Galois Representation.
$\overline{Q} = \text{algebraic closure of } Q$.
$G_Q := \text{Gal}(\overline{Q}/Q)$.

If $F$ is a field, $G_F := \text{Gal}(F/F)$.

Galois representation = representation of $G_Q$ or $G_F$.

Fix $\overline{Q} \rightarrow \overline{Q}_p \rightarrow$
$\text{Gal}(\overline{Q}_p/\mathbb{Q}_p) \rightarrow G_Q$

$\downarrow$

$G_{\overline{Q}_p} \leftarrow \text{decomposition group at } p.$

Given a representation
$p : G_Q \rightarrow \text{GL}_n(K),$
restriction gives $p|_{G_{\overline{Q}_p}} : G_{\overline{Q}_p} \rightarrow \text{GL}_n(K)$.
Arm: study such representations of $G_\mathbb{Q}$ and their restrictions to the Gal.

**Example**

Fix $p > 2$ prime.

$\mathbb{Q}(\sqrt{p})/\mathbb{Q}$. Ramified at $p$, and possibly at 2.

$x: G_\mathbb{Q} = \text{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q}) \to \text{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q})$.

$x: G_\mathbb{Q} \to \pm 13$.

Take $l \neq 2, p$. Then $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ is unramified at $l$.

Then we have a canonical element $F_{ijl} \in \text{Gal}(\mathbb{Q}(\sqrt{p})/\mathbb{Q})$, lifting the mod $l$ Frobenius.
\[ X(\text{Frob}_l) = \pm 1. \text{ When is } X = 1? \]
\[ X(\text{Frob}_l) = 1 \iff \text{Frob}_l (\sqrt{p}) = \sqrt{p} \]
\[ \iff (\sqrt{p})^2 = \sqrt{p} \text{ in } \overline{\mathbb{Q}} \]
\[ \iff \sqrt{p} \in \overline{\mathbb{Q}} \]
\[ \iff p \text{ is a quadratic residue mod } l. \]

i.e. \[ X(\text{Frob}_l) = \left( \frac{p}{l} \right). \]

Assume \[ p \equiv 1 \pmod{4}. \] Then \[ \mathbb{Q}(\sqrt{p})/\mathbb{Q} \]

is only ramified at \( p \), and it's the

unique quadratic field with this property.

\[ \mathbb{Q}(\sqrt{3p})/\mathbb{Q} \]

is also ramified only at \( p \).

↑

primitive \( p \)th root of 1

\[ \mathbb{Q}(\sqrt{3p})/\mathbb{Q} \] is Galois, with Galois gp
\[ \text{Gal} \left( \mathbb{Q}(\sqrt[3]{p}) / \mathbb{Q} \right) \cong \left( \mathbb{Z}/p\mathbb{Z} \right)^{\times} \]
\[ (3_p \mapsto 3^{a}) \leftrightarrow a \pmod{p}. \]

In particular, this is cyclic of even order, so \( \mathbb{Q}(\sqrt[3]{p}) / \mathbb{Q} \) necessarily contains a quadratic field only ramified at \( p \), i.e. \( \mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\sqrt[3]{p}) \).

\[
X : \mathcal{O}_\mathbb{A} \to \text{Gal} \left( \mathbb{Q}(\sqrt[3]{p}) / \mathbb{Q} \right) \to \text{Gal} \left( \mathbb{Q}(\sqrt[p]{p}) / \mathbb{Q} \right) \\
\frac{12}{12} \left( \mathbb{Z}/p\mathbb{Z} \right)^{\times} \to \frac{12}{12} \left( \mathbb{Z}/p\mathbb{Z} \right)^{\times} \to \frac{12}{12} \mathbb{Z} / 15.
\]

Since \( \left( \mathbb{Z}/p\mathbb{Z} \right)^{\times} \) is cyclic, so \( X \) is the unique non-trivial finite quadratic character of \( \left( \mathbb{Z}/p\mathbb{Z} \right)^{\times} \), and the kernel of \( X \) is just the quadratic residue in \( \left( \mathbb{Z}/p\mathbb{Z} \right)^{\times} \).

\[ \text{Frob}_2(3p) = 3^p \]

So \( \text{Frob}_2 \leftrightarrow 2 \pmod{p} \in \left( \mathbb{Z}/p\mathbb{Z} \right)^{\times}. \)
$X(F_{p^2}) = 1 \iff l$ is a quadratic residue mod $p$. \\
\text{ie. } X(F_{p^2}) = \left( \frac{l}{p} \right). \\
\text{So } \left( \frac{p}{l} \right) = X(F_{p^2}) = \left( \frac{l}{p} \right). \\
\text{Exercise prove the rest of quadratic reciprocity in this way.} \\
\text{Also generalize this.} \\
\text{Started with a Galois representation,} \\
\text{and observed that it encoded arithmetic information.} \\
\text{Then computed the local information in terms of something else.} \\
\text{e.g. } \prod_{n=1}^{\infty} \left(1-q^n\right)^2 \left(1-q^{11n}\right)^2 \\
q = e^{2\pi i} \text{ eigenform at 2, level } \Gamma_0(11).
\begin{align*}
&= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 \\
&\quad - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + q^{13} + \cdots \\
E &: y^2 + y = x^3 - x^2 \\
\text{Coefficients in the } q\text{-expansion.}
\end{align*}

E is modular, corresponding to \( f \).

Where is the Galois representation?

**Answer**: use the action of \( G_\mathbb{Q} \) on torsion points of \( E \).

For any \( N \geq 1 \), let \( E[N] = \Sigma^{N}_{V \text{-torsion points of } E} \).
$E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$ as an abelian group

The coordinates of points in $E[N]$ are in $\mathbb{Q}$, so $Ga \subset E[N]$

i.e. $p: Ga \rightarrow GL_2(\mathbb{Z}/N\mathbb{Z})$

Fact If $\ell \nmid \#N$, then $p_\ell$ is unramified at $\ell$, and $trp_\ell(Frob_\ell) = a_\ell \pmod{N}$.

If determined by the $a_\ell$ $p_\ell$ is determined up to isomorphism by $trp_\ell(Frob_\ell)$ \[ \text{user $\{Frob_\ell\}_{\ell \neq 11}$ are dense in $Ga \leftarrow Cebotararu$} \]

Consider all of these representations $p_\ell : Ga \rightarrow GL_2(\mathbb{Z}/N\mathbb{Z})$ at once.

By CRT, enough to consider $N = p^r, r \geq 1.$
Then the representations compile together to give

$$\rho_{E,p} : G \rightarrow GL_2(\mathbb{Z}[\frac{1}{p}])$$

$$= GL_2(\mathbb{Z}_p).$$

Continuous w.r.t. natural topologies: proximity topology on $G$, and $p$-adic topology on $GL_2(\mathbb{Z}_p)$.

Consider all of the $\rho_{E,p}$ as $p$ varies: get a compatible system or compatible family of Galois representations

$$\rho_{E,p} : G \rightarrow GL_2(\mathbb{Z}_p).$$

Compatible: 3 common unramification set $\mathcal{I}_{113}$, in the sense that if $l \neq 11, p$ then $\rho_{E,p}$ is unramified at $l$, and
tr \( PE, p \) (Frb.L) is independent of \( p \neq 11, \ell \).

In particular, \( tr PE, p \) (Frb.L) \( \in \mathbb{Z} \).

The property of being in a compatible system is restrictive: conjecturally, it implies that the representation "come from geometry" + "come from automorphic forms". Aim of modularity lifting theorems: show that Galois representations do indeed come from automorphic forms. [It in some cases, then declares that they come from geometry].