of a. So, V is such an extension for all choices of a! We can even swap the roles of α and β and obtain extensions 'the other way around'. This behaviour is definitely crazy! If one wants to get something useful out of this, one must consider all these different choices 'the same', but, I am not sure how to do this properly.

Semi-simplification

The semi-simplification is traditionally defined as the direct sum of the Jordan-Hölder factors of a composition series. But, the Jordan Hölder factors are, of course, simple (by definition), as such they are $\mathbb{F}_p$-vector spaces and not at all free $\mathbb{Z}/(p^n)$-modules. A free rank 1 module over $\mathbb{Z}/(p^n)$ has a composition series consisting of n $\mathbb{F}_p$-vector spaces, so that the traditional semi-simplification would be an n-dimensional representation over $\mathbb{F}_p$ and there would be no $\mathbb{Z}/(p^n)$-structure left at all!

In favourable cases, we can do the following: Take the mod p reduction and assume it is reducible. Hence, there are two characters mod p appearing. If the two characters are distinct, then we can use them to split the $\mathbb{Z}/(p^n)$-module into a direct sum of two free ones of rank 1 via Hensel's Lemma (the characteristic polynomial will have precisely two roots mod p^n which are distinct mod p and one can just take the eigenvectors for these eigenvalues).

But, if the characters coincide mod p, we have seen that there are many possibilities of identifying characters. If there's an eigenvector that generates a free rank 1-submodule, we may define a semi-simplification as the direct sum of the two characters appearing. In the example there are p ways for doing so!

Note that in a representation mod p^n, which is not irreducible, there need not be such an eigenvector. Consider the representation generated by

$$\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \text{ and } \left(\begin{smallmatrix} 1+p & 0 \\ p & 1+p \end{smallmatrix}\right).$$

Seeing these matrices over $\mathbb{Q}_p$, they form an irreducible representation. Modulo p, the representation is clearly reducible. Mod p^2, there is no eigenvector that generates a free rank 1 submodule.

2.3 1-dimensional Galois representations

We have seen that 2-dimensional representation theory mod p^n behaves like crazy. Now, we draw a crazy conclusion on the number theory side. To make things easier we study 1-dimensional representations first.

Theorem 2.4. *Let p be an odd prime. The set*

$$\{\chi : G_{\mathbb{Q}} \to \overline{\mathbb{F}}_p^{\times} \mid \text{ unramified outside } p\}$$

is finite. It contains $p-1$ elements.

Proof. Let $\chi : G_{\mathbb{Q}} \to \overline{\mathbb{F}}_p^{\times}$ be any character. Its image is finite (due to continuity). By the Kronecker-Weber theorem, χ factors through $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ for some primitive N-th root of unity for some integer N. However, assuming in addition that χ is unramified outside p means that we may take N to be a power of p. But, since the only p^n-th root of unity in $\overline{\mathbb{F}}_p$ is 1, the character χ takes values in $\mathbb{F}_p^{\times}$ and factors through $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong \mathbb{F}_p^{\times}$. Hence, there are precisely $p-1$ characters in the set of the assertion. □

We will now see that this statement completely breaks down when working mod p^n.

One of the first statement one learns about characters with finite image is that the image is cyclic. The reason being that every finite subgroup of the multiplicative group of a field is cyclic, namely contained in the roots of unity. The only things one uses in order to prove this is that the polynomial $X^N - 1$ has at most N roots, namely the N-th roots of unity, which we know form a cyclic group. But, not working in an integral domain, a polynomial of degree N may have more than N-roots, so we'd be leaving the roots of unity.

If we have a character mod p^n with non-cyclic image, then it consequently cannot be the reduction of a finite image character to $\overline{\mathbb{Z}}_p^\times$, as otherwise the image would be cyclic (any quotient of a cyclic group is cyclic). But, I have not really thought about whether the character could be the reduction of a character to $\overline{\mathbb{Z}}_p^\times$ of infinite order.

Theorem 2.5. *Let p be an odd prime. The set*

$$\{\chi : G_{\mathbb{Q}} \to \overline{\mathbb{Z}/p^2\mathbb{Z}}^\times \mid \text{ unramified outside } p\}$$

is infinite.

We develop this step by step.

Lemma 2.6. *Let p be an odd prime and $n \in \mathbb{N}$. By ζ_{p^n} we denote a primitive p^n-root of unity in $\overline{\mathbb{Q}}_p$.*

(a) $\mathbb{Z}_p[\zeta_{p^n}]$ is the ring of integers of $\mathbb{Q}_p(\zeta_{p^n})$, which is a totally ramified extension of degree $e_n = \varphi(p^n) = (p-1)p^{n-1}$. A uniformiser is $\pi_n := 1 - \zeta_{p^n}$. Any element x in $\mathbb{Z}_p[\zeta_{p^n}]$ can be uniquely written in its π-adic expansion: $x = a_0 + a_1\pi_n + a_2\pi_n^2 + \dots$ with $a_i \in \{0, 1, \dots, p-1\}$. Taking x mod π^{e_n+1} just means breaking off this expansion at $\pi_n^{e_n}$.

(b) Let $x = a_0 + a_1\pi_n + a_2\pi_n^2 + \dots$. Then $x^{p-1} = 1 + b_1\pi_n + \dots$.

(c) Let $1 \neq x = 1 + a_1\pi_n + a_2\pi_n^2 + \dots \in \mathbb{Z}_p[\zeta_{p^n}]$. Let $i \geq 1$ be the smallest index such that $a_i \neq 0$. Then the order of x in $\mathbb{Z}_p[\zeta_{p^n}]/(\pi_n^{e_n+1})^\times$ is equal to p^{n-r} with $r = \lceil \log_p \frac{i}{p-1} \rceil$.

(d) $\left(\mathbb{Z}_p[\zeta_{p^n}]/(\pi_n^{e_n+1})\right)^\times$ has a subgroup of the form $\mathbb{F}_p^\times \times \underbrace{\mathbb{F}_p \times \dots \times \mathbb{F}_p}_{(p-1)^2p^{n-2} \text{ copies}}$.

(e) There are elements of order $(p-1)p^n$.

Proof. (a) is well-known and will not be proved here.

(b) This is because $a_0^{p-1} \equiv 1 \pmod{p}$.

(c) We have $x = 1 + a_i\pi_n^i + \dots$. Hence, $x^p = (1 + a_i\pi_n^i + \dots)^{p^s} = 1 + a_i\pi_n^{ip^s} + \dots$ and this is non-zero if and only if $ip^s \leq e_n = (p-1)p^{n-1}$, which is the case if and only if $\frac{i}{p-1} \leq p^{n-s-1}$ and that is true if and only if $\lceil \log_p \frac{i}{p-1} \rceil \leq n - s - 1$. The result follows.

(d) Using (c), we just count the number of elements having order dividing p, by counting the coefficients that may be chosen

(e) follows from (c). □

It is not difficult to derive the full group structure of $\left(\mathbb{Z}_p[\zeta_{p^n}]/(\pi_n^{e_n+1})\right)^\times$ from the above, but, I have not done so.

Proof of Theorem 2.5. Recall $\mathrm{Gal}(\mathbb{Q}(\zeta_p^2)/\mathbb{Q}) \cong \mathbb{F}_p^\times \oplus \mathbb{F}_p$. Working mod p^2 and with fixed n, Lemma 2.6 (d) allows us to send the generator of $\mathbb{F}_p$ to $p^{p^{n-2}} - 1$ different non-zero elements. As n grows, this number tends to infinity. □

Here is another corollary.

Corollary 2.7. *There are characters $\chi : G_{\mathbb{Q}_p} \to \overline{\mathbb{Z}/p^2\mathbb{Z}}$, unramified outside p, of arbitrarily high conductor. This means the following. Let $k \in \mathbb{N}$. Then there is a character χ as before such that $G^k_{\mathbb{Q}_p}$ is not in the kernel of χ.*

Proof. The m-th ramification group of $G(\mathbb{Q}_p(\zeta_{p^m}/\mathbb{Q}_p))$ is $\mathbb{Z}/(p^{m-1})$ (if I remember correctly). By Lemma 2.6 (e), this can be send injectively into $\overline{\mathbb{Z}/p^2\mathbb{Z}}$. □

I put this corollary because in the mod p setting G^{p+2} is always in the kernel (if I remember correctly). This is an indication why the weights do not become arbitrarily high mod p, so that we might now expect that they might become arbitrarily high mod p^n.

2.4 My main motivation

Let $f \in S_k(Nq)$ with $q \nmid Np$ a prime be a newform and $\rho_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ be the attached p-adic Galois representation. (We assume that the nebentype, if any, is unramified at q.)

What is the shape of ρ_ℓ restricted to D_q? Local Langlands tells us that there is a $\overline{\mathbb{Q}}_p$-basis such that

$$\rho_p|_{I_q} \sim \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right).$$

Now let us assume that $\overline{\rho_p}$ is absolutely irreducible, so that we have a unique representation

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

We ask the same question. From local Langlands we derive:

$$\rho_p|_{I_q} \sim \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$$

for some $0 \neq x \in \overline{\mathbb{Z}}_p$. Note that the matrix $\left(\begin{smallmatrix} 1 & p \\ 0 & 1 \end{smallmatrix}\right)$ cannot be conjugated to $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ in $\mathbb{Z}_p$ (because their reductions mod p are obviously not conjugated).

This answer is insufficient: We don't know anything about x!

What is the p-valuation of x?

Answer, the $v_p(x) > n-1$ if and only if $x = 0$ in $\overline{\mathbb{Z}/p^n\mathbb{Z}}$ if and only if $\rho_p \pmod{p^n}$ is unramified at q.

So, I want to detect at which n, the representation $\rho_p \pmod{p^n}$ stops being unramified at q.

One could conjecture that this should be detected by the existence of a weak eigenform g modulo p^n of level N in the same weight which has the same q-expansion as f modulo p^n, away from a finite set of primes.

3 Galois Representations Attached to dc-Weak Eigenforms

This part is essentially copy-and-paste from the article Chen-Kiming-Wiese.

3.1 dc-weak eigenforms

Let $\mathcal{S} = \bigoplus_{k\in\mathbb{N}} S_k(M)$ be the $\mathbb{C}$-vector space of all cusp forms of any positive weight at a fixed level M. Let each Hecke operator T_n act on $\mathcal{S}$ via the diagonal action. We will be considering finite-dimensional subspaces $S \subseteq \mathcal{S}$ of the following type:

$$S = S^b(M) := \bigoplus_{k=1}^{b} S_k(M)$$

for any $b \in \mathbb{N}$, $M \geq 1$. Such a subspace S is mapped into itself by T_n for all $n \geq 1$.

For $f \in \mathcal{S}$, let $f(q) \in \mathbb{C}[[q]]$ denote its q-expansion. We denote the *q-expansion map* on $S \subset \mathcal{S}$ by

$$\Phi_S : S \to \mathbb{C}[[q]], f \mapsto f(q) = \sum_{n\geq 1} a_n(f)q^n.$$

Proposition 3.1. *Fix $M \in \mathbb{N}$ and $b \in \mathbb{N}$. Let $S := S^b(M)$. Then Φ_S is injective.*

Proof. Let $f_k \in S_k(M)$, for $k = 1, \ldots, b$ be such that $\sum_{k=1}^b f_k(q) = 0$. The function $\sum_{k=1}^b f_k$ is holomorphic and 1-periodic and hence uniquely determined by its Fourier series. Hence, $\sum_{k=1}^b f_k = 0$ and it then follows from [2], Lemma 2.1.1, that we have $f_k = 0$ for each k. □

We will identify an integral structure in S by making use of the results of the first talk.

Definition 3.2. *Let $\mathcal{H}(S)$ be the $\mathbb{C}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(S)$ generated by the T_n for $n \geq 1$. Let $\mathbb{T}(S)$ be the subring of $\mathrm{End}_{\mathbb{C}}(S)$ generated by the T_n for $n \geq 1$.*

As was proved in the first lecture, the spaces $S_k(M)$ have an integral structure: $S_k(M)(\mathbb{Z})$. It follows that the space $S = S^b(\Gamma_1(M)) := \bigoplus_{k=1}^b S_k(M)$ also contains an integral structure, namely, $\bigoplus_{k=1}^b S_k(M)(\mathbb{Z})$. This is clear because tensoring it over $\mathbb{Z}$ with $\mathbb{C}$ clearly gives back S and the $\mathbb{Z}$-rank on the left is the $\mathbb{C}$-dimension on the right.

Thus, $\mathbb{T}(S)$ sits inside an integer matrix ring, we get, as before:

Proposition 3.3. *(a)* $\mathbb{C} \otimes_{\mathbb{Z}} \mathbb{T}(S) \cong \mathcal{H}(S)$.

(b) *$\mathbb{T}(S)$ is free of finite rank as $\mathbb{Z}$-module and the rank is equal to the $\mathbb{C}$-dimension of $\mathcal{H}(S)$ (which is equal to the $\mathbb{C}$-dimension of S due to the q-pairing, see below).*

As the complex q-pairing $S \times \mathcal{H}(S) \to \mathbb{C}$, given, as before, by $(f, T) \mapsto a_1(Tf)$, is non-degenerate (same proof!), we obtain the isomorphism

$$S \cong \mathrm{Hom}_{\mathbb{C}}(\mathcal{H}(S), \mathbb{C}) \longrightarrow \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}(S), \mathbb{C}).$$

For any commutative ring R we make the definition, as before,

$$S(R) := \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}(S), R) \quad (\mathbb{Z}\text{-linear homomorphisms}).$$

We call $S(R)$ the *cusp forms in S with coefficients in R*. This definition comes together, as before, with a natural action of $\mathbb{T}(S)$ on $S(R)$ given by $(T.f)(T') = f(TT')$. Note that, as before, $S(\mathbb{C}) \cong S$. Moreover, for any ring homomorphism $R_1 \to R_2$ we obtain

$$R_2 \otimes_{R_1} S(R_1) \cong S(R_2).$$

We remark that for any ring R and any $1 \leq k \leq b$, the map

$$S_k(M)(R) \to S^b(M)(R), \quad f \mapsto f \circ \pi,$$

is an R-module monomorphism, where π is the surjective ring homomorphism

$$\mathbb{T}(S^b(M)) \to \mathbb{T}(S_k(M)),$$

defined by restricting Hecke operators.

For a positive integer D, let $\mathbb{T}^{(D)}(S)$ be the subring of $\mathbb{T}(S)$ generated by those Hecke operators T_n for which n and D are coprime.

As before, we have for $f \in S(R)$ that the following two statements are equivalent:

(i) f is an eigenvector with eigenvalue $f(T)$ for every $T \in \mathbb{T}^{(D)}(S)$ and $f(1) = 1$.

(ii) The restriction of f to $\mathbb{T}^{(D)}$ is a ring homomorphism.

We again use the terminology *Hecke eigenform* for such objects. Moreover, via our chosen field isomorphism $\mathbb{C} \cong \overline{\mathbb{Q}}_p$ we identify the two spaces $S(\mathbb{C})$ and $S(\overline{\mathbb{Q}}_p)$.

Let us now specialise to $R = \overline{\mathbb{Z}/p^n\mathbb{Z}}$. We first record the following simple lifting property.

Lemma 3.4. *Fix $M, b \in \mathbb{N}$ and let $S := \bigoplus_{k=1}^{b} S_k(M)$.*

Let $f \in S(\overline{\mathbb{Z}/p^m\mathbb{Z}})$. Then there is a number field (and hence there is also a p-adic field) K and $\tilde{f} \in S(\mathcal{O}_K)$ such that $\tilde{f} \equiv f \pmod{p^m}$, in the sense that $\tilde{f}(T_n) \equiv f(T_n) \pmod{p^m}$ for all $n \in \mathbb{N}$.

Proof. As $\mathbb{T}(S)$ is a free Z-module of finite rank, it is a projective $\mathbb{Z}$-module. Moreover, the image of the homomorphism (of abelian groups) $f : \mathbb{T}(S) \to \overline{\mathbb{Z}/p^m\mathbb{Z}}$ lies in $\mathcal{O}_K/\mathfrak{p}_K^{\gamma_K(m)}$ for some number field (or, p-adic field) K. The projectivity implies by definition that f lifts to a homomorphism $\tilde{f} : \mathbb{T}(S) \to \mathcal{O}_K$. □

We stress again that eigenforms mod p^m cannot, in general, be lifted to eigenforms if $m > 1$.

Divided congruence forms 'mix' weights. However, when we are over a characteristic 0 field, there's no mixing, in the following sense.

Lemma 3.5. *Fix $M, b \in \mathbb{N}$ and let $S := \bigoplus_{k=1}^{b} S_k(M)$. Put $S_k := S_k(M)$ for each k.*

If K is any $\mathbb{Q}$-algebra, then one has $S(K) = \bigoplus_{k=1}^{b} S_k(K)$. Moreover, if K is a field extension of $\mathbb{Q}$ and $f \in S(K)$ is a normalized eigenform, then there is k, a normalized eigenform $\tilde{f} \in S_k(L)$ for some finite extension L/K and a positive integer D such that $f(T_n) = \tilde{f}(T_n)$ for all n coprime with D.

Proof. For each $1 \leq k \leq b$, we have a natural homomorphism $\mathbb{T}_{\mathbb{Q}}(S) \to \mathbb{T}_{\mathbb{Q}}(S_k)$ given by restriction, and hence taking the product of these, we obtain a monomorphism $\mathbb{T}_{\mathbb{Q}}(S) \to \prod_{k=1}^{b} \mathbb{T}_{\mathbb{Q}}(S_k)$ of $\mathbb{Q}$-algebras. By the existence of an integral structure, we have that

$$\dim_{\mathbb{Q}} \mathbb{T}_{\mathbb{Q}}(S) = \dim_{\mathbb{C}} S = \sum_{k=1}^{b} \dim_{\mathbb{C}} S_k = \sum_{k=1}^{b} \dim_{\mathbb{Q}} \mathbb{T}_{\mathbb{Q}}(S_k),$$

showing that $\mathbb{T}_{\mathbb{Q}}(S) \cong \prod_{k=1}^{b} \mathbb{T}_{\mathbb{Q}}(S_k)$. Now, we see that

$$\begin{aligned} S(K) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}(S), K) &\cong \mathrm{Hom}_{\mathbb{Q}}(\mathbb{T}(S) \otimes_{\mathbb{Z}} \mathbb{Q}, K) \cong \mathrm{Hom}_{\mathbb{Q}}(\mathbb{T}_{\mathbb{Q}}(S), K) \\ &\cong \mathrm{Hom}_{\mathbb{Q}}(\prod_{k=1}^{b} \mathbb{T}_{\mathbb{Q}}(S_k), K) \cong \bigoplus_{k=1}^{b} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(S_k), K) = \bigoplus_{k=1}^{b} S_k(K). \end{aligned}$$

Now assume that K is a field extension of $\mathbb{Q}$ and that f is a normalized eigenform (for all operators T_n with n coprime to D), giving a ring homomorphism $\mathbb{T}_{\mathbb{Q}}^{(D)} \to K$. It can be extended to a ring homomorphism $\tilde{f} : \mathbb{T}_{\mathbb{Q}}(S) \to L$ for some finite extension L/K, since in the integral extension of rings $\mathbb{T}_{\mathbb{Q}}^{(D)} \hookrightarrow \mathbb{T}_{\mathbb{Q}}(S)$ we need only choose a prime ideal of $\mathbb{T}_{\mathbb{Q}}(S)$ lying over the prime ideal $\ker(f) \lhd \mathbb{T}_{\mathbb{Q}}^{(D)}$ by 'going up'.

To conclude, it suffices to note that every ring homomorphism $\mathbb{T}_{\mathbb{Q}}(S) \to K$ factors through a unique $\mathbb{T}_{\mathbb{Q}}(S_k)$. In order to see this, one can consider a complete set of orthogonal idempotents $e_1, \ldots, e_n$ of $\mathbb{T}_{\mathbb{Q}}(S)$, i.e. $e_i^2 = e_i$, $e_i e_j = 0$ for $i \neq j$ and $1 = e_1 + \cdots + e_n$. As K is a field and idempotents are mapped to idempotents, each e_i is either mapped to 0 or 1, and as 0 maps to 0 and 1 maps to 1, there is precisely one idempotent that is mapped to 1, the others to 0. This establishes the final assertion. □

[COMPARE $S(\mathbb{Z})$ and $\bigoplus_{k=1}^{b} S_k(M)(\mathbb{Z})$]

Note that in general it is not true that a normalised f (as in the lemma), which is an eigenform for all T_n with n coprime to some integer D, lies $S_k(K)$ for any k: Let $D \in \mathbb{N}$, let $f \in S_k(K)$ be an eigenform for all T_n and let $0 \neq g \in S_r(K)$ be a modular form such that $g(T_n) = 0$ for all n coprime with D; then $f + g$ is an eigenform (outside D) but does not lie in a single weight.

We explicitly point out the following easy consequence of Lemma 3.5.

Lemma 3.6. *Let $\mathcal{O}$ be the ring of integers of K, where K is a number field or a finite extension of $\mathbb{Q}_p$. Let $S = \bigoplus_{k=1}^{b} S_k(M)$.*

Then:

$$S(\mathcal{O}) = \{f \in S(K) \mid f(T_n) \in \mathcal{O}\ \forall n\} = \{f \in \bigoplus_{k=1}^{b} S_k(M)(K) \mid f(T_n) \in \mathcal{O}\ \forall n\}.$$

This establishes that $S(\mathcal{O})$ is the space also used by Hida on p. 550 of [1].

Now, we give an indication for the name 'divided congruence'. It shows that, when working over a ring, there really is some 'mixing', unlike the situation for $\mathbb{Q}$-algebras of Lemma 3.5.

Any $f \in S(\mathcal{O})$ is of the form $f = \sum_k f_k$ with $f_k \in S_k(M)(K)$, and although none of the f_k need be in $S_k(\mathcal{O})$, the sum has all its coefficients in $\mathcal{O}$. This is the origin of the name 'divided congruence' for such an f: Suppose for example that we have forms $g_k \in S(\mathcal{O})$ for various weights k and that $\sum_k g_k \equiv 0 \pmod{\pi^m}$ for some m, where π is a uniformizer of $\mathcal{O}$. Putting $f_k := g_k/\pi^m$ for each k we then have $f_k \in S_k(M)(K)$ for all k as well as $f := \sum_k f_k \in S(\mathcal{O})$. Conversely, any element of $S(\mathcal{O})$ arises in this way by 'dividing a congruence'.

3.2 Some general representation theory

Theorem 3.7 (Carayol, Serre)**.** *Let R be a complete local ring with finite residue field. Let R' be a semi-local ring containing R. Let $\rho' : G \to \mathrm{GL}_n(R')$ be a continuous representation of a group G which is residually absolutely irreducible. Assume that all traces $\mathrm{Tr}(\rho(g))$ for $g \in G$ lie in R.*

Then ρ' is obtained by scalar extension to a representation of the form $\rho : G \to \mathrm{GL}_n(R)$.

3.3 Galois representations

From here on we only work with Γ_1.

In this section we construct a Galois representation attached to a dc-weak eigenform mod p^m. For expressing its determinant, we find it convenient to work with Hida's stroke operator $_{|\ell}$, which we denote $[\ell]$. We recall its definition from [1], p. 549. Let us consider again a space of the form $S = \bigoplus_{k=1}^{b} S_k(M)$ for some b. We now consider specifically a level M written in the form

$$M = Np^r$$

where $p \nmid N$.

Let $Z = \mathbb{Z}_p^\times \times (\mathbb{Z}/N\mathbb{Z})^\times$, into which we embed $\mathbb{Z}$ diagonally with dense image. We have a natural projection $\pi : Z \to Z\,\mathrm{Z}\,/p^r\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \cong \mathbb{Z}/Np^r\mathbb{Z}$. Let first $f \in S$ be of weight k. Hida defines for $z = (z_p, z_0) \in Z$ the stroke operator:

$$[z]f = z_p^k \langle \pi(z) \rangle f.$$

The diamond operator $\langle d \rangle$ for $d \in \mathbb{Z}/Np^r\mathbb{Z}$ is defined as $f_{|_k\sigma_d}$ with $\sigma_d \in \mathrm{SL}_2(\mathbb{Z})$ such that $\sigma_d \equiv \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) d^{-1} * 0 d \mod Np^r$. Since the diamond operator is multiplicative (it gives a group action of $\mathbb{Z}/Np^r\mathbb{Z}^\times$), so is the stroke operator.

We now show that for $z \in \mathbb{Z}$ the definition of $[z]$ can be made so as not to involve the weight. Let $\ell \nmid Np$ be a prime. Due to the well known equalities $T_{\ell,\ell} = \ell^{k-2}\langle \ell \rangle$ and $\ell T_{\ell,\ell} = T_\ell^2 - T_{\ell^2}$, one obtains

$$[\ell] = \ell^k \langle \ell \rangle = \ell^2 T_{\ell,\ell} = \ell(T_\ell^2 - T_{\ell^2}).$$

This first of all implies that $[\ell] \in \mathbb{T}(S)$, since the right hand side clearly makes sense on S and is an element of $\mathbb{T}(S)$. Due to multiplicativity, all $[n]$ lie in $\mathbb{T}(S)$ for $n \in$ Z. Consequently, $[n]$ acts on $S(A)$ for any ring A by its action via $\mathbb{T}(S)$. Moreover, if $f \in S(A)$ is an eigenform for all T_n ($n \in \mathbb{N}$), then it is also an eigenfunction for all $[n]$.

One can extend the stroke operator to a group action of Z on $S(\mathcal{O})$ for all complete $\mathbb{Z}_p$-algebras $\mathcal{O}$ by continuity (which one must check). Thus, if $f \in S(\mathcal{O})$ is an eigenfunction for all Hecke operators, then it is in particular an eigenfunction for all $[z]$ for $z \in Z$, whence sending $[z]$ to its eigenvalue on f gives rise to a character $\theta : Z \to \mathcal{O}^\times$, which we may also factor as $\theta = \eta\psi$ with $\psi : \mathbb{Z}/N\mathbb{Z}^\times \to \mathcal{O}^\times$ and $\eta : \mathbb{Z}_p^\times \to \mathcal{O}^\times$.

Since it is the starting point and the fundamental input to the sequel, we recall the existence theorem on p-adic Galois representations attached to normalized Hecke eigenforms for $k = 2$ by Shimura, for $k > 2$ by Deligne and for $k = 1$ by Deligne and Serre. By Frob_ℓ we always mean an arithmetic Frobenius element at ℓ.

Theorem 3.8. *Suppose that $S = S_k(\Gamma_1(Np^r))$ with $k \geq 1$. Suppose $f \in S(\overline{\mathbb{Q}}_p)$ is a normalized eigenform, so that $\langle\ell\rangle f = \chi(\ell)f$ for a character $\chi : (\mathbb{Z}/Np^r\mathbb{Z})^\times \to \overline{\mathbb{Q}}_p^\times$ for primes $\ell \nmid Np$.*

Then there is a continuous odd Galois representation

$$\rho = \rho_{f,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$$

that is unramified outside Np and satisfies

$$\mathrm{Tr}(\rho(\mathrm{Frob}_\ell)) = f(T_\ell) \text{ and } \det(\rho(\mathrm{Frob}_\ell)) = \ell^{k-1}\chi(\ell)$$

for all primes $\ell \nmid Np$.

Corollary 3.9. *Suppose that $S = \bigoplus_{k=1}^b S_k(\Gamma_1(Np^r))$. Suppose $f \in S(\overline{\mathbb{Q}}_p)$ is a normalized eigenform, so that $[\ell]f = \eta(\ell)\psi(\ell)f$ for some characters $\psi : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Q}}_p^\times$ and $\eta : \mathbb{Z}_p^\times \to \overline{\mathbb{Q}}_p^\times$.*

Then there is a continuous Galois representation

$$\rho = \rho_{f,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$$

that is unramified outside Np and satisfies

$$\mathrm{Tr}(\rho(\mathrm{Frob}_\ell)) = f(T_\ell) \text{ and } \det(\rho(\mathrm{Frob}_\ell)) = f(\ell^{-1}[\ell]) = \ell^{-1}\eta(\ell)\psi(\ell)$$

for all primes $\ell \nmid Np$.

Proof. From Lemma 3.5 we know that f has a unique weight k, i.e. lies in some $S_k(\overline{\mathbb{Q}}_p)$. Thus, f also gives rise to a character $\chi : \mathbb{Z}/Np^r\mathbb{Z}^\times \to \overline{\mathbb{Q}}_p^\times$ by sending the diamond operator $\langle\ell\rangle$ to its eigenvalue on f. The assertion now follows from the equation $\ell^k\langle\ell\rangle = [\ell]$ and Theorem 3.8. □

Corollary 3.10. *Suppose that $S = \bigoplus_{k=1}^b S_k(\Gamma_1(Np^r))$. Suppose $\bar{f} \in S(\overline{\mathbb{F}}_p)$ is a normalized eigenform, so that $[\ell]\bar{f} = \eta(\ell)\psi(\ell)\bar{f}$ for some characters $\psi : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{F}}_p^\times$ and $\eta : \mathbb{Z}_p^\times \to \overline{\mathbb{F}}_p^\times$.*

Then there is a semisimple continuous Galois representation

$$\rho = \rho_{\bar{f},p,1} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$$

that is unramified outside Np and satisfies

$$\mathrm{Tr}(\rho(\mathrm{Frob}_\ell)) = \bar{f}(T_\ell) \text{ and } \det(\rho(\mathrm{Frob}_\ell)) = \ell^{-1}\eta(\ell)\psi(\ell)$$

for all primes $\ell \nmid Np$.

Proof. By the Deligne-Serre lifting lemma, there is an eigenform $f \in S(\overline{\mathbb{Z}}_p)$ whose reduction is $\bar{f}$, whence by Corollary 3.9 there is an attached Galois representation $\rho_{f,p}$. Due to the compactness of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and the continuity, there is a finite extension $K/\mathbb{Q}_p$ such that the representation is isomorphic to one of the form $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}_K)$. We define $\rho_{\bar{f},p,1}$ as the semisimplification of the reduction of this representation modulo the maximal ideal of $\mathcal{O}_K$. It inherits the assertions on the characeristic polynomial at Frob_ℓ from $\rho_{f,p}$. □

Next we construct a Galois representation into the completed Hecke algebra.

Theorem 3.11. *Suppose that* $S = \bigoplus_{k=1}^{b} S_k(\Gamma_1(Np^r))$.

Let D be a positive integer and let $\mathfrak{m}$ be a maximal ideal of $\hat{\mathbb{T}}^{(D)}(S) := \mathbb{Z}_p \otimes_{\mathbb{Z}} \mathbb{T}^{(D)}(S)$ and denote by $\hat{\mathbb{T}}^{(D)}(S)_{\mathfrak{m}}$ the completion of $\hat{\mathbb{T}}^{(D)}(S)$ at $\mathfrak{m}$. Assume that the residual Galois representation attached to

$$\mathbb{T}^{(D)}(S) \hookrightarrow \hat{\mathbb{T}}^{(D)}(S) \to \hat{\mathbb{T}}^{(D)}(S)_{\mathfrak{m}} \to \hat{\mathbb{T}}^{(D)}(S)/\mathfrak{m} \hookrightarrow \overline{\mathbb{F}}_p$$

is absolutely irreducible (note that this ring homomorphism can be extended to a ring homomorphism $\mathbb{T}(S) \to \overline{\mathbb{F}}_p$).

Then there is a continuous representation

$$\rho = \rho_{\mathfrak{m}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\hat{\mathbb{T}}^{(D)}(S)_{\mathfrak{m}}),$$

that is unramified outside Np and satisfies

$$\mathrm{Tr}(\rho(\mathrm{Frob}_\ell)) = T_\ell \text{ and } \det(\rho(\mathrm{Frob}_\ell)) = \ell^{-1}[\ell]$$

for all primes $\ell \nmid DNp$.

Proof. Assume first that all prime divisors of Np also divide D. As the Hecke operators T_n with n coprime to D commute with each other and are diagonalizable (as elements of $\mathrm{End}_{\mathbb{C}}(S)$), there is a $\mathbb{C}$-basis Ω for S consisting of eigenforms for $\mathbb{T}^{(D)}(S)$. As $\mathbb{T}^{(D)}(S)$ is finite over $\mathbb{Z}$, for each $f \in \Omega$, its image onto $\mathbb{T}^{(D)}(\mathbb{C}f)$ is an order in a number field. Here, obviously $\mathbb{T}^{(D)}(\mathbb{C}f)$ denotes the $\mathbb{Z}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(\mathbb{C}f)$ generated by the T_n with $(n, D) = 1$.

Consider the natural map

$$\mathbb{T}^{(D)}(S) \to \prod_{f \in \Omega} \mathbb{T}^{(D)}(\mathbb{C}f),$$

which is a monomorphism because Ω is a $\mathbb{C}$-basis for S. Letting $R = \mathbb{T}^{(D)}(S) \otimes \mathbb{Q}$, we see that $\prod_{f\in\Omega} \mathbb{T}^{(D)}(\mathbb{C}f) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a semi-simple R-module, as each $\mathbb{T}^{(D)}(\mathbb{C}f) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a simple R-module. Thus, the R-submodule $R \subset \prod_{f\in\Omega} \mathbb{T}^{(D)}(\mathbb{C}f) \otimes \mathbb{Q}$ is also a semi-simple R-module, and $R = \mathbb{T}^{(D)}(S) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a semi-simple ring. It follows that $\mathbb{T}^{(D)}(S) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \prod_i F_i$, where the F_i are a finite collection of number fields. This means that $\mathbb{T}^{(D)}(S) \otimes_{\mathbb{Z}} \mathbb{Q}_p \cong \prod_i K_i$ with the K_i a finite collection of finite extensions of $\mathbb{Q}_p$.

Thus, there is a monomorphism $\hat{\mathbb{T}}^{(D)}(S) \hookrightarrow \prod_i \mathcal{O}_i$, where $\mathcal{O}_i$ is the ring of integers of K_i. Hence, there is a monomorphism $\hat{\mathbb{T}}^{(D)}(S)_{\mathfrak{m}} \hookrightarrow \prod_i \mathcal{O}_i$, which is obtained from the previous one by discarding

factors where $\mathfrak{m}$ is not sent into the maximal ideal of $\mathcal{O}_i$. Each projection $\hat{\mathbb{T}}^{(D)}(S)_{\mathfrak{m}} \to \mathcal{O}_i$ is a map of local rings.

Each ring homomorphism $g_i : \mathbb{T}^{(D)}(S) \to K_i$ lifts to a ring homomorphism $f_i : \mathbb{T}(S) \to E_i$, where E_i is a finite extension of K_i. By Corollary 3.9, for each i, there is a continuous Galois representation $\rho_i : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}_i')$, where $\mathcal{O}_i'$ is the ring of integers of E_i.

Let $\rho = \prod_i \rho_i : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \prod_i \mathrm{GL}_2(\mathcal{O}_i') = \mathrm{GL}_2(\prod_i \mathcal{O}_i')$ be the product representation. Under the inclusion $\mathbb{T}^{(D)}(S) \hookrightarrow \prod_i \mathcal{O}_i'$, we see for $\ell \nmid DNp$, that $\mathrm{Tr}\,\rho(\mathrm{Frob}_\ell) = T_\ell$ and $\det \rho(\mathrm{Frob}_\ell) = \ell^{-1}[\ell]$. The residual Galois representations $\overline{\rho}_i : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(k_i')$, where k_i' is the residue field of $\mathcal{O}_i'$, are all isomorphic to the Galois representation attached to $\mathbb{T}^{(D)}(S) \to \hat{\mathbb{T}}^{(D)}(S)/\mathfrak{m}$, and hence are absolutely irreducible.

Applying Theorem 3.7, with $A = \hat{\mathbb{T}}^{(D)}(S)_{\mathfrak{m}}$ and $A' = \prod_i \mathcal{O}_i'$ (which is a semi-local extension of A), we deduce that the representation ρ descends to a continuous Galois representation

$$\rho_{\mathfrak{m}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\hat{\mathbb{T}}^{(D)}(S)_{\mathfrak{m}}),$$

as claimed.

For the general case, when D is not divisible by all prime divisors of Np, one first applies the above with $D' := DNp$ and the maximal ideal $\mathfrak{m}'$ of $\hat{\mathbb{T}}^{(D')}$ given as $\mathfrak{m} \cap \hat{\mathbb{T}}^{(D')}$ to obtain $\rho_{\mathfrak{m}'} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\hat{\mathbb{T}}^{(D')}(S)_{\mathfrak{m}'})$, which can finally be composed with the natural map $\hat{\mathbb{T}}^{(D')}(S)_{\mathfrak{m}'} \to \hat{\mathbb{T}}^{(D)}(S)_{\mathfrak{m}}$. □

Corollary 3.12. *Suppose that $S = \bigoplus_{k=1}^{b} S_k(\Gamma_1(Np^r))$. Let A be a complete local ring with maximal ideal $\mathfrak{p}$ of residue characteristic p. Suppose $f \in S(A)$ is a normalized eigenform, so that $[\ell]f = \eta(\ell)\psi(\ell)\bar{f}$ for some characters $\psi : (\mathbb{Z}/N\mathbb{Z})^\times \to A^\times$ and $\eta : \mathbb{Z}_p^\times \to A^\times$. Assume the Galois representation attached to the reduction $\bar{f} : \mathbb{T}(S) \to A \to A/\mathfrak{p}$ mod $\mathfrak{p}$ of f, which defines an element of $S(\overline{\mathbb{F}}_p)$, is absolutely irreducible (cf. Corollary 3.10).*

Then there is a continuous Galois representation

$$\rho = \rho_{f,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(A)$$

that is unramified outside Np and satisfies

$$\mathrm{Tr}(\rho(\mathrm{Frob}_\ell)) = f(T_\ell) \text{ and } \det(\rho(\mathrm{Frob}_\ell)) = \ell^{-1}\eta(\ell)\psi(\ell)$$

for all primes $\ell \nmid DNp$ (where D any the integer such that the restriction of f to $\mathbb{T}^{(D)}(S)$ is a ring homomorphism).

Proof. Since $S(A)$ is a normalized eigenform, $f : \mathbb{T}^{(D)}(S) \to A$ is a ring homomorphism, which factors through $\hat{\mathbb{T}}^{(D)}(S)_{\mathfrak{m}}$ for some maximal ideal $\mathfrak{m}$, since A is complete and local. (The ideal $\mathfrak{m}$ can be seen as the kernel of $\hat{\mathbb{T}}^{(D)}(S) \to A \twoheadrightarrow A/\mathfrak{p}$.) We thus have a ring homomorphism $\hat{\mathbb{T}}^{(D)}(S)_{\mathfrak{m}} \to A$. Composing this with the Galois representation $\rho_{\mathfrak{m}}$ from Theorem 3.11 yields the desired Galois representation $\rho_{f,p}$. □

3.4 Nebentype obstructions

We show here that in order to strip powers of p from the level of a Galois representation which is strongly modular, it is necessary in general to consider the Galois representations attached to dc-weak eigenforms. The argument uses certain nebentypus obstructions that also – in general – prohibit 'weak' eigenforms of level prime-to-p from coinciding with 'dc-weak' eigenforms.

Assume $p \nmid N$ and let $f \in S_k(\Gamma_1(Np^r))(\overline{\mathbb{Z}}_p)$ be a strong eigenform. A consequence of the result of stripping powers of p from the level is that the Galois representation $\rho_{f,p,m}$ dc-weakly arises from $\Gamma_1(N)$. We show that $\rho_{f,p,m}$ does not, in general, weakly arise from $\Gamma_1(N)$.

Suppose that $\langle \ell \rangle f = \chi(\ell) f$ for primes ℓ with $\ell \nmid DNp$ (for some positive integer D), with a character χ that we decompose as $\chi = \psi\omega^i\eta$, where ψ is a character of conductor dividing N, ω is the Teichmüller lift of the mod p cyclotomic character, and η is a character of conductor dividing p^r and order a power of p. Assume p is odd, $r \geq 2$, $\eta \neq 1$, and $m \geq 2$. Let $\rho_{f,p,m}$ be the mod p^m representation attached to f. Then it is not possible to find a weak eigenform $g \in S_{k'}(\Gamma_1(N))(\overline{\mathbb{Z}/p^m\mathbb{Z}})$ of any weight k' such that $\rho_{g,p,m} \cong \rho_{f,p,m}$ by the argument below.

Let η have order p^s where $1 \leq s \leq r-1$. Then we may regard η as a character $\eta : (\mathbb{Z}/p^r\mathbb{Z})^\times \to \mathbb{Z}_p[\zeta]^\times$, where ζ is a primitive p^s-th root of unity. Assume there exists a weak eigenform g on $\Gamma_1(N)$ such that $\rho_{f,p,m} \cong \rho_{g,p,m}$. As g is an eigenform for $\langle \ell \rangle$ for primes ℓ with $\ell \nmid DNp$, we have that $\langle \ell \rangle g = \psi'(\ell) g$, where

$$\psi' : (\mathbb{Z}/N\mathbb{Z})^\times \to \overline{\mathbb{Z}/p^m\mathbb{Z}}^\times$$

is a mod p^m character of conductor dividing N. Since $\rho_{f,p,m} \cong \rho_{g,p,m}$, we have that $\det \rho_{g,p,m} = \det \rho_{f,p,m}$. Now, we know that

$$\det \rho_{f,p,m} \equiv \epsilon^{k-1}\psi\omega^i\eta \pmod{p^m},$$

with ϵ the p-adic cyclotomic character. Also, from the construction of the Galois representation attached to g, we have that

$$\det \rho_{g,p,m} \equiv \epsilon^{k'-1}\psi' \pmod{p^m}.$$

Hence, after restricting to the inertia group at p, we have that

$$\epsilon^{k'-1} \equiv \eta\epsilon^{k-1} \pmod{p^m}$$

as characters of $\mathbb{Z}_p^\times$, or equivalently, $\eta \equiv \epsilon^{k'-k} \pmod{p^m}$.

The cyclotomic character $\epsilon(x) = x$ has values in $\mathbb{Z}_p$, however the image of the character η in $\mathbb{Z}_p[\zeta]$ contains ζ. Since $m \geq 2$, the injection

$$\mathbb{Z}_p/(p^m) \hookrightarrow \mathbb{Z}_p[\zeta]/(1-\zeta)^{(m-1)p^{s-1}(p-1)+1}$$

is not a surjection. Thus, the reduction mod p^m of $\epsilon^{k'-k}$ has values in $\mathbb{Z}_p/(p^m)$, but the reduction mod p^m of η does not. This contradicts the equality $\eta \equiv \epsilon^{k'-k} \pmod{p^m}$.

Note for $m = 1$, we always have $\eta \equiv 1 \pmod{p}$ and hence it is possible to have the equality of characters in this situation.

Although the main purpose of this section is to show that there exist $\rho_{f,p,m}$ which arise strongly from $\Gamma_1(Np^r)$ and do not arise weakly from $\Gamma_1(N)$, we note the proof shows there exist dc-weak eigenforms of level N which are not weak eigenforms of level N.

3.5 On the weights in divided congruences

In this subsection we show that under *certain* conditions, the weights occurring in a dc-weak eigenform satisfy enough congruence conditions so that one can equalize them using suitable powers of Eisenstein series. In fact, Corollary 3.15 below is a generalization of some of the results in Chen-Kiming-Rasmussen, using different methods. We impose here that $p > 2$.

Lemma 3.13. *Let $\mathcal{O}$ be a local ring with maximal ideal $\mathfrak{p}$, and let M be a finite projective $\mathcal{O}$-module. If $\bar{f}_1, \ldots, \bar{f}_n \in M/\mathfrak{p}M$ are linearly independent over $\mathcal{O}/\mathfrak{p}$, then $f_1, \ldots, f_n \in M/\mathfrak{p}^m M$ are linearly independent over $\mathcal{O}/\mathfrak{p}^m$.*

Proof. M is isomorphic to $F \oplus \bigoplus_{i=1}^n \mathcal{O} f_i$ with F a free $\mathcal{O}$-module, from which the assertion immediately follows. □

Proposition 3.14. *Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$. Let $f_i \in S_{k_i}(\Gamma_1(Np^r))(\mathcal{O})$ for $i = 1, \ldots, t$, where the k_i are distinct, and suppose $[\ell]f_i = \ell^{k_i}\psi_i(\ell)\eta_i(\ell)f_i$, for $\ell \nmid DNp$ (for some positive integer D), where $\psi_i : \mathbb{Z}/N\mathbb{Z}^\times \to \mathcal{O}^\times$, $\eta_i : \mathbb{Z}/p^r\mathbb{Z}^\times \to \mathcal{O}^\times$ have finite order. Suppose also that the q-expansions $f_i(q) \pmod{p}$ are linearly independent over $\overline{\mathbb{Z}/p\mathbb{Z}} = \overline{\mathbb{F}}_p$.*

Put $f := \sum_{i=1}^t f_i$ and assume that f is an eigenform for the operators $[\ell]$ (e.g. this is the case if f is a dc-weak eigenform).

Then $k_1 \equiv k_2 \equiv \cdots \equiv k_t \pmod{\varphi(p^m)/h}$, where φ is the Euler-φ-function, and h is the least common multiple of the orders of the $\eta_i \pmod{p^m}$.

Proof. Denote by λ, λ_i the $[\ell]$-eigenvalue of f and the f_i, respectively. Then we have

$$\lambda f \equiv \sum_{i=1}^t \lambda_i f_i(q) \pmod{p^m},$$

whence $\sum_{i=1}^t (\lambda - \lambda_i) f_i(q) \equiv 0 \pmod{p^m}$. Lemma 3.13 applied with $M = \mathcal{O}[[q]]/(q^L)$ for suitable L large enough (for instance, take L so that the q-expansion map $\oplus_{i=1}^t S_{k_i}(\Gamma_1(Np^r))(\mathcal{O}) \to \mathcal{O}[[q]]/(q^L)$ is injective), shows that $\lambda \equiv \lambda_i \pmod{p^m}$ for all i. In particular, we have $\lambda_i \equiv \lambda_j \pmod{p^m}$ for all i, j.

We have $\lambda_i = \ell^{k_i}\psi_i(\ell)\eta_i(\ell)$. If $\ell \equiv 1 \pmod{N}$ then $\psi_i(\ell) = 1$. For such ℓ we thus have

$$\ell^{k_i h} = \lambda_i^h \equiv \lambda_j^h = \ell^{k_j h} \pmod{p^m}$$

for all i, j, by the definition of h.

By Chebotarev's density theorem, we can choose ℓ so that in addition to the property $\ell \equiv 1 \pmod{N}$, we have that ℓ is a generator of $(\mathbb{Z}/p^m\mathbb{Z})^\times$ (here we use that p is odd and that $p \nmid N$.) It then follows that $k_1 h \equiv k_2 h \equiv \ldots \equiv k_t h \pmod{\varphi(p^m)}$ as desired. □

The proposition has the following application. Suppose that f is a dc-weak eigenform mod p^m at level N of the form $f = \sum_{i=1}^t f_i$ with $f_i \in S_{k_i}(\Gamma_1(N))(\mathcal{O})$ for $i = 1, \ldots, t$, where the k_i are distinct. Suppose that each f_i has a nebentypus and that, crucially, the q-expansions $f_i(q) \pmod{p}$ are linearly independent over $\overline{\mathbb{F}}_p$.

Then the proposition applies with $h = 1$ and shows that we have $k_1 \equiv \cdots \equiv k_t \pmod{\varphi(p^m)}$. Without loss of generality suppose that k_t is the largest of the weights. When $p \geq 5$, we can use the Eisenstein series $E := E_{p-1}$ of weight $p-1$ and level 1, normalized in the usual way so that its q-expansion is congruent to $1 \pmod{p}$. The form $\tilde{E} := E^{p^{m-1}}$ is of weight $\varphi(p^m) = (p-1)p^{m-1}$, level 1, and is congruent to $1 \pmod{p^m}$. Due to the congruence on the weights, we may multiply each f_i for $i = 1, \ldots, t-1$ with a suitable power of $\tilde{E}$ so as to make it into a form of weight k_t with the same q-expansion mod p^m. Consequently, in weight k_t and level N there is a form that is congruent to f mod p^m, i.e., f is in fact a weak eigenform mod p^m at level N.

We also record the following variant of Proposition 3.14 as it represents a generalization of some of the results of Chen-Kiming-Rasmussen.

Corollary 3.15. *Let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$. Let $f_i \in S_{k_i}(\Gamma_1(Np^r))(\mathcal{O})$ for $i = 1, \ldots, t$ satisfy $f_1(q) + \ldots + f_t(q) \equiv 0 \pmod{p^m}$, where the k_i are distinct, and suppose $[\ell]f_i = \ell^{k_i}\psi_i(\ell)\eta_i(\ell)f_i$, where $\psi_i : \mathbb{Z}/N\mathbb{Z}^\times \to \mathcal{O}^\times$, $\eta_i : \mathbb{Z}/p^r\mathbb{Z}^\times \to \mathcal{O}^\times$ have finite order. Suppose for some i, the q-expansions $f_j(q) \pmod{p}$, $j \neq i$ are linearly independent over $\overline{\mathbb{Z}/p\mathbb{Z}} = \overline{\mathbb{F}}_p$.*

Then $k_1 \equiv k_2 \equiv \cdots \equiv k_t \pmod{\varphi(p^m)/h}$, where φ is the Euler-φ-function, and h is the least common multiple of the orders of the $\eta_j \pmod{p^m}$.

Proof. Without loss of generality, assume $i = 1$. As $-f_1(q) \equiv \sum_{i=2}^t f_i \pmod{p^m}$ the proof of Proposition 3.14 shows that we have

$$\ell^{k_1}\psi_1(\ell)\eta_1(\ell) \equiv \ell^{k_i}\psi_i(\ell)\eta_i(\ell) \pmod{p^m}$$

for $i = 2, \ldots, t$, and the desired congruences then follow in the same way. □

References

[1] H. Hida: 'Galois representations into $\mathrm{GL}_2(\mathrm{Z}_p[[X]])$ attached to ordinary cusp forms', Invent. Math. **85** (1986), 545–613.

[2] T. Miyake: 'Modular Forms', Springer-Verlag, 1989.

[3] X. Taixés i Ventosa and G. Wiese: 'Computing Congruences of Modular Forms and Galois Representations Modulo Prime Powers' in Arithmetic, Geometry, Cryptography and Coding

Theory 2009, edited by: David Kohel and Robert Rolland. Contemporary Mathematics **521** (2010), 145–166.

[4] Gabor Wiese. *Computational Arithmetic of Modular Forms*. Wintersemester 2007/2008. Universität Duisburg-Essen, http://maths.pratum.net/notes/MFII.pdf