Abelian *l*-Adic Representations and Elliptic Curves

Jean-Pierre Serre

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

W. A. BENJAMIN, INC.

NEW YORK • AMSTERDAM

1968

ABELIAN ℓ-ADIC REPRESENTATIONS
AND ELLIPTIC CURVES

Library of Congress Catalog Card Number 68-20843
Manufactured in the United States of America

*The manuscript was put into production on January 5, 1968;
this volume was published on April 8, 1968.*

W. A. BENJAMIN, INC.
New York, New York 10016

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 are 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

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 " <u>locally algebraic</u> " 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 <u>ipso facto</u> 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 <u>elliptic curve</u> E. Its aim is to determine, as precisely as possible, the image of the Galois group by ρ_ℓ, or at least its <u>Lie algebra</u>. 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], [30] 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.

$\mathbf{Z}$ (resp. $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$) is the ring (resp. the field) of integers (resp. of rational numbers, of real numbers, of complex numbers).

If p is a prime number, $\mathbf{F}_p$ denotes the prime field $\mathbf{Z}/p\mathbf{Z}$ and $\mathbf{Z}_p$ (resp. $\mathbf{Q}_p$) the ring of p-adic integers (resp. the field of p-adic rational numbers). One has:

$$\mathbf{Z}_p = \varprojlim \mathbf{Z}/p^n\mathbf{Z} \quad , \quad \mathbf{Q}_p = \mathbf{Z}_p[\tfrac{1}{p}] .$$

Prime numbers

They are denoted by $\ell, \ell', p, \ldots$; 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 $\mathrm{Gal}(L/K)$; it is a projective limit of finite groups.

<u>Algebraic groups</u>

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, $GL_V(K) = \mathrm{Aut}(V)$.

CONTENTS

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 $\mathrm{Aut}(V) \simeq GL(n, Q_\ell)$.

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_m of ℓ^m-th roots of unity, and hence also on $T_\ell(\mu) = \varprojlim \mu_m$. 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

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

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

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