Foray Into Galois Representations

Tyler Genao

July 31, 2020

Our plan for these slides:

1. See some examples of Galois representations in nature.
2. Define a **Galois representation.**
3. Define what it means for a Galois representation to be unramified.
4. End with a hallmark theorem in the theory of elliptic curves.

Some conventions:

- K is a number field;
- $\overline{K}$ is a fixed algebraic closure of K;
- $G_K := \mathrm{Gal}(\overline{K}/K)$ is the **absolute Galois group** of K.

First steps: roots of unity

- G_K acts on the roots of unity $\mu := \mu(\overline{K})$, e.g. the elements of finite multiplicative order:

$$\mu = \{\zeta \in \overline{K} : \exists n \in \mathbb{Z}^+ \ \zeta^n = 1\}.$$

- For $\sigma \in G_K$, the group action is via

$$\sigma : \zeta \mapsto \sigma(\zeta).$$

- This restricts to an action on the n'th roots of unity $\mu_n := \{\zeta \in \overline{K} : \zeta^n = 1\}$:

$$\zeta^n = 1 \Rightarrow (\sigma\zeta)^n = 1.$$

- **Q:** Which elements of $\sigma \in G_K$ act trivially on μ_n?
- **A:** Those which fix a primitive n'th root of unity: e.g., $\sigma(\zeta) = \zeta$ for all $\zeta \in \mu_n$.
- We see that such σ are precisely those in $\mathrm{Gal}(\overline{K}/K(\zeta_n))$ where $K(\zeta_n)$ is the n-cyclotomic field, and ζ_n is a(ny) primitive n'th root of unity.
- Conclusion: G_K acts on μ_n, and cuts out the Galois extension $K(\zeta_n)/K$.

Second steps: torsion points on elliptic curves

- An **elliptic curve** over a field K is the set of solutions to an equation of the form

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

where $\Delta_E := -16(4A^3 + 27B^2) \neq 0$.

- The set of $E(\overline{K})$ of all algebraic points, along with the "point at infinity" O, forms a group under a "geometric group law":

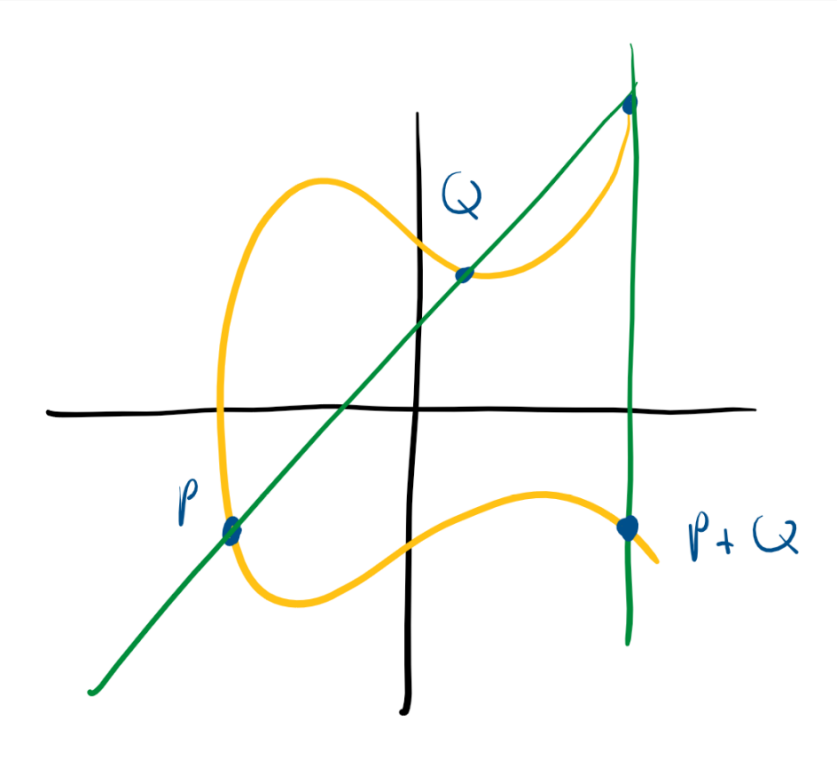

Figure: Group law on an elliptic curve.

- One can consider the subgroup of torsion points of E:

$$E[\text{tors}] := \{P \in E : \exists n \in \mathbb{Z}^+ \ nP = O\}.$$

- G_K acts on $E[\text{tors}]$: for $\sigma \in G_K$ and $P := (x, y) \in E$,

$$\sigma(P) := (\sigma(x), \sigma(y)).$$

- "Addition is rational":

$$n(\sigma(P)) = \sigma(nP).$$

So G_K sends n-torsion to n-torsion.

- Focus our attention on the n-torsion points:

$$E[n] := \{P \in E : nP = O\}.$$

- The fixed field of this action is the **n-division field**

$$K(E[n]) := K(\{P\}_{P \in E[n]}) = K(\{x, y : (x, y) \in E[n]\}).$$

- Conclusion: G_K acts on $E[n]$, and cuts out the Galois extension $K(E[n])/K$.

Summary

- So G_K acts on torsion subgroups of various groups, and cuts out important fields like cyclotomic fields and division fields.
- Fixed fields such as $\mathbb{Q}(\zeta_n)$ and $K(E[n])$ satisfy interesting properties.
- **Kronecker-Weber**: every finite abelian extension of $\mathbb{Q}$ is contained in some $\mathbb{Q}(\zeta_n)$.
- **Néron-Ogg-Shafarevich**: an elliptic curve has good reduction at a prime $\mathfrak{p} \subseteq K$ iff

$$\rho : \mathrm{Gal}(K(E[n])/K) \hookrightarrow \mathrm{Aut}_{(\mathbb{Z}/n\mathbb{Z})}(E[n])$$

is *unramified* at $\mathfrak{p}$.

Galois representations: definitions

- A **group action** is a homomorphism from a group G to the symmetric group on a set X:

$$\rho : G \to \mathrm{Sym}(X).$$

- A **group representation** is a group homomorphism from a group G to the space of automorphisms of a k-linear vector space V:

$$\rho : G \to \mathrm{Aut}_k(V).$$

- A **Galois representation** is a continuous homomorphism from a Galois group $\mathrm{Gal}(L/K)$ to the space of automorphisms of a finite-dimensional vector space V over a normed field F:

$$\rho : \mathrm{Gal}(L/K) \to \mathrm{Aut}_F(V).$$

Warning! Number theory ahead.

Algebraic number theory I

- Let L/K be a finite Galois extension of number fields.
- A prime $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ of K factorizes in $\mathcal{O}_L$ has

$$\mathfrak{p}\mathcal{O}_L = \left(\prod_{i=1}^{r} \mathfrak{P}_i\right)^{e}.$$

  We call the number e the **ramification index** of $\mathfrak{p}$ in L.
- We call the degree $f := [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ the **inertial degree** of $\mathfrak{p}$ in $\mathcal{O}_K$.

- e and f show up in a related concept:
- Fix a prime $\mathfrak{P} \subseteq \mathcal{O}_L$ above $\mathfrak{p}$.
- Then $\mathbb{F}_{\mathfrak{P}} := \mathcal{O}_L/\mathfrak{P}$ is both a finite field and an extension of $\mathbb{F}_{\mathfrak{p}} := \mathcal{O}_K/\mathfrak{p}$.
- If $\sigma \in \mathrm{Gal}(L/K)$ is so that $\sigma(\mathfrak{P}) = \mathfrak{P}$, then σ induces an automorphism $\tilde{\sigma} : \mathbb{F}_{\mathfrak{P}} \to \mathbb{F}_{\mathfrak{P}}$ fixing $\mathbb{F}_{\mathfrak{p}}$:

$$\tilde{\sigma}(\alpha + \mathfrak{P}) := \sigma(\alpha) + \mathfrak{P}.$$

- Call $\tilde{\sigma}$ the reduction of σ mod $\mathfrak{P}$.

- Let $D_{\mathfrak{P}}$ be the **decomposition group**

$$D_{\mathfrak{P}} := \{\sigma \in \mathrm{Gal}(L/K) : \sigma(\mathfrak{P}) = \mathfrak{P}\}.$$

- We have a homomorphism by pointwise reduction:

$$\mathrm{red} : D_{\mathfrak{P}} \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}).$$

- The **inertia group** is the kernel of reduction:

$$I_{\mathfrak{P}} := \{\sigma \in D_{\mathfrak{P}} : \tilde{\sigma} = 1_{\mathbb{F}_{\mathfrak{P}}}\}.$$

- It is a fact that reduction is surjective. Therefore,

$$D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}).$$

- The sizes $|D_{\mathfrak{P}}| = ef$ and $|I_{\mathfrak{P}}| = e$.

- Call $\mathfrak{p} \subseteq K$ is **unramified** if $e = 1$.
- If $\mathfrak{p}$ is unramified, then $I_{\mathfrak{P}}$ is trivial and thus

$$\mathrm{red} : D_{\mathfrak{P}} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}).$$

- In particular, $D_{\mathfrak{P}}$ is cyclic and generated by the **Frobenius element**

$$\left[\frac{L/K}{\mathfrak{P}}\right] := \mathrm{red}^{-1}(\mathrm{Frob}_{\mathfrak{p}}) \in \mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}}),$$

  where

$$\mathrm{Frob}_{\mathfrak{p}} : \alpha \mapsto \alpha^{\#\mathbb{F}_{\mathfrak{p}}}$$

  is the Frobenius automorphism.

- **Fact:** the images $\rho\left(\left[\frac{L/K}{\mathfrak{P}}\right]\right)$ *topologically* generate $\rho(G_F)$.
  - If $\rho(G_F)$ is finite, we can drop *topologically*.

Ramification in Galois representations

- Consider a Galois representation

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

  which has *finite* image.
- Then our action cuts out the fixed field K^ρ. Our representation then becomes

$$\rho : \mathrm{Gal}(K^\rho/K) \hookrightarrow \mathrm{Aut}_F(V).$$

- So we are reduced to studying *finite* Galois representations.

- Let $\mathfrak{p} \subseteq K$ be a prime.
- Say our representation

$$\rho : \mathrm{Gal}(K^{\rho}/K) \hookrightarrow \mathrm{Aut}_F(V) \tag{1}$$

is **unramified at** $\mathfrak{p}$ if its restriction to the inertia group is trivial:

$$\rho(I_{\mathfrak{P}}) = \{I\}.$$

- If K^{ρ} is unramified at $\mathfrak{p}$, then so is (1).
- Thus, our Galois representation is ramified at only finitely many primes.

Mod n Galois representations, revisited

- Let us return to the Galois representation on the n-torsion of an elliptic curve $E_{/K}$:

$$\rho : \mathrm{Gal}(K(E[n])/K) \hookrightarrow \mathrm{Aut}_{(\mathbb{Z}/n\mathbb{Z})}(E[n]).$$

- The following theorem relates good reduction of E at a prime to ramification of its Galois representations:

Theorem (Néron-Ogg-Shavarevich).

For a prime $\mathfrak{p} \subseteq K$, E has good reduction at $\mathfrak{p}$ if and only if every mod n Galois representation $E[n]$ with $\mathfrak{p} \nmid n$ is unramified at $\mathfrak{p}$.

References

[1] Joseph Silverman, *The Arithmetic of Elliptic Curves*, second edition. Graduate Texts in Mathematics, 106, Springer, 2009.
[2] Gabor Wiese, *Galois Representations*, version of 13th February 2012. `www.math.uni/lu/~wiese/notes/GalRep.pdf`. 2012.