1 Introduction (Vladimir)

1.1 Galois representations

Galois representations really mean representations of Galois groups.

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

\[ \text{Gal}(\overline{K}/K) \to \text{Gal}(F/K) \to \text{GL}_n(\mathbb{C}) \]

Note. e.g., the trivial representation is the same Artin representation for all $F/K$.

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

<table>
<thead>
<tr>
<th></th>
<th>$\text{id}$</th>
<th>$(12)$</th>
<th>$(123)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{I}$</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\epsilon$</td>
<td>1</td>
<td>$-1$</td>
<td>1</td>
</tr>
<tr>
<td>$\rho$</td>
<td>2</td>
<td>0</td>
<td>$-1$</td>
</tr>
</tbody>
</table>

- $I(s) = I(t) = 1$
- $\epsilon(s) = 1, \epsilon(t) = -1$
- $\rho(s) = \left( \begin{array}{cc} -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{array} \right)$, $\rho(t) = \left( \begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right)$

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

Hence Dirichlet characters can be seen as representation $\chi : \mathcal{G} \to \mathbb{C}^1 = \text{GL}_1(\mathbb{C})$.
Definition 1.2. A mod l Galois representation is the same thing with matrices in GL_n(\mathbb{F}_l).

Example. Let E/\mathbb{Q} be an elliptic curve. We know E(\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

\[ \rho : \mathbb{Q} \to GL_2(\mathbb{F}_l) \]

G acts on E[l] and preserves addition, i.e., \( g(P + Q) = g(P) + g(Q) \). Therefore we get \( \rho : G \to GL_2(\mathbb{F}_l) \).

E.g: Let \( y^2 = x^3 - 5 \), then \( E[2] = \{ 0, (\sqrt{5}, 0), (\zeta_5 \sqrt{5}, 0), (\zeta_5^2 \sqrt{5}, 0) \} \). So take \( F = \mathbb{Q}(\zeta_5, \sqrt{5}) \), then \( G = \text{Gal}(F/\mathbb{Q}) \) permutes \( E[2] \) (we see that \( G = S_3 \)). Let us write down the matrix, so let \( P = (\sqrt{5}, 0) \) and \( Q = (\zeta_3 \sqrt{5}, 0) \).

- \( g \in S_3 \) be a 3-cycle, \( \rho(g) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_2) \)
- \( g \in S_3 \), be a transposition, \( \rho(g) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_2) \)

1.2 l-adic representations

Definition 1.3. A continuous l-adic representation over K is a continuous homomorphism \( \text{Gal}(K^{\text{sep}}/K) \to GL_d(\mathbb{F}) \) for some finite \( \mathbb{F}/\mathbb{Q}_l \).

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 \( \text{Gal}(K^{\text{sep}}/F_n) \to \text{id} \mod l^n \). I.e., \( \rho \) \mod l^n factors through a finite extension \( F_n/K \).

So \( \text{Gal}(K^{\text{sep}}/F_1) \) map to \( \begin{pmatrix} 1 + lO_F & lO_F \\ lO_F & 1 + lO_F \end{pmatrix} \).

Example. Let E/\mathbb{Q} be an elliptic curve:
- \( P_1, Q_1 \) basis for \( E(\mathbb{Q})[l] \).
- \( P_2, Q_2 \) basis for \( E(\mathbb{Q})[l^2] \), with \( lP_2 = P_1 \), \( lQ_2 = Q_1 \)
- \( \vdots \)
- \( P_n, Q_n \) basis for \( E(\mathbb{Q})[l^n] \), with \( lP_n = P_{n-1} \), \( lQ_n = Q_{n-1} \).

For \( g \in \text{Gal}(\mathbb{Q}/\mathbb{Q}) \) define \( 0 \leq a_n, b_n, c_n, d_n < l \) by \( gP_1 = a_1 P_1 + b_1 Q_1 \), \( gQ_1 = c_1 P_1 + d_1 Q_1 \), and \( gP_n = (a_1 + \cdots + a_n l^{n-1}) P_n + (b_1 + \cdots + b_n l^{n-1}) Q_n \) and \( gQ_n = (c_1 + \cdots + c_n l^{n-1}) P_n + (d_1 + \cdots + d_n l^{n-1}) Q_n \). Then

\[ \rho(g) = \begin{pmatrix} a_1 + \cdots + l^{n-1} a_n + \cdots & c_1 + \cdots + l^{n-1} c_n + \cdots \\ b_1 + \cdots + l^{n-1} b_n + \cdots & d_1 + \cdots + l^{n-1} d_n + \cdots \end{pmatrix} \in GL_2(\mathbb{Z}_l) \]

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

2 Galois Representations: vocabulary (Matthew S)

2.1 Galois Theory of Infinite Algebraic Extensions

Notation. \( G(F/K) := \text{Gal}(F/K) \), \( G_K = G(\overline{K}/K) \) 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 \( F = \mathbb{F}_p \), let \( \phi_p \) 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 \( G(K''/K') \sim G(K'/K) \).

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

\( B = \{ \text{left/right cosets of finite index subgroups} \} \)

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

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

Example. Back to the example, \( G(\mathbb{F}_p^n/\mathbb{F}_p) = \mathbb{Z}/n\mathbb{Z} \), so \( G_{\mathbb{F}_p} = \lim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}} \).

2.2 Galois groups of \( \mathbb{Q} \).

Fix \( \mathbb{Q} \rightarrow \mathbb{Q}_p, \overline{\mathbb{Q}} \rightarrow \overline{\mathbb{Q}}_p \):

\[
\overline{\mathbb{Q}}_p \rightarrow \mathbb{F}_p \\
\mathbb{Q}^\text{ur}_p \rightarrow \mathbb{F}_p \\
\mathbb{Q}_p \rightarrow \mathbb{F}_p
\]

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

\[
\xymatrix{ G_{\mathbb{Q}_p} \ar[r] & G(\mathbb{Q}^\text{ur}_p/\mathbb{Q}_p) \ar[r] & G_{\mathbb{F}_p} }
\]

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 \( \Theta : G_{\mathbb{Q}_p} \rightarrow G(K/\mathbb{Q}_p) \), 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:

\( G(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^* \), \( K_l = \cup_{n \in \mathbb{Z} \geq 0} \mathbb{Q}(\zeta^n) \) we have an isomorphism \( G(K_l/\mathbb{Q}) \rightarrow \mathbb{Z}_l^* \). Let \( \epsilon_l : G_{\mathbb{Q}} \rightarrow \mathbb{Z}^*_l \), defined as for: \( \sigma \in G_{\mathbb{Q}}, \sigma(\zeta) = \zeta^{\epsilon_l(\sigma)} \). \( K_l \) is ramified at \( \infty \) and at \( l \). For \( p \neq l \), recall \( \phi_p \), 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 $\text{Hom}_{\text{cont}}(G_{K,S}/\mathbb{Z}/p\mathbb{Z})$ 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 $G_{\mathbb{Q}_p} \rightarrow G_{\mathbb{Q},S}$ is an inclusion
- If $p \notin S$, the map $G_{\mathbb{Q}_p} \rightarrow G_{\mathbb{Q},S}$ has kernel exactly $I_p$. So $G_{\mathbb{Q}_p}/I_p \rightarrow G_{\mathbb{Q},S}$.

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 $T \supset S$ 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, $\rho : G_{\mathbb{Q},S} \rightarrow \text{GL}_n(A)$.

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:

- $G$ (a profinite group) acts continuously
- $M = \varprojlim_H M^H$ 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 $\rho$, 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, $\rho : G_{\mathbb{Q}} \rightarrow \text{GL}_n(\mathbb{C})$, is determined by trace($\rho(\phi_p)$) on $p \notin S$ such that $\rho$ is unramified at $p$.

2. A semisimple mod $l$ representation, $\rho : G_{\mathbb{Q}} \rightarrow \text{GL}_n(k)$, is determined by the values of trace($\wedge^i(\rho(\phi_p))$) where $i = 1, \ldots, n$ on primes $p \notin S$ at which $\rho$ is unramified. If $l > n$ it is sufficient to use trace($\rho(\phi_p)$) at the same primes.

3. A semisimple $l$-adic representations, $\rho : G_{\mathbb{Q}} \rightarrow \text{GL}_n(A)$, is determined by trace($\rho(\phi_p)$) on $p \notin S$ at which $\rho$ is unramified.
2.5 Conductors of representation

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

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

**Definition 2.9.** Conductor of $\rho$ at $p$ is the integer

$$m_p(\rho) = \text{codim}(\rho |_{I^p_F}) + \int_0^\infty \text{codim}(\rho |_{I^v_p})du$$

The conductor of $\rho$ 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.**
- $\pi_K$ be a fixed uniformiser of $K$
- $\mathcal{O}_K$ the ring of integers of $K$
- $\nu_K$ the normalized valuation on $K$
- $I_{F/K}$ the inertia group
- $\text{Frob}_{F/K}$ for a Frobenius element
- $\Phi_{F/K} = \text{Frob}_{F/K}^{-1}$ 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 $\rho$ over a local field $K$ is

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

where $\rho$ 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

$$F = \mathbb{Q}_5(\zeta_3, \sqrt[3]{5})$$

$$\mathbb{Q}_5(\zeta_3) \quad \mathbb{Q}_5(\sqrt[3]{5})$$

$$K = \mathbb{Q}_5$$

We have $\text{Gal}(F/K) \cong S_3$, $I_{F/K} \cong C_3 \cong \text{Gal}(F/K(S_3))$ and $\text{Frob}_{F/K} = t$ (an element of order 2). Then
For $I$ we have $P(I, T) = \det (1 - \Phi_{F/K}T|_{I_{F/K}}) = \det (1 - T) = 1 - T$ (Since $I^{C_3} = I$)

For $\epsilon$ (the sign representation) $P(\epsilon, T) = \det (1 - \Phi_{F/K}\epsilon T|_{I_{F/K}}) = \det (1 - (1 - 1)T|_{\epsilon}) = 1 + T$ (since $\epsilon_{F/K} = \epsilon$, so $\epsilon(t) = -1$)

For $\rho$ the 2-dimensional representation: $P(\rho, T) = \det (1 - \Phi_{F/K}\rho T|_{I_{F/K}}) = 1$ (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

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

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

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

**Example.**

- Let $K$ be a number field, $\rho = I$ then $P_{\mathcal{I}}(s, T) = 1 - T$ is a function of the non-trivial Dirichlet character $\mathbb{Z}/3\mathbb{Z} \rightarrow \mathbb{C}^*$

Putting it together we get

$$L(\rho, s) = \prod_{\mathcal{P} \neq \mathcal{I}} \frac{1}{1 - (\frac{4}{3})^s \mathcal{P}^{-s}} = \sum_{n=1}^{\infty} \left(\frac{4}{3}\right)^n n^{-s}$$

**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 $\rho_1$ and $\rho_2$ 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, $\rho$ an Artin representations over $F$ then $P_F(\rho, T_f) = P_K(\text{Ind}_e, T)$ 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, $\rho$ Artin representation over $F$, then $L(\rho, s) = L(\text{Ind}_e, s)$ (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 $n_{\rho, \text{wilde}} = \sum_{k=1}^{\infty} \frac{1}{\nu_k} \dim \rho^{I/F_k}$ where $\rho$ factors through $F/K$ and $I_{F/K} = I = I_0$, $I_k = \{ \sigma \in \text{GL}(F/K) | (\sigma(\alpha) \mod \pi^{k+1} \forall \alpha \in \mathcal{O}_F) \}$ are the higher ramification groups (with lower numbering).

So $I_1 = \text{Syl}_p I = \text{wild inertia}$ and $I/I_1 = \text{tame inertia}$.

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

**Definition 3.4.** The conductor of $\rho$ is the ideal $N_\rho = (\pi^n)$

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

**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 $\rho$ be an Artin representation over a local field $K$ which factors throughout $\text{Gal}(F/K)$. Then $n_{\rho, \text{wilde}} = (\text{Trace } \rho, b)$ 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).

Let $F/K$ be Galois, $\rho$ be a representation of $H = \text{Gal}(F/L)$. Then $n_{\text{Ind}_G^H \rho} = (\dim \rho) \cdot \nu_K(\Delta_{L/K}) + P_{L/K} n_\rho$

equivalently $N_{\text{Ind}\rho} = \Delta_{L/K} \text{Nm}_{L/K}(N_\rho)$

**Example.**

Let $F = \mathbb{Q}_5(\zeta_3, \sqrt[3]{5})$, $\mathbb{Q}_5(\sqrt[3]{5})$, $\mathbb{Q}_5(\zeta_3)$.

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

- $n_1 = 0$ as $n_{\rho, \text{tame}} = 1 - 1$ and $n_{\rho, \text{wilde}} = 0$
- $n_e = 0$
- $n_\rho = 2 = 2 - 0$

By the Conductor-discriminant formula:

$\Delta_{L/K} = N_{\text{Ind}_{\mathbb{Q}_5}^\mathbb{Q}_5} = M_{\rho} N_3 = 5^2$ (up to units)

$\Delta_{F/K} = N_{\text{Ind}_{\mathbb{Q}_5}^\mathbb{Q}_5} = N_{\rho \oplus \rho \oplus \rho} = 5^4$ (up to units)
Definition 3.8. The conductor of an Artin representation over a number field $K$

$$N_\rho = \prod_P \mathcal{P}^{n_P(\rho)}$$

where $n_P(\rho)$ is the conductor exponent of $\rho$ restricted to $\text{Gal}(\overline{K}_P/K_P)$.

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

3.1.3 Functional equations

Theorem 3.9. The Artin $L$-function of $\rho$ satisfies the functional equation

$$\Lambda(\rho, s) = \omega A^{1/2-s} \Lambda(1-s, \rho \hat)$$

where

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

3.2 $l$-adic Representations

3.2.1 Local Polynomials

Definition 3.10. Let $K/Q_p$ be finite, $\rho : \text{Gal}(K/K) \to \text{GL}_d(F)$ where $F/Q_l$ with $l \neq p$, be a continuous $l$-adic representation. The local polynomial of $\rho$ is

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

3.2.2 Conductor

Definition 3.11. The conductor exponent is $n_\rho = n_{\rho, \text{tame}} + n_{\rho, \text{wild}}$ where $n_{\rho, \text{tame}} = \dim_{\rho/P} \pi_K$, $n_{\rho, \text{wild}} = \sum_{k \geq 1} \frac{1}{[F/F_{K,k}]} \dim_{\rho/P} \pi_{F/K,k}$ 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 $\text{Gal}(\overline{K}/F)$ lies in $\begin{pmatrix} 1 + l \mathcal{O}_F & l \mathcal{O}_F \\ l \mathcal{O}_F & 1 + l \mathcal{O}_F \end{pmatrix}$ and $\text{im}(I_1) = \text{id}$ since it is a (pro) $p$-group sent into a (pro) $l$-group.

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

8
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 $L$
- $I_w^e$ the (absolute) wild inertia group of a field $L$
- $\Phi_L$ a geometric Frobenius element

### 4.1 Finite Image of Inertia

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

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

$0 \to W \to V \xrightarrow{f} V/W \to 0$

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 $\tau$ 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 $\text{Gal}(L'/K)$ is generated by $H$ and $\Phi_L$. We have $\Phi_L = \Phi_L^f$, so $\Phi_L'$ doesn't commute with $\Phi_L$. 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 $[\sigma, \Phi_L'] = H \cap \langle \Phi_L' \rangle$. So we have that $|\sigma, \Phi_L'| = 1$. By Schur’s lemma we have that $\tau(\Phi_L') = \lambda \text{id}_d$. Define $\chi$ to be

- $\chi(I_K) = 1$
- $\chi(\Phi_K) = \sqrt[|\chi|]{\lambda}$

Set $\rho := \tau \otimes \chi^{-1}$. So $\rho(\Phi_L') = \rho(\Phi_K') = 1$. □
### 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 $\sigma(i\sqrt{\pi_K}) = \zeta_l^{t_l(\sigma)} i\sqrt{\pi_K}$. (Where $\zeta_l$ is a primitive $l$th root of unity) This is called the $l$-adic tame character.

2. For any $n \geq 0$,
   $$\text{sp}(n)(\sigma) = \begin{pmatrix}
   1 & t & t^2/2! & \ldots & t^n/n! \\
   0 & 1 & & & \\
   \vdots & & \ddots & & \\
   \vdots & & & \ddots & t \\
   0 & & & & 1
   \end{pmatrix}$$

   where $t = t_l(\sigma), \sigma \in I_K$. And we define
   $$\text{sp}(n)(\Phi_K) = \begin{pmatrix}
   1 & 0 \\
   q & \cdots \\
   0 & q^m
   \end{pmatrix}$$

   where $q = \# \mathbb{F}_K$.

**Theorem 4.4.** Let $\tau : G_K \to \text{GL}_d(F)$ be an $l$-adic Galois representation such that $\Phi_K$ acts semisimply on $\tau^l$, for every finite index subgroup $I' \subseteq I$, and for every choice of $\Phi_K$. Then

$$\tau = \oplus_i (\rho_i \otimes \text{sp}(n_i))$$

(after a finite extension) where $\rho_i$ 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 $H = \text{Gal}(L_l/L^{nm}) \cong \mathbb{Z}_p$, where $L_l = \cup_{m=1}^{m} L^{nm} (i\sqrt{\pi_L})$.

Note that $\sigma \in H$ and $\Phi_K$ 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 $\tau(\sigma)^q = \tau(\sigma^q) = \tau(\Phi^{-1}_L \sigma \Phi_L) = \tau(\Phi^{-1}_L) \tau(\sigma) \tau(\Phi_L) = \tau(\sigma)$. 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 $F$ if necessary, we can assume that

$$\tau(\sigma) = \begin{pmatrix}
   \lambda & 0 \\
   0 & \lambda
   \end{pmatrix}. $$

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 $i$th 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 $\mu(\Phi_K v_1) = \sigma(\Phi_K v_1) = \Phi_K(\sigma^q v_1) = \lambda^q \Phi_K v_1$. Similarly $\lambda(\Phi_K v_2) = \mu^q \Phi_K v_2$. Hence $\lambda, \mu$ 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 Gal(\( L_4/L^m \)) and \( \theta \in \text{Gal}(L_4/K^m) \) we have \( \sigma \theta = \theta \sigma \).

\( \square \)

5 \( l \)-adic representations of Elliptic curves (Heline)

5.1 Definition

Notation.

- Let \( K = \mathbb{Q} \) or \( \mathbb{Q}_p \)
- \( G_K := \text{Gal}(\overline{K}/K) \)
- \( E/K \) 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 \( G_K \rightarrow \text{Aut}(E[m]) \cong \text{GL}_2(\mathbb{Z}/m\mathbb{Z}) \) 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 \( E[m^n] \xrightarrow{l^n} E[m^{n-1}] \rightarrow \cdots \rightarrow E[l] \xrightarrow{l} 0 \)

Definition 5.1. For 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 \( p_{E,l} : G_K \rightarrow \text{Aut}(E[l]) \cong \text{GL}_2(\mathbb{Z}/l\mathbb{Z}) \).

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

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

We have the Weil pairing: \( \epsilon([,]) : E[m] \times E[m] \rightarrow \mu_m \) (Where \( \mu_m \) 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

\[
\sigma e[P, Q] = e[\sigma P, \sigma Q] = e[aP + cQ, bP + dQ] = e[P, P]^{ab} e[P, Q]^{ad} e[Q, P]^{cd} e[Q, Q]^{cd} e[P, Q]^{ad - bc}.
\]

But from \( \sigma(\zeta_l) = \zeta_l^{\epsilon_l(\sigma)} \), 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 $G_{\mathbb{F}_p} = \text{Gal}(\mathbb{F}_p/\mathbb{F}_p)$ and consider the short exact sequence $1 \to I \to G_{\mathbb{Q}_p} \to G_{\mathbb{F}_p} \to 1$ where $I = \{\sigma \in G_{\mathbb{Q}_p} : \sigma = 1\}$. 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 $Q_5(\zeta_8) = Q_5(\zeta_3)$, unramified), $E_1 : y^2 = x^3 - 1$ and $E_2 : y^2 = (x - 1)(x^2 - 5)$.

Over $\mathbb{F}_5$ we get $E_1 : y^2 = x^3 - 1$ (curve of good reduction) and $E_2 : y^2 = x^3 - x^2$ (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 $Q_5(E_1[2])$ is unramified $E_2[2] = \{0, (1, 0), (\sqrt{5}, 0), (-\sqrt{5}, 0)\}$ so in $Q_5(\sqrt{5})$ ramified.

\[
\begin{align*}
Q_5(E[4]) & \quad Q_5(E[16]) & \quad Q_5(\sqrt{5}) \\
Q_5(E[2]) & \quad Q_5(\zeta_8) & \quad Q_5(\sqrt{5}) \\
Q_5 & \quad Q_5 & \quad Q_5
\end{align*}
\]

Recall the definition of the local polynomial $P_p(\rho_{E,l}, T) = \det(1 - \text{Frob}_p^{-1}T)(V_lE^*)^l$.

**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 \[\square\]

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 $\epsilon_p(\text{Frob}_p) = p = \det \rho(\text{Frob}_p)$. Hence Frob$_p$ is a $2 \times 2$ matrix with determinant $p$.

**Fact.**

- $Q \in E(\mathbb{F}_p) \iff \text{Frob}_p(Q) = Q$, $\#E(\mathbb{F}_p) = \#\ker(1 - \text{Frob}_p)$. But $1 - \text{Frob}_p$ is separable implies that $\ker(1 - \text{Frob}_p) = \deg(1 - \text{Frob}_p)$

- If $\psi \in \text{End}(E)$, then $\text{tr}(\psi) = 1 + \deg \psi - \deg(1 - \psi)$. Hence $\text{tr}(\text{Frob}_p) = 1 + p - \#E(\mathbb{F}_p) =: a_p$. So the characteristic polynomial of Frob$_p$ is $T^2 - aT + p$

Now $(V_lE^*)^l = V_lE^*$, so $P_p(T) = 1 - aT + pT^2$.

**Example.** $E_1 : y^2 = x^3 - 1$, $E_1(\mathbb{F}_5) = \{0, (\pm 2, 0), (1, 0), (3, \pm 1)\}$, 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 Frob$_p \to \begin{pmatrix} 0 & -5 \\ 1 & 0 \end{pmatrix}$.

**Multiplicative Reduction:**

Suppose the reduction is split multiplicative. Recall $E/C \cong C/(Z + \tau Z)^{\exp} C^*/q^{\mathbb{Z}}$ (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 $0 \neq q \in \mathbb{Z}_p$ such that $E \cong E_0 : y^2 + xy = x^3 + a_4(q)x + a_6(q)$ where $a_4(q)$ and $a_6(q)$ are power series in $\mathbb{Z}[[q]]$ which converges. Furthermore, $r(E_0) = 1/q + 744 + 196884q + \ldots$ and $\Delta(E_0) = q \prod (1 - q^n)^{24}$. Hence $E(\mathbb{Q}_p) \cong E_0(\mathbb{Q}_p) \cong \mathbb{Q}_p^*/q^{\mathbb{Z}}$ (as $G_{\mathbb{Q}_p}$-modules)*

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

So $Q(E[l^n])$ 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 $\mathbb{Q}_5(E[2^n]) \cong \mathbb{Q}_5 \left( \sqrt[5]{5}, \zeta_{2^n} \right)$ for all $n \geq 1$.

Action of $I$ on $E[l^n]$, so consider $\sigma(\zeta_l) = \zeta_l$ and $\sigma(\sqrt[l]{l}) = \zeta_l^t \sqrt[l]{l}$, 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 $\text{Frob}_p(\zeta_l) = \zeta_l^p$, and we know that the determinant is $p$, so $\text{Frob}_p \mapsto \begin{pmatrix} p & * \\ 0 & 1 \end{pmatrix}$. To determine $*$, we can use the previous section: $\rho_E = \rho \otimes \text{sp}(1)$, but $\rho$ is trivial, so $*$ is trivial and $\text{Frob}_p \mapsto \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$.

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

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

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

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

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 $V$)
- $\Lambda, \Lambda'$ are classes of lattices $L, L'$ with respect to homothety
- $\rho : G_K \to \text{GL}(V) \cong \text{GL}_2(\mathbb{Q}_l)$

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

$$G_K \twoheadrightarrow \text{GL}_2(\mathbb{Q}_l) \xrightarrow{j} \text{GL}_2(\mathbb{Z}_l)$$

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 $\rho$ is surjective mod $l$ then $\rho$ is surjective.

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

1. Vertices, $\Lambda := [l]$, where $\Lambda$ 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 $L \supset L' \supset llL$
Example. There are eight 2-isogony classes for the elliptic curves of conductor

\[
\begin{array}{c}
\bullet \\
\bullet \\
\bullet \\
\bullet \\
\bullet \\
\bullet \\
\bullet \\
\bullet \\
\end{array}
\]

6.1 Stable lattices and Galois representations

\[\rho : G_K \to \text{GL}_2(\mathbb{Q}_l)\]

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

Proposition 6.3. Every representation \(\rho\) 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 \(G_K\) finite index in \(G_K\) because \(G_K\) is compact. Hence the lattice generated by the sum is stable under \(G_K\).

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

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

Example. Let \(E_1, E_2\) be two elliptic curve over \(K\). Suppose there exists a \(K\) 2-rational isogeny \(E_1 \rightarrow E_2\). 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 \(\rho\) is irreducible.

Proposition 6.7. Let \(\rho\) 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 \(\text{PGL}_2(\mathbb{F}_l)\). Then a conjugate of \(H\) is one of the following groups:

1. A finite subgroup of the upper triangular matrices (Borel subgroup)
2. \(\text{PSL}_2(\mathbb{F}_r)\) or \(\text{PGL}_2(\mathbb{F}_r)\) 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 \( \rho_2 \) is surjective \mod 2 but not mod 4; and mod 4 but not mod 8
- Elkies showed that for \( l = 3, \rho_3 \) 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 \{a^n \}. Then

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

7 Galois Representations of Modular Curves (Chris Williams)

7.1 Modular Curves

Let \( \Gamma = \Gamma_0(N) \leq \text{SL}_2(\mathbb{Z}) \). Define the (compactified) modular curve to be \( X(\Gamma) = X_0(N) := \Gamma/\mathcal{H}^* \) 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

\[
\begin{array}{ccc}
\Gamma & x \rightarrow \gamma_p x \gamma_p^{-1} & \Gamma'' \\
\Gamma' & \Gamma & \Gamma \\
\end{array}
\]

This descent to

\[
\begin{array}{ccc}
X(\Gamma') & \xrightarrow{\alpha} & X(\Gamma'') \\
X(\Gamma) & \xrightarrow{\pi_1} & X(\Gamma) \\
X(\Gamma) & \xrightarrow{\pi_2} & X(\Gamma) \\
\end{array}
\]

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

7.2 Picard Groups

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

If \( \phi \) is a “nice” map \( X \rightarrow Y \), then we get maps on the Picard group as follows:

- **Pushforward:** \( \phi_* : \text{Pic}(X) \rightarrow \text{Pic}(Y) \) defined as \( \sum_x n_x[x] \mapsto \sum_x n_x[\phi(x)] \)
- **Pullback:** \( \phi^* : \text{Pic}(Y) \rightarrow \text{Pic}(X) \) 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 \( \text{Pic}(Y) \) \( \deg(\phi) = \phi_* \circ \phi^* \).

**Remark.** The action of \( T_p \) on \( \text{Div}(X_0(N)) \) descend to \( \text{Pic}(X_0(N)) \).

\( \text{Pic}(X_0(N)) \) “is” an abelian variety of dimension \( g = \text{genus}(X_0(X)) = \dim_{\mathbb{C}} S_2(\Gamma_0(N)) \).
7.3 Eichler-Schimura

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

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 $X_0(N)/\mathbb{Z}[\frac{1}{N}]$ to $\mathbb{F}_p$.

- There is a map $\overline{T}_p$ on $\text{Pic}(\overline{X}_0(N))$ making the following commute:

$$
\begin{array}{ccc}
\text{Pic}(X_0(N)) & \xrightarrow{T_p} & \text{Pic}(\overline{X}_0(N)) \\
\downarrow & & \downarrow \\
\text{Pic}(\overline{X}_0(N)) & \xrightarrow{T_p} & \text{Pic}(\overline{X}_0(N))
\end{array}
$$

**Theorem 7.2** (Eichler-Shimura). $\overline{T}_p = \sigma_p + \sigma_p^*$ as endomorphism of $\text{Pic}(\overline{X}_0(N))$.

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

2. The natural surjection (for $p \nmid lN$) $\text{Pic}(X_0(N)_{\mathbb{Q}})[l^n] \rightarrow \text{Pic}(\overline{X}_0(N))[l^n]$ 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 $\text{Pic}(X_0(N))$ is $\text{T}_l\text{Pic}(X_0(N)) = \lim_{\leftarrow n} \text{Pic}(X_0(N))[l^n] \cong \mathbb{Z}_l^{2g}$.

$G_{\mathbb{Q}} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the points of $X_0(N)$ in the natural way. This gives a natural action of $G_{\mathbb{Q}}$ on $\text{Div}(X_0(N))$, 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 $\text{Pic}(X_0(N))$. The action is linear so preserves $\text{Pic}(X_0(N))[l^n]$ for all $l$ and $n$. This action is compatible with the connecting maps: $\text{Pic}(X_0(N))[l^{n+1}] \rightarrow \text{Pic}(X_0(N))[l^n]$. Thus we get an action on $\text{T}_l\text{Pic}(X_0(N))$.

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

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

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

2. If $\mathcal{P}|p$ any Frobenius element, then $\rho_{X_0(N),l}(\text{Frob}_p)$ satisfies $X^2 - T_pX + p = 0$.

Proof.
1. We have a commutative diagram

$$D_p \xrightarrow{\rho_{X_0(N), t}} \text{Aut}(\text{Ta}_1\text{Pic}(X_0(N)))$$

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

2. We have a commutative diagram

$$ \begin{array}{ccc} 
\text{Pic}(X_0(N))[l^n] & \xrightarrow{T_p} & \text{Pic}(X_0(N))[l^n] \\
\downarrow & & \downarrow \\
\sigma_p + \sigma_p^* & \xrightarrow{\sigma_p + \sigma_p^*} & \text{Pic}(X_0(N))[l^n] 
\end{array} $$

we can describe the lifts of $\sigma_p$ and $\sigma_p^*$. $\text{Frob}_p$ is a lift of $\sigma_p$ as $\sigma_p$ 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 $p\text{Frob}_p^{-1}$. So we get a commutative diagram:

$$ \begin{array}{ccc} 
\text{Pic}(X_0(N))[l^n] & \xrightarrow{\text{Frob}_p + p\text{Frob}_p^{-1}} & \text{Pic}(X_0(N))[l^n] \\
\downarrow & \cong \downarrow & \downarrow \\
\sigma_p + \sigma_p^* & \xrightarrow{\sigma_p + \sigma_p^*} & \text{Pic}(X_0(N))[l^n] 
\end{array} $$

Hence $T_p = \text{Frob}_p + p\text{Frob}_p^{-1}$. This holds for all $n$, hence it holds for $\text{Ta}_1\text{Pic}(X_0(N))$. So $\text{Frob}_p^2 - T_p\text{Frob}_p + p = 0$

8 Modular Galois Representations (Nicolas)

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

This week we use $\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\}$. Note that $\Gamma_0(N) \subset \Gamma_1(N)$, we have a map $\Gamma_0(N)/\Gamma_1(N) \rightarrow (\mathbb{Z}/N\mathbb{Z})^*$ defined by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \mod N$. Define $X_1(N) = (\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})) / \Gamma_1(N)$.

We have $\Gamma_0 \rightarrow \Gamma_0/\Gamma_1$ 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 $J_1(N) = \text{Pic}^0(X_1(N))$, let $l \in \mathbb{N}$ be a prime. We define $T_lJ_1(N) = \lim_{\leftarrow n} J_1(N)[l^n]$ and $V_lJ_1(N) = T_lJ_1(N) \otimes \mathbb{Q}$.

**Theorem 8.1.** $G_Q \otimes V_lJ_1(N)$ afforded $\rho_{X_1(N), t} : G_Q \rightarrow \text{GL}_2(\mathbb{Q}_l)$ (where $g = \text{genus of } X_1(N)$) unramified at $lN$. For all $p \mid lN$ we have $\rho_{X_1(N), t}(\text{Frob}_p)$ satisfies $X^2 - T_pX + p(p) = 0$.

Actually $V_lJ_1(N)$ is a free $(\mathbb{T} \otimes \mathbb{Q}_l)$-module of rank 2, so $\rho_{X_1(N), t} : G_Q \rightarrow \text{GL}_2(\mathbb{T} \otimes \mathbb{Q}_l)$ and the characteristic polynomial of $\rho_{X_1(N), t}(\text{Frob}_p)$ is $X^2 - T_pX + p(p)$.

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 $D[N]$, $\mathcal{N}_k(N) \subseteq S_k(\Gamma_1(N))$.

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

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

17
• For all $\sigma \in G_Q$, $f^\sigma = q + \sum \sigma(a_n)q^n$ with $\sigma(a_n) \in \mathcal{N}_k(N)$. char$^\sigma = \sigma \circ \epsilon$

Pick $f \in \mathcal{N}_2(N)$ with $f = \sum a_n q^n$. Define $I_f = \{ T \in \mathbb{T} | T \gamma = 0 \} \subset \mathbb{T}$. 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 $A_f = J_1(N)/I_fJ_1(N)$. It is an abelian variety over Q of dimension $d = [K_f : \mathbb{Q}]$.

**Theorem 8.2.** $J_1(N) \sim \prod_{D | N, F \in G_Q \backslash \mathcal{N}_2(D)} A^\rho_1(N/D)$. And actually $V_1J_1(N) \cong \prod_{D | N, F \in G_Q \backslash \mathcal{N}_2(D)} V_1A^\rho_1(N/D)$ as $G_Q$-modules

$K_1 \otimes \mathbb{Q}_l \cong \prod_{\ell \mid p} K_{f, \ell}$, therefore

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

8.1 Residual maps

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

**Example.** Let $\rho = \left( \begin{array}{cc} \chi & \psi \\ 0 & \chi \end{array} \right) \sim \left( \begin{array}{cc} \chi & \psi \\ 0 & \chi \end{array} \right)$ but reduced mod $\ell$ we have $\left( \begin{array}{cc} \chi & \psi \\ 0 & \chi \end{array} \right)$.

**Definition 8.4.** Let $\rho : G \to \text{GL}(V)$ 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 - Nabbitt). Let $\xrightarrow{\rho_1} \xrightarrow{\rho_2} \text{GL}(V)$ 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 $\ell \mid l$ in $K_f$, there exists $\rho_{f, \ell}: G_Q \to \text{GL}_2(K_{f, \ell})$ unramified outside in $\mathbb{N}$. We have that the characteristic polynomial of $\rho_{f, \ell} (\text{Frob}_p)$ is $X^2 - \alpha_p X + p\epsilon(p)$

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

The last step relied on: for all $\gamma = \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \Gamma_0(N), f(\gamma z) = \epsilon(d)(cz + d)^k f(z)$. In particular $\gamma = \left( \begin{array}{cc} 1 & 1 \\ 0 & 1 \end{array} \right)$ in $\Gamma_0$ so $\epsilon(-1)(-1)^k = +1$.

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

8.3 Weight 1

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

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

1. There exists $\overline{\rho}_{f, \ell}$ for infinitely many $\ell$.
2. $\{a_p, \text{pprime}\}$ is “almost finite”
3. If \( G_l = \text{Im} \bar{\rho}_{f,l} \subset \text{GL}_2(\mathbb{F}_l) \) 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 \( \text{GL}_2(\mathbb{C}) \). This gives \( \rho_{f,l} \) to representations in \( \text{GL}_2(\mathbb{C}) \).

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 \( E = \mathbb{Q}(\{a_n\}) \), \( \epsilon_f \) 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 \( \lambda \)-adic representation \( \rho_{f,\lambda} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(E_{\lambda}) \) where \( \lambda \subset \mathcal{O}_E \) and \( E_{\lambda} \) is the completion of \( E \) at \( \lambda \). We have \( \rho_{f,\lambda} \) is irreducible and \( \forall \rho \in \mathcal{O}_E \), \( \text{Tr}(\rho_{f,\lambda}(\text{Frob}_p)) = a_p \) and \( \det(\rho_{f,\lambda}(\text{Frob}_p)) = \epsilon_f(p) \cdot p^{k-1} \). To \( \rho_{f,\lambda} \) we can associate \( \rho_{f,\lambda} : G_{\mathbb{Q}} \to \text{GL}_2(\mathbb{F}_l) \) where \( \mathbb{F} = \mathcal{O}_{E_{\lambda}}/\lambda \) and this representation is only defined up to semisimplification.

Let \( \rho : G_{\mathbb{Q}} \to \text{GL}_2(\overline{\mathbb{F}}_l) \) the question is when is \( \rho \equiv \rho_{f,\lambda}^{\text{ss}} \).

“Serre” A necessary and sufficient condition is that \( \rho \) is odd if \( \rho \) is semisimple.

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

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

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

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

Remark. Buzzard generalised the above for the case \( l = 2 \).

Theorem 9.3. Suppose that \( \rho \) 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 \( \rho \) arises from \( S_2(\Gamma_1(N)) \).

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 (Edixhoven). Let \( \gcd(N, l) = 1 \) and assume \( \rho \) arises from \( S_k(\Gamma_1(N)) \) then \( \rho \) 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 \( \rho \) 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 \( \chi \) is the mod \( l \) Cyclotomic character.

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

- \( N_1 = \{ N \mid \gcd(N, l) = 1, \rho \text{ arises from } S_k(\rho)(\Gamma_1(N)) \} \)
- \( N_2 = \{ N \mid \gcd(N, l) = 1, \rho \text{ arises from } \Gamma_1(N) \} \)
- \( N_3 = \{ N \mid \gcd(N, l) = 1, \rho \text{ arises from } \Gamma_1(N^\alpha), \alpha > 0 \} \)
- \( N_4 = \{ N \mid \gcd(N, l) = 1, \rho \text{ arises from } S_2(\Gamma_1(N^2)) \} \)

Theorem 9.6. If \( l \geq 5 \) then the four sets \( N_1, N_2, N_3 \) and \( N_4 \) 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 \( \rho \) 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 \( S_2(\Gamma_1(N)) \). Now tensoring with \( \chi^i \) changes the level of a modular form but not the weight. Look at \( \chi^i \) as a Dirichlet character, \( f : \overline{\rho_{f,\lambda}} \cong \rho \otimes \chi^i \) then consider \( f \otimes \chi^{-i} \in S_2(\Gamma_1(N^2)) \). So \( \rho = (\rho \otimes \chi^i) \otimes \chi^{-i} \) arises from \( S_2(\Gamma_1(N^2)) \).

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** (Livné). Suppose \( \rho \) arises from \( \Gamma_1(N) \) then \( N(\rho)||N \).

Let \( f \) be an eigenform giving rise to \( \rho \). 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 \( \rho \).

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 \( \rho_p : \text{Gal}(\overline{Q}/Q_p) \rightarrow GL_2(Q_l) \) 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 \( n_{\overline{\rho}_p} = n_p = \dim(V) - \dim \left( V^I \right) + n_{\overline{\rho}_p,\text{wild}} \). We know that \( n_{\rho_p,\text{wild}} = n_{\overline{\rho}_p,\text{wild}} \), we also know that \( \dim V^I \geq \dim V^I \), so \( n_p \leq n_p \). We want to study when \( \pi_p < n_p \).

**Theorem 9.8.** The representation \( \rho_p \) which can degenerate (i.e., \( \pi_p < n_p \)) can be one of the following

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

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 \( p|N/N(\overline{\rho}_{f,\lambda}) \) there exists a Dirichlet character \( \phi \) 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 \( M = N/\prod p \) such that \( p|N/N(\overline{\rho}_{f,\lambda}) \).