A CONNECTEDNESS CRITERION FOR ℓ-ADIC GALOIS REPRESENTATIONS

BY

Michael Larsen*

Department of Mathematics, University of Pennsylvania

Philadelphia, PA 19104, USA

AND

Richard Pink

Fakultät für Mathematik und Informatik, Universität Mannheim

D-68131 Mannheim, Germany

ABSTRACT

To every compatible system of Galois representations of a global field K, there is associated a natural invariant K^{conn}, the smallest extension of K over which the associated algebraic monodromy groups become connected. We present a purely field-theoretic construction of K^{conn} for all Galois representations arising from cohomology.

0. Introduction

Let K be a global field, that is, a number field or a function field in one variable over a finite field. Let X be a complete non-singular variety over K, and k a non-negative integer. Let $\bar{K}$ denote a separable closure of K and $\bar{X}$ the variety obtained from X by extension of scalars to $\bar{K}$. Then the dimension N of the ℓ-adic étale cohomology groups $H^k(\bar{X}, \mathbb{Q}_\ell)$ is independent of ℓ, and the natural action of the Galois group $\mathrm{Gal}(\bar{K}/K)$ corresponds, after choosing a basis, to a continuous representation $\rho_\ell\colon \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_N(\mathbb{Q}_\ell)$. The Zariski closure of $\mathrm{im}(\rho_\ell)$ inside the algebraic group $\mathrm{GL}_{N,\mathbb{Q}_\ell}$ is called the algebraic monodromy group. Denote it by G_ℓ and let G_ℓ° be its identity component.

In [9] and [10], Serre showed that the open normal subgroup $\rho_\ell^{-1}(G_\ell^\circ)$ of $\mathrm{Gal}(\bar{K}/K)$ is independent of ℓ. This is proved for the Tate modules of an abelian variety in [10], but the argument works in general (*cf.* also [5]). If K^{conn} denotes

* Partially supported by the Sloan Foundation and by NSF Grant DMS94-00833

the finite extension of K corresponding to this open subgroup, then by Serre's result K^{conn} is characterized uniquely as the smallest subextension of $\bar{K}$ such that the Zariski closure of $\rho_\ell(\mathrm{Gal}(\bar{K}/K^{\mathrm{conn}}))$ is connected for any fixed ℓ, or equivalently for all ℓ. Letting K_ℓ denote the (usually infinite) extension of K corresponding to the kernel of ρ_ℓ, it is clear from this property that $K^{\mathrm{conn}} \subset K_\ell$. Serre asked [11] whether the field K^{conn} can be characterized purely in terms of the K_ℓ, or, more precisely, whether the inclusion

$$K^{\mathrm{conn}} \subset \bigcap_{\ell > n} K_\ell$$

is an equality for all n. We can answer a somewhat stronger question affirmatively:

THEOREM 0.1: *Let E be any finite extension of $\mathbb{Q}$. Let $\mathcal{L}$ be a set of rational primes which includes all those that split completely in E except a set of Dirichlet density zero. Then*

$$K^{\mathrm{conn}} = \bigcap_{\ell \in \mathcal{L}} K_\ell.$$

The authors would like to thank the Hebrew University for its hospitality while this work was carried out and J-P. Serre for his permission to reproduce Theorem 1.2 below.

1. Galois Representations and Maximal Tori

The representations ρ_ℓ: $\mathrm{Gal}(\bar{K}/K) \to GL_N(\mathbb{Q}_\ell)$ associated with $H^k(\bar{X}, \mathbb{Q}_\ell)$ form a strictly compatible system in the sense of Serre [6]. This means the following. Let Σ denote the finite set of primes of K where X has bad reduction, and consider any prime $v \notin \Sigma$ of K and any rational prime ℓ that is not divisible by v. Then it is known firstly that the restriction of ρ_ℓ to any decomposition group at v is unramified. This property implies that $\rho_\ell(\mathrm{Frob}_v)$ determines a well-defined conjugacy class in $\mathrm{im}(\rho_\ell)$, and so its characteristic polynomial depends at most on ℓ and v. Secondly it is known that the coefficients of this characteristic polynomial, which *a priori* lie in $\mathbb{Q}_\ell$, are already in $\mathbb{Z}$. Thirdly, as elements of $\mathbb{Z}[x]$, the characteristic polynomials of $\rho_\ell(\mathrm{Frob}_v)$ can be compared, and they turn out to be independent of ℓ. We can (and will) therefore speak of "the characteristic polynomial" or "the eigenvalues" of Frob_v for any $v \notin \Sigma$.

Since ρ_ℓ arises from cohomology, we have some additional information on the eigenvalues of Frob_v. Let p_v be the characteristic and $q_v = p_v^{n_v}$ the cardinality of the residue field of v.

THEOREM 1.1: *Let $\alpha \in \bar{\mathbb{Q}}^*$ be any eigenvalue of Frob_v.*

(a) The absolute value of α in every complex embedding is $q_v^{k/2}$.

(b) α is a unit at any non-archimedean place not above p_v.

(c) For any non-archimedean valuation w of $\bar{\mathbb{Q}}$ such that $w(p_v) > 0$, the ratio $w(\alpha)/w(q_v)$ lies in the interval $[0, k]$ and its denominator is less than or equal to N.

Assertion (a) means that α is a q_v-Weil number of weight k; this is a celebrated theorem of Deligne [2]. Assertion (b) follows easily from the fact that α is an eigenvalue of $\rho_\ell(\mathrm{Frob}_v)$ which lies in a compact subgroup of $GL_N(\mathbb{Q}_\ell)$. Concerning assertion (c), the fact that α is an algebraic integer together with Poincaré duality imply that the ratio lies in the interval $[0, k]$. The denominator estimate is a consequence of the fact that α is also an eigenvalue of Frobenius on crystalline cohomology. This results from the properties of crystalline cohomology as a "Weil cohomology", mostly due to Berthelot; see for instance the survey article by Illusie [3] 1.3 (c), and Katz-Messing [4]. We will need assertion (c) only insofar as it implies that the number of possibilities for the ratio $w(\alpha)/w(q_v)$ is finite. In the number field case this can be seen without an appeal to crystalline cohomology, because from the inequality $n_v \leq [K : \mathbb{Q}]$ and the rationality of the characteristic polynomial one can easily deduce that the denominator of the ratio is at most $N \cdot [K : \mathbb{Q}]$.

Serre [8] (*cf.* also Chi [1] Th. 3.7) showed that the properties listed in Theorem 1.1 have the following remarkable consequence. For any $v \notin \Sigma$ and any ℓ not divisible by v let $H_{v,\ell} \subset G_\ell$ denote the Zariski closure of the subgroup generated by the semisimple part of $\rho_\ell(\mathrm{Frob}_v)$.

THEOREM 1.2: *For any ℓ there exists a Zariski closed proper subvariety $Y \subset G_\ell^\circ$ such that $H_{v,\ell}$ is a maximal torus of G_ℓ° whenever $\rho_\ell(\mathrm{Frob}_v) \in G_\ell^\circ \setminus Y$.*

For any $\rho_\ell(\mathrm{Frob}_v) \in G_\ell^\circ$ it is clear that $H_{v,\ell}$ is contained in some maximal torus of G_ℓ°. The main problem in Theorem 1.2 is that, as a subgroup of a maximal torus, there are *a priori* infinitely many different possibilities for $H_{v,\ell}$. This difficulty is overcome by using the valuation information to show that the number of possibilities for the identity component is in fact finite and that the

exponent of the group of connected components is bounded. For the convenience of the reader we reproduce a version of Serre's proof.

Proof: Fix a prime ℓ and consider some $v \notin \Sigma$ not dividing ℓ. We tacitly choose a basis of $H^k(\bar{X}, \mathbb{Q}_\ell) \otimes_{\mathbb{Q}_\ell} \bar{\mathbb{Q}}_\ell$ for which the semisimple part of $\rho_\ell(\mathrm{Frob}_v)$ becomes a diagonal matrix t_v, say with entries $\alpha_1, \ldots, \alpha_N$. Then $H_{v,\ell}$ is identified with a subgroup of the standard torus $\mathbb{G}_m^N$ of invertible diagonal matrices. For every non-archimedean valuation w of $\bar{\mathbb{Q}}$ set

$$\lambda_{v,w} := \Big(\frac{w(\alpha_1)}{w(q_v)}, \ldots, \frac{w(\alpha_N)}{w(q_v)}\Big). \tag{1.2.1}$$

Consider a character

$$\chi\colon \mathbb{G}_m^N \to \mathbb{G}_m,\ (x_1, \ldots, x_N) \mapsto \prod_{i=1}^N x_i^{a_i}.$$

LEMMA 1.3: *With definitions as above:*

(a) The character χ is trivial on $H_{v,\ell}^\circ$ if and only if, for all w,

$$(\chi, \lambda_{v,w}) := \sum_{i=1}^N a_i \cdot \frac{w(\alpha_i)}{w(q_v)} = 0.$$

(b) There is a positive integer n depending only on N, such that, if χ is trivial on $H_{v,\ell}^\circ$, then χ^n is trivial on $H_{v,\ell}$.

(c) As v runs through all primes not in Σ and not dividing ℓ, there are only finitely many possibilities for the group $H_{v,\ell} \times_{\mathbb{Q}_\ell} \bar{\mathbb{Q}}_\ell$ up to conjugation by $\mathrm{GL}_N(\bar{\mathbb{Q}}_\ell)$.

Proof: By its definition as Zariski closure, $H_{v,\ell}$ lies in the kernel of χ if and only if t_v does. Similarly, χ is trivial on $H_{v,\ell}^\circ$ if and only if $\chi(t_v)$ is a root of unity. Now observe that

$$(\chi, \lambda_{v,w}) = \frac{w(\chi(t_v))}{w(q_v)}.$$

Hence for $\chi(t_v)$ to be a root of unity, it is clearly necessary that these values be zero. We must show that this is also sufficient. If they are zero, then $\chi(t_v)$ is a unit in the ring of all algebraic integers. On the other hand, by the Weil number property, its absolute value in every complex embedding is the same. It follows that this absolute value must be 1. Since the only algebraic numbers whose absolute value at every archimedean or non-archimedean place is 1 are the roots

of unity, this proves (a). For (b) we note that this root of unity lies in the splitting field of the characteristic polynomial of Frob_v which is of degree at most $N!$ over $\mathbb{Q}$. Thus its order can be bounded purely in terms of N, as desired. For (c) we first note that Theorem 1.1 (b) and (c) implies that the number of possibilities for the tuple (1.2.1) is finite. On the other hand, any Zariski closed subgroup of $\mathbb{G}_m^N$ is determined uniquely by the set of characters χ whose restrictions to this subgroup are trivial. This, together with (a) and (b) implies (c). □

Returning to Theorem 1.2, let r denote the dimension of any maximal torus of G_ℓ°. Let $Z \subset \mathbb{G}_m^N$ denote the union of all the possible subgroups $H_{v,\ell}$ given by Lemma 1.3 (c) whose dimension is strictly less than r. Then the subset $Y \subset G_\ell^\circ$ of all points whose semisimple part is conjugate under GL_N to an element of Z is a Zariski closed proper subset. Suppose that $\rho_\ell(\mathrm{Frob}_v)$ lies in $G_\ell^\circ \setminus Y$. Then $H_{v,\ell}$ is contained in some maximal torus of G_ℓ°. If it is not itself a maximal torus, its dimension must be strictly less than r. Then by construction $H_{v,\ell}$ and hence t_v is contained in Z. This contradicts the assumption $\rho_\ell(\mathrm{Frob}_v) \notin Y$, thus finishing the proof. □

Recall that an element $t \in \mathrm{GL}_N(F)$ for a field F is called **neat** if and only if the subgroup of $\bar{F}^*$ generated by the eigenvalues of t is torsion free. Theorem 1.2 has the following consequence.

COROLLARY 1.4: *For a set of primes v of Dirichlet density 1, if v splits in K^{conn}, then $\rho_\ell(\mathrm{Frob}_v)$ is neat for any ℓ not divisible by v.*

Proof: By strict compatibility the neatness property does not depend on ℓ. Thus we may apply Theorem 1.2 to any fixed ℓ, noting that $\rho_\ell(\mathrm{Frob}_v)$ must be neat whenever it comes to lie in $G_\ell^\circ \setminus Y$. As a closed subgroup of $\mathrm{GL}_N(\mathbb{Q}_\ell)$, the image of ρ_ℓ may be regarded as an ℓ-adic analytic subvariety of the affine space $\mathbb{A}^{N^2}$. As it is Zariski-dense in G_ℓ, its intersection with Y is an analytic subvariety of lower dimension. It follows from [7] §3 that in the limit as $r \to 0$, the proportion of balls in $\mathrm{im}(\rho_\ell)$ of radius r which contain a point in Y tends to zero. Therefore, the set of v such that $\rho_\ell(\mathrm{Frob}_v) \in Y$ has Dirichlet density zero. □

2. The Behavior of Algebraic Eigenvalues at Different Primes ℓ

Consider a collection of elements $t_\ell \in \mathrm{GL}_N(\bar{\mathbb{Q}}_\ell)$ for all but finitely many rational primes ℓ such that the set of eigenvalues of t_ℓ consists of algebraic numbers

and is independent of ℓ. Here we use a fixed embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$ for each ℓ. Forgetting finitely many primes ℓ we suppose that the eigenvalues are units at all primes above ℓ. Then the closed subgroup $\langle t_\ell \rangle \subset \mathrm{GL}_N(\bar{\mathbb{Q}}_\ell)$ generated by t_ℓ in the ℓ-adic topology is the direct product of a pro-ℓ-group with a finite cyclic group of order prime to ℓ. We are asking what the prime-to-ℓ parts have in common as ℓ varies. Although we really only need Corollary 2.2, to understand better what is going on we study the problem in slightly greater generality. Fix a finite set P of rational primes, and for any abelian group A and any rational prime p let $n_p(A)$ denote the order of the p-power torsion part of A. Let M denote the subgroup of $\bar{\mathbb{Q}}^*$ generated by the eigenvalues of the t_ℓ. Let E be any finite extension of $\mathbb{Q}$.

PROPOSITION 2.1: *For all ℓ for which t_ℓ is defined and all $p \neq \ell$ we have $n_p(\langle t_\ell \rangle) \geq n_p(M)$. On the other hand, there exists a set of primes $\ell \notin P$ of positive Dirichlet density satisfying*

(a) ℓ splits completely in E, and

(b) $n_p(\langle t_\ell \rangle) = n_p(M)$ for each $p \in P$.

COROLLARY 2.2: *Suppose that the t_ℓ are neat, i.e. that M is torsion free. Then there is a set of primes $\ell \notin P$ of positive Dirichlet density satisfying*

(a) ℓ splits completely in E, and

(b) every continuous homomorphism from $\langle t_\ell \rangle$ to a finite group of order $p \in P$ is trivial.

Proof: Let t'_ℓ denote the component of t_ℓ in the prime-to-ℓ factor of $\langle t_\ell \rangle$. The torsion part of M consists of roots of unity, so it is finite cyclic of some order n. For any prime p, the p-part of n is just $n_p(M)$, and there exists a multiplicative linear combination of the eigenvalues of t_ℓ which is a root of unity of precise order $n_p(M)$. If $p \neq \ell$, then the same is true for the eigenvalues of t'_ℓ. This implies that the order of t'_ℓ is divisible by $n_p(M)$, proving the first assertion of Proposition 2.1. If we replace all t_ℓ by t_ℓ^n and consequently M by its subgroup M^n, then both sides of the equation in Proposition 2.1 (b) decrease by the same factor, namely by $n_p(M)$. Thus it suffices to prove the remaining assertion after the replacement has been made, *i.e.* under the assumption that M is torsion free.

Enlarge E so that it contains M. For any positive integer n let μ_n denote the group of roots of unity of order n in $\bar{E}$, and $E(\mu_n)$ the extension of E generated by them. We suppose that E contains μ_p for every $p \in P$. Then the field $E(\mu_{p^n}, M^{p^{-n}})$ generated by all p^n-th roots of elements of M is a Galois

extension of E of p-power order, for any $p \in P$. By Proposition 2.3 below, the field $E(\mu_{p^{n+1}}, M^{p^{-n}})$ is strictly larger whenever n is sufficiently large. Note that its degree over $E(\mu_{p^n}, M^{p^{-n}})$ is equal to p. Now fix some large n and let E' be the compositum of the fields $E(\mu_{p^n}, M^{p^{-n}})$ for all $p \in P$. Then $E'(\mu_{p^{n+1}})$ still has degree p over E' for each $p \in P$, and in particular these extensions of E' are all disjoint. The Čebotarev density theorem implies that the set of primes ℓ which split completely in E' but not in any of the fields $E'(\mu_{p^{n+1}})$ has positive Dirichlet density.

We claim that these primes have the desired properties. Indeed, the complete splitting of ℓ in E' implies that the eigenvalues of t_ℓ lie in $(\mathbb{Q}_\ell^*)^{p^n}$ for any $p \in P$. Since they are also units at ℓ, they are contained in $(\mathbb{Z}_\ell^*)^{p^n}$. On the other hand we have arranged matters such that ℓ splits completely in $\mathbb{Q}(\mu_{p^n})$ but not in $\mathbb{Q}(\mu_{p^{n+1}})$, which means that p^n is the highest power of p dividing $\ell - 1$. It follows that the p-part of any element of $(\mathbb{Z}_\ell^*)^{p^n}$ is trivial. Thus the p-part of $\langle t_\ell \rangle$ is trivial for any $p \in P$, as desired. □

PROPOSITION 2.3: *Consider a finite extension E of $\mathbb{Q}$, a finitely generated torsion free subgroup $M \subset E^*$, and a rational prime p. Then for any sufficiently large integer n we have*

$$\mu_{p^{n+1}} \not\subset E(\mu_{p^n}, M^{p^{-n}}).$$

Proof: For the sake of brevity, we work at the finite level, but it is not difficult and may be more natural, to work at the level of $\mathbb{Z}_p$-extensions.

We enlarge E so that it contains μ_p, and also μ_4 if $p = 2$. Among other things this ensures that the Galois group over E of the extension $E(\mu_{p^\infty})$ generated by all p-power roots of unity is topologically cyclic, say generated by an element σ.

LEMMA 2.4: *If $\mu_{p^{n+1}} \not\subset E$, then*

$$(E(\mu_{p^n})^*)^{p^n} \cap E^* = (E^*)^{p^n}.$$

Proof: Consider $x \in E(\mu_{p^n})^*$ such that $x^{p^n} \in E$. Then $\sigma(x)/x$ is a p^n-th root of unity. Choose a p-power root of unity ζ such that $\sigma(\zeta)/\zeta = \sigma(x)/x$. Then $y := x/\zeta$ is fixed by σ, in other words, $y \in E^*$. This implies that

$$\zeta = x/y \in E(\mu_{p^n})^* \cap \mu_{p^\infty} = \mu_{p^n}$$

under the assumption in the lemma. We conclude that $x^{p^n} = y^{p^n} \in (E^*)^{p^n}$, as desired. □

Now choose a compatible system of p-power roots of unity, that is, for each $n \geq 0$ a root of unity $\zeta_n \in \bar{E}^*$ of precise order p^n such that $\zeta_{n+1}^p = \zeta_n$. Suppose that $\zeta_{n+1} \in E(\mu_{p^n}, M^{p^{-n}})$. By Kummer theory, for $n \geq 1$,

$$\zeta_{n+1} \in M^{p^{-n}} \cdot E(\mu_{p^n})^*.$$

Taking p^n-th powers we deduce

$$\zeta_1 \in M \cdot (E(\mu_{p^n})^*)^{p^n}.$$

Since both ζ_1 and M are contained in E, we in fact have

$$\zeta_1 \in M \cdot \big((E(\mu_{p^n})^*)^{p^n} \cap E^*\big).$$

Now Lemma 2.4 implies

$$\zeta_1 \in M \cdot (E^*)^{p^n} \tag{2.4.1}$$

whenever n is sufficiently large. Recall that E^* is the product of its (finite) torsion subgroup with a free abelian group of infinite rank. Thus the saturation

$$M^{\mathrm{sat}} := \{x \in E^* |\ \exists m \geq 1 :\ x^m \in M\}$$

of M is a direct factor of E^* and finitely generated, and the equation (2.4.1) reduces to

$$\zeta_1 \in M \cdot (M^{\mathrm{sat}})^{p^n}.$$

Since for large enough n the p-primary part of M^{sat}/M is annihilated by p^n, this implies $\zeta_1 \in M$. But this is impossible since M is torsion free. □

3. Proof of Theorem 0.1

Suppose that K^{conn} is properly contained in $\bigcap_{\ell\in\mathcal{L}} K_\ell$. Since this intersection is Galois over K, there exists a subfield L which is finite Galois over K and contains K^{conn} properly. By the definition of K_ℓ the natural surjection $\mathrm{Gal}(\bar{K}/K) \to \mathrm{Gal}(L/K)$ factors through ρ_ℓ for every $\ell \in \mathcal{L}$.

Fix an element $\sigma \in \mathrm{Gal}(L/K^{\mathrm{conn}})$ of prime order p. By the Čebotarev density theorem we can choose a prime $v \notin \Sigma$ of K, unramified in L, such that the image of Frob_v in $\mathrm{Gal}(L/K)$ is conjugate to σ. The order of this image is then equal to p. By Corollary 1.4 we can also achieve that $\rho_\ell(\mathrm{Frob}_v)$ is neat for any ℓ not divisible by v.

Now we apply Corollary 2.2 to the elements $t_\ell := \rho_\ell(\mathrm{Frob}_v)$. Since $\mathcal{L}$ contains all primes that split completely in E except a set of Dirichlet density 0, we can find a prime $p \neq \ell \in \mathcal{L}$ satisfying Corollary 2.2 (b). That is, every continuous homomorphism from the closed subgroup $\langle \rho_\ell(\mathrm{Frob}_v)\rangle$ to a group of order p is trivial. But this contradicts the choice of v, and Theorem 0.1 is proved. □

REFERENCES

[1] W. Chi, ℓ-adic and λ-adic representations associated to abelian varieties defined over number fields, *Amer. J. Math.* **114** (1992) 315-353.

[2] P. Deligne, La Conjecture de Weil, II, *Publ. Math. I.H.E.S.* **52** (1980), 138–252.

[3] L. Illusie, Crystalline cohomology, in: Proc. of the Summer Research Conference on Motives, Seattle 1991, *Proc. Symp. Pure Math.* **55** (1994) 43–70.

[4] N. M. Katz, W. Messing, Some Consequences of the Riemann Hypothesis for Varieties over Finite Fields, *Invent. Math.* **23** (1974) 73–77.

[5] M. Larsen and R. Pink, On ℓ-independence of algebraic monodromy groups in compatible systems of representations, *Invent. Math.* **107** (1992) 603–636.

[6] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves.* W.A. Benjamin, Inc, New York (1968).

[7] J.-P. Serre, Quelques applications du théorème de densité de Cebotarev, *Publ. Math. I.H.E.S.* **54** (1981), 123–201.

[8] J.-P. Serre, Letter to K. Ribet, Jan. 1, 1981.

[9] J.-P. Serre, Letter to K. Ribet, Jan. 29, 1981.

[10] J.-P. Serre, Résumé des cours 1984-85. in *Annuaire du Collège de France* (1985), 85-91.

[11] A. Silverberg and Yu. B. Zarhin, Connectedness results for ℓ-adic representations associated to abelian varieties, preprint.