Tohoku Math. J.
59 (2007), 67–77

ON THE FINITENESS OF MOD p GALOIS REPRESENTATIONS OF A LOCAL FIELD

SHINYA HARADA

(Received August 10, 2005, revised March 24, 2006)

Abstract. Let K be a local field and k an algebraically closed field. We prove the finiteness of isomorphism classes of semisimple Galois representations of K into $\mathrm{GL}_d(k)$ with bounded Artin conductor and residue degree. We calculate explicitly the number of totally ramified finite abelian extensions of K with bounded conductor. Using this result, we give an upper bound for the number of certain Galois extensions of K.

Introduction. Let K be a local field, i.e., a complete discrete valuation field with finite residue field $\boldsymbol{F}$. Fix a separable closure K^{sep} of K and let G_K be its absolute Galois group. Let k be an algebraically closed field of characteristic $p \geq 0$. The purpose of this paper is to prove a finiteness result for semisimple Galois representations of G_K into $\mathrm{GL}_d(k)$ with restricted ramification and residue degree, and to investigate them quantitatively.

For any continuous representation $\rho : G_K \to \mathrm{GL}_d(k) \xrightarrow{\simeq} \mathrm{GL}_k(V)$ (we consider $\mathrm{GL}_d(k)$ as a discrete group), we define (the exponent of) its *Artin conductor* $n(\rho)$ as follows.

$$n(\rho) = \sum_{i=0}^{\infty} \frac{1}{(G_0 : G_i)} \dim_k(V/V^{G_i}),$$

where G_i is the i-th lower ramification subgroup of $G = \mathrm{Gal}\,(L/K)$, and L is the finite Galois extension of K corresponding to $\mathrm{Ker}\,\rho$. We denote by V^{G_i} the G_i-invariant subspace of V.

It is known that $n(\rho)$ is an integer if $\mathrm{char}\, k \neq \mathrm{char}\, \boldsymbol{F}$ (cf. [Tag02, Introduction]), and that we have $n(\rho) = 0$ if and only if ρ is unramified, and $n(\rho) = \dim_k(V/V^{G_0})$ if and only if ρ is tamely ramified. So the Artin conductor of ρ measures the 'depth' of the ramification of ρ. Denote by $f(\rho)$ the residue degree of L/K. In Section 1 we prove the following:

THEOREM 1. *Let K be a local field and d a positive integer.*

(1) *For any positive integers f and N, there exist only finitely many isomorphism classes of semisimple continuous representations $\rho : G_K \to \mathrm{GL}_d(k)$ with $n(\rho) \leq N$ and $f(\rho) \leq f$.*

(2) *If $\mathrm{char}\, k = p > 0$ and K is a finite extension of $\boldsymbol{Q}_p$, then for any positive integer f there exist only finitely many isomorphism classes of semisimple continuous representations $\rho : G_K \to \mathrm{GL}_d(k)$ with $f(\rho) \leq f$.*

2000 *Mathematics Subject Classification.* Primary 11F80; Secondary 11S15.
Key words and phrases. Galois representations, local fields.

This has been pointed out by Taguchi in [Tag] without proof. For a finite group G there exist only finitely many (in particular $\leq |G|$) isomorphism classes of irreducible representations of G over k. Hence Theorem 1 is equivalent to the following:

THEOREM 1′. *Let K be a local field.*

(1) *There exist only finitely many finite Galois extensions of K in K^{sep} which correspond to the kernels of representations as in* (1) *of Theorem* 1.

(2) *If* $\operatorname{char} k = p > 0$ *and K is a finite extension of $\mathbf{Q}_p$, then there exist only finitely many finite Galois extensions of K in K^{sep} which correspond to the kernels of representations as in* (2) *of Theorem* 1.

Furthermore in Section 2, we prove the finiteness for the set of certain Galois extensions of a local field K (Theorem 2), which is stronger than Theorem 1′ since for a representation ρ as in Theorem 1 the Artin conductor of ρ is bounded in terms of the valuation of its different (cf. Lemma 1.1).

THEOREM 2. *Let K be a local field and d a positive integer.*

(1) *For any positive integers f and N, there exist only finitely many finite Galois extensions L of K in K^{sep} such that $v_K(\mathcal{D}_{L/K}) \leq N$, $f(L/K) \leq f$ and that* $\operatorname{Gal}(L/K)$ *can be embedded in* $\mathrm{GL}_d(k)$.

(2) *If* $\operatorname{char} k = p > 0$ *and K is a finite extension of $\mathbf{Q}_p$, then for any positive integer f there exist only finitely many finite Galois extensions L of K in K^{sep} such that $f(L/K) \leq f$ and that* $\operatorname{Gal}(L/K)$ *can be embedded in* $\mathrm{GL}_d(k)$.

This is proved by local class field theory and ramification theory. It can also be proved in another way by using local class field theory, Serre's mass formula and group theory.

The Galois extensions of K as in (1) (resp. (2)) of Theorem 1′ satisfy the conditions in (1) (resp. (2)) of Theorem 2. Hence Theorem 2 implies Theorem 1. However, (1) of Theorem 1 is derived from a weaker theorem in group theory ([Sup76, Chap. V, §19, Theorem 6]) than what is needed to prove Theorem 2. In fact, it is appropriate for giving an effective upper bound for the number of finite Galois extensions of K corresponding to irreducible representations (see Proposition 1.3 and Section 3).

In Section 3 we estimate the number of finite Galois extensions of K which correspond to the kernels of irreducible continuous representations $\rho : G_K \to \mathrm{GL}_d(k)$ with $n(\rho) \leq N$ and $f(\rho) \leq f$. For this, first we calculate explicitly (Proposition 3.5) the number of totally ramified finite abelian extensions of K with conductor $\leq u$ in terms of the number of subgroups of U_K^1/U_K^u, where U_K^u is the u-th higher unit group of K. Using this result and Serre's mass formula, we have an upper bound for the number of such finite Galois extensions of K (Theorem 3.9). From this we have an upper bound for the number of isomorphism classes of irreducible representations (Corollary 3.10).

Now we explain the motivation of this paper. The finiteness problem of mod p Galois representations with bounded Artin conductor has been considered in the global field case (cf. Khare ([Kha00]) and Moon ([Moo00])) motivated by a conjecture of Serre [Ser87]. Classically many results for the finiteness of such representations of $G_{\boldsymbol{Q}}$ were already known for some primes p (for the references, see Moon [Moo00, Introduction]). In the general settings Moon and Taguchi proved the finiteness for semisimple mod p Galois representations with solvable image for arbitrary p and for arbitrary global field ([MT01]). In the algebraic function field case, in [BK] Böckle and Khare show the finiteness for almost all the case without the assumption that the images of representations are solvable. In this paper we consider the finiteness of mod p Galois representations of a local field. Theorem 1 is an analog in the local field case.

Effective upper bounds have also been studied for the number of isomorphism classes of mod p Galois representations. In [Moo03], Moon gave an explicit upper bound for the number of isomorphism classes of monomial mod p Galois representations of the rational field $\boldsymbol{Q}$ with bounded Artin conductor outside p. It is an open problem to have an explicit upper bound for the number of isomorphism classes of representations as in Theorem 1 in the local field case. However in Section 3 we give an upper bound for the number of isomorphism classes of irreducible ones following the line of the proof of Proposition 1.3.

I would like to express my sincere gratitude to Professor Yuichiro Taguchi who proposed the theme of this paper to me, and gave suggestions on the proof of Theorem 1 and valuable advice for the composition of this paper. I also thank the referee for many comments. In particular, he provided a new proof of Theorem 2, which is more sophisticated and shorter than the original one.

NOTATION. Throughout this paper, K denotes a local field with finite residue field $\boldsymbol{F} = \boldsymbol{F}_q$. Fix a separable closure K^{sep} of K, and we assume that all separable extensions of K are contained in K^{sep}. We denote by G_K the absolute Galois group $\text{Gal}\,(K^{\text{sep}}/K)$ of K. k denotes an algebraically closed field. Unless otherwise mentioned, the characteristic of k is arbitrary.

1. Proof of Theorem 1. First we recall a lemma, which states the relationship among the valuation of the different, the conductor of a finite Galois extension of local fields, and the Artin conductor, and which is a key to the proof of Theorem 1.

LEMMA 1.1 ([MT01], Lemma 3.2). *Let K be a local field, and l the characteristic of $\boldsymbol{F}$. Let L/K be a finite Galois extension with ramification index $e \geq 2$, G its Galois group, and let $u_{L/K}$ be the supremum of the real numbers $u \geq 0$ such that $G^{u-1} \neq 1$. If $\rho : G \to \text{GL}_d(k)$ is a faithful representation, then $n(\rho)$, the different $\mathcal{D}_{L/K}$ of L/K, and $u_{L/K}$ have the following relations.*

(1) $\nu_K(\mathcal{D}_{L/K}) \leq u_{L/K} \leq 2\nu_K(\mathcal{D}_{L/K})$,

(2) $u_{L/K} \leq n(\rho) \leq d u_{L/K}$,

where ν_K is the normalized discrete valuation of K.

In this paper, we call the above $u_{L/K}$ the *conductor* of L/K.

REMARK 1.2. In [MT01, Lemma 3.2] the above lemma is stated when $k = \bar{\boldsymbol{F}}_p$. But the statement still holds for arbitrary field. The proof is the same as in the case of $k = \bar{\boldsymbol{F}}_p$.

It is sufficient for the proof of Theorem 1 to prove the theorem in the case where ρ is irreducible, since $n(\rho') \leq n(\rho)$ if ρ' is an irreducible subrepresentation of ρ. Precisely speaking, we prove the following:

PROPOSITION 1.3. *Let K be a local field and d a positive integer.*

(1) *For given positive integers f and N, there exist only finitely many isomorphism classes of irreducible continuous representations $\rho : G_K \to \mathrm{GL}_d(k)$ with $n(\rho) \leq N$ and with $f(\rho) \leq f$.*

(2) *If* $\mathrm{char}\, k = p > 0$ *and K is a finite extension of $\boldsymbol{Q}_p$, then for any positive integer f there exist only finitely many isomorphism classes of irreducible continuous representations $\rho : G_K \to \mathrm{GL}_d(k)$ with $f(\rho) \leq f$.*

PROOF. First we show (1) of this proposition. As mentioned in Introduction, for a finite group there exist only finitely many isomorphism classes of irreducible representations of G over k (cf. [Ser77, Chap.18, §2, Corollary 3]). Hence it is sufficient to show that there exist only finitely many finite Galois extensions L of K corresponding to the kernels of ρ's. If L is such a Galois extension of K, its Galois group $G = \mathrm{Gal}\,(L/K)$ can be considered as a subgroup of $\mathrm{GL}_d(k)$. Let G' be the inertia subgroup of G. Then by [Sup76, Chap. V, §19, Theorem 6], there exists an abelian normal subgroup G'' of G' with $(G' : G'') \leq J(d)$, where $J(d)$ is a positive integer depending only on d. Let K' be the inertia field of L/K. By the assumption, there exist only finitely many such K'/K. Let K'' be the intermediate field of L/K' corresponding to G''. By Lemma 1.1 we have $\nu_{K'}(\mathcal{D}_{K''/K'}) \leq n(\rho) \leq N$. Since $[K'' : K'] = (G' : G'') \leq J(d)$, we have $\nu_{K''}(\mathcal{D}_{K''/K'}) \leq J(d)N$. Thus there exist only finitely many such K''/K' by Serre's mass formula ([Ser78]). From Lemma 1.1 we also have

$$u_{L/K''} \leq 2\nu_{K''}(\mathcal{D}_{L/K''}) \leq 2[K'' : K']n(\rho) \leq 2J(d)N\,,$$

where $u_{L/K''}$ is the conductor of the abelian extension L/K''. Hence by local class field theory there exist only finitely many such L/K''. This proves (1) of this proposition.

Now we derive (2) of this proposition from (2) of Theorem 2. (2) of Theorem 2 implies that there are only finitely many finite Galois extensions of K corresponding to the kernels of representations as in (2) of this proposition. Hence we have the desired result from the fact stated first in the proof of (1) of this proposition. □

REMARK 1.4. For instance we can take $J(d) = d!(\prod_{i=0}^{2^r-1}(d^2 - i))^d$, where $r = [\log_2 d^2]$ ([Sup76, Chap. V, §19]). Here $[a]$ means the largest integer less than or equal to a.

2. Proof of Theorem 2. In this section, we present a proof of Theorem 2, which was suggested by the referee. The original proof is summarized in Remark 2.1.

Let L be a finite Galois extension of K as in Theorem 2, i.e., such that its Galois group $G = \mathrm{Gal}\,(L/K)$ is embedded into $\mathrm{GL}_d(k)$. Let $0 < x_1 < x_2 < \cdots < x_r$ be all the upper breaks of G:

$$G = G^{-1} > G^{0} > G^{x_1} > \cdots > G^{x_{r+1}} = 1\,,$$

where, for any $x \in \boldsymbol{R}_{>0}$, G^x is the x-th ramification subgroup of G in the upper numbering. Here, x is said to be an *upper break* of G if $G^x \neq G^{x+}$, where $G^{x+} := \bigcup_{y>x} G^y$.

Let K_i be the intermediate field of L/K corresponding to G^{x_i} ($x_0 := 0$). Note that K_0/K is an unramified extension and K_{i+1}/K_i is a totally ramified abelian extension for every $0 \le i \le r$. Since $f(L/K) \le f$, there are only finitely many possibilities of K_0. It is sufficient for the proof of Theorem 2 to show that there are only finitely many possibilities of K_{i+1} for each K_i, $0 \le i \le r$, and that r is bounded.

We first consider the case (1) of Theorem 2. By the assumption $v_K(\mathcal{D}_{L/K}) \le N$ and (1) of Lemma 1.1, x_i and u_{K_{i+1}/K_i} are bounded in terms of N. Hence, from local class field theory, there are only finitely many possibilities of K_{i+1} for each K_i, $0 \le i \le r$. From [Kat88, Chap. 1, 1.9, Proposition], we know that x_i is a rational number whose denominator $d(x_i)$ can be taken as $1 \le d(x_i) \le d$. Hence there are only finitely many possibilities of x_i. In particular, r is bounded in terms of d and N. Thus we have proved (1) of Theorem 2.

Next we consider the case (2) of Theorem 2. In this case we have $\operatorname{char} \boldsymbol{F} = p$. Then the conductor u_{K_{i+1}/K_i} is bounded in terms of p and the absolute ramification index $e(K_i/\boldsymbol{Q}_p)$ by [Moo00, Lemma 2.1] and Lemma 1.1. Thus we obtain inductively that there are only finitely many possibilities of K_{i+1} for each K_i, $0 \le i \le r$. Since the p-length of $\mathrm{GL}_d(k)$ is bounded in terms of d (cf. [Moo00, §3]), and $G^{x_i}/G^{x_{i+1}}$ is elementary p-abelian ($1 \le i \le r$), it follows that r is bounded in terms of d. Hence we have proved (2) of Theorem 2.

REMARK 2.1. Compared with the above proof of Theorem 2, the original proof was somewhat longer but more elementary. The difference is to use a structure theorem of $\mathrm{GL}_d(k)$ instead of the ramification subgroups in the upper numbering. Here we summarize the original proof: Let $G = \mathrm{Gal}\,(L/K)$ be as in Theorem 2 and let H_0 be the inertia subgroup of G. By the theorem of Larsen-Pink ([LP]) (this is equal to the theorem of Mal'cev, Kolchin [Sup76, Chap. V, §19, Theorem 7] since G is solvable), there exist normal subgroups H_1, H_2 of H_0 such that

(1) $H_2 \subset H_1 \subset H_0$,
(2) $(H_0 : H_1) \le \tilde{J}(d)$,
(3) H_1/H_2 is abelian with order prime to p,
(4) H_2 is a p-group,

where $\tilde{J}(d)$ is a positive integer which depends only on d. When $\operatorname{char} k = 0$, this means that $H_2 = 1$ and H_1 is abelian. Now suppose that $\operatorname{char} k = p > 0$. Since the p-length of $\mathrm{GL}_d(k)$ is bounded, there exists a filtration $\{H_i\}_{2 \le i \le r}$ of subgroups of G of bounded length r such that H_{i+1} is normal in H_i and H_i/H_{i+1} is elementary p-abelian for any $i \ge 2$. Let K_i be the intermediate field of L/K corresponding to H_i. In the case of (1) of Theorem 2, there are only finite number of K_{i+1} for each K_i by Serre's mass formula (resp. local class field theory) for $i = 0$ (resp. $i > 0$) and Lemma 1.1. In view of the proof of (1), it is sufficient for the proof of (2) to show that for each field extension K_{i+1}/K_i the valuation of its different is bounded inductively. For K_{i+1}/K_i $(i \geq 1)$, we have already explained in the proof of Theorem 2. For K_1/K_0, since char $K = 0$, we can bound the valuation of the different of K_1/K_0 in terms of $\tilde{J}(d)$ (cf. [Ser79, Chap. III, §6, P. 58, Remarks].

3. Estimate for the number of L. In this section, we give an upper bound for the number of finite Galois extensions L of K corresponding to the kernels of irreducible continuous representations with bounded Artin conductor and residue degree. This is done by examining each step of the proof of Proposition 1.3. Then we easily have an upper bound for the number of isomorphism classes of such representations.

Let $\rho : G_K \to \mathrm{GL}_d(k)$ be an irreducible representation as in Proposition 1.3, and let the notation be as in the proof of Proposition 1.3. It is clear from the proof of Proposition 1.3 that

$$(\text{the number of } L) \leq \big(\text{the number of towers } K \subset K' \subset K'' \subset L \text{ which satisfy } (*')\big) ,$$

where $(*')$ is as follows:

$$(*') \begin{cases} K'/K \text{ is unramified with } [K' : K] \leq f, \\ v_{K'}(\mathcal{D}_{L/K'}) \leq N, \\ K''/K' \text{ is a totally ramified Galois extension with } [K'' : K'] \leq J(d), \\ L/K'' \text{ is a totally ramified abelian extension.} \end{cases}$$

From the condition $(*')$ and the proof of Proposition 1.3, easily we have the following:

LEMMA 3.1.
(1) $[L : K''] \leq (q^f - 1)q^{f(2J(d)N-1)}$,
(2) $u_{L/K''} \leq 2J(d)N$.

Hence we calculate the number of totally ramified extensions K''/K' and L/K'' satisfying the conditions of Lemma 3.1 respectively.

First we prove a lemma. This is useful to count the number of totally ramified finite abelian extensions of K with conductor $\leq u$.

Let K^{ur} be the maximal unramified extension of K in K^{sep}, and let K_u be the compositum of all the finite abelian extensions of K in K^{sep} with conductor $\leq u$. Note that $K_0 = K^{\mathrm{ur}}$. For any totally ramified finite abelian extensions L and L' of K, we define an equivalence relation $L \sim L'$ by $N_{L/K}U_L = N_{L'/K}U_{L'}$, where $N_{L/K}$ denotes the norm map of L/K.

LEMMA 3.2. *The correspondence $L \mapsto K^{\mathrm{ur}}L$ gives a bijection between the set of equivalence classes of totally ramified finite abelian extensions of K with conductor $\leq u$ and the set of intermediate fields of K_u/K^{ur}.*

PROOF. Since the reciprocity map $\rho : K^\times \to \mathrm{Gal}\,(K^{\mathrm{ab}}/K)$ maps $N_{L/K}U_L$ to $\mathrm{Gal}\,(K^{\mathrm{ab}}/K^{\mathrm{ur}}L)$, the map in question is well-defined. First we prove the surjectivity of the map. For every intermediate field M of K_u/K^{ur}, by [Iwa86, Chap. III, Lemma 3.4], there exists a totally ramified extension L/K such that $M = K^{\mathrm{ur}}L$ and $K^{\mathrm{ur}} \cap L = K$. We have $U_K/(U_K)^u \xrightarrow{\simeq} (G_K^{\mathrm{ab}})^0/(G_K^{\mathrm{ab}})^u = \mathrm{Gal}\,(K_u/K^{\mathrm{ur}})$ by [Ser79, Chap. XV, §2, Theorem 2]. Here the first isomorphism is induced by the reciprocity map ρ. So K_u/K^{ur} is a finite extension, and $\mathrm{Gal}(M/K^{\mathrm{ur}}) = \mathrm{Gal}(K^{\mathrm{ur}}L/K^{\mathrm{ur}}) \xrightarrow{\simeq} \mathrm{Gal}(L/K)$, which implies L/K is a finite abelian extension. Thus this map is surjective.

Next we show the map is injective. Let L/K be a totally ramified finite abelian extension. For every prime element π_L of L, we have

$$K^\times = \langle N_{L/K}\pi_L \rangle \times U_K, \quad N_{L/K}L^\times = \langle N_{L/K}\pi_L \rangle \times N_{L/K}U_L .$$

Hence we have

$$\rho_L : U_K \to U_K/N_{L/K}U_L \overset{\tilde{\rho}}{\xrightarrow{\simeq}} \mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}})/\mathrm{Gal}(K^{\mathrm{ab}}/K^{\mathrm{ur}}L),$$

where $\tilde{\rho}$ is induced by the reciprocity map.

Let L, L' be totally ramified finite abelian extensions of K. Suppose $K^{\mathrm{ur}}L = K^{\mathrm{ur}}L'$. Then we have $\rho_L = \rho_{L'}$. Hence we have $N_{L/K}U_L = N_{L'/K}U_{L'}$. □

REMARK 3.3. As the case of $u \to \infty$ of the above lemma, the correspondence $L \mapsto K^{\mathrm{ur}}L$ gives a bijection between the set of equivalence classes of totally ramified finite abelian extensions of K and the set of finite intermediate fields of $K^{\mathrm{ab}}/K^{\mathrm{ur}}$.

From Lemma 3.2, there is a one-to-one correspondence between the equivalence classes of totally ramified finite abelian extensions of K with conductor $\le u$ and the subgroups of U_K/U_K^u. Next we calculate the number of totally ramified finite abelian extensions L'/K with conductor $\le u$ and $N_{L'/K}U_{L'} = N_{L/K}U_L$ for a given L as in Lemma 3.2.

LEMMA 3.4. *The cardinality of the equivalence class of L is $[L : K]$.*

PROOF. Let

$$U_K = \bigsqcup_{i=1}^{[L:K]} a_i N_{L/K}U_L$$

be the residue class decomposition of U_K modulo $N_{L/K}U_L$. Fix prime elements π_L and $\pi_{L'}$ of L and L' respectively. Then we have $N_{L'/K}\pi_{L'} = a_i N_{L/K}u_L N_{L/K}\pi_L$ for some i and u_L, where $u_L \in U_L$. Thus we have

$$\begin{aligned} N_{L'/K}L'^\times &= \langle N_{L'/K}\pi_{L'} \rangle \times N_{L'/K}U_{L'} = \langle a_i N_{L/K}u_L N_{L/K}\pi_L \rangle \times N_{L/K}U_L \\ &= \langle a_i N_{L/K}\pi_L \rangle \times N_{L/K}U_L . \end{aligned}$$

Hence there are $[L : K]$ totally ramified finite abelian extensions L'/K with $N_{L'/K}U_{L'} = N_{L/K}U_L$ for each L. □

Now we calculate the number of totally ramified finite abelian extensions of K with conductor $\le u$. We say that a finite abelian p-group A is *of type* $\lambda = (\lambda_1, \dots, \lambda_r)$ (where $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_r \ge 1$) if A is isomorphic to $(\mathbf{Z}/p^{\lambda_1}) \oplus \cdots \oplus (\mathbf{Z}/p^{\lambda_r})$. For a finite abelian p-group A of type λ, we denote by $\alpha_\lambda(k; p)$ the number of subgroups of A with order p^k. If the order of A is p^n, it is well-known that $\alpha_\lambda(k; p) = \alpha_\lambda(n-k; p)$ for $0 \le k \le n$ (cf. [Mac95, P. 181]).

PROPOSITION 3.5. *Let K be a local field with finite residue field $\boldsymbol{F}_q$, where $q = l^n$, and u a positive integer. Let λ_u be the type of U_K^1/U_K^u. Then the number of totally ramified finite abelian extensions of K with conductor $\leq u$ is*

$$\sigma_1(q-1)\sum_{k=0}^{n(u-1)} l^k \alpha_{\lambda_u}(k;l)\,.$$

Here, $\sigma_1(q-1)$ is defined by $\sum_d d$, where d runs through all the divisors of $q-1$.

PROOF. From Lemma 3.2 and Lemma 3.4, the number of totally ramified finite abelian extensions of K with conductor $\leq u$ is

$$\sum_{1\leq j\leq |U_K/U_K^u|} j \times (\text{the number of subgroups of } U_K/U_K^u \text{ with index } j)\,.$$

Since $U_K/U_K^u \xrightarrow{\simeq} V \times U_K^1/U_K^u$, where V is cyclic with order $q-1$, and $|V|$ is coprime to $|U_K^1/U_K^u|$, this is equal to

$$\begin{aligned}
&\sum_{1\leq j\leq |V|} j \times (\text{the number of subgroups of } V \text{ with index } j)\\
&\qquad \times \sum_{1\leq j'\leq |U_K^1/U_K^u|} j' \times (\text{the number of subgroups of } U_K^1/U_K^u \text{ with index } j')\\
&\quad = \sigma_1(q-1)\sum_{0\leq k\leq n(u-1)} l^k \alpha_{\lambda_u}(n(u-1)-k;l)\\
&\quad = \sigma_1(q-1)\sum_{0\leq k\leq n(u-1)} l^k \alpha_{\lambda_u}(k;l)\,. \qquad \square
\end{aligned}$$

REMARK 3.6. Note that we can calculate $\alpha_{\lambda_u}(k;l)$ explicitly if λ_u is determined (cf. [But87, §1]). If K is a finite extension of $\boldsymbol{Q}_l$ with $e = v_K(l) < l-1$, then we have the type λ_u easily since $U_K^1/U_K^u \xrightarrow{\simeq} \mathfrak{O}_K/\mathfrak{p}_K^{u-1}$ for any $u \geq 1$, where $\mathfrak{O}_K$ is the valuation ring of K and $\mathfrak{p}_K$ is the maximal ideal of $\mathfrak{O}_K$. The type of U_K^1/U_K^u is as follows: If $me+2 \leq u \leq (m+1)e+1$ $(m \geq 0)$, we have $\lambda_u = (\underbrace{m+1,\dots,m+1}_{n(u-1-me)},\ \underbrace{m,\dots,m}_{n((m+1)e-u+1)})$. In particular, if K is absolutely unramified (i.e., $v_K(l) = 1$), we have $\lambda_u = (\underbrace{u-1,\dots,u-1}_{n})$ for any $u > 1$.

From Lemma 3.2 and Lemma 3.4, we can calculate the number of totally ramified finite abelian extensions of K explicitly in some cases.

EXAMPLES. (1) Let K be a local field with residue field $\boldsymbol{F}_q$. Then there are $\sigma_1(q-1)$ tamely totally ramified finite abelian extensions L of K. This is a consequence of Proposition 3.5, since L/K is tamely ramified if and only if its conductor is less than or equal to 1.

(2) Let K be a local field with residue field $\boldsymbol{F}_q$, where $q = l^n$, and $u \geq 1$ a positive integer. Suppose that U_K^1/U_K^u is an abelian l-group of type $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r)$. There are $l^k \begin{bmatrix} r \\ k \end{bmatrix}_l$ totally ramified elementary l-abelian extensions of K with degree l^k $(0 \leq k \leq r)$ and with conductor $\leq u$. Here, $\begin{bmatrix} r \\ k \end{bmatrix}_l := \prod_{i=1}^{k} \frac{l^{r-i+1} - 1}{l^i - 1}$, is the l-binomial coefficient. This is proved as follows: Since U_K^1/U_K^u is an abelian group of type $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_r)$, the quotient group $(U_K^1/U_K^u)/(U_K^1/U_K^u)^l$ is isomorphic to $\boldsymbol{F}_l^r$. The number of subgroups of U_K appearing as $N_{L/K}U_L$ is equal to the number of $(r-k)$-dimensional $\boldsymbol{F}_l$-subspaces of $\boldsymbol{F}_l^r$, which is $\begin{bmatrix} r \\ r-k \end{bmatrix}_l = \begin{bmatrix} r \\ k \end{bmatrix}_l$.

Note that if $k > r$ then there exists no totally ramified elementary l-abelian extension of K with degree l^k and with conductor $\leq u$. Thus the number of totally ramified elementary l-abelian extensions of K with conductor $\leq u$ is

$$\sum_{k=0}^{r} l^k \begin{bmatrix} r \\ k \end{bmatrix}_l .$$

Let A be a finite p-group of order p^n. It is known that the number of subgroups of order p^k $(0 \leq k \leq n)$ is less than or equal to $\begin{bmatrix} n \\ k \end{bmatrix}_p$ (cf. [LS03, Proposition 1.6.1]). Thus we have the following:

COROLLARY 3.7. *Let K be a local field with finite residue field $\boldsymbol{F}_q$, where $q = l^n$. Then the number of totally ramified finite abelian extensions of K with conductor $\leq u$ is less than or equal to*

$$\sigma_1(q-1) \sum_{k=0}^{n(u-1)} l^k \begin{bmatrix} n(u-1) \\ k \end{bmatrix}_l .$$

We need to prepare another lemma for giving an upper bound mentioned at the beginning of this section.

LEMMA 3.8. *Let K be a local field with residue field $\boldsymbol{F}_q$.*

(1) *For any positive integers m and N, the number of totally ramified finite separable extensions of K with degree m and with $\nu_L(\mathcal{D}_{L/K}) \leq N$ is less than or equal to mq^{N-m+1}.*

(2) *If* char $K = 0$, *then for any positive integer m the number of totally ramified finite extensions of K with degree m is less than or equal to $mq^{m\nu_K(m)}$.*

PROOF. This is an easy consequence of Serre's mass formula. Let Σ_m (resp. $\Sigma_{m,N}$) be the set of totally ramified separable extensions L of K with degree m (resp. with degree m and $\nu_L(\mathcal{D}_{L/K}) \leq N$). From the mass formula we have

$$\sum_{L \in \Sigma_{m,N}} \frac{1}{q^{(N-m+1)}} \leq \sum_{L \in \Sigma_m} \frac{1}{q^{\nu_L(\mathcal{D}_{L/K})-m+1}} = m .$$

This proves (1) of the lemma.

When char $K = 0$, we have the result since $e - 1 \leq \nu_L(\mathcal{D}_{L/K}) \leq e - 1 + \nu_L(e)$, where $e = e(L/K)$. □

Finally we have the following upper bound.

THEOREM 3.9. *Let K be a local field with finite residue field $\boldsymbol{F}_q$, where $q = l^n$. Then the number of finite Galois extensions of K corresponding to the kernels of continuous irreducible representations $\rho : G_K \to \mathrm{GL}_d(k)$ with $n(\rho) \leq N$ and with $f(\rho) \leq f$ is less than or equal to*

$$\sum_{k=1}^{f} \sigma_1(q^k - 1)\left(\sum_{i=0}^{kn(2NJ(d)-1)} l^i \begin{bmatrix} kn(2NJ(d)-1) \\ i \end{bmatrix}_l\right)\left(\sum_{j=1}^{J(d)} jq^{k(NJ(d)-j+1)}\right).$$

If K is a finite extension of $\boldsymbol{Q}_p$, then we can replace the last factor $\sum_{j=1}^{J(d)} jq^{k(NJ(d)-j+1)}$ by $\sum_{j=1}^{J(d)} jq^{kj(\nu_K(j))}$.

PROOF. This is an easy consequence of Lemma 3.1, Corollary 3.7 and Lemma 3.8, since

$$\begin{aligned} &(\text{the number of towers } K \subset K' \subset K'' \subset L \text{ which satisfy } (*')) \\ &= \sum_{k=1}^{f} (\text{the number of towers } K'_k \subset K'' \subset L \text{ which satisfy } (*')), \end{aligned}$$

where K'_k is the unramified extension of K in K^{sep} with degree k. □

From this we also have an upper bound for the number of isomorphism classes of irreducible ones.

COROLLARY 3.10. *Let K be a local field with finite residue field $\boldsymbol{F}_q$, where $q = l^n$. Then the number of isomorphism classes of irreducible continuous representations $\rho : G_K \to \mathrm{GL}_d(k)$ with $n(\rho) \leq N$ and with $f(\rho) \leq f$ is less than or equal to*

$$\begin{aligned} fJ(d)(q^f - 1)q^{f(2NJ(d)-1)} \sum_{k=1}^{f} \sigma_1(q^k - 1)\left(\sum_{i=0}^{kn(2NJ(d)-1)} l^i \begin{bmatrix} kn(2NJ(d)-1) \\ i \end{bmatrix}_l\right) \\ \times \left(\sum_{j=1}^{J(d)} jq^{k(NJ(d)-j+1)}\right). \end{aligned}$$

If K is a finite extension of $\boldsymbol{Q}_p$, then we can replace the last factor $\sum_{j=1}^{J(d)} jq^{k(NJ(d)-j+1)}$ by $\sum_{j=1}^{J(d)} jq^{kj(\nu_K(j))}$.

PROOF. Let M be the maximum of $[L : K]$, where L runs through all the finite Galois extensions of K corresponding to the kernels of ρ's in question. Then from Lemma 3.1 we have $M \leq fJ(d)(q^f - 1)q^{f(2NJ(d)-1)}$. It is clear that the product $M \times$ (the number of subgroups of G_K which appear as the kernels of ρ's in question) is an upper bound for the number of isomorphism classes of those ρ's. □

REFERENCES

[But87] L. M. BUTLER, A unimodality result in the enumeration of subgroups of a finite abelian group, Proc. Amer. Math. Soc. 101 (1987), 771–775.

[BK] G. BÖCKLE AND C. KHARE, Finiteness results for mod l Galois representations over function fields, preprint.

[Iwa86] K. IWASAWA, Local class field theory, Oxford Math. Monogr., Oxford Sci. Publ., The Clarendon Press, Oxford Univ. Press, New York, 1986.

[Kat88] N. M. KATZ, Gauss sums, Kloosterman sums, and monodromy groups, Ann. of Math. Stud. 116, Princeton Univ. Press, Princeton, N.J., 1988.

[Kha00] C. KHARE, Conjectures on finiteness of mod p Galois representations, J. Ramanujan Math. Soc. 15 (2000), 23–42.

[LP] M. J. LARSEN AND R. PINK, Finite subgroups of algebraic groups, preprint.

[LS03] A. LUBOTZKY AND D. SEGAL, Subgroup growth, Progr. Math. 212, Birkhäuser Verlag, Basel, 2003.

[Mac95] I. G. MACDONALD, Symmetric functions and Hall polynomials, second edition, Oxford Math. Monogr., Oxford Sci. Publ., The Clarendon Press, Oxford Univ. Press, New York, 1995.

[Moo00] H. MOON, Finiteness results on certain mod p Galois representations, J. Number Theory 84 (2000), 156–165.

[Moo03] H. MOON, The number of monomial mod p Galois representations with bounded conductor, Tohoku Math. J. (2) 55 (2003), 89–98.

[MT01] H. MOON AND Y. TAGUCHI, Mod p-Galois representations of solvable image, Proc. Amer. Math. Soc. 129 (2001), 2529–2534 (electronic).

[Ser77] J.-P. SERRE, Linear representations of finite groups, Grad. Texts in Math. 42, Springer-Verlag, New York, 1977.

[Ser78] J.-P. SERRE, Une “formule de masse” pour les extensions totalement ramifiées de degré donné d’un corps local, C. R. Acad. Sci. Paris Sér. A-B 286 (1978), A1031–A1036.

[Ser79] J.-P. SERRE, Local fields, Grad. Texts in Math. 67, Springer-Verlag, New York, 1979.

[Ser87] J.-P. SERRE, Sur les représentations modulaires de degré 2 de Gal$(\bar{\boldsymbol{Q}}/\boldsymbol{Q})$, Duke Math. J. 54 (1987), 179–230.

[Sup76] D. A. SUPRUNENKO, Matrix groups, Trans. Math. Monogr. 45, Amer. Math. Soc., Providence, R.I., 1976.

[Tag] Y. TAGUCHI, On the finiteness of various Galois representations, To appear in : Proc. Symp. “Primes and Knots”, (T. Kohno and M. Morishita, eds.), Contemp. Math., Amer. Math. Soc.

[Tag02] Y. TAGUCHI, Induction formula for the Artin conductors of mod l Galois representations, Proc. Amer. Math. Soc. 130 (2002), 2865–2869 (electronic).

GRADUATE SCHOOL OF MATHEMATICS
KYUSHU UNIVERSITY
FUKUOKA 812–8581
JAPAN

E-mail address: s.harada@math.kyushu-u.ac.jp