GALOIS REPRESENTATIONS AND MODULAR FORMS

COURSE: ANNA MEDVEDOVSKY & ALEXANDRU GHITZA
NOTES: ROSS PATERSON

DISCLAIMER. These notes were taken live during lectures at the Introduction to SAGA winter school held at the CIRM from 30th January to 3rd February 2023. Any errors are the fault of the transcriber and not of the lecturer.

LECTURE 1 (MEDVEDOVSKY): GALOIS GROUPS

Our plan will be to try to cover the following:

- Galois Groups
- Galois Representations
- Tate Modules of Elliptic Curves
- Modular Forms attached to Galois Representations
- Mod-p phenomena

1. GALOIS GROUPS

Let K be a field (e.g. $\mathbb{F}_p$, $\mathbb{Q}_p$, $\mathbb{Q}$), and $\overline{K}$ be an algebraic closure. Note that if $\overline{K}'$ is a second algebraic closure of K then the two are (non-canonically) isomorphic via some σ. This isomorphism is in no way canonical, and when we form the Galois groups $\mathrm{Gal}(\overline{K}/K) \cong \mathrm{Gal}(\overline{K}'/K)$ the induced isomorphism is

$$\tau \mapsto \sigma\tau\sigma^{-1}.$$

This is to say: there are no good elements, only good conjugacy classes.

Note that $G_K := \mathrm{Gal}(\overline{K}/K) := \varprojlim_{L/K} \mathrm{Gal}(L/K)$, where the limit is now over *finite* Galois extensions, with the maps being restriction maps: for $M/L/K$ we have $\mathrm{res} : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$. In particular, G_K is a profinite group and so comes with an associated Krull topology. In this topology a basis of open neighbourhoods of 1 the subgroups $\mathrm{Gal}(\overline{K}/L)$ for finite Galois L/K – they're very large! Galois correspondence in this setting says that *closed* subgroups $H \leq G_K$ correspond to extensions $M = \overline{K}^H/K$, and that *open* subgroups further correspond to the finite suck extensions. Moreover normal (closed) subgroups, as for finite Galois theory, correspond to Galois extensions of K.

1.1. **Finite Fields.** $K = \mathbb{F}_q$ where $q = p^d$ for some prime p. For L/K some finite extension, we know $L = \mathbb{F}_{q^n}$ for some n and moreover that $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$ with isomorphism given by mapping frobenius ($x \mapsto x^q$) to the element $1 \in \mathbb{Z}/n\mathbb{Z}$. Taking an inverse limit we obtain

$$G_K = \varprojlim_{L/K} \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}} = \prod_{\ell \text{ prime}} \mathbb{Z}_\ell.$$

1.2. **Local Fields.** $K/\mathbb{Q}_p$ finite, having an absolute value $|\cdot| : K \to \mathbb{R}_{\geq 0}$, integers $\mathcal{O}_K$, maximal ideal $\mathfrak{m}_K$, residue field k_K. Then for every finite extension L/K the absolute value extends uniquely to L. We then have a short exact sequence

$$1 \to I(L/K) \to \mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k_K) \to 1,$$

where $I(L/K)$ is the so-called 'inertia subgroup'. This gives us a maximal unramified extension $L^{\mathrm{nr}} := L^{I(L/K)}$. Note that $\mathrm{Gal}(L_{\mathrm{nr}}/K) \cong \mathrm{Gal}(k_L/k_K)$ is cyclic by §1.1. Then we take an inverse limit to obtain

$$1 \to I_K \to G_K \to G_{k_K} \to 1,$$

where now $G_{k_K} \cong \widehat{Z}$ as in §1.1. In this setting I_K is quite complicated. It has a huge (normal) p-sylow subgroup I_K^{wild}, the quotient by which is tame inertia I_K^{tame}. We denote by $K^{\mathrm{nr}} := \overline{K}^{I_K}$ the maximal unramified extension.

1.3. **Number Fields.** $K/\mathbb{Q}$ finite, so a number field. We'd like to look at this locally and try to patch together information from the local fields. Ostrowski's theorem says (for Ω_K the set of equivalence classes of absolute values on K),

$$v \in \Omega_K \leftrightarrow \begin{cases} \text{primes } \mathfrak{p} \mid p \text{ of } \mathcal{O}_K \text{ (finite places) where } K_v/\mathbb{Q}_p \text{ is finite} \\ (K \to \mathbb{C})/(\text{complex conjugation}) \text{ (infinite places) where } K_v = \mathbb{R} \text{ or } \mathbb{C} \end{cases}$$

Then for each $v \in \Omega_K$ there may be several places $w \in \Omega_L$ such that $w \mid v$. However, $\mathrm{Gal}(L/K)$ acts transitively on $\{w \in \Omega_L \ : \ w \mid v\}$, and for a choice of $w \mid v$ we have the stabiliser $D_w := \mathrm{stab}_{\mathrm{Gal}(L/K)}(w)$ which is known as the 'decomposition group of w'. Note that the elements of $\{D_w \ : \ w \mid v\}$ are all conjugate subgroups inside of $\mathrm{Gal}(L/K)$. Moreover, it is not hard to show that

$$D_w \cong \mathrm{Gal}(L_w/K_v),$$

and so $D_w \supseteq I_w$ where I_w is the inertia for the extension L_w/K_v (see §1.2). Taking a compatible system of $w \mid v$ for each L/K finite (so $w \mid w' \mid v$ whenever $L \supseteq L' \supseteq K$) is equivalent to choosing an embedding $\overline{K} \to \overline{K_v}$, and then we can take a limit to obtain the inertia group

$$I_v := \varprojlim_{L_w/K_v} I(L_w/K_v)$$

where the limit is over our compatible system.

To close: let $S \subseteq \Omega_K$ be a finite set of places, and let

$$G_{K,S} := G_K / {}^{\text{Smallest normal subgroup}}_{\text{containing } I_v \ \forall \ v \notin S} = \mathrm{Gal}(K_{\mathrm{nr},S}/K),$$

where $K_{\mathrm{nr},S}/K$ is the maximal extension of K unramified for $v \notin S$. Then in fact frobenii (topologically) generate $G_{K,S}$:

Theorem 1 (Chebotarev density theorem)**.** *Conjugacy classes of* Frob_v *for* $v \notin S$ *are dense in* $G_{K,S}$*.*

Lecture 2 (Medvedovsky & Ghitza): Lecture 2

2. Galois Representations

Definition 2. Let K be a field, F a topological field (think $F/\mathbb{Q}_p, \mathbb{R}, \mathbb{C}$). Then a Galois representation (ρ, V) (i.e. a G_K-rep) is a continuous group homomorphism

$$\rho : G_K \to \mathrm{GL}_F(V).$$

where V is a finite dimensional F-vector space. A morphism of G_K-reps from V to W is a G_K-equivariant F-linear map ϕ such that for all $g \in G_K$, the diagram

$$\begin{array}{ccc} V & \xrightarrow{\phi} & W \\ \downarrow{\scriptstyle \rho_V(g)} & & \downarrow{\scriptstyle \rho_W} \\ V & \xrightarrow{\phi} & W \end{array}$$

commutes.

We then have some properties

Definition 3. For a given G_K-rep (ρ, V):

- a *subrepresentation* W is a G_K-stable subspace $W \subset V$. W is proper if it is nonzero and not equal to V;
- V is *irreducible* if it has no proper subrepresentations;
- V is *indecomposable* if it is not a sum of proper subrepresentations;
- V is *semisimple* if it is a direct sum of irreducible subrepresentations.

Remark 4. Unlike for finite groups, there are, in general, indecomposable representations which are not irreducible.

Now assume K is a number field with (ρ, V) a G_K-rep.

Definition 5. We say

- (ρ, V) is unramified at v if $I_v \subseteq \ker(\rho)$;
- If (ρ, V) is unramified at every $v \notin S$ then (ρ, V) factors through $G_{K,S}$.

Note that we have the following corollary of the Brauer-Nesbitt theorem.

Theorem 6. *If* $\mathrm{char}(F)$*, then* $v \mapsto \mathrm{tr}\rho(\mathrm{Frob}_v)$ *for* $v \notin S$ *determines a semisimple representation of* $G_{K,S}$*.*

2.1. Artin Representations.

Consider the case $F = \mathbb{C}$, then we call such a representation an *Artin representation*. In this case we have the following:

Theorem 7. *Every Artin representation has finite image. Moreover, as a result, these representations are semisimple and are unramified almost everywhere (as they must factor through a finite extension).*

2.2. p-adic representations.

Consider the case $F = \mathbb{Q}_p$, then we have the first example given by the p-adic cyclotomic character. Assume that K is any field, then we have an injection

$$\mathrm{Gal}(K(\mu_n)/K) \hookrightarrow \mathbb{Z}/n\mathbb{Z}^\times,$$

given by mapping $\sigma \mapsto a$ where $\sigma(\zeta_n) = \zeta_n^a$. Consider the case that $n = p^k$, then taking limits on k we obtain a continuous map

$$\omega_p : G_K \to \mathrm{Gal}(K(\mu_{p^\infty})/K) \hookrightarrow \mathbb{Z}_p^\times \subseteq \mathbb{Q}_p^\times.$$

We call this the p-adic cyclotomic character. If $K = \mathbb{Q}$ then note that this character ramifies only at p. In particular, for $\ell \neq p$ prime we have

$$\omega_p(\mathrm{Frob}_\ell) = \ell$$

since $\mathrm{Frob}_\ell(x) \equiv x^\ell \mod \ell$ and so $\mathrm{Frob}_\ell(\zeta_p^k) = \zeta_{p^k}^\ell$.

3. Elliptic Curves

Let E/K be a smooth projective curve of genus 1 with a K-rational point. Then we (as long as K does not have characteristic $2, 3$) can reduce to

$$E : y^2 = x^3 + Ax + B,$$

for $A, B \in K$ such that $4A^3 + 27B^2 \neq 0$. Then the K-rational points on these curves form an abelian group, and recall that we have maps for each $m \in \mathbb{Z}$

$$[m] : E \to E,$$

given by multiplication by m, and we denote by $E[m] = \ker([m])$. If m is coprime to $\mathrm{char}(K)$ we have $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$. Now let ℓ be a prime, then we have the ℓ-adic Tate module

$$T_\ell(E) := \varprojlim_k E[\ell^k] \cong \mathbb{Z}_\ell^2$$

where the second isomorphism is as abelian groups. Note that the action of G_K on each $E[\ell^k]$ commutes with the transition maps in the limit and so G_K acts continuously on $T_\ell(E)$. Moreover we then have an associate ℓ-adic representation on the vector space

$$V_\ell(E) := T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

That we denote by

$$\rho_{E,\ell} : G_K \to \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E)) \subseteq \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Q}_\ell).$$

One useful property here is that in fact V_ℓ is functorial, and so induces a map for each pair E_1, E_2 of elliptic curves

$$\mathrm{Hom}(E_1, E_2) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to \mathrm{Hom}_{\mathbb{Z}_\ell}(T_\ell(E_1), T_\ell(E_2))$$

which is an injection.

Lecture 3 (Ghitza)

We recall the representation $\rho_{E,\ell}$ associated to an elliptic curve and prime ℓ from last time. Recall that for an isogeny $\phi : E_1 \to E_2$ is always surjective with finite kernel, and that there is a dual isogeny $\phi^\vee : E_2 \to E_1$, and that

$$\phi^\vee \circ \phi = [\deg(\phi)]_{E_1} \quad \phi \circ \phi^\vee = [\deg(\phi)]_{E_2}$$

Example 8. *For $m \in \mathbb{Z}$ we have the isogeny $[m] : E \to E$, the dual is $[m]^\vee = [m]$, and so the degree is m^2.*

Example 9. *If $E/\mathbb{F}_p$ then we have a Frobenius isogeny*

$$F : E \to E; \quad (x, y) \mapsto (x^p, y^p)$$

We have maps

$$\mathrm{End}(E) \otimes \mathbb{Z}_\ell \hookrightarrow \mathrm{End}_{\mathbb{Z}_\ell}(T_\ell(E))$$
$$\phi \mapsto \phi_\ell$$

Proposition 10. *We always have:*

(1) $\det(\phi_\ell) = \deg(\phi)$*;*
(2) $\mathrm{tr}(\phi_\ell) = 1 + \det(\phi_\ell) - \det(I - \phi_\ell)$

3.1. **Elliptic Curves over Finite Fields.** Consider the case $K = \mathbb{F}_p$ for some $p \neq \ell$ and E/K an elliptic curve. Then G_K is topologically generated by Frobenius $\mathrm{Frob} : x \mapsto x^p$. We have

$$F_\ell := \rho_{E,\ell}(\mathrm{Frob}) \in \mathrm{Aut}_{\mathbb{Z}_\ell}(T_\ell(E)),$$

where F is the Frobenius as in Example 9.

Theorem 11. *If $E/\mathbb{F}_p$, $p \neq \ell$, then $\deg(F) = p$, $\deg(I - F) = \#E(\mathbb{F}_p)$. So that*
(a) $\det \rho_{E,\ell}(\mathrm{Frob}) = p$*;*
(b) $\mathrm{tr}\rho_{E,\ell}(\mathrm{Frob}) = p + 1 - \#E(\mathbb{F}_p)$.

Remark 12. Note that there is **no dependence** on ℓ (other than not being p).

3.2. **Elliptic Curves over Local Fields.** Consider the case $K = \mathbb{Q}_p$, again $p \neq \ell$, and E/K an elliptic curve. We assume that E is presented to us with a minimal Weierstrass equation with $\mathbb{Z}_p$-coefficients, with discriminant $\Delta_{\min}$.

3.2.1. *Good Reduction.*

Definition 13. Say that $E/\mathbb{Q}_p$ has good reduction if $v_p(\Delta_{\min}) = 0$.

We can reduce our model mod p to give a curve $\tilde{E}\mathbb{F}_p$.

Theorem 14 (Néron–Ogg–Shafarevich)**.** *If $p \neq \ell$, then $E/\mathbb{Q}_p$ has good reduction if and only if $\rho_{E,\ell}$ is unramified.*

Moreover, if E has good reduction then the diagram below commutes

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I_{\mathbb{Q}_p} & \longrightarrow & G_{\mathbb{Q}_p} & \longrightarrow & G_{\mathbb{F}_p} & \longrightarrow & 1 \\ & & & & \downarrow{\scriptstyle \rho_{E,\ell}} & & \downarrow{\scriptstyle \rho_{\tilde{E},\ell}} & & \\ & & & & \mathrm{Aut}(V_\ell(E)) & \longrightarrow & \mathrm{Aut}(V_\ell(\tilde{E})). & & \end{array}$$

Corollary 15. *If $\ell \neq p$ and $E/\mathbb{Q}_p$ has good reduction, then*

$$\det(\rho_{E,\ell}(\mathrm{Frob})) = p,$$
$$\mathrm{tr}(\rho_{E,\ell}(\mathrm{Frob})) = p + 1 - \#\tilde{E}(\mathbb{F}_p),$$

where Frob *is a choice of Frobenius element. Note that by Néron–Ogg–Shafarevich we know that the representation $\rho_{E,\ell}$ is unramified and so the choice is unimportant.*

3.2.2. *Bad Reduction.* Ok so what about when we don't have good reduction? Well we have...bad reduction. There are several possibilities

- Multiplicative Reduction: i.e. $\tilde{E}/\mathbb{F}_p$ has a node. In this case the reduction can be:
  - split if the slopes of the tangent are defined over $\mathbb{F}_p$
  - nonsplit if the slopes of the tangent are not defined over $\mathbb{F}_p$
- additive: $\tilde{E}/\mathbb{F}_p$ has a cusp.

Remark 16. In the (split) multiplicative case, there is Tate's uniformization which identifies $E(\mathbb{Q}_p)$ with $\mathbb{Q}_p^\times/q^{\mathbb{Z}}$ for some parameter $q \in p\mathbb{Z}_p$.

3.3. **Elliptic Curves over Number Fields.** Consider the case $K = \mathbb{Q}$, say $E/\mathbb{Q}$ has been presented to us with a minimal Weierstrass equation with coefficients in $\mathbb{Z}$ and write $\Delta_{\min}$ for the discriminant of this model.

Definition 17. $E/\mathbb{Q}$ has good reduction at p if $p \nmid \Delta_{\min}$. In this case the reduction mod p of the model gives an elliptic curve $\tilde{E}/\mathbb{F}_p$.

Theorem 18. *If $p \neq \ell$, then $E/\mathbb{Q}$ has good reduction at p if and only if $\rho_{E,\ell}$ is unramified at p. In this case:*

(1) $\det \rho_{E,\ell}(\mathrm{Frob}_p) = p$,

(2) $\mathrm{tr}\rho_{E,\ell}(\mathrm{Frob}_p) = p + 1 - \#\tilde{E}(\mathbb{F}_p) =: a_p(E)$,

where Frob_p *is a choice of Frobenius at p.*

Remark 19. Again, since the representation is unramified, the choice of Frobenius is unimportant.

Remark 20. $\det(\rho_{E,\ell}) \cong \omega_\ell$, the ℓ-adic cyclotomic character.

Theorem 21 (Serre)**.** *(If $\mathrm{End}_{\mathbb{Q}}(E) \cong \mathbb{Z}$) then $\rho_{E,\ell}$ is irreducible for all ℓ.*

Whilst the bracket is a trivial statement, one cannot realise additional CM endomorphisms over $\mathbb{Q}$, if we were to replace $\mathbb{Q}$ with a number field then this could potentially be nontrivial.

Remark 22. Ideally we'd study the G_K module $E(\overline{K})$, but this isn't even linear. We linearise by taking the Tate module. In general, inspired by geometry, one could take modules arising in cohomology instead. In fact, it turns out that

$$V_\ell(E) \cong H^1_{\text{ét}}(E_{\overline{K}}, \mathbb{Q}_\ell)^\vee.$$

Lecture 4 (Ghitza): Modular Forms

4. Modular Forms

It's about time we talked about modular forms.

Theorem 23 (Eichler–Shimura–Deligne)**.** *Let $k \geq 2$, $N \geq 1$, ε a Dirichlet character mod N. Let $f \in S_k(N, \varepsilon)$ be a newform with Hecke eigenvalues $T_p(f) = a_p f$ for $p \nmid N$. Take the number field $K = \mathbb{Q}(\{a_p, \varepsilon(p) \ : \ p \nmid N\})$, and let λ be a finite place of K with residue characteristic ℓ and completion K_λ.*

Then there exists an irreducible Galois representation

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_\lambda),$$

that is unramified outside of $N\ell$ such that for all $p \nmid N\ell$

$$\det \rho_{f,\lambda}(\mathrm{Frob}_p) = \varepsilon(p)p^{k-1},$$
$$\mathrm{tr}\rho_{f,\lambda}(\mathrm{Frob}_p) = a_p.$$

Remark 24. Notice that $\det \rho_{f,\lambda}(\mathrm{Frob}_p) = \varepsilon\omega_\ell^{k-1}$ for ω_ℓ the ℓ-adic cyclotomic character.

Remark 25. Linking to last time, roughly: there is a correspondence

$$E/\mathbb{Q} \to f \in S_2(N, 1)$$

to those with rational eigenvalues and such that $\rho_{E,\ell} = \rho_{f,\ell}$ and $a_p(E) = a_p(f)$ for all p.

4.1. **Classical Modular Forms.**

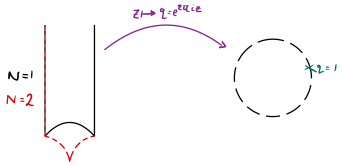
Definition 26. A modular form $f \in M_k(N, \varepsilon)$ is a map $f : \mathfrak{h} \to \mathbb{C}$, where $\mathfrak{h}$ is the upper half plane in $\mathbb{C}$, which is holomorphic, satisfies

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z\right) = \varepsilon(d)(cz+d)^k f(z),$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z})$ (the ones with $c \equiv 0 \mod N$), and is 'holomorphic at the cusps'.

Remark 27 (Holomorphy at cusps). Indeed, a modular form f has a q-expansion $f(z) = \sum_{n\in\mathbb{Z}} a_n q^n$ where $q = q(z) = e^{2\pi i z}$, and f is holomorphic at the cusp $i\infty$ if $a_n = 0$ for all $n < 0$. For the other cusps: $\mathbb{P}^1(\mathbb{Q})/\Gamma_0(N)$ classifies the cusps, and f has a Fourier expansion at each cusp (much like the q-expansion is at $i\infty$), holomorphy at the cusp means that $a_n = 0$ for $n < 0$ in that Fourier expansion.

The q-expansion is the fourier expansion around a cusp, the picture to have in ones head when looking at the fundamental domain is below.



Definition 28. For a modular form $f \in M_k(N, \varepsilon)$, if $a_0 = 0$ at all cusps (i.e. f vanishes at the cusps) then we call f a cusp form and denote the set of such $S_k(N, \varepsilon)$.

Example 29.
- *Eisenstein series $G_k \in M_k(1)$ for $k \geq 4$.*
- *Theta series, which arise from certain quadratic forms.*
- $\eta(z) = q^{1/24}\prod_{n\geq 1}(1-q^n)$, *which has 'weight $q/2$'.*
- $\Delta(z) = \sum_{n\geq 1}\tau(n)q^n \in S_{12}(1)$

4.2. **Geometry.** Recall the subgroup

$$\Gamma_0(N) \supseteq \Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \mod N, \ a \equiv d \equiv 1 \mod N \right\}$$

One can prove that there is a decomposition

$$M_k(\Gamma_1(N)) = \bigoplus_{\varepsilon \text{dir. char.}} M_k(N, \varepsilon).$$

Now consider f of weight $k = 2$, for

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 f(z)$$

for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$. Note that f is not a function on $\mathfrak{h}/\Gamma_1(N) =: Y_1(N)_{\mathbb{C}}$. The transformation property shows that $f(z)dz$ is infact a differential on this geometric space: a global section of $\Omega^1_{Y_1(N)_{\mathbb{C}}}$.

Observe now that

$$Y_1(N)_{\mathbb{C}} = \left\{ \text{isom. classes of } (E, P), \ {}^{E/\mathbb{C}\text{Celliptic curve},}_{P\in E[N]} \right\},$$

so why not define a functor

$$Y_1(N) : \mathrm{Sch} \to \mathrm{Sets}$$

by

$$Y_1(N)(S) = \left\{\text{isom. classes of } (E,P),\ {}^{E/S \text{ elliptic curve,}}_{P \in E[N]}\right\}.$$

In fact, for $N \geq 4$ we get that $Y_1(N)$ is smooth and quasiprojective over $\mathbb{Z}[\frac{1}{N}]$. There is then a result of Kodaira–Spencer:

$$\Omega^1_{Y_1(N)} \cong \underline{\omega}^{\otimes 2},$$

giving

$$M_2(\Gamma_1(N), \mathbb{C}) = H^0(X_1(N)_{\mathbb{C}}, \underline{\omega}^{\otimes 2})$$

Remark 30. The condition $N > 4$ is because if N is smaller then there are extra automorphisms and then we will not obtain a scheme. If you're happy with algebraic stacks then one has to work in that realm to make geometric sense of this.

4.3. **Hecke Operators.** For $p \nmid N$ we could look at the group

$$\Gamma_1(N) \cap \Gamma_0(p) \subset \mathrm{SL}_2(\mathbb{Z}).$$

In this case it classifies triples (E, C, P) where $C \leq E[p]$ is a cyclic subgroup and $P \in E[N]$. Then we have

$$\mathfrak{h}/\Gamma_1(N) \cap \Gamma_0(p) = Y(\Gamma_1(N) \cap \Gamma_0(p)),$$

and there is the so-called Hecke correspondence

$$\begin{array}{ccccc} & & Y(\Gamma_1(N) \cap \Gamma_0(p)) & & \\ & \swarrow^{\beta} & & \searrow^{\alpha} & \\ Y_1(N) & & & & Y_1(N) \end{array}$$

where $\alpha(E, C, P)$ is equivalent to $(E/C, \pi(P))$ ($\phi : E \to E/C$ induced morphism to quotient), and $\beta(E, C, P)$ is equivalent to (E, P).

Have Hecke operators

$$T_p : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))$$
$$T_p \cdot f(z) = \sum_{n \geq 0} a_{n_p} q^n + \varepsilon(p) p^{k-1} \sum_{n \geq 0} a_n q^{n_p}$$

Lecture 5 (Ghitza & Medvedovsky)

5. Eichler–Shimura–Deligne (the speed dating version)

Recall the Eichler–Shimura–Deligne theorem, as in Theorem 23, which we restate below.

Theorem 31 (Eichler–Shimura–Deligne)**.** *Let $k \geq 2$, $N \geq 1$, ε a Dirichlet character mod N. Let $f \in S_k(N, \varepsilon)$ be a newform with Hecke eigenvalues $T_p(f) = a_p f$ for $p \nmid N$. Take the number field $K = \mathbb{Q}(\{a_p, \varepsilon(p) \ : \ p \nmid N\})$, and let λ be a finite place of K with residue characteristic ℓ and completion K_λ.*

Then there exists an irreducible Galois representation

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_\lambda)$$

that is unramified outside of $N\ell$ such that for all $p \nmid N\ell$

$$\det \rho_{f,\lambda}(\mathrm{Frob}_p) = \varepsilon(p)p^{k-1},$$
$$\mathrm{tr}\rho_{f,\lambda}(\mathrm{Frob}_p) = a_p.$$

How do we build this Galois representation? Look at $J_1(N) := \mathrm{Jac}(X_1(N))$, let $\mathbb{T}$ be the $\mathbb{Z}$-subalgebra of $\mathrm{End}(S_2(\Gamma_1(N)))$ generated by T_p for $p \nmid N$.

$$S_2(\Gamma_1(N)) = H^0(X_1(N)_{\mathbb{C}}, \Omega^1_{X_1(N)_{\mathbb{C}}})$$

which is the cotangent space at 0 in $J_1(N)_{\mathbb{C}}$. Thinking a little, $\mathbb{T}$ can be reinterpreted as $\mathrm{End}_{\mathbb{Z}}(J_1(N)_{\mathbb{C}})$. Our eigenform f defines

$$\phi : \mathbb{T} \to K$$
$$T_p \mapsto a_p$$

and $\ker \phi$ is an ideal, so

$$\ker(\phi) \cdot J_1(N)$$

is $\mathbb{T}$-stable and we can form the abelian variety

$$A_f = J_1(N)/\ker \phi \cdot J_1(N),$$

upon which T_p acts as multiplication by a_p. Then

$$\mathrm{End}(A_f) \otimes \mathbb{Q} = K$$

and $\dim A_f = [K : \mathbb{Q}]$. The obvious thing now would be to consider

$$G_{\mathbb{Q}} \to \mathrm{Aut}(V_\ell A_f),$$

but this is a $2[K : \mathbb{Q}]$ dimensional representation, not 2... However we note that $V_\ell(A_f)$ is in fact a rank 2 $K \otimes \mathbb{Q}_\ell$-module and so

$$G_{\mathbb{Q}} \to \mathrm{GL}_2(K \otimes \mathbb{Q}_\ell).$$

But then $K \otimes \mathbb{Q}_\ell = \prod_{\lambda|\ell} K_\lambda$ isn't a field... ok so pick your favourite factor to, finally, obtain:

$$\begin{array}{ccc} G_{\mathbb{Q}} & \longrightarrow & \mathrm{GL}_2(K \otimes \mathbb{Q}_\ell) \\ & \overset{\rho_{f,\lambda}}{\searrow} & \downarrow \\ & & \mathrm{GL}_2(K_\lambda). \end{array}$$

Now what about these determinant and trace properties?

Fix $p \nmid N$, let $\alpha : \mu_n \to E[n]$ and look at frobenius

$$F : X_1(N)_{\mathbb{F}_p} \to X_1(N)_{\mathbb{F}_p},$$
$$(E/R, \alpha) \mapsto (E^{(p)}/R, F \circ \alpha).$$

The dual of Frobenius is then a map on the divisors

$$F^\vee : J_1(N)_{\mathbb{F}_p} \to J_1(N)_{\mathbb{F}_p}$$
$$(E, \alpha) \mapsto \sum_{F : E_0 \to E} (E_0, F^\vee \circ \alpha).$$

Eichler–Shimura prove that $T_p = F + F^\vee$ as isogenies on $J_1(N)_{\mathbb{F}_p}$. We then consider the inclusion

$$\mathrm{End}(\tilde{A}_f) \hookrightarrow \mathrm{End}(V_\ell \tilde{A}_f)$$

which sends $F = T_p \mapsto \begin{pmatrix} a_p & 0 \\ 0 & a_p \end{pmatrix}$ Note that $F \circ F^\vee$ is multiplication by p. We stare for a moment and note that the trace and determinant properties are then immediate.

6. Galois side

Say we start with a Galois representation

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

where $\rho = \rho_{f,\mathfrak{p}}$ where $\mathfrak{p}$ is a degree 1 prime of K_f which is the Hecke eigenvalue field. Then $V \cong \mathbb{Q}_p^2$ always has an invariant lattice $\mathbb{Z}_p^2$, so ρ is the base-change of an integral representation

$$\begin{array}{ccc} G_{\mathbb{Q}} & \xrightarrow{\rho_\Lambda} & \mathrm{GL}(\Lambda) \\ & \searrow^{\overline{\rho_\Lambda}} & \downarrow \\ & & \mathrm{GL}_2(\mathbb{F}_p) \end{array}$$

Some points:

- Λ is not unique in general, so ρ_λ, $\overline{\rho_\lambda}$ is not determined by p alone
- However, the semisimplification $\overline{\rho_\lambda}^{ss}$ *is* determined by p!

6.1. **Modular Forms Side.** Consider $\Gamma_0(N)$, $p \nmid N$, look at $M_k(N, \mathbb{Q}_p)$ which is finite dimensional, say $d_k \sim \frac{k}{12}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$ is the dimension of this space. The finitely many normalised eigenforms $f_1, \ldots, f_{d_k}$ all have $\mathbb{Z}_p$-coefficients, so we reduce mod p and in the end we only get finitely many $\overline{f}$, *even as* $k \to \infty$!

Example 32. $p = 2$, $N = 1$ *then any cuspidal eigenform mod* 2 *is congruent to* Δ *modulo* 2.

You can prove this finitude by working mod p. How? Well we define, following Serre–Swinnerton-Dyer,

$$M_k(N, \mathbb{F}_p) := \mathrm{im}\left(M_k(N, \mathbb{Z}) \to \mathbb{F}_p[[q]]\right).$$

Remark 33. Can also define this geometrically as in the previous section.

We have an action of Hecke operators on the left hand side

Theorem 34 (Deligne–Serre Lifting Lemma)**.** *Any system of mod p Hecke eigenvalues lifts.*

Consider

$$M_{k-p+1}(N, \mathbb{F}_p) \hookrightarrow M_k(N, \mathbb{F}_p) \to W_k(N) \to 1f \qquad \mapsto f\overline{E}_{p-1}$$

and $\overline{E}_{p-1} \sim G_{p-1}$.

Theorem 35 (Jochnowitz–Serre–Tate–Robert)**.**

$$W_k(N) \cong W_{k+p^2-1}(N)$$

as Hecke modules for $k \geq p_1$*, and the isomorphism is given explicitly by*

$$f \mapsto f \cdot \overline{E_{p+1}^{p-1}}$$