Abelian *l*-Adic Representations and Elliptic Curves

Jean-Pierre Serre
Collège de France

McGill University Lecture Notes
written with the collaboration of
Willem Kuyk and John Labute

ADDISON-WESLEY PUBLISHING COMPANY, INC.
THE ADVANCED BOOK PROGRAM
Redwood City, California • Menlo Park, California • Reading, M[illegible]
New York • Amsterdam • Don Mills, Ontario • Sydney • Madrid
Singapore • Tokyo • San Juan • Wokingham, United Kingdom

Abelian *l*-Adic Representations and Elliptic Curves

Originally published in 1968 by W. A. Benjamin, Inc.

Library of Congress Cataloging-in-Publication Data

Serre, Jean Pierre.
Abelian L-adic representations and elliptic curves.

(Advanced book classics series)
On t.p. "l" in l-adic is transcribed in lower-case script.
Bibliography: p.
Includes index.
1. Representations of groups. 2. Curves, Elliptic.
3. Fields, Algebraic. I. Title. II. Series.
QA171.S525 1988 512'.22 88-19268
ISBN 0-201-09384-7

Manufactured in the United States of America
Published simultaneously in Canada

Publisher's Foreword

"Advanced Book Classics" is a reprint series which has come into being as a direct result of public demand for the individual volumes in this program. That was our initial criterion for launching the series. Additional criteria for selection of a book's inclusion in the series include:

- Its intrinsic value for the current scholarly buyer. It is not enough for the book to have some historic significance, but rather it must have a timeless quality attached to its content, as well. In a word, "uniqueness."
- The book's global appeal. A survey of our international markets revealed that readers of these volumes comprise a boundaryless, worldwide audience.
- The copyright date and imprint status of the book. Titles in the program are frequently fifteen to twenty years old. Many have gone out of print, some are about to go out of print. Our aim is to sustain the lifespan of these very special volumes.

We have devised an attractive design and trim-size for the "ABC" titles, giving the series a striking appearance, while lending the individual titles unifying identity as part of the "Advanced Book Classics" program. Since "classic" books demand a long-lasting binding, we have made them available in hardcover at an affordable price. We envision them being purchased by individuals for reference and research use, and for personal and public libraries. We also foresee their use as primary and recommended course materials for university level courses in the appropriate subject area.

The "Advanced Book Classics" program is not static. Titles will continue to be added to the series in ensuing years as works meet the criteria for inclusion which we've imposed. As the series grows, we naturally anticipate our book buying audience to grow with it. We welcome your support and your suggestions concerning future volumes in the program and invite you to communicate directly with us.

Vita

Jean-Pierre Serre

Professor of Algebra and Geometry at the Collège de France, Paris, was born in Bages, France, on September 15, 1926. He graduated from Ecole 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.

Special Preface

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

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

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

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

l-adic representations associated to abelian varieties over number fields

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

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

$$\mathrm{Hom}_K(A,B) \otimes \mathbf{Z}_l \to \mathrm{Hom}_{\mathrm{Gal}}(T_l(A), T_l(B))$$

is an isomorphism (A and B being abelian varieties over a number field K), together with the semi-simplicity of the Galois module $\mathbf{Q}_l \otimes T_l(A)$ and similar results for $T_l(A)/lT_l(A)$

Preface

This book reproduces, with a few complements, a set of lectures given at McGill University, Montreal, from Sept.5 to Sept.18, 1967. It has been written in collaboration with John LABUTE (Chap. I, IV) and Willem KUYK (Chap. II, III). To both of them, I want to express my heartiest thanks.

Thanks also due to the secretarial staff of the Institute for Advanced Study for its careful typing of the manuscript.

JEAN-PIERRE SERRE

Princeton, Fall 1967

when l is large enough. These results may be used to study the structure of the Galois group of the division points of A, cf. [80]. For instance, if dimA is odd and $\mathrm{End}_K A = \mathbf{Z}$, one can show that this Galois group has finite index in the group of symplectic similitudes; for elliptic curves, i.e. dimA = 1, this was already proved in [76].

Modular forms and l-adic representations

The existence of l-adic representations attached to modular forms, conjectured in the first edition of this book, has been proved by Deligne ([50], see also Langlands [65] and Carayol [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 diagram

$$\begin{array}{ccc} \text{motives} & & \\ \Big| & \rightarrow & \text{automorphic representations of} \\ \text{rational } l\text{-adic representations} & & \text{reductive groups} \end{array}$$

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 $\mathbf{Q}$). Chapters II and III of the present book, supplemented by the results of Deligne ([53]) and Waldschmidt ([63], [83]), may be viewed as a partial realization of this ambitious program in the abelian case.

Local theory of l-adic representations

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

Contents

Chapter III Locally Algebraic Abelian Representations

Chapter IV *l*-adic Representations Attached to Elliptic Curves

INTRODUCTION

The " ℓ-adic representations " considered in this book are the algebraic analogue of the locally constant sheaves (or " local coefficients ") of Topology. A typical example is given by the ℓ^n-th division points of abelian varieties (cf. chap.I, 1.2); the corresponding ℓ-adic spaces, first introduced by Weil [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 ℓ-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 ℓ-adic representations relative to different prime numbers ℓ via the properties of the Frobenius elements (see below). In the same paper, Taniyama also studied some abelian representations which are closely related to complex multiplication (cf. Weil [41], [42] and Shimura-Taniyama [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 ℓ-adic representations (§1). In §2, the ground field is assumed to be a number field. Hence, Frobenius elements are defined, and one has the notion of a rational ℓ-adic representation : one for which their characteristic polynomials have rational coefficients (instead of merely ℓ-adic ones). Two representations corresponding to different primes are compatible if the characteristic polynomials of their Frobenius elements are the same (at least almost everywhere) ; not much is known about this notion in the non abelian case (cf. the list of open questions at the end of 2.3). A last section shows how one attaches L-functions to rational ℓ-adic representations; the well known connection between equidistribution and analytic properties of L-functions is discussed in the Appendix.

Chapter II gives the construction of some abelian ℓ-adic representations of a number field K. As indicated above, this construction is essentially due to Shimura, Taniyama and Weil. However, I have found it convenient to present their results in a slightly different way, by defining first some algebraic groups over Q (the groups S_m) whose representations - in the usual algebraic sense - correspond to the sought for ℓ-adic representations of K. The same groups had been considered before by Grothendieck in his still conjectural theory of " motives " (indeed, motives are supposed to be " ℓ-adic cohomology without ℓ " so the connection is not surprising). The construction of these groups S_m and of the ℓ-adic representations attached to them, is given in §2 (§1 contains some preliminary constructions on algebraic groups, of a rather

elementary kind). I have also briefly indicated what relations these groups have with complex multiplication (cf. 2.8). The last § contains some more properties of the S_m's.

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

Chapter IV is concerned with the ℓ-adic representation ρ_ℓ defined by an elliptic curve E. Its aim is to determine, as precisely as possible, the image of the Galois group by ρ_ℓ, or at least its Lie algebra. Here again the ground field is assumed to be a number field (the case of a function field has been settled by Igusa [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 $\mathrm{Im}(\rho_\ell)$ then follows, using the properties of abelian representations given in chap.II, III; one has to know that ρ_ℓ, if abelian, is locally algebraic, but this is a consequence of the result of Tate given in chap.III. The variation of $\mathrm{Im}(\rho_\ell)$ with ℓ is dealt with in §3. Similar results for the local case are given in the Appendix.

NOTATIONS

General notations

Positive means ≥ 0.

Z (resp. Q, R, C) is the ring (resp. the field) of integers (resp. of rational numbers, of real numbers, of complex numbers).

If p is a prime number, F_p denotes the prime field Z/pZ and Z_p (resp. Q_p) the ring of p-adic integers (resp. the field of p-adic rational numbers). One has:

$$Z_p = \varprojlim Z/p^n Z \quad , \qquad Q_p = Z_p[\tfrac{1}{p}] .$$

Prime numbers

They are denoted by ℓ, ℓ', p, ... ; we mostly use the letter ℓ for "ℓ-adic representations" and the letter p for the residue characteristic of some valuation.

Fields

If K is a field, we denote by $\overline{K}$ an algebraic closure of K, and by K_s the separable closure of K in $\overline{K}$; most of the fields we consider are perfect, in which case $K_s = \overline{K}$.

If L/K is a (possibly infinite) Galois extension, we denote its Galois group by $Gal(L/K)$; it is a projective limit of finite groups.

Algebraic groups

If G is an algebraic group over a field K, and if K' is a commutative K-algebra, we denote by $G(K')$ the group of K'-points of G (the "K'-rational" points of G). When K' is a field, we denote by $G_{/K'}$ the K'-algebraic group $G \times_K K'$ obtained from G by extending the ground field from K to K'.

Let V be a finite dimensional K-vector space. We denote by $\mathrm{Aut}_K(V)$, or $\mathrm{Aut}(V)$, the group of its K-linear automorphisms, and by GL_V the corresponding K-algebraic group (cf. chap. I, 2.4). For any commutative K-algebra K', the group $GL_V(K')$ of K'-points of GL_V is $\mathrm{Aut}_{K'}(V \otimes_K K')$; for instance, $GL_V(K) = \mathrm{Aut}(V)$.

Abelian l-Adic Representations and Elliptic Curves

CHAPTER I

ℓ-ADIC REPRESENTATIONS

§1. THE NOTION OF AN ℓ-ADIC REPRESENTATION

1.1. Definition

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

DEFINITION - An ℓ-adic representation of G (or, by abuse of language, of K) is a continuous homomorphism $\rho : G \longrightarrow \mathrm{Aut}(V)$.

Remarks

1) A lattice of V is a sub-Z_ℓ-module T which is free of finite rank, and generate V over Q_ℓ, so that V can be identified with $T \otimes_{Z_\ell} Q_\ell$. 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.

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

2) If ρ is an ℓ-adic representation of G, the group $G_\rho = \mathrm{Im}(\rho)$ is a closed subgroup of Aut(V), and hence, by the ℓ-adic analogue of Cartan's theorem (cf. [28], LG, p. 5-42) G_ρ is itself an ℓ-adic Lie group. Its Lie algebra $\underline{g}_\rho = \mathrm{Lie}(G_\rho)$ is a subalgebra of $\mathrm{End}(V) = \mathrm{Lie}(\mathrm{Aut}(V))$. The Lie algebra $\underline{g}_\rho$ 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 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 Aut(V).

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

a) T' is stable by G

b) Either T' is a sublattice of index ℓ of T and G acts trivially on T/T' or T is a sublattice of index ℓ of T' and G

acts trivially on T'/T.

(Apply exercise 1) above to $k = F_\ell$ and $V = T/\ell T$.)

3) Let ρ be a semi-simple ℓ-adic representation of G and let U be an invariant subgroup of G. Assume that, for all $x \in U$, $\rho(x)$ is unipotent (all its eigenvalues are equal to 1). Show that $\rho(x) = 1$ for all $x \in U$. (Show that the restriction of ρ to U is semi-simple and use Kolchin's theorem to bring it to triangular form.)

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

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

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

1.2. Examples

1. Roots of unity. Let $\ell \neq \mathrm{char}(K)$. The group $G = \mathrm{Gal}(K_s/K)$ acts on the group μ_{ℓ^m} of ℓ^m-th roots of unity, and hence also on $T_\ell(\mu) = \varprojlim \mu_{\ell^m}$. The Q_ℓ-vector space $V_\ell(\mu) = T_\ell(\mu) \otimes_{Z_\ell} Q_\ell$ is of dimension 1, and the homomorphism $\chi_\ell : G \longrightarrow \mathrm{Aut}(V_\ell) = Q_\ell^*$ defined by the action of G on V_ℓ is a 1-dimensional ℓ-adic representation of G. The character χ_ℓ takes its values in the group of units U_ℓ of Z_ℓ; by definition

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

2. Elliptic curves. Let $\ell \neq \mathrm{char}(K)$. Let E be an elliptic curve defined over K with a given rational point 0. One knows that

there is a unique structure of group variety on E with 0 as neutral element. Let E_m be the kernel of multiplication by ℓ^m in $E(K_s)$, and let

$$T_\ell(E) = \varprojlim E_m, \quad V_\ell(E) = T_\ell(E) \otimes_{Z_\ell} Q_\ell .$$

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

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

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

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

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

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

$$H^i(X_s, Z_\ell) = \varprojlim H^i((X_s)_{\text{ét}}, Z/\ell^n Z) ,$$

$$H^i_\ell(X_s) = H^i(X_s, Z_\ell) \otimes_{Z_\ell} Q_\ell .$$

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

Exercise

(a) Show that there is an elliptic curve E, defined over $K_o = Q(T)$, with j-invariant equal to T.

(b) Show that for such a curve, over $K = C(T)$, one has $G_\ell = SL(T_\ell(E))$ (cf. Igusa [10] for an algebraic proof).

(c) Using (b), show that, over K_o, we have $G_\ell = GL(T_\ell(E))$.

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

§2. ℓ-ADIC REPRESENTATIONS OF NUMBER FIELDS

2.1. Preliminaries

(For the basic notions concerning number fields, see for instance Cassels-Fröhlich [6], Lang [13] or Weil [44].) Let K be a number field (i.e. a finite extension of Q). Denote by Σ_K the set of all finite places of K, i.e., the set of all normalized discrete valuations of K (or, alternatively, the set of prime ideals in the ring A_K of integers of K). The residue field k_v of a place $v \in \Sigma_K$ is a finite field with $Nv = p_v^{\deg(v)}$ elements, where

$p_v = \mathrm{char}(k_v)$ and $\deg(v)$ is the degree of k_v over F_{p_v}. The ramification index e_v of v is $v(p_v)$.

Let L/K be a finite Galois extension with Galois group G, and let $w \in \Sigma_L$. 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 $v \in \Sigma_K$; by abuse of language, we also say that v is the restriction of w to K, and we write $w|v$ ("w divides v"). Let L_w (resp. K_v) be the completion of L (resp. K) with respect to w (resp. v). We have $D_w \simeq \mathrm{Gal}(L_w/K_v)$. The group D_w is mapped homomorphically onto the Galois group $\mathrm{Gal}(\ell_w/k_v)$ of the corresponding residue extension ℓ_w/k_v. The kernel of $G \longrightarrow \mathrm{Gal}(\ell_w/k_v)$ 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 $F(\lambda) = \lambda^{Nv}$ for all $\lambda \in \ell_w$. 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 $\mathbf{Q}$, one defines Σ_L to be the projective limit of the sets Σ_{L_a}, where L_a ranges over the finite sub-extensions of $L/\mathbf{Q}$. Then, if L/K is an arbitrary Galois extension of the number field K, and $w \in \Sigma_L$, one defines D_w, I_w, F_w as before. If v is an unramified place of K, and w is a place of L extending v, we denote by F_v the conjugacy class of F_w in $G = \mathrm{Gal}(L/K)$.

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

If the representation ρ is unramified at v, then the

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

2.2. Čebotarev's density theorem

Let P be a subset of Σ_K. For each integer n, let $a_n(P)$ be the number of $v \in P$ such that $Nv \leq n$. If a is a real number, one says that P has density a if

$$\lim. \frac{a_n(P)}{a_n(\Sigma_K)} = a \quad \text{when} \quad n \longrightarrow \infty .$$

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

$$a_n(P) = a.n/\log(n) + o(n/\log(n)) .$$

Examples

A finite set has density 0. The set of $v \in \Sigma_K$ of degree 1 (i.e. such that Nv is prime) has density 1. The set of ordinary prime numbers whose first digit (in the decimal system, say) is 1 has no density.

We can now state Čebotarev's density theorem:

THEOREM - 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 be the set of places $v \in \Sigma_K$, unramified in L, such that the Frobenius class F_v is contained in X. Then P_X has density equal to Card(X)/Card(G).

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

COROLLARY 1 - For every $g \in G$, there exist infinitely many unramified places $w \in \Sigma_L$ such that $F_w = g$.

For infinite extensions, we have:

COROLLARY 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 Gal(L/K).

b) Let X be a subset of Gal(L/K), stable by conjugation. Assume that the boundary of X has measure zero with respect to the Haar measure μ of X, and normalize μ such that its total mass is 1. Then the set of places $v \notin S$ such that $F_v \subset X$ has a density equal to $\mu(X)$.

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

Exercise

Let G be an ℓ-adic Lie group and let X be an analytic subset of G (i.e. a set defined by the vanishing of a family of analytic functions on G). Show that the boundary of X has measure zero

with respect to the Haar measure of G.

2.3. Rational ℓ-adic representations

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

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

(a) Any element of $\Sigma_K - S$ is unramified with respect to ρ.

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

Remark

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

Examples

The ℓ-adic representations of K given in examples 1, 2, 3 of section 1.2 are rational (even integral) representations. In example 1, one can take for S the set S_ℓ of elements v of Σ_K with $p_v = \ell$; the corresponding Frobenius is Nv, viewed as an element of U_ℓ. In examples 2, 3, one can take for S the union of S_ℓ and the set S_A where A has "bad reduction"; the fact that the corresponding Frobenius has an integral characteristic polynomial (which is independent of ℓ) is a consequence of Weil's results on endomorphisms of abelian varieties (cf. [40] and [12], chap. VII). The rationality of

the cohomology representations is a well-known open question.

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

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

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

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

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

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

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

Proof. Let ρ'_1, ρ'_2 be semi-simple ℓ'-adic representations of K

which are rational and compatible with ρ.

We first prove that $\mathrm{Tr}(\rho_1'(g)) = \mathrm{Tr}(\rho_2'(g))$ for all $g \in G$. Let $H = G/(\mathrm{Ker}(\rho_1') \cap \mathrm{Ker}(\rho_2'))$; the representations ρ_1', ρ_2' may be regarded as representations of H, and it suffices to show that $\mathrm{Tr}(\rho_1'(h)) = \mathrm{Tr}(\rho_2'(h))$ for all $h \in H$. Let $M \subset \overline{K}$ be the fixed field of H. Then by the compatibility of ρ_1', ρ_2' there is a finite subset S of Σ_K such that for all $v \in \Sigma_K - S$, $w \in \Sigma_M$, $w|v$, we have $\mathrm{Tr}(\rho_1'(F_w)) = \mathrm{Tr}(\rho_2'(F_w))$. But, by cor. 2 to Čebotarev's theorem (cf. 2.2) the F_w are dense in H. Hence $\mathrm{Tr}(\rho_1'(h)) = \mathrm{Tr}(\rho_2'(h))$ for all $h \in H$ since $\mathrm{Tr} \circ \rho_1'$, $\mathrm{Tr} \circ \rho_2'$ are continuous.

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

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

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

DEFINITION - For each prime ℓ let ρ_ℓ be a rational ℓ-adic representation of K. The system (ρ_ℓ) is said to be compatible if ρ_ℓ, $\rho_{\ell'}$ are compatible for any two primes ℓ, ℓ'. The system (ρ_ℓ) is said to be strictly compatible if there exists a finite subset S of Σ_K such that:

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

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

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

Examples

The systems of ℓ-adic representations given in examples 1, 2, 3 of section 1.2 are each 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 ρ be a rational ℓ-adic representation. Is it true that $P_{v,\rho}$ has rational coefficients for all v such that ρ is unramified at v?

A somewhat similar question is:

Is any compatible system strictly compatible?

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

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

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

(i) If ρ is abelian (i.e., if $\mathrm{Im}(\rho)$ is abelian), is it true that ρ' is abelian? (We shall see in chapter III that this is true at least if ρ is "locally algebraic".) → [yes: this follows from [63].]

(ii) Is it true that $\mathrm{Im}(\rho)$ and $\mathrm{Im}(\rho')$ are Lie groups of the

same dimension? More optimistically, is it true that there exists a Lie algebra $\underline{g}$ over $\mathbb{Q}$ such that $\mathrm{Lie}(\mathrm{Im}(\rho)) = \underline{g} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, $\mathrm{Lie}(\mathrm{Im}(\rho')) = \underline{g} \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell'}$?

5. Let X be a non-singular projective variety defined over K, and let i be an integer. Is the i-th cohomology representation $H^i_\ell(X_s)$ 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.) → [yes for i=1: see [48] and also [75].]

Remark

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

Exercises

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

Generalize this to λ-adic representations (with respect to a number field E).

2) Let ρ (resp. ρ') be a rational ℓ-adic (resp. ℓ'-adic) representation of K, of degree n. Assume ρ and ρ' are compatible. If $s \in G = \mathrm{Gal}(\overline{K}/K)$, let $\sigma_i(s)$ (resp. $\sigma'_i(s)$) be the

i-th coefficient of the characteristic polynomial of $\rho(s)$ (resp. of $\rho'(s)$). Let $P(X_o, \ldots, X_n)$ be a polynomial with rational coefficients, and let X_P (resp. X'_P) be the set of $s \in G$ such that $P(\sigma_o(s), \ldots, \sigma_n(s)) = 0$ (resp. $P(\sigma'_o(s), \ldots, \sigma'_n(s)) = 0$).

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

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

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

2.4. Representations with values in a linear algebraic group

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

DEFINITION - Let H be a linear algebraic group over Q, and let K be a field. A continuous homomorphism $\rho : \mathrm{Gal}(K_s/K) \longrightarrow H(Q_\ell)$ is called an ℓ-adic representation of K with values in H.

(Note that $H(Q_\ell)$ is, in a natural way, a topological group and even an ℓ-adic Lie group.)

If K is a number field, one defines in an obvious way what it

means for ρ to be unramified at a place $v \in \Sigma_K$; if $w|v$, one defines the Frobenius element $F_{w,\rho} \in H(Q_\ell)$ and its conjugacy class $F_{v,\rho}$. We say, as before, that ρ is rational if

(a) there is a finite set S of Σ_K such that ρ is unramified outside S,

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

Two rational representations ρ, ρ' (for primes ℓ, ℓ') are said to be compatible if there exists a finite subset S of Σ_K such that ρ and ρ' are unramified outside S and such that for any central element $f \in A$ and any $v \in \Sigma_K - S$ 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.

Remarks

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

2. Let V_o be a finite-dimensional vector space over Q, and let GL_{V_o} be the linear algebraic group over Q whose group of points in any commutative Q-algebra k is $\mathrm{Aut}(V_o \otimes_Q k)$; in particular, if $V_\ell = V_o \otimes_Q Q_\ell$, then $GL_{V_o}(Q_\ell) = \mathrm{Aut}(V_\ell)$. If $\phi : H \longrightarrow GL_{V_o}$ is a homomorphism of linear algebraic groups over Q, call ϕ_ℓ the induced homomorphism of $H(Q_\ell)$ into $GL_{V_o}(Q_\ell) = \mathrm{Aut}(V_\ell)$. If ρ is an ℓ-adic representation of $\mathrm{Gal}(\bar{K}/K)$ into $H(Q_\ell)$, one gets by composition a linear ℓ-adic representation $\phi_\ell \circ \rho : \mathrm{Gal}(K_s/K) \longrightarrow \mathrm{Aut}(V_\ell)$. Using the fact that the coefficients of the characteristic polynomial are central functions, one sees that

$\phi_\ell \circ \rho$ is rational if ρ is rational (K a number field). Of course, compatible representations in H give compatible linear representations. We will use this method of constructing compatible representations in the case where H is abelian (see ch. II, 2.5).

2.5. L-functions attached to rational representations

Let K be a number field and let $\rho = (\rho_\ell)$ be a strictly compatible system of rational ℓ-adic representations, with exceptional set S. If $v \notin S$, denote by $P_{v,\rho}(T)$ the rational polynomial $\det(1 - F_{v,\rho_\ell} T)$, for any $\ell \neq p_v$; by assumption, this polynomial does not depend on the choice of ℓ. Let s be a complex number. One has:

$$P_{v,\rho}(Nv)^{-s}) = \det(1 - F_{v,\rho}/(Nv)^s)$$

$$= \prod_i (1 - \lambda_{i,v}/(Nv)^s),$$

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:

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

This is a formal Dirichlet series $\sum_{n=1}^{\infty} a_n/n^s$, with coefficients in Q. In all known cases, there exists a constant k such that $|\lambda_{i,v}| \leq (Nv)^k$, and this implies that L_ρ is convergent in some half plane $R(s) > C$; one conjectures it extends to a meromorphic function in the whole

plane. When ρ comes from ℓ-adic cohomology, there are some further conjectures on the zeros and poles of L_ρ, cf. Tate [36]; these, as indicated by Tate, may be applied to get equidistribution properties of the Frobenius elements, cf. Appendix.

Remarks

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

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

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

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

There is considerable numerical evidence for this, based on the congruence properties of τ (Swinnerton-Dyer, unpublished); of course, such a ρ would be of dimension 2, and its exceptional set S would be empty. → [proved by Deligne: see [49], [50], [65], ...]

More generally, there seems to be a close connection between

modular forms, such as $\Sigma \tau(n) x^n$, and rational (or algebraic) ℓ-adic representations; see for instance Shimura [33] and Weil [45].

→ [see also [49], [51], [65], [66], [68], [84].]

Examples

1. If G acts through a finite group, L_ρ is an Artin (non abelian) L-series, at least up to a finite number of factors (cf. [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 ρ is the system associated with an elliptic curve E (cf. 1.2), the corresponding L-function gives the non-trivial part of the zeta function of E. The symmetric powers of ρ give the zeta functions of the products $E \times \ldots \times E$, cf. Tate [36].

APPENDIX

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 $\|f\| = \operatorname{Sup}_{x \in X} |f(x)|$. For each $x \in X$ let δ_x be the Dirac measure associated to x; if $f \in C(X)$, we have $\delta_x(f) = f(x)$.

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

$$\mu_n = (\delta_{x_1} + \ldots + \delta_{x_n})/n$$

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

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

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

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

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

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

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

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

$$\liminf (n - n_U)/n \geq \mu(X - U) .$$

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

Examples

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

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

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

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

The map $C(X) \longrightarrow C(G)$ is an isomorphism of $C(X)$ onto the space of central functions on G; by the Peter-Weyl theorem, the

irreducible characters χ of G generate a dense subspace of C(X). Hence the proposition follows from lemma 1.

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

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

This follows from Prop. 2 and the following facts:

$$\mu(\chi) = 0 \quad \text{if } \chi \text{ is irreducible} \neq 1$$
$$\mu(1) = 1 .$$

COROLLARY 2 - (H. Weyl [46]) Let G = R/Z, and let μ be the normalized Haar measure on G. Then (x_n) is μ-equidistributed if and only if for any integer $m \neq 0$ we have

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

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

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, $v \in \Sigma$, be a family of elements of X, indexed by a denumerable set Σ, and let $v \longmapsto Nv$ be a function on Σ with values in the set of integers ≥ 2.

We make the following hypotheses:

(1) The infinite product $\prod_{v \in \Sigma} \frac{1}{1-(Nv)^{-s}}$ converges for every $s \in C$ with $R(s) > 1$, and extends to a meromorphic function on $R(s) \geq 1$ having neither zero nor pole except for a simple pole at $s = 1$.

(2) Let ρ be an irreducible representation of G, with character χ, and put

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

Then this product converges for $R(s) > 1$, and extends to a meromorphic function on $R(s) \geq 1$ 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 $v \in \Sigma$ with $Nv \leq n$ is equivalent to $n/\log n$ (as $n \longrightarrow \infty$).

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

$$\sum_{Nv \leq n} \chi(x_v) = c_\chi \, n/\log n + o(n/\log n) \qquad (n \longrightarrow \infty).$$

The theorem results, by a standard argument, from the theorem of Wiener-Ikehara, cf. A.3 below.

Suppose now that the function $v \longmapsto Nv$ has the following property:

(3) There exists a constant C such that, for every $n \in Z$, the number of $v \in \Sigma$ with $Nv = n$ is $\leq C$.

One may then arrange the elements of Σ as a sequence $(v_i)_{i \geq 1}$ so that $i \leq j$ implies $Nv_i \leq Nv_j$ (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 Σ. Applying theorem 1 and proposition 2, we obtain

THEOREM 2 - The elements x_v ($v \in \Sigma$) are equidistributed in X with respect to a measure μ such that for any irreducible character χ of G we have

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

COROLLARY - The elements x_v ($v \in \Sigma$) are equidistributed for the 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 Σ be the set of unramified places of K, let x_v be the Frobenius conjugacy class defined by $v \in \Sigma$, and let Nv 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 $L(s,1)$ 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 $R(s) = 1$, cf. for instance Lang [13], chap. VII; for a proof of (2), cf. Artin [1], p. 121. Hence theorem 2 gives the equidistribution of the Frobenius elements, i.e. the Čebotarev density theorem, cf. 2.2.

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

(*) The homomorphism ρ maps the group C^0 of idèles of volume 1 onto G.

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

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

Remark

This example (essentially due to Hecke) is given in Lang (loc. cit., ch. VIII, §5) except that Lang has replaced the condition (*) by the condition "ρ is surjective", which is insufficient. This led him to affirm that, for example, the sequence (log p) (and also the sequence (log n)) is uniformly distributed modulo 1; however,

one knows that this sequence is not uniformly distributed for any measure on R/Z (cf. Pólya-Szegö [22], p. 179-180).

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

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

On the other hand, let $G = SU(2)$ be the Lie group of 2×2 unitary matrices with determinant 1. Any element of the space X of conjugacy classes of G contains a unique matrix of the form $\begin{pmatrix} e^{i\phi} & 0 \\ 0 & e^{-i\phi} \end{pmatrix}$, $0 \leq \phi \leq \pi$. 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 ρ_m of the natural representation ρ_1 of degree 2.

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

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

If we put:

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

we have

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

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

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

A. 3. Proof of theorem 1

The logarithmic derivative of L is

$$L'/L = -\sum_{v,\, m\geq 1} \frac{\chi(x_v^m)\log(Nv)}{(Nv)^{ms}} ,$$

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

$$\prod_{i,v} \frac{1}{1 - \lambda_v^{(i)}(Nv)^{-s}}$$

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

$$\sum_{v,\, m \geq 2} \frac{\log(Nv)}{|(Nv)^{ms}|}$$

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

$$\sum_v \frac{\log(Nv)}{(Nv)^{\sigma}} < \infty$$

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

$$(\text{Constant}) \times \sum_v \frac{1}{(Nv)^{\sigma+\varepsilon}} \qquad (\varepsilon > 0) .$$

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

$$\prod_v \frac{1}{1 - (Nv)^{-\sigma}}$$

shows that

$$\sum_v \frac{1}{(Nv)^{\sigma}} < \infty$$

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

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

where $\phi(s)$ is holomorphic for $R(s) > \frac{1}{2}$. Moreover, by hypothesis,

L'/L can be extended to a meromorphic function on $R(s) \geq 1$ 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], p. 123):

THEOREM - *Let* $F(s) = \Sigma a_n/n^s$ *be a Dirichlet series with complex coefficients. Suppose there exists a Dirichlet series* $F^+(s) = \Sigma a_n^+/n^s$ *with positive real coefficients such that*

(a) $|a_n| \leq a_n^+$ *for all* n;

(b) *The series* F^+ *converges for* $R(s) > 1$;

(c) *The function* F^+ *(resp.* F*) can be extended to a meromorphic function on* $R(s) \geq 1$ *having no poles except (resp. except possibly) for a simple pole at* $s=1$ *with residue* $c_+ > 0$ *(resp.* c*).*

Then

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

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

One applies this theorem to

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

and we take for F^+ the series

$$d \sum \frac{\log(Nv)}{(Nv)^s},$$

where d is the degree of the given representation ρ; this is possible

since $\chi(x_v)$ is a sum of d complex numbers of absolute value 1, hence $|\chi(x_v)| \leq d$; moreover, the series

$$\sum_v \frac{\log(Nv)}{(Nv)^s}$$

differs from the logarithmic derivative of

$$\prod \frac{1}{1 - (Nv)^{-s}}$$

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

$$\sum_{Nv \leq n} \chi(x_v)\log(Nv) = c_\chi n + o(n) \qquad (n \longrightarrow \infty).$$

Consequently, by the Abel summation trick (cf. [13], p. 124, prop. 1),

$$\sum_{Nv \leq n} \chi(x_v) = c_\chi n/\log n + o(n/\log n) \qquad (n \longrightarrow \infty),$$

and in particular,

$$\sum_{Nv \leq n} 1 = n/\log n + o(n/\log n) \qquad (n \longrightarrow \infty).$$

Hence,

$$\Big(\sum_{Nv \leq n} \chi(x_v)\Big)\Big/\Big(\sum_{Nv \leq n} 1\Big) \longrightarrow c_\chi \qquad \text{as} \qquad n \longrightarrow \infty,$$

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

CHAPTER II

THE GROUPS S_m

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

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 T

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

to $G_{m/\bar{Q}} \times \ldots \times G_{m/\bar{Q}}$ (d times). More precisely, let Γ be the set of embeddings of K into $\bar{Q}$; each $\sigma \in \Gamma$ extends to a homomorphism $K \otimes_Q \bar{Q} \to \bar{Q}$, hence defines a morphism $[\sigma]: T_{/\bar{Q}} \to G_{m/\bar{Q}}$. The collection of all $[\sigma]$'s gives the isomorphism $T_{/\bar{Q}} \to G_{m/\bar{Q}} \times \ldots \times G_{m/\bar{Q}}$. Moreover, the $[\sigma]$'s form a basis of the character group $X(T) = \mathrm{Hom}_{\bar{Q}}(T_{/\bar{Q}}, G_{m/\bar{Q}})$ of T. Note that the Galois group $\mathrm{Gal}(\bar{Q}/Q)$ 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 T

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

Exercise

a. Let K be quadratic over Q, so that dim T = 2. Let E be the group of units of K. Show that T_E 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.

(For more examples, see 3.3.)

1.3. Enlarging groups

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

(*) $$0 \longrightarrow Y_1 \longrightarrow Y_2 \longrightarrow Y_3 \longrightarrow 0$$

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

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

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 $A \longrightarrow B$ 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 morphisms $A \longrightarrow B'$, $Y_2 \longrightarrow B'(k)$ such that (a) is true (with B replaced by B'), there exists a unique algebraic morphism $f: B \longrightarrow B'$ such that the given maps $A \longrightarrow B'$ and $Y_2 \longrightarrow B(k)$ 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.)

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

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

with $c(y, y') \in Y_1$; the cochain c is a 2-cocycle defining the extension (*). 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

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

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

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

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

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

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

and a commutative diagram

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

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

Remarks

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

Exercise

a) Let k' be a commutative k-algebra, with $k' \neq 0$, and 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 $\mathrm{Spec}(k')$ 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 Σ_K of finite places of the number field K. Let now Σ_K^∞ be the set of equivalence classes of archimedian absolute values of K, and let $\overline{\Sigma}_K$ be the union of Σ_K and Σ_K^∞. If $v \in \overline{\Sigma}_K$ then K_v denotes the completion of K with respect to v. For $v \in \Sigma_K^\infty$ we have $K_v = R$ or $K_v = C$, and K_v is ultrametric if $v \in \Sigma_K$. For $v \in \Sigma_K$, the group of units of K_v is denoted by U_v. The idèle group I of K is the subgroup of $\prod_{v \in \overline{\Sigma}_K} K_v^*$ consisting of the families (a_v) with $a_v \in U_v$, for almost all v; it is given a topology by decreeing that the subgroup (with the product topology)

$$\prod_{v \in \Sigma_K^\infty} K_v^* \times \prod_{v \in \Sigma_K} U_v$$

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

Let S be a finite subset of Σ_K. Then by a modulus of support S we mean a family $m = (m_v)_{v \in S}$ where the m_v are integers ≥ 1.

If $v \in \overline{\Sigma}_K$ and m is a modulus of support S, we let $U_{v,m}$ denote the connected component of K_v^* if $v \in \Sigma_K^\infty$, 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 $v \in \Sigma_K - S$. The group $U_m = \prod_v U_{v,m}$ is an open subgroup of I.

If E is the group of units of K, let $E_m = E \cap U_m$. The subgroup E_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_m for a suitable modulus m.)

Let I_m be the quotient I/U_m and C_m the quotient $I/K^*U_m = C/$ (Image of U_m in C). One then has the exact sequence

$$1 \longrightarrow K^*/E_m \longrightarrow I_m \longrightarrow C_m \longrightarrow 1 .$$

The group C_m is finite; in fact, the image of U_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_m's, hence C/D is the projective limit of the C_m's. Class field theory (cf. for instance Cassels-Fröhlich [6]), gives an isomorphism of $C/D = \varprojlim C_m$ onto the Galois group G^{ab} of the maximal abelian extension of K.

Remark

A more classical definition of C_m is as follows. Let Id_S be the group of fractional ideals of K prime to S, and $P_{S,m}$ the subgroup of principal ideals (γ), where γ is totally positive and

$\gamma \equiv 1 \bmod \mathfrak{m}$ (i.e. γ belongs to $U_{v,\mathfrak{m}}$ for all $v \in S$ and $v \in \Sigma_K^\infty$). Let $Cl_{\mathfrak{m}} = Id_S / P_{S,\mathfrak{m}}$. We have the exact sequence:

$$1 \to P_{S,\mathfrak{m}} \to Id_S \to Cl_{\mathfrak{m}} \to 1.$$

For each $\underline{a} = \prod_{v \notin S} v^{a_v} \in Id_S$, choose an idèle $\alpha = (\alpha_v)$, with $\alpha_v \in U_{v,\mathfrak{m}}$ if $v \in S$ or $v \in \Sigma_K^\infty$, and $v(\alpha_v) = a_v$ if $v \in \Sigma_K - S$. The image of α in $I_{\mathfrak{m}} = I/U_{\mathfrak{m}}$ depends only on $\underline{a}$. We then get a homomorphism $g: Id_S \to I_{\mathfrak{m}}$. One checks readily that g extends to a commutative diagram

$$\begin{array}{ccccccccc} 1 & \to & P_{S,\mathfrak{m}} & \to & Id_S & \to & Cl_{\mathfrak{m}} & \to & 1 \\ & & \downarrow & & \downarrow g & & \downarrow f & & \\ 1 & \to & K^*/E_{\mathfrak{m}} & \to & I_{\mathfrak{m}} & \to & C_{\mathfrak{m}} & \to & 1 \end{array},$$

and that $f: Cl_{\mathfrak{m}} \to C_{\mathfrak{m}}$ is an isomorphism; hence $C_{\mathfrak{m}}$ 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 (*) the sequence

$$1 \to K^*/E_{\mathfrak{m}} \to I_{\mathfrak{m}} \to C_{\mathfrak{m}} \to 1$$

and for A the algebraic group $T_{\mathfrak{m}} = T/\overline{E}_{\mathfrak{m}}$, where $E_{\mathfrak{m}}$ is as before, T is the torus $R_{K/\mathbb{Q}}(G_{m/K})$ defined in 1.1, and $\overline{E}_{\mathfrak{m}}$ is the

Zariski closure of E_m in T, cf. 1.2.

The construction of 1.3 now yields a $\mathbb{Q}$-algebraic group S_m with an algebraic morphism $T_m \to S_m$ and a group homomorphism $\varepsilon: I_m \to S_m(\mathbb{Q})$. The sequence

$$1 \to T_m \to S_m \to C_m \to 1$$

is exact (C_m being identified with the corresponding constant algebraic group) and the diagram

$$\begin{array}{ccccccc} 1 & \to & K^*/E_m & \to & I_m & \to & C_m \to 1 \\ & & \downarrow & & \downarrow \varepsilon & & \downarrow \mathrm{id.} \\ 1 & \to & T_m(\mathbb{Q}) & \to & S_m(\mathbb{Q}) & \to & C_m \to 1 \end{array} \qquad (**)$$

is commutative.

Remark

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

Exercises

1) Let $\overline{E}_m(\mathbb{Q})$ be the Zariski-closure of E_m in $K^* = T(\mathbb{Q})$. Show that the kernel of $\varepsilon_m : I/U_m \to S_m(\mathbb{Q})$ is the image of $\overline{E_m}(\mathbb{Q}) \to I/U_m$.

2) Let $H_{m'/m}$ be the kernel of $S_{m'} \to S_m$, where $m' \geq m$.

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

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

$$1 \to (E_m \cap \overline{E}_{m'}, (Q))/E_{m'} \to U_m / U_{m'} \to H_{m'/m} \to 1.$$

2.3. The canonical ℓ-adic representation with values in S_m

Let m be a modulus, and let ℓ be a prime number. Let $\varepsilon: I \to I_m \to S_m(Q)$ be the homomorphism defined in 2.2. Let $\pi: T \to S_m$ be the algebraic morphism $T \to T_m \to S_m$; by taking points with values in Q_ℓ, π defines a homomorphism

$$\pi_\ell : T(Q_\ell) \to S_m(Q_\ell).$$

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

$$\alpha_\ell = \pi_\ell \circ pr_\ell : I \to T(Q_\ell) \to S_m(Q_\ell)$$

is a continuous homomorphism.

LEMMA - α_ℓ and ε coincide on K^*.

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

Now, let $\varepsilon_\ell : I \longrightarrow S_m(\mathbb{Q}_\ell)$ be defined by

$$(***) \qquad \varepsilon_\ell(a) = \varepsilon(a)\alpha_\ell(a^{-1})$$

$$\text{i.e.} \qquad \varepsilon_\ell = \varepsilon \cdot \alpha_\ell^{-1}$$

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

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

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

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

PROPOSITION

a) The representation $\varepsilon_\ell : G^{ab} \longrightarrow S_m(\mathbb{Q}_\ell)$ is a rational representation with values in S_m.

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

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

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

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

COROLLARY - The representations ε_ℓ form a system of strictly compatible ℓ-adic representations with values in $S_{\mathfrak{m}}$.

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

Remark

By construction, $\varepsilon_\ell : I \longrightarrow S_{\mathfrak{m}}(\mathbb{Q}_\ell)$ is given by $x \longrightarrow \pi_\ell(x^{-1})$ on the open subgroup $U_{\ell,\mathfrak{m}} = \prod_{v \mid \ell} U_{v,\mathfrak{m}}$ of K_ℓ^*.

Hence, $\mathrm{Im}(\varepsilon_\ell)$ contains $\pi_\ell(U_{\ell,\mathfrak{m}}) \subset T_{\mathfrak{m}}(\mathbb{Q}_\ell) \subset S_{\mathfrak{m}}(\mathbb{Q}_\ell)$, and is an open subgroup of $S_{\mathfrak{m}}(\mathbb{Q}_\ell)$. This open subgroup maps onto $C_{\mathfrak{m}}$, as remarked above. These properties imply, in particular, that $\mathrm{Im}(\varepsilon_\ell)$ is Zariski-dense in $S_{\mathfrak{m}}$.

Exercises

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

a) Show that $E_m = \{1\}$, $C_m = \{1\}$, hence $T_m = S_m = G_m$ and $S_m(Q) = Q^*$, $S_m(Q_\ell) = Q_\ell^*$.

b) Show that I is the direct product of its subgroups I_m and Q^*; hence any $a \in I$ may be written as

$$a = u.\gamma \qquad u \in U_m \ , \ \gamma \in Q^* .$$

Show that, if $a = (a_p)$, one has

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

c) Show that

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

and

$$F_p = p .$$

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

(2) Let $K = Q$, $\mathrm{Supp}(m) = \{2\}$ and $m_2 = 1$. Show that the groups E_m, C_m, T_m, S_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 $X(H) = \mathrm{Hom}_{\overline{k}}(H_{/\overline{k}}, G_{m/\overline{k}})$ be the group of characters of H (of degree 1). Here we write the characters of X(H) multiplicatively. The group $G = \mathrm{Gal}(\overline{k}/k)$ acts on X(H).

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

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

where $\overline{k}[X(H)]$ is the group algebra of X(H) over $\overline{k}$. This is a G-homomorphism if the action of G is defined by $s(\Sigma a_\chi \chi) = \Sigma s(a_\chi) s(\chi)$ for $a_\chi \in \overline{k}$ and $\chi \in X(H)$. It is well-known (linear independence of characters) that α is <u>injective</u>. It is <u>bijective</u> if and only if H is a group of multiplicative type (cf. 1.3, remark 2). Hence we may identify $\overline{k}[X(H)]$ with a subalgebra of $\overline{\Lambda}$.

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

$$\phi: H \longrightarrow GL_V$$

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

$$\theta_\phi = \Sigma n_\chi(\phi)\chi$$

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

We have $\theta_\phi(h) = Tr(\phi(h))$ for any point h of H (with value in any commutative k-algebra). Let $Rep_k(H)$ 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 $Rep_k(H) \longrightarrow Rep_{k_1}(H_{/k_1})$ which is easily seen to be injective. We say that an element of $Rep_{k_1}(H_{/k_1})$ can be defined over k, if it is in the image of this map.

PROPOSITION 1 - The map $\phi \longmapsto \theta_\phi$ defines a bijection between $Rep_k(H)$ and the set of elements $\theta = \Sigma n_\chi \chi$ of $Z[X(H)]$ which satisfy:

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

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

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

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

The fixed field k_χ of $G(\chi)$ in $\bar{k}$ is the smallest subfield of $\bar{k}$ such that $\chi \in \Lambda \otimes k_\chi$. Consider χ as a representation of degree 1 of $H_{/k_\chi}$. One gets, by restriction of scalars to k, a representation

ϕ of H of degree $[k_\chi : k]$. One sees easily that the trace θ_ϕ of ϕ is equal to θ. The surjectivity of $\phi \mapsto \theta_\phi$ now follows from the fact that any θ satisfying (a) and (b) is a sum of elements of the form (*) above.

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

(c) We return now to the groups S_m :

PROPOSITION 2 - Let k_1 be an extension of k and let $\phi \in \mathrm{Rep}_{k_1}(S_m/k_1)$. The following properties are equivalent:

(i) ϕ can be defined over k,

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

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

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

LEMMA - The set of Frobeniuses F_v, $v \in \Sigma$, is dense in S_m for the Zariski topology.

Proof. Let X be the set of all F_v's, $v \in \Sigma$, and let ℓ be a prime number. Let $\overline{X} \subset S_m$ (resp. $\overline{X}_\ell \subset S_m(Q_\ell)$) the closure of X in the Zariski topology (resp. ℓ-adic topology). It is clear that

$\overline{X}_\ell \subset \overline{X}(\Omega_\ell)$. On the other hand, Čebotarev's theorem (cf. Chapter I, 2.2) implies that $\overline{X}_\ell = \mathrm{Im}(\varepsilon_\ell)$ (cf. 2.3). The set $\mathrm{Im}(\varepsilon_\ell)$, however, is Zariski dense in S_m (cf. Remark in 2.3). Hence $\overline{X} = S_m$, which proves the lemma.

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

Exercise

Show that the characters of S_m correspond in a one-one way to the homomorphisms $\chi : I \longrightarrow \overline{Q}^*$ having the following two properties:

(a) $\chi(x) = 1$ if $x \in U_m$

(b) For each embedding σ of K into $\overline{Q}$, there exists an integral number $n(\sigma)$ such that

$$\chi(x) = \prod_{\sigma \in \Gamma} \sigma(x)^{n(\sigma)}$$

for all $x \in K^*$.

2.5. ℓ-adic representations associated to a linear representation of S_m

1) The ℓ-adic case

Let V_ℓ be a finite-dimensional Q_ℓ-vector space and

$$\phi: S_{m/Q_\ell} \longrightarrow GL_{V_\ell}$$

a linear representation of S_{m/Q_ℓ} in V_ℓ. This defines a homomorphism

$$\phi: S_m(Q_\ell) \longrightarrow GL_{V_\ell}(Q_\ell) = \mathrm{Aut}(V_\ell)$$

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

By composition with the map $\varepsilon_\ell: G^{ab} \longrightarrow S_m(Q_\ell)$ defined in 2.3, we get a map

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

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

PROPOSITION - a) The representation ϕ_ℓ is semi-simple.

b) Let $v \in \Sigma_k$, with $v \notin \mathrm{Supp}(m)$ and $p_v \neq \ell$. Then ϕ_ℓ is unramified at v; the corresponding Frobenius element $F_{v,\phi_\ell} \in \mathrm{Aut}(V_\ell)$ is equal to $\phi(F_v)$, where F_v denotes the element of $S_m(Q)$ defined in 2.3.

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

Since S_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 Proposition 2 of 2.4.

Remark

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

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

e) Let $\phi_T: T_{/Q_\ell} \to GL_{V_\ell}$ be defined by composing $T_{/Q_\ell} \to S_{m/Q_\ell}$ with ϕ. If x belongs to the open subgroup $U_{\ell,m} = \prod_{v|\ell} U_{v,m}$ of $T(Q_\ell)$, one has

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

These properties follow readily from those of ε_ℓ.

2) The rational case

Let now V_o be a finite dimensional vector space over Q and $\phi_o: S_m \to GL_{V_o}$ a linear representation of S_m. For each prime number ℓ we may apply the preceding construction to the representation $\phi_{o/\ell}: S_{m/Q_\ell} \to GL_{V_\ell}$, where $V_\ell = V_o \otimes Q_\ell$;

we then get an ℓ-adic representation $\phi_\ell : G^{ab} \longrightarrow \mathrm{Aut}(V_\ell)$.

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

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

3) There exist infinitely many primes ℓ such that ϕ_ℓ is diagonalizable over Q_ℓ.

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 Q over which ϕ_o becomes diagonalizable. If ℓ is a prime number which splits completely in E, one can embed E into Q_ℓ and this shows that ϕ_ℓ is diagonalizable. Assertion 3) now follows from the well-known fact that there exist infinitely many such ℓ (this is, for instance, a consequence of Čebotarev's theorem, cf. Chap. I, 2.2).

Remark

The Frobenius elements $\phi_o(F_v) \in \mathrm{Aut}(V_o)$ can also be defined using the homomorphism

$$\phi_o \circ \varepsilon : I \longrightarrow S_{\mathfrak{m}}(Q) \longrightarrow \mathrm{Aut}(V_o).$$

Note that their eigenvalues generate a finite extension of Q; indeed they are contained in any field over which ϕ_o can be brought in diagonal form.

Exercises

1) Let $\phi_o : S_m \longrightarrow GL_{V_o}$ be a linear representation of S_m, and let ℓ be a prime number.

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

b) Let $\underline{s}_m$ be the Lie algebra of S_m and $\phi_o(\underline{s}_m)$ be its image by ϕ_o, i.e. the Lie algebra of $\phi_o(S_m)$. Show that the Lie algebra of the ℓ-adic Lie group $\mathrm{Im}(\phi_\ell)$ is $\phi_o(\underline{s}_m) \otimes Q_\ell$. (Use the fact that $\mathrm{Im}(\varepsilon_\ell)$ is open in $S_m(Q_\ell)$, cf. 2.3.)

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

$$N : S_m \longrightarrow G_m$$

such that $N(F_v) = Nv \in Q^*$ for all $v \notin \mathrm{Supp}(\mathfrak{m})$.

b) Show that the morphism $T \longrightarrow S_m \xrightarrow{N} G_m$ is the one induced by the norm map from K to Q.

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

2.6. Alternative construction

Let $\phi_o : S_m \longrightarrow GL_{V_o}$ be as in 2.5. If we compose ϕ_o with the map $\varepsilon : I \longrightarrow S_m(Q)$ defined in 2.2, we obtain a homomorphism

$$\phi_o \circ \varepsilon : I \longrightarrow GL_{V_o}(Q) = \mathrm{Aut}(V_o).$$

Conversely:

PROPOSITION - Let $f: I \longrightarrow \mathrm{Aut}(V_o)$ be a homomorphism. There exists a $\phi_o: S_m \longrightarrow GL_{V_o}$ such that $\phi_o \circ \varepsilon = f$ if and only if the following conditions are satisfied:

(a) The kernel of f contains U_m

(b) There exists an algebraic homomorphism $\psi: T \longrightarrow GL_{V_o}$ such that $\psi(x) = f(x)$ for every $x \in K^* = T(Q)$.

Moreover, such a ϕ_o is unique.

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

$$T \longrightarrow T_m \longrightarrow GL_{V_o} .$$

By the universal property of S_m (cf. 1.3 and 2.2), the maps $I/U_m \longrightarrow GL_{V_o}(Q)$ and $T_m \longrightarrow GL_{V_o}$ define an algebraic morphism $\phi_o: S_m \longrightarrow GL_{V_o}$, and one checks easily that ϕ_o has the required properties, and is unique.

Remark

Since U_m is open, property (a) implies that f is continuous

with respect to the discrete topology of $\mathrm{Aut}(V_o)$. Conversely, any continuous homomorphism $f: I \longrightarrow \mathrm{Aut}(V_o)$ is trivial on some U_m; moreover, there is a smallest such m; it is called the conductor of f.

Exercise

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

(a) The F_v's commute pairwise.

(b) There exists an algebraic morphism $\psi: T \longrightarrow GL_{V_o}$ such that $\psi(\alpha) = \prod F_v^{v(\alpha)}$ for $\alpha \in K^*$, $\alpha \equiv 1 \pmod{m}$, and $\alpha > 0$ at each real place.

Show that there exists an algebraic morphism $\phi_o: S_m \longrightarrow GL_{V_o}$ for which the Frobenius elements are equal to the F_v's.

2.7. The real case

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

Let $\pi: T \longrightarrow S_m$ be the canonical map defined in 2.3, and let

$$\pi_\infty: T(\mathbf{R}) \longrightarrow S_m(\mathbf{R})$$

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

factor; the map

$$\alpha_\infty = \pi_\infty \circ pr_\infty : I \longrightarrow T(R) \longrightarrow S_m(R)$$

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

$$\varepsilon_\infty : I \longrightarrow S_m(R)$$

by

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

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

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

When one composes $\varepsilon_\infty : C \longrightarrow S_m(R)$ with a complex character $S_{m/C} \longrightarrow G_{m/C}$, one gets a homomorphism $C \longrightarrow C^*$, i.e. a Grössencharakter of K, in the sense of Hecke. It is easily seen that the characters obtained in this way coincide with the "Grössencharakter of type (A_o)" of Weil (cf. [35], [41]), whose conductor divide m.

Exercise

Let

$$e: I \longrightarrow S_m(\mathbb{R}) \times \prod_{\ell} S_m(\mathbb{Q}_\ell)$$

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

a) Show that the image of e is contained in the subgroup $S_m(A)$ of $S_m(\mathbb{R}) \times \prod_{\ell} S_m(\mathbb{Q}_\ell)$, where A denotes the ring of adèles of $\mathbb{Q}$, and that $e: I \longrightarrow S_m(A)$ is continuous (for the natural topology of the adelized group $S_m(A)$).

b) Let $\pi_A: T(A) \longrightarrow S_m(A)$ be the map defined by $\pi: T \longrightarrow S_m$. Show that, if one identifies $T(A)$ with I in the obvious way, one has

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

where $\varepsilon: I \longrightarrow S_m(\mathbb{Q}) \subset S_m(A)$ is the map defined in 2.3. [Note that this gives an alternate definition of the ε_ℓ's.]

c) Show that $e(I)$ is not open in $S_m(A)$ if $C_m \neq \{1\}$.

2.8. An example: complex multiplication of abelian varieties

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

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

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

$$i: E \longrightarrow \mathrm{End}_K(A)_o$$

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

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

LEMMA - V_ℓ is a free E_ℓ-module of rank 1.

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

$$\rho_\ell: \mathrm{Gal}(\overline{K}/K) \longrightarrow E_\ell^* .$$

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

THEOREM 1 - (a) The system (ρ_ℓ) is a strictly compatible system of rational ℓ-adic representations of K with values in T_E (in the

sense of Chap. I, 2.4).

(b) There is a modulus m and a morphism

$$\phi: S_m \longrightarrow T_E$$

such that ρ_ℓ is the image by ϕ of the canonical system (ε_ℓ) attached to S_m, cf. 2.3.

Moreover, the restriction of ϕ to T_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 $j: K \longrightarrow \mathrm{End}_E(t)$. In particular, if $x \in K^*$, $\det_E j(x)$ is an element of E^*; the map $\det_E j: K^* \longrightarrow E^*$ is clearly the restriction of an algebraic morphism $\delta: T \longrightarrow T_E$.

THEOREM 2 - The map $\delta: T \longrightarrow T_E$ coincides with the composition map $T \longrightarrow T_m \longrightarrow S_m \xrightarrow{\phi} T_E$.

Example

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 $E \longrightarrow K$. The map $\det_E j: K^* \longrightarrow E^*$ 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 $v \in \Sigma_K$ where A has "bad reduction". If $v \notin S$, and

$\ell \neq p_v$, one shows easily that ρ_ℓ is unramified at v (the converse is also true, see [32]); moreover the corresponding Frobenius element F_{v,ρ_ℓ} may be identified with the Frobenius endomorphism F_v of the reduced variety $\tilde{A}_v$. But F_v commutes with E in $\mathrm{End}(\tilde{A}_v)_0$ and the commuting algebra of E in $\mathrm{End}(\tilde{A}_v)_0$ is E itself (cf. [34], p. 39). Hence F_v belongs to $E^* = T_E(Q)$ and this implies (a).

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

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

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

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

This is essentially what is proved in [34], p. 148, 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 " $\prod_\alpha N_{K/K^*}(x)^{\psi_\alpha}$ ".

Remark

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

Let ℓ be a prime integer distinct from any of the p_v, $v \in S$. One then sees that the Galois-module V_ℓ is of Hodge-Tate type in the sense of Chapter III, 1.2 (indeed, the corresponding local modules

are associated with ℓ-divisible groups, and one may apply Tate's theorem [39]). Hence ρ_ℓ is "locally algebraic" (Chapter III, loc. cit.), and using the theorem of Chapter III, 2.3 one sees it defines a morphism $\phi: S_m \to T_E$. One has $\phi \circ \varepsilon_\ell = \rho_\ell$ by construction; the same is true for any prime number ℓ', since $\phi \circ \varepsilon_{\ell'}$ and $\rho_{\ell'}$ have the same Frobenius elements for almost all v. This proves part (b) of Theorem 1. As for Theorem 2, one uses the explicit form of the Hodge-Tate decomposition of V_ℓ, as given by Tate [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 ω is a complex place of $\bar{Q}$, the completion of $\bar{Q}$ with respect to ω is isomorphic to C; the decomposition group of ω is thus cyclic of order 2; its non-trivial element will be denoted by c_ω (the "Frobenius at the infinite place ω"). The c_ω's are conjugate in $G = \mathrm{Gal}(\bar{Q}/Q)$; let C_∞ denote their conjugacy class. (By a theorem of Artin [1], p. 257, the elements of C_∞ are the only non-trivial elements of finite order in G.)

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

$$Y^o = Y^G = \{y \in Y \mid gy = y \quad \text{for all} \quad g \in G\},$$

$$Y^- = \{y \in Y \mid cy = -y \quad \text{for all} \quad c \in C_\infty\}$$

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

More explicitly, if $\sigma \in \Gamma$ is an embedding of K into $\bar{Q}$, let $[\sigma] \in X(T)$ be the corresponding character of T; the $[\sigma]$'s, $\sigma \in \Gamma$, form a basis of $X(T)$ and $g.[\sigma] = [g.\sigma]$ if $g \in G$. The space Y^o is generated by the norm element $\sum_{\sigma \in \Gamma} [\sigma]$, and its G-invariant supplement is $Y^- \oplus Y^+ = \{ \sum_{\sigma \in \Gamma} b_\sigma [\sigma] \mid b_\sigma \in Q, \sum_{\sigma \in \Gamma} b_\sigma = 0 \}$. Hence, any character $\chi \in X(T)$ can be written in the form

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

$$a, b_\sigma \in Q, \ \Sigma b_\sigma = 0, \ a + b_\sigma \in Z .$$

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

$$Y^- = \{ \Sigma b_\sigma [\sigma] \mid b_\sigma \in Q, \ \Sigma b_\sigma = 0, \ b_{c\sigma} = -b_\sigma \text{ for}$$

$$\text{all } c \in C_\infty \text{ and } \sigma \in \Gamma \}.$$

On the other hand, the projection $T \longrightarrow T_m$ defines an injection of $X(T_m)$ into $X(T)$; we identify $X(T_m)$ with its image under this injection.

PROPOSITION - $X(T_m) \otimes_Z Q = Y^o \oplus Y^-$.

This follows from Appendix, A. 2.

COROLLARY 1 - The character group $X(T_m)$ is a sublattice of finite index of $X(T) \cap (Y^o \oplus Y^-)$.

COROLLARY 2 - If $\chi \in X(T_m)$ is written in the form (*), then $2a \in Z$.

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

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

3.2. The morphism $j^*: G_m \to T_m$

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 $a, b_\sigma \in Q$, $\Sigma b_\sigma = 0$, $2a \in Z$. Hence $\chi \mapsto 2a$ defines a homomorphism $j: X(T_m) \to X(G_m) = Z$ and we obtain by duality a morphism of algebraic groups $j^*: G_m \to T_m$. If $\phi_o: S_m \to GL_{V_o}$ is a representation of S_m, we obtain by composition with j^* a morphism of algebraic groups $G_m \to GL_{V_o}$. This representation of G_m defines (and is defined by) a grading $V_o = \sum_{i \in Z} V_o^{(i)}$ of V_o; recall that G_m acts on $V_o^{(i)}$ by means of the character $i \in Z = X(G_m)$.

We say that V_o is homogeneous of degree n if $V_o = V_o^{(n)}$.

Remark

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

Exercise

1) Let $N: S_m \to G_m$ be the morphism defined in Exercise 2 of 2.5. Show that $N \circ j: G_m \to S_m \to G_m$ is $\lambda \mapsto \lambda^2$. Show that any morphism $S_m \to G_m$ is equal to εN^n, where ε is a character of C_m with values in $\{\pm 1\}$ and $n \in Z$.

2) Let $\phi: S_m \to GL_{V_o}$ be a linear representation of S_m. Assume ϕ is homogeneous of degree d, and put $h = \dim V_o$.

a) Show that dh is even (apply Exerc. 1 to $\det(\phi): S_m \to G_m$).

b) Prove that there exists on V_o a positive definite quadratic form Q such that

$$Q(\rho(x)y) = N(x)^d Q(y)$$

for any $y \in V_o$ and any $x \in S_m(Q)$. [Let H be the kernel of $N: S_m \to G_m$. Using the fact that $H(\mathbb{R})$ is compact, prove the existence of a positive definite quadratic form Q on V_o invariant by H; then note that S_m is generated by H and $j^*(G_m)$.]

3.3. Structure of T_m

We need first some notations:

Let H_c be the closed subgroup of $G = \mathrm{Gal}(\overline{Q}/Q)$ generated by C_∞ (cf. 3.1). There is a unique continuous homomorphism

$\varepsilon: H_c \longrightarrow \{\pm 1\}$ such that $\varepsilon(c) = -1$ for all $c \in C_\infty$. Indeed the unicity of ε is clear, and one proves its existence by taking the restriction to H_c of the homomorphism $G \longrightarrow \{\pm 1\}$ associated with an imaginary quadratic extension of 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 Q; we identify it with a subfield of $\overline{Q}$; let $G_K = \mathrm{Gal}(\overline{Q}/K)$ be the corresponding subgroup of G. The field K is totally real if and only if all the elements c of C_∞ act trivially on K, i.e. if and only if G_K contains G_c. Hence, there exists a maximal totally real subfield K_o of K, whose Galois group is $G_{K_o} = G_K \cdot H_c$. We let K_1 be the field corresponding to $G_K \cdot H$. We have

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

As shown by Weil (cf. [47], p. 4) the fields K_o and K_1 are closely connected to the groups T_m relative to K. Indeed, if $\chi = \Sigma b_\sigma [\sigma]$ 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 $h = c_1 \ldots c_n$, 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 - The norm map defines an isomorphism of the space $Y^o_{K_1}$ relative to K_1 onto the space Y^-_K relative to K.

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

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

where σ/K_1 is the restriction of σ to K_1. It is clear that this map is injective. Conversely, if $\chi = \Sigma b_\sigma[\sigma]$ 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 $h \in H.G_K$. This shows that b_σ depends only on the restriction of σ to K_1, and hence that χ belongs to the image of the norm map.

COROLLARY - 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) $K_1 = K_o$. In this case, we have $Y^- = 0$ and T_m is one-dimensional, and isomorphic to G_m.

Indeed, if $\chi = \Sigma b_\sigma[\sigma]$ 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 $c \in G_K.H_c = G_K.H$. This shows that $b_\sigma = 0$ for all σ, hence $Y^- = 0$.

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

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

Remark

In this last case (which is the most interesting one), the torus T_m is isogenous to the product of G_m by the d-dimensional torus kernel of the norm map from K_1 to K_o.

3.4. How to compute Frobeniuses

Let ϕ be a linear representation of S_m of degree n. By extending the groundfield, the restriction of ϕ to T_m can be put in diagonal form; let $\chi_1, \ldots, \chi_n$ be the n characters of T_m so obtained and write (in additive notation)

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

We say that χ_i is positive if all the $n_\sigma(i)$'s are ≥ 0. Let $v \nmid \mathrm{Supp}(m)$, and let $F_v \in S_m$ (Q) be the corresponding Frobenius element, cf. 2.3. Since $C_m = S_m / T_m$ is finite, there exists an integer $N \geq 1$ such that $F_v^N \in T_m$ (Q). If p_v is the prime ideal of v, this means that there exists $\alpha \in K^*$, with $p_v^N = (\alpha)$, $\alpha \equiv 1 \bmod m$, and $\alpha > 0$ at all real places of K.

PROPOSITION 1 - The eigenvalues of $\phi(F_v^N)$ are the numbers $\chi_i(\alpha) = \prod_\sigma \sigma(\alpha)^{n_\sigma(i)}$ $(i = 1, \ldots, n)$.

This is trivial by construction, because F_v^N is the image of α under $T(Q) \longrightarrow T_m(Q)$.

COROLLARY 1 - The eigenvalues of $\phi(F_v)$ are $\{p_v\}$-units (i.e. they are units at all places of $\bar{Q}$ not dividing p_v).

COROLLARY 2 - Let $z_1, \ldots, z_n$ be the eigenvalues of $\phi(F_v)$, indexed so that $z_i^N = \chi_i(\alpha)$. Let w be a place of $\bar{Q}$ dividing p_v, normalized so that $w(p_v) = v(p_v) = e_v$. Then $w(z_i) = \sum_{\substack{\sigma \in \Gamma \\ w \circ \sigma = v}} n_\sigma(i)$.

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

$$w \circ \sigma(\alpha) = 0 \quad \text{if} \quad w \circ \sigma \neq v$$

$$w \circ \sigma(\alpha) = N \quad \text{if} \quad w \circ \sigma = v,$$

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

Hence the result.

COROLLARY 3 - Let ℓ be a prime number and let $\phi_\ell : \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Aut}(V_\ell)$ be the ℓ-adic representation of K associated to ϕ. Then ϕ_ℓ is integral (cf. Ch. I, 2.2) if and only if all the characters χ_i occurring in ϕ are positive.

Proof of Corollary 3. Assume first the χ_i's are positive. Let $v \notin \mathrm{Supp}(m)$ and let $z_1, \ldots, z_n$ be the corresponding eigenvalues of

F_v as in Corollary 2. Corollaries 1 and 2 show that the $w(z_i)$ are positive for all valuations w of $\bar{Q}$; hence the z_i are integral over Z. Hence the ϕ_ℓ's are integral.

Conversely, assume ϕ_ℓ is integral for some ℓ. There exists a finite subset S' of Σ_K, containing $\mathrm{Supp}(m)$, 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 $\bar{Q}$ 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 $z_1, \ldots, z_n$ be the eigenvalues of $\phi(F_v)$. By Corollary 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.

PROPOSITION 2 - Let $v \notin \mathrm{Supp}(m)$ and let χ be a character of S_m. Let $\chi_T \in X(T_m)$ be the restriction of χ to T_m and let $i = j(\chi_T)$ be the integer defined in 3.2. Then, for any archimedian absolute value ω of $\bar{Q}$ extending the usual absolute value of Q, we have

$$\omega(\chi(F_v)) = (Nv)^{i/2}.$$

Proof. If $\chi = a \sum_{\sigma \in \Gamma} [\sigma] + \sum_{\sigma \in \Gamma} b_\sigma [\sigma]$ 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 $\prod_\sigma \omega \circ \sigma(\alpha)^a = \omega(N(\alpha))^a = Nv^{aN} = Nv^{iN/2}$, where $i = 2a$. It remains to show that $x = \prod_\sigma \omega \circ \sigma(\alpha)^{b_\sigma}$ is equal to 1. Let $c = c_\omega$ be the "Frobenius" attached to ω (cf. 3.1). Since $b_\sigma + b_{c\sigma} = 0$, we have $x.y = 1$ 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 $x > 0$.

Exercises

1) Check the product formula for the eigenvalues of the $\phi(F_v)$. (Use Cor. 1 and 2 to Prop. 1 and Prop. 2.)

2) Show that Prop. 2 and Cor. 1 and 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 to Prop. 1). Let (ρ_ℓ) be a strictly compatible system of rational ℓ-adic representations, with exceptional set S (cf. Chap. I, 2.3). Show that, for any $v \in \Sigma_K - S$, the eigenvalues of F_{v,ρ_ℓ}, $\ell \neq p_v$, are p_v-units.

APPENDIX

Killing arithmetic groups in tori

A.1. Arithmetic groups in tori

Let A be a linear algebraic group over Q, and let Γ be a subgroup of the group $A(Q)$ of rational points of A. Then Γ is said to be an arithmetic subgroup if for any algebraic embedding

$A \subset GL_n$ (n arbitrary) the groups Γ and $A(\mathbb{Q}) \cap GL_n(\mathbb{Z})$ are commensurable (two subgroups Γ_1, Γ_2 are said to be commensurable if $\Gamma_1 \cap \Gamma_2$ is of finite index in Γ_1 and Γ_2). It is well-known that it suffices to check that Γ and $A(\mathbb{Q}) \cap GL_n(\mathbb{Z})$ are commensurable for one embedding $A \subset GL_n$.

Example

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

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

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

This is due to T. Ono; for a proof of a more general statement ("Godement's conjecture") see Mostow-Tamagawa [18].

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

Exercise

Let T be a torus over Q, with character group X.

a) Show that

$$T(Q) = \mathrm{Hom}_{\mathrm{Gal}}(X, \overline{Q}^*).$$

b) Let U be the subgroup of $\overline{Q}^*$ whose elements are the algebraic units of $\overline{Q}$. Let

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

Show that Γ is an arithmetic subgroup of $T(Q)$ and that any arithmetic subgroup of $T(Q)$ is contained in Γ.

A. 2. Killing arithmetic subgroups

Let T be a torus over Q, and let $X(T)$ be its character group; put $Y(T) = X(T) \otimes_Z Q$. Let Λ be the set of classes of Q-irreducible representations of $G = \mathrm{Gal}(\overline{Q}/Q)$ through its finite quotients. For each $\lambda \in \Lambda$, let Y_λ be the corresponding isotypic sub-G-module of Y, i.e. the sum of all sub-G-modules of Y isomorphic to λ. One has the direct sum decomposition

$$Y = \coprod_{\lambda \in \Lambda} Y_\lambda .$$

Let $Y^o = Y_1$, where 1 is the unit representation of G; let Y^- be the sum of those Y_λ where for all the infinite Frobeniuses $c \in C_\infty$ (cf. 3.1) we have $\lambda(c) = -1$; let Y^+ be the sum of the other Y_λ. We have

$$Y^o = Y^G = \{y \in Y \mid gy = y \quad \text{for all} \quad g \in G\}$$

$$Y^- = \{y \in Y \mid cy = -y \quad \text{for all} \quad c \in C_\infty\},$$

$$Y = Y^o \oplus Y^- \oplus Y^+ .$$

Note that $Y = Y^o$ if and only if T is anisotropic.

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

PROPOSITION - Let Γ be an arithmetic subgroup of the torus T, and $\bar{\Gamma}$ its Zariski closure (cf. 1.2). Then:

$$(*) \qquad Y(T/\bar{\Gamma}) = Y^o \oplus Y^- .$$

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

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

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

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

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

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^o, hence $\mathrm{Ker}(N) = Y^- \oplus Y^+$.

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

CHAPTER III

LOCALLY ALGEBRAIC ABELIAN REPRESENTATIONS

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

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

In the local case, an abelian semi-simple representation is locally algebraic if and only if it has a "Hodge-Tate decomposition". This fact, due to Tate (Collège 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 Q_p; let $T = R_{K/Q_p}(G_{m/K})$ be the corresponding algebraic torus over

Q_p (cf. Weil [43], Chap. I).

Let V be a finite dimensional Q_p-vector space and denote, as usual, by GL_V the corresponding linear group; it is an algebraic group over Q_p, and $GL_V(Q_p) = \mathrm{Aut}(V)$.

Let $\rho: \mathrm{Gal}(\bar{K}/K)^{ab} \to \mathrm{Aut}(V)$ be an abelian p-adic representation of K in V, where $\mathrm{Gal}(\bar{K}/K)^{ab}$ denotes the Galois group of the maximal abelian extension of K. If $i: K^* \to \mathrm{Gal}(\bar{K}/K)^{ab}$ is the canonical homomorphism of local class field theory (cf. for instance Cassels-Fröhlich [6], chap. VI, §2), we then get a continuous homomorphism $\rho \circ i$ of $K^* = T(Q_p)$ into $\mathrm{Aut}(V)$.

DEFINITION - The representation ρ is said to be locally algebraic if there is an algebraic morphism $r: T \to GL_V$ such that $\rho \circ i(x) = r(x^{-1})$ for all $x \in K^*$ close enough to 1.

Note that, if $r: T \to GL_V$ satisfies the above condition, it is unique; this follows from the fact that any non-empty open set of $K^* = T(Q_p)$ is Zariski dense in T. We say that r is the algebraic morphism associated with ρ.

Examples

1) Take $K = Q_p$, and dim $V = 1$, so that ρ is given by a continuous homomorphism $\mathrm{Gal}(\bar{Q}_p/Q_p)^{ab} \to U_p$, where U_p is the group of p-adic units. It is easy to see that there exists an element $\nu \in Z_p$ such that $\rho \circ i(x) = x^{\nu}$ if x is close enough to 1. The representation ρ is locally algebraic if and only if ν belongs to Z. This happens for instance when $V = V_p(\mu)$, cf. Chap. I, 1.2, in which case $\nu = -1$ and r is the canonical one-dimensional representation of $T = G_{m/Q_p}$.

2) The abelian representation associated to a Lubin-Tate formal group (cf. [17] and [6], Chap. VI, §3) is locally algebraic (and also of the form $u \mapsto u^{-1}$ on the inertia group).

PROPOSITION 1 - Let $\rho: \mathrm{Gal}(\bar{K}/K)^{ab} \to \mathrm{Aut}(V)$ be a locally algebraic abelian representation of K. The restriction of ρ to the inertia subgroup of $\mathrm{Gal}(\bar{K}/K)^{ab}$ is semi-simple.

Let us identify the inertia subgroup of $\mathrm{Gal}(\bar{K}/K)^{ab}$ 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 T into 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 $\pi: V \to W$ which commutes with the action of 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 $\pi': V \to W$ which commutes with all $\rho(s)$, $s \in U_K$, q.e.d.

Conversely, let us start from a representation ρ whose restriction to U_K is semi-simple. If we make a suitable large finite extension E of Q_p, the restriction of ρ to U_K may be brought into diagonal form, i.e. is given by continuous characters $\chi_i: U_K \to E^*$, $i=1,\ldots,n$. We assume E large enough to contain all conjugates of K, and we denote by Γ_K the set of all Q-embeddings of K into E. Recall (cf. chap. II, 1.1) that the $[\sigma]$, $\sigma \in \Gamma_K$, make a basis of the character group $X(T)$ of T.

PROPOSITION 2 - The representation ρ is locally algebraic if and only if there exist integers $n_\sigma(i)$ 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.

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 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 Q_p (cf. chap. II, 2.4). But the trace $\theta_r = \Sigma r_i$ of r (loc. cit.) is such that $\theta_r(u) \in Q_p$ for all $u \in U'$. Since U' is Zariski-dense in T, this implies that θ_r is "defined over Q_p", hence that r can be defined over Q_p (loc. cit.), q.e.d.

Extension of the ground field

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

$$r: T \longrightarrow GL_V \ , \ r': T' \longrightarrow GL_V$$

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

All this follows easily from the commutativity of the diagram

$$\begin{array}{ccc} K^* & \longrightarrow & \mathrm{Gal}(\bar{K}/K)^{ab} \\ \uparrow N & & \uparrow \\ K'^* & \longrightarrow & \mathrm{Gal}(\bar{K}/K')^{ab} \end{array} ,$$

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

Exercise

Give an example of a locally algebraic abelian p-adic representation of dimension 2 which is not semi-simple.

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 $\mathrm{char}(K) = 0$, $\mathrm{char}(k) = p$. Denote by C the completion $\hat{\bar{K}}$ of the algebraic closure of K.

The group $G = \mathrm{Gal}(\bar{K}/K)$ acts continuously on $\bar{K}$. 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

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

Let $\chi: G \longrightarrow U_p$ be the homomorphism of G into the group $U_p = Z_p^*$ of p-adic units, defined by its action on the p^ν-th roots of unity (cf. chap. I, 1.2):

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

Define for every $i \in Z$ 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-vectorspace upon which G acts in a natural way (i.e. by the formula $s(c \otimes y) = s(c) \otimes s(y)$). The inclusion $W^i \longrightarrow W$ extends uniquely to a C-linear map $\alpha_i : W(i) \longrightarrow W$, which commutes with the action of G.

PROPOSITION (Tate) - Let $\coprod W(i)$ be the direct sum of the $W(i)$, $i \in Z$. Let $\alpha : \coprod W(i) \longrightarrow W$ be the sum of the α_i's defined above. Then α is injective.

For the proof see [27], §2, prop. 4.

COROLLARY - The K-spaces $W^i (i \in Z)$ are of finite dimension. They are linearly independent over C.

DEFINITION 1 - The module W is of Hodge-Tate type if the homomorphism $\alpha : \coprod_{i \in Z} W(i) \longrightarrow W$ is an isomorphism.

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

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

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

Example

Let F be a p-divisible group of finite height (cf. [26], [39]); let T be its Tate module (loc. cit.) and $V = Q_p \otimes T$. 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 (Tate) - Assume K is a finite extension of Q_p (i.e. its residue field is finite). Let $\rho: G \longrightarrow \mathrm{Aut}(V)$ be an abelian p-adic representation of K. The following properties are equivalent:

(a) ρ is locally algebraic (cf. 1.1).

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

For the proof, see the Appendix.

§2 - THE GLOBAL CASE

2.1. Definitions

We now go back to the notations of chap. II, i.e. K denotes a number field. Let ℓ be a prime number and let

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

be an abelian ℓ-adic representation of K. Let $v \in \Sigma_K$ be a place

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

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

DEFINITION - The representation ρ is said to be locally algebraic if all the local representations ρ_v, with $p_v = \ell$, are locally algebraic (in the sense defined in 1.1, with $p = \ell$).

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

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

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

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

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

PROPOSITION - The representation ρ is locally algebraic if and only if there exists an algebraic morphism

$$f: T_{/\mathbb{Q}_\ell} \longrightarrow GL_{V_\ell}$$

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

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

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

where T_v is the $\mathbb{Q}_\ell$-torus defined by K_v, cf. 1.1. The proposition follows from this decomposition.

Exercise

Give a criterion for local algebraicity analogous to the one of Prop. 2 of 1.1.

2.2. Modulus of a locally algebraic abelian representation

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

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

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

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

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

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

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

PROPOSITION - Let H be a Lie group over $\mathbb{Q}_\ell$ (resp. R) and let α be a continuous homomorphism of the idèle group I into H.

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

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

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

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

$\alpha(U_v)$ is finite; hence $\alpha(U_v) = \{1\}$ for almost all v's, q.e.d.

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

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

Remark

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

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

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

Remark

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

Exercise

Let $z_1, \ldots, z_n, \ldots \in K^*$. For each n, let E_n be the subfield of $\bar{K}$ generated by all the ℓ^n-th roots of the element $z_1 z_2^{\ell} \ldots z_n^{\ell^{n-1}}$.

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

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 Z_ℓ.

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

2.3. Back to S_m

Let m be a modulus of K and let

$$\phi: S_m / Q_\ell \longrightarrow GL_{V_\ell}$$

be a linear representation of S_{m/Q_ℓ}. Let

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

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

THEOREM 1 - The representation ϕ_ℓ is locally algebraic and defined mod m. The associated algebraic morphism

$$f: T_{/Q_\ell} \to GL_{V_\ell}$$

is $\phi \circ \pi$, where π denotes the canonical morphism of T into S_m (cf. chap. II, 2.2).

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

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

THEOREM 2 - Let $\rho: \mathrm{Gal}(\bar{K}/K)^{ab} \to \mathrm{Aut}(V_\ell)$ be an abelian ℓ-adic representation of the number field K. Assume ρ is rational (chap. I, 2.3) and is locally algebraic with m as a modulus of definition (cf. 2.2). Then, there exist a Q-vector subspace V_o of V_ℓ, with $V_\ell = V_o \otimes_Q Q_\ell$, and a morphism $\phi_o: S_m \to GL_{V_o}$ of Q-algebraic groups such that ρ is equal to the ℓ-adic representation ϕ_ℓ associated to ϕ_o (cf. chap. II, 2.5).

(The condition $V_\ell = V_o \otimes_Q Q_\ell$ means that V_o is a "Q-structure" on V_ℓ, cf. Bourbaki Alg., chap. II, 3rd ed.)

Proof. Let $r: T_{/Q_\ell} \to GL_{V_\ell}$ be the algebraic morphism associated with ρ. We have

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

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

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

where x_ℓ is the ℓ^{th} component of the idèle x. One checks immediately that ψ is trivial on U_m and coincides with r on K^*. Hence r is trivial on $E_m = K^* \cap U_m$ and factors through an algebraic morphism $r_m : T_{m/Q_\ell} \longrightarrow GL_{V_\ell}$. By the universal property of the Q_ℓ-algebraic group S_{m/Q_ℓ} (cf. chap. II, 1.3 and 2.2), there exists an algebraic morphism

$$\phi: S_{m/Q_\ell} \longrightarrow GL_{V_\ell}$$

with the following properties:

(a) The morphism $T_{m/Q_\ell} \longrightarrow S_{m/Q_\ell} \xrightarrow{\phi} GL_{V_\ell}$ is r_m.

(b) the map $I \xrightarrow{\varepsilon} S_m(Q_\ell) \xrightarrow{\phi} \mathrm{Aut}(V_\ell)$ is ψ.

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

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

$$= \psi(a)\phi(\pi_\ell(a_\ell^{-1}))$$

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

$$= \rho \circ i(a)$$

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

Hence $\phi_\ell = \rho$; the fact that ρ is rational then implies that ϕ can be defined over Q (chap. II, 2.4, Prop.), and this gives V_o and ϕ_o, q.e.d.

Remark

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

COROLLARY 1 - For each prime number ℓ' there exists a unique (up to isomorphism) ℓ'-adic rational semi-simple representation $\rho_{\ell'}$ of K, compatible with ρ. It is abelian and locally algebraic. These representations form a strictly compatible system (cf. chap. I, 2.3) with exceptional set contained in Supp($\mathfrak{m}$). For an infinite number of ℓ', $\rho_{\ell'}$ can be brought in diagonal form.

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

COROLLARY 2 - The eigenvalues of the Frobenius elements $F_{v,\rho}$ ($v \notin$ Supp($\mathfrak{m}$), $p_v \neq \ell$) generate a finite extension of Q.

This follows from the corresponding property of ϕ_ℓ, cf. chapter II, 2.5, Remark 1.

2.4. A mild generalization

Most results of this and the previous Chapter may be extended to the case where we take for ground field of the linear representation a number field E (instead of $\mathbb{Q}$). More precisely, let λ be a finite place of E and let E_λ be the λ-adic completion of E. The notion of an E-rational λ-adic representation of K has been defined in chap. I, 2.3, Remark. Let

$$\rho: \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(V_\lambda)$$

be such a representation, and assume ρ is abelian. Let ℓ be the residue characteristic of λ, so that E_λ contains $\mathbb{Q}_\ell$. As in 2.1, we say that ρ is locally algebraic if there exists an algebraic morphism

$$f: T_{/E_\lambda} \longrightarrow GL_{V_\lambda}$$

such that $\rho \circ i_\ell(x) = f(x^{-1})$ for $x \in K_\ell^*$ close enough to 1 (note that $K_\ell^* = T(\mathbb{Q}_\ell)$ is a subgroup of $T(E_\lambda)$) As in 2.3, one proves that such a ρ comes from an E-linear representation of some S_m (and conversely).

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 m is a modulus for K (i.e. a positive divisor) we define the subgroup U_m of the idèle group I as in chap. II, 2.1, and we put

$$\Gamma_m = I/U_m K^* .$$

The degree map $\deg: I \to Z$ is trivial on U_m, hence defines an exact sequence

$$1 \to J_m \to \Gamma_m \to Z \to 1.$$

One sees easily that the group J_m is finite; moreover, it may be interpreted as the group of rational points of the "generalized Jacobian variety defined by m". If $\hat{\Gamma}_m$ denotes the completion of Γ_m with respect to the topology of subgroups of finite index, it is known (class field theory) that $\mathrm{Gal}(\bar{K}/K)^{ab} \simeq \varprojlim \hat{\Gamma}_m$.

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

PROPOSITION - A homomorphism $\phi: \Gamma_m \to \mathrm{Aut}(V_\ell)$ can be extended to a continuous homomorphism of $\hat{\Gamma}_m$ if and only if there exists a lattice of V_ℓ which is stable by $\rho(\Gamma_m)$.

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

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

THEOREM - An abelian ℓ-adic representation

$$\phi: \hat{\Gamma}_m \longrightarrow \mathrm{Aut}(V_\ell)$$

of K is rational if and only if $\mathrm{Tr}\,\phi(\gamma)$ belongs to $\mathbb{Q}$ for every $\gamma \in \Gamma_m$.

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

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

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

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

continuity to

$$\hat{\phi}: \hat{\Gamma} \longrightarrow GL(n; E \otimes Q_{\ell'})$$

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

$$\mathrm{Tr}\,\phi(\Gamma) \in E \cap Q_{\ell'} = Q, \qquad \text{q.e.d.}$$

Exercises

1) Let $\phi: \Gamma_m \longrightarrow \mathrm{Aut}(V_\ell)$ be a semi-simple ℓ-adic representation of Γ_m. Show the equivalence of:

(a) ϕ extends continuously to $\hat{\Gamma}_m$.

(b) For every $\gamma \in \Gamma_m$, the eigenvalues of $\phi(\gamma)$ are units (in a suitable extension of Q_ℓ).

(c) There exists $\gamma \in \Gamma_m$, with $\deg(\gamma) \neq 0$, such that the eigenvalues of $\phi(\gamma)$ are units.

(d) For every $\gamma \in \Gamma_m$, one has $\mathrm{Tr}\,\phi(\gamma) \in Z_\ell$.

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

§3. THE CASE OF A COMPOSITE OF QUADRATIC FIELDS

3.1. Statement of the result

The aim of this § is to prove:

THEOREM - Let ρ be a rational, semi-simple, ℓ-adic abelian representation of K. Assume

(*) K is a composite of quadratic extensions of $\mathbb{Q}$.

Then ρ is locally algebraic (and hence stems from a linear representation of some S_m, cf. 2.3).

This applies in particular when $K = \mathbb{Q}$ or when K is quadratic over $\mathbb{Q}$.

Remarks

1) An analogous result holds for E-rational semi-simple abelian λ-adic representations (cf. 2.4).

2) It is quite likely that condition (*) is not necessary. But proving this seems to require stronger results on transcendental numbers than the ones now available.

3.2. A criterion for local algebraicity

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

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

$$\chi_i(x) = \chi_i^{alg}(x^{-1}) = \prod \sigma(x)^{-n_\sigma(i)}$$

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

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

Proof of the lemma

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

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

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

rational coefficients.

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

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

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

where α is as above.

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

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

Assume now that $n_\sigma(i)$ is not divisible by N. Then x, which is an N^{th}-root of y, does not belong to $\tilde{L}$. Hence there is a

non-trivial N^{th}-root of unity z such that x and zx are conjugate over $\tilde{L}$, and a fortiori over Q. Since the characteristic polynomial of $F_{v,\rho}$ has rational coefficients, any conjugate over Q of an eigenvalue of $F_{v,\rho}$ is again an eigenvalue of $F_{v,\rho}$. Hence, there exists an index j such that

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

But $f_v \in K^* U_m$ and all ψ_j are trivial on K^* and map U_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 has been chosen.

Proof of the proposition

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

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

if x is close enough to 1. Hence $\phi_i(x)\psi_i(x)$ is an N^{th}-root of unity when x is close enough to 1, and, by continuity, it is equal to 1 in a neighbourhood of 1. Hence, the restriction of ρ to K_ℓ^* is locally equal to ϕ^{-1}, where ϕ is the (algebraic) representation of T defined by the family $(\phi_1, \ldots, \phi_n)$. The representation ϕ, a priori defined over $\bar{Q}_\ell$, can be defined over Q_ℓ (and even over Q); this follows, for instance, from the fact that the family $(\phi_1, \ldots, \phi_n)$ is stable under the action of $Gal(\bar{Q}/Q)$, since the family $(\chi_1^{alg}, \ldots, \chi_n^{alg})$ is.

Hence ρ is locally algebraic, q.e.d.

3.3. An auxiliary result on tori

In [15], Lang proved that two exponential functions $\exp(b_1 z)$, $\exp(b_2 z)$, $b_1, b_2 \in C$, which take algebraic values for at least 3 Q-linearly independent values of z, are multiplicatively dependent: the ratio b_1/b_2 is a rational number. This had also been noticed by Siegel.

Lang proved the following ℓ-adic analogue:

PROPOSITION 1 - Let E be a field containing Q_ℓ and complete for a real valuation extending the valuation of Q_ℓ. Let $b_1, b_2 \in E$ and let Γ be an additive subgroup of E. Assume:

(1) Γ is of rank at least 3 over Z.

(2) The exponential series $\exp(z) = \Sigma z^n/n!$ 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 Q.

Then b_1 and b_2 are linearly dependent over Q (i.e. b_1/b_2 belongs to 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 $\overline{Q}_\ell$. We need a few definitions first:

a/ Let T be an n-dimensional torus over Q, with character group $X(T)$. As before, we identify $X(T)$ with the group of morphisms of $T_{/E}$ into $G_{m/E}$. 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 $T_1 \times \ldots \times T_n \to T$ is surjective (and hence has a finite kernel). An equivalent condition is:

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

b/ Let f be a continuous homomorphism of $T(Q_\ell)$ into E^*. We say that f is locally algebraic if there is a neighbourhood U of 1 in the ℓ-adic Lie group $T(Q_\ell)$, and an element $\phi \in X(T)$ such that $f(x) = \phi(x)$ 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 $T(Q_p)$; denote by W the family $(W_p)_{p \in S}$.

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

PROPOSITION 2 - Let $f: T(Q_\ell) \to E^*$ be a continuous homomorphism. Assume:

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

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

Then f is almost locally algebraic.

Proof.

i) We suppose first that T is one-dimensional, and we denote by χ a generator of $X(T)$. If χ is invariant by $\mathrm{Gal}(\bar{Q}/Q)$, T is isomorphic to G_m and $T(Q) \simeq Q^*$. If not, $\mathrm{Gal}(\bar{Q}/Q)$ acts on $X(T)$ via a group of order 2, corresponding to some quadratic

extension F of Q; the character χ defines an isomorphism of $T(Q)$ onto the group F_1^* of elements of F of norm 1. In both cases, one sees that $T(Q)$ is an abelian group of infinite rank (for a more precise result, see Exercise below). On the other hand, each quotient $T(Q_p)/W_p$ is a finitely generated abelian group of rank ≤ 1. Hence $T(Q)/T(Q)_W$ is finitely generated, and this implies that $T(Q)_W$ is also of infinite rank.

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

$$e: Z_\ell \to T(Q_\ell)$$

which is an isomorphism of Z_ℓ onto an open subgroup of $T(Q_\ell)$. By composition we get two continuous homomorphisms

$$f \circ e: Z_\ell \to E^* , \qquad \chi \circ e: Z_\ell \to E^* .$$

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

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

with absolute convergence of the exponential series.

Let now Γ be the set of elements $z \in Z_\ell$ such that $e(z) \in T(Q)_W$. Since $T(Q_\ell)/e(Z_\ell)$ is finitely generated, and $T(Q)_W$ is of infinite rank, Γ is of infinite rank. If $z \in \Gamma$, $e(z)$

belongs to $T(Q)_W$, hence $f \circ e(z)$ is algebraic over Q; the same is true for $\chi \circ e(z)$ since χ maps $T(Q)$ either into Q^* or into the group F_1^* defined above. Proposition 1 then shows that b_1/b_2 is rational. This means that some integral power f^N of f, with $N \geq 1$, is locally equal to an integral power of χ, hence f is almost locally algebraic.

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

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). → [This has been done by Waldschmidt: see [63], [83].]

Exercise

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

3.4. Proof of the theorem

We go back to the notations and hypotheses of 3.1. Let

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

be a rational, semi-simple, abelian ℓ-adic representation of K. If E is the completion of $\overline{Q}_\ell$, as in 3.3, we may bring ρ in diagonal form over E. This gives rise to a family $(\psi_1, \ldots, \psi_n)$ of continuous characters of $\mathrm{Gal}(\overline{K}/K)^{ab}$ (hence also of the idèle group I) into E^*; here, $n = \dim. V_\ell$.

Let $f_i: K_\ell^* \longrightarrow E^*$ be the restriction of ψ_i to the ℓ^{th}-component K_ℓ^* of I. Note that $K_\ell^* = T(Q_\ell)$, where T is, as usual, the torus defined by K (chap. II, 1.1).

LEMMA - The torus T and the homomorphism f_i satisfy the assumptions (a) and (b) of Prop. 2, 3.3.

Verification of (a)

Let S be a finite set of primes, with $\ell \notin S$, such that if $v \in \Sigma_K$, $p_v \neq \ell$, $p_v \notin S$, the representation ρ is unramified at v, and the characteristic polynomial of $F_{v,\rho}$ has rational coefficients. If $p \in S$, Prop. 1 of 2.2 shows that there exists an open subgroup W_p of $K_p^* = T(Q_p)$ such that $\psi_i(W_p) = 1$. Let $W = (W_p)_{p \in S}$ and let $x \in T(Q)_W$. Since $x \in K^*$, we have $\psi_i(x) = 1$, when x is identified with an idèle of K. On the other hand, let us split the idèle x in its components

$$x = x_\infty \cdot x_\ell \cdot x_S \cdot x'$$

according to the decomposition of I in

$$I = K_\infty^* \times K_\ell^* \times K_S^* \times I' .$$

(Here $K^* = (K \otimes R)^*$, $K_S^* = \prod_{p \in S} K_p^*$ and I' is the restricted product of the K_v^*, for $v \in \Sigma_K$, and $p_v \neq \ell$, $p_v \notin S$.) The relation $\psi_i(x) = 1$, together with $\psi_i(x_\ell) = f_i(x)$, gives

$$f_i(x)^{-1} = \psi_i(x_\infty)\psi_i(x_S)\psi_i(x').$$

By construction, we have $\psi_i(x_S) = 1$ and it is clear that $\psi_i(x_\infty) = \pm 1$. Hence:

$$f_i(x) = \pm \psi_i(x')^{-1} .$$

But, for each $v \in \Sigma_K$, with $p_v \notin S$, $p_v \neq \ell$, we know that the eigenvalues of $F_{v,\rho}$ are algebraic; hence, if f_v is an idèle which is a uniformizing element at v, and is equal to 1 elsewhere, $\psi_i(f_v)$ is algebraic. If $a(v)$ is the valuation of x' at v, we have:

$$\psi_i(x') = \prod \psi_i(f_v)^{a(v)} ;$$

hence $\psi_i(x')$ and $f_i(x)$ are algebraic and we have checked (a).

Verification of (b).

Since K is a composite of quadratic fields, it is a Galois extension of Q, and its Galois group G is a product of groups of order 2. The character group $X(T)$ of T is isomorphic to the

regular representation of G, and it is clear that $X(T) \otimes Q$ splits as a direct sum of one-dimensional G-stable subspaces (each correspond to a character of G). Hence T is a sum of one-dimensional tori.

End of the proof of the theorem

Using prop. 2 of 3.3, we see that each f_i is almost locally algebraic. Hence there is an integer $N \geq 1$ such that the f_i^N are locally algebraic. This implies, cf. 1.1, that ρ^N is locally algebraic, hence (cf. 3.2) that ρ itself is locally algebraic, q.e.d.

Exercise

Assume that K is a composite of quadratic fields. Let χ be a Grössencharakter of K and suppose that the values of χ (on the ideals prime to the conductor) are algebraic numbers. Show that χ is "of type (A)" in the sense of Weil [41]. (Use the same method than above, with E replaced by C.) If the values of χ lie in a finite extension of Q, show that χ is "of type (A_o)" . → [no assumption on K is necessary, thanks to [83].]

APPENDIX

Hodge-Tate decompositions and locally algebraic representations

Let K be a field of characteristic zero, complete with respect to a discrete valuation and with perfect residue field k of characteristic $p > 0$. In this Appendix we deal with Hodge-Tate decomposition of p-adic abelian representations of K.

Sections A1 and A2 give invariance properties of these decompositions under ground field extensions. Special characters of $\mathrm{Gal}(\overline{K}/K)$ are defined in A4; they are closely connected both with Hodge-Tate modules (A4 and A5) and local algebraicity (A6). The proof of Tate's theorem (cf. 1.2) is given in the last section.

A1. Invariance of Hodge-Tate decompositions

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

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

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

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

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

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

COROLLARY 1 - The Galois modules $W(n)$ and $W(n)'$ are equal.

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

COROLLARY 2 - The Galois module W is of Hodge-Tate type over K if and only if it is so over $\hat{K}'$.

Proof of Theorem 1

Note first that replacing the action of $\mathrm{Gal}(\bar{K}/K)$ on W by $(s,w) \mapsto \chi(s)^{-i} sw$, $i \in \mathbf{Z}$, just changes W^n to W^{n+i}. This shifting process reduces the problem to the case $n = 0$; in that case, W^n (resp. $W^n_{K'}$) is the set of elements of W which are invariant under $\mathrm{Gal}(\bar{K}/K)$ (resp. under $\mathrm{Gal}(\bar{K}/K')$). Note also that the injectivity of $\hat{K}' \otimes W^o \to W^o_{K'}$ is trivial, since we know that $C \otimes_K W^o \to W$ is injective (cf. 1.2).

On the other hand, an easy up-and-down argument shows that one can assume K'/K to be either finite Galois or unramified Galois. In both cases, since $\mathrm{Gal}(\bar{K}/K')$ acts trivially on $W^o_{K'}$, we have a semi-linear action of $\mathrm{Gal}(K'/K)$ on $W^o_{K'}$. When K'/K is finite, it is well known that this implies that $W^o_{K'}$ is generated by the elements invariant by $\mathrm{Gal}(K'/K)$, i.e. by W^o (this is a non-commutative analogue of Hilbert's "Theorem 90", cf. for instance [29], p. 159).

Let now K'/K be unramified Galois and let G be its Galois group. Let $\hat{O}'$ denote the ring of integers of $\hat{K}'$. Let Λ be an $\hat{O}'$-lattice of $W^o_{K'}$ (i.e. a free $\hat{O}'$-submodule of $W^o_{K'}$ of the same rank as $W^o_{K'}$). Since G acts continuously on $W^o_{K'}$, the stabilizer in G of Λ is open, hence of finite index, and the lattice Λ has

finitely many transforms. The sum Λ^o of these transforms is invariant by G. Let $e_1, \ldots, e_N$ be a basis of Λ^o. Let $s \in G$. Then

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

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

LEMMA - $H^1(G, GL(N, \hat{O}')) = \{1\}$.

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

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

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

Proof of the lemma

Let π be a uniformizing element of $\hat{O}'$. Filter the ring $A = GL(N, \hat{O}')$ by means of $A_n = \{a \in A \mid a \equiv 1 \mod \pi^n\}$. We get $A/A_1 \cong GL(N, k'/k)$, where k'/k is the residue field extension of K'/K. Moreover, for $n \geq 1$, there is an isomorphism $A_n/A_{n+k} \cong M_N(k')$, 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 $H^1(G, GL(N, k'))$ and $H^1(G, M_N(k'))$, where now k' is endowed with the discrete topology (so this is ordinary Galois cohomology, cf. [29], p. 158-159).

A2. Admissible characters

Let $G = Gal(\bar{K}/K)$ and let $\phi: G \to K^*$ be a continuous homomorphism.

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

Remarks

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

2) Let $H^1(G, C^*)$ be the first cohomology group of G with values in C^* (cohomology being defined by continuous cochains, as in A1). A continuous character $\phi: G \to K^*$ is a 1-cocycle, hence defines an element $\bar{\phi}$ of $H^1(G, C^*)$. One has $\bar{\phi} = \bar{\phi}'$ if and only if $\phi \sim \phi'$.

3) Define a new action of G on C by means of

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

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

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

Proof. Let K'/K be the subextension of $\bar{K}/K$ corresponding to N; it is a finite extension of an unramified one. Let $W = C(\phi)$, as in Remark 3, and let W^o (resp. $W^o_{K'}$) be the subspace of W consisting of elements invariant by G (resp. by N). By hypothesis, $W^o_{K'}$ is $\neq 0$. Hence, by A1, Theorem 1, we also have $W^o \neq 0$, and this means that ϕ is admissible, q.e.d.

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 $\bar{k}^*$ with the group of multiplicative representatives, so that $U_C = U_C^1 \times \bar{k}^*$, cf. [29], p. 44. Define the logarithm map

$$\log: U_C \to C$$

by

$$\log(x) = 0 \qquad \text{if } x \in \bar{k}^*$$

$$\log(x) = \sum_{n=1}^{\infty} (-1)^{n-1}(x-1)^n/n \qquad \text{if } x \in U_C^1 .$$

This is a continuous homomorphism and even a local isomorphism.

Moreover:

LEMMA - (a) log is surjective.

(b) The kernel of log: $U_C \to C$ is $\bar{k}^* \times \mu_{p^\infty}$,

where μ_{p^∞} is the set of all p^n-th roots of unity, for $n = 1, 2, \ldots$

Assertion (a) follows from the fact that C is algebraically closed, hence that U_C is divisible.

On the other hand, if $u \in U_C^1$ is such that $\log(u) = 0$, one has $\lim. u^{p^N} = 1$, hence, if N is large enough, u^{p^N} belongs to a subgroup of U_C^1 where log is injective (for instance the subgroup of elements x with $x \equiv 1 \bmod p^2$). Hence $u^{p^N} = 1$, and $u \in \mu_{p^\infty}$; this implies (b).

We now apply the log map to the cohomology groups of G with values in $U_C, C, C^*, \ldots$ (cohomology being, as usual, defined by continuous cochains). First, since the valuation group of C is $\mathbb{Q}$, we have the exact sequence

$$1 \to U_C \to C^* \to \mathbb{Q} \to 1 .$$

By Tate's theorem ([39], §3.3) one has $H^0(G, C^*) = K^*$, hence an exact sequence

$$K^* \to \mathbb{Q} \to H^1(G, U_C) \to H^1(G, C^*) \to 0 ,$$

or, equivalently:

$$0 \longrightarrow Q/Z \xrightarrow{\delta} H^1(G, U_C) \xrightarrow{i} H^1(G, C^*) \longrightarrow 0 .$$

Let $N = \mathrm{Ker}(\log)$. We have the exact sequence

$$H^1(G, N) \xrightarrow{j} H^1(G, U_C) \xrightarrow{\lambda} H^1(G, C),$$

where λ is induced by the log. Since $H^1(G, C)$ is a K-vector space, the composite $\lambda \circ \delta: Q/Z \longrightarrow H^1(G, C)$ is 0, hence there is a unique map

$$L: H^1(G, C^*) \longrightarrow H^1(G, C)$$

such that $L \circ i = \lambda$.

PROPOSITION 2 - The map $L: H^1(G, C^*) \longrightarrow H^1(G, C)$ is injective.

Using the exact sequences above, one sees it is enough to prove that $i \circ j: H^1(G, N) \longrightarrow H^1(G, C^*)$ is trivial. But N is a discrete subgroup of $\overline{K}^*$, hence $i \circ j$ factors through $H^1(G, \overline{K}^*)$, where now $\overline{K}^*$ is viewed as a discrete group; by Theorem 90, $H^1(G, \overline{K}^*)$ is trivial, hence also $i \circ j$, q. e. d.

Let now $\phi: G \longrightarrow K^*$ be a continuous character. Since $\phi(G)$ is compact, it is contained in U_K, hence in U_C, and $\log \phi: G \longrightarrow C$ is an additive 1-cocycle. Its cohomology class in $H^1(G, C)$ is $L\overline{\phi}$, where $\overline{\phi}$ is the cohomology class of ϕ in $H^1(G, C^*)$.

PROPOSITION 3 - The properties $\phi \sim 1$ and $L\overline{\phi} = 0$ are equivalent.

This follows from the injectivity of L.

COROLLARY - If there exists a non-zero integer n such that $\phi^n \sim 1$, then $\phi \sim 1$.

Indeed, $L\overline{\phi} = \frac{1}{n} L\overline{\phi}^n = 0$.

Remark

Springer has proved that $H^1(G, C)$ is of dimension 1 over K (cf. Tate [39], §3.3). Hence, one can take for basis of $H^1(G, C)$ the element $L\overline{\chi}$, where χ is the fundamental character defined in chap. I, 1.2. In particular, for any $\phi: G \to K^*$, there is an element $c(\phi)$ of K such that $L\overline{\phi} = c(\phi) L\overline{\chi}$; when K is locally compact, this $c(\phi)$ may be computed explicitly, see A6, Exer. 2.

A3. A criterion for local triviality

From now on, E denotes a subfield of K having the following properties:

(a) E contains Q_p and $[E: Q_p] < \infty$ (so that E is locally compact).

(b) K contains all Q_p-conjugates of E.

We denote by Γ_E the set of all Q_p-embeddings of E in K. Consider a continuous character

$$\psi: \mathrm{Gal}(\overline{K}/K) \to E^*$$

with values in E. For each $\sigma \in \Gamma_E$ this gives a character $\sigma \circ \psi: G \to E^* \xrightarrow{\sigma} K^*$ of $G = \mathrm{Gal}(\overline{K}/K)$ into K^*.

PROPOSITION 3 - The following two properties are equivalent :

(1) ψ is equal to 1 on an open subgroup of the inertia group of G,

(2) $\sigma \circ \psi \sim 1$ for all $\sigma \in \Gamma_E$.

Proof

(1) $\Rightarrow$ (2) is trivial from the result of A1 (since we know that admissibility can be seen on an open subgroup of the inertia group).

(2) $\Rightarrow$ (1). We use the log map defined in A2. Note that ψ takes values in the group U_E of units of E, hence $\log \psi: G \longrightarrow E$ is well defined. Let I be the inertia group of G; the subgroup $\log \psi(I)$ of E is compact, and hence isomorphic to Z_p^n for some n. If W is the Q_p-vector subspace of E generated by $\log \psi(I)$, we see that $\log \psi(I)$ is a lattice in W, and dim W = n. Note that saying that ψ is equal to 1 on an open neighbourhood of 1 in I is equivalent to saying that $\log \psi(I) = 0$ (since log: $U_E \longrightarrow E$ is a local isomorphism). Suppose this is not the case, i.e. suppose that $n \geq 1$. Choose a Q_p-linear map $f: E \longrightarrow K$ such that dim f(W) = 1; such a map obviously exists. By Galois theory (independence of characters) the set Γ_E is a basis of $\mathrm{Hom}_{Q_p}(E, K)$. Hence, there exist $k_\sigma \in K$ with

$$f = \sum_{\sigma \in \Gamma_E} k_\sigma \sigma$$

and we have $f \circ \log \psi = \Sigma k_\sigma \sigma \circ \log \psi = \Sigma k_\sigma \log(\sigma \circ \psi)$.

But by assumption (and Prop. 3 of A2), the additive 1-cocycle $\log(\sigma \circ \psi)\colon G \longrightarrow K$ is cohomologous to 0. Hence the same is true for $f \circ \log \psi$. But we may assume (replacing f by $p^N f$, with N large, if necessary) that there exists a continuous homomorphism $F\colon U_E \longrightarrow U_K$ such that $f \circ \log = \log \circ F$. We then have $\log(F \circ \psi) = f \circ \log \psi$ and hence (cf. Prop. 3 of A2), $F \circ \psi \sim 1$, i.e. $F \circ \psi$ is admissible. But $F \circ \psi$ has now the property that $F \circ \psi(I) \subset U_K$ is a p-adic Lie group of dimension 1 (product of Z_p with a finite group). This contradicts a theorem of Tate ([39], §3, Th. 2), hence the result.

A4. The character χ_E

We keep the same hypotheses on K and E as in the previous section. By class field theory, the group $\mathrm{Gal}(\bar{E}/E)^{ab}$ may be identified with the completion $\hat{E}^*$ of E^* with respect to the topology of open subgroups of finite index. In particular, we have an exact sequence

$$1 \longrightarrow U_E \longrightarrow \mathrm{Gal}(\bar{E}/E)^{ab} \longrightarrow \hat{Z} \longrightarrow 1\ ,$$

where $\hat{Z} \cong \prod Z_\ell$ denotes the completion of Z with respect to the topology of subgroups of finite index (cf. for instance Artin-Tate [2] or Cassels-Fröhlich [6], Chap. VI, §2).

Let now π be a uniformizing element of E. The image of π in $\mathrm{Gal}(\bar{E}/E)^{ab}$ generates a subgroup whose closure is isomorphic to $\hat{Z}$, and this gives an isomorphism:

$$\mathrm{Gal}(\bar{E}/E)^{ab} \simeq U_E \times \hat{Z}.$$

Let $\mathrm{pr}_\pi : \mathrm{Gal}(\bar{E}/E)^{ab} \to U_E$ be the projection associated with this decomposition (the Galois extension of E corresponding to $\mathrm{Ker}(\mathrm{pr}_\pi)$ is the composite of all finite abelian extensions of E for which π is a norm, cf. [6], p. 144-145).

On the other hand, the inclusion $E \to K$ defines a homomorphism $\mathrm{Gal}(\bar{K}/K) \to \mathrm{Gal}(\bar{E}/E)$, hence also a homomorphism

$$r_E : G \to \mathrm{Gal}(\bar{E}/E)^{ab}.$$

Define $\chi_{E,\pi}$ (abbr. χ_E) to be the composite homomorphism

$$G \to \mathrm{Gal}(\bar{E}/E)^{ab} \to U_E \xrightarrow{i} U_E,$$

where $i(x) = x^{-1}$ for $x \in U_E$. Observe that the restriction of χ_E to the inertia group of G is $x \mapsto r_E(x^{-1})$, and hence is independent of the choice of π.

PROPOSITION 4 - Let F_π be the Lubin-Tate formal group ([17], see also [6], chap. VI, §3) associated to E and π. Let T be its Tate-module, which is free of rank 1 over the ring O_E of integers of E. The action of $\mathrm{Gal}(\bar{K}/K)$ on T is given by the character $\chi_E : G \to U_E$, defined above.

This follows from the main theorem of [17] (see also [6], Th. 3, p. 149).

COROLLARY - If $E = Q_p$ and $\pi = p$, then the character χ_E coincides with the character χ defined in chap. I, 1.2.

Indeed, the Lubin-Tate group is now the multiplicative group G_m and its Tate module is the module $T_p(\mu)$ defined in chap. I, 1.2.

Remark

If K is locally compact, we may identify G^{ab} to $\hat{K}^*$ and the character χ_E is given by

$$\hat{K}^* \xrightarrow{N} \hat{E}^* \xrightarrow{pr_\pi} U_E \xrightarrow{i} U_E ,$$

where $N = N_{K/E}$ is the norm map. [This follows from the functorial properties of the "reciprocity law" of local class field theory.]

In particular, the restriction of χ_E to the inertia subgroup U_K of G^{ab} is $x \mapsto N_{K/E}(x^{-1})$.

A5. Characters associated with Hodge-Tate decompositions

Retaining the notation of the previous sections, let $\rho: G \to U_E$ be a continuous homomorphism. Let V be a one-dimensional vector space over E; we make G act on V by

$$(s, y) \mapsto \rho(s)y, \qquad s \in G,\ y \in V.$$

Hence V is a G-module. Let $W = C \otimes_{Q_p} V$, where $C = \hat{\bar{K}}$ as

before. This is a d-dimensional vector space over C, where $d = [E: Q_p]$. Every element x of E defines a C-endomorphism a_x of W by

$$a_x(\Sigma c_i \otimes y_i) = \Sigma c_i \otimes xy_i , \quad c_i \in C, \ y_i \in V.$$

We get in this way a representation of E in the C-vector space W; note that the action of a_x commutes with the action of G.

Let $\sigma \in \Gamma_E$ and put

$$W_\sigma = \{w \mid w \in W, a_x(w) = \sigma(x)w \quad \text{for all } x \in E\}.$$

LEMMA 1 - (a) Each W_σ is a one-dimensional C-vector space stable by G.

(b) W is the direct sum of the W_σ's, $\sigma \in \Gamma_E$.

(c) For each $\sigma \in \Gamma_E$, the Galois module W_σ is isomorphic to $C(\sigma \circ \rho)$.

[For the definition of the "twisted" module $C(\sigma \circ \rho)$ see A2, Remark 3.]

Proof. The assertions (a) and (b) are consequences of the well-known fact that $C \otimes_{Q_p} E$ is a product of d copies of C, the projections $C \otimes_{Q_p} E \to C$ being given by the elements of Γ_E.

For (c) note that the same decomposition holds for $V_K = K \otimes_{Q_p} V$, since K contains all the Q_p-conjugates of E; hence for each $\sigma \in \Gamma_E$, there exists a $w \in W_\sigma$ contained in V_K.

For such a w, say $w = \Sigma k_i \otimes y_i$ $(k_i \in K,\ y_i \in V)$ we have

$$\begin{aligned} s(w) &= \Sigma k_i \otimes s(y_i) \\ &= \Sigma k_i \otimes \rho(s) y_i \\ &= a_{\rho(s)} w \\ &= \sigma \circ \rho(s) w \qquad \text{since } w \text{ belongs to } W_\sigma , \end{aligned}$$

and this implies that W_σ is isomorphic to $C(\sigma \circ \rho)$.

If ρ_1 and ρ_2 are two characters of G into K^*, then we shall write $\rho_1 \equiv \rho_2$ if ρ_1 and ρ_2 coincide on an open subgroup of the inertia group of G.

THEOREM 2 - Let ρ, V, W be as above and, for each $\sigma \in \Gamma_E$, let n_σ be an integer. The following are equivalent:

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

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

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

[Recall that χ is the character defined in chap. I, 1.2, and that $\chi_{\sigma E}$ is the one attached to the subfield σE of K, as in A4. Note that, since $\chi_{\sigma E}$ restricted to the inertia group depends only on σE, (i) is meaningful.]

COROLLARY - V is of Hodge-Tate type if and only if there exist $n_\sigma \in Z$ such that $\rho \equiv \prod_{\sigma \in \Gamma_E} \sigma^{-1} \cdot \chi_{\sigma E}^{n_\sigma}$

This follows from (iii) and the fact that $W = C \otimes V$ is the direct sum of the W_σ's.

Proof of Theorem 2

We prove first:

LEMMA 2 - (a) $\chi_E \sim \chi$

(b) If $\sigma \in \Gamma_E$ is not the inclusion map, $\sigma\chi_E \sim 1$.

Proof. Let π be a uniformizing parameter of E, let F_π be the Lubin-Tate group associated to E and π, let T_π be its Tate module, and $V_\pi = T_\pi \otimes Q_p$. Since V_π is a one-dimensional vector space over E, and G acts on V_π through $\chi_E: G \to U_E$ (cf. A4, Prop. 4), the above constructions apply to V_π and χ_E. By a theorem of Tate ([39], §4, Cor. 2 to Th. 3), $W_\pi = C \otimes_{Q_p} V_\pi$ has a Hodge-Tate decomposition of the type

$$W_\pi = W_\pi(0) \oplus W_\pi(1)$$

where $\dim W_\pi(0) = d-1$, $\dim W_\pi(1) = 1$. More precisely, Tate defines canonical isomorphisms $W_\pi(0) = C \otimes_K \mathrm{Hom}_E(t', K)$, where t'

is the (d-1)-dimensional tangent space of the dual of F_π, $W_\pi(1) = (C \otimes_{Q_p} V_p(\mu)) \otimes_K t$, where t is the one-dimensional tangent space to F_π, and $V_p(\mu)$ is the Q_p-vector space of dimension 1 defined in Chap. I, 1.2.

Note that $C \otimes_{Q_p} V_p(\mu)$ is isomorphic to $C(\chi)$, hence one gets an isomorphism

$$W_\pi(1) \cong C(\chi) \otimes_K t.$$

These isomorphisms commute with the action of E.

Since E acts on t by the inclusion map $\sigma_1 : E \to K$, this shows that the component $(W_\pi)_{\sigma_1}$ of W_π is $W_\pi(1)$. Hence, using Lemma 1, we have $C(\chi) \simeq C(\chi_E)$, and this implies $\chi_E \sim \chi$, whence (a). On the other hand, the same argument shows that $(W_\pi)_\sigma$, $\sigma \neq \sigma_1$, are contained in the other factor $W_\pi(0)$ of W_π; hence $C(\sigma \circ \chi_E) \cong C(1)$, (where 1 stands, of course, for the unit character), and this proves (b).

We now go back to the proof of Theorem 2. The equivalence of (ii) and (iii) follows from Lemma 1. To show (i) $\Longleftrightarrow$ (ii), note first that $\chi_{\sigma E}$ takes values in σE^*, hence $\sigma^{-1} \circ \chi_{\sigma E}$ takes values in E^*, and the same is true for the character

$$\rho_1 = \prod_{\sigma \in \Gamma_E} \sigma^{-1} \circ \chi_{\sigma E}^{n_\sigma} .$$

Let $\tau \in \Gamma_E$. We have

$$\tau \circ \rho_l = \prod_{\sigma \in \Gamma_E} \tau\circ\sigma^{-1} \circ \chi_{\sigma E}^{n_\sigma} .$$

From Lemma 2, applied to the field σE, we see that $\tau \circ \sigma^{-1} \circ \chi_{\sigma E} \sim 1$ if $\tau\circ\sigma^{-1}$ is not the identity on σE, i.e. if $\tau \neq \sigma$; if $\tau = \sigma$, we have $\tau\circ\sigma^{-1} \circ \chi_{\sigma E} = \chi_{\sigma E} \sim \chi$. Hence $\tau \circ \rho_l \sim \chi^{n_\tau}$, and (ii) is equivalent to

$$\tau \circ \rho_l \sim \tau \circ \rho \quad \text{for all } \tau \in \Gamma_E .$$

By Prop. 3 of A3, this is equivalent to $\rho_l \equiv \rho$, q.e.d.

A6. Locally compact case

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

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

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

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

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

PROPOSITION 5 - (a) $r_\sigma(u^{-1}) = \sigma^{-1} \circ \chi_{\sigma E}(u)$ for all $u \in U_K$,
(b) the r_σ ($\sigma \in \Gamma_E$) make a Z-basis of $\mathrm{Hom}_{alg}(T, T_E)$.

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

Assertion (a) follows from the remark at the end of A4. 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 $r_\sigma: T \to T_E$ defines by transposition a homomorphism

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

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

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

Assertion (b) then follows from:

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

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

$$\phi([\tau]) = \Sigma n(\tau, s)[s].$$

If $\alpha \in \mathrm{Gal}(\bar{Q}_p / Q_p)$ is equal to the identity on τE, we have $\alpha[\tau] = [\tau]$, hence $\alpha\phi([\tau]) = \phi([\tau])$, 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

$$\phi([\tau]) = \sum_{\sigma \in \Gamma_E} n_\sigma \sum_{s\sigma=\tau} [s]$$

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

This proves the lemma.

PROPOSITION 6 - Let ρ and $(n_\sigma), \sigma \in \Gamma_E$, be as in Th. 2 of A5. Let $r: T \to T_E$ be the morphism defined by

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

The equivalent properties (i), (ii), (iii) of Th. 2 are equivalent to:

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

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

COROLLARY - The following are equivalent:

(a) ρ is locally algebraic.

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

This follows from Theorem 2, combined with Prop. 5 and Prop. 6.

Exercises

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

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

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

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

$$c_K(a) = \sum_i a(e_i)e_i' \quad \text{if } a \in A.$$

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

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

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

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

2) Let $\phi: G^{ab} \longrightarrow K^*$ be a continuous homomorphism, and let a_ϕ be the Q_p-linear endomorphism of K such that the diagram

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

is commutative. Let $L\overline{\phi}$ (resp. $L\overline{\chi}$) be the image of ϕ (resp. χ) in the one-dimensional K-vector space $H^1(G, C)$, cf. A2. Show that

$$L\overline{\phi} = c.\, L\overline{\chi}$$

where $c = -c_K(a_\phi)$. (Check the formula first when K is a Galois

extension of Q_p and $\phi = \sigma^{-1} \circ \chi_K$, $\sigma \in \mathrm{Gal}(K(Q_p))$, in which case $a_\phi = -\sigma^{-1}$ and $c_K(a_\phi)$ is given by Exer. 1, d.)

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

A7. Tate's Theorem

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

THEOREM 3 - Let V be a finite dimensional vector space over Q_p and let $\rho: G^{al} \longrightarrow \mathrm{Aut}(V)$ be an abelian p-adic representation of K. The following are equivalent :

(1) ρ is locally algebraic

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

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

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

Hence we may assume that (*) holds.

Let π be a uniformizing element of K, and let pr_π denote the projection map of G^{ab} onto its inertia group U_K associated to π (cf. A4 and Cassels-Fröhlich [6], p. 144-145). Define a new representation ρ' of G^{ab} by

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

Replacing ρ by ρ' does not affect the local algebraicity (clear), nor the Hodge-Tate property (this follows from A1, Cor. 2 to Th. 1). Since (*) implies that ρ' is semi-simple, this means

that, after replacing ρ by ρ', we may assume that ρ is semi-simple and even (by an easy reduction) that it is simple. Let then $E \subset \mathrm{End}(V)$ be the commuting algebra of ρ. Since ρ is abelian and simple, E is a commutative field, of finite degree over Q_p, and V is a one-dimensional vector space over E; the representation ρ is given by a continuous character $\rho: G \longrightarrow E^*$.

Let now K' be a finite extension of K which is large enough to contain all the Q_p-conjugates of E. Call (1') and (2') the properties corresponding to (1) and (2), when K' is taken as groundfield instead of K. We know (cf. 1.1) that (1) $\Longleftrightarrow$ (1'). By Cor. 2 to Th. 1 of A1, we have (2) $\Longleftrightarrow$ (2'). Hence it is enough to prove that (1') $\Longleftrightarrow$ (2'), and this has been done in A6 (Cor. to Prop. 6), q.e.d.

CHAPTER IV

ℓ-ADIC REPRESENTATIONS ATTACHED TO ELLIPTIC CURVES

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

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

be the corresponding ℓ-adic representation of K, cf. chap. I, 1.2. The main result of this Chapter is the determination of the Lie algebra of the ℓ-adic Lie group $G_\ell = \mathrm{Im}(\rho_\ell)$. This is based on a finiteness theorem of Šafarevič (1.4) combined with the properties of locally algebraic abelian representations (chap. III) and Tate's local theory of elliptic curves with non-integral modular invariant (Appendix, A1). The variation of G_ℓ with ℓ is studied in §3.

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

§1. PRELIMINARIES

1.1. Elliptic curves (cf. Cassels [5], Deuring [9], Igusa [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_o, taken as an origin for the composition law (and often written 0).

Let E be such a curve. It is well known that E may be embedded, as a non-singular cubic, in the projective plane $P_{2/K}$, in such a way that P_o becomes a "flex" (one takes the projective embedding defined by the complete linear series containing the divisor $3.P_o$). 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_o 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 $g_2 \longmapsto u^4 g_2$, $g_3 \longmapsto u^6 g_3$, $u \in K^*$. The modular invariant j of E is

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

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

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

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

Here again, 0 is the point at infinity on the y-axis and the corresponding tangent is the line at infinity. There are corresponding definitions for Δ and j, for which we refer to Deuring [9] or Ogg [20]; note, however, that there is a misprint in Ogg's formula for Δ: the coefficient of β_4^3 should be -8 instead of -1.)

1.2. Good reduction

Let $v \in \Sigma_K$ be a place of the number field K. We denote by O_v (resp. $\underline{m}_v$, 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 $P_{2/K}$ such that the corresponding equation f for E has coefficient in O_v and its reduction $\tilde{f}$ mod $\underline{m}_v$ defines a non-singular cubic $\tilde{E}_v$ (hence an elliptic curve) over the residue field k_v (in other words, the discriminant $\Delta(f)$ of f must be an invertible element of 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 $\Delta(f) \in O_v^*$.

One can prove that the above definition is equivalent to the following one: there is an abelian scheme E_v over $\mathrm{Spec}(O_v)$, in the sense of Mumford [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 O_v) and its reduction $\tilde{j} \bmod \underline{m}_v$ is the j invariant of the reduced curve $\tilde{E}_v$.

The converse is almost true, but not quite: if j belongs to O_v, there is a finite extension L of K such that $E \times_K L$ has good reduction at all the places of L dividing v (this is the "potential good reduction" of Serre-Tate [32], §2). For the proof of this, see Deuring [29], §4, n° 3.

Remark

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

1.3. Properties of V_ℓ related to good reduction

Let ℓ be a prime number. We define, as in chap. I, 1.2, the Galois modules T_ℓ and V_ℓ by:

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

where E_{l^n} is the kernel of $l^n : E(\bar{K}) \longrightarrow E(\bar{K})$.

We denote by ρ_l the corresponding homomorphism of $\mathrm{Gal}(\bar{K}/K)$ into $\mathrm{Aut}(T_l)$. Recall that E_{l^n}, T_l and V_l are of rank 2 over Z/l^nZ, Z_l and Q_l, respectively.

Let now v be a place of K, with $p_v \neq l$ and let $\bar{v}$ be some extension of v to $\bar{K}$; 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 $\bar{v}$ defines an isomorphism of E_{l^n} onto the corresponding module for the reduced curve $\tilde{E}_v$. In particular, E_{l^n}, T_l, V_l are unramified at v (chap. I, 2.1) and the Frobenius automorphism F_{v,ρ_l} of T_l corresponds to the Frobenius endomorphism F_v of $\tilde{E}_v$. Hence:

$$\det(F_{v,\rho_l}) = \det(F_v) = Nv$$

and

$$\det(1-F_{v,\rho_l}) = \det(1-F_v) = 1 - \mathrm{Tr}(F_v) + Nv$$

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

Conversely:

CRITERION OF NÉRON-OGG-ŠAFAREVIČ. If V_l is unramified at v for some $l \neq p_v$, then E has good reduction at v.

For the proof, see Serre-Tate [32], §1.

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

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

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

Remark

For a direct proof of this corollary, see Koizumi-Shimura [11].

Exercise

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

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

(i) $t_v \equiv 0 \bmod \ell^m$ for all $v \in \Sigma_K - S$, $p_v \neq \ell$.

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

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

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

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

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

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

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

(The implication (iv) $\Longrightarrow$ (iii) is easy. For the proof of the converse, use Exer. 2 of chap. I, 1.1.) $\longrightarrow$ [for $m \geq 2$, see Katz [64].]

1.4. Šafarevič's theorem

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

THEOREM - 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 - 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 - Let S be a finite set of places of K containing the divisors of 2 and 3, and such that the ring 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 $g_i \in O_S$ and $\Delta = g_2^3 - 27g_3^2 \in O_S^*$ (the group of units of O_S).

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

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

with $g_i' \in K$. Let v be a place of K not in S. Then, since there is good reduction at v, and since the divisors of 2 and 3 do not belong

to S, the curve E can be written in the form

$$y^2 = 4x^3 - g_{2,v}x - g_{3,v}$$

with $g_{i,v}$ in the local ring at v and the discriminant Δ_v a unit in this ring. Using the properties of the Weierstrass form, there is an element $u_v \in K^*$ such that $g_{2,v} = u_v^4 g_2'$, $g_{3,v} = u_v^6 g_3'$, $\Delta_v = u^{12}\Delta'$; 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 O_S is principal, there is an element $u \in K^*$ 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, $g_i \in O_S$ and $\Delta \in O_S^*$, the lemma is established.

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

$$y^2 = 4x^3 - g_2x - g_3 \qquad (*)$$

with $g_i \in O_S$ and $\Delta = g_2^3 - 27g_3^2 \in O_S^*$. But, since we are free to multiply Δ by any $u \in (O_S^*)^{12}$, and since $O_S^*/(O_S^*)^{12}$ is a finite group, we see that there is a finite set $X \subset O_S^*$ such that any elliptic

curve of the above type can be written in the form (*) with $g_i \in O_S$ and $\Delta \in X$. But, for a given Δ, the equation

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

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

Remark

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

§2. THE GALOIS MODULES ATTACHED TO E

In this section, E denotes an elliptic curve over K. We are interested in the structure of the Galois modules E_{l^n}, T_l, V_l defined in 1.3.

2.1. The irreducibility theorem

Recall first that the ring $\mathrm{End}_K(E)$ of K-endomorphisms of E is either Z or of rank 2 over 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 - Assume that E has no complex multiplication over K.

Then:

(a) V_ℓ is irreducible for all primes ℓ;

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

We need the following elementary result:

LEMMA - Let E be an elliptic curve defined over K with $\mathrm{End}_K(E) = Z$. Then, if $E' \longrightarrow E$, $E'' \longrightarrow E$ 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 $E' \longrightarrow E$ and $E'' \longrightarrow E$. Suppose that E' and E'' are isomorphic over K, and let $E' \longrightarrow E''$ be an isomorphism. If $E \longrightarrow E'$ is the transpose of the isogeny $E' \longrightarrow E$, it has a cyclic kernel of order n', and hence the isogeny $E \longrightarrow E$, obtained by composition of $E \longrightarrow E'$, $E' \longrightarrow E''$, $E'' \longrightarrow E$, has for kernel an extension of $Z/n''Z$ by $Z/n'Z$. But, since $\mathrm{End}_K(E) = Z$, this isogeny must be multiplication by an integer a, and its kernel must therefore be of the form $Z/aZ \times Z/aZ$. Hence n' and n'' divide a. Since $a^2 = n'n''$, we obtain $a = n' = n''$, a contradiction.

Proof of the theorem.

(a) It suffices to show that, if $\mathrm{End}_K(E) = Z$, there is no one-dimensional Q_ℓ-subspace of V_ℓ stable under $\mathrm{Gal}(\bar{K}/K)$. Suppose there were one; its intersection X with T_ℓ would be a submodule of T_ℓ with X and T_ℓ/X free Z_ℓ-modules of rank 1. For $n \geq 0$, consider the image $X(n)$ of X in $E_{\ell^n} = T/\ell^n T$. This is a submodule of E_{ℓ^n} which is cyclic of order ℓ^n and stable by $\mathrm{Gal}(\bar{K}/K)$. Hence it corresponds to a finite K-algebraic subgroup of

E and one can define the quotient curve $E(n) = E/X(n)$. The kernel of the isogeny $E \longrightarrow E(n)$ is cyclic of order ℓ^n. The above lemma then shows that the curves $E(n)$, $n \geq 0$, are pairwise non-isomorphic, contradicting the corollary to Šafarevič's theorem (1.4).

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

Remark

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

2.2. Determination of the Lie algebra of G_ℓ

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

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

Proof. The irreducibility theorem of 2.1 shows that, for any open subgroup U of G_ℓ, V_ℓ is an irreducible U-module. Hence, V_ℓ is an irreducible $\underline{g}_\ell$-module. By Schur's lemma, it follows that the commuting algebra $\underline{g}'_\ell$ of $\underline{g}_\ell$ in $\mathrm{End}(V_\ell)$ is a field; since $\dim V_\ell = 2$, this field is either Q_ℓ or a quadratic extension of Q_ℓ. If $\underline{g}'_\ell = Q_\ell$, then $\underline{g}_\ell$ is equal to either $\mathrm{End}(V_\ell)$, or the subalgebra

$s\ell(V_\ell)$ of $\mathrm{End}(V_\ell)$ consisting of the endomorphisms with trace 0; but, in the second case, the action of $\underline{g}_\ell$ on $\overset{2}{\Lambda} V_\ell$ would be trivial, and this would contradict the fact that the Galois modules $\overset{2}{\Lambda} V_\ell$ and $V_\ell(\mu)$ are isomorphic (chap. I, 1.2). Hence $\underline{g}_\ell = s\ell(V_\ell)$ is impossible.

Suppose now that $\underline{g}'_\ell$ is a quadratic extension of Q_ℓ. Then V_ℓ is a one-dimensional $\underline{g}'_\ell$-vector space and the commuting algebra of $\underline{g}'_\ell$ in $\mathrm{End}(V_\ell)$ is $\underline{g}'_\ell$ itself. Hence $\underline{g}_\ell$ is contained in $\underline{g}'_\ell$, and is <u>abelian</u> ($\underline{g}'_\ell$ is a "non-split Cartan algebra" of $\mathrm{End}(V_\ell)$). After replacing K by a finite extension (this does not affect $\underline{g}_\ell$, cf. chap. I, 1.1), we may then suppose that G_ℓ itself is abelian. The ℓ-adic representation V_ℓ is then semi-simple, abelian and rational. It is, moreover, <u>locally algebraic</u>. To see this, we first remark that, at a place v dividing ℓ, we have $v(j) \geq 0$ since otherwise the decomposition group of v in G_ℓ would be non-abelian by Tate's theory (cf. Appendix, A.1.3); hence, after a finite extension of K, we can assume that E has good reduction at all places v dividing ℓ (cf. 1.2). Let $E(\ell)$ be the ℓ-divisible group attached to E at v (cf. Tate [39], 2.1, example (a)). We have $V_\ell \simeq V_\ell(E(\ell))$ and this module is known to be of Hodge-Tate type (<u>loc. cit.</u>, §4). Using another result of Tate (chap. III, 1.2), this implies that the representation V_ℓ is locally algebraic, as claimed above. (This could also be seen by using, instead of the theory of Hodge-Tate modules, the local results of the Appendix, A2.)

We may now apply to V_ℓ the results of chap. III, 2.3. Hence, there is, for each prime ℓ', a rational, abelian, semi-simple ℓ'-adic representation $W_{\ell'}$ compatible with V_ℓ. But $V_{\ell'}$ is compatible with V_ℓ, and $V_{\ell'}$ is semi-simple. Hence $V_{\ell'}$ is isomorphic to $W_{\ell'}$ (cf. chap. I, 2.3). But we know (chap. III, 2.3)

that we may choose ℓ' such that $W_{\ell'}$ is the direct sum of one-dimensional subspaces stable under $\mathrm{Gal}(\bar{K}/K)$. This contradicts the irreducibility of $V_{\ell'}$. Hence, we must have $\underline{g}'_\ell = \mathbb{Q}_\ell$ and $\underline{g}_\ell = \mathrm{End}(V_\ell)$, q.e.d.

Remark

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

Exercises

(In these exercises, we assume E has no complex multiplication. Let S be the set of places $v \in \Sigma_K$ where E has bad reduction. If $v \in \Sigma_K - S$, 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_ℓ.)

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

2) The eigenvalues of F_v may be identified with complex numbers of the form

$$(Nv)^{\frac{1}{2}} e^{\pm i\varphi_v}, \quad 0 \leq \varphi_v \leq \pi,$$

cf. chap. I, Appendix A.2. Show that the set of v for which φ_v is a given angle φ has density zero. (Show that $\mathrm{Tr}(F_v)^2 = 4(Nv)\cos^2\varphi$ and then use the preceding exercise.)

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

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

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

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

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

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

2.3. The isogeny theorem

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

We need the following result:

PROPOSITION - Let E and E' be elliptic curves over K. The following conditions are equivalent:

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

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

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

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

Clearly (a) implies (b), and (c) implies (d). The implication (b) $\Longrightarrow$ (c) follows from the fact that $Tr(F_v)$ is known when V_ℓ is known. To prove (d) $\Longrightarrow$ (a) one remarks first that the representations of $Gal(\bar{K}/K)$ 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.

Remarks

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):

$$t_v = 1 - Tr(F_v) + Nv$$

$$t'_v = 1 - Tr(F'_v) + Nv$$

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), (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 $\ell \neq p$, 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 $T_p(E_{q'})$ 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 $f : E \times_K L \longrightarrow E' \times_K L$. We will show that f is automatically defined over K. For this, it suffices to show that $f = {}^s f$ for all $s \in \mathrm{Gal}(\bar{K}/K)$, or, equivalently, that $V(f) : V_p(E) \longrightarrow V_p(E')$ commutes with the action of Galois. However, if $G_L = \mathrm{Gal}(\bar{K}/L)$ is the open subgroup of $G = \mathrm{Gal}(\bar{K}/K)$ which corresponds to L, then V(f) commutes with the action of G_L. It is then enough to show that $\mathrm{Hom}_{G_L}(V, V') = \mathrm{Hom}_G(V, V')$. But V and V' are isomorphic as G-modules. Hence we have to show that $\mathrm{End}_{G_L}(V) = \mathrm{End}_G(V)$. But this is clearly true; in fact, G and G_L are open in Aut(V) by the theorem in section 4, and hence their commuting algebra is reduced to the homotheties in each case, i.e. $\mathrm{End}_{G_L}(V) = \mathrm{End}_G(V) = \mathbb{Q}_p$. This completes the proof of the theorem.

Remark

It is very likely that the theorem is true without the hypothesis that j is not integral. This could be proved (by Tate's method [38]) if the following generalization of Šafarevič's theorem were true: given a finite subset S of Σ_K, the abelian varieties over K, of dimension 2, with polarization of degree one, and good reduction outside S, are in finite number (up to isomorphism). → [this has been proved by Faltings, see [54], [56], [82].]

§3. VARIATION OF G_ℓ AND $\tilde{G}_\ell$ WITH ℓ

3.1. Preliminaries

We keep the notations of the preceding paragraphs. For each prime number ℓ, we denote by ρ_ℓ the homomorphism

$$\mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Aut}(T_\ell) \simeq \mathrm{GL}(2, Z_\ell)$$

defined by the action of $\mathrm{Gal}(\bar{K}/K)$ on T_ℓ. The ρ_ℓ's define a homomorphism

$$\rho : \mathrm{Gal}(\bar{K}/K) \longrightarrow \prod_\ell \mathrm{Aut}(T_\ell) \ ,$$

where the product is taken over the set of all prime numbers.

Let $G = \mathrm{Im}(\rho) \subset \prod_\ell \mathrm{Aut}(T_\ell)$ and $G_\ell = \mathrm{Im}(\rho_\ell) \subset \mathrm{Aut}(T_\ell)$, so that G_ℓ is the image of G under the ℓ^{th} projection map. Let $\tilde{G}_\ell$ be the image of G_ℓ in $\mathrm{Aut}(E_\ell) = \mathrm{Aut}(T_\ell/\ell T_\ell) \simeq \mathrm{GL}(2, F_\ell)$.

LEMMA - (1) *The image of* G *by* $\det : \prod \mathrm{Aut}(T_\ell) \longrightarrow \prod Z_\ell^*$ *is open.* (2) *For almost all* ℓ, $\det(G_\ell) = Z_\ell^*$ *and* $\det(\tilde{G}_\ell) = F_\ell^*$.

We know (cf. chap. I, 1.2) that $\det(\rho_\ell) : \mathrm{Gal}(\bar{K}/K) \longrightarrow Z_\ell^*$ is the character χ_ℓ giving the action of $\mathrm{Gal}(\bar{K}/K)$ on ℓ^n-th roots of unity. Hence $\det(G) \subset \prod Z_\ell^*$ is the Galois group $\mathrm{Gal}(K_c/K)$, where $K_c = Q_c K$ is the extension of K generated by all roots of unity. Since one knows that $\mathrm{Gal}(Q_c/Q) = \prod Z_\ell^*$ (cf. for instance [13], chap. IV) it follows that $\det(G)$ is the open subgroup of $\prod Z_\ell^*$ corresponding to the field $K \cap Q_c$, hence (1). Assertion (2) follows

from (1) and the definition of the product topology.

Assume now that E has no complex multiplication. We know (cf. 2.2) that each G_ℓ is open in $\mathrm{Aut}(T_\ell)$. This does not a priori imply that G itself is open. However:

PROPOSITION - The following properties are equivalent:

(i) G is open in $\prod_\ell \mathrm{Aut}(T_\ell)$.

(ii) $G_\ell = \mathrm{Aut}(T_\ell)$ for almost all ℓ.

(iii) $\tilde{G}_\ell = \mathrm{Aut}(E_\ell)$ for almost all ℓ.

(iv) $\tilde{G}_\ell$ contains $\mathrm{SL}(E_\ell)$ for almost all ℓ.

The implications (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) are trivial. Implication (iv) $\Rightarrow$ (i) follows from the following group-theoretical result, whose proof will be given in section 3.4 below:

MAIN LEMMA - Let G be a closed subgroup of $\prod \mathrm{GL}(2, Z_\ell)$ and let G_ℓ and $\tilde{G}_\ell$ denote its images in $\mathrm{GL}(2, Z_\ell)$ and $\mathrm{GL}(2, F_\ell)$ as above. Assume:

(a) G_ℓ is open in $\mathrm{GL}(2, Z_\ell)$ for all ℓ.

(b) The image of G by $\det : \prod \mathrm{GL}(2, Z_\ell) \longrightarrow \prod Z_\ell^*$ is open.

(c) G_ℓ contains $\mathrm{SL}(2, F_\ell)$ for almost all ℓ.

Then G is open in $\prod \mathrm{GL}(2, Z_\ell)$.

Remark

For each integer $n \geq 1$, let E_n be the group of points of $E(\bar{K})$ of order dividing n, and let $\tilde{G}_n$ be the image of the canonical map $\mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{Aut}(E_n) \simeq \mathrm{GL}(2, Z/nZ)$. One sees easily that property (i) above is equivalent to

(i') The index of $\tilde{G}_n$ in $\mathrm{Aut}(E_n)$ is bounded.

3.2. The case of a non-integral j

THEOREM - 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_v which corresponds to j by Tate's theory (cf. Appendix, A.1.1) and let E_q be the corresponding elliptic curve over K_v. 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 $v'(K'^*) = Z$, and let

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

We have $n \geq 1$.

LEMMA 1 - Assume ℓ 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 F_ℓ-basis of E_ℓ.

This is true for the curve E_q over K', cf. Appendix, A.1.5. The result for E follows from the isomorphism $E_{/K'} \tilde{=} E_{q/K'}$.

LEMMA 2 - Let H be a subgroup of $GL(2, F_\ell)$ which acts irreducibly on $F_\ell \times F_\ell$ and which contains a transvection. Then H contains $SL(2, F_\ell)$.

For any transvection $s \in H$, let D_s be the unique one dimensional subspace of $F_\ell \times F_\ell$ 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 $F_\ell \times F_\ell$, 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 $SL(2, F_\ell)$.

Proof of the theorem. Lemma 1 shows that, for almost all ℓ, $I_{v,\ell}$, 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 ℓ. Applying lemma 2 to $\tilde{G}_\ell$ we then see that $\tilde{G}_\ell$ contains $SL(E_\ell)$ for almost all ℓ; hence we have (iv), q.e.d.

Remark

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

3.3. Numerical example

When E is given explicitly and has a non-integral j, one may sometimes determine the finite set of ℓ's with $\tilde{G}_\ell \neq GL(2, F_\ell)$. Take for instance $K = Q$, and E defined by the equation:

$$y^2 + x^3 + x^2 + x = 0 .$$

This is the curve 3^+ of Ogg's list [20]; its j invariant is $2^{11}3^{-1}$,

its discriminant is $\Delta = -2^4 3$, its "conductor" is 24 (it is 2-isogenous to the modular curve J_{24} corresponding to the congruence subgroup $\Gamma_0(24)$, cf. [20]). The existence of a non-trivial 2-isogeny for E shows that $\widetilde{G}_\ell \neq GL(2, F_\ell)$ for $\ell = 2$ ($\widetilde{G}_2$ is cyclic of order 2 and corresponds to the quadratic field $Q(\sqrt{-3})$). But, for $\ell \neq 2$, one has $\widetilde{G}_\ell = GL(2, F_\ell)$. Indeed, $\widetilde{G}_\ell$ has the following properties:

a) $\det(\widetilde{G}_\ell) = F_\ell^*$, cf. 3.1.

b) $\widetilde{G}_\ell$ contains a transvection. This follows from Lemma 1 and the fact that n is here equal to 1.

c) $\widetilde{G}_\ell$ is irreducible. If not, there would be an isogeny $E \longrightarrow E'$ of degree ℓ (defined over Q). The curve E' would have the same conductor 24 as E, hence would be one of the curves 1^-, 2^+, 3^+, 4^-, 5^-, 6^+ of Ogg's list. But Ogg has proved that, for each such curve, there is an isogeny $E' \longrightarrow E$ of degree 1, 2, 4 or 8. The map $E \longrightarrow E' \longrightarrow E$ would then be an endomorphism of E of degree ℓ, 2ℓ, 4ℓ or 8ℓ, and this is impossible for $\ell \neq 2$ since $End(E) = Z$.

Now, using lemma 2, one sees that properties a), b), c) imply that $\widetilde{G}_\ell = GL(2, F_\ell)$.

Exercise

Prove that $\widetilde{G}_\ell = GL(2, F_\ell)$ for all $\ell \neq 2$ when $K = Q$ and E is an elliptic curve of conductor 3.2^λ, where $\lambda \leq 6$. (Use Ogg's Table 1. For $\lambda = 5$, note that the curves 7^+ and 7^- become isomorphic over Q(i), but are not isogenous over Q. For $\lambda = 6$, use a similar argument, and observe that the curves 10^+ and 18^+ do not have the same number of points mod. 5, hence are not isogenous over Q.)

What happens when $\lambda = 7, 8$?

3.4. Proof of the main lemma of 3.1

We need first a few lemmas:

LEMMA 1 - Let $S_\ell = PSL(2, F_\ell) = SL(2, F_\ell)/\{\pm 1\}$, $\ell \geq 3$. Then S_ℓ is a simple group if $\ell \geq 5$. Every proper subgroup of S_ℓ is solvable or isomorphic to the alternating group A_5: the last possibility occurs only if $\ell = \pm 1 \bmod. 5$.

This is well known, cf. for instance Burnside [4], chap. XX.

LEMMA 2 - No proper subgroup of $SL(2, F_\ell)$ maps onto $PSL(2, F_\ell)$.

This is clear for $\ell = 2$, since $PSL(2, F_2) = SL(2, F_2)$. For $\ell \neq 2$, suppose there is such a proper subgroup X. We would then have

$$SL(2, F_\ell) = \{\pm 1\} \times X \ ,$$

and this is absurd, since $SL(2, F_\ell)$ 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 ℓ, hence contained in X.

LEMMA 3 - Let X be a closed subgroup of $SL(2, Z_\ell)$ whose image in $SL(2, F_\ell)$ is $SL(2, F_\ell)$. Assume $\ell \geq 5$. Then $X = SL(2, Z_\ell)$.

We prove by induction on n that X maps onto $SL(2, Z/\ell^n Z)$. 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 $s = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, Z_\ell)$ which is congruent to 1 mod. ℓ^n, there is $x \in X$ with $x \equiv s \bmod. \ell^{n+1}$. Write $s = 1 + \ell^n u$; since $\det(s) = 1$, one has $Tr(u) \equiv 0 \bmod. \ell$. But it is easy to see that any such u is congruent mod. ℓ 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 Z_ℓ. Put

$x = y^{\ell}$. We have:

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

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

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

But $(u + \ell v)^2 \equiv \ell(uv + vu) \bmod \ell^2$, hence:

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

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

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

LEMMA 4 - Let S be a finite set of primes, and $X_S = \prod_{\ell \in S} GL(2, \mathbf{Z}_{\ell})$. The image G_S of G by the projection $X \longrightarrow X_S$ is open in X_S.

Replacing G by an open subgroup if necessary, we can assume that each G_{ℓ}, $\ell \in S$, is contained in the group of elements congruent to 1 mod. ℓ, hence that each G_{ℓ} is a pro-ℓ-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_{ℓ} is

open in $GL(2, Z_\ell)$ by property (a), we see that G_S is open in X_S.

Before we go further, we introduce some terminology. Let Y be a profinite group, and Σ a finite simple group. We say that Σ 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_2/Y_1 is isomorphic to Σ. We denote by $Occ(Y)$ the set of classes of finite simple non abelian groups occurring in Y. If $Y = \varprojlim Y_\alpha$, and each $Y \longrightarrow Y_\alpha$ is surjective, we have

$$Occ(Y) = \bigcup Occ(Y_\alpha) \ .$$

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

$$Occ(Y) = Occ(Y') \cup Occ(Y'') \ .$$

Using these formulae and lemma 1, one gets:

$$Occ(GL(2, Z_\ell)) = Occ(SL(2, Z_\ell)) = Occ(S_\ell)$$

where $S_\ell = PSL(2, F_\ell)$ as before, and:

$$Occ(S_\ell) = \emptyset \text{ if } \ell = 2, 3$$

$$Occ(S_\ell) = \{S_\ell\} = \{A_5\} \text{ if } \ell = 5$$

$$Occ(S_\ell) = \{S_\ell\} \text{ if } \ell \equiv \pm 2 \bmod 5, \ \ell > 5$$

$$Occ(S_\ell) = \{S_\ell, A_5\} \text{ if } \ell \equiv \pm 1 \bmod 5, \ \ell > 5 \ .$$

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

$\ell \notin S \Rightarrow \tilde{G}_\ell \supset SL(2, F_\ell)$. Property (c) shows that such a set exists.

LEMMA 5 - The group G contains $\prod_{\ell \notin S} SL(2, Z_\ell)$.

(This partial product is understood as a subgroup of the full product $X = \prod_\ell GL(2, Z_\ell)$.)

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

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

we then have $S_\ell \in Occ(H_\ell)$. Let $\tilde{H}_\ell$ be the image of H_ℓ in $SL(2, F_\ell)$; the kernel of $H_\ell \longrightarrow \tilde{H}_\ell$ being a pro-ℓ-group, we have $Occ(H_\ell) = Occ(\tilde{H}_\ell)$, hence $S_\ell \in Occ(\tilde{H}_\ell)$. Hence $\tilde{H}_\ell$ maps onto $S_\ell = PSL(2, F_\ell)$, and, by lemma 2, we have $\tilde{H}_\ell = SL(2, F_\ell)$ and, by lemma 3, $H_\ell = SL(2, Z_\ell)$. Hence G contains $SL(2, Z_\ell)$.

LEMMA 6 - The group G contains an open subgroup of $\prod_\ell SL(2, Z_\ell)$.

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

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

Lemma 5 shows that H'_S contains $\prod_{\ell \notin S} SL(2, Z_\ell)$, 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 $\prod_{\ell \in S} GL(2, Z_\ell)$. It is easy to see that this implies that (G_S, G_S) contains an open subgroup of $\prod_{\ell \in S} SL(2, Z_\ell)$ (this follows for instance from the fact that the derived Lie algebra of gl_2 is sl_2). Hence H_S contains an open subgroup U of $\prod_{\ell \in S} SL(2, Z_\ell)$. Using lemma 5, we then see that G contains $U \times \prod_{\ell \notin S} SL(2, Z_\ell)$ which is open in $\prod_\ell SL(2, Z_\ell)$.

End of the proof

Consider the determinant map

$$\det : \prod_\ell GL(2, Z_\ell) \longrightarrow \prod_\ell Z_\ell^* \ ,$$

whose kernel is $\prod SL(2, Z_\ell)$. Hypothesis (c) means that the image of G by this map is open and lemma 6 shows that $G \cap \mathrm{Ker}(\det)$ is open in $\mathrm{Ker}(\det)$. This is enough to imply that G itself is open, q.e.d.

Exercises

1) a) Generalize lemma 3 to $SL(d, Z_\ell)$ for $d \geq 2$, $\ell \geq 5$ (same method).

b) Show that the only closed subgroup of $SL(d, Z_3)$ which maps onto $SL(d, Z/3^2 Z)$ is $SL(d, Z_3)$ itself.

c) Show that the only closed subgroup of $SL(d, Z_2)$ which maps onto $SL(d, Z/2^3 Z)$ is $SL(d, Z_2)$ itself.

2) Let E be the unramified quadratic extension of Q_2, and

O_E its ring of integers. Let $x \longmapsto \bar{x}$ be the non trivial automorphism of E.

a) Show that O_E contains a primitive third root of unity z.

b) Show that O_E contains an element u with $u.\bar{u} = -1$ (take for instance $u = (1+\sqrt{5})/2$).

c) Let α and β be the Z_2-linear endomorphisms defined by $\alpha(x) = zx$, $\beta(x) = \bar{ux}$, where z and u are as in a), b) above. Show that α is of order 3, β of order 4, and $\beta\alpha\beta^{-1} = \alpha^{-1}$, so that α and β generate a non-abelian group G of order 12.

d) Show that G is contained in $SL(O_E) \simeq SL(2, Z_2)$ and that reduction mod. 2 defines a homomorphism of G onto $SL(2, F_2)$. (Hence lemma 3 does not extend to the case $\ell = 2$.)

3) Let $S_9 = SL(2, Z/9Z)$, $S_3 = SL(2, Z/3Z)$ and $g = \mathrm{Ker}(S_9 \longrightarrow S_3)$. The group g is isomorphic to a three-dimensional vector space over 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 $SL(2, Z)$ 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 $SL(2, Z_3)$ is a non-trivial subgroup which is mapped onto S_3; hence lemma 3 does not extend to the case $\ell = 3$.)

APPENDIX

Local Results

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

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

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 $v(j) < 0$.

A.1.1. The elliptic curves of Tate

Let q be an element of K with $v(q) > 0$, and let Γ_q be the discrete subgroup of K^* 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'^*/Γ_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

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

with

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

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

$$j(q) = \frac{(1 + 48b_2)^3}{q\prod_{n\geq 1}(1-q^n)^{24}} = \frac{1}{q} + 744 + 196884q + \dots ,$$

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

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

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 $E = E_q$.

A.1.2. An exact sequence

We conserve the notation of A.1.1. Let E_n be the kernel of multiplication by ℓ^n in K_s^*/Γ_q. If μ_n is the group of ℓ^n-th roots of unity in K_s, we have an injection $\mu_n \longrightarrow E_n$. 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 $Z/\ell^n Z$, we obtain a homomorphism of E_n into $Z/\ell^n Z$, and the resulting sequence

$$0 \longrightarrow \mu_n \longrightarrow E_n \longrightarrow Z/\ell^n Z \longrightarrow 0 \qquad (1)$$

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

$$0 \longrightarrow T_\ell(\mu) \longrightarrow T_\ell(E_q) \longrightarrow Z_\ell \longrightarrow 0 \qquad (2)$$

where $\mathrm{Gal}(K_s/K)$ acts trivially on Z_ℓ. Tensoring with Q_ℓ, we obtain the exact sequence

$$0 \longrightarrow V_\ell(\mu) \longrightarrow V_\ell(E_q) \longrightarrow Q_\ell \longrightarrow 0 \ . \qquad (3)$$

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

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

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

PROPOSITION - (a) The isomorphism $\delta : K^*/K^{*\ell^n} \longrightarrow H^1(G,\mu_n)$ of Kummer theory transforms the class of $q \bmod K^{*\ell^n}$ into x_n.

(b) The element x is of infinite order.

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

$$1 \longrightarrow \mu_n \longrightarrow \bar{K}^* \xrightarrow{\ell^n} \bar{K}^* \longrightarrow 1.)$$

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

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

and hence a homomorphism

$$f : \varprojlim K^*/K^{*\ell^n} \longrightarrow Z_\ell .$$

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

COROLLARY - The sequence (3) does not split.

Assume it does, i.e. there is a G-subspace X of $V_\ell(E_q)$ which is mapped isomorphically onto Q_ℓ. Let $X_T = T_\ell(E_q) \cap X$. The image of X_T in Z_ℓ is $\ell^N Z_\ell$, for some $N \geq 0$. It is then easy to see that $\ell^N x = 0$, and this contradicts the fact that x is of

infinite order.

A.1.3. Determination of $\underline{g}_\ell$ and $\underline{i}_\ell$

We keep the notation of A.1.1 and A.1.2. If X is a one-dimensional subspace of $V_\ell = V_\ell(E)$, let $\underline{r}_X$ denote the subalgebra of $\mathrm{End}(V_\ell)$ consisting of those endomorphisms u for which $u(V_\ell) \subset X$, and let $\underline{n}_X$ be the subalgebra of $\underline{r}_X$ formed by those $u \in \underline{r}_X$ with $u(X) = 0$.

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

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

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

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

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

(b) Since $\ell = p$, we must have $\mathrm{char}(K) = 0$ as $\ell \neq \mathrm{char}(K)$. In this case, the action of $\mathrm{Gal}(\bar{K}/K)$ on $V_\ell(\mu)$ is by means of the character χ_ℓ (cf. chap. I, 1.2) which is of infinite order. It follows

that $\underline{g}_\ell = \underline{r}_X$, where $X = V_\ell(\mu)$; in fact, $\underline{g}_\ell \supset \underline{n}_X$ since the sequence (3) does not split, and we cannot have $\underline{g}_\ell = \underline{n}_X$.

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

Exercise

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

A.1.4. Application to isogenies

Here, we assume that k is finite and K is of characteristic 0 (i.e. K is a finite extension of Q_p).

THEOREM - Let $q, q' \in K^*$ with $v(q)$ and $v(q') > 0$. Let $E = E_q$ and $E' = E_{q'}$ be the corresponding elliptic curves over K. Then the following are equivalent:

(1) E_q is K-isogenous to $E_{q'}$.

(2) There are integers $A, B \geq 1$ such that $q^A = q'^B$.

(3) $V_p(E)$ and $V_p(E')$ are isomorphic as $\mathrm{Gal}(\bar{K}/K)$-modules.

Proof. (2) $\Rightarrow$ (1). It suffices to show that E_q and E_{q^A} are isogenous over K. But every meromorphic function F/G invariant under multiplication by q is invariant under multiplication by q^A; hence the function field of E_q is contained in the function field of E_{q^A}, i.e., E_q and E_{q^A} are isogenous.

(1) $\Rightarrow$ (3). Trivial.

(3) $\Rightarrow$ (2). Choose an isomorphism φ of $V_p(E)$ onto $V_p(E')$. Since $V_p(\mu)$ is the only one-dimensional subspace of $V_p(E)$ (resp. $V_p(E')$) stable by $G = \mathrm{Gal}(\bar{K}/K)$, φ maps $V_p(\mu)$ into itself. Moreover, after multiplying φ by an homothety, we may suppose that φ maps $T_p(E)$ into $T_p(E')$. We then have a commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_p(\mu) & \longrightarrow & T_p(E) & \longrightarrow & Z_p & \longrightarrow & 0 \\ & & \rho\downarrow & & \varphi\downarrow & & \downarrow\sigma & & \\ 0 & \longrightarrow & T_p(\mu) & \longrightarrow & T_p(E') & \longrightarrow & Z_p & \longrightarrow & 0 \end{array} \qquad (4)$$

where ρ (resp. σ) is the multiplication by a p-adic integer r (resp. s). If x, x' are the elements of $\varprojlim H^1(G,\mu_n)$ associated to E and E' (cf. A.1.2), the commutativity of (4) shows that

$$rx = sx' \ .$$

But the valuation v yields a homomorphism of $\varprojlim H^1(G,\mu_n) = \varprojlim K^*/K^{*p^n}$ into Z_p, and we have seen that the image of x is $v(q)$, and the image of x' is $v(q')$. Hence

$$rv(q) = sv(q') \ .$$

We will now show that the element

$$z = q^{v(q')}/q'^{v(q)}$$

is a root of unity. First of all, the image of z in $\varprojlim K^*/K^{*p^n}$ is a p^a-th root of unity; in fact, this image is

$$v(q')x - v(q)x' ,$$

and multiplying by s, we find 0 in virtue of the above formulae (note that $\varprojlim K^*/K^{*p^n}$ is a Z_p-module, hence multiplication by s makes sense). We then use the fact that the kernel of $K^* \longrightarrow \varprojlim K^*/K^{*p^n}$ is k^* (viewed, as usual as a subgroup of K^*). To see this, one decomposes K^* as a product $Z \times k^* \times U^1$, where U^1 is the group of units congruent to 1. The functor $A \longmapsto \varprojlim A/A^{p^n}$ transforms Z into Z_p, kills k^* and leaves U^1 unchanged, since U^1 is a finitely generated Z_p-module. Hence, we have $z \in k^*$, and z is a root of unity. This implies (1), q.e.d.

Remark

The equivalence (1) $\Longleftrightarrow$ (2) was remarked by Tate. It is true without any hypothesis on K.

Exercise

Show that the hypothesis "k is finite" may be replaced by "k is algebraic over F_p."

A.1.5. Existence of transvections in the inertia group

Let E be the elliptic curve E_q (cf. A.1.1), let $\tilde{G}_\ell$ be the image of $\mathrm{Gal}(K_s/K)$ in $\mathrm{Aut}(T_\ell/\ell T_\ell)$, and let $\tilde{I}_\ell$ be the inertia subgroup of $\tilde{G}_\ell$. We assume that v is normalized, i.e. that $v(K^*) = Z$.

PROPOSITION - If ℓ does not divide $v(q)$, then $\tilde{I}_\ell$ contains a transvection, i.e. an element whose matrix is $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ for a suitable F_ℓ-basis of $T_\ell/\ell T_\ell$.

Proof. After possibly replacing K by a larger field, we can suppose that the residue field k is algebraically closed, and that K contains the ℓ-th roots of unity. In fact, if $\ell \neq p$, this last condition is implied by the first; if $\ell = p$, we must adjoin these roots; but the degree of the extension thus obtained divides $\ell-1$, hence is prime to ℓ, and the valuation of q remains prime to ℓ. This being said, the hypothesis on $v(q)$ shows that $q^{1/\ell}$ is not in K. Thus there is an automorphism $s \in \mathrm{Gal}(K_s/K)$ such that $s(q^{1/\ell}) = zq^{1/\ell}$, with $z \neq 1$. Then z is a primitive ℓ-th root of unity, and $z, q^{1/\ell}$ form a basis of T_ℓ modulo ℓT_ℓ. Since $s(z) = z$, we see that the image of s in $\tilde{G}_\ell = \tilde{I}_\ell$ is the required transvection.

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.

A.2.1. The case $\ell \neq p$

Suppose that $\ell \neq p$. Since E has good reduction, the module T_ℓ can be identified with the Tate module $T_\ell(\tilde{E})$ of the reduced curve $\tilde{E}$, cf. 1.3. Hence the inertia algebra i_ℓ is 0. If the

residue field k is finite, the group G_ℓ is topologically generated by the Frobenius F_ℓ. Hence, in this case, $\underline{g}_\ell = \mathrm{Lie}(G_\ell)$ is a one-dimensional subalgebra of $\mathrm{End}(V_\ell)$.

A.2.2. 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^h is the inseparable part of the degree of the homothety "multiplication by p." An elliptic curve is of height 2 if and only if its Hasse invariant (cf. Deuring [9]) is 0. Since E has good reduction, it defines an abelian scheme E_v over O_K, hence a p-divisible group E(p) over O_K (cf. Tate [39], 2.1 - see also [26], §1, Ex. 2). The Tate module of E(p) can be identified with T_p. The connected component $E(p)^o$ of E(p) coincides with the formal group (over 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 $E(p) = E(p)^o$ since the height is assumed to be 2.

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

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

Proof. The Lie algebra $\underline{g}_p$ has the property that $\underline{g}_p z = V_p$ for any non zero element z of V_p (cf. [27], p. 128, Prop. 8). In particular, V_p is an irreducible $\underline{g}_p$-module; its commuting algebra is either a field of degree 2 (which is then necessarily equal to $\underline{g}_p$) or the

field Q_p, in which case $\underline{g}_p$ is a priori $s\ell_2$ or $g\ell_2$. But $\underline{g}_p \neq s\ell_2$ since $\Lambda^2 V_p$ is canonically isomorphic to $V_p(\mu)$, and the action of $\mathrm{Gal}(\bar{K}/K)$ on $V_p(\mu)$ is by means of the character χ_p, which is of infinite order (indeed, no finite extension of K can contain all p^n-th roots of unity, $n = 1, 2, \ldots$). Hence the Lie algebra $\underline{g}_p$ is either $\mathrm{End}(V_p)$ or a non split Cartan subalgebra of $\mathrm{End}(V_p)$. Since the above applies to the completion of the maximal unramified extension of K, we have the same alternative for $\underline{i}_p$. Moreover, $\underline{i}_p$ is contained in $\underline{g}_p$. We have a priori three possibilities:

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

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

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

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

Remarks

1) By a theorem of Tate ([39], §4, cor. 1 to th. 4), the algebra $\underline{g}_p$ is a Cartan subalgebra of $\mathrm{End}(V_p)$ if and only if E(p) has "formal complex multiplication," i.e. if and only if the ring of endomorphisms of E(p), over a suitable extension of K, is of rank 2 over 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 $\underline{g}_p$ is a Cartan subalgebra of $\mathrm{End}(V_p)$, and let $H = \underline{g}_p \cap \mathrm{Aut}(V_p)$ be the corresponding Cartan subgroup of $\mathrm{Aut}(V_p)$. If N is the normalizer of H in $\mathrm{Aut}(V_p)$, then one knows that N/H is cyclic of order 2. Since $G_p \subset N$, it follows that G_p is commutative if and only if $G_p \subset H$. The case $G_p \subset H$ corresponds to the case where the formal complex multiplication of E(p) is

defined over K, and the case $G_p \not\subset H$ 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. g_p itself, viewed as an associative subalgebra of $\mathrm{End}(V_p)$). If U_F denotes the group of units of F, the action of $\mathrm{Gal}(\bar{K}/K)$ on V_p is given by a homomorphism

$$\varphi : \mathrm{Gal}(\bar{K}/K) \longrightarrow U_F$$

By local class field theory, we may identify the inertia group of $\mathrm{Gal}(\bar{K}/K)^{ab}$ with the group U_K of units of K. Hence the restriction φ_I of φ to the inertia group is a homomorphism of U_K into U_F. To determine φ_I, we first remark that the action of 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)

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

Indeed, by a result of Lubin (Ann. of Math. 85, 1967), there is a formal group E' which is K-isogenous to E(p), and has for ring of endomorphisms the ring of integers of F. But then, if E'' is a Lubin-Tate group over K (cf. Lubin-Tate [17]), the formal groups E' and E'' are isomorphic over the completion of the maximal unramified extension of K (cf. Lubin [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].

A.2.3. 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 O_K, cf. Tate [39]). Let $\tilde{A}$ and $\tilde{B}$ (resp. $\tilde{A}(p)$ and $\tilde{B}(p)$) be the reductions of A and B (resp. of A(p) and B(p)).

THEOREM 1 - Let $\tilde{f} : \tilde{A} \longrightarrow \tilde{B}$ be a morphism of abelian varieties, and let $\tilde{f}(p)$ be the corresponding morphism of $\tilde{A}(p)$ into $\tilde{B}(p)$. Assume there is a morphism $f(p) : A(p) \longrightarrow B(p)$ whose reduction is $\tilde{f}(p)$. Then, there is a morphism $f : A \longrightarrow B$ 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).

THEOREM 2 - Assume $T_p(A)$ is a direct sum of Z_p-modules of rank 1 invariant under the action of $Gal(\bar{K}/K)$. Then every endomorphism of $\tilde{A}$ lifts to an endomorphism of A, i.e., the reduction homomorphism $End(A) \longrightarrow End(\tilde{A})$ is surjective (and hence bijective, since it is known to be injective).

Using theorem 1, one sees that it is enough to show that any endomorphism of $\tilde{A}(p)$ can be lifted to an endomorphism of A(p). But the assumption made on T_p implies (cf. Tate [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 - Let H_1, H_2 be two p-divisible groups over O_K, both of height one. Then the reduction map: $Hom(H_1, H_2) \longrightarrow Hom(\tilde{H}_1, \tilde{H}_2)$ is bijective.

Proof. This is clear if both H_1 and H_2 are étale. If both are not étale, their duals are étale and we are reduced to the previous case. If one of them is étale, and the other is not, one checks readily that $\mathrm{Hom}(H_1, H_2) = \mathrm{Hom}(\widetilde{H}_1, \widetilde{H}_2) = 0$.

COROLLARY - Assume:

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

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

Then A is isogenous to a product of abelian varieties of (CM) type (in the sense of Shimura-Taniyama [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 Z_p-modules of rank 1 stable under $\mathrm{Gal}(\bar{K}/K)$. One can find an isogeny $A_1 \longrightarrow A$ such that $T_p(A_1)$ is mapped onto T'. This means that, after replacing A by an isogenous variety, we may apply Th. 2 to A, i.e. $\mathrm{End}(A) \longrightarrow \mathrm{End}(\widetilde{A})$ is an isomorphism. But, since k is finite, it follows from a result of Tate [38] that $Q \otimes \mathrm{End}(\widetilde{A})$ contains a semi-simple commutative Q-subalgebra Λ 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 $Q \otimes \mathrm{End}(A)$. If we now write Λ as a product of commutative fields Λ_a, one sees that A is isogenous to a product $\prod A_a$, where A_a has complex multiplication of type Λ_a, q.e.d.

A.2.4. The case $\ell = p$ with good reduction of height 1

In this section, we assume that the reduced curve $\widetilde{E}$ is of height 1 i.e. that its Hasse invariant is $\neq 0$ (cf. Deuring [9]). The connected component $E_1 = E(p)^0$ of the p-divisible group $E(p)$

attached to E (cf. Tate [39]) is then a formal group of height 1. Since E(p) is an extension of E_1 by an étale group, we obtain an exact sequence of $\mathrm{Gal}(\bar{K}/K)$-modules

$$0 \longrightarrow X \longrightarrow V_p \longrightarrow Y \longrightarrow 0 \ , \qquad (*)$$

where X corresponds to the Tate module of E_1, and Y to the points of order a power of p of $\tilde{E}$.

THEOREM - Suppose that the residue field k is finite. Then the following statements are equivalent:

(a) The elliptic curve E has complex multiplication over K.

(a') The elliptic curve E has complex multiplication over an extension of K.

(b) There exists a one-dimensional subspace D of V_p, which is a supplementary subspace of X, and is stable under the action of G_p.

(b') There exists a one-dimensional subspace D of V_p which is a supplementary subspace of X, and is stable under the action of $\mathfrak{g}_p = \mathrm{Lie}(G_p)$.

Proof. If D is stable under the action of G_p, it is also stable under the action of its Lie algebra $\mathfrak{g}_p$, hence (b) $\Longrightarrow$ (b'). Conversely, if D is stable under $\mathfrak{g}_p$, its transforms by G_p are in finite number; a standard mean value argument then shows that the sequence (*) splits, hence (b') $\Longrightarrow$ (b). The implication (b) $\Longrightarrow$ (a) (the only non-trivial one) follows from the corollary to theorem 2 of A.2.3. Conversely, if E has complex multiplication by an imaginary quadratic field F, the group $\mathrm{Gal}(\bar{K}/K)$ acts on V_p through $F \otimes \mathbb{Q}_p$ (see chap. II, 2.8) and this action is thus semi-simple. Consequently, the

exact sequence (*) splits; this shows that (a) $\Longrightarrow$ (b), hence also that (a') $\Longrightarrow$ (b'). Since (a) $\Longrightarrow$ (a') is trivial, the theorem is proved.

COROLLARY 1 - If E has no complex multiplication, $\underline{g}_p$ is the Borel subalgebra $\underline{b}_X$ of $\mathrm{End}(V_p)$ formed by those $u \in \mathrm{End}(V_p)$ such that $u(X) \subset X$; the inertia algebra $\underline{i}_p$ is the subalgebra $\underline{r}_X$ of $\underline{b}_X$ formed by those $u \in \mathrm{End}(V_p)$ such that $u(V_p) \subset X$.

Let χ_X and χ_Y be the characters of $\mathrm{Gal}(\bar{K}/K)$ defined by the one-dimensional modules X and Y. Since k is finite, χ_Y is of infinite order. If χ is the character defined by the action of $\mathrm{Gal}(\bar{K}/K)$ on $V_p(\mu)$, the isomorphisms

$$X \otimes Y \simeq \Lambda^2 V_p \simeq V_p(\mu)$$

show that $\chi_X \chi_Y = \chi$. Hence the restriction of χ_X and $\chi_X \chi_Y^{-1}$ to the inertia subgroup of $\mathrm{Gal}(\bar{K}/K)$ are of infinite order. This shows first that $\underline{g}_p$ is either $\underline{b}_X$ or a Cartan subalgebra of $\underline{b}_X$; since the second case would imply (b'), it is impossible, hence $\underline{g}_p = \underline{b}_X$. Similarly, one sees first that $\underline{i}_p$ is contained in $\underline{r}_X$, then that its action on X is non trivial; since it is an ideal in $\underline{g}_p = \underline{b}_X$, these properties imply $\underline{i}_p = \underline{r}_X$.

Remark

The above result is given in [25], p. 245, Th. 1, but misstated: the algebra $\underline{r}_X$ has been wrongly defined as formed of those u such that $u(X) = 0$ (instead of $u(V_p) \subset X$).

COROLLARY 2 - If E has complex multiplication, $\underline{g}_p$ is a split Cartan subalgebra of $\mathrm{End}(V_p)$. If D is a supplementary subspace

to X stable under $\mathrm{Gal}(\bar{K}/K)$, then X and D are the characteristic subspaces of g_p and the inertia algebra i_p is the subalgebra of $\mathrm{End}(V_p)$ formed by those $u \in \mathrm{End}(V_p)$ such that $u(D) = 0$, $u(X) \subset X$.

The proof is analogous to the one of Cor. 1 (and in fact simpler).

BIBLIOGRAPHY

[1] E. ARTIN - Collected Papers (edited by S. Lang and J. Tate), Addison-Wesley, 1965.

[2] E. ARTIN and J. TATE - Class field theory. Harvard, 1961.

[3] M. ARTIN et A. GROTHENDIECK - Cohomologie étale des schémas. Sém. Géom. alg., I.H.E.S., 1963/64, Bures sur Yvette.

[4] W. BURNSIDE - The Theory of Groups (Second Edit.). Cambridge Univ. Press, 1911.

[5] J. CASSELS - Diophantine equations with special reference to elliptic curves. J. London Math. Soc., 41, 1966, p. 193-291.

[6] J. CASSELS and A. FRÖHLICH - Algebraic Number Theory. Academic Press, 1967.

[7] N. ČEBOTAREV - Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören. Math. Annalen, 95, 1925, p. 151-228.

[8] C. CHEVALLEY - Deux théorèmes d'arithmétique. J. Math. Soc. Japan, 3, 1951, p. 36-44.

[9] M. DEURING - Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hamburg, 14, 1941, p. 197-272.

[10] J. IGUSA - Fibre systems of Jacobian varieties, I. Amer. J. of Maths., 78, 1956, p. 171-199; II, id., p. 745-760; III, id., 81, 1959, p. 453-476.

[11] S. KOIZUMI and G. SHIMURA - On Specializations of Abelian Varieties. Sc. Papers Coll. Gen. Ed., Univ. Tokyo, 9, 1959, p. 187-211.

[12] S. LANG - Abelian varieties. Intersc. Tracts n° 7, New York, 1957.

[13] S. LANG - Algebraic numbers. Addison-Wesley, New York, 1964.

[14] S. LANG - Diophantine Geometry. Intersc. Tracts n° 11, New York, 1962.

[15] S. LANG - Introduction to transcendental numbers. Addison-Wesley, New York, 1966.

[16] J. LUBIN - One parameter formal Lie groups over p-adic integer rings. Ann. of Maths., 80, 1964, p. 464-484.

[17] J. LUBIN and J. TATE - Formal complex multiplication in local fields. Ann. of Maths., 81, 1965, p. 380-387.

[18] G. D. MOSTOW and T. TAMAGAWA - On the compactness of arithmetically defined homogeneous spaces. Ann. of Maths., 76, 1962, p. 446-463.

[19] D. MUMFORD - Geometric Invariant Theory. Ergebnisse der Math., Bd. 34, Springer-Verlag, 1965.

[20] A. P. OGG - Abelian curves of small conductor. Journ. für die reine und ang. Math., 226, 1967, p. 204-215.

[21] T. ONO - Arithmetic of algebraic tori. Ann. of Maths., 74, 1961, p. 101-139.

[22] G. PÓLYA und G. SZEGÖ - Aufgaben und Lehrsätze aus der Analysis. Band I. Springer-Verlag, 2$^{\text{te}}$ Aufl., 1954.

[23] I. ŠAFAREVIČ - Algebraic Number Fields. Proc. Int. Congress, Stockholm, 1962, p. 163-176 (A.M.S. Transl., Ser. 2, vol. 31, p. 25-39).

[24] J.-P. SERRE - Sur les groupes de congruence des variétés abéliennes. Izv. Akad. Nauk. S.S.S.R., 28, 1964, p. 3-20.

[25] J.-P. SERRE - Groupes de Lie ℓ-adiques attachés aux courbes elliptiques. Coll. Clermont-Ferrand, C.N.R.S., 1964, p. 239-256.

[26] J.-P. SERRE - Groupes p-divisibles (d'après J. Tate). Sém. Bourbaki, 1966/67, exposé 318.

[27] J.-P. SERRE - Sur les groupes de Galois attachés aux groupes p-divisibles. Proceed. Conf. on Local Fields, Springer-Verlag, 1967, p. 113-131.

[28] J.-P. SERRE - Lie algebras and Lie groups. Benjamin, New York, 1965.

[29] J.-P. SERRE - Corps Locaux. Hermann, Paris, 1962.

[30] J.-P. SERRE - Dépendance d'exponentielles p-adiques. Sém. Delange-Pisot-Poitou, 7e année, 1965/66, exposé 15.

[31] J.-P. SERRE - Résumé des cours 1965/66. Annuaire du Collège de France, 1966-67, p. 49-58.

[32] J.-P. SERRE and J. TATE - Good reduction of abelian varieties, Ann. of Math. 88 (1968), p. 492-517

[33] G. SHIMURA - A reciprocity law in nonsolvable extensions. Journal für die reine und ang. Math., 221, 1966, p. 209-220.

[34] G. SHIMURA and Y. TANIYAMA - Complex multiplication of abelian varieties and its applications to number theory. Publ. Math. Soc. Japan, 6, 1961.

[35] Y. TANIYAMA - L functions of number fields and zeta functions of abelian varieties. Journ. Math. Soc. Japan,

9, 1957, p. 330-366.

[36] J. TATE - Algebraic cycles and poles of zeta functions. Proc. Purdue Univ. Conf., 1963, p. 93-110, New York, 1965.

[37] J. TATE - On the conjecture of Birch and Swinnerton-Dyer and a geometric analog. Sém. Bourbaki, 1965/66, exposé 306.

[38] J. TATE - Endomorphisms of Abelian Varieties over finite fields. Inven. math., 2, 1966, p. 134-144.

[39] J. TATE - p-divisible groups. Proc. Conf. on Local Fields, Springer-Verlag, 1967, p. 158-183.

[40] A. WEIL - Variétés abéliennes et courbes algébriques. Hermann, Paris, 1948.

[41] A. WEIL - On a certain type of characters of the idèle-class group of an algebraic number field. Proc. Int. Symp. Tokyo-Nikko, 1955, p. 1-7.

[42] A. WEIL - On the theory of complex multiplication. Proc. Int. Symp. Tokyo-Nikko, 1955, p. 9-22.

[43] A. WEIL - Adèles and algebraic groups (Notes by M. Demazure and T. Ono). Princeton, Inst. Adv. Study, 1961.

[44] A. WEIL - Basic Number Theory. Springer-Verlag, 1967.

[45] A. WEIL - Ueber die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. Math. Annalen, 168, 1967, p. 149-156.

[46] H. WEYL - Über die Gleichverteilung von Zahlen mod. Eins. Math. Annalen, 77, 1914, p. 313-352.

SUPPLEMENTARY BIBLIOGRAPHY

[47] S. BLOCH and K. KATO—p-adic étale cohomology, Publ. Math. I.H.E.S. 63 (1986), p. 107-152.

[48] F. BOGOMOLOV—Sur l'algébricité des représentations l-adiques, C. R. Acad. Sci. Paris 290 (1980), p. 701-703.

[49] H. CARAYOL—Sur les représentations l-adiques associées aux formes modulaires de Hilbert, Ann. Sci. E.N.S. 19 (1986), p. 409-468.

[50] P. DELIGNE—Formes modulaires et représentations l-adiques, Séminaire Bourbaki 1968/69, exposé 355, Lecture Notes in Math. 179, p. 139-186, Springer-Verlag, 1971.

[51] P. DELIGNE—Valeurs de fonctions L et périodes d'intégrales, Proc. Symp. Pure Math. 33, A.M.S. (1979), vol. 2, p. 313-346.

[52] P. DELIGNE—Hodge cycles on abelian varieties, Lecture Notes in Math. 900, p. 9-100, Springer-Verlag, 1982.

[53] P. DELIGNE—Motifs et groupes de Taniyama, Lecture Notes in Math. 900, p. 261-279, Springer-Verlag, 1982.

[54] G. FALTINGS—Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. 73 (1983), p. 349-366; Erratum, ibid. 75 (1984), p. 381.

[55] G. FALTINGS—p-adic Hodge theory, Journal A.M.S. 1 (1988), p. 255-299.

[56] G. FALTINGS, G. WÜSTHOLZ et al—Rational Points, Vieweg, 1984.

[57] J.-M. FONTAINE—Groupes p-divisibles sur les corps locaux, Astérisque 47-48, S.M.F., 1977.

[58] J.-M. FONTAINE—Modules galoisiens, modules filtrés et anneaux de Barsotti-Tate, Astérisque 65 (1979), p. 3-80.

[59] J.-M. FONTAINE—Sur certains types de représentations p-adiques du groupe de Galois d'un corps local, construction d'un anneau de Barsotti-Tate, Ann. of Math. 115 (1982), p. 529-577.

[60] J.-M. FONTAINE—Formes différentielles et modules de Tate des variétés abéliennes sur les corps locaux, Invent. Math. 65 (1982), p. 379-409.

[61] J.-M. FONTAINE—Représentations p-adiques, Proc. Int. Congress 1983, vol. 1, p. 475-486.

[62] J.-M. FONTAINE and W. MESSING—p-adic periods and p-adic étale cohomology, Contemp. Math. 67 (1987), p. 179-207.

[63] G. HENNIART—Représentations l-adiques abéliennes, Séminaire de Théorie des Nombres 1980/81, Birkhäuser-Verlag 1982, p. 107-126.

[64] N. KATZ—Galois properties of torsion points on abelian varieties, Invent. Math. 62 (1981), p. 481-502.

[65] R. P. LANGLANDS—Modular forms and l-adic representations, Lecture Notes in Math. 349, p. 361-500, Springer-Verlag, 1973.

[66] R. P. LANGLANDS—Automorphic representations, Shimura varieties, and motives. Ein Märchen, Proc. Symp. Pure Math. 33, A.M.S. (1979), vol. 2, p. 205-246.

[67] D. MUMFORD—Families of abelian varieties, Proc. Symp. Pure Math. IX, A.M.S. 1966, p. 347-351.

[68] M. OHTA—On l-adic representations attached to automorphic forms, Jap. J. Math. 8 (1982) p. 1-47.

[69] K. RIBET—On l-adic representations attached to modular forms, Invent. Math. 28 (1975), p. 245-275; II, Glasgow Math. J. 27 (1985), p. 185-194.

[70] K. RIBET—Galois action on division points of abelian varieties with many real multiplications, Amer. J. Math. 98 (1976), p. 751-804.

[71] K. RIBET—Galois representations attached to eigenforms with Nebentypus, Lecture Notes in Math. 601, p. 18-52, Springer-Verlag, 1977.

[72] S. SEN—Lie algebras of Galois groups arising from Hodge-Tate modules, Ann. of Math. 97 (1973), p. 160-170.

[73] J.-P. SERRE—Une interprétation des congruences relatives à la fonction τ de Ramanujan, Séminaire D.P.P. 1967/68, n°14 (=Oe.80).

[74] J.-P. SERRE—Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures), Séminaire D.P.P. 1969/70, n°19 (=Oe.87).

[75] J.-P. SERRE—Sur les groupes de congruence des variétés abéliennes II, Izv. Akad. Nauk S.S.S.R. 35 (1971), p. 731-735 (=Oe.89).

[76] J.-P. SERRE—Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (1972), p. 259-331 (=Oe.94).

[77] J.-P. SERRE—Congruences et formes modulaires (d'après H.P.F. Swinnerton-Dyer), Séminaire Bourbaki 1971/72, n°416 (=Oe.95).

[78] J.-P. SERRE—Représentations l-adiques, Kyoto Symp. on Algebraic Number Theory, 1977, p. 177-193 (=Oe.112).

[79] J.-P. SERRE—Groupes algébriques associés aux modules de Hodge-Tate, Astérisque 65 (1979), p. 155-188 (=Oe.119).

[80] J.-P. SERRE—Résumé des cours de 1985-86, Annuaire du Collège de France, 1986, p. 95-100.

[81] H. P. F. SWINNERTON-DYER—On l-adic representations and congruences for coefficients of modular forms, Lecture Notes in Math. 350, p. 1-55, Springer-Verlag, 1973; II, ibid. 601, p. 63-90, Springer-Verlag, 1977.

[82] L. SZPIRO—Séminaire sur les pinceaux arithmétiques: la conjecture de Mordell, Astérisque 127, S.M.F., 1985.

[83] M. WALDSCHMIDT—Transcendance et exponentielles en plusieurs variables, Invent. Math. 63 (1981), p. 97-127.

[84] A. WILES—On ordinary λ-adic representations associated to modular forms, preprint, Princeton, 1987.

[85] J.-P. WINTENBERGER—Groupes algébriques associés à certaines représentations p-adiques, Amer. J. Math. 108 (1986), p. 1425-1466.

[86] Y. G. ZARHIN—Abelian varieties, l-adic representations and SL_2, Math. USSR Izv. 14 (1980), p. 275-288.

[87] Y. G. ZARHIN—Abelian varieties, l-adic representations and Lie algebras. Rank independence on l, Invent. Math. 55 (1979), p. 165-176.

[88] Y. G. ZARHIN—Weights of simple Lie algebras in the cohomology of algebraic varieties, Math. USSR Izv. 24 (1985), p. 245-281.

INDEX