Journal of Algebra **249,** 528–543 (2002)
doi:10.1006/jabr.2001.9079, available online at http://www.idealibrary.com on IDEAL®

Unramified Subextensions of Ray Class Field Towers

Farshid Hajir

Department of Mathematics, California State University, San Marcos, San Marcos, California 92096
E-mail: fhajir@csusm.edu

and

Christian Maire[1]

Laboratoire A2X, Université Bordeaux I, Cours de la Libération, 33405 Talence Cedex, France
E-mail: maire@math.u-bordeaux.fr

Communicated by Eva Bayer-Fluckiger

Received May 25, 2001

Fix a prime l. In this paper, we explore various senses in which the ramification in an infinite l-extension of number fields can be "small." In particular, (1) we construct infinitely many pairs of primes p, q (distinct from l) such that $\mathbb{Q}$ admits an infinite l-extension unramified outside $\{p, q\}$; and (2) we explore the possibility of finding infinite unramified subextensions inside infinite ramified l-extensions of number fields. © 2002 Elsevier Science (USA)

1. INTRODUCTION

Let l be a prime number, let k be a number field, and let T be a finite set of places of k. Let k_T be the maximal l-extension of k unramified outside T (inside some fixed algebraic closure of k), and put $G_{k,T} = \mathrm{Gal}(k_T/k)$. When is $G_{k,T}$ infinite? While we do not currently possess an algorithm for deciding such questions, we do have a number of sufficient conditions for the infinitude of $G_{k,T}$.

[1] Research at MSRI is supported in part by NSF Grant DMS-9701755.

0021-8693/02 $35.00

For example, if T contains *all* places of k dividing l, then k_T contains the cyclotomic (and all other) $\mathbb{Z}_l$-extensions of k; indeed, in this case, the resulting characters of $G_{k,T}$ onto $\mathbb{Z}_l$ go a long way toward revealing the structure of this group (cf. [18, 26]). For some results regarding the intermediate case where T contains some but not all primes dividing l, see [24].

By contrast, the tamely ramified (T is away from l) and unramified (T is empty) cases are not well understood; essentially the only result is the criterion of Golod–Shafarevich, which states that if k admits sufficiently many independent cyclic extensions of degree l unramified outside T, then $G_{k,T}$ is infinite. In other words, if the l-rank of $\mathrm{Cl}_{k,T}$ (the ray class group of k modulo $\mathfrak{m}_T = \prod_{\mathfrak{p}\in T}\mathfrak{p}$) is large, with respect to the l-rank of the unit group of k, then $G_{k,T}$ is infinite. The latter can happen either because the l-rank of the ideal class group of k is large, or because T has large cardinality. In Section 2, using a result of Gras and Munnier [9], we show that $G_{k,T}$ can be infinite in a large number of cases even when the ideal class group is trivial and T is small, for instance: $k = \mathbb{Q}$ and $|T| = 2$. This answers a question in [29, p. 413]. Note that for $k = \mathbb{Q}$ and $|T| = 1$, $G_{k,T}$ is cyclic, hence finite.

Let us abbreviate the tame condition (the finite places in T have absolute norm congruent to 1 modulo l) by $(T, l) = 1$. The main question we consider in this paper is: When T is nonempty, $(T, l) = 1$, and k_T/k is infinite, how can we measure the amount of ramification that actually takes place in this tower? To state a more precise question, let us introduce some more terminology. Let us say that F is an intermediate number field of k_T/k when $k \subseteq F \subseteq k_T$ and F/k is finite. For such a field F, let $T(F)$ be the set of F-divisors of the places in T. By a subextension of k_T/k, we will understand a field extension L/F, where $k \subseteq F \subset L \subseteq k_T$ with $[F : k] < \infty$.

Question 1.1. Suppose $(T, l) = 1$ and k_T/k is infinite. Is there an intermediate number field k' of k_T/k and a *proper* subset T' of $T(k')$ such that $G_{k',T'}$ is infinite?

Our main focus will in fact be the following particular case:

Question 1.2. Suppose $(T, l) = 1$ and k_T/k is infinite. Does k_T/k admit an infinite unramified subextension? In other words, is there an intermediate number field F in k_T/k such that $G_{F,\varnothing}$ is infinite?

One of our main results is that the answer to this question is "yes" when $|T|$ is large enough (Theorem 4.1). We also produce a number of infinite families of examples with T of small cardinality where Question 1.2 has a positive answer, for example, with base field $k = \mathbb{Q}$ and T consisting of two odd primes (Theorem 5.1 and Remark 5.4).

A recent conjecture of Fontaine and Mazur (Conj 5a of [6]) states that, when $(T, l) = 1$, $G_{k,T}$ has no infinite l-adic analytic quotients. In the final

section, we formulate a hypothesis regarding the subgroup growth of the groups $G_{k,T}$ (Question 6.8). As well as providing a positive response to Question 1.2, this hypothesis encompasses the Fontaine–Mazur conjecture, and even a generalization of it due to Boston; cf. Section 6, especially Remark 6.9.

On the other hand, a positive answer to the following strong version of Question 1.2 would clearly reduce the verification of the Fontaine–Mazur conjecture to the unramified case ($T = \emptyset$).

Question 1.3. Does every infinite tamely ramified l-extension K of a number field k admit an infinite unramified subextension; i.e., are there intermediate fields $k \subseteq F \subset L \subseteq K$, with F/k finite, such that L/F is infinite and unramified?

Note that the restriction to tame extension in the above questions (and in the Fontaine–Mazur conjecture) is necessary. For example, a $\mathbb{Z}_1$-extension admits no infinite unramified subextension. On the other hand, in a recent paper [15], we have studied Galois groups with wild ramification of "bounded depth" (meaning the higher ramification groups in the upper numbering at primes dividing l vanish at some prescribed finite level), and shown that they behave very much like tame Galois groups. The questions above and the Fontaine–Mazur conjecture are valid in this more general setting, but to fix ideas, we will deal from now on with the tame case only.

Our initial motivation for asking Questions 1.1 and 1.2 was the following. In previous papers [12–14], we have demonstrated the utility of tamely ramified extensions in lowering Martinet's record on asymptotically minimal root discriminants [25]. If inside a given record infinite tamely ramified tower, one could locate an infinite unramified tower, one would obtain a corresponding lowering of the estimate for the asymptotically minimal root discriminants of number fields of the given signature; see also Remark 5.12.

2. GOLOD–SHAFAREVICH FOR TAME TOWERS

Notation. Fix a prime l. For a pro-l group G, define the generator rank $d(G)$ and relation rank $r(G)$ by

$$d(G) = \dim_{\mathbb{F}_l} H^1(G, \mathbb{F}_l), \qquad r(G) = \dim_{\mathbb{F}_l} H^2(G, \mathbb{F}_l).$$

We will call a finitely generated pro-l group G "Golod–Shafarevich (**GS**)" if $r(G) \leq d(G)^2/4$; such groups are infinite (this is the Golod–Shafarevich Theorem [8] as improved by Vinberg and Gaschütz. For any group G, we write $d_l(G) = d(G/G^l)$ for its l-rank.

Let k be a number field, and let T be a finite set of prime ideals of k. We assume that $(T, l) = 1$; i.e., $N_{k/\mathbb{Q}}\mathfrak{p} \equiv 1 \bmod l$ for all $\mathfrak{p} \in T$. Put $\theta_T = 1$ if T is empty and k contains a primitive lth root of unity, 0 otherwise. Let E_k^T be the subgroup of E_k consisting of units congruent to 1 modulo all primes in T. If k has r_1 real and r_2 complex infinite places, then $d_l(E_k^T) = r_1 + r_2 - 1 + \theta_T$. We write $\mathrm{Cl}_{k,T}$ for the ray class group of k modulo $\mathfrak{m}_T = \prod_{\mathfrak{p}\in T}\mathfrak{p}$. We recall the criterion of Golod–Shafarevich for the infinitude of $G_{k,T}$ (see [18, 26, 28, 33]).

THEOREM 2.1 (Golod–Shafarevich criterion). *With notation as above, if*

$$d_l(\mathrm{Cl}_{k,T}) \geq 2 + 2\sqrt{r_1 + r_2 + \theta_T},$$

then $G_{k,T}$ is infinite.

We recall briefly the ingredients of the proof. The main arithmetic component of it is the estimate $0 \leq r(G_{k,T}) - d(G_{k,T}) \leq d_l(E_k^T)$ due to Shafarevich. The above criterion then follows from the fact that **GS** groups are infinite. Note that $d(G_{k,T}) = d(G_{k,T}^{ab}) = d_l(\mathrm{Cl}_{k,T})$. Also, all open subgroups of $G_{k,T}$ have *finite* maximal abelian quotients (we say that G is **FAb**). If $d(\mathrm{Cl}_{k,T}) = 1$, then $G_{k,T}$ is abelian, hence finite. Moreover, by a Theorem of Taussky, if $l = 2$ and $\mathrm{Cl}_{k,T} = (2, 2)$, then $G_{k,T}$ is finite (see [16, 21]).

3. A THEOREM OF GRAS AND MUNNIER

Fix a prime number l, a number field k, and a set $T = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ of prime ideals of k with cardinality n. A natural question is whether there exists a cyclic extension K/k of degree l which is "exactly-T-ramified," by which we mean that the set of (finite and infinite) places of k ramified in K is precisely T.

A theorem of Gras and Munnier [9] or [10] provides an answer. Let

$$A_k = \{\alpha \in k^\times | (\alpha) = \mathcal{A}^l \text{ for some fractional ideal } \mathcal{A} \text{ of } k\}.$$

The map sending $\alpha \in A_k$ to $\mathcal{A}$, where $(\alpha) = \mathcal{A}^l$, induces an exact sequence

$$1 \longrightarrow E_k/E_k^l \longrightarrow A_k/k^{\times l} \longrightarrow \mathrm{Cl}_k[l] \longrightarrow 1.$$

Hence, $d_l(A_k) = d_l(E_k) + d_l(\mathrm{Cl}_k)$.

THEOREM 3.1 (Gras–Munnier). *For each $\mathfrak{p}_i \in T$, let $\mathfrak{p}_i'$ be a prime of $k(\mu_l)$ dividing $\mathfrak{p}_i$. Then there exists an exactly-T-ramified cyclic extension of degree l over k if and only if there exists $(a_1, \ldots, a_n) \in (\mathbb{F}_l^\times)^n$ such that*

$$\prod_{i=1}^{n} \left(\frac{k(\mu_l, A_k^{1/l})/k(\mu_l)}{\mathfrak{p}_i'} \right)^{a_i} = 1.$$

In other words, the existence of such an extension is governed by the existence of a multiplicative relation between the relevant Frobenius symbols in the Kummer extension $k(\mu_l, A_k^{1/l})/k(\mu_l)$. We derive two consequences of this theorem, which will be very useful for us.

PROPOSITION 3.2. *Let k be a number field. Suppose F/k is an extension of degree n, and $\mathfrak{p}$ is a prime of k which splits completely in $F(\mu_l, A_F^{1/l})/k$. Let $S = \{\mathfrak{P}_1, \ldots, \mathfrak{P}_n\}$ be the set consisting of the n primes of F dividing $\mathfrak{p}$. Then,*

(1) $d_l \mathrm{Cl}_{F,S} \geq n$.

(2) *There exists a cyclic degree l extension K/F, exactly-S-ramified. Moreover, for any such K, one has $d_l \mathrm{Cl}_K \geq n - 1$.*

Proof. (1) The hypothesis for the decomposition of $\mathfrak{p}$ forces the triviality of all the Frobenius symbols appearing in an application of the Gras–Munnier criterion to F and implies that, for all $i = 1, \ldots, n$, there exists a cyclic degree l extension F_i/F exactly-$\{\mathfrak{P}_i\}$-ramified. Hence the compositum of these F_i is a subfield of the S-ray class field of F, and its Galois group over F (which is a quotient of $\mathrm{Cl}_{F,S}$ by class field theory) is an elementary abelian l-group of rank n. Thus, $d_l \mathrm{Cl}_{F,S} \geq n$.

(2) Again the Gras–Munnier criterion assures the existence of K. We can now give two proofs for the second claim. First, since K/k is ramified at each $\mathfrak{P}_i$, KF_i/K is unramified. Moreover, the n cyclic degree l extensions $K/F, F_1/F, \ldots, F_{n-1}/F$ are independent. So the Hilbert class field of K contains the $n - 1$ independent cyclic degree l extensions $KF_1/K, \ldots, KF_{n-1}/K$, giving us, by class field theory, that $d_l \mathrm{Cl}_K \geq n - 1$.

Alternatively, we can use the following genus theory formula (see, e.g., Schoof [31]),

$$d_l \mathrm{Cl}_K \geq \rho_{F/K} - 1 - d_l \frac{E_F}{E_F \cap N_{K/F} U_F},$$

where $\rho_{F/K}$ is the number of places of F which are ramified in K/F, E_F is group of units of F, and $E_F \cap N_{K/F} U_F$ are units of F which are everywhere local norms (U_F is the group of idèle units of F). At places prime to $\mathfrak{p}$, every unit of F is a local norm in K/F (since K/F is ramified only at $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$). Now, $\mathfrak{P}$ is decomposed in $F(E_F^{1/l})/F$, hence every unit $\varepsilon \in E_F$ is an lth power in $F_{\mathfrak{P}_i}$, and thus a norm in $K_{\mathfrak{P}_i}/F_{\mathfrak{P}_i}$. As consequence, we have

$$E_F = E_F \cap N_{K/F} U_F,$$

which gives $d_l \mathrm{Cl}_K \geq n - 1$. ∎

PROPOSITION 3.3. *For any finite set T of k-primes,*

(1) *There is a set S of k-primes of positive density such that, for all $\mathfrak{q} \in S$, k admits a $T \cup \{\mathfrak{q}\}$-exactly-ramified cyclic degree l extension.*

(2) *If $|T| > d_l(A_k)$, there exists a subset T_0 of T with $|T_0| \geq |T| - d_l(A_k)$ such that k admits a T_0-exactly-ramified cyclic degree l extension.*

Proof. The first claim is a simple consequence of the Cebotarev Density Theorem. To prove (2), consider $\mathrm{Gal}(k(\mu_l, A_k^{1/l})/k(\mu_l))$ as a vector space over $\mathbb{F}_l$, and let V be the subspace spanned by $\sigma_i = ((k(\mu_l, A_k^{1/l})/k(\mu_l))/\mathfrak{p}_i')$ for $i = 1, \ldots, n$. After renumbering we can assume that $\sigma_1, \ldots, \sigma_m$ generate V. Note that $m \leq d_l(A_k)$. Writing each σ_j $(m < j \leq n)$ as a "linear combination" of the basis vectors and then multiplying these together, we find a relation involving at least $n - m \geq n - d_l(A_k)$ of the σ_i. We then apply Theorem 3.1. ∎

4. UNRAMIFIED SUBEXTENSIONS WHEN $|T|$ IS LARGE

We can now show that Question 1.2 has a positive answer whenever $|T|$ is large (with respect to the unit rank of k).

THEOREM 4.1. *For a given number field k, there is a constant t with the following property: for every set of k-primes T satisfying $(T, l) = 1$ and $|T| \geq t$, there is a cyclic degree l extension K of k contained in k_T such that $G_{K,\varnothing}$ is infinite. In fact, we may take $t = 2u + 4 + 2\sqrt{lu+2} + 2\sqrt{u+1}$, which only depends on $u = r_1 + r_2$.*

Proof. First, if $d_l(\mathrm{Cl}_k) \geq 2 + \lceil 2\sqrt{u+1} \rceil$, then $G_{k,\varnothing}$ is infinite, so any $t \geq 0$ will do. We may assume, then, that $d_l(\mathrm{Cl}_k) \leq 1 + \lceil 2\sqrt{u+1} \rceil$, which gives the estimate $d_l(A_k) = d_l(\mathrm{Cl}_k) + d_l(E_k) \leq u + 1 + \lceil 2\sqrt{u+1} \rceil$. Now suppose $|T| > d_l(A_k)$. By Proposition 3.3(2), there exists a cyclic degree l extension K of k inside k_T such that $d_l(\mathrm{Cl}_K) \geq |T| - d_l(A_k) - 1 - d_l(E_K)$. By applying the Golod–Shafarevich criterion, K has an infinite unramified l-extension as soon as

$$|T| - d_l(A_k) - 1 - d_l(E_K) \geq 2 + 2\sqrt{d_l(E_K) + 1}.$$

The proof is now complete upon combining the estimate on $d_l(A_k)$ with the estimate $d_l(E_K) \leq ul + 1$. ∎

In the above proof, if we replace Proposition 3.3(2) with Proposition 3.3(1), then we can obtain infinite unramified subextensions of $k_{T \cup \{\mathfrak{q}\}}$, for appropriate auxiliary primes $\mathfrak{q}$, with a corresponding lowering of the threshold for the size of T to $t = 2 + u + 2\sqrt{lu+1}$; we leave the details to the reader.

5. INFINITE $G_{k,T}$ WHEN $|T|$ IS SMALL

Let us examine what is possibly the simplest situation by imposing the following conditions: T is nonempty and $k = \mathbb{Q}$. Then we have $r(G_{k,T}) = d(G_{k,T})$, so, by Golod–Shafarevich, this group is infinite as soon as its generator rank is at least 4, leaving the interesting cases of 2-generator and 3-generator groups.

First we focus on the case $l = 2$.

5.1. *Groups with Two Generators*

We now give the existence of infinitely many sets T consisting of odd primes with $|T| = 2$ or $|T| = 3$ such that $G_{\mathbb{Q},T}$ is an infinite group with $r = d = 2$. This answers (the first part of) Question 15 in [29, p. 413].

Recall that for any odd prime p, the maximal 2-extension of $\mathbb{Q}$ unramified outside $\{p\}$ or even outside $\{p, \infty\}$ is finite. By the result of Taussky mentioned at the end of Section 2, $G_{\{p,q,\infty\}}$ is finite if $p \equiv q \equiv 3 \bmod 4$. On the other hand, we have the following theorem.

THEOREM 5.1. (1) *There exist infinitely many pairs of odd primes p and q such that $\mathbb{Q}$ admits an infinite 2-extension unramified outside $\{p, q, \infty\}$.*

(2) *There exist infinitely many pairs of odd primes p and q such that $\mathbb{Q}$ admits an infinite 2-extension unramified outside $\{p, q\}$.*

The infinite groups $G_{\mathbb{Q},\{p,q,\infty\}}$ for part (1) *and $G_{\mathbb{Q},\{p,q\}}$ for part* (2) *have $r = d = 2$.*

Proof. First some notation: For an odd prime p and a divisor m of $p - 1$, let K_m be the unique subfield of degree m of the cyclotomic field $\mathbb{Q}(\mu_p)$.

(1) Suppose $p \equiv 17 \bmod 32$, so that K_{16}/K_8 is a CM extension ramified at the unique place of K_8 dividing p. Choose $\alpha \in K_8$ such that $K_{16} = K_8(\sqrt{\alpha})$. Let q be a prime that is totally decomposed in $K_8(i)/\mathbb{Q}$ (such primes have Dirichlet density 1/16). Then $N = K_8(\sqrt{q\alpha})$ is a totally complex quadratic extension of K_8 ramified at the eight places dividing q as well as the unique place above p and all the infinite places. By genus theory (see the proof of Proposition 3.2), $d_2\mathrm{Cl}_N \geq 9 - 1 = 8$, so that by Theorem 2.1, N, a $\{p, q, \infty\}$-ramified 2-extension of $\mathbb{Q}$, admits an infinite unramified 2-extension.

(2) Now suppose p is a prime satisfying $p \equiv 1 \bmod 16$ and $K = K_8$. Let $F = K(\sqrt{A_K})$; we may note, from genus theory, that since only one prime is ramified in $K/\mathbb{Q}$, the class number of K is odd and $d_l(A_K) = d_l(E_K)$. Thanks to the Cebotarev Density Theorem, there exist infinitely many primes q that split completely in $F/\mathbb{Q}$. Let $T = \{\mathfrak{q}_1, \ldots, \mathfrak{q}_8\}$ be the

set of primes of K over q. Proposition 3.2 implies that the 2-rank of the T-ray class group of k is at least 8. By the Golod–Shafarevich criterion, $G_{K,T}$ is infinite, so $K_T/\mathbb{Q}$ is an infinite 2-extension, ramified at p, q and nowhere else. ∎

Remark 5.2. After this paper was written, Lemmermeyer informed us that Part (1) of this theorem, with the same proof, can be found in [22]. For further results about the structure of $G_{\mathbb{Q},T}$ for small sets T, see Boston and Perry [4], Boston and Leedham-Green [5], and Koch [20].

Note that we have in fact proven a stronger result: for each prime $p \equiv 17 \bmod 32$, there is a set of primes S_p of Dirichlet density 1/16 such that, for all $q \in S_p$, $G_{\mathbb{Q},\{p,q,\infty\}}$ is infinite. (A similar set S'_p with much smaller density exists in the totally real case as well.) Indeed, in the totally complex case, an examination of the proof of (1) gives, via the cyclotomic reciprocity law, a fairly explicit criterion:

PROPOSITION 5.3. *Suppose p, q are odd primes satisfying*

$$p \equiv 17 \bmod 32, \qquad q^{(p-1)/16} \equiv 1,\ 2p - 1 \bmod 4p.$$

Then, $G_{\mathbb{Q},\{p,q,\infty\}}$ is infinite.

Remark 5.4. In view of Question 1.2, we note that the proof of (1) in the above theorem shows that there are infinitely many pairs of primes $\{p, q\}$ such that $\mathbb{Q}_{\{p,q,\infty\}}/\mathbb{Q}$ admits an intermediate number field with infinite unramified 2-tower.

EXAMPLE 5.5. For $T = \{17, 101, \infty\}$ and $T = \{17, 37501\}$, $G = G_{\mathbb{Q},T}$ is infinite, with $d(G) = r(G) = 2$. For the latter, we used PARI to find the first split prime in the appropriate governing field $K(\sqrt{A_K})$. The former gives an infinite unramified 2-tower whose layers have root discriminant less than $17^{15/16}101^{1/2} < 144$.

5.2. *Groups with Three Generators*

We can easily obtain examples of infinite $G_{\mathbb{Q},T}$ with generator rank 3; it suffices to take an example of rank 2 from above and throw in an extra prime! Further examples can be found in Schmithals [30] and Schoof [31], where imaginary quadratic fields with three discriminantal divisors and infinite 2-class field towers are constructed. But, we want to mention another construction which has the merit of allowing only small primes to ramify. We begin with a lemma.

LEMMA 5.6. *Let p_1, p_2, p_3 be three odd prime numbers. Suppose p_1 and p_2 split and p_3 ramifies in an imaginary quadratic extension k of $\mathbb{Q}$. Then the maximal 2-extension of k, unramified outside places dividing p_1, p_2, and p_3, is infinite.*

Proof. It is not difficult to see that the 2-rank of the T-ray class group of k, where T consists of the places of k dividing p_1, p_2, p_3, is 4. Thus, $G_{k,T}$ has $r = d = 4$ and is therefore infinite by Theorem 2.1. ∎

THEOREM 5.7. *Let $p_3 \equiv 3 \bmod 4$ be a prime. Then there exists a set S of rational primes of density 1/2 such that, for any pair of distinct primes $p_1, p_2 \in S$, $G_{\mathbb{Q},\{p_1,p_2,p_3,\infty\}}$ is an infinite 3-generator pro-2 group.*

Proof. We apply the previous lemma with $k = \mathbb{Q}(\sqrt{-p_3})$, where S is the set of primes which split in k. ∎

EXAMPLE 5.8. Since 3 and 5 split completely in $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}$ admits an infinite 2-extension unramified outside $\{3, 5, 11, \infty\}$. The fields in this tower have root discriminant bounded by $3 \cdot 5 \cdot 11 = 165$. By the discriminant lower bounds (see Odlyzko [27]), assuming the Generalized Riemann Hypothesis, $\mathbb{Q}_{\{3,5,11\}}/\mathbb{Q}$ is a finite extension. The possibility is raised in [29, p. 413] that, for all triples of odd primes p, q, r, $\mathbb{Q}_{\{p,q,r,\infty\}}/\mathbb{Q}$ is an infinite 2-extension; in this direction, see Remark 5.12 below. It is unknown to us even whether $\mathbb{Q}_{\{3,5,7,\infty\}}/\mathbb{Q}$ is an infinite tower or not; note that the product of these primes, 105, is well above the GRH bound $8\pi e^{\gamma} \approx 44.7$.

5.3. *The Case $l > 2$*

THEOREM 5.9. *For every prime l, there exist infinitely many pairs of primes p and q (distinct from l) such that $\mathbb{Q}$ admits an infinite l-extension unramified outside $\{p, q\}$.*

Proof. We have already discussed the case $l = 2$, so assume l is odd, and let $n = l$ if $l \geq 11$, else put $n = l^2$. Suppose p is a prime satisfying $p \equiv 1 \bmod n$ and $K = K_n$, with notation as in the proof of Theorem 5.1. Let $F = K(\mu_l, A_K^{1/l})$. Thanks to the Cebotarev Density Theorem, there exist infinitely many primes q that split completely in $F/\mathbb{Q}$. The rest of the proof, showing that $G_{\mathbb{Q},\{p,q\}}$ is infinite, is exactly as in the proof of Theorem 5.1(2), and is left to the reader. ∎

5.4. *Infinite $G_{k,T}$ with T a Singleton*

We may ask for a criterion for the existence of a single prime $\mathfrak{p}$ such that $k_{\{\mathfrak{p}\}}/k$ is infinite. For instance, if k has trivial l-class group, then no such prime exists. We now show that, on the other hand, if k possesses even a mildly nontrivial l-class group (compared to its degree), then such primes, indeed infinitely many, always exist. For simplicity, we restrict to $l = 2$ and k totally complex; it is clear how to adapt the idea to the general case.

THEOREM 5.10. *Let k be a totally complex number field of degree m over $\mathbb{Q}$. Suppose that there exists an unramified extension F of degree 2^n over k. If*

$$2^n \geq 2m + 3 + 2\sqrt{m^2 + 3m + 1},$$

then there exists infinitely many prime ideals $\mathfrak{p}$ of k such that $k_{\{\mathfrak{p}\}}/k$ admits an infinite unramified subextension.

Proof. Thanks to the Cebotarev Density Theorem, there exist infinitely many primes $\mathfrak{p}$ of k such that $\mathfrak{p}$ is totally decomposed in $F(\sqrt{A_F})/k$. By Proposition 3.2, there is a quadratic extension K of F contained in $k_{\{\mathfrak{p}\}}$ satisfying $d_2(\mathrm{Cl}_K) \geq 2^n - 1$. The hypothesis on n ensures that $2^n - 1 \geq 2 + 2\sqrt{2^n m + 1}$, so K satisfies the Golod–Shafarevich criterion for the infinitude of $G_{K,\varnothing}$. If k is imaginary quadratic, one needs only $n \geq 4$. ∎

Note that if we merely want $\mathfrak{p}$ such that $k_{\{\mathfrak{p}\}}/k$ is infinite, we can use a slightly better bound.

5.5. *When is k_T/k Infinite for all Singleton T?*

Suppose k is a number field and l is any prime. There is a least number $b = b_l(k) \geq 0$ such that whenever T satisfies $(T, l) = 1$ and $|T| \geq b$, k_T/k is infinite. Indeed, the l-rank of the T-ray class group tends to infinity with $|T|$, hence it surpasses the Golod–Shafarevich bound eventually. Of course, $b_l(k) = 0$ if and only if k has an infinite unramified l-class field tower. Is it true that there are no number fields k with $b_l(k) = 1$? We rephrase this question more directly as follows.

Question 5.11. Suppose k is a number field such that, for every prime $\mathfrak{p}$ not dividing l, the group $G_{k,\{\mathfrak{p}\}}$ is an infinite pro-l group. Does this imply that $G_{k,T}$ is infinite?

Remark 5.12. A positive answer to this question is essentially an improvement of the Golod–Shafarevich criterion. It would follow, for example, that an imaginary quadratic field with five discriminantal divisors has an infinite 2-class field tower (apply Theorem 2.1, noting that $\theta_T = 0$ when T is nonempty). In particular, the quadratic field of discriminant $-5460 = -4 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ with class group $(2, 2, 2, 2)$ would have an infinite unramified 2-tower, with root discriminant $\sqrt{5460} < 74$. The current record is 82.11 [14].

5.6. *A Reinterpretation*

Here we will recast the questions we have investigated thus far in a more group-theoretical framework. For a number field k and a prime l, let S be the set of all places of k not dividing l (including the infinite ones).

Then k_S/k is the maximal tame l-extension of k, with Galois group $G_{k,S}$. Choose a prime $\mathfrak{P}$ of k_S lying over each prime $\mathfrak{p} \in S$ and let $I_\mathfrak{p}$ be the inertia group corresponding to these choices. For finite subsets T of S, the group of interest to us, $G_{k,T}$, is the quotient $G_{k,S}/N_{k,T}$ corresponding to the closed normal subgroup $N_{k,T}$ generated by the collection $\mathfrak{C}_{k,T} = \{I_\mathfrak{q} | \mathfrak{q} \notin T\} \subseteq \mathfrak{C}_k = \mathfrak{C}_{k,\emptyset}$ of pairwise nonconjugate subgroups of $G_{k,S}$.

In a previous subsection, we asked: Suppose $\mathfrak{C}_k$ generates a closed subgroup of finite index in $G_{k,S}$; i.e., $G_{k,\emptyset}$ is finite; is it possible that by removing a single element of $\mathfrak{C}_k$, the resulting new subgroup has infinite index? (In other words, is there a prime $\mathfrak{p} \in S$ such that $k_{\{\mathfrak{p}\}}/k$ is infinite?) For $k = \mathbb{Q}$, for example, the answer is no. But for $k = \mathbb{Q}$, we showed in Theorems 5.1 and 5.9 how, by removing two elements of $\mathfrak{C}_\mathbb{Q}$, we can get subgroups of infinite index.

The interpretation of Question 5.11 in these terms is as follows.

Question 5.13. Consider the Galois group $G_{k,S}$ of the maximal tame l-extension of k, equipped with the family of pairwise nonconjugate subgroups $\mathfrak{C}_k$ as above. Suppose by removing *any* single element $I_\mathfrak{p}$ of $\mathfrak{C}_k$, the closed subgroup $N_{k,\{\mathfrak{p}\}}$ generated by the remaining elements has infinite index in $G_{k,S}$. Does it follow that the closed subgroup generated by $\mathfrak{C}_k$ itself has infinite index in $G_{k,S}$?

6. FONTAINE–MAZUR AND GENERALIZATIONS

In this section, we recall the Fontaine–Mazur conjecture and some generalizations. After defining some invariants measuring the subgroup growth of pro-l groups, we introduce a hypothesis on the subgroup growth of the tame Galois groups $G_{k,T}$ which would have as consequence not only a positive answer to Question 1.2, but also to the Fontaine–Mazur conjecture and even a generalization of it due to Boston (for the latter, we require a second conjecture of Boston's as well).

6.1. *Measures of Subgroup Growth*

To a finitely generated pro-l group G, we will attach a function $a_G(s)$ on the unit interval, and an associated invariant $\gamma(G)$, both of which measure the rate at which the generator-rank of open subgroups grows.

DEFINITION 6.1. For a finitely generated pro-l-group G and a real number $s \in [0, 1]$, we put

$$a_G(s) = \liminf_{U \subset_o G} d(U)/[G : U]^s,$$

where $U \subset_O G$ means U is an open subgroup of G. Let $\gamma(G) = \sup\{s \geq 0 | a_G(s) > 0\}$ be the "growth exponent" of G; if $a_G(s)$ vanishes on [0, 1], we put $\gamma(G) = 0$.

It is clear that $a_G(s)$ is a nonincreasing, nonnegative function on the unit interval.

PROPOSITION 6.2. *For a finitely generated pro-l group G, we have*:

(1) $a_G(1) \leq d(G) - 1$;
(2) *if G is free-pro-l, then* $a_G(1) = d(G) - 1$;
(3) *if G is a Demuskin group, then* $a_G(1) = d(G) - 2$;
(4) $\gamma(G) = 1$ *if G is free pro-l or a Demuskin group*;
(5) *if G is l-adic analytic, then* $a_G(1) = 0$.

Proof. (1) and (2) are consequences of Schreier's Theorem: for an open subgroup U of G,

$$d(U) - 1 \leq [G : U](d(G) - 1),$$

with equality for all U if and only if G is free. (3) This is well known (see [32] for example). (4) follows from (2) and (3). (5) It is a result of Lubotzky and Mann that G is l-adic analytic if and only if it has bounded generator rank [23, 34]. ∎

6.2. *Boston's Conjectures*

We recall two conjectures due to Boston. The first generalizes the Fontaine–Mazur conjecture, which states that an l-adic representation of the absolute Galois group of a number field k which factors through $G_{k,T}$ (for a finite set of primes T satisfying $(T, l) = 1$) must "come from algebraic geometry" (in a precise sense); algebro-geometric considerations then imply that such an extension must be finite. To summarize,

Conjecture 6.3 (Fontaine–Mazur). If k is a number field and T is a finite set of primes of k with $(T, l) = 1$, then for every $n \geq 1$, the image of every continuous l-adic Galois representation $G_{k,T} \to \mathrm{GL}_n(\mathbb{Z}_l)$ is finite.

This is equivalent to the conjecture stated in the Introduction, since every finitely generated l-adic analytic group is linear over $\mathbb{Z}_l$. Motivated by considerations concerning the deformation rings of l-adic Galois representations, Boston [2] has extended this conjecture as follows.

Conjecture 6.4 (Boston's generalization of Fontaine–Mazur). Let k and T be as above. For every complete, Noetherian local ring R with finite residue field of characteristic l, and $n \geq 1$, a continuous homomorphism $G \to \mathrm{GL}_n(R)$ has finite image. In particular, if G is a subgroup of $\mathrm{GL}_n(R)$, then G is finite.

An earlier conjecture of Boston's (see [3]) concerns the generator-rank-growth of groups embedded in $\mathrm{GL}_n(R)$.

Conjecture 6.5 (Boston). If G is a finitely generated pro-l-subgroup of $\mathrm{GL}_n(R)$, where R is a complete, Noetherian local ring with finite residue field of characteristic l with Krull dimension r, then there is a constant C depending on G such that

$$d(U) \leq C[G : U]^{1-1/r},$$

for all open subgroups $U \subset_O G$.

Remark 6.6. If $R = \mathbb{Z}_l$, then $r = 1$, and the conjecture asserts that the open subgroups have bounded generator rank. This conjecture is true in that case (Proposition 6.2).

Some examples from [11] reveal a relationship between Boston's two conjectures.

THEOREM 6.7. *Let l be a prime number. Suppose Conjecture* 6.5 *is true. There exist infinitely many number fields k such that, for every complete Noetherian local ring with finite residue field of characteristic l, and every $n \geq 1$, $G_{k,\varnothing}$ cannot be realized as a subgroup of* $\mathrm{GL}_n(R)$.

Proof. Given an integer $t > 0$, the first author has constructed [11] infinitely many number fields k equipped with a sequence of unramified l-extensions k_n/k $(n = 1, 2, \ldots)$ such that

(1) the degree $[k_n : k] \to \infty$,

(2) $t \leq d_l(\mathrm{Cl}_{k_n})/[k_n : k] \leq d_l(\mathrm{Cl}_k)$.

This shows that $G_{k,\varnothing}$ has a sequence of open subgroups U_n with index tending to infinity such that $d(U_n) \geq t[G_{k,\varnothing} : U_n]$. According to Conjecture 6.5, $G_{k,\varnothing}$ is not linear over any complete, Noetherian local ring with finite residue field of characteristic l. ∎

6.3. *A Final Question*

In this subsection, we will present a final question about the structure of the groups $G_{k,T}$, a positive answer to which would imply (a) a positive answer to Question 1.2, (b) the Fontaine–Mazur conjecture, and even (c) Boston's generalization of the latter, as long as we admit his Conjecture 6.5.

Question 6.8. Suppose $(T, l) = 1$ and $G_{k,T}$ is infinite. Is it true that $\gamma(G) = 1$ for every infinite quotient G of $G_{k,T}$?

Remark 6.9. (1) Even the much weaker statement: Every infinite quotient G of $G_{k,T}$ satisfies $\gamma(G) > 0$ would imply the Fontaine–Mazur conjecture, since l-adic analytic groups have bounded generator-rank.

(2) Moreover, a positive answer to Question 6.8 together with Conjecture 6.5 would mean that no infinite quotient of $G_{k,T}$ is linear over complete Noetherian local rings with finite residue field of characteristic l, so l-adic representations of $G_{k,T}$ over such rings must have finite image, verifying Conjecture 6.4.

(3) On the other hand, a positive answer to Question 1.3, which is stronger than Questions 1.1 and 1.2, would reduce the verification of Question 6.8 to the unramified case ($T = \varnothing$).

Since the only current method for showing $G_{k,T}$ is infinite is to show it has an open subgroup which is Golod–Shafarevich, we begin by asking what one can say about the growth exponent $\gamma(G)$ of groups G which are **GS**, i.e., have few relations? First, we describe a construction of Shalev, which shows that $\gamma(G)$ can vanish for such groups.

EXAMPLE 6.10. Let F_d be free pro-l of rank d ($d \geq 1$), and let $\mathbb{Z}_l$ be the l-adic integers. Let $G = F_d \times \mathbb{Z}_l$. Then G has $d+1$ generators and d relations, so it is a **GS**-group. Now for integers m and n, if we take $U(m,n) = A_m \times l^n\mathbb{Z}_l$, with $A_m \subset_O F_d$, $|F_d/A_m| = m$, then $U(m,n)$ is an open subgroup of G. Now, $|G/U(m,n)| = m \cdot l^n$, and $U(m,n)$ is a pro-l-group with $(1 + m(d-1)) + 1$ generators. Thus,

$$d(U(m,n))/[G : U(m,n)] = \frac{2}{m \cdot l^n} + \frac{d-1}{l^n}.$$

In particular, $a_G(1) = 0$ for this group. Note, however, that this group is not **FAb** (it has open subgroups with infinite abelianization), so is not one of our groups $G_{k,T}$.

We are led to the following purely group-theoretical.

Question 6.11. Suppose G is a finitely generated pro-l group which is **GS** and **FAb**; does it follow that $\gamma(G) = 1$?

Finally, let us show how a positive answer to Question 6.8 (in fact a much milder condition) would imply an affirmative answer to Question 1.2. Our proof uses the following theorem of Furuta [7].

THEOREM 6.12 (Furuta). *Suppose K/k is a tamely ramified l-extension of number fields, with t finite places of k ramified in K. Let $u_0 = d(E_k/E_k^l)$ be the l-rank of the unit group of k. If*

$$d(\mathrm{Gal}(K/k)) \geq 2 + 2\sqrt{t + u_0 + 1},$$

then the l-class field tower of K is infinite.

THEOREM 6.13. *Suppose $(T, l) = 1$ and $G_{k,T}$ is infinite. Moreover, assume that $\gamma(G_{k,T}) > 1/2$. Then, there exists an intermediate number field $k \subseteq K \subset$*

k_T such that $G_{k,\varnothing}$ is **GS**. *In particular, k_T/k admits an infinite unramified subextension.*

Proof. By assumption, we may choose $r > 1/2$ such that $a_{G_{k,T}}(r) > 0$. Let k_i be a nested sequence of subfields in k_T/k such that

$$\lim_i \frac{d_l(U_i)}{[G_{k,T} : U_i]^r} > 0,$$

where each $U_i = \mathrm{Gal}(k_T/k_i)$ is open. Let us write $m_i = [k_i : k]$ for its degree. Then the unit rank $u_i = d(E_k/E_k^l)$ is at most $m_i u_0 + 1$. The set T_i of places of k_i above those in T has cardinality bounded above by $m_i t_0$. If for all i, $d_l(U_i) < 2 + 2\sqrt{t_i + u_i + 1}$, then

$$\lim_i \frac{d_l(U_i)}{[G_{k,T} : U_i]^r} \leq \lim \frac{c\sqrt{m_i}}{m_i^r} = 0,$$

where c is a constant independent of i. This contradicts the condition on k_i. Thus, there exists i such that $d_l(U_i) \geq 2 + 2\sqrt{t_i + u_i + 1}$. Let k_i^{ab} the maximal abelian extension of k_i in k_T. Since k_i^{ab}/k_i is ramified in at most t_i places, and has Galois group of l-rank $d_l(U_i)$. Furuta's theorem shows that k_i^{ab} has an infinite unramified Hilbert l-class field tower. ∎

ACKNOWLEDGMENTS

We thank A. Shalev for helpful correspondence, and especially for providing Example 6.10. The first author was partially supported by a CSUSM Faculty Development Grant. The second author was supported by a postdoctoral fellowship at Mathematical Sciences Research Institute (Berkeley), by CNRS, and by Department A2X of Bordeaux I.

REFERENCES

1. N. Boston, Some cases of the Fontaine-Mazur conjecture, *J. Number Theory* **42** (1992), 285–291.
2. N. Boston, Some cases of the Fontaine-Mazur conjecture, II, *J. Number Theory* **75** (1999), 161–169.
3. N. Boston, Explicit deformation of galois representations, *Invent. Math.* **103** (1991), 181–196.
4. N. Boston and D. Perry, Maximal 2-extensions with restricted ramification. *J. Algebra* **232** (2000), 664–672.
5. N. Boston and C. Leedham-Green, Explicit computation of Galois p-groups unramified at p, preprint, 2000.
6. J.-M. Fontaine and B. Mazur, Geometric Galois representations, elliptic curves and modular forms, Proceedings of a Conference held in Hong Kong, December 18–21, 1993 (J. H. Coates and S. T. Yau, Eds.), International Press, Cambridge, MA, and Hong Kong.
7. Y. Furuta, On class field towers and the rank of ideal class groups, *Nagoya Math. J.* **48** (1972), 147–157.
8. E. Golod and I. Shafarevich, On class field towers, *Izv. Akad. Nauk SSSR* **28** (1964), 261–272 [In Russian]; English transl. in *Amer. Math. Soc. Transl.* **48** (1965), 91–102.

9. G. Gras and A. Munnier, Extensions cycliques T-totalement ramifiées, *Publ. Math. Besançon*, 1996/97, 1997/98.
10. G. Gras, Pratique de la théorie du corps de classes global, in preparation.
11. F. Hajir, On the growth of p-class groups in p-class field towers, *J. Algebra* **188** (1997), 256–271.
12. F. Hajir and C. Maire, Tamely ramified towers and discriminant bounds for number fields, *Compositio Math.* **128** (2001), 35–53.
13. F. Hajir and C. Maire, Asymptotically good towers of global fields, Proceedings of the European Congress of Math., Barcelona 2000, Progr. Math. **202**, 207–218.
14. F. Hajir and C. Maire, Tamely ramified towers and discriminant bounds for number fields II, *J. Symbolic Comput.*, to appear.
15. F. Hajir and C. Maire, Extensions of number fields with wild ramification of bounded depth, *Internat. Math. Res. Notices* **13** (2002), 667–696.
16. H. Kisilevsky, Number fields with class number congruent to 4 mod 8 and Hilbert' theorem 94, *J. Number Theory* **8** (1976), 271–279.
17. G. Klass, C. R. Leedham-Green, and W. Plesken, "Linear Pro-p-Groups of Finite Width," Lecture Notes in Math., Vol. 1674, Springer-Verlag, New York/Berlin, 1997.
18. H. Koch, "On p-extensions with given ramification, Appendix 1, Galois cohomology of algebraic number fields," Deutscher Ver. der Wiss., Berlin, 1978.
19. H. Koch, "Galoissche Theorie der p-Erweiterungen," Springer-Verlag, New York/Berlin/ Heidelberg, 1970.
20. H. Koch, On maximal 2-extensions of $\mathbb{Q}$ with given ramification, preprint.
21. F. Lemmermeyer, Unramified quaternion extensions of quadratic number fields. *J. Théor. Nombres Bordeaux* **9** (1997), 51–68.
22. F. Lemmermeyer, manuscript in preparation.
23. A. Lubotzky and A. Mann, Powerful p-groups II, *J. Algebra* **113** (1988), 207–214.
24. C. Maire, On the $\mathbb{Z}_l$-rank of abelian extensions with restricted ramification, *J. Number Theory*, to appear.
25. J. Martinet, Tours de corps de classes et estimations de discriminants, *Invent. Math.* **44** (1978), 65–73.
26. J. Neukirch, A. Schmidt, and K. Wingberg, Cohomology of number fields, *Grundlehren Math. Wiss.* 323, Springer-Verlag, Berlin 2000.
27. A. M. Odlyzko, Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: A survey of recent results, *Sém. Théorie Nombres, Bordeaux* **2** (1990), 119–141.
28. P. Roquette, On class field towers, *in* "Algebraic Number Theory" (J. Cassels and A. Fröhlich, Eds.), Academic Press, New York, 1980.
29. M. du Sautoy, D. Segal, and A. Shalev, New horizons in pro-p-groups, *Progr. Math.* **184**, 2000.
30. B. Schmithals, Konstruktion imaginärquadratischer Körper mit unendlichem Klassenkörperturm (German) *Arch. Math. (Basel)* **34** (1980), 307–312.
31. R. Schoof, Infinite class field towers of quadratics fields, *J. Reine Angew. Math.* **372** (1986), 209–220.
32. J.-P. Serre, "Cohomologie Galoisienne," Lecture Notes in Math., Vol. 5, Springer-Verlag, New York/Berlin/Heidelberg, 1994.
33. I. Shafarevich, Extensions with prescribed ramification points, *Publ. Math. IHES* **18** (1964), 71–95 [In Russian]; English transl. in *Amer. Math. Soc. Transl.* **59** (1966), 128–149.
34. A. Shalev, Finite groups, *in* "Finite and Locally Finite Groups," pp. 401–450, Kluwer Academic, Dordrecht, 1995.
35. M. A. Tfasman and S. G. Vladut, Asymptotic properties of global fields and generalized Brauer–Siegel Theorem, preprint 1999.