Galois Representations

Samir Siksek

12 July 2016

Representations of Elliptic Curves—Crash Course

- $E/\mathbb{Q}$ elliptic curve;
- $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$;
- p prime.

Fact: There is a $\tau \in \mathbb{H}$ such that

$$E(\mathbb{C}) \;\cong\; \frac{\mathbb{C}}{\mathbb{Z} + \tau\mathbb{Z}} \;\cong\; \frac{\mathbb{R}}{\mathbb{Z}} \times \frac{\mathbb{R}}{\mathbb{Z}}.$$

Easy to see: $E[p] \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ (2-dim'l $\mathbb{F}_p$-vector space).

$G_{\mathbb{Q}}$ acts on $E[p]$:

$$\overline{\rho}_{E,p} \ : \ G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p).$$

Example

Suppose P is a **rational** point of order p. Choose $Q \in E[p]$ so that P, Q are an $\mathbb{F}_p$-basis. For any $\sigma \in G_{\mathbb{Q}}$,

$$\sigma(P) = P, \qquad \sigma(Q) = b_\sigma P + d_\sigma Q.$$

Hence

$$\overline{\rho}_{E,p}(\sigma) = \begin{pmatrix} 1 & b_\sigma \\ 0 & d_\sigma \end{pmatrix}.$$

Conclusion: E has p-torsion defined over $\mathbb{Q}$ iff

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} 1 & * \\ 0 & \psi \end{pmatrix}, \qquad (\psi : G_{\mathbb{Q}} \to \mathbb{F}_p^* \text{ is a character}).$$

Example

Suppose E has a p-isogeny $\phi : E \to E$ defined over $\mathbb{Q}$. Then $\mathrm{Ker}(\phi) = \langle P \rangle$ is a cyclic subgroup of order p.
Choose $Q \in E[p]$ so that P, Q are an $\mathbb{F}_p$-basis. For any $\sigma \in G_{\mathbb{Q}}$,

$$\sigma(P) = a_\sigma P, \qquad \sigma(Q) = b_\sigma P + d_\sigma Q.$$

Hence

$$\overline{\rho}_{E,p}(\sigma) = \begin{pmatrix} a_\sigma & b_\sigma \\ 0 & d_\sigma \end{pmatrix}.$$

Conclusion: E has p-isogeny defined over $\mathbb{Q}$ iff

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}, \qquad (\psi_1,\ \psi_2 : G_{\mathbb{Q}} \to \mathbb{F}_p^* \text{ are characters}).$$

i.e. $\overline{\rho}_{E,p}$ **is reducible**.

Mazur's Isogeny Theorem

Theorem (Mazur)

Let E be an elliptic curve over $\mathbb{Q}$. For $p > 163$, the elliptic curve E has no p-isogenies defined over $\mathbb{Q}$.

Equivalent theorem:

Theorem (Mazur)

Let E be an elliptic curve over $\mathbb{Q}$. If $p > 163$, the mod p representation $\overline{\rho}_{E,p}$ is irreducible.

Exercise

Denote by ζ_p *a primitive* p*-th root of unity. Define the* **mod** p **cyclotomic character**

$$\chi_p : G_{\mathbb{Q}} \to \mathbb{F}_p^*, \qquad \sigma(\zeta_p) = \zeta_p^{\chi_p(\sigma)}.$$

(i) *Show that* χ_p *is a character (i.e. a homomorphism).*

(ii) *Let* $\sigma \in G_{\mathbb{Q}}$ *denote complex conjugation. Show that* $\chi_p(\sigma) = -1$.

(ii) *Let* $\ell \neq p$ *be a prime, and let* σ_ℓ *be a Frobenius element at* ℓ*. Show that* $\chi_p(\sigma_\ell) \equiv \ell \pmod{p}$.

(iv) *Show that for all* $\sigma \in G_{\mathbb{Q}}$ *we have*

$$\det(\overline{\rho}_{E,p}(\sigma)) = \chi_p(\sigma).$$

Hint: *Think about the Weil pairing.*

Note that for complex conjugation σ we have

$$\det(\overline{\rho}_{E,p}(\sigma)) = -1.$$

We say that $\overline{\rho}_{E,p}$ is **odd**.

Galois Representations from Modular Forms

Theorem (Eichler, Shimura, Deligne)

Let f be a newform of level N and weight $k \geq 2$, and write $f = q + \sum c_n q^n$. Let $K = \mathbb{Q}(c_1, c_2, \dots)$. Let p be a rational prime. Then there is some prime ideal $\mathfrak{P} \mid p$ of $\mathcal{O}_K$ and a representation:

$$\overline{\rho}_{f,\mathfrak{P}} \; : \; G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_{\mathfrak{P}}), \qquad \mathbb{F}_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}.$$

Moreover, if $\ell \nmid Np$ is a prime, and $\sigma_\ell \in G_{\mathbb{Q}}$ is the Frobenius element at ℓ then

$$\mathrm{Tr}(\overline{\rho}_{f,\mathfrak{P}}(\sigma_\ell)) \equiv c_\ell \pmod{\mathfrak{P}}.$$

Serre's Modularity Conjecture

Theorem (Khare and Wintenberger)

Let p be and odd prime and let $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$ (here $q = p^r$) be an odd irreducible representation. Then there is a newform f of level $N = N(\overline{\rho})$ (given by an explicit recipe) and a weight $k = k(\overline{\rho})$ (given by an explicit recipe) and a prime ideal $\mathfrak{P} \mid p$ such that

$$\overline{\rho} \sim \overline{\rho}_{f,\mathfrak{P}}.$$

Theorem (Khare and Wintenberger)

Let p be and odd prime and let $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_q)$ (here $q = p^r$) be an odd irreducible representation. Then there is a newform f of level $N = N(\overline{\rho})$ (given by an explicit recipe) and a weight $k = k(\overline{\rho})$ (given by an explicit recipe) and a prime ideal $\mathfrak{P} \mid p$ such that

$$\overline{\rho} \sim \overline{\rho}_{f,\mathfrak{P}}.$$

- We say $\overline{\rho}$ is **unramified** at ℓ if $\overline{\rho}(I_\ell) = 1$ where $I_\ell \subset G_{\mathbb{Q}}$ is the inertia subgroup at ℓ.
- The primes $\ell \mid N$ are the ramified primes $\ell \neq p$.
- $k = 2$ if $p \nmid \#\overline{\rho}(I_p)$.

Ribet's Theorem

- $E/\mathbb{Q}$ elliptic curve;
- p prime.

We know that $\overline{\rho}_{E,p} \; : \; G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_p)$ is odd.

Suppose E has no p-isogenies. Then $\overline{\rho}_{E,p}$ is irreducible.

By Serre's modularity conjecture, there is a newform f of weight k_p and level N_p and a prime ideal $\mathfrak{P} \mid p$ such that $\overline{\rho}_{E,p} \sim \overline{\rho}_{f,\mathfrak{P}}$ (this is equivalent to $E \sim_p f$).

Goal: Demystifying the recipe for N_p. In particular, we want to show that if $\ell \,||\, N$ and $p \mid \mathrm{ord}_\ell(\Delta)$ then $\overline{\rho}_{E,p}$ is unramified at ℓ.

Complex Parametrization Revisited

Recall for $E/\mathbb{C}$, we have

$$E(\mathbb{C}) \;\cong\; \frac{\mathbb{C}}{\mathbb{Z}+\tau\mathbb{Z}}.$$

Let $q = \exp(2\pi i\tau)$. Then

$$E(\mathbb{C}) \cong \frac{\mathbb{C}}{\mathbb{Z}+\tau\mathbb{Z}} \;\cong\; \mathbb{C}^*/q^{\mathbb{Z}}, \qquad z + (\mathbb{Z}+\tau\mathbb{Z}) \mapsto \exp(2\pi i z)\cdot q^{\mathbb{Z}}.$$

The Tate Curve

Theorem (Tate)

Let ℓ be a prime, and E an elliptic curve with split multiplicative reduction at ℓ. Then there is $q \in \ell\mathbb{Z}_\ell$ such that

$$E(\overline{\mathbb{Q}_\ell}) \cong \overline{\mathbb{Q}_\ell}^\times / q^{\mathbb{Z}}$$

as G_ℓ-modules ($G_\ell = \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$).

- $p \neq \ell$ prime

Corollary

$$E[p] \cong \langle \zeta_p \rangle \times \langle q^{1/p} \pmod{q^{\mathbb{Z}}} \rangle \qquad \textit{as } G_\ell\textit{-modules.}$$

Corollary

$$E[p] \cong \langle \zeta_p \rangle \times \langle q^{1/p} \pmod{q^{\mathbb{Z}}} \rangle \qquad \textit{as } G_\ell\textit{-modules.}$$

If $\sigma \in G_\ell$ then

$$\sigma(\zeta_p) = \zeta_p^a, \qquad \sigma(q^{1/p}) = \zeta_p^b q^{1/p}, \qquad a, b \in \mathbb{F}_p.$$

Think of ζ_p and $q^{1/p}$ as an $\mathbb{F}_p$-basis for $E[p]$. The action of σ is given by

$$\overline{\rho}_p(\sigma) := \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}.$$

Obtain a representation

$$\overline{\rho}_p : G_\ell \to \mathrm{GL}_2(\mathbb{F}_p).$$

Image of Inertia

- $I_\ell \subset G_\ell$ inertia subgroup

As $p \neq \ell$, the extension $\mathbb{Q}_\ell(\zeta_p)/\mathbb{Q}_\ell$ is unramified, so

$$\sigma(\zeta_p) = \zeta_p, \qquad \text{for all } \sigma \in I_\ell.$$

So

$$\overline{\rho}_p(I_\ell) \leq \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{F}_p \right\} \qquad \text{(cyclic of order } p\text{)}.$$

The extension $\mathbb{Q}_\ell(q^{1/p})/\mathbb{Q}_\ell$ is unramified if and only if $p \mid \upsilon_\ell(q)$.

Lemma

- *If $p \mid \upsilon_\ell(q)$ then $\#\overline{\rho}_p(I_\ell) = 1$.*
- *If $p \nmid \upsilon_\ell(q)$ then $\#\overline{\rho}_p(I_\ell) = p$.*

The discriminant Δ of E is given by

$$\Delta = q \prod_{n \geq 1} (1 - q^n)^{24} \qquad \text{(observe } \upsilon_\ell(q) = \upsilon_\ell(\Delta)\text{)}.$$

Lemma

- *If* $p \mid \upsilon_\ell(\Delta)$ *then* $\#\overline{\rho}_p(I_\ell) = 1$.
- *If* $p \nmid \upsilon_\ell(\Delta)$ *then* $\#\overline{\rho}_p(I_\ell) = p$.

Conclusion: Let $E/\mathbb{Q}$ of conductor N. Suppose $\overline{\rho}_{E,p}$ is irreducible. By Serre's modularity conjecture, there is a newform f of level N_p and a prime ideal $\mathfrak{P} \mid p$ such that $\overline{\rho}_{E,p} \sim \overline{\rho}_{f,\mathfrak{P}}$. Let $\ell \mid\mid N$ (i.e. E has multiplicative reduction at N) and $p \mid \mathrm{ord}_\ell(\Delta)$ then the above tells us that $\ell \nmid N_p$.