GLOBAL GALOIS REPRESENTATIONS ASSOCIATED TO ELLIPTIC CURVES

AARON GREICIUS

Let K be a number field. Let E be an elliptic curve over K. Let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group. For each m, we have $\rho_m \colon G_K \to \mathrm{Aut}(E[m]) \simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Let $\rho_{\ell^\infty} \colon G_K \to \mathrm{Aut}(E[\ell^\infty]) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell)$. Let $\rho \colon G_K \to \mathrm{Aut}(E^{\mathrm{tor}}) \simeq \mathrm{GL}_2(\hat{\mathbb{Z}})$. Let $G := \mathrm{GL}_2(\hat{\mathbb{Z}})$.

On the one hand, $G \simeq \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$. On the other hand, $G \simeq \varprojlim \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Let $\pi_\ell \colon G \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ be the projection. If S is a set of primes, let $\pi_S \colon G \to \prod_{\ell \in S} \mathrm{GL}_2(\mathbb{Z}_\ell)$. Let $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$. Let $r_m \colon G \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. For $X \subseteq G$, define $X_\ell = \pi_\ell(X)$ and $X_S = \pi_S(X)$, and $X(m) = r_m(X)$.

Serre's open image theorem (1972): If E is non-CM, then $\rho(G_K)$ is open in $G = \mathrm{GL}_2(\hat{\mathbb{Z}})$ (equivalently, of finite index).

One can show (with some work) that the following formulation is equivalent: If E is non-CM, then $\rho_\ell(G_K)$ is open for all ℓ and $\rho_{\ell^\infty}(G_K) = G_\ell$ for $\ell \gg 0$.

Call ℓ *exceptional* for E if $\rho_{\ell^\infty}(G_K) \neq G_\ell$. Let $c(E, K)$ be the smallest integer such that for all $\ell \geq c(E, K)$, the representation ρ_{ℓ^∞} is surjective. Serre asks if $c(E, K)$ is bounded by a function $S(K)$ of K. For $K = \mathbb{Q}$, the constant $S(\mathbb{Q}) = 41$ is a candidate.

Mazur (1978) showed that for semistable $E/\mathbb{Q}$, the representation ρ_{ℓ^∞} is surjective for $\ell \geq 11$.

Cojocaru (2005) comes up with upper bounds for $c(E, \mathbb{Q})$ in terms of the conductor N_E of E.

Duke (1997) showed that the set of isomorphism classes of $E/\mathbb{Q}$ with no exceptional primes has density 1 with respect to a certain naive height.

When is ρ surjective? Obvious necessary condition: E/K has no exceptional primes. But this is not sufficient. In fact, when $K = \mathbb{Q}$, we have that ρ is *never* surjective. Consider the character sgn obtained as the composition

$$\mathrm{GL}_2(\hat{\mathbb{Z}}) \xrightarrow{r_2} \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3 \xrightarrow{\mathrm{sgn}} \{\pm 1\}$$

and χ_Δ defined as the composition

$$\mathrm{GL}_2(\hat{\mathbb{Z}}) \xrightarrow{\det} \hat{\mathbb{Z}}^\times \simeq \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\sqrt{\Delta})/\mathbb{Q}) \hookrightarrow \{\pm 1\}.$$

Let $S_\Delta = \ker(\mathrm{sgn} \cdot \chi_\Delta^{-1})$. We claim that $\rho(G_\mathbb{Q}) \subseteq S_\Delta$. Proof: $\sigma \in G_\mathbb{Q}$ fixes $\sqrt{\Delta}$ if and only if it induces an even permutation of the roots of the cubic defining E, which holds if and only if $\mathrm{sgn}(\sigma) = 1$.

When $\rho(G_\mathbb{Q}) = S_\Delta$, we call E a *Serre curve*. Nathan Jones (a student of Duke) showed that almost all elliptic curves over $\mathbb{Q}$ are Serre curves.

Date: June 4, 2007.

1. Maximal closed subgroups of $\mathrm{GL}_2(\hat{\mathbb{Z}})$

Definition 1.1. If G is a topological group, $H \subsetneq G$ (subgroups are closed by convention) is *maximal* if $H \subsetneq H' \subseteq G$ implies $H' = G$.

Since G is profinite,

- Every closed subgroup is contained in a maximal subgroup.
- Maximal closed subgroups are open.

Proposition 1.2. *Let $G = \mathrm{GL}_2(\hat{\mathbb{Z}})$. Let $H \subsetneq G$ be maximal. Then either*

(1) *$H_\ell \neq G_\ell$ for some ℓ, in which case H_ℓ is maximal in G_ℓ and $H = H_\ell \times \prod_{\ell' \neq \ell} G_{\ell'}$; or*
(2) *$H_\ell = G_\ell$ for all ℓ, in which case H contains the closure G' of the commutator subgroup $[G, G]$.*

We have $G \overset{\det}{\twoheadrightarrow} \hat{\mathbb{Z}}^\times$ and $G \overset{\mathrm{sgn}}{\twoheadrightarrow} \{\pm 1\}$. It turns out that $G' = N \cap \mathrm{SL}_2(\hat{\mathbb{Z}})$ where $N := \ker(\mathrm{sgn})$. So the abelianization map is $G \xrightarrow{\mathrm{sgn},\det} \{\pm 1\} \times \hat{\mathbb{Z}}^\times$.

Theorem 1.3. *Let $H \leq G$ be a closed subgroup satisfying*

(1) *$H_\ell = G_\ell$ for all ℓ; and*
(2) *$(\mathrm{sgn}, \det)|_H$ is surjective.*

Then $H = G$.

Theorem 1.4. *Let E/K be an elliptic curve. Then ρ is surjective if and only if*

(1) *E has no exceptional primes; and*
(2) *$K \cap \mathbb{Q}^{\mathrm{cyc}} = \mathbb{Q}$*
(3) *$K(\sqrt{\Delta}) \not\subseteq K^{\mathrm{cyc}}$.*

2. Suitable field

Let $K = \mathbb{Q}(\alpha)$ where α is a real root of $x^3 + x + 1$. We have $\Delta_K = -31$, and $\mathcal{O}_K = \mathbb{Z}[\alpha]$, and $\mathcal{O}_K^\times = \{\pm 1\} \times \langle \alpha \rangle$, and $\mathrm{Cl}(K) = 1$ (in fact, the narrow class number is 1). Given any E/K, we know $\det \colon \rho(G_K) \to \hat{\mathbb{Z}}^\times$ is surjective.

Theorem 2.1. *Let $K = \mathbb{Q}(\alpha)$. Let E/K be semistable. Suppose that $\ell \neq 31$. If $\ell = 2, 3, 5$, suppose further that there exists a place $v \in S_E$ such that $\ell \nmid v(j_E)$. Then either $\rho_\ell(G_K) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ or*

(1) *$\rho_\ell(G_K)$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$;*
(2) *the semisimplification is a direct sum of the trivial character and the determinant character; and*
(3) *For all $v \notin S_E$, the prime ℓ divides $\#\tilde{E}_v(k_v) =: A_v$.*

Example 2.2. Define E by $y^2 + 2xy + \alpha y = x^3 - x^2$. We have $(\Delta_E) = P_{131} Q_{2207}$ and $N_E = P_{131} Q_{2207}$. The j-invariant is of the form $c/P_{131} Q_{2207}$. For $v = Q_{11}$, we have $A_v = 16$. For $v = Q_{23}$, we have $A_v = 15$. This has surjective ρ.