Ann. Sci. Math. Québec **33** (2009), no 2, 145–154

THE FEWEST PRIMES RAMIFIED IN A G-EXTENSION OF $\mathbb{Q}$

NIGEL BOSTON AND NADYA MARKIN

Dedicated to Paulo Ribenboim on the occasion of his 80th birthday.

RÉSUMÉ. Si G est un groupe fini, nous conjecturons qu'il existe une G-extension de $\mathbb{Q}$ ramifiée en exactement d premiers, où $d \geq 1$ est le nombre minimal de générateurs de l'abélianisation de G (et nous montrons qu'aucune G-extension de $\mathbb{Q}$ n'est ramifiée en moins de premiers). Nous conjecturons aussi que pour tout $n \geq d$, il y a une densité positive de G-extensions qui sont ramifiées en n premiers et dont la conjugaison complexe est égale à n'importe quel élément donné de G d'ordre 1 ou 2. Nous apportons quelques éléments de preuves pour ces conjectures ainsi que des preuves complètes pour certains cas particuliers.

ABSTRACT. If G is a finite group, then we conjecture that there exists a G-extension of $\mathbb{Q}$ ramified at exactly d primes, where $d \geq 1$ is the minimal number of generators of the abelianisation of G (and show that no G-extension of $\mathbb{Q}$ is ramified at fewer primes). We also conjecture that for any $n \geq d$ there is a positive density of G-extensions ramified at n primes with complex conjugation equal to any given element of G of order 1 or 2. Evidence for these conjectures, together with proof in special cases, is given.

1. Introduction

Let G be a nontrivial finite group. The inverse Galois problem indicates that there should exist a Galois extension $K/\mathbb{Q}$ with Galois group isomorphic to G. We call this a G-extension of $\mathbb{Q}$. Indeed, there should be such an extension of $\mathbb{Q}(t)$ that yields, by Hilbert's irreducibility theorem, infinitely many G-extensions of $\mathbb{Q}$ [16]. In this paper we seek to refine this conjecture further by introducing constraints on ramification of primes. In particular, if n is a positive integer, should there exist a G-extension of $\mathbb{Q}$ ramified at no more than n primes and, if so, how many? For this question we also need to specify whether the infinite prime is counted.

Throughout this paper, d will denote the minimal number of generators of the abelianisation G^{ab} of G, where if $G^{ab} = \{1\}$, then d is taken to be 1. It is easy to see by cyclotomic theory that if G is abelian, then there exists a G-extension $K/\mathbb{Q}$ ramified at d primes, where K can even be specified to be totally real (so that there is no ramification at the infinite prime). For certain groups there exist G-extensions $K/\mathbb{Q}$

Reçu le 27 juillet 2009 et, sous forme définitive, le 4 décembre 2009.

ramified at $d-1$ finite primes (for example, $G = \mathbb{Z}/2 \times \mathbb{Z}/2$ and $K = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$), but none of these are totally real. We conclude with the following theorem.

Theorem 1.1. *If G is a nontrivial finite abelian group with exactly d generators, then there exists a G-extension of $\mathbb{Q}$ ramified at exactly d primes (counting the infinite prime). Moreover, there is no such extension ramified at fewer than d primes.*

Proof. We sketch the proof. Suppose $G \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_d$. By Dirichlet's theorem we can pick primes $p_i \equiv 1 \pmod{2n_i}$. Then G is a quotient of

$$\mathbb{Z}/\left((p_1-1)/2\right) \times \cdots \times \mathbb{Z}/\left((p_d-1)/2\right)$$

and so is isomorphic to $\mathrm{Gal}(K/\mathbb{Q})$, where K is a subfield of the compositum of the maximal real subfields of the p_i-th cyclotomic fields ($1 \le i \le d$). Note that K is ramified at exactly d primes.

Conversely, suppose $K/\mathbb{Q}$ has Galois group G and the only finite primes ramified in K are $p_1, \ldots, p_k$. By Kronecker-Weber K is a subfield of the n-th cyclotomic field L, where $n = p_1^{r_1} \ldots p_k^{r_k}$ (the p_i's are distinct, $r_i \ge 1$ and $r_i \ge 2$ if $p_i = 2$). Note that G is a quotient of $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/p_1^{r_1})^* \times \cdots \times (\mathbb{Z}/p_k^{r_k})^*$, which has at most $k+1$ generators. If K is totally real, then $K \subseteq L^+$, the maximal real subfield of L. Then G is a quotient of $\mathrm{Gal}(L^+/\mathbb{Q})$, which has at most k generators. In either case, the number of generators of G is less than or equal to the number of ramified (finite or infinite) primes. □

If G is nonabelian, then the above yields a G^{ab}-extension of $\mathbb{Q}$ ramified at exactly d primes. We believe that there need be no further primes ramified in obtaining a G-extension of $\mathbb{Q}$. In other words, our first main conjecture states the following.

Conjecture 1.2. *If G is a nontrivial finite group and $d \ge 1$ denotes the minimal number of generators of G^{ab}, then there exists a G-extension of $\mathbb{Q}$ ramified at exactly d primes (counting the infinite prime). Moreover, there is no such extension ramified at fewer than d primes.*

Note that the last sentence is proven by Theorem 1.1 and, if $G^{ab} = \{1\}$, Minkowski's Theorem. We refine this conjecture further to count G-extensions of $\mathbb{Q}$ ramified at n finite primes with complex conjugation specified to be a particular element σ of order 1 or 2 of G. This allows us, for instance, to specify whether we are considering only totally real extensions ($\sigma = \{1\}$) or not. Let $\pi_n(x)$ denote the number of n-tuples of rational primes all of which are less than or equal to x.

Conjecture 1.3. *Let G be a nontrivial finite group and $d \ge 1$ denote the minimal number of generators of G^{ab}. Let $\sigma \in G$ have order 1 or 2 and n be any positive integer. Let $S_{\sigma,n,x}$ be the set of all G-extensions of $\mathbb{Q}$ ramified at at most n primes less than or equal to x and with a complex conjugation equal to σ. Then $|S_{\sigma,n,x}|/\pi_n(x)$ tends to a limit as $x \to \infty$, depending only on G and n. Call this limit $\delta(G,n)$. Furthermore, $\delta(G,n) > 0$ if and only if $n \ge d$. Set $\epsilon = 2$ if G has even order, and 1 otherwise. Then $\epsilon\delta(G,n)|\mathrm{Aut}(G)|$ is an integer $A(G,n)$.*

These two conjectures include special cases investigated by others, the history of which is described in the next section. Subsequent sections give evidence for the conjectures in the cases when G has small order and when G belongs to certain families of groups.

2. History

There is a long history of realising various finite groups as Galois groups over $\mathbb{Q}$. For example, in 1937, Scholz and Reichardt independently (see Serre [16]) realised every group of odd prime power order, and in 1954, Shafarevich [18] realised every finite solvable group. There are, however, still many open cases. For example, if G is the Mathieu group on 23 letters, no G-extension of $\mathbb{Q}$ is currently known. It is widely believed that G-extensions of $\mathbb{Q}$ (and even $\mathbb{Q}(t)$) exist for any finite group G and this is termed the inverse Galois problem.

Recently the question of the minimal number of primes ramified in a G-extension of $\mathbb{Q}$ has been considered. In [15], Plans showed that Schinzel's Hypothesis H implies that Conjecture 1.2 above holds for all symmetric groups and dihedral groups. In [7], Jones and Roberts made both conjectures in the case that $d = n = 1$, providing plenty of evidence of both. In several of these cases they give a conjectural value for $\delta(G, 1)$ based on work of Bhargava [1]. We discuss this more in the last section of this paper.

In the case that G is a finite p-group of order p^m, Serre [16] noted that the Scholz-Reichardt method produces a G-extension ramified at no more than m primes. Several authors already made the conjecture that if d is the minimal number of generators for G^{ab} (and so, by Burnside's basis theorem, for G itself), then there exists a G-extension of $\mathbb{Q}$ ramified at no more than d finite primes. The purported proof by Cueto-Hernández and Villa-Salvador [4] is flawed, as noted by Plans. Nomura [14] checked the conjecture for all 3-groups of order less than or equal to 3^5. The most general result so far is the recent proof by Kisilevsky and Sonn [8] that Conjecture 1.2 is true for all p-groups in the class generated by cyclic p-groups and closed under direct products, wreath products, and rank-preserving quotients. This also equals the class of semiabelian p-groups. It does not contain any p-groups with derived length greater than their minimal number of generators.

As regards Conjecture 1.3, we should also note that Malle [12, 13] has made some far-reaching conjectures regarding the number of G-extensions of $\mathbb{Q}$ of discriminant of absolute value less than or equal to x. Bhargava has several results in this direction [2]. Also, a preprint [3] of the first author and Ellenberg gives related conjectures regarding which finite p-groups should arise as the Galois group of the maximal p-extension of $\mathbb{Q}$ unramified outside a finite set of primes not including p and how often they should arise. Connections between this and Conjecture 1.3, leading to proofs of several cases of Conjecture 1.3, are discussed in the last section of this paper.

3. Small groups

In this section we describe various methods for establishing Conjecture 1.2 for groups of small order. In particular these establish the following theorem.

Theorem 3.1. *Conjecture 1.2 holds for all groups of order less than or equal to* 32.

The rest of the section outlines a proof of Theorem 3.1. First, note that by Theorem 1.1 we need only consider nonabelian groups. The method of Kisilevsky and Sonn [8] takes care of the class of semiabelian p-groups, which by a result of Dentzer [5] includes all p-groups of order less than or equal to 32. We therefore focus on nonabelian groups which are not p-groups.

The first technique used is the bruteforce method of employing Klüners's database [9] of extensions of $\mathbb{Q}$ with root field of degree at most 15. The database allows one to request the number of ramified primes and the signature. In each such case the Galois group is a permutation group of degree at most 15. This method can therefore only work for finite groups that have a subgroup with trivial core and index less than or equal to 15. There exist groups with such a subgroup for which the database provides no suitable extension, presumably because such an extension lies beyond the tables. In any case, this method resolves Conjecture 1.2 affirmatively for all groups of order less than or equal to 32 except for the i-th group of order n `SmallGroup(n,i)` in the GAP SmallGroups Library, where $[n, i]$ is in the following list:

(1) $\{[12,1],[18,3],[20,3],[24,4],[24,7],[24,11],[24,13],[28,3],[30,2],[30,3]\}$.

The remaining groups are taken care of by a variety of methods, the first one being the following use of quadratic fields.

Lemma 3.2. *Let h be odd and $G = \mathbb{Z}/h \rtimes \mathbb{Z}/k$, such that the image of the action $\mathbb{Z}/k \to \mathrm{Aut}(\mathbb{Z}/h)$ is generated by the inversion automorphism. If there exists a quadratic field $K = \mathbb{Q}(\sqrt{p})$ whose ideal class group has a cyclic quotient of order h and $p \equiv 1 \pmod{2k}$ is a prime, then Conjecture 1.2 holds for G.*

Proof. Let K_k denote the totally real subfield of $\mathbb{Q}(\zeta_p)$ of degree k over $\mathbb{Q}$ and H denote the subfield of the Hilbert class field of K corresponding to the cyclic quotient of order h. This is Galois over $\mathbb{Q}$. The extensions K_k and H are disjoint over K, since K_k/K is totally ramified at the prime $\mathfrak{p}$ above p, while H/K is unramified. Hence $\mathrm{Gal}(HK_k/K) \cong \mathbb{Z}/(k/2) \times \mathbb{Z}/h$ while $\mathrm{Gal}(H/\mathbb{Q}) \cong D_h$. We conclude $\mathrm{Gal}(HK_k/\mathbb{Q}) \cong \mathbb{Z}/h \rtimes \mathbb{Z}/k$, with the action of the generator of $\mathbb{Z}/k$ given by inversion. □

The other useful method is to employ the so-called simplest fields [11]. These are one-parameter families of fields $K_i(m)$ of degree $i = 2, 3, 4, 5$, and 6 whose members are Galois over $\mathbb{Q}$, totally real, and have cyclic Galois group. The simplest cubics were introduced by Shanks in 1974 [17] and further families have since been introduced and studied because of their explicit form and often large class numbers.

Definition 3.3 (Simplest Fields).

(a) Suppose m is not a square. The *simplest quadratic field* $K_2(m)$ is the splitting field of polynomial $x^2 - m$ with discriminant $4m$.

(b) The *simplest cubic field* $K_3(m)$ is the splitting field of polynomial

$$x^3 - mx^2 - (m+3)x - 1$$

with discriminant $(m^2 + 3m + 9)^2$.

(c) Let $m \neq 0, \pm 3$. The *simplest quartic field* $K_4(m)$ is the splitting field of polynomial

$$x^4 - mx^3 - 6x^2 + mx + 1$$

with discriminant $4(m^2+16)^3$.

(d) The *simplest quintic field* $K_5(m)$ is the splitting field of polynomial

$$x^5 + m^2x^4 - (2m^3 + 6m^2 + 10m + 10)x^3 + a_2x^2 + a_1x + 1$$

with $a_2 = m^4+5m^3+11m^2+15m+5, a_1 = m^3+4m^2+10m+10$ and discriminant $(m^3+5m^2+10m+7)^2(m^4+5m^3+15m^2+25m+25)^4$.

(e) Let $m \neq -8, -3, 0, 5$. The *simplest sextic field* $K_6(m)$ is the splitting field of polynomial

$$x^6 - 2mx^5 - (5m+15)x^4 - 20x^3 + 5mx^2 + (2m+6)x + 1$$

with discriminant $46656(m^2+3m+9)^5$.

Similarly to the previous lemma, simplest fields provide a method of resolving Conjecture 1.2 for metacyclic groups with cyclic abelianisation of order $i \leq 6$. We simply search through values of m that ensure $K_i(m)$ has prime power discriminant, for a field $K_i(m)$ with the desired ideal class group.

We now systematically eliminate the groups remaining in list (1).

`SmallGroup(12,1)`: This has $G^{ab} \cong \mathbb{Z}/4$ and $G' \cong \mathbb{Z}/3$. Searching with MAGMA among primes that are $1 \pmod 8$ eventually yields $p = 257$ for which $\mathbb{Q}(\sqrt{p})$ has class number divisible by 3. By application of Lemma 3.2 we are done.

`SmallGroup(18,3)`: This has $G^{ab} \cong \mathbb{Z}/6$ and $G' \cong \mathbb{Z}/3$. We search with MAGMA through primes that are $1 \pmod{12}$ and find that for $p = 229$, $\mathbb{Q}(\sqrt{p})$ has class number divisible by 3, giving by Lemma 3.2 the desired G-extension.

`SmallGroup(20,3)`: This has $G^{ab} \cong \mathbb{Z}/4$ and $G' \cong \mathbb{Z}/5$. We search through the fields $K_4(m)$ for one with prime power discriminant and class number divisible by 5. The first such is for $m = 21$ and the corresponding prime p is 457.

`SmallGroup(24,4)`: This group G is the only group of order 24 with quotients isomorphic to S_3 and to the quaternion group Q_8 of order 8. We therefore look in [9] for a totally real S_3-extension ramified at exactly one prime p, together with a totally real Q_8-extension ramified at the same p and exactly one other prime. This method works for $p = 229$, the other prime being 5.

`SmallGroup(24,7)`: This group is isomorphic to

$$\texttt{SmallGroup(12,1)} \times \mathbb{Z}/2$$

and so this case is resolved by compositing our first example above with $\mathbb{Q}(\sqrt{p})$ for any prime $p \equiv 1 \pmod 4, p \neq 257$.

`SmallGroup(24,11)`: This group G is isomorphic to $Q_8 \times \mathbb{Z}/3$ with G^{ab} just 2-generated. Reference [9] yields a totally real Q_8-extension ramified only at 13 and 61 whose compositum with the cubic subfield of the 61st cyclotomic field is then a G-extension.

SmallGroup(24,13): This group is isomorphic to a semidirect product $(\mathbb{Z}/2 \times \mathbb{Z}/2) \rtimes \mathbb{Z}/6$. The field $K_6(17)$ has class group isomorphic to $(\mathbb{Z}/2)^4$ and discriminant 349^5. All the groups of order 96 with a normal subgroup isomorphic to $(\mathbb{Z}/2)^4$ with quotient $\mathbb{Z}/6$ have a quotient isomorphic to `SmallGroup(24,13)`.

SmallGroup(28,3): This group G is isomorphic to $D_7 \times \mathbb{Z}/2$. Reference [9] gives a totally real D_7-extension ramified only at 577, whose compositum with any $\mathbb{Q}(\sqrt{p})$ with prime $p \equiv 1 \pmod 4, p \neq 577$ then produces the desired G-extension.

SmallGroup(30,2): This has $G^{ab} \cong \mathbb{Z}/6$ and $G' \cong \mathbb{Z}/5$. We use MAGMA to search for a prime $p \equiv 1 \pmod{12}$ such that the class number of $\mathbb{Q}(\sqrt{p})$ is divisible by 5. Application of Lemma 3.2 with prime $p = 1093$ produces the desired G-extension.

SmallGroup(30,3): This is D_{15}. Looking for a quadratic field $\mathbb{Q}(\sqrt{p})$ with $p \equiv 1 \pmod 4$ and class number divisible by 15 works for $p = 11321$.

4. Families of groups

As indicated earlier, Conjecture 1.2 is known for various families without further hypothesis (*e.g.,* all abelian groups and semiabelian p-groups) and various others with further hypothesis (*e.g.,* all dihedral groups under Schinzel's Hypothesis H). Families where G^{ab} is cyclic were studied in great detail by Jones and Roberts [7]. They, however, did not impose requirements on the infinite prime. Searching for totally real extensions increases the difficulties and disallows some arithmetic geometric methods. For example, cuspidal eigenforms of level 1 yield Galois representations into $\mathrm{GL}(2,p)$, for which the only finite prime ramified is p. For large enough p their image contains $\mathrm{SL}(2,p)$ but they are surjective if and only if $\gcd(p-1, k-1) = 1$, where k is the weight of the eigenform. This yields, for many primes p, a $\mathrm{GL}(2,p)$-extension of $\mathbb{Q}$ ramified at exactly one finite prime p. Unfortunately they do not resolve Conjecture 1.2 for $\mathrm{GL}(2,p)$ since these extensions are totally imaginary. Not enough is known about even Galois representations to help, but Darrin Doud kindly supplied the authors with results from his investigations [6]. In particular, Conjecture 1.2 holds for $A_5 \times A_5$ since there exist disjoint totally real A_5-extensions ramified at only the prime 26591.

As regards Conjecture 1.3, Jones and Roberts [7] made this conjecture in the case G^{ab} cyclic, *i.e.*, $d = 1$ and $n = 1$. For example, following heuristics of Bhargava [1], they propose that $\delta(S_n, 1)$ equals the number of conjugacy classes in S_n which lie outside A_n, divided by $2|\operatorname{Aut}(S_n)|$. Note that their δ_G is obtained by summing over all possible complex conjugations, so will be our $\delta(G,1)$ multiplied by the number of elements of G of order 1 or 2.

For example, this gives $\delta(S_n, 1) = 1/2, 1/12, 1/24, 1/80, 1/576, 1/1440, 1/8064$ for $n = 2, 3, \ldots, 8$. Recall that $A(S_n, 1)$ is defined to be $2\delta(S_n,1)|\operatorname{Aut}(S_n)|$. In this case, it is the number of conjugacy classes of S_n that lie outside A_n.

In general, $A(G,n)$ is the number of n-tuples of conjugacy classes of G that generate G and that satisfy condition $(*)$. To describe $(*)$, suppose that

$$G^{ab} \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_d.$$

We need that d of the conjugacy classes are closed under taking q_i-th powers (with $1 \leq i \leq d$), where q_i is some prime that is $1 \pmod{n_i}$, which is explained as follows.

The n-tuples of primes containing a prime dividing the order of G are of vanishing density among all n-tuples of primes. The generic case is therefore that of a tamely ramified G-extension. Let $K/\mathbb{Q}$ be such an extension. Let q be one of the n primes that are tamely ramified in $K/\mathbb{Q}$. Then the corresponding inertia subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic, generated by say τ_q, which is defined up to conjugacy. Let c_q denote the conjugacy class of $\mathrm{Gal}(K/\mathbb{Q})$ containing τ_q. The element τ_q is conjugate to its q-th power by a lift of Frobenius – equivalently c_q is closed under taking q-th powers.

Since there are no nontrivial extensions of $\mathbb{Q}$ unramified at every finite prime, the subgroup generated by all the c_q must be the whole of $\mathrm{Gal}(K/\mathbb{Q})$. Thus, $\mathrm{Gal}(K/\mathbb{Q})$ is generated by n conjugacy classes, each closed under certain power maps. If $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to G, then G must also be generated by such conjugacy classes. All we are conjecturing is that the frequency with which G arises is proportional to the number of ways such conjugacy classes can be found in G. As noted in [3], this should be weighted by $1/|\operatorname{Aut}(G)|$.

Thus $A(G,n)$ is simply counting all the possibilities for $(c_{q_1},\dots,c_{q_n})$. Note that not every n-tuple of conjugacy classes whose images generate G^{ab} generate G, but there is the following consistency between Conjectures 1.2 and 1.3.

Lemma 4.1. *Let $d_1 \geq 1$ be the minimal number of generators of G^{ab}. Let d_2 be the minimal number of conjugacy classes of G that generate G. Then $d_1 = d_2$.*

Proof. If conjugacy classes generate G, then their images generate G^{ab} and so $d_1 \leq d_2$. As for the other direction, let $R(G)$ denote the intersection of all maximal normal subgroups of G. Then $G/R(G) \cong S_1 \times \cdots \times S_k$, where the S_i are finite simple groups. Suppose the last $k-r$ are abelian, so that

$$G/R(G) \cong S_1 \times \cdots \times S_r \times A,$$

where A is an abelian quotient of G and so generated by d_1 elements. Extending these d_1 elements to elements of $G/R(G)$ by picking nontrivial elements of the $S_1,\dots,S_r$ components, we see that $G/R(G)$ is generated by the conjugates of d_1 elements. Pick any lifts of these to G. If the conjugates of these d_1 elements do not generate G, then they lie in some maximal normal subgroup N. But then their images in $G/R(G)$ lie in $N/R(G)$ and so do not generate $G/R(G)$, a contradiction. Thus, $d_1 = d_2$. □

We can prove several cases of the positive density part of Conjecture 1.3 for nilpotent groups G. By this we mean that if the density exists, then it is positive. Alternatively, we obtain a positive lower bound for the density defined as a lim inf rather than a limit.

Theorem 4.2. *Let G be a d-generated nilpotent group of odd order, such that the commutator subgroup $[G,G]$ is contained in the center of G. Then $\delta(G,d)$ is positive.*

Proof. Let e denote the exponent of G. Suppose $G^{ab} \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_d$. Consider any d-tuple S of primes $\{p_1,\dots p_d\}$ satisfying

(a) $p_i \equiv 1 \pmod{e}, \quad 1 \leq i \leq d,$

(b) $p_i \pmod{p_j} \in (\mathbb{Z}/{p_j}^{\times})^{n_j}, \quad 1 \leq i \neq j \leq d.$

There exists a unique G^{ab}-extension K of $\mathbb{Q}$ unramified outside S.

First consider the case when G is a p-group. Note that the conditions on the primes in S guarantee that K satisfies the Scholz condition S_N [16], where $p^N = e$. Having obtained a G^{ab}-extension K, we proceed to obtain a G-extension L of $\mathbb{Q}$ containing K by solving a series of central embedding problems each having a kernel of prime order using the method of Scholz-Reichardt as in [16]. By Corollary 2.1.8 [16], there exists a G-extension unramified outside S.

Now consider the case when G is nilpotent. For each Sylow-p subgroup G_p of G, the maximal p-subfield K_p of K is a G_p^{ab}-extension. We obtain a G_p-extension L_p containing K_p unramified outside S as in the p-group case. The compositum $\prod_{p||G|} L_p$ gives the desired G-extension ramified only at $\{p_1, \ldots, p_d\}$.

In each case, the density of the set of d-tuples of primes satisfying the two conditions above gives us the lower bound $\phi(e)^{-d}(n_1 \cdots n_d)^{1-d} \leq \delta(G, d)$, where ϕ is Euler's phi function. □

The result above also follows from the work of Plans [15]. Note that the conditions given in the proof of Theorem 4.2 are sufficient but not necessary. For example, Koch [10, p. 121] showed that if $\{p, q\}$ are primes satisfying

(a) $p, q \equiv 1 \pmod{l}$,

(b) $p, q \not\equiv 1 \pmod{l^2}$,

(c) $x^l - p$ has no solutions $\pmod{q}$,

then the Galois group of the maximal l-extension unramified outside $\{p, q\}$ is the nonabelian group of order l^3 and exponent l^2. The set of primes $\{p, q\}$ satisfying the three conditions above is of positive density and is disjoint from the set of primes satisfying the conditions of Theorem 4.2. Taking the union of the two sets we obtain a tighter lower bound on $\delta(G, 2)$ for nonabelian groups G of order l^3 and exponent l^2.

Lemma 4.3. *The positive density part of Conjecture* 1.3 *holds for all the nilpotent groups of order less than or equal to* 32.

The method of Kisilevsky and Sonn [8] chooses ramifying primes from a set of primes which split completely in given finite extensions. This implies a positive lower bound, call it $\lambda(G)$, for $\delta(G, d)$ when G is a p-group of order less than or equal to 32. There are only two nonabelian nilpotent non-p groups of order less than or equal to 32, namely `SmallGroup(24,10)`, `SmallGroup(24,11)`, and each has a positive density $\delta(G, d) \geq \lambda(G)/3$. This follows by using the method in [8] to realise the Sylow-2 subgroup of G with two ramifying primes. The factor $1/3$ comes from choosing one of the primes to be additionally $1 \pmod 3$, which gives the Sylow-3 subgroup.

Whereas the above is proven by solving embedding problems, an alternative approach is to work from above instead of below, *i.e.,* by realising larger groups mapping onto our desired groups. This is related to work in a recent preprint of the first author and Ellenberg [3].

Suppose that G is a finite p-group with the same number d of generators as relators. Suppose $G^{ab} \cong \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_d$. If p is odd, let $A(G)$ be the number of d-tuples of conjugacy classes $(c_1, \ldots, c_d)$ that generate G and where c_i is closed under taking $(1+n_i)$-th powers. (There is a more complicated version for $p = 2$ that takes account of the greater diversity of subgroups of $\mathbb{Z}_2^*$.) The preprint contains the conjecture that among all finite p-groups which have the same abelianisation as G, the probability (measured as a natural density) that a d-tuple S of primes, all $1 \pmod p$, will satisfy that the Galois group of the maximal p-extension of $\mathbb{Q}$ unramified outside S is isomorphic to G, is $A(G)/|\operatorname{Aut}(G)|$.

Thus, for all the p-groups G in [3] for which this conjecture is proven and for which $A(G) \neq 0$, we have proven the positive density part of Conjecture 1.3. Moreover, if G is a quotient of such a p-group, then we also deduce the positive density part of Conjecture 1.3. In general, that density will be

$$\sum_H \frac{a_H A(H)}{|H^{ab}||\operatorname{Aut}(H)|}$$

summed over all finite p-groups H with generator rank and relation rank both equal to d (the generator rank of G), where a_H denotes the number of normal subgroups N of H such that H/N is isomorphic to G. The above results suggest that the infinite sum is always rational.

Acknowledgements. Research supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006 and Stokes Professorship award, Science Foundation Ireland Grant 07/SK/I1252b. We thank Darrin Doud, Steve Ullom, and the anonymous referee for their helpful input.

REFERENCES

[1] M. Bhargava, *Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants*, Int. Math. Res. Not. **17** (2007), Art. ID rnm052, 20 pp.

[2] M. Bhargava and M. Wood, *The density of discriminants of S_3-sextic number fields*, Proc. Amer. Math. Soc. **136** (2008), no. 5, 1581–1587.

[3] N. Boston and J. Ellenberg, *Random pro-p groups, braid groups, and random tame Galois groups*, preprint.

[4] A. Cueto-Hernández and G.D. Villa-Salvador, *Nilpotent extensions of number fields with bounded ramification*, Pacific J. Math. **196** (2000), no. 2, 297–316.

[5] R. Dentzer, *On geometric embedding problems and semiabelian groups*, Manuscripta Math. **86** (1995), no. 2, 199–216.

[6] D. Doud and M.W. Moore, *Even icosahedral Galois representations of prime conductor*, J. Number Theory **118** (2006), no. 1, 62–70.

[7] J.W. Jones and D.P. Roberts, *Number fields ramified at one prime*, Algorithmic number theory, 226–239, Lecture Notes in Comput. Sci., 5011, Springer, Berlin, 2008.

[8] H. Kisilevsky and J. Sonn, *On the minimal ramification problem for l-groups*, arXiv: 0811.2978v1 [math.NT], 2008.

[9] J. Klüners and G. Malle, *A database for field extensions of the rationals*, LMS J. Comput. Math. **4** (2001), 182–196.

[10] H. Koch, *Galois theory of p-extensions*, Springer-Verlag, Berlin, 2002, xiv+190 pp.

[11] S. Louboutin, *Efficient computation of root numbers and class numbers of parametrized families of real abelian number fields*, Math. Comp. **76** (2007), no. 257, 455–473.

[12] G. Malle, *On the distribution of Galois groups*, J. Number Theory **92** (2002), no. 2, 315–329.

[13] G. Malle, *On the distribution of Galois groups II*, Experiment. Math. **13** (2004), no. 2, 129–135.

[14] A. Nomura, *Notes on the minimal number of ramified primes in some l-extensions of $\mathbb{Q}$*, Arch. Math. (Basel) **90** (2008), no. 6, 501–510.

[15] B. Plans, *On the minimal number of ramified primes in some solvable extensions of $\mathbb{Q}$*, Pacific J. Math. **215** (2004), no. 2, 381–391.

[16] J.-P. Serre, *Topics in Galois theory*, A.K. Peters, Wellesley, 2008, xvi+120 pp.

[17] D. Shanks, *The simplest cubic fields*, Math. Comp. **28** (1974), 1137–1152.

[18] I.R. Shafarevich, *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk SSSR **18** (1954), no. 6, 525–578. Amer. Math. Soc. Transl. Ser. **4** (1956), no. 2, 185–237.

N. BOSTON, DEPT. OF MATH., U. OF WISCONSIN, MADISON, USA
boston@math.wisc.edu

N. MARKIN, SCHOOL OF MATH. SCIENCES, U. COLLEGE DUBLIN, IRELAND
nadyaomarkin@gmail.com