Galois representations

1 Introduction (Vladimir)

1.1 Galois representations

Galois representations really mean representations of Galois groups.

Definition 1.1. An *Artin representation,* ρ*,* over a field K is a finite dimensional complex representation of $\mathrm{Gal}(\overline{K}/K)$ which factors through a finite quotient (by an open subgroup). I.e., there exists finite Galois extension F/K, such that ρ comes from a representation of $\mathrm{Gal}(F/K)$

$$\begin{tikzcd} \overline{K} \arrow[d, dash] \\ F \arrow[d, dash, "G"] \\ K \arrow[uu, dash, bend left=60, "\mathcal{G}"] \end{tikzcd}$$

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(F/K) \to \mathrm{GL}_n(\mathbb{C})$$

Note. e.g., $\mathbb{I}$ the trivial representation is the same Artin representation for all F/K

Example. Let $F = \mathbb{Q}(\zeta_3, \sqrt[3]{5})$, $K = \mathbb{Q}$, $G = \mathrm{Gal}(F/\mathbb{Q}) = S_3 = \left\langle s, t | s^3 = t^2 = \mathrm{id}, tst = s^{-1} \right\rangle$. The character table is

	id	(12)	(123)
$\mathbb{I}$	1	1	1
ϵ	1	-1	1
ρ	2	0	-1

So:

- $\mathbb{I}(s) = \mathbb{I}(t) = 1$
- $\epsilon(s) = 1$,$\epsilon(t) = -1$
- $\rho(s) = \begin{pmatrix} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$, $\rho(t) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Example. Dirichlet characters: $\mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$ multiplicative.

$$\begin{tikzcd} \mathbb{Q}(\zeta_N) \arrow[d, dash] \\ \mathbb{Q} \arrow[u, dash, bend left=60, "\mathcal{G}=(\mathbb{Z}/N\mathbb{Z})^*"] \end{tikzcd}$$

Hence Dirichlet characters can be seen as representation $\chi : \mathcal{G} \to \mathbb{C}^1 = \mathrm{GL}_1(\mathbb{C})$

Definition 1.2. A *mod l Galois representation* is the same thing with matrices in $\mathrm{GL}_n(\mathbb{F}_l)$.

Example. Let $E/\mathbb{Q}$ be an elliptic curve. We know $E(\overline{\mathbb{Q}})[l] \cong \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$. Set $F = \mathbb{Q}(E[l])$, the smallest field generated by the x-coordinates and y-coordinates of the points of order l. We end up with a Galois group

$$\begin{tikzcd} F \arrow[d, dash, "\mathcal{G}"'] \\ \mathbb{Q} \end{tikzcd}$$

$\mathcal{G}$ acts on $E[l]$ and preserves addition, i.e., $g(P+Q) = g(P) + g(Q)$. Therefore we get $\rho : G \to \mathrm{GL}_2(\mathbb{F}_l)$.

E.g.: Let $y^2 = x^3 - 5$, then $E[2] = \{0, (\sqrt[3]{5}, 0), (\zeta_3\sqrt[3]{5}, 0), (\zeta_3^2\sqrt[3]{5}, 0)\}$. So take $F = \mathbb{Q}(\zeta_3, \sqrt[3]{5})$, then $G = \mathrm{Gal}(F/\mathbb{Q})$ permutes $E[2]$ (we see that $G = S_3$). Let us write down the matrix, so let $P = (\sqrt[3]{5}, 0)$ and $Q = (\zeta_3\sqrt[3]{5}, 0)$.

- $g \in S_3$ be a 3-cycle, $\rho(g) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$
- $g \in S_3$, be a transposition, $\rho(g) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_2)$

1.2 l-adic representations

Definition 1.3. A *continuous l-adic representation* over K is a continuous homomorphism $\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{GL}_d(\mathcal{F})$ for some finite $\mathcal{F}/\mathbb{Q}_l$.

Remark. An l-adic representation is continuous if and only if for all n there exists a finite Galois extension F_n/K such that $\mathrm{Gal}(K^{\mathrm{sep}}/F_n) \to \mathrm{id} \mod l^n$. I.e., $\rho \mod l^n$ factors through a finite extension F_n/K.

So $\mathrm{Gal}(K^{\mathrm{sep}}/F_1)$ map to $\begin{pmatrix} 1 + l\mathcal{O}_{\mathcal{F}} & l\mathcal{O}_{\mathcal{F}} \\ l\mathcal{O}_{\mathcal{F}} & 1 + l\mathcal{O}_{\mathcal{F}} \end{pmatrix}$.

Example. Let $E/\mathbb{Q}$ be an elliptic curve:

- P_1, Q_1 basis for $E(\overline{\mathbb{Q}})[l]$.
- P_2, Q_2 basis for $E(\overline{\mathbb{Q}})[l^2]$, with $lP_2 = P_1$, $lQ_2 = Q_1$
- $\vdots$
- P_n, Q_n basis for $E(\overline{\mathbb{Q}})[l^n]$, with $lP_n = P_{n-1}$, $lQ_n = Q_{n-1}$.

For $g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ define $0 \le a_n, b_n, c_n, d_n < l$ by $gP_1 = a_1P_1 + bQ_1$, $gQ_1 = c_1P_1 + d_1Q_1$, and $gP_n = (a_1 + \cdots + a_nl^{n-1})P_n + (b_1 + \cdots + b_nl^{n-1})Q_n$ and $gQ_n = (c_1 + \cdots + c_nl^{n-1})P_n + (d_1 + \cdots + d_nl^{n-1})Q_n$. Then

$$\rho(g) = \begin{pmatrix} a_1 + \cdots + l^{n-1}a_n + \dots & c_1 + \cdots + l^{n-1}c_n + \dots \\ b_1 + \cdots + l^{n-1}b_n + \dots & d_1 + \cdots + l^{n-1}d_n + \dots \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_l)$$

Note that $\rho(g) \mod l^n$ tells you what g does to $E[l^n]$. This does give a 2d continuous l-adic representations.

2 Galois Representations: vocabulary (Matthew S)

2.1 Galois Theory of Infinite Algebraic Extensions

Notation. $G(F/K) := \mathrm{Gal}(F/K)$, $G_K = G(\overline{K}/K)$ the absolute Galois group

For this section we assume K is a perfect field (so every extensions is separable) and F is a normal algebraic extension of K.

Example. Let p be a prime, $K = \mathbb{F}_p$ and $F = \overline{\mathbb{F}}_p$, let ϕ_p be defined as $\phi_p(x) = x^p$. $\mathbb{F}_p$ is fixed by $\langle \phi_p \rangle$. Naively we would think $G_{\mathbb{F}_p} = \langle \phi_p \rangle \cong \mathbb{Z}$, but this is not true at all. To see this, take $\phi \in G_{\mathbb{F}_p}$ such that $\phi|_{\mathbb{F}_{p^n}} = \phi_p^{a_n}$ where $\{a_n\}$ is a sequence such that $a_n \equiv a_m \mod m$ where $m|n$. This shows $G_{\mathbb{F}_p} > \langle \phi_p \rangle$.

Definition 2.1. Let F/K be a Galois extension. For each finite subextension K' consider $G(K'/K)$. When we have two of them, such that $K' \subseteq K''$ consider

$$G(K''/K) \to G(K'/K).$$

This defines an inverse system of groups. $G(F/K) = \varprojlim_{K'/K} G(K'/K)$.

$\mathcal{B} = \{\text{left/right cosets of finite index subgroups}\}$

Fact. *$G(F/K)$ is Hausdorff, compact and totally disconnected.*

Theorem 2.2. *Let F/K be a Galois extension. The map $K' \to G(F/K')$ is a bijective inclusion reversing correspondence between K' and closed subgroups of $G(F/K)$, $H \to F^H$.*

Example. Back to the example, $G(\mathbb{F}_{p^n}/\mathbb{F}_p) = \mathbb{Z}/n\mathbb{Z}$, so $G_{\mathbb{F}_p} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \widehat{\mathbb{Z}}$.

2.2 Galois groups of $\mathbb{Q}$.

Fix $\mathbb{Q} \to \mathbb{Q}_p$, $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$:

$$\begin{tikzcd}
\overline{\mathbb{Q}}_p \arrow[r, dash] \arrow[d, dash] & \overline{\mathbb{F}}_p \\
\mathbb{Q}_p^{\mathrm{ur}} \arrow[r, dash] \arrow[d, dash] & \overline{\mathbb{F}}_p \\
\mathbb{Q}_p \arrow[r, dash] & \mathbb{F}_p
\end{tikzcd}$$

Note $G(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p) \cong G_{\mathbb{F}_p}$.

$$\begin{tikzcd}
G_{\mathbb{Q}_p} \arrow[r, two heads] \arrow[rr, bend right] & G(\mathbb{Q}_p^{\mu_r}/\mathbb{Q}_p) \arrow[r, "\cong"] & G_{\mathbb{F}_p}
\end{tikzcd}$$

The kernel of such a map is I_p. I_p admits a large normal p-subgroup, W_p,the wild inertia group. I_p/W_p tame inertia

Let Θ :$G_{\mathbb{Q}_p} \twoheadrightarrow G(K/\mathbb{Q}_p)$, for a Galois extension of $\mathbb{Q}_p$ if :

- $\Theta(I_p) = 0$ we say that K is *unramified*
- $\Theta(W_p) = 0$ then we say that K is *tamely ramified*
- $\Theta(W_p) \neq 0$ then we say that K is *widely ramified*

Example. Cyclotomic extensions:

$G(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$, $K_l = \cup_{n \in \mathbb{Z}_{>0}} \mathbb{Q}(\zeta_{l^n})$ we have an isomorphism $G(K_l/\mathbb{Q}) \to \mathbb{Z}_l^*$. Let $\epsilon_l : G_{\mathbb{Q}} \to \mathbb{Z}_l^*$, defined as for: $\sigma \in G_{\mathbb{Q}}$,$\sigma(\zeta) = \zeta^{\epsilon_l(\sigma)}$. K_l is ramified at ∞ and at l, For $p \neq l$, recall ϕ_p, then $\epsilon(\phi_p) = p$, $\phi_p(\zeta) = \zeta^p$.

Conjecture. *Any finite group is a discrete quotient of $G_{\mathbb{Q}}$*

2.3 Restricting the ramification

Let S be a set of primes including $\{\infty\}$. Let $\mathbb{Q}_S$ be the maximal extension of $\mathbb{Q}$ unramified outside S. Let $G_{\mathbb{Q},S} = G(\mathbb{Q}_S/\mathbb{Q})$.

Theorem 2.3 (Hermito-Minkowski)**.** *Let $K/\mathbb{Q}$ finite, S a finite set of primes, $d \in \mathbb{Z}_{>0}$. Then there exists finitely many degree d extensions F/K unramified outside F.*

In particular $\mathrm{Hom}_{\mathrm{cont}}(G_{K,S}, \mathbb{Z}/p\mathbb{Z})$ is finite.

Theorem 2.4 (p-finiteness condition)**.** *Let p be a prime, K a number field, S a finite set of primes (non-archimedean). Let $G \subset G_{K,S}$ which is open then there exists only finitely many continuous homomorphism from G to $\mathbb{Z}/p\mathbb{Z}$.*

Theorem 2.5. *If K is a finite extension $\mathbb{Q}_p$ then G_K is topologically finite generated.*

Conjecture.

- *If $p \in S$, the map $G_{\mathbb{Q}_p} \to G_{\mathbb{Q},S}$ is an inclusion*
- *If $p \notin S$, the map $G_{\mathbb{Q}_p} \to G_{\mathbb{Q},S}$ has kernel exactly I_p. So $G_{\mathbb{Q}_p}/I_p \hookrightarrow G_{\mathbb{Q},S}$.*

Suppose now that we have not fixed our embedding.

Theorem 2.6 (Chebotarov)**.** *Let $K/\mathbb{Q}$ be a Galois extension unramified outside a finite set of primes S. Let $T \supseteq S$ be a finite set of primes. For each $p \notin T$ there exists a well-defined $[\phi_p] \subset G(K/\mathbb{Q})$, the union of these classes is dense in $G(K/\mathbb{Q})$*

2.4 Galois Representations

Definition 2.7. A Galois representation over a topological ring A unramified outside S (a set of primes) is a continuous homomorphism, $\rho : G_{\mathbb{Q},S} \to \mathrm{GL}_n(A)$.

Let M be a free rank n A-module, we can equip it with a G action: $g \cdot a = \rho(g) \cdot a$. More formally:
Suppose we have a free A-module M such that:

- G (a profinite group) acts continuously
- $M = \varinjlim_H M^H$ where H runs over open normal subgroups of G,

then we can make M into a $A[[G]]$-module: $A[[G]] = \varprojlim_H A[G/H]$ where H is as before.
We say ρ, a representation of $G_{\mathbb{Q}}$, is :

- unramified at p if it is trivial on I_p.
- tamely ramified at p if it is trivial on W_p
- otherwise it is widely ramified.

Proposition 2.8. *Let S be any set of primes:*

1. *An Artin representation, $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathbb{C})$, is determined by $\mathrm{trace}(\rho(\phi_p))$ on $p \notin S$ such that ρ is unramified at p.*
2. *A semisimple $\mod l$ representation, $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(k)$, is determined by the values of $\mathrm{trace}(\wedge^i(\rho(\phi_p)))$ where $i = 1, \dots, n$ on primes $p \notin S$ at which ρ is unramified. If $l > n$ it is sufficient to use $\mathrm{trace}(\rho(\phi_p))$ at the same primes.*
3. *A semisimple l-adic representations, $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(A)$, is determined by $\mathrm{trace}(\rho(\phi_p))$ on $p \notin S$ at which ρ is unramified.*

2.5 Conductors of representation

The inertia group I_p is filtered by $I_p^u \lhd G_{\mathbb{Q},p}$, closed and for $u \in [-1, \infty]$

- If $u \leq v$ then $I_p^u \supset I_p^v$
- If $u \leq 0$, then $I_p^u = I_p$ and $I_p^\infty = \{1\}$
- $W_p = \cup_{u>0} I_p^u$
- $I_p^u = \cap_{v<u} I_p^v$

Definition 2.9. Conductor of ρ at p is the integer

$$m_p(\rho) = \operatorname{codim}(\rho^{I_p}) + \int_0^\infty \operatorname{codim}(\rho^{I_p^u}) du$$

.

The conductor of ρ is the integer

$$N(\rho) = \prod_p p^{m_p(\rho)}$$

where p runs over all $p \neq l$ (unless its Artin)

3 Invariants of Artin and l-adic Representations (Céline)

Notation.

- π_K be a fixed uniformiser of K
- $\mathcal{O}_K$ the ring of integers of K
- ν_K the normalized valuation on K
- $I_{F/K}$ the inertia group
- $\mathrm{Frob}_{F/K}$ for a Frobenius element
- $\Phi_{F/K} = \mathrm{Frob}_{F/K}^{-1}$ also called the Geometric Frobenius

3.1 Artin Representation

3.1.1 Local polynomials and l-functions

Definition 3.1. The *local polynomial* of an Artin Representation ρ over a local field K is

$$P(\rho, T) = \det\left(1 - \Phi_{F/K} T|_{\rho^{I_{F/K}}}\right)$$

where ρ factors through F/K and $\rho^{I_{F/K}}$ is the subspace of $I_{F/K}$-invariant vectors.

Remark. $P(\rho, T)$ is essentially the characteristic polynomial of $\Phi_{F/K}$ on $\rho^{I_{F/K}}$

Example. Consider

$$\begin{tikzcd}
 & F = \mathbb{Q}_5(\zeta_3, \sqrt[3]{5}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}_5(\zeta_3) \arrow[dr, dash] & & \mathbb{Q}_5(\sqrt[3]{5}) \arrow[dl, dash] \\
 & K = \mathbb{Q}_5 &
\end{tikzcd}$$

We have $\mathrm{Gal}(F/K) \cong S_3$, $I_{F/K} \cong C_3 \cong \mathrm{Gal}(F/K(S_3))$ and $\mathrm{Frob}_{F/K} = t$ (an element of order 2). Then

- For $\mathbb{I}$ we have $P(\mathbb{I},T) = \det(1-\Phi_{F/K}T|_{\mathbb{I}^{I_{F/K}}}) = \det(1-T) = 1-T$ (Since $\mathbb{I}^{C_3} = \mathbb{I}$)
- For ϵ (the sign representation) $P(\epsilon,T) = \det(1-\Phi_{F/J}T|_{\epsilon^{I_{F/K}}}) = \det(1-(-1)T|_{\epsilon}) = 1+T$ (since $\epsilon^{I_{F/K}} = \epsilon$, so $\epsilon(t) = -1$)
- For ρ the 2-dimensional representation: $P(\rho,T) = \det(1-\Phi_{F/K}T|_{\rho^{I_{F/K}}}) = 1$ (since $\rho^{C_3} = 0$, we have no invariant subspace)

Definition 3.2. The *Artin L-function* of an Artin representation over a number field K is

$$L(\rho,s) = \prod_{\mathcal{P}\subset\mathcal{O}_K} \frac{1}{P_{\mathcal{P}}(\rho,\mathrm{Nm}(\mathcal{P})^{-s})}$$

where $P_{\mathcal{P}}(\rho,T)$ is the local polynomial of ρ restricted to $\mathrm{Gal}(\overline{K}_{\mathcal{P}}/K_{\mathcal{P}})$.

The Euler product converges to an analytic function if $\mathrm{re}(s) > 1$

Example.

- Let K be a number field, $\rho = \mathbb{I}$ then $P_{\mathcal{P}}(\mathbb{I},T) = 1-T$ for all $\mathcal{P}$, so $L(\mathbb{I},s) = \prod_{\mathcal{P}} \frac{1}{1-\mathrm{Nm}(\mathcal{P})^{-s}} = \zeta_K(s)$ the Dedekind ζ-function of K
- $K = \mathbb{Q}$, ρ the order 2 character of $\mathrm{Gal}(\mathbb{Q}(S_3)/\mathbb{Q}) \cong C_2$. Need $I_{F/K}$ and $p(t)$
  - $p = 3$, then $\mathbb{Q}_3(S_3)/\mathbb{Q}_3$ is totally ramified, hence $I_{F/K} = C_2$ and $\rho^{I_{F/K}} = 0$. So $P_3(\rho,T) = 1$
  - $p \equiv 1 \mod 3$ then $\mathbb{Q}_p(S_3) = \mathbb{Q}_p$, $I_{f/K} = \{e\}$ and $P_p(\rho,T) = 1-T$
  - $p \equiv 2 \mod 3$ then $\mathbb{Q}_p(S_3)/\mathbb{Q}_p$ is unramified so $I_{F/K} = \{e\}$ and $\rho(t) = -1$. So $P_p(\rho,T) = 1+T$.

  Putting it together we get

  $$\begin{aligned} L(\rho,s) &= \prod_{p\neq 3} \frac{1}{1-\left(\frac{p}{3}\right)p^{-s}} \\ &= \sum_{n=1}^{\infty} \left(\frac{n}{3}\right) n^{-s} \end{aligned}$$

  the L function of the non-trivial Dirichlet character $\mathbb{Z}/3\mathbb{Z} \to \mathbb{C}^*$

Fact. *The Artin L-function of 1-dimensional Artin representation over $\mathbb{Q}$ correspond to Dirichlet L-functions of primitive characters.*

Basic Properties

1. For ρ_1 and ρ_2 Artin representations over a local field K, $P(\rho_1 \oplus \rho_2, T) = P(\rho_1,T)P(\rho_2,T)$
2. When F/K is a finite extension, ρ an Artin represetnations over F then $P_F(\rho,T^f) = P_K(\mathrm{Ind}_\rho,T)$ where f is the residue degree of F/K.
3. When K is a number field, $L(\rho_1 \oplus \rho_2, s) = L(\rho_1,s)L(\rho_2,s)$. If F/K is finite, ρ Artin representation over F, then $L(\rho,s) = L(\mathrm{Ind}_\rho,s)$ (where the first one is an Artin L-function over F and the second over K)

Conjecture (Artin). *Let $\rho \neq \mathbb{I}$ be irreducible Artin representation over a number field, then its L-function is analytic*

3.1.2 Conductor

Definition 3.3. *The conductor exponent* of an Artin representation over a local field K is $n_\rho = n_{\rho,\text{tame}} + n_{\rho,\text{wilde}}$, where $n_{\rho,\text{tame}} = \dim\rho - \dim\rho^{I_{F/K}}$ and $n_{\rho,\text{wild}} = \sum_{k=1}^{\infty}\frac{1}{[I:I_k]}\dim\rho/\rho^{I_k}$ where ρfactors through F/K and $I_{F/K} = I = I_0$, $I_k = \left\{\sigma \in \mathrm{GL}(F/K) | \sigma(\alpha)\alpha \mod \pi^{k+1} \forall \alpha \in \mathcal{O}_F\right\}$ are the higher ramification group (with lower numbering)

So $I_1 = \mathrm{Syl}_\rho I$ =wild inertia and I/I_1 =tame inertia

We say ρ is unramified (respectively tame) if $n_\rho = 0$ (respectively $n_{\rho,\text{wilde}} = 0$) if and only if I acts trivial on ρ (respectively I_1)

Definition 3.4. The *conductor of* ρ is the ideal $N_\rho = (\pi^{n_\rho})$

Theorem 3.5 (Artin)**.** $n_p \in \mathbb{Z}$

Remark. $n_{\rho_1\oplus\rho_2} = n_{\rho_1} + n_{\rho_2}$. Hence $N_{\rho_1\oplus\rho_2} = N_{\rho_1}N_{\rho_2}$

Theorem 3.6 (Swan's character)**.** *Let ρ be an Artin representation over a local field K which factors through* $\mathrm{Gal}(F/K)$*. Then* $n_{\rho,\text{wild}} = \langle \mathrm{Trace}\rho, b\rangle$ *where*

$$b(g) = \begin{cases} 1 - \nu_F(g(\pi_F) - \pi_F) & \text{for } g \in I_{F/K} \setminus \{e\} \\ -\sum_{h\neq e} b(h) & \text{for } g \in e \end{cases}$$

Theorem 3.7 (Conductor-Discriminant formula)**.**

$$\begin{tikzcd} F \arrow[dd, dash, "G"'] \arrow[dr, dash, "H"] & \\ & L \arrow[dl, dash] \\ K & \end{tikzcd}$$

Let F/K be Galois, ρ be a representation of $H =$ $\mathrm{Gal}(F/L)$. Then $n_{\mathrm{Ind}_H^G\rho} = (\dim\rho)\cdot\nu_K(\Delta_{L/K}) + \mathcal{P}_{L/K}n_\rho$ *equivalently* $N_{\mathrm{Ind}\rho} = \Delta_{L/K}^{\dim\rho}\mathrm{Nm}_{L/K}(N_\rho)$

Example.

$$\begin{tikzcd} & F = \mathbb{Q}_5(\zeta_3, \sqrt[3]{5}) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}_5(\zeta_3) \arrow[dr, dash] & & \mathbb{Q}_5(\sqrt[3]{5}) \arrow[dl, dash] \\ & K = \mathbb{Q}_5 & \end{tikzcd}$$

Then $I_{F/K} = C_3$, $I_1 = \{1\}$:

- $n_{\mathbb{I}} = 0$ as $n_{\rho,\text{tame}} = 1 - 1$ and $n_{\rho,\text{wild}} = 0$
- $n_\epsilon = 0$
- $n_\rho = 2 = 2 - 0$

By the Conductor-discriminant formula:

$\Delta_{L/K} = N_{\mathrm{Ind}_{C_2}^{S_3}\mathbb{I}} = M_\rho N_{\mathbb{I}} = 5^2$ (up to units)

$\Delta_{F/K} = N_{\mathrm{Ind}_{\{1\}}^{S_3}\mathbb{I}} = N_{\rho\oplus\rho\oplus\epsilon\oplus\mathbb{I}} = 5^4$ (up to units)

Definition 3.8. The *conductor* of an Artin representation over a number field K

$$N_\rho = \prod_{\mathcal{P}} \mathcal{P}^{n_{\mathcal{P}}(\rho)}$$

where $n_{\mathcal{P}}(\rho)$ is the conductor exponent of ρ restricted to $\mathrm{Gal}(\overline{K}_{\mathcal{P}}/K_{\mathcal{P}})$.

Example of Application:
Suppose $F/\mathbb{Q}$ is Galois, $\mathrm{Gal}(F/\mathbb{Q}) = D_{10}$. Let K and L be intermediate with $[K:\mathbb{Q}] = 2$ and $[L:\mathbb{Q}] = 5$. Then $S_F(s)S_{\mathbb{Q}}(s)^2 = S_L(s)^2 S_K(s)$

3.1.3 Functional equations

Theorem 3.9. *The Artin L-function of ρ satisfies the functional equation $\Lambda(\rho, s) = \omega A^{1/2-s}\Lambda(\widehat{\rho}, 1-s)$ where*

- $$\Lambda(s) = L(\rho, s) \prod_{\nu \text{real}} \Gamma_{\mathbb{R}}(s)^{d_+(\rho)}\Gamma_{\mathbb{R}}(s+1)^{d_-(\rho)} \prod_{\nu \text{complex}} \Gamma_{\mathbb{C}}(s)$$
- $d_\pm(\rho)$ *is the dimension of the $\pm$ eigenspace of the image of complex conjugation at ν, $\omega \in \mathbb{C}^*$,*
- $|\omega| = 1$ *global root number*
- $A = \mathrm{Nm}(N_\rho)\sqrt{|\Lambda_K|^{\dim_\rho}}$
- $\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2)$
- $\Gamma_{\mathbb{C}}(s) = (2\pi)^{-s}\Gamma(s)$
- $\Gamma(s) = \begin{cases} (s)! & s \in \mathbb{N} \\ \int_0^\infty x^{s-1}e^{-x}dx \end{cases}$

3.2 l-adic Representations

3.2.1 Local Polynomials

Definition 3.10. Let $K/\mathbb{Q}_p$ be finite, $\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_d(\mathcal{F})$ where $\mathcal{F}/\mathbb{Q}_l$ with $l \neq p$, be a continuous l-adic representation. The *local polynomial of* ρ is

$$P(\rho, T) = \det(1 - \Phi_{\overline{K}/K} T|_{\rho^{I_{\overline{K}/K}}})$$

3.2.2 Conductor

Definition 3.11. The *conductor exponent* is $n_\rho = n_{\rho,\text{tame}} + n_{\rho,\text{wilde}}$ where $n_{\rho,\text{tame}} = \dim_{\rho/\rho^{I_{\overline{K}/K}}}$, $n_{\rho,\text{wild}} = \sum_{k\geq 1} \frac{1}{[I_{F/K}, I_{F/K,k}]} \dim \rho/\rho^{I_{F/K,k}}$ where F/K is a finite extension chosen so that the action of wild inertia factors through. We can take $F = F_1$, then the image of $\mathrm{Gal}(\overline{K}/F)$ lies in $\begin{pmatrix} 1 + l\mathcal{O}_{\mathcal{F}} & l\mathcal{O}_{\mathcal{F}} \\ l\mathcal{O}_{\mathcal{F}} & 1 + l\mathcal{O}_{\mathcal{F}} \end{pmatrix}$ and $\mathrm{im}(I_1) = \mathrm{id}$ since it is a (pro) p-group send into a (pro) l-group.

Definition 3.12. The *conductor of* ρ is $N_\rho = (\pi_K)^{n_\rho}$.

4 Decomposition Theorems (Pedro)

Notation.

- Let p and l be distinct primes.
- K a p-adic field
- $\mathcal{F}$ an l-adic field
- I_L the (absolute) inertia group of a field L
- I_L^w the (absolute) wild inertia group of a field L
- Φ_L a geometric Frobenius element

4.1 Finite Image of Inertia

Theorem 4.1. *Let $\tau : G_K \to \mathrm{GL}_d(\mathcal{F})$ be an l-adic Galois representation such that $\tau(I_K)$ is finite and Φ_K acts semisimple, for any choice of Φ_K. Then we can write $\tau = \oplus_i(\rho_i \otimes \chi_i)$ (after possible a finite extension of $\mathcal{F}$) where ρ_i is an l-adic Galois representation which factors through a finite quotient and χ_i is a one dimensional unramified Galois representation.*

To show this thing, we use the following:

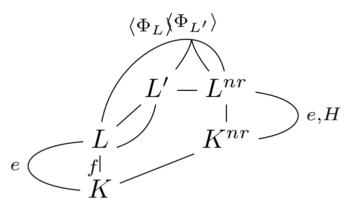
Proposition 4.2. *Let k be a field of characteristic $c \geq 0$, V a finite dimensional vector space, G a group and $\rho : G \to \mathrm{GL}(V)$ a representation of G. Assume that there exists a finite index subgroup $H \leq G$ such that $\rho|_H$ is semisimple and $c \nmid [G : H]$. Then ρ is semisimple.*

Proof. Choose a subrepresentation W of ρ and let W' be $k[H]$-module such that $V = W \oplus W'$ (As $k[H]$ modules). Consider

$$\begin{tikzcd} 0 \arrow[r] & W \arrow[r] & V \arrow[r, "\pi"] & V/W \arrow[r] \arrow[l, bend left, "f"] & 0 \end{tikzcd}$$

For $u \in V/W$, take $h(u) = \frac{1}{[G:H]} \sum_{g \in G/H} g f(g^{-1}u)$. ☐

Proof of Theorem 4.1. By the previous proposition, we can assume that τ is irreducible. We can take a totally ramified extension L/K such that $\tau(I_L) = 1$



Let L' be the Galois closure of L. Note that $\mathrm{Gal}(L^{\mathrm{nr}}/K)$ is generated by H and Φ_L. We have $\Phi_{L'} = \Phi_L^f$, so $\Phi_{L'}$ doesn't commute with Φ_L. Pick $\sigma \in H$, we then have $\sigma^{-1}\Phi_{L'}^{-1}\sigma\Phi_{L'} \in H$, but $\sigma^{-1}\Phi_{L'}^{-1}\sigma \in \langle \Phi_{L'} \rangle$ so $\sigma^{-1}\Phi_{L'}^{-1}\sigma\Phi_{L'} \in \langle \Phi_{L'} \rangle$ .Hence $[\sigma, \Phi_{L'}] \in H \cap \langle \Phi_{L'} \rangle$. So we have that $[\sigma, \Phi_{L'}] = 1$. By Schur's lemma we have that $\tau(\Phi_{L'}) = \lambda \, \mathrm{id}_d$. Define χ to be

- $\chi(\mathbb{I}_K) = 1$
- $\chi(\Phi_K) = \sqrt[f]{\lambda}$

Set $\rho := \tau \otimes \chi^{-1}$. So $\rho(\Phi_{L'}) = \rho(\Phi_K^f \sigma) = 1$. ☐

4.2 Infinite image of inertia

Definition 4.3.

1. Let $t_l : I_K \to \mathbb{Z}_l$ be the character defined in the following way: $\sigma \mapsto t_l(\sigma)$ where $\sigma(\sqrt[l^n]{\pi_K}) = \zeta_{l^n}^{t_l(\sigma)} \sqrt[l^n]{\pi_K}$. (Where ζ_{l^n} is a primitive l^nth root of unity) This is called the *l-adic tame character*

2. For any $n \geq 0$,
$$\mathrm{sp}(n)(\sigma) = \begin{pmatrix} 1 & t & t^2/2! & \dots & t^n/n! \\ 0 & 1 & \ddots & & \\ \vdots & & \ddots & \ddots & \\ \vdots & & & \ddots & t \\ 0 & & & & 1 \end{pmatrix}$$
where $t = t_l(\sigma)$, $\sigma \in I_k$. And we define
$$\mathrm{sp}(n)\left(\Phi_K\right) = \begin{pmatrix} 1 & & & 0 \\ & q & & \\ & & \ddots & \\ 0 & & & q^m \end{pmatrix}$$
where $q = \#\mathbb{F}_K$

Theorem 4.4. *Let $\tau : G_K \to \mathrm{GL}_d(\mathcal{F})$ be an l-adic Galois representation such hat Φ_K acts semisimply on $\tau^{I'}$, for every finite index subgroup $I' \subseteq I$, and for every choice of Φ_K. Then*
$$\tau = \oplus_i \left(\rho_i \otimes \mathrm{sp}(n_i)\right)$$
(after a finite extension) where ρ_i is an l-adic Galois representation such that $\rho_i(I_K)$ is finite and with Frobenius acting semisimply.

Remark. By continuity, we can find a finite Galois extension L/K such that $\tau(I_L) = \tau(H)$, where $H = \mathrm{Gal}(L_l/L^{\mathrm{rn}}) \cong \mathbb{Z}_p$, where $L_l = \cup_{n-1}^{\infty} L^{\mathrm{nr}}\left(\sqrt[l^n]{\pi_L}\right)$.

Note that $\sigma \in H$ and Φ_K is a Frobenius element, then $\sigma\Phi_L = \Phi_L\sigma^q$ where $q = \#\mathbb{F}_L$.

Proof.

Case 1. $d = 1$

Let $\sigma \in H$. Then $\tau(\sigma)^q = \tau(\sigma^q) = \tau(\Phi_L^{-1}\sigma\Phi_L) = \tau(\Phi_L^{-1})\tau(\sigma)\tau(\Phi_L) = \tau(\sigma)$. Hence $\tau(\sigma)^{q-1} = 1$, so $\tau(\sigma) \in \mu_{q-1}$.

Case 2. $d = 2$

Pick $\sigma \in H$ which is a topological generator of H. By extending $\mathcal{F}$ if necessary, we can assume that $\tau(\sigma) = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. We have three cases:

Case i. $\tau(\sigma) = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$. This is the same as the case $d = 1$.

Case ii. $\tau(\sigma) = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$, $\lambda \neq \mu$. Let V_i be the subrepresentation spanned by the ith vector. We use the above note. Let $v_1 \in V_1$, then $\sigma\Phi_K(v_1) = \Phi_K\sigma^q(v_1)$, hence $\Phi_K V_1$ is a subrepresentation of $\tau|_H$. Similarly, we can conclude that $\Phi_K V_2$ is a subrepresentation of $\tau|_H$. If $\Phi_K V_1 = V_2$, then $\mu(\Phi_K v_1) = \sigma(\Phi_K v_i) = \Phi_K(\sigma^q v_1) = \lambda^q \Phi_K v_1$. Similarly $\lambda(\Phi_K v_2) = \mu^q \Phi_K v_2$. Hence λ, μ are roots of unity so the image of inertia is finite.

Case iii. $\tau(\sigma) = \begin{pmatrix} \lambda & * \\ 0 & \lambda \end{pmatrix}$ and $* \neq 0$. $\Phi_K V_1$ is a subrepresentation of $\tau|_H$ implies that $\Phi_K V_1 = V_1$. We can write $\tau' = \tau \otimes \chi^{-1}$, $\tau'(\sigma) = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ with $\sigma \in H$.

Claim. For any $\mathrm{Gal}(L_l/L^{\mathrm{nr}})$ and $\theta \in \mathrm{Gal}(L_l/K^{\mathrm{nr}})$ we have $\sigma\theta = \theta\sigma$.

□

5 l-adic representations of Elliptic curves (Heline)

5.1 Definition

Notation.

- Let $K = \mathbb{Q}$ or $\mathbb{Q}_p$
- $G_K := \mathrm{Gal}(\overline{K}/K)$
- E/K an elliptic curve
- $2 \leq m \in \mathbb{Z}$
- $E[m] = \{P \in (\overline{K}) : mP = 0\} \cong (\mathbb{Z}/m\mathbb{Z})^2$
- For $\sigma \in G_K$ and $P \in E[m]$, we have $m\sigma(P) = \sigma(mP) = 0$, hence G_K acts on $E[m]$.
- Pick a basis P_1, Q_1 for $E[m]$, then for $\sigma \in G_K$ we have $\sigma(P_1) = aP_1 + cQ_1$ and $\sigma(Q_1) = bP_1 + dQ_1$ for some $a, b, c, d \in \mathbb{Z}$. Hence we have $G_K \to \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ defined by $\sigma \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. If $\gcd(m, n') = 1$ then $E[mn'] \cong E[m] \times E[n']$.
- We are going to be taking $m = l^n$ with l a prime distinct from p.

Note. We have natural maps $E[l^n] \xrightarrow{[l]} E[l^{n-1}] \to \cdots \to E[l] \xrightarrow{[l]} 0$

Definition 5.1. For E an elliptic curve and l a prime, we define the *l-adic Tate module of E* to be $T_l E := \varprojlim E[l^n] \cong (\mathbb{Z}_l)^2$.

We also define $V_l E := T_l E \otimes_{\mathbb{Z}_l} \mathbb{Q}_l \cong (\mathbb{Q}_l)^2$.

Note that G_K acts on both $T_l E$ and $V_l E$.

Definition 5.2. The *mod l representation* of E is $\overline{\rho}_{E,l} : G_K \to \mathrm{Aut}(E[l]) \cong \mathrm{GL}_2(\mathbb{Z}/l\mathbb{Z})$.

The *l-adic representation* is $\rho_{E,l} : G_K \to \mathrm{Aut}(T_l(E)) \cong \mathrm{GL}_2(\mathbb{Z}_l)$ or depending of reference $\rho_{E,l} : G_K \to \mathrm{Aut}(V_l E) \cong \mathrm{GL}_2(\mathbb{Q}_l) \hookrightarrow \mathrm{GL}_2(\mathbb{C})$

Recall the cyclotomic character $\epsilon_l : G_k \to \mathbb{Z}_l^*$ defined by, for $\sigma \in G_K : \sigma(\zeta_l) = \zeta_l^{\epsilon_l(\sigma)}$.

We have the Weil pairing: $e[\,,\,] : E[m] \times E[m] \to \mu_m$ (Where μ_m is the m-th root of unity), which is bilinear, alternating, Galois invariant, non-degenerate and "computable".

Given $\sigma \in G_K$ with $\rho_{E,l}(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, and $P, Q \in E[m]$ be a basis, we have that

$$\begin{aligned} \sigma e[P,Q] &= e[\sigma P, \sigma Q] \\ &= e[aP + cQ, bP + dQ] \\ &= e[P,P]^{ab} e[P,Q]^{ad} e[Q,P]^{cb} e[Q,Q]^{cd} \\ & \quad\; e[P,Q]^{ad-bc} \end{aligned}$$

But from $\sigma(\zeta) = \zeta^{\epsilon_l(\sigma)}$, we see that $ad - bc = \epsilon_l(\sigma)$. Hence

$$\epsilon_l(\sigma) = \det \rho(\sigma) \, \forall \sigma \in G_K$$

5.2 Local invariants

Let $G_{\mathbb{F}_p} = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ and consider the short exact sequence $1 \to I \to G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p} \to 1$ where $I = \{\sigma \in G_{\mathbb{Q}_p} : \overline{\sigma} = 1\}$. Let Frob_p be any elements of $G_{\mathbb{Q}_p}$ that reduces to $x \mapsto x^p$. Recall that a $G_{\mathbb{Q}_p}$ module M is unramified if I acts trivially on M.

Example. Let $K = \mathbb{Q}_5$ (note $\sqrt{-1} \in \mathbb{Q}_5$ and $\mathbb{Q}_5(\zeta_8) = \mathbb{Q}_5(\zeta_3)$, unramified), $E_1 : y^2 = x^3 - 1$ and $E_2 : y^2 = (x-1)(x^2-5)$.

Over $\mathbb{F}_5$ we get $\widetilde{E}_1 : y^2 = x^3 - 1$ (curve of good reduction) and $\widetilde{E}_2 : y^2 = x^3 - x^2$ (multiplicative reduction, and note that it is equivalent to $(y + \sqrt{-1}x)(y - \sqrt{-1}x) = x^3$)

We consider $E[l^n]$ with $l = 2$. So $E_1[2] = \{0, (1,0), (\zeta_3, 0), (\zeta_3^2, 0)\}$ so $\mathbb{Q}_5(E_1[2])$ is unramified

$E_2[2] = \{0, (1,0), (\sqrt{5}, 0), (-\sqrt{5}, 0)\}$ so in $\mathbb{Q}_5(\sqrt{5})$ ramified.

$$\begin{array}{ccc} \mathbb{Q}_5(E[4]) & \mathbb{Q}_5(\zeta_{16}) & \mathbb{Q}_5(\sqrt[4]{5}) \\ | & | & | \\ \mathbb{Q}_5(E[2]) & \mathbb{Q}_5(\zeta_8) & \mathbb{Q}_5(\sqrt{5}) \\ | & | & | \\ \mathbb{Q}_5 & \mathbb{Q}_5 & \mathbb{Q}_5 \end{array}$$

Recall the definition of the local polynomial $P_p(\rho_{E,l}, T) = \det(1 - \mathrm{Frob}_p^{-1} T | (V_l E^*)^I)$

Good Reduction:

Theorem 5.3 (Neron-Ogg-Shaferevich). *If $E/\mathbb{Q}_p$ is an elliptic curve, $l \neq p$. Then E has good reduction at p if and only if $E[l^n]$ is unramified for all n (if and only if I acts trivially on $E[l^n]$ for all n)*

Proof. Silverman pg 201 □

From this we know that $I \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Furthermore we want to know what Frob_p is, but $\epsilon_\rho(\mathrm{Frob}_p) = p = \det \rho(\mathrm{Frob}_p)$. Hence Frob_p is a 2×2 matrix with determinant p.

Fact.

- $Q \in E(\mathbb{F}_p) \iff \mathrm{Frob}_p(Q) = Q$, $\#E(\mathbb{F}_p) = \#\ker(1 - \mathrm{Frob}_p)$. *But* $1 - \mathrm{Frob}_p$ *is separable implies that* $\ker(1 - \mathrm{Frob}_p) = \deg(1 - \mathrm{Frob}_p)$
- *If* $\psi \in \mathrm{End}(E)$, *then* $\mathrm{tr}(\psi) = 1 + \deg \psi - \deg(1 - \psi)$. *Hence* $\mathrm{tr}(\mathrm{Frob}_p) = 1 + p - \#E(\mathbb{F}_p) =: a_p$. *So the characteristic polynomial of* Frob_p *is* $T^2 - aT + p$

Now $(V_l E^*)^I = V_l E^*$, so $P_p(T) = 1 - aT + pT^2$.

Example. $E_! : y^2 = x^3 - 1$, $E_1(\mathbb{F}_5) = \{0, (\pm 2, 0), (1, 0), (3, \pm 1)\}$, hence $\#E_1(\mathbb{F}_5) = 6$, we have $P_5 = 1 + 5T^2$. So in some basis $I \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\mathrm{Frob}_p \to \begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix}$.

Multiplicative Reduction:

Suppose the reduction is split multiplicative. Recall $E/\mathbb{C} \cong \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z}) \overset{\exp}{\to} \mathbb{C}^*/q^{\mathbb{Z}}$ (where $q = e^{2\pi i \tau}$) are isomorphic as complex Lie groups.

Theorem 5.4 (Tate). *Let $E/\mathbb{Q}_p$ has split multiplicative reduction, then there exists unique $0 \neq q \in p\mathbb{Z}_p$ such that $E \cong E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)$ where $a_4(q)$ and $q_6(q)$ are power series in $\mathbb{Z}[[q]]$ which converges. Furthermore, $j(E_q) = 1/q + 744 + 196884q + \dots$ and $\Delta(E_q) = q \prod (1 - q^n)^{24}$. Hence $E(\overline{\mathbb{Q}}_p) \cong E_q(\overline{\mathbb{Q}}_p) \cong \overline{\mathbb{Q}}_p^*/q^{\mathbb{Z}}$ (as $G_{\mathbb{Q}_p}$-modules)*

Corollary 5.5. $E[l] = \langle \zeta_l, \sqrt[l]{q} \rangle$ *and* $E[l^n] = \langle \zeta_{l^n}, \sqrt[l^n]{q} \rangle$

So $\mathbb{Q}(E[l^n])$ has growing ramification for $n \geq 1$ (it can be the same at each step, but it will slowly grow)

Example. $E_2/\mathbb{Q}_5$, $y^2 = (x-1)(x^2-5)$. We get $j(E_2) = 2^{14}/5$ and $\Delta = 2^{10}\cdot 5$, hence q is a 5-unit. So $\mathbb{Q}_5(E[2^n]) \cong \mathbb{Q}_5\left(\sqrt[2^n]{5}, \zeta_{2^n}\right)$ for all $n \geq 1$.

Action of I on $E[l^n]$, so consider $\sigma(\zeta_{l^n}) = \zeta_{l^n}$ and $\sigma(\sqrt[l^n]{q}) = \zeta_{l^n}^t \sqrt[l^n]{q}$, where $t = t_l(\sigma) = l$-adic tame character. Hence $I \mapsto \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$. Now we look at the action of Frobenius. We saw that $\mathrm{Frob}_p(\zeta_{l^n}) = \zeta_{l^n}^p$, and we know that the determinant is p, so $\mathrm{Frob}_p \mapsto \begin{pmatrix} p & * \\ 0 & 1 \end{pmatrix}$. To determine $*$, we can use the previous section: $\rho_E = \rho \otimes \mathrm{sp}(1)$, but ρ is trivial, so $*$ is trivial and $\mathrm{Frob}_p \to \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$.

Now we calculate $(V_l E)^*$ and conclude that $P_p(T) = 1 - T$.

In the non-split case, we find that $P_p(T) = 1 + T$. Putting all this together we get

$$P_p(T) = \begin{cases} 1 - aT + pT^2 & \text{good reduction} \\ 1 - T & \text{split mult} \\ 1 + T & \text{non} - \text{split mult} \\ 1 & \text{additive} \end{cases}$$

For an elliptic curve E over a number field K we can define

$$L(\rho_E, s) = \prod_{\mathcal{P} \in \mathcal{O}_K} \frac{1}{P_{\mathcal{P}}(\rho_E, \mathrm{Norm}(\mathcal{P})^{-s})}$$

6 Examples of l-adic representations for elliptic curves (Alejandro)

In this section $\rho_{E,l} = \rho_l = \rho$.

Notation.

- l is a prime
- $V = \mathbb{Q}_l^2$
- L, L' are lattices (i.e., rank 2 $\mathbb{Z}_l$-submodules of V)
- Λ, Λ' are classes of lattices L, L' with respect to homothety
- $\rho : G_k \to \mathrm{GL}(V) \cong \mathrm{GL}_2(\mathbb{Q}_l)$

For a given l-adic Galois representation ρ, we are going to show that there exists a (non-canonical) lattice

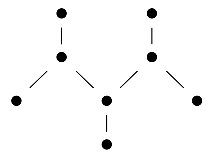
$$\begin{tikzcd} G_K \arrow[r] \arrow[dr] & \mathrm{GL}_2(\mathbb{Q}_l) \\ & \mathrm{GL}_2(\mathbb{Z}_l) \arrow[u, hook] \end{tikzcd}$$

we are going to see proposition and examples. We will see Dictson's theorem and we will show that over $\mathbb{Q}$ for $l \geq 5$, if ρ is surjective $\mod l$ then ρ is surjective.

Definition 6.1. The *Bichat-Tits tree* is the graph T with:

1. Vertices, $\Lambda := [l]$, where Λ is the equivalence class of some lattice L of $\mathbb{Q}_l^2$
2. There is an edge between two vertices v_1, v_2 of T if and only if there exists L and L' such that $v_1 = \Lambda$ and $v_2 = \Lambda'$ and $L \supset L' \supset lL$

Example. There are eight 2-isogony classes for the elliptic curves of conductor



6.1 Stable lattices and Galois representations

$\rho : G_K \to \mathrm{GL}_2(\mathbb{Q}_l)$

Definition 6.2. A lattice L is *G_K-stable with respect to ρ* if $\rho(G_K)(L) \subseteq L$. This property only depends on the homothety class Λ of L.

Proposition 6.3. *Every representation ρ as at least one stable lattice.*

Sketch of proof. Let L be any lattice of $\mathbb{Q}_l^2$ and H be the subgroup of G_K such that $\rho(\sigma)(L) \subseteq (L)$ for $\sigma \in H$. This is an open subgroup since ??? finite index in G_K because G_K is compact. Hence the lattice generated by the sum is stable under G_K. $\square$

Definition 6.4. Two integral representations $\rho_j : G_K \to \mathrm{GL}_2(\mathbb{Z}_l)$ are *isogeneous* if they are conjugate as representations in $\mathrm{GL}_2(\mathbb{Q}_l)$, i.e., there exists $U \in \mathrm{GL}_2(\mathbb{Q}_l)$ such that $\rho_2(\sigma) = U\rho_1(\sigma)U^{-1}$ for all $\sigma \in G_K$.

Definition 6.5. Let $\rho : G_K \to \mathrm{GL}_2(\mathbb{Z}_l)$ be an integral representation. The *Residual representation* associated to ρ is the map $\overline{\rho} : G_K \to \mathrm{GL}_2(\mathbb{F}_l)$ obtained by composing ρ with the reduction map.

$$\begin{tikzcd} G_K \arrow[r, "\rho"] \arrow[dr, "\overline{\rho}"'] & \mathrm{GL}_2(\mathbb{Z}_l) \arrow[d, "\bmod l"] \\ & \mathrm{GL}_2(\mathbb{F}_l) \end{tikzcd}$$

Example. Let E_1, E_2 be two elliptic curve over K. Suppose there exists a K 2-rational isogeny $E_1 \to E_2$. For each curve we have $\rho_{E_1,2}, \rho_{E_2,2}$. The residual have image which is of order either 1 (if $E_j(K)[2]$ has order 4) or 2 (if $E_j(K)[2]$ has order 2).

Proposition 6.6. *The number of stable lattice (up to homothety) is finite if and only if ρ is irreducible.*

Proposition 6.7. *Let ρ be an integral representation. The number of stable lattices (up to homothety) if 1 if and only if the residual representation $\overline{\rho}$ is irreducible.*

6.2 Dickson's Theorem

Theorem 6.8. *Let $l \geq 3$ be a prime and H a finite subgroup of $\mathrm{PGL}_2(\overline{\mathbb{F}}_l)$. Then a conjugate of H is one of the following groups:*

1. *A finite subgroup of the upper triangular matrices (Borel subgroup)*
2. $\mathrm{PSL}_2(\mathbb{F}_{l^r})$ *or* $\mathrm{PGL}_2(\mathbb{F}_{l^r})$ *for some* $r \in \mathbb{Z}_{>0}$
3. *A dihedral group D_{2n} with $n \in \mathbb{Z}_{>1}$ and $(l, n) = 1$*
4. *A subgroup isomorphic to either A_4, S_4 or A_5.*

6.3 Surjectivity $l \geq 5$ and non-surjectivity for $l = 2$ or 3.

Here we are only talking about representations attached to elliptic curves.

- Tim and Vlad published a paper showing that ρ_2 is surjective mod 2 but not mod 4; and mod 4 but not mod 8
- Elkies showed that for $l = 3$, ρ_3 is surjective mod 3 but not mod 9.

Theorem 6.9. *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{Q}$ with $\Delta = -16(4a^3 + 27b^2)$ and j invariant $-1728\frac{4a^3}{\Delta}$. Then*

1. *$\overline{\rho}_2$ is surjective if and only if $x^3 + ax + b$ irreducible over $\mathbb{Q}$ and $\Delta \notin (\mathbb{Q}^*)^2$*
2. *$\overline{\rho}_4$ is surjective if and only if $\overline{\rho}_2$ is surjective, $\Delta \notin -1 \cdot (\mathbb{Q}^*)^2$ and $j \neq 4t^3(t+8)$ for any $t \in \mathbb{Q}$*
3. *$\overline{\rho}_8$ is surjective if and only if $\overline{\rho}_4$ is surjective and $\Delta \notin -2 \cdot (\mathbb{Q}^*)^2$.*

7 Galois Representations of Modular Curves (Chris Williams)

7.1 Modular Curves

Let $\Gamma = \Gamma_0(N) \leq \mathrm{SL}_2(\mathbb{Z})$. Define the (compactified) modular curve to be $X(\Gamma) = X_0(N) := \Gamma\backslash\mathcal{H}^*$ where $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$

Fact.

- *$X_0(N)$ is a compact Hausdorff Riemann surface*
- *$g(X_0(N)) = \dim_{\mathbb{C}} S_2(\Gamma_0(N))$*
- *$X_0(N)$ has a model as an algebraic curve over $\mathbb{Q}$. (In fact it has a model as a scheme over $\mathbb{Z}\left[\frac{1}{N}\right]$)*

Hecke operators have a geometric interpretation. If we define $\gamma_p = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$, $\Gamma' = \Gamma \cap \gamma_p^{-1}\Gamma\gamma_p$ and $\Gamma'' = \gamma_p\Gamma\gamma_p^{-1} \cap \Gamma$ we then get

$$\begin{tikzcd} \Gamma' \arrow[r, "x \mapsto \gamma_p x \gamma_p^{-1}"] \arrow[d, hook] & \Gamma'' \arrow[d, hook] \\ \Gamma & \Gamma \end{tikzcd}$$

This descent to

$$\begin{tikzcd} X(\Gamma') \arrow[r, "\alpha"] \arrow[d, "\pi_1"'] & X(\Gamma'') \arrow[d, "\pi_2"'] \\ X(\Gamma) & X(\Gamma) \end{tikzcd}$$

To $x \in X(\Gamma) = X_0(N)$ we get $T_p(x) = \pi_2 \circ \alpha \circ \pi_1^{-1}(x) \in \mathrm{Div}(X(\Gamma))$. This extends linearly to $T_p : \mathrm{Div}(X(\Gamma)) \to \mathrm{Div}(X(\Gamma))$.

7.2 Picard Groups

Definition 7.1. Let X be an algebraic curve over a field K. The *Picard group* of X/K is $\mathrm{Pic}(X)_K = \mathrm{Div}^0(X/K)/K(X)^*$.

If ϕ is a "nice" map $X \to Y$, then we get maps on the Picard group as follows:

- *Pushforward*: $\phi_* : \mathrm{Pic}(X) \to \mathrm{Pic}(Y)$ defined as $\sum_x n_x[x] \mapsto \sum_x n_x[\phi(x)]$
- *Pullback*: $\phi^* : \mathrm{Pic}(Y) \to \mathrm{Pic}(X)$ defined as $\sum_y n_y[y] \mapsto \sum_y n_y \sum_{x\in\phi^{-1}(y)} e_x[x]$

Fact. *As endomorphism of* $\mathrm{Pic}(Y)$ $\deg(\phi) = \phi_* \circ \phi^*$.

Remark. The action of T_p on $\mathrm{Div}(X_0(N))$ descend to $\mathrm{Pic}(X_0(N))$.
$\mathrm{Pic}(X_0(N))$ "is" an abelian variety of dimension $g = \mathrm{genus}(X_0(X)) = \dim_{\mathbb{C}} S_2(\Gamma_0(N))$.

7.3 Eichler-Schimura

Recall that if E is an elliptic curve over $\mathbb{Q}$, $p \nmid lN_p$ a prime, $\mathcal{P}|p$ a prime of $\overline{\mathbb{Z}}$. Then $\rho_{E,l}(\mathrm{Frob}_{\mathcal{P}})$ has characteristic polynomial $x^2 - q_p(E)X + p$. $\left|\widetilde{E}(\mathbb{F}_p)\right| = |\ker(\sigma_p - 1)| = \deg(\sigma_p - 1) = (\sigma_p - 1)_* \circ (\sigma_p - 1)^*$ as endomorphism of $\mathrm{Pic}(\overline{E})$, hence $\left|\widetilde{E}(\mathbb{F}_p)\right| = \sigma_{p*}\sigma_p^* - (\sigma_{p*} + \sigma_p^*) + 1 = p + 1 - (\sigma_{p*} + \sigma_p^*)$. In particular, as endomorphism of $\mathrm{Pic}(\widetilde{E})$ $a_p(E) = \sigma_{p*} + \sigma_p^*$.

Fact.

- *For $p \nmid N$, there exists a smooth projective curve $\overline{X_0(N)}$ defined over $\mathbb{F}_p$ and a surjective map $X_0(N) \to \overline{X_0(N)}$, which we call "the reduction of $X_0(N) \mod p$".*

  Remark. This is base change of $X_0(N)/\mathbb{Z}\left[\frac{1}{N}\right]$ to $\mathbb{F}_p$

- *There is a map $\overline{T_p}$ on $\mathrm{Pic}(\overline{X_0(N)})$ making the following commute:*

$$\begin{array}{ccc} \mathrm{Pic}(X_0(N)) & \xrightarrow{T_p} & \mathrm{Pic}(X_0(N)) \\ \downarrow & & \downarrow \\ \mathrm{Pic}(\overline{X_0(N)}) & \xrightarrow{T_p} & \mathrm{Pic}(\overline{X_0(N)}) \end{array}$$

Theorem 7.2 (Eichler - Shimura)**.** $\overline{T_p} = \sigma_{p*} + \sigma_p^*$ *as endomorphism of* $\mathrm{Pic}(\overline{X_0(N)})$.

Outline of proof. Igusa's theorem (See D-S Section 8.6) says that reduction of $X_0(N)$ as a curve is compatible with its interpretation as a moduli space. Then look at what $\overline{T_p}$ does at the level of moduli spaces. □

7.4 The Galois representations of $X_0(N)$

Assume $l \nmid N$

Fact.

1. *The natural inclusion* $\mathrm{Pic}(X_0(N)_{\mathbb{Q}})[l^n] \hookrightarrow \mathrm{Pic}(X_0(N)_{\mathbb{C}})[l^n] \cong (\mathbb{Z}/l^n\mathbb{Z})^{2g}$ *is an isomorphism for all n.*

2. *The natural surjection (for $p \nmid lN$)* $\mathrm{Pic}(X_0(N)_{\mathbb{Q}})[l^n] \twoheadrightarrow \mathrm{Pic}(\overline{X_0(N)})[l^n]$ *is also an isomorphism.*

   Hence from now on $X_0(N)$ will be for $X_0(N)_{\mathbb{Q}}$.

Definition 7.3. The *l-adic Tate module* of $\mathrm{Pic}(X_0(N))$ is $\mathrm{Ta}_l\mathrm{Pic}(X_0(N)) = \varprojlim_n \mathrm{Pic}(X_0(N))[l^n] \cong \mathbb{Z}_l^{2g}$.

$G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the points of $X_0(N)$ in the natural way. This gives a natural action of $G_{\mathbb{Q}}$ on $\mathrm{Div}(X_0(N))$, i.e., $\sigma \cdot \sum n_x[x] = \sum n_x[\sigma(x)]$. This preserves degree 0 and principal divisors. Thus we get an action of $G_{\mathbb{Q}}$ on $\mathrm{Pic}(X_0(N))$. The action is linear so preserves $\mathrm{Pic}(X_0(N))[l^n]$ for all l and n. This action is compatible with the connecting maps: $\mathrm{Pic}(X_0(N))[l^{n+1}] \to \mathrm{Pic}(X_0(N))[l^n]$. Thus we get an action on $\mathrm{Ta}_l\mathrm{Pic}(X_0(N))$.

Definition 7.4. For $l \nmid N$, define $\rho_{X_0(N),l} : G_{\mathbb{Q}} \to \mathrm{Aut}(\mathrm{Ta}_l\mathrm{Pic}(X_0(N)) \cong \mathrm{GL}_{2g}(\mathbb{Z}_l)$.

Theorem 7.5. *Let $p \nmid lN$.*

1. *$\rho_{X_0(N),l}$ is unramified at p*

2. *If $\mathcal{P}|p$ is a prime of $\overline{\mathbb{Z}}$,* $\mathrm{Frob}_{\mathcal{P}}$ *any Frobenius element, then $\rho_{X_0(N),l}(\mathrm{Frob}_{\mathcal{P}})$ satisfies $X^2 - T_pX + p = 0$.*

Proof.

1. We have a commutative diagram

$$\begin{tikzcd} D_p \arrow[r, "\rho_{X_0(N),l}"] \arrow[d] & \mathrm{Aut}(\mathrm{Ta}_l\mathrm{Pic}(X_0(N))) \arrow[d] \\ G_{\mathbb{F}_p} \arrow[r] & \mathrm{Aut}(\mathrm{Ta}_l\mathrm{Pic}(\overline{X_0(N)})) \end{tikzcd}$$

Now, the inertia $I_{\mathcal{P}}$ is in the kernel of the left hand map. The right hand map is an isomorphism (by fact 2.) In particular, $I_{\mathcal{P}} \subset \ker(\rho_{X_0(N),l})$ and hence $\rho_{X_0(N),l}$ is unramified at p.

2. We have a commutative diagram

$$\begin{tikzcd} \mathrm{Pic}(X_0(N)[l^n] \arrow[r, "T_p"] \arrow[d] & \mathrm{Pic}(X_0(N))[l^n] \arrow[d] \\ \mathrm{Pic}(\overline{X_0(N)})[l^n] \arrow[r, "\sigma_{p*}+\sigma_p^*"] & \mathrm{Pic}(\overline{X_0(N)})[l^n] \end{tikzcd}$$

we can describe the lifts of $\sigma_{p,*}$ and σ_p^*. $\mathrm{Frob}_{\mathcal{P}}$ is a lift of $\sigma_{p,*}$ as σ_p is totally ramified of degree p. While $\sigma_p^*([x]) = \sum_{y\in\sigma^{-1}(x)} e_x[y] = p[\sigma_p^{-1}[x]$ so in particular, a lift is $p\mathrm{Frob}_{\mathcal{P}}^{-1}$. So we get a commutative diagram:

$$\begin{tikzcd} \mathrm{Pic}(X_0(N)[l^n] \arrow[r, "\mathrm{Frob}_{\mathcal{P}}+p\mathrm{Frob}_{\mathcal{P}}^{-1}"] \arrow[d, "\cong"'] & \mathrm{Pic}(X_0(N))[l^n] \arrow[d, "\cong"'] \\ \mathrm{Pic}(\overline{X_0(N)})[l^n] \arrow[r, "\sigma_{p*}+\sigma_p^*"] & \mathrm{Pic}(\overline{X_0(N)})[l^n] \end{tikzcd}$$

Hence $T_p = \mathrm{Frob}_{\mathcal{P}} + p\mathrm{Frob}_{\mathcal{P}}^{-1}$. This holds for all n, hence it holds for $\mathrm{Ta}_l\mathrm{Pic}(X_0(N))$. So $\mathrm{Frob}_{\mathcal{P}}^2 - T_p\mathrm{Frob}_{\mathcal{P}} + p = 0$

□

8 Modular Galois Representations (Nicolas)

Last week we had $N \in \mathbb{N}$, $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\}$

This week we use $\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}$. Note that $\Gamma_0(N) \lhd \Gamma_1(N)$, we have a map $\Gamma_0(N)/\Gamma_1(N) \to (\mathbb{Z}/N\mathbb{Z})^*$ defined by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \mod N$. Define $X_1(N) = \left(\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})\right)/\Gamma_1(N)$. We have $\Gamma_0 \twoheadrightarrow \Gamma_0/\Gamma_1$ acting on X_1, which gives rise to the diamond operator $\langle d \rangle \in \mathbb{T}$ for all $d \in (\mathbb{Z}/N\mathbb{Z})^*$.

Let $J_1(N) = \mathrm{Pic}^0(X_1(N))$, let $l \in \mathbb{N}$ be a prime. We define $T_lJ_1(N) = \varprojlim_n J_1(N)[l^n]$ and $V_lJ_1(N) = T_lJ_1(N) \otimes \mathbb{Q}$

Theorem 8.1. *$G_{\mathbb{Q}} \circlearrowleft V_lJ_1(N)$ affords $\rho_{X_1(N),l} : G_{\mathbb{Q}} \to \mathrm{GL}_{2g}(\mathbb{Q}_l)$ (where $g =$ genus of $X_1(N)$)) unramified at lN. For all $p \nmid lN$ we have $\rho_{X_1(N),l}(\mathrm{Frob}_p)$ satisfies $X^2 - T_qX + p\langle p \rangle = 0$.*

Actually $V_lJ_1(N)$ is a free $(\mathbb{T} \otimes \mathbb{Q}_l)$-module of rank 2, so $\rho_{X_1(N),l} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{T} \otimes \mathbb{Q}_l)$ and the characteristic polynomial of $\rho_{X_1(N),l}(\mathrm{Frob}_p)$ is $X^2 - T_qX + p\langle p \rangle$.

Let $k \in \mathbb{N}$, and let $\mathcal{N}_k(N) = \{\text{new forms in } S_k(\Gamma_1(N))\}$. Reminder: a new form is an normalised eigenform which is genuinely of level N (i.e., does not come from lower level)

Remark. For all $D|N$, $\mathcal{N}_k(N) \overset{\subset}{\subset} S_k(\Gamma_1(N))$.

For all $f = q + \sum a_n q^n \in \mathcal{N}_k(N)$, we have that:

- $K_f = \mathbb{Q}(a_n)$ is a number field.
- There exists $\epsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ such that for all d, $\langle d \rangle f = \epsilon(d)f$.

- For all $\sigma \in G_{\mathbb{Q}}$, $f^\sigma = q + \sum \sigma(a_n) q^n$ with $\sigma(a_n) \in \mathcal{N}_k(N)$. $\text{char}\epsilon^\sigma = \sigma \circ \epsilon$

Pick $f \in \mathcal{N}_2(N)$ with $f = \sum a_n q^n$. Define $I_f = \{T \in \mathbb{T} | Tf = 0\} \subset \mathbb{T}$. We have the isomorphism $(\mathbb{T} \otimes \mathbb{Q})/I_f \to K_f$ defined by $T_p \mapsto a_p$, $\langle d \rangle \mapsto \epsilon(d)$

Define $A_f = J_1(N)//I_f J_1(N)$. It is an abelian variety over $\mathbb{Q}$ of dimension $d = [K_f : \mathbb{Q}]$.

Theorem 8.2. $J_1(N) \sim \prod_{D|N, F \in G_{\mathbb{Q}} \backslash \mathcal{N}_2(D)} A_F^{\sigma_0(N/D)}$. *And actually* $V_l J_1(N) \cong \prod_{D|N, F \in G_{\mathbb{Q}} \backslash \mathcal{N}_2(D)} V_l A_F^{\sigma_0(N/D)}$ *as* $G_{\mathbb{Q}}$*-modules*

$K_l \otimes \mathbb{Q}_l \cong \prod_{\ell | l} K_{f,\ell}$, therefore

Theorem 8.3. *For all* $\ell | l$ *in* K_f*, there exists* $\rho_{f,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{f,\ell})$ *unramified outside in* lN*. The characteristic polynomial of* $\rho_{f,\ell}(\mathrm{Frob}_p)$ *is* $X^2 - a_p X + p\epsilon(p)$ *(for* $p \nmid lN$*).*

8.1 Residual maps

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_d(K_\ell)$ with $K_\ell/\mathbb{Q}_l$ finite. There exists $\rho' \sim \rho$ such that $\mathrm{Im}\rho' \subseteq \mathrm{GL}_d(\mathbb{Z}_{K_\ell})$. We want to define $\overline{\rho} = \rho' \mod \ell$. This is not well defined!

Example. Let $\rho = \begin{pmatrix} \chi & \psi \\ 0 & \chi \end{pmatrix} \sim \begin{pmatrix} \chi & l\psi \\ 0 & \chi \end{pmatrix}$ but reduced mod l we have $\begin{pmatrix} \overline{\chi} & \overline{\psi} \\ 0 & \overline{\chi} \end{pmatrix} \not\sim \begin{pmatrix} \overline{\chi} & 0 \\ 0 & \overline{\chi} \end{pmatrix}$.

Definition 8.4. Let $\rho : G \to \mathrm{GL}(V)$ be a representation. Define $V^{ss} = V$ if there is no $W \subset V$ subrepresentation with $V^{ss} = (W) \oplus (V/W)$

So we define $\overline{\rho} = (\rho' \mod \ell)^{ss}$

Theorem 8.5 (Brauer - Nabitt)**.** *Let* $G \underset{\rho_2}{\overset{\rho_1}{\rightrightarrows}} \mathrm{GL}(V)$ *be 2 semi-simple representation. If for all* $g \in G$ *we have that the characteristic polynomial of* $\rho_1(g)$ *is equal to the characteristic polynomial of* $\rho_2(g)$*, then* $\rho_1 \sim \rho_2$*.*

8.2 Higher weights

Theorem 8.6 (Deligne 1971)**.** *Let* $k \geq 2$*, for all* $f = \sum a_n q^n \in \mathcal{N}_k(N)$*, for all* $\ell | l$ *in* K_f*, there exists* $\rho_{f,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_{f,\ell})$ *unramified outside* lN*. We have that the characteristic polynomial of* $\rho_{f,\ell}(\mathrm{Fob}_p)$ *is* $X^2 - a_p X + p^{k-1}\epsilon(p)$

Remark. We have $\det \rho_{f,\ell} = \chi_l^{k-1}\epsilon$ where χ_l is the l-adic cyclotomic character. In particular, let $c \in G_{\mathbb{Q}}$ be complex conjugation we have $\det \rho_{f,\ell}(c) = \chi_l^k(c)\epsilon(c) = (-1)^{k-1}\epsilon(-1) = -1$. Hence $\rho_{f,\ell}$ is odd

The last step relied on: for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, $f(\gamma z) = \epsilon(d)(cz+d)^k f(z)$. In particular $\gamma = \begin{pmatrix} -1 & \\ & -1 \end{pmatrix} \in \Gamma_0$ so $\epsilon(-1)(-1)^k = +1$.

Remark. For all $K_f \hookrightarrow \mathbb{C}$ and for all p prime, we have $|a_p| \leq 2p^{\frac{k-1}{2}}$. For all $n \in \mathbb{N}$ we have $|a_n| \leq \sigma_0(n) n^{\frac{k-1}{2}}$ where $\sigma_0(n) = \#\{d|n\}$

8.3 Weight 1

Theorem 8.7 (Deligne - Serre, 1976)**.** *For all* $f \in \mathcal{N}_1(N)$ *there exists* $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{C})$*, unramified outside* N*. The characteristic polynomial of* $\rho_f(\mathrm{Frob}_p)$ *is* $X^2 - a_p X + \epsilon(p)$*. Actually* ρ_f *is irreducible and the conductor is* N*.*

Sketch of Proof. The steps for this proof are as follow

1. There exists $\overline{\rho}_{f,l}$ for infinitely many l.
2. $\{a_p, p\text{prime}\}$ is "almost finite"

3. If $G_l = \mathrm{Im}\overline{\rho}_{f,l} \subset \mathrm{GL}_2(\mathbb{F}_l)$ then there exists constant C for all l such that $\#G_l \leq C$
4. For $l \gg 1$, G_l may be lifted to $\mathrm{GL}_2(\mathbb{C})$. This gives $\rho_{f,l}$ to representations in $\mathrm{GL}_2(\mathbb{C})$
5. Calculate characteristic polynomials
6. For all l, l', $\rho_{f,l} \sim \rho_{f,l'} = \rho_f$.

□

9 From l-adic to mod l representations. Serre's conjecture: the level (Samuele)

Let N and k be integers, $k \geq 2$. Let $f \in S_k(\Gamma_1(N))$ be an eigenform, $f(z) = q + \sum_{n\geq 2} a_n q^n$. Let $E = \mathbb{Q}(\{a_n\})$, ϵ_f a character of f, then $\langle d \rangle f = \epsilon_f(d) f$. From the previous section we know there exists a family of continuous λ-adic representation $\rho_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(E_\lambda)$ where $\lambda \subset \mathcal{O}_E$ and E_λ is the completion of E at λ. We have $\rho_{f,\lambda}$ is irreducible and $\forall p \nmid N \cdot \mathrm{Nm}(\lambda)$, $\mathrm{Tr}(\rho_{f,\lambda}(\mathrm{Frob}_p)) = a_p$ and $\det(\rho_{f,\lambda}(\mathrm{Frob}_p)) = \epsilon_f(p) \cdot p^{k-1}$. To $\rho_{f,\lambda}$ we can associate $\overline{\rho_{f,\lambda}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ where $\mathbb{F} = \mathcal{O}_{E,\lambda}/\lambda$ and this representation is only defined up to semisimplification.

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_l)$ the question is when is $\rho \cong \overline{\rho_{f,\lambda}}^{\mathrm{ss}}$?

"Serre": A necessary and sufficient condition is that ρ is odd if ρ is semisimple.

Let us forget about $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_l)$ which are reducible

Theorem 9.1 (Khane, Witenberger, Kism, Dieulefait. (Serre's conjecture))**.** *Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2\left(\overline{\mathbb{F}}_l\right)$ be a continuous, irreducible, odd representation then ρ is modular*

Modular means that there exists integers N, k such that $\rho \cong \overline{\rho}_{f,\lambda}$ where $f \in S_k(\Gamma_1(N))$. There exists $N(\rho)$, $k(\rho)$ minimal. $N(\rho)$ is the Artin conductor of ρ away from l and $k(\rho)$ is weight in terms of $\rho|_{I_l}$.

Theorem 9.2 (Ribet)**.** *Assume $l \geq 3$ and suppose that ρ arises from $\Gamma_1(M)$ when $M = N \cdot l^\alpha$, $\gcd(N, l) = 1$. Then ρ arises from $\Gamma_1(N)$.*

Remark. Buzzard generalised the above for the case $l = 2$.

Theorem 9.3. *Suppose that ρ arises from $S_k(\Gamma_1(N))$ with $\gcd(N, l) = 1$ and $2 \leq k \leq l + 1$. Assume either $l > 3$ or $N > 3$, then ρ arises from $S_2(\Gamma_1(Nl))$.*

This theorem comes from Ash-Stevens under the condition that $l \geq 5$ and Serre-Gross under the assumption that $N \geq 4$.

Theorem 9.4 (Edixhoron)**.** *Let $\gcd(N, l) = 1$ and assume ρ arises from $S_k(\Gamma_1(N))$ then ρ arises from $S_{k(\rho)}(\Gamma_1(N))$, where $k(\rho)$ is Serre's weight, furthermore $k \equiv k(\rho) \mod l - 1$ and $k \geq k(\rho)$ if l is odd.*

Corollary 9.5. *If ρ arises from $\Gamma_1(N)$ and $\gcd(N, l) = 1$ then there exists $i \in \mathbb{Z}$ such that $\rho \otimes \chi^i$ arises from $S_k(\Gamma_1(N))$ for $k \leq l + 1$, where χ is the mod l Cyclotomic character.*

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_l})$ be irreducible and consider the following four sets

- $\mathcal{N}_1 = \left\{N \middle| \gcd(N, l) = 1, \rho \,\text{arises from}\, S_{k(\rho)}(\Gamma_1(N))\right\}$
- $\mathcal{N}_2 = \left\{N \middle| \gcd(N, l) = 1, \rho \,\text{arises from}\, \Gamma_1(N)\right\}$
- $\mathcal{N}_3 = \left\{N \middle| \gcd(N, l) = 1, \rho \,\text{arises from}\, \Gamma_1(Nl^\alpha), \alpha > 0\right\}$
- $\mathcal{N}_4 = \left\{N \middle| \gcd(N, l) = 1, \rho \,\text{arises from}\, S_2(\Gamma_1(Nl^2))\right\}$

Theorem 9.6. *If $l \geq 5$ then the four sets $\mathcal{N}_1, \mathcal{N}_2, \mathcal{N}_3$ and $\mathcal{N}_4$ are equal*

Proof. $\mathcal{N}_1 = \mathcal{N}_2$ are equal by Theorem 9.4

$\mathcal{N}_2 = \mathcal{N}_3$ are equal by Theorem 9.2

By definition $\mathcal{N}_4 \subseteq \mathcal{N}_3$ so we want to show that $\mathcal{N}_3 \subseteq \mathcal{N}_4$ or equivalently $\mathcal{N}_2 \subseteq \mathcal{N}_4$. Assume that ρ arises from $\Gamma_1(N)$ and choose $i \geq 0$ by Corollary 9.5 such that $\rho \otimes \chi^i$ arises from $S_k(\Gamma_1(N))$ with $2 \leq k \leq l+1$. By Theorem 9.3 then $\rho \otimes \chi^i$ arises from $S_2(\Gamma_1(Nl))$. Now tensoring with χ^i changes the level of a modular form but not the weight. Look at χ^i as a Dirichlet character, $f : \overline{\rho_{f,\lambda}} \cong \rho \otimes \chi^i$ then consider $f \otimes \chi^{-i} \in S_2(\Gamma_1(Nl^2))$. So $\rho = (\rho \otimes \chi^i) \otimes \chi^{-i}$ arises from $S_2(\Gamma_1(Nl^2))$. □

We shall denote the four equal sets by $\mathcal{N}(\rho)$. So the question now becomes is $N(\rho) \in \mathcal{N}(\rho)$?

Theorem 9.7 (Livne)**.** *Suppose ρ arises from $\Gamma_1(N)$ then $N(\rho)|N$.*

Let f be an eigenform giving rise to ρ. Then N the level of f is such that $N(\rho)|N$, or better $N(\rho)|N'$ where N' is the prime-to-l part of N.

The aim is: If $N(\rho) \neq N'$ then we want to find another form at level $N(\rho)$ giving rise to ρ.

Note that we can replace f by a newform, f', giving the same eigensystem. $\rho_{f,\lambda} = \rho_{f',\lambda'}$. We have $N(\rho)|\text{level}(f')$. So from now on, assume f is a newform. Let us look at the conductors $N(\rho) = N(\overline{\rho}_{f,\lambda}) < N(\rho_{f,\lambda}) = \text{level}(f)$.

Assume $l \neq p$ and consider $\rho_p : \text{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \text{GL}_2(\mathbb{Q}_l)$ and $\overline{\rho}_p$ reduction. We look at the conductor exponents $n_{\rho_p} = n_p = \dim(V) - \dim V^I + n_{\rho_p,\text{wild}}$ and $n_{\overline{\rho}_p} = \overline{n}_p = \dim(\overline{V}) - \dim\left(\overline{V}^I\right) + n_{\overline{\rho}_p,\text{wild}}$. We know that $n_{\rho_p,\text{wild}} = n_{\overline{\rho}_p,\text{wild}}$, we also know that $\dim \overline{V}^I \geq \dim V^I$, so $\overline{n}_p \leq n_p$. We want to study when $\overline{n}_p < n_p$.

Theorem 9.8. *The representation ρ_p which can degenerate (i.e., $\overline{n}_p < n_p$) can be one of the following*

1. *Principal series: $\rho_p \cong \mu \oplus \nu$ such that $n_\mu = 1$ and $n_{\overline{\mu}} = 0$, then $n_p = n_\nu + 1$ and $\overline{n}_p = n_{\overline{\nu}}$.*
2. *Special case (Steinberg I): $\rho_p = \mu \otimes \text{sp}(1)$ such that $n_\mu = 0$ (then $n_p = 1$ and $\overline{n}_p = 0$)*
3. *Special case (Twist Steinberg): $\rho_p = \mu \otimes \text{sp}(1)$ such that $n_\mu = 1$ and $n_{\overline{\mu}} = 0$ (then $n_p = 2$ and $\overline{n}_p = 0$)*
4. *(Super) Cuspidal case: $\rho_p = \text{Ind}\zeta$ such that $n_\zeta = 1$ and $n_{\overline{\zeta}} = 0$ (then $n_p = 2$ and $\overline{n}_p = 0$)*

Back to modular forms:

Theorem 9.9 (Ribet level lowering)**.** *Assume that $N(\overline{\rho}_{f,\lambda}) < N$ where f is a newform of level $\Gamma_1(N)$ and $\gcd(N, l) = 1$. Then for every $p \big| N/N(\overline{\rho}_{f,\lambda})$ there exists a Dirichlet character ϕ of conductor p and l-power order such that the newform attached to $f \otimes \phi$ has level dividing N/p. In particular, $\overline{\rho}_{f,\lambda}$ is modular of level M where $M = N/\prod p$ where $p|N/N(\overline{\rho}_{f,\lambda})$.*