Review of **Abelian l-adic Representations and Elliptic Curves**

Kenneth A. Ribet, U.C. Math Department, Berkeley CA 94720

Addison-Wesley has just reissued Serre's 1968 treatise on l-adic representations in their Advanced Book Classics series. This circumstance presents a welcome excuse for writing about the subject, and for placing Serre's book in a historical perspective.

The theory of l-adic representations is an outgrowth of the study of abelian varieties in positive characteristic, which was initiated by Hasse and Deuring (see, e.g., [3], [1]) and continued in Weil's 1948 treatise [12]. Over the complex field $\mathbf{C}$, an abelian variety A of dimension g may be viewed as an (algebrizable) complex torus W/L, where $L \approx \mathbf{Z}^{2g}$ is a lattice in the $\mathbf{C}$-vector space W of dimension g. The classical study of A relies heavily on the lattice L, which is intrinsically the first homology group $H_1(A, \mathbf{Z})$. However, the quotients L/nL (for $n \geq 1$) have a purely algebraic definition. Indeed, over $\mathbf{C}$ the quotient L/nL is canonically the group

$$A[n] = \{\, P \in A \mid n \cdot P = 0 \,\}$$

of n-division points on A. Over an arbitrary field K, one defines $A[n]$ as the group of points on A (with values in a separable closure $\overline{K}$ of K) of order dividing n. When n is prime to the characteristic of K, $A[n]$ is a free $\mathbf{Z}/n\mathbf{Z}$-module of rank $2g = 2 \dim A$, just as in the classical case. Moreover, the module $A[n]$ carries natural commuting actions of the Galois group $\mathrm{Gal}(\overline{K}/K)$ and the ring $\mathrm{End}_K(A)$ of K-endomorphisms of A. Most information provided by L can be extracted from the collection of groups $A[l^\nu]$ ($\nu \geq 1$), where l is a fixed prime which is different from the characteristic of K.

In the 1950's, J. Tate suggested packaging together the groups $A[l^\nu]$ in the projective system

$$\cdots \to A[l^3] \to A[l^2] \to A[l]$$

in which the maps are induced by multiplication by l. The projective limit $T_l(A) = \varprojlim A[l^\nu]$ is a free rank-$2g$ module over $\mathbf{Z}_l$ (the $\mathbf{Z}_l$-adic Tate module attached to A). The $\mathbf{Q}_l$-adic Tate module

$$V_l(A) = T_l(A) \otimes_{\mathbf{Z}_l} \mathbf{Q}_l$$

is then a $\mathbf{Q}_l$-vector space of dimension $2g$. The natural continuous representation

$$\rho_{l,A} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}\, T_l(A) \subseteq \mathrm{Aut}\, V_l(A)$$

is the *l-adic representation of* $\mathrm{Gal}(\overline{K}/K)$ *attached to* A.

The image of this representation is *a priori* a compact, hence closed, subgroup of the l-adic Lie group $\mathrm{Aut}\, V_l(A) \approx \mathbf{GL}(2g, \mathbf{Q}_l)$. It is therefore a Lie subgroup of $\mathrm{Aut}\, V_l(A)$. Its Lie algebra $\mathfrak{g}_l$ is then a subalgebra of $\mathfrak{gl}(V_l(A)) \approx \mathfrak{gl}(2g, \mathbf{Q}_l)$ which measures $\rho_{l,A}(\mathrm{Gal}(\overline{K}/K))$ "up to finite groups." In particular, $\mathfrak{g}_l$ remains unchanged if K is replaced by a finite extension of K in $\overline{K}$.

A fundamental problem is to determine the Lie algebras $\mathfrak{g}_l$ attached to A when the base field K is a number field. The conjectured "answer" involves fixing an embedding $K \hookrightarrow \mathbf{C}$ and exploiting the resulting interpretation of $V_l = V_l(A)$ as $L \otimes \mathbf{Q}_l$, where L is the lattice $H_1(A(\mathbf{C}), \mathbf{Z})$, as above. The Hodge decomposition of $L \otimes \mathbf{C}$ defines a certain algebraic subgroup $\mathsf{MT}(A)$ of the algebraic group $\mathbf{GL}_{L\otimes\mathbf{Q}} \approx \mathbf{GL}(2g)$ over $\mathbf{Q}$. This is the *Mumford-Tate group* of $A/\mathbf{C}$. Its Lie algebra is a subalgebra $\mathfrak{h}$ of $\mathfrak{gl}(L \otimes \mathbf{Q})$, so that $\mathfrak{h}_l = \mathfrak{h} \otimes \mathbf{Q}_l$ is a subalgebra of $\mathfrak{gl}(V_l)$. An important conjecture of Mumford and Tate [5, 7] states that $\mathfrak{g}_l = \mathfrak{h}_l$ inside $\mathfrak{gl}(V_l)$ for each prime l. In particular, the family of Lie algebras $\mathfrak{g}_l$ is conjectured to be "independent of l."

In proving special cases of this conjecture, it has often been useful to deal with the entire system $(\rho_{l,A})$ as l varies, rather than to work with a single $\rho_{l,A}$. Transferring information from one $\rho_{l,A}$ to another is frequently possible because the following compatibility, which was first stressed by Y. Taniyama [11]. Consider a prime ideal $\mathfrak{p}$ of the ring of integers of K and try to reduce A "mod $\mathfrak{p}$." The attempt succeeds for all $\mathfrak{p}$ outside a finite set of primes (those at which A has bad reduction). Assuming that $\mathfrak{p}$ lies outside this exceptional set, the representation $\rho_{l,A}$ is first of all unramified at $\mathfrak{p}$ whenever l is prime to $\mathfrak{p}$. This means that we can associate to $\mathfrak{p}$ a distinguished conjugacy class in the image of $\rho_{l,A}$, the set of Frobenius elements for $\mathfrak{p}$ in the image. Taking the characteristic polynomial of any such Frobenius element, we obtain a polynomial $P_{\mathfrak{p},l}(T) \in \mathbf{Q}_l[T]$. The essential fact is that this polynomial lies in $\mathbf{Q}[T]$ and depends only on $\mathfrak{p}$, but not on the prime number l. This compatibility property is proved by regarding $P_{\mathfrak{p},l}$ as the characteristic polynomial of the Frobenius *endomorphism* of A mod $\mathfrak{p}$, and applying results of Weil.

The Mumford-Tate conjecture was first proved for complex multiplication (CM) abelian varieties as a corollary of the main theorems of Shimura and Taniyama [10]. With this case understood, the simplest case to attack was that for which A is an elliptic curve ($g = 1$) with no complex multiplications, i.e., one for which $\mathrm{End}_{\overline{K}}(A) = \mathbf{Z}$. This case was treated by J-P. Serre in the book under review, or rather in the original 1968 Benjamin edition of the book. Serre showed that $\mathfrak{g}_l = \mathfrak{gl}(V_l) \approx \mathfrak{gl}(2, \mathbf{Q}_l)$, by an argument which we now outline.

The first point is that, for non-CM elliptic curves, V_l is irreducible as a $\mathfrak{g}_l$-module. This is a theorem of Shafarevich, which in turn depends on Siegel's theorem on the finiteness of integral points on curves. The second point is that $\mathfrak{g}_l$ cannot be contained in the subalgebra $\mathfrak{sl}(V_l)$ of $\mathfrak{gl}(V_l)$, because of information on the determinant of $\rho_{l,A}$ which is furnished by the e_m pairings of Weil. This leaves two possibilities for $\mathfrak{g}_l$: either $\mathfrak{g}_l$ is the desired $\mathfrak{gl}(2, \mathbf{Q}_l)$, or else $\mathfrak{g}_l$ is a non-split Cartan subalgebra of $\mathfrak{gl}(2, \mathbf{Q}_l)$ (an abelian semisimple algebra coming from a quadratic field extension of $\mathbf{Q}_l$). The second possibility occurs for "half" the prime numbers l in the excluded case of an elliptic curve with complex multiplication — those l which remain inert in the field of complex multiplication. The other primes l in the CM case lead to *split* Cartan subalgebras of $\mathfrak{gl}(2, \mathbf{Q}_l)$, which act *reducibly* on their representation spaces. Serre showed that if at least one $\mathfrak{g}_l$ is a Cartan subalgebra, then there are many $\mathfrak{g}_l$ which are split Cartan subalgebras, even in the non-CM case. Once proved, this assertion eliminates the second possibility in the non-CM case, since split Cartan subalgebras of $\mathfrak{gl}(2, \mathbf{Q}_l)$ are incompatible with Shafarevich's theorem. To prove the assertion, Serre made a detailed study of semisimple abelian l-adic representations with certain local properties; this explains their appearance in the title of the book.

Since the publication of Serre's book in 1968, there have been numerous advances in the theory of l-adic representations attached to abelian varieties over number fields. The most spectacular are contained in Faltings' paper on the Mordell Conjecture [2], which proves two important facts about the representations $\rho_{l,A}$. First of all, Faltings proved that each $\rho_{l,A}$ is a semisimple representation of $\mathrm{Gal}(\overline{K}/K)$ over $\mathbf{Q}_l$. Secondly, Faltings proved the Tate Conjecture on endomorphisms of abelian varieties, which states that the natural map

$$\mathrm{End}(A) \otimes \mathbf{Q}_l \hookrightarrow \mathrm{End}_{\mathfrak{g}_l}(V_l)$$

is an isomorphism for all l. This fact immediately rules out the Cartan subalgebra case in the elliptic curve argument, those proving that $\mathfrak{g}_l = \mathfrak{gl}(2, \mathbf{Q}_l)$ in the case of non-CM elliptic curves. Similarly, the theorems of Faltings easily prove the conjecture $\mathfrak{g}_l = \mathfrak{h} \otimes \mathbf{Q}_l$ in the case of abelian varieties with real multiplications: A's whose endomorphism algebras are totally real number fields of degree $2\dim(A)$ over $\mathbf{Q}$. Finally, using Faltings' theorems, and a family of new ideas suggested by papers of Yu. Zarhin, Serre proved several years ago [9] that $\mathfrak{g}_l = \mathfrak{h} \otimes \mathbf{Q}_l$ whenever A has no non-trivial endomorphisms and the dimension of A is 2, 6, or an odd number.

Despite these recent developments, the 1968 book of Serre is hardly outmoded. For one thing, as the cover of the new edition reminds us, it's the only book on the subject. More importantly, it can be viewed as a toolbox which contains clear and concise explanations of fundamental facts about a series of related topics: abstract l-adic representations, Hodge-Tate decompositions, elliptic curves, L-functions, etc. The algebraic groups introduced in the book form the toric part (or "Serre group") of the Taniyama group of [4] (see also [6]). The tools introduced in this book have been, and will continue to be, extremely useful in other contexts, such as the study of l-adic representations arising from étale cohomology groups $H^i(X_{\overline{K}}, \mathbf{Q}_l)$ with $i > 1$ (in particular, representations associated to modular forms). The book remains a valuable textbook and reference.

The new edition differs from the old one in minor ways. First, misprints in the first edition have been corrected. (A list of errata to the first edition was given at the end of [8].) Secondly, a number of remarks concerning recent developments have been squeezed into the original text. (They are prefaced by arrows $\rightarrow$ and appear in **heavy type**.) Thirdly, a 42-item bibliography of post-1968 articles has been added. Finally, a new two-page "Special Preface" begins the volume. In this preface, the condition "$\mathrm{End}_K A = \mathbf{Z}$" should read "$\mathrm{End}_{\overline{K}} A = \mathbf{Z}$," as was pointed out to me by the author.

References

[1] Deuring, M. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hans. Univ. **14**, 197–272 (1941)

[2] Faltings, G. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math **73**, 349–366 (1983). English translation in: Arithmetic Geometry, G. Cornell and J. H. Silverman, eds. New York: Springer-Verlag (1986)

[3] Hasse, H. Zur Theorie des abstrakten elliptischen Funktionenkörper, I–III. Journal für die reine und angewandte Mathematik **175**, 55–62, 69–88, 193–208 (1936). (= Mathematische Abhandlungen **2**, 223–266)

[4] Langlands, R.P. Automorphic representations, Shimura varieties, and motives. Ein Märchen. Proc. Symp. Pure Math **33**(2), 205–246 (1979)

[5] Mumford, D.: Families of Abelian varieties. Proc. Symp. Pure Math. **9**, 347–351 (1966)

[6] Deligne, P., Milne, J.S., Ogus, A and K-y. Shih. Hodge Cycles, Motives, and Shimura Varieties. Lecture Notes in Mathematics **900** (1982)

[7] Serre, J-P.: Représentations l-adiques. In: Algebraic Number Theory (International Symposium, Kyoto 1976), S. Iyanaga, ed. Tokyo: Japanese Society for the Promotion of Science (1977)

[8] Serre, J-P.: Groupes algébriques associés aux modules de Hodge-Tate. Astérisque **65**, 155–188 (1979)

[9] Serre, J-P.: Course at the Collège de France, 1984–85

[10] Shimura, G. and Y. Taniyama. Complex Multiplication of Abelian Varieties and its Applications to Number Theory. Tokyo: The Mathematical Society of Japan (1961)

[11] Taniyama, Y. L-functions of number fields and zeta functions of abelian varieties. J. Math. Soc. Japan **9**, 330–366 (1957)

[12] Weil, A. Courbes Algébriques et Variétés Abéliennes (réimpression). Paris: Hermann (1971).