Galois groups arising from ℓ-division points of elliptic curves over number fields

Ken Ribet
UC Berkeley

April 4, 2006

Suppose that E is an elliptic curve over a number field K, and let $\overline{K}$ be an algebraic closure of K (e.g., the field of complex algebraic numbers). For each prime ℓ, the group $E[\ell]$ of ℓ-division points of E (with coordinates in $\overline{K}$) is a 2-dimensional vector space over the field $\mathbf{F}_\ell$ with ℓ elements. The action of $G_K := \mathrm{Gal}(\overline{K}/K)$ on $E[\ell]$ defines a continuous homomorphism

$$\rho_\ell : G_K \to \mathrm{Aut}(E[\ell]) \approx \mathbf{GL}(2, \mathbf{F}_\ell).$$

We are interested in the images of ρ_ℓ as ℓ varies.

Let $G_\ell = \rho_\ell(G_K)$, so that G_ℓ is (non-canonically) a subgroup of $\mathbf{GL}(2, \mathbf{F}_\ell)$.

If E has complex multiplication (over $\overline{K}$), then G_ℓ is essentially abelian. Let $\mathcal{O} = \mathrm{End}_{\overline{K}}(E)$ be the endomorphism ring of E. Then G_ℓ has a natural abelian subgroup H_ℓ with $(G_\ell : H_\ell) \leq 2$, namely $\mathrm{Aut}_{\mathcal{O}} E[\ell] = (\mathcal{O}/\ell\mathcal{O})^*$. The group H_ℓ coincides with $\mathrm{Aut}_{\mathcal{O}} E[\ell]$ for almost all ℓ (i.e., all but finitely many ℓ).

We are interested in the opposite case: that where E has no complex multiplication. Let's assume from now on that we're in this case.

The subject of this talk is the following theorem of Serre, from his celebrated 1972 article "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques":

Theorem 1. *For almost all ℓ, ρ_ℓ is surjective.*

In other words, there is a constant $C(E, K)$ such that $G_\ell = \mathbf{GL}(2, \mathbf{F}_\ell)$ whenever ℓ is bigger than $C(E, K)$.

Serre began working on problems of this type in the 1960s. In article #70 of his Œuvres, "Groupes de Lie l-adiques attachés aux courbes elliptiques" (1966), he considered the ℓ-adic representation of G_K arising from E/K, where ℓ is a fixed prime and E is again has no CM. The image of this representation is a subgroup G_{ℓ^∞} of $\mathbf{GL}(2, \mathbf{Z}_\ell)$. Serre proved that G_{ℓ^∞} is an open subgroup of $\mathbf{GL}(2, \mathbf{Z}_\ell)$ if the j-invariant of E is not an algebraic integer. In his 1968 book "Abelian l-adic representations and elliptic curves," Serre removed this hypothesis.

Let's go back to the mod ℓ situation. Because of the Weil pairing, the determinant of ρ_ℓ is the mod ℓ cyclotomic character $\chi_\ell : G_K \to \mathbf{F}_\ell^*$. This character is surjective for almost all ℓ, e.g., whenever ℓ is unramified in $K/\mathbf{Q}$. Hence, for almost all ℓ, $G_\ell = \mathbf{GL}(2, \mathbf{F}_\ell)$ if and only if G_ℓ contains the kernel of the determinant map, namely $\mathbf{SL}(2, \mathbf{F}_\ell)$.

Group theory shows that G_ℓ contains $\mathbf{SL}(2, \mathbf{F}_\ell)$ if and only if (1) the order of G_ℓ is divisible by ℓ and (2) the representation ρ_ℓ is irreducible.

Already in 1968, Serre proved the irreducibility of ρ_ℓ for almost all ℓ: If E_ℓ is reducible, it has a Galois-stable cyclic subgroup C_ℓ of order ℓ. The quotient E/C_ℓ is an elliptic curve over K with good reduction exactly where E has good reduction. Because E has no CM (over K), the curves E/C_ℓ are pairwise non-isomorphic. This contradicts a theorem of Shafarevich (1962) to the effect that there are only a finite number of isomorphism classes of elliptic curves over K with good reduction outside a given finite set of places.

Knowing that the subgroup G_ℓ of $\mathbf{GL}(2, \mathbf{F}_\ell)$ is irreducible, let's focus on the statement that it's of order divisible by ℓ. Equivalently, we need to show that the image $\overline{G}_\ell$ of G_ℓ in $\mathbf{PGL}(2, \mathbf{F}_\ell)$ is of order divisible by ℓ. One thing we know is that $\overline{G}_\ell$ has a subgroup of size roughly ℓ: Suppose that ℓ is large enough so that there is an unramified place $v|\ell$ of K at which E has good reduction. Then the inertia subgroup of $\overline{G}_\ell$ for the place v is cyclic of order $\ell - 1$ or $\ell + 1$, depending on whether the reduction of E at v is ordinary or supersingular.

A consequence of this observation (for almost all ℓ) is that $\overline{G}_\ell$ is *not* isomorphic to one of the three exceptional groups $\mathbf{S}_4$, $\mathbf{A}_4$, $\mathbf{A}_5$. Adapting the methods that study finite subgroups of $\mathbf{GL}(2, \mathbf{C})$, one deduces (for large ℓ) that $\overline{G}_\ell$ is either cyclic or dihedral if it has order prime to ℓ.

Assume now that G_ℓ is irreducible and of order prime to ℓ and that ℓ is large enough to avoid the three exceptional groups.

Then one of two things happens:

- G_ℓ is contained in the normalizer of a split Cartan subgroup of $\mathbf{GL}(2, \mathbf{F}_\ell)$ (but not in the split Cartan itself);

- G_ℓ is contained in the normalizer of a non-split Cartan subgroup (and perhaps even in the Cartan itself).

The split Cartan is conjugate to the group of diagonal matrices. The non-split Cartan is like $\mathbf{F}_{\ell^2}^*$.

Schematically, we have $G = G_\ell \subseteq N$, where N is the normalizer of C. The index $(N : C)$ is 2. If G is not contained in C, then the character $\epsilon : G_K \to G \to N/C \approx \{\pm 1\}$ cuts out a quadratic extension of K. This extension (as well as ϵ) depends on ℓ, at least a priori.

In order to understand the ramification of the quadratic extension, we need to understand ramification properties of ρ_ℓ.

The representation ρ_ℓ can be ramified only at primes of K dividing ℓ and at primes of K at which E has bad reduction. We can and do replace K by a small finite extension to ensure that E/K is semistable. Then at primes of K, E either has good or multiplicative reduction. In the latter case, the local behavior of ρ_ℓ may be deduced from the theory of the Tate curve. In particular, if v is a prime of bad reduction and v is prime to ℓ, then the inertia group at v acts unipotently on $E[\ell]$: $\rho_\ell(\sigma)$ is of order dividing ℓ if σ is in the inertia group.

It follows from this that the character $\epsilon : G_K \to N/C$ is ramified only at ℓ. For primes v dividing ℓ, we infer that the image of the inertia group at v in ρ_ℓ must be contained fully in C. If not, its image in $\overline{G}_\ell$ would be of order ≤ 2, contradicting what we said before about its order being $\ell \pm 1$. Hence ϵ is in fact unramified everywhere. Replacing K by the compositum of its unramified quadratic extensions, we can and will assume that $\epsilon = 1$, i.e., that G_ℓ is contained in C. Because of the irreducibility, C must be a *non-split* Cartan subgroup of $\mathbf{GL}(2, \mathbf{F}_\ell)$.

Let's sum up so far: after replacing K by a finite extension of K (which serves only to shrink the G_ℓ), we have gotten into the situation where all but finitely many G_ℓ are either $\mathbf{GL}(2)$ or non-split Cartan subgroups of $\mathbf{GL}(2)$. We need to rule out the case where infinitely many G_ℓ are non-split Cartans.

This bad case can never occur if E has multiplicative reduction at some prime of K, i.e., the j-invariant of E is not an algebraic integer. In that situation, almost all G_ℓ have order divisible by ℓ.

Serre's idea was to think about the family of groups G_ℓ arising from an elliptic curve with CM over K. In that case, all the G_ℓ are abelian, and all but finitely many of them are Cartan subgroups of $\mathbf{GL}(2)$. However, half of the Cartans are split and half are non-split: it depends on whether ℓ splits in the field of muliplication.

Having lots of non-split Cartans but no split Cartans was an anomaly that he succeeded in exploiting.

Before saying how he did this, I'll toss in some inputs from the 1980s. Let A be an abelian variety over a number field K, and let ℓ be a prime. Let V_ℓ be the $\mathbf{Q}_\ell$-adic Tate module attached to A: this is a $\mathbf{Q}_\ell$-vector space of dimension $2\dim A$ with functorial actions of G_K and the ring $\mathbf{Q}_\ell \otimes \mathrm{End}_K A$. Faltings proved in 1983 that G_K acts semisimply on V_ℓ and that the natural map $\mathbf{Q}_\ell \otimes \mathrm{End}_K A \hookrightarrow \mathrm{End}_{G_K} V_\ell$ is in fact an isomorphism (Tate conjecture).

Zarhin, in his 1985 Inventiones article "A finiteness theorem for unpolarized Abelian varieties. . . ," established mod ℓ analogues of Faltings's results. For all sufficiently large ℓ, G_K acts semisimply on $A[\ell]$, and the rings $\mathrm{End}_{G_K} A[\ell]$ and $(\mathrm{End}_K A)/\ell(\mathrm{End}_K A)$ are naturally isomorphic.

Especially, if $\mathrm{End}\, A = \mathbf{Z}$, then $A[\ell]$ is absolutely irreducible as a G_K-module for all sufficiently large ℓ.

When $A = E$ is our elliptic curve, the results of Faltings–Zarhin rule out the possibility that G_ℓ is a non-split Cartan subgroup infinitely often. The endomorphism ring of E is $\mathbf{Z}$, by hypothesis.

On the other hand, the non-split Cartan subgroups of $\mathbf{GL}(2, \mathbf{F}_\ell)$ are quintessential examples of groups whose actions on the underlying 2-dimensional vector space are irreducible but not absolutely irreducible.

Back to Serre's 1972 article. Let Λ be the set of primes ℓ for which the image of ρ_ℓ is a non-split Cartan subgroup of $\mathbf{GL}(2, \mathbf{F}_\ell)$. We suppose that Λ is infinite. Serre shows that the ρ_ℓ ($\ell \in \Lambda$) arise from a collection of Großencharacters of type A_0 of K with values in some algebraic number field F. By results that are due essentially to Weil, we may associate a family $\tilde{\rho}_\ell$ of ℓ-adic representations of G_K to the collection of characters. By comparing characteristic polynomials, we recognize that the $\tilde{\rho}_\ell$ are in fact the ℓ-adic representations associated to E.

The punchline is that the images of infinitely many of the ρ_ℓ will then be split Cartan subgroups; we take the ℓ that split completely in F (if I remember correctly). We get a contradiction to the irreducibility result of Shafarevich.

In this subject, a great deal of activity has centered around the following problem, which was suggested initially by Serre: Consider elliptic curves $E/\mathbf{Q}$ and the associated representations $\rho_\ell : G_{\mathbf{Q}} \to \mathbf{GL}(2, \mathbf{F}_\ell)$. Is there an absolute constant C such that ρ_ℓ is surjecive whenever $\ell > C$. Here, the important point is that C should be independent of E.

A key result is Mazur's 1978 theorem to the effect that ρ_ℓ is irreducible for $\ell > 163$. A consequence of this theorem is that, for $\ell > 163$, G_ℓ is either all of $\mathbf{GL}(2, \mathbf{F}_\ell)$ or else is contained in the normalizer of a Cartan subgroup of $\mathbf{GL}(2)$. In the latter case, G_ℓ is not contained in the Cartan subgroup itself.

A great deal of work has been done to understand and control situations where G_ℓ is contained in a split Cartan subgroup. The non-split case seems to be more difficult.