Abelian ℓ-adic Representations and Elliptic Curves

Jean-Pierre Serre

June 13, 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**
Σ_K	M_K^0	Set of finite places of a number field K.
ℓ	λ	The residue field of a field L relative to a finite place.
R^*	$R^\times$	The group of units of a ring R.
U°	$\mathring{U}$	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.
$\mathrm{N}\,v$	$\mathbf{N}\,v$	$= [\mathcal{O}_v : \mathfrak{m}_v]$.
$\mathbb{G}_{m/K}$	$\mathbb{G}_{m,K}$	The multiplicative group of 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.

We also did some minor corrections and errata we found:

- Page **??** (I-3): it originally said "T'/T", and it should be "T/T'".
- Page **??** (IV-8): it originally said "$\Delta_v = u^{12}\Delta'$", and it should be "$\Delta_v = u_v^{12}\Delta'$".

CHAPTER I

ℓ-ADIC REPRESENTATIONS

§1. The notion of an ℓ-adic representation

1.1 Definition

Let K be a field, and let K_{s} be a separable algebraic closure of K. Let I-1
$G = \mathrm{Gal}(K_{\mathrm{s}}/K)$ be the Galois group of the extension K_{s}/K. The group G, with the Krull topology, is compact and totally disconnected. Let ℓ be a prime number, and let V be a finite-dimensional vector space over the field $\mathbb{Q}_\ell$ of ℓ-adic numbers. The full linear group $\mathrm{Aut}(V)$ is an ℓ-adic Lie group, its topology being induced by the natural topology of $\mathrm{End}(V)$; if $n = \dim(V)$, we have $\mathrm{Aut}(V) \cong \mathrm{GL}(n, \mathbb{Q}_\ell)$.

Definition 1.1. An ℓ-adic representation of $\mathfrak{G}$ (or, by abuse of language, of K) is a continuous homomorphism $\rho\colon G \to \mathrm{Aut}(V)$.

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 I-2
$g \in \mathfrak{G}$ such that $\rho(g)L = L$. This is an open subgroup of G, and G/H is finite. The lattice T generated by the lattices $\rho(g)L$, $g \in G/H$, is stable under G.

Notice that L may be identified with the projective limit of the free $(\mathbb{Z}/\ell\mathbb{Z})$-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 ρ is an ℓ-adic representation of $\mathfrak{G}$, the group $\mathfrak{G} = \mathrm{Im}(\rho)$ is a closed subgroup of $\mathrm{Aut}(V)$, and hence, by the ℓ-adic analogue of Cartan's theorem (cf. [**28**]) $\mathfrak{G}$ is itself an ℓ-adic Lie group. Its Lie algebra $\mathfrak{g} = \mathrm{Lie}(\mathfrak{G})$ is a subalgebra of $\mathrm{End}(V) = \mathrm{Lie}(\mathrm{Aut}(V))$. 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 $\mathrm{Aut}(V)$. 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 $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$ or in the subgroup $\left(\begin{smallmatrix} 1 & 0 \\ * & * \end{smallmatrix}\right)$ of $\mathrm{Aut}(V)$.

2) Let $\rho\colon G \to \mathrm{Aut}(V_\ell)$ be an ℓ-adic representation of $\mathfrak{G}$, where V_ℓ is a $\mathbb{Q}_\ell$-vector space of dimension 2. Assume $\det(1-\rho(s)) = 0 \mod \ell$ for all $s \in G$. Let T be a lattice of V_ℓ stable by G. Show the existence of a lattice T' of V_ℓ with the following two properties:

   (a) T' is stable by G.

   I-3 (b) Either T' is a sublattice of index ℓ of T and G acts trivially on T/T' or T is a sublattice of index ℓ of T' and G acts trivially on T/T'.

   (Apply exercise **??** above to $k = F_\ell$ and $V = T/\ell T$.)

3) Let ρ be a semi-simple ℓ-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 ρ to U is semi-simple and use Kolchin's theorem to bring it to triangular form.)

4) Let $\rho\colon G \to \mathrm{Aut}(V_\ell)$ be an ℓ-adic representation of G, and T a lattice of V_ℓ stable under G. Show the equivalence of the following properties:

   (a) The representation of G in the F_ℓ-vector space $T/\ell T$ is irreducible.

   (b) The only lattices of V_ℓ stable under G are the $\ell^n T$, with $n \in \mathbb{Z}$.

1.2 Examples

Roots of unity. Let $\ell \neq \operatorname{char}(K)$. The group $\mathfrak{G} = \operatorname{Gal}(K_{\mathrm{s}}/K)$ acts on the group μ_m of ℓ^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 $\chi_\ell \colon \mathfrak{G} \to \operatorname{Aut}(V_\ell) = \mathbb{Q}_\ell^\times$ defined by the action of $\mathfrak{G}$ on V_ℓ is a 1-dimensional ℓ-adic representation of $\mathfrak{G}$. The character χ_ℓ takes its values in the group of units U of $\mathbb{Z}_\ell$; by definition

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

Elliptic curves. Let $\ell \neq \operatorname{char}(K)$. Let E be an elliptic curve defined over K with a given rational point o. One knows that there is a unique structure I-4 of group variety on E with o as neutral element. Let E_m be the kernel of multiplication by ℓ^m in $E(K_{\mathrm{s}})$, and let

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

The Tate module $T_\ell(E)$ is a free $\mathbb{Z}_\ell$-module on which $\mathfrak{G} = \operatorname{Gal}(K_{\mathrm{s}}/K)$ acts (cf. [**12**], chap. VII). The corresponding homomorphism $\pi_\ell \colon \mathfrak{G} \to \operatorname{Aut}(V_\ell(E))$ is an ℓ-adic representation of $\mathfrak{G}$. The group $G_\ell = \operatorname{Im}(\pi_\ell)$ is a closed subgroup of $\operatorname{Aut}(T_\ell(E))$, a 4-dimensional Lie group isomorphic to $\operatorname{GL}(2, \mathbb{Z}_\ell)$. (In chapter IV, we will determine the Lie algebra of G_ℓ, 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

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

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

Abelian varieties. Let A be an abelian variety over K of dimension d. If $\ell \neq \operatorname{char}(K)$, 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 $\mathfrak{G} = \operatorname{Gal}(K_{\mathrm{s}}/K)$ acts.

Cohomology representations. Let X be an algebraic variety defined over the field K, and let $X_{\mathrm{s}} = X \times_K K_{\mathrm{s}}$ be the corresponding variety over K_{s}. Let $\ell \neq \mathrm{char}(K)$, and let i be an integer. Using the étale cohomology of **3** [**3**] we let

$$H^i(X_{\mathrm{s}}, \mathbb{Z}_\ell) = \varprojlim_n H^i((X_{\mathrm{s}})_{\text{ét}}, \mathbb{Z}/\ell^n\mathbb{Z}), \qquad H^i_\ell(X_{\mathrm{s}}) = H^i(X_{\mathrm{s}}, \mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

I-5 The group $H^i_\ell(X_{\mathrm{s}})$ is a vector space over $\mathbb{Q}_\ell$ on which $G = \mathrm{Gal}(K_{\mathrm{s}}/K)$ acts (via the action of G on X_{s}). It is finite dimensional, at least if $\mathrm{char}(K) = 0$ or if X is proper. We thus get an ℓ-adic representation of G associated to $H^i_\ell(X_{\mathrm{s}})$; by taking duals we also get homology ℓ-adic representations. Examples 1, 2, 3 are particular cases of homology ℓ-adic representations where $i = 1$ and X is respectively the multiplicative group $\mathbb{G}_m$, 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 $G_\ell = \mathrm{SL}(T_\ell(E))$ (cf. **10** [**10**] for an algebraic proof).

(c) Using **??**, show that, over K_0, we have $G_\ell = \mathrm{GL}(T_\ell(E))$.

(d) Show that for any closed subgroup H of $\mathrm{GL}(2, \mathbb{Z}_\ell)$ there is an elliptic curve (defined over some field) for which $G_\ell = H$.

§2. ℓ-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^0_K 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 $v \in M^0_K$ is a finite field with $\mathbf{N}(v) = p_v^{\deg(v)}$ elements, where $p_v = \mathrm{char}(k_v)$ and $\deg(v)$ is the I-6 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 $D_w = \mathrm{Gal}(L_w/K_v)$. The group D_w is mapped homomorphically onto the Galois group $\mathrm{Gal}(\lambda_w/k_v)$ of the corresponding residue extension λ_w/k_v. The kernel of $G \to \mathrm{Gal}(\lambda_w/k_v)$ 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_α 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 $G = \mathrm{Gal}(L/K)$.

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

If the representation ρ is unramified at v, then the restriction of ρ to D_w I-7
factors through D_w/I_w for any $w \mid v$; hence $\rho(F_w) \in \mathrm{Aut}(V)$ is defined; we call $\rho(F_w)$ the ***Frobenius*** of w in the representation ρ, and we denote it by $F_{w,\rho}$. The conjugacy class of $F_{w,\rho}$ in $\mathrm{Aut}(V)$ depends only on v; it is denoted by $F_{v,\rho}$. If L/K is the extension of K corresponding to $H = \mathrm{Ker}(\rho)$, then ρ 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

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

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.

I-8 **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* $\operatorname{Card}(X)/\operatorname{Card}(G)$.

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 $\operatorname{Gal}(L/K)$.

b) Let K be a subset of $\operatorname{Gal}(L/K)$, *stable by conjugation. Assume that the boundary of X has measure zero with respect to the Haar measure μ of X, and normalize μ 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 neghborhood of a given class of $\operatorname{Gal}(L/K)$.

Exercise. Let G be an ℓ-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 I-9 G). Show that the boundary of X has measure zero with respect to the Haar measure of G.

2.3 Rational ℓ-adic representations

Let ρ be an ℓ-adic representation of the number field K. If $v \in M_K^0$, and if v is unramified with respect to ρ, we let $P_{v,\rho}(T)$ denote the polynomial $\det(1 - F_{v,\rho}T)$.

The ℓ-adic representation ρ is said to be rational (resp. integral) if there exists a finite subset S of M_K^0 such that

(a) Any element of $M_K^0 - S$

♡ Ver si la notación de eliminar conjunto está bien

(b)

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 $\rho \colon \mathrm{Gal}(K_{\mathrm{s}}/K) \to H(\mathbb{Q}_\ell)$ is called an ℓ-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 ℓ-adic Lie group.)

If K is a number field, one defines in an obvious way what it means for I-10 ρ 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 ρ is ***rational*** if

(a) there is a finite set S of M_K^0 such that ρ is unramified outside S,

(b) if $v \notin S$, the conjugacy class $F_{v,\rho}$ is rational over $\mathbb{Q}$.

Two rational representations ρ, $\rho^{'}$ (for primes ℓ, $\ell^{'}$) are said to be ***compatible*** if there exists a finite subset S of M_K^0 such that ρ 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 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 $\varphi \colon H \to \mathrm{GL}_{V_0}$ is a homomorphism of linear algebraic groups over $\mathbb{Q}$, call φ_ℓ the induced homomorphism of $\underline{H}(\mathbb{Q}_\ell)$ into $\mathrm{GL}_{V_0}(\mathbb{Q}_\ell) = \mathrm{Aut}(V_\ell)$. If ρ is an ℓ-adic representation of $\mathrm{Gal}(\overline{K}/K)$ into $H(\mathbb{Q}_\ell)$, one gets by composition a linear ℓ-adic representation $\varphi_\ell \circ \rho \colon \mathrm{Gal}(K_{\mathrm{s}}/K) \to \mathrm{Aut}(V_\ell)$. Using the fact that the coefficients of the I-11 characteristic polynomial are central functions, one sees that $\varphi_\ell \circ \rho$ is *rational* if ρ 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 δ_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 μ 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 ***μ-equidistributed***, or *μ-uniformly distributed*, if $\mu_n \to \mu$ *weakly* as $n \to \infty$, i.e. if $\mu_n(f) \to \mu(f)$ as $n \to \infty$ for any $f \in C(X)$. Note that this implies that μ is positive and of total mass 1. Note also that $\mu_n(f) \to \mu(f)$ means that

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

Lemma 1. *Let (φ_α) be a family of continuous functions on X with the property that their linear combinations are dense in $C(X)$. Suppose that, for all α, the sequence $(\mu_n(\varphi_\alpha))_{n>1}$ has a limit. Then the sequence (x_n) is equidistributed with respect to some measure μ it is the unique measure such that $\mu(\varphi_\alpha) = \lim_{n\to\infty} \mu_n(\varphi_\alpha)$ for all α.*

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

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

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

from which we obtain $\liminf n_U/n \ge \mu(U)$. The same argument applied to $X \setminus U$ shows that I-12

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

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

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

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 μ be a measure on G; its image of $G \to X$ is a measure on X, which we also denote by μ. We then have:

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

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

The map $C(X) \to C(G)$ is an isomorphism of $C(X)$ onto the space of I-13 central functions on G; by the Peter-Weyl theorem, the irreducible characters χ of G generate a dense subspace of $C(X)$. Hence the proposition follows from lemma **??**.

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

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

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

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

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

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

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 I-14 values in the set of integers ≥ 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 ρ be an irreducible representation of G, with character χ, 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 $\mathbf{N}\,v \le n$ is equivalent to $n/\log n$ (as $n \to \infty$).*

(b) For any irreducible character χ of G, we have

$$\sum_{\mathbf{N}\,v\le n}\chi(x_v) = c_\chi\frac{n}{\log n} + o(n/\log n), \qquad (n\to\infty).$$

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: I-15

(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 $\le C$.

One may then arrange the elements of M as a sequence $(v_i)_{i\ge 1}$. so that $i \le j$ implies $\mathbf{N}\,v_i \le \mathbf{N}\,v_j$ (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 μ such that for any irreducible character χ 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 $\Re(s) = 1$, I-16 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 ρ be a continuous homomorphism of C into a compact abelian Lie group G. An easy argument (cf. ch. III, 2.2) shows that ρ 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 ρ 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 ρ maps the group C of idèles of volume 1 onto G.*

(Recall that the ***volume*** of an idèle $\vec{a} = (a_v)$ 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 χ of G are Hecke L-functions with Grössencharakters; 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 "ρ 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 I-17 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 $\mathrm{Aut}(T_\ell(E))$. The eigenvalues of F_v are algebraic numbers; when embedded into $\mathbb{C}$ they give conjugate complex numbers π_v, $\bar{\pi}_v$ with $|\pi_v| = (\mathbf{N}\,v)^{1/2}$. We may write then

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

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

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

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

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

we have I-18

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

The function L has been considered by **36** [**36**]. He conjectures that L^1_m, 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 ϕ_v of the Frobenius elements are uniformly distributed in $[0,\pi]$ with respect to the measure $\frac{2}{\pi}\sin^2\phi\,\mathrm{d}\phi$ ("conjecture of Sato-Tate").

One can expect analogous results to be true for other ℓ-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

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

I-19 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

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

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 I-20
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

$$\sum_{m \leq n} a_n = cn + o(n) \qquad (n \to \infty),$$

(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 ρ; this is possible since I-21

$\chi(x_v)$ 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 $\mathfrak{R}(s) > 1/2$ as we saw above. Hence by the Wiener-Ikehara theorem we have

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

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

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

and in particular,

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

Hence,

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

and we may apply proposition 2 to conclude the proof. q.e.d.

CHAPTER II

THE GROUPS S_m

Throughout this chapter, K denotes an algebraic number field. We associate to K a projective family (S_m) of commutative algebraic groups over $\mathbb{Q}$, and we show that each S_m gives rise to a strictly compatible system of rational ℓ-adic representations of K. II-1

In the next chapter, we shall see that all "locally algebraic" abelian rational representations are of the form described here.

§1. Preliminaries

1.1 The torus $\mathbb{T}$

Let $\mathbb{T} = \mathfrak{R}_{K/\mathbb{Q}}(\mathbb{G}_{m,K})$ be the algebraic group over $\mathbb{Q}$, obtained from the multiplicative group $\mathbb{G}_m$ by restriction of scalars from K to $\mathbb{Q}$, cf. **43** [**43**], §1.3. If A is a commutative $\mathbb{Q}$-algebra, the points of $\mathbb{T}$ with values in A form by definition the multiplicative group $(K \otimes_{\mathbb{Q}} A)^{\times}$ of invertible elements of $K \otimes_{\mathbb{Q}} A$. In particular, $\mathbb{T}(\mathbb{Q}) = K^{\times}$. If $d = [K : \mathbb{Q}]$, the group $\mathbb{T}$ is a torus of dimension d; this means that the group $\mathbb{T}_{/\overline{\mathbb{Q}}} = \mathbb{T} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$ obtained from $\mathbb{T}$ by extending the scalars from $\mathbb{Q}$ to $\overline{\mathbb{Q}}$, is isomorphic to... II-2

Belen

1.2 Cutting down $\mathbb{T}$

Let E be a subgroup of $K = \mathbb{T}(\mathbb{Q})$ and let $\overline{E}$ be the Zariski closure of E in $\mathbb{T}$. Using the formula $\overline{E} \times \overline{E} = \overline{E \times E}$, one sees that E is an algebraic subgroup of $\mathbb{T}$. Let $\mathbb{T}_E$ be the quotient group $\mathbb{T}/E$; then $\mathbb{T}_E$ is also a torus over $\mathbb{Q}$. Its character group $X_E = X(\mathbb{T}_E)$ is the subgroup of $X = X(T)$ consisting of those characters which take the value 1 on E. If $\lambda = \prod_{\sigma\in\Gamma}[\sigma]^{n_\sigma}$ denotes a character of $\mathbb{T}$, then X_E is the subgroup of those $\lambda \in X$ for which $\prod_{\sigma\in\Gamma}[\sigma]^{n_\sigma} = 1$, for all $x \in E$.

Exercise.

a. Let K be quadratic over $\mathbb{Q}$, so that $\dim T = 2$. Let E be the group of units of K. Show that T is of dimension 2 (resp. 1) if K is imaginary (resp. real).

b. Take for K a cubic field with one real place and one complex one, and let again E be its group of units (of rank 1). Show that $\dim T = 3$ and $\dim T_E = 1$.

II-3 (For more examples, see 3.3.)

1.3 Enlarging groups

Belen

CHAPTER III

ℓ-ADIC REPRESENTATIONS ATTACHED TO ELLIPTIC CURVES

Let K be a number field and let E be an elliptic curve over K. If ℓ is a prime number, let III-1

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

be the corresponding ℓ-adic representation of K, cf. chap. **??**, **??**. The main result of this Chapter is the determination of the Lie algebra of the ℓ-adic Lie group $G_\ell = \mathrm{Im}(\rho_\ell)$. 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, Al). The variation of G_ℓ with ℓ is studied in §**??**.

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

§1. Preliminaries

III-2

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 $\mathbb{P}^2_K$, 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

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

III-3 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 Δ and j, for which we refer to **9** [**9**] or **20** [**20**]; note, however, that there is a misprint in Ogg's formula for Δ: the coefficient of β_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 $\tilde{f}$ mod $\mathfrak{m}_v$ defines a non-singular cubic $\widetilde{E}_v$ (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
4 $\mathcal{O}_v$). The curve $\widetilde{E}_v$ 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 $\operatorname{Spec}(\mathcal{O}_v)$, in the sense of **19** [**19**], chap. VI, whose generic fiber is E; this scheme is then unique, and its special fiber is $\widetilde{E}_v$. Note that $\widetilde{E}_v$ 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 $\tilde{\jmath}$ mod $\mathfrak{m}_v$ is the j invariant of the reduced curve $\widetilde{E}_v$.

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_ℓ related to good reduction

Let ℓ be a prime number. We define, as in chap. **??**, **??**, the Galois modules T_ℓ and V_ℓ by:

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

where E_{ℓ^n} is the kernel of $\ell^n \colon E(\overline{K}) \to E(\overline{K})$. III-5

We denote by ρ_ℓ the corresponding homomorphism of $\operatorname{Gal}(\overline{K}/K)$ into $\operatorname{Aut}(T_\ell)$. Recall that E_{ℓ^n}, T_ℓ and V_ℓ 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 $\underline{v}$ 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_{ℓ^n} onto the corresponding module for the reduced curve $\widetilde{E}_v$. In particular, E_{ℓ^n}, T_ℓ, V_ℓ are *unramified at v* (chap. **??**, 2.1) and the Frobenius automorphism F_{v,ρ_ℓ} of T_ℓ corresponds to the Frobenius endomorphism F_v of $\widetilde{E}_v$. Hence:

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

and

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

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

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.*

III-6 (Recall that E and $E^{'}$ are said to be ***isogenous*** if there exists a non-trivial morphism $E \to E^{'}$.)

This follows from the theorem, since the ℓ-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 $\widetilde{E}_v$.

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

(i) $t_v \equiv 0 \mod \ell^m$ 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 $t_v \equiv 0 \mod \ell^m$ has density one (cf. chap. **??**, 2.2).

(iii) For all $s \in \mathrm{Im}(\rho)$, one has $\det(1 - s) \equiv 0 \mod \ell^m$.

(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:

(α) Either E' is isomorphic to E, or there exist an isogeny $E' \to E$ of degree ℓ.

(β) The group $E'(K)$ contains an element of order ℓ.

(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**]): III-7

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.*

Since isogenous curves have the same bad reduction set (cf. 1.3), this implies:

Corollary 2.1. *Let E be an elliptic curve over K. Then, up to isomorphism, there are only a finite number of elliptic curves which are K-isogenous to E.*

To prove the theorem, we use the following criterion for good reduction:

Lemma 1. *Let S be a finite set of places of K containing the divisors of 2 and 3, and such that the ring $\mathcal{O}_S$ of S-integers is principal. Then, an elliptic curve E defined over K has good reduction outside S if and only if its equation can be put in the Weierstrass form $y^2 = 4x^3 - g_2x - g_3$ with $g_i \in \mathcal{O}_S$ and $\Delta = g_2^3 - 27g_2^3 \in \mathcal{O}_S^\times$ (the group of units of $\mathcal{O}_S$).*

Proof. The sufficiency is trivial. To prove necessity, we write the curve E in the form

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

with $g_i' \in K$. Let v be a place of K not in S. Then, since there is good reduction at v, and since the divisors of 2 and 3 do not belong to S, the III-8 curve E can be written in the form

$$y^2 = 4x^3 - g'_{2,v}x - g'_{3,v}$$

with $g_{i,v}$ in the local ring at v and the discriminant Δ_v a unit in this ring. Using the properties of the Weierstrass form, there is an element $u_v \in K$ such that $g_{2,v} = u_v^4 g'_2$, $g_{3,v} = u_v^6 g'_3$, $\Delta_v = u_v^{12}\Delta'$; moreover, as we can take $g_{i,v} = g'_i$ for almost all v, we see that we can assume that $u_v = 1$ for almost all $v \notin S$. Since the ring $\mathcal{O}_S$ is principal, there is an element $u \in K^\times$ with $v(u) = v(u_v)$ for all $v \notin S$. Then, if we replace x by $u^{-2}x$ and y by $u^{-3}y$ in (**??**), the curve E takes the form

$$y^2 = 4x^3 - g'_2x - g'_3$$

with $g_2 = u^4 g'_2$, $g_3 = u^6 g'_3$ and $\Delta = u^{12}\Delta'$. Since, by construction, $g_i \in \mathcal{O}_S$ and $\Delta \in \mathcal{O}_S^\times$ the lemma is established. □

Proof of the theorem. After possibly adding a finite number of places of K to S, we may assume that S contains all the divisors of 2 and 3, and that the ring $\mathcal{O}_S$ is principal. If E is an elliptic curve defined over K having good reduction outside S, the above lemma tells us that we can write E in the form

$$y^2 = 4x^3 - g'_2x - g'_3 \qquad (*)$$

with $g_i \in \mathcal{O}_S$ and $\Delta = g_2^3 - 27g_2^3 \in \mathcal{O}_S$. But, since we are free to 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, we see that there is a finite set $X \subset \mathcal{O}_S^\times$ such that any elliptic curve of the above type can be written in the form (**??**) with $g_i \in \mathcal{O}_S$ and $\Delta \in X$. But, for a given Δ, the equation III-9

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

represents an affine elliptic curve. Using a theorem of Siegel (generalized by Mahler and Lang, cf. **14** [**14**], chap. VII), one sees that this equation has only a *finite* number of solutions in $\mathcal{O}_S$. This finishes the proof of the theorem. □

Remark. There are many ways in which one can deduce Šafarevič's theorem from Siegel's. The one we followed has been shown to us by Tate.

§2. The Galois module attached to E

In this section, E denotes an elliptic curve over K. We are interested in the structure of the Galois modules E_{ℓ^n}, T_ℓ, V_ℓ defined in **??**.

2.1 The irreducibility theorem

Recall first that the ring $\mathrm{End}_K(E)$ of K-endomorphisms of E is either $\mathbb{Z}$ or of rank 2 over $\mathbb{Z}$. In the first case, we say that E has "no complex multiplication over K." If the same is true for any finite extension of K, we say that E has "no complex multiplication."

Theorem 1. *Assume that E has no complex multiplication over K. Then:* III-10

(a) V_ℓ is irreducible for all primes ℓ;

(b) E_ℓ is irreducible for almost all primes ℓ.

We need the following elementary result:

Lemma 1. *Let E be an elliptic curve defined over K with* $\mathrm{End}_K(E) = \mathbb{Z}$. *Then, if $E' \to E$, $E'' \to E$ are K-isogenies with non-isomorphic cyclic kernels, the curves E' and E'' are non-isomorphic over K.*

Proof. Let n' and n'' be respectively the orders of the kernels of $E' \to E$ and $E'' \to E$. Suppose that E' and E'' are isomorphic over K, and let $E' \to E''$ be an isomorphism. If $E \to E'$ is the transpose of the isogeny $E' \to E$, it has a cyclic kernel of order n', and hence the isogeny $E \to E$, obtained by composition of $E \to E'$, $E' \to E''$, $E'' \to E$, has for kernel an extension of $\mathbb{Z}/n''\mathbb{Z}$ by $\mathbb{Z}/n'\mathbb{Z}$. But, since $\mathrm{End}_K(E) = \mathbb{Z}$, this isogeny must be multiplication by an integer a, and its kernel must therefore be of the form $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z}$. Hence n' and n'' divide a. Since $a^2 = n'n''$, we obtain $a = n' = n''$, a contradiction. □

Proof of the theorem.

(a) It suffices to show that, if $\mathrm{End}_K(E) = \mathbb{Z}$, there is no one-dimensional $\mathbb{Q}_\ell$-subspace of V_ℓ stable under $\mathrm{Gal}(\overline{K}/K)$. Suppose there were one; its intersection X with T_ℓ would be a submodule of T_ℓ with X and T_ℓ/X free Z_ℓ-modules of rank 1. For $n \geq 0$, consider the image $X(n)$ of X in $E_{\ell^n} = T/\ell^n T$. This is a submodule of E_ℓ which is cyclic of order ℓ^n and stable by $\mathrm{Gal}(\overline{K}/K)$. Hence it corresponds to a finite K-algebraic subgroup of E and one can define the quotient curve $E(n) = E/X(n)$. III-11
The kernel of the isogeny $E \to E(n)$ is cyclic of order ℓ^n. The above lemma then shows that the curves $E(n)$, $n \geq 0$, are pairwise non-isomorphic, contradicting the corollary to Šafarevič's theorem (**??**).

(b) If E is not irreducible, there exists a Galois submodule X of E which is one-dimensional over ${}_{\ell}$. In the same way as above, this defines an isogeny $E \to E/X_\ell$ whose kernel is cyclic of order ℓ. The above lemma shows that the curves which correspond to different values of ℓ are non-isomorphic, and one again applies the corollary to Šafarevič's theorem. □

Remark. One can prove part **??** of the above theorem by a quite different method (cf. [**25**], §3.4); instead of the Šafarevič's theorem, one uses the properties of the decomposition and inertia subgroups of $\mathrm{Im}(\rho_\ell)$, cf. Appendix.

INDEX

Equidistribution, 8