MAXIMAL UNRAMIFIED 3-EXTENSIONS OF IMAGINARY QUADRATIC FIELDS AND $SL_2(\mathbb{Z}_3)$

MICHAEL R. BUSH
(JOINT WORK WITH LAURENT BARTHOLDI)

Let k be a number field and let p be a prime. The *p-class tower of k* is the chain of fields

$$k = k_0 \subseteq k_1 \subseteq \ldots \subseteq k_n \subseteq \ldots$$

where k_{n+1} is the maximal unramified abelian p-extension of k_n for each $n \geq 0$. If we let $k^{ur,p} = \cup_{n\geq 0} k_n$ and $G = \mathrm{Gal}(k^{ur,p}/k)$ then G is a pro-p group whose structure incorporates a lot of arithmetic information about the field k and its unramified p-extensions. For instance, if H is an open subgroup of G and L is the associated fixed field then by class field theory $H/[H,H] \cong Cl_p(L)$ where $[H,H]$ is the commutator subgroup of H and $Cl_p(L)$ is the p-Sylow subgroup of the class group of L. One consequence of this is that the length of the p-class tower is the same as the length of the derived series of G.

In general determining the structure of G is difficult. We know that G can be infinite for certain choices of k and p due to work of Golod and Shafarevich [7]. We also know many examples where G is finite. One observes, however, that the finite examples usually have very small derived length ≤ 3 and so one is lead to ask whether or not there is a bound on the derived length when G is finite, and if not, how one can find examples where the length is large?

If k is an imaginary quadratic field and p is an odd prime then a result of Koch and Venkov [8] shows that G can be finite only if $d(G) \leq 2$ where $d(G)$ is the smallest number of generators for G as a pro-p group. Their proof exploits the fact that G has the structure of a Schur σ-group. By definition this is a finitely presented pro-p group G in which $d(G) = r(G)$ where $r(G)$ is the relation rank, $G/[G,G]$ is finite and there exists an automorphism $\sigma : G \to G$ such that $\sigma^2 = 1$ and the automorphism induced by σ on $G/[G,G]$ is the inversion map $x \mapsto x^{-1}$.

An obvious question that one might now ask is whether or not there exist finite Schur σ-groups with arbitrarily large derived length for some fixed prime p? The answer is yes and we give a family of examples below demonstrating this.

Let F be the free pro-3 group on two generators x and y. Let G_n be defined by the pro-3 presentation

$$G_n = \langle x, y \mid r_n^{-1}\sigma(r_n),\, t^{-1}\sigma(t)\rangle$$

where $r_n = x^3 y^{-3^n}$, $t = yxyx^{-1}y$ and $\sigma : F \to F$ is the automorphism defined by $x \mapsto x^{-1}$ and $y \mapsto y^{-1}$. The group G_n is a Schur σ-group with respect to the automorphism induced by σ.

Theorem 1. *For $n \geq 1$ the following hold:*
(i) *G_n is a finite 3-group of order 3^{3n+2};*
(ii) *G_n is nilpotent of class $2n+1$;*
(iii) *G_n has derived length $\lfloor \log_2(3n+3) \rfloor$.*

Each group G_n is a central extension of a finite quotient of the pro-3 group $H = \langle x, y \mid x^3, t^{-1}\sigma(t) \rangle$. The key step in the proof of Theorem 1 is the following lemma which exhibits an explicit matrix representation for H.

Lemma 1. *Let $\alpha \in \mathbb{Z}_3$ satisfy $\alpha^2 = -2$. The map $\rho : H \to \mathrm{SL}_2(\mathbb{Z}_3)$, given by*

$$x \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \qquad y \mapsto \alpha \begin{pmatrix} 0 & 1/2 \\ 1 & -1 \end{pmatrix},$$

is an isomorphism between H and a pro-3 Sylow subgroup of $\mathrm{SL}_2(\mathbb{Z}_3)$.

See [1] for a proof of the lemma and theorem as well as several examples of imaginary quadratic fields $k = \mathbb{Q}(\sqrt{d})$ in which the Galois group of the 3-class tower is G_1. The first three discriminants for which this occurs are $d = -4027$, -8751 and -19651. These and other examples were found by applying a computational method first used by Boston and Leedham-Green [3] to compute the Galois groups of certain maximal tamely ramified extensions of $\mathbb{Q}$. The method makes use of the p-group generation algorithm [9] to systematically enumerate all d-generated finite p-groups. Information about the Galois group one is seeking is used to eliminate some of these groups. In some cases the process terminates leaving a finite number of groups as candidates for the desired Galois group. The computations for the examples above were carried out using Magma [2]. (We note that the 3-class tower of the first field $d = -4027$ has previously been investigated in [10] using other methods). For other applications of the method (including the first examples of 2-class towers of length 3) see [5], [4] and [6].

For $n \geq 2$ there is a limited amount of numerical evidence suggesting that the groups G_n may arise as Galois groups of 3-class towers. Whether or not this is actually the case is still open.

References

[1] L. Bartholdi, M. R. Bush, *Maximal unramified 3-extensions of imaginary quadratic fields and* $\mathrm{SL}_2(\mathbb{Z}_3)$, preprint, arXiv: math.NT/0602364.
[2] W. Bosma, J. J. Cannon, *Handbook of Magma functions*, School of Mathematics and Statistics, University of Sydney (1996).
[3] N. Boston, C. R. Leedham-Green, *Explicit computation of Galois p-groups unramified at p*, J. Algebra **256** (2002), 402–413.

[4] N. Boston, H. Nover, *Computing pro-p Galois groups*, preprint, 2006.

[5] M. R. Bush, *Computation of the Galois groups associated to the 2-class towers of some quadratic fields*, J. Number Theory **100** (2003), 313–325.

[6] B. Eick, H. Koch, *On the maximal 2-extensions of $\mathbb{Q}$ with given ramification*, to appear in Proc. St. Petersburg Math. Soc. (Russian); English transl.: to appear in Amer. Math. Soc. Trans..

[7] E. Golod, I. Shafarevich, *On class field towers*, Izv. Akad. Nauk SSSR **28** (1964), 261–272 (Russian); English transl.: Amer. Math. Soc. Trans. **48** (1965), 91–102.

[8] H. Koch, B. B. Venkov, *Über den p-Klassenkörperturm eines imaginär-quadratischen Zahlkörpers*, Astérisque **24-25** (1975), 57–67.

[9] E. A. O'Brien, *The p-group generation algorithm*, J. Symbolic Computation **9** (1990), no. 5–6, 677–698.

[10] A. Scholz, O. Taussky, *Die Hauptideale der kubischen Klassenkörper imaginär-quadratischer Zahlkörper: ihre rechnerische Bestimmung und ihr Einfluß auf den Klassenkörperturm*, J. Reine Angew. Math. **171** (1934), 19–41.

Dept. of Mathematics & Statistics, University of Massachusetts, Amherst, MA 01003-9305, USA

E-mail address: bush@math.umass.edu