Serre's Open Image Theorem

S. M.-C.

12 October 2016

Today we're talking about Serre's open image theorem, which is a result about the Galois representations associated to elliptic curves (without complex multiplication). We essentially follow the master's thesis of Can Ozan Oguz, entitled Galois Representations Attached to Elliptic Curves.

First let's recall how these Galois representations are made (and other definitions we'll need).

1 Definitions

Let E be an elliptic curve over a number field K. As an abelian variety it has distinguished morphisms, defined over the base field K, given by "multiplication by integers" in the group law:

$$\begin{aligned}[n] : E &\to E \\ P &\mapsto nP.\end{aligned}$$

This shows that $\mathbb{Z} \subset \mathrm{End}_K(E)$. If there are other endomorphisms over K, i.e. $\mathrm{End}_K(E) \neq \mathbb{Z}$, then E is said to have *complex multiplication* (or CM) over K. It can also happen that $\mathrm{End}_K(E) = \mathbb{Z}$, but that E has more endomorphims defined over some extension L of K, i.e. $\mathrm{End}_L(E_L) \neq \mathbb{Z}$; in this case E has complex multiplication over L.

Example: the curve $y^2 = x^3 - x$ is defined over $\mathbb{Q}$, has no CM over $\mathbb{Q}$, but does have CM over $\mathbb{Q}(i)$ on account of the extra automorphism $(x, y) \mapsto (-x, iy)$.

Now let's recall the Tate module. The kernel $E[n]$ of the multiply by n map (on $\overline{K}$-points, let's say) consists of the n-torsion points of E, and is isomorphic to $(\mathbb{Z}/n)^2$. Fixing a prime ℓ, we have an inverse system

$$\cdots \longrightarrow E[\ell^3] \xrightarrow{\ell} E[\ell^2] \xrightarrow{\ell} E[\ell],$$

whose limit $T_\ell E$ we call the *ℓ-adic Tate module* of E. Each $E[\ell^n]$ is a (rank-2 free) module over $\mathbb{Z}/\ell^n$, so $T_\ell E$ is a (rank 2 free) module over $\varprojlim \mathbb{Z}/\ell^n = \mathbb{Z}_\ell$.

Furthermore, the $\overline{K}$-points of E get an action by $\mathrm{Gal}(\overline{K}/K) = G_K$, and the group law is rational so n-torsion points are sent to n-torsion points. This induces an action of G_K on $T_\ell E \cong \mathbb{Z}_\ell^2$, i.e. a representation

$$G_K \to \mathrm{GL}_2 \mathbb{Z}_\ell \subset \mathrm{GL}_2 \mathbb{Q}_\ell.$$

This is continuous because it comes from actions on the finite quotients.

Recall: if E has no complex multiplication, then $V_\ell E = T_\ell E \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is an irreducible G_K-representation for all ℓ, and $E[\ell]$ is an irreducible G_K-representation for almost all ℓ.

State Serre's open image theorem.

Shows the Galois reps we get are interesting.

2 Inertia Groups

Let K be a local field with residue characteristic p, $I = \mathrm{Gal}(K^{sep}/K^{nr})$ its inertia group, $I_p = \mathrm{Gal}(K^{sep}/K^t)$ its wild inertia group, and $I_t = I/I_p = \mathrm{Gal}(K^t/K^{nr})$ its tame inertia group.

Proposition 1. *Let*

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

be a finite dimensional representation over a characteristic p field. If ρ is semisimple, then $\rho(I_p) = 1$.

Now we determine I_t. If π is a uniformizer of K^{nr} and $(d, p) = 1$, then $K^{nr}(\pi^{1/d})$ is a tamely ramified extension with Galois group $(\mathbb{Z}/d)^\times$. Furthermore, K^t is the union of such extensions, so

$$I_t = \mathrm{Gal}(K^t/K^{nr}) = \varprojlim \mathrm{Gal}(K^{nr}(\pi^{1/d}), K^{nr}) = \varprojlim (\mathbb{Z}/d)^\times$$

for $(d, p) = 1$.

The continuous characters $I_t \to (\mathbb{F}_p^{sep})^*$ are precisely the powers of the characters $I_t \to (\mathbb{Z}/d)^* = \mu_d \subset (\mathbb{F}_p^{sep})^*$.

This stuff allows us to determine what the image of the tame inertia group will be like in representations associated to elliptic curves.

Let E be an elliptic curve over a finite extension $K/\mathbb{Q}_p$, $\overline{E}$ the reduction over the residue field k. Suppose that $\overline{E}$ is good and has non-zero j-invariant (i.e. height 1). Then $\overline{E}[p]$ has order p, and the kernel X_p of the reduction map $E[p] \to \overline{E}[p]$ has order p. The action of G_K fixes X_p, so the image of G_K in $\mathrm{Aut}(E[p]) = \mathrm{GL}_2 \mathbb{F}_p$ is contained in the Borel subgroup $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ (for some suitable choice of basis). The wild inertia I_p is contained in the unipotent subgroup $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$, and so I_t acts on X_p by a character χ_x and acts on $\overline{E}[p]$ by a character χ_y.

Proposition 2. *χ_x is the e^{th} power of the character $I_t \to \mu_{p-1} \subset (\mathbb{F}_p^{sep})^*$ (e being the ramification degree of K over $\mathbb{Q}_p$), and χ_y is the trivial character.*

Corollary 3. *Suppose that K is unramified. Then the image of I in* $\mathrm{Aut}(E[p]) = \mathrm{GL}_2 \mathbb{F}_p$ *is either* $\begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$ *or* $\begin{pmatrix} * & * \\ 0 & 1 \end{pmatrix}$*, corresponding as I_p acts trivially on $E[p]$ or not.*

3 ℓ-adic Representations

Let K be a number field.

An ℓ-adic representation of G_K is a continuous representation $\rho : G_K \to \mathrm{GL}_n(\mathbb{Q}_\ell)$. Recall that ρ is said to be unramified at a place v of K if $\rho(I_w) = 1$ for any place w of $\overline{K}$ extending v.

If ρ is unramified at a finite place v of K, then we can speak of the image of Frob_v in $\mathrm{GL}_n \mathbb{Q}_\ell$, which has a characteristic polynomial $P_{v,\rho}(T)$.

An ℓ-adic representation ρ is said to be *rational* if there exists a finite subset S of finite places of K such that for $v \notin S$, ρ is unramified at v and $P_{v,\rho}(T) \in \mathbb{Q}[T]$.

Let ℓ, ℓ' be primes, and ρ, ρ' rational ℓ, ℓ'-adic representations of G_K. The ρ, ρ' are said to be *compatible* if there is a finite subset S of finite places of K such that for $v \notin S$, ρ and ρ' are unramified at v and $P_{v,\rho}(T) = P_{v,\rho'}(T)$.

A system (ρ_ℓ) of ℓ-adic representations for each ℓ is *compatible* if they are pairwise compatible in the above sense.

4 The Algebraic Group $S_{\mathfrak{m}}$

Let's recall Weil restriction. If X is a variety over a number field K, then we define the Weil restriction $\mathrm{Res}_{K/\mathbb{Q}} X$ of X from K to $\mathbb{Q}$ by setting, for any $\mathbb{Q}$-algebra A,

$$\mathrm{Res}_{K/\mathbb{Q}} X(A) = X(A \otimes_{\mathbb{Q}} K).$$

If X is affine or projective this is representable, and thus gives a variety over $\mathbb{Q}$.

Let $\mathfrak{m}$ be a modulus of K, $C_{\mathfrak{m}} = C_K/U_{\mathfrak{m}}$ the ray class group of modulus $\mathfrak{m}$, and $T = \mathrm{Res}_{K/\mathbb{Q}} \mathbb{G}_{m,K}$. T is a torus of dimension $[K:\mathbb{Q}]$.

The ray class group $C_{\mathfrak{m}}$ sits in an exact sequence

$$1 \to K^*/(\mathcal{O}_K^* \cap U_{\mathfrak{m}}) \to \mathbb{A}_K^*/U_{\mathfrak{m}} \to C_{\mathfrak{m}} \to 1.$$

Also $\mathcal{O}_K^* \cap U_{\mathfrak{m}}$ is a subgroup of T, and we denote by $T_{\mathfrak{m}}$ the quotient of T by (the Zariski closure of) this subgroup.

Now we have a diagram

$$\begin{array}{ccc} K^*/(\mathcal{O}_K^* \cap U_{\mathfrak{m}}) & \longrightarrow & \mathbb{A}_K^*/U_{\mathfrak{m}} \\ \downarrow & & \\ T_{\mathfrak{m}}(\mathbb{Q}) & & \end{array}$$

and we define $S_{\mathfrak{m}}$ to be the universal thing in the bottom right corner with $\mathbb{Q}$-points making the diagram commute (which can be described pretty explicitly, but we won't). Then in fact the above diagram extends to

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^*/(\mathcal{O}_K^* \cap U_{\mathfrak{m}}) & \longrightarrow & \mathbb{A}_K^*/U_{\mathfrak{m}} & \longrightarrow & C_{\mathfrak{m}} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & T_{\mathfrak{m}}(\mathbb{Q}) & \longrightarrow & S_{\mathfrak{m}}(\mathbb{Q}) & \longrightarrow & C_{\mathfrak{m}} & \longrightarrow & 1 \end{array}$$

where the $C_{\mathfrak{m}}$ in the bottom row is the constant group scheme. Note that $S_{\mathfrak{m}}$ is commutative.

Now we want to define some ℓ-adic representations coming from $S_{\mathfrak{m}}$. First of all, from the diagram we have a morphism

$$\beta : \mathbb{A}_K^* \to \mathbb{A}_K^*/U_{\mathfrak{m}} \to S_{\mathfrak{m}}(\mathbb{Q}).$$

Also, note that $T(\mathbb{Q}_\ell) = (K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)^\times = \prod_{v|\ell} K_v^\times$ is a quotient of $\mathbb{A}_K^*$, so we get a morphism

$$\alpha : \mathbb{A}_K^* \to T(\mathbb{Q}_\ell) \to S_{\mathfrak{m}}(\mathbb{Q}_\ell)$$

also using the diagram. Now define $\epsilon : \mathbb{A}_K^* \to S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ by $\epsilon(x) = \beta(x)\alpha(x^{-1})$. Since this is trivial on K^* it factors through the idele class group $C_K = \mathbb{A}_K^*/K^*$; since $S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ is totally disconnected, it also factors through C_K/D_K where D_K is the connected component of the identity. Now C_K/D_K can be identified with $\mathrm{Gal}(K^{ab}/K)$, so we get a morphism

$$\epsilon : \mathrm{Gal}(K^{ab}/K) \to S_{\mathfrak{m}}(\mathbb{Q}_\ell).$$

Finally we obtain ℓ-adic representations of G_K by composing ϵ above with $G_K \to \mathrm{Gal}(K^{ab}/K)$ and any character $S_{\mathfrak{m}} \to \overline{\mathbb{Q}}_\ell^*$.

5 Serre's Open Image Theorem

Theorem. *Let E be an elliptic curve without complex multiplication over $\overline{K}$, and*

$$\phi_\ell : G_K \to \mathrm{Aut}(E[\ell]) = \mathrm{GL}_2 \mathbb{F}_\ell$$

the representation of G_K on the ℓ-torsion of E. Then ϕ_ℓ is surjective for almost all ℓ.

We now sketch the proof. We assume there are infinitely many ℓ for which ϕ_ℓ is not surjective, and show that E must have complex multiplication. There are four main steps:

1. Use our knowledge of the inertia subgroups of G and subgroups of $\mathrm{GL}_2 \mathbb{Z}_\ell$ to show that if ϕ_ℓ is not surjective, then

   (a) $\phi_\ell(G_K)$ is contained in a Borel subgroup $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$ or a Cartan subgroup $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$; or

   (b) $\phi_\ell(G_K)$ is contained in the normalizer N_ℓ of a Cartan subgroup C_ℓ but not in C_ℓ.

2. Show that the second case implies E has complex multiplication: a Cartan subgroup C has index 2 in its normalizer N, so we get a map $G_K \to N \to N/C \cong \{\pm 1\}$ corresponding to a quadratic extension L of K.

   Lemma 4. *This quadratic extension is unramified.*

   We know there are only finitely many unramified quadratic extensions of K, so if we produce infinitely many there must be one the occurs infinitely often; call such a one K'.

   Lemma 5. *If a place v of K is inert in K' and E has good reduction at v, then the reduced curve $\overline{E}_v$ has zero j-invariant (i.e. height 2).*

   By Chebotarev density, the set of inert places in a quadratic extension has density $1/2$ (and bad reduction happens finitely many times, so doesn't change this); but if E has no complex multiplication, then the set of places for which the reduction has zero j-invariant has density 0. This implies E has complex multiplication.

3. Assuming the first case, show that our representations are isomorphic to a system of representations arising from the algebraic group $S_{\mathfrak{m}}$, and therefore are abelian.

   A Borel or Cartan subgroup always fixes a line, so in the first case the semi-simplification of our representation will be abelian, i.e. the direct sum of two characters. Use this somehow to show that the original representations are isomorphic to a system of representations arising from $S_{\mathfrak{m}}$.

4. Conclude that E has complex multiplication, maybe because abelian implies reducible and we've seen that curves without CM give irreducible representations.