

# Abelian $\ell$ -adic Representations and Elliptic Curves

Jean-Pierre Serre

June 11, 2024



# CONTENTS



## EDITORS' NOTES

We have tried to keep the book as similar to the original with minor changes. Here are some changes in notation:

Original	New	Meaning
$\Sigma_K$	$M_K^0$	Set of finite places of a number field $K$ .
$\ell$	$\lambda$	The residue field of a field $L$ relative to a finite place.
$R^*$	$R^\times$	The group of units of a ring $R$ .
$U^\circ$	$\mathring{U}$	The interior of a subset $U$ of a topological space.
$A_K$	$\mathcal{O}_K$	The ring of algebraic integers of a number field $K$ .
$\mathbb{P}_{n/K}$	$\mathbb{P}_K^n$	The $n$ -dimensional projective space over a field $K$ .
$X \times_K L$	$X \otimes_K L$	The base change of a $K$ -scheme $X$ by a field extension $L/K$ .



# CHAPTER I

## $\ell$ -ADIC REPRESENTATIONS

### §1. The notion of an $\ell$ -adic representation

#### 1.1 Definition

Let  $K$  be a field, and let  $K_s$  be a separable algebraic closure of  $K$ . Let  $\mathfrak{G} = \text{Gal}(K_s/K)$  be the Galois group of the extension  $K_s/K$ . The group  $\mathfrak{G}$ , with the Krull topology, is compact and totally disconnected. Let  $\ell$  be a prime number, and let  $V$  be a finite-dimensional vector space over the field  $\mathbb{Q}_\ell$  of  $\ell$ -adic numbers. The full linear group  $\text{Aut}(V)$  is an  $\ell$ -adic Lie group, its topology being induced by the natural topology of  $\text{End}(V)$ ; if  $n = \dim(V)$ , we have  $\text{Aut}(V) \cong \text{GL}(n, \mathbb{Q}_\ell)$ .

**Definition 1.1.** An  $\ell$ -adic representation of  $\mathfrak{G}$  (or, by abuse of language, of  $K$ ) is a continuous homomorphism  $\rho: \mathfrak{G} \rightarrow \text{Aut}(V)$ .

**Remark.** 1) A *lattice* of  $V$  is a sub- $\mathbb{Z}_\ell$ -module  $T$  which is free of finite rank, and generate  $V$  over  $\mathbb{Q}_\ell$ , so that  $V$  can be identified with  $T \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ . Notice that there exists a lattice of  $V$  which is stable under  $\mathfrak{G}$ . This follows from the fact that  $\mathfrak{G}$  is compact.

Indeed, let  $L$  be any lattice of  $V$ , and let  $H$  be the set of elements  $g \in \mathfrak{G}$  such that  $\rho(g)L = L$ . This is an open subgroup of  $\mathfrak{G}$ , and  $\mathfrak{G}/H$  is finite. The lattice  $T$  generated by the lattices  $\rho(g)L$ ,  $g \in \mathfrak{G}/H$ , is stable under  $G$ .

Notice that  $L$  may be identified with the projective limit of the free  $(\mathbb{Z}/\ell^m\mathbb{Z})$ -modules  $T/\ell^m T$ , on which  $\mathfrak{G}$  acts; the vector space  $V$  may be reconstructed from  $T$  by  $V = T \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ .

- 2) If  $\rho$  is an  $\ell$ -adic representation of  $\mathfrak{G}$ , the group  $\mathfrak{G} = \text{Im}(\rho)$  is a closed subgroup of  $\text{Aut}(V)$ , and hence, by the  $\ell$ -adic analogue of Cartan's theorem (cf. [28])  $\mathfrak{G}$  is itself an  $\ell$ -adic Lie group. Its Lie algebra  $\mathfrak{g} = \text{Lie}(\mathfrak{G})$  is a subalgebra of  $\text{End}(V) = \text{Lie}(\text{Aut}(V))$ . The Lie algebra  $\mathfrak{g}$  is easily seen to be invariant under extensions of finite type of the ground field  $K$  (cf. [24], 1.2).

### Exercises.

- 1) Let  $V$  be a vector space of dimension 2 over a field  $k$  and let  $H$  be a subgroup of  $\text{Aut}(V)$ . Assume that  $\det(1 - h) = 0$  for all  $h \in H$ . Show the existence of a basis of  $V$  with respect to which  $H$  is contained either in the subgroup  $\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix}$  or in the subgroup  $\begin{pmatrix} 1 & 0 \\ * & * \end{pmatrix}$  of  $\text{Aut}(V)$ .
- 2) Let  $\rho: G \rightarrow \text{Aut}(V_\ell)$  be an  $\ell$ -adic representation of  $\mathfrak{G}$ , where  $V_\ell$  is a  $\mathbb{Q}_\ell$ -vector space of dimension 2. Assume  $\det(1 - \rho(s)) = 0 \pmod{\ell}$  for all  $s \in \mathfrak{G}$ . Let  $T$  be a lattice of  $V_\ell$  stable by  $G$ . Show the existence of a lattice  $T'$  of  $V_\ell$  with the following two properties:
  - (a)  $T'$  is stable by  $\mathfrak{G}$
  - (b) Either  $T'$  is a sublattice of index  $\ell$  of  $T$  and  $\mathfrak{G}$  acts trivially on  $T/T'$  or  $T$  is a sublattice of index  $\ell$  of  $T'$  and  $\mathfrak{G}$  acts trivially on  $T'/T$ .
 (Apply exercise ?? above to  $k = F_\ell$  and  $V = T/\ell T$ .)
- 3) Let  $\rho$  be a semi-simple  $\ell$ -adic representation of  $G$  and let  $U$  be an invariant subgroup of  $G$ . Assume that, for all  $x \in U$ ,  $\rho(x)$  is unipotent (all its eigenvalues are equal to 1). Show that  $\rho(x) = 1$  for all  $x \in U$ . (Show that the restriction of  $\rho$  to  $U$  is semi-simple and use Kolchin's theorem to bring it to triangular form.)
- 4) Let  $\rho: G \rightarrow \text{Aut}(V_\ell)$  be an  $\ell$ -adic representation of  $G$ , and  $T$  a lattice of  $V_\ell$  stable under  $G$ . Show the equivalence of the following properties:
  - (a) The representation of  $G$  in the  $F_\ell$ -vector space  $T/\ell T$  is irreducible.
  - (b) The only lattices of  $V_\ell$  stable under  $G$  are the  $\ell^n T$ , with  $n \in \mathbb{Z}$ .



## 1.2 Examples

**Roots of unity.** Let  $\ell \neq \text{char}(K)$ . The group  $\mathfrak{G} = \text{Gal}(K_s/K)$  acts on the group  $\mu_m$  of  $\ell^m$ -th roots of unity, and hence also on  $T_\ell(\mu) = \varprojlim_{m \in \mathbb{N}} \mu_m$ . The  $\mathbb{Q}_\ell$ -vector space  $V_\ell(\mu) = T_\ell(\mu) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$  is of dimension 1, and the homomorphism  $\chi_\ell: \mathfrak{G} \rightarrow \text{Aut}(V_\ell) = \mathbb{Q}_\ell^\times$  defined by the action of  $\mathfrak{G}$  on  $V_\ell$  is a 1-dimensional  $\ell$ -adic representation of  $\mathfrak{G}$ . The character  $\chi_\ell$  takes its values in the group of units  $U$  of  $\mathbb{Z}_\ell$ ; by definition

$$g(z) = z^{\chi_\ell(g)} \quad \text{if } g \in \mathfrak{G}, \quad z^{\ell^m} = 1.$$

**Elliptic curves.** Let  $\ell \neq \text{char}(K)$ . Let  $E$  be an elliptic curve defined over  $K$  with a given rational point  $o$ . One knows that there is a unique structure of group variety on  $E$  with  $o$  as neutral element. Let  $E_m$  be the kernel of multiplication by  $\ell^m$  in  $E(K_s)$ , and let

$$T_\ell(E) = \varprojlim_m E_m, \quad V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

The Tate module  $T_\ell(E)$  is a free  $\mathbb{Z}_\ell$ -module on which  $\mathfrak{G} = \text{Gal}(K_s/K)$  acts (cf. [12], chap. VII). The corresponding homomorphism  $\pi_\ell: \mathfrak{G} \rightarrow \text{Aut}(V_\ell(E))$  is an  $\ell$ -adic representation of  $\mathfrak{G}$ . The group  $G_\ell = \text{Im}(\pi_\ell)$  is a closed subgroup of  $\text{Aut}(T_\ell(E))$ , a 4-dimensional Lie group isomorphic to  $\text{GL}(2, \mathbb{Z}_\ell)$ . (In chapter IV, we will determine the Lie algebra of  $G_\ell$ , under the assumption that  $K$  is a number field.)

Since we can identify  $E$  with its dual (in the sense of the duality of abelian varieties) the symbol  $(x, y)$  (cf. [12], *loc. cit.*) defines canonical isomorphisms

$$\bigwedge^2 T_\ell(E) = T_\ell(\mu), \quad \bigwedge^2 V_\ell(E) = V_\ell(\mu).$$

Hence  $\det(\pi_\ell)$  is the character  $\chi_\ell$  defined in example 1.

**Abelian varieties.** Let  $A$  be an abelian variety over  $K$  of dimension  $d$ . If  $\ell \neq \text{char}(K)$ , we define  $T_\ell(A)$ ,  $V_\ell(A)$  in the same way as in example 2. The group  $T_\ell(A)$  is a free  $\mathbb{Z}_\ell$ -module of rank  $2d$  (cf. [12], *loc. cit.*) on which  $\mathfrak{G} = \text{Gal}(K_s/K)$  acts.

**Cohomology representations.** Let  $X$  be an algebraic variety defined over the field  $K$ , and let  $X_s = X \times_K K_s$  be the corresponding variety over  $K_s$ . Let

$\ell \neq \text{char}(K)$ , and let  $i$  be an integer. Using the étale cohomology of **3** [3] we let

$$H^i(X_s, \mathbb{Z}_\ell) = \varprojlim_n H^i((X_s)_{\text{ét}}, \mathbb{Z}/\ell^n \mathbb{Z}), \quad H_\ell^i(X_s) = H^i(X_s, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

The group  $H_\ell^i(X_s)$  is a vector space over  $\mathbb{Q}_\ell$  on which  $G = \text{Gal}(K_s/K)$  acts (via the action of  $G$  on  $X_s$ ). It is finite dimensional, at least if  $\text{char}(K) = 0$  or if  $X$  is proper. We thus get an  $\ell$ -adic representation of  $G$  associated to  $H_\ell^i(X_s)$ ; by taking duals we also get homology  $\ell$ -adic representations. Examples 1, 2, 3 are particular cases of homology  $\ell$ -adic representations where  $i = 1$  and  $X$  is respectively the multiplicative group  $m$ , the elliptic curve  $E$ , and the abelian variety  $A$ .

### Exercise.

- (a) Show that there is an elliptic curve  $E$ , defined over  $K_0 = \mathbb{Q}(T)$ , with  $j$ -invariant equal to  $T$ .
- (b) Show that for such a curve, over  $K = \mathbb{C}(T)$ , one has  $G_\ell = \text{SL}(T_\ell(E))$  (cf. **10** [10] for an algebraic proof).
- (c) Using ??, show that, over  $K_0$ , we have  $G_\ell = \text{GL}(T_\ell(E))$ .
- (d) Show that for any closed subgroup  $H$  of  $\text{GL}(2, \mathbb{Z}_\ell)$  there is an elliptic curve (defined over some field) for which  $G_\ell = H$ .

## §2. $\ell$ -adic representations of number fields

### 2.1 Preliminaries

(For the basic notions concerning number fields, see for instance **6** [6], **13** [13] or **44** [44].) Let  $K$  be a number field (i.e. a finite extension of  $\mathbb{Q}$ ). Denote by  $M_K^0$  the set of all finite places of  $K$ , i.e., the set of all normalized discrete valuations of  $K$  (or, alternatively, the set of prime ideals in the ring  $\mathcal{O}_K$  of integers of  $K$ ). The **residue field**  $k_v$  of a place  $v \in M_K^0$  is a finite field with  $\mathbf{N}(v) = p_v^{\deg(v)}$  elements, where  $p_v = \text{char}(k_v)$  and  $\deg(v)$  is the degree of  $k_v$  over  $F_{p_v}$ . The ramification index  $e_v$  of  $v$  is  $v(p_v)$ .

Let  $L/K$  be a finite Galois extension with Galois group  $G$ , and let  $w \in M_L^0$ . The subgroup  $D_w$  of  $G$  consisting of those  $g \in G$  for which  $gw = w$  is the **decomposition group** of  $w$ . The restriction of  $w$  to  $K$  is an integral multiple of an element  $v \in M_K^0$ ; by abuse of language, we also say that  $v$  is the restriction of  $w$  to  $K$ , and we write  $w \mid v$  (“ $w$  divides  $v$ ”). Let  $L$  (resp.  $K$ ) be the completion of  $L$  (resp.  $K$ ) with respect to  $w$  (resp.  $v$ ). We have  $D_w = \text{Gal}(L_w/K_v)$ . The group  $D_w$  is mapped homomorphically onto the Galois group  $\text{Gal}(\lambda_w/k_v)$  of the corresponding residue extension  $\lambda_w/k_v$ . The kernel of  $G \rightarrow \text{Gal}(\lambda_w/k_v)$  is the inertia group  $I_w$  of  $w$ . The quotient group  $D_w/I_w$  is a finite cyclic group generated by the **Frobenius element**  $F_w$ ; we have  $F(\lambda) = \lambda^{\mathbf{N}(v)}$  for all  $\lambda \in \lambda_w$ . The valuation  $w$  (resp.  $v$ ) is called **unramified** if  $I_w = \{1\}$ . Almost all places of  $K$  are unramified.

If  $L$  is an arbitrary algebraic extension of  $\mathbb{Q}$ , one defines  $M_K^0$  to be the projective limit of the sets  $M_{L_\alpha}^0$ , where  $L_\alpha$  ranges over the finite sub-extensions of  $L/\mathbb{Q}$ . Then, if  $L/K$  is an arbitrary Galois extension of the number field  $K$ , and  $w \in M_L^0$ , one defines  $D_w, I_w, F_w$  as before. If  $v$  is an unramified place of  $K$ , and  $w$  is a place of  $L$  extending  $v$ , we denote by  $F_v$  the conjugacy class of  $F_w$  in  $G = \text{Gal}(L/K)$ .

**Definition 2.1.** Let  $\rho: \text{Gal}(\overline{K}/K) \rightarrow \text{Aut}(V)$  be an  $\ell$ -adic representation of  $K$ , and let  $v \in M_K^0$ . We say that  $\rho$  is unramified at  $v$  if  $\rho(I_w) = \{1\}$  for any valuation  $w$  of  $\overline{K}$  extending  $v$ .

If the representation  $\rho$  is unramified at  $v$ , then the restriction of  $\rho$  to  $D_w$  factors through  $D_w/I_w$  for any  $w \mid v$ ; hence  $\rho(F_w) \in \text{Aut}(V)$  is defined; we call  $\rho(F_w)$  the **Frobenius** of  $w$  in the representation  $\rho$ , and we denote it by  $F_{w,\rho}$ . The conjugacy class of  $F_{w,\rho}$  in  $\text{Aut}(V)$  depends only on  $v$ ; it is denoted by  $F_{v,\rho}$ . If  $L/K$  is the extension of  $K$  corresponding to  $H = \text{Ker}(\rho)$ , then  $\rho$  is unramified at  $v$  if and only if  $v$  is unramified in  $L/K$ .

## 2.2 Čebotarev’s density theorem

Let  $P$  be a subset of  $M_K^0$ . For each integer  $n$ , let  $a_n(P)$  be the number of  $v \in P$  such that  $\mathbf{N}v \leq n$ . If  $a$  is a real number, one says that  $P$  **has density**  $a$  if

$$\lim_{n \rightarrow \infty} \frac{a_n(P)}{a_n(M_K^0)} = a \quad \text{when } n \rightarrow \infty.$$

Note that  $a_n(M_K^0) \sim n/\log(n)$ , by the prime number theorem (cf. Appendix, or [13], chap. VIII), so that the above relation may be rewritten:

$$a_n(P) = a \cdot \frac{n}{\log(n)} + o\left(\frac{n}{\log(n)}\right).$$

**Examples.** A finite set has density 0. The set of  $v \in M_K^0$  of degree 1 (i.e. such that  $\mathbf{N}v$  is prime) has density 1. The set of ordinary prime numbers whose first digit (in the decimal system, say) is 1 has no density.

**Theorem 1.** *Let  $L$  be a finite Galois extension of the number field  $K$ , with Galois group  $G$ . Let  $X$  be a subset of  $G$ , stable by conjugation. Let  $P_X$  has density equal to  $\text{Card}(X)/\text{Card}(G)$ .*

For the proof, see [7], [1], or the Appendix.

**Corollary 1.1.** *For every  $g \in G$ , there exist infinitely many unramified places  $w \in M_K^0$  such that  $F_w = g$ .*

For infinite extensions, we have:

**Corollary 1.2.** *Let  $L$  be a Galois extension of  $K$ , which is unramified outside a finite set  $S$ .*

- a) *The Frobenius elements of the unramified places of  $L$  are dense in  $\text{Gal}(L/K)$ .*
- b) *Let  $X$  be a subset of  $\text{Gal}(L/K)$ , stable by conjugation. Assume that the boundary of  $X$  has measure zero with respect to the Haar measure  $\mu$  of  $X$ , and normalize  $\mu$  such that its total mass is 1. Then the set of places  $v \notin S$  such that  $F_v \subset X$  has a density equal to  $\mu(X)$ .*

Assertion (b) follows from the theorem, by writing  $L$  as an increasing union of finite Galois extensions and passing to the limit (one may also use Prop. 1 of the Appendix). Assertion (a) follows from (b) applied to a suitable neighborhood of a given class of  $\text{Gal}(L/K)$ .

**Exercise.** Let  $G$  be an  $\ell$ -adic Lie group and let  $X$  be an analytic subset of  $G$  (i.e. a set defined by the vanishing of a family of analytic functions on  $G$ ). Show that the boundary of  $X$  has measure zero with respect to the Haar measure of  $G$ .

### 2.3 Rational $\ell$ -adic representations

Belen.

### 2.4 Representations with values in a linear algebraic group

Let  $H$  be a linear algebraic group defined over a field  $K$ . If  $k'$  is a commutative  $k$ -algebra, let  $H(k')$  denote the group of points of  $H$  with values in  $k'$ . Let  $A$  denote the coordinate ring (or “affine ring”) of  $H$ . An element  $f \in A$  is said to be **central** if  $f(xy) = f(yx)$  for any  $x, y \in H(k')$  and any commutative  $k$ -algebra  $k'$ . If  $x \in H(k')$  we say that the conjugacy class of  $x$  in  $H$  is **rational over  $k$**  if  $f(x) \in k$  for any central element  $f$  of  $A$ .

**Definition 2.2.** Let  $H$  be a linear algebraic group over  $\mathbb{Q}$ , and let  $K$  be a field. A continuous homomorphism  $\rho: \text{Gal}(K_s/K) \rightarrow H(\mathbb{Q}_\ell)$  is called an  $\ell$ -adic representation of  $K$  with values in  $H$ .

(Note that  $H(\mathbb{Q}_\ell)$  is, in a natural way, a topological group and even an  $\ell$ -adic Lie group.)

If  $K$  is a number field, one defines in an obvious way what it means for  $\rho$  to be unramified at a place  $v \in M_K^0$ ; if  $w \mid v$ , one defines the Frobenius element  $F_{w,\rho} \in H(\mathbb{Q}_\ell)$  and its conjugacy class  $F_{v,\rho}$ . We say, as before, that  $\rho$  is **rational** if

- (a) there is a finite set  $S$  of  $M_K^0$  such that  $\rho$  is unramified outside  $S$ ,
- (b) if  $v \notin S$ , the conjugacy class  $F_{v,\rho}$  is rational over  $\mathbb{Q}$ .

Two rational representations  $\rho, \rho'$  (for primes  $\ell, \ell'$ ) are said to be **compatible** if there exists a finite subset  $S$  of  $M_K^0$  such that  $\rho$  and  $\rho'$  are unramified outside  $S$  and such that for any central element  $f \in A$  and any  $v \in M_K^0 \setminus S$  we have  $f(F_{v,\rho}) = f(F_{v,\rho'})$ . One defines in the same way the notions of **compatible** and **strictly compatible systems** of rational representations.

**Remark.** 1) If the algebraic group  $H$  is abelian, then condition ?? above means that  $F_{v,\rho}$  (which is now an element of  $H(\mathbb{Q}_\ell)$ ) is rational over  $\mathbb{Q}$ , i.e. belongs to  $H(\mathbb{Q})$ .

- 2) Let  $V_0$  be a finite-dimensional vector space over  $\mathbb{Q}$ , and let  $\mathrm{GL}_{V_0}$  be the linear algebraic group over  $\mathbb{Q}$  whose group of points in any commutative  $\mathbb{Q}$ -algebra  $k$  is  $\mathrm{Aut}(V_0 \otimes_{\mathbb{Q}} k)$ ; in particular, if  $V_\ell = V_0 \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ , then  $\mathrm{GL}_{V_0}(\mathbb{Q}_\ell) = \mathrm{Aut}(V_\ell)$ . If  $\varphi: H \rightarrow \mathrm{GL}_{V_0}$  is a homomorphism of linear algebraic groups over  $\mathbb{Q}$ , call  $\varphi_\ell$  the induced homomorphism of  $H(\mathbb{Q}_\ell)$  into  $\mathrm{GL}_{V_0}(\mathbb{Q}_\ell) = \mathrm{Aut}(V_\ell)$ . If  $\rho$  is an  $\ell$ -adic representation of  $\mathrm{Gal}(\bar{K}/K)$  into  $H(\mathbb{Q}_\ell)$ , one gets by composition a linear  $\ell$ -adic representation  $\varphi_\ell \circ \rho: \mathrm{Gal}(\bar{K}/K) \rightarrow \mathrm{Aut}(V_\ell)$ . Using the fact that the coefficients of the characteristic polynomial are central functions, one sees that  $\varphi_\ell \circ \rho$  is *rational* if  $\rho$  is rational ( $K$  a number field). Of course, compatible representations in  $H$  give compatible linear representations. We will use this method of constructing compatible representations in the case where  $H$  is abelian (see ch. ??, ??).

## §I.A. Equipartition and $L$ -functions

### I.A.1 Equipartition

Let  $X$  be a compact topological space and  $C(X)$  the Banach space of continuous, complex-valued, functions on  $X$ , with its usual norm  $\|f\| = \sup_{x \in X} |f(x)|$ . For each  $x \in X$  let  $\delta_x$  be the Dirac measure associated to  $x$ ; if  $f \in C(X)$ , we have  $\delta_x(f) = f(x)$ .

Let  $(x_n)_{n \geq 1}$  be a sequence of points of  $X$ . For  $n \geq 1$ , let

$$\mu_n = \frac{\delta_{x_1} + \cdots + \delta_{x_n}}{n}$$

and let  $\mu$  be a Radon measure on  $X$  (i.e. a continuous linear form on  $C(X)$ , cf. Bourbaki, Int., chap. III, §1). The sequence  $(x_n)$  is said to be  **$\mu$ -equidistributed**, or  *$\mu$ -uniformly distributed*, if  $\mu_n \rightarrow \mu$  weakly as  $n \rightarrow \infty$ , i.e. if  $\mu_n(f) \rightarrow \mu(f)$  as  $n \rightarrow \infty$  for any  $f \in C(X)$ . Note that this implies that  $\mu$  is positive and of total mass 1. Note also that  $\mu_n(f) \rightarrow \mu(f)$  means that

$$\mu(f) = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=1}^n f(x_i).$$

**Lemma 1.** *Let  $(\varphi_\alpha)$  be a family of continuous functions on  $X$  with the property that their linear combinations are dense in  $C(X)$ . Suppose that,*

for all  $\alpha$ , the sequence  $(\mu_n(\varphi_\alpha))_{n>1}$  has a limit. Then the sequence  $(x_n)$  is equidistributed with respect to some measure  $\mu$  it is the unique measure such that  $\mu(\varphi_\alpha) = \lim_{n \rightarrow \infty} \mu_n(\varphi_\alpha)$  for all  $\alpha$ .

If  $f \in C(X)$ , an argument using equicontinuity shows that the sequence  $(\mu_n(f))$  has a limit  $\mu(f)$ , which is continuous and linear in  $f$ ; hence the lemma.

**Proposition 1.** *Suppose that  $(x_n)$  is  $\mu$ -equidistributed. Let  $U$  be a subset of  $X$  whose boundary has  $\mu$ -measure zero, and, for all  $n$ , let  $n_U$  be the number of  $m \leq n$  such that  $x_m \in U$ . Then  $\lim_{n \rightarrow \infty} (n_U/n) = \mu(U)$ .*

Let  $\mathring{U}$  be the interior of  $U$ . We have  $\mu(\mathring{U}) = \mu(U)$ . Let  $\varepsilon > 0$ . By the definition of  $\mu(\mathring{U})$  there is a continuous function  $\varphi \in C(X)$ ,  $0 \leq \varphi \leq 1$ , with  $\varphi = 0$  on  $X \setminus \mathring{U}$  and  $\mu(\varphi) \geq \mu(U) - \varepsilon$ . Since  $\mu_n(\varphi) \leq n_U/n$  we have

$$\liminf_{n \rightarrow \infty} \frac{n_U}{n} \geq \lim_{n \rightarrow \infty} \mu_n(\varphi) = \mu(\varphi) \geq \mu(U) - \varepsilon,$$

from which we obtain  $\liminf n_U/n \geq \mu(U)$ . The same argument applied to  $X \setminus U$  shows that

$$\liminf_{n \rightarrow \infty} \frac{n - n_U}{n} \geq \mu(X \setminus U).$$

Hence  $\limsup_n n_U/n \leq \mu(U) \leq \liminf n_U/n$ , which implies the proposition.

**Examples.** 1. Let  $X = [0, 1]$ , and let  $\mu$  be the Lebesgue measure. A sequence  $(x_n)$  of points of  $X$  is  $\mu$ -equidistributed if and only if for each interval  $[a, b]$ , of length  $d > 0$  in  $[0, 1]$  the number of  $m \leq n$  such that  $x_m \in [a, b]$  is equivalent to  $dn$  as  $n \rightarrow \infty$ .

2. Let  $G$  be a compact group and let  $X$  be the space of conjugacy classes of  $G$  (i.e. the quotient space of  $G$  by the equivalence relation induced by inner automorphisms of  $G$ ). Let  $\mu$  be a measure on  $G$ ; its image of  $G \rightarrow X$  is a measure on  $X$ , which we also denote by  $\mu$ . We then have:

**Proposition 2.** *The sequence  $(x_n)$  of elements of  $X$  is  $\mu$ -equidistributed if and only if for any irreducible character  $\chi$  of  $G$  we have*

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=1}^n \chi(x_i) = \mu(\chi).$$

The map  $C(X) \rightarrow C(G)$  is an isomorphism of  $C(X)$  onto the space of central functions on  $G$ ; by the Peter-Weyl theorem, the irreducible characters  $\chi$  of  $G$  generate a dense subspace of  $C(X)$ . Hence the proposition follows from lemma ??.

**Corollary 2.1.** *Let  $\mu$  be the Haar measure of  $G$  with  $\mu(G) = 1$ . Then a sequence  $(x_n)$  of elements of  $X$  is  $\mu$ -equidistributed if and only if for any irreducible character  $\chi$  of  $G$ ,  $\chi \neq 1$  we have*

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=1}^n \chi(x_i) = 0.$$

This follows from Prop. ?? and the following facts:

$$\begin{aligned} \mu(\chi) &= 0 && \text{if } \chi \text{ is irreducible } \neq 1 \\ \mu(1) &= 1. \end{aligned}$$

**Corollary 2.2** (46 [46]). *Let  $G = \mathbb{R}/\mathbb{Z}$ , and let  $\mu$  be the normalized Haar measure on  $G$ . Then  $(x_n)$  is  $\mu$ -equidistributed if and only if for any integer  $m \neq 0$  we have*

$$\sum_{n \leq N} e^{2\pi m i x_n} = o(N) \quad (N \rightarrow \infty).$$

For the proof, it suffices to remark that the irreducible characters of  $\mathbb{R}/\mathbb{Z}$  are the mappings  $x \mapsto e^{2\pi m i x}$  ( $m \in \mathbb{Z}$ ).

### I.A.2 The connection with $L$ -functions

Let  $G$  and  $X$  be as in Example ?? above:  $G$  a compact group and  $X$  the space of its conjugacy classes. Let  $x_v, v \in M$ , be a family of elements of  $X$ , indexed by a denumerable set  $M$ , and let  $v \mapsto \mathbf{N}v$  be a function on  $M$  with values in the set of integers  $\geq 2$ . We make the following *hypotheses*:

- (1) The infinite product  $\prod_{v \in M} \frac{1}{1 - (\mathbf{N}v)^{-s}}$  converges for every  $s \in \mathbb{C}$  with  $\Re(s) > 1$ , and extends to a meromorphic function on  $\Re(s) > 1$  having neither zero nor pole except for a simple pole at  $s = 1$ .
- (2) Let  $\rho$  be an irreducible representation of  $G$ , with character  $\chi$ , and put

$$L(s, \rho) = \prod_{v \in M} \frac{1}{\det(1 - \rho(x_v)(\mathbf{N}v)^{-s})}.$$



Then this product converges for  $\Re(s) > 1$ , and extends to a meromorphic function on  $\Re(s) > 1$  having neither zero nor pole except possibly for  $s = 1$ .

The order of  $L(s, \rho)$  at  $s = 1$  will be denoted by  $-c_\chi$ . Hence, if  $L(s, \rho)$  has a pole (resp. a zero) of order  $m$  at  $s = 1$ , one has  $c_\chi = m$  (resp.  $c_\chi = -m$ ).

Under these assumptions, we have:

**Theorem 1.** (a) *The number of  $v \in M$  with  $\mathbf{N}v \leq n$  is equivalent to  $n/\log n$  (as  $n \rightarrow \infty$ ).*

(b) *For any irreducible character  $\chi$  of  $G$ , we have*

$$\sum_{\mathbf{N}v \leq n} \chi(x_v) = c_\chi \frac{n}{\log n} + o(n/\log n), \quad (n \rightarrow \infty).$$

The theorem results, by a standard argument, from the theorem of Wiener-Ikehara, cf. ?? below. Suppose now that the function  $v \mapsto \mathbf{N}v$  has the following property:

(3) *There exists a constant  $C$  such that, for every  $n \in \mathbb{Z}$ , the number of  $v \in M$  with  $\mathbf{N}v = n$  is  $\leq C$ .*

One may then arrange the elements of  $M$  as a sequence  $(v_i)_{i \geq 1}$ , so that  $i \leq j$  implies  $\mathbf{N}v_i \leq \mathbf{N}v_j$  (in general, this is possible in many ways). It then makes sense to speak about the equidistribution of the sequence of  $x_v$ 's; using (3), one shows easily that this does not depend on the chosen ordering of  $M$ . Applying theorem 1 and proposition 2, we obtain:

**Theorem 2.** *The elements  $x_v$  ( $v \in M$ ) are equidistributed in  $X$  with respect to a measure  $\mu$  such that for any irreducible character  $\chi$  of  $G$  we have*

$$\mu(\chi) = c_\chi.$$

**Corollary 2.1.** *The elements  $x_v$  ( $v \in M$ ) are equidistributed in  $X$  normalized Haar measure of  $G$  if and only if  $c_\chi = 0$  for every irreducible character  $\chi \neq 1$  of  $G$ , i.e., if and only if the  $L$ -functions relative to the non trivial irreducible characters of  $G$  are holomorphic and non zero at  $s = 1$ .*

**Examples.** 1) Let  $G$  be the Galois group of a *finite* Galois extension  $L/K$  of the number field  $K$ , let  $M$  be the set of unramified places of  $K$ , let  $x_v$  be the Frobenius conjugacy class defined by  $v \in M$ , and let  $\mathbf{N} v$  be the norm of  $v$ , cf. §??.

Properties (1), (2), (3) are satisfied with  $c_\chi = 0$  for all irreducible  $\chi \neq 1$ . This is trivial for (3). For (1), one remarks that  $L(s, l)$  is the zeta function of  $K$  (up to a finite number of terms), hence has a simple pole at  $s = 1$  and is holomorphic on the rest of the line  $\Re(s) = 1$ , cf. for instance **13** [13], chap. VII; for a proof of (2), cf. **1** [1]. Hence theorem 2 gives the equidistribution of the Frobenius elements, i.e. the Čebotarev density theorem, cf. 2.2.

2) Let  $C$  be the idèle class group of a number field  $K$ , and let  $\rho$  be a continuous homomorphism of  $C$  into a compact abelian Lie group  $G$ . An easy argument (cf. ch. III, 2.2) shows that  $\rho$  is almost everywhere unramified (i.e., if  $U_v$  denotes the group of units at  $v$ , then  $\rho(U_v) = 1$  for almost all  $v$ ). Choose  $\pi_v \in K$  with  $v(\pi_v) = 1$ . If  $\rho$  is unramified at  $v$ , then  $\rho(\pi_v)$  depends only on  $v$ , and we set  $x_v = \rho(\pi_v)$ . We make the following *assumption*:

(\*) *The homomorphism  $\rho$  maps the group  $C$  of idèles of volume 1 onto  $G$ .*

(Recall that the **volume** of an idèle  $\mathbf{a} = (a_v)$  is defined as the product of the normalized absolute values of its components  $a_v$ , cf. **13** [13] or **44** [44].)

Then, the elements  $x_v$  are *uniformly distributed* in  $G$  with respect to the normalized Haar measure. This follows from theorem 1 and the fact that the  $L$ -functions relative to the irreducible characters  $\chi$  of  $G$  are Hecke  $L$ -functions with Grössencharakteren; these  $L$ -functions are holomorphic and non-zero for  $\Re(s) \geq 1$  if  $\chi \neq 1$ , see [13], chap. VII.

**Remark.** This example (essentially due to Hecke) is given in Lang (*loc. cit.*, ch. VIII, §5) except that Lang has replaced the condition (\*) by the condition “ $\rho$  is surjective”, which is insufficient. This led him to affirm that, for example, the sequence  $(\log p)_p$  (and also the sequence  $(\log n)_n$ ) is uniformly distributed modulo 1; however, one knows that this sequence is not uniformly distributed for any measure on  $\mathbb{R}/\mathbb{Z}$  (cf. **22** [22]).

- 3) (Conjectural example). Let  $E$  be an elliptic curve defined over a number field  $K$  and let  $M$  be the set of finite places  $v$  of  $K$  such that  $E$  has good reduction at  $v$ , cf. 1.2 and chap. ?? . Let  $v \in M$ , let  $\ell \neq p_v$  and let  $F_v$  be the Frobenius conjugacy class of  $v$  in  $\text{Aut}(T_\ell(E))$ . The eigenvalues of  $F_v$  are algebraic numbers; when embedded into  $\mathbb{C}$  they give conjugate complex numbers  $\pi_v, \bar{\pi}_v$  with  $|\pi_v| = (\mathbf{N} v)^{1/2}$ . We may write then

$$\pi_v = (\mathbf{N} v)^{1/2} e^{i\phi_v}; \quad \bar{\pi}_v = (\mathbf{N} v)^{1/2} e^{-i\phi_v} \quad \text{with } 0 \leq \phi_v \leq \pi.$$

On the other hand, let  $G = \text{SU}(2)$  be the Lie group of  $2 \times 2$  unitary matrices with determinant 1. Any element of the space  $X$  of conjugacy classes of  $G$  contains a unique matrix of the form

$$\begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{pmatrix}, \quad 0 \leq \phi \leq \pi.$$

The image in  $X$  of the Haar measure of  $G$  is known to be  $\frac{2}{\pi} \sin^2 \phi d\phi$ . The irreducible representations of  $G$  are the  $m$ -th symmetric powers  $\rho_m$  of the natural representation  $\rho_1$  of degree 2.

Take now for  $x_v$  the element of  $X$  corresponding to the angle  $\phi = \phi_v$  defined above. The corresponding  $L$  function, relative to  $\rho_m$ , is:

$$L_{\rho_m}(s) = \prod_v \prod_{a=0}^{a=m} \frac{1}{1 - e^{i(m-2a)\phi_v} (\mathbf{N} v)^{-s}}.$$

If we put:

$$L_m^1(s) = \prod_v \prod_{a=0}^{a=m} \frac{1}{1 - \pi_v^{m-a} \bar{\pi}_v^a (\mathbf{N} v)^{-s}}$$

we have

$$L_{\rho_m}(s) = L_m^1(s - m/2).$$

The function  $L$  has been considered by **36** [36]. He conjectures that  $L_m^1$ , for  $m \geq 1$ , is holomorphic and non zero for  $\Re(s) \geq 1 + m/2$ , provided that  $E$  has no complex multiplication. Granting this conjecture, the corollary to theorem 2 would yield the uniform distribution of the  $x_v$ 's, or, equivalently, that the angles  $\phi_v$  of the Frobenius elements are uniformly distributed in  $[0, \pi]$  with respect to the measure  $\frac{2}{\pi} \sin^2 \phi d\phi$  ("conjecture of Sato-Tate").

One can expect analogous results to be true for other  $\ell$ -adic representations.

### I.A.3 Proof of theorem 1

The logarithmic derivative of  $L$  is

$$\frac{L'(s)}{L(s)} = - \sum_{\substack{v \geq 1 \\ m \geq 1}} \frac{\chi(x_v^m) \log(\mathbf{N} v)}{(\mathbf{N} v)^{ms}},$$

where  $x_v^m$  is the conjugacy class consisting of the  $m$ -th powers of elements in the class  $x_v$ . One sees this by writing  $L$  as the product

$$\prod_{j,v} \frac{1}{1 - \lambda_v^{(j)} (\mathbf{N} v)^{-s}}$$

where the  $\lambda_v^{(j)}$  are the eigenvalues of  $x_v$  in the given representation. Now the series

$$\sum_{\substack{v \geq 1 \\ m \geq 1}} \frac{\log(\mathbf{N} v)}{|(\mathbf{N} v)^{ms}|},$$

converges for  $\Re(s) > 1/2$ . Indeed it suffices to show that

$$\sum_v \frac{\log(\mathbf{N} v)}{(\mathbf{N} v)^\sigma} < \infty$$

if  $\sigma > 1$ ; but this series is majorized by

$$(\text{Constant}) \times \sum_v \frac{1}{(\mathbf{N} v)^{\sigma+\varepsilon}}, \quad (\varepsilon > 0).$$

On the other hand, the convergence for  $\sigma > 1$  of the product

$$\prod_v \frac{1}{1 - (\mathbf{N} v)^{-\sigma}}$$

shows that

$$\sum_v \frac{1}{(\mathbf{N} v)^\sigma} < \infty$$

for  $\sigma > 1$ ; hence our assertion. One can therefore write

$$\frac{L'(s)}{L(s)} = - \sum_v \frac{\chi(x_v) \log(\mathbf{N} v)}{(\mathbf{N} v)^s} + \phi(s)$$

where  $\phi(s)$  is holomorphic for  $\Re(s) > \frac{1}{2}$ . Moreover, by hypothesis,  $L'/L$  can be extended to a meromorphic function on  $\Re(s) \geq 1$  which is holomorphic except possibly for a simple pole at  $s = 1$  with residue  $-c_\chi$ . One may then apply the Wiener-Ikehara theorem (cf. [13]):

**Theorem 3.** *Let  $F(s) = \sum_{n=1}^{\infty} a_n/n^s$  be a Dirichlet series with complex coefficients. Suppose there exists a Dirichlet series  $F(s) = \sum_n a_n^+/n^s$  with positive real coefficients such that*

- (a)  $|a_n| \leq a_n^+$  for all  $n$ ;
- (b) The series  $F^+$  converges for  $\Re(s) > 1$ ;
- (c) The function  $F$  (resp.  $F^+$ ) can be extended to a meromorphic function on  $\Re(s) \geq 1$  having no poles except (resp. except possibly) for a simple pole at  $s = 1$  with residue  $c_+ > 0$  (resp.  $c$ ).

Then

$$\sum_{m \leq n} a_m = cn + o(n) \quad (n \rightarrow \infty),$$

(where  $c = 0$  if  $F$  is holomorphic at  $s = 1$ ).

One applies this theorem to

$$F(s) = - \sum_v \frac{\chi(x_v) \log(\mathbf{N} v)}{(\mathbf{N} v)^s},$$

and we take for  $F^+$  the series

$$d \sum_v \frac{\log(\mathbf{N} v)}{(\mathbf{N} v)^s},$$

where  $d$  is the degree of the given representation  $\rho$ ; this is possible since  $\chi(x_v)$  is a sum of  $d$  complex numbers of absolute value 1, hence  $|\chi(x_v)| \leq d$ ; moreover, the series

$$\sum_v \frac{\log(\mathbf{N} v)}{(\mathbf{N} v)^s}$$

differs from the logarithmic derivative of

$$\prod_v \frac{1}{1 - (\mathbf{N} v)^{-s}}$$

by a function which is holomorphic for  $\Re(s) > 1/2$  as we saw above. Hence by the Wiener-Ikehara theorem we have

$$\sum_{\mathbf{N}v \leq n} \chi(x_v) \log(\mathbf{N}v) = c_\chi n + o(n) \quad (n \rightarrow \infty).$$

Consequently, by the Abel summation trick (cf. [13], Prop. 1),

$$\sum_{\mathbf{N}v \leq n} \chi(x_v) = c_\chi \frac{n}{\log n} + o(n/\log n) \quad (n \rightarrow \infty).$$

and in particular,

$$\sum_{\mathbf{N}v \leq n} 1 = \frac{n}{\log n} + o(n/\log n) \quad (n \rightarrow \infty).$$

Hence,

$$\frac{\sum_{\mathbf{N}v \leq n} \chi(x_v)}{\sum_{\mathbf{N}v \leq n} 1} \longrightarrow c_\chi \quad \text{as } n \rightarrow \infty,$$

and we may apply proposition 2 to conclude the proof.

q.e.d.

## CHAPTER II

### $\ell$ -ADIC REPRESENTATIONS ATTACHED TO ELLIPTIC CURVES

Let  $K$  be a number field and let  $E$  be an elliptic curve over  $K$ . If  $\ell$  is a prime number, let

$$\rho_\ell: \text{Gal}(\overline{K}/K) \longrightarrow \text{Aut}(V_\ell(E))$$

be the corresponding  $\ell$ -adic representation of  $K$ , cf. chap. ??, ??. The main result of this Chapter is the determination of the Lie algebra of the  $\ell$ -adic Lie group  $G_\ell = \text{Im}(\rho_\ell)$ . This is based on a finiteness theorem of Šafarevič (1.4) combined with the properties of locally algebraic abelian representations (chap. III) and Tate's local theory of elliptic curves with non-integral modular invariant (Appendix, A1). The variation of  $G_\ell$  with  $\ell$  is studied in §??.

The Appendix gives analogous results in the local case (i.e. when  $K$  is a local field).

## §1. Preliminaries

### 1.1 Elliptic curves (cf. 5 [5], 9 [9], 10 [10])

By an elliptic curve, we mean an abelian variety of dimension 1, i.e. a complete, non singular, connected curve of genus 1 with a given rational point  $P_0$ , taken as an origin for the composition law (and often written  $o$ ).

Let  $E$  be such a curve. It is well known that  $E$  may be embedded, as a non-singular cubic, in the projective plane  $\mathbb{P}_K^2$ , in such a way that  $P_0$  becomes a “flex” (one takes the projective embedding defined by the complete linear series containing the divisor  $3 \cdot P_0$ ). In this embedding, three points  $P_1, P_2$ ,

$P_3$  have sum 0 if and only if the divisor  $P_1 + P_2 + P_3$  is the intersection of  $E$  with a line. By choosing a suitable coordinate system, the equation of  $E$  can be written in Weierstrass form

$$y^2 = 4x^3 - g_2x - g_3$$

where  $x, y$  are non-homogeneous coordinates and the origin  $P_0$  is the point at infinity on the  $y$ -axis. The discriminant

$$\Delta = g_2^3 - 27g_3^2$$

is non-zero.

The coefficients  $g_2, g_3$  are determined up to the transformations  $g_2 \mapsto u^4g_2, g_3 \mapsto u^6g_3, u \in K^\times$ . The modular invariant  $j$  of  $E$  is

$$j = 2^6 3^3 \frac{g_2^3}{g_2^3 - 27g_3^2} = 2^6 3^3 \frac{g_2^3}{\Delta}.$$

Two elliptic curves have the same  $j$  invariant if and only if they become isomorphic over the algebraic closure of  $K$ .

(All this remains valid over an arbitrary field, except that, when the characteristic is 2 or 3, the equation of  $E$  has to be written in the more general form

$$y^2 + a_1xy + a_3y + x^3 + a_2x^2 + a_4x + a_6 = 0.$$

Here again, 0 is the point at infinity on the  $y$ -axis and the corresponding tangent is the line at infinity. There are corresponding definitions for  $\Delta$  and  $j$ , for which we refer to **9** [9] or **20** [20]; note, however, that there is a misprint in Ogg's formula for  $\Delta$ : the coefficient of  $\beta_4^3$  should be  $-8$  instead of  $-1$ .)

## 1.2 Good reduction

Let  $v \in M_K^0$  be a finite place of the number field  $K$ . We denote by  $\mathcal{O}_v$  (resp.  $\mathfrak{m}_v, k_v$ ) the corresponding local ring in  $K$  (resp. its maximal ideal, its residue field).

Let  $E$  be an elliptic curve over  $K$ . One says that  $E$  has **good reduction at**  $v$  if one can find a coordinate system in  $\mathbb{P}_K^2$  such that the corresponding equation  $f$  for  $E$  has coefficient in  $\mathcal{O}_v$  and its reduction  $\tilde{f} \bmod \mathfrak{m}_v$  defines a



non-singular cubic  $\tilde{E}_v$  (hence an elliptic curve) over the residue field  $k_v$  (in other words, the discriminant  $\Delta(f)$  of  $f$  must be an invertible element of  $\mathcal{O}_v$ ). The curve  $\tilde{E}_v$  is called the **reduction** of  $E$  at  $v$ ; it does not depend on the choice of  $f$ , provided, of course, that  $\Delta(f) \in \mathcal{O}_v^\times$ .

One can prove that the above definition is equivalent to the following one: there is an abelian scheme  $E_v$  over  $\text{Spec}(\mathcal{O}_v)$ , in the sense of **19** [19], chap. VI, whose generic fiber is  $E$ ; this scheme is then unique, and its special fiber is  $\tilde{E}_v$ . Note that  $\tilde{E}_v$  is defined over the finite field  $k_v$ ; we denote its **Frobenius endomorphism** by  $F_v$ .

On either definition, one sees that  $E$  has **good reduction for almost all places of  $K$** .

If  $E$  has good reduction at a given place  $v$ , its  $j$  invariant is **integral at  $v$**  (i.e. belongs to  $\mathcal{O}_v$ ) and its reduction  $\tilde{j} \bmod \mathfrak{m}_v$  is the  $j$  invariant of the reduced curve  $\tilde{E}_v$ .

The converse is almost true, but not quite: if  $j$  belongs to  $\mathcal{O}_v$ , there is a finite extension  $L$  of  $K$  such that  $E \otimes_K L$  has good reduction at all the places of  $L$  dividing  $v$  (this is the “potential good reduction” of **32** [32], §2). For the proof of this, see **29** [29], §4, n° 3.

**Remark.** The definitions and results of this section have nothing to do with number fields. They apply to every field with a discrete valuation.

### 1.3 Properties of $V_\ell$ related to good reduction

Let  $\ell$  be a prime number. We define, as in chap. ??, ??, the Galois modules  $T_\ell$  and  $V_\ell$  by:

$$V_\ell = T_\ell \otimes \mathbb{Q}_\ell, \quad T_\ell = \varprojlim_n E_{\ell^n}$$

where  $E_{\ell^n}$  is the kernel of  $\ell^n: E(\overline{K}) \rightarrow E(\overline{K})$ .

We denote by  $\rho_\ell$  the corresponding homomorphism of  $\text{Gal}(\overline{K}/K)$  into  $\text{Aut}(T_\ell)$ . Recall that  $E_{\ell^n}$ ,  $T_\ell$  and  $V_\ell$  are of rank 2 over  $\mathbb{Z}/\ell^n\mathbb{Z}$ ,  $\mathbb{Z}_\ell$  and  $\mathbb{Q}_\ell$ , respectively.

Let now  $v$  be a place of  $K$ , with  $p_v \neq \ell$  and let  $\tilde{v}$  be some extension of  $v$  to  $\overline{K}$ ; let  $D$  (resp.  $I$ ) be the corresponding decomposition group (resp. inertia group), cf. chap. ??, 2.1. If  $E$  has good reduction at  $v$ , one easily sees that reduction at  $v$  defines an *isomorphism* of  $E_{\ell^n}$  onto the corresponding module for the reduced curve  $\tilde{E}_v$ . In particular,  $E_{\ell^n}$ ,  $T_\ell$ ,  $V_\ell$  are *unramified*

at  $v$  (chap. ??, 2.1) and the Frobenius automorphism  $F_{v,\rho_\ell}$  of  $T_\ell$  corresponds to the Frobenius endomorphism  $F_v$  of  $\tilde{E}_v$ . Hence:

$$\det(F_{v,\rho_\ell}) = \det(F_v) = \mathbf{N} v$$

and

$$\det(1 - F_{v,\rho_\ell}) = \det(1 - F_v) = 1 - \operatorname{tr}(F_v) + \mathbf{N} v$$

is equal to the number of  $k_v$ -points of  $\tilde{E}_v$ .

Conversely:

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

For the proof, see **32** [32], §1.

**Corollary 1.1.** *Let  $E$  and  $E'$  be two elliptic curves which are isogenous (over  $K$ ). If one of them has good reduction at a place  $v$ , the same is true for the other one.*

(Recall that  $E$  and  $E'$  are said to be **isogenous** if there exists a non-trivial morphism  $E \rightarrow E'$ .)

This follows from the theorem, since the  $\ell$ -adic representations associated with  $E$  and  $E'$  are isomorphic.

**Remark.** For a direct proof of this corollary, see **11** [11].

**Exercise.** Let  $S$  be the finite set of places where  $E$  does not have good reduction. If  $v \in M_K^0 \setminus S$ , we denote by  $t_v$  the number of  $k_v$ -points of the reduced curve  $\tilde{E}_v$ .

(a) Let  $\ell$  be a prime number and let  $m$  be a positive integer. Show that the following properties are equivalent:

- (i)  $t_v \equiv 0 \pmod{\ell^m}$  for all  $v \in M_K^0 \setminus S$ ,  $p_v \neq \ell$ .
- (ii) The set of  $v \in M_K^0 \setminus S$  such that  $t_v \equiv 0 \pmod{\ell^m}$  has density one (cf. chap. ??, 2.2).
- (iii) For all  $s \in \operatorname{Im}(\rho)$ , one has  $\det(1 - s) \equiv 0 \pmod{\ell^m}$ .

(The equivalence of ?? and ?? follows from Čebotarev's density theorem. The implications ??  $\implies$  ?? and ??  $\implies$  ?? are easy.)

(b) We take now  $m = 1$ . Show that the properties ??, ?? and ?? are equivalent to:

(iv) There exists an elliptic curve  $E'$  over  $K$  such that:

( $\alpha$ ) Either  $E'$  is isomorphic to  $E$ , or there exist an isogeny  $E' \rightarrow E$  of degree  $\ell$ .

( $\beta$ ) The group  $E'(K)$  contains an element of order  $\ell$ .

(The implication ??  $\implies$  ?? is easy. For the proof of the converse, use Exer. ?? of chap. ??, ??.) [For  $m > 2$ , see 64 [64].]

## 1.4 Šafarevič's theorem

It is the following (cf. [23]):

**Theorem 2.** *Let  $S$  be a finite set of places of  $K$ . The set of isomorphism classes of elliptic curves over  $K$ , with good reduction at all places not in  $S$ , is finite.*



## INDEX

$\mu$ -equidistributed, 8