Serre on Galois Representations of Elliptic Curves

Translated by Pete L. Clark

Contents

CHAPTER 1

Selections from [MG, Ch. IV]: ℓ-adic representations attached to elliptic curves

This is taken from [**MG**, Ch. IV]. Since it is written in English, it is not a translation on my part, but rather a selection with some commentary. –PLC

Let $E_{/K}$ be an elliptic curve defined over a number field. For a prime number ℓ, let

$$\rho_{\ell^\infty} : \mathfrak{g}_K \to \operatorname{Aut} V_\ell(E)$$

be the ℓ-adic Galois representation. The main result of this chapter is the determination of the Lie algebra of the ℓ-adic Lie group $G_\ell = \rho_{\ell^\infty}(\mathfrak{g}_K)$. This is based on a finiteness theorem of Shafarevich combined with the properties of locally algebraic abelian representations (Ch. III of [**MG**]) and the theory of Tate curves.

1. Preliminaries

Let $E_{/K}$ be an elliptic curve defined over a number field. For a finite place $v \in \Sigma_K$, we denote by $\mathcal{O}_v$ (resp. $\mathfrak{m}_v$, k_v) the corresponding local ring (resp. its maximal ideal, its residue field). We say that E has **good reduction** at v if there is some Weierstrass equation f for E with coefficients in $\mathcal{O}_v$ such that its reduction over k_v is a nonsingular cubic: it is necessary and sufficeint that the discriminant $\Delta(f) \in \emptyset_v^\times$. The curve $\tilde{E}_v$ is the **reduction** of E at v; it does not depend on the choice of f (so long as $\Delta(f) \in \mathcal{O}_v^\times$).

One can show that E has good reduction at v iff there is an abelian scheme E_v over $\operatorname{Spec} \mathcal{O}_v$ with generic fiber E; this scheme is then unique and its special fiber is $\tilde{E}_v$, which is defined over the finite field k_V; we denote its Frobenius endomorphism by F_v.

We see (either way) that E has good reduction for all but finitely many places of K. If E has good reduction at v, then $j(E) \in \mathcal{O}_v$ and its reduction $j(\tilde{E})$ is the j-invariant of the reduced curve $\tilde{E}_v$.

Conversely, if $j \in \mathcal{O}_v$, there is a finite extension L/K such that $E_{/L}$ has good reduction at all places of L dividing v: this is the "potential good reduction" of Serre-Tate [**30**, §2].

REMARK 1. *These definitions and results are not particular to number fields but rather hold for any discretely valued field.*

Let ℓ be a prime number. Put

$$T_\ell = \varprojlim E[\ell^n] \text{ and } V_\ell = T_\ell[\frac{1}{\ell}] = T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell,$$

and let $\rho_{\ell^\infty} : \mathfrak{g}_K \to \operatorname{Aut} T_\ell$ be the ℓ-adic Galois representation.

Let v be a place of K with $p_v \neq \ell$, and let w be some extension to $\overline{K}$; let D_w and I_w be the corresponding decomposition and inertia groups. If E has good reduction at v, then the reduction map gives an isomorphism $E[\ell^n] \xrightarrow{\sim} \tilde{E}_v[\ell^n]$. In particular, $E[\ell^n]$, T_ℓ and V_ℓ are unramified at v and the Frobenius automorphism $F_{v,\rho_{\ell^\infty}}$ of T_ℓ corresponds to the Frobenius endomorphism F_v of $\tilde{E}_v$. Hence:

$$\det F_{v,\rho_{\ell^\infty}} = \det F_v = N_v$$

and

$$\#\tilde{E}_v(k_v) = \det(1 - F_{V,\rho_{\ell^\infty}}) = \det(1 - F_v) = 1 - \operatorname{Tr} F_v + Nv.$$

The converse is also true:

THEOREM 1. *(Criterion of Néron-Ogg-Shafarevich) If V_ℓ is unramified at v for some $\ell \neq p_v$, then E has good reduction at v.*

PROOF. See [**32**, §1]. □

COROLLARY 1. *Let $E_{/K}$ and $E'_{/K}$ be two elliptic curves. If E and E' are K-rationally isogenous, then they have the same places of good reduction.*

PROOF. An isogeny $E \to E'$ induces a Gal_K-isomorphism $V_\ell(E) \to V_\ell(E')$. □

THEOREM 2. *(Shafarevich) Let K be a number field, and let $S \subset \Sigma_K$ be a finite set. The set of K-isomorphism classes of elliptic curves $E_{/K}$ with good reduction outside of S is finite.*

Since isogenous elliptic curves have the same places of bad reduction, we have the following important consequence.

COROLLARY 2. *For every elliptic curve defined over a number field $E_{/K}$, the number of K-isomorphism classes in the K-rational isogeny class of E is finite.*

To prove Shafarevich's Theorem we will use the following result. This is a version of the existence of global minimal Weierstrass models over a PID. –PLC

LEMMA 1. *Let K be a number field, and let $S \subset \Sigma_K$ be a finite subset containing all places lying over 2 and 3, and such that the S-integer ring $\mathcal{O}_S$ is a PID. Then an elliptic curve $E_{/K}$ has good reduction outside of S iff it admits a Weierstrass equation of the form*

$$y^2 = 4x^3 - g_2 x - g_3, \text{ with } g_i \in \mathcal{O}_S \text{ and } \Delta = g_2^3 - 27g_3^2 \in \mathcal{O}_S^\times.$$

PROOF. □

Now we give the proof of Theorem 2. After adding finitely many places to S if needed, we may assume that S contains all places lying over 2 and 3 and that $\mathcal{O}_S$ is a PID. If $E_{/K}$ has good reduction outside of S, Lemma 1 gives us a Weierstrass model of the form

$$(*) y^2 = 4x^3 - g_2 x - g_3$$

with $g_i \in \mathcal{O}_s$ and $\Delta = g_2^3 - 27g_3^2 \in \mathcal{O}_S^\times$. Since we may multiply Δ by any $u \in \mathcal{O}_S^{\times 12}$, and since $\mathcal{O}_S^\times / \mathcal{O}_S^{\times 12}$ is a finite group Dirichlet S-Unit Theorem. –PLC, we see that there is a finite subset $X \subset \mathcal{O}_S^\times$ such that any elliptic curve of the above type can be written in the form $(*)$ with $g_i \in \mathcal{O}_S$ and $\Delta \in X$. For fixed Δ, the equation

$$U^3 - 27V^2 = \Delta$$

has only finitely many solutions in $\mathcal{O}_S$: Siegel's Theorem [**AECI**, §IX.3].

2. The Galois Modules Attached to E

An elliptic curve $E_{/K}$ defined over a number field has **K-rational CM** if the ring of K-rational endomorphisms is larger than $\mathbb{Z}$. In other words, E has complex multiplication and the ground field contains the CM field. – PLC

LEMMA 2. *Let K be a number field, and let $E_{/K}$ be an elliptic curve without K-rational CM, and let $E' \to E$, $E'' \to E$ be K-rational isogenies with cyclic kernels of orders $n_1 \neq n_2$. Then $E' \not\cong_K E''$.*

THEOREM 3. *Suppose $E_{/K}$ is an elliptic curve defined over a number field without K-rational CM. Then:*
(a) V_ℓ is irreducible for all primes ℓ, and
(b) $E[\ell]$ is irreducible for all but finitely many primes ℓ.

The following result is the main theorem of [**MG**].

THEOREM 4. *Let $E_{/K}$ be an elliptic curve defined over a number field K. If E has no CM, then $\rho_{\ell^\infty}(\mathrm{Gal}_K)$ has finite index in $\mathrm{Aut}\, T_\ell(E)$.*

3. Variation of G_{ℓ^∞} and G_ℓ with ℓ

Let

$$\hat{\rho} : \mathrm{Gal}_K \to \prod_\ell \mathrm{Aut}\, T_\ell \cong \mathrm{GL}_2\, \hat{Z}$$

be the adelic Galois representation. Put

$$\begin{aligned} G &= \hat{\rho}(\mathrm{Gal}_K), \\ G_{\ell^\infty} &= \rho_{\ell^\infty}(\mathrm{Gal}_K), \\ G_\ell &= \rho_\ell(\mathrm{Gal}_K). \end{aligned}$$

LEMMA 3. *Let $E_{/K}$ be an elliptic curve over a number field K. We have:*
(i) $\det G$ is open in $\hat{\mathbb{Z}}^\times$.
(ii) For all but finitely many ℓ we have $\det G_{\ell^\infty} = \mathbb{Z}_\ell^\times$ and $\det G_\ell = \mathbb{F}_\ell^\times$.

PROOF. Left to the reader: an exercise on the cyclotomic character. –PLC □

To get from the ℓ-adic open image theorem to an adelic open image theorem, we have the following key result.

LEMMA 4. *(MAIN LEMMA) Let $G \subset \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$ be a closed subgroup, and let G_{ℓ^∞} and G_ℓ denote its images in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ and $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Suppose:*
(i) G_{ℓ^∞} is open in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for all primes ℓ;
(ii) $\det G$ is open in $\hat{\mathbb{Z}}^\times$; and
(iii) G_ℓ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ for all but finitely many ℓ.
Then G is open (equivalently, has finite index) in $\mathrm{GL}_2\, \hat{\mathbb{Z}}$.

PROPOSITION 1. *Suppose that $E_{/K}$ is a non-CM elliptic curve defined over a number field. The following are equivalent:*
(i) G is open in $\prod_\ell \mathrm{Aut}\, T_\ell$.
(ii) $G_{\ell^\infty} = \mathrm{Aut}\, T_\ell$ for all but finitely many ℓ.
(iii) $G_\ell = \mathrm{Aut}\, E[\ell]$ for all but finitely many ℓ.
(iv) $G_\ell \supset \mathrm{SL}\, E[\ell]$ for all but finitely many ℓ.

PROOF. (i) $\Longrightarrow$ (ii) $\Longrightarrow$ (iii) $\Longrightarrow$ (iv) is immediate. To show (iv) $\Longrightarrow$ (i), we plug Theorem 4 and Lemma 3 into Lemma 4. □

3.1. Proof of the Open Image Theorem for non-Integral j.

The following is a special case of the main theorem of Serre's 1972 paper. It is interesting to see how much easier the proof becomes under an additional hypothesis. It is also related to many examples given in §5 of that paper.

THEOREM 5. *Let $E_{/K}$ be an elliptic curve defined over a number field such that $j(E) \notin \mathcal{O}_K$. Then E satisfies the equivalent properties of Proposition 1.*

3.2. Proof of the Main Lemma.

CHAPTER 2

Galois properties of points of of finite order on elliptic curves

Introduction

The present work completes my McGill course [**MG**]. It concerns showing that the Galois groups associated to torsion points on elliptic curves are "as large as possible". The methods of [**MG**] succeed if we restrict ourselves to points of order ℓ^n for ℓ a fixed prime number. They become insufficient when one varies ℓ: it is essentially this variation that we are going to study.

More precisely, let K be a number field, $\overline{K}$ an algebraic closure of K, and let $G = \mathrm{Aut}(\overline{K}/K)$. Let $E_{/K}$ be an elliptic curve. Then $E(\overline{K})$ is a G-module. If $n \in \mathbb{Z}^+$, we denote by $E[n]$ the subgroup $E(\overline{K})[n]$; this is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2, and the action of G on $E[n]$ is given by a homomorphism

$$\rho_n : G \to \mathrm{Aut}\, E[n] \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

The group $\rho_n(G)$ is the Galois group of the extension $K(E[n])/K$ obtained by adjoining the coordinates of the points of $E[n]$.

The properties of ρ_n are well known when E has complex multiplication, i.e., when the ring of $\overline{K}$-endmorphisms has rank 2 over $\mathbb{Z}$ [**9**], [**10**], [**30**] as well as §4.5. For now let us steer clear of this case; otherwise put we suppose that E does not have complex multiplication. The result we have in mind can be stated as follows:

(1) The index of $\rho_n(G)$ in $\mathrm{Aut}\, E[n] \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ is bounded by a constant depending only on E and K.

It is of interest to reformulate (1) by "passing to the limit" on n. The group $\mathrm{Aut}(E[\mathrm{tors}])$ is the inverse limit of the finite groups $\mathrm{Aut}\, E[n]$; this is a profinite group, isomorphic to

$$\varprojlim \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) = \mathrm{GL}_2(\widehat{\mathbb{Z}}), \text{ where } \widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}.$$

The action of G on $E[\mathrm{tors}]$ defines a continuous homomorphism

$$\rho_\infty : G \to \mathrm{Aut}\, E[\mathrm{tors}].$$

The assertion (1) is equivalent to:

(2) The group $\rho_\infty(G)$ has finite index in $\mathrm{Aut}\, E[\mathrm{tors}]$.

Because $\rho_\infty(G)$ and $\mathrm{Aut}\, E[\mathrm{tors}]$ are compact, (2) amounts to saying that $\rho_\infty(G)$ is *open* in $\mathrm{Aut}\, E[\mathrm{tors}]$. Otherwise put:

(3) There is $m \in \mathbb{Z}^+$ such that $\rho_\infty(G)$ contains every automorphism of $E[\text{tors}]$ which acts trivially on $E[m]$.

Let $\mathcal{P}$ be the set of prime numbers. If $\ell \in \mathcal{P}$, let $E[\ell^\infty] = \bigcup_n E[\ell^n]$, i.e., the ℓ-primary component of $E[\text{tors}]$. Its automorphism group is isomorphic to $\mathrm{GL}_2(\mathbb{Z}_\ell)$, where $\mathbb{Z}_\ell$ is the ring of ℓ-adic integers. One has

$$E[\text{tors}] = \bigoplus_{\ell \in \mathcal{P}} E[\ell^\infty]$$

and

$$\mathrm{Aut}\, E[\text{tors}] = \prod_{\ell \in \mathcal{P}} \mathrm{Aut}\, E[\ell^\infty] \cong \prod_{\ell \in \mathcal{P}} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Let us write $\rho_{\ell^\infty} : G \to \mathrm{Aut}\, E[\ell^\infty]$ for the ℓ-component of ρ_∞; it gives the action of G on $E[\ell^\infty]$. The assertion (3) is equivalent to the conjunction of the following two statements:

(4) For every $\ell \in \mathcal{P}$, $\rho_{\ell^\infty}(G)$ is open in $\mathrm{Aut}\, E[\ell^\infty]$.

(5) For all but finitely many $\ell \in \mathcal{P}$, $\varphi_\infty(G)$ contains $\mathrm{Aut}\, E[\ell^\infty]$.

The assertion (4) was already known: this is the principal result of [**MG**]: c.f. page IV-11. The new result is (5), which implies:

(6) For all but finitely many $\ell \in \mathcal{P}$, we have $\rho_{\ell^\infty}(G) = \mathrm{Aut}\, E[\ell^\infty]$.

In particular:

(7) For all but finitely many $\ell \in \mathcal{P}$, we have $\rho_\ell(G) = \mathrm{Aut}\, E[\ell]$.

In fact, given what was shown in [**MG**], the assertions (5), (6) and (7) are equivalent [**MG**, IV-19]. Everything comes down to showing (7): otherwise put, if we identify $\mathrm{Aut}\, E[\ell]$ with $\mathrm{GL}_2(\mathbb{F}_\ell)$, we must show that

$$\rho_\ell : G \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

is surjective for all but finitely many ℓ. The main idea of the proof is the following:

Let v be a place of K of residue characteristic ℓ, w a place of $\overline{K}$ extending v, and let I_w be the correponding inertia subgroup of G. We suppose that v is unramified over $\mathbb{Q}$ and E has good reduction at v (as is the case for all but finitely many ℓ). An easy local argument shows that $\rho_\ell(I_w)$ is a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ of one of the following types:

(i) **split semi-Cartan**: a cyclic group of order $\ell - 1$, with matrix representation $\begin{bmatrix} * & 0 \\ 0 & 1 \end{bmatrix}$.
(i′) **semi-Borel**: a solvable group of order $\ell(\ell - 1)$, with matrix representation $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$.
(ii) **nonsplit Cartan**: a cyclic subgroup of order $\ell^2 - 1$.

Thus $\rho_\ell(G)$ contains a subgroup of type (i), (i′) or (ii). Now one can list the subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ which have this property. We deduce that if (7) fails, there is an infinite subset $L \subset \mathcal{P}$ such that for all $\ell \in K$, we are in one of the following situations:

(a) $\rho_\ell(G)$ is contained in a Cartan or a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$; or
(b) $\rho_\ell(G)$ is contained in the normalizer N_ℓ of a Cartan subgroup C_ℓ and *not* contained in C_ℓ.

In case (b) N_ℓ/C_ℓ has order 2 and the homomorphism $G \to N_\ell/C_\ell$ cuts out a quadratic extension K'_ℓ/K; we show that this extension is unramified outside of a finite set of places of K which is independent of ℓ. The compositum K' of K'_ℓ is therefore finite over K This uses Hermite's finiteness theorem from algebraic number theory – PLC. By replacing K by K' we reduce to the case where $\{\rho_\ell\}_{\ell\in L}$ are all of type (a). Let $\tilde{\rho}_\ell : G \to \mathrm{GL}_2(\mathbb{F}_\ell)$ be the *semisimplification* of ρ_ℓ. The groups $\tilde{\rho}_\ell(G)$ are abelian; using class field theory, one can interpret the $\tilde{\rho}_\ell$ as *idele class characters* of K. The family $\{\tilde{\rho}_\ell\}_{\ell\in L}$ enjoys certain global properties – existence of a conductor; rationality of Frobenius elements – and local properties – characters of bounded exponent – which are made explicit later on. These properties allow us to show that the system ρ_ℓ comes from a representation

$$\rho_0 : S_{\mathfrak{m}} \to \mathrm{GL}_2$$

of algebraic groups $S_{\mathfrak{m}}$ defined in [**MG**, Ch. II]. Using the results of [**MG**, Ch. IV] we deduce that E has complex multiplication, contrary to our hypothesis.

The proof sketched above is the subject of §4. The first three sections contain various preliminaries. §1 gives results of a local nature, mainly concerning the tame inertia group and its action of torsion points of elliptic curves and formal groups: we find that this action can by given by products of *fundamental characters* with exponents bounded by the ramification index of the local field considered: the existence of such a bound plays an essential role in what follows (as the hypothesis "locally algebraic" of [**MG**, Ch. III-IV]. §2 compiles some elementary results on subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ and notably on those which contain a Cartan or semi-Cartan. §3 supplements [**MG**] by giving a condition which allows us to show that a system of ℓ-adic representations of a number field comes from a representation of some $S_{\mathfrak{m}}$: this condition is essentially on the mod ℓ reduction: c.f. Thm. 6 of §3.6. §5 contains special results over $\mathbb{Q}$ and gives numerical examples, treated in detail: I have tried to make it as independent as possible of the preceding sections. A final § treats the case of a product of two elliptic curves.

1. Tame Inertia

1.1. Notation.

In this §, K will denote a field which is complete with respect to a discrete valuation v, which we will suppose is normalized: $v(K^\times) = \mathbb{Z}$. Let A denote the valuation ring, $\mathfrak{m}$ is maximal ideal, and put $k = A/\mathfrak{m}$. We suppose that the residue field k has characteristic $p > 0$. Let $e = v(p)$, so $1 \leq e \leq \infty$. Starting in §1.9 we will

assume $e \neq \infty$: i.e., that K has characteristic 0.

When we want to specify the dependence on K we will write $v_K, A_K, \dots, e_K$.

1.2. Galois Groups.

(The results recalled in §1.2 through §1.4 are well known: see for example [**25**, Ch. IV] or [**5**, Ch. I].)

Let K^{sep} be a separable closure of K. The valuation v extends uniquely to K^{sep}, and the corresponding residual field is an algebraic closure $\overline{k}$ of k. We have

$$K^{\mathrm{sep}} \supset K^t \supset K^{\mathrm{unr}} \supset K,$$

where K_{unr} is the maximal unramified extension of K and K^t/K^{unr} is the maximal tamely ramified extension of K. The residue fields of K^{unr} and K^t may be identified with the separable closure k^{sep} of k in $\overline{k}$. We put

$$G = \mathrm{Aut}(K^{\mathrm{sep}}/K),\ I = \mathrm{Aut}(K^{\mathrm{sep}}/K^{\mathrm{unr}}),\ I_p = \mathrm{Aut}(K^{\mathrm{sep}}/K^t).$$

We have $G \supset I \supset I_p$. The group I (resp. I_p) is called the *inertia group* (resp. the *p-inertia group* I would say **wild inertia group** – PLC. of the Galois group G; it is a closed normal subgroup of G. The group $G/I = \mathrm{Aut}(K^{\mathrm{unr}}/K)$ is identified with $G_k = \mathrm{Aut}(k^{\mathrm{sep}}/k)$.

The group I_p is the largest pro-p-group contained in I. The quotient $I^t = I/I_p = \mathrm{Aut}(K^t/K^{\mathrm{unr}})$ is the *tame inertia group* of G (or of K); this group will play an essential role in all that follows.

1.3. Structure of the Tame Inertia Group.

Let d be a positive integer, prime to p. We denote by μ_d the group of dth roots of unity in K^{unr}; under reduction modulo the maximal ideal, this group is identified with the group of dth roots of unity in k^{sep}.

Let x be a uniformizer of K^{unr}, and let $K^d = K^{\mathrm{unr}}(x^{\frac{1}{d}})$. The extension K^d/K^{unr} is totally tamely ramified, with Galois group isomorphic to μ_d. More precisely, if $s \in \mathrm{Aut}(K^d/K^{\mathrm{unr}})$, there is a unique dth root of nuity $\theta_d(s)$ such that

$$s(x^{\frac{1}{d}}) = \theta_d(s) = x^{\frac{1}{d}},$$

and the map $\theta_d : \mathrm{Aut}(K^d/K^{\mathrm{unr}}) \to \mu_d$ defined in this way is an isomorphism. Moreover, K_d and θ_d do not depend on the choice of x, nor on the choice of its dth root.

The field K^t is the union of the K^d for all $\gcd(d,p) = 1$. Thus:

$$I_t = \mathrm{Aut}(K^t/K^{\mathrm{unr}}) = \varprojlim_d \mathrm{Aut}(K^d/K^{\mathrm{unr}}),$$

and we obtain:

PROPOSITION 2. *The isomorphisms θ_d define an isomorphism*

$$\theta : I_t \to \varprojlim_d \mu_d.$$

(To be sure: the transition maps $\mu_{dd'} \to \mu_d$ of the inverse system are $\alpha \mapsto \alpha^{d'}$.)

REMARK 2. *When k is algebraically closed, the group $\varprojlim_d \mu_d$ can be viewed as the fundamental group $\pi_1(\mathbb{G}_m)$ of the multiplicative group $\mathbb{G}_m$ and the isomorphism $\theta : I_t \to \pi_1(\mathbb{G}_m)$ obtained in this way coincides with the one furnished by* geometric *local class field theory, c.f.* [**24**].

We return to the general case. If q is a power of p, let us denote by $\mathbb{F}_q$ the q-element subfield of k^{sep}. We have $\mathbb{F}_q^\times = \mu_{q-1}$. Moreover, the integers of the form $q-1$ are *cofinal* in the set of integers prime to p ordered by divisibility: indeed, if d is susch an integer, there is $n \geq 1$ such that $p^n \equiv 1 \pmod{d}$, for example $n = \varphi(d)$. Thus the inverse system (μ_d) is *equivalent* to the inverse system formed by $\mathbb{F}_q^\times$ and the norm maps

$$N : \mathbb{F}_{q^m} \to \mathbb{F}_q^\times,\ N(\alpha) = \alpha^{1+q+\ldots+q^{m-1}}.$$

Proposition 1 is thus equivalent to:

PROPOSITION 3. *The isomorphisms θ_{q-1} define an isomorphism*

$$\theta : I_t \to \varprojlim \mathbb{F}_q^\times,$$

where $\mathbb{F}_q$ ranges over finite subfields of k^{sep}.

1.4. Functoriality of θ.

Let K' be a closed, non-discrete subfield of K, and let $e(K/K')$ be the ramification index of K over K', in other words the index of $v_K(K'^\times)$ in $\mathbb{Z}$. We denote by $I_{t,K}$ (resp. $I^t_{K'}$) the tame ramification group of K (resp. K'). Then there is an evident homomorphism $I_{t,K} \to I_{t,K'}$ and the diagram

$$\begin{array}{ccc} I^t_K & \xrightarrow{\sim} & \varprojlim \mu_d \\ & & \\ I^t_{K'} & \xrightarrow{\sim} & \varprojlim \mu_d \end{array}$$

with right hand vertical map being multiplication by $e(K/K')$ is *commutative*: one verifies this without difficulty, either directly or by using Proposition 7 below.

1.5. Case of a finite residue field.

In this section we suppose that k is a finite field $\mathbb{F}_q$.

Let L/K be a tamely ramified abelian extension of K. The inertia subgroup $I(L/K)$ of $\mathrm{Aut}(L/K)$ is a quotient of I_t, whence a canonical surjective homomorphism

$$\alpha : I_t \to \varprojlim \mu_d \to I(L/K).$$

On the other hand, local class field theory associates to L/K a homomorphism $\omega : K^\times \to \mathrm{Gal}(L/K)$, the reciprocity map. If U is the group of units of $K^\times$, we have $\omega(U) = I(L/K)$ and $\omega(1+\mathfrak{m}) = \{1\}$, c.f. [**25**, Ch. XV]. As $U/(1+\mathfrak{m}) = k^\times$, we see that ω defines by passage to the quotient a surjective homomorphism

$$\omega : k^\times \to I(L/K).$$

Since $k^\times = \mathbb{F}_q^\times = \mu_{q-1}$, it is natural and biblical? – PLC to compare α and ω.

PROPOSITION 4. *The homomorphisms α and ω are inverses. More precisely, we have*

$$\alpha(s) = \omega \circ \theta_{q-1}(s^{-1}) \text{ for all } s \in I_t,$$

where θ_{q-1} denotes the homomorphism from I_t onto $k^\times = \mu_{q-1}$ defined in §1.3.

PROOF. Put $d = q - 1$. Let x be a uniformizer of K and let $K^d = K^{\mathrm{unr}}(x^{\frac{1}{d}})$, c.f. §1.3. Since $\omega : k^\times \to I(L/K)$ is surjective, $I(L/K)$ is finite of order a divisosr of d, which shows that L is contained in K^d. In view of the functorial properties of α and ω, we may thus suppose that $L = K^d$.

If $s \in I_t$, we have, by definition of θ_d,

$$s(x^{\frac{1}{d}}) = \theta_d(s)x^{\frac{1}{d}}.$$

On the other hand, let $t \in k^\times$, and let $\omega(t)$ be the corresponding element of $I(L/K)$. We have

$$\omega(t)(x^{\frac{1}{d}}) = (x,t)_d x^{\frac{1}{d}},$$

where $(x,t)_d \in \mu_d$ is the *local symbol* associated to x and t, c.f. [**25**, Ch. XIV] (here and hereafter, we identify the element t of $k^\times$ with the corresponding root of unity of $K^\times$, i.e., with its *multiplicative representative*). But, according to a known formula [**25**, p. 217, Cor. to Prop. 8], we have

$$(x,t)_d = t^{-v(x)} = t^{-1}.$$

If we take $t = \theta_d(s^{-1})$, we thus have $\omega(t)(x^{\frac{1}{d}}) = s(x^{\frac{1}{d}})$, and, since s and $\omega(t)$ act trivially on K^{unr}, one sees easily that s and $\omega(t)$ in the same way on $K^d = L$. □

1.6. Representations of G in characteristic p.

Let V be a vector space of finite dimension n over a field k_1 of characteristic p, and let $\rho : G \to \mathrm{GL}\, V$ be a continuous (i.e., with open kernel) linear representation of G on V.

PROPOSITION 5. *If ρ is semisimple, we have $\rho(I_p) = \{1\}$.*
(Recall that I_p is the wild inertia group of $G = \mathrm{Aut}(K^{\mathrm{sep}}/K)$, c.f. §1.2.)

PROOF. It suffices to show that $\rho(I_p) = \{1\}$ when ρ is *simple*. Let V' be the set of elements of V which are pointwise fixed by $\rho(I_p)$. Since $\rho(I_p)$ is a finite p-group, we have $V' \neq 0$ [**25**, p. 146, Thm. 2], and as I_p is normal in G, V' is invariant under $\rho(G)$ a fun three line exercise here – PLC hence equal to V. □

Let us suppose that ρ is semisimple. Proposition 5 shows that I_p acts trivially on V, and the action on I factors through an action on the tame inertia group $I_t = I/I_p$. The image of I_t under ρ is a cyclic group of order prime to p; if k_1 is sufficiently large (e.g. separably closed), on can diagonalize $\rho(I_t)$. Otherwise put, the restriction of ρ to I_t is given by *characters* $\psi_i : I_t \to k_1^\times$, $i = 1, \ldots, n$. We will see a little later on how to make these characters explicit.

EXAMPLE 5. *Let V_p be a vector space of dimension n over the p-adic field $\mathbb{Q}_p$, and let $\varphi : G \to \mathrm{GL}\, V_p$ be a continuous linear representation of G on V_p. Let us choose a $\mathbb{Z}_p$-lattice T_p of V_p stable under G* [**MG**, p. I-1]. *The $\mathbb{F}_p$-vector space T_p/pT_p has dimension n; the natural representation of G on this space is not necessarily semisimple; let us denote by $\tilde{\varphi}$ its* semisimplifiation*, in other words the direct sum of the simple represetantations occuring in a Jordan-Hölder sequence for T_p/pT_p. According to a theorem of Brauer-Nesbitt* [**6**, §82.1]*, the isomorphism class of $\tilde{\varphi}$ does not depend on the choice of lattice T_p. Applying Proposition 5 to $\tilde{\varphi}$ one obtains a representation of the group G/I_p, hence characters $\psi_1, \ldots, \psi_n$ of I_t as above.*

This applies notably to the representation ρ attached to the Tate module V_p of

an abelian variety (resp. a p-divisible group) defined over K (resp. defined over the ring A), it being understood that K has characteristic 0.

1.7. Characters of I_t.

We are going to make explicit the group $X = \mathrm{Hom}(I_t, k^{\mathrm{sep}\,\times})$ of continuous characters of I_t with values in $k^{\mathrm{sep}\,\times}$ (or in the union of the $\mathbb{F}_q^\times$, which amounts to the same thing).

The characters $\theta_d : I_t \to \mathrm{Aut}(K^d/K^{\mathrm{unr}}) \cong \mu_d$ of §1.3 belong to X, and we will use them to *parameterize* X. More precisely, we denote by $(\mathbb{Q}/\mathbb{Z})'$ the set of elements of $\mathbb{Q}/\mathbb{Z}$ of order prime to p. Every element α of $(\mathbb{Q}/\mathbb{Z})'$ can be written as $\alpha = \frac{a}{d}$ with $a, d \in \mathbb{Z}$ and $\gcd(d,p) = 1$; denote by χ_a the ath power of θ_d; one checks immediately that χ_α depends only on α and not on a and d. Morover:

PROPOSITION 6. *The map $\alpha \mapsto \chi_\alpha$ is an isomorphism from $(\mathbb{Q}/\mathbb{Z})'$ to the group X of characters of I_t.*

PROOF. The group $(\mathbb{Q}/\mathbb{Z})'$ is the union of the subgroups $\frac{1}{d}\mathbb{Z}/\mathbb{Z}$; on the other hand I_t is the inverse limit of the μ_d, and X is the direct limit of the groups $X_d = \mathrm{Hom}(\mu_d, k^{\mathrm{sep}\,\times})$. The proposition follows from this and the fact that $\alpha \mapsto \chi_\alpha$ is an isomorphism from $\frac{1}{d}\mathbb{Z}/\mathbb{Z}$ onto X_d. □

If $\psi \in X$, the element α of $(\mathbb{Q}/\mathbb{Z})'$ such that $\psi = \chi_\alpha$ is called the *invariant* of ψ. In particular the invariant of θ_d is $\frac{1}{d}$.

REMARK 3. *The p-primary component of $\mathbb{Q}/\mathbb{Z}$ is $\mathbb{Q}_p/\mathbb{Z}_p$, and we have direct sum decompositions*

$$\mathbb{Q}/\mathbb{Z} = \mathbb{Q}_p/\mathbb{Z}_p \oplus (\mathbb{Q}/\mathbb{Z})' \text{ and } (\mathbb{Q}/\mathbb{Z})' = \bigoplus_{\ell \neq p} \mathbb{Q}_\ell/\mathbb{Z}_\ell.$$

We have in particular a canonical projection $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to (\mathbb{Q}/\mathbb{Z})'$ with kernel $\mathbb{Z}[\frac{1}{p}]$. If $\alpha \in \mathbb{Q}$, we will allow ourselves to denote by χ_α the character $\chi_{\alpha'}$ corresponding to t he image α' of α in $(\mathbb{Q}/\mathbb{Z})'$, and we will say that the invariant of χ_α is α (mod $\mathbb{Z}[\frac{1}{p}]$).

EXAMPLE 6. *(Fundamental Characters) Let $n \in \mathbb{Z}^+$, and let $q = p^n$. A* fundamental character of level n *is a character obtained by composing the character*

$$\theta_{q-1} : I_t \to \mu_{q-1} = \mathbb{F}_q^\times$$

with a field *isomorphism of $\mathbb{F}_q$; in other words such a character is conjugate over $\mathbb{F}_p$ to the character θ_{q-1}; one can write it as*

$$\chi = \theta_{q-1}^{p^i}, i = 0, 1, \ldots, n-1.$$

There are thus n fundamental characters of level n; their invariants are $\frac{p^i}{q-1} = \frac{p^i}{p^n-1}$, where $0 \leq i \leq n-1$.

More generally, let k_1 be a field of characteristic p. A character χ of I_t with values in $k_1^\times$ is fundamental of level n *if it is obtained by composing θ_{q-1} with a field embedding $\mathbb{F}_q \hookrightarrow k_1$.*

1.8. Representation of G on $\mathfrak{m}_\alpha/\mathfrak{m}_\alpha^+$.

We extend the valuation v from K to K^{sep}; in this way we obtain a valuation on K^{sep} with value group $v(K^{\mathrm{sep}\,\times})$ equal to $\mathbb{Q}$. For $\alpha \in \mathbb{Q}$, denote by $\mathfrak{m}_\alpha$ (resp. $\mathfrak{m}_\alpha^+$) the set of $x \in K^{\mathrm{sep}}$ with $v(x) \geq \alpha$ (resp. $v(x) > \alpha$); the quotient

$$V_\alpha = \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^+$$

is a vector space of dimension 1 over the residue field $\overline{k}$ of K^{sep}. The group $G = \mathrm{Aut}(K^{\mathrm{sep}}/K)$ acts naturally on V_α.

PROPOSITION 7. *Let $s \in G$, and let σ be the image of s in the group $G_K = \mathrm{Aut}(k^{\mathrm{sep}}/k) = \mathrm{Aut}(\overline{k}/k)$. The automorphism of V_α defined by s is σ-linear.*

PROOF. Indeed, the map $(\lambda, x) \mapsto \lambda x$ from $\overline{k} \times V_\alpha$ to V_α commutes with the action of G, hence we have

$$s(\lambda x) = s(\lambda)s(x) = \sigma(\lambda)s(x),$$

which means by definition – PLC that $x \mapsto s(x)$ is σ-linear. □

According to Proposition 7 the elements of I act *linearly* on V_α; since V_α has dimension 1, that means that I acts on V_α by means of a *character* $\varphi_\alpha : I \to \overline{k}^\times$; we have

$$s(x) = \varphi_\alpha(s)x \text{ for all } s \in I \text{ and } x \in V_\alpha.$$

Since $\overline{k}^\times$ contains no element of order p, the character φ_α is trivial on I_p, hence can be considered as a character on the tame inertia group $I_t = I/I_p$.

PROPOSITION 8. *The character φ_α giving the action of I_t on V_α is the character χ_α defined in* §1.7.

PROOF. Let $\alpha, \beta \in \mathbb{Q}$. The map $(x, y) \mapsto xy$ from $\mathfrak{m}_\alpha \times \mathfrak{m}_\beta$ to $\mathfrak{m}_{\alpha+\beta}$ defines by passage to the quotient an isomorphism from $V_\alpha \otimes V_\beta$ to $V_{\alpha+\beta}$; this isomorphism commutes with the G-action. One concludes that $\varphi_{\alpha+\beta} = \varphi_\alpha\varphi_\beta$, otherwise put that $\alpha \mapsto \varphi_\alpha$ is a homomorphism.

On the other hand, let d be a positive integer prime to p, and elt x be a dth root of a uniformizer of K. We have

$$v(x) = \frac{1}{d} \text{ and } s(x) = \theta_d(x)x \text{ for all } s \in I_t, \text{ c.f. } \S 1.3.$$

It follows that $\varphi_{\frac{1}{d}} = \theta_d = \chi_{\frac{1}{d}}$. Thus, since $\alpha \in \mathbb{Q}$, there is a power q of p such that $q\alpha = \frac{a}{d}$ with $a \in \mathbb{Z}$ and d positive and prime to p. In view of the additivity of the maps $\alpha \mapsto \varphi_\alpha$ and $\alpha \mapsto \chi_\alpha$ we conclude that

$$\varphi_\alpha^q = \varphi_{\frac{a}{d}} = \varphi_{\frac{1}{d}}^a = \chi_{\frac{1}{d}}^a = \chi_\alpha^q,$$

whence $\varphi_\alpha = \chi_\alpha$ since the character group of I_t has no p-torsion. □

Application: the action of I_t on μ_p

Suppose that K has characteristic 0. Let μ_p be the group of pth roots of unity in K^{sep}. The group G acts on μ_p and its subgroup I_p acts trivially (Prop. 4). We thus obtain an action of I_t on μ_p, whence a character now called the mod p cyclotomic character – PLC

$$\chi : I_t \to \mathbb{F}_p^\times = \mathrm{Aut}(\mu_p).$$

PROPOSITION 9. *The character χ giving the action of I_t on μ_p is the eth power of the fundamental character θ_{p-1} of level 1.*
(Recall that $e = v(p)$ is the absolute ramification index of K.)

PROOF. Put $\alpha = \frac{e}{p-1}$. If $z \in \mu_p \setminus \{1\}$, we know that $v(z-1) = \alpha$. We thus conclude that the map $z \mapsto z-1$ induces by passage to the quotient an injective homomorphism of μ_p into V_α; this homomorphism commutes with the action of G, and in particular with that of I_t. The proposition follows, since I_t acts on V_α via the character $\chi_\alpha = \theta_{p-1}^e$, c.f. Prop. 8. □

COROLLARY 3. *If $e = 1$, then $\chi = \theta_{p-1}$.*

1.9. Representation of G defined by a formal group ($e = 1$ case).

In this section we suppose that $e = 1$, i.e., that p is a uniformizer of K; in particular, K has characteristic 0. We denote by A^{sep} he valuation ring of K^{sep} and by $\mathfrak{m}^{\text{sep}}$ the maximal ideal of A^{sep}. Let

$$F(X,Y) = X + Y + \sum_{i,j \geq 1} c_{ij} X^i Y^j,\ c_{ij} \in A$$

a one-dimensional *formal group law* over the ring A (c.f. e.g. [**12**, Ch. III-IV]). Let

$$[p](X) = \sum_{i=1}^{\infty} a_i X^i,\ a_i \in A$$

be the "multiplication by p" map for the group law F; this is a formal power series for which the first coefficient a_1 is equal to p. We suppose that F has *finite height* h [**12**, Ch. IV, §2]; if we put $q = p^h$, this means that we have

$$a_i \in \quad (\text{mod } \mathfrak{m})\ \forall i < q,\ a_q \notin \mathfrak{m},$$

so that the reduction modulo $\mathfrak{m}$ of $[p]$ has leading term X^q.

We denote by V the *kernel of* $[p]$, i.e., the set of $x \in \mathfrak{m}^{\text{sep}}$ such that $[p](x) = 0$; we furnish V with the composition law $(x,y) \mapsto F(x,y)$. One knows (c.f. [**14**] or [**12**, p. 107]) that V is an $\mathbb{F}_p$-vector space of dimension h. The group G acts naturally on V, and we find ourselves in the situation of §1.6.

PROPOSITION 10. *There exists on V the structure of a 1-dimensional $\mathbb{F}_q$-vector space enjoying the following properties:*
(i) For $s \in G$, let σ be the image of s in $G_k = \text{Aut}(k^{\text{sep}}/k)$, and let σ_q be the restriction of σ to $\mathbb{F}_q$. The automorphism of V defined by s is σ_q-linear.
(ii) The group I_p acts trivially on V, and the group $I_t = I/I_p$ acts by means of the fundamental character $\theta_{q-1} : I_t \to \mathbb{F}_q^\times$ of level h.
(Recall that $\mathbb{F}_q$ is the subfield of $q = p^h$ elements of k^{sep}.)

PROOF. The proof is essentially the same as that of Proposition 9 (which we recover by taking for F the multiplicative formal group law $X + Y + XY$). If x is a nonzero element of V, we have

$$p + a_2 x + \ldots + a_q x^{q-1} + \ldots = 0,$$

and as the a_i are divisible by p for $i < q$, one sees, by comparing valuations, that $v(x) = \frac{1}{q-1}$. Put $\alpha = \frac{1}{q-1}$. If $x, y \in V$, then $x, y \in \mathfrak{m}_\alpha$ and

$$F(x,y) \equiv x + y \pmod{\mathfrak{m}_\alpha^+}.$$

We deduce that the projection $\mathfrak{m}_\alpha \to V_\alpha = \mathfrak{m}_\alpha/\mathfrak{m}_\alpha^+$ defines an injective homomorphism $V \hookrightarrow V_\alpha$; this homomorphism commutes with the G-action, which already shows that I_p acts trivially on V. If we identify V with its image in V_α, then Proposition 8 shows that I_t acts on V according to the formula

$$s(x) = \theta_{q-1}(s)x \text{ if } s \in I_t,\ x \in V.$$

Since $\theta_{q-1} : I_t \to \mathbb{F}_q^\times$ is surjective, this implies that V is stable under multiplication by $\mathbb{F}_q^\times$ and thus is an $\mathbb{F}_q$-subspace of V_α; since $\#V = q$, it has dimension 1. Then (i) follows from Propostion 7 and (ii) follows from Proposition 8. □

COROLLARY 4. *The image of I_t in $\mathrm{GL}\,V$ is formed by the homotheties $x \mapsto \lambda v$ with $\lambda \in \mathbb{F}_q^\times$; this is a cyclic group of order $q-1$.*

PROOF. This results from the fact that $\theta_{q-1} : I_t \to \mathbb{F}_q^\times$ is surjective. □

COROLLARY 5. *Suppose $k = \mathbb{F}_p$. The image of G in $\mathrm{GL}\,V$ is formed by all semilinear automorphisms of the $\mathbb{F}_q$-vector space V.*
(In other words, the image of G in $\mathrm{GL}_h(\mathbb{F}_p)$ is the normalizer of the Cartan subgroup $\mathbb{F}_q^\times$.)

PROOF. Indeed, the hypothesis $k = \mathbb{F}_p$ implies that every automorphism of $\mathbb{F}_q$ is of the form σ_q, hence is induced by an element of G. □

REMARK 4. *1) The $\mathbb{F}_q$-vector space structure on V is independent of the choice of x; it depends only on the* formal group *defined by F.*

2) Let k_1 be an algebraic closure of $\mathbb{F}_p$ and $V_1 = k_1 \otimes_{\mathbb{F}_p} V$. The action of G on V extends to a k_1-linear action on V_1; moreover, upon restriction to I_t one can diagonalize this action (§1.6). More precisely:

COROLLARY 6. *The h characters giving the action of I_t on V_1 are the h fundamental characters $I_t \to k_1^\times$ of level h.*

PROOF. Indeed, let Γ be the set of embeddings of $\mathbb{F}_q$ in k_1. For $\gamma \in \Gamma$, let $V_{(\gamma)}$ be the 1-dimensional vector space obtained from V via scalar extension $\gamma : \mathbb{F}_q \to k_1$. One checks immediately that V_1 is the direct sum $\bigoplus_{\gamma\in\Gamma} V_{(\gamma)}$ and that I_t acts on $V_{(\gamma)}$ via the character $\gamma \circ \theta_{q-1}$. The corollary follows, since $\gamma \circ \theta_{q-1}$ are precisely the h fundamental characters of I_t of level h. □

1.10. Representation of G defined by a formal group (general case).

The results of §1.9, concerning the case $e = 1$, are sufficient for the applications we have in view. We will limit ourselves to rapidly indicating what happens when e is any integer.

Let F be a one-dimensional formal group law over A, of finite height h, and let $[p](X)$ be the corresponding multiplication by p map:

$$[p])(X) = \sum_{i=1}^{\infty} a_i X_i,$$

with $a_i \in A$, $a_1 = p$, $v(a_i) \geq 1$ if $i < q = p^h$ and $v(a_q) = 0$.

Again we denote by V the kernel of $[p]$ on $\mathfrak{m}^{\mathrm{sep}}$; this is an $\mathbb{F}_p$-vector space of dimension h. The valuations of the element of V can be read off of the *Newton*

polygon[1] of the formal power series $[p](X)$. Because we are only concerned with elements of positive valation, only the part of the polygon of negative slope interests us. In view of the properties of the $v(a_i)$'s given above, this part is a "broken line" i.e., piecewise linear – PLC whose projection onto the axis Ox is the segment $[1, q]$. Let $P_i = (q_i, e_i)$ be the vertices, with

$$1 = q_0 < q_1 < q_2 < \ldots < q_m = q.$$

There is a figure at this point which I do not reproduce – PLC.
We have $e_i = v(a_{q_i})$ and in particular $e_0 = v(a_1) = v(p) = e$ and $e_m = v(a_q) = 0$; the e_i's form a strictly decreasing sequence.

The *slope* of the ith side $P_{i-1}P_i$ is $-\alpha_i$, where $\alpha_i = \frac{e_{i-1}-e_i}{q_i-q_{i-1}}$, and the length of the projection of $P_{i-1}P_i$ on Ox is $q_i - q_{i-1}$. It follows that *the number of elements of V of valuation α_i is $q_i - q_{i-1}$* and that *every nonzero element of V has valuation α_i for some i*. We have

$$\alpha_1 > \alpha_2 > \ldots > \alpha_m.$$

For $1 \leq i \leq m$, let $V^i = \{x \in V \mid v(x) \geq \alpha_i\}$; put $V^0 = \{0\}$. One checks without difficulty that the V^i are *subgroups* of V; they form a *strictly increasing filtration*

$$0 = V^0 \subset V^1 \subset V^2 \subset \ldots \subset V^m = V.$$

Since $\#V^i = q_i$, we conclude that q_i is of the form p^{h_i} with $0 < h_1 < h_2 < \ldots < h_m = h$. Put $\mathrm{gr}^i V = V^i/V^{i-1}$ for $i = 1, \ldots, m$. The group G acts on V and preserves the filtration $\{V^i\}$, so it also acts on $\mathrm{gr}^i V$ for all i.

PROPOSITION 11. *a) The group I_p acts trivially on $\mathrm{gr}^i V$.*
b) Let k_1 be an algebraic closure of $\mathbb{F}_p$. The characters giving the action of I_t on $k_1 \otimes_{\mathbb{F}_p} \mathrm{gr}^i V$ are the $(e_{i-1} - e)$th powers of the fundamental characters of level $h_i - h_{i-1}$.

PROOF. The inclusion of V^i in $\mathfrak{m}_{\alpha_i}$ defines by passage to the quotient an injective homomorphism $\mathrm{gr}^i V \to V_{\alpha_i} = \mathfrak{m}_{\alpha_i}/\mathfrak{m}^+_{\alpha_i}$. Since I_p acts trivially on V_{α_i}, this shows part a). For b), we first remark that I_t acts on V_{α_i} by the character χ_{α_i}; writing α_i in the form

$$\alpha_i = \frac{e_{i-1} - e_i}{p^{h_{i-1}}(p^{h_i - h_{i-1}} - 1)},$$

we see that χ_{α_i} is he $(e_{i-1} - e_i)$th power of one of the fundamental characters of level $h_i - h_{i-1}$; the assertion (b) can be deduced from this without great difficulty ! – PLC using the fact that the set of characters of I_t giving the action of this group on $k_1 \otimes \mathrm{gr}^i V$ is invariant under conjugation over $\mathbb{F}_p$. □

REMARK 5. *We will see that the exponents $e_{i-1} - e_i$ which show up in part b) are* between 1 and e*; we will return to this point in* §1.13.

1.11. Representation of G defined by an elliptic curve having good reduction.

In this section as well as the next, we suppose that K has characteristic 0. The

[1]For all that concerns Newton polygons and formal power series, see for instance F. Bruhat, *Lecture on some aspects of p-adic analysis*, pp. 111-114, Tata Institute, Bombay, 1963.

letter E denotes an elliptic curve[2] over K. We denote by $E[p]$ the kernel of multiplication by p in $E(K^{\mathrm{sep}})$; this is an $\mathbb{F}_p$-vector space of dimension 2. We are interested in the natural representation of G on $E[p]$. As $\wedge^2 E[p]$ is canonically isomorphic to the group μ_p of pth roots of unity [**4**, Thm. 8.1], the *determinant* of the representation of G in $E[p]$ is the cyclotomic! – PLC character $G \to \mathbb{F}_p^\times$ giving the action of G on μ_p; according to Proposition 8, the restriction of this character to I_t is the eth power of the fundamental character θ_{p-1} of level 1. This gives a first piece of information about the Galois module $E[p]$.

Let us now make the hypotheses that E has *good reduction* over A; this means that one can represent E by a plane cubic equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with coefficients $a_i \in A$, the discriminant $\Delta = \Delta(a_1, \ldots, a_6)$ being *invertible* in A (for a formula giving Δ, see for example §5.1); the point at infinity is taken as the origin. If $\tilde{a}_i$ denotes the image of a_i in k, the equation

$$y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6$$

defines an elliptic curve $\tilde{E}$ over k, called the **reduction of E modulo $\mathfrak{m}$**. Let us now distinguish two cases:

(i) Good reduction of height 1 Henceforth called **ordinary reduction** – PLC

This is the case in which the Hasse invariant of $\tilde{E}$ is nonzero c.f. [**8**]; the kernel of multiplication by p on $\tilde{E}(\overline{k})$ is a group $\tilde{E}[p]$ of order p. We have an exact sequence

$$0 \to X[p] \to E[p] \to \tilde{E}[p] \to 0,$$

where $E[p] \to \tilde{E}[p]$ is the reduction map modulo $\mathfrak{m}^{\mathrm{sep}}$; the kernel $X[p]$ is cylic of order p. The group G stabilizes $X[p]$. If we choose a basis (e_1, e_2) of $E[p]$ such that $x[p] = \langle e_1 \rangle_{\mathbb{F}_p}$, then the image of G in $\operatorname{Aut} E[p] = \mathrm{GL}_2 \mathbb{F}_p$ is *contained in the Borel subgroup* $\begin{bmatrix} * & * \\ 0 & * \end{bmatrix}$. The image of I_p is contained in the unipotent group $\begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}$; the group I_t acts on $X[p]$ (resp. on $\tilde{E}_p$) by means of a character χ_X (resp. χ_Y) with values in $\mathbb{F}_p^\times$. In fact:

Proposition 12. *(Good ordinary reduction) We have*

$$\chi_X = \theta_{p-1}^e, \ \chi_Y = 1.$$

Proof. The fact that $\chi_Y = 1$ results from the fact that G acts on $\tilde{E}[p]$ via the canonical homomorphism $G \to G_k$. On the other hand, the product $\chi_X\chi_Y$ is the determinant of the action of I_t on $E[p]$, hence equal to θ_{p-1}^e, according to what we saw earlier more precisely, by Proposition 9 – PLC. □

Corollary 7. *Suppose $e = 1$. Then:*
a) The two characters giving the action of I_t on the semisimplifcation of $E[p]$ are the trivial character and the fundamental character θ_{p-1}.
b) If I_p acts trivially on $E[p]$, the image of I in $\mathrm{GL}\, E[p]$ is a cyclic group of order

[2]For general properties of elliptic curves, see Cassels [**4**], Deuring [**8**], Roquette [**22**] and Mumford [**15**, pp. 214-220]. For Néron models and the properties of good or bad reudction, see Néron [**16**], Ogg [**19**] and [**30**].

$p-1$, representable by matrices of the form $\begin{bmatrix} * & 0 \\ 0 & 1 \end{bmatrix}$*, by means of a basis* (e_1, e_2) *of* $E[p]$ *with* $e_1 \in X[p]$.
c) If I_p *does not act trivially on* $E[p]$*, the image of* I *in* $\mathrm{GL}\, E[p]$ *has order* $p(p-1)$. *It is representable by matrices of the form* $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$.

PROOF. Part a) is immediate. It follows that $\chi_X : I_t \to \mathbb{F}_p^\times$ is surjective, so the image of I has order divisible by $p-1$. Since this image is a subgroup of the group $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$, its order is either $p-1$ or $p(p-1)$. The former case corresponds to part b), the latter to part c). □

REMARK 6. *I do not know a simple criterion for recongizing whether one is in case b) or case c). The question is visibly linked to one of the* canonical lifting of $\tilde{E}$.

Here is a related question: let E_0 *be an elliptic curve, without CM, over a number field* K_0. *Denote by* Σ_b *(resp.* Σ_c*) the set of places of* K_0 *at which* E_0 *has good ordinary reduction and of type b) (resp. of type c)) in the above sense. One knows that the* density *of* $\Sigma_b \cup \Sigma_c = 1$ [**26**, Cor. 1 to Thm. 6]*; see also* [**MG**, p. IV-13, Exc.]. *This type of problem is why I started reading this paper as a student in (I think) 2000. – PLC Can we determine the densities of* Σ_b *and* Σ_c*? Is it true that the density of* Σ_b *is* 0*?*

(ii) Good reduction of height 2 Henceforth called **supersingular reduction** – PLC

This is the case in which $\tilde{E}$ has Hasse invariant zero; the curve $\tilde{E}$ has no points of order p, and every element of $E[p]$ reduces to the identity element of $\tilde{E}$.

Let us write as above the equation of E in the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in A$ and $\Delta \in A^\times$. If $(x, y) \in E(K^{\mathrm{sep}})$ reduces to the identity element of $\tilde{E}$, one sees easily that $t = \frac{x}{y}$ belongs to $\mathfrak{m}^{\mathrm{sep}}$, and every element of $\mathfrak{m}^{\mathrm{sep}}$ is obtained exactly once in this way. Moreover, the composition law on the elliptic curve E induces a *formal group law*

$$F(t, t') = t + t' + a_1tt' - a_2(t^2t' + t(t')^2) + \dots$$

with coefficients in A. (The associated formal group is the *formal completion* of the Néron model of E over A.)

Let $[p](t) = pt + a_1\binom{p}{2}t^2 + \dots$ be the formal power series giving multiplication by p with respect to F (c.f. §1.9). According too the above, the group $E[p]$ is identifed under $(x, y) \mapsto t = \frac{x}{y}$ with the *kernel* of $[p]$. Since $\#E[p] = p^2$, it follows that the height h of F is 2, a result which one can also see directly. We may therefore apply Proposition 9 and its corollaries. Thus:

PROPOSITION 13. *(Good supersingular reduction) Suppose* $e = 1$. *Then:*
a) The action of I_p *on* $E[p]$ *is trivial.*
b) There exists on $E[p]$ *the structure of a one-dimensional* $\mathbb{F}_{p^2}$*-vector space such that the action of* I_t *is given by the fundamental character* θ_{p^2-1} *of level* 2.
c) The image of I *in* $\mathrm{GL}\, E[p]$ *is a cyclic group of order* $p^2 - 1$ *(nonsplit Cartan*

subgroup; c.f. §2.1*).*
d) The image of G in $\mathrm{GL}\, E[p]$ *is equal to C or to its normalizer N according to whether k contains or does not contain $\mathbb{F}_{p^2}$.*

In particular:

COROLLARY 8. *Let K_1 be an algebraic closure of $\mathbb{F}_p$. The action of I_t on $k_1 \otimes E[p]$ is given by the two fundamental characters $I_t \to k_1^\times$ of level* 2.

REMARK 7. *When $e > 1$, Proposition 11 gives information on the Galois module $E[p]$, under the condition that one knows the Newton polygon of the formal power series $[p](t)$. There is a recent* Pacific Journal *paper of Álvaro Lozano-Robledo which is very much in the spirit of this remark. – PLC In view of what was shown in* §1.10*, it suffices to know the* valuation *of the pth coefficient of this formal power series. Here is a simple example:*

Let us take $p = 5$, and suppose that E has the form

$$y^2 = x^3 + a_4 x + a_6 \text{ with } v(a_4) > 0 \text{ and } v(a_6) = 0.$$

We have

$$[5](t) = 5t - 1248 a_4 t^5 + \dots .$$

Put $f = v(a_4)$, $P_0 = (1, e)$, $P_1 = (5, f)$, $P_2 = (25, 0)$. There are two cases to distinguish:
• *One has $f \geq \frac{5e}{6}$, i.e., the point P_1 lies on or above the segment P_0P_2. The Newton polygon on $[5](t)$ is P_0P_2. The characters of I_t which show up are the eth powers of the fundamental characters of level* 2.
• *One has $f < \frac{5e}{6}$, i.e., P_1 lies strictly below P_0P_2. The Newton polygon is the broken line $P_0P_1P_2$; the characters of I_t which show upare the fth and $(e-f)$th powers of the fundamental character of level* 1.
For much larger values of p, it is not necessary to exactly calculate the pth coefficient of $[p](t)$. It suffices to know its value modulo p; moreover one can check that this value is equal to the Hasse invariant *of the mod p reduction (and not only mod $\mathfrak{m}$!) of E; this can be expressed in terms of functions of the covariants c_4 and c_6 using known formulas: c.f. e.g.* [**8**].

1.12. Representation of G defined by an elliptic curve with multiplicative bad reduction.

We now suppose that the elliptic curve E can be written as a plane cubic whose reduction $\tilde{E}$ is irreducible of genus zero having a single double point with split tangent directions i.e., multiplicative reduction – PLC. The Néron model of E is of type b_m I_m – PLC. The identity component of the its special fiber is a "form" of the multiplicative group. In other words, the identity component of the Néron model is an algebraic group which is isomorphic to $\mathbb{G}_m$ over the algebraic closure but not necessarily over the ground field: this isomorphism takes place over the ground field iff the reduction is *split* iff the tangent directions have rational slope. – PLC

To study the Galois module $E[p]$, the simplest thing is to use the theory of the Tate curve. The j-invariant of E has negative valuation, say $v(j) = -m$. There is

then a unique $q \in \mathfrak{m}$ such that

$$j = j(q) = \frac{1}{q} + 744 + 196884q + \dots$$

This is explained very nicely and at length by Silverman. – PLC To q we may associate the **Tate curve**

$$E(q) = \mathbb{G}_m/q^{\mathbb{Z}}.$$

The curves E and $E(q)$ have the same j-invariant so since $v(j) < 0$, certainly $j \neq 0, 1728$ – PLC if they are not isomorphic over K there is a unique quadratic extension K'/K over which they become isomorphic. One can show that K'/K is unramified [again, see Silverman...]; the corresponding residual extension is the smallest one over which the tangent directions at the double point are rational. It follows that over K' we have a short exact sequence of Galois modules

$$0 \to \mu_p \to E[p] \to \mathbb{Z}/p\mathbb{Z} \to 0.$$

Whence, as in the case of good ordinary reduction:

PROPOSITION 14. *(Multiplicative Bad Reduction) The image of the inertia group I in $\mathrm{GL}(E[p])$ is contained in a subgroup of type $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$. The two characters of I_t associated to this representation are the unit character and the character θ_{p-1}^e.*

As above, we deduce:

COROLLARY 9. *Suppose that $e = 1$. Then:*
a) The two characters givin the action of I_t on the semisimplification of $E[p]$ are trivial character 1 and the character θ_{p-1}.
b) If I_p acts trivially on $E[p]$, the image of I in $\mathrm{GL}(E[p])$ is cyclic of order $p-1$ and has a matrix representation $\begin{bmatrix} * & 0 \\ 0 & 1 \end{bmatrix}$.
c) If I_p does not act trivially on $E[p]$, the image of I has a matrix representation $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$.

Here it is easy to give a criterion for being in case b): this occurs iff q has a pth root in K^{unr}. Notice that this condition implies

$$v(j) = -v(q) \equiv 0 \pmod{p}.$$

We conclude that if $v(j) \not\equiv 0 \pmod{p}$ then we are necessarily in case c): c.f. MG IV-37.

Remark: Instead of Tate curves, one could use the fact that the formal group of E is isomorphic to the multiplicative group over the ring of integers of K': in particular, it has height 1.

1.13. Complements.

In all the examples treated above, one notices tha tthe characters of I_t which occur can be expressed as powers of the fundamental characters *with exponents between 0 and e* (hence 0 or 1 when $e = 1$). One can ask if this is a general fact, linked to good reduction (or more generally, semistable reduction). The answer is *yes*. More

precisely, Raynaud just well, just over 40 years ago – PLC showed the following result: – see [**21**] for more details.

Let E be a finite flat commutative group scheme over A. We suppose that E is p-torsion and that its rank is p^h. Let $E[p] = E(K^{\mathrm{sep}})$ be the group of points of E with values in K^{sep}. This is an $\mathbb{F}_p$-vector space of dimension h on which G (hence also I) acts. Let V be a Jordan-Hölder quotient of the I-module $E[p]$, and let n be its dimension over $\mathbb{F}_p$; put $q = p^n$. Then V has the structure of a 1-dimensional $\mathbb{F}_q$-vector space such that the action of I_t on V is given by a character $\psi : I_t \to \mathbb{F}_q^\times$ of the form

$$\psi = \psi_1^{e(1)} \cdots \psi_n^{e(n)},$$

where the ψ_i's are the different fundamental characters of I_t of level n and the $e(i)$ are integers between 0 and e.

This result applies in particular to the p-torsion subgroup scheme of a p-divisible group or to an abelian variety having good reduction.

One can also ask if there are analogous results for etale co/homology of any dimension d: the case treated by Raynaud is essentially $d = 1$. More precisely, let X be a smooth, projective A-scheme, and let H be the dth etale homology group of $X_{/K^{\mathrm{sep}}}$, with coefficients in $\mathbb{Z}/p\mathbb{Z}$. Let V be a Jordan-Hölder factor of the I-module H; put $n = \dim V$ and $q = p^n$. The action of I on V is given by a character

$$\psi : I_t \to \mathbb{F}_q^\times.$$

Is it true that one can write ψ in the form $\psi_1^{e(1)} \cdots \psi_n^{e(n)}$ as above, with exponents $e(i)$ integers between 0 and e?

One can ask analogous questions for other mod p Galois representations, for example those associated to Ramanujan's τ function: is it true that the corresponding exponents $e(i)$ are between 0 and 11? If so, this would permit us to apply the arguments of §4 to this representation.

2. Subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$

In this §, V denotes a 2-dimensional vector space over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The group $\mathrm{GL}\, V$ of automorphisms of V is isomorphic to $\mathrm{GL}_2\, \mathbb{F}_p$; we are interested in its subgroups.

2.1. Cartan subgroups.

There are two kinds: split and nonsplit.

a) Split case:

Let D_1 and D_2 be distinct lines in V, so $V = D_1 \oplus D_2$. Let C be the subgroup of $\mathrm{GL}\, V$ consisting of elements s such that $sD_1 = D_1$ and $sD_2 = D_2$. One says that C is the **split Cartan subgroup** defined by $\{D_1, D_2\}$. If one chooses a basis (e_1, e_2) for V with $e_i \in D_i$, then the matrix representation of C consists of the diagonal matrices. The group C is abelian of type $(p-1, p-1)$: if $p \neq 2$, then from C we can recover the pair of lines $\{D_1, D_2\}$ from C. These are the only two lines in V which are invariant under C. – PLC

Let C_1 be the subgroup of matrices which act trivially on D_1. This is a cyclic group of order $p-1$, with matrix representation $\begin{bmatrix} 1 & 0 \\ 0 & * \end{bmatrix}$. Such a subgroup is called a *split semi-Cartan*.

Let C' be a split semi-Cartan, and let $C = C'\mathbb{F}_p^\times$ be the subgroup generated by C' and by the homotheties. The group C is the unique split Cartan containing C'. The image of C in the projective group $\mathrm{PGL}\, V = \mathrm{GL}(V)/\mathbb{F}_p^\times$ is equal to the image of C'; it is a cyclic group of order $p-1$, called *split semi-Cartan of* $\mathrm{PGL}\, V$.

b) Nonsplit case

Let k be a subalgebra of $\mathrm{End}\, V$ which is a field with p^2 elements. The subgroup $k^\times$ of $\mathrm{GL}\, V$ is cyclic of order p^2-1. Its image in $\mathrm{PGL}\, B$ is cyclic of order $p+1$. Such a subgroup of $\mathrm{GL}\, V$ (respectively, of $\mathrm{PGL}\, V$) is called a *nonsplit Cartan*.

The intersection of two Cartan subgroups is the group $\mathbb{F}_p^\times$ of homotheties. Their union is the set of semisimple elements (i.e., elements of order prime to p) of $\mathrm{GL}\, V$. If $p \neq 2$ and if $s \in \mathrm{GL}\, V$ is such that

$$(\mathrm{tr}\, s)^2 - 4 \det s \neq 0,$$

the element s belongs to a unique Cartan,; this group is split iff $(\mathrm{tr})^2 - 4dets \in \mathbb{F}_p^{\times 2}$.

2.2. Normalizers of Cartan subgroups.

Let C be a Cartan subgroup of $\mathrm{GL}\, V$; we suppose $p \neq 2$ if C is split. The subalgebra $k = \mathbb{F}_p C$ of $\mathrm{End}\, V$ generated by C is then a commutative semisimple algebra of rank 2 and $C = k^\times$ is the multiplicative group of k. Let N be the *normalizer* of C in $\mathrm{GL}\, V$. If $s \in N$, the map $x \mapsto sxs^{-1}$ is an automorphism of k; this automorphism is the identity iff s commutes with k, hence belongs to k this seems to use a special case of something like the Double Centralizer Theorem – PLC and thus also to C. We conclude $[N : C] = 2$. This seems to use the Noether-Skolem Theorem. See Bourdon-Clark-Stankewicz! If C is split and $\{D_1, D_2\}$ are the lines eigenspaces – PLC then the elements of $N \setminus C$ are the elements $s \in \mathrm{GL}\, V$ such that $sD_1 = D_2$ and $sD_2 = D_1$. If $C$is nonsplit, the elements of $N \setminus C$ are the elements $s \in \mathrm{GL}\, V$ such that $s(ax) = a^p s(x)$ for $a \in k$, $x \in V$: they are *Frobenius-semilinear*.

Let C_1 and N_1 be the images of C and N in $\mathrm{PGL}\, V$. The group N_1 is the normalizer of C_1 in $\mathrm{PGL}\, V$. This is a dihedral group: the semidirect product of an order two group $\{1, \sigma\}$ by the cyclic group C_1; one has $\sigma x \sigma^{-1} = x^{-1}$ for all $x \in C_1$; every element of $N_1 \setminus C_1$ has order 2.

PROPOSITION 15. *Let C be a Cartan subgroup of $\mathrm{GL}\, V$ and N its normalizer. Let C' be a Cartan subgroup (resp. a split semi-Cartan) of $\mathrm{GL}\, V$ contained in N. Suppose $p \geq 5$ if C' is split and $p \geq 3$ otherwise. Then we have $C' = C$ (resp. $C' \subset C$).*

PROOF. Let C_1, N_1 and C_1' be the projective images of C, N and C_1. In view of the hypotheses, C_1' is cyclic of order $p \pm 1 > 2$. If s is a generator of C_1' then we have $s \in C_1$: if not, $s \in N_1 \setminus C_1$ and thus $s$has order 2. But two distinct Cartan subgroups of $\mathrm{PGL}\, V$ intersect trivially. Since $s \in C_1 \cap C_1'$, we thus have $C_1 = C_1'$, whence $C'\mathbb{F}_p^\times = C$ and the result follows. □

REMARK 8. *Proposition 15 does not extend to the case $p = 3$. Indeed, in this case V has 4 lines D_1, D_2, D_3, D_4 and the split Cartan subgroups associated to $\{D_1, D_2\}$ and $\{D_3, D_4\}$ have the same normalizer; moreover, the latter is strictly contained in the normalizer of a nonsplit Cartan.*
Let's explain the first claim. The normalizer of a Cartan is the collection of all elements which stabilize the corresponding pair *of lines. But if there are exactly four lines total, the elements which stabilize any two of them must also stabilize the other two! – PLC*

2.3. Borel subgroups.

Let D be a line in V. The subgroup B of $\mathrm{GL}\, V$ of all elements s such that $sD = D$ has order $p(p-1)^2$; it has matrix representation $\begin{bmatrix} * & * \\ 0 & * \end{bmatrix}$. Such a subgroup is called a *Borel subgroup* of $\mathrm{GL}\, V$; the corresponding line D is the unique line of V stabilized by B.

If a Cartan subgroup, or a semi-Cartan subgroup, is contained in B, this subgroup is split and (if $p \geq 3$) then D is one of the two lines associated to the Cartan.

2.4. Subgroups of order divisible by p.

PROPOSITION 16. *Let G be a subgroup of $\mathrm{GL}\, V$ of order divisible by p. Then G either contains $\mathrm{SL}\, V$ or is contained in a Borel subgroup of $\mathrm{GL}\, V$.*

PROOF. Every order p element of $\mathrm{GL}\, V$ can be represented by a matrix of the form $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ Jordan form – PLC, hence pointwise fixes a unique line D_x. If all of the lines D_x corresponding to the order p elements of G are equal to the same line D, then G stabilizes D there is a nice little exercise here – PLC and thus is contained in the corresponding Borel. If there are at least two different lines D_x, we can choose a basis of V whose basis vectors lie in these lines, and then G contains elements

$$x = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}, \; y = \begin{bmatrix} 1 & 0 \\ b & 1 \end{bmatrix}.$$

But $\mathrm{SL}_2(\mathbb{F}_p)$ is generated by these elements the general fact here is that SL_n over a field is generated by **transvections** – PLC. □

2.5. Exceptional finite subgroups of $\mathrm{PGL}_2(k)$.

In this section k denotes a field and $\mathrm{PGL}_2(k) = \mathrm{GL}_2(k)/k^\times$.

PROPOSITION 17. *Let H be a finite subgroup of $\mathrm{PGL}_2(k)$ of order prime to the characteristic of k. We suppose that H is neither cyclic nor dihedral. Then H is isomorphic to A_4, S_4 or A_5. In particular H has order 12, 24 or 60 and every element of H has order at most 5.*

This result is well known when $k = \mathbb{C}$, c.f. e.g. [**36**, §68]. One can deduce it from the fact that $\mathrm{PGL}_2(\mathbb{C})$ has $\mathrm{SO}_3(\mathbb{R})$ as a maximal compact subgroup, from which it follows that H is isomorphic to a finite group of rotations of $\mathbb{R}^3$ and thus corresponds to a "regular polyhedron": in this way A_4, S_4 and A_5 correspond to the tetrahedron, the cube and the icosahedron.

In the general case one can proceed in several ways. For example:

1) One can look back at Weber's arguments and see that they remain valid in the general case, using the fact that the order of H is prime to k.

2) Since k has characteristic 0 one can also apply the *Lefschetz principle* to reduce to $k = \mathbb{C}$. Briefly: since the subgroup H is finite, the subfield $k' = \mathbb{Q}(H)$ of k generated by the matrix entries is finitely generated over $\mathbb{Q}$ and thus embeds into $\mathbb{C}$. –PLC When k has characteristic $p > 0$, one can write k as the residue field of of a CDVR A with characteristic 0 fraction field K. First enlarge k to $\overline{k}$ – this is harmless – and then take Witt vectors. –PLC Because H has order prime to p, a standard argument shows that one can lift H to a subgroup of $\mathrm{PGL}_2(A)$ and thus also to $\mathrm{PGL}_2(K)$, and we have reduced to the characteristic 0 case.

COROLLARY 10. *If k has characteristic 2 or 3, every finite subgroup of $\mathrm{PGL}_2(k)$ of order prime to the characteristic of k is cyclic or dihedral.*

This is clear.

REMARK 9. *One can ask under what condition $\mathrm{PGL}_2(k)$ contains a subgroup isomorphic to A_4, S_4 or A_5. The answer is the following:*
a) $\mathrm{PGL}_2(k)$ contains A_4 if only if:
- *There is $x \in k$ with $x^2 + x - 1 = 0$ (if k has characteristic 2);*
- *There are $y, z \in k$ such that $y^2 + z^2 = -1$ (otherwise).*

b) $\mathrm{PGL}_2(k)$ contains S_4 iff k has characteristic not equal to 2 and ther are $y, z \in k$ with $y^2 + z^2 = -1$.
c) $\mathrm{PGL}_2(k)$ contains A_5 iff: there are $x, y, z \in k$ such that $x^2 + x - 1 = 0$ and $y^2 + z^2 = -1$.

Note that the condition on (y, z) is always satisfied when k has positive characteristic. When k has characteristic 0, it means that k is a splitting field for the quaternions $\left(\frac{-1,-1}{\mathbb{Q}}\right)$. The condition on x is that k contains $\sqrt{5}$ when it has characteristic different from 2 and a cube root of unity when the characteristic is 2.

2.6. Subgroups of order prime to p.

Let G be a subgroup of $\mathrm{GL}\, V$ of order prime to p, and let H be its image in $\mathrm{PGL}\, V$. Proposition 16 applied in the field $k = \mathbb{F}_p$ shows that we have the following possibilities:

(i) H is cyclic, hence contained in a Cartan subgroup of $\mathrm{PGL}\, V$, and a unique one if $H$is nontrivial; we conclude that G is contained in a Cartan subgroup of $\mathrm{GL}\, V$.

(ii) H is dihedral, hence contains a nontrivial cyclic subgroup C' of index 2. The group C' is contained in a unique Cartan subgroup C of $\mathrm{PGL}\, V$; since H normalizes C', it also normalizes C. Coming back to $\mathrm{GL}\, V$, we conclude that G is *contained in the normalizer of a Cartan subgroup.*

(iii) H is isomorphic to A_4, S_4 or A_5; the last case is only possible if $p \equiv \pm 1 \pmod 5$. The elements of H are therefore of order 1, 2, 3, 4 or 5. We deduce easily that if $s \in G$, the element $u = \mathrm{tr}(s)^2/\det(s)$ is equal to $4, 0, 1, 2$ or satisfies $u^2 - 3u + 1 = 0$.

2.7. Subgroups containing a Cartan.

The following result will play an essential role in §4:

PROPOSITION 18. *Let $G \subset \mathrm{GL}\, V$ be a subgroup contianing a Cartan C (resp. a split semi-Cartan C). We suppose $p \neq 5$ and that C is split. Then one of the following holds:*
- *$G = \mathrm{GL}\, V$; or*
- *G is contained in a Borel; or*
- *G is contained in the normalizer of a Cartan.*

PROOF. Case 1: $p \mid \#G$. By Propsition 15, G is either cntained in a Borel or contains $\mathrm{SL}\, V$. In the latter case, since G contains C, $detG = \mathbb{F}_p^\times$, so $G = \mathrm{GL}\, V$.
Case 2: $p \nmid \#G$. Let H be the image of G in $\mathrm{PGL}\, V$. According to §2.6, it comes down to showing that H is cyclic or dihedral, i.e., is not isomorphic to A_4, S_4 or A_5. This is clear if $p \leq 3$. So suppose $p \geq 5$. The image C_1 of C in $\mathrm{PGL}\, V$ is cyclic of order $p + 1 \geq 6$ (because $p \geq 7$ if C is split). But none of A_4, S_4, or A_5 contain any elements of order at least 6. □

REMARK 10. *If $p = 5$ and C is split, there is a fourth possibility: the image of G in $\mathrm{PGL}\, V$ could be ismorphic to S_4. This case is characterized by the fact that the function $s \mapsto (\mathrm{tr}\, s)^2/\det s$ takes on G the value 1 and does not take the value 3.*

The case in which G is *normal* is much simpler:

PROPOSITION 19. *Let G be a subgroup of $\mathrm{GL}\, V$ containing a Cartan (resp. a split semi-Cartan). We suppose that $p \neq 2$ and that G is normal. Then $G = \mathrm{GL}\, V$.*

PROOF. Suppose $p \geq 5$. By a known result [**1**, IV. Thm. 4.9], the fact that G is normal in $\mathrm{GL}\, V$ implies that G is either contained in the center of $\mathrm{GL}\, V$ or contains $\mathrm{SL}\, V$. The first case is excluded since G contains C. The second case implies $G = \mathrm{GL}\, V$ since $\det C = \mathbb{F}_p^\times$.
If $p = 3$, we can identify $\mathrm{PGL}\, V$ with S_4 and the image H of G in $\mathrm{PGL}\, V$ becomes a normal subgroup of S_4. If C is split (resp. nonsplit) then H contains a transposition (resp. a 4-cycle). It follows easily that $H = S_4$, so the order of G is divisible by 3. Since G is not contained in a Borel subgroup the order of a Borel in this case is 12 – PLC, Proposition 16 shows G contains $\mathrm{SL}\, V$, and we finish as above. □

2.8. A criterion for $G = \mathrm{GL}\, V$.

LEt G be a subgroup of $\mathrm{GL}\, V$. Proposition 17 furnishes a criterion for $G = \mathrm{GL}\, V$: for $p \geq 7$, it suffices that G contains a Cartan subgroup and is contained in neither a Borel subgroup nor the normalizer of a Cartan subgroup. Here is a slightly different criterion.

PROPOSITION 20. *Suppose $p \geq 5$ and make the following hypotheses:*
(i) G contains an element s with $(\mathrm{tr}\, s)^2 - 4 \det s \in \mathbb{F}_p^{\times 2}$ and $\mathrm{tr}\, s \neq 0$.
(ii) G contains an element S' with $(\mathrm{tr}\, s)^2 - 4 \det s' \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}$ and $\mathrm{tr}\, s' \neq 0$.
(iii) G contains an element s'' such that $u = (\mathrm{tr}\, s'')^2 - 4 \det s'' \notin \{0, 1, 2, 4\}$ and such that $u^2 - 3u + 1 \neq 0$.
Then G contains $\mathrm{SL}\, V$. In particular, if $\det : G \to \mathbb{F}_p^\times$ is surjective then $G = \mathrm{GL}\, V$.

PROOF. We again consider two cases:
a) $p \mid \#G$: if G did not contain $\mathrm{SL}\, V$, then G would be contained in a Borel subgroup (Proposition 16) and thus the eigenvalues of all elements of G would belong to $\mathbb{F}_p$, contradicting (ii).
b) $p \nmid \#G$: let H be the image of G in $\mathrm{PGL}\, V$. Condition (iii) shows that H cannot be isomorphic to A_4, S_4 or A_5: c.f. §2.6.

Thus H is cyclic or dihedral and G is contained in the normalizer N of a Cartan subgroup C. If C is split, the element s' cannot appear – not in C, because $(\mathrm{tr}\, s')^2 - 4 \det s'$ would be a sequare – nor in $N \setminus C$: because $\mathrm{tr}(s')$ would be zero. If C is nonsplit, the same argument shows that s cannot appear – not in C and not in $N \setminus C$. Case b) is thus impossible. □

Corollary [**32**, Lemma 4] Make the following hypothesis:
($\star$) For all $t \in \mathbb{F}_p$, $d \in \mathbb{F}_p^\times$, there is $s \in G$ such that $\mathrm{tr}\, s = t$ and $\det s = d$. Then, if $p \geq 5$ we have $G = \mathrm{GL}\, V$.

PROOF. Indeed, conditions (i), (ii) and (iii) of Proposition 20 are satisfied and $\det : G \to \mathbb{F}_p^\times$ is surjective. □

REMARK 11. *When $p = 2$ (resp. $p = 3$) the hypothesis ($\star$) does not force $G = \mathrm{GL}\, V$. It only forces G to contain the 3-Sylow subgroup (resp. the 2-Sylow subgroup) of $\mathrm{GL}\, V$. More precisely:*
- *If $p = 2$, then $\mathrm{GL}\, V \cong S_3$, and for G to contain an element of order 3 in $\mathrm{GL}\, V$ it is necessary and sufficient for there to be $s \in G$ with $\mathrm{tr}\, s = 1$.*
- *If $p = 3$, then $\mathrm{PGL}\, V \cong S_4$, and for G to contain a 2-Sylow subgroup of $\mathrm{GL}\, V$ – i.e., a normalizer of a nonsplit Cartan subgroup – it is necessary and sufficient for there to be $s, s' \in G$ such that*

$$\det s = \det s' = -1 \text{ and } \mathrm{tr}\, s = 0,\ \mathrm{tr}\, s' = \pm 1.$$

3. Systems of abelian representations modulo ℓ

3.1. Notations.

These are as in [**MG**, Ch. II]. We briefly recall them:

K is a number field (i.e., a finite extension of $\mathbb{Q}$), with algebraic clsoure $\overline{K}$;
$\mathcal{O}_K$ is the ring of integer of K and $E = \mathcal{O}_K^\times$ is the unit group of K;
Σ is the set of ultrametric places of K, and Σ^∞ is the set of Archimedean places; we put $\overline{\Sigma} = \Sigma \cup \Sigma^\infty$.
K_v is the completion of K at v (for $v \in \overline{\Sigma}$); U_v, k_v, Nv, p_v are, respectively, the group of units, the residue field, the cardinality of the residue field and the residue characteristic of the local field K_v (for $v \in \Sigma$).

$\mathbb{I}$ is the idele group of K; if $a \in \mathbb{I}$ and $v \in \overline{\Sigma}$, we denote by a_v the component of a at v; we have $a_v \in K_v^\times$ for all $v \in \overline{\Sigma}$ and $a_v \in U_v$ for almost all v i.e., all but finitely many – PLC;
$C = \mathbb{I}/K^\times$ is the idele class group of K.

We give ourselves a finite subset S of Σ and a *modulus* $\mathfrak{m} = (m_v)_{v \in S}$ supported on S, the m_v being positive integers. We define $U_{v,\mathfrak{m}}$ as follows: the identity component of $K_v^\times$ if $v \in \Sigma^\infty$; the group U_v if $v \in \Sigma \setminus S$, and the subgroup of U_v formed by elements x such that $v(1-x) \geq m_v$ if $v \in S$. The group $U_\mathfrak{m} = \prod_v U_{v,\mathfrak{m}}$ is an

open subgroup of I. We put $E_{\mathfrak{m}} = E \cap U_{\mathfrak{m}}$ and $C_{\mathfrak{m}} = I/K^{\times}U_{\mathfrak{m}}$, whence an exact sequence

$$0 \to K^{\times}/E_{\mathfrak{m}} \to I/U_{\mathfrak{m}} \to C_{\mathfrak{m}} \to 0.$$

The group $C_{\mathfrak{m}}$ can also be interpreted as the group of classes (mod $\mathfrak{m}$) of ideals prime to S; this is a finite group; let $h_{\mathfrak{m}}$ be its order.

The projective limit $\varprojlim C_{\mathfrak{m}}$ is equal to the quotient of C by its identity component; according to class field theory [**5**], [**42**], this quotient can be identified with $\mathrm{Aut}(K^{\mathrm{ab}}/K)$, where K^{ab} is the abelian closure of K in $\overline{K}$. In particular we have, for each $\mathfrak{m}$, a canonical homomorphism

$$\mathrm{Aut}(K^{\mathrm{ab}}/K) \to C_{\mathfrak{m}}$$

which is surjective; in this way, the group $C_{\mathfrak{m}}$ may be identified with the maximal abelian extension of K of conductor dividing $\mathfrak{m}$.

3.2. The algebraic groups T, $T_{\mathfrak{m}}$ and $S_{\mathfrak{m}}$.

These are the affine algebraic groups over $\mathbb{Q}$ defined in [**MG**, Ch. II]:

The group T is the torus w2hich represents the multiplicative group over K; more precisely, for any commutative $\mathbb{Q}$-algebra A, the group $T(A)$ of A-valued points is $(K \otimes_{\mathbb{Q}} A)^{\times}$; in particular, $T(\mathbb{Q}) = K^{\times}$. In more modern termninology, this is the **restriction of scalars**, or **Weil restriction**, of the multiplicative group $\mathbb{G}_m$ from K down to $\mathbb{Q}$. This has become quite a standard construction. –PLC

The group $T_{\mathfrak{m}}$ is the torus obtained by taking the quotient of T by the closure of $E_{\mathfrak{m}}$ in the Zariski topology (this makes sense because $E_{\mathfrak{m}} \subset K^{\times} = T(\mathbb{Q})$).

The group $S_{\mathfrak{m}}$ is an extension of the finite group $C_{\mathfrak{m}}$ – considered as a constant algebraic group, of dimension 0 – by the torus $T_{\mathfrak{m}}$. It is equipped with a homomorphism $\mathbb{I}/U_{\mathfrak{m}} \to S_{\mathfrak{m}}(\mathbb{Q})$ rendering commutative the following diagram:

$$\begin{array}{ccccccc} 0 & \to & K^{\times}/E_{\mathfrak{m}} & \to & \mathbb{I}/U_{\mathfrak{m}} & \to & C_{\mathfrak{m}} \to 0 \\ 0 & \to & T_{\mathfrak{m}}(\mathbb{Q}) & \to & S_{\mathfrak{m}}(\mathbb{Q}) & \to & C_{\mathfrak{m}} \to 0. \end{array}$$

3.3. Characters of T, $T_{\mathfrak{m}}$ and $S_{\mathfrak{m}}$.

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. If $G_{/\mathbb{Q}}$ is an algebraic group, the *character group* $X(G)$ is the group of $\overline{\mathbb{Q}}$-homomorphisms of $G_{/\overline{\mathbb{Q}}}$ into the multiplicative group $(\mathbb{G}_m)/\overline{\mathbb{Q}}$. This applies in particular to the groups T, $T_{\mathfrak{m}}$ and $S_{\mathfrak{m}}$; we will now make explicit these corresponding character groups.

Let Γ be the set of embeddings of K in $\overline{\mathbb{Q}}$. To every element of Γ one can attach a character $[\sigma]$ of T [**MG**, §II.1.1], and we have

$$[\sigma](x) = \sigma(x) \text{ if } x \in T(\mathbb{Q}) = K^{\times}.$$

These characters $[\sigma]$ form a basis of the group $X(T)$. Every element φ of $X(T)$ may be uniquely written as (in multiplicative notation)

$$\varphi = \prod_{\sigma \in \Gamma} [\sigma]^{n(\sigma)}, \text{ with } n(\sigma) \in \mathbb{Z}.$$

We call the $n(\sigma)$'s the *exponents* of φ.

Since $T_{\mathfrak{m}} = T/\overline{E_{\mathfrak{m}}}$, the group $X(T_{\mathfrak{m}})$ may be identified with the subgroup of $X(T)$ formed by characters φ of the above type such that we have

$$\varphi(X) = \prod_{\sigma \in \Gamma} \sigma(x)^{n(\sigma)} = 1 \text{ for all } x \in E_{\mathfrak{m}}.$$

Finally, the construction of $S_{\mathfrak{m}}$ given in [**MG**, §II.2.2] shows that an element of $X(S_{\mathfrak{m}})$ is a pair (φ, f) where $\varphi \in X(T)$ and $f \in \mathrm{Hom}(\mathbb{I}, \overline{\mathbb{Q}}^{\times})$ with:
i) $f(x) = 1$ for all $x \in U_{\mathfrak{m}}$, and
ii) $f(x) = \varphi(X)$ for all $x \in K^{\times}$.

These two properties imply that $\varphi(x) = 1$ for all $x \in E_{\mathfrak{m}}$, i.e., we have $\varphi \in X(T_{\mathfrak{m}})$. On the other hand, property ii) shows that knowing f means that we know φ.

Taking character groups on the exact sequence $0 \to T_{\mathfrak{m}} \to S_{\mathfrak{m}} \to C_{\mathfrak{m}} \to 0$, we get a dual exact sequence

$$0 \to X(C_{\mathfrak{m}}) \to X(S_{\mathfrak{m}}) \to X(T_{\mathfrak{m}}) \to 0,$$

where $X(C_{\mathfrak{m}}) = \mathrm{Hom}(C_{\mathfrak{m}}, \overline{\mathbb{Q}}^{\times})$ is just the dual of the finite commutative group $C_{\mathfrak{m}}$. In particular, every chracter φ of $T_{\mathfrak{m}}$ can be extended to a character (φ, f) of $S_{\mathfrak{m}}$, and the number of possible extensions is precisely $h_{\mathfrak{m}} = \#C_{\mathfrak{m}}$.

Remark 12. *1) There is a natural action of* $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$ *on the character groups* $X(T)$, $X(T_{\mathfrak{m}})$ *and* $X(S_{\mathfrak{m}})$ *which furnishes these groups with Galois module structures; from the knowledge of this Galois module structure we can recover* T, $T_{\mathfrak{m}}$ *and* $S_{\mathfrak{m}}$ *since these are groups of multiplicative type. Again, this is very standard nowadays: over any field* K*, one has a categorical equivalence between algebraic tori over* K *and Galois modules whose underlying group is* $\mathbb{Z}^n$ *for some* $n \in \mathbb{N}$*. –PLC*
2) The chracters $S_{\mathfrak{m}}$ *are morally the idele class characters of conductor dividing* $\mathfrak{m}$ *and "of type* (A_0)*" in the sense of Weil* [**39**]*. As Weil himself has shown, these chracters also play an essential role in the theory of complex multiplication* [**40**], [**30**, §7] *and in the arithmetic (and the homology) of varieties with equations*

$$a_0 x_0^{n_0} + \ldots + a_r x_r^{n_r} = 0$$

[**37**], [**38**].

3.4. Representations of $\mathrm{Aut}(K^{\mathrm{ab}}/K)$ defined by a character of $S_{\mathfrak{m}}$.
Let us first introduce some notation:

Let ℓ be a prime number. We say that $v \in \Sigma$ divides ℓ if $p_v = \ell$, and then we write $v \mid \ell$. We put

$$K_\ell = \prod_{v|\ell} K_v = K \otimes \mathbb{Q}_\ell.$$

The multiplicative group $K_\ell^{\times} = \prod_{v|\ell} K_v^{\times}$ can be naturally identified as a direct factor of the idele group $\mathbb{I}$ of K. If $a \in \mathbb{I}$, we denote by a_ℓ the component of a in $K_\ell^{\times}$; we have $a_\ell = (a_v)_{v|\ell}$. We also put:

$$U_\ell = \prod_{v|\ell} U_v \text{ and } U_{\ell,\mathfrak{m}} = \prod_{v|\ell} U_{v,\mathfrak{m}}.$$

On the other hand, we *choose* a valuation v_ℓ of $\overline{\mathbb{Q}}$ extending the ℓ-adic valuation of $\mathbb{Q}$. The completion $\overline{\mathbb{Q}_\ell}$ of $\overline{\mathbb{Q}}$ for v_ℓ is an algebraic closure of $\mathbb{Q}_\ell$. We denote by $\mathcal{O}_\ell$ (resp. $\mathfrak{p}_\ell$, resp. k_ℓ) the the ring (resp. the maximal ideal, resp, the residue field) of v_ℓ extended to $\overline{\mathbb{Q}}_\ell$; the field k_ℓ is an algebraic closure of the prime field $\mathbb{F}_\ell$.

Every embedding σ of K into $\overline{\mathbb{Q}}$ extends by linearity to a homomorphism of $\mathbb{Q}_\ell$-algebras $\sigma_\ell : K_\ell \to \overline{\mathbb{Q}_\ell}$; this homomorphism is trivial on all the components K_v of K_ℓ except one (the one corresponding to the unique v which is equivalent to $v_\ell \circ \sigma$). Conversely, every $\mathbb{Q}_\ell$-homomorphism of K_ℓ into $\overline{\mathbb{Q}_\ell}$ is of the form σ_ℓ, for a

uniquely determined element $\sigma \in \Gamma$. Finally, if $\varphi = \prod_{\sigma\in\Gamma}[\sigma]^{n(\sigma)}$ is a character of the torus T, we denote by φ_ℓ the homomorphism of $K_\ell^\times = T(\mathbb{Q}_\ell)$ into $\overline{\mathbb{Q}_\ell}$ defined by the formula

$$\varphi_\ell(X) = \prod_{\sigma\in\Gamma} \sigma_\ell(x)^{n(\sigma)}.$$

We will now define the *ℓ-adic character* of $\mathrm{Aut}(K^{ab}/K)$ attached to a character of $S_\mathfrak{m}$:

Let $\psi = (\varphi, f)$ be an element of $X(S_\mathfrak{m})$, cf. §3.3. If a is an idele of K, put

$$\psi_\ell(a) = f(a)\varphi_\ell(a_\ell^{-1}). \tag{1}$$

We obtain in this way a homomorphism $\psi_\ell : \mathbb{I} \to \overline{\mathbb{Q}_\ell}^\times$, and one immediately verifies (cf. [**MG**, Ch. II.2]) that it is continuous and trivial on $K^\times$; by passage to the quotient, it defines a continuous homomorphism from the idele class group $C = \mathbb{I}/K^\times$ to $\overline{\mathbb{Q}_\ell}^\times$, a homomorphism which is trivial on the identity component of C since $\overline{\mathbb{Q}_\ell}^\times$ is totally disconnected. Using class field theory, one finally obtains a continuous homomorphism

$$\psi_\ell : \mathrm{Aut}(K^{\mathrm{ab}}/K) \to \overline{\mathbb{Q}_\ell}^\times,$$

i.e., an ℓ-adic character of the Galois group $\mathrm{Aut}(K^{\mathrm{ab}}/K)$.

(One can also define ψ_ℓ as the composite of the homomorphism

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

cf. [**MG**, II-11] with the homomorphism $S_\mathfrak{m}(\mathbb{Q}_\ell) \to \overline{\mathbb{Q}_\ell}^\times$ defined by the character ψ.)

From the fact that $f \equiv 1$ on $U_\mathfrak{m}$, we have:

$$\psi_\ell(A) = \varphi_\ell(a_\ell^{-1}) = \prod_{\sigma\in\Gamma} \sigma_\ell(a_\ell^{-1})^{n(\sigma)} \text{ for all} a \in U_\mathfrak{m}, \tag{2}$$

where the integers $n(\sigma)$ are the *exponents* of φ.

The image of φ_ℓ is compact, hence contained in the unit group of $\overline{\mathbb{Q}_\ell}^\times$. By reduction modulo $\mathfrak{p}_\ell$ we obtain from ψ_ℓ a "modulo ℓ character"

$$\tilde{\psi}_\ell : \mathrm{Aut}(K^{\mathrm{ab}}/K) \to k_\ell^\times.$$

Being discrete and compact, the image of $\tilde{\psi}_\ell$ is a finite subgroup of $k_\ell^\times$. The formula (2) gives:

$$\tilde{\psi}_\ell(a) \equiv \prod_{\sigma\in\Gamma} \sigma_\ell(a_\ell^{-1})^{n(\sigma)} \pmod{\mathfrak{p}_\ell} \text{ for all} a \in U_\mathfrak{m}. \tag{3}$$

For future use we rewrite (3) as the conjunction of the following two properties:

(3_1) We have $\tilde{\psi}_\ell(a) = 1$ for all $a \in U_{v,\mathfrak{m}}$ if $v \nmid \ell$.

(3_2) If $v \mid \ell$, denote by $\Gamma(v)$ the subset of Γ formed by embeddings $\sigma : K \to \overline{\mathbb{Q}}_\ell$ such that $v_\ell \circ \sigma$ is equivalent to v. If $\sigma \in \Gamma(v)$, σ extends to an embedding of K_v into $\overline{\mathbb{Q}_\ell}$ and defines by passage to the residue field an embedding $\tilde{\sigma}_\ell$ of k_v into k_ℓ. We then have

$$\tilde{\psi}_\ell(a) = \prod_{\sigma\in\Gamma(v)} \tilde{\sigma}_\ell(\tilde{a}^{-1})^{n(\sigma)} \text{ for all} a \in U_{v,\mathfrak{m}},$$

where $\tilde{a}$ dnoetes the image of a in $k_v^\times$.

REMARK 13. *If $v \notin S = \mathrm{Supp}(\mathfrak{m})$, the properties (3_1) and (3_2) entirely determine $\tilde{\psi}_\ell$ on U_v; in view of class field theory, this gives the restriction of $\tilde{\psi}_\ell$ to the inertia subgroup I_v of $\mathrm{Aut}(K^{\mathrm{ab}}/K)$ relative to v:*
a) If $v \nmid \ell$,we have $\tilde{\psi}_v(I_v) = \{1\}$, i.e., $\tilde{\psi}_\ell$ is unramified at v;
b) If $v \mid \ell$, the restriction of $\tilde{\psi}_\ell$ to I_v is the product of the characters $\alpha \mapsto \tilde{\sigma}_\ell(\alpha^{-1})$ $(\sigma \in \Gamma(v))$ using the exponents $n(\sigma)$. (Notice that, according to Proposition 4 of §1.5, each of the characters $\alpha \mapsto \tilde{\sigma}_\ell(\alpha^{-1})$ is a fundamental character of the tame inertia group at v.)

3.5. Converse: passage from a system of characters modulo ℓ to an element of $X(S_\mathfrak{m})$.

In the following statement, L denotes an *infinite* set of prime numbers. For each $\ell \in L$, suppose given a continuous homomorphism

$$\theta_\ell : \mathrm{Aut}(K^{\mathrm{ab}}/K) \to k_\ell^\times;$$

we identify θ_ℓ, via class field theory, with a homomorphism $\mathbb{I} \to k_\ell^\times$.

PROPOSITION 21. *Suppose that ther is a family of integers $n(\sigma, \ell)$, where σ ranges over Γ and ℓ over L, such that:*
i) the aboslute values of the $n(\sigma, \ell)$ are bounded by an integer N independent of σ, ℓ;
ii) for all $\ell \in L$ and all $a \in U_\mathfrak{m}$, we have

$$\theta_\ell(a) \equiv \prod_{\sigma \in \Gamma} \sigma_\ell(a_\ell^{-1})^{n(\sigma,\ell)} \pmod{\mathfrak{p}_\ell}. \tag{4}$$

Then there exists $\psi \in X(S_\mathfrak{m})$ such that $\tilde{\psi}_\ell = \theta_\ell$ for infinitely many ℓ.

PROOF. Since the $n(\sigma, \ell)$ can only take finitely many values and L is infinite, there is an infinite subset $L' \subset L$ such that the $n(\sigma, \ell)$ are independent of ℓ for $\ell \in L'$; we denote by $n(\sigma)$ this common value $n(\sigma, \ell)_{\ell \in L'}$ and let φ be the character of T having the exponents $n(\sigma)$. We will see that φ is a character of $T_\mathfrak{m}$, i.e., that $x \in E_\mathfrak{m}$ implies $\varphi(x) = 1$. Let x be a principal idele of the field K. We have $\theta_\ell(x) = 1$ for all $\ell \in L$. On the other hand, since x belongs to $U_\mathfrak{m}$, the hypothesis ii) shows that we have

$$\theta_\ell(X) = \prod_{\sigma \in \Gamma} \sigma(x^{-1})^{n(\sigma)} \equiv \varphi(x^{-1}) \pmod{\mathfrak{p}_\ell} \text{ for all } \ell \in L'.$$

We thus have $\varphi(x) \equiv 1 \pmod{\mathfrak{p}_\ell}$ for infinitely many values of ℓ, which implies that $\varphi(x) = 1$ (indeed a nonzero element of $\overline{\mathbb{Q}}$ can only belong to $\mathfrak{p}_\ell$ for finitely many ℓ).

Since φ is a character of $T_\mathfrak{m}$, it can be extended (cf. §3.3) to a character $\chi = (\varphi, f)$ of $S_\mathfrak{m}$. Let $\tilde{\chi}_\ell$ be the associated mod ℓ character, and put

$$\theta'_\ell = \tilde{\chi}_\ell \theta_\ell^{-1} \text{ for all } \ell \in L'.$$

Since $\tilde{\chi}_\ell$ and θ_ℓ satisfy (4) with the same exponents $n(\sigma)$, we have $\theta'_{ell}(a) = 1$ for all $a \in U_\mathfrak{m}$; otherwise put, θ'_ℓ may be identified with a homomorphism $C_\mathfrak{m} \to k_\ell^\times$; its values belong to the group $H_{\mathfrak{m},\ell}$ of $h_\mathfrak{m}$th roots of unity of k_ℓ, with $h_m = \#C_\mathfrak{m}$. After slightly shrinking L', we may suppose that no element ℓ of L' divides $h_\mathfrak{m}$. If $H_\mathfrak{m}$ denotes the group of $h_\mathfrak{m}$th roots of unity in $\overline{\mathbb{Q}}$, reduction modulo $\mathfrak{p}_\ell$ defines an isomorphism $H_\mathfrak{m} \to H_{\mathfrak{m},\ell}$ and θ'_ℓ can be lifted to a homomorphism $\theta''_\ell : C_\mathfrak{m} \to H_\mathfrak{m}$. Since $C_\mathfrak{m}$ and $H_\mathfrak{m}$ are finite, there is an infinite subset $L'' \subset L'$ such that θ''_ℓ is equal to the same homomorphism θ'' for each $\ell \in L''$. We have $\theta'' \in X(C_\mathfrak{m})$,

whence $\theta'' \in X(S_{\mathfrak{m}})$ and the character $\psi = (\theta'')^{-1}\chi$ is such that $\tilde{\psi}_\ell = (\theta'_\ell)^{-1}\tilde{\chi}_\ell = \theta_\ell$ for all $\ell \in L''$, which demonstrates the proposition. □

REMARK 14. *Proposition 21 concerns an* infinite set *of prime numbers, and that is the form in which we will use it. It is however possible to reformulate it* in finite terms*; one arrives at the following statement:*

PROPOSITION 22. *For $\mathfrak{m}$ and $n(\sigma)_{\sigma\in\Gamma}$ given, there is a constant ℓ_0 such tha, if $\ell \geq \ell_0$, and if $\theta : \mathrm{Aut}(K^{\mathrm{ab}}/K) \to k_\ell^\times$ is a homomorphism such that*

$$\theta(a) \equiv \prod_{\sigma\in\Gamma} \sigma_\ell(a_\ell^{-1})^{n(\sigma)} \pmod{\mathfrak{p}_\ell} \text{ for all } a \in U_{\mathfrak{m}},$$

there is a unique character $\psi = (\varphi, f)$ of $S_{\mathfrak{m}}$ such that $\tilde{\psi}_\ell = \theta$ and the exponents of φ are equal to the $n(\sigma)$.

Moreover, the constant ℓ_0 can be effectively calculated in terms of K, $\mathfrak{m}$ and the $n(\sigma)$.

3.6. Application to certain systems of ℓ-adic representations.

Let P denote the set of prime numbers. In what follows, $(\rho_\ell)_{\ell\in P}$ will denote a system of ℓ-adic representations of K: for each $\ell \in P$, we are given a finite-dimensional $\mathbb{Q}_\ell$-vector space V_ℓ and a continuous homomorphism

$$\rho_\ell : \mathrm{Aut}(\overline{K}/K) \to \mathrm{GL}\, V_\ell.$$

We suppose that the ρ_ℓ are semisimple, rational [**MG**, I-9] and form a strcitly compatible system [**MG**, I-11]. LEt us recall that the last two properties are equivalent to the existence of a finite subset $S_\rho \subset \Sigma$ satsifying the following two properties:

(i) If $v \in \Sigma \setminus S_\rho$ and $\ell \neq p_v$, the representation ρ_ℓ is unramified at v.

We may thus speak of the Frobenius element F_{w,ρ_ℓ} of $\mathrm{Im}(\rho_\ell)$ attached to an extension w of v to $\overline{K}$ [**MG**, I-7]. Its conjugacy class depends onl on v; in particular, if t is an indeterminate, the polynomial

$$P_{v,\rho_\ell}(t) = \det(1 - tF_{w,\rho_\ell})$$

depends only on v and ℓ.

(ii) For all $v \in \Sigma \setminus S_\rho$, there is a polynomial $P_v(t) \in \mathbb{Q}[t]$ such that $P_v(t) = P_{v,\rho_\ell}(t)$ for all $\ell \neq p_v$.

Here are two consequences of (i) and (ii):

(iii) The V_ℓ have the same dimension, say d.

(iv) For all $\ell \in P$, $\mathrm{Im}(\rho_\ell)$ is compact, hence leaves stable a $\mathbb{Z}_\ell$-lattice T_ℓ of V_ℓ [**MG**, I-1]; it follows that, for all $\alpha \in \mathrm{Im}(\rho_\ell)$ the coefficients of $\det(1 - t\alpha)$ belong to $\mathbb{Z}_\ell$. In view of (ii), the coefficients of $P_v(t)$ belong to $\mathbb{Z}_\ell$ for all $\ell \neq p_v$ and thus are elements of $\mathbb{Z}[\frac{1}{p_v}]$.

Examples of systems (ρ_ℓ) satisfying the above conditions:

(1) The system defined by an elliptic curve (cf. §4 and [**MG**, Ch. IV]);

(2) The system (φ_ℓ) attached to a linear representation $\varphi_0 : S_{\mathfrak{m}} \to \mathrm{GL}_d$ of the algebraic group $S_{\mathfrak{m}}$ [**MG**, II-19]; note that this system is abelian, i.e., for all ℓ, $\mathrm{Im}(\varphi_\ell)$ has abelian image, so that φ_ℓ may be identified with a continus homomorphism from $\mathrm{Aut}(K^{\mathrm{ab}}/K)$ into $\mathrm{GL}\, V_\ell$.

We return to the general case. Let $\ell \in P$, and as above let T_ℓ a $\mathbb{Z}_\ell$-lattice which is stable under $\mathrm{Im}(\rho_\ell)$. The group $\mathrm{Aut}(\overline{K}/K)$ acts on $T_\ell/\ell T_\ell$; we denote by $\tilde{V}_\ell$ the

semisimplifciation of $T_\ell/\ell T_\ell$, and we denote by $\tilde{\rho}_\ell$ the corresponding homomorphism $\mathrm{Aut}(\overline{K}/K) \to \mathrm{GL}\,\tilde{V}_\ell$; this is a degree d linear representation of $\mathrm{Aut}(\overline{K}/K)$ over the field $\mathbb{F}_\ell$. According to Brauer-Nesbitt [**6**, §82.1], the isomorphism class of the representation $\tilde{\rho}_\ell$ does not depend on the choice of lattice T_ℓ; by abuse of language we will say say that $\tilde{V}_\ell$ is the *reduction modulo* ℓ of ρ_ℓ.

If $\tilde{\rho}_\ell$ is abelian, we may diagonalize it after extending scalars from $\mathbb{F}_\ell$ to its algebraic closure k_ℓ (cf. §3.4); we obtain d characters

$$\theta_\ell^{(i)} : \mathrm{Aut}(K^{\mathrm{ab}}/K) \to k_\ell^\times,\ i = 1, \dots, d.$$

Cassels noted in his MathReview that this is a bad choice of notation, because θ has been used for something else in §1. In the endnotes to this paper in his collected works, Serre mentions this and agrees with it. For now I have maintained the original notation. –PLC

As usual we will identify these characters with homomorphisms $\mathbb{I} \to k_\ell^\times$.

We come now to the main result of this section:

THEOREM 6. *Let (ρ_ℓ) be a system of semisimple ℓ-adic representations having properties (i) and (ii) above. Suppose that there is an integer N and an infinite subset L of P satisfying the following property:*
(*) For all $\ell \in L$, the reduction $\tilde{\rho}_\ell$ of ρ_ℓ modulo ℓ is abelian, and, for any associated character $\theta_\ell^{(i)} : \mathbb{I} \to k_\ell^\times$ there are integers $n(\sigma, \ell, i)_{\sigma\in\Gamma}$ less than N in absolute value such that

$$\theta_\ell^{(i)}(a) \equiv \prod_{\sigma\in\Gamma} \sigma_\ell(a_\ell^{-1})^{n(\sigma,\ell,i)} \pmod{\mathfrak{p}_\ell} \text{ for all } a \in U_{\mathfrak{m}}.$$

Then the system (ρ_ℓ) is isomorphic to the system (φ_ℓ) associated to a representation $\varphi_0 : S_{\mathfrak{m}} \to \mathrm{GL}_d$ defined over $\mathbb{Q}$ (cf. example 2 above).

In particular:

COROLLARY 11. *For all $\ell \in P$, ρ_ℓ is abelian.*

The remainder of this section is devoted to a proof of Theorem 6. –PLC

In view of (*), the $(\theta_\ell^{(1)})_{\ell\in L}$ satisfy the hypotheses of Proposition 21. There is thus an infinite subset $L_1 \subset L$ and a character $\psi^{(1)}$ of $S_{\mathfrak{m}}$ such that $\tilde{\psi}_\ell^{(1)} = \theta_\ell^{(1)}$ for all $\ell \in L_1$. Similarly, applying Proposition 21 to $(\theta_\ell^{(2)})_{\ell\in L_1}$ we obtain an infinite subset $L_2 \subset L_1$ and a character $\psi^{(2)}$ of $S_{\mathfrak{m}}$ such that $\tilde{\psi}_\ell^{(2)} = \theta_\ell^{(2)}$ for all $\ell \in L_2$. Continuing in this way, we finally obtain an infinite subset L' of L and characters $\psi^{(i)}$, $i = 1, \dots, d$, of $S_{\mathfrak{m}}$ such that $\tilde{\psi}^{(i)} = \theta_\ell^{(i)}$ for all $\ell \in L'$.

Let φ be the $\overline{\mathbb{Q}}$-representation $S_{\mathfrak{m}} \to \mathrm{GL}_d$ given by the direct sum of the d one-dimensional representations corresponding to the characters $\psi^{(i)}$. If $v \in \Sigma \setminus S$, let f_v be an idele whose vth component is a uniformizer of K_V and whose other components are equal to 1, and let $F_v \in S_{\mathfrak{m}}(\mathbb{Q})$ be the image of f_v under the canonical homomorphism $\epsilon : \mathbb{I} \to S_{\mathfrak{m}}(\mathbb{Q})$ [**MG**, II-11]; we have $\varphi(F_v) \in \mathrm{GL}_d(\overline{\mathbb{Q}})$.

LEMMA 7. *If $v \in \Sigma \setminus (S_\rho \cup S)$, then $\det(1 - t\varphi(F_v)) = P_v(t)$.*

PROOF. Put

$$P'_v(t) = \det(1 - t\varphi(F_v)) = \prod_{i=1}^{d} (1 - t\psi^{(i)}(F_v)).$$

If $\ell \neq p_v$, we have $\psi^{(i)}(F_v) = \psi_\ell^{(i)}(f_v)$ according to the formula (1) of §3.4; if moreover ℓ belongs to L', we deduce that

$$\psi^{(i)}(F_v) \equiv \psi_\ell^{(i)}(f_v i) \equiv \theta_\ell^{(i)}(f_v) \pmod{\mathfrak{p}_\ell},$$

whence

$$P'_v(t) \equiv \prod(1 - t\theta_\ell^{(i)}(f_v)) \pmod{\mathfrak{p}_\ell}.$$

But the $\theta_\ell^{(i)}(f_v)$ are the eigenvalues of the Frobenius element associated to v in the representation $\tilde{\rho}_\ell$. Thus we have

$$\prod(1 - t\theta_\ell^{(i)}(f_v)) \equiv P_v(t) \pmod{\ell},$$

whence

$$P'_v(t) \equiv P_v(t) \pmod{\mathfrak{p}_\ell}, \text{ if } \ell \in L',\ \ell \neq p_v.$$

Since this congruence holds for infinitely many values of ℓ, we deduce that $P'_v(t) = P_v(t)$. □

Lemma 7 shows in particular that the trace of the matrix $\varphi(F_V)$ belongs to $\mathbb{Q}$ for all $v \in \Sigma \setminus (S_\rho \cup S)$. As the F_v are dense in $S_\mathfrak{m}$ for the Zariski topology, it follows that φ is *definable over* $\overline{\mathbb{Q}}$ [**MG**, II-16, Prop. 2]. In other words, there is a linear representation

$$\varphi_0 : S_\mathfrak{m} \to \mathrm{GL}_d$$

of $S_\mathfrak{m}$, defined over $\mathbb{Q}$, such that φ and φ_0 become isomorphic after ext3ension of scalars to $\overline{\mathbb{Q}}$. If $\ell \in P$, denote by φ_ℓ the ℓ-adic representation attached to φ_0. If $v \in \Sigma \setminus (S_\rho \cup S)$ does not divide ℓ, we have – by [**MG**, II-20] and then by Lemma 7 – that

$$P_{v,\varphi_\ell}(t) = \det(1 - t\varphi(F_v)) = P_v(t)$$
$$= P_{v,\rho_\ell}(t).$$

The two representations φ_ℓ and ρ_ℓ are therefore *compatible* in the sense of [**MG**, I-10]. As they are also semi-simple, it follows that they are isomorphic (*loc. cit.*, which completes the proof of the theorem.

4. Elliptic curves (general results)

4.1. Notation; recalled facts.

In this §, K is a number field and $E_{/K}$ is an elliptic curve, equipped with a rational point !! – PLC, taken as the origin; we denote by j the modular invariant of E. For everything pertaining to K (resp. to E) we keep the notation of §3 (resp. of the introduction). In particular, if n is a positive integer, we denote by $E[n]$ the kernel of multiplication by n on $E(\overline{K})$, and we denote by

$$\varphi_n : G \to \mathrm{Aut}\, E[N]$$

the homomoprhism which gives the action of $G = \mathrm{Aut}(\overline{K}/K)$ on $E[n]$.

Alongside of the $E[n]$, it is useful "commodious" – PLC to utilize the *Tate modules* T_ℓ and V_ℓ of E [**MG**, p. I-3]. Recall that for $\ell \in P$, we put

$$T_\ell = \varprojlim E[\ell^n] \text{ and } V_\ell = T_\ell[\frac{1}{\ell}] = T_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell,$$

and that T_ℓ (resp. V_ℓ) is a free $\mathbb{Z}_\ell$-module (resp. a $\mathbb{Q}_\ell$-vector space) of rank 2. The group $\mathrm{GL}\, T_\ell$ is isomorphic to $\mathrm{GL}_2(\mathbb{Z}_\ell)$ and is compact and open in $\mathrm{GL}\, V_\ell$, which is isomorphic to $\mathrm{GL}_2(\mathbb{Q}_\ell)$. The φ_{ℓ^n} define a continuous homomorphism

$$\rho_\ell : G \to \mathrm{GL}\, T_\ell \subset \mathrm{GL}\, V_\ell.$$

Remark 15. *1) We have*

$$V_\ell/T_\ell = \bigcup_n \ell^{-n} T_\ell/T_\ell = \bigcup_n E[\ell^n] = E[\ell^\infty].$$

From this we deduce a homomorphism $\mathrm{GL}\, T_\ell \to \mathrm{Aut}\, E[\ell^\infty]$ *which is in fact an isomorphism, as one verifies immediately; this allows us to identify* ρ_ℓ *with the homomorphism* φ_{ℓ^∞} *defined in the introduction.*
2) One knows [**MG**, p. I-11, IV-5] *that the* ℓ*-adic representations* ρ_ℓ *are* rational *and form a* strictly compatible system*; the corresponding exceptional set is the set* S_E *of places of* K *at which* E *has* bad reduction *(c.f.* [**30**] *as well as* [**MG**, IV-5]*). More precisely, if* $v \in \Sigma \setminus S_E$ *and* $\ell \neq p_v$*, the representation* ρ_ℓ *is unramifed at* v *and the corresponding polynomial* $P_{v,\rho_\ell}(T)$ *is given by*

$$P_{v,\rho_\ell}(T) = 1 - \mathrm{Tr}(F_v)T + NvT^2;$$

in this formula, F_v *is the* Frobenius endomorphism *of the elliptic curve* $\tilde{E}_v$ *deduced from* E *by reduction modulo* v*, and* $\mathrm{Tr}(F_v)$ *is the* trace *of* F_v*. The number of points of* $\tilde{E}_v$ *over the finite field* k_v *is linked to* $\mathrm{Tr}(F_v)$ *by the formula:*

$$\#\tilde{E}_v(k_v) = 1 + Nv - \mathrm{Tr}(F_v).$$

4.2. Surjectivity of the φ_ℓ.

Now we will demonstrate the main results announced in the introduction.

Theorem 7. *Suppose that the elliptic curve* E *has no complex multiplication over* $\overline{K}$*. Then, for almost every prime number* ℓ*, the homomorphism* $\varphi_\ell : \mathrm{Aut}(\overline{K}/K) \to \mathrm{Aut}\, E[\ell]$ *is surjective.*

(Otherwise put, the Galois group of the "ℓ-torsion field" is almost always isomorphic to $\mathrm{GL}_2(\mathbb{F}_\ell)$.)

The proof consists of several steps:

a) Reduction to the semistable case

After replacing K by a finite extension, we may suppose (and we will in what follows) that E has *good reduction* at every place $v \in \Sigma$ such that $v(j) \geq 0$ and *multiplicative reduction* at every place v such that $v(j) < 0$ (it suffices, for example, to adjoin to K the coordinates of the 12-torsion points of E). Thus the Néron model of E over $\mathcal{O}_K$ has every fiber either an elliptic curve over an extension of a torus by a finite group: it is *semistable* in the sense of Grothendieck and Mumford.

b) Structure of the groups $\varphi_\ell(G)$

In what follows, we will suppose that there is an infinite subset L of P such that $\varphi_\ell(G) \neq \mathrm{Aut}\, E[\ell]$ for all $\ell \in L$ and seek to show that E has complex multiplication. By removing a finite subset from L we may assume that every element of L is at least 7 and is unramified in K.

Let $\ell \in L$, let v be a place of K lying over ℓ, and choose a place w of $\overline{K}$ extending v; let I_w be the corresponding inertia subgroup of G. The local study of §1, applied to the field K_V, gives the structure of the subgroup $\varphi_\ell(I_w)$ of $\varphi_\ell(G)$:

if, at v, E has ordinary good reduction or multiplicative bad reduction, then $\varphi_\ell(I_w)$ has order $\ell - 1$ or $\ell(\ell - 1)$, and one can represent it matrices of the form $\begin{bmatrix} * & 0 \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix}$, c.f. §1.11, Corollary to Proposition 12 and §1.12, Corollary to Proposition 14;

if, at v, E has supersingular good reduction, then $\varphi_\ell(I_w)$ is cyclic of order $\ell^2 - = 1$, cf. §1.12, Proposition 13.

In the first case, $\varphi_\ell(G)$ contains a split semi-Cartan subgroup, and in the second case it contains a nonsplit Cartan subgroup. Moreover, we have $\varphi_\ell(G) \neq \operatorname{Aut} E[\ell]$ by hypothesis. Proposition 18 leaves us with the following two possibilities:

i) $\varphi_\ell(G)$ is contained in a Borel subgroup or a Cartan subgroup;
(ii) $\varphi_\ell(G)$ is contained in the normalizer of a Cartan subgroup C_ℓ and is not contained in C_ℓ.

We will now show that ii) can occur for only finitely many values of ℓ (if E does not have complex multiplication):

c) Elimination of case ii)

Let $\ell \in L$ be of type ii) above, with $\varphi_\ell(G) \subset N_\ell$ and $\varphi_\ell(G) \not\subset C_\ell$. We may uniquely! – PLC identify N_ℓ/C_ℓ with the group $\{\pm 1\}$ and denote by ϵ_ℓ the composition

$$G \to N_\ell \to N_\ell/C_\ell \xrightarrow{\sim} \{\pm 1\}.$$

This is an order 2 character of G; it corresponds to a quadratic extension K'_ℓ of K.

LEMMA 8. *The extension $K_{\ell'}/K$ is unramified.*

PROOF. Let $v \in \Sigma$, let w be an extension of v to $\overline{K}$, and let I_w be the corresponding inertia subgroup. We must show that $\epsilon)_\ell(I_w) = \{1\}$. We distinguish three cases:

v_1) We have $p_v = \ell$. We saw above the structure of $\varphi_\ell(I_w)$: it is either a split semi-Cartan subgroup or a nonsplit subgroup (the case in which $\varphi_\ell(I_w)$ would have order $\ell(\ell - 1)$ is ruled out, since $\varphi_\ell(I_w)$ is contained in N_ℓ which has order prime to ℓ). Proposition 15 then shows that $\varphi_\ell(I_w)$ is contained in C_ℓ, i.e., $\epsilon_\ell(I_w) = \{1\}$.

v_2) We have $p_v \neq \ell$ and E has good reduction at v. Then $\varphi_\ell(I_w) = \{1\}$, hence certainly $\epsilon_\ell(I_w) = \{1\}$.

v_3) We have $p_v \neq \ell$ and E has bad reduction at v. In view of a), the reduction must be multiplicative. According to Tate's theory [**MG**, IV-31], we have an exact sequence

$$0 \to \mu_\ell \to E[\ell] \to \mathbb{Z}/\ell\mathbb{Z} \to 0$$

which is compatible with the action of I_W. It follows that $\varphi_\ell(I_w)$ is either trivial or cyclic of order ℓ. The second case is impossible since N_ℓ has order prime to ℓ. Thus we have $\varphi_\ell(I_w) = \{1\}$, so $\epsilon_\ell(I_w) = \{1\}$. □

Now suppose that there is an infinite subset $L' \subset L$ such that, for all $\ell \in L'$, $\varphi_\ell(G)$ is of type (ii). Since the unramified quadratic extensions of K are finite in

number, there is such one such extension K' which is equal to K'_ℓ for infinitely many $\ell \in L'$.

LEMMA 9. *If $v \in \Sigma$ is inert in K' and if E has good reduction at v, then we have $\operatorname{Tr} F_v = 0$ and the curve $\tilde{E}_v$ is supersingular.*

(Recall that F_v denotes the Frobenius endomorphism of $\tilde{E}_v$ over the finite field k_v.)

PROOF. If $\ell \neq p_v$, then φ_ℓ is unramified at v; if π_w denotes the Frobenius element associated to the extension w of v, we have $\operatorname{Tr} F_v \equiv \operatorname{Tr} \pi_w \pmod{\ell}$. Suppose moreover that ℓ belongs to L' and that $K'_\ell = K'$; we have $\pi_w \in N_\ell$ and, since v is inert in K', we have $\epsilon_\ell(\pi_w) = -1$, i.e., $\pi_w \in N_\ell \setminus C_\ell$. But the elements of $N_\ell \setminus C_\ell$ have trace zero. We deduce:

$$\operatorname{Tr} F_v \equiv \operatorname{Tr} \pi_w \equiv 0 \pmod{\ell}.$$

Since this congruence holds for infinitely many ℓ in fact we have $\operatorname{Tr} F_v = 0$, and one knows that this implies that $\tilde{E}_v$ is supersingular. □

Let Σ' be the set of places satisfying the hypotheses of Lemma 9. According to the Cebotarev Density Theorem, the density of Σ' is $\frac{1}{2}$. On the other hand, one knows (c.f. [**26**, Cor. 1 to Thm. 6] and [**MG**, IV-13, Exc.] that if E does not have complex multiplication, the set of places v of supersingular reduction has density 0. Thus Lemma 9 implies that E has complex multiplication in the case considered.

Variant: Instead of using the vanishing of $\operatorname{Tr} F_v$ and a density argument, one could also observe that, if one extends the ground field to K', the groups $\varphi_\ell(G)_{\ell \in L'}$ become of type i), which permits the application of the arguments of d) and e) below.

d) The case i)

Let $\ell \in L$ be such that $\varphi_\ell(G)$ is of type i). Denote by

$$\tilde{\varphi}_\ell : G \to \mathrm{GL}_2(\mathbb{F}_\ell)$$

the representation of G deduced from φ_ℓ by semisimplification. Because $\varphi_\ell(G)$ is of type i), the representation $\tilde{\varphi}_\ell$ is abelian. By extending scalars from $\mathbb{F}_\ell$ to its algebraic closure k_ℓ (cf. §3.4), one can put $\tilde{\varphi}_\ell$ in diagonal form, and it is then given by two characters

$$\theta_\ell^{(i)} : \mathrm{Aut}(K^{\mathrm{ab}}/K) \to k_\ell^\times, \ i = 1, 2;$$

as usual, we will identify the $\theta_\ell^{(i)}$ with homomorphisms from $\mathbb{I}$ into $k_\ell^\times$, where $\mathbb{I}$ is the idele group of K.

LEMMA 10. *Let $\mathfrak{m}$ be the modulus of K with support $S = \varnothing$. There is a family of integers $n(\sigma, \ell, i)$ ($i \in \{1, 2\}$, $\sigma \in \Gamma$) equal to 0 or 1, such that*

$$\theta_\ell^{(i)}(a) \equiv \prod_{\sigma \in \Gamma} \sigma_\ell(a_\ell^{-1}))^{n(\sigma,\ell,i)} \pmod{\mathfrak{p}_\ell}$$

for all $i \in \{1, 2\}$ and $a \in U_\mathfrak{m}$.

(Notation as in §3; in particular, Γ denotes the set of embeddings of K in $\overline{\mathbb{Q}}$).

PROOF. Let us first check that $\tilde{\varphi}_\ell$ is unramified at every place $v \in \Sigma$ not dividing ℓ. This is clear if E has good reduction at v. Otherwise E has multiplicative bad reduction at v; the argument used in the proof of Lemma 8 shows that the inertia group $\varphi_\ell(I_w)$ corresponding to v is either trivial or cyclic of order ℓ; after semisimplification such a group becomes trivial, which shows that $\tilde{\varphi}_\ell(I_w) = \{1\}$.

In this way the characters $\theta_\ell^{(i)}$ are unramified outside of places dividing ℓ. According to class field theory it is equivalent to show that $\theta_\ell^{(i)}(a) = 1$ if $a \in U_{v,\mathfrak{m}}$ and $p_v \neq \ell$. To show (*) it thus suffices to find exponents $n(\sigma, i, \ell)$ equal to 0 or 1 such that we have

$$(*') \qquad \theta_\ell^{(i)}(a) \equiv \prod_{\sigma \in \Gamma} \sigma_\ell(a^{-1})^{n(\sigma,\ell,i)} \pmod{\mathfrak{p}_\ell} \text{ for all } a \in U_\ell.$$

We use the decomposition $U_\ell = \prod_{v|\ell} U_v$, and denote by $\Gamma(v)$ the set of embeddings $\sigma : K \hookrightarrow \overline{\mathbb{Q}}$ such that $v_\ell \circ \sigma$ is equivalent to v. The $\Gamma(v)$, for $v \mid \ell$, form a partition of Γ, cf. §3.4, and the formula $(*')$ is equivalent to:

$$(**) \qquad \theta_\ell^{(i)}(A) \equiv \prod_{\sigma \in \Gamma(v)} \sigma_\ell(a^{-1})^{n(\sigma,\ell,i)} \pmod{\mathfrak{p}_\ell} \text{ for all } a \in U_v.$$

The question is now local on v. From the fact that v is unramified over $\mathbb{Q}$, $[K_v : \mathbb{Q}_\ell]$ equals the residual degree $f_v = [k_v : \mathbb{F}_\ell]$ of v, and $\Gamma(v)$ has f_v elements. Moreover, the homomorphisms

$$\tilde{\sigma}_\ell : k_v \to k_l \ (\sigma \in \Gamma(v)),$$

deduced from the σ_ℓ by reduction modulo $\mathfrak{p}_\ell$, are nothing else than the disinct embeddings of k_v in the algebraically closed field k_ℓ. It then follows from local class field theory (cf. §1.5, Proposition 4), that the homomorphisms

$$a \mapsto \sigma_\ell(a^{-1}) \pmod{\mathfrak{p}_v}$$

constitute, as σ ranges over $\Gamma(v)$, the different fundamental characters of level f_v of the tame inertia group of K_v. The formula (**) is thus equivalent to saying that the restriction of $\theta_\ell^{(i)}$ to the inertia group I_v at v is the product of the fundamental characters of level f_v with exponents 0 or 1. Thus this assertion results from the explicit determinations of §1.11 and §1.12. More precisely there are three cases to consider:

d_1) E has ordinary good reduction at v. According to the Corollary to Proposition 12, the restrictions of the $\theta_\ell^{(i)}$ to I_V are either trivial or the fundamental character $I_v \to \mathbb{F}_\ell^\times$ of level 1. In the first case, we take all the exponents $n(\sigma, \ell, i)$ equal to 0, and in the second all equal to 1.

d_2) E has supersingular good reduction at v. According to Proposition 13b), the restrictions of the $\theta_\ell^{(i)}$ to I_v are the two fundamental characters $\chi^{(1)}$ and $\chi^{(2)}$ of level 2; moreover, Proposition 13d) shows that k_v contains $\mathbb{F}_{\ell^2}$, so that $\chi^{(1)}$ and $\chi^{(2)}$ are obtained by composing the fundamental character

$$\theta_{\ell^2-1} : I_v \to \mathbb{F}_{\ell^2}^\times$$

with the two embeddings $\tau^{(1)}$ and $\tau^{(2)}$ of $\mathbb{F}_{\ell^2}$ into k_ℓ. We then take

$$n(\sigma, \ell, i) = \begin{cases} 1 & \text{if } \tilde{\sigma}_\ell \text{ extends } \tau^{(i)} \\ 0 \text{ otherwise,} & \end{cases},$$

which proves the assertion in this case.
d_3) E has multiplicative bad reduction at v. According to the Corollary of Proposition 14, the situation is the same as in case d_1. □

e) End of the proof of Theorem 2

In view of b) and c), we may suppose that $\varphi_\ell(G)$ is of type i) for all $l \in L$. The system of ℓ-adic representations

$$\rho_\ell : G \to \mathrm{GL}\, V_\ell$$

satisfies the hypotheses of Theorem 1 of §3.6, the integer N of that result being taken equal to 1; this follows from Lemma 10 and from the fact that the ρ_ℓ are rational, semisimple (and even irreducible if E has no complex multiplication, cf. [**MG**, IV-9, §2.1] and form a strictly compatible system. The corollary to Theorem 1 then shows that the ρ_ℓ are abelian, which by [**MG**, IV-11] implies that E has complex multiplication. QED.

4.3. Questions.

We suppose that E has no complex multiplication. Theorem 2 shows the existence of an integer N such that $\varphi_\ell(G) = \mathrm{Aut}\, E_\ell$ for all primes $\ell \geq N$. Can we *effectively determine* such an N as a function of the coefficients of an equation of E? This seems likely; however, it seems that one would first need to establish an *effective form of the Cebotarev density theorem*, which has not yet been done. (When E is explicitly given, one can often determine N simply by revisiting the method of proof of Theorem 2; we will see some examples in §5.)

The following question appears more difficult: can we take N to be an integer *depending only on* K, and not on E? For example, can we take $N = 19$ when $K = \mathbb{Q}$? One can hope that the methods of Manin and Demjanenko, based on properties of *heights* of points of E, will give an answer to this kind of question.

4.4. Image of φ_∞.

The family $(\rho_\ell)_{\ell \in P}$ defines a continuous homomorphism

$$\rho : G \to \prod_{\ell \in P} \mathrm{GL}\, T_\ell \cong \prod_{\ell \in P} \mathrm{GL}_2(\mathbb{Z}_\ell);$$

this is essentially the homomorphism $\varphi_\infty : G \to \mathrm{Aut}\, E_\infty$ of *the introduction.*

THEOREM 8. *If E has no complex multiplication, then $\rho(G)$ is an open subgroup of $\prod_{\ell \in P} \mathrm{GL}\, T_\ell$.*

This results from Theorem 7 of §4.2 and the proposition proved in [**MG**, IV-19].

As we have already indicated, Theorem 8 is equivalent to:

THEOREM 9. *The index of $\varphi_n(G)$ in $\mathrm{Aut}\, E[n]$ remains bounded as n varies.*

This implies:

COROLLARY 12. *For almost every ℓ, $\rho(G)$ contains the ℓth factor $\mathrm{GL}\, T_\ell$ of the product $\prod_{\ell \in P} \mathrm{GL}\, T_\ell$.*

We will make this result more precise later on: c.f. Theorem 10 below.

COROLLARY 13. *Let K^{cyc} be the subfield of $\overline{K}$ obtained by adjoining to K all roots of unity. The image of $\mathrm{Aut}(\overline{K}/K^{\mathrm{cyc}})$ under ρ is an open subgroup of $\prod_{\ell\in P}\mathrm{SL}\,T_\ell$.*

PROOF. We know that the composite of the maps

$$\rho_\ell : G \to \mathrm{GL}\,T_\ell \text{ and } \det : \mathrm{GL}\,T_\ell \to \mathbb{Z}_\ell^\times$$

is the ℓ-adic character $\chi_\ell : G \to \mathbb{Z}_\ell^\times$ giving the action of G on the ℓ^nth roots of unity i.e., the **cyclotomic character** – PLC [**MG**, I-3 and I-4]. Since $\mathrm{Aut}(\overline{K}/K^{\mathrm{cyc}})$ is the intersection of the kernels of the χ_ℓ, we deduce that the image of ρ is the intersection of $\rho(G)$ and $\prod_{\ell\in P}\mathrm{SL}\,T_\ell$. The corollary follows. □

REMARK 16. *More generally, let L be a subfield of $\overline{K}$ containing K^{cyc}, such that L/K^{cyc} is Galois and* solvable. *Then $\rho(\mathrm{Aut}(\overline{K}/L))$ is an* open *subgroup of $\prod_{\ell\in P}\mathrm{SL}\,T_\ell$. This follows from Corollary 13 and the following easily verified fact: if U is an open subgroup of $\prod_{\ell\in P}\mathrm{SL}_2(\mathbb{Z}_\ell)$, the closure of the commutator subgroup of U is* open *in U. Let us note that this applies in particular to the case $L = K^{\mathrm{ab}}$.*

We continue to assume that E has no complex multiplication. For $v \in \Sigma$, we choose an extension w of v to $\overline{K}$ and let I_w be the corresponding inertia subgroup of G; we denote by J_v the smallest closed normal subgroup of G containing I_w; it does not depend on the choice of w.

THEOREM 10. *For almost every p, $\rho(J_v)$ is equal to the p_vth factor $\mathrm{GL}\,T_{p_v}$ in the product $\prod_{\ell\in P} GLT_\ell$.*

(We recall that p_v denotes the *residue characteristic* of v.)

Theorem 10 is implied by the following more precise statement:

THEOREM 11. *Put $\ell = p_v$. Suppose $\ell \geq 5$, $\varphi_\ell : G \to \mathrm{Aut}\,E[\ell]$ is surjective, E has good reduction at v, and v is unramified over $\mathbb{Q}$. Then $\rho(J_v) = \mathrm{GL}\,T_\ell$.*
(In view of Theorem 2, the above hypotheses hold for almost every v.)

PROOF. Since E has good reduction at v, the inertia group I_w acts trvially on $T_{\ell'}$ for $\ell' \neq \ell$, and thus the same holds for J_v. The group $\rho(J_v)$ is thus a subgroup H of the the factor $\mathrm{GL}\,T_\ell$ of the product $\prod_{\ell\in P}\mathrm{GL}\,T_\ell$. The image $\tilde{H}$ of H in $\mathrm{Aut}\,E[\ell] = \mathrm{Aut}\,T_\ell/\ell T_\ell$ is a normal subgroup of $\varphi_\ell(G) = \mathrm{Aut}\,E[\ell]$. Since v is unramified over $\mathbb{Q}$, the corollaries to Propositions 11 and 12 of §1.11 show that $\tilde{H}$ contain either a split semi-Cartan or a nonplsit Cartan. In view of Proposition 17 of §2.7, we thus have $\tilde{H} = \mathrm{Aut}\,E[\ell]$. Now let H' be the closure of the commutator subgroup of H: we have $H' \subset \mathrm{SL}\,T_\ell$ and the image $\widetilde{H'}$ of H' in $\mathrm{SL}\,E[\ell]$ is the commutator subgroup of $\tilde{H}$, i.e., $\mathrm{SL}\,E[\ell]$. Applying [**MG**, Lemma 3, IV-23] to H' we deduce that $H' = \mathrm{SL}\,T_\ell$. On the other hand, the fact thtat v is unramified over $\mathbb{Q}$ implies that $\chi_\ell(I_w) = \mathbb{Z}_\ell^\times$, and the image of H under the map

$$\det : \mathrm{GL}\,T_\ell \to \mathbb{Z}_\ell^\times$$

is thus equal to $\mathbb{Z}_\ell^\times$. Since we just saw that H contains the kernel $\mathrm{SL}\,T_\ell$ of this homomorphism, it follows that $H = \mathrm{GL}\,T_\ell$. □

REMARK 17. *Assuming only that E has good reduction at v, one can show that $\rho(J_v)$ is an* open subgroup *of the p_vth factor $\mathrm{GL}\,T_{p_v}$ in the product $\prod_{\ell\in P}\mathrm{GL}\,T_\ell$.*

4.5. Curves with complex multiplication.

As indicated in the introduction, this case has been known for a long time. I'm going to limit myself to rapidly summarizing the main results, referring to [**9**], [**10**], [**30**] or [**34**] for more details:

Let $R = \mathrm{End}_{\overline{K}}(E)$. We suppose that $R \neq \mathbb{Z}$, in which case it is an "order" in the imaginary quadratic field $F = \mathbb{Q} \otimes R$. We suppose that the elements of R are defined over K; their action on the Lie algebra of E i.e., on the tangent space at the origin – PLC is given by a homomorphism $R \to K$; by passage to the fracion field, this allows us *to identify F with a subfield of K*.

If $\ell \in P$, we put $R_\ell = \mathbb{Z}_\ell \otimes R$ and $F_\ell = \mathbb{Q}_\ell \otimes F$. The Tate module T_ℓ is a free, rank one R_ℓ-module [**30**, §4] and V_ℓ is an F_ℓ-vector space of dimensoin 1. The image of G under

$$rho_\ell : G \to GLT_\ell$$

commutes with the elements of R_ℓ hence is contained in $R_\ell^\times$. [Thus i]t is abelian, and one can identify it with a homomorphism

$$\rho_\ell : \mathbb{I} \to R_\ell^\times,$$

where $\mathbb{I}$ is the idele group of K.

THEOREM 12. *There is exactly one continuous homomorphism $\epsilon : \mathbb{I} \to F^\times$ such that*

- *For all $x \in K^\times$, $\epsilon(x) = N_{K/F}(x)$ and*
- *For all $\ell \in P$ and $a \in \mathbb{I}$, $\rho_\ell(a) = \epsilon(a) N_{K_\ell/F_\ell}(a_\ell^{-1})$.*

This is a reformulation – essentially due to Weil [**39**], [**40**]; see also [**30**, §7] – of classical results.

COROLLARY 14. *The image of G under ρ is an open subgroup of the product $\prod_{\ell \in P} R_\ell^\times$.*

PROOF. Since ϵ is continuous for the discrete topology on F – PLC, its kernel is open, hence contains a subgroup $U_{\mathfrak{m}}$ for a suitable $\mathfrak{m}$ (if one takes the smallest possible $\mathfrak{m}$, its support is the set of places at which E has bad reduction, cf. [**30**, Cor. 1 to Thm. 11]. It suffices to show that $\rho(U_{\mathfrak{m}})$ is open in $\prod_{\ell \in P} R_\ell^\times$. Now, for $a \in U_m$, by Theorem 5 we have

$$\forall \ell \in P,\ \rho_\ell(a) = N_{K_\ell/F_\ell}(a_\ell^{-1}).$$

We are thus reduced to showing that the map

$$N_{K_\ell/F_\ell} : U_{\ell,m} \to R_\ell^\times$$

is *open* for all ℓ and *surjective* for almost all ℓ, which is well known. □

REMARK 18. *1) Corollary 14 is the analogue of Theorem 8. There is also a (partial) analogue of Theorem 10: for almost every v, $\rho(J_v)$ is equal to the compnent of $R_{p_v}^\times$ coresponding to the place of F induced by v; we note however that if ℓ splits in F, this component* is not *equal to $R_{p_v}^\times$.*
2) One can show that every homomorphism $\epsilon : \mathbb{I} \to F^\times$ satisfying the conditions of Theorem 12 corresponds, as above, to an elliptic curve $E_{/K}$ such that $\mathrm{End}_K(E)$ is an order of F; moreover E is unique up to isogeny.

5. Elliptic curves (examples)

The object of this § is to explicitly determine, for certain elliptic curves E, the set of prime numbers ℓ such that $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$.

5.1. Notation.

The curve E is given as a nonsingular cubic:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{5}$$

the point at infinity being taken as the origin. We put, following Néron and Tate[3]:

$$b_2 = a_1^2 + 4a_2,\ b_4 = a_1a_3 + 2a_4,\ b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 = \frac{1}{4}(b_2b_6 - b_2^2),$$
$$c_4 = b_2^2 - 24b_4,\ c_6 = 36b_2b_4 - b_2^3 - 216b_6,$$
$$\Delta = b_4^3 - 27b_6^2 + b_8(36b_4 - b_2^2) = \frac{1}{1728}(c_4^3 - c_6^2);$$

the modular invariant j of E is equal to $\frac{c_4^3}{\Delta}$.

Throughout this section (except for §5.10) *the base field is the field $\mathbb{Q}$ of rational numbers*, and (5) is chosen to so as to give a *standard model* of E in the sense of Néron [**16**] i.e., a minimal Weierstrass model! – PLC. In particular, the coefficients $a_1, \dots, c_6$ are *integers*.

We denote by S_E the set of $p \in P$ at which E has bad reduction; this is the set of prime divisors of Δ; we have $S_E \neq \varnothing$, cf. Shafarevich [**23**] or Ogg [**18**]. We denote by N *the conductor* of E, in the sense of Weil; for the definition, see Weil [**41**], Ogg or [**29**, §2.4]; we have

$$N = \prod_{p \in S_E} p^{n(p)}$$

with $n(p) \geq 1$ and even $n(p) \in \{1, 2\}$ if $p \geq 5$.

If $p \notin S_e$, we denote by $\tilde{E}(p)$ the reduction of E modulo p, and by t_p the trace of its Frobenius endomorphism. We have

$$t_p = 1 + p - A_p,$$

where $A_p = \#\tilde{E}(p)(\mathbb{F}_p)$.

5.2. Remarks on $\varphi_\ell(G)$.

We have at our disposal a certain amount of information about the subgroups $\varphi_\ell(G)$ of $\operatorname{Aut} E[\ell]$:

(i) Their *inertia subgroups* are essentially known, cf. §1.

(ii) Every $p \notin S_E \cup \{\ell\}$ gives a Frobenius element $\pi_p \in \varphi_\ell(G)$, well-defined up to conjugacy, such that

$$Tr\pi_p \equiv t_p \pmod{\ell} \text{and } \det \pi_p \equiv p \pmod{\ell}.$$

(iii) The homomorphism $\det : \varphi_\ell(G) \to \mathbb{F}_\ell^\times$ is *surjective*; indeed, its image is the Galois group of the ℓth cyclotomic field.

---

[3]Here Serre makes reference to a mildly different normalization due to Ogg. Since this paper was written, the Néron-Tate normalization has become completely standard, so I will not reproduce Serre's footnote. – PLLC

(iv) $\varphi_\ell(G)$ contains an element c with eigenvalues $\{1,-1\}$; this is furnished by complex conjugation (relative to an embedding of $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$). It follows that, if $\ell \neq 2$, then $\varphi_\ell(G)$ *is not contained in a nonsplit Cartan subgroup of* $\operatorname{Aut} E[\ell]$.

The information furnished by (ii), combined with Proposition 20, is sometimes sufficient to show that $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$. We take for example the curve

$$E : y^2 + y = x^3 - x^2$$

of conductor 11. We have $\#\tilde{E}(2)(\mathbb{F}_2) = 5$ and $\#\tilde{E}(3)(\mathbb{F}_3) = 5$), whence:

$$\operatorname{Tr} \pi_2 = t_2 = 1 + 2 - 5 = -2,\ \det \pi_2 = 2,\ (\operatorname{Tr} \pi_2)^2 - 4 \det \pi_2 = -4,$$

and

$$\operatorname{Tr} \pi_3 = t_3 = 1 + 3 - 5 = -1,\ \det \pi_3 = 3,\ (\operatorname{Tr} \pi_3)^2 - 4 \det \pi_3 = -11.$$

Suppose $\ell \geq 13$ and $\left(\frac{11}{\ell}\right) = -1$. Then one of the numbers $-4, -11$ is a square modulo ℓ and the other is not. Moreover the elements

$$u = \operatorname{Tr}(\pi_3)^2 / \det \pi_3$$

satisfies:

$$u \not\equiv 0, 1, 2, 4 \pmod{\ell} \text{ and } u^2 - 3u + 1 \not\equiv 0 \pmod{\ell}.$$

All of the conditions of Proposition 20 are thus satisfied by $\varphi_\ell(G)$. We conclude that, for such an ℓ (e.g. 13, 17, 23, 29, ...), *we have* $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$. This is essentially the method followed by Shimura [**32**]; it has the inconvenience of only applying to values of ℓ satisfying certain congruences and cannot give a result valid "for almost all ℓ". We will see in §5.5 that one can obtain, with a little calculation, a more complete result, by making use of information of type (i) above.

5.3. The particular cases $\ell = 2$ and $\ell = 3$.

These cases are well known. We recall them briefly:

a) $\ell = 2$

The curve E has three points of order two, of which the x-coordinates $\{e_1, e_2, e_3\}$ are solutions of the equation

$$4x^2 + b_2 x^2 + 2b_4 x + b_6 = 0.$$

The square root of Δ can be expressed in terms of the e_i by:

$$\Delta^{\frac{1}{2}} = \pm 4(e_1 - e_2)(e_2 - e_3)(e_3 - e_1).$$

The group $\operatorname{Aut} E[2] \cong \mathrm{GL}_2 F_2$ can be identified with the group S_3 acting by permutation of indices on $\{e_1, e_2, e_3\}$. Denote by $\epsilon : S_3 \to \{\pm 1\}$ the "signature" homomorphism. Composing $\varphi_2 : G \to AutE[2]$ with ϵ, we obtain a homomorphism from G to $\{\pm 1\}$ which corresponds to an extension of the base field of degree at most 2. The formula above shows that this extension is the one defined by $\Delta^{\frac{1}{2}}$. In this way, *for* $\varphi_2(G)$ *to be contained in* A_3*, it is necessary and sufficient that* Δ *be a square* (when $j \neq 1728$, this is equivalent to saying that $j - 1728$ is a square, since $j - 1728 = \frac{c_6^2}{\Delta}$.

a) $\ell = 3$

The curve E has eight points of order 3, which come in four mutually inverse pairs. Their x-coordinates x_i $(1 \leq i \leq 4)$ are the roots of the equation

$$3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8 = 0.$$

The group $(\mathrm{Aut}\, E[3])/\{\pm 1\} \cong \mathrm{PGL}_2(\mathbb{F}_3)$ may be identified with the group S_4 acting by permutation of indices on $\{x_1, \ldots, x_4\}$. There are three ways to decompose $\{1,2,3,4\}$ into disjoint subsets $\{i,j\}$ and $\{k,\ell\}$; each of these decompositions corresponds to a cube root of Δ via the formula

$$\Delta^{\frac{1}{3}} = b_4 - 3(x_ix_j + x_kx_\ell).$$

Let $\sigma : S_4 \to S_3$ be the homomorphism giving the action of S_4 on the three decompositions above; according to the above formula, this homomorphism is the one that gives the action of G on the three cube roots of Δ. In particular, *the order of $\varphi_3(G)$ is divisible by 3 iff Δ is not a cube* (when $j \neq 0$, this is equivalent to saying that j is not a cube, since $j = \frac{c_4^3}{\Delta}$).

One will find further information on the case $\ell = 3$ in Neumann [**17**, §1]. Let us mention that one can also express $\Delta^{\frac{1}{4}}$ in terms of the coordinates of the points of order 4 of E.

5.4. Semistable curves.

In this §, as well as the following one, we treat the simplest case, in which the Néron model of E is *semi-stable*. This means (cf. §4.2) that, if E has bad reduction at a prime number p (i.e., if $p \in S_E$), this bad reduction *is of multiplicative type*; one thus has

$$v_p(j) = -v_p(\Delta) < 0, \text{ where } v_p \text{ is the } p\text{-adic valuation of } \mathbb{Q}.$$

By passage to an unramified extension of $\mathbb{Q}_p$ (that one could take to be equal to $\mathbb{Q}_p(\sqrt{-c_6})$ the curve E becomes isomorphic to the *Tate curve* attached to j (§1.12).

The *conductor* N of E is the product of the primes p appearing in S_E; it is *squarefree*.

We will see that, for sucha curve, the presence of a point of order ℓ is essentially the only obstacle to $\varphi_\ell(G) = \mathrm{Aut}\, E[\ell]$. More precisely:

Proposition 23. *Let $E_{/\mathbb{Q}}$ be a semistable elliptic curve, and let ℓ be a prime number. Suppose: a) $\varphi_\ell \neq \mathrm{Aut}\, E[\ell]$; and*
b) Either $\ell \neq 2,3,5$ or ℓ does not divide $v_p(j)$ for some $p \in S_E$.
Then:
(i) $\varphi_\ell(G)$ is contained in a Borel subgroup of $\mathrm{Aut}\, E[\ell]$;
(ii) The G-module $E[\ell]$ has a Jordan-Hölder sequence with quotients isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ;
(iii) $t_p \equiv 1 + p \pmod{\ell}$ for all $p \in P \setminus S_E$.

proof of (i): Suppose first that there is $p \in S_E$ such that $v_p(j) \not\equiv 0 \pmod{\ell}$. By [**MG**, IV-37], $\varphi_\ell(G)$ contains an element of order ℓ, coming from the inertia at p. According to Proposition 16, it follows that $\varphi_\ell(G)$ is either contained in a Borel or contains $\mathrm{SL}\, E[\ell]$. However in the latter case one would have $\varphi_\ell(G) = \mathrm{Aut}\, E[\ell]$, since $\det : \varphi_\ell(G) \to \mathbb{F}_\ell^\times$ is surjective – cf. §5.2 – and that would contradict the hypothesis a). This gives (i) in the case considered.

Now suppose $\ell \geq 7$. According to what we saw in §1 (applied to the ℓ-adic field

$\mathbb{Q}_\ell$), the group $\varphi_\ell(G)$ contains either a nonsplit Cartan or a split semi-Cartan. In view of Proposition 18, there are only three possibilities:
1) $\varphi_\ell(G)$ is contained in a Borel;
2) $\varphi_\ell(G)$ is contained in a nonsplit Cartan;
3) $\varphi_\ell(G)$ is contained in the normalizer N_ℓ of a Cartan C_ℓ and is not contained in C_ℓ.

Case 2) is imposisible, cf. §5.2. So is case 3): indeed, the composition $G \to \varphi_\ell(G) \to N_\ell/C_\ell = \{\pm 1\}$ would give an *unramified* quadratic extension – cf. Lemma **??**. Thus only case 1) remains, which completes the proof of (i).

Proof of (ii): Suppose that $\varphi_\ell(G)$ is contained in a Borel. First of all we have:

LEMMA 11. *The curve E either has ordinary good reduction at ℓ or multiplicative bad reduction at ℓ.*

PROOF. If not, E would have supersingular good reduction and $\varphi_\ell(G)$ would contain a nonsplit Cartan, c.f. Proposition 13; but a Borel subgroup does not contain a nonsplit Cartan. □

Now let L_1 be a G-stable line in $E[\ell]$. The action of G on L_1 and $L_2 = E[\ell]/L_1$ is given by characters

$$\chi_1,\ \chi_2 : G \to \mathbb{F}_\ell^\times,$$

and φ_ℓ can be represented as $\begin{bmatrix} \chi_1 & * \\ 0 & \chi_2 \end{bmatrix}$. It remains to determine χ_1 and χ_2.

LEMMA 12. *The characters χ_1 and χ_2 are unramified away from ℓ. One of the two is unramified at ℓ.*

PROOF. If $p \neq \ell$ and $p \notin S_E$, the representation φ_ℓ is unramified at p, hence so are χ_1 and χ_2. If $p \neq \ell$ and $p \in S_E$, one checks easily using Tate curves that the inertia group of $\varphi_\ell(G)$ at p is either trivial or has order ℓ; either way, the image under χ_1 and χ_2 is trivial. On the other hand, Lemma 11 shows that at ℓ one has either ordinary good reduction or multiplicative bad reduction. According to the corollaries to Propositions 12 and 14, it follows that one of the two characters χ_1, χ_2 is unramified at ℓ. □

proof of (ii): This is now immediate. Indeed, $\mathbb{Q}$ admits no unramified extension of degree greater than 1, and thus every unramified character of G is trivial. We thus have either $\chi_1 = 1$ or $\chi_2 = 1$. As the product $\chi_1\chi_2$ is the mod ℓ cyclotomic character χ, we see that we have

$$\chi_1 = 1, \chi_2 = \chi \text{ or } \chi_1 = \chi, \chi_2 = 1,$$

or equivalently

$$L_1 \cong \mathbb{Z}/\ell\mathbb{Z},\ L_2 \cong \mu_\ell \text{ or } L_1 \cong \mu_\ell,\ L_2 \cong \mathbb{Z}/\ell\mathbb{Z}.$$

REMARK 19. *In the first case, E has a rational point of order ℓ; in the second case, the curve $E' = E/L_1$ has a rational point of order ℓ; we note that E' is linked to E by an isogeny of degree ℓ.*

proof of (iii): We maintain the above notation. Let $p \notin S_E$, $p \neq \ell$, and let $\pi_p \in \varphi_\ell(G)$ be the Frobenius element (well-defined up to conjugacy). We have

$$t_p = \operatorname{Tr} \pi_p \equiv \alpha'_p + \alpha''_p \pmod{\ell},$$

where α'_p (resp. α''_p) denotes the eigenvalue of α_p on the subspace L_1 (resp. the quotient L_2) of $E[\ell]$. Since $L_1 \oplus L_2$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \oplus \mu_\ell$, we have $\{\alpha'_p, \alpha''_p\} = \{1, p\}$, whence

$$t_p \equiv 1 + p \mod \ell \text{ for all} p \notin S_E, p \neq \ell, \tag{6}$$

which shows (iii) for $p \neq \ell$. (Conversely, if (6) holds for almost every p – or even for a set of p of density 1 – then the semisimplification of $E[\ell]$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z} \oplus \mu_\ell$: cf. [**MG**, IV-6, Exercise].)

It remains to show that when $\ell \notin S_E$, the above formula is still valid when $p = \ell$, or in other words that $t_\ell \equiv 1 \pmod{\ell}$. We distinguish two cases:

(iii$_1$) $\ell = 2$.

According to Lemma 11, the elliptic curve $\tilde{E}(2)$ obtained from E by reduction modulo 2 has ordinary reduction; it thus has exactly one point of order 2; this point is rational over $\mathbb{F}_2$. Thus $\#\tilde{E}(2)(\mathbb{F}_2)$ is *even*, which shows that

$$A_2 = 1 + 2 - t_2 \equiv 0 \pmod 2, \text{ i.e., } t_2 \equiv 1 \pmod 2.$$

(iii$_2$) $\ell \geq 3$.

Suppose first that $L_1 \cong \mathbb{Z}/\ell\mathbb{Z}$, i.e., E has a rational point of order ℓ. By reduction modulo ℓ this point gives an element of order 1 or ℓ of $\tilde{E}(l)$. The first case is in fact impossible: we saw in §1.11 that the inertia group at ℓ acts on the kernel of reduction modulo ℓ be means of the fundamental character of level 1, and this character is nontrivial for $\ell \geq 3$ since its image is $\mathbb{F}_\ell^\times$. Thus $\tilde{E}(\ell)(\mathbb{F}_\ell)$ has a point of order ℓ, whence:

$$A_l = 1 + \ell - t_\ell \equiv 0 \pmod \ell, \text{ i.e., } t_\ell \equiv 1 \pmod \ell.$$

Now suppose that $L_2 \cong \mathbb{Z}/\ell\mathbb{Z}$. We use the curve $E' = E/L_1$ instead; since t_p is unchanged under isogeny, this gives the desired result.

REMARK 20. *The argument used above to treat the case $p = \ell$ can also be used in the case $p \neq \ell$: a point of order ℓ of E gives by reduction modulo p a point of order ℓ of $\tilde{E}(p)$, which shows that $A_p = 1 + p - t_p$ is divisible by ℓ.*

Let us now give some applications of Proposition 23.

COROLLARY 15. *Let p be the smallest prime number at which E has good reduction. We have $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ for all $\ell > (\sqrt{p} + 1)^2$.*

PROOF. Arguing by contradiction, we suppose that $\ell > (\sqrt{p} + 1)^2$ and that $\varphi_\ell(G) \neq \operatorname{Aut} E[\ell]$. Since $p \geq 2$, we have $\ell \geq 1 + 2 + 2\sqrt{2} \geq > 5$, and Proposition 23 shows that the integer $A_p = 1 + p - t_p$ is divisible by ℓ. We thus have $A_p \geq \ell > 1 + p + 2\sqrt{p}$, so $t_p < -2\sqrt{p}$, contradicting the "Riemann hypothesis" for $\tilde{E}(p)$. □

(One obtains in this way an *effective* upper bound on the primes ℓ for which $\varphi_\ell(G) \neq \operatorname{Aut} E[\ell]$.)

COROLLARY 16. *We have $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ if $\ell = 11$ or 17.*

PROOF. If not, one of the curves E and $E' = E/L_1$ would have a rational point of orde rℓ, which is known to be impossible for $\ell = 11$ and $\ell = 17$, cf. [**2**], [**20**]. □

Of course, after Mazur's work done a few years later, we know that Corollary **??** applies for all $\ell > 7$. – PLC

5.5. Semistable curves: numerical examples. The examples of §5.5 and §5.7 are taken from a list of elliptic curves of small conductor which Swinnerton-Dyer generously gave to me.

5.5.1. Consider again the curve

$$y^2 + y = x^3 - x^2$$

of conductor $N = 11$ (cf. §5.2). We have $\Delta = -11$, $j = -2^{12}/11$, thus

$$v_{11}(j) = -v_{11}(\Delta) = -1,$$

which shows that condition b) of Proposition 23 is satisfied for all ℓ. It follows that $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ provided that for some $p \neq 11$, $A_p = 1 + p - t_p$ is not divisible by ℓ. Since $A_2 = 5$, this holds *for all* $\ell \neq 5$. The case $\ell = 5$ makes for an exception: the point $(0, 0)$ has order 5, and the group $\varphi_5(G)$ is a "semi-Borel subgroup", representable by matrices of the form $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$.

The curve 5.5.1 corresponds to the modular group $\Gamma_1(11)$. It is linked via a 5-isogeny (made explicit by Vélu [**35**]) to the curve

5.5.2. Consider the curve

$$y^2 + y = x^3 - x^2 - 10x - 20 \ (\Delta = -11^5,\ j = -2^{12}31^3/11^5,$$

which corresponds to the group $\Gamma_0(11)$, c.f. Shimura [**31**]. For this latter curve we have $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ for all $\ell \neq 5$, and $\varphi_5(G)$ is a split semi-Cartan $\begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}$.

5.5.3. Consider the curve

$$y^2 + xy + y = x^3 - x; N = 2 \cdot 7; \Delta = -2^2 7;\ j = \frac{-5^6}{2^2 7}.$$

We have $A_3 = 6$, hence $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ for all $\ell \neq 2, 3$. The cases $\ell = 2$ and $\ell = 3$ give exceptions: the groups $\varphi_2(G)$ and $\varphi_3(G)$ are semi-Borel subgroups $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$.

5.5.4. Consider the curve

$$y^2 + xy + y = x^3 - x^3 - 3x + 3;\ N = 2 \cdot 13;\ \Delta = -2^7 13;\ j = \frac{-3^3 43^2}{2^7 13}.$$

We have $A_3 = 7$, hence $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ for all $\ell \neq 7$. The case $\ell = 7$ gives an exception: $(1, 0)$ is a point of order 7; the group $\varphi_7(G)$ is a semi-Borel.

5.5.5. Consider the curve

$$y^2 + xy + y = x^3 + x^2 - 4x + 5;\ N = 2 \cdot 3 \cdot 7;\ \Delta = -2^8 3^2 7;\ j = \frac{-193^2}{2^8 3^2 7}.$$

We have $A_5 = 8$, hence $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ for all $\ell \neq 2$. The case $\ell = 2$ gives an exception: $(-1, 3)$ is a point of order 8; the group $\varphi_2(G)$ is representable by $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.

5.5.6. Consider the curve

$$y^2 + y = x^3 - x;\ N = 37;\ \Delta = 37;\ j = \frac{2^{12}3^3}{37}.$$

We have $A_2 = 5$ and $A_3 = 7$, hence $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ for all ℓ. (Note that here the point $(0, 0)$ has *infinite order*; the same holds in the following examples.)

5.5.7. Consider the curve

$$y^2 + y = x^3 + x^2;\ N = 43; \Delta = -43;\ j = \frac{-2^{12}}{43}.$$

We have $A_2 = 5$ and $A_3 = 6$, hence $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ for all ℓ.

5.5.8. Consider the curve

$$y^2 + xy + y = x^3 - x^2;\ N = 53; \Delta = 53; j = \frac{-3^3 5^3}{53}.$$

We have $A_2 = 4$ and $A_3 = 7$, hence $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ for all ℓ.

In the last three examples, we have $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ for all $\ell \in P$. One can ask (the question was posed to me by Tate) if we have more generally that $\varphi_n(G) = \operatorname{Aut} E[n]$ for all $n \geq 1$, or equivalently, if the homomorphism

$$\varphi_\infty : G \to \operatorname{Aut} E[\text{tors}] \cong \prod_{\ell \in P} \mathrm{GL}_2\, \mathbb{Z}_\ell$$

is *surjective*. The answer is negative.

PROPOSITION 24. *For every elliptic curve E over $\mathbb{Q}$, the image of*

$$\varphi_\infty : G \to \operatorname{Aut} E[\text{tors}]$$

is contained in an index 2 subgroup of $\operatorname{Aut} E[\text{tors}]$.

PROOF. For $a \in \operatorname{Aut} E[\text{tors}]$, denote by a_n the image of a in $\operatorname{Aut} E[n]$; for $n = 2$, we have $\operatorname{Aut} E[2] \cong S_3$, and the *signature* $\epsilon(a_2)$ of a_2 is defined. We saw in §5.3 that, for every $s \in G$, we have

$$\epsilon(\varphi_2(s)) = \chi_d(s),$$

where $\chi_d : G \to \{\pm 1\}$ is the character of G defined by the extension $\mathbb{Q}(\sqrt{\Delta})$. Since every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension, one can find an integer m (e.g. $4|\Delta|$) such that χ_Δ is the composition of the canonical homomorphism

$$G \to \operatorname{Aut}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^\times$$

with the Kronecker symbol $a \in (\mathbb{Z}/m\mathbb{Z})^\times \mapsto \left(\frac{\Delta}{a}\right)$. The above formula can thus be rewritten in the form

$$\epsilon(\varphi_2(s)) = \left(\frac{\Delta}{\det \varphi_m(s)}\right) \text{ for all } s \in G.$$

This shows that $\varphi_\infty(G)$ is contained in the subgroup H_Δ of $\operatorname{Aut} E[\text{tors}]$ consisting of elements a such that

$$\epsilon(a_2) = \left(\frac{\Delta}{\det a_m}\right).$$

It is clear that H_Δ is an open subgroup of index 2 in $\operatorname{Aut} E[\text{tors}]$, qed. □

(When E is one of the curves 5.5.5, 5.5.6, 5.5.7, one can show that $\varphi_\infty(G) = H_\Delta$. In particular, the homomorphisms $\rho_\ell : G \to \mathrm{GL}\, T_\ell$ are surjective for all ℓ.)

5.6. Nonsemistable curves: the groups Φ_p.

When E is not semistable at a prime number p, we need to introduce a certain nontrivial finite group Φ_p which measures the failure of semistability at p; this group plays an essential role in the representations

$$\varphi_\ell : G \to \operatorname{Aut} E[\ell], \text{ for } \ell \neq p.$$

We define it differently according to whether j is, or is not, integral at p.

a) Definition of Φ_p when j is integral at p

Then there is *potentially good reduction* at p, and we can apply results of Serre-Tate [**30**, §2]. We denote by I_p the inertia subgroup of G at p (well-defined up to conjugagy). According to [**30**], the action of I_p on the $E[n]$ for $p \nmid n$ acts through a certain finite quotient Φ_p:

$$I_p \to \Phi_p \to \operatorname{Aut} E[n],$$

and $\Phi_p \to \operatorname{Aut} E[n]$ is injective if $n \geq 3$. If $\mathbb{Q}_p^{\mathrm{unr}}$ is the maximal unramified extension of $\mathbb{Q}_p$, one can also interpret Φ as $\operatorname{Aut}(L/\mathbb{Q}_p^{\mathrm{unr}})$, where L is the smallest extension of $\mathbb{Q}_p^{\mathrm{unr}}$ over which E acquires good reduction [**30**, p. 498, cor. 3]. Moreover [**30**, p. 497, proof of th. 2], Φ_p is isomorphic to a subgroup of the automorphism group of the elliptic curve $\tilde{E}_{/\overline{\mathbb{F}_p}}$ obtained from $E_{/L}$ by reduction. In view of the known structure of automorphism groups of elliptic curves, we are led to consider the following three cases:

a_1) $p \neq 2, 3$. The group Φ_p is then cyclic of order 2, 3, 4 or 6. More precisely, one checks on the Néron model [**16**, p. 124-125] that:

$$\#\Phi_p = 2 \iff E \text{ is of type } c_4 \iff v_p(\Delta) \equiv 6 \pmod{12},$$
$$\#\Phi_p = 3 \iff E \text{ is of type } c_3 \text{ or } c_6 \iff v_p(\Delta) \equiv 4, 8 \pmod{12},$$
$$\#\Phi_p = 4 \iff E \text{ is of type } c_2 \text{ or } c_7 \iff v_p(\Delta) \equiv 3, 9 \pmod{12},$$
$$\#\Phi_p = 6 \iff E \text{ is of type } c_1 \text{ or } c_8 \iff v_p(\Delta) \equiv 2, 10 \pmod{12}.$$

The field L is obtained by adjoining to $\mathbb{Q}_p^{\mathrm{unr}}$ the 12th roots of Δ.

a_2) $p = 3$. The group Φ_p is cyclic of order $2, 3, 4, 6$ or is a non-abelian semi-direct product of a cyclic group of order 4 by a normal subgroup of order 3.

a_3) $p = 2$. The group Φ_p is isomorphic to a subgroup of $\mathrm{SL}_2(\mathbb{F}_3)$. Its order is $2, 3, 4, 6, 8$ or 24.

In the latter two cases, knowing $v_p(\Delta)$ is not sufficient to determine $\#\Phi_p$. One can merely say that one has

$$\#\Phi_p v_p(\Delta) \equiv 0 \pmod{12},$$

since the valuation of Δ becomes divisible by 12 in the field L.

b) Definition of Φ_p when j is not integral at p

Over $\mathbb{Q}_p$, the curve E is obtained from the Tate curve with the same j-invariant by *twisting* via the quadratic extension $L = \mathbb{Q}_p(\sqrt{-c_6})$; under our assumption that E is not semistable, this extension is ramified at p. Its Galois group is the group Φ_p that we're interested in; as above, we view it as a quotient of the inertia group I_p; we have $\Phi_p \cong \{\pm 1\}$. If $s \in I_p$ has image $\epsilon(s) = \pm 1 \in \Phi_p$, the automorphism $\varphi_\ell(s)$ of $E[\ell]$ ($\ell \neq p$) has both eigenvalues equal to $\epsilon(s)$: it is the product of $\epsilon(s)$ and a unipotent element.

Application to the case in which $\varphi_\ell(G)$ is contained in a Borel subgroup

Let ℓ be a prime number such that $\varphi_\ell(G)$ is contained in a Borel subgroup, and let $\chi_1, \chi_2 : G \to \mathbb{F}_\ell^\times$ be the corresponding characters. By class field theory, one can identify χ_1 and χ_2 with *Dirichlet characters*

$$\chi_1 : (\mathbb{Z}/f_1\mathbb{Z})^\times \to \mathbb{F}_\ell^\times \text{ and } \chi_2 : (\mathbb{Z}/f_2\mathbb{Z})^\times \to \mathbb{F}_\ell^\times,$$

where f_1 and f_2 are the conductors of χ_1 and χ_2. Let us write f_1 in the form $\prod_{p\in P} p^{n_1(p)}$. The group $(\mathbb{Z}/f_1\mathbb{Z})^\times$ decomposes as a product of $(\mathbb{Z}/p^{n_1(p)}\mathbb{Z})^\times$. The restriction of χ_1 to the pth factor $(\mathbb{Z}/p^{n_1(p)}\mathbb{Z})^\times$ will be called the *p-component of* χ_1, and denoted $\chi_{1,p}$: knowing $\chi_{1,p}$ is equivalent to knowing the restriction of χ_1 to I_p. In the same way we define the p-component $\chi_{2,p}$ of χ_2. Let S'_E denote the subset of S_E consisting of the primes p at which E is not semistable. We then have:

PROPOSITION 25. *(a) The characters χ_1 and χ_2 are unramified away from $\{\ell\} \cup S'_E$. For all $p \notin \{\ell\} \cup S_E$, we have*

$$t_p \equiv \chi_1(p) \pmod{\ell},$$

$$p \equiv \chi_1(p)\chi_2(p) \pmod{\ell}.$$

(b) Suppose $\ell \geq 5$. Let $p \in S'_E \setminus \{\ell\}$. Then the image of $\chi_{1,p}$ (resp. $\chi_{2,p}$) in $\mathbb{F}_\ell^\times$ is isomorphic to the group Φ_p; this is a cyclic group of order 2, 3, 4 or 6.
(c) Suppose $\ell \notin S_E$. Then one of the characters χ_1 and χ_2 is unramified at ℓ. If we denote this character by α_ℓ, we have

$$t_p \equiv \alpha_\ell(p) + p\alpha_\ell(p)^{-1} \pmod{\ell} \text{ for all } p \notin S_E.$$

PROOF. The assertion (a) is shown by arguments already used several times above. In (b) the hypothesis $\ell \leq 5$ serves to insure that an automorphism of an elliptic curve which fixes a point of order ℓ must be trivial; in view of the preceding, this implies that $\chi_{1,p}$ and $\chi_{2,p}$ map Φ_p *injectively* into $\mathbb{F}_\ell^\times$. The group Φ_p is therefore cyclic, and of order 2, 3, 4 or 6. The first assertion of (c) is shown by observing that E has either good reduction of height 1 at ℓ or multiplicative bad redeuction, and applying propositions 12 and 14 of §1. The congruence

$$t_p \equiv \alpha_\ell(p) + p\alpha_\ell(p)^{-1} \pmod{\ell} \text{ for } p \notin S_E$$

follows from (a) since $p \neq \ell$. The remaining case is $p = \ell \notin S_E$, in which we must prove that $t_\ell \equiv \alpha_\ell(\ell) \pmod{\ell}$. First notice that the reduction $\tilde{E}$ of E at ℓ has height 1, hence contains a unique subgroup of order ℓ. Moreover, one knows that the Frobenius endomorphism π_ℓ of $\tilde{E}$ acts on the subgroup in question via multiplication by t_ℓ. The desired formula follows easily from this, via an arugment analogous to the one used in §5.4; we leave the details to the reader. □

COROLLARY 17. *Suppose $\ell \notin S_E$ and $\ell \geq 5$. Then the Φ_p are cyclic. With the notation of (c), the order of α_ℓ is the least common multiple of the orders of the Φ_p; in particular, we have $\alpha_\ell^{12} = 1$.*

PROOF. The cyclicity of the Φ_p follows from part (b). On the other hand, the order of the character α_ℓ is the least common multiple of the orders of its p-components, i.e., of the orders of the Φ_p; since these are divisors of 12, we have $\alpha_\ell^{12} = 1$. □

COROLLARY 18. *Let $\ell \geq 5$ be a prime of good reduction for E such that $\varphi_\ell(G)$ is contained in a Borel subgroup. I have made the hypotheses more explicit here. – PLC Let p be the least prime number at which E has good reduction. Then:*

$$\ell \leq (\sqrt{p}+1)^8.$$

PROOF. According to (c), we have

$$t_p \equiv z + pz^{-1} \pmod{\ell}$$

where z is a 12th root of unity in $\mathbb{F}_\ell$. Let d be the order of z, let $S_d(X)$ be the dth cyclotomic polynomial, and let $T_p(X) = X^2 - T_p X + p$. The above congruence shows that S_d and T_p have a common root modulo ℓ. Their *resultant* R is thus an integer divisible by ℓ. We can decompose R in the form

$$R = \prod (x-\zeta)(x'-\zeta')$$

where x and x' are the two roots of T_p (the eigenvalues of π_p) and ζ runs through the set of primitive dth roots of unity. We have $|x| = |x'| = \sqrt{p}$ and $|\zeta| = 1$, whence:

$$0 < |R| \leq (\sqrt{p}+1)^{2n}, \text{ where } n = \deg S_d = \varphi(d).$$

Since $d \mid 12$ we have $\varphi(D) \leq 4$ and thus $|R| \leq (\sqrt{p}+1)^8$. Since $\ell \mid R$, we have the same inequality for ℓ. □

We give an application of Corollary 18:

PROPOSITION 26. *Suppose that $j \notin \mathbb{Z}$; let $p_0 \in P$ be such that $v_{p_0}(j) < 0$. Let p be the least prime at which E has good reduction. If $\ell \notin S_E$, $\ell \nmid v_{p_0}(j)$ and $\ell > (\sqrt{p}+1)^8$, we have $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$.*

(Here again we get an *effective* upper bound on the ℓ for which $\varphi_\ell(G) \subsetneq \operatorname{Aut} E[\ell]$.)

PROOF. Evidently we have $\ell \geq 5$. It follows that $\ell \nmid 2v_{p_0}(j)$. So there is an extension of $\mathbb{Q}_{p_0}$ of degree at most 2 over which E becomes a Tate curve; the valuation of j in this extension is $v_{p_0}(j)$ or $2v_{p_0}(j)$, hence is not divisible by ℓ. According to [**MG**, IV-20], the inertia group of $\varphi_\ell(G)$ at p_0 contains an element of order ℓ. If we had $\varphi_\ell(G) \subsetneq \operatorname{Aut} E[\ell]$, the group $\varphi_\ell(G)$ would be contained in a Borel subgroup, which is impossible because of Corollary 18 above. □

5.7. Curves with nonintegral j: numerical examples.

5.7.1. Consider the curve

$$y^2 = x^3 + x^2 - x;\ N = 2^2 5;\ \Delta = 2^4 5;\ j = 2^{14}/5.$$

There is multiplicative bad reduction at 5 and $v_5(\Delta) = 1$. The group $\varphi_\ell(G)$ thus contains an element of order ℓ and, if it is distinct from $\operatorname{Aut} E[\ell]$, is contained in a Borel subgroup. On the other hand, there is bad reduction at 2, and one can check[4] that the corresponding group Φ_2 is cyclic of order 3. One thus concludes (cf. §5.6) that if $\varphi_\ell(G)$ is contained in a Borel subgroup, and if $\ell \geq 5$, the corresponding characters $\chi_1, \chi_2 : G \to \mathbb{F}_\ell^\times$ have a 2-component whose image in $\mathbb{F}_\ell^\times$ has order 3; but this is impossible, since no quotient of $(\mathbb{Z}/2^n\mathbb{Z})^\times$ has order 3. This contradiction *shows that* $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ for $\ell \neq 2, 3$. The cases $\ell = 2$ and $\ell = 3$ give exceptions: $(0,0)$ is a point of order 2 and $(1,1)$ is a point of order 3.

[4]This can be seen, for example, by making the change of variables $x = \pi^2 X + 1$, $y = \pi^3 Y + 1$, where $\pi = \sqrt{32}$; one obtains the equation $Y^2 + Y = X^3 + \pi^4 X^2 + \pi^2 X$, which makes the good reduction at the ideal (π) clear.

5.7.2. Consider the curve

$$y^2 = x^3 - x^2 + x;\ N = 2^3 3;\ \Delta = -2^4 3;\ j = 2^{11}/3.$$

The fact that $v_2(\Delta) = 4$ implies that the order of Φ_2 is divisible by 3. The same arugment as in 5.7.1 thus shows that $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ for $\ell \geq 5$. This formula remains valid for $\ell = 3$: it suffices to show that $\varphi_3(G)$ contains an element not contained in any Borel subgroup, and one can take for this element the Frobenius π_5: one has indeed

$$A_5 = 8,\ \text{whence}\ \operatorname{Tr}(\pi_5)^2 - 4\det(\pi_5) = 4 - 20 = -16,$$

and -16 is not a square modulo 3. The case $\ell = 2$ gives an exception: $(0, 0)$ is a point of order 2.

[Compare with [**MG**, IV-21], where the same curve is treated by a different method, based on results of Ogg [**18**].]

5.7.3. Consider the curve

$$y^2 + xy = x^3 - x^2 - 5;\ N = -3^2 5;\ \Delta = -3^7 5;\ j = \frac{-1}{3 \cdot 5}.$$

The multiplicative bad reduction at 5 shows that, if $\varphi_\ell(G)$ is distinct from $\operatorname{Aut} E[\ell]$ then it is contained in a Borel subgroup. Let us suppose that this is the case and that $\ell \geq 5$; we denote by $\chi_1, \chi_2 : G \to \mathbb{F}_\ell^\times$ the corresponding characters. As Φ_3 has order 2, we see that one of the characters χ_1 and χ_2 is unramified away from 3 and that its 3-component has order 2; it is then the character $x \mapsto \left(\frac{x}{3}\right)$, and we have

$$t_p \equiv \left(\frac{p}{3}\right) + p\left(\frac{p}{3}\right) \pmod{\ell} \text{ for all } p \neq 3, 5.$$

But $A_2 = 2$, $t_2 = 1$ and $\left(\frac{2}{3}\right) = -1$; thus we have $1 \equiv -3 \pmod{\ell}$, which is impossible. This formula remains true when $\ell = 3$; this can be seen as in 5.7.2., by noticing that $\operatorname{Tr}(\pi_2)^2 - 4\det(\pi_2) = -7$ is not a square modulo 3. The case $\ell = 2$ gives an exception: $(2, -1)$ is a point of order 2.[5]

5.7.4. Consider the curve

$$y^2 + xy + y = x^3 + x^3 - 3x + 1; N = 2 \cdot 5^2;\ \Delta = -2^5 \cdot 5^2;\ j = \frac{-5 \cdot 29^3}{2^5}.$$

The fact that $v_5(\Delta) = 2$ shows that Φ_5 is cyclic of order 6. Thus there is no character of G whose 5-component has an image of order 6 (or 3). This suffices to show, as above, that for $\ell \neq 3, 5$, $\varphi_\ell(G)$ cannot be contained in a Borel subgroup. On the other hand, the multiplicative bad reduction at 2, together with the fact that $v_2(\Delta) = 5$, shows that for all $\ell \neq 5$, $\varphi_\ell(G)$ contains an element of order ℓ. We then conclude that $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ for $\ell \neq 3, 5$. The cases $\ell = 3$ and $\ell = 5$ give exceptions: $(1, 0)$ is a point of order 5, and $E[3]$ contains a G-stable subgroup of order 3, formed by the point at ∞ and the two points with y-coordinate zero; for all $p \neq 2, 5$ we have

$$t_p = 1 + p \pmod{5} \text{ and } t_p \equiv \left(\frac{p}{5}\right) + p\left(\frac{p}{5}\right) \pmod{3}.$$

[5]Another way of treating this curve would consist of "twisting it" by the quadratic extension $\mathbb{Q}(\sqrt{-3})/\mathbb{Q}$; it gets transformed in this way to the curve $y^2 + xy + y = x^3 + x^2$ ($N = 3 \cdot 5$; $\Delta = -3 \cdot 5$), which has the advantage of being *semistable*.

5.8. Curves with integral j.

This is the most difficult case; we no longer have at our disposal the unipotent elements furnished by Tate's theory.

We are led to examine the fuollowing possibilities:
(a) $\varphi_\ell(G)$ is contained in a Borel subgroup.

This case can be treated by the methods of §5.6; we get an *effective* bound on ℓ.
(b) $\varphi_\ell(G)$ is contained in a Cartan subgroup.

This subgroup is necessarily split (if $\ell \geq 3$), cf. §5.2; it is thus contained in a Borel subgroup, and we are reduced to the preceding case.
(c) $\varphi_\ell(G)$ is contained in the normalizer N_ℓ of a Cartan subgroup C_ℓ and is not contained in C_ℓ.

This case is treated as follows. For simplicity we suppose $\ell \geq 5$. Denote by ϵ the order 2 character of G defined by the composition

$$G \to \varphi_\ell(G) \to N_\ell/C_\ell \cong \{\pm 1\}.$$

We have the following information about ϵ:
(c_1) ϵ is unramified outside of $S_E \cup \{\ell\}$. This is clear.
(c_2) If $\ell \notin S_E$, ϵ is unramified at ℓ and $\epsilon(\ell) = 1$ or $\epsilon(\ell) = 01$ according to whether E has ordinary or supersingular reduction at ℓ. This is seen via the structure of the decomposition group D_ℓ of $\varphi_\ell(G)$ relative to ℓ, as given in §1.11. When the reduction is ordinary, the inertia subgroup of D_ℓ is a semi-Cartan subgroup or a semi-Borel subgroup; since it is contained in N_ℓ, only the first case is possible, and it implies that the group in question is one of the semi-Cartan subgroups of C_ℓ (it is here that the hypothesis $\ell \geq 5$ intervenes, cf. §2.2, Proposition 15); the group D_ℓ is then contained in C_ℓ, which shows at the same time that ϵ is unramified at ℓ and that $\epsilon(\ell) = 1$. When the reduction is supersingular, the inertia group of D_ℓ is a nonsplit Cartan subgroup, hence equal to C_ℓ, and D_ℓ is equal to N_ℓ (§1.11, Proposition 13); this shows that ϵ is unramified and that $\epsilon(\ell) = 1$.
(c_3) IF E has multiplicative bad reduction at p, then ϵ is unramified at p. This can be checked using Tate curves.
(c_4) Suppose that E is not semistable at p and that $p \neq \ell$. If the corresponding group Φ_p (§5.6) has order 2, 3 or 6, then ϵ is unramified at p. Indeed, we must see that the image of Φ_p in $\varphi_\ell(G)$ is contained in C_ℓ; but an order 2 element of Φ_p has image -1 in $\operatorname{Aut} E[\ell]$, hence belongs to C_ℓ; on the other hands, it is clear that an order 3 element of Φ_p has trivial image in N_ℓ/C_ℓ.
(c_5) If $p \notin S_E$ and $\epsilon(p) = -1$, we have $t_p \equiv 0 \pmod{\ell}$. If $p \neq \ell$, this amounts to saying that the trace of the Frobenius element π_p of $\varphi_\ell(G)$ is zero, which is clear since π_p belongs to $N_\ell \setminus C_\ell$. If $p = \ell$, the hypothesis $\epsilon(\ell) = -1$ implies that E has supersingular reduction at ℓ (cf. (c_2) above) and one knows that this is equivalent to $t_\ell \equiv 0 \pmod{\ell}$.

The properties (c_1) through (c_4) allow us to make a list of the possible characters ϵ. For each of them, we consider the primes p such that $\epsilon(p) = -1$ and we search for such a p with $t_p \neq 0$. If we find one, the condition $t_p \equiv 0 \pmod{\ell}$ gives an upper bound on ℓ. If we cannot, the curve E has complex multiplication by the quadratic field corresponding to ϵ.

5.9. Curves with integral j: numerical examples.

5.9.1. Consider the curve

$$y^2 = x^3 - 2x^2 - x;\ N = 2^7;\ \Delta = 2^7;\ j = 2^5 \cdot 7^3.$$

The fact that $v_2(\Delta) = 7$ shows that the order of Φ_2 is divisible by 12, hence equal to 12 or 24; but $\mathrm{SL}_2(\mathbb{F}_3)$ has no subgroup of order 12; the first case is thus impossible, which shows that Φ_2 is isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$. The image of Φ_2 in $\mathrm{Aut}\, E[\ell]$, $\ell \geq 3$, is a group of order 24 which acts irreducibly; moreover, the group is not abelian and does not contain any abelian index 2 subgroup. We deduce that $\varphi_\ell(G)$, for $\ell \geq 3$, cannot be contained in a Borel subgroup or the normalizer of a Cartan subgroup; since moreover it contains either a Cartan subgroup or a semi-Cartan subgroup (coming from the inertia at ℓ), Proposition 18 shows that $\varphi_\ell(G) = \mathrm{Aut}\, E[\ell]$ for $\ell \geq 3$ (For $\ell = 5$, we must moreover check that $\varphi_\ell(G)$ contains an element s such that $\mathrm{Tr}(s)^2/\det(s) = 3$, which is done by taking $s = \pi_3$; we have $A_3 = 6$, whence $\mathrm{Tr}(\pi_3)^2/\det(\pi_3) = 2^2/3 \equiv 3 \pmod 5$. The case $\ell = 2$ gives an exception: $(0, 0)$ is a point of order 2.

5.9.2. Consider the curve[6]

$$y^2 = x^3 + 6x - 2;\ N = 2^6 \cdot 3^3;\ \Delta = -2^6 \cdot 3^5;\ j = 2^9 \cdot 3.$$

There is bad reduction at 2 and 3. The fact that $v_3(\Delta) = 5$ shows that Φ_3 has order 12. The image of Φ_3 in $\mathrm{Aut}\, E[2]$ is $\Phi_3/\{\pm 1\}$, which has order 6; thus certainly $\varphi_2(G) = \mathrm{Aut}\, E[2]$. For $\ell = 3$, the fact that Δ is not a cube shows that $\varphi_3(G)$ contains an element of order 3 (cf. §5.3); on the other hand, we have $A_5 = 4$, whence $\mathrm{Tr}(\pi_5)^2 - 4\det(\pi_5) = -16$ which is not a square modulo 3, and $\varphi_3(G)$ is not contained in a Borel subgroup; these two pieces of information imply that $\varphi_3(G) = \mathrm{Aut}\, E[3]$. Now suppose that $\ell \geq 7$; since $\varphi_\ell(G)$ contains Φ_3, $\varphi_\ell(G)$ cannot be contained in either a Borel or a Cartan; on the other hand, it contains a Cartan or a split semi-Cartan subgroup (coming from inertia at ℓ); Proposition 18 shows then that $\varphi_\ell(G)$ is either equal to $\mathrm{Aut}\, E[\ell]$ or contained in the normalizer N_ℓ of a Cartan subgroup C_ℓ. We will show that the latter case is impossible: that case gives us an order 2 character

$$\epsilon : G \to \varphi_\ell(G) \to N_\ell/C_\ell \cong \{\pm 1\}$$

of G, and we would have (cf. §5.8):

$$(*) t_p \equiv 0 \pmod \ell \text{ if } \epsilon(p) = -1 \text{ and } p \neq 2, 3.$$

The character ϵ is ramified at 3 (using the structure of Φ_3 and is unramified outside of $\{2, 3\}$. Let us take $p = 17$. Since $p \equiv 1 \pmod 8$, the 2-component of ϵ takes the value 1 at p; since $p \equiv -1 \pmod 3$, the 3-component takes the value -1 at p. We thus have $\epsilon(p) = -1$, whence $t_{17} \equiv 0 \pmod \ell$. But we find that $A_{17} = 24$, whence $t_{17} = -6$. The congruence above is thus impossible, whence $\varphi_\ell(G) = \mathrm{Aut}\, E[\ell]$. The same argument applies to $\ell = 5$, up to the fact that we must verify the existence in $\varphi_5(G)$ of an element s such that $\mathrm{Tr}(s)^2/\det(s) = 3$; the element π_{17} works. In conclusion, we have $\varphi_\ell(G) = \mathrm{Aut}\, E[\ell]$ for all ℓ.

[6]This curve was pointed out to me by J. Vélu.

5.9.3. Consider the curve

$$y^2 + xy = x^3 - x^2 - 2x - 1;\ N = 7^2;\ \Delta = -7^3;\ j = -3^3 5^3.$$

There is bad reduction at 7 and Φ_7 has order 4. Let us see whether, for $\ell \neq 2, 7$, it is possible for $\varphi_\ell(G)$ to be contained in the normalizer of a Cartan C_ℓ without being contained in C_ℓ. The corresponding character $\epsilon : G \to \{\pm 1\}$ is ramified only at 7; it is thus the Legendre symbol $a \mapsto \frac{a}{7}$. We conclude that if $\left(\frac{p}{7}\right) = -1$ then $t_p \equiv 0 \pmod{\ell}$. The smallest values of p such such that $\left(\frac{p}{7}\right) = -1$ are $3, 5, 13, 17$; one finds each time that $t_p = 0$. This suggests that E has complex multiplication by $\mathbb{Q}(\sqrt{-7})$; indeed, one knows [**5**, p. 295] that $-35^3 = j(\frac{1+\sqrt{-7}}{2})$, so that E has for its ring of endomorphisms (over $\overline{\mathbb{Q}}$) the ring of integers of $\mathbb{Q}(\sqrt{-7})$. We deduce easily that, for $\ell \neq 2, 7$, $\varphi_\ell(G)$ is the normalizer of a Cartan subgroup and that, for $\ell = 2, 7$, $\varphi_\ell(G)$ is contained in a Borel subgroup; in particular, we have $\varphi_\ell(G) \neq \operatorname{Aut} E[\ell]$ for all ℓ.

5.9.4. Consider the curve

$$y^2 + xy = x^3 + x^2 - 2x - 7;\ N = 11^2;\ \Delta = -11^4;\ j = -11^2.$$

(This curve has the remarkable property of having a Galois stable subgroup of order 11, c.f. Vélu [**35**].)

There is bad reduction at 11 and Φ_{11} has order 3. Let $\ell \neq 11$; if $\varphi_\ell(G)$ were contained in a Borel subgroup, the two corresponding characters $\chi_1, \chi_2 : G \to \mathbb{F}_\ell^\times$ would have an 11-component with image of order 3, which is impossible since $11 - 1$ is not divisible by 3; hence $\varphi_\ell(G)$ cannot be contained in a Borel subgroup, hence *a fortiori* not in a split Cartan subgroup. It cannot be contained in a nonsplit Cartan subgroup §5.2. It cannot be contained in the normalizer of a Cartan subgroup C_ℓ, as the corresponding order 2 character would be everywhere unramified (since Φ_{11} has order 3), which is impossible. Finally, for $\ell = 5$, $\varphi_\ell(G)$ contains an element s such that $\operatorname{Tr}(s)^2/\det(s) = 3$, namely π_2 (one checks that $A_2 = 2$, whence $t_2 = 1$ and $t_2^2/2 = 1/2 \equiv 3 \pmod{5}$). This information implies that $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ for $\ell \neq 1$, c.f. §2.7. The case $\ell = 11$ gives an exception, by virtue of the result of Vélu cited above: we have $t_p \equiv p^4 + p^7 \pmod{11}$ for all $p \neq 11$.

5.10. An example over the field $\mathbb{Q}(\sqrt{29})$.

In this section, the base field K is the real quadratic field $\mathbb{Q}(\sqrt{29})$. The ring of integers $\mathcal{O}_K$ is a PID. We have

$$\mathcal{O}_K = \mathbb{Z}[\epsilon],\ \text{where } \epsilon = \frac{5 + \sqrt{29}}{2} \text{ is the fundamental unit.}$$

The norm of ϵ is -1. The group of totally positive units is generated by $\epsilon^2 = 1 + 5\epsilon$.

We take the elliptic curve

$$E : y^2 + xy + \epsilon^2 y = x^3.$$

We have:

$$b_2 = 1,\ b_4 = \epsilon^2,\ b_6 = \epsilon^4,\ b_8 = 0,\ c_4 = 1 - 24\epsilon^2$$

and

$$\Delta = b_4^3 4 - 27 b_6^2 = \epsilon^6 - 27\epsilon^8 = -\epsilon^{10}.$$

The fact that Δ is a unit shows that E has everywhere good reduction.[7]

If v is a finite place of V, as usual we denote by A_v the number of points of the reduction of E at v; we have

$$A_V = 1 + Nv - t_v, \text{ where } t_v = \operatorname{Tr} \pi_v.$$

We will need to know several values A_v:

$$p_v = 2, N_v = 4 \text{ gives } A_v = 6,\ t_v = -1,\ \operatorname{Tr}(\pi_v)^2 - 4 \det \pi_v = -15;$$

$$p_v = 5,\ N_v = 5 \text{ gives } A_v = 9,\ t_v = -3,\ \operatorname{Tr}(\pi_v)^2 - 4 \det \pi_v = -11;$$

$$p_v = 7,\ N_v = 7 \text{ gives} A_v = 6,\ t_v = 2,\ \ tr(\pi_v)^2 - 4 \det \pi_v = -24.$$

We turn to the determination of the $\varphi_\ell(G)$. We begin with some particular cases:

a) $\ell = 2$. We have $\varphi_2(G) = \operatorname{Aut} E[2]$. Indeed, we have seen that $Nv = 5$ yields $t_v = -3 \equiv 1 \pmod 2$, which shows that $\varphi_2(G)$ contains an element of order 3. On the other hand, $\Delta = -\epsilon^{10}$ is not a square in K, and $\varphi_2(G)$ thus contains an element of order 2, cf. §5.3.

b) $\ell = 3$. The point $(0, 0)$ has order 3. On the other hand Δ is not a cube, hence $\varphi_3(G)$ contains an element of order 3 (§5.3); since $\det \varphi_3(G) = \mathbb{F}_3^\times$, we conclude that $\varphi_3(G)$ is a semi-Borel subgroup $\begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix}$. We have $t_v \equiv 1 + N_v \pmod 3$ for all v.

c) $\ell = 29$. The field $\mathbb{Q}(\sqrt{29})$ is contained in the cyclotomic field $\mathbb{Q}(\zeta_{29})$. It follows that $\det \varphi_{29}(G)$ is the set of squares in $\mathbb{F}_{29}^\times$. On the other hand, we saw that

$$N_v = 4 \text{ gives} \operatorname{Tr}(\pi_v)^2 - 4 \det(\pi_v) = -15 \text{ and } \left(\frac{-15}{29}\right) = -1,$$

$$N_v = 7 \text{ gives} \operatorname{Tr}(\pi_v)^2 - 4 \det(\pi_v) = -24 \text{ and } \left(\frac{-24}{29}\right) = 1.$$

Applying Proposition 20, we deduce that $\varphi_{29}(G)$ is the index 2 subgroup of $\operatorname{Aut} E[29]$ consisting of elements of square determinant.

Suppose now that $\ell \geq 5$ and $\ell \neq 29$. The field $\mathbb{Q}(\sqrt{29})$ is linearly disjoint from the cyclotomic field $\mathbb{Q}(\zeta_\ell)$, which shows $\det \varphi_\ell(G) = \mathbb{F}_\ell^\times$. On the other hand:

i) The group $\varphi_\ell(G)$ cannot be contained in a nonsplit Cartan subgroup; this is shown as in the case of $\mathbb{Q}$, using complex conjugation, c.f. §5.2, iv).

ii) The group $\varphi_\ell(G)$ cannot be contained in the normalizer N_ℓ of a Cartan subgrtoup C_ℓ without being contained in C_ℓ. Indeed, the corresponding character $G \to \{\pm 1\}$ would be unramified (§4.2, Lemma 8): but such a character does not exist, since $\mathcal{O}_K$ is principal and contains an element of norm -1, hence its narrow ideal class group is trivial.

iii) Let us see if $\varphi_\ell(G)$ can be contained in a Borel subgroup. Suppose this is the case, and let $\chi_1, \chi_2 : G \to \mathbb{F}_\ell^\times$ be the corresponding quadratic characters. These characters are unramified away from places of v dividing ℓ. Suppose first that there is only one such place, i.e., that $\left(\frac{\ell}{29}\right) = -1$. According to §1.11, E has ordinary reduction at ℓ and one of the characters χ_1, χ_2 is unramified at v, hence everywehre, hence is trivial (see above). We then have

$$t_v \equiv 1 + N_v \pmod \ell \text{ if } p_v \neq \ell.$$

[7]The curve E was shown to me by Tate, who has obatined analogous examples over other quadratic fields, both real and imaginary.

Taking $N_v = 4$, $t_v = -1$, we have $6 \equiv 0 \pmod{\ell}$, which is impossible since $\ell \geq 5$.

Suppose now that there are two places v_1 and v_2 dividing ℓ, i.e., that $\left(\frac{\ell}{29}\right) = 1$. According to §1.11, E has ordinary reduction at v_1 and and one of the characters χ_1 and χ_2 is unramified at v_1 (resp. at v_2). If the same character is unramified at both places, this character is trivial and the same reasoning as above shows that this is impossible. We are left with the case in which, for example, χ_1 is unramified at v_1 and ramified at v_2 (in which case it is the fundamental character of height 1 at v_2, according to §1.11). Such a character only exists if $\ell = 5$. Indeed, let $\mathfrak{p}_2$ denote the prime ideal corresponding to v_2. Class field theory allows us to interpret χ_1 as a homomorphism $(\mathcal{O}_K/\mathfrak{p}_2)^\times \to \mathbb{F}_\ell^\times$, equal to 1 at every totally positive unit; moreover, since χ_1 is the fundamental character, if we identify $\mathcal{O}_K/\mathfrak{p}_2$ with the field $\mathbb{F}_\ell$, the homomorphism $\chi_1 : \mathbb{F}_\ell^\times \to \mathbb{F}_\ell^\times$ obtained in this way is the identity map. Since ϵ^2 generates the group of totally positive units, we see that $\epsilon^2 - 1 = 5\epsilon$ must be contained in $\mathfrak{p}_2$, which holds iff $\ell = 5$.

Finaqlly, if $\ell \neq 29$, the group $\varphi_\ell(G)$ contains either a nonsplit Cartan or a split semi-Cartan, cf. §1.11. Combinging this information with that given in i), ii), iii) above, we say that $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ for all $\ell \geq 7$, $\ell \neq 29$.

We are left with the case $\ell = 5$. With current technology, this case should be a straightforward computation. I encourage someone to give it a try. –PLC We saw that $N_v = 4$ gives an element π_v such that $\operatorname{Tr}(\pi_V) = -1$, $\det(\pi_v) =$, whence $\operatorname{Tr}(\pi_v)^2 - 4\det(\pi_v) = -15$. Since the 5-adic valuation of -15 is 1, we deduce from this (cf. [**32**, Lemma 1]) that the image of π_v in $\operatorname{Aut} E[5]$ is representable by the matrix $\begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$, hence has order 10. In view of what was demonstrated above, we are left with only the following two possibilities:

5_1) We have $\varphi_5(G) = \operatorname{Aut} E[5]$.

5_2) The group $\varphi_5(G)$ is a Borel subgroup $\begin{bmatrix} * & * \\ 0 & * \end{bmatrix}$ and the corresponding characters χ_1 and χ_2 are the fundamental characters relative to the places v_1 and v_2 of K of residue characteristic 5, cf. iii) above. In terms of the t_v, this last property can be translated as follows: for each $v \in \Sigma$, choose a totally positive generator α_v of the prime ideal of $\mathcal{O}_K$ defined by v; then we have

$$t_B \equiv \operatorname{Tr}_{K/\mathbb{Q}}(\alpha_v) \pmod{5}.$$

We will note that this congruence is satisfied when $N_v = 4, 5, 7$, as one sees by taking $\alpha_v = 2, 1+\epsilon$ (or $6-\epsilon$) and $1+2\epsilon$ (or $11-2\epsilon$). This makes one think that it is 5_2) which is correct and not 5_1), or in other words that $\varphi_5(G)$ is a Borel subgroup of $\operatorname{Aut} E[5]$. This is indeed the case. To show it, it's enough to dheck that $E[5]$ contains a Galois stable subgroup of order 5, or what comes to the same (f. [**11**, p. 399]), $j(E)$ can be written in the form $(\tau^2 + 10\tau + 5)^3/\tau$ with $\tau \in K$. And indeed this is the case: take $\tau = \epsilon - 14 = (-1+\epsilon)^3/\epsilon^2$.

In summary, one has $\varphi_\ell(G) = \operatorname{Aut} E[\ell]$ for $\ell \neq 3, 5, 29$.

Shimura's curve

In [**33**, §7.5] (see also [**32**]), Shimura constructs an elliptic curve E_1 over $K = \mathbb{Q}(\sqrt{29})$ which has properties very close to those of our curve E above: it has good reduction everywhere [**3**], and the same number of points as E at places dividing $2, 3, 5, 7, 13$; the traces $t_v(E_1)$ of the Frobenius elements of E_1 satisfy the same

congruences as the $t_v(E)$, that is:

$$t_v(E_1) \equiv 1 + N_v \pmod 3,$$
$$t_v(E_1) \equiv \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_v) \pmod 5.$$

(The second congruence is demonstrated in [**33**, p. 206]; the first follows from the expression of the zeta function of E_1 given by Shimura, combined with formulas of Hecke [**13**, p. 787, p.905].)

The curve E_1 is 5-isogenous to its Galois conjugate E_1^σ, where σ denotes the nontrivial automorphism of K. Such curves are called $\mathbb{Q}$-curves and are now much more widely studied. –PLC The curve E satisfies an analogous property: this can be shown using results of Fricke (*loc. cit.*) and by noticing that we have $\tau\tau^\sigma = 125$ in the above notation.

The arguments used above for E to determine $\varphi_\ell(G)$ apply without change to E_1. In particular the Galois group of $(E_1)_\ell$ is $\mathrm{GL}_2(\mathbb{F}_\ell)$ for $\ell \neq 3, 5, 29$. It would be interesting to see if E_1 is igoenous (or even isomorphic) to E.

6. Products of two elliptic curves

In this §, E and E' denote two elliptic curves over a number field K. The notation $E[n]$, φ_n, ρ_ℓ, T_ℓ, V_ℓ relative to E are defined as in the introduction and in §4. We use for E' the corresponding notation $E'[n]$, φ'_n, ρ'_ℓ, T'_ℓ, V'_ℓ.

The notation relative to K is as in §3, 4. In particular, the letter G denotes the Galois group $\mathrm{Aut}(\overline{K}/K)$.

6.1. Curves without complex multiplication.

If n is a positive integer, the homomorphisms

$$\varphi_n : G \to \mathrm{Aut}\, E[n],\ \ \varphi'_n : G \to \mathrm{Aut}\, E'[n]$$

define a homomorphism

$$\psi_n : G \to \mathrm{Aut}\, E[n] \times \mathrm{Aut}\, E'[n].$$

As $\det \varphi_n = \det \varphi'_n$, the image of ψ_n is contained in the subgroup A_n of $\mathrm{Aut}\, E[n] \times \mathrm{Aut}\, E[n]$ consisting of pairs (s, s') such that $\det s = \det s' \in (\mathbb{Z}/n\mathbb{Z})^\times$.

By passage to the limit on n, we obtain a homomorphism

$$\psi_\infty : G \to A_\infty = \varprojlim A[n],$$

where A_∞ is a certain closed subgroup of $\mathrm{Aut}\, E[\mathrm{tors}] \times \mathrm{Aut}\, E'[\mathrm{tors}]$. More precisely, one has

$$A_\infty = \prod_{\ell \in P} A_{\ell^\infty},$$

where A_{ℓ^∞} is the subgroup of $\mathrm{GL}\, T_\ell \times \mathrm{GL}\, T'_\ell$ consisting of pairs (s, s') such that $\det s = \det s' \in \mathbb{Z}_\ell^\times$.

THEOREM 13. *Make the following hypotheses:*
(i) E and E' have no complex multiplication.
(ii) The systems of ℓ-adic representations (ρ_ℓ) and (ρ'_ℓ) attached to E and E' do not become isomorphic over any finite extension of K.
Later work of Faltings shows that (ii) is equivalent to: E and E' are not geometrically isogenous. – PLC
Then the group $\psi_\infty(G)$ is an open subgroup of the group A_∞ defined above.

The proof will be given in §6.2.

COROLLARY 19. *For each $\ell \in P$, the image of G in $\mathrm{GL}\, T_\ell \times \mathrm{GL}\, T'_\ell$ under (ρ_ℓ, ρ'_ℓ) is an open subgroup of A_{ℓ^∞}; for almost every ℓ, this image is equal to A_{ℓ^∞}.*

In particular:

COROLLARY 20. *For almost every $\ell \in P$, we have $\psi_\ell(G) = A_\ell$.*

REMARK 21. *1) Hypothesis (ii) implies:*
(iii) E and e' are not $\overline{K}$-isogenous.
It is likely that (ii) and (iii) are equivalent*; this is true when the modular invariant j of E is not an integer* [**MG**, IV-14]*; it would be very interesting to show this in general.*
2) Suppose (i) holds. One can show that (ii) is equivalent to each of the following conditions:
(iv) There is no continuous character $\epsilon : G \to \{\pm 1\}$ such that ρ'_ℓ is isomorphic to $\epsilon \otimes \rho_\ell$ for all ℓ (or for a single ℓ, it comes to the same thing).
(v) There is $v \in \Sigma$ such that E and E' have good reduction at v and $t_v(E') \neq \pm t_v(E)$.
(The equivalence of (ii) and (iv) is shown by a Galois descent argument; the implication (v) $\Longrightarrow$ (iv) is immediate; the implication (ii) $\Longrightarrow$ (v) follows from Theorem 13.)
3) Let K^{cyc} be the subfield of $\overline{K}$ obtained by adjoining to K all the roots of unity (cf. §4.4). We can reformulate Theorem 13 as follows:

THEOREM 14. *Under hypotheses (i) and (ii) of Theorem 13, the image of $\mathrm{Aut}(\overline{K}/K^{\mathrm{cyc}})$ in $\prod_{\ell \in P} \mathrm{SL}\, T_\ell \times \mathrm{SL}\, T'_\ell$ is open.*

Let us say that two Galois extensions M and M' of a field L are *almost disjoint* if $M \cap M'$ has finite degree over L, or equivalently, that $\mathrm{Aut}(M'M/L)$ is an *open* subgroup of $\mathrm{Aut}(M/L) \times \mathrm{Aut}(M'/L)$. Theorem 14 is equivalent to:

THEOREM 15. *Let $K(E[\mathrm{tors}])$ and $K(E'[\mathrm{tors}])$ be the subfields of $\overline{K}$ obtained by adjoining to K the coordinates of the torsion points of E and E'. These fields contain K^{cyc}. If hypotheses (i) and (ii) of Theorem 13 are satisfied, the extensions $K(E[\mathrm{tors}])/K^{\mathrm{cyc}}$ and $K(E'[\mathrm{tors}])/K^{\mathrm{cyc}}$ are almost disjoint.*

6.2. Proof of Theorem 13.

We will use several lemmas:

LEMMA 13. *For all $\ell \in P$, the image G_{ℓ^∞} of G in $\mathrm{GL}\, T_\ell \times \mathrm{GL}\, T'_\ell$ is an open subgroup of A_{ℓ^∞}.*

PROOF. We denote by $\mathfrak{g}_\ell$ (resp. $\mathfrak{h}_\ell$) the $\mathbb{Q}_\ell$-Lie algebra associated to the ℓ-adic Lie group G_{ℓ^∞} (resp. A_{ℓ^∞}). In view of the definition of A_{ℓ^∞}, $\mathfrak{h}_\ell$ is the subalgebra of

$$\mathrm{End}\, V_\ell \times \mathrm{End}\, V_\ell$$

formed by pairs (u, u') such that $\mathrm{Tr}\, u = \mathrm{Tr}\, u'$. We have $\mathfrak{g}_\ell \subset \mathfrak{h}_\ell$, and the lemma comes down to showing that $\mathfrak{g}_\ell = \mathfrak{h}_\ell$. Since E and E' have no complex multiplication, the projections $\mathfrak{g}_\ell \to \mathrm{End}\, V_\ell$ and $g_\ell \to \mathrm{End}\, V'_\ell$ are surjective. But it is easy to find all subalgbras of $\mathfrak{h}_\ell$ with this property. One finds that, if $\mathfrak{g}_\ell \neq \mathfrak{h}_\ell$, then g_ℓ is the graph of an isomorphism of $\mathbb{Q}_\ell$-Lie algebras

$$\alpha : \mathrm{End}\, V_\ell \to V'_\ell$$

mapping 1 to 1; this last property shows that α is determined by its restriction to $\mathfrak{sl}V_\ell$. But every automorphism of the Lie algebra $\mathfrak{sl}_2$ comes from an element of PGL_2; we deduce that there is a $\mathbb{Q}_\ell$-linear bijection $f : V_\ell \to V'_\ell$ such that $\alpha(u) = f \circ u \circ f^{-1}$ for all $u \in \operatorname{End} V_\ell$, and $\mathfrak{g}_\ell$ is the set of pairs $(u, f \circ f^{-1})$. The mapping $f : V_\ell \to V'_\ell$ is an isomorphism of $\mathfrak{g}_\ell$-modules. By Lie theory, there is an open subgroup U of $G_{\ell\infty}$ such that f is an *isomorphism of U-modules.* If K' is the finite extension of K corresponding to U, we see that ρ_ℓ and ρ'_ℓ become isomorphic after extension of scalars to K', contradicting hypothesis (ii). Thus we must have $\mathfrak{g}_\ell = \mathfrak{h}_\ell$, whence the lemma. □

LEMMA 14. *Let $\ell \geq 5$ be a prime number. Suppose that the homomorphisms*

$$\varphi_\ell : G \to \operatorname{Aut} E[\ell] \text{ and } \varphi'_\ell : G \to \operatorname{Aut} E'[\ell]$$

are surjective and that $\psi_\ell : G \to A_\ell$ is not. Then there is a continuous character $\epsilon_\ell \to \{\pm 1\}$ and an isomorphism of groups $f : E[\ell] \to E'[\ell]$ such that

$$f \circ \varphi_\ell(s) = \epsilon_\ell(s)\varphi'_\ell(s) \circ f \ \forall s \in G.$$

Moreover, ϵ_ℓ is unramified at every ultrametric place v of K which is unramified over $\mathbb{Q}$ and at which E and E' have good reduction.

PROOF. Put $B = \operatorname{Aut} E[\ell]$, $B = \operatorname{Aut} E'[\ell]$, $H = \psi_\ell(G)$ and $A = A_\ell$. Then we have:

$$H \subset A \subset B \times B',\ H \neq A,\ \operatorname{pr}_1 H = B,\ \operatorname{pr}_2 H = B'.$$

We identify B with the subgroup $B \times \{1\}$ of $B \times B'$ and put $N = B \cap H$. Similarly we define $N' = B' \cap H$. It follows from the above properties that N is normal in B and N' is normal in B'; moreover, the image of H in $B/N \times B'/N'$ is the graph of an isomorphism $\alpha : B/N \to B'/N'$ (cf. Bourbaki, A.I, p. 124, exerc. 7). The keyword here is **Goursat's Lemma** – PLC Because H is contained in A, we have $N \subset \mathrm{SL}\, E[\ell]$; one sees easily that, if N were *equal* to $SLE[\ell]$, we would have $H = A$. One thus has $N \neq \mathrm{SL}\, E[\ell]$; as N is normal in $B = \operatorname{Aut} E[\ell]$, this implies that N is contained in the center $\{\pm 1\}$ of $\mathrm{SL}\, E[\ell]$. Similarly we have $N' \subset \{\pm 1\}$. The *center* of B/N is $\mathbb{F}_\ell^\times/N$ and the center of B'/N' is $\mathbb{F}_\ell^\times/N'$. The isomorphism $\alpha : B/N \to B'/N'$ thus carries $\mathbb{F}_\ell^\times/N$ onto $\mathbb{F}_\ell^\times/N'$ and induces by passage to the quotient an isomorphism $\tilde{\alpha}$ from the group $B/\mathbb{F}_\ell^\times = \mathrm{PGL}_2\, E[\ell]$ to the group $\mathrm{PGL}\, E'[\ell]$. But it is known that every automorphism of $\mathrm{PGL}_2\, \mathbb{F}_\ell$ is inner. We conclude that there is an isomorphism $f : E[\ell] \to E'[\ell]$ such that $\tilde{\alpha}(u) = f \circ u \circ f^{-1}$ for all $u \in \mathrm{PGL}\, E[\ell]$. This means that, if $h = (u, u')$ is an element of H, there is a homothety $\epsilon(h) \in \mathbb{F}_\ell^\times$ such that

$$u' = \epsilon(h) f \circ u \circ f^{-1}.$$

Taking the determinant of both sides, we get $\epsilon(h)^2 = 1$, and ϵ is a mapping from H into $\{\pm 1\}$; one checks immediately that it is a homomorphism. The composite of ϵ and the homomorphism $\psi_\ell : G \to H$ is the desired character ϵ_ℓ. The formula above shows that we indeed have

$$f \circ \varphi_\ell(s) = \epsilon_\ell(s)\varphi'_\ell(s) \circ f \text{ for all } s \in G.$$

In other terms, f defines an isomorphism from the G-module $E[\ell]$ to the G-module obtained from $E'[\ell]$ via "twisting" by ϵ_ℓ.

Let $v \in \Sigma$. Suppose that E and E' have good reduction at v and that v is unramified over $\mathbb{Q}$, i.e., that the ramification index $e(v)$ is 1. We must show that

ϵ_ℓ is *unramified at* v. This is clear if $p_v \neq \ell$. Suppose $p_v = \ell$. Choose an algebraic closure k_ℓ of $\mathbb{F}_\ell$; denote by λ_1 and λ_2 (resp. λ'_1 and λ'_2) the tame inertia characters at v, with values in $k_\ell^\times$, occurring in the Galois module $E[\ell] \otimes k_\ell$ (resp. $E'[\ell] \otimes k_\ell$), cf. §1.11. If we denote by ϵ_v the restriction of ϵ_ℓ to the inertia group at v, we have (up to permuting λ'_1 and λ'_2):

$$\lambda_1 = \epsilon_v \lambda'_1 \text{ and } \lambda_2 = \epsilon_v \lambda'_2. \tag{7}$$

Since $e(v) = 1$, the corollaries to Propositions 12 and 13 show that the λ_i and λ'_i are either trivial or fundamental characters of level 1 or 2. Their invariants in $(\mathbb{Q}/\mathbb{Z})'$ (cf. §1.7) belong to the set

$$X = \{0, \frac{1}{\ell-1}, \frac{1}{\ell^2-1}, \frac{\ell}{\ell^2-1}\}.$$

Since $\epsilon_v^2 = 1$, the invariant of ϵ_v is 0 or $\frac{1}{2}$; on the other hand (7) shows that the invariant is of the form $x - x'$ with $x, x' \in X$. Since $\ell \geq 5$ one checks that $\frac{1}{2}$ is not of the form $x - x'$. The invariant ϵ_v is thus equal to 0, meaning that $\epsilon_v = 1$, i.e., that ϵ_ℓ is unramified at v, which proves the lemma. □

LEMMA 15. *We have $\psi_\ell(G) = A_\ell$ for almost every ℓ.*

PROOF. We proceed by contradiction: suppose not, and let $L \subset P$ be an infinite subset such that $\psi_\ell(G) \neq A[\ell]$ for all $\ell \in L$. After reomoving a finite subest from L we may suppose that for all $\ell \in L$ we have $\ell \geq 5$ and the homomorphisms

$$\varphi_\ell : G \to \operatorname{Aut} E[\ell] \text{ and } \varphi'_\ell : G \to \operatorname{Aut} E'[\ell]$$

are surjective (cf. Theorem 7). For $\ell \in L$, let denote by ϵ_ℓ the character of G with values in $\{\pm 1\}$ defined in Lemma 14. It follows from this lemma that the ϵ_ℓ are unramified outside of a finite set of places of K which is independent of ℓ. This implies, as we know, that the ϵ_ℓ are *finite in number*. After replacing L by one of its infinite subsets, we may thus assume that ϵ_ℓ is independent of ℓ and denote it by ϵ. The character ϵ corresponds to an extension K'/K of degree at most 2; put $G' = \operatorname{Aut}(\overline{K}/K) = \operatorname{Ker} \epsilon$. By Lemma 14, for all $\ell \in L$, $E[\ell]$ and $E'[\ell]$ are isomorphic as G'-modules. We deduce that, for v a place of K' at which E and E' each have good reduction, the Frobenius traces of the reductions of E and E' at v satsify the congruences

$$t_v(E) \equiv t_v(E') \pmod{\ell} \text{ for all } \ell \in L \setminus \{p_\ell\}.$$

Since L is infinite, this implies $t_v(E) = t_v(E')$, which shows that the systems of ℓ-adic representations attached to E and E' become isomorphic over K' [**MG**, IV-15]; this contradicts hypothesis (ii). □

LEMMA 16. *Let $\ell \geq 5$ be a prime number, and let H be a closed subgroup of $\mathrm{GL}_2 \mathbb{Z}_\ell \times \mathrm{GL}_2 \mathbb{Z}_\ell$. We suppose that the image of H in*

$$\mathrm{GL}_2 \mathbb{F}_\ell \times \mathrm{GL}_2 \mathbb{F}_\ell$$

under reduction modulo ℓ contains $\mathrm{SL}_2 \mathbb{F}_\ell \times \mathrm{SL}_2 \mathbb{F}_\ell$. Then H contains $\mathrm{SL}_2 \mathbb{Z}_\ell \times \mathrm{SL}_2 \mathbb{Z}_\ell$.

PROOF. Let H' be the closure of the commutator subgroup of H. This is a subgroup of $\mathrm{SL}_2 \mathbb{Z}_\ell \times \mathrm{SL}_2 \mathbb{Z}_\ell$ and its image under reduction modulo ℓ contains the derived subgroup of $\mathrm{SL}_2 \mathbb{F}_\ell \times \mathrm{SL}_2 \mathbb{F}_\ell$, which is $\mathrm{SL}_2 \mathbb{F}_\ell \times \mathrm{SL}_2 \mathbb{F}_\ell$ itself since $\ell \geq 5$. It all comes down to showing that $H' = \mathrm{SL}_2 \mathbb{Z}_\ell \times \mathrm{SL}_2 \mathbb{Z}_\ell$. Let X be the intersection of

H' with $\mathrm{SL}_2\,\mathbb{Z}_\ell \times \{1\}$; let Y be the set of elements of H' whose second component is congruent to 1 modulo ℓ. We have $Y \supset X$, and the quotient Y/X is a pro-ℓ-group. Let $\tilde{Y}$ and $\tilde{X}$ be the images of Y and X in $\mathrm{SL}_2\,\mathbb{F}_\ell$ under reduction modulo ℓ of the first compnent. By hypothesis we have $\tilde{Y} = \mathrm{SL}_2\,\mathbb{F}_\ell$; on the other hand, $\tilde{Y}/\tilde{X}$ is isomorphic to a quotient of Y/X, hence is an ℓ-group. Since $\mathrm{SL}_2\,\mathbb{F}_\ell$ has no proper normal subgroup of index a power of ℓ, we have $\tilde{X} = \tilde{Y} = \mathrm{SL}_2\,\mathbb{F}_\ell$. By [**MG**, Lemma 3, IV-23], this implies that $X = \mathrm{SL}_2\,\mathbb{Z}_\ell \times \{1\}$. Thus H' contains the first factor of the product $\mathrm{SL}_2\,\mathbb{Z}_\ell \times \mathrm{SL}_2\,\mathbb{Z}_\ell$; an analogous argument shows that it contains the second factor; thus it is equal to $\mathrm{SL}_2\,\mathbb{Z}_\ell \times \mathrm{SL}_2\,\mathbb{Z}_\ell$, establishing the lemma. □

In the following statement, J_v denotes the smallest closed normal subgroup of G containing the inertia groups at the places of $\overline{K}$ extending v, cf. §4.4.

LEMMA 17. *For almost all v, $\psi_\infty(J_v)$ is equal to the ℓth factor $A_{\ell\infty}$ of A, with $\ell = p_v$.*

PROOF. Put $H_v = \psi_\infty(J_v)$. By Lemma 15 and Theorem 10, we have, for almost all v:
a) H_v is contained in the ℓth factor $A_{\ell\infty}$ of A, where $\ell = p_v$.
b) The projections $H_v \to \mathrm{GL}\,T_\ell$ and $H_v \to \mathrm{GL}\,T'_\ell$ are surjective.
c) $\psi_\ell(G) = A[\ell]$.
We suppose that all of the above hold and that $\ell \geq 5$. Let $\tilde{H}_v = \psi_\ell(J_v)$ be the image of H_v in $\mathrm{Aut}\,E[\ell] \times \mathrm{Aut}\,E'[\ell]$ under reduction modulo ℓ. By b) and c), the two projections $\tilde{H}_v \to \mathrm{Aut}\,E[\ell]$ and $\tilde{H}_v \to \mathrm{Aut}\,E'[\ell]$ are surjective and $\tilde{H}_v$ is a normal subgroup of $A_\ell = \psi_\ell(G)$. It is easy to see that these properties imply $\tilde{H}_v = A_\ell$. Applying Lemma 16, we thus conclude that H_v contains $\mathrm{SL}\,T_\ell \times \mathrm{SL}_2\,T_\ell$, which certainly implies that $H_v = A_{\ell\infty}$. □

End of the proof of Theorem 13

Lemma 17 shows that there is a finite subset S of P such that $\psi_\infty(G)$ contains the factors $A_{\ell\infty}$ of A_∞ for all $\ell \in P \setminus S$. It thus suffices to show that the image of $\psi_\infty(G)$ in the product of the $A_{\ell\infty}$, for $\ell \in S$, is *open*, which follows from Lemma 13 combined with a standard argument on Sylow subgroups [**MG**, IV-24, proof of Lemma 4].

REMARK 22. *The above proof lends itself to numerical calculations of the kind pursued in §5. For example, the reader will check that, if one takes E and E' to be the curves 5.5.6 and 5.57 of §5.5 and $K = \mathbb{Q}$, then we have $\psi_\ell(G) = A_\ell$ for all $\ell \in P$.*

6.3. Curves with complex multiplication.

One has a result analogous to Theorem 15:

THEOREM 16. *Suppose that E and E' are not $\overline{K}$-isogenous and that at least one has complex multiplication. Then the extensions $K(E[\mathrm{tors}])/K^{\mathrm{cyc}}$ and $K(E'[\mathrm{tors}])/K^{\mathrm{cyc}}$ are almost disjoint.*

(One could also formulate this result in the style of Theorems 13 and 14. We leave that to the reader.

Since E and E' play a symmetric role, it suffices to prove Theorem 16 in each of the following caes:

a) E' has complex multiplication (that we may assume to be defined over K) and E does not. If we put $L = K(E[\text{tors}]) \cap K(E'[\text{tors}])$, the extension L/K is contained in $K(E'[\text{tors}])/K$, hence abelian. If follows (cf. §4.4) that $\operatorname{Aut} K(E[\text{tors}]/L)$ is an open subgroup of $\prod_{\ell \in P} \operatorname{SL} T_\ell$, hence an open subgroup of $\operatorname{Aut}(K(E[\text{tors}])/K^{\text{cyc}})$, which shows that the extension L/K^{cyc} has finite degree.

b) E and E' have complex multiplication by imaginary quadratic fields F and F', which we may suppose are contained in K. Since E and E' are not $\overline{K}$-isogenous, the fields F and F' are distinct. Moreover, the aaction of G on $E[\text{tors}]$ and $E'[\text{tors}]$ is abelian, described by Theorem 12. In particular, the Galois group of $K(E[\text{tors}]/K$ may be identified with an open subgroup of the product of the $U_\ell(F)$. Theorem 16 is thus reduced to the following statement, whose verification is elementary:

Let $\theta_\ell : U_\ell(K) \to U_\ell(F) \times U_\ell(F')$ be the homomorphism defined by N_{K_ℓ/F_ℓ} and N_{K_ℓ/F'_ℓ}; the image of θ_ℓ is contained in the group H_ℓ consisting of pairs (u, u') such that $N_{F_\ell/Q_\ell}(u) = N_{F'_\ell/\mathbb{Q}_\ell}(u')$ and, for all ℓ (resp. for almost every ℓ), θ_ℓ is an *open* (resp. *surjective*) mapping of $U_\ell(K)$ into H_ℓ.

Bibliography

[1] Artin, E. Geometric algebra. Interscience Publishers, Inc., New York-London, 1957.

[2] Billing, G.; Mahler, K. On exceptional points on cubic curves. J. London Math. Soc. 15, (1940). 32-43.

[3] Casselman, W. On abelian varieties with many endomorphisms and a conjecture of Shimura's. Invent. Math. 12 (1971), 225-236.

[4] Cassels, J. W. S. Diophantine equations with special reference to elliptic curves. J. London Math. Soc. 41 (1966), 193-291.

[5] Cassels, J. and Fröhlich, A. (ed.): Algebraic number theory. New York: Academic Press 1967.

[6] Curtis, C. and Reiner, I. Representation theory of finite groups and associative algebras. New York: Interscience Publ. 1962.

[7] Deligne, P. Formes modulaires and représentations ℓ-adiques. Sém. Bourbaki, 1968/69, exposé 355: LNM 179. Berlin-Heidelberg-New York: Springer 1971.

[8] Deuring, M. Die Typen der Multipliakorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hamburg 14 (1941), 197–272.

[9] Deuring, M. Die Zetafunktion einer algebraiscehn kurve vom Geschlechte Eins. Gött. Nach. (1953), 85–94; II, *ibid.* (1955), 13–42; III. *ibid.* (1956) 37–76; IV *ibid.* (1957), 55–80.

[10] Deuring, M. Die Klassenkörper der komplexen Multiplikation. Enz. Math. Wisws., Band I-2, Heft 10, Teil II. Stuttgart: Teubner 1958.

[11] Fricke, R. Lehrbuch der Algebra, Bd. III. Braunschweig: Fried. Vieweg & Sohn 1928.

[12] Fröhlich, A. Formal groups. Lecture Notes in Mathematics, No. 74 Springer-Verlag, Berlin-New York 1968.

[13] Hecke, E. Mathematische Werke. Göttingen: Vandenhoeck und Ruprecht 1959.

[14] Lubin, J. Finite subgroups and isogenies of one-parameter formal Lie groups. Ann. of Math. 85 (1967), 296-302.

[15] Mumford, D. Abelian varieties. Tata Institute of Fundamental Research Studies in Mathematics, No. 5 Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London 1970.

[16] Néron, A. *Modèles minimaux des varietés abéliennes sur les corps locaux and globaux.* Inst. Hautes Études Sci. Publ.Math. No. 21 1964.

[17] Neumann, O. Zur Reduktion der elliptischen Kurven. Math. Nachr. 46 (1970), 285-310.

[18] Ogg, A. P. Abelian curves of 2-power conductor. Proc. Cambridge Philos. Soc. 62 (1966), 143-148.

[19] Ogg, A. P. Elliptic curves and wild ramification. Amer. J. Math. 89 (1967), 1-21.

[20] Ogg, A. Rational points of finite order on elliptic curves. Invent. Math. 12 (1971), 105-111.

[21] Raynaud, M. Schémas en groupes de type $(p, \ldots, p)$. Bull. Soc. Math. France 102 (1974), 241-280.

[22] Roquette, P. Analytic theory of elliptic functions over local fields. Hamburger Mathematische Einzelschriften (N.F.), Heft 1 Vandenhoeck & Ruprecht, Göttingen 1970.

[23] Shafarevich, I. Corps de nombres algébriques (in Russian). Proc. Inter. Congr. MAth. Stockholm, 163–176 (1962). [English translation: Amer. Math. Transl., ser. 2, vol. 31, 25–39 (1963).]

[24] Serre, J.-P. Serre, Jean-Pierre Sur les corps locaux à corps résiduel algébriquement clos. Bull. Soc. Math. France 89 (1961), 105-154.

[25] Serre, J.-P. Corps Locaux (second edition). Paris: Hermann 1968.

[26] Serre, J.-P., Groups de Lie ℓ-adiques attachés aux courbes elliptiques. Colloque Clermont-Ferrand, 239–256, C.N.R.S. 1964.

[27] Serre, J.-P. Abelian ℓ-adic representations and elliptic curves. New York: Benjamin 1968 (cited as [**MG**]).

[28] Serre, J.-P. Une interprétation des congruences relatives à la fonction τ de Ramanujan. 1969 Séminaire Delange-Pisot-Poitou: 1967/68, Théorie des Nombres, Fasc. 1, Exp. 14 17 pp. Secrétariat mathématique, Paris.

[29] Serre, J.-P. Facteurs locaux des fonctions zêta des varíetés algébriques (définitions et conjectures). Séminaire Delange-Pisot-Poitou, 1969/70, n. 19.

[30] Serre, J.-P. and Tate, J. Good reduction of abelian varieties. Ann. of Math. (2) 88 (1968), 492-517.

[31] Shimura, G. A reciprocity law in non-solvable extensions. J. Reine Angew. Math. 221 (1966), 209-220.

[32] Shimura, G. Class fields over real quadratic fields in the theory of modular functions. Several complex variables, II (Proc. Internat. Conf., Univ. Maryland, College Park, Md., 1970), pp. 169-188. Lecture Notes in Math., Vol. 185, Springer, Berlin, 1971.

[33] Shimura, G. Introduction to the arithmetic theory of automorphic functions. Publ. Math. Soc. Japan, no. 11, Tokyo-Princeton, 1971.

[34] Shimura, G. and Taniyama, Y. Complex multiplication of abelian varieties and its applications to number theory. Publ. Math. Soc. Japan 6 (1961).

[35] Vélu, J. Courbes elliptiques sur $\mathbb{Q}$ ayant bonne réduction en dehors de 11. C. R. Acad. Sci. Paris Sér. A-B 273 (1971), A73-A75.

[36] Weber, H. Lehrbuch der Algebra, Bd. II (Zw. Auf.). Braunschweig 1899.

[37] Weil, A. Numbers of solutions of equations in finite fields. Bull. Amer. Math. Soc. 55 (1949), 497-508.

[38] Weil, A. Jacobi sums as "Grössencharaktere". Trans. Amer. Math. Soc. 73 (1952), 487-495.

[39] Weil, A. On a certain type of characters of the idèle-class group of an algebraic number-field. Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955, pp. 1-7. Science Council of Japan, Tokyo, 1956.

[40] Weil, A. On the theory of complex multiplication. Proceedings of the international symposium on algebraic number theory, Tokyo & Nikko, 1955, pp. 9022. Science Council of Japan, Tokyo, 1956.

[41] Weil, A. Uber die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. Math. Ann. 168 (1967), 149-156.

[42] Weil, A. Basic number theory. Berlin-Heidelberg-New York: Springer 1967.

[AECI] J.H. Silverman, *Arithmetic of Elliptic Curves*.

[Ka81] N. Katz, *Galois properties of torsion points on abelian varieties*. Invent. Math. 62 (1981), 481–502.

[MG] J.-P. Serre, *Abelian ℓ-adic Galois representations and elliptic curves*.