

MOD p GALOIS REPRESENTATIONS OF SOLVABLE IMAGE

HYUNSUK MOON AND YUICHIRO TAGUCHI

(Communicated by David E. Rohrlich)

ABSTRACT. It is proved that, for a number field K and a prime number p , there exist only finitely many isomorphism classes of continuous semisimple Galois representations of K into $\mathrm{GL}_d(\overline{\mathbb{F}}_p)$ of fixed dimension d and bounded Artin conductor outside p which have solvable images. Some auxiliary results are also proved.

0. INTRODUCTION

Let K be an algebraic number field of finite degree over \mathbb{Q} , and let G_K be its absolute Galois group $\mathrm{Gal}(\overline{K}/K)$. Let $\overline{\mathbb{F}}_p$ be an algebraic closure of the finite field \mathbb{F}_p of p elements. In [9], one of the authors proposed to study the following:

Problem. *Fix an integer $d \geq 1$ and a nonzero integral ideal \mathfrak{N} of K . Then do there exist only finitely many isomorphism classes of continuous semisimple representations $\rho : G_K \rightarrow \mathrm{GL}_d(\overline{\mathbb{F}}_p)$ whose Artin conductor $\mathfrak{N}(\rho)$ outside p divides \mathfrak{N} ?*

This problem has been motivated by a conjecture of Serre ([12]), which implies the finiteness of isomorphism classes of odd and irreducible representations $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_p)$. Recent work of Ash and Sinnott ([2]) is also in favor of an affirmative answer to the problem in certain cases for higher d and $K = \mathbb{Q}$. For more discussions on this problem, we refer the reader to §4 of [9].

In this paper, we give some further remarks concerning the problem. First, we recall in §1 that the finiteness statement holds true for classical Artin representations ([1]), i.e., if we replace $\overline{\mathbb{F}}_p$ by the complex number field \mathbb{C} and $\mathfrak{N}(\rho)$ by the usual Artin conductor. Second, it is also true if we restrict to those ρ 's with solvable images (§2). In these cases, keys in the proofs are the finiteness of ideal class groups (or global class field theory) and the Hermite-Minkowski theorem. This suggests us to view the above problem, if answered affirmatively, as a generalization of these two. Third, we show in §3 that the problem is reduced to a special case in which the image of ρ is a finite simple group of Lie type in characteristic p . This is based on a theorem of Larsen and Pink ([8]) on the structure of finite subgroups of $\mathrm{GL}_d(\overline{\mathbb{F}}_p)$. Finally in §4, we explain that these results also hold for function fields K over a finite field under a reasonable condition that there are no constant field extensions.

Thus in this paper, we use Artin conductors in three different contexts, which are all denoted $\mathfrak{N}(\rho)$; we hope this causes no confusion.

Received by the editors January 12, 2000.

2000 *Mathematics Subject Classification.* Primary 11R29, 11R32.

1. THE CLASSICAL CASE

Let V be a d -dimensional \mathbb{C} -vector space. For a continuous representation $\rho : G_K \rightarrow \mathrm{GL}_{\mathbb{C}}(V) \simeq \mathrm{GL}_d(\mathbb{C})$ (where $\mathrm{GL}_{\mathbb{C}}(V)$ is endowed with the discrete topology), we define its Artin conductor $\mathfrak{N}(\rho)$ as follows (cf. [11], Chap. VI): choose a finite Galois extension L/K such that ρ factors through $\mathrm{Gal}(L/K)$ and define

$$(*) \quad \mathfrak{N}(\rho) := \prod_{\mathfrak{q}} \mathfrak{q}^{n(\mathfrak{q}, \rho)},$$

where \mathfrak{q} runs through the nonzero prime ideals of K and, for each \mathfrak{q} ,

$$n(\mathfrak{q}, \rho) := \sum_{i=0}^{\infty} \frac{1}{(G_0 : G_i)} \dim_{\mathbb{C}}(V/V^{G_i}),$$

where V^{G_i} is the fixed part of V by the i th ramification subgroup G_i of the decomposition group of a prime of L lying above \mathfrak{q} . The exponent $n(\mathfrak{q}, \rho)$ may be defined also as the inner product of ρ with the Artin representation of G . It is an integer which does not depend on our choice of L/K . We have $n(\mathfrak{q}, \rho) > 0$ if and only if ρ ramifies at \mathfrak{q} .

Theorem 1. *Given an integer $d \geq 1$ and a nonzero integral ideal \mathfrak{N} of K , there exist only finitely many isomorphism classes of continuous representations $\rho : G_K \rightarrow \mathrm{GL}_{\mathbb{C}}(V)$ with $\mathfrak{N}(\rho)$ dividing \mathfrak{N} .*

This is proved in [1] as a corollary to their finiteness theorem for representations of the Weil group with bounded conductor (it is mentioned there that the above Theorem had been obtained also by R. Greenberg). The proof consists in the combination of Jordan's theorem ([13], Chap. VI, §24, Th. 3) on the structure of finite subgroups of $\mathrm{GL}_d(\mathbb{C})$, the Hermite-Minkowski theorem on discriminants, and class field theory (finiteness of abelian extensions of bounded conductor).

2. SOLVABLE IMAGE CASE

Let p be a prime number. In this section, we consider Galois representations into $\mathrm{GL}_d(\overline{\mathbb{F}}_p)$. For a continuous representation $\rho : G_K \rightarrow \mathrm{GL}_d(\overline{\mathbb{F}}_p)$, we define its Artin conductor outside p , called also $\mathfrak{N}(\rho)$, by the same formula as in (*) but with the product over only those \mathfrak{q} 's which do not divide p . It has similar properties as the $\mathfrak{N}(\rho)$ in §1 except that, in the positive characteristic case, the exponent $n(\mathfrak{q}, \rho)$ may not coincide with the inner product of ρ with the Artin representation (cf. [14]).

Theorem 2. *Given an integer $d \geq 1$ and a nonzero integral ideal \mathfrak{N} of K , there exist only finitely many isomorphism classes of continuous semisimple representations $\rho : G_K \rightarrow \mathrm{GL}_d(\overline{\mathbb{F}}_p)$ with solvable image and with $\mathfrak{N}(\rho)$ dividing \mathfrak{N} .*

Proof. By the assumption of semisimplicity together with Lemma 3.2 of [9], it is enough to show that there are only finitely many possibilities of Galois extensions L/K which may correspond to the kernel of a representation ρ as in the Theorem. So suppose L/K is such a Galois extension.

By a theorem of Mal'cev and Kolchin ([13], Chap. V, §19, Th. 7), there exists an integer $J(d)$, depending only on d , such that any solvable subgroup G of $\mathrm{GL}_d(\overline{\mathbb{F}}_p)$

contains a normal subgroup N with $(G : N) \leq J(d)$ which is conjugate to a subgroup of the group of upper triangular matrices. Apply this to $G = \text{Gal}(L/K)$. Then the extension K'/K corresponding to N is unramified outside $\mathfrak{N}p$ and $[K' : K] \leq J(d)$. By Hermite-Minkowski, there exist only finitely many such K'/K .

Let N_1 be the p -Sylow subgroup of N . Then N_1 is normal in N , and the quotient N/N_1 is abelian of order prime to p . Let K''/K' be the extension which corresponds to N_1 . It is an abelian extension unramified outside $\mathfrak{N}p$. More precisely, it is at most tamely ramified at primes above p and, outside p , its conductor is bounded by $\mathfrak{N}\mathcal{O}_{K'}$. It follows from class field theory that there exist only finitely many such K''/K' .

As explained in §3 of [9], the p -group N_1 has a filtration of finite length ($\leq [\log_2(d-1)]+1$) such that each of the successive quotients is elementary abelian. It is enough to show, for each step, the finiteness of the possibilities of the corresponding field extensions. By induction on the length, we may assume $N_1 = \text{Gal}(L/K'')$ itself is elementary abelian. Then the exponent of the conductor of L/K'' at each prime above p is bounded as in the proof of Lemma 2.1 of [9]. Outside p , the extension L/K'' is at most tamely ramified. By class field theory, there are only finitely many such extensions. \square

3. REDUCTION TO A SPECIAL CASE

In this section, we show that our problem can be reduced to a special case in which $\text{Im}(\rho)$ is a finite simple group of Lie type, by using a general theorem of Larsen and Pink on finite subgroups of $\text{GL}_d(\overline{\mathbb{F}}_p)$. In what follows, we mean by *finite simple group of Lie type in characteristic p* a group of the form $(\mathbb{G}^F)^{\text{der}}$, where \mathbb{G} is an adjoint connected simple linear algebraic group over $\overline{\mathbb{F}}_p$, F is a Frobenius endomorphism of \mathbb{G} , \mathbb{G}^F is the subgroup of $\mathbb{G}(\overline{\mathbb{F}}_p)$ consisting of the points fixed by F and, for any group G , we denote by G^{der} its derived group $[G, G]$. Such a group is indeed simple (cf. [3, §11.1, §14.4], [4, §2.9] and [8, §3]). Also, for a finite extension L/K , we denote by $\widetilde{\mathcal{D}}_{L/K}$ the prime-to- p part of the different of L/K .

Proposition 3. *The following statements are equivalent, in which K is an algebraic number field of finite degree, d is an integer ≥ 1 , and \mathfrak{N} is a nonzero integral ideal of K :*

(1) *For any K , d and \mathfrak{N} , there exist only finitely many isomorphism classes of continuous semisimple representations $\rho : G_K \longrightarrow \text{GL}_d(\overline{\mathbb{F}}_p)$ such that $\mathfrak{N}(\rho) | \mathfrak{N}$.*

(1)' *For any K , d and \mathfrak{N} , there exist only finitely many finite Galois extensions L/K such that $\widetilde{\mathcal{D}}_{L/K} | \mathfrak{N}\mathcal{O}_L$ and $\text{Gal}(L/K)$ can be embedded semisimply into $\text{GL}_d(\overline{\mathbb{F}}_p)$.*

(2) *For any K , d and \mathfrak{N} , there exist only finitely many isomorphism classes of continuous semisimple representations $\rho : G_K \longrightarrow \text{GL}_d(\overline{\mathbb{F}}_p)$ such that $\mathfrak{N}(\rho) | \mathfrak{N}$ and $\text{Im}(\rho)$ is a finite simple group of Lie type in characteristic p .*

(2)' *For any K , \mathfrak{N} and an adjoint connected simple linear algebraic group \mathbb{G} over $\overline{\mathbb{F}}_p$, there exist only finitely many Galois extensions L/K such that $\widetilde{\mathcal{D}}_{L/K} | \mathfrak{N}\mathcal{O}_L$ and $\text{Gal}(L/K)$ is a finite simple group of Lie type arising from \mathbb{G} .*

Note that, in these statements, the finiteness is equivalent to the nonexistence of such ρ (resp. L/K) with large enough $|\text{Im}(\rho)|$ (resp. $[L : K]$).

Proof. The implication (1)' \Rightarrow (2)' follows from the following:

Lemma 3.1. *If \mathbb{G} is as in (2)', there exists an integer $d \geq 1$ such that there exists a semisimple embedding $(\mathbb{G}^F)^{\text{der}} \hookrightarrow \text{GL}_d(\overline{\mathbb{F}}_p)$ for any Frobenius endomorphism F of \mathbb{G} .*

Proof. For some $d \geq 1$, one can find a closed embedding $\mathbb{G} \hookrightarrow \text{GL}_d$ of algebraic groups over $\overline{\mathbb{F}}_p$, which yields an injective homomorphism $(\mathbb{G}^F)^{\text{der}} \hookrightarrow \text{GL}_d(\overline{\mathbb{F}}_p)$ for each F . Its semisimplification remains injective, since $(\mathbb{G}^F)^{\text{der}}$ is simple (and $\not\cong \mathbb{Z}/p\mathbb{Z}$). \square

To show (1) \Leftrightarrow (1)' and (2) \Leftrightarrow (2)', we first consider the relation between the different, conductor and upper break in the local case. Let F be a complete discrete valuation field with perfect residue field of characteristic ℓ , and let E/F be a finite Galois extension with Galois group G . Let $\mathcal{D}_{E/F}$ be the different of E/F . For a representation $\rho : G \rightarrow \text{GL}_{\overline{\mathbb{F}}_p}(V)$, define $n(\rho) := \sum_{i \geq 0} (G_0 : G_i)^{-1} \dim V/V^{G_i}$, where G_i is the i th ramification subgroup of G . We denote by v_F the normalized valuation of F .

Lemma 3.2. *Assume E/F has ramification index $e \geq 2$. Put $c := \min(\ell, e)$. Then:*

- (i) $n(\rho) \leq (1 - 1/c)^{-1} \dim(\rho)v_F(\mathcal{D}_{E/F})$.
- (ii) *If ρ is faithful, one has: $v_F(\mathcal{D}_{E/F}) \leq n(\rho)$.*

Proof. In fact, we show more precisely the following: let $u_{E/F}$ be the largest real number u such that $G^{u-1} \neq 1$, where G^u is the u th ramification group in the upper numbering. Then one has:

- (o) $v_F(\mathcal{D}_{E/F}) \leq u_{E/F} \leq (1 - 1/c)^{-1}v_F(\mathcal{D}_{E/F})$,
- (i)' $n(\rho) \leq \dim(\rho)u_{E/F}$,
- (ii)' if ρ is faithful, one has $u_{E/F} \leq n(\rho)$.

Indeed, if $j_{E/F}$ denotes the largest integer i such that $G_i \neq 1$, then one has $u_{E/F} = \sum_{i=0}^{j_{E/F}} (G_0 : G_i)^{-1}$ (cf. [5], §1), from which (i)' follows. If ρ is faithful, then $\dim V/V^{G_i} \geq 1$ as long as $G_i \neq 1$, whence (ii)'. To show (o), recall that (*loc. cit.*)

$$v_F(\mathcal{D}_{E/F}) = u_{E/F} - i_{E/F},$$

where $i_{E/F} := (j_{E/F} + 1)/e$. The two numbers $i_{E/F}$ and $u_{E/F}$ are related by $i_{E/F} = \int_0^{u_{E/F}} (G_{ex-1} : 1)^{-1} dx$ (*loc. cit.*). Hence $i_{E/F} \leq c^{-1}u_{E/F}$, and we obtain (o). \square

Now we turn to the global case to show (1) \Leftrightarrow (1)' and (2) \Leftrightarrow (2)'. This is basically because a fixed finite group has only finitely many semisimple representations (up to isomorphism) into $\text{GL}_d(\overline{\mathbb{F}}_p)$ (cf. Lemma 3.2 of [9]). Then the first equivalence relation follows from Lemma 3.2 above. To show (2) \Leftrightarrow (2)', we have to be more careful; use Lemma 3.1 for (2) \Rightarrow (2)' and, for the converse, note that ([9], §12, Proof of Th. 0.2) there exist a finite number of simple algebraic groups \mathbb{G} from which arise all finite simple subgroups of $\text{GL}_d(\overline{\mathbb{F}}_p)$ of Lie type in characteristic p .

Finally, we shall show (2)' \Rightarrow (1)'. Suppose we are given a finite Galois extension L/K as in (1)' and set $G = \text{Gal}(L/K)$. According to Theorem 0.2 of [8], there exists an integer $J(d)$, depending only on d , such that any finite subgroup G of $\text{GL}_d(\overline{\mathbb{F}}_p)$

has a filtration $G \supset G_1 \supset G_2 \supset G_3$ by normal subgroups G_i of G such that:

- $(G : G_1) \leq J(d)$,
- G_1/G_2 is a direct product of finite simple groups of Lie type in characteristic p , and the number of direct factors is bounded uniformly in d ,
- G_2/G_3 is abelian of order prime to p ,
- G_3 is a p -group.

As in §2, the first step, G/G_1 , is taken care of by the Hermite-Minkowski theorem; the third, G_2/G_3 , by class field theory; the last, G_3 , by finding a filtration of bounded length and applying class field theory to each of the steps. Thus the finiteness in (1)' is reduced to that in (2)', since the different of L/K bounds that of the extension K_2/K_1 corresponding to G_1/G_2 . □

To conclude this section, it is tempting to conjecture that the statement (2)' could be strengthened somewhat; to have the finiteness as in (2)', do we need only to fix a finite set S of places of K outside which the extensions L/K are unramified? Even stronger: do there exist only finitely many finite Galois extensions which are unramified outside S and have simple Galois groups? In the function field case, the last question is answered in the negative; there exists an algebraic function field over a finite field which has an infinite unramified regular Galois extension with Galois group of the form $\prod_{p_i} \text{PSL}(d, \mathbb{F}_{p_i})$, where p_i runs through an infinite set of prime numbers ([6], Cor. 4.11). Can one construct such an example in which the Galois group is an infinite product of, say, $\text{PSL}(d, \mathbb{F}_q)$'s with various powers q of a fixed prime p ?

4. SUPPLEMENTS FOR THE FUNCTION FIELD CASE

In this section, we explain that, with suitable modifications, all the above holds true also in the function field case. Let K be an algebraic function field in one variable over a finite field, and let G_K be its absolute Galois group. Let k be either \mathbb{C} or $\overline{\mathbb{F}}_p$, and consider continuous representations $\rho : G_K \rightarrow \text{GL}_d(k)$. For such a ρ , define its Artin conductor $\mathfrak{N}(\rho)$ by the same formula (*) in §1 (regardless of $\text{char}(k)$):

$$\mathfrak{N}(\rho) := \prod_{\mathfrak{q}} \mathfrak{q}^{n(\mathfrak{q}, \rho)},$$

where \mathfrak{q} runs through all the prime divisors of K . We say that a finite extension L/K is *geometric* if there is no constant field extension, and that a representation ρ of G_K is *geometric* if so is the extension L/K corresponding to $\text{Ker}(\rho)$. Then we have analogous results to those in the previous sections *if* we restrict ourselves to geometric objects:

Theorem 4. *Suppose we are given an integer $d \geq 1$ and an effective divisor \mathfrak{N} of K .*

(i) *There exist only finitely many isomorphism classes of continuous geometric representations $\rho : G_K \rightarrow \text{GL}_d(\mathbb{C})$ with $\mathfrak{N}(\rho) | \mathfrak{N}$.*

(ii) *There exist only finitely many isomorphism classes of continuous semisimple geometric representations $\rho : G_K \rightarrow \text{GL}_d(\overline{\mathbb{F}}_p)$ with solvable image and with $\mathfrak{N}(\rho) | \mathfrak{N}$. (Here, $\text{char}(K)$ may coincide with p .)*

Furthermore, the “geometric version” of Proposition 3 for function fields is true.

The proof is basically identical with the number field case; some points to be noted are:

(a) We have the following analogue of the Hermite-Minkowski theorem (cf. [7], Th. 8.23.5): For any $n \geq 1$ and a divisor \mathfrak{d} of K , there exist only finitely many extensions L/K with degree $\leq n$ and discriminant $d_{L/K}|\mathfrak{d}$.

(b) The intermediate field extensions K'/K which appeared in the proofs of Theorems 1 and 2 have discriminants bounded in terms of $\mathfrak{N}(\rho)$. This follows from Lemma 3.2.

(c) By class field theory, there exist only finitely many geometric abelian extensions of bounded conductor (these are governed by a finite group of the form $K_{\mathbb{A}}^1/(K^\times \cdot \prod_v U_v^{n_v})$, where $K_{\mathbb{A}}^1$ is the norm-one subgroup of the idele group of K and $U_v^{n_v}$ is the group of local units at the place v which are congruent to 1 modulo the n_v th power of the maximal ideal at v ; cf. also [10]).

ACKNOWLEDGMENTS

We thank Richard Pink for his discussions and hospitality during our stay at Universität Mannheim, where part of this work was done. We are also grateful to the Deutsche Forschungsgemeinschaft for financial support for the stay. The second-named author thanks the Inamori Foundation for its partial support. Finally, we thank David Rohrlich, who drew our attention to the paper [1].

REFERENCES

1. G. Anderson, D. Blasius, R. Coleman and G. Zettler, *On representations of the Weil group with bounded conductor*, Forum Math. **6** (1994), 537–545. MR **95h**:11123
2. A. Ash and W. Sinnott, *An analogue of Serre's conjecture for Galois representations and Hecke eigenclasses in the mod- p cohomology of $\mathrm{GL}(n, \mathbb{Z})$* , to appear in Duke Math. J.
3. R.W. Carter, *Simple groups of Lie type*, Wiley, London, 1972. MR **53**:10946
4. R.W. Carter, *Finite Groups of Lie type*, Wiley, Chichester, 1985. MR **87d**:20060
5. J.-M. Fontaine, *Il n'y a pas de variété abélienne sur \mathbb{Z}* , Invent. math. **81** (1985), 515–538. MR **87g**:11073
6. G. Frey, E. Kani and H. Völklein, *Curves with infinite K -rational geometric fundamental group*, Aspects of Galois Theory, H. Völklein, P. Müller, D. Habater and J.G. Thompson (eds.), London Math. Soc. Lect. Note Ser., vol. 256, pp. 85–118. CMP 2000:01
7. D. Goss, *Basic Structures of Function Field Arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, vol. 35, Springer-Verlag, 1996. MR **97i**:11062
8. M.J. Larsen and R. Pink, *Finite subgroups of algebraic groups*, preprint (1998).
9. H. Moon, *Finiteness results on certain mod p Galois representations*, J. Number Theory **84** (2000), 156–165.
10. J.-P. Serre, *Groupes algébriques et corps de classes*, Hermann, Paris, 1959. MR **21**:1973
11. J.-P. Serre, *Corps Locaux*, 3^e éd., Hermann, Paris, 1980.
12. J.-P. Serre, *Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* , Duke Math. J. **54** (1987), 179–230. MR **88g**:11022
13. D.A. Suprunenko, *Matrix Groups*, A.M.S., Providence, 1976. MR **52**:10852
14. Y. Taguchi, *On Artin conductors of mod ℓ Galois representations*, in preparation.

DEPARTMENT OF MATHEMATICS, HOKKAIDO UNIVERSITY, SAPPORO, 060-0810, JAPAN

E-mail address: moon@math.sci.hokudai.ac.jp

Current address: Department of Mathematics, College of Natural Sciences, Seoul National University, Seoul, 151-742, Korea

E-mail address: hmoon@math2.snu.ac.kr

DEPARTMENT OF MATHEMATICS, HOKKAIDO UNIVERSITY, SAPPORO, 060-0810, JAPAN

E-mail address: taguchi@math.sci.hokudai.ac.jp