

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

Jean-Pierre Serre

December 19, 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 Supérieure, 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:

### $\ell$ -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.

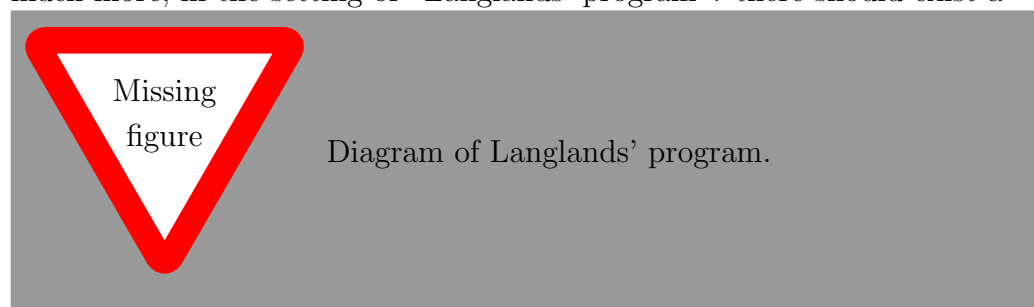
Faltings ([54], see also 82 [82] and 56 [56]), has proved Tate's conjecture that the map

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

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  $\ell$  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 $\ell$ -adic representations

The existence of  $\ell$ -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 [49]). 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 [49]; 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 $\ell$ -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  $\text{char } K = 0$  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  $\ell$ -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 vast program by Fontaine, relating Galois representa-

tions and modules of Dieudonné type (over some “Barsotti-Tate rings”, cf. [58], [59], [61]).





# CONTENTS

<b>I</b>	<b><math>\ell</math>-adic representations</b>	<b>1</b>
1	The notion of an $\ell$ -adic representation . . . . .	1
1.1	Definition . . . . .	1
1.2	Examples . . . . .	3
2	$\ell$ -adic representations of number fields . . . . .	4
2.1	Preliminaries . . . . .	4
2.2	Čebotarev’s density theorem . . . . .	5
2.3	Rational $\ell$ -adic representations . . . . .	7
2.4	Representations with values in a linear algebraic group	10
2.5	$L$ -functions attached to rational representations . . . . .	12
A	Equipartition and $L$ -functions . . . . .	13
A.1	Equipartition . . . . .	13
A.2	The connection with $L$ -functions . . . . .	16
A.3	Proof of theorem 1 . . . . .	19
<b>II</b>	<b>The groups <math>S_m</math></b>	<b>23</b>
1	Preliminaries . . . . .	23
1.1	The torus $\mathbb{T}$ . . . . .	23
1.2	Cutting down $\mathbb{T}$ . . . . .	24
1.3	Enlarging groups . . . . .	24
2	Construction of $T_m$ and $S_m$ . . . . .	26
2.1	Idèles and idèles-classes . . . . .	26
2.2	The groups $T_m$ and $S_m$ . . . . .	28
2.3	The canonical $\ell$ -adic representation with values in $S_m$ .	29
2.4	Linear representations of $S_m$ . . . . .	32
2.5	$\ell$ -adic representations associated to a linear represen- tation of $S_m$ . . . . .	34
2.6	Alternative construction . . . . .	37

2.7	The real case . . . . .	38
2.8	An example: complex multiplication of abelian varieties . . . . .	39
3	Structure of $T_m$ and applications . . . . .	42
3.1	Structure of $X(T_m)$ . . . . .	42
3.2	The morphism $j^*: \mathbb{G}_m \rightarrow T_m$ . . . . .	43
3.3	Structure of $T_m$ . . . . .	44
3.4	How to compute Frobeniuses . . . . .	46
A	Killing arithmetic groups in tori . . . . .	48
A.1	Arithmetic groups in tori . . . . .	48
A.2	Killing arithmetic subgroups . . . . .	49
<b>III Locally algebraic abelian representations</b>		<b>51</b>
1	The local case . . . . .	51
1.1	Definitions . . . . .	51
1.2	Alternative definition of “locally algebraic” via Hodge-Tate modules . . . . .	54
2	The global case . . . . .	55
2.1	Definitions . . . . .	55
2.2	Modulus of a locally algebraic abelian representation . . . . .	56
2.3	Back to $S_m$ . . . . .	58
2.4	A mild generalization . . . . .	60
2.5	The function field case . . . . .	60
3	The case of a composite of quadratic fields . . . . .	63
3.1	Statement of the result . . . . .	63
3.2	A criterion for local algebraicity . . . . .	63
3.3	An auxiliary result on tori . . . . .	65
3.4	Proof of the theorem . . . . .	68
A	Hodge-Tate decompositions and locally algebraic representations . . . . .	68
A.1	Invariance of Hodge-Tate decompositions . . . . .	68
A.2	Admissible characters . . . . .	70
A.3	A criterion for local triviality . . . . .	71
A.4	The character $\xi$ . . . . .	71
A.5	Characters associated with Hodge-Tate decompositions . . . . .	71
A.6	Locally compact case . . . . .	72
A.7	Tate’s theorem . . . . .	75

<b>IV</b>	<b><math>\ell</math>-adic representations attached to elliptic curves</b>	<b>77</b>
1	Preliminaries . . . . .	77
1.1	Elliptic curves . . . . .	77
1.2	Good reduction . . . . .	78
1.3	Properties of $V_\ell$ related to good reduction . . . . .	79
1.4	Šafarevič's theorem . . . . .	81
2	The Galois module attached to $E$ . . . . .	82
2.1	The irreducibility theorem . . . . .	83
2.2	Determination of the Lie algebra of $G_\ell$ . . . . .	84
2.3	The isogeny theorem . . . . .	86
3	Variation of $G_\ell$ and $\tilde{G}_\ell$ with $\ell$ . . . . .	88
3.1	Preliminaries . . . . .	88
3.2	The case of a non integral $j$ . . . . .	88
3.3	Numerical example . . . . .	89
3.4	Proof of the main lemma of 3.1 . . . . .	90
A	Local results . . . . .	94
A.1	The case $v(j) < 0$ . . . . .	94
A.2	The case $v(j) \geq 0$ . . . . .	98
	<b>Index</b>	<b>107</b>



# INTRODUCTION

The “ $\ell$ -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  $\ell^n$ -th division points of abelian varieties (cf. chap. I, 1.2); the corresponding  $\ell$ -adic spaces, first introduced by 40 [40] 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  $\ell$ -adic representation was first defined by Taniyama [35] (see also the review of this paper given by Weil in *Math. Rev.*, 20, 1959, rev.1667). He showed how one can relate  $\ell$ -adic representations relative to different prime numbers  $\ell$  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 34 [34]). 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  $\ell$ -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*  $\ell$ -adic representation: one for which their characteristic polynomials have rational coefficients (instead of merely  $\ell$ -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  $\ell$ -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  $\ell$ -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  $\mathbb{S}$ ) whose representations – in the usual algebraic sense – correspond to the sought for  $\ell$ -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 “ $\ell$ -adic cohomology without  $\ell$ ” so the connection is not surprising). The construction of these groups  $\mathbb{S}$  and of the  $\ell$ -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  $S_m$ ’s.

Chapter III is concerned with the following question: let  $p$  be an abelian  $\ell$ -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  $\ell$ -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 transcendence result of Siegel and Lang (cf. §3).

Chapter IV is concerned with the  $\ell$ -adic representation  $\rho_\ell$ , defined by an *elliptic curve*  $E$ . Its aim is to determine, as precisely as possible, the image of the Galois group by  $\rho_\ell$ , 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 10 [10]). Most of the results have been stated in [25], [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 [25]. 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  $\text{Im}(\rho_\ell)$  then follows, using the properties of abelian representations given in chap. II, III; one has to know that  $\rho_\ell$ , if abelian, is locally algebraic, but this is a consequence of the result of Tate given in chap. III. The variation of  $\text{Im}(\rho_\ell)$  with  $\ell$  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
$\Sigma_K$	$M_K^0$	Set of finite places of a number field $K$ .
$\ell$	$\lambda$	The residue field of a field $L$ relative to a finite place.
$R^*$	$R^\times$	The group of units of a ring $R$ .
$U^\circ$	$\mathring{U}$	The interior of a subset $U$ of a topological space.
$A_K$	$\mathcal{O}_K$	The ring of algebraic integers of a number field $K$ .
$\mathbf{N}v$	$\mathbf{N}v$	$= [\mathcal{O}_v : \mathfrak{m}_v]$ .
$\mathbb{G}_{m/K}$	$\mathbb{G}_{m,K}$	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 70 (III-34): it originally said “ $A_n/A_{n+k}$ ”, and it should be “ $A_n/A_{n+1}$ ”.
- Page 82 (IV-8): it originally said “ $\Delta_v = u^{12}\Delta'$ ”, and it should be “ $\Delta_v = u_v^{12}\Delta'$ ”.
- Page 88 (IV-17): it originally said “by the theorem on section 4”, but the correct reference was 2.2.



# CHAPTER I

## $\ell$ -ADIC REPRESENTATIONS

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

#### 1.1 Definition

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

**Definition 1.** An  $\ell$ -adic representation of  $G$  (or, by abuse of language, of  $K$ ) is a continuous homomorphism  $\rho: G \rightarrow \text{Aut}(V)$ .

**Remark.** 1) A *lattice* of  $V$  is a sub- $\mathbb{Z}_\ell$ -module  $T$  which is free of finite rank, and generate  $V$  over  $\mathbb{Q}_\ell$ , so that  $V$  can be identified with  $T \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ . Notice that there exists a lattice of  $V$  which is stable under  $G$ . 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  $g \in G$  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  $G$ . I-2

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

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

### Exercises.

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

## 1.2 Examples

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

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

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

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

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

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

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

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

**3. Abelian varieties.** Let  $A$  be an abelian variety over  $K$  of dimension  $d$ . If  $\ell \neq \text{char}(K)$ , we define  $T_\ell(A)$ ,  $V_\ell(A)$  in the same way as in example 2. The group  $T_\ell(A)$  is a free  $\mathbb{Z}_\ell$ -module of rank  $2d$  (cf. [12], *loc. cit.*) on which  $G = \text{Gal}(K_s/K)$  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  $\ell \neq \text{char}(K)$ , and let  $i$  be an integer. Using the étale cohomology of **3** [3] we let

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

I-5 The group  $H_\ell^i(X_s)$  is a vector space over  $\mathbb{Q}_\ell$  on which  $G = \text{Gal}(K_s/K)$  acts (via the action of  $G$  on  $X_s$ ). It is finite dimensional, at least if  $\text{char}(K) = 0$  or if  $X$  is proper. We thus get an  $\ell$ -adic representation of  $G$  associated to  $H_\ell^i(X_s)$ ; by taking duals we also get homology  $\ell$ -adic representations. Examples 1, 2, 3 are particular cases of homology  $\ell$ -adic representations where  $i = 1$  and  $X$  is respectively the multiplicative group  $\mathbb{G}_m$ , 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  $G_\ell = \text{SL}(T_\ell(E))$  (cf. **10** [10] for an algebraic proof).
- (c) Using (b), show that, over  $K_0$ , we have  $G_\ell = \text{GL}(T_\ell(E))$ .
- (d) Show that for any closed subgroup  $H$  of  $\text{GL}(2, \mathbb{Z}_\ell)$  there is an elliptic curve (defined over some field) for which  $G_\ell = H$ .

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

### 2.1 Preliminaries

(For the basic notions concerning number fields, see for instance **6** [6], **13** [13] or **44** [44].) Let  $K$  be a number field (i.e. a finite extension of  $\mathbb{Q}$ ). Denote by  $M_K^0$  the set of all finite places of  $K$ , i.e. the set of all normalized discrete valuations of  $K$  (or, alternatively, the set of prime ideals in the ring  $\mathcal{O}_K$  of integers of  $K$ ). The **residue field**  $k_v$  of a place  $v \in M_K^0$  is a finite field with  $\mathbf{N}(v) = p_v^{\deg(v)}$  elements, where  $p_v = \text{char}(k_v)$  and  $\deg(v)$  is the degree of  $k_v$  over  $\mathbb{F}_{p_v}$ . 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  $D_w = \text{Gal}(L_w/K_v)$ . The group  $D_w$  is mapped homomorphically onto the Galois group  $\text{Gal}(\lambda_w/k_v)$  of the corresponding residue extension  $\lambda_w/k_v$ . The kernel of  $G \rightarrow \text{Gal}(\lambda_w/k_v)$  is the inertia group  $I_w$  of  $w$ . The quotient group  $D_w/I_w$  is a finite cyclic group generated by the **Frobenius element**  $F_w$ ; we have  $F(\lambda) = \lambda^{\mathbf{N}(v)}$  for all  $\lambda \in \lambda_w$ . The valuation  $w$  (resp.  $v$ ) is called **unramified** if  $I_w = \{1\}$ . Almost all places of  $K$  are unramified.

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

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

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

## 2.2 Čebotarev’s density theorem

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

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

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

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

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

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

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

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

For infinite extensions, we have:

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

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

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

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



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

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

**Definition 1.** The  $\ell$ -adic representation  $\rho$  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  $\rho$ .
- (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  $\ell$ -adic representation  $\rho$  of  $K$  defines (by restriction) an  $\ell$ -adic representation  $\rho_{/K'}$  de  $K'$ . If  $\rho$  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  $\ell$ -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  $S_\ell$  of elements  $v$  of  $M_K^0$  with  $\rho_v = \ell$ ; In examples 2, 3, one can take for  $S$  the union of  $S_\ell$  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  $\ell$ ) is a consequence of Weil’s results on endomorphisms of abelian varieties (cf. [40] and [12], chap. VII). The rationality of the cohomology representation is a well-known open question. I-10

Belén ♥: Ver si sigue siendo una pregunta abierta.

**Definition 2.** Let  $\ell'$  be a prime,  $\rho'$  an  $\ell'$ -adic representation of  $K$ , and assume that  $\rho, \rho'$  are rational. Then  $\rho, \rho'$  are said to be **compatible** if there exists a finite subset  $S$  of  $M_K^0$  such that  $\rho$  and  $\rho'$  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 are the same for  $\rho$  and  $\rho'$ , at least for almost all  $v$ ’s.)

If  $\rho: \text{Gal}(\overline{K}/K) \rightarrow \text{Aut}(V)$  is rational  $\ell$ -adic representation of  $K$ , then  $V$  has a composition series

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

of  $\rho$ -invariants subspaces with  $V_i/V_{i+1}$  ( $0 \leq i \leq q-1$ ) *simple* (i.e. *irreducible*). The  $\ell$ -adic representation  $\rho'$  of  $K$  defined by  $V' = \sum_{i=0}^{q-1} V_i/V_{i+1}$  is

semi-simple, rational, and compatible with  $\rho$ ; it is the “semi-simplification” of  $V$ .

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

(Hence there exists a unique (up to isomorphism) rational semi-simple  $\ell$ -adic representation compatible with  $\rho$ .)

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

We first prove that  $\text{Tr}(\rho'_1(g)) = \text{Tr}(\rho'_2(g))$  for all  $g \in G$ . Let  $H = G/(\text{Ker}(\rho'_1) \cap \text{Ker}(\rho'_2))$ ; the representations  $\rho'_1, \rho'_2$  may be regarded as representations of  $H$ , and it suffices to show that  $\text{Tr}(\rho'_1(h)) = \text{Tr}(\rho'_2(h))$  for all  $h \in H$ . Let  $K' \subset \bar{K}$  be the fixed field of  $H$ . Then by the compatibility of  $\rho'_1, \rho'_2$  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  $\text{Tr}(\rho'_1(F_w)) = \text{Tr}(\rho'_2(F_w))$ . But, by cor. 1 to Čebotarev’s theorem (cf. 2.2) the  $F_w$  are dense in  $H$ . Hence  $\text{Tr}(\rho'_1(h)) = \text{Tr}(\rho'_2(h))$  for all  $h \in H$  since  $\text{Tr} \circ \rho'_1, \text{Tr} \circ \rho'_2$  are continuous.

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

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

Belén ♥: Cómo citar esto

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

**Definition 3.** For each prime  $\ell$  let  $\rho_\ell$  be a rational  $\ell$ -adic representation of  $K$ . The system  $(\rho_\ell)$  is said **to be compatible** if  $\rho_\ell, \rho_{\ell'}$  are compatible for any two primes  $\ell, \ell'$ . The system  $(\rho_\ell)$  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  $v \notin S \cup S_\ell$ ,  $\rho_\ell$  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  $(\rho_\ell)$  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  $\ell$ -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. [32].

### Questions.

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

A somewhat similar question is:

Is any compatible system strictly compatible?

- 2) Can any rational  $\ell$ -adic representation be obtained (by tensor products, direct sums, etc.) from ones coming from  $\ell$ -adic cohomology?
- 3) Given a rational  $\ell$ -adic representation  $\rho$  of  $K$ , and a prime  $\ell'$ , does there exist a rational  $\ell'$ -adic representation  $\rho'$  of  $K$  compatible with  $\rho$ ?  $\rightarrow$  [no: easy counter-examples].
- 4) Let  $\rho, \rho'$  be rational  $\ell, \ell'$ -adic representations of  $K$  which are compatible and semi-simple.

- (i) If  $\rho$  is abelian (i.e. , if  $\text{Im}(\rho)$  is abelian), is it true that  $\rho'$  is abelian? (We shall see in chapter III that this is true at least if  $\rho$  is “locally algebraic”.)  $\rightarrow$  [yes: this follows from [36].]

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

- 5) Let  $X$  be a non-singular projective variety defined over  $K$ , and let  $i$  be an integer. Is the  $i$ -th cohomology representation  $H_\ell^i(X_s)$  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 “congruence subgroup problem” on abelian varieties, cf. [24], §3.)  $\rightarrow$  [yes: for  $i = 1$ : see [48] and also [75].]

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

**Exercise.**

- I-14
- 1) Let  $\rho$  and  $\rho'$  be two rational, semi-simple, compatible representations. Show that, if  $\text{Im}(\rho)$  is finite, the same is true for  $\text{Im}(\rho')$  and that  $\text{Ker}(\rho) = \text{Ker}(\rho')$ . (Apply exer. 3 of 1.1 to  $\rho'$  and to  $U = \text{Ker}(\rho)$ .) Generalize this to  $\lambda$ -adic representations (with respect to a number field  $E$ ).
  - 2) Let  $\rho$  (resp.  $\rho'$ ) be a rational  $\ell$ -adic (resp.  $\ell'$ -adic) representation of  $K$ , of degree  $n$ . Assume  $\rho$  and  $\rho'$  are compatible. If  $s \in G = \text{Gal}(\bar{K}/K)$ , let  $\sigma_i(s)$  (resp.  $\sigma'_i(s)$ ) be the  $i$ -th coefficient of the characteristic polynomial of  $\rho(s)$  (resp.  $\rho'(s)$ ). Let  $P(X_0, \dots, X_n)$  be a polynomial with rational coefficients, and let  $X_P$  (resp.  $X'_P$ ) be the set of  $s \in G$  such that  $P(\sigma_0(s), \dots, \sigma_n(s)) = 0$  (resp.  $P(\sigma'_0(s), \dots, \sigma'_n(s)) = 0$ ).
    - (a) Show that the boundaries of  $X_P$  and  $X'_P$  have measure zero for the Haar measure  $\mu$  of  $G$  (use Exer. of 2.2).
    - (b) Assume that  $\mu$  is normalized, i.e.  $\mu(G) = 1$ . Let  $T_P$  be the set of  $v \in M_K^0$  at which  $\rho$  is unramified, and for which the coefficients  $\sigma_0, \dots, \sigma_n$  of characteristic polynomial of  $F_{v,\rho}$  satisfy the equation  $P(\sigma_0, \dots, \sigma_n) = 0$ . 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  $\rho: \text{Gal}(K_s/K) \rightarrow H(\mathbb{Q}_\ell)$  is called an  $\ell$ -adic representation of  $K$  with values in  $H$ .

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

If  $K$  is a number field, one defines in an obvious way what it means for I-15  
 $\rho$  to be unramified at a place  $v \in M_K^0$ ; if  $w \mid v$ , one defines the Frobenius element  $F_{w,\rho} \in H(\mathbb{Q}_\ell)$  and its conjugacy class  $F_{v,\rho}$ . We say, as before, that  $\rho$  is **rational** if

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

Two rational representations  $\rho, \rho'$  (for primes  $\ell, \ell'$ ) are said to be **compatible** if there exists a finite subset  $S$  of  $M_K^0$  such that  $\rho$  and  $\rho'$  are unramified outside  $S$  and such that for any central element  $f \in A$  and any  $v \in M_K^0 - S$  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  $\text{GL}_{V_0}$  be the linear algebraic group over  $\mathbb{Q}$  whose group of points in any commutative  $\mathbb{Q}$ -algebra  $k$  is  $\text{Aut}(V_0 \otimes_{\mathbb{Q}} k)$ ; in particular, if  $V_\ell = V_0 \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ , then  $\text{GL}_{V_0}(\mathbb{Q}_\ell) = \text{Aut}(V_\ell)$ . If  $\varphi: H \rightarrow \text{GL}_{V_0}$  is a homomorphism of linear algebraic groups over  $\mathbb{Q}$ , call  $\varphi_\ell$  the induced homomorphism of  $H(\mathbb{Q}_\ell)$  into  $\text{GL}_{V_0}(\mathbb{Q}_\ell) = \text{Aut}(V_\ell)$ . If  $\rho$  is an  $\ell$ -adic representation of  $\text{Gal}(\overline{K}/K)$  into  $H(\mathbb{Q}_\ell)$ , one gets by composition a linear  $\ell$ -adic representation  $\varphi_\ell \circ \rho: \text{Gal}(K_s/K) \rightarrow \text{Aut}(V_\ell)$ . 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  $\rho$  is rational ( $K$  a number field). Of course, compatible

representations in  $H$  give compatible linear representations. We will use this method of constructing compatible representations in the case where  $H$  is abelian (see ch. 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  $\ell$ -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  $\ell$ . 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  $|\lambda_{i,v}| \leq (\mathbf{N}v)^k$ , and this implies that  $L_\rho$  is convergent in some half plane  $\Re(s) > C$ ; one conjectures it extends to a meromorphic function in the whole plane. When  $\rho$  comes from  $\ell$ -adic cohomology, there are some further conjectures on the zeros and poles of  $L_\rho$ , cf. Tate [36]; 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  $\lambda$ -adic representations (2.3, Remark), where  $E$  is a number field, once an embedding of  $E$  into  $\mathbb{C}$  has been chosen.

2) We have given a definition of the local factors of  $L_\rho$  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.  $\rightarrow$  [see [51], [74].]

Belén ♡: No  
cacho si el  $\mathbb{C}$  es  
los complejos o  
qué weá

- 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  $\phi$ ) 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

$$x \prod_{n=1}^{\infty} (1 - x^n)^{24} = \sum_{n=1}^{\infty} \tau(n) x^n?$$

There is considerable numerical evidence for this, based on the congruence properties of  $\tau$  (Swinerton-Dyer, unpublished); of course, such a  $\rho$  would be of dimension 2, and its exceptional set  $S$  would be empty.  $\rightarrow$  [proved by Deligne: see [49], [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)  $\ell$ -adic representations; see for instance **33** [33] and **45** [45].  $\rightarrow$  [see also [49], [51], [65], [66], [68], [84].]

- Examples.** 1. If  $G$  acts through a *finite* group,  $L_\rho$  is an Artin (non abelian)  $L$ -series, at least up to a finite number of factors (cf. [1]). 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  $\rho$  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  $\rho$  give the zeta functions of the products  $E \times \dots \times E$ , cf. **36** [36].

## §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  $\delta_x$  be the Dirac measure associated to  $x$ ; if  $f \in C(X)$ , we have  $\delta_x(f) = f(x)$ .

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

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

I-19 and let  $\mu$  be a Radon measure on  $X$  (i.e. a continuous linear form on  $C(X)$ , cf. Bourbaki, Int., chap. III, §1). The sequence  $(x_n)$  is said to be  **$\mu$ -equidistributed**, or  **$\mu$ -uniformly distributed**, if  $\mu_n \rightarrow \mu$  weakly as  $n \rightarrow \infty$ , i.e. if  $\mu_n(f) \rightarrow \mu(f)$  as  $n \rightarrow \infty$  for any  $f \in C(X)$ . Note that this implies that  $\mu$  is positive and of total mass 1. Note also that  $\mu_n(f) \rightarrow \mu(f)$  means that

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

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

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

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

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

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

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

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

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  $\mu$  be the Lebesgue measure. A sequence  $(x_n)$  of points of  $X$  is  $\mu$ -equidistributed if and only if for each interval  $[a, b]$ , of length  $d > 0$  in  $[0, 1]$  the number of  $m \leq n$  such that  $x_m \in [a, b]$  is equivalent to  $dn$  as  $n \rightarrow \infty$ .
2. Let  $G$  be a compact group and let  $X$  be the space of conjugacy classes of  $G$  (i.e. the quotient space of  $G$  by the equivalence relation induced by inner automorphisms of  $G$ ). Let  $\mu$  be a measure on  $G$ ; its image of  $G \rightarrow X$  is a measure on  $X$ , which we also denote by  $\mu$ . We then have:

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

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

The map  $C(X) \rightarrow C(G)$  is an isomorphism of  $C(X)$  onto the space of central functions on  $G$ ; by the Peter-Weyl theorem, the irreducible characters  $\chi$  of  $G$  generate a dense subspace of  $C(X)$ . Hence the proposition follows from lemma 1. I-21

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

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

This follows from Prop. 2 and the following facts:

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

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

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

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

## 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  $\geq 2$ . We make the following *hypotheses*:

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

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

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

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

Under these assumptions, we have:

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

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

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

The theorem results, by a standard argument, from the theorem of Wiener-Ikehara, cf. 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  $\mu$  such that for any irreducible character  $\chi$  of  $G$  we have*

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

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

**Examples.** 1) Let  $G$  be the Galois group of a *finite* Galois extension  $L/K$  of the number field  $K$ , let  $M$  be the set of unramified places of  $K$ , let  $x_v$  be the Frobenius conjugacy class defined by  $v \in M$ , and let  $\mathbf{N}v$  be the norm of  $v$ , cf. §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  $\Re(s) = 1$ , I-24 cf. for instance **13** [13], chap. VII; for a proof of (2), cf. **1** [1]. Hence theorem ?? gives the equidistribution of the Frobenius elements, i.e. the Čebotarev density theorem, cf. ~??sec:I22.

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

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

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

Then, the elements  $x_v$  are *uniformly distributed* in  $G$  with respect to the normalized Haar measure. This follows from theorem 1 and the fact that the  $L$ -functions relative to the irreducible characters  $\chi$  of  $G$

are Hecke  $L$ -functions with Grössencharakteren; these  $L$ -functions are holomorphic and non-zero for  $\Re(s) \geq 1$  if  $\chi \neq 1$ , see [13], chap. VII.

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

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

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

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

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

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

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

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

If we put:

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

I-26 we have

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

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

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

### 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

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

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

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

shows that

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

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

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

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. [13]):

**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

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

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

One applies this theorem to

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

and we take for  $F^+$  the series

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

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

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

differs from the logarithmic derivative of

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

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

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

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

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

and in particular,

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

Hence,

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

and we may apply proposition 2 to conclude the proof.

q.e.d.





## CHAPTER II

### THE GROUPS $S_{\mathfrak{m}}$

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

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

### §1. Preliminaries

#### 1.1 The torus $\mathbb{T}$

Let  $\mathbb{T} = \mathfrak{R}_{K/\mathbb{Q}}(\mathbb{G}_{m,K})$  be the algebraic group over  $\mathbb{Q}$ , obtained from the multiplicative group  $\mathbb{G}_m$  by restriction of scalars from  $K$  to  $\mathbb{Q}$ , cf. **43** [43], §1.3. If  $A$  is a commutative  $\mathbb{Q}$ -algebra, the points of  $\mathbb{T}$  with values in  $A$  form by definition the multiplicative group  $(K \otimes_{\mathbb{Q}} A)^{\times}$  of invertible elements of  $K \otimes_{\mathbb{Q}} A$ . In particular,  $\mathbb{T}(\mathbb{Q}) = K^{\times}$ . If  $d = [K : \mathbb{Q}]$ , the group  $\mathbb{T}$  is a **torus** of dimension  $d$ ; this means that the group  $\mathbb{T}_{/\overline{\mathbb{Q}}} = \mathbb{T} \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}$  obtained from  $\mathbb{T}$  by extending the scalars from  $\mathbb{Q}$  to  $\overline{\mathbb{Q}}$ , is isomorphic to  $\mathbb{G}_{m,\overline{\mathbb{Q}}} \times \dots \times \mathbb{G}_{m,\overline{\mathbb{Q}}}$  II-2  
 ( $d$  times). More precisely, let  $\Gamma$  be the set of embeddings of  $K$  into  $\overline{\mathbb{Q}}$ ; each  $\sigma \in \Gamma$  extends to a homomorphism  $K \otimes_{\mathbb{Q}} \overline{\mathbb{Q}} \rightarrow \overline{\mathbb{Q}}$ , hence defines a morphism  $[\sigma]: \mathbb{T}_{/\overline{\mathbb{Q}}} \rightarrow \mathbb{G}_{m,\overline{\mathbb{Q}}}$ . The collection of all  $[\sigma]$ ’s gives the isomorphism  $\mathbb{T}_{/\overline{\mathbb{Q}}} \rightarrow \mathbb{G}_{m,\overline{\mathbb{Q}}} \times \dots \times \mathbb{G}_{m,\overline{\mathbb{Q}}}$ . Moreover, the  $[\sigma]$ ’s form a basis of the *character group*  $X(T) = \text{Hom}_{\overline{\mathbb{Q}}}(\mathbb{T}_{/\overline{\mathbb{Q}}}, \mathbb{G}_{m,\overline{\mathbb{Q}}})$  of  $T$ . Note that the Galois group  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  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 [21].)

## 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  $X = X(\mathbb{T})$  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

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

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

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

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  $A \rightarrow B$  and a homomorphism of  $Y_2$  into  $B(k)$  such that,

(a) *the diagram*

$$\begin{array}{ccc} Y_1 & \longrightarrow & A(k) \\ \downarrow & & \downarrow \\ Y_2 & \longrightarrow & B(k) \end{array}$$

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

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

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

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

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

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  $A \rightarrow B$  and  $Y_2 \rightarrow B(k)$  being defined as follows:

$A \rightarrow B$  is the natural map  $A \rightarrow A_0$  followed by translation by  $-c(0, 0)$ ,  
 $Y_2 \rightarrow B(k)$  maps an element  $\bar{y} + z$ ,  $y \in Y_3$ ,  $z \in Y_1$  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

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

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  $Y_1 \rightarrow A(k) \rightarrow A'(k')$ . 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  $\text{char}(k) = 0$  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  $X(B) = \text{Hom}_{\bar{k}}(B/\bar{k}, \mathbb{G}_{m, \bar{k}})$ , which is a Galois-module of finite type over  $\mathbb{Z}$ . Here  $X(B)$  can be described as the set of pairs  $(\phi, \chi)$ , where  $\phi: Y_2 \rightarrow \bar{k}^\times$  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.**

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

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

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

## §2. Construction of $T_m$ and $S_m$

### 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  $M_K^\infty$  be the set of equivalence classes of archimedean absolute values of  $K$ , and let  $M_K$  be the union of  $M_K^0$  and  $M_K^\infty$ . If  $v \in M_K$  then  $K_v$  denotes the *completion* of  $K$  with respect to  $v$ . For  $v \in M_K^\infty$  we have  $K_v = \mathbb{R}$  or  $K_v = \mathbb{C}$ , and  $K$  is ultrametric if  $v \in M_K^0$ . For  $v \in M_K^0$ , the group of units

of  $K_v$  is denoted by  $U_v$ . The **idèle group**  $I$  of  $K$  is the subgroup of

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

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

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

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

Let  $S$  be a finite subset of  $M_K^0$ . Then by a **modulus of support**  $S$  we mean a family  $\mathfrak{m} = (m_v)_{v \in S}$  where the  $m_v$  are integers  $\geq 1$ . 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 ([8], see also [24], n° 3.5) every subgroup of finite index in  $E$  contains an  $E_{\mathfrak{m}}$  for a suitable modulus  $\mathfrak{m}$ .)

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

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

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

**Remark.** A more classical definition of  $C_{\mathfrak{m}}$  is as follows. Let  $\text{Id}_S$  be the group of fractional ideals of  $K$  prime to  $S$ , and  $P$  the subgroup of principal ideals  $(\gamma)$ , where  $\gamma$  is totally positive and  $\gamma \equiv 1 \pmod{\mathfrak{m}}$  (i.e.  $\gamma$  belongs to

$U_{v,\mathfrak{m}}$  for all  $v \in S$  and  $v \in M_K^\infty$ ). Let  $\text{Cl}_{\mathfrak{m}} = \text{Id}_S / P_{S,\mathfrak{m}}$ . We have the exact sequence:

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

For each  $a = \prod_{v \notin S} v^{a_v} \in \text{Id}_S$ , 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  $\alpha$  in  $I_{\mathfrak{m}} = I/U_{\mathfrak{m}}$  depends only on  $\mathbf{a}$ . We then get a homomorphism  $g: \text{Id}_S \rightarrow I_{\mathfrak{m}}$ . One checks readily that  $g$  extends to a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & P_{S,\mathfrak{m}} & \longrightarrow & \text{Id}_S & \longrightarrow & \text{Cl}_{\mathfrak{m}} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow g & & \downarrow f & & \\ 1 & \longrightarrow & K^\times/E_{\mathfrak{m}} & \longrightarrow & I_{\mathfrak{m}} & \longrightarrow & C_{\mathfrak{m}} & \longrightarrow & 1 \end{array}$$

and that  $f: \text{Cl}_{\mathfrak{m}} \rightarrow C_{\mathfrak{m}}$  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 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  $T_{\mathfrak{m}} \rightarrow S_{\mathfrak{m}}$  and a group homomorphism  $\varepsilon_{\mathfrak{m}} \rightarrow S_{\mathfrak{m}}(\mathbb{Q})$ . 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

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^\times/E_{\mathfrak{m}} & \longrightarrow & I_{\mathfrak{m}} & \longrightarrow & C_{\mathfrak{m}} & \longrightarrow & 1 \\ & & \downarrow & & \downarrow \varepsilon & & \downarrow \text{id} & & \\ 1 & \longrightarrow & T_{\mathfrak{m}}(\mathbb{Q}) & \longrightarrow & S_{\mathfrak{m}}(\mathbb{Q}) & \longrightarrow & C_{\mathfrak{m}} & \longrightarrow & 1 \end{array} \quad (**)$$

is commutative.

**Remark.** Let  $\mathfrak{m}'$  be another modulus; assume  $\mathfrak{m}' \geq \mathfrak{m}$ , i.e.  $\text{Supp}(\mathfrak{m}') \supset \text{Supp}(\mathfrak{m})$  and  $\mathfrak{m}'_v \geq \mathfrak{m}_v$  if  $v \in \text{Supp}(\mathfrak{m})$ . From the inclusion  $U_{\mathfrak{m}'} \subset U_{\mathfrak{m}}$  one deduces maps  $T_{\mathfrak{m}'} \rightarrow T_{\mathfrak{m}}$  and  $I_{\mathfrak{m}'} \rightarrow I_{\mathfrak{m}}$ , whence a morphism  $S_{\mathfrak{m}'} \rightarrow S_{\mathfrak{m}}$ . 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  $\varepsilon_{\mathfrak{m}}: I/U_{\mathfrak{m}} \rightarrow S_{\mathfrak{m}}(\mathbb{Q})$  is the image of  $\overline{E_{\mathfrak{m}}}(\mathbb{Q}) \rightarrow I/U_{\mathfrak{m}}$ .
- 2) Let  $H_{\mathfrak{m}'/\mathfrak{m}}$  be the kernel of  $S_{\mathfrak{m}'} \rightarrow S_{\mathfrak{m}}$ , where  $\mathfrak{m}' \geq \mathfrak{m}_v$ . 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)

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

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

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

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

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  $\text{pr}_{\ell}$  denote the projection of  $I$  onto this factor. The map

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

is a continuous homomorphism.

**Lemma 1.**  $\alpha_{\ell}$  and  $\varepsilon$  coincide on  $K^{\times}$ .

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

Now, let  $\varepsilon_\ell: I \rightarrow S_{\mathfrak{m}}(\mathbb{Q}_\ell)$  be defined by

II-11

$$\begin{aligned} \varepsilon_\ell(\mathbf{a}) &= \varepsilon(\mathbf{a})\alpha_\ell(\mathbf{a}^{-1}) \\ \text{i.e. } \varepsilon_\ell &= \varepsilon \cdot \alpha_\ell^{-1}. \end{aligned} \quad (***)$$

(If  $\mathbf{a} \in I$ , write  $a_\ell$  the  $\ell$ -component of  $\mathbf{a}$ . Then

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

By the lemma,  $\varepsilon_\ell$  is trivial on  $K$  and, hence, defines a map  $C \rightarrow S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ ; since  $S_{\mathfrak{m}}(\mathbb{Q}_\ell)$  is totally disconnected (it is an  $\ell$ -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  $G^{\text{ab}}$  of the maximal abelian extension of  $K$ . So we end up with a homomorphism  $\varepsilon_\ell: G^{\text{ab}} \rightarrow S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ , 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  $v \notin \text{Supp}(\mathfrak{m})$ , and let  $f_v \in I$  be an idèle which is a uniformizing parameter at  $v$ , and which is equal to 1 everywhere else; let  $F_v = \varepsilon(f_v)$  be the image of  $f_v$  in  $S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ . With these notations we have:

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

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

II-12 *c) If  $v \notin \text{Supp}(\mathfrak{m}) \cup S_\ell$ , then the Frobenius element  $F_{v, \varepsilon_\ell}$  (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  $C/D \xrightarrow{\sim} G^{\text{ab}}$  maps  $K_v^\times$  (resp.  $U_v$ ) onto a dense subgroup of the decomposition group of  $v$  in  $G^{\text{ab}}$  (resp. onto the inertia group of  $v$  in  $G^{\text{ab}}$ ), and that a uniformizing element  $f_v$  of  $K_v^\times$  is mapped onto the Frobenius class of  $v$ .

If  $v \notin \text{Supp}(\mathfrak{m})$  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  $\varepsilon_\ell$  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  $\varepsilon$  form a system of strictly compatible  $\ell$ -adic representations with values in  $S_{\mathfrak{m}}$ .*



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

**Remark.** By construction,  $\varepsilon_\ell: I \rightarrow S_{\mathfrak{m}}(\mathbb{Q}_\ell)$  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,  $\text{Im}(\varepsilon_\ell)$  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  $\text{Im}(\varepsilon_\ell)$  is *Zariski-dense* in  $S_{\mathfrak{m}}$ .

II-13

**Exercises.**

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

- 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  $\mathbf{a} \in I$  may be written as

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

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

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

- c) Show that

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

and

$$F_p = p.$$

- d) Show that  $\rho_\ell$  coincides with the character  $\chi_\ell$  of Chap. I, 1.2.

- (2) Let  $K = \mathbb{Q}$ ,  $\text{Supp}(\mathfrak{m}) = \{2\}$  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 $S_m$

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  $X(H) = \text{Hom}_{\bar{k}}(H_{/\bar{k}}, \mathbb{G}_{m, \bar{k}})$  be the group of characters of  $H$  (of degree 1). Here we write the characters of  $X(H)$  multiplicatively. The group  $G = \text{Gal}(\bar{k}/k)$  acts on  $X(H)$ . II-14

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

$$\alpha: \bar{k}[X(H)] \longrightarrow \bar{\Lambda}$$

where  $\bar{k}[X(H)]$  is the group algebra of  $X(H)$  over  $\bar{k}$ . 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  $a_{\chi} \in \bar{k}$  and  $\chi \in X(H)$ . It is well-known (linear independence of characters) that  $\alpha$  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  $\bar{k}[X(H)]$  with a subalgebra of  $\bar{\Lambda}$ .

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

$$\phi: H \longrightarrow \text{GL}_V$$

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

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

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

- II-15 We have  $\theta_{\phi}(h) = \text{Tr}(\phi(h))$  for any point  $h$  of  $H$  (with value in any commutative  $k$ -algebra). Let  $\text{Rep}_k(H)$  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  $\text{Rep}_k(H) \rightarrow \text{Rep}_{k_1}(H_{/k_1})$  which is easily seen to be *injective*. We say that an element of  $\text{Rep}_{k_1}(H_{/k_1})$  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  $\text{Rep}_k(H)$  and the set of elements  $\theta = \sum n_\chi \chi$  of  $\mathbb{Z}[X(H)]$  which satisfy:*

- (a)  $\theta$  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  $\theta$  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  $\chi$ , then

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

The fixed field  $k_\chi$  of  $G(\chi)$  in  $k$  is the smallest subfield of  $k$  such that  $\chi \in \Lambda \otimes k_\chi$ . Consider  $\chi$  as a representation of degree 1 of  $H_{/k_\chi}$ . One gets, by restriction of scalars to  $k$ , a representation  $\phi$  of  $H$  of degree  $[k_\chi : k]$ . One sees II-16 easily that the trace  $\theta_\phi$  of  $\phi$  is equal to  $\theta$ . The surjectivity of  $\phi \mapsto \theta_\phi$  now follows from the fact that any  $\theta$  satisfying (a) and (b) is a sum of elements of the form (\*) above.  $\square$

**Corollary 1.1.** *In order that  $\phi_1 \in \text{Rep}_{k_1}(H_{/k_1})$  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  $\phi \in \text{Rep}_{k_1}(S_{\mathfrak{m}/k_1})$ . The following properties are equivalent:*

- (i)  $\phi$  can be defined over  $k$ ,
- (ii) for every  $v \notin \text{Supp}(\mathfrak{m})$ , 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  $\text{Tr}(\phi(F_v)) \in k$  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  $\ell$  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 (resp.  $\ell$ -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  $\overline{X} = \text{Im}(\varepsilon_{\ell})$  (cf. 2.3). The set  $\text{Im}(\varepsilon_{\ell})$ , 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  $\theta_{\phi}$  be the trace of  $\theta$  in  $\Lambda \otimes_k k_1$ , where  $\Lambda$  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  $\alpha_0$ . We have  $\theta_{\phi} = \sum_{\alpha} \lambda_{\alpha} \otimes \ell_{\alpha}$  ( $\lambda_{\alpha} \in \Lambda$ ); hence  $\text{Tr}(\phi(h)) = \theta_{\phi}(h) = \sum_{\alpha} \lambda_{\alpha}(h) \ell_{\alpha}$  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  $\alpha$ ; since  $\text{Tr}(\phi(F_v)) \in k$ , 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  $\Lambda$  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  $\chi: I \rightarrow \overline{\mathbb{Q}}^{\times}$  having the following two properties:

- (a)  $\chi(x) = 1$  if  $x \in U_{\mathfrak{m}}$ .
- (b) For each embedding  $\sigma$  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 $\ell$ -adic representations associated to a linear representation of $S_{\mathfrak{m}}$

II-18

**1.  $\ell$ -adic case.** Let  $V_{\ell}$  be a finite-dimensional  $\mathbb{Q}_{\ell}$ -vector space and

$$\phi: S_{\mathfrak{m}/\mathbb{Q}_{\ell}} \rightarrow \text{GL}_{V_{\ell}}$$

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

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

which is continuous for the  $\ell$ -adic topologies of those groups.

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

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

i.e. an *abelian  $\ell$ -adic representation of  $K$*  in  $V_\ell$ .

Belén ♥: Lo dejo cómo  $G$  o como galois de algo

**Proposition 1.** *a) The representation  $\phi_\ell$  is semi-simple.*

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

*Then  $\phi_\ell$  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.*

Belén ♥: no per-tence?

II-19

*c) The representation  $\phi_\ell$  is rational (Chap. I, 2.3) if and only if  $\phi$  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  $\phi_\ell$  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  $\phi_T: T/\mathbb{Q}_\ell \rightarrow \mathrm{GL}_{V_\ell}$  be defined by composing  $T/\mathbb{Q}_\ell \rightarrow S_{\mathfrak{m}/\mathbb{Q}_\ell}$  with  $\phi$ . 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  $\varepsilon_\ell$ .

Belén ♥: Es T de toro?

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

**Theorem 1.** 1) *The  $\phi_\ell$  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  $(\phi_\ell)$  is the element  $\phi_0(F_v)$  of  $\mathrm{Aut}(V_0)$ .*

3) *There exist infinitely many primes  $\ell$  such that  $\phi_\ell$  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  $\phi_0$  becomes diagonalizable. If  $\ell$  is a prime number which splits completely in  $E$ , one can embed  $E$  into  $\mathbb{Q}_\ell$  and this shows that  $\phi_\ell$  is diagonalizable. Assertion 3) now follows from the well-known fact that there exist infinitely many such  $\ell$  (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

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

Note that their eigenvalues generate a *finite extension* of  $\mathbb{Q}$ ; indeed they are contained in any field over which  $\phi_0$  can be brought in diagonal form.

II-21

### Exercises.

- 1) Let  $\phi_0: S_{\mathfrak{m}} \rightarrow \mathrm{GL}_{V_0}$  be a linear representation of  $S_{\mathfrak{m}}$ , and let  $\ell$  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  $\phi_0$ , i.e. the Lie algebra of  $\phi_0(S_{\mathfrak{m}})$ . Show that the Lie algebra of the  $\ell$ -adic Lie group  $\text{Im}(\phi_{\ell})$  is  $\phi_0(\mathfrak{s}_{\mathfrak{m}}) \otimes \mathbb{Q}_{\ell}$ . (Use the fact that  $\text{Im}(\varepsilon_{\ell})$  is open in  $S_{\mathfrak{m}}(\mathbb{Q}_{\ell})$ , cf. 2.3.)
- 2) a) Show that there exists a unique one-dimensional representation

$$\mathbf{N}: S_{\mathfrak{m}} \rightarrow \mathbb{G}_m$$

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

- b) Show that the morphism  $T \rightarrow S_{\mathfrak{m}} \xrightarrow{\mathbf{N}} \mathbb{G}_m$  is the one induced by the norm map from  $K$  to  $\mathbb{Q}$ .
- c) Show that the  $\ell$ -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  $\phi_0: S_{\mathfrak{m}} \rightarrow \text{GL}_{V_0}$  be as in 2.5. If we compose  $\phi_0$  with the map  $\varepsilon: I \rightarrow S_{\mathfrak{m}}(\mathbb{Q})$  defined in 2.2, we obtain a homomorphism

$$\phi_0 \circ \varepsilon: I \longrightarrow \text{GL}_{V_0}(\mathbb{Q}) = \text{Aut}(V_0).$$

Conversely:

II-22

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

*Moreover, such a  $\phi_0$  is unique.*

*Proof.* The necessity of the conditions (a) and (b) is trivial. Conversely, if  $f$  has properties (a), (b), it defines a homomorphism  $I/U_{\mathfrak{m}} \rightarrow \text{Aut}(V_0)$ . On the other hand, since  $f$  and  $\psi$  agree on  $K^{\times}$  the morphism  $\psi$  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  $\psi$  factors through

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

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

**Remark.** Since  $U$  is open, property (a) implies that  $f$  is *continuous* with respect to the discrete topology of  $\mathrm{Aut}(V_0)$ . Conversely, any continuous homomorphism  $f: I \rightarrow \mathrm{Aut}(V_0)$  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  $\psi: \mathbb{T} \rightarrow \mathrm{GL}_{V_0}$  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  $\phi_0: S_{\mathfrak{m}} \rightarrow \mathrm{GL}_{V_0}$  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  $\ell$ . However, they have an archimedean analogue, as follows:

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

$$\pi_\infty: \mathbb{T}(R) \rightarrow S_{\mathfrak{m}}(R)$$

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 group  $I$ . Let  $\mathrm{pr}_\infty$  be the projection on this factor; the map

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

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

$$\varepsilon_\infty: I \rightarrow S_{\mathfrak{m}}(R)$$

by

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



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

The main difference with the “finite” case is that  $\varepsilon_{\infty}$  *is not trivial on the connected component of  $C$* , hence has no Galois group interpretation.

When one composes  $\varepsilon_{\infty}: C \rightarrow S_{\mathfrak{m}}(R)$  with a complex character  $S_{\mathfrak{m}/C} \rightarrow \mathbb{G}_{m,C}$ , one gets a homomorphism  $C \rightarrow C^{\times}$ , i.e. that the characters obtained in this way coincide with the “Größencharakter of type  $(A_0)$ ” of Weil (cf. [35], [41]), whose conductor divide  $\mathfrak{m}$ .

**Exercise.** Let

II-25

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

be the map defined by  $\varepsilon_{\infty}$  and the  $\varepsilon_{\ell}$ '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  $e: I \rightarrow S_{\mathfrak{m}}(A)$  is continuous (for the natural topology of the adèlized group  $S_{\mathfrak{m}}(A)$ ).
- b) Let  $\pi_A: T(A) \rightarrow S_{\mathfrak{m}}(A)$  be the map defined by  $\pi: \mathbb{T} \rightarrow S_{\mathfrak{m}}$ . 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  $\varepsilon: I \rightarrow S_{\mathfrak{m}}(\mathbb{Q}) \subset S_{\mathfrak{m}}$  is the map defined in 2.3. [Note that this gives an alternate definition of the  $\varepsilon_{\ell}$ '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 34 [34], 35 [35], 41 [41], [42] and 32 [32].)

Let  $A$  be an abelian variety of dimension  $d$  defined over  $K$ . Let  $\text{End}_K(A)$  be its ring of endomorphisms and put  $\text{End}_K(A)_0 = \text{End}_K(A) \otimes \mathbb{Q}$ .

Let  $E$  be a number field of degree  $2d$ , and

II-26

$$i: E \rightarrow \text{End}_K(A)_0$$

be an injection of  $E$  into  $\text{End}_K(A)_0$ . 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  $\ell$  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  $\text{End}_K(A)_0$  acts on  $V_\ell$ ; 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.**  *$V_\ell$  is a free  $E_\ell$ -module of rank 1.*

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

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

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  $\rho$  takes values in  $T_E(\mathbb{Q}_\ell)$ .

**Theorem 1.** (a) *The system  $(\rho_\ell)$  is a strictly compatible system of rational  $\ell$ -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*

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

*such that  $\rho$  is the image by  $\varphi$  of the canonical system  $(\varepsilon_\ell)$  attached to  $S_{\mathfrak{m}}$ , cf. 2.3.*

Moreover, the restriction of  $\varphi$  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  $j: K \rightarrow \text{End}_E(t)$ . In particular, if  $x \in K^\times$ ,  $\det_E j(x)$  is an element of  $E^\times$ ; the map  $\det_E j: K^\times \rightarrow E^\times$  is clearly the restriction of an algebraic morphism  $\delta: \mathbb{T} \rightarrow T_E$ .

**Theorem 2.** *The map  $\delta: \mathbb{T} \rightarrow T_E$  coincides with the composition map  $\mathbb{T} \rightarrow T_{\mathfrak{m}} \xrightarrow{\varphi} T_E$ .*

**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  $E \rightarrow K$ . The map  $\det_E j: K^\times \rightarrow E^\times$  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  $p_\ell$  is unramified at  $v$  (the converse is also true, see [32]); moreover the corresponding Frobenius element  $F_{v, \rho_\ell}$  may be identified with the Frobenius endomorphism  $F_v$  of the reduced variety  $\tilde{A}_v$ . But  $F_v$  commutes with  $E$  in  $\text{End}(\tilde{A}_v)_0$  and the commuting algebra of  $E$  in  $\text{End}(\tilde{A}_v)_0$  is  $E$  itself (cf. [34]). Hence  $F_v$  belongs to  $E^\times = T_E(\mathbb{Q})$  and this implies (a). II-28

Theorem 2 and part (b) of Theorem 1 are less easy; they are proved, in a somewhat different form in 34 [34] (see also [32]). Note that one could express them (as in 2.6) by saying that *there exists a homomorphism  $f: I \rightarrow E^\times$  (where  $I$  denotes, as usual, the group of idèles of  $K$ ) having the following properties:*

- 1)  $f$  is trivial on  $U_{\mathfrak{m}}$ , for some modulus  $\mathfrak{m}$  with support  $S$ .
- 2) If  $v \notin S$ , the image by  $f$  of a uniformizing parameter at  $v$  is the Frobenius element  $F_v \in E^\times$ .
- 3) If  $x \in K^\times$  is a principal idèle, one has  $f(x) = \det_E j(x)$ .

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

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

Let  $\ell$  be a prime integer distinct from any of the  $p_v$ ,  $v \in S$ . One then sees that the Galois-module  $V_\ell$  is of Hodge-Tate type in the sense of Chapter III, 1.2 (indeed, the corresponding local modules are associated with  $\ell$ -divisible II-29 groups, and one may apply Tate’s theorem [39]). Hence  $\rho_\ell$  is “locally algebraic” (Chapter III, *loc. cit.*), and using the theorem of Chapter III, 2.3 one sees it defines a morphism  $\varphi: S_{\mathfrak{m}} \rightarrow T_E$ . One has  $\varphi \circ \varepsilon_\ell = \rho_\ell$  by construction; the same is true for any prime number  $\ell'$ , 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  $V_\ell$ , as given by 39 [39], combined with the results of the Appendix to Chapter III.

### §3. Structure of $T_m$ and applications

#### 3.1 Structure of $X(T_m)$

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  $w$  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  $G = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ; let  $C_\infty$  denote their conjugacy class. (By a theorem of Artin [1], the elements of  $C_\infty$  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

$$\begin{aligned} \chi &= a \sum_{\sigma \in \Gamma} [\sigma] + \sum_{\sigma \in \Gamma} b_\sigma [\sigma] \\ a, b_\sigma &\in \mathbb{Q}, \sum_{\sigma} b_\sigma = 0, a + b_\sigma \in \mathbb{Z}. \end{aligned} \tag{*}$$

(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  $\mathbb{T} \rightarrow T_m$  defines an injection of  $X(T_m)$  into  $X(\mathbb{T})$ ; we identify  $X(T_m)$  with its image under this injection.

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

This follows from Appendix, A.2.

II-31

**Corollary 1.1.** *The character group  $X(T_m)$  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 $j^*: \mathbb{G}_m \rightarrow T_m$

We have seen that any character  $\chi \in X(T_m)$  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  $j: X(T_m) \rightarrow X(\mathbb{G}_m) = \mathbb{Z}$  and we obtain by duality a morphism of algebraic groups  $j^*: \mathbb{G}_m \rightarrow T_m$ . If  $\phi_0: S_m \rightarrow \mathrm{GL}_{V_0}$  is a representation of  $S_m$ , we obtain by composition with  $j^*$  a morphism of algebraic groups  $\mathbb{G}_m \rightarrow \mathrm{GL}_{V_0}$ . 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  $\ell$ -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  $N: S_m \rightarrow \mathbb{G}_m$  be the morphism defined in Exercise 2) of 2.5. Show that  $N \circ j: \mathbb{G}_m \rightarrow S_m \rightarrow \mathbb{G}_m$  is  $\lambda \mapsto \lambda^2$ . Show that any morphism  $S_m \rightarrow \mathbb{G}_m$  is equal to  $\varepsilon N^n$ , where  $\varepsilon$  is a character of  $C_m$  with values in  $\{\pm 1\}$  and  $n \in \mathbb{Z}$ .

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

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

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

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  $\mathbf{N}: S_{\mathfrak{m}} \rightarrow \mathbb{G}_m$ . 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  $C_{\infty}$  (cf. II-33 3.1). There is a unique continuous homomorphism  $\varepsilon: H_c \rightarrow \{\pm 1\}$  such that  $\varepsilon(c) = -1$  for all  $c \in C_{\infty}$ . Indeed the unicity of  $\varepsilon$  is clear, and one proves its existence by taking the restriction to  $H_c$  of the homomorphism  $G \rightarrow \{\pm 1\}$  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  $C_{\infty}$  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

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

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

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

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

**Proposition 1.** *The norm map defines an isomorphism of the space  $Y_{K_1}^0$  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  $\chi_1$ , by the norm map is II-34

$$N_{K_1/K_0}^*(\chi_1) = \sum_{\sigma} b_{\sigma/K_1}[\sigma], \quad \sigma \in \Gamma_K,$$

where  $\sigma/K_1$  is the restriction of  $\sigma$  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  $b_{\sigma}$  depends only on the restriction of  $\sigma$  to  $K_1$ , and hence that  $\chi$  belongs to the image of the norm map.

**Corollary 1.1.** *The tori  $T_m$  attached to  $K$  and  $K_1$  are isogenous to each other.*

There remains to describe the tori  $T_m$  attached to  $K_1$ . There are two cases:

- (1)  $K_1 = K_0$ . In this case, we have  $Y^- = 0$  and  $T_m$  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  $\sigma$ , 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  $T_m$  is  $(d+1)$ -dimensional.

More precisely, the space  $Y$  attached to  $K_1$  is  $2d$ -dimensional and the involution  $\sigma$  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  $\sigma$ . This is proved by the same argument as above, once one remarks that all  $c \in C_{\infty}$  induce  $\sigma$  on  $K_1$ . II-35

**Remark.** In this last case (which is the most interesting one), the torus  $T_m$  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

Let  $\phi$  be a linear representation of  $S_{\mathfrak{m}}$  of degree  $n$ . By extending the groundfield, the restriction of  $\phi$  to  $T_{\mathfrak{m}}$  can be put in diagonal form; let  $\chi_1, \dots, \chi_n$  be the  $n$  characteres of  $T_{\mathfrak{m}}$  so obtained and write (in additive notation)

$$\chi_i = \sum_{\sigma \in \Gamma} n_{\sigma}(i)[\sigma], \quad (n_{\sigma}(i) \in \mathbb{Z}).$$

We say that  $\chi_i$  is **positive** if all the  $n_{\sigma}(i)$ 's are  $\geq 0$ . Let  $v \in \text{Supp}(\mathfrak{m})$ , and let  $F_v \in S_{\mathfrak{m}}(\mathbb{Q})$  be the corresponding Frobenius element, cf. 2.3. Since  $C_{\mathfrak{m}} = S_{\mathfrak{m}}/T_{\mathfrak{m}}$  is finite, there exists an integer  $N \geq 1$  such that  $F_v \in T_{\mathfrak{m}}(\mathbb{Q})$ . If  $\mathfrak{p}_v$  is the prime ideal of  $v$ , this means that there exist  $\alpha \in K^{\times}$ , with  $\mathfrak{p}_v^N = (\alpha)$ ,  
II-36  $\alpha \equiv 1 \pmod{\mathfrak{m}}$ , and  $\alpha > 0$  at all real places of  $K$ .

**Proposition 1.** *The eigenvalues of  $\phi(F_v^N)$  are the numbers*

$$\chi_i(\alpha) = \prod_{\sigma} \sigma(\alpha)^{n_{\sigma}(i)}, \quad (i = 1, \dots, n).$$

*This is trivial by construction, because  $F_v^N$  is the image of  $\alpha$  under  $\mathbb{T}(\mathbb{Q}) \rightarrow T_{\mathfrak{m}}(\mathbb{Q})$ .*

**Corollary 1.1.** *The eigenvalues of  $\phi(F_v)$  are  $\{p_v\}$ -units (i.e. they are units at all places of  $\overline{\mathbb{Q}}$  not dividing  $p_v$ ).*

**Corollary 1.2.** *Let  $z_1, \dots, z_n$  be the eigenvalues of  $\phi(F_v)$ , indexed so that  $z_i^N = \chi_i(\alpha)$ . Let  $w$  be a place of  $\overline{\mathbb{Q}}$  dividing  $p_v$ , normalized so that  $w(p_v) = v(p_v) = e_v$ . Then  $w(z_i) = \sum_{\substack{\sigma \in \Gamma \\ w \circ \sigma}} n_{\sigma}(i)$ .*

We have  $w(z_i^N) = w(\prod_{\sigma \in \Gamma} (\sigma(\alpha)^{n_{\sigma}(i)})) = \sum_{\sigma \in \Gamma} n_{\sigma}(i) w \circ \sigma(\alpha)$ , and

$$\begin{aligned} w \circ \sigma(\alpha) &= 0 & \text{if } w \circ \sigma \neq v, \\ w \circ \sigma(\alpha) &= N & \text{if } w \circ \sigma = v, \end{aligned}$$

since  $(\alpha) = \mathfrak{p}_v^N$ .

Hence the result.

**Corollary 1.3.** *Let  $\ell$  be a prime number and let  $\phi_{\ell}: \text{Gal}(\overline{K}/K) \rightarrow \text{Aut}(V_{\ell})$  be the  $\ell$ -adic representation of  $K$  associated to  $\phi$ . Then  $\phi_{\ell}$  is integral (cf. Ch. I, 2.2) if and only if all the characteres  $\chi_i$  occuring in  $\phi$  are positive.*



II-37 *Proof of Corollary 3.* Assume first the  $\chi_i$ 's are positive. Let  $v \notin \text{Supp}(\mathfrak{m})$  and let  $z_1, \dots, z_n$  be the corresponding eigenvalues of  $F_v$  as in Corollary 1.2. Corollaries 1.1 and 1.2 show that the  $w(z_i)$  are positive for all valuations  $w$  of  $\overline{\mathbb{Q}}$ ; hence the  $z_i$  are integral over  $\mathbb{Z}$ . Hence the  $\phi_\ell$ 's are integral.

Conversely, assume  $\phi_\ell$  is integral for some  $\ell$ . There exists a finite subset  $S'$  of  $M_K^0$ , containing  $\text{Supp}(\mathfrak{m})$ , such that if  $v \notin S'$ , the eigenvalues of  $\phi(F_v)$  are integral. Choose a prime number  $p$  which splits completely in  $K$  and is such that  $p_v = p$  implies  $v \notin S'$ . Let  $w$  be a valuation of  $\overline{\mathbb{Q}}$  dividing  $p$ . The valuations  $w \circ \sigma$ ,  $\sigma \in \Gamma$ , are pairwise inequivalent. Let  $\sigma \in \Gamma$ ; and let  $v$  be the normalized valuation of  $K$  equivalent to  $w \circ \sigma$  so that  $\lambda v = w \circ \sigma$  for some  $\lambda > 0$ . Let  $z_1, \dots, z_n$  be the eigenvalues of  $\phi(F_v)$ . By Corollary 1.2,  $w(z_i) = \lambda n_\sigma(i)$ . Since the  $z_i$  are integral, this shows that the  $n_\sigma(i)$ 's are all positive.  $\square$

**Proposition 2.** *Let  $v \notin \text{Supp}(\mathfrak{m})$  and let  $\chi$  be a character of  $S_{\mathfrak{m}}$ . Let  $\chi_{\mathbb{T}} \in X(T_{\mathfrak{m}})$  be the restriction of  $\chi$  to  $T_{\mathfrak{m}}$  and let  $i = j(\chi_{\mathbb{T}})$  be the integer defined in ???. Then, for any archimedian absolute value  $\omega$  of  $\overline{\mathbb{Q}}$  extending the usual absolute value of  $\overline{\mathbb{Q}}$ , we have*

$$\omega(\chi(F_v)) = (\mathbf{N}_v)^{i/2}.$$

*Proof.* Si  $\chi = a \sum_{\sigma \in \Gamma} [\sigma] + \sum_{\sigma \in \Gamma} b_\sigma [\sigma]$  as in 3.1, we have

$$\omega(\chi(F_v))^N = \omega(\chi(F_v^N)) = \prod_{\sigma} \omega \circ \sigma(\alpha)^a \cdot \prod_{\sigma} \omega \circ \sigma(\alpha)^{b_\sigma},$$

and  $\prod_{\sigma} \omega \circ \sigma(\alpha)^a = \omega(\mathbf{N}(\alpha))^a = \mathbf{N} v^{iN/2}$ , where  $i = 2a$ . It remains to show that  $\chi = \prod_{\sigma} \omega \circ \sigma(\alpha)^{b_\sigma}$  is equal to 1. Let  $c = c_\omega$  be the “Frobenius” attached to  $\omega$  (cf. ??). Since  $b_\sigma + b_{c\sigma} = 0$ , we have  $x \cdot y = 1$  with  $y = \prod_{\sigma} \omega \circ \sigma(\alpha)^{b_{c\sigma}}$ . But  $y = \prod_{\tau} \omega \circ c \circ \tau(\alpha)^{b_\tau}$ , and, since  $\omega \circ c = \omega$ , we have  $y = x$ , hence  $x^2 = 1$ , and  $x = 1$ , since  $x > 0$ .  $\square$

II-38

### Exercises.

- 1) Check the product formula for the eigenvalue of the  $\phi(F_v)$ . (Use Cor. 1.1 and 1.2 to Prop. 1 and Prop. 2).
- 2) Show that Prop. 2 and Cor.1.1 and 1.2 to Prop. 1 determine the eigenvalues of the  $\phi(F_v)$ 's up to multiplication by roots of unity.

- 3) (Generalization of Cor. 1.1 to Prop. 1). Let  $(\rho_\ell)$  be a strictly compatible system of rational  $\ell$ -adic representations, with exceptional set  $S$  (cf. Chap. I, 2.3). Show that, for any  $v \in M_K^0 - S$ , the eigenvalues of  $F_{v, \rho_\ell}$ ,  $\ell \neq p_v$ , are  $p_v$ -units.

## §A. Killing arithmetic groups in tori

### A.1 Arithmetic groups in tori

Let  $A$  be a linear algebraic group over  $\mathbb{Q}$ , and let  $\Gamma$  be a subgroup of the group  $A(\mathbb{Q})$  of rational points of  $A$ . Then  $\Gamma$  is said to be an **arithmetic subgroup** if for any algebraic embedding  $A \subseteq \mathrm{GL}_n$  ( $n$  arbitrary) the groups  $\Gamma$  and  $A(\mathbb{Q}) \cap \mathrm{GL}_n(\mathbb{Z})$  are **commensurable** (two subgroups  $\Gamma_1, \Gamma_2$  are said to be commensurable if  $\Gamma_1 \cap \Gamma_2$  is of finite index in  $\Gamma_1$  and  $\Gamma_2$ ). It is well-known that it suffices to check that  $\Gamma$  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  $\Gamma$  be an arithmetic subgroup of  $\mathbb{T}$ . Then  $\Gamma \cap \mathbb{T}^0$  is of finite index in  $\Gamma$ , 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 18 [18].

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

II-40

**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

$$\Gamma = \text{Hom}_{\text{Gal}}(X, U)$$

Show that  $\Gamma$  is an arithmetic subgroup of  $\mathbb{T}(\mathbb{Q})$  and that any arithmetic subgroup of  $\mathbb{T}(\mathbb{Q})$  is contained in  $\Gamma$ .

## 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  $\Lambda$  be the set of classes of  $\mathbb{Q}$ -irreducible representations of  $G = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  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  $\lambda$ . 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  $Y_\lambda$ . We have II-41

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

Note that  $Y = Y^0$  if and only if  $\mathbb{T}$  is anisotropic. If  $c \in C_\infty$ , and  $H = \{1, c\}$ , then, since  $\mathbb{T}(\mathbb{R}) = \text{Hom}_H(X(\mathbb{T}), \mathbb{C}^\times)$ , we see that  $\mathbb{T}(\mathbb{R})$  is compact if and only if  $Y = Y^-$ .

**Proposition 1.** *Let  $\Gamma$  be an arithmetic subgroup of the torus  $\mathbb{T}$ , and  $\overline{\Gamma}$  its Zariski closure (cf. 1.2). Then:*

$$Y(\mathbb{T}/\overline{\Gamma}) = Y^0 \oplus Y^-. \quad (*)$$

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

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

II-42 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  $\Gamma$  is commensurable with the image by  $\mathbb{T}' \rightarrow \mathbb{T}$  of an arithmetic subgroup of  $\mathbb{T}$ .  $\square$

**Exercise.** Let  $y \in Y$ . Define  $Ny$  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  $\text{Ker}(N) = Y^- \oplus Y^+$ .
- b. Prove that  $Y$  is generated by the elements  $cy + y$ , with  $y \in \text{Ker}(N)$  and  $c \in C_\infty$ .

# CHAPTER III

## LOCALLY ALGEBRAIC ABELIAN REPRESENTATIONS

In this Chapter, we define what it means for an abelian  $\ell$ -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  $S_m$  of Chapter II.

When the ground field is a composite of quadratic extensions of  $\mathbb{Q}$ , any rational semi-simple  $\ell$ -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. 43 [43], III-1 Chap. I).

Let  $V$  be a finite dimensional  $\mathbb{Q}_p$ -vector space and denote, as usual, by  $\mathrm{GL}_V$  the corresponding linear group; it is an algebraic group over  $\mathbb{Q}_{p'}$  and  $\mathrm{GL}_V(\mathbb{Q}_p) = \mathrm{Aut}(V)$ .

Let  $\rho: \mathrm{Gal}(\bar{K}/K) \rightarrow \mathrm{Aut}(V)$  be an abelian  $p$ -adic representation of  $K$

in  $V$ , where  $\text{Gal}(\overline{K}/K)$  denotes the Galois group of the maximal abelian extension of  $K$ . If  $i: K^\times \rightarrow \text{Gal}(\overline{K}/K)$  is the canonical homomorphism of local class field theory (cf. for instance Cassels - Frohlich [6], chap. VI, §2), we then get a continuous homomorphism  $\rho \circ i$  of  $K^\times = \mathbb{T}(\mathbb{Q}_p)$  into  $\text{Aut}(V)$ .

**Definition 1.** The representation  $\rho$  is said to be **locally algebraic** if there is an algebraic morphism  $r: \mathbb{T} \rightarrow \text{GL}_V$  such that  $\rho \circ i(x) = r(x^{-1})$  for all  $x \in K^\times$  close enough to 1.

Note that if  $r: \mathbb{T} \rightarrow \text{GL}_V$  satisfies the above condition, it is unique; this follows from the fact that any non-empty open set of  $K^\times = \mathbb{T}(\mathbb{Q}_p)$  is Zariski dense in  $\mathbb{T}$ . We say that  $r$  is the algebraic morphism *associated with*  $\rho$ .

### 1. Examples.

- 1) Take  $K = \mathbb{Q}_p$ , and  $\dim V = 1$ , so that  $\rho$  is given by a continuous homomorphism  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow U_p$ , where  $U_p$  is the group of  $p$ -adic units. It is easy to see there exists an element  $v \in \mathbb{Z}_p$  such that  $\rho \circ i(x) = x^v$  if  $x$  is close enough to 1. The representation  $\rho$  is locally algebraic if and only if  $v$  belongs to  $\mathbb{Z}$ . This happens for instance when  $V = V_p(\mu)$ , cf. Chap. I, 1.2, in which case  $v = -1$  and  $r$  is the canonical one-dimensional representation of  $\mathbb{T} = \mathbb{G}_{m, \mathbb{Q}_p}$ .
- 2) The abelian representation associated to a Lubin-Tate formal group (cf. ?? and ??, Chap. VI, §3) is locally algebraic (and also of the form  $u \mapsto u^{-1}$  on the inertia group).

**Proposition 1.** *Let  $\rho: \text{Gal}(\overline{K}/K) \rightarrow \text{Aut}(V)$  be a locally algebraic abelian representation of  $K$ . The restriction of  $\rho$  to the inertia subgroup of  $\text{Gal}(\overline{K}/K)$  is semi-simple.*

*Proof.* Let us identify the inertia subgroup of  $\text{Gal}(\overline{K}/K)$  with the group  $U_K$  of units of  $K$ . By assumption, there is an open subgroup  $U'$  of  $U_K$  and an algebraic morphism  $r$  of  $\mathbb{T}$  into  $\text{GL}_V$  such that  $\rho(x) = r(x^{-1})$  if  $x \in U'$ . Let  $W$  be a sub-vector space of  $V$  stable by  $\rho(U_K)$ ; it is then stable by  $\rho(U')$ , hence by  $r(T)$ . But every linear representation of a torus is semi-simple. Hence, there exists a projector  $\pi: V \rightarrow W$  which commutes with the action of  $\mathbb{T}$ . If we put  $\pi' = \frac{1}{(U_K:U')}$

$\sum_{s \in U_K - U'} \rho(s) \pi \rho(s^{-1})$ , we obtain a projector  $\pi': V \rightarrow W$  which commutes with all  $\rho(s)$ ,  $s \in U_K$ , q.e.d.  $\square$

Belén ♥: aquí  
termina la  
demostración??

Conversely, let us start from a representation  $\rho$  whose restriction to  $U_K$  is semi-simple. If we make a suitable large finite extension  $E$  of  $\mathbb{Q}_p$ , the restriction of  $\rho$  to  $U_K$  may be brought into diagonal form, i.e. is given by continuous characters  $\chi_i: U_K \rightarrow E^\times$ ,  $i = 1, \dots, n$ . We assume  $E$  large enough to contain all conjugates of  $K$  into  $E$ . Recall (cf. Chap. ??, 1.1) that the  $[\sigma]$ ,  $\sigma \in \Gamma_K$ , make a basis of the character group  $X(\mathbb{T})$  of  $T$ .

**Proposition 2.** *The representation  $\rho$  is locally algebraic if and only if there exists integer  $n_\sigma(i)$  such that*

$$\chi_i(u) = \prod_{\sigma \in \Gamma_K} \sigma(u)^{-n_\sigma(i)}$$

for all  $i$  and all  $u$  close enough to 1.

*Proof.* The necessity is trivial. Conversely, if there exist such integers  $n_\sigma(i)$ , they define algebraic characters  $r_i = \prod [\sigma]^{n_\sigma(i)}$  of  $\mathbb{T}$ , hence a linear representation  $r$  of  $T/E$ . It is clear that there is an open subgroup  $U'$  of  $U_K$ , such that  $\rho(u) = r(u^{-1})$  for all  $u \in U'$ . Hence it remains to see that  $r$  can be defined over  $\mathbb{Q}_p$  (cf. Chap. II, 2.4). But the trace  $\theta_r = \sum r_i$  of  $r$  (loc. cit. is such that  $\theta_r(u) \in \mathbb{Q}_p$  for all  $u \in U'$ . Since  $U'$  is Zariski-dense in  $\mathbb{T}$ , this implies that  $\theta_r$  is "defined over  $\mathbb{Q}_p$ ", hence that  $r$  can be defined over  $\mathbb{Q}_p$  (loc. cit.).  $\square$

**2. Extension of the ground field.** Let  $K'$  be a finite extension of  $K$ , and let  $\rho'$  be the restriction of the given representation  $\rho$  to  $\text{Gal}(\bar{K}/K')$ . Then  $\rho'$  is locally algebraic if and only  $\rho$  is; moreover, if this is so, the associated algebraic morphisms

Belén ♥: falta  
un if?

$$r: \mathbb{T} \rightarrow \text{GL}_V, \quad r': \mathbb{T}' \rightarrow \text{GL}_V$$

are such that  $r' = N_{K'/K} \circ r$ , where  $\mathbb{T}'$  is the torus associated with  $K'$  and  $N_{K'/K}: \mathbb{T}' \rightarrow \mathbb{T}$  is the algebraic morphism defined by the norm from  $K'$  to  $K$ .

All this follows easily from the commutativity of the diagram

$$\begin{array}{ccc} K^\times & \longrightarrow & \text{Gal}(\bar{K}/K) \\ \uparrow N & & \uparrow \\ K' & \longrightarrow & \text{Gal}(\bar{K}/K') \end{array}$$

and from the fact that the kernel of  $N_{K'/K}: \mathbb{T}' \rightarrow \mathbb{T}$  is connected for the Zariski topology.

Belén.

## 1.2 Alternative definition of “locally algebraic” via Hodge-Tate modules

Let us recall first the notion of a **Hodge-Tate module** (cf. [27], §2); here  $K$  is only assumed to be complete with respect to a discrete valuation, with perfect residue field  $k$  and  $\text{char}(K) = 0$ ,  $\text{char}(k) = p$ . Denote by  $C$  the completion  $\widehat{\overline{K}}$  of the algebraic closure of  $K$ .

The group  $G = \text{Gal}(\overline{K}/K)$  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

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

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

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

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  $W^i \rightarrow W$  extends uniquely to a  $C$ -linear map  $\alpha_i: W(i) \rightarrow W$ , 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  $\alpha: \coprod_i W(i) \rightarrow W$  be the sum of the  $\alpha_i$ 's defined above. Then  $\alpha$  is injective.*

For the proof see [27], §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  $\alpha: \coprod_{i \in \mathbb{Z}} W(i) \rightarrow W$  is an isomorphism.



Let now  $V$  be as in 1, a vector space over  $\mathbb{Q}_p$ , of finite dimension. Let  $\rho: G \rightarrow \text{Aut}(V)$  be a  $p$ -adic representation. Let  $W = C \otimes_{\mathbb{Q}_p} V$  and let  $G$  act on  $W$  by the formula

III-3

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

**Definition 2.** The representation  $\rho$  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. [26], [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  $\rho: G \rightarrow \text{Aut}(V)$  be an abelian  $p$ -adic representation of  $K$ . The following properties are equivalent:*

- (a)  $\rho$  is locally algebraic (cf. 1).
- (b)  $\rho$  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

We now go back to the notations of Chap. II, i.e.  $K$  denotes a number field. Let  $\ell$  be a prime number and let

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

be an abelian  $\ell$ -adic representation of  $K$ . Let  $v \in M_K^0$  be a place of  $K$  of residue characteristic  $\ell$  and let  $D_v \subset \text{Gal}(\overline{K}/K)$  be the corresponding decomposition group. This group is a quotient of the local Galois group  $\text{Gal}(\overline{K}_v/K_v)^{\text{ab}}$  (these two groups are, in fact, isomorphic, but we do not need this here). Hence, we get by composition an  $\ell$ -adic representation of  $K_v$

$$\rho_v: \text{Gal}(\overline{K}_v/K_v)^{\text{ab}} \longrightarrow D_v \xrightarrow{\rho} \text{Aut}(V_\ell).$$

**Definition 1.** The representation  $\rho$  is said to be **locally algebraic** if all the local representations  $\rho_v$ , with  $p_v = \ell$ , are locally algebraic (in the sense defined in 1, with  $p = \ell$ ).

It is convenient to reformulate this definition, using the torus  $T = \mathfrak{R}_{K/\mathbb{Q}}(\mathbb{G}_{m,K})$  of Chap. II, 1.1. Let  $\mathbb{T}_{/\mathbb{Q}_\ell} = \mathbb{T} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$  be the  $\mathbb{Q}_\ell$ -torus obtained from  $\mathbb{T}$  by extending the ground field from  $\mathbb{Q}$  to  $\mathbb{Q}_\ell$ . We have

$$\mathbb{T}_{/\mathbb{Q}_\ell}(\mathbb{Q}_\ell) = (K \otimes \mathbb{Q}_\ell)^\times = K_\ell^\times,$$

where  $K_\ell = K \otimes \mathbb{Q}_\ell$ .

Let  $I$  be the idèle group of  $K$ , cf. Chap. II, 2.1. The injection  $K_\ell^\times \rightarrow I$ , followed by the class field homomorphism  $i: I \rightarrow \text{Gal}(\overline{K}/K)^{\text{ab}}$ , define a homomorphism

$$i_\ell: K_\ell^\times \longrightarrow \text{Gal}(\overline{K}/K)^{\text{ab}}.$$

**Proposition 1.** *The proposition  $\rho$  is locally algebraic if and only if there exists an algebraic morphism*

$$f: \mathbb{T}_{/\mathbb{Q}_\ell} \longrightarrow \text{GL}_{V_\ell}$$

*such that  $\rho \circ i_\ell(x) = f(x^{-1})$  for all  $x \in K_\ell^\times$  close enough to 1.*

(Note that, as in the local case, the above condition determines  $f$  uniquely; one says it is the algebraic morphism associated with  $\rho$ .)

Since  $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell = \prod_{v|\ell} K_v$ , we have

$$\mathbb{T}_{/\mathbb{Q}_\ell} = \prod_{v|\ell} T_v,$$

where  $T_v$  is the  $\mathbb{Q}_\ell$ -torus defined by  $K_v$ , cf. ???. The proposition follow from this decomposition.

**Exercise.** Give a criterion for local algebraicity analogous to the one of Prop. ??? of 1.

## 2.2 Modulus of a locally algebraic abelian representation

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

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

**Definition 1.** Let  $\mathfrak{m}$  be a modulus (chap. II, 1.1). One says that  $\rho$  is defined mod  $\mathfrak{m}$  (or that  $\mathfrak{m}$  is a modulus of definition for  $\rho$ ) 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  $x \in \prod U_{v,\mathfrak{m}}$ .

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

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  $\mathbb{Q}_\ell$  (resp.  $\mathbb{R}$ ) and let  $\alpha$  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  $\alpha$  to  $K$  is equal to 1 on an open subgroup of  $K_v^\times$ .*

(b) *The restriction of  $\alpha$  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  $\ell$ -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  $\ell$ -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  $p_v \neq \ell$ , the group  $\alpha(U_v)$  is finite; hence  $\alpha(U_v) = \{1\}$  for almost all  $v$ 's. □ III-5

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

This follows from (b) applied to the homomorphism  $\alpha$  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  $\ell$ -adic representation has a modulus of definition.*

Let  $\rho: \text{Gal}(\overline{K}/K)^{\text{ab}} \rightarrow \text{Aut}(V_\ell)$  be the given representation and  $f$  the associated morphism of  $T_{/\mathbb{Q}_\ell}$  into  $\text{GL}_{V_\ell}$ . Let  $X$  be the set of places  $v \in M_K^0$ , with  $p_v \neq \ell$ , for which  $\rho$  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  $\rho \circ i: I \rightarrow \text{Aut}(V_\ell)$  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  $\rho$ .

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

III-6 **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  $\ell^n$ -th roots of the element  $z_1 z_2^\ell \cdots z_n^{\ell^{n-1}}$ .

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

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

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

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

be the corresponding  $\ell$ -adic representation (cf. chap. II, 2.5).

**Theorem 1.** *The representation  $\phi_\ell$  is locally algebraic and defined mod  $\mathfrak{m}$ .*

III-7 *The associated algebraic morphism*

$$f: \mathbb{T}_{/\mathbb{Q}_\ell} \longrightarrow \text{GL}_{V_\ell}$$

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

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

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

**Theorem 2.** *Let  $\rho: \text{Gal}(\overline{K}/K)^{\text{ab}} \rightarrow \text{Aut}(V_\ell)$  be an abelian  $\ell$ -adic representation of the number field  $K$ . Assume  $\rho$  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  $V_\ell$ , with  $V_\ell = V_0 \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ , and a morphism  $\phi_0: S_{\mathfrak{m}} \rightarrow \text{GL}_{V_\ell}$  of  $\mathbb{Q}$ -algebraic groups such that  $\rho$  is equal to the  $\ell$ -adic representation  $\phi_\ell$  associated to  $\phi_0$  (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  $V_\ell$ , cf. Bourbaki Alg., chap. II, 3<sup>rd</sup> ed.)

*Proof.* Let  $r: \mathbb{T}_{/\mathbb{Q}_\ell} \rightarrow \text{GL}_{V_\ell}$  be the algebraic morphism associated with  $\rho$ . We have

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

Define a map  $\psi: I \rightarrow \text{Aut}(V_\ell)$  by

III-8

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

where  $x_\ell$  is the  $\ell^{\text{th}}$  component of the idèle  $x$ . One checks immediately that  $\psi$  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  $r_{\mathfrak{m}}: T_{\mathfrak{m}/\mathbb{Q}_\ell} \rightarrow \text{GL}_{V_\ell}$ . 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

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

with the following properties:

- (a) The morphism  $T_{\mathfrak{m}/\mathbb{Q}_\ell} \longrightarrow S_{\mathfrak{m}/\mathbb{Q}_\ell} \xrightarrow{\phi} \text{GL}_{V_\ell}$  is  $r_{\mathfrak{m}}$ .
- (b) The map  $I \xrightarrow{\varepsilon} S_{\mathfrak{m}}(\mathbb{Q}_\ell) \xrightarrow{\phi} \text{Aut}(V_\ell)$  is  $\psi$ .

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

$$\phi_\ell \circ i(a) = \phi(\varepsilon_\ell(a)) = \phi(\varepsilon(a))\phi(\pi_\ell(a_\ell^{-1})) = \psi(a)\phi(\pi_\ell(a_\ell^{-1}))$$

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

$$= \rho \circ i(a)r(a_\ell)\phi(\pi_\ell(a_\ell^{-1})) = \rho \circ i(a).$$

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

III-9

Hence  $\phi_\ell = \rho$ ; the fact that  $\rho$  is *rational* then implies that  $\phi$  can be defined over  $\mathbb{Q}$  (chap. II, 2.4, Prop.), and this gives  $V_0$  and  $\phi_0$ .  $\square$

**Remark.** The subspace  $V_0$  of  $V_\ell$  constructed in the proof of the theorem is *not* unique; however, any other choice gives us a space of the form  $\sigma V_0$ , where  $\sigma$  is an automorphism of  $V_\ell$  commuting with  $\rho$ . To a given  $V_0$  corresponds of course a unique  $\phi$ .

**Corollary 2.1.** *For each prime number  $\ell'$  there exists a unique (up to isomorphism)  $\ell'$ -adic rational semi-simple representation  $\rho$  of  $K$ , compatible with  $\rho$ . It is abelian and locally algebraic. These representations form a strictly compatible system (cf. chap. I, 2.3) with exceptional set contained in  $\text{Supp}(\mathfrak{m})$ . For an infinite number of  $\ell'$ ,  $\rho_{\ell'}$  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  $\phi$  as in chapter II, 2.5. The remaining assertion follows from the proposition in chap. II, 2.5.  $\square$

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

This follows from the corresponding property of  $\phi_\ell$ , 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

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

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

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

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  $\Gamma$  with respect to the topology of subgroups of finite index, it is known (class field theory) that  $\text{Gal}(\overline{K}/K)^{\text{ab}} \cong \varprojlim_{\mathfrak{m}} \widehat{\Gamma}_{\mathfrak{m}}$ .

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

**Proposition 1.** *A homomorphism  $\phi: \Gamma_{\mathfrak{m}} \rightarrow \text{Aut}(V_{\ell})$  can be extended to a continuous homomorphism of  $\widehat{\Gamma}_{\mathfrak{m}}$  if and only if there exists a lattice of  $V_{\ell}$  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  $\ell$ -adic representation.

**Theorem 1.** *An abelian  $\ell$ -adic representation*

$$\phi: \widehat{\Gamma}_{\mathfrak{m}} \rightarrow \text{Aut}(V_{\ell})$$

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

III-11

If  $v \notin \text{Supp}(\mathfrak{m})$ , 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  $\text{Tr } \phi$  takes rational values on  $\Gamma_{\mathfrak{m}}$ , the characteristic polynomial of  $\phi(F_v)$  has rational coefficients for all  $v \notin \text{Supp}(\mathfrak{m})$  and  $\phi$  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  $\text{Tr } \rho(\gamma)$  belongs to some number field  $E$ . We can then construct an  $E$ -linear representation  $\phi: \Gamma_{\mathfrak{m}} \rightarrow \text{GL}(n, E)$  with the same trace as  $\rho$ , and the theorem follows from:

**Lemma 1.** *Let  $\Gamma$  be a finitely generated abelian group, and  $\phi: \Gamma \rightarrow \mathrm{GL}(n, E)$  a linear representation of  $\Gamma$  over a number field  $E$ . Let  $\Sigma$  be a subset of  $\Gamma$ , which is dense in  $\Gamma$  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  $\ell'$  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  $\phi$  extends by  
 III-12 continuity to

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

where  $\widehat{\Gamma}$  is the completion of  $\Gamma$  for the topology of subgroups of finite index. Since  $\Sigma$  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

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

### Exercises.

- 1) Let  $\phi: \widehat{\Gamma}_{\mathfrak{m}} \rightarrow \mathrm{Aut}(V_{\ell})$  be a semi-simple  $\ell$ -adic representation of  $\Gamma_{\mathfrak{m}}$ . Show the equivalence of:
  - (a)  $\phi$  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  $\phi: \widehat{\Gamma}_{\mathfrak{m}} \rightarrow \mathrm{Aut}(V_{\ell})$  be a rational  $\ell$ -adic representation of  $K$ . Show that, for almost all prime number  $\ell'$ , there is a rational  $\ell'$ -adic representation of  $K$  compatible with  $\phi$ . 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  $\rho: \text{Gal}(\overline{K}/K)^{\text{ab}} \rightarrow \text{Aut}(V_\ell)$  be a rational semi-simple  $\ell$ -adic abelian representation of  $K$ . Assume that there exists an integer  $N \geq 1$  such that  $\rho^N$  is locally algebraic. Then  $\rho$  is locally algebraic.*

*Proof.* Since  $\rho$  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  $\psi_i: C_K \rightarrow \overline{\mathbb{Q}_\ell}^\times$ , 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  $\rho^N$ . Since  $\rho^N$  is locally algebraic, to each  $\chi_i^N$  corresponds an algebraic character  $\chi_i^{\text{alg}} \in X(\mathbb{T})$  of the torus  $\mathbb{T}$  (here we identify  $X(\mathbb{T})$  with  $\text{Hom}(\mathbb{T}_{/\overline{\mathbb{Q}_\ell}}, \mathbb{G}_{m, \overline{\mathbb{Q}_\ell}})$ , since  $\overline{\mathbb{Q}_\ell}$  is algebraically closed). Each  $\chi_i^{\text{alg}}$  is of the form  $\prod_{\sigma \in \Gamma} [\sigma]^{n_{\sigma(i)}}$ , where  $\Gamma$  is the set of embeddings of  $K$  into  $\overline{\mathbb{Q}_\ell}$ , cf. Chap. II, 1.1. One has

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

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

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  $\text{Supp}(\mathfrak{m})$ , 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  $(\alpha)$ , with  $\alpha \equiv 1 \pmod{\mathfrak{m}}$  and  $\alpha$  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  $\psi_i$  and  $\chi_i$  relative to  $v$ . By definition of  $\chi_i^{\text{alg}}$ , we have

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

where  $\alpha$  is as above.

Hence  $y$  belongs to the subfield  $\tilde{L}$  of  $\mathbb{Q}$  corresponding to  $L$  (this field is well defined since  $L$  is a Galois extension of  $\mathbb{Q}$ ). Moreover, if  $w_{\sigma}$  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  $N^{\text{th}}$ -root of  $y$ , does not belong to  $\tilde{L}$ . Hence there is a non-trivial  $N^{\text{th}}$ -root of unity  $z$  such that  $x$  and  $zx$  are conjugate over  $\tilde{L}$ , and *a fortiori* over  $\mathbb{Q}$ . Since the characteristic polynomial of  $F_{v,\rho}$  has rational coefficients, any conjugate 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

$$\psi_j(f_v) = zx = z\psi_i(f_v).$$

But  $f_v \in K^{\times}U_{\mathfrak{m}}$  and all  $\psi_j$  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.  $\square$

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

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

if  $x$  is close enough to 1. Hence  $\varphi_i(x)\psi_i(x)$  is an  $N^{\text{th}}$ -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  $\rho$  to  $K_\ell^\times$  is locally equal to  $\varphi^{-1}$ , where  $\varphi$  is the (algebraic) representation of  $\mathbb{T}$  defined by the family  $(\varphi_1, \dots, \varphi_n)$ . The representation  $\varphi$ , *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  $(\varphi_1, \dots, \varphi_n)$  is *stable* under the action of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ , since the family  $(\chi_1^{\text{alg}}, \dots, \chi_n^{\text{alg}})$  is.

Hence  $\rho$  is locally algebraic.  $\square$

### 3.3 An auxiliary result on tori

In [15], 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  $\ell$ -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  $\Gamma$  be an additive subgroup of  $E$ . Assume:*

- 1)  $\Gamma$  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 [15], 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  $T_1 \times \dots \times T_n \rightarrow T$  is surjective (and hence has a finite kernel). An equivalent condition is:

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

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  $\ell$ -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  $f: T(\mathbb{Q}_\ell) \rightarrow E^\times$  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.*

- III-18 i) We suppose first that  $T$  is *one-dimensional*, and we denote by  $\chi$  a generator of  $X(T)$ . If  $\chi$  is invariant by  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ,  $T$  is isomorphic to  $\mathbb{G}_m$  and  $T(\mathbb{Q}) \cong \mathbb{Q}^\times$ . If not,  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  acts on  $X(T)$  via a group of order 2, corresponding to some quadratic extension  $F$  of  $\mathbb{Q}$ ; the character  $\chi$  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  $\leq 1$ . 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  $\ell$ -adic Lie group of dimension 1, it is locally isomorphic to the *additive group*  $\mathbb{Q}_\ell$ . This means that there exists a homomorphism

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

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

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

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

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

with absolute convergence of the exponential series.

Let now  $\Gamma$  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,  $\Gamma$  is of infinite rank. If  $z \in \Gamma$ ,  $e(z)$  belongs to  $T(\mathbb{Q})_W$ , hence  $f \circ e(z)$  III-19 is algebraic over  $\mathbb{Q}$ ; the same is true for  $\chi \circ e(z)$  since  $\chi$  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  $\chi$ , hence  $f$  is *almost locally algebraic*.

- ii) *General case.* Write  $T = T_1 \cdots T_n$  where  $T_1, \dots, T_n$  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).  $\rightarrow$  [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  $K$ .

III-20 Sections A.1 and A.2 give invariance properties of these decompositions under ground field extensions. Special characters of  $\text{Gal}(\bar{K}/K)$  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.

### A.1 Invariance of Hodge-Tate decompositions

Let  $C$  be the completion of  $\bar{K}$  (cf. 1.2); the group  $\text{Gal}(\bar{K}/K)$  acts continuously on  $C$ . Let  $\chi$  be the character of  $\text{Gal}(\bar{K}/K)$  into the group of  $p$ -adic units defined in chap. I, 1.2. Let  $K'/K$  be a subextension of  $\bar{K}/K$  on which the valuation  $\bar{v}$  of  $\bar{K}$  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  $\text{Gal}(\bar{K}/K)$  acts continuously and semi-linearly (see 1.2). As before, we denote by  $W^n$  (resp.  $W_{K'}^n$ ) the  $K$ - (resp.  $\widehat{K'}$ -) vector space defined by

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

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

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

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

Indeed, Theorem 1 shows that  $W^n$  and  $W_{K'}^n$ , 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  $\text{Gal}(\overline{K}/K)$  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.  $W_{K'}^n$ ) is the set of elements of  $W$  which are invariant under  $\text{Gal}(\overline{K}/K)$  (resp. under  $\text{Gal}(\overline{K}/K')$ ). Note also that the injectivity of  $\widehat{K'} \otimes W^0 \rightarrow W_{K'}^0$  is trivial, since we know that  $C \otimes_K W^0 \rightarrow W$  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  $\text{Gal}(\overline{K}/K')$  acts trivially on  $W_{K'}^0$ , we have a semi-linear action of  $\text{Gal}(K'/K)$  on  $W_{K'}^0$ . When  $K'/K$  is finite, it is well known that this implies that  $W_{K'}^0$  is generated by the elements invariant by  $\text{Gal}(K'/K)$ , i.e. by  $W^0$  (this is a non-commutative analogue of Hilbert's "Theorem 90", cf. for instance [29]).

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  $\Lambda$  be an  $\widehat{\mathcal{O}'}$ -lattice of  $W_{K'}^0$  (i.e. a free  $\widehat{\mathcal{O}'}$ -submodule of  $W_{K'}^0$ , of the same rank as  $W_{K'}^0$ ). Since  $G$  acts continuously on  $W_{K'}^0$ , the stabilizer in  $G$  of  $\Lambda$  is open, hence of finite index, and the lattice  $\Lambda$  has finitely many transforms. The sum  $\Lambda^0$  of these transforms is invariant III-22 by  $G$ . Let  $e_1, \dots, e_N$  be a basis of  $\Lambda^0$ . Let  $s \in G$ . Then

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

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

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

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  $e'_1, \dots, e'_N$  of  $W_{K'}^0$  by

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

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

III-23 *Proof of the lemma.* Let  $\pi$  be a uniformizing element of  $\widehat{\mathcal{O}'}$ . Filter the ring  $A = \mathrm{GL}(N, \widehat{\mathcal{O}'})$  by means of  $A_n = \{a \in A \mid a \equiv 1 \pmod{\pi^n}\}$ . We get  $A/A_1 \cong \mathrm{GL}(N, k'/k)$ , where  $k'/k$  is the residue field extension of  $K'/K$ . Moreover, for  $n \geq 1$ , there is an isomorphism  $A_n/A_{n+1} \cong M_N(k')$ , where  $M_N(k')$  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  $H^1(G, M_N(k'))$ , where now  $k'$  is endowed with the discrete topology (so this is ordinary Galois cohomology, cf. [29]).  $\square$

## A.2 Admissible characters

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

**Definition 1.** The character  $\varphi$  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  $\varphi, \varphi'$  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  $\varphi: G \rightarrow K^\times$  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  $\varphi \sim \varphi'$ .

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

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

Denote the  $C$ - $G$ -module thus obtained by  $C(\varphi)$ . Then  $\varphi$  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  $\varphi$  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.  $W_{K'}^0$ ) be the subspace of  $W$  consisting of elements invariant by  $G$  (resp. by  $N$ ). By hypothesis,  $W_{K'}^0$  is  $\neq 0$ . Hence, by A.1, Theorem 1, we also have  $W^0 \neq 0$ , and this means that  $\varphi$  is admissible.  $\square$

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. [29]. Define the logarithm map by

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

This is a continuous homomorphism and even a local isomorphism.

### A.3 A criterion for local triviality

Belén.

### A.4 The character $\xi$

Belén.

### A.5 Characters associated with Hodge-Tate decompositions

Belén.

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

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

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

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

## 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  $G^{\text{ab}}$  with  $\widehat{K}^\times$ , and the inertia subgroup of  $G^{\text{ab}}$  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  $E, \sigma E$ , where  $\sigma \in \Gamma_E$ ), cf. 1. The norm map from  $K$  to  $\sigma E$  defines an algebraic morphism

$$N_{K/\sigma E}: T \longrightarrow T_{\sigma E}.$$

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

$$r_\sigma = \sigma^{-1} \circ N_{K/\sigma E}: T \rightarrow T_E.$$

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

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

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

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.  $(\sigma)$ ,  $\sigma \in \Gamma_E$ ) make a basis of  $X(T)$  (resp. of  $X(T_E)$ ). The morphism  $r_\sigma: T \rightarrow T_E$  defines by transposition a homomorphism

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

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:

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

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

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

If  $\alpha \in \text{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$  is equal to the identity on  $\tau E$ , 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.  $\square$

**Proposition 2.** *Let  $\rho$  and  $(n_\sigma)$ ,  $\sigma \in \Gamma_E$ , be as in Th. 1 of A.5. Let  $r: T \rightarrow T_E$  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  $G^{\text{ab}}$  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)  *$\rho$  is locally algebraic.*

(b) *The Galois module  $V$  attached to  $\rho$  is of Hodge-Tate type.*

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

**Exercises.**

- 1) a) Let  $A = \text{End}_{\mathbb{Q}_p}(K)$  be the space of  $\mathbb{Q}_p$ -linear endomorphisms of  $K$ ; if  $a \in A$ , denote by  $\text{Tr}(a)$  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

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

- b) Show that the map  $c_K: A \rightarrow K$  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  $\text{Tr}_{K/\mathbb{Q}_p}(e_i e'_j) = \delta_{ij}$ . Show that

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

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

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

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

- e) If  $K$  is a Galois extension of  $\mathbb{Q}_p$ , show that  $c_K(\sigma) = 0$  for every  $\sigma \in \text{Gal}(K/\mathbb{Q}_p)$ ,  $\sigma \neq \text{id}$ , and  $c_K(\text{id}) = 1$ .
- 2) Let  $\varphi: G^{\text{ab}} \rightarrow K^\times$  be a continuous homomorphism, and let  $a_\varphi$  be the  $\mathbb{Q}_p$ -linear endomorphism of  $K$  such that the diagram

$$\begin{array}{ccc} U_K & \xrightarrow{\varphi} & U_K \\ \log \downarrow & & \downarrow \log \\ K & \xrightarrow{a_\varphi} & K \end{array}$$

is commutative. Let  $L\overline{\varphi}$  (resp.  $L\overline{\chi}$ ) be the image of  $\varphi$  (resp.  $\chi$ ) 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  $\varphi = \sigma^{-1} \circ \chi_K$ ,  $\sigma \in \text{Gal}(K/\mathbb{Q}_p)$ , in which case  $a_\varphi = -\sigma^{-1}$  and  $c_K(a_\varphi)$  is given by Exer. 1, d.)
- III-28

In particular,  $\varphi$  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  $\rho: G \rightarrow \text{Aut}(V)$  be an abelian  $p$ -adic representation of  $K$ . The following are equivalent:*

- (1)  $\rho$  is locally algebraic
- (2)  $\rho$  is of Hodge-Tate type and its restriction to the inertia group is semi-simple.

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

(\*) *The restriction of  $\rho$  to the inertia group is semi-simple.*

Hence we may assume that (\*) holds.

Let  $\pi$  be a uniformizing element of  $K$ , and let  $\text{pr}_\pi$  denote the projection map of  $G^{\text{ab}}$  onto its inertia group  $U_K$  associated to  $\pi$  (cf. A.4 and 6 [6]). Define a new representation  $\rho'$  of  $G^{\text{ab}}$  by

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

Replacing  $\rho$  by  $\rho'$  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  $\rho'$  is semi-simple, this means that, after replacing  $\rho$  by  $\rho'$ , we may assume that  $\rho$  is semi-simple and even (by an easy reduction) that it is *simple*. Let then  $E \subset \text{End}(V)$  be the commuting algebra of  $\rho$ . Since  $\rho$  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  $\rho$  is given by a continuous character  $\rho: G \rightarrow E^\times$ . III-29

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) 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

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

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

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

be the corresponding  $\ell$ -adic representation of  $K$ , cf. chap. I, 1.2. The main result of this Chapter is the determination of the Lie algebra of the  $\ell$ -adic Lie group  $G_\ell = \text{Im}(\rho_\ell)$ . This is based on a finiteness theorem of Šafarevič (1.4) combined with the properties of locally algebraic abelian representations (chap. III) and Tate's local theory of elliptic curves with non-integral modular invariant (Appendix, A.1). The variation of  $G_\ell$  with  $\ell$  is studied in §3.

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

#### §1. Preliminaries

IV-2

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

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

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

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

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

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

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

is non-zero.

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

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

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  $\Delta$  and  $j$ , for which we refer to **9** [9] or **20** [20]; note, however, that there is a misprint in Ogg's formula for  $\Delta$ : the coefficient of  $\beta_4^3$  should be  $-8$  instead of  $-1$ .)

## 1.2 Good reduction

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

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



IV-4 non-singular cubic  $\tilde{E}_v$  (hence an elliptic curve) over the residue field  $k_v$  (in other words, the discriminant  $\Delta(f)$  of  $f$  must be an invertible element of  $\mathcal{O}_v$ ). The curve  $\tilde{E}_v$  is called the **reduction** of  $E$  at  $v$ ; it does not depend on the choice of  $f$ , provided, of course, that  $\Delta(f) \in \mathcal{O}_v^\times$ .

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

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

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

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

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

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

Let  $\ell$  be a prime number. We define, as in chap. I, 1.2, the Galois modules  $T_\ell$  and  $V_\ell$  by:

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

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

IV-5

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

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

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

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

and

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

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

Conversely:

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

For the proof, see **32** [32], §1.

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

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

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

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

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

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

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

(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:

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

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

(The implication (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

IV-7

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

**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  $\Delta = g_2^3 - 27g_3^2 \in \mathcal{O}_S^\times$  (the group of units of  $\mathcal{O}_S$ ).*

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

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

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

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

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

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

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

with  $g_i \in \mathcal{O}_S$  and  $\Delta = g_2^3 - 27g_3^2 \in \mathcal{O}_S$ . But, since we are free to multiply  $\Delta$  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  $\Delta$ , the equation

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

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

**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  $E_{\ell^n}$ ,  $T_\ell$ ,  $V_\ell$  defined in 1.3.

## 2.1 The irreducibility theorem

Recall first that the ring  $\text{End}_K(E)$  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)  $V_\ell$  is irreducible for all primes  $\ell$ ;
- (b)  $E_\ell$  is irreducible for almost all primes  $\ell$ .

We need the following elementary result:

**Lemma 1.** *Let  $E$  be an elliptic curve defined over  $K$  with  $\text{End}_K(E) = \mathbb{Z}$ . Then, if  $E' \rightarrow E$ ,  $E'' \rightarrow E$  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  $E' \rightarrow E$  and  $E'' \rightarrow E$ . Suppose that  $E'$  and  $E''$  are isomorphic over  $K$ , and let  $E' \rightarrow E''$  be an isomorphism. If  $E \rightarrow E'$  is the transpose of the isogeny  $E' \rightarrow E$ , it has a cyclic kernel of order  $n'$ , and hence the isogeny  $E \rightarrow E''$ , obtained by composition of  $E \rightarrow E'$ ,  $E' \rightarrow E''$ ,  $E'' \rightarrow E$ , has for kernel an extension of  $\mathbb{Z}/n''\mathbb{Z}$  by  $\mathbb{Z}/n'\mathbb{Z}$ . But, since  $\text{End}_K(E) = \mathbb{Z}$ , 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.  $\square$

*Proof of the theorem.*

- (a) It suffices to show that, if  $\text{End}_K(E) = \mathbb{Z}$ , there is no one-dimensional  $\mathbb{Q}_\ell$ -subspace of  $V_\ell$  stable under  $\text{Gal}(\overline{K}/K)$ . Suppose there were one; its intersection  $X$  with  $T_\ell$  would be a submodule of  $T_\ell$  with  $X$  and  $T_\ell/X$  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  $E_\ell$  which is cyclic of order  $\ell^n$  and stable by  $\text{Gal}(\overline{K}/K)$ . 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  $E \rightarrow E(n)$  is cyclic of order  $\ell^n$ . 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  $E \rightarrow E/X_\ell$  whose kernel is cyclic of order  $\ell$ . The above lemma shows that the curves which correspond to different values of  $\ell$  are non-isomorphic, and one again applies the corollary to Šafarevič's theorem.  $\square$

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

## 2.2 Determination of the Lie algebra of $G_\ell$

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

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

*Proof.* The irreducibility theorem of 2.1 shows that, for any open subgroup  $U$  of  $G_\ell$ ,  $V_\ell$  is an irreducible  $U$ -module. Hence,  $V_\ell$  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  $\text{End}(V_\ell)$  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  $\text{End}(V_\ell)$ , or the subalgebra  $\mathfrak{sl}(V_\ell)$  of  $\text{End}(V_\ell)$  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  $V_\ell$  is a one-dimensional  $\mathfrak{g}'_\ell$ -vector space and the commuting algebra of  $\mathfrak{g}'_\ell$  in  $\text{End}(V_\ell)$  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  $\text{End}(V_\ell)$ ). After replacing  $K$  by a finite extension (this does not affect  $\mathfrak{g}_\ell$ , cf. chap. I, 1.1), we may then suppose that  $G_\ell$  itself is abelian. The  $\ell$ -adic representation  $V_\ell$  is then semi-simple, abelian and rational. It is, moreover, *locally algebraic*. To see this, we first remark that, at a place  $v$  dividing  $\ell$ , we have  $v(j) \geq 0$  since otherwise the decomposition group of  $v$  in  $G_\ell$  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  $\ell$  (cf. 1.2). Let  $E(\ell)$  be the  $\ell$ -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  $V_\ell$  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  $V_\ell$  the results of chap. III, 2.3. Hence, there is, for each prime  $\ell'$ , a rational, abelian, semi-simple  $\ell'$ -adic representation  $W_{\ell'}$  compatible with  $V_\ell$ . But  $V_{\ell'}$  is compatible with  $V_\ell$ , 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  $\ell'$  such that  $W_{\ell'}$  is the direct sum of one-dimensional IV-13 subspaces stable under  $\text{Gal}(\bar{K}/K)$ . This contradicts the irreducibility of  $V_\ell$ . Hence, we must have  $\mathfrak{g}'_\ell = \mathbb{Q}_p$  and  $\mathfrak{g}_\ell = \text{End}(V_\ell)$ .  $\square$

**Remark.** If  $E$  has complex multiplication, and  $L = \mathbb{Q} \otimes \text{End}(E \otimes_K \bar{K})$  is the corresponding imaginary quadratic field, one shows easily that  $\mathfrak{g}_\ell$  is the Cartan subalgebra of  $\text{End}(V_\ell)$  defined by  $L_\ell = \mathbb{Q}_\ell \otimes L$ . It splits if and only if  $\ell$  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  $\tilde{E}_v$ ; if  $\ell \neq p_v$ , we identify  $F_v$  to the corresponding automorphism of  $T_\ell$ .)

- 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  $H(\text{Tr}(F_v), \mathbf{N} v) = 0$ . If  $H$  is not the zero polynomial, show that  $V_H$  has density 0. (Show that the set of  $g \in \text{GL}(2, \mathbb{Z}_\ell)$  with  $H(\text{Tr}(g), \det(g)) = 0$  has Haar measure zero.)
- 2) The eigenvalues of  $F_v$  may be identified with complex numbers of the form

$$(\mathbf{N} v)^{1/2} e^{\pm i\varphi_v}, \quad 0 \leq \varphi_v \leq \pi,$$

cf. chap. I, Appendix A.2. Show that the set of  $v$  for which  $\varphi_v$  is a given angle  $\varphi$  has density zero. (Show that  $\text{Tr}(F_v)^2 = 4(\mathbf{N} v) \cos^2 \varphi$  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  $\ell$  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  $s \in \text{Aut}(V_\ell)$  such that the subalgebra  $\mathbb{Q}_\ell[s]$  of  $\text{End}(V_\ell)$  generated by  $s$  is isomorphic to  $C$ . Show that  $X_C$  is open in  $\text{Aut}(V_\ell)$ , and show that it has a non-empty intersection with every open subgroup of  $\text{Aut}(V_\ell)$ , in particular, with  $G_\ell$ .
- (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  $\ell_1, \dots, \ell_n$  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  $F_v \in X_{C_i}$  for  $i = 1, \dots, n$  has density  $> 0$ .  
(Use the fact that the image of  $\text{Gal}(\overline{K}/K)$  in any finite product of the  $\text{Aut}(V_\ell)$  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  $\ell$  be a prime number and let  $V_\ell(E)$  and  $V_\ell(E')$  be the corresponding  $\ell$ -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  $\ell$ .*
- (b) *The Galois modules  $V_\ell(E)$  and  $V_\ell(E')$  are isomorphic for one  $\ell$ .*
- (c) *If  $F_v$  and  $F'_v$  are the Frobeniuses of the reduced curves  $\tilde{E}_v$  and  $\tilde{E}'_v$ , we have  $\text{Tr}(F_v) = \text{Tr}(F'_v)$  for all  $v$  where there is good reduction.*
- (d) *For a set of places of  $K$  of density one we have  $\text{Tr}(F_v) = \text{Tr}(F'_v)$ .*



*Proof.* Clearly (a) implies (b), and (c) implies (d). The implication (b)  $\implies$  (c) follows from the fact that  $\text{Tr}(F_v)$  is known when  $V_\ell$  is known. To prove (d)  $\implies$  (a) one remarks first that the representations of  $\text{Gal}(\overline{K}/K)$  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.  $\square$

**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  $\tilde{E}_v$  (resp.  $\tilde{E}'_v$ ). We have the formulas (cf. 1.3): IV-16

$$\begin{aligned} t_v &= 1 - \text{Tr}(F_v) + \mathbf{N} v, \\ t'_v &= 1 - \text{Tr}(F'_v) + \mathbf{N} v. \end{aligned}$$

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  $T_q(E_{q'})$  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  $f: E \otimes_K L \rightarrow E' \otimes_K L$ . We will show that  $f$  is automatically defined over  $K$ . For this, it suffices to show that  $f = {}^s f$  for all  $s \in \text{Gal}(\overline{K}/K)$ , or, equivalently, that  $V(f): V_p(E) \rightarrow V_p(E')$  commutes with the action of Galois. However, if  $G_L = \text{Gal}(\overline{K}/L)$  is the open subgroup of  $G = \text{Gal}(\overline{K}/K)$  which corresponds to  $L$ , then  $V(f)$  commutes with the action of  $G_L$ . It is then enough to show that  $\text{Hom}_{G_L}(V, V') = \text{Hom}_G(V, V')$ . But  $V$  and  $V'$  are isomorphic as  $G$ -modules. Hence we have to show that  $\text{End}_{G_L}(V) = \text{End}_G(V)$ . But this is clearly true; in fact,  $G$  and  $G_L$  are open in  $\text{Aut}(V)$  by the theorem in section 2.2, and hence their commuting algebra is reduced to the homotheties in each case, i.e.  $\text{End}_{G_L}(V) = \text{End}_G(V) = \mathbb{Q}_p$ . This completes the proof of the theorem.  $\square$

**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 [38]) 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).  $\rightarrow$  [this has been proved by Faltings, see [54], [56], [82].]

### §3. Variation of $G_\ell$ and $\tilde{G}_\ell$ with $\ell$

#### 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  $\ell$  does not divide  $n$ , and let  $I_{v,\ell}$  be the inertia subgroup of  $\tilde{G}_\ell$  corresponding to some extension of  $v$  to  $\bar{K}$ . Then  $I_{v,\ell}$  contains a transvection, i.e. an element whose matrix form is  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  for a suitable  $\mathbb{F}_\ell$ -basis of  $E_\ell$ .*

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

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

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  $\ell$ ,  $I_{v,\ell}$  and a fortiori  $\tilde{G}_\ell$ , contains a transvection. On the other hand, we know (cf. 2.1) that  $\tilde{G}_\ell$  is irreducible for almost all  $\ell$ . Applying lemma 2 to  $\tilde{G}_\ell$  we then see that  $\tilde{G}_\ell$  contains  $\mathrm{SL}(2, \mathbb{F}_\ell)$  for almost all  $\ell$ ; hence we have (iv).  $\square$

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

### 3.3 Numerical example

Belen.

### 3.4 Proof of the main lemma of 3.1

IV-19

We need first a few lemmas:

**Lemma 1.** *Let  $S_\ell = (2, \mathbb{F}_\ell) = \mathrm{SL}(2, \mathbb{F}_\ell)/\{\pm 1\}$ , where  $\ell > 3$ . Then  $S_\ell$  is a simple group if  $\ell \geq 5$ . Every proper subgroup of  $S_\ell$  is solvable or isomorphic to the alternating group  $A_5$ : the last possibility occurs only if  $\ell \equiv \pm 1 \pmod{5}$ .*

*Proof.* This is well known, cf. for instance 4 [4], chap. XX.  $\square$

**Lemma 2.** *No proper subgroup of  $\mathrm{SL}(2, \mathbb{F}_\ell)$  maps onto  $(2, \mathbb{F}_\ell)$ .*

*Proof.* This is clear for  $\ell = 2$ , since  $(2, \mathbb{F}_2) = \mathrm{SL}(2, \mathbb{F}_2)$ . For  $\ell \neq 2$ , suppose there is such a proper subgroup  $X$ . We would then have

$$\mathrm{SL}(2, \mathbb{F}_\ell) = \{\pm 1\} \times X,$$

and this is absurd, since  $\mathrm{SL}(2, \mathbb{F}_\ell)$  is generated by the elements  $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$  and  $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$  which are of order  $\ell$ , hence contained in  $X$ .  $\square$

**Lemma 3.** *Let  $X$  be a closed subgroup of  $\mathrm{SL}(2, \mathbb{Z}_\ell)$  whose image in  $\mathrm{SL}(2, \mathbb{F}_\ell)$  is  $\mathrm{SL}(2, \mathbb{F}_\ell)$ . Assume  $\ell \geq 5$ . Then  $X = \mathrm{SL}(2, \mathbb{Z}_\ell)$ .*

*Proof.* We prove by induction on  $n$  that  $X$  maps onto  $\mathrm{SL}(2, \mathbb{Z}/\ell^n \mathbb{Z})$ . This is true for  $n = 1$ . Assume it is true for  $n$ , and let us prove it for  $n + 1$ . It is enough to show that, for any

$$s = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}_\ell)$$

which is congruent to 1 mod  $\ell^n$ , there is  $x \in X$  with  $x \equiv s \pmod{\ell^n}$ . Write  $s = 1 + \ell^n u$ ; since  $\det(s) = 1$ , one has  $\mathrm{Tr}(u) \equiv 0 \pmod{\ell^n}$ . But it is easy to see that any such  $u$  is congruent mod  $\ell$  to a sum of matrices  $u_i$  with  $u_i^2 = 0$ . Hence, we may assume that  $u^2 = 0$ . By the induction hypothesis, there exists  $y \in X$  such that  $y = 1 + \ell^{n-1}u + \ell^n v$ , where  $v$  has coefficients in  $\mathbb{Z}_\ell$ . Put

IV-20  $x = y^\ell$ . We have:

$$x = 1 + \ell(\ell^{n-1}u + \ell^n v) + \binom{\ell}{2}(\ell^{n-1}u + \ell^n v)^2 + \cdots + (\ell^{n-1}u + \ell^n v)^\ell.$$

If  $n \geq 2$ , it is clear that  $x \equiv 1 + \ell^n u \pmod{\ell^n}$ . This is also true for  $n = 1$ . Indeed, since  $u^2 = 0$ , and  $u + \ell v \equiv u \pmod{\ell}$ , we have

$$x \equiv 1 + \ell u + (u + \ell v)^2 \pmod{\ell^2}.$$

But  $(u + \ell v)^2 = \ell(uv + vu) \pmod{\ell^2}$ , hence:

$$(u + \ell v)^\ell \equiv \ell(uv + vu)u^{\ell-2} \equiv 0 \pmod{\ell^2} \quad \text{since } \ell > 4.$$

This shows that  $x \equiv 1 + \ell^n u \pmod{\ell^{n+1}}$  in all cases, and proves lemma 3.  $\square$

We now consider a closed subgroup  $G$  of  $X = \prod \mathrm{GL}(2, \mathbb{Z}_\ell)$  having the properties (a), (b), (c) of the main lemma of 3.1.

José: Update references.

**Lemma 4.** *Let  $S$  be a finite set of primes, and  $X_S = \prod_{\ell \in S} \mathrm{GL}(2, \mathbb{Z}_\ell)$ . The image  $G_S$  of  $G$  by the projection  $X \rightarrow X_S$  open in  $X_S$ .*

*Proof.* Replacing  $G$  by an open subgroup if necessary, we can assume that each  $G_\ell$ ,  $\ell \in S$ , is contained in the group of elements congruent to 1  $\pmod{\ell}$ , hence that each  $G_\ell$  is a pro- $\ell$ -group. Since  $G_S$  is a subgroup of  $\prod_{\ell \in S} G_\ell$ , it follows that  $G_S$  is *pro-nilpotent* (projective limit of finite nilpotent groups), hence is the product of its Sylow subgroups. This shows that  $G_S = \prod_{\ell \in S} G_\ell$ , and since  $G_\ell$  is open in  $\mathrm{GL}(2, \mathbb{Z}_\ell)$  by property (a), we see that  $G_S$  is open in  $X_S$ .  $\square$  IV-21

Before we go further, we introduce some terminology. Let  $Y$  be a profinite group, and  $\Sigma$  a finite simple group. We say that  $\Sigma$  **occurs** in  $Y$  if there exist closed subgroups  $Y_1, Y_2$  of  $Y$  such that  $Y_1$  is normal in  $Y_2$  and  $Y_1/Y_2$  is isomorphic to  $\Sigma$ . We denote by  $\mathrm{Occ}(Y)$  the set of classes of finite simple non abelian groups occurring in  $Y$ . If  $Y = \varprojlim_\alpha Y_\alpha$ , and each  $Y \rightarrow Y_\alpha$  is surjective, we have

$$\mathrm{Occ}(Y) = \bigcup_\alpha \mathrm{Occ}(Y_\alpha).$$

If  $Y$  is an extension of  $Y'$  and  $Y''$ , we have:

$$\mathrm{Occ}(Y) = \mathrm{Occ}(Y') \cup \mathrm{Occ}(Y'').$$

Using these formulae and lemma 1, one gets:

$$\mathrm{Occ}(\mathrm{GL}(2, \mathbb{Z}_\ell)) = \mathrm{Occ}(\mathrm{SL}(2, \mathbb{Z}_\ell)) = \mathrm{Occ}(S_\ell)$$

where  $S_\ell = (2, \mathbb{F}_\ell)$  as before, and:

$$\begin{aligned} \mathrm{Occ}(S_\ell) &= \emptyset & \text{if } \ell = 2, 3 \\ \mathrm{Occ}(S_\ell) &= \{S_\ell\} = \{A_5\} & \text{if } \ell = 5 \end{aligned}$$

$$\begin{aligned} \text{Occ}(S_\ell) &= \{S_\ell\} && \text{if } \ell \equiv \pm 2 \pmod{5}, \ell > 5 \\ \text{Occ}(S_\ell) &= \{S_\ell, A_5\} && \text{if } \ell \equiv \pm 1 \pmod{5}, \ell > 5. \end{aligned}$$

Let now  $S$  be a finite set of primes so that  $2, 3, 5 \in S$  and

IV-22

$$\ell \in S \implies \tilde{G}_\ell \supset \text{SL}(2, \mathbb{F}_\ell).$$

Property (c) shows that such a set exists.

**Lemma 5.** *The group  $G$  contains  $\prod_{\ell \notin S} \text{SL}(2, \mathbb{Z}_\ell)$ .*

(This partial product is understood as a subgroup of the full product  $X = \prod_\ell \text{GL}(2, \mathbb{Z}_\ell)$ .)

*Proof.* It is enough to show that  $G$  contains each  $\text{SL}(2, \mathbb{Z}_\ell)$ ,  $\ell \notin S$ . Let  $H_\ell = \text{GL}(2, \mathbb{Z}_\ell)$ . If  $\ell \notin S$ , the fact that  $\tilde{G}_\ell$  contains  $\text{SL}(2, \mathbb{F}_\ell)$  shows that  $S_\ell \in \text{Occ}(G_\ell)$  hence  $S_\ell \in \text{Occ}(G)$ . On the other hand,  $G/H_\ell$  is isomorphic to a closed subgroup of  $\prod_{\ell' \neq \ell} \text{GL}(2, \mathbb{Z}_{\ell'})$  hence  $S_\ell \notin \text{Occ}(G/H_\ell)$  (we use the obvious fact that the simple groups  $S_p$ ,  $p > 5$ , are pairwise non isomorphic). Since

$$\text{Occ}(G) = \text{Occ}(H_\ell) \cup \text{Occ}(G/H_\ell),$$

we then have  $S_\ell \in \text{Occ}(H_\ell)$ . Let  $\tilde{H}_\ell$  be the image of  $H_\ell$  in  $\text{SL}(2, \mathbb{F}_\ell)$ ; the kernel of  $H_\ell \rightarrow \tilde{H}_\ell$  being a pro- $\ell$ -group, we have  $\text{Occ}(H_\ell) = \text{Occ}(\tilde{H}_\ell)$ , hence  $S_\ell \in \text{Occ}(\tilde{H}_\ell)$ . Hence  $\tilde{H}_\ell$  maps onto  $S_\ell = (2, \mathbb{F}_\ell)$ , and, by lemma 2, we have  $\tilde{H}_\ell = \text{SL}(2, \mathbb{F}_\ell)$  and, by lemma 3,  $H_\ell = \text{SL}(2, \mathbb{Z}_\ell)$ . Hence  $G$  contains  $\text{SL}(2, \mathbb{Z}_\ell)$ .  $\square$

**Lemma 6.** *The group  $G$  contains an open subgroup of  $\prod \text{SL}(2, \mathbb{Z}_\ell)$ .*

*Proof.* Let  $S$  be as in lemma 5; let  $G_S$  be the projection of  $G$  into  $\prod_{\ell \in S} \text{GL}(2, \mathbb{Z}_\ell)$  and  $G'_S$  the projection into the complementary product  $\prod_{\ell \notin S} \text{GL}(2, \mathbb{Z}_\ell)$ . Let  $H_S$  be  $G \cap \prod_{\ell \in S} \text{GL}(2, \mathbb{Z}_\ell)$  and  $H'_S = G \cap \prod_{\ell \notin S} \text{GL}(2, \mathbb{Z}_\ell)$ , so that  $H_S \subset G_S$ ,  
IV-23  $H'_S \subset G'_S$ . One has canonical isomorphisms:

$$G_S/H_S \cong G/(H_S \times H'_S) \cong G'_S/H'_S.$$

Lemma ?? shows that  $H'$  contains  $\prod_{\ell \notin S} \text{SL}(2, \mathbb{Z}_\ell)$ , so that  $G'_S/H'_S$  is abelian. Hence  $G_S/H_S$  is abelian and  $H_S$  contains the adherence  $(G_S, G_S)$  of the commutator group of  $G_S$ . By lemma 4,  $G_S$  is open in  $\prod_{\ell \in S} \text{SL}(2, \mathbb{Z}_\ell)$ . It is easy to see that this implies that  $(G_S, G_S)$  contains an open subgroup of

$\prod_{\ell \in S} \mathrm{SL}(2, \mathbb{Z}_\ell)$  (this follows for instance from the fact that the derived Lie algebra of  $\mathfrak{gl}_2$  is  $\mathfrak{sl}_2$ ). Hence  $H_S$  contains an open subgroup  $U$  of  $\prod_{\ell \in S} \mathrm{SL}(2, \mathbb{Z}_\ell)$ . Using lemma ??, we then see that  $G$  contains  $U \times \prod_{\ell \notin S} \mathrm{SL}(2, \mathbb{Z}_\ell)$  which is open in  $\prod_{\ell} \mathrm{SL}(2, \mathbb{Z}_\ell)$ .  $\square$

*Proof of the main lemma.* Consider the determinant map

$$\det: \prod_{\ell} \mathrm{GL}(2, \mathbb{Z}_\ell) \longrightarrow \prod_{\ell} \mathbb{Z}_\ell^\times,$$

whose kernel is  $\prod_{\ell} \mathrm{SL}(2, \mathbb{Z}_\ell)$ . Hypothesis (c) means that the image of  $G$  by this map is open and lemma 6 shows that  $G \cap \ker(\det)$  is open in  $\ker(\det)$ . This is enough to imply that  $G$  itself is open.  $\square$

### Exercises.

- 1)
  - a) Generalize lemma 3 to  $\mathrm{SL}(d, \mathbb{Z}_\ell)$  for  $d > 2$ ,  $\ell > 5$  (same method).
  - b) Show that the only closed subgroup of  $\mathrm{SL}(d, \mathbb{Z}_\ell)$  which maps onto  $\mathrm{SL}(d, \mathbb{Z}/3^2\mathbb{Z})$  is  $\mathrm{SL}(d, \mathbb{Z}_3)$  itself.
  - c) Show that the only closed subgroup of  $\mathrm{SL}(d, \mathbb{Z}_2)$  which maps onto  $\mathrm{SL}(d, \mathbb{Z}/2^3\mathbb{Z})$  is  $\mathrm{SL}(d, \mathbb{Z}_2)$  itself.
- 2) Let  $E$  be the unramified quadratic extension of  $\mathbb{Q}_2$ , and  $\mathcal{O}_E$  its ring of integers. Let  $x \mapsto \bar{x}$  be the non trivial automorphism of  $E$ .
  - a) Show that  $\mathcal{O}_E$  contains a primitive third root of unity  $z$ .
  - b) Show that  $\mathcal{O}_E$  contains an element  $u$  with  $u \cdot \bar{u} = -1$  (take for instance  $u = (1 + \sqrt{5})/2$ ).
  - c) Let  $\alpha$  and  $\beta$  be the  $\mathbb{Z}_2$ -linear endomorphisms defined by  $\alpha(x) = zx$ ,  $\beta(x) = u\bar{x}$ , where  $z$  and  $u$  are as in a), b) above. Show that  $\alpha$  is of order 3,  $\beta$  of order 4, and  $\beta\alpha\beta^{-1} = \alpha^{-1}$ , so that  $\alpha$  and  $\beta$  generate a non-abelian group  $G$  of order 12.
  - d) Show that  $G$  is contained in  $\mathrm{SL}(\mathcal{O}_E) \cong \mathrm{SL}(2, \mathbb{Z}_2)$  and that reduction mod 2 defines a homomorphism of  $G$  onto  $\mathrm{SL}(2, \mathbb{F}_2)$ . (Hence lemma 3 does not extend to the case  $\ell = 2$ .)
- 3) Let  $S_9 = \mathrm{SL}(2, \mathbb{Z}/9\mathbb{Z})$ ,  $S_3 = \mathrm{SL}(2, \mathbb{Z}/3\mathbb{Z})$  and  $g = \ker(S_9 \rightarrow S_3)$ . The group  $g$  is isomorphic to a three-dimensional vector space over  $\mathbb{F}_3$ . Let  $x \in H^2(S_3, g)$  be the cohomology class corresponding to the extension

$$1 \longrightarrow g \longrightarrow S_9 \longrightarrow S_3 \longrightarrow 1.$$

- a) Show that the restriction of  $x$  to a 3-Sylow subgroup of  $S_3$  is zero (note that  $\mathrm{SL}(2, \mathbb{Z})$  contains an element of order 3, viz.  $\begin{pmatrix} 1 & 1 \\ -3 & -2 \end{pmatrix}$ ).
- b) Deduce from a) that  $x = 0$ , i.e. that there exists a subgroup  $X$  of  $S_9$  which is mapped isomorphically onto  $S_3$ . (The inverse image of  $X$  in  $\mathrm{SL}(2, \mathbb{Z}_3)$  is a non-trivial subgroup which is mapped onto  $S_3$ ; hence lemma 3 does not extend to the case  $\ell = 3$ .)

## §A. Local results

IV-25

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  $\ell$  be a prime number different from the characteristic of  $K$ . Let  $T_\ell$  and  $V_\ell$  be the corresponding Galois modules; we denote by  $G_\ell$  the image of  $\mathrm{Gal}(K_s/K)$  in  $\mathrm{Aut}(T_\ell)$ , and by  $I_\ell$  the inertia subgroup of  $G_\ell$ . 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  $I_\ell$  is an invariant subgroup of  $G_\ell$ , 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  $\Gamma_q$  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  $K'^\times/\Gamma_q$  is isomorphic to the group  $E_q(K')$  of points of  $E_q$  with values in  $K'$ . The equation defining  $E_q$  can be written in the form

$$y^2 + xy = x^3 - b_2x - b_3,$$

IV-26



with

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

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

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

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

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

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 IV-27 kernel of multiplication by  $\ell^n$  in  $K_s^\times/\Gamma_q$ . If  $\mu_n$  is the group of  $\ell^n$ -th roots of unity in  $K_s$ , we have an injection  $\mu_n \rightarrow E_n$ . 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

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

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

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

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

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

We now show that this sequence of  $\text{Gal}(K_s/K)$ -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  $G = \text{Gal}(K_s/K)$ . 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  $\delta: K^\times/K^{\times \ell^n} \rightarrow H^1(G, \mu_n)$  of Kummer theory transforms the class of  $q \bmod K^{\times \ell^n}$  into  $x_n$ .*

(b) *The element  $x$  is of infinite order.*

(Recall that  $\delta$  is induced by the coboundary map relative to the exact sequence

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

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

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

and hence a homomorphism

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

If we identify  $x$  with the corresponding element of  $\varprojlim_n K^\times/K^{\times \ell^n}$ , 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-28 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  $\text{End}(V_\ell)$  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  $V_\ell$  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  $V_\ell$  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  $V_\ell$ , 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  $\ell^n$ -th roots of unity, hence  $\text{Gal}(K_s/K)$  acts trivially on  $T_\ell(\mu)$ . Consequently, there is a basis  $e_1, e_2$  of  $T_\ell(E)$  such that, for all  $\sigma \in \text{Gal}(K_s/K)$ , 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  $\text{Im}(a)$  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  $\text{char}(K) = 0$  as  $\ell \neq \text{char}(K)$ . In this case, the action of  $\text{Gal}(\overline{K}/K)$  on  $V_\ell(\mu)$  is by means of the character  $\chi_\ell$  (cf. chap. I, 1.2) which is of infinite order. It follows that  $\mathfrak{g}_\ell = \mathfrak{r}_X$  where  $X = V_\ell(\mu)$ ; in fact,  $\mathfrak{g}_\ell \supset \mathfrak{n}_X$  since the sequence (IV.3) does not split, and we cannot have  $\mathfrak{g}_\ell = \mathfrak{n}_X$ . IV-29
- 3) Since  $k$  is finite, the action of  $\text{Gal}(K_s/K)$  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  $\text{Im}(a) = \ell^n \mathbb{Z}_\ell$ , where  $\ell^n$  is the highest power of  $\ell$  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  $\tilde{E}$  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. 9 [9]) 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 [26], §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  $\tilde{E}$  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  $\text{End}(V_p)$  or a non-split Cartan subalgebra of  $\text{End}(V_p)$ .*

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

*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. [27], 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  $\mathfrak{gl}_2$ . But  $\mathfrak{g}_p \neq \mathfrak{sl}_2$  since  $\bigwedge^2 V_p$  is canonically isomorphic to  $V_p(\mu)$ , and the action of  $\text{Gal}(\bar{K}/K)$  on  $V_p(\mu)$  is by means of the character  $\chi_p$ , 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  $\text{End}(V_p)$  or a non split Cartan subalgebra of  $\text{End}(V_p)$ . 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: IV-30

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

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

**Remark.** 1) By a theorem of Tate ([39], §4, cor. 1 to th. 4), the algebra  $\mathfrak{g}_p$  is a Cartan subalgebra of  $\text{End}(V_p)$  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  $\text{End}(V_p)$ , and let  $H = \mathfrak{g}_p \cap \text{Aut}(V_p)$  be the corresponding Cartan subgroup of  $\text{Aut}(V_p)$ . If  $N$  is the normalizer of  $H$  in  $\text{Aut}(V_p)$ , 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-31 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  $\text{End}(V_p)$ ). If  $U_F$  denotes

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

$$\varphi_I: \text{Gal}(\overline{K}/K) \longrightarrow U_F.$$

By local class field theory, we may identify the inertia group of  $\text{Gal}(\overline{K}/K)^{\text{ab}}$  with the group  $U_K$  of units of  $K$ . Hence the restriction  $\varphi_I$  of  $\varphi$  to the inertia group is a *homomorphism of  $U_K$  into  $U_F$* . To determine  $\varphi_I$ , we first remark that the action of  $\text{End}(E(p))$  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)

$$\varphi_I(x) = N_{K/F}(x^{-1}), \quad \text{for all } x \in U_K.$$

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. **17** [**17**]), the formal groups  $E'$  and  $E''$  are isomorphic over the completion of the maximal unramified extension of  $K$  (cf. **16** [**16**], 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 [**17**].

José: ¿A qué fórmula se refiere?

**3. Auxiliary results on abelian varieties.** Let  $A$  and  $B$  be two abelian 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  $\tilde{A}$  and  $\tilde{B}$  (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  $\tilde{f}: \tilde{A} \rightarrow \tilde{B}$  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  $f(p): A(p) \rightarrow B(p)$  whose reduction is  $\widetilde{f(p)}$ . Then, there is a morphism  $f: A \rightarrow B$  whose reduction is  $\tilde{f}$ .*

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  $\text{Gal}(\overline{K}/K)$ . Then every endomorphism of  $\tilde{A}$  lifts to an*

endomorphism of  $A$ , i.e., the reduction homomorphism  $\text{End}(A) \rightarrow \text{End}(\tilde{A})$  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:  $\text{Hom}(H_1, H_2) \rightarrow \text{Hom}(\tilde{H}_1, \tilde{H}_2)$  is bijective.*

*Proof.* This is clear if both  $H_1$  and  $H_2$  are étale. If both are not étale, their IV-33 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

$$\text{Hom}(H_1, H_2) = \text{Hom}(\tilde{H}_1, \tilde{H}_2) = 0. \quad \square$$

**Corollary 1.1.** *Assume:*

- (i)  $V_p(A)$  is a direct sum of one-dimensional subspaces stable under  $\text{Gal}(\bar{K}/K)$ .
- (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 **34** [34], 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  $\text{Gal}(\bar{K}/K)$ . One can find an isogeny  $A_1 \rightarrow A$  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.  $\text{End}(A) \rightarrow \text{End}(\tilde{A})$  is an isomorphism. But, since  $k$  is finite, it follows from a result of **38** [38] that  $\mathbb{Q} \otimes \text{End}(\tilde{A})$  contains a semi-simple commutative  $\mathbb{Q}$ -subalgebra  $\Lambda$  of rank  $2 \dim(A)$  (this is not explicitly stated in [38], but follows easily from its “Main Theorem”). Hence, the same is true for  $\mathbb{Q} \otimes \text{End}(A)$ . If we now write  $\Lambda$  as a product of commutative fields  $\Lambda_\alpha$ , one sees that  $A$  is isogenous to a product  $\prod_\alpha A_\alpha$ , where  $A_\alpha$  has complex multiplication of type  $\Lambda_\alpha$ .  $\square$

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

Belén.





## BIBLIOGRAPHY



## **SUPPLEMENTARY BIBLIOGRAPHY**



# INDEX

- $\ell$ -adic representation of a field, 11
- Admissible (character), 70
- Almost locally algebraic  
(homomorphism), 66
- Anisotropic (torus), 48
- Arithmetic subgroup, 48
- $C_K$ , 27
- $C_{\mathfrak{m}}$ , 27
- Commensurable (subgroups), 48
- Compatible (system  $(\rho_\ell)$ ), 8
- Conductor, 38, 58
- $D$ , 27
- $\varepsilon_\ell$ , 30
- $E_{\mathfrak{m}}$ , 27
- Equidistribution, 14
- Exceptional set (of a system), 9
- $G_\ell$ , 84
- $\mathbb{G}_m$ , 23
- Hodge-Tate module, 54
- Hodge-Tate representation, 55
- Hodge-Tate type (module), 54
- Hodge-Tate type (representation),  
55
- $I$ , 27
- Idèle, 27
- Idèle class, 27
- $I_{\mathfrak{m}}$ , 27
- Integral (representation), 7
- Locally algebraic  
(homomorphism), 66
- $M_K$ , 26
- $M_K^\infty$ , 26
- Rational (representation), 7
- Strictly compatible (system  $(\rho_\ell)$ ),  
8
- Tate's elliptic curves, 94
- Torus, 23
- Trace, 32
- $\mathbb{T} = \mathfrak{R}_{K/\mathbb{Q}}(\mathbb{G}_{m,K})$ , 23
- $U_v$ , 27
- $U_{v,\mathfrak{m}}$ , 27
- Weierstrass form (of an elliptic  
curve), 78