Galois representations attached to elliptic curves without complex multiplication

1 Introduction

Let K be a number field and $\bar{K}$ an algebraic closure of K. For an elliptic curve E defined over K, denote by E_n the kernel of the multiplication by n map, that is, the set of elements $x \in E(\bar{K})$ such that $nx = 0$. This is known to be a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2. If we let $G = \mathrm{Gal}(\bar{K}/K)$ denote the absolute Galois group of K, then G acts on E_n and this gives a homomorphism

$$\varphi_n : G \longrightarrow \mathrm{Aut}(E_n) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Taking inverse limit we see that there is a continuous action of G on

$$\mathrm{Aut}(E_\infty) = \varprojlim \mathrm{Aut}(E_n)$$

where E_∞ is the torsion subgroup of $E(\bar{K})$. We denote the corresponding homomorphism by

$$\varphi_\infty : G \longrightarrow \mathrm{Aut}(E_\infty) \simeq \mathrm{GL}_2(\hat{\mathbb{Z}}) = \prod \mathrm{GL}_2(\mathbb{Z}_\ell)$$

where the product is taken over all primes ℓ. It will also be useful to consider the ℓ-primary component of E_∞, which we shall denote by E_{ℓ^∞}. It is the subgroup of elements of E_∞ whose order is a power of ℓ. We denote by $\varphi_{\ell^\infty} : G \to \mathrm{Aut}(E_{\ell^\infty})$ the corresponding homomorphism given by the action of G; it is the projection onto the ℓ-th factor of φ_∞.

In what follows we will be concerned with the question of determining the image of φ_∞ in $\mathrm{Aut}(E_\infty)$ in the case where E does not have complex multiplication over $\bar{K}$. This is a highly non trivial question, however considerable progress has been made towards answering it. The most important result in this direction is the following theorem of Serre (see [3]), which says that $\varphi_\infty(G)$ is “as big as possible”.

Theorem 1.1 (Serre)**.** *Let E be an elliptic curve over a number field K such that E does not have complex multiplication over $\bar{K}$. Then the image of the homomorphism $\varphi_\infty : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}(E_\infty)$ is an open subgroup of $\mathrm{Aut}(E_\infty)$.*

The talk will consist primarily of the following parts. First we will briefly say a few words on the proof of Serre’s “open image” theorem, and why this does not in principle give an easy way of determining $\varphi_\infty(G)$ explicitly for each E without complex multiplication. The proof consists of two fundamental parts, as given by Serre in [2] and [3]. Second and mainly, we will see what can be said about computing the image of Galois explicitly, in which cases it is possible to do so, and where we can run into difficulties.

2 Serre's open image theorem

We keep the same notation as in the Introduction. As we mentioned there, the proof of Serre's theorem consists of two parts. Indeed, the assertion that $\varphi_\infty(G)$ is an open subgroup of $\mathrm{Aut}(E_\infty)$ is equivalent to the following two assertions holding simultaneously:

(i) For all primes ℓ, we have that $\varphi_{\ell^\infty}(G)$ is an open subgroup of $\mathrm{Aut}(E_{\ell^\infty})$.

(ii) For almost all primes ℓ (all but a finite number), we have that

$$\varphi_{\ell^\infty}(G) = \mathrm{Aut}(E_{\ell^\infty})$$

holds.

Part (i) is proved in [2] and part (ii) is proved in [3].

It is now convenient to introduce the ℓ-adic Tate module $T_\ell(E) = \lim E_{\ell^n}$. Also let $V_\ell = T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. This is a two-dimensional $\mathbb{Q}_\ell$-vector space on which G also acts continuously. Note that $V_\ell/T_\ell = E_{\ell^\infty}$ hence we have a homomorphism $\mathrm{Aut}(T_\ell) \to \mathrm{Aut}(E_{\ell^\infty})$ which is in fact an isomorphism, so we may identify the action of G on T_ℓ with the representation φ_{ℓ^∞}. The idea of Serre's proof of (i) relies firstly on the fact that the number of isomorphism classes of elliptic curves isogenous to E is finite. Using this one can show that the representation φ_{ℓ^∞} is irreducible for all primes ℓ. Denote by $\mathfrak{g}_\ell$ the Lie algebra of the ℓ-adic Lie group $\varphi_{\ell^\infty}(G)$. From the irreducibility of φ_{ℓ^∞} one obtains that V_ℓ is an irreducible $\mathfrak{g}_\ell$-module, hence by Schur's lemma, the commuting algebra $\mathfrak{g}'_\ell$ of $\mathfrak{g}_\ell$ in $\mathrm{End}(V_\ell)$ is a field. This field is either $\mathbb{Q}_\ell$ or a quadratic extension of $\mathbb{Q}_\ell$. Now one discards the case of $\mathfrak{g}'_\ell$ being a quadratic extension of $\mathbb{Q}_\ell$ by showing that if this were the case, then V_ℓ would be *locally algebraic*. From this, using the properties of locally algebraic representations, it would follow that there is an ℓ' such that $V_{\ell'}$ is isomorphic to a direct sum of one-dimensional subspaces stable under G, which would contradict the irreducibility of $V_{\ell'}$. One concludes after this that $\mathfrak{g}_\ell = \mathrm{End}(V_\ell)$, hence it follows that $\varphi_{\ell^\infty}(G)$ is open in $\mathrm{Aut}(T_\ell)$.

For part (ii) one shows that the homomorphism $\varphi_\ell : G \to \mathrm{Aut}(E_\ell)$ is surjective for almost all ℓ. This is shown to imply that $\varphi_{\ell^\infty}(G) = \mathrm{Aut}(E_{\ell^\infty})$ for almost all ℓ. This is done by showing that if there were an infinite set of primes L such that $\varphi_\ell(G) \neq \mathrm{Aut}(E_\ell)$ for all $\ell \in L$, then φ_{ℓ^∞} would be again locally algebraic, hence reaching the same contradiction as in part (i).

Of course we have excluded most of the details of these proofs, but it can already be seen that for example in proving (i), that this gives essentially no information on what the explicit ℓ-adic image of Galois is, beyond the fact that it is an open subgroup of $\mathrm{Aut}(T_\ell)$. We will see in the next section methods which are somewhat more explicit.

3 Computing the image of Galois

In this section we look at some techniques for computing the image of Galois for an elliptic curve over the rationals. In what follows, we let G_m denote the projection of $\varphi_\infty(G)$ into the finite product

$$\prod_{\ell \mid m} \mathrm{Aut}(E_{\ell^\infty}).$$

Then we have $G_m = \mathrm{Gal}(K_m/\mathbb{Q})$, where K_m is the m-power torsion field, that is, the infinite extension of $\mathbb{Q}$ obtained by adjoining the coordinates of all m^n-torsion points of E for all n. Also let $G(m)$ denote the reduction of $\varphi_\infty(G)$ mod m.

If we denote by

$$\pi_m : \mathrm{Aut}(E_\infty) \longrightarrow \mathrm{Aut}(E_m)$$

the reduction mod m map, then the statement that $\varphi_\infty(G)$ is open in $\mathrm{Aut}(E_\infty)$ is equivalent to saying that there exists an m such that $\varphi_\infty(G) = \pi_m^{-1}(G(m))$. Such an m has the property that:

(i) $\varphi_\infty(G) = G_m \times \prod_{\ell \nmid m} \mathrm{Aut}(E_{\ell^\infty})$.

(ii) $G_m = \pi_m^{-1}(G(m))$, where here

$$\pi_m : \prod_{\ell \mid m} \mathrm{Aut}(E_{\ell^\infty}) \longrightarrow \mathrm{Aut}(E_m)$$

denotes the reduction map taken from the product only over primes dividing m (sorry for the bad notation!).

When (i) holds we say m *splits* φ_∞, and when (ii) holds we say m is *stable.* Note that m splitting φ_∞ depends only on the primes dividing ℓ and not on the powers to which these primes occur, and m being stable depends on the primes dividing m and their respective powers. Given a split and stable m, the complete Galois representation of E is completely determined at a finite level, that is, it suffices to know $G(m)$ to obtain $\varphi_\infty(G)$.

The problem of computing the image of Galois can be split up into several parts. The first is to compute G_ℓ for each prime ℓ, and then to compute the full image in $\mathrm{GL}_2(\hat{\mathbb{Z}})$, which essentially translates into determining how the different ℓ-power torsion fields are related to one another.

So let us start with the computation of G_ℓ for each prime ℓ, a problem whose difficulty can vary depending on the type of elliptic curve we are considering. First we see that the problem of computing G_ℓ is essentially equivalent to the problem of computing $G(\ell)$, that is, the mod ℓ image of Galois. Serre showed in [2] that for $\ell > 3$ there is no proper closed subgroup of $\mathrm{SL}_2(\mathbb{Z}_\ell)$ that maps surjectively onto $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and concluded that if $G(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$, then $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$. Note that this fails for $\ell = 2$ and $\ell = 3$ (Elkies). Also, in many cases it is possible to bound the primes for which the mod ℓ image may fail to be surjective. For example, in the case of semi-stable elliptic curves it was shown by Serre in [3] that if $\varphi_\ell(G) \neq \mathrm{Aut}(E_\ell)$ then either E or a curve isogenous to E must have a rational ℓ-torsion point, something which cannot happen for $\ell > 7$ (although this was not yet known at the time Serre published this result). This already gives us that the mod ℓ image is surjective for $\ell > 7$ and hence that $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for $\ell > 7$. in the general case the bound is not quite so nice, however it is conjectured that the mod ℓ image is *always* surjective for $\ell > 37$.

The next thing to consider is how to deal with the cases when the mod ℓ image is not surjective, as well as the cases $\ell = 2, 3$. Here the idea for determining G_ℓ will be to recover it as the inverse image under the reduction map of $G(\ell^n)$ for some n, that is, finding an n such that ℓ^n is stable and computing $G(\ell^n)$ for that n. For that first we need to have a way of determining $G(\ell^n)$ for small n, something which is already not clear how to do.

For now we fix a prime ℓ. By successively adjoining to $\mathbb{Q}$ the ℓ-power torsion of E we obtain a tower of field extensions $\mathbb{Q} \subset \mathbb{Q}(E_\ell) \subset \mathbb{Q}(E_{\ell^2}) \subset \cdots \subset \mathbb{Q}(E_{\ell^\infty})$. Let us look more closely at the different Galois groups that arise in such a tower. Let $M = M_2(\mathbb{Z}_\ell)$ denote the set of all 2×2 matrices with coefficients in $\mathbb{Z}_\ell$, and let

$$\begin{aligned} V_n &= I + \ell^n M \\ &= Ker\, \pi_{\ell^n} \end{aligned}$$

where π_{ℓ^n} is the reduction map mod ℓ^n. Also, let

$$U_n = G_\ell \cap V_n = \mathrm{Gal}(\mathbb{Q}(E_{\ell^\infty})/\mathbb{Q}(E_{\ell^n})).$$

Note that we have $G_\ell/U_n \simeq G(\ell^n) = \mathrm{Gal}(\mathbb{Q}(E_{\ell^n})/\mathbb{Q})$. We obtain in this manner a filtration $G_\ell \supset U_1 \supset U_2 \supset \cdots \supset \{1\}$. Consider now the map

$$\begin{aligned} M/\ell M &\longrightarrow V_n/V_{n+1} \\ X \mod \ell M &\longmapsto I + \ell^n X \mod V_{n+1} \end{aligned}$$

Since mod ℓ^{n+1} we have $(I + \ell^n X)(I + \ell^n Y) = I + \ell^n(X + Y)$ with $X, Y \in M_2(\mathbb{F}_\ell)$, this is seen to be a group isomorphism, and $M/\ell M \simeq M_2(\mathbb{F}_\ell)$ is a vector space of dimension 4. From this we see that working in V_n/V_{n+1} is essentially doing linear algebra over a vector space of dimension 4. If we look at the extension $\mathbb{Q}(E_{\ell^{n+1}})/\mathbb{Q}(E_{\ell^n})$, its Galois group U_n/U_{n+1} is naturally a subspace of V_n/V_{n+1}, hence it follows that $[\mathbb{Q}(E_{\ell^{n+1}}) : \mathbb{Q}(E_{\ell^n})]$ divides ℓ^4. We will refer to U_n/U_{n+1} as the *vector space associated* to U_n. It has dimension at most 4 over $\mathbb{F}_\ell$.

We know that if $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ then $G(\ell^n) = \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ for all n, hence the associated vector space to U_n has dimension 4 for all n. It could happen however that $G_\ell \subsetneq \mathrm{GL}_2(\mathbb{Z}_\ell)$, for example if $G(\ell) \subsetneq \mathrm{GL}_2(\mathbb{F}_\ell)$. In such cases the following lemma allows us to reduce the problem of determining G_ℓ to a finite computation, namely, that of determining the smallest n such that U_n/U_{n+1} has dimension 4. It is separated into two cases depending on whether ℓ is even or odd.

Lemma 3.1. *(i) Let $\ell \geqslant 3$. With the notation introduced above, suppose that for some $n \geqslant 1$ the vector space associated to U_n has dimension 4. Then we have $U_n = V_n$.*

(ii) Let $\ell = 2$. Suppose that for some $n \geqslant 2$ the vector space associated to U_n has dimension 4. Then $U_n = V_n$. If the vector spaces associated to U_1 and U_2 each have dimension 4, then we have $U_1 = V_1$.

Proof. This is shown in [1], §6. □

Remark 3.2. From $U_n = V_n$ it follows that $G_\ell = \pi_\ell^{-1}(G(\ell^n))$, in other words, ℓ^n is stable. Of course we want to find the smallest n for which this holds in order to reduce computations as much as possible.

Normally the way to prove that the vector space associated to U_n has dimension 4 for some n is by means of Frobenius elements. Namely, we try to find 4 linearly independent Frobenius elements. This works quite well in specific cases since if the associated vector space does indeed have dimension 4, then Cebotarev's density theorem implies that a machine search should find the 4 Frobenius elements we require. However to show that these Frobenius elements are linearly independent requires we find them in a matrix form that allow them to remain linearly independent even after base change. This discussion raises the following question, could we find an algorithm which finds an n for which ℓ^n is stable which is guaranteed to terminate in a finite amount of time?

The preceding discussion makes the assumption that we have managed to compute $G(\ell^n)$ for small n, so it seems our first problem should be trying to compute at least the mod ℓ image of Galois. There is an algorithm by Andrew Sutherland which computes the mod ℓ image of Galois up to isomorphism, however it seems it does not do it up to conjugacy. When the mod ℓ image is surjective, it does compute it unconditionally.

As we mentioned previously, the final stage of computing the image of Galois is computing the relations between the different ℓ-power torsion fields. Perhaps the most useful result in this direction is the following one we know discuss. First we introduce some terminology. If X is a profinite group, and Y is a finite simple group, we say that Y *occurs* in X if there exist closed subgroups X_1, X_2 of X such that X_1 is normal in X_2 and X_2/X_1 is isomorphic to Y. We say a prime occurs in X if it divides the order of a group which occurs in X.

Theorem 3.3. *Let m be divisible by 2, 3 and all primes of bad reduction of an elliptic curve $E/\mathbb{Q}$. Suppose also that:*

(i) $G(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$ for all $\ell \nmid m$.

(ii) If $\ell \nmid m$ then ℓ does not occur in G_m.

Then m splits φ_∞.

Using this theorem, we may find an m which splits φ_∞, therefore reducing the computation of $\varphi_\infty(G)$ to the computation of G_m. This amounts to computing the intersection of the different ℓ-power torsion fields for the primes ℓ dividing m. This has been done in many specific instances but the methods applied have made use of specific properties (ramification, etc.) of the ℓ-power torsion fields (and hence of the elliptic curves) in question. For this reason it is not clear whether this can yield a general algorithm to perform such computations for any elliptic curve.

References

[1] S. Lang and H. Trotter. *Frobenius Distributions in* GL$_2$*-Extensions.* Springer, 1974.

[2] J.-P Serre. *Abelian ℓ-adic representations and elliptic curves.* Benjamin, 1968.

[3] J.-P Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15:259–331, 1972.