Abelian ℓ-adic Representations and Elliptic Curves

Jean-Pierre Serre

June 15, 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 2 (I-3): it originally said "T'/T", and it should be "T/T'".
- Page 38 (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 1 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

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

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

2. Elliptic curves. Let $\ell \neq \mathrm{char}(K)$. Let E be an elliptic curve defined over K with a given rational point o. One knows that there is a unique I-4
structure of group variety on E with o as neutral element. Let E_m be the kernel of multiplication by ℓ^m in $E(K_s)$, 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 $G = \mathrm{Gal}(K_s/K)$ acts (cf. [**12**], chap. VII). The corresponding homomorphism $\pi_\ell \colon G \to \mathrm{Aut}(V_\ell(E))$ is an ℓ-adic representation of G. The group $G_\ell = \mathrm{Im}(\pi_\ell)$ is a closed subgroup of $\mathrm{Aut}(T_\ell(E))$, a 4-dimensional Lie group isomorphic to $\mathrm{GL}(2, \mathbb{Z}_\ell)$. (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

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

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

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

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

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

I-5 The group $H^i_\ell(X_s)$ is a vector space over $\mathbb{Q}_\ell$ on which $G = \mathrm{Gal}(K_s/K)$ 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 $H^i_\ell(X_s)$; 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 (b), 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_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
I-6 field with $\mathbf{N}(v) = p_v^{\deg(v)}$ elements, where $p_v = \mathrm{char}(k_v)$ 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 $D_w = \mathrm{Gal}(L_w/K_v)$. 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 $\mathbf{N}\, v \le n$. 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.

Theorem 1. *Let L be a finite Galois extension of the number field K, with*
I-8 *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 $M_K^0 \setminus S$.

♡ 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, ρ' (for primes ℓ, ℓ') are said to be ***compatible*** if there exists a finite subset S of M_K^0 such that ρ and ρ' 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 (b) 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 $H(\mathbb{Q}_\ell)$ 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. **??**, 2.5).

§A. Equipartition and L-functions

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 $\mathring{U}$ 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 $\varphi \in C(X)$, $0 \le \varphi \le 1$, with $\varphi = 0$ on $X \setminus \mathring{U}$ 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 I-12
$X \setminus U$ shows that

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

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 1.

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. 2 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 $x \mapsto e^{2\pi m i x}$ $(m \in \mathbb{Z})$.

A.2 The connection with L-functions

Let G and X be as in Example 2 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 $(v_i)_{i\ge1}$. 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. §2.1.

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
I-16 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 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 $\boldsymbol{a} = (a_v)$ 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. III. 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.

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 $\Re(s) > 1/2$ as we saw above. Hence by the Wiener-Ikehara theorem we have

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

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 $S_{\mathfrak{m}}$

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

§2. Construction of $T_\mathfrak{m}$ and $S_\mathfrak{m}$

2.1 Idèles and idèles-classes

We defined in Chapter I, 2.1 the set M_K^0 of finite places of the number field K. Let now M_K^∞ be the set of equivalence classes of archimedean absolute values of K, and let M_K be the union of M_K and M_K^∞. If $v \in M_K$ then K_v denotes the *completion* of K with respect to v. For $v \in M_K^\infty$ we have $K_v = \mathbb{R}$ or $K_v = \mathbb{C}$, and K is ultrametric if $v \in M_K^0$. For $v \in M_K^0$, the group of units of K_v is denoted by U_v. The ***idèle group*** I of K is the subgroup of

$$\prod_{v\in M_K} K_v^\times,$$

consisting of the families (a_v) with $a_v \in U_v$, for almost all $v \in M_K^0$; it is given a topology by decreeing that the subgroup (with the product topology)

$$\prod_{v\in M_K^\infty} K_v^\times \times \prod_{v\in M_K^0} U_v$$

be open. We embed $K^\times$ into I by sending $a \in K^\times$ onto the idèle (a_v), where $a_v = a$ for all v. The topology induced on K is the discrete topology. The quotient group $C_K = I/K^\times$ is called the ***idèle class group*** of K. (For all this, see **6** [**6**], **13** [**13**] or **44** [**44**].)

Let S be a finite subset of M_K^0. Then by a ***modulus of support*** S we mean a family $\mathfrak{m} = (m_v)_{v\in S}$ where the m_v are integers ≥ 1. If $v \in M_K$ and $\mathfrak{m}$ is a modulus of support S, we let $U_{v,\mathfrak{m}}$ denote the connected component of $K_v^\times$ if $v \in M_K^\infty$, the subgroup of U_v consisting of those $u \in U_v$ for which $v(1-u) \geq m_v$ if $v \in S$, and U_v if $v \in M_K^0 \setminus S$. The group $U_{\mathfrak{m}} = \prod_v U_{v,\mathfrak{m}}$ is an *open subgroup* of I. If E is the group of units of K, let $E_{\mathfrak{m}} = E \cap U_{\mathfrak{m}}$. The subgroup $E_{\mathfrak{m}}$ is of finite index in E. (Conversely, by a theorem of Chevalley ([**8**], see also [**24**], n° 3.5) every subgroup of finite index in E contains an $E_{\mathfrak{m}}$ for a suitable modulus $\mathfrak{m}$.) II-4

Let $I_{\mathfrak{m}}$ be the quotient $I/U_{\mathfrak{m}}$ and $C_{\mathfrak{m}}$ the quotient $I/K^\times U_{\mathfrak{m}} = C/$(Image of $U_{\mathfrak{m}}$ in $C_{\mathfrak{m}}$). One then has the exact sequence:

$$1 \longrightarrow K^\times/E_{\mathfrak{m}} \longrightarrow I_{\mathfrak{m}} \longrightarrow C_{\mathfrak{m}} \longrightarrow 1$$

The group $C_{\mathfrak{m}}$ is finite; in fact, the image of $U_{\mathfrak{m}}$ in C is open, hence contains the connected component D of C, and the group C/D is known to be compact (see [**13**], [**44**]). Moreover, any open subgroup of I contains one of the $U_{\mathfrak{m}}$'s, hence *C/D is the projective limit* of the $C_{\mathfrak{m}}$'s. Class field theory (cf. for instance **6** [**6**]), gives *an isomorphism of $C/D = \varprojlim C_{\mathfrak{m}}$ onto the Galois group G^{ab}* of the maximal abelian extension of K.

Remark. A more classical definition of $C_{\mathfrak{m}}$ is as follows. Let Id_S be the group of fractional ideals of K prime to S, and P the subgroup of principal ideals (γ), where γ is totally positive and $\gamma \equiv 1 \mod \mathfrak{m}$ (i.e. γ belongs to II-5
$U_{v,\mathfrak{m}}$ for all $v \in S$ and $v \in M_K^\infty$). Let $\mathrm{Cl}_{\mathfrak{m}} = \mathrm{Id}_S/P_{S,\mathfrak{m}}$. We have the exact sequence:

$$1 \longrightarrow P_{S,\mathfrak{m}} \longrightarrow \mathrm{Id}_S \longrightarrow \mathrm{Cl}_{\mathfrak{m}} \longrightarrow 1.$$

For each $a = \prod_{v\notin S} v^{a_v} \in \mathrm{Id}_S$, choose an idèle $\alpha = (\alpha_v)$, with $\alpha_v \in U_{v,\mathfrak{m}}$ if $v \in S$ or $v \in M_K^\infty$, and $v(\alpha_v) = a_v$ if $v \in M_K^\infty \setminus S$. The image of α in $I_{\mathfrak{m}} = I/U_{\mathfrak{m}}$ depends only on $\boldsymbol{a}$. We then get a homomorphism $g\colon \mathrm{Id}_S \to I_{\mathfrak{m}}$.

One checks readily that g extends to a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & P_{S,\mathfrak{m}} \arrow[r] \arrow[d] & \mathrm{Id}_S \arrow[r] \arrow[d, "g"] & \mathrm{Cl}_{\mathfrak{m}} \arrow[r] \arrow[d, "f"] & 1 \\
1 \arrow[r] & K^\times/E_{\mathfrak{m}} \arrow[r] & I_{\mathfrak{m}} \arrow[r] & C_{\mathfrak{m}} \arrow[r] & 1
\end{tikzcd}$$

and that $f\colon \mathrm{Cl}_{\mathfrak{m}} \to C_{\mathfrak{m}}$ *is an isomorphism:* hence C can be identified with the ideal class group mod $\mathfrak{m}$ (and this shows again that it is finite).

2.2 The groups $T_{\mathfrak{m}}$ and $S_{\mathfrak{m}}$

Belen.

2.3 The canonical ℓ-adic representation with values in $S_{\mathfrak{m}}$

Let $\mathfrak{m}$ be a modulus, and let ℓ be a prime number. Let $\varepsilon\colon I \to I_{\mathfrak{m}} \to S_{\mathfrak{m}}(\mathbb{Q})$ be the homomorphism defined in 2.2. Let $\pi\colon T \to S_{\mathfrak{m}}$ be the algebraic morphism $T \to T_{\mathfrak{m}} \to S_{\mathfrak{m}}$; by taking points with values in $\mathbb{Q}_\ell$, π defines a homomorphism

$$\pi_\ell\colon T(\mathbb{Q}_\ell) \longrightarrow S_{\mathfrak{m}}(\mathbb{Q}_\ell)$$

Since $K \otimes \mathbb{Q}_\ell = \prod_{v|\ell} K_v$, the group $T(\mathbb{Q}_\ell)$ can be identified with $K_\ell^\times = \prod_{v|\ell} K_v^\times$, and is therefore a direct factor of the idele group I. Let pr_ℓ denote the projection of I onto this factor. The map

$$\alpha_\ell = \pi_\ell \circ \mathrm{pr}_\ell\colon I \longrightarrow T(\mathbb{Q}_\ell) \longrightarrow S_{\mathfrak{m}}(\mathbb{Q}_\ell)$$

is a continuous homomorphism.

Lemma 1. *α_ℓ and ε coincide on $K^\times$.*

This is trivial from the commutativity of the diagram (**) of 2.2.

II-6 Now, let $\varepsilon_\ell\colon I \to S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ be defined by

$$\varepsilon_\ell(\boldsymbol{a}) = \varepsilon(\boldsymbol{a})\alpha_\ell(\boldsymbol{a}^{-1}) \qquad (***)$$
$$\text{i.e.}\quad \varepsilon_\ell = \varepsilon \cdot \alpha_\ell^{-1}.$$

(If $\boldsymbol{a} \in I$, write a_ℓ the ℓ-component of $\boldsymbol{a}$. Then

$$\varepsilon_\ell(\boldsymbol{a}) = \varepsilon(\boldsymbol{a})\pi_\ell(a_\ell^{-1}).)$$

By the lemma, ε_ℓ is trivial on K and, hence, defines a map $C \to S_{\mathfrak{m}}(\mathbb{Q}_\ell)$; since $S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ is totally disconnected (it is an ℓ-adic Lie group), the latter homomorphism is trivial on the connected component D of C. We have already recalled that C/D may be identified with the Galois group G^{ab} of the maximal abelian extension of K. So we end up with a homomorphism $\varepsilon_\ell \colon G^{\mathrm{ab}} \to S_{\mathfrak{m}}(\mathbb{Q}_\ell)$, i.e. with an *$\ell$-adic representation of K with values in $S_{\mathfrak{m}}$* (cf. Chap. I, 2.3).

This representation is rational in the sense of Chapter I, 2.3. More precisely, let $v \notin \mathrm{Supp}(\mathfrak{m})$, and let $f_v \in I$ be an idèle which is a uniformizing parameter at v, and which is equal to 1 everywhere else; let $F_v = \varepsilon(f_v)$ be the image of f_v in $S_{\mathfrak{m}}(\mathbb{Q}_\ell)$. With these notations we have:

Proposition 1. *a) The representation $\varepsilon_\ell, : G^{\mathrm{ab}} \to S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ is a rational representation with values in $S_{\mathfrak{m}}$.*

b) ε_ℓ is unramified outside $\mathrm{Supp}(\mathfrak{m}) \cup S_\ell$, *where $S_\ell = \{v : p_v = \ell\}$.*

c) If $v \notin$ $\mathrm{Supp}(\mathfrak{m}) \cup S_\ell$, *then the Frobenius element F_{v,ε_ℓ} (cf. Chap. I, 2.3)* II-7
is equal to $F_v \in S_{\mathfrak{m}}(\mathbb{Q}_\ell)$.

Proof. It is known that the class field isomorphism $C/D \xrightarrow{\sim} G^{\mathrm{ab}}$ maps $K_v^\times$ (resp. U_v) onto a dense subgroup of the decomposition group of v in G^{ab} (resp. onto the inertia group of v in G^{ab}), and that a uniformizing element f_v of $K_v^\times$ is mapped onto the Frobenius class of v.

If $v \notin \mathrm{Supp}(\mathfrak{m})$ and $a \in U_v$, then $\varepsilon(a) = 1$; if moreover $p_v \neq \ell$, $\alpha_\ell(a) = 1$, hence $\varepsilon_\ell(a) = 1$ and ε_ℓ is unramified at v; this proves b). For such a v, we have $\varepsilon_\ell(f_v) = \varepsilon(f_v) = F_v$; hence c), and a) follows from c). □

Corollary 1.1. *The representations ε form a system of strictly compatible ℓ-adic representations with values in $S_{\mathfrak{m}}$.*

We also see that the exceptional set of this system is contained in $\mathrm{Supp}(\mathfrak{m})$; for an example where it is different from $\mathrm{Supp}(\mathfrak{m})$, see Exercise 2.

Remark. By construction, $\varepsilon_\ell \colon I \to S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ is given by $x \mapsto \pi_\ell(x^{-1})$ on the open subgroup $U_{\ell,\mathfrak{m}} = \prod_{v|\ell} U_{v,\mathfrak{m}}$ of $K_\ell^\times$. Hence, $\mathrm{Im}(\varepsilon_\ell)$ contains $\pi_\ell(U_{\ell,\mathfrak{m}}) \subset T_{\mathfrak{m}}(\mathbb{Q}_\ell) \subset S_{\mathfrak{m}}(\mathbb{Q}_\ell)$, and is an *open subgroup* of $S_{\mathfrak{m}}(\mathbb{Q}_\ell)$. This open subgroup maps onto $C_{\mathfrak{m}}$, as remarked above. These properties imply, in particular, that $\mathrm{Im}(\varepsilon_\ell)$ is *Zariski-dense* in $\mathrm{S}_{\mathfrak{m}}$.

II-8 **Exercises.**

(1) Let $K = \mathbb{Q}$, $\mathrm{Supp}(\mathfrak{m}) = \emptyset$.

a) Show that $E_\mathfrak{m} = \{1\}$, $C_\mathfrak{m} = \{1\}$, hence $T_\mathfrak{m} = S_\mathfrak{m} = \mathbb{G}_m$ and $S_\mathfrak{m}(\mathbb{Q}) = \mathbb{Q}^\times$, $S_\mathfrak{m}(\mathbb{Q}_\ell) = \mathbb{Q}_\ell^\times$.

b) Show that I is the direct product of its subgroups $I_\mathfrak{m}$ and $\mathbb{Q}^\times$; hence any $\boldsymbol{a} \in I$ may be written as

$$\boldsymbol{a} = u \cdot \gamma, \qquad u \in U_\mathfrak{m},\ \gamma \in \mathbb{Q}^\times.$$

Show that, if $\boldsymbol{a} = (a_p)$, one has

$$\varepsilon(\boldsymbol{a}) = \gamma = \mathrm{sgn}(a_\infty) \prod_p p^{v_p(a_p)}.$$

c) Show that

$$\rho_\ell(\boldsymbol{a}) = \gamma \cdot a_\ell^{-1},$$

and

$$F_p = p.$$

d) Show that ρ_ℓ coincides with the character χ_ℓ of Chap. I, 1.2.

(2) Let $K = \mathbb{Q}$, $\mathrm{Supp}(\mathfrak{m}) = \{2\}$ and $m_2 = 1$. Show that the groups $E_\mathfrak{m}$, $C_\mathfrak{m}$, $T_\mathfrak{m}$, $S_\mathfrak{m}$ coincide with those of Exercise 1, hence that the exceptional set of the corresponding system is empty.

2.4 Linear representations of $S_\mathfrak{m}$

We recall first some well known facts on representations.

II-9 a) Let k be a field of characteristic 0; let H be an affine commutative algebraic group over k. Let $X(H) = \mathrm{Hom}_{\overline{k}}(H_{/\overline{k}}, \mathbb{G}_{m,\overline{k}})$ be the group of characters of H (of degree 1). Here we write the characters of $X(H)$ multiplicatively. The group $G = \mathrm{Gal}(\overline{k}/k)$ acts on $X(H)$.

Let Λ be the affine algebra of H, and let $\overline{\Lambda} = \Lambda \otimes_k \overline{k}$ be the one of $H_{/\overline{k}}$. Every element $\chi \in X(H)$ can be identified with an invertible element of $\overline{\Lambda}$. Hence, by linearity, a homomorphism

$$\alpha \colon \overline{k}[X(H)] \longrightarrow \overline{\Lambda}$$

where $\overline{k}[X(H)]$ is the group algebra of $X(H)$ over $\overline{k}$. This is a G-homomorphism if the action of G is defined by

$$s\left(\sum_{\chi} a_\chi \chi\right) = \sum s(a_\chi) s(\chi)$$

for $a_\chi \in \overline{k}$ and $\chi \in X(H)$. It is well-known (linear independence of characters) that α is injective. It is bijective if and only if H is a group of multiplicative type (cf. 1.3, remark 2). Hence we may identify $\overline{k}[X(H)]$ with a subalgebra of Λ.

b) Let V be a finite-dimensional k-vector space and let

$$\phi \colon H \longrightarrow \mathrm{GL}_V$$

be a *linear representation* of H into V. Assume ϕ is *semi-simple* (this is always the case if H is of multiplicative type). We associate to ϕ its ***trace***

$$\theta_\phi = \sum_{\chi} n_\chi(\phi)\, \chi$$

in $\mathbb{Z}[X(H)]$, where $n_\chi(\phi)$ is the multiplicity of χ in the decomposition of χ over $\overline{k}$.

We have $\theta_\phi(h) = \mathrm{Tr}(\phi(h))$ for any point h of H (with value in any commutative k-algebra). Let $\mathrm{Rep}_k(H)$ be the set of isomorphism classes of linear semi-simple representations of H. If k_1 is an extension of k, then scalar extension from k to k_1 defines a map $\mathrm{Rep}_k(H) \to \mathrm{Rep}_{k_1}(H_{/k_1})$ which is easily seen to be *injective*. We say that an element of $\mathrm{Rep}_{k_1}(H_{/k_1})$ *can be defined over* k, if it is in the image of this map. II-10

Proposition 2. *The map $\phi \mapsto \theta_\phi$ defines a bijection between $\mathrm{Rep}_k(H)$ and the set of elements $\theta = \sum n_\chi \chi$ of $\mathbb{Z}[X(H)]$ which satisfy:*

(a) θ is invariant by G (i.e. $n_\chi = n_{s(\chi)}$ for all $s \in G$, $\chi \in X(H)$).

(b) $n_\chi \geq 0$ *for every* $\chi \in X(H)$.

Proof. The injectivity of the map $\phi \mapsto \theta_\phi$ is well-known (and does not depend on the commutativity of H). To prove surjectivity, consider first the case where θ has the form $\theta = \sum_i \chi^{(i)}$ where $\chi^{(i)}$ is a full set of different conjugates of a character $\chi \in X(H)$. If $G(\chi)$ is the subgroup of G fixing χ, then

$$\theta = \sum_{s \in G/G(\chi)} s(\chi). \tag{$*$}$$

The fixed field k_χ of $G(\chi)$ in k is the smallest subfield of k such that $\chi \in \Lambda \otimes k_\chi$. Consider χ as a representation of degree 1 of $H_{/k_\chi}$. One gets, by
II-11 restriction of scalars to k, a representation ϕ of H of degree $[k_\chi : k]$. One sees easily that the trace θ_ϕ of ϕ is equal to θ. The surjectivity of $\phi \mapsto \theta_\phi$ now follows from the fact that any θ satisfying (a) and (b) is a sum of elements of the form $(*)$ above. □

Corollary 2.1. *In order that* $\phi_1 \in \mathrm{Rep}_{k_1}(H_{/k_1})$ *can be defined over* k*, it is necessary and sufficient that* $\theta_{\phi_1} \in \Lambda \otimes_k k_1$ *belongs to* k_1*.*

c) We return now to the groups $S_\mathfrak{m}$:

Proposition 3. *Let* k_1 *be an extension of* k *and let* $\phi \in \mathrm{Rep}_{k_1}(S_{\mathfrak{m}/k_1})$*. The following properties are equivalent:*

(i) ϕ *can be defined over* k*,*

(ii) for every $v \notin \mathrm{Supp}(\mathfrak{m})$*, the coefficients of the characteristic polynomial* $\phi(F_v)$ *belong to* k*,*

(iii) there exists a set M *of places of* k *of density 1 (cf. Chapter I, 2.2) such that* $\mathrm{Tr}(\phi(F_v)) \in k$ *for all* $v \in M$*.*

Proof. The implications (i) $\implies$ (ii) $\implies$ (iii) are trivial. To prove (iii) $\implies$ (i) we need the following lemma. □

Lemma 2. *The set of Frobeniuses* F_v*,* $v \in M$*, is dense in* S *for the Zariski topology.*

Proof. Let X be the set of all F_v's, $v \in M$, and let ℓ be a prime number. Let $\overline{X} \subseteq S_{\mathfrak{m}}$ (resp. $\overline{X}_\ell \subseteq S_{\mathfrak{m}}(\mathbb{Q}_\ell)$) the closure of X in the Zariski topology
II-12 (resp. ℓ-adic topology). It is clear that $\overline{X} \subseteq \overline{X}(\mathbb{Q}_\ell)$. On the other hand, Čebotarev's theorem (cf. Chapter I, 2.2) implies that $\overline{X} = \mathrm{Im}(\varepsilon_\ell)$ (cf. 2.3). The set $\mathrm{Im}(\varepsilon_\ell)$, however, is Zariski dense in $S_{\mathfrak{m}}$ (cf. Remark in 2.3). Hence $\overline{X} = S_{\mathfrak{m}}$, which proves the lemma. □

Let us now prove that (iii) $\implies$ (i). Let θ_ϕ be the trace of θ in $\Lambda \otimes_k k_1$, where Λ is the affine algebra of $H = S_{\mathfrak{m}/k}$. Let $\{\ell_\alpha\}$ be a basis of the k-vector space k_1, with $\ell_{\alpha_0} = 1$ for some index α_0. We have $\theta_\phi = \sum_\alpha \lambda_\alpha \otimes \ell_\alpha$ ($\lambda_\alpha \in \Lambda$); hence $\mathrm{Tr}(\phi(h)) = \theta_\phi(h) = \sum_\alpha \lambda_\alpha(h)\ell_\alpha$ for all $h \in H(k_1)$. Take $h = F_v$, with $v \in M$, Since F_v belongs to $H(k)$ we have $\lambda_\alpha(F_v) \in k$ for all α; since $\mathrm{Tr}(\phi(F_v)) \in k$, we get $\lambda_\alpha(F_v) = 0$ for all $\alpha \neq \alpha_0$. By the lemma, the F_v's, $v \in M$, are Zariski-dense in H; hence $\lambda_\alpha = 0$ for $\alpha \neq \alpha_0$ and $\theta_\phi = \lambda_{\alpha_0}$ belongs to Λ and (i) follows from the corollary to Proposition 1. □

Exercise. Show that the characters of $S_{\mathfrak{m}}$ correspond in a one-one way to the homomorphisms $\chi\colon I \to \overline{\mathbb{Q}}^\times$ having the following two properties:

(a) $\chi(x) = 1$ if $x \in U_{\mathfrak{m}}$.

(b) For each embedding σ of K into $\overline{Q}$, there exists an integral number $n(\sigma)$ such that
$$\chi(x) = \prod_{\sigma \in \Gamma} \sigma(x)^{n(\sigma)}$$
for all $x \in K^\times$.

2.5 ℓ-adic representations associated to a linear representation of $S_{\mathfrak{m}}$

Belen.

2.6 Alternative construction

Let $\phi_0\colon S_{\mathfrak{m}} \to \mathrm{GL}_{V_0}$ be as in 2.5. If we compose ϕ_0 with the map $\varepsilon\colon I \to S_{\mathfrak{m}}(\mathbb{Q})$ defined in 2.2, we obtain a homomorphism
$$\phi_0 \circ \varepsilon\colon I \longrightarrow \mathrm{GL}_{V_0}(\mathbb{Q}) = \mathrm{Aut}(V_0).$$

Conversely: II-13

Proposition 4. *Let $f\colon I \to \mathrm{Aut}(V_0)$ be a homomorphism. There exists a $\phi_0\colon S_{\mathfrak{m}} \to GL_{V_0}$ such that $\phi_0 \circ \varepsilon = f$ if and only if the following conditions are satisfied:*

1) *The kernel of f contains $U_{\mathfrak{m}}$.*

2) *There exists an algebraic homomorphism $\psi\colon T \to \mathrm{GL}_{V_0}$ such that $\psi(x) = f(x)$ for every $x \in K^\times = T(\mathbb{Q})$.*

Moreover, such a ϕ_0 is unique.

Proof. The necessity of the conditions (a) and (b) is trivial. Conversely, if f has properties (a), (b), it defines a homomorphism $I/U_{\mathfrak{m}} \to \mathrm{Aut}(V_0)$. On the other hand, since f and ψ agree on $K^\times$ the morphism ψ is equal to 1 on $E_{\mathfrak{m}} = K^\times \cap U_{\mathfrak{m}}$, hence on its Zariski-closure $\overline{E}_{\mathfrak{m}}$. This means that ψ factors through

$$T \longrightarrow T_{\mathfrak{m}} \longrightarrow \mathrm{GL}_{V_0}\,.$$

By the universal property of $S_{\mathfrak{m}}$ (cf. 1.3 and 2.2), the maps $I/U_{\mathfrak{m}} \to \mathrm{GL}_{V_0}(\mathbb{Q})$ and $T_{\mathfrak{m}} \to \mathrm{GL}_{V_0}$ define an algebraic morphism $\phi_0\colon S_{\mathfrak{m}} \to GL_{V_0}$, and one checks easily that ϕ_0 has the required properties, and is unique. □

Remark. Since U is open, property (a) implies that f is *continuous* with
II-14 respect to the discrete topology of $\mathrm{Aut}(V_0)$. Conversely, any continuous homomorphism $f\colon I \to \mathrm{Aut}(V_0)$ is trivial on some $U_{\mathfrak{m}}$; moreover, there is a smallest such $\mathfrak{m}$; it is called the ***conductor*** of f.

Exercise. Let $\mathfrak{m}$ be a modulus and let V_0 be a finite dimensional $\mathbb{Q}$-vector space. For each $v \notin \mathrm{Supp}(\mathfrak{m})$ let F_v be an element of $\mathrm{Aut}(V_0)$. Assume:

1) The F_v's commute pairwise.

2) There exists an algebraic morphism $\psi\colon T \to \mathrm{GL}_{V_0}$ such that $\psi(\alpha) = \prod F_v^{v(\alpha)}$ for $\alpha \in K^\times$, $\alpha \equiv 1 \pmod{\mathfrak{m}}$, and $\alpha > 0$ at each real place.

Show that there exists an algebraic morphism $\phi_0\colon S_{\mathfrak{m}} \to \mathrm{GL}_{V_0}$ for which the Frobenius elements are equal to the F_v's.

2.7 The real case

Belen.

2.8 An example: complex multiplication of abelian varieties

(We give here only a brief sketch of the theory, with a few indications on the proofs. For more details, see **34** [**34**], **35** [**35**], **41** [**41**], [**42**] and **32** [**32**].)

Let A be an abelian variety of dimension d defined over K. Let $\mathrm{End}_K(A)$ be its ring of endomorphisms and put $\mathrm{End}_K(A)_0 = \mathrm{End}_K(A) \otimes \mathbb{Q}$. Let E be a number field of degree $2d$, and II-15

$$i\colon E \to \mathrm{End}_K(A)_0$$

be an injection of E into $\mathrm{End}_K(A)_0$. The variety A is then said to have "complex multiplication" by E; in the terminology of Shimura-Taniyama, it is a variety of "type (CM)".

Let ℓ be a prime integer and define $T_\ell(A)$ and $V_\ell = T_\ell(A) \otimes \mathbb{Q}_\ell$ as in Chapter I, 1.2. These are free modules over $\mathbb{Z}_\ell$ and $\mathbb{Q}_\ell$, of rank $2d$. The $\mathbb{Q}$-algebra $\mathrm{End}_K(A)_0$ acts on V_ℓ; hence the same is true for E, and, by linearity, for $E_\ell = E \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. One proves easily:

Lemma 3. *V_ℓ is a free E_ℓ-module of rank 1.*

Let $\rho\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(V_\ell)$ be the ℓ-adic representation defined by A. If $s \in \mathrm{Gal}(\overline{K}/K)$, it is clear that $\rho(s)$ commutes with E, hence with E_ℓ. But the lemma above implies that the commuting algebra of E_ℓ in $\mathrm{End}_K(V_\ell)$ is E_ℓ itself. Hence, ρ may be identified with a homomorphism

$$\rho_\ell\colon \mathrm{Gal}(\overline{K}/K) \longrightarrow E_\ell^\times$$

Let now T_E be the $2d$-dimensional torus attached to E (as $\mathbb{T}$ is attached to K), so that $T_E(\mathbb{Q}_\ell) = E_\ell^\times$, and ρ takes values in $T_E(\mathbb{Q}_\ell)$.

Theorem 1. *(a) The system (ρ_ℓ) is a strictly compatible system of rational ℓ-adic representations of K with values in T_E (in the sense of Chap. I, 2.4).* II-16 *(b) There is a modulus $\mathfrak{m}$ and a morphism*

$$\varphi\colon S_{\mathfrak{m}} \longrightarrow T_E$$

such that ρ is the image by φ of the canonical system (ε_ℓ) attached to $S_{\mathfrak{m}}$, cf. 2.3.

Moreover, the restriction of φ to $T_{\mathfrak{m}}$ can be given explicitly:

Let t be the tangent space at the origin of A. It is a K-vector space on which E acts, i.e. an (E, K)-*bimodule*. If we view it as an E-vector space, the action of K is given by a homomorphism $j\colon K \to \mathrm{End}_E(t)$. In particular, if $x \in K^\times$, $\det_E j(x)$ is an element of $E^\times$; the map $\det_E j\colon K^\times \to E^\times$ is clearly the restriction of an algebraic morphism $\delta\colon \mathbb{T} \to T_E$.

Theorem 2. *The map $\delta\colon \mathbb{T} \to T_E$ coincides with the composition map $\mathbb{T} \longrightarrow T_{\mathfrak{m}} \longrightarrow S_{\mathfrak{m}} \xrightarrow{\varphi} T_E$*

Examples. If A is an *elliptic curve*, E is an imaginary quadratic field, and the action of E on the one-dimensional K-vector space t defines an embedding $E \to K$. The map $\det_E j\colon K^\times \to E^\times$ is just the *norm* relative to this embedding.

Indications on the proofs of Theorems 1 and 2. Part (a) of Theorem 1 is proved as follows: Let S denote the finite set of $v \in M_K^0$ where A has "bad
II-17 reduction". If $v \notin S$, and $\ell \neq p_v$, one shows easily that p_ℓ is unramified at v (the converse is also true, see [**32**]); moreover the corresponding Frobenius element F_{v,ρ_ℓ} may be identified with the Frobenius endomorphism F_v of the reduced variety $\widetilde{A}_v$. But F_v commutes with E in $\mathrm{End}(\widetilde{A}_v)_0$ and the commuting algebra of E in $\mathrm{End}(\widetilde{A}_v)_0$ is E itself (cf. [**34**]). Hence F_v belongs to $E^\times = T_E(\mathbb{Q})$ and this implies (a).

Theorem 2 and part (b) of Theorem 1 are less easy; they are proved, in a somewhat different form in **34** [**34**] (see also [**32**]). Note that one could express them (as in **??**) by saying that *there exists a homomorphism $f\colon I \to E^\times$* (where I denotes, as usual, the group of idèles of K) *having the following properties:*

1) f is trivial on $U_{\mathfrak{m}}$, for some modulus $\mathfrak{m}$ with support S.

2) If $v \notin S$, the image by f of a uniformizing parameter at v is the Frobenius element $F_v \in E^\times$.

3) If $x \in K^\times$ is a principal idèle, one has $f(x) = \det_E j(x)$.

This is essentially what is proved in [**34**], formula (3), except that the result is expressed in terms of ideals instead of ideles, and $\det_E j(x)$ is written in a different form, namely "$\prod_\alpha \mathrm{N}_{K/K^\times}(x)^{\psi_\alpha}$".

Remark. Another possible way of proving Theorems 1 and 2 is the following:

Let ℓ be a prime integer distinct from any of the p_v, $v \in S$. One then sees that the Galois-module V_ℓ is of Hodge-Tate type in the sense of Chapter III, 1.2 (indeed, the corresponding local modules are associated with *ℓ-divisible* II-18 *groups*, and one may apply Tate's theorem [**39**]). Hence ρ_ℓ is "locally algebraic" (Chapter III, *loc. cit.*), and using the theorem of Chapter III, 2.3 one sees it defines a morphism $\varphi\colon S_{\mathfrak{m}} \to T_E$. One has $\varphi \circ \varepsilon_\ell = \rho_\ell$ by construction; the same is true for any prime number ℓ', since $\varphi \circ \varepsilon_{\ell'}$ and $\rho_{\ell'}$ have the same Frobenius elements for almost all v. This proves part (b) of Theorem 1. As for Theorem 2, one uses the explicit form of the Hodge-Tate decomposition of V_ℓ, as given by **39** [**39**], combined with the results of the Appendix to Chapter III.

§3. Structure of $T_{\mathfrak{m}}$ and applications

3.1 Structure of $X(T_{\mathfrak{m}})$

Belen.

3.2 The morphism $j^*\colon \mathbb{G}_m \to T_{\mathfrak{m}}$

Belen.

3.3 Structure of $T_{\mathfrak{m}}$

We need first some notations:

Let H_c be the closed subgroup of $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ generated by C_∞ (cf. 3.1). There is a unique continuous homomorphism $\varepsilon\colon H_c \to \{\pm 1\}$ such that II-19 $\varepsilon(c) = -1$ for all $c \in C_\infty$. Indeed the unicity of ε is clear, and one proves its existence by taking the restriction to H_c of the homomorphism $G \to \{\pm 1\}$

associated with an imaginary quadratic extension of $\mathbb{Q}$. We let $H = \mathrm{Ker}(\varepsilon)$. The groups H and H_c are closed invariant subgroups of G, and $(H : H_c) = 2$.

Let now K be, as before, a finite extension of $\mathbb{Q}$; we identify it with a subfield of $\mathbb{Q}$; let $G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ be the corresponding subgroup of G. The field K is *totally real* if and only if all the elements c of C_∞ act trivially on K, i.e. if and only if G_K contains G_c. Hence, there exists a *maximal totally real subfield* K_0 of K, whose Galois group is $G_{K_0} = G_K \cdot H_c$. We let K_1, be the field corresponding to $G_K \cdot H$. We have

$$K_0 \subset K_1 \subset K \qquad \text{and} \qquad [K_1 : K_0] = 1 \text{ or } 2.$$

As shown by Weil (cf. [**47**]) the fields K_0 and K_1 are closely connected to the groups $T_\mathfrak{m}$ relative to K. Indeed, if $\chi = \sum_\sigma b_\sigma[\sigma]$ is an element of the group denoted by Y^- in 3.1, we have $b_{c\sigma} = -b_\sigma$ for all $c \in C_\infty$. If $h = c_1 \cdots c_n$, this gives

$$b_{h\sigma} = (-1)^n b_\sigma = \varepsilon(h) b_\sigma$$

and by continuity the same holds for all $h \in H_c$. One deduces from this:

Proposition 1. *The norm map defines an isomorphism of the space $Y^0_{K_1}$ relative to K onto the space Y^-_K relative to K.*

II-20 More precisely, if $\chi_1 = \sum b_{\sigma_1}[\sigma_1]$ belongs to $Y^-_{K_1}$, where $\sigma_1 \in \Gamma_{K_1}$, the image of χ_1, by the norm map is

$$\mathrm{N}^*_{K_1/K_0}(\chi_1) = \sum_\sigma b_{\sigma/K_1}[\sigma], \qquad \sigma \in \Gamma_K,$$

where σ/K_1 is the restriction of σ to K. It is clear that this map is injective. Conversely, if $\chi = \sum_\sigma b_\sigma[\sigma]$ belongs to Y^-_K, we saw above that $b_{h\sigma} = \varepsilon(h)b_\sigma$ for all $h \in H_c$, hence $b_{h\sigma} = b_\sigma$ for $h \in H$ and of course also for $h \in H \cdot G_K$. This shows that b_σ depends only on the restriction of σ to K_1, and hence that χ belongs to the image of the norm map.

Corollary 1.1. *The tori $T_\mathfrak{m}$ attached to K and K_1 are isogenous to each other.*

There remains to describe the tori $T_\mathfrak{m}$ attached to K_1. There are two cases:

(1) $K_1 = K_0$. *In this case, we have* $Y^- = 0$ *and* $T_{\mathfrak{m}}$ *is one-dimensional, and isomorphic to* $\mathbb{G}_m$.

Indeed, if $\chi = \sum_\sigma b_\sigma[\sigma]$ belongs to Y^-, and $c \in C_\infty$, we have $b_{c\sigma} = -b_\sigma$ (cf. 3.1) but also $b_{c\sigma} = b_\sigma$ since $c \in G_K \cdot H_c = G_K \cdot H$. This shows that $b_\sigma = 0$ for all σ, hence $Y^- = 0$.

(2) $[K_1 : K_0] = 2$. The field K_1 is then a *totally imaginary quadratic extension* of K_0 (and it is the only one contained in K, as one checks readily). In this case Y^- is of dimension $d = [K_0 : \mathbb{Q}]$ and $T_{\mathfrak{m}}$ is $(d+1)$-dimensional.

More precisely, the space Y attached to K_1 is $2d$-dimensional and the involution σ of K_1 corresponding to K_0 decomposes Y in two eigenspaces of dimension d each; the space Y^- is the one corresponding to the eigenvalue -1 of σ. This is proved by the same argument as above, once one remarks that all $c \in C_\infty$ induce σ on K_1. II-21

Remark. In this last case (which is the most interesting one), the torus $T_{\mathfrak{m}}$ is isogenous to the product of $\mathbb{G}_m$ by the d-dimensional torus kernel of the norm map from K_1 to K_0.

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

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

be the corresponding ℓ-adic representation of K, cf. chap. I, 1.2. The main result of this Chapter is the determination of the Lie algebra of the ℓ-adic Lie group $G_\ell = \operatorname{Im}(\rho_\ell)$. 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

$$y^2 = 4x^3 - g_2 x - g_3$$

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 $g_2 \mapsto u^4 g_2$, $g_3 \mapsto u^6 g_3$, $u \in K^\times$. 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
III-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 $\mathrm{Spec}(\mathcal{O}_v)$, 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. I, 1.2, 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 $\mathrm{Gal}(\overline{K}/K)$ into $\mathrm{Aut}(T_\ell)$. 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 v be some extension of v to $\overline{K}$; let D (resp. I) be the corresponding decomposition group (resp. inertia group), cf. chap. I, 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. I, 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

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

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. I, 2.2).

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

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

(b) We take now $m = 1$. Show that the properties (i), (ii) and (iii) 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 (iv) $\implies$ (iii) is easy. For the proof of the converse, use Exer. 2 of chap. I, 1.1.) [For $m > 2$, see **64** [**64**].]

1.4 Šafarevič's theorem

III-7

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.*

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

$$y^2 = 4x^3 - g_2'x - g_3'$$

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

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

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
III-9 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

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

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 1.3.

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 (1.4).

(b) If E is not irreducible, there exists a Galois submodule X of E which is one-dimensional over $\mathbb{F}_\ell$. 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. $\square$

Remark. One can prove part (a) 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