20.1 Galois representations attached to elliptic curves

Let E be an elliptic curve over a number field K. For each positive integer m we use $E[m]$ to denote the m-torsion subgroup of $E(\overline{K})$. The Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$ acts on $E[m]$, since the coordinates of $P \in E[m]$ are roots of the m-division polynomials whose coefficients lie in K. This yields the mod-m Galois representation

$$\rho_{E,m} \colon G_K \to \mathrm{Aut}(E[m]).$$

The abelian group $E[m] \simeq \mathbb{Z}/m\mathbb{Z} \bigoplus \mathbb{Z}/m\mathbb{Z}$ is a free $\mathbb{Z}/m\mathbb{Z}$ module of rank 2, hence its automorphism group is isomorphic to $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. After fixing a $\mathbb{Z}/m\mathbb{Z}$-module basis for $E[m]$ we obtain a linear representation

$$\rho_{E,m} \colon G_K \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Note that this representation depends on a choice of basis and is defined only up to conjugation. When m is a prime ℓ we have $\mathbb{Z}/\ell Z \simeq \mathbb{F}_\ell$ and can view this as a 2-dimensional $\mathbb{F}_\ell$-representation.

The multiplication-by-ℓ map $P \mapsto \ell P$ defines a surjective homomorphism $E[\ell^{n+1}] \to E[\ell^n]$ for each $n \in \mathbb{Z}_{\geq 0}$. These maps uniquely determine an inverse system that is used to define the ℓ-adic Tate module

$$T_\ell(E) := \varprojlim_n E[\ell^n],$$

which is a free $\mathbb{Z}_\ell$-module of rank 2. If we fix a basis (P_1, Q_1) for $E[\ell]$, we can then choose (P_2, Q_2) so that $\ell P_2 = P_1$ and $\ell Q_2 = Q_1$, since the multiplication-by-ℓ map defines a surjection $E[\ell^2] \twoheadrightarrow E[\ell]$ (it is a homomorphism whose kernel has cardinality $\#E[\ell] = \ell^2 = [E[\ell^2] : E[\ell]]$, so it must be surjective). Continuing in this fashion yields a compatible system of bases that allows us to identify $\mathrm{Aut}(T_\ell(E))$ with $\mathrm{GL}_2(\mathbb{Z}_\ell)$ and we have the ℓ-adic Galois representation

$$\rho_{E,\ell^\infty} \colon G_K \to \mathrm{Aut}(T_\ell(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell).$$

As above, the isomorphism with $\mathrm{GL}_2(\mathbb{Z}_\ell)$ depends on a choice of basis, so this representation is determined only up to conjugation in $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

More generally, for any $m, n \in \mathbb{Z}_{\geq 1}$ with $n|m$ the multiplication-by-(m/n) map defines a surjective homomorphism $E[m] \twoheadrightarrow E[n]$, yielding an inverse system of torsion subgroups ordered by divisibility, and we can consider the adelic Tate module

$$T(E) := \varprojlim_m E[m],$$

which is a free $\widehat{\mathbb{Z}}$-module of rank 2. Now $\widehat{\mathbb{Z}} \simeq \prod_\ell \mathbb{Z}_\ell$, so any choice of compatible systems of bases for all the ℓ-adic Tate modules $T_\ell(E)$ yields a compatible system of bases for $T(E)$ and we obtain the adelic Galois representation

$$\rho_E \colon G_K \to \mathrm{Aut}(T(E)) \simeq \mathrm{GL}_2(\widehat{\mathbb{Z}}) \simeq \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell),$$

which is again defined only up to conjugation on $\mathrm{GL}_2(\widehat{\mathbb{Z}})$.

Note that G_K and $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ are both profinite groups, hence topological groups, and the representation ρ_E is continuous in this topology (in other word, ρ_E is a morphism of topological groups, not just a morphism of groups). Both groups can be defined as inverse limits of finite groups, which we regard as topological groups equipped with the discrete topology, and the inverse limit is a topological group that is compact and totally disconnected (any two points can be separated by open sets that partition the space).

In the case of G_K this topology is the Krull topology, and we recall that Galois theory for infinite algebraic extensions requires that we restrict our attention to subgroups that are closed in the Krull topology: there is a one-to-one inclusion reversing correspondence between closed subgroups of G_K and algebraic extensions of K in $\overline{K}$, but this is not true if consider arbitrary subgroups; indeed, every subgroup of G_K with the same closure will have the same fixed field.

Under this correspondence, finite extensions of K in $\overline{K}$ correspond to finite index closed subgroups of G_K, which are necessarily also open subgroups, since their complement is a finite union of closed cosets, hence closed. Conversely, every open subgroup of G_K is a closed subgroup of finite index (it must have finite index because G_K is compact and cosets form an open subcover with no proper subcovers, and every open subgroup of a topological group is also closed, since it is the complement of the open set formed by the union of its cosets).

We are thus particularly interested in open subgroups $H \le \mathrm{GL}_2(\widehat{\mathbb{Z}})$. It follows from the definition of the topology of an inverse limit of discrete groups that every such H is the inverse image of its projection to $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ for some positive integer m; the least such m is the level of H. The inverse image of any finite subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ is an open subgroup, but note the same subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ can be obtained from infinitely many different values of m. However, if we restrict our attention to subgroups of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ that are not the inverse image of their projection to $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ for any $n|m$ we obtain a one-to-one correspondence with open subgroups of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of level m.

20.2 Complex multiplication

Theorem 20.1. *Let E/k be an elliptic curve with endomorphism ring $\mathrm{End}(E)$ and endomorphism algebra $\mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. Then $\mathrm{End}(E)$ is a free $\mathbb{Z}$-module of rank r that is an order in the $\mathbb{Q}$-algebra $\mathrm{End}^0(E)$ of dimension r and exactly one of the following holds:*

$r = 1$ $\mathrm{End}^0(E) = \mathbb{Q}$ *and* $\mathrm{End}(E) = \mathbb{Z}$*;*

$r = 2$ $\mathrm{End}^0(E)$ *is an imaginary quadratic field $\mathbb{Q}(\alpha)$ with $\alpha^2 < 0$*

$r = 4$ $\mathrm{End}^0(E)$ *is a non-split quaternion algebra $\mathbb{Q}(\alpha, \beta)$ with $\alpha^2, \beta^2 < 0$ and $\mathrm{char}(k) \neq 0$.*

Proof. See Theorem 12.17 in [1] □

When k is a number field only the first two possibilities can occur, and when $\mathrm{End}^0(E)$ is an imaginary quadratic field we say that E has complex multiplication. Such E are rare: for any fixed number field K the set $\{j(E) : \mathrm{End}(E) \neq \mathbb{Z}\}$ is finite, and even if we let K range over all number fields of degree at most d, we still obtain a finite set.

We should note that $\mathrm{End}(E)$ is not invariant under base change; any endomorphisms defined over K are necessarily defined over any extension L/K, but E may acquire additional endomorphisms over an extension L/K. If $\mathrm{End}(E_{\overline{K}})$ is an imaginary quadratic field then we say that E has potential complex multiplication, and in this case there is a unique minimal extension L/K of degree at most 2 for which $\mathrm{End}(E_L) = \mathrm{End}(E_{\overline{K}})$: we can take L to be the compositum of K and the imaginary quadratic field $\mathrm{End}(E_{\overline{K}})$.[1]

The endomorphism ring of $E_{\overline{K}}$ has a profound impact on the Galois representation ρ_E. If $\mathrm{End}(E)$ is an imaginary quadratic order $\mathcal{O}$ (so E has complex multiplication) then $E[m]$ is not just a free $(\mathbb{Z}/m\mathbb{Z})$-module of rank 2, it is also a free $\mathcal{O}/m\mathcal{O}$-module of rank 1. If we fix a basis $\langle P, Q\rangle = E[m]$ and consider the orbit of P under the action of $\mathrm{End}(E) \simeq \mathcal{O} = [1\tau]$, we obtain all

[1] This fact is specific to elliptic curves; for a general abelian variety A/K whose geometric endomorphism algebra is a field F, the minimal field L for which $\mathrm{End}(A_L) = \mathrm{End}(A_{\overline{K}})$ is not necessarily KF.

of $E[m]$. The endomorphisms $\alpha \in \mathrm{End}(E)$ are defined over K, hence compatible with the action of G_K, and this implies that we can actually view the mod-m representation as a homomorphism

$$\rho_{E,m} \colon G_K \to \mathrm{GL}_1(\mathcal{O}/m\mathcal{O}) \simeq (\mathcal{O}/m\mathcal{O})^\times.$$

This implies that the image of $\rho_{E,m}$ is an abelian subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, which forces it to be much smaller than $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$; ignoring log factors, its cardinality will be quadratic in m, while the cardinality of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is roughly quartic in m. This is true for every m and implies that $\rho_E(G_K)$ is an abelian subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and it cannot be open because it must have infinite index.

Even when $\mathrm{End}(E) = \mathbb{Z}$, if $\mathrm{End}(E_{\overline{K}})$ is an imaginary quadratic order $\mathcal{O}$ (so E has potential complex multiplication), then over a quadratic extension L/K we will have $\mathrm{End}(E_L) = \mathcal{O}$, in which case $\rho_E(G_L)$ is an abelian subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ that has index 2 in $\rho_E(G_K)$; in this case $\rho_E(G_K)$ will not be abelian (it be a generalized dihedral group), but it will still have infinite index in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and cannot be open.

20.3 Images of Galois representations

Theorem 20.2 (Serre's open image theorem)**.** *Let E be an elliptic curve over a number field K. Then $\rho_E(G_K)$ is an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ if and only if E does not have potential complex multiplication.*

Proof. The forward direction was argued above; the reverse direction is Théorèm 3 in [2]. □

References

[1] Andrew V. Sutherland, *Lecture notes for Elliptic Curves (18.783)*, 2023.

[2] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.