GALOIS GROUPS ATTACHED TO POINTS OF FINITE ORDER ON ELLIPTIC CURVES OVER NUMBER FIELDS (D'APRÈS SERRE)

JACQUES VÉLU

1. Introduction

Let E be an elliptic curve defined over a number field K and equipped with a K-rational point $\mathcal{O}$. It is always possible to give E a model of the following type:

$$y^2 + a_1xy + a_3y \;=\; x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

where $a_i \in K$, the cubic in (1) is nonsingular, and where $\mathcal{O}$ is the "point at infinity" of the cubic.

The points of E defined over K form a group $E(K)$, where $A+B$ is calculated as follows:

[The diagram explaining the addition of points on elliptic curves is not repreoduced here.]

The theorem of Mordell-Weil states that if K is a number field, then $E(K)$ is finitely generated. Thus we have

$$E(K) \;\simeq\; E(K)_{\text{tors}} \oplus \mathbb{Z}^{r_K},$$

where $E(K)_{\text{tors}}$ is the finite subgroup of $E(K)$ formed by points of finite order, and where r_K is called the rank of E over K. The computation of r_K is not always possible although it is known how to do that for certain curves. It is the subject of numerous conjectures.

The computation of $E(K)_{\text{tors}}$ is easy since there is an algorithm allowing to find all its points and therefore its structure.

2. Points of finite order on an elliptic curve over a number field

These have the following properties:

a) The points $E[N]$ of order dividing N on the curve E defined over K form a group isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$.
b) The coordinates of points of $E[N]$ are algebraic over K, and the algebraic extension $K_N = K(E[N])$ is Galois over K. We put $G_N = \mathrm{Gal}(K_N/K)$.

c) The sum of two points A and B in $E[N]$ is a point C whose coordinates are rational functions over K of the coordinates of A and B. Consequently, if $\sigma \in G_N$, then $\sigma(A+B) = \sigma(A)+\sigma(B)$, and there is a homomorphism $G_N \longrightarrow \mathrm{Aut}(E[N])$. Moreover, since $E[N]$ generates K_N over K, this homomorphism is injective.

Thus we have

G_N is isomorphic to a subgroup of $\mathrm{Aut}(E[N]) \simeq \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

Next we pass to the limit. We define

$$\begin{array}{rcllcl} E_{\ell^\infty} & = & \bigcup_n E[\ell^n] & & = & \varinjlim E[\ell^n] \\ E_\infty & = & \bigcup_N E[N] & & = & \varinjlim E[N] \\ K_{\ell^\infty} & = & \bigcup_n K_{\ell^n}, & K_\infty & = & \bigcup_N K_N \\ G_{\ell^\infty} & = & \mathrm{Gal}(K_{\ell^\infty}/K), & G_\infty & = & \mathrm{Gal}(K_\infty/K). \end{array}$$

Then G_{ℓ^∞} is isomorphic to a subgroup of

$$\varprojlim \mathrm{GL}(2, \mathbb{Z}/\ell^n\mathbb{Z}) \;=\; GL(2, \mathbb{Z}_\ell),$$

and G_∞ is isomorphic to a subgroup of

$$\varprojlim \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \;=\; GL(2, \widehat{\mathbb{Z}}).$$

3. The analogue of the multiplicative group

An algebraic group that can be studied more easily than an elliptic curve E/K is the multiplicative group G_m.

The points of order N of G_m are the N^{th} roots of unity μ_N which form a group isomorphic to $\mathbb{Z}/N\mathbb{Z}$. Consider the field $K(\mu_N)$; this is a Galois extension of K, and the group $\mathrm{Gal}(K(\mu_N)/K)$ is a subgroup of $\mathrm{Aut}(\mu_N)$ which in turn is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^\times \simeq \mathrm{GL}(1, \mathbb{Z}/N\mathbb{Z})$. By passing to the limit, we get

$$\begin{array}{rcl} \mathrm{Gal}(K(\mu_{\ell^\infty}/K) & \simeq & \text{subgroup of } \mathbb{Z}_\ell^\times \simeq \mathrm{GL}(1, \mathbb{Z}_\ell), \\ \mathrm{Gal}(K(\mu_\infty/K) & \simeq & \text{subgroup of } \widehat{\mathbb{Z}}^\times \simeq \prod_\ell \mathrm{GL}(1, \mathbb{Z}_\ell). \end{array}$$

The following equivalent theorems are known to hold:

Theorem 1 *The group* $\mathrm{Gal}(K(\mu_\infty/K)$ *is isomorphic to an open subgroup of* $\widehat{\mathbb{Z}}^\times$*.*

Theorem 1' *For all primes* ℓ*, the group* $\mathrm{Gal}(K(\mu_{\ell^\infty}/K)$ *is isomorphic to an open subgroup of* $\mathbb{Z}_\ell^\times$*, with equality for almost all* ℓ*.*

It is therefore natural to ask the same question for the groups G_{ℓ^∞} and G_∞ associated to an elliptic curve.

4. Results

If E does not have complex multiplication, then the following three equivalent theorems are true:

Theorem 2 *The group G_∞ is isomorphic to an open subgroup of* $\mathrm{GL}(2, \widehat{\mathbb{Z}})$.

Theorem 2' *a) For all primes ℓ, the group G_{ℓ^∞} is isomorphic to an open subgroup of* $\mathrm{GL}(2, \mathbb{Z}_\ell)$;
b) for almost all ℓ, we have $G_{\ell^\infty} \simeq \mathrm{GL}(2, \mathbb{Z}_\ell)$.

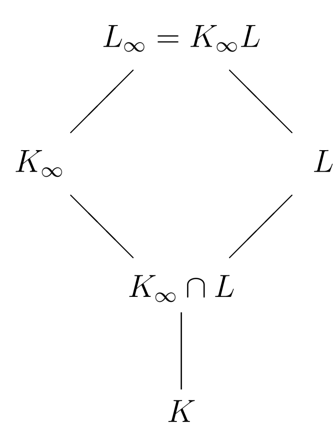
Theorem 2" *For all primes ℓ, the group G_{ℓ^∞} is isomorphic to an open subgroup of* $\mathrm{GL}(2, \mathbb{Z}_\ell)$;
b) for almost all ℓ, we have $G_\ell \simeq \mathrm{GL}(2, \mathbb{F}_\ell)$.

Property a) of Theorems 2' and 2" is proved in [1, IV-11]. The equivalence of Theorems 2, 2' and 2" is proved in [1, IV-19]. Property 2".b) is proved in [2, p. 294].

Remark 1. Theorem 2 can be reformulated in another form:

Theorem 2"' *If the elliptic curve E defined over K does not have complex multiplication, then there exists a finite extension L/K such that* $\mathrm{Gal}(L(E_{\mathrm{tors}})/L)$ *is isomorphic to an open subgroup of* $\mathrm{GL}(2, \widehat{\mathbb{Z}})$.

It is clear that Theorem 2 implies Theorem 2"' by taking $L = K$. Conversely, Theorem 2"' implies Theorem 2; in fact, since $\mathrm{Gal}(L_\infty/L) \simeq \mathrm{Gal}(K_\infty/K_\infty \cap L)$ which is a subgroup of $\mathrm{Gal}(K_\infty/K)$, this implies that if $\mathrm{Gal}(L_\infty/L)$ is isomorphic to an open subgroup of $\mathrm{GL}(2, \widehat{\mathbb{Z}})$, then so is $\mathrm{Gal}(K_\infty/K)$.



Remark 2. In [1], Theorems 2, 2' and 2" are proved under the assumption that the invariant j of E is not an integer in K, while in [2]

it is proved assuming that E does not have CM. Since it is known that curves with CM have integral j-invariant (the converse is false), the result in [2] is stronger than that in [1]. Moreover, if E has CM, it is known how to describe the groups $G_{\ell\infty}$. Let A denote the endomorphism ring of such an E. This is an order in the complex quadratic field $A \otimes \mathbb{Q}$. Then $(A \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)^\times$ embeds into $\mathrm{GL}(2, \mathbb{Z}_\ell)$. We have the following theorem ([2, p. 302]):

Theorem. *G_∞ is isomorphic to an open subgroup of $\prod_\ell (A \otimes_{\mathbb{Z}} \mathbb{Z}_\ell)^\times$.*

5. Sketch of the proof of property 2'.a)

The group $G_{\ell\infty}$ is isomorphic to a closed subgroup of $\mathrm{GL}(2, \mathbb{Z}_\ell)$. It is therefore a Lie group, and its Lie algebra $\mathcal{G}_\ell$ is isomorphic to a subalgebra of $M_2(\mathbb{Q}_\ell)$. The theory of Lie groups [3] shows that property a) is equivalent to the fact that $\mathcal{G}_\ell \simeq \mathbb{Q}_\ell$. Let $\mathcal{G}'_\ell$ denote the commutator of $\mathcal{G}_\ell$ in $M_2(\mathbb{Q}_\ell)$. It is a field, hence either $\mathbb{Q}_\ell$ or a quadratic extension of $\mathbb{Q}_\ell$. If $\mathcal{G}_\ell \simeq M_2(\mathbb{Q}_\ell)$, then $\mathcal{G}'_\ell \simeq \mathbb{Q}_\ell$. It can be shown that the converse holds. Finally, one shows using the theory of locally algebraic representations developed by Serre that $\mathcal{G}'_\ell$ cannot be a quadratic extension of $\mathbb{Q}_\ell$, and property a) follows.

6. Method of proof of property 2".b)

This is what we need to prove:

> Given an elliptic curve defined over a number field K and without complex multiplication, then for almost all primes ℓ we have $G_\ell \simeq \mathrm{GL}(2, \mathbb{F}_\ell)$.

A. It is known that G_ℓ is isomorphic to a subgroup of $\mathrm{GL}(2, \mathbb{F}_\ell)$; let us therefore make a list of all subgroups of $\mathrm{GL}(2, \mathbb{F}_\ell)$.

Theorem 3. *Let $H \subseteq \mathrm{GL}(2, \mathbb{F}_\ell)$ be a subgroup with $\ell \mid \# H$. Then either H contains $\mathrm{SL}(2, \mathbb{F}_\ell)$, or H is contained in some Borel subgroup, i.e. a subgroup consisting of elements of the form $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$.*

Proof. a) If $\ell \mid \# H$, then H contains an element of order ℓ.

b). **Lemma** Every element s of order ℓ in $\mathrm{GL}(2, \mathbb{F}_\ell)$ fixes a unique line D_s.

In fact, $s^\ell = 1$, so if λ is an eigenvalue of s, then $\lambda^s = 1$, and s fixes the line generated by an eigenvector associated to the eigenvalue 1. This is unique since if s fixes two lines, then s has the form $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$ with respect to the basis consisting of the vectors spanning the lines. But such an s does not have order ℓ.

c). If $t \in H$, then $D_{tst^{-1}} = tD_s$.

Thus there are two possibilities for H:

(1) *All lines D_s associated to all elements s of order ℓ in H are equal to one line D. By c), each $t \in H$ fixes D. Taking a vector spanning D as our first basis vector, we see that H must be a Borel subgroup.*
(2) *There exist $s, s' \in H$ of order ℓ such that $D_s \neq D_{s'}$. Taking the vectors spanning these lines as our basis, then $s = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ and $s' = \left(\begin{smallmatrix} 1 & 0 \\ a' & 1 \end{smallmatrix}\right)$, and since $s^k = \left(\begin{smallmatrix} 1 & ka \\ 0 & 1 \end{smallmatrix}\right)$, H contains the matrices $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ which generate $\mathrm{SL}(2, \mathbb{F}_\ell)$ by [4, p. 104]. This proves Theorem 3.*

For classifying the subgroups H of $\mathrm{GL}(2, \mathbb{F}_\ell)$ whose order is not divisible by ℓ, we look at the subgroups of $\mathrm{PGL}(2, \mathbb{F}_\ell)$ with order prime to ℓ.

Theorem 4. If $\widetilde{H}$ is a subgroup of $\mathrm{PGL}(2, \mathbb{F}_\ell)$ with order prime to ℓ, then $\widetilde{H}$ is isomorphic to a subgroup of one of the following groups:

i) a dihedral group;
ii) the alternating group A_4;
iii) the symmetric group S_4;
iv) the alternating group A_5.

This result is proved using the Lefschetz principle:

a) Since the order of $\widetilde{H}$ is prime to ℓ, a Hensel-type argument shows that $\widetilde{H}$ is isomorphic to a subgroup of $\mathrm{PGL}(2, \mathbb{Q}_\ell)$.

b) Since $\mathbb{C}$ is isomorphic as a field to $\mathbb{Q}_\ell$, H is isomorphic to a subgroup of $\mathrm{PGL}(2, \mathbb{C})$.

c) $\mathrm{PGL}(2, \mathbb{C})$ is the automorphism group of the Riemann sphere $\mathbb{P}_1(\mathbb{C})$. Take a point on $\mathbb{P}_1(\mathbb{C})$ and consider its orbit under $\widetilde{H}$. One obtains a regular polyhedron whose automorphism group contains $\widetilde{H}$ as a subgroup. There are the following possibilities:

polyhedron	automorphism group
polygon	dihedral group
tetrahedron	A_4
cube or octahedron	S_4
dodecahedron or icosahedron	A_5

Theorem 4 has the following consequence:

Theorem 4'. *If H is a subgroup of $\mathrm{GL}(2, \mathbb{F}_\ell)$ of order prime to ℓ, then H is one of the following:*

i) *H is contained in a Cartan subgroup;*
ii) *H is contained in the normalizer of a Cartan subgroup;*

iii) *H is isomorphic to A_4, S_4 or A_5.*

Proof i) If $\widetilde{H}$ is cyclic

B) Now that we have these theorems classifying the subgroups of $\mathrm{GL}(2,\mathbb{F}_\ell)$, we use the information given by the fact that E is an elliptic curve to eliminate the different cases.

We show that:

a) The extension K_ℓ/K is unramified outside the places of bad reduction or the places of K dividing ℓ.

Almost all the places of K are unramified over $\mathbb{Q}$ and at almost all places of K, the curve E has good reduction. Therefore, for almost all ℓ the places of K dividing ℓ are unramified over $\mathbb{Q}$, and E has good reduction there.

b) At such a place v, one can study the inertia subgroup of places w in K_ℓ above v. A local argument proves

Theorem 5. *The inertia subgroup is*

i) *either a cyclic subgroup of order $\ell - 1$ isomorphic to a 1/2-Cartan subgroup $\left(\begin{smallmatrix} * & 0 \\ 0 & 1 \end{smallmatrix}\right)$,*

ii) *or a cyclic subgroup of order $\ell^2 - 1$ isomorphic to $\mathbb{F}_{\ell^2}^\times$.*

Consequently, for almost all ℓ the group G_ℓ cannot be too small because of the following

Theorem 6. *Let $H \subseteq \mathrm{GL}(2,\mathbb{F}_\ell)$ be a subgroup such that H contains a subgroup as in Theorem 5.i). Then exactly one of the following assertions holds:*

- *$H = \mathrm{GL}(2,\mathbb{F}_\ell)$;*
- *H is contained in a Borel subgroup $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$,*
- *H is contained in the normalizer of a Cartan subgroup,*
- *$\ell = 5$, and the image of $\widetilde{H}$ of H in $\mathrm{PGL}(2,\mathbb{F}_\ell)$ is isomorphic to S_4.*

Theorem 6'. *Let $H \subseteq \mathrm{GL}(2,\mathbb{F}_\ell)$ be a subgroup such that H contains a subgroup as in Theorem 5.ii). Then*

- *either $H = \mathrm{GL}(2,\mathbb{F}_\ell)$;*
- *or H is contained in the normalizer of a Cartan subgroup*

Proof of Theorem 6.

If $\ell \mid \#H$ then $H \subseteq \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$ or $\mathrm{SL}(2,\mathbb{F}_\ell) \subseteq H$ but the map $\det : H \longrightarrow \mathbb{F}_\ell^\times$ is onto: thus if $\mathrm{SL}(2,\mathbb{F}_\ell) \subseteq H$ then in fact $H = \mathrm{GL}(2,\mathbb{F}_\ell)$.

If $(\ell, \#H) = 1$, let $\widetilde{H}$ denote the image of H in $\mathrm{PGL}(2,\mathbb{F}_\ell)$. $\widetilde{H}$ contains a cyclic subgroup of order $\ell - 1$, so if $\ell \geq 7$, then $\widetilde{H} \neq$

A_4, S_4, A_5; if $\ell = 5$, then the only possibility is $\widetilde{H} = S_4$; if $\ell = 2, 3$, since A_4, S_4, A_5 contain elements of order 2 and 3 and since $(\ell, \#H) = 1$, we deduce that $\widetilde{H} \neq A_4, S_4, A_5$. Finally, if $\widetilde{H}$ is cyclic or dihedral, then H is contained in a normalizer of a Cartan subgroup.

Proof of Theorem 6'.

If $\ell \mid \#H$ then we cannot have $H \subseteq \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$ since $(\ell^2 - 1) \mid \#H$ and $(\ell^2 - 1) \nmid \ell(\ell - 1)^2$, and again $\mathrm{SL}(2, \mathbb{F}_\ell) \subseteq H$ implies $H = \mathrm{GL}(2, \mathbb{F}_\ell)$.

If $(\ell, \#H) = 1$, then $\widetilde{H}$ contains a cyclic subgroup of order $\ell + 1$. For $\ell \geq 5$, this shows that $\widetilde{H} \neq A_4, S_4, A_5$, and if $\ell = 2, 3$, the argument in the proof of Theorem 6 applies.

Theorems 5, 6 and 6' show

Theorem 7. *For almost all ℓ, the group G_ℓ is*

(i) *isomorphic to* $\mathrm{GL}(2, \mathbb{F}_\ell)$*;*
(ii) *contained in a Borel subgroup or a Cartan subgroup;*
(iii) *or contained in the normalizer of a Cartan subgroup without being contained in a Cartan subgroup.*

It remains to eliminate the cases (ii) and (iii). For (iii), we proceed as follows: G_ℓ is contained in the normalizer of a Cartan subgroup N_ℓ but not contained in the Cartan subgroup C_ℓ. Thus the group G_ℓ / C_ℓ has order 2 (since $(N_\ell : C_\ell) = 2$), hence there exists a field $K'_\ell \subset K_\ell$ which is a quadratic extension of $\mathbb{Q}$ with Galois group G_ℓ / C_ℓ. By considering all possibilities it can be shown that the places of K_ℓ (places dividing ℓ, places not dividing ℓ with good reduction, places not dividing ℓ with bad reduction) that K'_ℓ is unramified over $\mathbb{Q}_\ell$, and since there are only finitely many unramified quadratic extensions of K_ℓ, the case (iii) can occur only finitely often.

The case (ii) is much more difficult. Since G_ℓ is isomorphic to a Cartan or Borel subgroup, there are two characters on G_ℓ with values in $\mathbb{F}_\ell^\times$, and using class field theory it can be shown that E has complex multiplication: this proves the theorem.

References

[1] J.P. Serre, *Abelian l-adic representations and elliptic curves*, McGill University lecture notes 1968 3, 4
[2] J.P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331 3, 4

[3] J.P. Serre, *Lie algebras and Lie groups*, Benjamin 1964 4
[4] N. Bourbaki, *Algèbre Chap. III: Algèbre multilineaire* Paris 1948 5

Translated by Franz Lemmermeyer