Filter

EXPLICIT GALOIS GROUPS OF INFINITE p-EXTENSIONS UNRAMIFIED AT p

Nigel Boston

Abstract. Galois groups of infinite p-extensions of number fields unramified at p are a complete mystery. We find by computer a family of pro-p groups that satisfy everything that such a Galois group must, and give evidence for the conjecture that these are the only such groups. This suggests that these mysterious Galois groups indeed have a specific form of presentation. There are surprising connections with knot theory and quantum field theory. Finally, the Fontaine-Mazur conjecture here reduces to a purely group-theoretic conjecture, and evidence for this conjecture and an extension of it is given.

0. Introduction.

Whereas much is now known about Galois groups of p-extensions of number fields when the extension is ramified at the primes above p and these extensions have been successfully related to the theory of p-adic Galois representations, not one Galois group of an infinite p-extension unramified at the primes above p has been written down. Wingberg [14] calls them amongst the most mysterious objects in algebraic number theory. In this paper we gather together the properties that such a Galois group must satisfy and observe that there is just one family of such groups.

These groups are then studied as abstract groups and some links with other areas of mathematics surprisingly arise. The conjecture of Fontaine-Mazur [8] then simply says that no subgroup of finite index has an infinite, analytic quotient. This appears to be true of all groups in the family. Moreover, all these groups are conjecturally just-infinite, and it is shown that in that case they are branch, confirming the author's proposed extension [5] of the Fontaine-Mazur conjecture. This is apparently a new collection of just-infinite branch groups, not among those introduced in section 8 of [11], unusually having such a simple, finite presentation.

1. Galois Pro-p Groups Unramified at p.

We shall focus on the simplest, most concrete situation available to us. Namely, let S be a finite set of odd primes, $\mathbf{Q}_S$ denote the maximal 2-extension of $\mathbf{Q}$ unramified outside S (allowing ramification at ∞), and $G_S = \mathrm{Gal}(\mathbf{Q}_S/\mathbf{Q})$. Then G_S is a pro-2 group with the following properties:

(a) (Shafarevich) $d(G_S) = r(G_S) = |S|$, and in fact the generators can be taken as the tame inertia generators $\{\tau_p : p \in S\}$ and the relations of the form $\tau_p^{r_p} = \tau^p (p \in S)$, where the r_p are as yet unknown [9];

(b) (Class Field Theory) every finite-index subgroup H of G_S has $|H/H'| < \infty$;

1991 *Mathematics Subject Classification.* 11R32, 11Y40, 12F10, 20D15.

Key words and phrases. Explicit Galois group, class tower, just-infinite.

The author thanks Y. Barnea, L. Bartholdi, M. Bush, F. Hajir, J. Klüners, T. Kuhnt, and B. Mazur for useful discussions. He was supported by NSF DMS 99-70184

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

(c) conjecturally (Fontaine-Mazur [8]), every finite-index subgroup H of G_S has no infinite analytic quotient.

Remarks. $d(H)$ and $r(H)$ denote the generator and relation ranks of H respectively. By (a), G_S is finite if $|S| = 1$ and is infinite (thanks to Golod-Shafarevich [10]) if $|S| \geq 4$. It can go either way if $|S| = 2$ or 3 (see [6],[12]). Property (b) follows from the finiteness of certain ray class groups.

In property (c), "analytic" means a closed subgroup of $GL_n(\mathbf{Z}_2)$ for some n. Extensions [3], [5] of (c) conjecture that H has no infinite quotient embeddable in $GL_n(R)$, where R is any complete, Noetherian local ring with finite residue field, and that the just-infinite quotients of H are all branch groups [11]. Just-infinite groups are ones all of whose proper quotients are finite.

Our objective now is to find all abstract presentations of infinite pro-2 groups that satisfy properties (a) and (b) above, and test whether (c) and its extensions hold for such groups.

2. A Computer Experiment.

If $S = \{p, q\}$, then G_S is a sometimes infinite pro-2 group with presentation of the form $< x, y | x^r = x^p, y^s = y^q >$, where r and s are certain (unknown) elements of the free pro-2 group on x and y. Here, x^r stands for $r^{-1}xr$. Since in [6] every case with $p \equiv 3 (\text{mod } 4), q \equiv 5 (\text{mod } 8)$, i.e. G_S having abelianization $C_2 \times C_4$, denoted $[2, 4]$ for short, leads to a finite G_S, we focus on the next simplest case, namely $p, q \equiv 5 (\text{mod } 8)$, i.e. $G_S/G'_S \cong [4,4]$. In the group $(\mathbf{Z}/2^n)^*$, any n, the subgroup generated by 5 is the same as that generated by any integer that is 5(mod 8), and so G_S actually has presentation $< x, y | x^a = x^5, y^b = y^5 >$ for certain a, b in the free pro-2 group on x and y.

Given a finitely presented group G, let $P_n(G) = [P_{n-1}(G), G]P_{n-1}(G)^2$, where $P_0(G) = G$. We say that G has 2-class c if $P_c(G) = \{1\}$ but $P_{c-1}(G) \neq \{1\}$. Let Q_n denote the maximal 2-class n 2-group quotient of G.

The computer algebra system MAGMA [2] allows us to start with an abstract group presentation $G =< x, y | x^a = x^5, y^b = y^5 >$, where a, b are randomly chosen words of the free group in x, y, and to check and see if

(i) $|Q_n| \neq |Q_{n+1}|$ for fairly large n (up to 63, if desired);

(ii) $|H/H'| < \infty$ for all subgroups H of index ≤ 16 with core of 2-power index (these subgroups arise in the pro-2 completion of G).

The reason for conducting such an experiment is that by the properties of section 1, if $S = \{p, q\}$, then G_S is a sometimes infinite pro-2 group that, if it is the pro-2 completion of G, satisfies these conditions (and more).

This was tried for $15,000$ choices of a, b, producing 92 presentations. The outcome of the experiment is that we obtained just one class $\mathcal{C}$ of very similar groups. If we let $|Q_n| = 2^{f(n)}$, then the sequence $(f(n))$ was always:

$(\Sigma) : 2, 5, 8, 11, 14, 16, 20, 24, 30, 36, 44, 52, 64, 76, 93, 110, 135, 160, 196, 232, 286,$
$340, 419, 498, 617, 736, 913, 1090, 1357, 1634, ...$

What is Σ? Consider the derived sequence $\Delta f(n) := f(n+1) - f(n) = \log_2 |P_n(G)/P_{n+1}(G)|$. This is:

$3, 3, 3, 3, 2, 4, 4, 6, 6, 8, 8, 12, 12, 17, 17, 25, 25, 36, 36, 54, 54, 79, 79, 119, 119, 177, 177, 267, 267, ...$

Plugging this sequence (ignoring repetitions) into Neal Sloane's On-Line Encyclopedia of Integer Sequences http://www.research.att.com/$\sim$ njas/sequences/Seis.html yields A001461, arising in the paper [7] concerning knot theory and quantum field theory. If so, $\Delta f(2n-2) = \Delta f(2n-1) = \sum_{m=1}^{n}(1/m)\sum_{d|m}\mu(m/d)(F_{d-1}+F_{d+1})$. Each term in the inner sum counts aperiodic binary necklaces with no subsequence 00, excluding the necklace "0". Here μ is the usual Möbius function and F_n the nth Fibonacci number.

Note that, for the free pro-2 group F on k generators, Witt's formula [15] gives that $\log_2|P_n(F)/P_{n+1}(F)| = \sum_{m=1}^{n}(1/m)\sum_{d|m}\mu(m/d)k^d$ and so since $F_{d-1}+F_{d+1}$ is approximately ϕ^d for large d, where ϕ is the golden ratio $(1+\sqrt{5})/2$, this suggests that G is something like a free pro-2 group on ϕ generators.

Moreover, in each case, a change of variable made the presentation $G =< x, y|x^a = x^5, y^4 = 1 >$ for some word a in x and y. This extensive evidence leads to the conjecture:

Conjecture 1. Let G be an infinite pro-2 group with presentation of the form $< x, y|x^a = x^5, y^b = y^5 >$ such that every subgroup of finite index has finite abelianization. Then G is isomorphic to $< x, y|x^a = x^5, y^4 = 1 >$ for $a \in \mathcal{F}$, a certain subset of the free pro-2 group on x, y, and $\log_2|G/P_c(G)|$ $(c = 1, 2, ...)$ is the sequence Σ. Here $\mathcal{F}$ consists of ...

The shortest elements in $\mathcal{F}$ have length 6 and there are 48 of them, for instance $y^2xyxy, y^2xyx^{-1}y^{-1}, ...$ There are 256 elements in $\mathcal{F}$ of length 7, 960 of length 8, 2880 of length 9, 8960 of length 10, and so on.

Group-Theoretic Consequences of Conjecture 1. If G is as in conjecture 1, then its three subgroups of index 2 have abelianization $[2, 4, 4]$. For the 13104 elements of $\mathcal{F}$ just listed, the abelianizations of its index 4 subgroups are always the same except that one subgroup H, normal with cyclic quotient, has $H/H' \cong [2, 4, 4, 8]$ for some groups G, $[4, 4, 4, 4]$ for others, and $[2, 2, 8, 16]$ for yet others. These subgroups, which we shall denote *critical*, always have 4 generators and 4 relations. The collection of abelianizations of the index 8 subgroups come in 8 flavors, of which 5 correspond to there being a critical subgroup with abelianization $[4, 4, 4, 4]$.

3. Number-Theoretical Evidence and Consequences.

All the groups G in our class $\mathcal{C}$ satisfy $G/G' \cong [4, 4]$. If this is isomorphic to some G_S with $S = \{p, q\}$, then both p and q are $5 (\bmod 8)$. Suppose this is the case. We find the following possibilities for H/H' for the three subgroups of G_S of index 2 (from computing ray class groups):

(i) If p is not a square mod q, then $[2, 8]$ twice and $[4, 4]$.

Suppose p is a square mod q (so by quadratic reciprocity q is a square mod p).

(ii) If p is not a 4th power mod q and q not a 4th power mod p, then $[2, 4, 4]$

twice and $[2,2,8]$.

(iii) If p is a 4th power mod q but q not a 4th power mod p, then $[2,4,4]$ three times.

(iv) If p is a 4th power mod q and q is a 4th power mod p, then $[2,4,4]$ twice and $[2,2,2^n]$ for some $n \geq 4$.

Case (i) forces (by my method with Leedham-Green [5]) G_S to be finite. I believe that cases (ii) and (iv) will lead to the same conclusion (but the computations are prohibitive - there is combinatorial explosion with thousands of candidate groups produced). Since the groups in $\mathcal{C}$ all have abelianizations of index 2 subgroups of type (iii), we focus on that case. The examples of such S with $p,q \leq 61$ are $\{13,29\},\{29,53\},\{37,53\},\{5,61\}$.

Corollary to Conjecture 1. If $p,q \equiv 5(\text{mod } 8)$, then G_S is infinite and $\cong < x,y|x^a = x^5, y^4 >$ for $a \in \mathcal{F}$ if p is a 4th power modulo q but not vice versa, and G_S is finite otherwise.

Proof. By a modified Golod-Shafarevich inequality, due to Thomas Kuhnt (to appear), applied to the quartic subfield of the cyclotomic field $\mathbf{Q}(\zeta_q)$, it follows that G_S is infinite.

In the other cases, if G_S were infinite, then its abelianizations of index 2 subgroups would have to be all $[2,4,4]$, but as noted above the corresponding ray class groups are not this.

Note that the quartic subfield used is the fixed field of the critical subgroup. Next, we look at subgroups of index 4 of G_S of type (iii). We find that their abelianizations match those of G in $\mathcal{C}$ exactly, which is strong evidence for conjecture 1, since one set of abelianizations is computed by number theory, the other by group theory, by completely different algorithms. Since the quartic subfield of $\mathbf{Q}(\zeta_q)$ always has 2-part of its pq-ray class group isomorphic to $[4,4,4,4]$, we thereby exclude some groups in $\mathcal{C}$.

Looking further at ray class groups of degree 8 fields, we find exact matching of abelianizations again, yielding further strong evidence for conjecture 1. The Galois group G_S with $S = \{13,29\}$ has such subgroups with abelianization $[2,4,4,16]$, corresponding to the root field of $x^8 + 1044x^6 + 273702x^4 - 98397x^2 + 142129$, which matches one of the five flavors. Again, this excludes some groups in $\mathcal{C}$. Ray class computations suggest that it is unlikely that all Galois groups in (iii) have this same behavior.

4. Fontaine-Mazur by Group Theory.

Proof of the Fontaine-Mazur conjecture and related conjectures now amounts to proving purely group-theoretical properties of groups in $\mathcal{C}$. Let G be such a group and $\rho : G \to GL_n(\mathbf{Z}_2)$ a continuous representation. Since $\rho(x)$ is conjugate to $\rho(x)^5$, its eigenvalues are a permutation of their 5th powers. In the semisimple case, where all these eigenvalues are distinct, this implies that $\rho(x)$ has finite order and now Fontaine-Mazur follows from the conjecture that if $a \in \mathcal{F}$, then $< x,y|x^a =$

$x^5, y^4, x^k >$ is finite for every 2-power k.

A lot more, however, appears to be true. Namely, $200,000$ times I added a random relation s of length ≤ 16 to the relations of various G in $\mathcal{C}$ and each time either got back G or a finite group. This suggests:

Conjecture 2. Each group in $\mathcal{C}$ is just-infinite.

The classification of just-infinite pro-p groups is a major topic, and as noted in [11], they come in two flavors, namely those which are branch and those which have a normal open subgroup which is a direct product of hereditarily just-infinite groups.

Corollary to Conjecture 2. Each group in $\mathcal{C}$ is a branch just-infinite group.

Proof This follows from the last comment, together with the observation that these groups have a subgroup H of index 4 with 4 generators and 4 relations. Since H thereby fails the Golod-Shafarevich test, it is not just-infinite, and so G is not hereditarily just-infinite. A modification of this argument shows that G can have no open subgroup that is a direct product of herditarily just-infinite groups.

In particular, this confirms my extension of the Fontaine-Mazur conjecture [2],[4]. It should be possible to construct G in $\mathcal{C}$ explicitly as a branch group, but note that G cannot be one of the special groups G_ω constructed in section 8 of [11], since those groups are generated by torsion elements (rooted and directed automorphisms), whereas (see below) our groups are not. This is therefore a new construction, surprising because the nicest branch groups have so far not been finitely presented [1]. The techniques of [11] then show that G is just-infinite.

Note that in the introduction to [11] Grigorchuk suggests that his construction might produce all branch groups. The above suggests not (and in fact since [11], articles have found new more general constructions - see e.g. [13]). In particular, Grigorchuk's special branch groups are all torsion-generated, whereas as noted below ours are not, although the (closed) subgroup generated by torsion is of finite index.

Let T_4 be the rooted tree with 4 vertices above each vertex, so having 4^n vertices at level n. Let W_n be the iterated wreath product given by $W_1 = C_4, W_n = W_{n-1} \wr C_4$. Then W_n acts on the subtree of T_4 consisting of vertices up to and including level n and their inverse limit W acts on T_4, i.e. $W \leq \mathrm{Aut}(T_4)$. $W_2 = C_4 \wr C_4 \cong G/H'$, where G is a typical group in $\mathcal{C}$ and H its critical subgroup. W_3 is of order 2^{42} and I have found subgroups K of it generated by elements x, y such that x is conjugate to x^5 and y has order 4 and such that the abelianizations of their index 2 subgroups are all $[2, 4, 4]$. The abelianizations of their index 4 subgroups do not always match the data for groups in $\mathcal{C}$. In particular, many of them have non-normal subgroups of index 4 with abelianization $[2, 8, 8]$, too large for K to be a quotient of a group in $\mathcal{C}$. If, however, we take certain x of order 64 such that $K =< x, y >$ has order 2^{18}, then the abelianizations of index 4 subgroups are small enough.

For certain groups in $\mathcal{C}$, the critical subgroup of index 4 can be nicely described. For instance, suppose $a = y^2xyxy$. Then $H =< x, u, v, w | x^{vu} = x^5, u^{wv} = u^5, v^{xw} = v^5, w^{ux} = w^5 >$ and it embeds in G by having $u = x^y, v = x^{y^2}, w = x^{y^3}$. Note that then $vu = a$ and the relations are obtained by conjugating the first relation by the powers of y. G is the semidirect product of H by $< y >$. On the number-theoretic side, H is generated by the inertia groups at p, four conjugate ones since p splits completely in the critical quartic field.

Apparently, the sequence $\log_2 |P_n(H)/P_{n+1}(H)| = 2\sum_{m=1}^{n}(1/m)\sum_{d|m}\mu(m/d)2^d$, so by Witt's formula [15] grows like that of $F \times F$, where F is the free pro-2 group on 2 generators.

As for Fontaine-Mazur holding for open subgroups of G, rather than just G itself, the following might be true:

Question 3. If H is an open subgroup of a group in $\mathcal{C}$, then is the closed subgroup $T(H)$ generated by all its torsion elements also open?

This has been checked for various groups in $\mathcal{C}$ and their subgroups. For instance, $T(G)$ is always of index 4 in G. Since $T(G) \neq G$, we obtain that G is not itself torsion-generated. A positive answer to question 3 implies that G is torsion-riddled, as proposed in [4], but is stronger. Note, however, that it is still unknown as to whether the critical subgroups have torsion, an important case for question 3 and the conjecture of [4]. We have:

Corollary to Positive Answer to Question 3. If G is in $\mathcal{C}$, then no open subgroup of G has a 2-adic representation with infinite image, i.e. the Fontaine-Mazur conjecture.

Proof The point is that if H is an open subgroup with such a representation, then it has an open subgroup with an infinite torsion-free quotient, which is forbidden by an affirmative answer to question 3.

5. Speculation.

Let G_S be of type (iii), with $S = \{p, q\}$. Let $T = \{2, p, q\}$. Consider G_T acting on π_1, the algebraic fundamental pro-2 group of P^1 minus three points $0, p, q$ in the usual way. π_1 is isomorphic to the free pro-2 group F on 2 generators. The normal subgroup N generated by inertia at 2 acts wildly on the $\mathbf{F}_p$-Lie algebra $L(F) = \sum P_n(F)/P_{n+1}(F)$, but the suggestion is that the subgroup H fixed by N is large enough to provide the indicated action of G_S on a necklace algebra, namely that provided by conjecture 1.

More generally, note that the groups G_S are interrelated - if $T = S \cup \{p\}$, then there is a natural surjection $G_T \to G_S$. The kernel of this map can be studied. For instance, for our situation, with $S = \{q\}, T = \{p, q\}$, the kernel is the critical subgroup. Note that since this is not just-infinite, there are many quotients of G_T mapping onto G_S.

BIBLIOGRAPHY

[1] L.Bartholdi, Endomorphic presentations of branch groups, J. Algebra (to appear).

[2] W.Bosma and J.Cannon, Handbook of MAGMA Functions, Sydney: School of Mathematics and Statistics, University of Sydney (1993).

[3] N.Boston, Some Cases of the Fontaine-Mazur Conjecture II, J. Number Theory **75** (1999), 161–169.

[4] N.Boston, The unramified Fontaine-Mazur conjecture, Proceedings of the ESF Conference on Number Theory and Arithmetical Geometry, Spain, 1997.

[5] N.Boston, Tree Representations of Galois groups (preprint - see http://www.math.uiuc.edu/Algebraic-Number-Theory/0259/index.html).

[6] N.Boston and C.R.Leedham-Green, Explicit computation of Galois p-groups unramified at p, J. Algebra **256** (2002), 402–413.

[7] D.J.Broadhurst, On the enumeration of irreducible k-fold Euler sums and their roles in knot theory and field theory, J. Math. Phys. (to appear).

[8] J.-M.Fontaine and B.Mazur, Geometric Galois representations, *in* "Elliptic curves and modular forms, Proceedings of a conference held in Hong Kong, December 18-21, 1993," International Press, Cambridge, MA and Hong Kong.

[9] A.Fröhlich, Central Extensions, Galois groups, and ideal class groups of number fields, *in* "Contemporary Mathematics," Vol. **24**, AMS, 1983.

[10] E.S.Golod and I.R.Shafarevich, On class field towers (Russian), Izv. Akad. Nauk. SSSR **28** (1964), 261–272. English translation in AMS Trans. (2) **48**, 91–102.

[11] R.Grigorchuk, Just infinite branch groups, *in* "New Horizons in pro-p Groups," (eds. du Sautoy, Segal, Shalev), Birkhauser, Boston 2000.

[12] F.Hajir and C.Maire, Unramified subextensions of ray class field towers, J. Algebra **249** (2002), 528–543.

[13] S.Sidki,

[14] K.Wingberg, On the maximal unramified p-extension of an algebraic number field, J. Reine Angew. Math. **440** (1993), 129–156.

[15] E.Witt, Treue Darstellung Liescher Ringe, J. Reine Angew. Math. **177** (1937, 152–160.

Department of Mathematics, University of Wisconsin, Madison, WI 53706
E-mail address: boston@math.wisc.edu