Abelian ℓ-adic Representations and Elliptic Curves

Jean-Pierre Serre

October 5, 2024

VITA

Jean-Pierre Serre

Professor of Algebra and Geometry at the Collège de France, Paris, was born in Bagcs, France, on September 15, 1926. He graduated from École Normale Superieure, Paris, in 1948, and obtained his Ph.D. from the Sorbonne in 1951. In 1954 he was awarded a Fields Medal for his work on topology (homotopy groups) and algebraic geometry (coherent sheaves). Since then, his main topics of interest have been number theory, group theory, and modular forms. Professor Serre has been a frequent visitor of the United States, especially at the Institute for Advanced Study, Princeton, and Harvard University. He is a foreign member of the National Academy of Sciences of the U.S.A.

PREFACE TO THE SECOND EDITION

The present edition differs from the original one (published in 1968) by:

- the inclusion of short notes giving references to new results;
- a supplementary bibliography.

Otherwise, the text has been left unchanged, except for the correction of a few misprints.

The added bibliography does not claim to be complete. Its aim is just to help the reader get acquainted with some of the many developments of the past twenty years (for those prior to 1977, see also the survey [**78**]). Among these developments, one may especially mention the following:

ℓ-adic representations associated to abelian varieties over number fields

Deligne (cf. [**52**]) has proved that Hodge cohomology classes behave under the action of the Galois group as if they were algebraic, thus providing a very useful substitute for the still unproved Hodge conjecture.

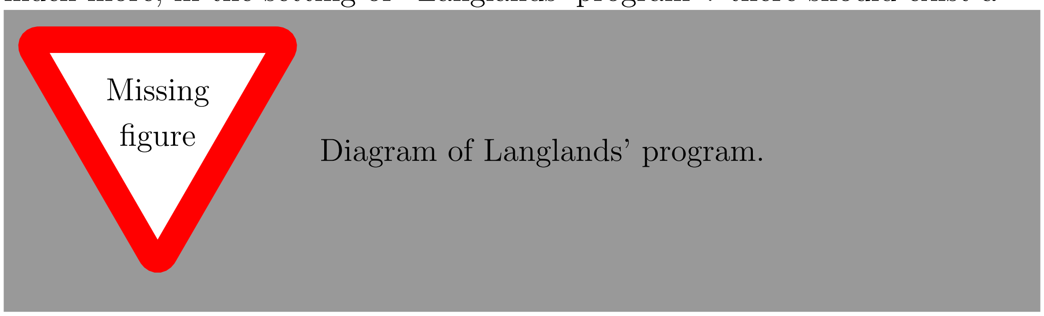
Faltings ([**54**], see also **82** [**82**] and **56** [**56**]), has proved Tate's conjecture that the map

$$\mathrm{Hom}_K(A, B) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \longrightarrow \mathrm{Hom}_{\mathrm{Gal}(\overline{\mathbb{Q}}/K)}(T_\ell(A), T_\ell(B))$$

is an isomorphism (A and B being abelian varieties over a number field K), together with the semi-simplicity of the Galois module $Q_\ell \otimes_{\mathbb{Z}_\ell} T_\ell(A)$ and similar results for $T_\ell(A)/\ell T_\ell(A)$ when ℓ is large enough. These results may be used to study the structure of the Galois group of the division points of A, cf. [**80**]. For instance, if $\dim A$ is odd and $\mathrm{End}_K\, A = \mathbb{Z}$, one can show that this Galois group has finite index in the group of symplectic similitudes; for elliptic curves, i.e. $\dim A = 1$, this was already proved in [**76**].

Modular forms and ℓ-adic representations

The existence of ℓ-adic representations attached to modular forms, conjectured in the first edition of this book, has been proved by Deligne ([**50**], see also Langlands [**65**] and Carayol [**0**]). This has many applications for instance to the Ramanujan conjecture (Deligne) and to congruence properties (Ribet [**69**], [**71**]; Swinnerton-Dyer [**81**]; [**73**], [**77**]). Some generalizations are known (e.g. Carayol [**0**]; Ohta [**68**]; Wiles [**84**]), but one can hope for much more, in the setting of "Langlands' program": there should exist a



where the vertical line is (essentially) bijective and the horizontal arrow injective with a precise description of its image (Deligne [**51**]; Langlands [**66**]; [**78**]). Such a diagram would incorporate, among other things, the conjectures of Artin (on the holomorphy of L-functions) and Taniyama-Weil (on elliptic curves over $\mathbb{Q}$). Chapters II and III of the presentbook, supplemented by the results of Deligne ([**53**]) and Waldschmidt ([**63**], [**83**]), may be viewed as a partial realization of this ambitious program in the abelian case.

Local theory of ℓ-adic representations

Here the ground field K, instead of being a number field, is a local field of residue characteristic p. The most interesting case is $\operatorname{char} K = 0$ and $p = \ell$, especially when a Hodge-Tate decomposition exists: indeed this gives precious information on the image of the inertia group (Sen [**72**]; [**79**]; Wintenberger [**85**]). When the ℓ-adic representation comes from a divisible group or an abelian variety, the existence of such a decomposition is well known (Tate [**39**]; see also Fontaine [**60**]); for representations coming from higher dimension cohomology, it has been proved recently by Fontaine-Messing (under some restrictions, cf. [**62**]) and Faltings ([**55**]). The results of Fontaine-Messing are parts of a vastprogram by Fontaine, relating Galois representations and modules of Dieudonné type (over some “Barsotti-Tate rings”, cf. [**58**], [**59**], [**61**]).

CONTENTS

INTRODUCTION

The "ℓ-adic representations" considered in this book are the algebraic analogue of the locally constant sheaves (or "local coefficients") of Topology. A typical example is given by the ℓ^n-th division points of abelian varieties (cf. chap. I, 1.2); the corresponding ℓ-adic spaces, first introduced by Weil [**0**] are one of our main tools in the study of these varieties. Even the case of dimension 1 presents non trivial problems; some of them will be studied in chap. IV.

The general notion of an ℓ-adic representation was first defined by Taniyama [**0**] (see also the review of this paper given by Weil in *Math. Rev.*, 20, 1959, rev.1667). He showed how one can relate ℓ-adic representations relative to different prime numbers ℓ *via* the properties of the Frobenius elements (see below). In the same paper, Taniyama also studied some *abelian* representations which are closely related to complex multiplication (cf. **41** [**41**], [**42**] and Shimura & Taniyama [**0**]). These abelian representations, together with some applications to elliptic curves, are the subject matter of this book.

There are four Chapters, whose contents are as follows:

Chapter I begins by giving the definition and some examples of ℓ-adic representations (§1). In §2, the ground field is assumed to be a *number field*. Hence, Frobenius elements are defined, and one has the notion of a *rational* ℓ-adic representation: one for which their characteristic polynomials have rational coefficients (instead of merely ℓ-adic ones). Two representations corresponding to different primes are *compatible* if the characteristic polynomials of their Frobenius elements are the same (at least almost everywhere); not much is known about this notion in the non abelian case (cf. the list of open questions at the end of 2.3). A last section shows how one attaches L-functions to rational ℓ-adic representations; the well known connection between equidistribution and analytic properties of L-functions is discussed in the Appendix.

Chapter II gives the construction of some abelian ℓ-adic representations of a number field K. As indicated above, this construction is essentially due to Shimura, Taniyama and Weil. However, I have found it convenient to present their results in a slightly different way, by defining first some algebraic groups over $\mathbb{Q}$ (the groups SS) whose representations – in the usual algebraic sense – correspond to the sought for ℓ-adic representations of K. The same groups had been considered before by Grothendieck in his still conjectural theory of "motives" (indeed, motives are supposed to be "ℓ-adic cohomology without ℓ" so the connection is not surprising). The construction of these groups SS and of the ℓ-adic representations attached to them, is given in §2 (§1 contains some preliminary constructions on algebraic groups, of a rather elementary kind). I have also briefly indicated what relations these groups have with complex multiplication (cf. 2.8). The last § contains some more properties of the $S_{\mathfrak{m}}$'s.

Chapter III is concerned with the following question: let p be an abelian ℓ-adic representation of the number field K; can p be obtained by the method of chap. II? The answer is: this is so if and only if p is *"locally algebraic"* in the sense defined in §1. In most applications, local algebraicity can be checked using a result of Tate saying that it is equivalent to the existence of a "Hodge-Tate" decomposition, at least when the representation is semi-simple. The proof of this result of Tate is rather long, and relies heavily on his theorems on p-divisible groups [**39**]; it is given in the Appendix. One may also ask whether any abelian rational semi-simple ℓ-adic representation of K is *ipso facto* locally algebraic; this may well be so, but I can prove it only when K is a composite of quadratic fields; the proof relies on a transcendency result of Siegel and Lang (cf. §3).

Chapter IV is concerned with the ℓ-adic representation ρ_ℓ, defined by an *elliptic curve E*. Its aim is to determine, as precisely as possible, the image of the Galois group by ρ_ℓ, or at least its *Lie algebra*. Here again the ground field is assumed to be a number field (the case of a function field has been settled by Igusa [**0**]). Most of the results have been stated in [**0**], [**31**] but with at best some sketches of proofs. I have given here complete proofs, granted some basic facts on elliptic curves, which are collected in §1. The method followed is more "global" than the one indicated in [**0**]. One starts from the fact, noticed by Cassels and others, that the number of isomorphism classes of elliptic curves isogenous to E is *finite*; this is an easy consequence of Šafarevič's theorem (cf. 1.4) on the finiteness of the number of elliptic curves having good reduction outside a given finite set of places. From this, one gets an irreducibility theorem (cf. 2.1). The determination of the Lie algebra of $\mathrm{Im}(\rho_\ell)$ then follows, using the properties of abelian representations given in chap. II, III; one has to know that ρ_ℓ, if abelian, is locally algebraic, but this is a consequence of the result of Tate given in chap. III. The variation of $\mathrm{Im}(\rho_\ell)$ with ℓ is dealt with in §3. Similar results for the local case are given in the Appendix.

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 65 (III-34): it originally said "A_n/A_{n+k}", and it should be "A_n/A_{n+1}".
- Page 76 (IV-8): it originally said "$\Delta_v = u^{12}\Delta'$", and it should be "$\Delta_v = u_v^{12}\Delta'$".
- Page 82 (IV-17): it originally said "by the theorem on section 4", but the correct reference was 2.2.

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. An ℓ-adic representation of 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 G. This follows from the fact that G is compact.

Indeed, let L be any lattice of V, and let H be the set of elements I-2
$g \in G$ 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 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 G, the group $G = \mathrm{Im}(\rho)$ is a closed subgroup of $\mathrm{Aut}(V)$, and hence, by the ℓ-adic analogue of Cartan's theorem (cf. [**0**, pp. 5–42]) G is itself an ℓ-adic Lie group. Its Lie algebra $\mathfrak{g} = \mathrm{Lie}(G)$ 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. [**0**], 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 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 $k = \mathbb{F}_\ell$ 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 $\mathbb{F}_\ell$-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 $\ell \neq \operatorname{char}(K)$. The group $G = \operatorname{Gal}(K_s/K)$ 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 $\chi_\ell \colon G \to \operatorname{Aut}(V_\ell) = \mathbb{Q}_\ell^\times$ 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 $\ell \neq \operatorname{char}(K)$. Let E be an elliptic curve defined over K with a given rational point o. One knows that there is a unique 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 $G = \operatorname{Gal}(K_s/K)$ acts (cf. [**0**], chap. VII). The corresponding homomorphism $\pi_\ell \colon G \to \operatorname{Aut}(V_\ell(E))$ is an ℓ-adic representation of 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 $\mathrm{GL}(2, \mathbb{Z}_\ell)$. (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. [**0**], *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.

3. 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. [**0**], *loc. cit.*) on which $G = \operatorname{Gal}(K_s/K)$ 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. Igusa [**0**] 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 Cassels & Fröhlich [**0**], Lang [**0**] or Weil [**0**].) 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
I-6 $v \in M_K^0$ 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 degree of k_v over $\mathbb{F}_{p_v}$. 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 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 [**0**], 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* $\mathrm{Card}(X)/\mathrm{Card}(G)$.

For the proof, see [**0**], [**0**], 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 $\mathrm{Gal}(L/K)$.

b) Let K be a subset of $\mathrm{Gal}(L/K)$*, 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 neighborhood of a given class of $\mathrm{Gal}(L/K)$.

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 $\det(1 - F_{v,\rho}T)$.

Definition 1. 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 $M_K^0 - S$ is unramified with respect to ρ.

(b) If $v \notin S$, the coefficients of $P_{v,\rho}(T)$ belong to $\mathbb{Q}$ (resp. to $\mathbb{Z}$).

Remark. Let K'/K be a finite extension. An ℓ-adic representation ρ of K defines (by restriction) an ℓ-adic representation $\rho_{/K'}$ de K'. If ρ is rational (resp. integral), then the same is true for $\rho_{/K'}$; this follows from the fact that the Frobenius elements relative to K' are powers of those relative to K.

Examples. The ℓ-adic representations of K given in examples 1, 2, 3 of section 1.2 are rational (even *integral*) representation. In example 1, one can take for S the set S_ℓ of elements v of M_K^0 with $\rho_v = \ell$; In examples 2, 3, one can take for S the union of S_ℓ and the set S_A where A has "bad reduction"; the fact that the corresponding Frobenius has an integral characteristic polynomial (which is independent of ℓ) is a consequence of Weil's results on endomorphisms of abelian varieties (cf. [**0**] and [**0**], chap. VII). The I-10
rationality of the cohomology representation is a well-known open question.

Ver si sigue siendo una pregunta abierta.

Definition 2. Let ℓ' be a prime, ρ' an ℓ'-adic representation of K, and assume that ρ, ρ' are rational. Then ρ, ρ' are said to be ***compatible*** if there exists a finite subset S of M_K^0 such that ρ and ρ' are unramified outside of S and $P_{v,\rho}(T) = P_{v,\rho'}(T)$ for $v \in M_K^0 - S$.

(In other words, the characteristic polynomials of the Frobenius elements arte the same for ρ and ρ', at least for almost all v's.)

If $\rho\colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(V)$ is rational ℓ-adic representation of K, then V has a composition series

$$V = V_0 \supset V_1 \supset \cdots \supset V_q = 0$$

of ρ-invariants subspaces with V_i/V_{i+1} $(0 \le i \le q-1)$ *simple* (i.e. *irreducible*). The ℓ-adic representation ρ' of K defined by $V' = \sum_{i=0}^{q-1} V_i/V_{i+1}$ is semi-simple, rational, and compatible with ρ; it is the "semi-simplification" of V.

Theorem 1. *Let ρ be a rational ℓ-adic representation of K, let ℓ' be a prime. Then there exists at most one (up to isomorphism) ℓ'-adic rational representation ρ' of K which is semi-simple and compatible with ρ.*

(Hence there exists a unique (up to isomorphism) rational semi-simple ℓ-adic representation compatible with ρ.)

I-11 *Proof.* Let ρ'_1, ρ'_2 be semi-simple ℓ-adic representations of K which are rational and compatible with ρ.

We first prove that $\mathrm{Tr}(\rho'_1(g)) = \mathrm{Tr}(\rho'_2(g))$ for all $g \in G$. Let $H = G/(\mathrm{Ker}(\rho'_1) \cap \mathrm{Ker}(\rho'_2))$; the representations ρ'_1, ρ'_2 may be regarded as representations of H, and it suffices to show that $\mathrm{Tr}(\rho'_1(h)) = \mathrm{Tr}(\rho'_2(h))$ for all $h \in H$. Let $K' \subset \overline{K}$ be the fixed field of H. Then by the compatibility of ρ'_1, ρ'_2 there is a finite subset S of M_K^0 such that for all $v \in M_K^0 - S$, $w \in M_K'^0$, $w \mid v$, we have $\mathrm{Tr}(\rho'_1(F_w)) = \mathrm{Tr}(\rho'_2(F_w))$. But, by cor. 1 to Čebotarev's theorem (cf. 2.2) the F_w are dense in H. Hence $\mathrm{Tr}(\rho'_1(h)) = \mathrm{Tr}(\rho'_2(h))$ for all $h \in H$ since $\mathrm{Tr} \circ \rho'_1$, $\mathrm{Tr} \circ \rho'_2$ are continuous.

The theorem now follows from the following result applied to the group ring $\Lambda = \mathbb{Q}_\ell[H]$. □

Lemma 1. *Let k be a field of characteristic zero, let Λ be a k-algebra, and let ρ_1, ρ_2 be two finite-dimensional linear representations of Λ. If ρ_1, ρ_2 are semi-simple and have the same trace ($\mathrm{Tr} \circ \rho_1 = \mathrm{Tr} \circ \rho_2$), then they are isomorphic.*

For the proof see Bourbaki, Alg., ch. 8, §12, n°1, prop. 3.

Cómo citar esto

Definition 3. For each prime ℓ let ρ_ℓ be a rational ℓ-adic representation of K. The system (ρ_ℓ) is said ***to be compatible*** if ρ_ℓ, ρ'_ℓ are compatible for any two primes ℓ, ℓ'. The system (ρ_ℓ) is said ***to be strictly compatible*** if there exists a finite subset S of M_K^0 such that:

(a) Let $S_\ell = \{v \mid \rho_v = \ell\}$. Then, for every $v \notin S \cup S_\ell$, ρ_ℓ is unramified at v and $P_{v,\rho_\ell}(T)$ has rational coefficients.

(b) $P_{v,\rho_\ell}(T) = P_{v,\rho_{\ell'}}(T)$ if $v \notin S \cup S_\ell \cup S_{\ell'}$.

I-12 When a system (ρ_ℓ) is strictly compatible, there is a smallest finite set S having properties (a) and (b) above. We call it the ***exceptional set*** of the system.

Examples. The systems of ℓ-adic representations given in examples 1, 2, 3 of section 1.2 are strictly compatible. The exceptional set of the first one is empty. The exceptional set of example 2 (resp. 3) is the set of places where the elliptic curve (resp. the abelian variety) has "bad reduction", cf. [**0**].

Questions.

1) Let ρ be a rational ℓ-adic representation. Is true that $P_{v,\rho}$ has coefficients for all v such that ρ is unramified at v?

   A somewhat similar question is:

   Is any compatible system strictly compatible?

2) Can any rational ℓ-adic representation be obtained (by tensor products, direct sums, etc.) from ones coming from ℓ-adic cohomology?

3) Given a rational ℓ-adic representation ρ of K, and a prime ℓ', does there exist a rational ℓ'-adic representation ρ' of K compatible with ρ? $\to$ [no: easy counter-examples].

4) Let ρ, ρ' be rational ℓ, ℓ'-adic representations of K which are compatible and semi-simple.

   (i) If ρ is abelian (i.e. , if $\mathrm{Im}(\rho)$ is abelian), is it true that ρ' is abelian? (We shall see in chapter III that this is true at least if ρ is "locally algebraic".) $\to$ [yes: this follows from [**0**].]

   (ii) Is it true that $\mathrm{Im}(\rho)$ and $\mathrm{Im}(\rho')$ are Lie groups of the same dimen- I-13
   sion? More optimistically, is it true that there exists a Lie algebra $\mathfrak{g}$ over $\mathbb{Q}$ such that $\mathrm{Lie}(\mathrm{Im}(\rho)) = \mathfrak{g} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ and $\mathrm{Lie}(\mathrm{Im}(\rho')) = \mathfrak{g} \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell'}$?

5) Let X be a non-singular projective variety defined over K, and let i be an integer. Is the i-th cohomology representation $H^i_\ell(X_{\mathrm{s}})$ semi-simple? Does its Lie algebra contain the homotheties if $i \geq 1$? (When $i = 1$,

an affirmative answer to either one of these questions would imply a positive solution for the "conguence subgroup problem" on abelian varieties, cf. [**0**], §3.) $\rightarrow$ [yes: for $i = 1$: see [**0**] and also [**75**].]

Remark. The concept of an ℓ-adic representation can be generalized by replacing the prime ℓ by a place λ of a number field E. A λ-adic representation is then a continuous homomorphism $\mathrm{Gal}(K_\mathrm{s}/K) \rightarrow \mathrm{Aut}(V)$, where V is a finite-dimensional vector space over the local field E_λ. The concepts of rational λ-adic representation, compatible representations, etc., can be defined in a way similar to the ℓ-adic case.

Exercise.

1) Let ρ and ρ' be two rational, semi-simple, compatible representations. Show that, if $\mathrm{Im}(\rho)$ is finite, the same is true for $\mathrm{Im}(\rho')$ and that $\mathrm{Ker}(\rho) = \mathrm{Ker}(\rho')$. (Apply exer. 3 of 1.1 to ρ' and to $U = \mathrm{Ker}(\rho)$.) Generalize this to λ-adic representations (with respect to a number field E).

2) Let ρ (resp. ρ') be a rational ℓ-adic (resp. ℓ'-adic) representation of K, of degree n. Assume ρ and ρ' are compatible. If $s \in G = \mathrm{Gal}(\overline{K}/K)$, let
I-14 $\sigma_i(s)$ (resp. $\sigma'_i(s)$) be the i-th coefficient of the characteristic polynomial of $\rho(s)$ (resp. $\rho'(s)$). Let $P(X_0, \ldots, X_n)$ be a polynomial with rational coefficients, and let X_P (resp. X'_P) be the set of $s \in G$ such that $P(\sigma_0(s), \ldots, \sigma_n(s)) = 0$ (resp. $P(\sigma'_0(s), \ldots, \sigma'_n(s)) = 0$).

   (a) Show that the boundaries of X_P and X'_P have measure zero for the Haar measure μ of G (use Exer. of 2.2).

   (b) Assume that μ is normalized, i.e. $\mu(G) = 1$. Let T_P be the set of $v \in M_K^0$ at which ρ is unramified, and for which the coefficients $\sigma_0, \ldots, \sigma_n$ of characteristic polynomial of $F_{v,\rho}$ satisfy the equation $P(\sigma_0, \ldots, \sigma_n) = 0$. Show that T_P has density equal to $\mu(X_P)$.

   (c) Show that $\mu(X_P) = \mu(X'_P)$.

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 1. 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-15
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 $v \in M_K^0 - S$ 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
characteristic polynomial are central functions, one sees that $\varphi_\ell \circ \rho$ I-16
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. II, 2.5).

2.5 L-functions attached to rational representations

Let K be a number field and let $\rho = (\rho_\ell)$ be a strictly compatible system of rational ℓ-adic representations, with exceptional set S. If $v \notin S$, denote by $P_{v,\rho}(T)$ the rational polynomial does not depend on the choice of ℓ. Let s be a complex number.

One has:

$$\begin{aligned} P_{v,\rho}(\mathbf{N}\, v)^{-s} &= \det(1 - F_{v,\rho}/(\mathbf{N}\, v)^s) \\ &= \prod_i (1 - \lambda_{i,v}/(\mathbf{N}\, v)^s), \end{aligned}$$

where the $\lambda_{i,v}$'s are the eigenvalues of $F_{v,\rho}$ (note that the $\lambda_{i,v}$'s are algebraic numbers and hence may be identified with complex numbers). Put:

$$L_\rho(s) = \prod_{v \notin S} \frac{1}{P_{v,\rho}((\mathbf{N}\, v)^{-s})}.$$

This is a *formal* Dirichlet series $\sum_{n=1}^{\infty} a_n/n^s$, with coefficients in $\mathbb{Q}$.

In all known cases, there exists a constant k such that $\left|\lambda_{i,v} \leq (\mathbf{N}\, v)^k\right|$, and this implies that L_ρ is convergent in some half plane $\Re(s) > C$; one
I-17 conjectures it extends to a meromorphic function in the whole plane. When ρ comes from ℓ-adic cohomology, there are some further conjectures on the zeros and poles of L_ρ, cf. Tate [**0**]**;** these, as indicated by Tate, may be applied to get equidistribution properties of Frobenius elements, cf. Appendix A.

Remark. 1) One can also associate L-functions to *E-rational* systems of λ-adic representations (2.3, Remark), where E is a number field, once an embedding of E into $\mathbb{C}$ has been chosen.

Belén ♡: No cacho si el C es los complejos o qué weá

2) We have given a definition of the local factors of L_ρ only at the places $v \notin S$. One can give a more sophisticated definition in which local factors are defined for all places, even (with suitable hypotheses) for primes at infinity (gamma factors); this is necessary when one wants to study functional equations. We don't go into this here. → [see [**51**], [**74**].]

3) Let $\phi(s) = \sum a_n/n^s$ be a Dirichlet series. Using the theorem in 2.3, one sees that there is (up to isomorphism) at most one semi-simple system $\rho = (\rho_\ell)$ over $\mathbb{Q}$ such that $L_\rho = \phi$. Whether there does exist one (for a given ϕ) is often a quite interesting question. For instance, is it so for Ramanujan's $\phi(s) = \sum_{n=1}^{\infty} \tau(n)/n^s$, where $\tau(n)$ is defined by the identity

$$x \prod_{n=1}^{\infty} (1 - x^n)^2 4 = \sum_{n=1}^{\infty} \tau(n) x^n ?$$

There is considerable numerical evidence for this, based on the congruence properties of τ (Swinnerton-Dyer, unpublished); of course, such a ρ would be of dimension 2, and its exceptional set S would be empty. $\rightarrow$ [proved by Deligne: see [**0**], [**50**], [**65**],...]

Belén ♡:
¿Seguirá así?

More generally, there seems to be a close connection between modular forms, such as $\sum \tau(n)x^n$, and rational (or algebraic) ℓ-adic representations; see for instance Shimura [**0**] and Weil [**0**]. $\rightarrow$ [see also [**0**], [**51**], [**65**], [**66**], [**68**], [**84**].] I-18

Examples. 1. If G acts through a *finite* group, L_ρ is an Artin (non abelian) L-series, at least up to a finite number of factors (cf. [**0**]). All Artin L-series are gotten in this way, provided of course one uses E-rational representations (cf. Remark 1) and not merely rational ones.

2. If ρ is the system associated with an elliptic curve E (cf. 1.2), the corresponding L-function gives the non-trivial part of zeta function of E. The symmetric powers of ρ give the zeta functions of the products $E \times \ldots \times E$, cf. Tate [**0**].

§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

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

I-19 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 $m \leq n$ 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 $\varphi \in C(X)$, $0 \leq \varphi \leq 1$, with $\varphi = 0$ on $X - \mathring{U}$ and $\mu(\varphi) \geq \mu(U) - \varepsilon$. Since $\mu_n(\varphi) \leq n_U/n$ we have

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

I-20 from which we obtain $\liminf n_U/n \geq \mu(U)$. The same argument applied to $X - U$ shows that

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

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

Examples. 1. Let $X = [0,1]$, and let 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 $m \leq n$ 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 central functions on G; by the Peter-Weyl theorem, the irreducible characters I-21
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 (Weyl [**0**])**.** *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-22 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 $\mathbf{N}\,v \leq n$ is equivalent to $n/\log n$ (as $n \to \infty$).*

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

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

The theorem results, by a standard argument, from the theorem of Wiener-Ikehara, cf. A.3 below. Suppose now that the function $v \mapsto \mathbf{N}\,v$ has the
I-23 following property:

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

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

Theorem 2. *The elements x_v $(v \in M)$ are equidistributed in X with respect to a measure 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 pole at $s = 1$ and is holomorphic on the rest of the line $\Re(s) = 1$, cf. I-24
for instance Lang [**0**], chap. VII; for a proof of (2), cf. Artin [**0,** p. 121]. Hence theorem **??** gives the equidistribution of the Frobenius elements, i.e. the Čebotarev density theorem, cf.˜**??**sec:I$_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. Lang [**0**] or Weil [**0**].)

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 [**0**], 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
I-25 distributed modulo 1; however, one knows that this sequence is not uniformly distributed for any measure on $\mathbb{R}/\mathbb{Z}$ (cf. Pólya & Szegő [**0,** pp. 179–180]).

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. IV. 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:

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

I-26 we have

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

The function L has been considered by Tate [**0**]. 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

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

where the $\lambda_v^{(j)}$ are the eigenvalues of x_v in the given representation. Now the I-27
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

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

I-28 where $\phi(s)$ is holomorphic for $\Re(s) > \frac{1}{2}$. Moreover, by hypothesis, L'/L can be extended to a meromorphic function on $\Re(s) \geq 1$ which is holomorphic except possibly for a simple pole at $s = 1$ with residue $-c_\chi$. One may then apply the Wiener-Ikehara theorem (cf. [**0,** p. 123]):

Theorem 1. *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

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

I-29 where d is the degree of the given representation ρ; this is possible since $\chi(x_v)$ is a sum of d complex numbers of absolute value 1, hence $|\chi(x_v)| \leq d$; moreover, the series

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

differs from the logarithmic derivative of

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

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

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

Consequently, by the Abel summation trick (cf. [**0,** p. 124], 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. Weil [**0**], §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 $\mathbb{G}_{m,\overline{\mathbb{Q}}} \times \ldots \times \mathbb{G}_{m,\overline{\mathbb{Q}}}$ II-2 (d times). More precisely, let Γ be the set of embeddings of K into $\overline{\mathbb{Q}}$; each $\sigma \in \Gamma$ extends to a homomorphism $K \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$, hence defines a morphism $[\sigma]\colon \mathbb{T}_{/\overline{\mathbb{Q}}} \to \mathbb{G}_{m,\overline{Q}}$. The collection of all $[\sigma]$'s gives the isomorphism $T_{/\overline{\mathbb{Q}}} \to G_{m/\overline{\mathbb{Q}}} \times \ldots \times G_{m/\overline{\mathbb{Q}}}$. Moreover, the $[\sigma]$'s form a basis of the *character group* $X(T) = \mathrm{Hom}_{\overline{\mathbb{Q}}}(\mathbb{T}_{/\overline{\mathbb{Q}}}, \mathbb{G}_{m,\overline{\mathbb{Q}}})$ of T. Note that the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts in a natural way on $X(T)$, viz. by permuting the $[\sigma]'s$. (For the dictionary between tori and Galois modules, see for instance T. Ono [**0**].)

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 **??**.)

1.3 Enlarging groups

Let k be a field and A a commutative algebraic group over k. Let

$$0 \longrightarrow Y_1 \longrightarrow Y_2 \longrightarrow Y_3 \longrightarrow 0 \qquad \text{(II.1)}$$

an exact sequence of (abstract) commutative groups, with Y_3 *finite*. Let

$$\varepsilon : Y_1 \to A(k)$$

be a homomorphism of Y_1 into the group of k-rational points of A. We intend to construct an algebraic group B, together with a morphism of algebraic groups $A \to B$ and a homomorphism of Y_2 into $B(k)$ such that,

(a) *the diagram*

$$\begin{tikzcd} Y_1 \arrow[r] \arrow[d] & A(k) \arrow[d] \\ Y_2 \arrow[r] & B(k) \end{tikzcd}$$

is commutative,

(b) *B is "universal" with respect to* (a).

The universality of B means that, for any algebraic group B' over k and morphism $A \to B'$, $Y_2 \to B'(k)$ such that (a) is true (with B replaced by B'), there exists a unique algebraic morphism $f : B \to B'$ such that the given maps $A \to B'$ and $Y_2 \to B(k)$ can be obtained by composing those of II-4
B with f. (In other words, B is a *push-out* over Y_1 of A and the "constant" group scheme defined by Y_2.)

The uniqueness of B is assured by its universality. Let us prove its existence. For each $y \in Y_3$ let $\overline{y}$ be a representative of y in Y_2. If y, $y' \in Y_3$, we have

$$\overline{y} + \overline{y'} = \overline{y + y'} + c(y, y')$$

with $c(y, y') \in Y_1$; the cochain c is a 2-cocycle defining the extension II.1. Let B be the disjoint union of copies A_y of A, indexed by $y \in Y_3$. Define a group law on B via the mappings

$$\pi_{y,y'} : A_y \times A_{y'} \to A_{y+y'} \qquad (y,\ y' \in Y_3),$$

given by addition in A followed by translation by $\varepsilon(c(y, y'))$. One then checks easily that B has the required universal property, the maps $A \to B$ and $Y_2 \to B(k)$ being defined as follows:

$A \to B$ is the natural map $A \to A_0$ followed by translation by $-c(0, 0)$,

$Y_2 \to B(k)$ maps an element $\overline{y} + z$, $y \in Y_3$, $z \in Y_1$ onto the image of z in A_y.

Note that for any extension *field* k' of k we have an *exact sequence*

$$0 \longrightarrow A(k') \longrightarrow B(k') \longrightarrow Y_3 \longrightarrow 0,$$

and a *commutative diagram* II-5

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Y_1 & \longrightarrow & Y_2 & \longrightarrow & Y_3 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A(k') & \longrightarrow & B(k') & \longrightarrow & Y_3 & \longrightarrow & 0
\end{array}$$

The algebraic group B is thus an *extension* of the "constant" algebraic group Y_3 by A.

Remark. 1) Let k' be an extension of k and $A' = A \times_k k'$. We may apply the above construction to the k'-algebraic group A', with respect to the exact sequence II.1 and to the map $Y_1 \to A(k) \to A'(k')$. The group B' thus obtained is canonically isomorphic to $B \times_k k'$; this follows, for instance, from the explicit construction of B and B'.

2) We will only use the above construction when $\mathrm{char}(k) = 0$ and A is a torus. The enlarged group B is then a "group of multiplicative type"; this means that, after a suitable finite extension of the ground field, B becomes isomorphic to the product of a torus and a finite abelian group. Such a group is uniquely determined by its character group $X(B) = \mathrm{Hom}_{\overline{k}}(B_{/\overline{k}}, \mathbb{G}_{m,\overline{k}})$, which is a Galois-module of finite type over $\mathbb{Z}$. Here $X(B)$ can be described as the set of pairs (ϕ, χ), where $\phi \colon Y_2 \to \overline{k}^{\times}$ is a homomorphism and $\chi \in Z(A)$ is such that $\phi(y_1) = \chi(y_1)$ for all $y_1 \in Y_1$. Note that this gives an alternate definition of B.

Exercise.

a) Let k' be a commutative k-algebra, with $k' \neq 0$, and $\mathrm{Spec}(k')$ connected (i.e. k' contains exactly two idempotents: 0 and 1). Show the existence
II-6 of an exact sequence:

$$0 \longrightarrow A(k') \longrightarrow B(k') \longrightarrow Y_3 \longrightarrow 0.$$

b) What happens when $\mathrm{Spec}(k')$ is not connected?

§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 archimedian 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 Cassels & Fröhlich [**0**], Lang [**0**] or Weil [**0**].)

Let S be a finite subset of M_K^0. Then by a ***modulus of support*** S we II-7
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 $v \in M_K^0 - S$. 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 ([**0**], see also [**0**], n° 3.5) every subgroup of finite index in E contains an $E_{\mathfrak{m}}$ for a suitable modulus $\mathfrak{m}$.)

Let $I_{\mathfrak{m}}$ be the quotient $I/U_{\mathfrak{m}}$ and $C_{\mathfrak{m}}$ the quotient $I/K^\times U_{\mathfrak{m}} = C/(\text{Image of } U_{\mathfrak{m}} \text{ in } C_{\mathfrak{m}})$. 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 [**0**], [**0**]). 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 Cassels & Fröhlich [**0**]), 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-8

$U_{v,\mathfrak{m}}$ 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 $v \in M_K^\infty - S$. 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 $S_\mathfrak{m}$

We are now in a position to apply the group construction of 1.3. We take for exact sequence II.1 the sequence

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

and for A the algebraic group $T_\mathfrak{m} = \mathbb{T}/\overline{E_\mathfrak{m}}$, where $E_\mathfrak{m}$ is as before, $\mathbb{T}$ is the
II-9 torus $\mathfrak{R}_{K/\mathbb{Q}}(\mathbb{G}_{m,K})$ defined in 1.1, and $\overline{E_\mathfrak{m}}$ is the Zariski closure of $E_\mathfrak{m}$ in $\mathbb{T}$, cf. 1.2.

The construction of 1.3 now yields a $\mathbb{Q}$-*algebraic group* $S_\mathfrak{m}$ with an algebraic morphism $T_\mathfrak{m} \to S_\mathfrak{m}$ and a group homomorphism $\varepsilon_\mathfrak{m} \to S_\mathfrak{m}(\mathbb{Q})$. The sequence

$$1 \longrightarrow T_\mathfrak{m} \longrightarrow S_\mathfrak{m} \longrightarrow C_\mathfrak{m} \longrightarrow 1$$

is exact ($C_\mathfrak{m}$ being identified with the corresponding constant algebraic group) and the diagram

$$\begin{tikzcd}
1 \arrow[r] & K^\times/E_\mathfrak{m} \arrow[r] \arrow[d] & I_\mathfrak{m} \arrow[r] \arrow[d, "\varepsilon"] & C_\mathfrak{m} \arrow[r] \arrow[d, "\mathrm{id}"] & 1 \\
1 \arrow[r] & T_\mathfrak{m}(\mathbb{Q}) \arrow[r] & S_\mathfrak{m}(\mathbb{Q}) \arrow[r] & C_\mathfrak{m} \arrow[r] & 1
\end{tikzcd} \qquad (**)$$

is commutative.

Remark. Let $\mathfrak{m}'$ be another modulus; assume $\mathfrak{m}' \geq \mathfrak{m}$, i.e. $\mathrm{Supp}(\mathfrak{m}') \supset \mathrm{Supp}(\mathfrak{m})$ and $\mathfrak{m}'_v \geq \mathfrak{m}_v$ if $v \in \mathrm{Supp}(\mathfrak{m})$. From the inclusion $U_{\mathfrak{m}'} \subset U_\mathfrak{m}$ one deduces maps $T_{\mathfrak{m}'} \to T_\mathfrak{m}$ and $I_{\mathfrak{m}'} \to I_\mathfrak{m}$, whence a morphism $S_{\mathfrak{m}'} \to S_\mathfrak{m}$. Hence the $S_\mathfrak{m}$'s form a projective system; their limit is a proalgebraic group over $\mathbb{Q}$, extension of the profinite group $C/D = \varprojlim C_\mathfrak{m}$ by a torus.

Exercises.

1) Let $\overline{E_\mathfrak{m}}(\mathbb{Q})$ be the Zariski-closure of $E_\mathfrak{m}$ in $K^\times = (\mathbb{Q})$. Show that the kernel of $\varepsilon_\mathfrak{m} \colon I/U_\mathfrak{m} \to S_\mathfrak{m}(\mathbb{Q})$ is the image of $\overline{E_\mathfrak{m}}(\mathbb{Q}) \to I/U_\mathfrak{m}$.

2) Let $H_{\mathfrak{m}'/\mathfrak{m}}$ be the kernel of $S_{\mathfrak{m}'} \to S_\mathfrak{m}$, where $\mathfrak{m}'_v \geq \mathfrak{m}_v$. II-10

   a) Show that $H_{\mathfrak{m}'/\mathfrak{m}}$ is a finite subgroup of $S_{\mathfrak{m}'}(\mathbb{Q})$ and that it is contained in the image of $\varepsilon_{\mathfrak{m}'}$.

   b) Construct an exact sequence (cf. Exer. 1)

$$1 \longrightarrow \left(E_\mathfrak{m} \cap \overline{E_{\mathfrak{m}'}}(\mathbb{Q})\right)/E_{\mathfrak{m}'} \longrightarrow U_\mathfrak{m}/U_{\mathfrak{m}'} \longrightarrow H_{\mathfrak{m}'/\mathfrak{m}} \longrightarrow 1.$$

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 $\pi \colon \mathbb{T} \to S_\mathfrak{m}$ be the algebraic morphism $\mathbb{T} \to T_\mathfrak{m} \to S_\mathfrak{m}$; by taking points with values in $\mathbb{Q}_\ell$, π defines a homomorphism

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

Since $K \otimes \mathbb{Q}_\ell = \prod_{v|\ell} K_v$, the group $\mathbb{T}(\mathbb{Q}_\ell)$ 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

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

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.

Now, let $\varepsilon_\ell \colon I \to S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ be defined by II-11

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

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

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

II-12 *c) If $v \notin \mathrm{Supp}(\mathfrak{m}) \cup S_\ell$, then the Frobenius element F_{v,ε_ℓ} (cf. Chap. I, 2.3) 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). $\square$

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-13

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.

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 $X(H)$. II-14

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 $\overline{k}$.

II-15 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.

Proposition 1. *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

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

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 restriction of scalars to k, a representation ϕ of H of degree $[k_\chi : k]$. One sees II-16
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 1.1. *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 2. *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. $\square$

Lemma 1. *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-17 (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. $\square$

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. $\square$

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 $\overline{\mathbb{Q}}$, 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 $S_{\mathfrak{m}}$

II-18

1. ℓ-adic case. Let V_ℓ be a finite-dimensional $\mathbb{Q}_\ell$-vector space and
$$\phi\colon S_{\mathfrak{m}/\mathbb{Q}_\ell} \to \mathrm{GL}_{V_\ell}$$

a linear representation of $S_{\mathfrak{m}/\mathbb{Q}_\ell}$ in V_ℓ. This defines a homomorphism

$$\phi\colon S_{\mathfrak{m}}(\mathbb{Q}_\ell) \to \mathrm{GL}_{V_\ell}(\mathbb{Q}_\ell) = \mathrm{Aut}(V_\ell)$$

which is continuous for the ℓ-adic topologies of those groups.

By composition with the map $\varepsilon_\ell\colon G^{\mathrm{ab}} \to S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ defined in 2.3, we get a map

$$\phi_\ell = \phi \circ \varepsilon\colon G^{\mathrm{ab}} \to \mathrm{Aut}(V_\ell),$$

i.e. an *abelian ℓ-adic representation of K* in V_ℓ.

Belén ♡: Lo dejo cómo G o como galois de algo

Proposition 1. *a) The representation ϕ_ℓ is semi-simple.*

b) Let $v \in M_K^0$, with $v \notin \mathrm{Supp}(\mathfrak{m})$ and $p_v \neq \ell$.

Then ϕ_ℓ is unramified at v; the corresponding Frobenius element $F_{v,\phi_v} \in \mathrm{Aut}(V_\ell)$ is equal to $\phi(F_v)$, where F_v denotes the element of $S_{\mathfrak{m}}(\mathbb{Q})$ defined in 2.3. II-19

Belén ♡: no pertence?

c) The representation ϕ_ℓ is rational (Chap. I, 2.3) if and only if ϕ can be defined over $\mathbb{Q}$ (cf. 2.4).

Since $S_{\mathfrak{m}}$ is a group of multiplicative type, all its representations can be brought to diagonal form on a suitable extension of the ground field; hence a). Assertion b) follows from 2.3, and assertion c) follows from prop. 2 of 2.4.

Remark. Let us identify ϕ_ℓ with the corresponding homomorphism of the idèle group I into $\mathrm{Aut}(V_\ell)$. Then

d) $\mathrm{Ker}(\phi_\ell)$ contains $U_{v,\mathfrak{m}}$ if $v \notin \mathrm{Supp}(\mathfrak{m})$, $p_v \neq \ell$.

e) Let $\phi_T\colon T_{/\mathbb{Q}_\ell} \to \mathrm{GL}_{V_\ell}$ be defined by composing $T_{/\mathbb{Q}_\ell} \to S_{\mathfrak{m}/\mathbb{Q}_\ell}$ with ϕ. If x belongs to the open subgroup $U_{\ell,\mathfrak{m}} = \prod_{v|\ell} U_{v,\mathfrak{m}}$ of $T(\mathbb{Q}_\ell)$, one has

$$\phi_\ell(x) = \phi_T(x^{-1}).$$

These properties follow readily from those of ε_ℓ.

Es T de toro?

2. The rational case. Let now V_0 be a finite dimensional vector space over $\mathbb{Q}$ and $\phi_0\colon S_{\mathfrak{m}} \to \mathrm{GL}_{V_0}$ a linear representation of $S_{\mathfrak{m}}$. For each prime number ℓ we may apply the preceding construction to the representation $\phi_{0/\ell}\colon S_{\mathfrak{m}/\mathbb{Q}_\ell} \to \mathrm{GL}(V_\ell)$, where $V_\ell = V_0 \otimes \mathbb{Q}_\ell$; we then get an ℓ-adic representation $\phi_\ell\colon G^{\mathrm{ab}} \to$ II-20
$\mathrm{Aut}(V_\ell)$.

Theorem 1. *1) The ϕ_ℓ form a strictly compatible system of rational abelian semi-simple representations. Its exceptional set is contained in* $\mathrm{Supp}(\mathfrak{m})$.

2) For each $v \notin \mathrm{Supp}(\mathfrak{m})$ the Frobenius element of v with respect to the system (ϕ_ℓ) is the element $\phi_0(F_v)$ of $\mathrm{Aut}(V_0)$.

3) There exist infinitely many primes ℓ such that ϕ_ℓ is diagonalizable over $\mathbb{Q}_\ell$.

The first two assertions follow directly from the proposition above. To prove the third one, note first that there exists a finite extension E of $\mathbb{Q}$ over which ϕ_0 becomes diagonalizable. If ℓ is a prime number which splits completely in E, one can embed E into $\mathbb{Q}_\ell$ and this shows that ϕ_ℓ is diagonalizable. Assertion 3) now follows from the well-known fact that there exist infinitely many such ℓ (this is, for instance, a consequence of Čebotarev's theorem, cf. Chap. I, 2.2).

Remark. The Frobenius elements $\phi_0(F_v) \in \mathrm{Aut}(V_0)$ can also be defined using the homomorphism

$$\phi_0 \circ \varepsilon\colon I \longrightarrow S_{\mathfrak{m}}(\mathbb{Q}) \longrightarrow \mathrm{Aut}(V_0).$$

Note that their eigenvalues generate *a finite extension* of $\mathbb{Q}$; indeed they are contained in any field over which ϕ_0 can be brought in diagonal form.

II-21

Exercises.

1) Let $\phi_0\colon S_{\mathfrak{m}} \to \mathrm{GL}_{V_0}$ be a linear representation of $S_{\mathfrak{m}}$, and let ℓ be a prime number.

   a) Show that the Zariski closure of $\mathrm{Im}(\phi_\ell)$ is the algebraic group $\phi_0(S_{\mathfrak{m}})$. (Use the fact that $(\mathrm{Im}(\varepsilon_\ell))$ is Zariski dense in $S_{\mathfrak{m}}$, cf. 2.3.)

b) Let $\mathfrak{s}_{\mathfrak{m}}$ be the Lie algebra of $S_{\mathfrak{m}}$ and $\phi_0(\mathfrak{s}_{\mathfrak{m}})$ be its image by ϕ_0, i.e. the Lie algebra of $\phi_0(S_{\mathfrak{m}})$. Show that the Lie algebra of the ℓ-adic Lie group $\mathrm{Im}(\phi_\ell)$ is $\phi_0(\mathfrak{s}_{\mathfrak{m}}) \otimes \mathbb{Q}_\ell$. (Use the fact that $\mathrm{Im}(\varepsilon_\ell)$ is open in $S_{\mathfrak{m}}(\mathbb{Q}_\ell)$, cf. 2.3.)

2) a) Show that there exists a unique one-dimensional representation

$$\mathbf{N}\colon S_{\mathfrak{m}} \to \mathbb{G}_m$$

such that $\mathbf{N}(F_v) = \mathbf{N}\,v \in \mathbb{Q}^\times$ for all $v \notin \mathrm{Supp}(\mathfrak{m})$.

b) Show that the morphism $T \longrightarrow S_{\mathfrak{m}} \xrightarrow{\mathbf{N}} \mathbb{G}_m$ is the one induced by the norm map from K to $\mathbb{Q}$.

c) Show that the ℓ-adic representation defined by $\mathbf{N}$ is isomorphic to the representation $V_\ell(\mu)$ defined in Chap. I, 1.2.

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-22

Proposition 1. *Let $f\colon I \to \mathrm{Aut}(V_0)$ be a homomorphism. There exists a $\phi_0\colon S_{\mathfrak{m}} \to \mathrm{GL}_{V_0}$ 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 $\psi\colon \mathbb{T} \to \mathrm{GL}_{V_0}$ such that $\psi(x) = f(x)$ for every $x \in K^\times = \mathbb{T}(\mathbb{Q})$.

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 $\phi_0 \colon S_{\mathfrak{m}} \to \mathrm{GL}_{V_0}$, 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-23 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 $\psi \colon \mathbb{T} \to \mathrm{GL}_{V_0}$ 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

The preceding constructions are relative to a given prime number ℓ. However, they have an archimedean analogue, as follows:

Let $\pi \colon \mathbb{T} \to S_{\mathfrak{m}}$ be the canonical map defined in 2.3, and let

$$\pi_\infty \colon \mathbb{T}(R) \to S_{\mathfrak{m}}(R)$$

be the corresponding homomorphism of real Lie groups. Since $\mathbb{T}(R) = (K \otimes R)^\times = \prod_{v \in M_K^\infty} K_v^\times$, we can identify $\mathbb{T}(R)$ with a direct factor of the idèle
II-24 group I. Let pr_∞ be the projection on this factor; the map

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

is continuous, and one checks as in 2.3 that α_∞ coincides with ε on $K^\times$. One may then define a map

$$\varepsilon_\infty \colon I \to S_{\mathfrak{m}}(R)$$

by

$$\varepsilon_\infty(a) = \varepsilon(a)\alpha_\infty(a^{-1}).$$

One has $\varepsilon_\infty(a) = 1$ if $a \in K^\times$, hence ε_∞ may be viewed as *a homomorphism of the idèle class group $C = I/K^\times$ into the real Lie gruop $S_{\mathfrak{m}}(R)$*.

The main difference with the "finite" case is that ε_∞ *is not trivial on the connected component of C*, hence has no Galois group interpretation.

When one composes $\varepsilon_\infty\colon C \to S_{\mathfrak{m}}(R)$ with a complex character $S_{\mathfrak{m}/C} \to \mathbb{G}_{m,C}$, one gets a homomorphism $C \to C^\times$, i.e. that the characters obtained in this way coincide with the "Größencharakter of type (A_0)" of Weil (cf. [**0**], [**41**]), whose conductor divide $\mathfrak{m}$.

Exercise. Let II-25

$$e\colon I \to S_{\mathfrak{m}}(R) \times \prod_{\ell} S_{\mathfrak{m}}(\mathbb{Q}_\ell)$$

be the map defined by ε_∞ and the ε_ℓ's.

a) Show that the image of e is contained in the subgroup $S_{\mathfrak{m}}(A)$ of $S_{\mathfrak{m}}(R) \times \prod_\ell S_{\mathfrak{m}}(\mathbb{Q}_\ell)$, where A denote the ring of adèles of $\mathbb{Q}$, and that $e\colon I \to S_{\mathfrak{m}}(A)$ is continuous (for the natural topology of the adelized group $S_{\mathfrak{m}}(A)$).

b) Let $\pi_A\colon T(A) \to S_{\mathfrak{m}}(A)$ be the map defined by $\pi\colon \mathbb{T} \to S_{\mathfrak{m}}$. Show that, if one identifies $\mathbb{T}(A)$ with I in the obvious way, one has

$$e(x) = \varepsilon(x)\pi_A(x^{-1})$$

where $\varepsilon\colon I \to S_{\mathfrak{m}}(\mathbb{Q}) \subset S_{\mathfrak{m}}$ is the map defined in 2.3. [Note that this gives an alternate definition of the ε_ℓ's.]

c) Show that $\varepsilon(I)$ is not open in $S_{\mathfrak{m}}(A)$ if $C_{\mathfrak{m}} \neq \{1\}$.

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 Shimura & Taniyama [**0**], Taniyama [**0**], **41** [**41**], [**42**] and Serre & Tate [**0**].)

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-26

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

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 1. *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*
II-27 *ℓ-adic representations of K with values in T_E (in the sense of Chap. I, 2.4).*

(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 reduction". If $v \notin S$, and $\ell \neq p_v$, one shows easily that p_ℓ is unramified at II-28
v (the converse is also true, see [**0**]); 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. [**0,** p. 39]). 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 Shimura & Taniyama [**0**] (see also [**0**]). Note that one could express them (as in 2.6) 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 [**0,** p. 148], 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-29
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 $X(T_{\mathfrak{m}})$

If w is a complex place of $\overline{\mathbb{Q}}$, the completion of $\overline{\mathbb{Q}}$ with respect to w is isomorphic to $\mathbb{C}$; the decomposition group of ω is thus cyclic of order 2; its non-trivial element will be denoted by c_w (the "Frobenius at the infinite place w"). The c_w's are conjugate in $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$; let C_∞ denote their conjugacy class. (By a theorem of Artin [**0,** p. 257], the elements of C_∞ are the only non-trivial elements of finite order in G.)

Let $X(\mathbb{T})$ be the character group of the torus $\mathbb{T}$, cf. 1.1; we write $X(\mathbb{T})$ additively and put $Y(\mathbb{T}) = X(\mathbb{T}) \otimes_{\mathbb{Z}} \mathbb{Q}$. We decompose Y as a direct sum $Y = Y^0 \oplus Y^- \oplus Y^+$ of G-invariant subspaces, as follows (cf. Appendix, A.2)

$$\begin{aligned} Y^0 &= Y^G = \{y \in Y \mid gy = y \text{ for all } g \in G\} \\ Y^- &= \{y \in Y \mid cy = -y \text{ for all } c \in C_\infty\} \end{aligned}$$

II-30 and Y^+ is a G-invariant supplement to $Y^0 \oplus Y^-$ in Y; one proves easily that Y^+ is unique, cf. Appendix, *loc. cit.*

More explicitly, if $\sigma \in \mathbb{T}$ is an embedding of K into $\overline{\mathbb{Q}}$, let $[\sigma] \in X(\mathbb{T})$ be the corresponding character of T; the $[\sigma]$'s, $\sigma \in \Gamma$, form a basis of $X(\mathbb{T})$ and $g \cdot [\sigma] = [g \circ \sigma]$ if $g \in G$. The space Y^0 is generated by the norm element $\sum_{\sigma\in\Gamma}[\sigma]$, and its G-invariant supplement is

$$Y^- \oplus Y^+ = \left\{ \sum_{\sigma\in\Gamma} b_\sigma\,[\sigma] \mid b_\sigma \in \mathbb{Q},\ \sum_{\sigma\in\Gamma} b_\sigma = 0 \right\}.$$

Hence, any character $\chi \in X(\mathbb{T})$ can be written in the form

$$\chi = a \sum_{\sigma\in\Gamma} [\sigma] + \sum_{\sigma\in\Gamma} b_\sigma\,[\sigma] \tag{$*$}$$

$$a, b_\sigma \in \mathbb{Q},\ \sum_{\sigma} b_\sigma = 0,\ a + b_\sigma \in \mathbb{Z}.$$

(In particular, we see that $da \in \mathbb{Z}$ where $d = [K : \mathbb{Q}]$.) The subspace Y^- can now be described as follows

$$Y^- = \left\{ \sum_\sigma b_\sigma\,[\sigma] \mid b_\sigma \in \mathbb{Q},\ \sum_\sigma b_\sigma = 0,\ b_{c\sigma} = -b_\sigma \text{ for all } c \in C_\infty \text{ and } \sigma \in \Gamma \right\}.$$

On the other hand, the projection $\mathbb{T} \to T_{\mathfrak{m}}$ defines an injection of $X(T_{\mathfrak{m}})$ into $X(\mathbb{T})$; we identify $X(T_{\mathfrak{m}})$ with its image under this injection.

Proposition 1. *$X(T_{\mathfrak{m}}) \otimes_{\mathbb{Z}} \mathbb{Q} = Y^0 \oplus Y^-$.*

This follows from Appendix, A.2.

II-31

Corollary 1.1. *The character group $X(T_{\mathfrak{m}})$ is a sublattice of finite index of $X(\mathbb{T}) \cap (Y^0 \oplus Y^-)$.*

Corollary 1.2. *If $\chi \in X(\mathbb{T})$ is written in the form $(*)$, then $2a \in \mathbb{Z}$.*

In fact, given $c \in C_\infty$ and $\sigma \in \Gamma$, we have

$$2a = 2a + b_\sigma + b_{c\sigma} = (a + b_\sigma) + (a + b_{c\sigma}) \in \mathbb{Z}.$$

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

We have seen that any character $\chi \in X(T_{\mathfrak{m}})$ can be written in the form

$$\chi = a \sum_{\sigma\in\Gamma} [\sigma] + \sum_{\sigma\in\Gamma} b_\sigma [\sigma]$$

with $a, b_\sigma \in \mathbb{Q}$, $\sum b_\sigma = 0$, $2a \in \mathbb{Z}$. Hence $\chi \mapsto 2a$ defines a homomorphism $j\colon X(T_{\mathfrak{m}}) \to X(\mathbb{G}_m) = \mathbb{Z}$ and we obtain by duality a morphism of algebraic groups $j^*\colon \mathbb{G}_m \to T_{\mathfrak{m}}$. If $\phi_0\colon S_{\mathfrak{m}} \to \mathrm{GL}_{V_0}$ is a representation of $S_{\mathfrak{m}}$, we obtain by composition with j^* a morphism of algebraic groups $\mathbb{G}_m \to \mathrm{GL}_{V_0}$. This representation of $\mathbb{G}_m$ defines (and is defined by) a grading $V_0 = \sum_{i\in\mathbb{Z}} V_0^{(i)}$ of V_0; recall that $\mathbb{G}_m$ acts on $V_0^{(i)}$ by means of the character $i \in \mathbb{Z} = X(\mathbb{G}_m)$.

We say that V_0 is homogeneous of degree n if $V_0 = V_0^{(n)}$. II-32

Remark. For representations coming from the ℓ-adic homology $H_*(\overline{X})$ of a projective smooth variety X, the grading defined above should coincide with the natural one: $H_*(\overline{X}) = \sum_i H_i(\overline{X})$.

Exercise.

1) Let $\mathbf{N}\colon S_{\mathfrak{m}} \to \mathbb{G}_m$ be the morphism defined in Exercise 2) of 2.5. Show that $\mathbf{N} \circ j\colon \mathbb{G}_m \to S_{\mathfrak{m}} \to \mathbb{G}_m$ is $\lambda \mapsto \lambda^2$. Show that any morphism $S_{\mathfrak{m}} \to \mathbb{G}_m$ is equal to $\varepsilon\, \mathbf{N}^n$, where ε is a character of $C_{\mathfrak{m}}$ with values in $\{\pm 1\}$ and $n \in \mathbb{Z}$.

2) Let $\phi\colon S_{\mathfrak{m}} \to \mathrm{GL}_{V_0}$ be a linear representation of $S_{\mathfrak{m}}$.

   Assume ϕ is homogeneous of degree d, and put $h = \dim_{V_0}$.

   a) Show that dh is even (apply Exerc. 1 to $\det(\phi)\colon S_{\mathfrak{m}} \to \mathbb{G}_m$).

   b) Prove that there exists on V_0 a positive definite quadratic form $\mathbb{Q}$ such that
   $$\mathbb{Q}(\rho(x)y) = \mathbf{N}(x)^d \mathbb{Q}(y)$$
   for any $y \in V_0$ and any $x \in S_{\mathfrak{m}}(\mathbb{Q})$. [Let H be the kernel of $\mathbf{N}\colon S_{\mathfrak{m}} \to \mathbb{G}_m$. Using the fact that $H(R)$ is compact, prove the existence of a positive definite quadratic form $\mathbb{Q}$ on V_0 invariant by H; then note that $S_{\mathfrak{m}}$ is generated by H and $j^*(\mathbb{G}_m)$.]

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.
II-33 3.1). There is a unique continuous homomorphism $\varepsilon\colon H_c \to \{\pm 1\}$ such that $\varepsilon(c) = -1$ 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. [**0,** p. 4]) 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.*

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 II-34

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

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-35

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.

3.4 How to compute Frobeniuses

Belen.

§A. Killing arithmetic groups in tori

A.1 Arithmetic groups in tori

Let A be a linear algebraic group over $\mathbb{Q}$, and let Γ be a subgroup of the group $A(\mathbb{Q})$ of rational points of A. Then Γ is said to be an ***arithmetic***
II-36 ***subgroup*** if for any algebraic embedding $A \subseteq \mathrm{GL}_n$ (n arbitrary) the groups Γ and $A(\mathbb{Q}) \cap \mathrm{GL}_n(\mathbb{Z})$ are ***commensurable*** (two subgroups Γ_1, Γ_2 are said to be commensurable if $\Gamma_1 \cap \Gamma_2$ is of finite index in Γ_1 and Γ_2). It is well-known that it suffices to check that Γ and $A(\mathbb{Q}) \cap \mathrm{GL}_n(\mathbb{Z})$ are commensurable for one embedding $A \subseteq \mathrm{GL}_n$.

Examples. Let K be a number field and let E be the group of units of K. Then E is an arithmetic subgroup of $\mathbb{T} = \mathfrak{R}_{K/\mathbb{Q}}(\mathbb{G}_m)$.

If $\mathbb{T}$ is a torus over $\mathbb{Q}$, let $\mathbb{T}^0$ be the intersection of the kernels of the homomorphisms of $\mathbb{T}$ into $\mathbb{G}_m$. The torus $\mathbb{T}$ is said to be ***anisotropic*** if $\mathbb{T} = \mathbb{T}^0$; in terms of the character group $X = X(\mathbb{T})$ this means that X has no non-zero elements which are left fixed by $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Theorem 1. *Let $\mathbb{T}$ be a torus over $\mathbb{Q}$, and let Γ be an arithmetic subgroup of $\mathbb{T}$. Then $\Gamma \cap \mathbb{T}^0$ is of finite index in Γ, and the quotient $\mathbb{T}^0(R)/\Gamma \cap \mathbb{T}^0$ is compact.*

This is due to T. Ono; for a proof of a more general statement ("Godement's conjecture") see Mostow & Tamagawa [**0**].

Corollary 1.1. *Let $\mathbb{T}$ be a torus over $\mathbb{Q}$, and let Γ be an arithmetic subgroup of $\mathbb{T}$. If $\mathbb{T}$ is anisotropic, then $\mathbb{T}(R)/\Gamma$ is compact.*

II-37
Exercise. Let $\mathbb{T}$ be a torus over $\mathbb{Q}$, with character group X.

a) Show that
$$\mathbb{T}(\mathbb{Q}) = \mathrm{Hom}_{\mathrm{Gal}}(X, \overline{\mathbb{Q}}^{\times}).$$

b) Let U be the subgroup of $\overline{\mathbb{Q}}^{\times}$ whose elements are the algebraic units of $\overline{\mathbb{Q}}$. Let
$$\Gamma = \mathrm{Hom}_{\mathrm{Gal}}(X, U)$$
Show that Γ is an arithmetic subgroup of $\mathbb{T}(\mathbb{Q})$ and that any arithmetic subgroup of $\mathbb{T}(\mathbb{Q})$ is contained in T.

A.2 Killing arithmetic subgroups

Let $\mathbb{T}$ be a torus over $\mathbb{Q}$, and let $X(\mathbb{T})$ be its character group; put $Y(\mathbb{T}) = X(\mathbb{T}) \otimes_{\mathbb{Z}} \mathbb{Q}$. Let Λ be the set of classes of $\mathbb{Q}$-irreducible representations of $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ through its finite quotients. For each $\lambda \in \Lambda$, let Y be the corresponding isotypic sub-G-module of Y, i.e. the sum of all sub-G-modules of Y isomorphic to λ. One has the direct sum decomposition
$$Y = \coprod_{\lambda \in \Lambda} Y_\lambda$$
Let $Y^0 = Y_1$, where 1 is the unit representation of G; let Y^- be the sum of those Y where for all the infinite Frobeniuses $c \in C_\infty$ (cf. 3.1) we have $\lambda(c) = -1$; let Y^+ be the sum of the other Y_λ. We have II-38
$$\begin{aligned} Y^0 &= Y^G = \{y \in Y \mid gy = y \text{ for all } g \in G\} \\ Y^- &= \{y \in Y \mid cy = -y \text{ for all } c \in C_\infty\}, \\ Y &= Y^0 \oplus Y^- \oplus Y^+. \end{aligned}$$
Note that $Y = Y^0$ if and only if $\mathbb{T}$ is anisotropic. If $c \in C_\infty$, and $H = \{1, c\}$, then, since $\mathbb{T}(\mathbb{R}) = \mathrm{Hom}_H(X(\mathbb{T}), \mathbb{C}^\times)$, we see that $\mathbb{T}(\mathbb{R})$ *is compact if and only if* $Y = Y^-$.

Proposition 1. *Let Γ be an arithmetic subgroup of the torus $\mathbb{T}$, and $\overline{\Gamma}$ its Zariski closure (cf. 1.2). Then:*
$$Y(\mathbb{T}/\overline{\Gamma}) = Y^0 \oplus Y^-. \qquad (*)$$

[Since the torus $\mathbb{T}/\overline{\Gamma}$ is a quotient of $\mathbb{T}$, we identify $Y(\mathbb{T}/\overline{\Gamma})$ with a submodule of $Y(\mathbb{T})$.]

Proof. Suppose first that Y is *irreducible*, i.e. that $\mathbb{T}$ has no proper subtori and is $\neq 0$.

If $Y = Y^0$, then $\mathbb{T}$ is isomorphic to $\mathbb{G}_m$ and hence Γ is finite. This shows that $Y(\mathbb{T}/\overline{\Gamma}) = Y(\mathbb{T})$, hence $(*)$. If $Y = Y^-$, then $\mathbb{T}(\mathbb{R})$ is compact. Since Γ is a discrete subgroup of $\mathbb{T}(\mathbb{R})$, it is finite. Hence $Y(\mathbb{T}/\overline{\Gamma}) = Y(\mathbb{T})$ and $(*)$ follows.

If $Y = Y^+$, then $\mathbb{T}(\mathbb{R})$ is not compact. Consequently, Γ is infinite since $\mathbb{T}(\mathbb{R})/\mathbb{T}$ is compact by Ono's theorem. Hence $\overline{\Gamma}$ is an algebraic subgroup of $\mathbb{T}$ of dimension ≥ 1. Its connected component is a non-trivial subtorus of $\mathbb{T}$. This shows that $\overline{\Gamma} = \mathbb{T}$, hence $Y(\mathbb{T}/\overline{\Gamma}) = 0$. Hence again $(*)$.

II-39 The general case follows easily from the irreducible one; for instance, choose a torus $\mathbb{T}'$ to $\mathbb{T}$ which splits in direct product of irreducible tori and note that Γ is commensurable with the image by $\mathbb{T}' \to \mathbb{T}$ of an arithmetic subgroup of $\mathbb{T}$. □

Exercise. Let $y \in Y$. Define $\mathrm{N}\,y$ as the mean value of the transforms of y by G.

a. Prove that N is a G-linear projection of Y onto Y^0 hence $\mathrm{Ker}(\mathrm{N}) = Y^- \oplus Y^+$.

b. Prove that Y is generated by the elements $cy + y$, with $y \in \mathrm{Ker}(\mathrm{N})$ and $c \in C_\infty$.

CHAPTER III

LOCALLY ALGEBRAIC ABELIAN REPRESENTATIONS

In this Chapter, we define what it means for an abelian ℓ-adic representation to be *locally algebraic* and we prove (cf. 2.3) that such a representation, when rational, comes from a linear representation of one of the groups $S_{\mathfrak{m}}$ of Chapter II.

When the ground field is a composite of quadratic extensions of $\mathbb{Q}$, any rational semi-simple ℓ-adic representation is *ipso facto* locally algebraic; this is proved in §3, as a consequence of a result on transcendental numbers due to Siegel and Lang.

In the local case, an abelian semi-simple representation is locally algebraic if and only if it has a "Hodge-Tate decomposition". This fact, due to Tate (College de France, 1966), is proved in the Appendix, together with some complements.

§1. The local case

1.1 Definitions

Let p be a prime number and K a finite extension of $\mathbb{Q}_p$; let $\mathbb{T} = \mathfrak{R}_{K/\mathbb{Q}_p}(\mathbb{G}_{m,K})$ be the corresponding algebraic torus over $\mathbb{Q}_p$ (cf. Weil [**0**], III-1
Chap. I).

Belén.

1.2 Alternative definition of "locally algebraic" via Hodge-Tate modules

Let us recall first the notion of a ***Hodge-Tate module*** (cf. [**0**], §2); here K is only assumed to be complete with respect to a discrete valuation, with perfect residue field k and $\mathrm{char}(K) = 0$, $\mathrm{char}(k) = p$. Denote by C the *completion* $\widehat{\overline{K}}$ *of the algebraic closure* of K.

The group $G = \mathrm{Gal}(\overline{K}/K)$ acts continuously on K. This action extends continuously to C. Let W be a C-vector space of finite dimension upon which G acts continuously and semi-linearly according to the formula

$$s(cw) = s(c) \cdot s(w) \qquad (s \in G,\ c \in C \text{ and } w \in W).$$

Let $\chi\colon G \to U_p$ be the homomorphism of G into the group $U_p = \mathbb{Z}_p^\times$ of p-adic
III-2 units, defined by its action on the p^ν-th roots of unity (cf. chap. I, 1.2):

$$s(z) = z^{\chi(s)} \qquad \text{if } s \in G \text{ and } z^{p^\nu} = 1.$$

Define for every $i \in \mathbb{Z}$ the subspace

$$W^i = \{w \in W \mid sw = \chi(s)^i w \text{ for all } s \in G\}$$

of W. This is a K-vector subspace of W. Let $W(i) = C \otimes_K W^i$. This is a C-vector space upon which G acts in a natural way (i.e. by the formula $s(c \otimes y) = s(c) \otimes s(y)$). The inclusion $W^i \to W$ extends uniquely to a C-linear map $\alpha_i\colon W(i) \to W$, which commutes with the action of G.

Proposition 1 (Tate)**.** *Let $\coprod_{i\in\mathbb{Z}} W(i)$ be the direct sum of the $W(i)$. Let $\alpha\colon \coprod_i W(i) \to W$ be the sum of the α_i's defined above. Then α is injective.*

For the proof see [**0**], §2, prop. 4.

Corollary 1.1. *The K-spaces W^i ($i \in \mathbb{Z}$) are of finite dimension. They are linearly independent over C.*

Definition 1. The module W is of ***Hodge-Tate type*** if the homomorphism $\alpha\colon \coprod_{i\in\mathbb{Z}} W(i) \to W$ is an isomorphism.

Let now V be as in 1.1, a vector space over $\mathbb{Q}_p$, of finite dimension. Let $\rho\colon G \to \mathrm{Aut}(V)$ be a p-adic representation. Let $W = C \otimes_{\mathbb{Q}_p} V$ and let G act
III-3 on W by the formula

$$s(c \otimes v) = s(c) \otimes s(v) \qquad s \in \Gamma,\ c \in C,\ v \in V.$$

Definition 2. The representation ρ is of ***Hodge-Tate type*** if the C-space $W = C \otimes_{\mathbb{Q}_p} V$ is of Hodge-Tate type (cf. def. 1).

Examples. Let F be a p-divisible group of finite height (cf. [**0**], [**39**]); let T be its Tate module (*loc. cit.*) and $V = \mathbb{Q}_p \otimes T$. The group G acts on V, and Tate has proved ([**39**], Cor. 2 to Th. 3) that this Galois module is of Hodge-Tate type; more precisely, one has $W = W(0) \oplus W(1)$, where $W = C \otimes V$ as above.

Theorem 1 (Tate)**.** *Assume K is a finite extension of $\mathbb{Q}_p$ (i.e. its residue field is finite). Let $\rho\colon G \to \mathrm{Aut}(V)$ be an abelian p-adic representation of K. The following properties are equivalent:*

(a) ρ is locally algebraic (cf. 1.1).

(b) ρ is of Hodge-Tate type and its restriction to the inertia group is semi-simple.

For the proof, see the Appendix.

§2. The global case

2.1 Definitions

Belén.

2.2 Modulus of a locally algebraic abelian representation

Let $\rho\colon \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \to \mathrm{Aut}(V_\ell)$ be as above; by composition with the class field homomorphism $i\colon I \to \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$, ρ defines a homomorphism $\rho \circ i\colon I \to \mathrm{Aut}(V_\ell)$.

We assume that ρ is locally algebraic and we denote by f the associated algebraic morphism $T_{/\mathbb{Q}_\ell} \to \mathrm{GL}_{V_\ell}$. III-4

Definition 1. Let $\mathfrak{m}$ be a modulus (chap. II, 1.1). One says that ρ is defined mod $\mathfrak{m}$ (or that $\mathfrak{m}$ is a modulus of definition for ρ) if

(i) $\rho \circ i$ is trivial on $U_{v,\mathfrak{m}}$ when $p_v \neq \ell$.

(ii) $\rho \circ i_\ell(x) = f(x^{-1})$ for $x \in \prod_{v|\ell} U_{v,\mathfrak{m}}$.

(Note that $\prod_{v|\ell} U_{v,\mathfrak{m}}$ is an open subgroup of $K_\ell^\times = T_{/\mathbb{Q}_\ell}(\mathbb{Q}_\ell)$.)

In order to prove the existence of a modulus of definition, we need the following auxiliary result:

Proposition 1. *Let H be a Lie group over Q_ℓ (resp. $\mathbb{R}$) and let α be a continuous homomorphism of the idèle group I into H.*

(a) If $p_v \neq \ell$ (resp. $p_v \neq \infty$), the restriction of α to K is equal to 1 on an open subgroup of $K_v^\times$.

(b) The restriction of α to the unit group U_v of $K_v^\times$ is equal to 1 for almost all v's.

Proof. Part (a) follows from the fact that $K_v^\times$ is a p_v-adic Lie group and that a homomorphism of a p-adic Lie group into an ℓ-adic one is locally equal to 1 if $p \neq \ell$.

To prove (b), let N be a neighborhood of 1 in H which contains no finite subgroup except $\{1\}$; the existence of such an N is classical for real Lie groups, and quite easy to prove for ℓ-adic ones. By definition of the idèle topology, $\alpha(U_v)$ is contained in N for almost all v's. But (a) shows that, if
III-5 $p_v \neq \ell$, the group $\alpha(U_v)$ is finite; hence $\alpha(U_v) = \{1\}$ for almost all v's. □

Corollary 1.1. *Any abelian ℓ-adic representation of K is unramified outside a finite set of places.*

This follows from (b) applied to the homomorphism α of I induced by the given representation, since the $\alpha(U_v)$ are known to be the inertia subgroups.

Remark. This does not extend to non-abelian representations (even solvable ones), cf. Exercise.

Proposition 2. *Every locally algebraic abelian ℓ-adic representation has a modulus of definition.*

Let $\rho\colon \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \to \mathrm{Aut}(V_\ell)$ be the given representation and f the associated morphism of $T_{/\mathbb{Q}_\ell}$ into GL_{V_ℓ}. Let X be the set of places $v \in M_K^0$, with $p_v \neq \ell$, for which ρ is ramified; the corollary 1.1 to Prop. 1 shows that X is finite. By Prop. 1, (a), we can choose a modulus $\mathfrak{m}$ such that $\rho \circ i\colon I \to \mathrm{Aut}(V_\ell)$ is trivial on all the $U_{v,\mathfrak{m}}$, $v \in X$. Enlarging $\mathfrak{m}$ if necessary, we can assume that $\rho \circ i_\ell(x) = f(x^{-1})$ for $x \in \prod_{p_v=\ell} U_{v,\mathfrak{m}}$. Hence, $\mathfrak{m}$ is a modulus of definition for ρ.

Remark. It is easy to show that there is a smallest modulus of definition for ρ; it is called the ***conductor*** of ρ.

Exercise. Let $z_1, \dots, z_n, \dots \in K^\times$. For each n, let E_n be the subfield of $\overline{K}$ generated by all the ℓ^n-th roots of the element $z_1 z_2^{\ell} \cdots z_n^{\ell^{n-1}}$. III-6

a) Show that E_n is a Galois extension of K, containing the ℓ^n-th roots of unity and that its Galois group is isomorphic to a subgroup of the affine group $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$ in $\mathrm{GL}(2, \mathbb{Z}/\ell^n\mathbb{Z})$.

b) Let E be the union of the E_n's. Show that E is a Galois extension of K, whose Galois group is a closed subgroup of the affine group relative to $\mathbb{Z}_\ell$.

c) Give an example where E (and hence the corresponding 2-dimensional ℓ-adic representation) is ramified at all places of K.

2.3 Back to $S_{\mathfrak{m}}$

Let $\mathfrak{m}$ be a modulus of K and let

$$\phi\colon S_{\mathfrak{m}/\mathbb{Q}_\ell} \longrightarrow \mathrm{GL}_{V_\ell}$$

be a linear representation of $S_{\mathfrak{m}/\mathbb{Q}_\ell}$. Let

$$\phi_\ell\colon\ \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \longrightarrow \mathrm{Aut}(V_\ell)$$

be the corresponding ℓ-adic representation (cf. chap. II, 2.5).

Theorem 1. *The representation ϕ_ℓ is locally algebraic and defined mod $\mathfrak{m}$. The associated algebraic morphism* III-7

$$f\colon \mathbb{T}_{/\mathbb{Q}_\ell} \longrightarrow \mathrm{GL}_{V_\ell}$$

is $\phi \circ \pi$, where π denotes the canonical morphism of $\mathbb{T}$ into $S_{\mathfrak{m}}$ (cf. chap. II, 2.2).

This is trivial from the construction of ϕ_ℓ as $\phi \circ \varepsilon$ (chap. II, 2.5) and the corresponding properties of ε_ℓ (chap. II, 2.3).

The converse of Theorem 1 is true. We state it only for the case of rational representations:

Theorem 2. *Let $\rho\colon \operatorname{Gal}(\overline{K}/K)^{\mathrm{ab}} \to \operatorname{Aut}(V_\ell)$ be an abelian ℓ-adic representation of the number field K. Assume ρ is rational (chap. I, 2.3) and is locally algebraic with $\mathfrak{m}$ as a modulus of definition (cf. 2.2). Then, there exist a $\mathbb{Q}$-vector subspace V_0 of V_ℓ, with $V_\ell = V_0 \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, and a morphism $\phi_0\colon S_{\mathfrak{m}} \to \mathrm{GL}_{V_\ell}$ of $\mathbb{Q}$-algebraic groups such that ρ is equal to the ℓ-adic representation ϕ_ℓ associated to ϕ_0 (cf. chap. II, 2.5).*

(The condition $V_\ell = V_0 \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ means that V_0 is a "$\mathbb{Q}$-structure" on V_ℓ, cf. Bourbaki Alg., chap. II, 3rd ed.)

Proof. Let $r\colon \mathbb{T}_{/\mathbb{Q}_\ell} \to \mathrm{GL}_{V_\ell}$ be the algebraic morphism associated with ρ. We have

$$\rho \circ i(x) = r(x^{-1}) \qquad \text{for } x \in K_\ell^\times \cap U_{\mathfrak{m}} = \prod_{v \mid \ell} U_{v,\mathfrak{m}}$$

III-8 Define a map $\psi\colon I \to \operatorname{Aut}(V_\ell)$ by

$$\psi(x) = \rho \circ i(x) \cdot r(x_\ell)$$

José: ¿Estandarizar notación $\boldsymbol{x}$ para idèles?

where x_ℓ is the ℓ^{th} component of the idèle x. One checks immediately that *ψ is trivial on $U_{\mathfrak{m}}$ and coincides with r on $K^\times$*. Hence r is trivial on $E_{\mathfrak{m}} = K^\times \cap U_{\mathfrak{m}}$ and factors through an algebraic morphism $r_{\mathfrak{m}}\colon T_{\mathfrak{m}/\mathbb{Q}_\ell} \to \mathrm{GL}_{V_\ell}$. By the universal property of the $\mathbb{Q}_\ell$-algebraic group $S_{\mathfrak{m}/\mathbb{Q}_\ell}$ (cf. chap. II, 1.3 and 2.2), there exists an algebraic morphism

$$\phi\colon S_{\mathfrak{m}/\mathbb{Q}_\ell} \longrightarrow \mathrm{GL}_{V_\ell}$$

with the following properties:

(a) The morphism $T_{\mathfrak{m}/\mathbb{Q}_\ell} \longrightarrow S_{\mathfrak{m}/\mathbb{Q}_\ell} \xrightarrow{\phi} \mathrm{GL}_{V_\ell}$ is $r_{\mathfrak{m}}$.

(b) The map $I \xrightarrow{\varepsilon} S_{\mathfrak{m}}(\mathbb{Q}_\ell) \xrightarrow{\phi} \operatorname{Aut}(V_\ell)$ is ψ.

It is trivial to check that the ℓ-adic representation ϕ_ℓ attached to ϕ as above coincides with ρ. Indeed, if $a \in I$, we have (with the notations of chap. II)

$$\begin{aligned}\phi_\ell \circ i(a) &= \phi(\varepsilon_\ell(a)) = \phi(\varepsilon(a))\phi(\pi_\ell(a_\ell^{-1})) = \psi(a)\phi(\pi_\ell(a_\ell^{-1}))\\ &= \rho \circ i(a) r(a_\ell)\phi(\pi_\ell(a_\ell^{-1})) = \rho \circ i(a).\end{aligned}$$

III-9 since $\phi \circ \pi_\ell = r$ by (a) above.

Hence $\phi_\ell = \rho$; the fact that ρ is *rational* then implies that ϕ *can be defined over* $\mathbb{Q}$ (chap. II, 2.4, Prop.), and this gives V_0 and ϕ_0. □

Remark. The subspace V_0 of V_ℓ constructed in the proof of the theorem is *not* unique; however, any other choice gives us a space of the form σV_0, where σ is an automorphism of V_ℓ commuting with ρ. To a given V_0 corresponds of course a unique ϕ.

Corollary 2.1. *For each prime number ℓ' there exists a unique (up to isomorphism) ℓ'-adic rational semi-simple representation ρ of K, compatible with ρ. It is abelian and locally algebraic. These representations form a strictly compatible system (cf. chap. I, 2.3) with exceptional set contained in* $\mathrm{Supp}(\mathfrak{m})$. *For an infinite number of ℓ', $\rho_{\ell'}$ can be brought in diagonal form.*

Proof. The unicity of the $\rho_{\ell'}$, follows from the theorem of chap. I, 2.3. For the existence, take $\rho_{\ell'}$ to be the $\phi_{\ell'}$ associated to ϕ as in chapter II, 2.5. The remaining assertion follows from the proposition in chap. II, 2.5. □

Corollary 2.2. *The eigenvalues of the Frobenius elements $F_{v,\rho}$ ($v \notin \mathrm{Supp}(\mathfrak{m})$, $p_v \neq \ell$) generate a finite extension of $\mathbb{Q}$.*

This follows from the corresponding property of ϕ_ℓ, cf. chapter II, 2.5, Remark **??**.

2.4 A mild generalization

Belén.

2.5 The function field case

The above constructions have a (rather elementary) analogue for *function fields of one variable over a finite field:*

Let K be such a field, and let p be its characteristic. If $\mathfrak{m}$ is a modulus for K (i.e. a positive divisor) we define the subgroup $U_\mathfrak{m}$ of the idèle group I as in chap. II, 2.1, and we put

$$\Gamma_\mathfrak{m} = I/U_\mathfrak{m}K^\times.$$

The degree map $\deg\colon I \to \mathbb{Z}$ is trivial on $U_\mathfrak{m}$, hence defines an exact sequence III-10

$$1 \longrightarrow J_\mathfrak{m} \longrightarrow \Gamma_\mathfrak{m} \longrightarrow \mathbb{Z} \longrightarrow 1.$$

One sees easily that the group $J_{\mathfrak{m}}$ is finite; moreover, it may be interpreted as the group of rational points of the "generalized Jacobian variety defined by $\mathfrak{m}$". If $\widehat{\Gamma}_{\mathfrak{m}}$ denotes the completion of r with respect to the topology of subgroups of finite index, it is known (class field theory) that $\mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \cong \varprojlim_{\mathfrak{m}} \widehat{\Gamma}_{\mathfrak{m}}$.

Let now $\rho\colon \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \to \mathrm{Aut}(V_\ell)$ be an abelian ℓ-adic representation of K, with $\ell \neq p$. One proves as in 2.2 that there exists a modulus $\mathfrak{m}$ such that ρ is trivial on $U_{\mathfrak{m}}$, i.e. such that ρ may be identified with a *homomorphism of* $\widehat{\Gamma}_{\mathfrak{m}}$ *into* $\mathrm{Aut}(V_\ell)$. Moreover

Proposition 1. *A homomorphism $\phi\colon \Gamma_{\mathfrak{m}} \to \mathrm{Aut}(V_\ell)$ can be extended to a continuous homomorphism of $\widehat{\Gamma}_{\mathfrak{m}}$ if and only if there exists a lattice of V_ℓ which is stable by $\rho(\Gamma_{\mathfrak{m}})$.*

The necessity follows from Remark 1 of chap. I, 1.1. The sufficiency is clear.

Note that, as in the number field case, we have Frobenius elements and we can define the notion of *rationality* of an ℓ-adic representation.

Theorem 1. *An abelian ℓ-adic representation*

$$\phi\colon \widehat{\Gamma}_{\mathfrak{m}} \to \mathrm{Aut}(V_\ell)$$

III-11 *of K is rational if and only if $\mathrm{Tr}\,\phi(\gamma)$ belongs to $\mathbb{Q}$ for every $y \in \Gamma_{\mathfrak{m}}$.*

If $v \notin \mathrm{Supp}(\mathfrak{m})$, and if f_v is a uniformizing parameter at v, the image F_v of f_v in $\Gamma_{\mathfrak{m}}$ is the Frobenius element of the Galois group $\widehat{\Gamma}_{\mathfrak{m}}$. Hence, if $\mathrm{Tr}\,\phi$ takes rational values on $\Gamma_{\mathfrak{m}}$, the characteristic polynomial of $\phi(F_v)$ has rational coefficients for all $v \notin \mathrm{Supp}(\mathfrak{m})$ and ϕ is rational.

To prove the converse, note first that Čebotarev's theorem (Chap. I, 2.2) is valid for K, if one uses a somewhat weaker definition of equipartition. Hence, the Frobenius elements F_v are *dense* in $\widehat{\Gamma}_{\mathfrak{m}}$. In particular, they generate $\Gamma_{\mathfrak{m}}$, and, from this, one sees that $\mathrm{Tr}\,\rho(\gamma)$ belongs to some number field E. We can then construct an E-linear representation $\phi\colon \Gamma_{\mathfrak{m}} \to \mathrm{GL}(n, E)$ with the same trace as ρ, and the theorem follows from:

Lemma 1. *Let Γ be a finitely generated abelian group, and $\phi\colon \Gamma \to \mathrm{GL}(n, E)$ a linear representation of Γ over a number field E. Let Σ be a subset of Γ, which is dense in Γ for the topology of subgroups of finite index. Assume that $\mathrm{Tr}\,\phi(\gamma) \in \mathbb{Q}$ for all $\gamma \in \Sigma$. Then $\mathrm{Tr}\,\phi(\gamma) \in \mathbb{Q}$ for all $\gamma \in \Gamma$.*

Proof. Since $\phi(\Gamma)$ is finitely generated, there is a finite S of places of E such that all the elements of $\phi(\Gamma)$ are S-integral matrices. If ℓ' is a prime number not divisible by any element of S, the image of $\phi(\Gamma)$ in $\mathrm{GL}(n, E \otimes \mathbb{Q}_{\ell'})$ is contained in a compact subgroup of $\mathrm{GL}(n, E \otimes \mathbb{Q}_{\ell'})$; hence ϕ extends by continuity to III-12

$$\widehat{\phi}\colon \widehat{\Gamma} \to \mathrm{GL}(n, E \otimes \mathbb{Q}_{\ell'})$$

where $\widehat{\Gamma}$ is the completion of Γ for the topology of subgroups of finite index. Since Σ is dense in $\widehat{\Gamma}$, it follows that $\mathrm{Tr}\,\widehat{\phi}(\hat{\gamma})$ belongs to the adherence $\mathbb{Q}_{\ell'}$ of $\mathbb{Q}$ in $E \otimes \mathbb{Q}_{\ell'}$ for every $\hat{\gamma} \in \widehat{\Gamma}$. Hence, if $\gamma \in \Gamma$, we have

$$\mathrm{Tr}\,\phi(\Gamma) \in E \cap \mathbb{Q}_{\ell'} = \mathbb{Q}. \qquad \square$$

Exercises.

1) Let $\phi\colon \widehat{\Gamma}_{\mathfrak{m}} \to \mathrm{Aut}(V_\ell)$ be a semi-simple ℓ-adic representation of $\Gamma_{\mathfrak{m}}$. Show the equivalence of:

   (a) ϕ extends continuously to $\widehat{\Gamma}_{\mathfrak{m}}$.

   (b) For every $\gamma \in \Gamma_{\mathfrak{m}}$, the eigenvalues of $\phi(\gamma)$ are units (in a suitable extension of $\mathbb{Q}_\ell$).

   (c) There exists $\gamma \in \Gamma_{\mathfrak{m}}$, with $\deg(\gamma) \neq 0$, such that the eigenvalues of $\phi(\gamma)$ are units.

   (d) For every $\gamma \in \Gamma_{\mathfrak{m}}$, one has $\mathrm{Tr}\,\phi(\gamma) \in \mathbb{Z}_\ell$.

2) Let $\phi\colon \widehat{\Gamma}_{\mathfrak{m}} \to \mathrm{Aut}(V_\ell)$ be a rational ℓ-adic representation of K. Show that, for almost all prime number ℓ', there is a rational ℓ'-adic representation of K compatible with ϕ. Show that this holds for all $\ell' \neq p$ if and only if the following property is valid: for all $\gamma \in \Gamma_{\mathfrak{m}}$, the coefficients of the characteristic polynomial of $\phi(\gamma)$ are p-integers.

§3. The case of a composite of quadratic fields

III-13

3.1 Statement of the result

Belén.

3.2 A criterion for local algebraicity

Proposition 1. *Let $\rho\colon \mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} \to \mathrm{Aut}(V_\ell)$ be a rational semi-simple ℓ-adic abelian representation of K. Assume that there exists an integer $N \geq 1$ such that ρ^N is locally algebraic. Then ρ is locally algebraic.*

III-14 *Proof.* Since ρ is semi-simple, it can be brought in diagonal form over a finite extension of $\mathbb{Q}_\ell$, hence gives rise to a family $\{\psi_1, \dots, \psi_n\}$ of n continuous characters $\psi_i\colon C_K \to \overline{\mathbb{Q}}_\ell^\times$, where C_K is the idèle-class group of K, and $n = \dim V_\ell$. Let $\chi_1 = \psi_1^N, \dots, \chi_n = \psi_n^N$ be the corresponding characters occurring in ρ^N. Since ρ^N is locally algebraic, to each χ_i^N corresponds an algebraic character $\chi_i^{\mathrm{alg}} \in X(\mathbb{T})$ of the torus $\mathbb{T}$ (here we identify $X(\mathbb{T})$ with $\mathrm{Hom}(\mathbb{T}_{/\overline{\mathbb{Q}}_\ell}, \mathbb{G}_{m,\overline{\mathbb{Q}}_\ell})$, since $\overline{\mathbb{Q}}_\ell$ is algebraically closed). Each χ_i^{alg} is of the form $\prod_{\sigma\in\Gamma}[\sigma]^{n_\sigma(i)}$, where Γ is the set of embeddings of K into $\overline{\mathbb{Q}}_\ell$, cf. Chap. II, 1.1. One has

$$\chi_i(x) = \chi_i^{\mathrm{alg}}(x^{-1}) = \prod_{\sigma\in\Gamma} \sigma(x)^{-n_\sigma(i)}$$

for all $x \in K_\ell^\times$ close enough to 1. □

Lemma 1. *All the integers $n_\sigma(i)$, $1 \leq i \leq n$, $\sigma \in \Gamma$, are divisible by N.*

Proof. Let U be an open subgroup of $\overline{\mathbb{Q}}_\ell^\times$ containing no N^{th}-root of unity except 1, and let $\mathfrak{m}$ be a modulus of K such that $\psi_i(x) \in U$ for all $x \in U_\mathfrak{m}$ and $i = 1, \dots, n$; the existence of such an $\mathfrak{m}$ follows from the continuity of $\psi_1, \dots, \psi_n$. We take $\mathfrak{m}$ large enough so that:

a) It is a modulus of definition for ρ^N.

b) ρ is unramified at all $v \in \mathrm{Supp}(\mathfrak{m})$, and the corresponding Frobenius
III-15 elements $F_{v,\rho}$ have a characteristic polynomial with rational coefficients.

Let $K_\mathfrak{m}$ be the abelian extension of K corresponding to the open subgroup $K^\times U_\mathfrak{m}$ of the idèle group I, and let L be a finite Galois extension of $\mathbb{Q}$ containing $K_\mathfrak{m}$. Choose a prime number p which is distinct from 1, is not divisible by any place of $\mathrm{Supp}(\mathfrak{m})$, and splits completely in L. Let v be a place of K dividing p, and let f_v be an idèle which is a uniformizing element at v and is equal to 1 elsewhere. The fact that v splits completely in $K_\mathfrak{m}$ (since it does in L) implies that f_v is the norm of an idèle of $K_\mathfrak{m}$, hence (by class-field theory) belongs to $K^\times U_\mathfrak{m}$; this means that the prime ideal $\mathfrak{p}_v$ is a principal ideal (α), with $\alpha \equiv 1 \mod \mathfrak{m}$ and α positive at all real places of K.

Let $x = \psi_i(f_v)$ and $y = \chi_i(f_v)$, so that $y = x^N$; these are the Frobenius elements of ψ_i and χ_i relative to v. By definition of χ_i^{alg}. we have

$$y = \chi_i^{\mathrm{alg}}(\alpha) = \prod_{\sigma\in\Gamma} \sigma(\alpha)^{n_\sigma(i)}$$

where α is as above.

Hence y belongs to the subfield $\widetilde{L}$ of $\mathbb{Q}$ corresponding to L (this field is well defined since L is a Galois extension of $\mathbb{Q}$). Moreover, if w_σ is any place of L such that $w_\sigma \circ \sigma$ induces v on K, we have (as in chap. II, 3.4):

$$w_\sigma(y) = n_\sigma(i).$$

Assume now that $n_\sigma(i)$ is not divisible by N. Then x, which is an N^{th}-root of y, does not belong to $\widetilde{L}$. Hence there is a non-trivial N^{th}-root of unity z III-16
such that x and zx are conjugate over $\widetilde{L}$, and *a fortiori* over $\mathbb{Q}$. Since the characteristic polynomial of $F_{v,\rho}$ has rational coefficients, any coniugate over $\mathbb{Q}$ of an eigenvalue of $F_{v,\rho}$ is again an eigenvalue of $F_{v,\rho}$. Hence, there exists an index j such that

$$\psi_j(f_v) = z\,x = z\,\psi_i(f_v).$$

But $f_v \in K^\times U_\mathfrak{m}$ and all ψ_j are trivial on $K^\times$ and map $U_\mathfrak{m}$ into the open subgroup U we started with. Hence $z = \psi_j(f_v)\,\psi_i(f_v)^{-1}$ belongs to U, and this contradicts the way $U_\mathfrak{m}$ has been chosen. □

Proof of the proposition. Since the $n_\sigma(i)$ are divisible by N, there exist $\varphi_i \in X(\mathbb{T})$ with $\varphi_i^N = \chi_i^{\mathrm{alg}}$. If $x \in K_\ell^\times$, we have:

$$\varphi_i(x^{-1})^N = \chi_i^{\mathrm{alg}}(x^{-1}) = \chi_i(x) = \psi_i(x)^N$$

if x is close enough to 1. Hence $\varphi_i(x)\psi_i(x)$ is an N^{th}-root of unity when x is close enough to 1, and, by continuity, it is equal to 1 in a neighbourhood of 1. Hence, the restriction of ρ to $K_\ell^\times$ is locally equal to φ^{-1}, where φ is the (algebraic) representation of $\mathbb{T}$ defined by the family $(\varphi_1, \ldots, \varphi_n)$. The representation φ, *a priori* defined over $\overline{\mathbb{Q}}_\ell$, can be defined over $\mathbb{Q}_\ell$ (and even over $\mathbb{Q}$); this follows, for instance, from the fact that the family $(\varphi_1, \ldots, \varphi_n)$ is *stable* under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, since the family $(\chi_1^{\mathrm{alg}}, \ldots, \chi_n^{\mathrm{alg}})$ is.

Hence ρ is locally algebraic. □

3.3 An auxiliary result on tori

In [**0**], Lang proved that two exponential functions $\exp(b_1 z)$, $\exp(b_2 z)$, $b_1, b_2 \in \mathbb{C}$, which take algebraic values for at least three $\mathbb{Q}$-linearly independent values of z, are multiplicatively dependent: the ratio b_1/b_2 is a rational number. This had also been noticed by Siegel.

Lang proved the following ℓ-adic analogue:

Proposition 1. *Let E be a field containing $\mathbb{Q}_\ell$ and complete for a real valuation extending the valuation of $\mathbb{Q}_\ell$. Let $b_1, b_2 \in E$ and let Γ be an additive subgroup of E. Assume:*

1) Γ *is of rank at least 3 over* $\mathbb{Z}$.

2) The exponential series $\exp(z) = \sum_{n=1}^{\infty} z^n/n!$ *converges absolutely on* $b_1\Gamma$ *and* $b_2\Gamma$.

3) For all $z \in \Gamma$ *the elements* $\exp(b_1 z)$ *and* $\exp(b_2 z)$ *are algebraic over* $\mathbb{Q}$.

Then b_1 *and* b_2 *are linearly dependent over* $\mathbb{Q}$ *(i.e.* b_1/b_2 *belongs to* $\mathbb{Q}$ *if* $b_2 \neq 0$*).*

For the proof, see [**0**], Appendix, or [**30**], §1.

We will apply this result to tori, taking for E the completion of $\overline{\mathbb{Q}}_\ell$. We need a few definitions first:

a/ Let T be an n-dimensional torus over $\mathbb{Q}$, with character group $X(T)$. As before, we identify $X(T)$ with the group of morphisms of $T_{/E}$ into $\mathbb{G}_{m,E}$. We say that T *is a sum of one-dimensional tori* if there exist one-dimensional subtori T_i of T, $1 \leq i \leq n$, such that the sum map $T_1 \times \cdots \times T_n \to T$ is surjective (and hence has a finite kernel). An equivalent condition is:

III-17 $X(T) \otimes \mathbb{Q}$ *is a direct sum of one-dimensional subspaces stable by* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

b/ Let f be a continuous homomorphism of $T(\mathbb{Q}_\ell)$ into E. We say that f is ***locally algebraic*** if there is a neighbourhood U of 1 in the ℓ-adic Lie group $T(\mathbb{Q}_\ell)$, and an element $\varphi \in X(T)$ such that $f(x) = \varphi(x)$ for all $x \in U$. We say that f is ***almost locally algebraic*** if there is an integer $N \geq 1$ such that f^N is locally algebraic.

c/ Let S be a finite set of prime numbers, and, for each $p \in S$, let W_p be an open subgroup of $T(\mathbb{Q}_p)$; denote by W the family $(W_p)_{p\in S}$.

Let $T(\mathbb{Q})_W$ be the set of elements $x \in T(\mathbb{Q})$ whose images in $T(\mathbb{Q}_p)$ belong to W for all $p \in S$; this is a subgroup of $T(\mathbb{Q})$. With these notations, we have:

Proposition 2. *Let $f\colon T(\mathbb{Q}_\ell) \to E^\times$ be a continuous homomorphism. Assume:*

(a) There exists a family $W = (W_p)_{p\in S}$ such that $f(x)$ is algebraic over $\mathbb{Q}$ for all $x \in T(\mathbb{Q})_W$.

(b) T is a sum of one-dimensional tori.

Then f is almost locally algebraic.

Proof.

i) We suppose first that T is *one-dimensional*, and we denote by χ a generator of $X(T)$. If χ is invariant by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, T is isomorphic to $\mathbb{G}_m$ and $T(\mathbb{Q}) \cong \mathbb{Q}^\times$. If not, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $X(T)$ *via* a group of order 2, corresponding to some quadratic extension F of $\mathbb{Q}$; the III-18
character χ defines an isomorphism of $T(\mathbb{Q})$ onto the group $F_1^\times$ of elements of F of norm 1. In both cases, one sees that $T(\mathbb{Q})$ is an abelian group of *infinite rank* (for a more precise result, see Exercise below). On the other hand, each quotient $T(\mathbb{Q}_p)/W_p$ is a finitely generated abelian group of rank ≤ 1. Hence $T(\mathbb{Q})/T(\mathbb{Q})_W$ is finitely generated, and this implies that $T(\mathbb{Q})_W$ is also of *infinite rank*.

Since $T(\mathbb{Q}_\ell)$ is an ℓ-adic Lie group of dimension 1, it is locally isomorphic to the *additive group* $\mathbb{Q}_\ell$. This means that there exists a homomorphism

$$e\colon \mathbb{Z}_\ell \longrightarrow T(\mathbb{Q}_\ell)$$

which is an isomorphism of $\mathbb{Z}$ onto an open subgroup of $T(\mathbb{Q}_\ell)$. By composition we get two continuous homomorphisms

$$f\circ e\colon \mathbb{Z}_\ell \longrightarrow E^\times, \qquad \chi\circ e\colon \mathbb{Z}_\ell \longrightarrow E^\times.$$

But any continuous homomorphism of $\mathbb{Z}$ into E^* is locally an exponential. This implies that, after replacing $\mathbb{Z}_\ell$ by $\ell^m\mathbb{Z}_\ell$ if necessary, there exist $b_1, b_2 \in E$ such that

$$f\circ e(z) = \exp(b_1 z), \qquad \chi\circ e(z) = \exp(b_2 z),$$

with absolute convergence of the exponential series.

Let now Γ be the set of elements $z \in \mathbb{Z}_\ell$ such that $e(z) \in T(\mathbb{Q})_W$. Since $T(\mathbb{Q}_\ell)/e(\mathbb{Z}_\ell)$ is finitely generated, and $T(\mathbb{Q})_W$ is of infinite rank,
III-19 Γ is of infinite rank. If $z \in \Gamma$, $e(z)$ belongs to $T(\mathbb{Q})_W$, hence $f \circ e(z)$ is algebraic over $\mathbb{Q}$; the same is true for $\chi \circ e(z)$ since χ maps $T(\mathbb{Q})$ either into $\mathbb{Q}^\times$ or into the group F defined above. Proposition 1 then shows that b_1/b_2 is rational. This means that some integral power f^N of f, with $N \geq 1$, is locally equal to an integral power of χ, hence f is *almost locally algebraic*.

ii) *General case*. Write $T = T_1 \cdots T_n$ where $T_1, \ldots, T_n$ are one-dimensional subtori of T. Since $X(T) \otimes \mathbb{Q}$ is the direct sum of the $X(T_i) \otimes \mathbb{Q}$, it is enough to show that, for all i, the restriction f_i of f to $T_i(\mathbb{Q}_\ell)$ is almost locally algebraic. But we may choose open subgroups $W_{i,p}$ of $T_i(\mathbb{Q}_p)$ such that $W_{1,p} \cdots W_{n,p} \subset W_p$. If we put $W_i = (W_{i,p})_{p \in S}$, we then see that f_i takes algebraic values on $T_i(\mathbb{Q})_{W_i}$, hence is almost locally algebraic by i) above. $\square$

Remark. If one could suppress condition (b) from Prop. 2, all the results of this § would extend to arbitrary number fields. This would be possible if one had a sufficiently strong n-dimensional version of Prop. 1 above; the one given in [**30**], §2 does not seem strong enough (it requires density properties which are unknown in the case considered here). $\to$ [This has been done by Waldschmidt: see [**63**], [**83**].]

Exercise. Let T be a non-trivial torus over $\mathbb{Q}$. Show that $T(\mathbb{Q})$ is the direct sum of a finite group and a free abelian group of infinite rank.

3.4 Proof of the theorem

Belén.

§A. Hodge-Tate decompositions and locally algebraic representations

Let K be a field of characteristic zero, complete with respect to a discrete valuation and with perfect residue field k of characteristic $p > 0$. In this

Appendix we deal with Hodge-Tate decomposition of p-adic abelian representations of K.

Sections A.1 and A.2 give invariance properties of these decompositions under ground field extensions. Special characters of $\mathrm{Gal}(\overline{K}/K)$ are defined in A.4; they are closely connected both with Hodge-Tate modules (A.4 and A.5) and local algebraicity (A.6). The proof of Tate's theorem (cf. 1.2) is given in the last section. III-20

A.1 Invariance of Hodge-Tate decompositions

Let C be the completion of $\overline{K}$ (cf. 1.2); the group $\mathrm{Gal}(\overline{K}/K)$ acts continuously on C. Let χ be the character of $\mathrm{Gal}(\overline{K}/K)$ into the group of p-adic units defined in chap. I, 1.2. Let K'/K be a subextension of $\overline{K}/K$ on which the valuation $\overline{v}$ of $\overline{K}$ is discrete; this means that K' is a finite extension of an unramified one of K. Let $\widehat{K'}$ denote the closure of K' in C.

Let now W be a finite dimensional C-vector space on which $\mathrm{Gal}(\overline{K}/K)$ acts continuously and semi-linearly (see 1.2). As before, we denote by W^n (resp. $W^n_{K'}$) the K- (resp. $\widehat{K'}$-)vector space defined by

$$W^n = \{w \in W \mid s(w) = \chi(s)^n w \text{ for all } s \in \mathrm{Gal}(\overline{K}/K) \quad (\text{resp. } s \in \mathrm{Gal}(\overline{K}/K'))\}$$

Let $W(n) = C \otimes_K W^n$ and $W(n)' = C \otimes_{\widehat{K'}} W^n_{K'}$. Identifying the modules $W(n)$ and $W(n)'$ with their canonical images in W, we prove

Theorem 1. *The canonical map $\widehat{K'} \otimes_K W^n \to W^n_{K'}$ is a $\widehat{K'}$-isomorphism.*

Corollary 1.1. *The Galois modules $W(n)$ and $W(n)'$ are equal.* III-21

Indeed, Theorem 1 shows that W^n and $W^n_{K'}$, generate the same C-vector subspace of W.

Corollary 1.2. *The Galois module W is of Hodge-Tate type over K if and only if it is so over $\widehat{K'}$.*

Proof of Theorem 1. Note first that replacing the action of $\mathrm{Gal}(\overline{K}/K)$ on W by $(s, w) \mapsto \chi(s)^{-i} sw$, $i \in \mathbb{Z}$, just changes W^n to W^{n+i}. This shifting process reduces the problem to the case $n = 0$; in that case, W^n (resp. $W^n_{K'}$) is the set of elements of W which are invariant under $\mathrm{Gal}(\overline{K}/K)$ (resp. under

$\mathrm{Gal}(\overline{K}/K'))$. Note also that the injectivity of $\widehat{K'} \otimes W^0 \to W^0_{K'}$ is trivial, since we know that $C \otimes_K W^0 \to W$ is injective (cf. 1.2).

On the other hand, an easy up-and-down argument shows that one can assume K'/K to be either *finite Galois* or *unramified Galois*. In both cases, since $\mathrm{Gal}(\overline{K}/K')$ acts trivially on $W^0_{K'}$, we have a semi-linear action of $\mathrm{Gal}(K'/K)$ on $W^0_{K'}$. When K'/K is finite, it is well known that this implies that $W^0_{K'}$, is generated by the elements invariant by $\mathrm{Gal}(K'/K)$, i.e. by W^0 (this is a non-commutative analogue of Hilbert's "Theorem 90", cf. for instance [**0,** p. 159]).

Let now K'/K be unramified Galois and let G be its Galois group. Let $\widehat{\mathcal{O}'}$ denote the ring of integers of $\widehat{K'}$. Let Λ be an $\widehat{\mathcal{O}'}$-lattice of $W^0_{K'}$ (i.e. a free $\widehat{\mathcal{O}'}$-submodule of $W^0_{K'}$ of the same rank as $W^0_{K'}$). Since G acts continuously on $W^0_{K'}$, the stabilizer in G of Λ is open, hence of finite index, and the lattice
III-22 Λ has finitely many transforms. The sum Λ^0 of these transforms is invariant by G. Let $e_1, \ldots, e_N$ be a basis of Λ^0. Let $s \in G$. Then

$$s(e_j) = \sum_{i=1}^{N} a_{ij}(s) e_i, \qquad a_{ij} \in \widehat{\mathcal{O}'}$$

and the matrix $a(s) = (a_{ij}(s))$ belongs to $\mathrm{GL}(N, \widehat{\mathcal{O}'})$. We have $a(st) = a(s)\, s(a(t))$; this means that a is a *continuous* 1-*cocycle on G with values in* $\mathrm{GL}(N, \widehat{\mathcal{O}'})$. Recall that two such cocycles a and a' are said to be cohomologous if there exists $b \in \mathrm{GL}(N, \widehat{\mathcal{O}'})$ such that $a'(s) = b^{-1} a(s)\, s(b)$ for all $s \in G$. This is an equivalence relation on the set of cocycles and the corresponding quotient space is denoted by $H^1(G, \mathrm{GL}(N, \widehat{\mathcal{O}'}))$. In fact:

Lemma 1. $H^1(G, \mathrm{GL}(N, \widehat{\mathcal{O}'})) = \{1\}$.

Assuming the lemma, the proof of the theorem is concluded as follows. Since $a(s)$ is cohomologous to 1, there exists $b \in \mathrm{GL}(N, \widehat{\mathcal{O}'})$ such that $b = a(s)\, s(b)$ for all $s \in G$. If $b = (b_{ij})$, define a new basis $e'_1, \ldots, e'_N$ of $W^0_{K'}$ by

$$e'_j = \sum_{i=1} b_{ij} e_i.$$

Using the identity $b = a(s)\, s(b)$, one sees that $e'_1, \ldots, e'_N$ are invariant under G, hence belong to W^0; this proves the surjectivity of $\widehat{K'} \otimes_K W^0 \to W^0_{K'}$. $\square$

III-23 *Proof of the lemma.* Let π be a uniformizing element of $\widehat{\mathcal{O}'}$. Filter the ring

$A = \mathrm{GL}(N, \widehat{\mathcal{O}'})$ by means of $A_n = \{a \in A \mid a \equiv 1 \mod \pi^n\}$. We get $A/A_1 \cong GL(N, k'/k)$, where k'/k is the residue field extension of K'/K. Moreover, for $n \geq 1$, there is an isomorphism $A_n/A_{n+1} \cong \mathrm{M}_N(k')$, where $\mathrm{M}_N(k')$ is the additive group of $N \times N$ matrices with coefficients in k'. The lemma follows now from the triviality of $H^1(G, \mathrm{GL}(N, k'))$ and $H^1(G, \mathrm{M}_N(k'))$, where now k' is endowed with the discrete topology (so this is ordinary Galois cohomology, cf. [**0,** pp. 158–159]). □

A.2 Admissible characters

Let $G = \mathrm{Gal}(\overline{K}/K)$ and let $\varphi \colon G \to K^\times$ be a continuous homomorphism.

Definition 1. The character φ is said to be ***admissible*** (notation: $\varphi \sim 1$) if there exists $x \in C$, $x \neq 0$, such that $s(x) = \varphi(s)\, x$ for all $s \in G$.

Remark. 1) The admissible characters form a subgroup of the group of all characters of G with values in $K^\times$; if φ, φ' are two characters, we write $\varphi \sim \varphi'$ if $\varphi^{-1}\varphi' \sim 1$.

2) Let $H^1(G, C^\times)$ be the first cohomology group of G with values in C (cohomology being defined by *continuous* cochains, as in A.1). A continuous character $\varphi \colon G \to K^\times$ is a 1-cocycle, hence defines an element $\overline{\varphi}$ of $H^1(G, C^\times)$. One has $\overline{\varphi} = \overline{\varphi'}$ if and only if $\varphi \sim \varphi'$.

3) Define a new action of G on $C^\times$ by means of III-24

$$(s, c) \longmapsto \varphi(s)\, s(c), \qquad s \in G,\ c \in C,$$

Denote the C-G-module thus obtained by $C(\varphi)$. Then φ is admissible if and only if $C(\varphi)$ and C are isomorphic as C-G-modules.

Proposition 1. *Suppose there exists $c \in C^\times$ such that $\varphi(s) = s(c)/c$ for s in some open subgroup N of the inertia group of G. Then φ is admissible.*

Proof. Let K'/K be the subextension of $\overline{K}/K$ corresponding to N; it is a finite extension of an unramified one. Let $W = C(\varphi)$, as in Remark 3, and let W^0 (resp. $W^0_{K'}$) be the subspace of W consisting of elements invariant by G (resp. by N). By hypothesis, $W^0_{K'}$ is $\neq 0$. Hence, by A.1, Theorem 1, we also have $W^0 \neq 0$, and this means that φ is admissible. □

Let now U_C be the group of units of C, U_C^1 the subgroup of units congruent to 1 modulo the maximal ideal, and identify $\overline{k}^\times$ with the group of multiplicative representatives, so that $U_C = U_C^1 \times \overline{k}^\times$, cf. [**0,** p. 44]. Define the logarithm map by

$$\begin{aligned} \log\colon U_C &\longrightarrow C \\ x &\longmapsto \begin{cases} 0, & \text{if } x \in \overline{k}^\times \\ \displaystyle\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n}(x-1)^n, & \text{if } x \in U_C^1 \end{cases} \end{aligned}$$

This is a continuous homomorphism and even a local isomorphism.

A.3 A criterion for local triviality

Belén.

A.4 The character ξ

Belén.

A.5 Characters associated with Hodge-Tate decompositions

Belén.

Theorem 1. *Let ρ, V, W be as above and, for each $\sigma \in \Gamma_E$, let n_σ be an integer. The following are equivalent:*

(i) $\rho \equiv \displaystyle\prod_{\sigma \in \Gamma_E} \sigma^{-1} \circ \chi_{\sigma E}^{n_\sigma}$,

(ii) $\sigma \circ \rho \sim \chi^{n_\sigma}$ *for all* $\sigma \in \Gamma_E$,

(iii) for every $\sigma \in \Gamma_E$ *the Galois-module* W_σ *is isomorphic to* $C(\chi^{n_\sigma})$.

A.6 Locally compact case

We now add to all the previous assumptions regarding K and E, the assumption that K is *finite* over $\mathbb{Q}$ (i.e. K is locally compact). By local class field theory, we may then identify G^{ab} with $\widehat{K}^{\times}$, and the inertia subgroup of G^{ab} with U_K, the group of units of K.

Let T (resp. T_E, $T_{\sigma E}$) be the $\mathbb{Q}_p$-torus associated to K (resp. to E, σE, where $\sigma \in \Gamma_E$), cf. 1.1. The norm map from K to σE defines an algebraic morphism

$$\mathrm{N}_{K/\sigma E}\colon T \longrightarrow T_{\sigma E}.$$

By composition with $\sigma^{-1}\colon T_{\sigma E} \to T_E$, this gives a morphism III-25

$$r_\sigma = \sigma^{-1} \circ \mathrm{N}_{K/\sigma E}\colon T \to T_E.$$

Proposition 1. *(a)* $r_\sigma(u^{-1}) = \sigma^{-1} \circ \chi_{\sigma E}(u)$ *for all* $u \in U_K$,

(b) the r_σ $(\sigma \in \Gamma_E)$ *make a* $\mathbb{Z}$*-basis of* $\mathrm{Hom}_{\mathrm{alg}}(T, T_E)$.

(Note that (a) makes sense, since U_K has been identified with the inertia group of G^{ab}.)

Assertion (a) follows from the remark at the end of A.4. On the other hand, let $X(T)$ and $X(T_E)$ be the character groups of T and T_E respectively. The characters $[s]$, $s \in \Gamma_K$ (resp. (σ), $\sigma \in \Gamma_E$) make a basis of $X(T)$ (resp. of $X(T_E)$). The morphism $r_\sigma\colon T \to T_E$ defines by transposition a homomorphism

$$X(r_\sigma)\colon X(T_E) \longrightarrow X(T).$$

One checks easily that the effect of $X(r_\sigma)$ on the basis $[\tau]$, $\tau \in \Gamma_E$ is:

$$X(r_\sigma)([\tau]) = \sum_{s\sigma=\tau} [s].$$

Assertion (b) then follows from:

Lemma 1. *The elements* $X(r_\sigma)$, $\sigma \in \Gamma_E$, *form a basis of* $\mathrm{Hom}_{\mathrm{Gal}}(X(T_E),$ III-26
$X(T))$.

Proof. The independence of the $X(r_\sigma)$ is clear. On the other hand, let $\varphi \in \mathrm{Hom}_{\mathrm{Gal}}(X(T_E), X(T))$ be such that

$$\varphi([\tau]) = \sum_s n(\tau, s)[s].$$

If $\alpha \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ is equal to the identity on τE, we have $\alpha[\tau] = [\tau]$, hence $\alpha\varphi([\tau]) = \varphi([\tau])$, i.e. $n(\tau, \alpha s) = n(\tau, s)$ for all $s \in \Gamma_K$. This means that $n(\tau, s)$ depends only on the element $\sigma = s^{-1}\tau$; if we put $n_\sigma = n(\tau, s)$, we then have

$$\varphi([\tau]) = \sum_{\sigma \in \Gamma_E} n_\sigma \sum_{s\sigma = \tau} [s] = \sum_{\sigma \in \Gamma_E} n_\sigma X(r_\sigma)([\tau]).$$

This proves the lemma. □

Proposition 2. *Let ρ and (n_σ), $\sigma \in \Gamma_E$, be as in Th. 1 of A.5. Let $r\colon T \to T_E$ be the morphism defined by*

$$r = \prod_{\sigma \in \Gamma_E} r_\sigma^{n_\sigma}.$$

The equivalent properties (i), (ii), (iii) of Th. 1 are equivalent to:

(iv) There exists an open subgroup U' of the inertia subgroup U_K of G^{ab} such that $r(u)\rho(u) = 1$ if $u \in U'$.

Indeed, (iv) is just a reformulation of (i), since we know that $\sigma^{-1} \circ \chi_{\sigma E}(u) = r_\sigma(u^{-1})$ if $u \in U_K$.

Corollary 2.1. *The following are equivalent:*

(a) ρ is locally algebraic.

(b) The Galois module V attached to ρ is of Hodge-Tate type.

This follows from Theorem 1, combined with Prop. 1 and Prop. 2.

Exercises.

1) a) Let $A = \mathrm{End}_{\mathbb{Q}_p}(K)$ be the space of $\mathbb{Q}_p$-linear endomorphisms of K; if $a \in A$, denote by $\mathrm{Tr}(a)$ the trace of a. If $x \in K$, denote by u_x the endomorphism $y \mapsto xy$ of K. Show that, for any $a \in A$, there exists a unique element $c_K(a)$ of K such that

$$\mathrm{Tr}(u_x \circ a) = \mathrm{Tr}_{K/\mathbb{Q}_p}(x \cdot c_K(a)) \qquad \text{for all } x \in K.$$

b) Show that the map $c_K\colon A \to K$ so defined is K-linear for both the natural structures of K-vector space on A.

III-27 c) Let e_i be a $\mathbb{Q}_p$-basis of K and let e_i' be the dual basis, so that $\mathrm{Tr}_{K/\mathbb{Q}_p}(e_i e_j') = \delta_{ij}$. Show that

$$c_K(a) = \sum_{i=1}^{n} a(e_i)e_i', \qquad \text{if } a \in A.$$

d) If $L \supset K$ and $a \in A$, show that

$$c_L(a \circ \mathrm{Tr}_{L/K}) = c_K(a).$$

Show that $c_K(\mathrm{Tr}_{K/\mathbb{Q}_p}) = 1$.

e) If K is a Galois extension of $\mathbb{Q}_p$, show that $c_K(\sigma) = 0$ for every $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$, $\sigma \neq \mathrm{id}$, and $c_K(\mathrm{id}) = 1$.

2) Let $\varphi\colon G^{\mathrm{ab}} \to K^\times$ be a continuous homomorphism, and let a_φ, be the $\mathbb{Q}_p$-linear endomorphism of K such that the diagram

$$\begin{tikzcd} U_K \arrow[r, "\varphi"] \arrow[d, "\log"'] & U_K \arrow[d, "\log"] \\ K \arrow[r, "a_\varphi"] & K \end{tikzcd}$$

is commutative. Let $L\overline{\varphi}$ (resp. $L\overline{\chi}$) be the image of φ (resp. χ) in the one-dimensional K-vector space $H^1(G, C)$, cf. A.2. Show that

$$L\overline{\varphi} = c \cdot L\overline{\chi},$$

where $c = -c_K(a_\varphi)$. (Check the formula first when K is a Galois extension of $\mathbb{Q}_p$ and $\varphi = \sigma^{-1} \circ \chi_K$, $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$, in which case III-28
$a_\varphi = -\sigma^{-1}$ and $c_K(a_\varphi)$ is given by Exer. 1, d.)

In particular, φ is admissible if and only if $c_K(a_\varphi) = 0$.

A.7 Tate's theorem

We recall the statement (cf. 1.2); here again, K is locally compact.

Theorem 1. *Let V be a finite dimensional vector space over $\mathbb{Q}_p$ and let $\rho\colon G \to \mathrm{Aut}(V)$ be an abelian p-adic representation of K. The following are equivalent:*

(1) ρ is locally algebraic

(2) ρ is of Hodge-Tate type and its restriction to the inertia group is semi-simple.

Proof. We have already remarked (cf. 1.1) that (1) implies:

> ***(*)*** *The restriction of ρ to the inertia group is semi-simple.*

Hence we may assume that (*) holds.

Let π be a uniformizing element of K, and let pr_π denote the projection map of G^{ab} onto its inertia group U_K associated to π (cf. A.4 and Cassels & Fröhlich [**0,** pp. 144–145]). Define a new representation ρ' of G^{ab} by

$$\rho' = \rho \circ \mathrm{pr}_\pi \,.$$

Replacing ρ by ρ' does not affect the local algebraicity (clear), nor the Hodge-Tate property (this follows from A.1, Cor. 1.2 to Th. 1). Since (*) implies that
III-29 ρ' is semi-simple, this means that, after replacing ρ by ρ', we may assume that ρ is semi-simple and even (by an easy reduction) that it is *simple*. Let then $E \subset \mathrm{End}(V)$ be the commuting algebra of ρ. Since ρ is abelian and simple, E is a commutative field, of finite degree over $\mathbb{Q}_p$, and V is a one-dimensional vector space over E; the representation ρ is given by a continuous character $\rho\colon G \to E^\times$.

Let now K' be a finite extension of K which is large enough to contain all the $\mathbb{Q}_p$-conjugates of E. Call $(1')$ and $(2')$ the properties corresponding to (1) and (2), when K' is taken as groundfield instead of K. We know (cf. 1.1) that $(1) \iff (1')$. By Cor. 1.2 to Th. 1 of A.1, we have $(2) \iff (2')$. Hence it is enough to prove that $(1') \iff (2')$, and this has been done in A.6 (Cor. to Prop. 1). $\square$

CHAPTER IV

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 IV-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, A.1). The variation of G_ℓ with ℓ is studied in §3.

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

§1. Preliminaries

1.1 Elliptic curves (cf. Cassels [**0**], Deuring [**0**], Igusa [**0**]) IV-2

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

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

IV-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 Deuring [**0**] or Ogg [**0**]**;** 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
IV-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 Mumford [**0**], 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 Serre & Tate [**0**], §2). For the proof of this, see Serre [**0**], §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 $\ell^n \colon E(\overline{K}) \to E(\overline{K})$. IV-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

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

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 Serre & Tate [**0**]**,** §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.*

IV-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 Koizumi & Shimura [**0**]**.**

Exercise. Let S be the finite set of places where E does not have good reduction. If $v \in M_K^0 - S$, 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 $v \in M_K^0 - S$, $p_v \neq \ell$.

  (ii) The set of $v \in M_K^0 - S$ such that $t_v \equiv 0 \mod \ell^m$ has density one (cf. chap. I, 2.2).

  (iii) For all $s \in \mathrm{Im}(\rho)$, 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

It is the following (cf. [**23**]): IV-7

Theorem 1. *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 1.1. *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 IV-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
IV-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. Lang [**0**], 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:* IV-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 $\mathbb{Z}_\ell$-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 $E(n) = E/X(n)$. IV-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. □

Remark. One can prove part (a) of the above theorem by a quite different method (cf. [**0**], §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.

2.2 Determination of the Lie algebra of G_ℓ

Let $G_\ell = \mathrm{Im}(\rho_\ell)$ denote the image of $\mathrm{Gal}(\overline{K}/K)$ in $\mathrm{Aut}(T_\ell)$, and let $\mathfrak{g}_\ell \subset \mathrm{End}(V_\ell)$ be the Lie algebra of G_ℓ.

Theorem 1. *If E has no complex multiplication (cf. 2.1), then $\mathfrak{g}_\ell = \mathrm{End}(V_\ell)$, i.e. G_ℓ is open in $\mathrm{Aut}(T_\ell)$.*

Proof. The irreducibility theorem of 2.1 shows that, for any open subgroup U of G_ℓ, V_ℓ is an irreducible U-module. Hence, V_ℓ is an irreducible $\mathfrak{g}_\ell$-module. By Schur's lemma, it follows that the commuting algebra $\mathfrak{g}'_\ell$ of $\mathfrak{g}_\ell$ in $\mathrm{End}(V_\ell)$ is a field; since $\dim V_\ell = 2$, this field is either $\mathbb{Q}_\ell$ or a quadratic extension of $\mathbb{Q}_\ell$. If $\mathfrak{g}'_\ell = \mathbb{Q}_\ell$, then $\mathfrak{g}_\ell$ is equal to either $\mathrm{End}(V_\ell)$, or the subalgebra $\mathfrak{sl}(V_\ell)$
IV-12 of $\mathrm{End}(V_\ell)$ consisting of the endomorphisms with trace 0; but, in the second case, the action of $\mathfrak{g}_\ell$ on $\bigwedge^2 V_\ell$ would be trivial, and this would contradict the fact that the Galois modules $\bigwedge^2 V_\ell$ and $V_\ell(\mu)$ are isomorphic (chap. I, 1.2). Hence $\mathfrak{g}_\ell = \mathfrak{sl}(V_\ell)$ is impossible.

Suppose now that $\mathfrak{g}'_\ell$ is a quadratic extension of $\mathbb{Q}_p$. Then V_ℓ is a one-dimensional $\mathfrak{g}'_\ell$-vector space and the commuting algebra of $\mathfrak{g}'_\ell$ in $\mathrm{End}(V_\ell)$ is $\mathfrak{g}'_\ell$ itself. Hence $\mathfrak{g}_\ell$ is contained in $\mathfrak{g}'_\ell$, and is *abelian* ($\mathfrak{g}'_\ell$ is a "non-split Cartan algebra" of $\mathrm{End}(V_\ell)$). After replacing K by a finite extension (this does not affect $\mathfrak{g}_\ell$, cf. chap. I, 1.1), we may then suppose that G_ℓ itself is abelian. The ℓ-adic representation V_ℓ is then semi-simple, abelian and rational. It is, moreover, *locally algebraic*. To see this, we first remark that, at a place v dividing ℓ, we have $v(j) \geq 0$ since otherwise the decomposition group of v in G_ℓ would be non-abelian by Tate's theory (cf. Appendix, 3); hence, after a finite extension of K, we can assume that E has good reduction at all places v dividing ℓ (cf. 1.2). Let $E(\ell)$ be the ℓ-divisible group attached to E at v

(cf. **39** [**39**], 2.1, example (a)). We have $V_\ell \cong V_\ell(E(\ell))$ and this module is known to be of Hodge-Tate type (*loc. cit.*, §4). Using another result of Tate (chap. III, 1.2), this implies that the representation V_ℓ is locally algebraic, as claimed above. (This could also be seen by using, instead of the theory of Hodge-Tate modules, the local results of the Appendix, A.2.)

We may now apply to V_ℓ the results of chap. III, 2.3. Hence, there is, for each prime ℓ', a rational, abelian, semi-simple ℓ'-adic representation $W_{\ell'}$ compatible with V_ℓ. But $V_{\ell'}$ is compatible with V_ℓ, and $V_{\ell'}$ is semi-simple. Hence $V_{\ell'}$, is isomorphic to $W_{\ell'}$ (cf. chap. I, 2.3). But we know (chap. III, 2.3) that we may choose ℓ' such that $W_{\ell'}$ is the direct sum of one-dimensional IV-13
subspaces stable under $\mathrm{Gal}(\overline{K}/K)$. This contradicts the irreducibility of V_ℓ. Hence, we must have $\mathfrak{g}'_\ell = \mathbb{Q}_p$ and $\mathfrak{g}_\ell = \mathrm{End}(V_\ell)$. □

Remark. If E has complex multiplication, and $L = \mathbb{Q} \otimes \mathrm{End}(E \otimes_K \overline{K})$ is the corresponding imaginary quadratic field, one shows easily that $\mathfrak{g}_\ell$ is the Cartan subalgebra of $\mathrm{End}(V_\ell)$ defined by $L_\ell = \mathbb{Q}_\ell \otimes L$. It splits if and only if ℓ decomposes in L.

Exercises. (In these exercises, we assume E has no complex multiplication. Let S be the set of places $v \in M_K^0$ where E has bad reduction. If $v \in M_K^0 - S$, we denote by F_v the Frobenius endomorphism of the reduced curve $\widetilde{E}_v$; if $\ell \neq p_v$, we identify F_v to the corresponding automorphism of T_ℓ.)

1) Let $H(X, Y)$ be a polynomial in two indeterminates X, Y with coefficients in a field of characteristic zero. Let V_H be the set of those $v \in M_K^0 - S$ for which $H(\mathrm{Tr}(F_v), \mathbf{N}\, v) = 0$. If H is not the zero polynomial, show that V_H has density 0. (Show that the set of $g \in \mathrm{GL}(2, \mathbb{Z}_\ell)$ with $H(\mathrm{Tr}(g), \det(g)) = 0$ has Haar measure zero.)

2) The eigenvalues of F_v may be identified with complex numbers of the form
$$(\mathbf{N}\, v)^{1/2} e^{\pm i\varphi_v}, \qquad 0 \le \varphi_v \le \pi,$$
cf. chap. I, Appendix A.2. Show that the set of v for which φ_v is a given angle φ has density zero. (Show that $\mathrm{Tr}(F_v)^2 = 4(\mathbf{N}\, v)\cos^2\varphi$ and then use the preceding exercise.)

3) Let $L_v = \mathbb{Q}(F_v)$ be the field generated by F_v. By the preceding exercise, IV-14
L_v is quadratic imaginary except for a set of v of density 0.

(a) Let ℓ be a fixed prime. Let C be a semi-simple commutative $\mathbb{Q}_\ell$-algebra of rank 2. Let X_C be the set of elements $s \in \mathrm{Aut}(V_\ell)$ such that the subalgebra $\mathbb{Q}_\ell[s]$ of $\mathrm{End}(V_\ell)$ generated by s is isomorphic to C. Show that X_C is open in $\mathrm{Aut}(V_\ell)$, and show that it has a non-empty intersection with every open subgroup of $\mathrm{Aut}(V_\ell)$, in particular, with G_ℓ.

(b) Show that $F_v \in X_C$ if and only if the field L_v is quadratic and $L_v \otimes \mathbb{Q}_\ell$ is isomorphic to C.

(c) Let $\ell_1, \ldots, \ell_n$ be distinct prime numbers, and choose for each an algebra C_i of the type considered in 3a. Show that the set of v for which $F_v \in X_C$ for $i = 1, \ldots, n$ has density > 0.

(Use the fact that the image of $\mathrm{Gal}(\overline{K}/K)$ in any finite product of the $\mathrm{Aut}(V_\ell)$ is open; this is an easy consequence of the theorem proved above.)

(d) Deduce that, for any finite set P of prime numbers, there exist an infinity of v such that L_v is ramified at all $\ell \in P$. In particular, there are an infinite number of distinct fields L_v.

2.3 The isogeny theorem

Theorem 1. *Let E and E' be elliptic curves over K, let ℓ be a prime number and let $V_\ell(E)$ and $V_\ell(E')$ be the corresponding ℓ-adic representations of K. Suppose that the Galois modules $V_\ell(E)$ and $V_\ell(E')$ are isomorphic and that the modular invariant j of E (cf. 1.1) is not an integer K. Then E and E' are K-isogenous.*

IV-15 We need the following result:

Proposition 1. *Let E and E' be elliptic curves over K. The following conditions are equivalent:*

(a) The Galois modules $V_\ell(E)$ and $V_\ell(E')$ are isomorphic for all ℓ.

(b) The Galois modules $V_\ell(E)$ and $V_\ell(E')$ are isomorphic for one ℓ.

(c) If F_v and F'_v are the Frobeniuses of the reduced curves $\widetilde{E}_v$ and $\widetilde{E}'_v$, we have $\mathrm{Tr}(\mathrm{F}_v) = \mathrm{Tr}(\mathrm{F}'_v)$ for all v where there is good reduction.

(d) For a set of places of K of density one we have $\mathrm{Tr}(\mathrm{F}_v) = \mathrm{Tr}(\mathrm{F}'_v)$.

Proof. Clearly (a) implies (b), and (c) implies (d). The implication (b) $\Longrightarrow$ (c) follows from the fact that $\mathrm{Tr}(\mathrm{F}_v)$ is known when V_ℓ is known. To prove (d) $\Longrightarrow$ (a) one remarks first that the representations of $\mathrm{Gal}(\overline{K}/K)$ in $V_\ell(E)$ and $V_\ell(E')$ have the same trace, by Čebotarev's density theorem (chap. I, 2.2). Moreover, $V_\ell(E)$ (and also $V_\ell(E')$) is semi-simple. This is clear if E has no complex multiplication over K since $V_\ell(E)$ is then irreducible (2.1); if E has complex multiplication, it follows from the Remark in 2.2. Since $V_\ell(E)$ and $V_\ell(E')$ are semi-simple and have the same trace, they are isomorphic. □

Remark. 1) If E and E' have good reduction at v, let t_v (resp. t'_v) be the number of k_v-points of $\widetilde{E}_v$ (resp. $\widetilde{E}'_v$). We have the formulas (cf. 1.3): IV-16

$$t_v = 1 - \mathrm{Tr}(\mathrm{F}_v) + \mathbf{N}\,v,$$
$$t'_v = 1 - \mathrm{Tr}(\mathrm{F}'_v) + \mathbf{N}\,v.$$

Hence condition (c) (resp. condition (d)) is equivalent to saying that $t_v = t'_v$ for all v where there is good reduction (resp. for a set of v's of density one).

2) If E and E' are K-isogenous, it is clear that conditions (a), (b), (c), (d) are satisfied.

Proof of the theorem. In view of Remark 2 above, it suffices to show that the equivalent conditions (a), (b), (c) and (d) imply that the elliptic curves E and E' are isogenous when the modular invariant j of E is not an integer of K. Let v be a place of K such that $v(j) < 0$, and let p be the characteristic of the residue field k_v.

If $j' = j(E')$, we first show that $v(j')$ is also < 0. Suppose that $v(j') \geq 0$. Then, after possibly replacing K by a finite extension, we may assume that E' has good reduction at v.

Then, if $\ell \neq p_v$, the Galois-module $V_\ell(E')$ is unramified at v (cf. 1.3); but $V_\ell(E)$ is ramified at v: this follows either from the criterion of Néron-Ogg-Šafarevič (1.3) or from the determination of the inertia group given in the Appendix A.1.3. This contradicts the fact that $V_\ell(E)$ and $V_\ell(E')$ are isomorphic.

Let now q and q' be the elements of K_v which correspond to j and j' in Tate's theory (cf. Appendix A.1.1), and let E_q and $E_{q'}$, be the corresponding elliptic curves (*loc. cit.*). Since E and E_q have the same modular invariant j, there is a finite extension K' of K_v where they become isomorphic, and

we can do the same for E' and $E_{q'}$. Hence, the Tate modules $T_p(E_q)$ and
IV-17 $T_q(E_{q'})$ become isomorphic over K'. But, in this case the isogeny theorem is true (cf. Appendix A.1.4), i.e. the curves E_q and $E_{q'}$, hence also E and E', are K'-isogenous. However, if two elliptic curves are isogenous over some extension of the ground field, they are isogenous over a *finite* extension of the ground field. We may thus choose a finite extension L of K and an L-isogeny $f\colon E \otimes_K L \to E' \otimes_K L$. We will show that f is automatically defined over K. For this, it suffices to show that $f = {}^s f$ for all $s \in \mathrm{Gal}(\overline{K}/K)$, or, equivalently, that $V(f)\colon V_p(E) \to V_p(E')$ commutes with the action of Galois. However, if $G_L = \mathrm{Gal}(\overline{K}/L)$ is the open subgroup of $G = \mathrm{Gal}(\overline{K}/K)$ which corresponds to L, then $V(f)$ commutes with the action of G_L. It is then enough to show that $\mathrm{Hom}_{G_L}(V, V') = \mathrm{Hom}_G(V, V')$. But V and V' are isomorphic as G-modules. Hence we have to show that $\mathrm{End}_{G_L}(V) = \mathrm{End}_G(V)$. But this is clearly true; in fact, G and G_L are open in $\mathrm{Aut}(V)$ by the theorem in section 2.2, and hence their commuting algebra is reduced to the homotheties in each case, i.e. $\mathrm{End}_{G_L}(V) = \mathrm{End}_G(V) = \mathbb{Q}_p$. This completes the proof of the theorem. □

Remark. It is very likely that the theorem is true without the hypothesis that j is not integral. This could be proved (by Tate's method [**0**]) if the following generalization of Šafarevič's theorem were true: given a finite subset S of M_K^0, the abelian varieties over K, of dimension 2, with polarization of degree one, and good reduction outside S, are in finite number (up to isomorphism). → [this has been proved by Fairings, see [**54**], [**56**], [**82**].]

§3. Variation of G_ℓ and $\widetilde{G}_\ell$ with ℓ

3.1 Preliminaries

Belen.

3.2 The case of a non integral j

IV-18 **Theorem 1.** *Assume that the modular invariant j of E is not an integer of K. Then E enjoys the equivalent properties (i), (ii), (iii), (iv) of 3.1.*

Since j is not integral, we can choose a place v of K such that $v(j) < 0$. Let q be the element of the local field K which corresponds to j by Tate's theory (cf. Appendix, 1) and let E be the corresponding elliptic curve over K. There is a finite extension K' of K_v over which E and E_q are isomorphic; one can even take for K' either K_v or a quadratic extension of K_v. Let v' be the valuation of K' which extends v; assume v' is normalized so that $v'(K'^{\times}) = \mathbb{Z}$, and let

$$n = v'(q) = -v'(j)$$

We have $n > 1$.

Lemma 1. *Assume ℓ does not divide n, and let $I_{v,\ell}$ be the inertia subgroup of $\widetilde{G}_\ell$ corresponding to some extension of v to $\overline{K}$. Then $I_{v,\ell}$ contains a transvection, i.e. an element whose matrix form is $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ for a suitable $\mathbb{F}_\ell$-basis of E_ℓ.*

This is true for the curve E_q over K', cf. Appendix, 5. The result for E follows from the isomorphism $E_{/K'} \cong E_{q/K'}$.

Lemma 2. *Let H be a subgroup of $\mathrm{GL}(2, \mathbb{F}_\ell)$ which acts irreducibly on $\mathbb{F}_\ell \times \mathbb{F}_\ell$ and which contains a transvection. Then H contains $\mathrm{SL}(2, \mathbb{F}_\ell)$.*

For any transvection $s \in H$, let D be the unique one dimensional subspace of $\mathbb{F}_\ell \times \mathbb{F}_\ell$ which is fixed by s. If all such lines were the same, the line so defined would be stable by H, and H would not be irreducible. Hence there are transvections $s, s' \in H$ such that $D_s \neq D_{s'}$. If we choose a suitable basis (e, e') of $\mathbb{F}_\ell \times \mathbb{F}_\ell$, this means that the matrix forms of s, s' are

$$s = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \qquad s' = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$$

The lemma follows then from the well known fact that these two matrices generate $\mathrm{SL}(2, \mathbb{F}_\ell)$.

Proof of the theorem. Lemma 1 shows that, for almost all ℓ, $I_{v,\ell}$. and *a fortiori* $\widetilde{G}_\ell$, contains a transvection. On the other hand, we know (cf. 2.1) that $\widetilde{G}_\ell$ is irreducible for almost all ℓ. Applying lemma 2 to $\widetilde{G}_\ell$ we then see that $\widetilde{G}_\ell$ contains $\mathrm{SL}(E_\ell)$ for almost all ℓ; hence we have (iv). □

Remark. It seems likely that the condition "j is not integral" can be replaced by the weaker one "E has no complex multiplication." → [yes: see [**76**].]

3.3 Numerical example

Belen.

3.4 Proof of the main lemma of 3.1

José.

§A. Local results

IV-19 In what follows, K denotes a field which is complete with respect to a discrete valuation v; we denote by $\mathcal{O}_K$ (resp. by k) the ring of integers (resp. the residue field) of K; we assume that k is perfect and of characteristic $p \neq 0$.

Let E be an elliptic curve over K and let ℓ be a prime number different from the characteristic of K. Let T_ℓ and V_ℓ be the corresponding Galois modules; we denote by G_ℓ the image of $\mathrm{Gal}(K_s/K)$ in $\mathrm{Aut}(T_\ell)$, and by I_ℓ the inertia subgroup of G_ℓ. The Lie algebras $\mathfrak{g}_\ell = \mathrm{Lie}(G_\ell)$, $\mathfrak{i}_\ell = \mathrm{Lie}(I_\ell)$ are subalgebras of $\mathrm{End}(V_\ell)$ and we will determine them under suitable assumptions on K and v; note that, since I_ℓ is an invariant subgroup of G_ℓ, its Lie algebra $\mathfrak{i}_\ell$ is an *ideal* of $\mathfrak{g}_\ell$.

If $j = j(E)$ is the modular invariant of E (cf. 1.1), we consider the cases $v(j) < 0$ and $v(j) \geq 0$ separately.

A.1 The case $v(j) < 0$

In this section we assume that the modular invariant j of the elliptic curve E has a pole, i.e. that $v(j) < 0$.

1. The elliptic curves of Tate. Let q be an element of K with $v(q) > 0$, and let Γ_q be the discrete subgroup of $K^\times$ generated by q. Then, by Tate's theory of ultrametric theta functions (unpublished, but see Morikawa, *Nagoya Math. Journ.*, 1962), there is an elliptic curve E_q defined over K with the property that, for any finite extension K' of K, the analytic group

José: Añadir referencia

IV-20 $K'^\times/\Gamma_q$ is isomorphic to the group $E_q(K')$ of points of E_q with values in K'. The equation defining E_q can he written in the form

$$y^2 + xy = x^3 - b_2 x - b_3,$$

with

$$b_2 = 5\sum_{n\geq 1} n^3 \frac{q^n}{1-q^n}, \qquad \text{and} \qquad b_3 = \sum_{n\geq 1}(7n^5 + 5n^3)\frac{q^n}{12(1-q^n)},$$

these series converging in K. The modular invariant $j(q)$ of E_q is given by the usual formula

$$j(q) = \frac{(1+48b_2)^3}{q\prod_{n\geq 1}(1-q^n)^{24}} = \frac{1}{q} + 744 + 196\,884q + \cdots$$

a series with integral coefficients. The function field of E_q consists of the fractions F/G, where F and G are Laurent series

$$F = \sum_{n=-\infty}^{+\infty} a_n z^n, \qquad G = \sum_{n=-\infty}^{+\infty} b_n z^n$$

with coefficients in K, converging for all values of $z \neq 0, \infty$, and such that $F(qz)/G(qz) = F(z)/G(z)$.

Since the modular invariant j of the given elliptic curve E is such that $v(j) < 0$, and since the series for $j(q)$ has integral coefficients, one can choose q so that $j = j(q)$. The elliptic curves E and E_q become then isomorphic over a finite extension of K (which can be taken to be of degree 2). Hence, after possibly replacing K by a finite extension, *we may assume that* $E = E_q$.

2. An exact sequence. We conserve the notation of 1. Let E_n be the kernel of multiplication by ℓ^n in $K_s^\times/\Gamma_q$. If μ_n is the group of ℓ^n-th roots of unity in K_s, we have an injection $\mu_n \to E_n$. On the other hand, if $z \in E_n$, we have $z^{\ell^n} \in \Gamma_q$, and hence there exists an integer c such that $z^{\ell^n} = q^c$. If we associate to z the image of c in $\mathbb{Z}/\ell^n\mathbb{Z}$, we obtain a homomorphism of E_n into $\mathbb{Z}/\ell^n\mathbb{Z}$, and the resulting sequence IV-21

$$0 \longrightarrow \mu_n \longrightarrow E_n \longrightarrow \mathbb{Z}/\ell^n\mathbb{Z} \longrightarrow 0 \qquad \text{(IV.1)}$$

is an exact sequence of $\mathrm{Gal}(K_s/K)$-modules, $\mathrm{Gal}(K_s/K)$ acting trivially on $\mathbb{Z}/\ell^n\mathbb{Z}$. Passing to the limit, we obtain an exact sequence of Galois modules

$$0 \longrightarrow T_\ell(\mu) \longrightarrow T_\ell(E_n) \longrightarrow \mathbb{Z}_\ell \longrightarrow 0 \qquad \text{(IV.2)}$$

where $\mathrm{Gal}(K_s/K)$ acts trivially on $\mathbb{Z}_\ell$. Tensoring with $\mathbb{Q}_\ell$, we obtain the exact sequence

$$0 \longrightarrow V_\ell(\mu) \longrightarrow V_\ell(E_n) \longrightarrow \mathbb{Q}_\ell \longrightarrow 0. \qquad \text{(IV.3)}$$

We now show that this sequence of $\mathrm{Gal}(K_s/K)$-modules does not split. To do this we introduce an invariant x which belongs to the group $\varprojlim_n H^1(G,\mu_n)$, where $G = \mathrm{Gal}(K_s/K)$. Let d be the coboundary homomorphism:

$$H^0(G,\mathbb{Z}/\ell^n\mathbb{Z}) \longrightarrow H^1(G,\mu_n)$$

with respect to the exact sequence (IV.1) and let $x_n = d(1)$. The invariant x is the element of $\varprojlim_n H^1(G,\mu_n)$ defined by the family $(x_n)_{n\geq 1}$.

Proposition 1. *(a) The isomorphism $\delta\colon K^\times/K^{\times\ell^n} \to H^1(G,\mu_n)$ of Kummer theory transforms the class of $q \mod K^{\times\ell^n}$ into x_n.*

(b) The element x is of infinite order.

(Recall that δ is induced by the coboundary map relative to the exact sequence

$$1 \longrightarrow \mu_n \longrightarrow \overline{K}^\times \xrightarrow{()^{\ell^n}} \overline{K}^\times \longrightarrow 1.)$$

Proof. Assertion (a) is proved by an easy computation. To prove (b), note that the valuation v defines a homomorphism

$$f_n\colon K^\times/K^{\times\ell^n} \longrightarrow \mathbb{Z}/\ell^n\mathbb{Z},$$

and hence a homomorphism

$$f\colon \varprojlim_n K^\times/K^{\times\ell^n} \longrightarrow \mathbb{Z}_\ell.$$

If we identify x with the corresponding element of $\varprojlim K^\times/K^{\times\ell^n}$, as in (a), we have $f(x) = v(q)$, hence x is of infinite order. $\square$

Corollary 1.1. *The sequence* (IV.3) *does not split.*

Proof. Assume it does, i.e. there is a G-subspace X of $V_\ell(E_q)$ which is mapped isomorphically onto $\mathbb{Q}_\ell$. Let $X_T = T_\ell(E_q)\cap X$. The image of X_T in $\mathbb{Z}_\ell$ is $\ell^N\mathbb{Z}_\ell$, for some $N \geq 0$. It is then easy to see that $\ell^N x = 0$, and this contradicts the
IV-22 fact that x is of infinite order. $\square$

3. Determination of $\mathfrak{g}_\ell$ and $\mathfrak{i}_\ell$. We keep the notation of 1 and 2. If X is a one-dimensional subspace of $V_\ell = V_\ell(E)$, let $\mathfrak{r}_X$ denote the subalgebra of $\mathrm{End}(V_\ell)$ consisting of those endomorphisms u for which $u(V_\ell) \subset X$, and let $\mathfrak{n}_X$ be the subalgebra of $\mathfrak{r}_X$ formed by those $u \in \mathfrak{r}_X$ with $u(X) = 0$.

Theorem 1. *(a) If k is algebraically closed and $\ell \neq p$, then there is a one-dimensional subspace X of V_ℓ such that $\mathfrak{g}_\ell = \mathfrak{n}_X$.*

(b) If k is algebraically closed and $\ell = p$, then there is a one-dimensional subspace X of V_ℓ such that $\mathfrak{g}_\ell = \mathfrak{r}_X$.

(c) If k is finite, then $\mathfrak{g}_\ell = \mathfrak{r}_X$ for some one-dimensional subspace X of V_ℓ, and $\mathfrak{i}_\ell = \mathfrak{n}_X$ (resp. $\mathfrak{i}_\ell = \mathfrak{r}_X$) if $\ell \neq p$ (resp. $\ell = p$).

Proof. Note first that, since $\mathfrak{g}_\ell$ and $\mathfrak{i}_\ell$ are invariant under finite extension of K, we may assume that $E = E_q$.

1) In this case, K contains the ℓ^n-th roots of unity, hence $\mathrm{Gal}(K_\mathrm{s}/K)$ acts trivially on $T_\ell(\mu)$. Consequently, there is a basis e_1, e_2 of $T_\ell(E)$ such that, for all $\sigma \in \mathrm{Gal}(K_\mathrm{s}/K)$, we have $\sigma(e_1) = e_1$, $\sigma(e_2) = a(\sigma)e_1 + e_2$ with $a(\sigma) \in \mathbb{Z}_\ell$. Moreover, the homomorphism $\sigma \mapsto a(\sigma)$ cannot be trivial since the sequence (IV.3) does not split. It follows that $\mathrm{Im}(a)$ is an open subgroup of $\mathbb{Z}_\ell$, and hence that $\mathfrak{g}_\ell = \mathfrak{n}_X$ with $X = V_\ell(\mu)$.

2) Since $\ell = p$, we must have $\mathrm{char}(K) = 0$ as $\ell \neq \mathrm{char}(K)$. In this case, the action of $\mathrm{Gal}(\overline{K}/K)$ on $V_\ell(\mu)$ is by means of the character χ_ℓ (cf. chap. I, 1.2) which is of infinite order. It follows that $\mathfrak{g}_\ell = \mathfrak{r}_X$ where IV-23
$X = V_\ell(\mu)$; in fact, $\mathfrak{g}_\ell \supset \mathfrak{n}_X$ since the sequence (IV.3) does not split, and we cannot have $\mathfrak{g}_\ell = \mathfrak{n}_X$.

3) Since k is finite, the action of $\mathrm{Gal}(K_\mathrm{s}/K)$ on $T_\ell(\mu)$ is not trivial nor even of finite order. Hence, the argument used in (b) shows that $\mathfrak{g}_\ell = \mathfrak{r}_X$. where $X = V_\ell(\mu)$. Applying (a) to the completion of the maximal unramified extension of K, we see that $\mathfrak{i}_\ell = \mathfrak{n}_X$ if $\ell \neq p$, and that $\mathfrak{i}_\ell = \mathfrak{r}_X$ if $\ell = p$. $\square$

Exercise. In case (a), show that $\mathrm{Im}(a) = \ell^n\mathbb{Z}_\ell$, where ℓ^n is the highest power of ℓ which divides $v(q) = -v(j)$.

4. Application to isogenies.

Belén.

5. Existence of transvections in the inertia group.

Belén.

A.2 The case $v(j) \geq 0$

In this section we assume that the modular invariant j of the elliptic curve E is integral, i.e. that $v(j) \geq 0$. Hence, after possibly replacing K by a finite extension, we may assume that E has *good reduction* (cf. 1.2). We also assume that K *is of characteristic zero.*

1. The case $\ell \neq p$.

Belén.

2. The case $\ell = p$ with good reduction of height 2. Here we assume that the reduced curve $\widetilde{E}$ is of height 2; recall that, if A is an abelian variety defined over a field of characteristic p, its height can be defined as the integer h for which p is the inseparable part of the degree of the homothety "multiplication by p." An elliptic curve is of height 2 if and only if its *Hasse invariant* (cf. Deuring [**0**]) is 0. Since E has good reduction, it defines an *abelian scheme* $E(p)$ over $\mathcal{O}_{K'}$, hence a *p-divisible group* $E(p)$ over $\mathcal{O}_K$ (cf. **39** [**39**], 2.1 – see also [**0**]**,** §1, Ex. 2). The Tate module of $E(p)$ can be identified with T_p. The connected component $E(p)^\circ$ of $E(p)$ coincides with the *formal group* (over $\mathcal{O}_K$) attached to E_v; the height of $\widetilde{E}$ is precisely the height of this formal group (in the usual sense). In our case, we have $E(p) = E(p)^\circ$ since the height is assumed to be 2.

Theorem 1. *One has* $\mathfrak{g}_p = \mathfrak{i}_p$. *This Lie algebra is either* $\mathrm{End}(V_p)$ *or a non-split Cartan subalgebra of* $\mathrm{End}(V_p)$.

(Recall that a non-split Cartan subalgebra of $\mathrm{End}(V_p)$ is a commutative subalgebra of rank 2 with respect to which V_p is irreducible. It is given by a quadratic subfield of $\mathrm{End}(V_p)$.)

Proof. The Lie algebra $\mathfrak{g}_p$ has the property that $\mathfrak{g}_p z = V_p$ for any non zero element z of V_p (cf. [**0,** p. 128], Prop. 8). In particular, V_p is an irreducible $\mathfrak{g}_p$-module; its commuting algebra is either a field of degree 2 (which is then necessarily equal to $\mathfrak{g}_p$) or the field $\mathbb{Q}_p$, in which case $\mathfrak{g}_p$ is *a priori* $\mathfrak{sl}_2$ or IV-24
$\mathfrak{gl}_2$. But $\mathfrak{g}_p \neq \mathfrak{sl}_2$ since $\bigwedge^2 V_p$ is canonically isomorphic to $V_p(\mu)$, and the action of $\mathrm{Gal}(\overline{K}/K)$ on $V_p(\mu)$ is by means of the character χ_p, which is of infinite order (indeed, no finite extension of K can contain all p^n-th roots of unity, $n = 1, 2, \dots$). Hence the Lie algebra $\mathfrak{g}_p$ is either $\mathrm{End}(V_p)$ or a non split Cartan subalgebra of $\mathrm{End}(V_p)$. Since the above applies to the completion of the maximal unramified extension of K, we have the same alternative for $\mathfrak{i}_p$. Moreover, $\mathfrak{i}_p$ is contained in $\mathfrak{g}_p$. We have *a priori* three possibilities:

(a) $\mathfrak{i}_p = \mathfrak{g}_p = \mathrm{End}(V_p)$.

(b) $\mathfrak{i}_p = \mathfrak{g}_p$ is a non split Cartan subalgebra of $\mathrm{End}(V_p)$.

(c) $\mathfrak{i}_p$ is a Cartan subalgebra and $\mathfrak{g}_p = \mathrm{End}(V_p)$.

However, $\mathfrak{i}_p$ is an ideal of $\mathfrak{g}_p$. Hence, (c) is impossible, and this proves the theorem. □

Remark. 1) By a theorem of Tate ([**39**], §4, cor. 1 to th. 4), the algebra $\mathfrak{g}_p$ is a Cartan subalgebra of $\mathrm{End}(V_p)$ if and only if $E(p)$ has "formal complex multiplication", i.e. if and only if the ring of endomorphisms of $E(p)$, over a suitable extension of K, is of rank 2 over $\mathbb{Z}_p$. There exist elliptic curves without complex multiplication (in the algebraic sense) whose p-completion $E(p)$ have formal complex multiplication.

2) Suppose that $\mathfrak{g}_p$ is a Cartan subalgebra of $\mathrm{End}(V_p)$, and let $H = \mathfrak{g}_p \cap \mathrm{Aut}(V_p)$ be the corresponding Cartan subgroup of $\mathrm{Aut}(V_p)$. If N is the normalizer of H in $\mathrm{Aut}(V_p)$, then one knows that N/H is cyclic of order 2. Since $G_p \subset N$, it follows that G_p is commutative if and only if $G_p \subset H$. The case $G_p \subset H$ corresponds to the case where the formal complex multiplication of $E(p)$ is defined over K, and the case $G_p \not\subset H$ IV-25
corresponds to the case where this formal multiplication is defined over a quadratic extension of K.

3) Suppose that G_p is commutative, and that the residue field k is *finite*. Let F be the quadratic field of formal complex multiplication (i.e. $\mathfrak{g}_p$ itself, viewed as an associative subalgebra of $\mathrm{End}(V_p)$). If U_F denotes

the group of units of F, the action of $\mathrm{Gal}(\overline{K}/K)$ on V_p is given by a homomorphism

$$\varphi_I\colon \mathrm{Gal}(\overline{K}/K) \longrightarrow U_F.$$

By local class field theory, we may identify the inertia group of $\mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}}$ with the group U_K of units of K. Hence the restriction φ_I of φ to the inertia group is a *homomorphism of U_K into U_F*. To determine φ_I, we first remark that the action of $\mathrm{End}(E(p))$ on the tangent space to $E(p)$ defines an *embedding* of F into K. For that embedding, one has (compare with chap. III, A.4)

$$\varphi_I(x) = \mathrm{N}_{K/F}(x^{-1}), \qquad \text{for all } x \in U_K.$$

José: Añadir referencia.

Indeed, by a result of Lubin (*Ann. of Math.* 85, 1967), there is a formal group E' which is K-isogenous to $E(p)$, and has for ring of endomorphisms the ring of integers of F. But then, if E'' is a Lubin-Tate group over K (cf. Lubin & Tate [**0**]), the formal groups E' and E'' are isomorphic over the completion of the maximal unramified extension of K (cf. Lubin [**0**], th. 4.3.2). Hence to prove the formula (*), we may assume that $E(p)$ is a Lubin-Tate group, in which case the formula (*) follows from the main result of [**0**].

José: ¿A qué fórmula se refiere?

3. Auxiliary results on abelian varieties. Let A and B be two abelian
IV-26 varieties over K, with good reduction, so that the associated p-divisible groups $A(p)$ and $B(p)$ are defined (these are p-divisible groups *over the ring* $\mathcal{O}_{K'}$, cf. **39** [**39**]). Let $\widetilde{A}$ and $\widetilde{B}$ (resp. $\widetilde{A(p)}$ and $\widetilde{B(p)}$) be the reductions of A and B (resp. of $A(p)$ and $B(p)$).

Theorem 2. *Let $\tilde{f}\colon \widetilde{A} \to \widetilde{B}$ be a morphism of abelian varieties, and let $\widetilde{f(p)}$ be the corresponding morphism of $\widetilde{A(p)}$ into $\widetilde{B(p)}$. Assume there is a morphism $f(p)\colon A(p) \to B(p)$ whose reduction is $\widetilde{f(p)}$. Then, there is a morphism $f\colon A \to B$ whose reduction is f.*

A proof of this "lifting" theorem has been given by Tate in a Seminar (Woods Hole, 1964), but has not yet been published; a different proof has been given by W. Messing (*L. N.* 264, 1972).

José: Añadir referencia

Theorem 3. *Assume $T_p(A)$ is a direct sum of $\mathbb{Z}_p$-modules of rank 1 invariant under the action of* $\mathrm{Gal}(\overline{K}/K)$. *Then every endomorphism of $\widetilde{A}$ lifts to an* *endomorphism of A, i.e., the reduction homomorphism* $\mathrm{End}(A) \to \mathrm{End}(\widetilde{A})$ *is surjective (and hence bijective, since it is known to be injective).*

Using theorem 2, one sees that it is enough to show that any endomorphism of $\widetilde{A(p)}$ can be lifted to an endomorphism of $A(p)$. But the assumption made on T_p implies (cf. **39** [**39**], 4.2) that $A(p)$ is a product of p-divisible groups of height 1. Hence we are reduced to proving the following elementary result:

Lemma 1. *Let H_1, H_2 be two p-divisible groups, over $\mathcal{O}_{K'}$ both of height one. Then the reduction map:* $\mathrm{Hom}(H_1, H_2) \to \mathrm{Hom}(\widetilde{H}_1, \widetilde{H}_2)$ *is bijective.*

Proof. This is clear if both H_1 and H_2 are étale. If both are not étale, their IV-27
duals are étale and we are reduced to the previous case. If one of them is étale, and the other is not, one checks readily that

$$\mathrm{Hom}(H_1, H_2) = \mathrm{Hom}(\widetilde{H}_1, \widetilde{H}_2) = 0. \qquad \square$$

Corollary 1.1. *Assume:*

(i) $V_p(A)$ is a direct sum of one-dimensional subspaces stable under $\mathrm{Gal}(\overline{K}/K)$.

(ii) The residue field k of K is finite.

*Then A is isogenous to a product of abelian varieties of (CM) type (m the sense of Shimura & Taniyama [**0**], cf. also chap. II, 2.8).*

Proof. Assumption (i) implies that $T_p(A)$ contains a lattice T' which is a direct sum of free $\mathbb{Z}_p$-modules of rank 1 stable under $\mathrm{Gal}(\overline{K}/K)$. One can find an isogeny $A_1 \to A$ such that $T_p(A_1)$ is mapped onto T'. This means that, after replacing A by an isogenous variety, we may apply Th. 3 to A, i.e. $\mathrm{End}(A) \to \mathrm{End}(\widetilde{A})$ is an isomorphism. But, since k is finite, it follows from a result of Tate [**0**] that $\mathbb{Q} \otimes \mathrm{End}(\widetilde{A})$ contains a semi-simple commutative $\mathbb{Q}$-subalgebra Λ of rank $2\dim(A)$ (this is not explicitly stated in [**0**], but follows easily from its "Main Theorem"). Hence, the same is true for $\mathbb{Q} \otimes \mathrm{End}(A)$. If we now write Λ as a product of commutative fields Λ_α, one sees that A is isogenous to a product $\prod_\alpha A_\alpha$, where A_α has complex multiplication of type Λ_α. $\square$

4. The case $\ell = p$ with good reduction of height 1.

Belén.

BIBLIOGRAPHY

0. Artin, E. *Collected Papers* (eds Lang, S. & Tate, J.) (Addison-Wesley, 1965).
0. Bloch, S. & Kato, K. p-adic étale cohomology. *Publ. Math. I.H.E.S.* **63,** 107–152 (1986).
0. Bogomolov, F. Sur l'algebricité des représentations l-adiques. *C. R. Acad. Sci. Paris* **290,** 701–703 (1980).
0. Carayol, H. Sur les représentations l-adiques associées aux formes modulaires de Hilbert. *Ann. Sci. E.N.S.* **19,** 409–468 (1986).
0. Cassels, J. Diophantine equations with special reference to elliptic curves. *J. London Math. Soc.* **41,** 193–291 (1966).
0. Cassels, J. & Fröhlich, A. *Algebraic Number Theory* (Academic Press, 1967).
0. Čebotarev, N. Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. *Math. Annalen* **95,** 151–228 (1925).
0. Chevalley, C. Deux théorèmes d'arithmétique. *J. Math. Soc. Japan* **3,** 36–44 (1951).
0. Deuring, M. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg* **14,** 197–272 (1941).
0. Igusa, J. Fibre systems of Jacobian varieties. *I. Amer. J. of Maths.* **78,** 171–199 (1956).
0. Koizumi, S. & Shimura, G. On Specializations of Abelian Varieties. *Sc. Papers Coll. Gen. Ed., Univ. Tokyo* **9,** 187–211 (1959).
0. Lang, S. *Abelian varieties* **7** (Intersc. Tracts, New York, 1957).
0. Lang, S. *Diophantine Geometry* **11** (Intersc. Tracts, New York, 1962).
0. Lang, S. *Algebraic numbers* (Addison-Wesley, New York, 1964).
0. Lang, S. *Introduction to transcendental numbers* (Addison-Wesley, New York, 1966).

0. Lubin, J. One parameter formal Lie groups over p-adic integer rings. *Ann. of Maths.*, **80,** 464–484 (1964).
0. Lubin, J. & Tate, J. Formal complex multiplication in local fields. *Ann. of Maths.*, **81,** 380–387 (1965).
0. Mostow, G. D. & Tamagawa, T. On the compactness of arithmetically defined homogeneous spaces. *Ann. of Maths.*, **76,** 446–463 (1962).
0. Mumford, D. *Geometric Invariant Theory* (Ergebnisse der Math., Bd. 34, Springer-Verlag, 1965).
0. Ogg, A. P. Abelian curves of small conductor. *Journ. fur die reine und ang. Math.*, **226,** 204–215 (1967).
0. Ono, T. Arithmetic of algebraic tori. *Ann. of Maths.* **74,** 101–139 (1961).
0. Pólya, G. & Szegő, G. *Aufgaben und Lehrsätze aus der Analysis. Band I* (Springer-Verlag, 2—Aufl, 1954).
0. Serre, J.-P. *Corps Locaux* (Hermann, Paris, 1962).
0. Serre, J.-P. *Lie algebras and Lie groups* (Benjamin, New York, 1965).
0. Serre, J.-P. *Sur les groupes de Galois attachés aux groupes p-divisibles* in *Proceedings of a Conference on Local Fields* (ed Springer, T. A.) (Springer Berlin Heidelberg, Berlin, Heidelberg, 1967), 113–131. ISBN: 978-3-642-87942-5.
0. Serre, J.-P. & Tate, J. Good reduction of abelian varieties. *Ann. of Math.* **88,** 492–517 (1968).
0. Serre, J.-P. Groupes de Lie p-adiques attachés aux courbes elliptiques. *Coll. Clermont-Ferrand, C.N.R.S.*, 239–256 (1964).
0. Serre, J.-P. Sur les groupes de congruence des variétés abéliennes. *Izv. Akad. Nauk. S.S.S.R.*, **28,** 3–20 (1964).
0. Serre, J.-P. in *Séminaire Bourbaki : années 1966/67 1967/68, exposés 313-346 Séminaire Bourbaki* 10. talk:318, 73–86 (Société mathématique de France, 1968).
0. Shimura, G. A reciprocity law in nonsolvable extensions. *Journal fur die reine und ang. Math.*, **221,** 209–220 (1966).
0. Shimura, G. & Taniyama, Y. *Complex multiplication of abelian varieties and its applications to number theory* (Publ. Math. Soc. Japan, 6, 1961).
0. Taniyama, Y. L-functions of number fields and zeta functions of abelian varieties. *Journ. Math. Soc. Japan* **9,** 330–366 (1957).

0. Tate, J. in *Proc. Purdue Univ. Conf., 1963* 93–110 (New York, 1965).

0. Tate, J. Endomorphisms of Abelian Varieties over finite fields. *Inven. math.* **2,** 134–144 (1966).

0. Weil, A. *Variétés abéliennes et courbes algébriques* (Hermann, Paris, 1948).

0. Weil, A. *Adèles and algebraic groups (Notes by M. Demazure and T. Ono)* (Princeton, Inst. Adv. Study, 1961).

0. Weil, A. *Basic Number Theory* (Springer-Verlag, 1967).

0. Weil, A. Ueber die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. *Math. Annalen,* **168,** 149–156 (1967).

0. Weyl, H. Über die Gleichverteilung von Zahlen mod. Eins. *Math. Annalen* **77,** 313–352 (1914).

INDEX