Available at
WWW.MATHEMATICSWEB.ORG
POWERED BY SCIENCE @ DIRECT•

Journal of Number Theory 100 (2003) 313–325

JOURNAL OF
Number
Theory

http://www.elsevier.com/locate/jnt

Computation of Galois groups associated to the 2-class towers of some quadratic fields

M.R. Bush

Mathematics Department, University of Illinois, Urbana-Champaign, IL 61801, USA

Received 25 March 2002
Communicated by D. Goss

Abstract

The p-group generation algorithm from computational group theory is used to obtain information about large quotients of the pro-2 group $G = \mathrm{Gal}\,(k^{nr,2}/k)$ for $k = \mathbb{Q}(\sqrt{d})$ with $d = -445, -1015, -1595, -2379$. In each case we are able to narrow the identity of G down to one of a finite number of explicitly given finite groups. From this follow several results regarding the corresponding 2-class tower.

© 2003 Elsevier Science (USA). All rights reserved.

MSC: primary: 11Y40; secondary: 11R37; 20D15

Keywords: Class tower; Class field; Quadratic field; Explicit Galois group

1. Introduction

In recent years there has been much interest in trying to determine the behaviour of the p-class tower of a quadratic field especially in the case where $p = 2$. See for instance [1,2,4,7,11]. Note that by (p-)*class tower of* k we mean the chain of fields

$$k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_n \subseteq \cdots ,$$

where k_{n+1} is the Hilbert (p-)class field of k_n for each nonnegative integer n. We say that the tower is *finite* if $k_n = k_{n+1}$ for some n, and infinite otherwise. If it is finite then the minimal such n is called the *length* of the tower. In this paper we show that the 2-class towers of four imaginary quadratic fields k are finite using a

E-mail address: mrbush@math.uiuc.edu.

0022-314X/03/$ - see front matter © 2003 Elsevier Science (USA). All rights reserved.
doi:10.1016/S0022-314X(02)00128-2

computational method first introduced by Boston and Leedham-Green [4]. In fact we are able to give a short list of candidates for the Galois group $\mathrm{Gal}(k^{nr,2}/k)$ in each case. Here $k^{nr,2}$ denotes the maximal unramified 2-extension of k which is obtained by taking the union of the fields occurring in the 2-class tower of k.

The first field we consider is $k = \mathbb{Q}(\sqrt{-2379})$. It was noted by Stark [10] that this field has root discriminant $\sqrt{|d_k|} \approx 48.8$ which is just above the best known lower bound (≈ 44.7 under GRH) for $R = \liminf_{n\to\infty} R_n$, where R_n is the minimal root discriminant over all imaginary number fields of degree n (see [9]). If the class tower above k were infinite we would thus obtain a fairly tight upper bound on possible sharpenings of this lower bound (since root discriminants remain constant in class towers). Currently the best known upper bound on this lower bound is around 83.9 (see [6]) so this would be a significant improvement. We do not resolve whether or not the class tower of k is infinite here but our methods do show that the 2-class tower is finite of length 2.

The three other fields we consider are $k = \mathbb{Q}(\sqrt{-445})$, $\mathbb{Q}(\sqrt{-1015})$ and $\mathbb{Q}(\sqrt{-1595})$. It is observed in [2] that under GRH these fields are the first examples of imaginary fields with finite (2-)class towers and $\mathrm{rank}\,\mathrm{Cl}_2(k_1) \geqslant 3$. Here we determine that each field has finite 2-class tower unconditionally. We are also able to obtain the exact length of the tower and the 2-class groups which occur in it in each case.

2. The method

The method is based on the p-group generation algorithm introduced by O'Brien [8]. We now recall some definitions. Let G be a pro-p group. We recursively define a series of closed subgroups of G

$$G = P_0(G) \geqslant P_1(G) \geqslant P_2(G) \geqslant \cdots$$

by setting $P_n(G) = P_{n-1}(G)^p[G, P_{n-1}(G)]$ for each $n \geqslant 1$. Here the group on the righthand side is the closed subgroup generated by all pth powers of elements in $P_{n-1}(G)$, and commutators of elements from G and $P_{n-1}(G)$. If G is a finite p-group then the series above is finite and the smallest c such that $P_c(G) = \{1\}$ will be called the *p-class* of G. A p-group H is called a *descendant* of G if $H/P_c(H) \cong G$ where c is the p-class of G. It is an *immediate descendant* if it has p-class $c+1$. The p-group generation algorithm finds representatives (up to isomorphism) of all the immediate descendants of a given finite p-group G.

Now, fix an ordered pair $(G, \{G_i\}_{i=1}^n)$ where $G = \mathrm{Gal}\,(k^{nr,2}/k)$ is a pro-2 group and G_i is a closed subgroup of G for $i = 1, \dots, n$. We will be interested in the pairs $G_{(m)} = (G/P_m(G), \{\overline{G_i}\}_{i=1}^n)$, where $m \geqslant 0$ and $\overline{G_i}$ denotes the image of the subgroup G_i under the natural map to the quotient $G/P_m(G)$. We note that $G/P_m(G)$ is always finite.

Definition 1. A pair $(H, \{H_i\}_{i=1}^n)$ will be called a *representative* of the pair $G_{(m)}$ if there exists an isomorphism $\psi : H \to G/P_m(G)$ such that $\psi(H_i) = \overline{G_i}$ for each $i = 1, \dots, n$.

We now have a lemma which follows easily from the definitions.

Lemma 1. *Suppose that $(P, \{P_i\}_{i=1}^n)$ is a representative of $G_{(m)}$ and $(Q, \{Q_i\}_{i=1}^n)$ is a representative of $G_{(m+1)}$, then*

(1) *Q is an immediate descendant of P.*
(2) *There exists a surjective map $f : Q \to P$ such that $f(Q_i) = P_i$ for $i = 1, \dots, n$.*

Given a representative of $G_{(m)}$ Lemma 1 allows us to compute a finite list of pairs containing a representative of $G_{(m+1)}$. This is because a finite group P has only finitely many immediate descendants Q up to isomorphism and for each descendant Q there are only finitely many surjective maps $f : Q \to P$. Thus, starting with a list of pairs known to contain a representative of $G_{(t)}$ for some t we can (by applying Lemma 1 repeatedly) compute a list of pairs which must contain a representative of $G_{(m)}$ for any $m > t$.

As it stands the above is not particularly useful since the number of pairs grows very quickly with m. To try to eliminate some of these we now suppose that we know the direct product decomposition of the abelian group G_i/G_i' into cyclic groups for $i = 1, \dots, n$. From now on this information about the decomposition will be referred to as the *abelian quotient invariants of* G_i. It will usually be given by listing the orders of the cyclic subgroups involved, so for instance if $G_i/G_i' \cong C_2 \times C_4 \times C_4$ (where C_2 and C_4 are cyclic groups of orders 2 and 4, respectively) then we would say that G_i has abelian quotient invariants $[2, 4, 4]$. We note that in practice it is possible to get hold of such information for low index subgroups of G by computing the 2-Sylow subgroups of the ideal class groups of small subextensions of $k^{nr,2}/k$ and then applying class field theory. If we also assume that $G_i \supseteq P_t(G)$ for each i then for $m \geqslant t$ the abelian quotient invariants of the image of G_i in $G/P_m(G)$ must be a quotient of those of G_i. In the examples considered below the application of these additional restrictions drastically reduces the number of candidates for representatives of $G_{(m)}$ for each m allowing us to obtain useful information about the extension $k^{nr,2}/k$.

In summary, given a list of pairs $\mathbf{L}_m$ containing a representative of $G_{(m)}$ we compute a list $\mathbf{L}_{m+1}$ containing a representative of $G_{(m+1)}$ as follows

(1) For each pair $(P, \{P_i\}_{i=1}^n)$ in $\mathbf{L}_m$ we compute a list of all the immediate descendants of P (up to isomorphism) using the p-group generation algorithm.
(2) For each immediate descendant Q we construct all possible surjective maps $f : Q \to P$.
(3) For each Q and $f : Q \to P$ we check to see whether the abelian quotient invariants of $f^{-1}(P_i)$ are a quotient of those of G_i for every $i = 1, \dots, n$. If this is the case then the pair $(Q, \{f^{-1}(P_i)\}_{i=1}^n)$ is appended to the list $\mathbf{L}_{m+1}$.

In practice, we can usually compute a suitable starting list $\mathbf{L}_1$ or $\mathbf{L}_2$. In the examples considered in the next section the sequence of lists $\mathbf{L}_m$ that are then generated terminate, i.e. $\mathbf{L}_m$ is empty for sufficiently large m. This implies that $G = \mathrm{Gal}\,(k^{nr,2}/k)$ actually occurs as a group in one of the pairs on these lists and so must be finite. We now note that if $(H, \{H_i\}_{i=1}^n)$ is a representative of $(G, \{G_i\}_{i=1}^n)$ then the abelian quotient invariants of H_i must match those of G_i exactly. This observation motivates the following definition.

Definition 2. A finite group H will be called a *candidate for* G if there exists a pair $(H, \{H_i\}_{i=1}^n)$ such that the abelian quotient invariants of H_i are equal to those of G_i for all $i = 1, \dots, n$.

As we generate pairs we keep track of all the candidates for G that we find since in the event the sequence of lists terminate we know that G must be isomorphic to one of them.

3. Some examples

Two packages were used to carry out the actual computations in this section. KASH (see [5]) was used to construct 2-class fields above k up to degree 16, as well as for some ideal class group computations. MAGMA (see [3]) was used to calculate ideal class groups, as well as determining the subfield lattices and Galois groups of certain degree 16 extensions of $\mathbb{Q}$. We also made use of MAGMA's implementation of the p-group generation algorithm. Throughout this section $G = \mathrm{Gal}\,(k^{nr,2}/k)$.

3.1. The field $k = \mathbb{Q}(\sqrt{-2379})$

Using KASH we have $G/G' \cong [4,4]$. It follows from this that $G/P_1(G) \cong [2,2]$. Calculation of some 2-class fields shows that $\mathbb{Q}(\sqrt{-3}, \sqrt{13}, \sqrt{61})$ is a degree 4 subextension of $k^{nr,2}/k$ with Galois group over k equal to $[2,2]$. This implies that the subgroup $P_1(G)$ of G corresponds to the subfield $\mathbb{Q}(\sqrt{-3}, \sqrt{13}, \sqrt{61})$. The following table shows the intermediate fields together with the abelian invariants of the 2-Sylow subgroup of the corresponding ideal class group.

$k = \mathbb{Q}(\sqrt{-3 \cdot 13 \cdot 61})$	$[4,4]$
$k(\sqrt{61})$	$[2,2,8]$
$k(\sqrt{-3})$	$[2,2,8]$
$k(\sqrt{13})$	$[2,2,16]$
$\mathbb{Q}(\sqrt{-3}, \sqrt{13}, \sqrt{61})$	$[4,4,8]$

We can thus construct a representative of $G_{(1)} = (G/P_1(G), \{\overline{G_i}\}_{i=1}^5)$ where the groups G_i are the subgroups of G corresponding to the intermediate fields of the extension $\mathbb{Q}(\sqrt{-3}, \sqrt{13}, \sqrt{61})/k$. Let $\mathbf{L}_1$ be the list containing just this pair. We now apply the method from Section 2 using the abelian quotient invariants given in the table to generate a sequence of lists $\mathbf{L}_m$ for $m > 1$. The collection of groups that occur in the pairs in these lists can be represented by a tree as shown in Fig. 1.

In this picture we have only displayed vertices which represent groups having at least one immediate descendant and which occur in one of the lists $\mathbf{L}_m$. Groups which do not have any descendants but which occur in one of the lists are not shown. This is done primarily for convenience since including such (terminal) groups would clutter up the picture and we are really only interested in determining whether or not this and other such trees are finite. Note that in this tree a vertex Q is a child of another vertex P if the group corresponding to Q is an immediate descendant of the group corresponding to P. Thus the vertex numbered 0 corresponds to the group $[2, 2]$ of 2-class 1 (from the pair in $\mathbf{L}_1$). The groups numbered 1 to 6 have 2-class 2 and come from the pairs in $\mathbf{L}_2$ and so on. Note that the groups in each level of the tree are pairwise non isomorphic but each one may occur in more than one pair on the corresponding list.

While generating the lists a total of 81 candidates for G were found (all of them descendants of the group corresponding to vertex 6). Most of these are not displayed in Fig. 1 since they do not have any descendants. At this stage we cannot conclude that G must be one of these groups since after several computations part of the tree (below vertex 4) is still growing. We have however gained some useful information about the quotient $G/P_2(G)$. In particular, since no candidates for G were found in

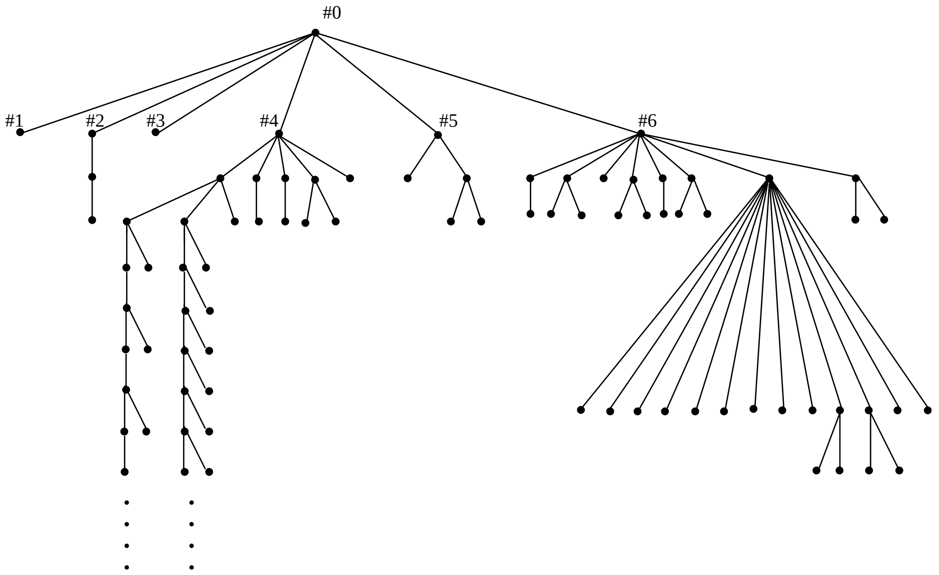

Fig. 1. A tree of groups.

the finite subtrees lying below vertices 1, 2, 3 and 5 we can conclude that $G/P_2(G)$ must be isomorphic to the group corresponding to either vertex 4 or vertex 6. Let us denote these two groups by H_4 and H_6, respectively. H_4 is generated by $\{x_i\}_{i=1}^4$ subject to the power commutator presentation

$$H_4\colon\ x_1^2 = x_4, \quad [x_2, x_1] = x_3,$$

H_6 is generated by $\{x_i\}_{i=1}^5$ subject to the power commutator presentation

$$H_6\colon\ x_1^2 = x_4, \quad x_2^2 = x_5, \quad [x_2, x_1] = x_3.$$

Remark 1. Note that in any power commutator presentation if a power x_r^2 or commutator $[x_r, x_s]$ does not occur on the left hand side of the given relations then it is assumed to be trivial.

Using KASH we can find a degree 16 Galois extension L over $\mathbb{Q}$ unramified over k. One such field is defined by the polynomial

$$\begin{aligned} &x^{16} - 2158x^{14} - 1166x^{13} + 1886402x^{12} + 1125558x^{11} - 738996514x^{10} \\ &\quad + 24633036x^9 + 88589769625x^8 - 114401828130x^7 + 12435312336118x^6 \\ &\quad + 15732271973132x^5 + 506694031967064x^4 - 98005626098698x^3 \\ &\quad + 10557300816504844x^2 - 7195589177918350x + 41648817878658175 \end{aligned}$$

and its Galois group is the direct product of the dihedral group of order 8 and the cyclic group of order 2. By considering the lattice of subfields of this extension over k it can be shown that $\mathrm{Gal}\,(L/k) \cong [2, 4]$. The lattice of subfields and the 2-Sylow subgroups of the corresponding ideal class groups are shown in Fig. 2. The degree 2

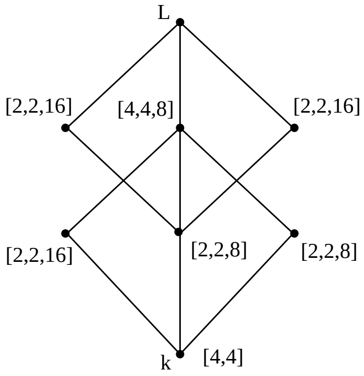

Fig. 2. A lattice of subfields and 2-class groups.

extensions of k in this lattice (from left to right) are $k(\sqrt{13})$, $k(\sqrt{61})$ and $k(\sqrt{-3})$. The degree 4 extensions of k in this lattice (from left to right) are $k(\sqrt{\mu})$, $\mathbb{Q}(\sqrt{-3}, \sqrt{13}, \sqrt{61})$ and $k(\sqrt{-3\mu})$ where $\mu = 25 + 4\sqrt{61}$.

Now $[2, 4]$ is a group of 2-class 2 which means that the subgroup $P_2(G)$ of G corresponds to some intermediate field of the extension $k^{nr,2}/L$. So we consider the pair $G_{(2)} = (G/P_2(G), \{\overline{G_i}\}_{i=1}^{7})$ where G_i are the subgroups of G corresponding to the intermediate fields (of degree at most 4) in the lattice above. A list $\mathbf{L}_2$ containing a representative of $G_{(2)}$ can be constructed by taking each group H_r ($r = 4$ or $r = 6$) and adjoining all pairs of the form $(H_r, \{f^{-1}(R_i)\}_{i=1}^{7})$ where f runs through all the surjective homomorphisms from H_r onto $[2, 4]$ and $\{R_i\}_{i=1}^{7}$ are the subgroups of $[2, 4]$ of index at most 4. When the method from Section 2 is applied to $\mathbf{L}_2$ the sequence of lists generated terminates. The extra information about the abelian quotient invariants of the two additional subgroups of index 4 is restrictive enough to show G must be finite.

The number of candidates for G found (with the additional restrictions) decreases from 81 to 24. An investigation of these 24 groups shows that they fall naturally into two classes based on the abelian quotient invariants of their subgroups of index 4. In one of the classes (consisting of 8 groups) each group has several subgroups of index 4 with abelian quotient invariants $[4, 32]$. None of the subgroups of index 4 of the groups in the other class have these invariants. It can be checked that the field $k(\sqrt{v})$ where $v = 5 + 4\sqrt{13}$ is an unramified cyclic extension of k of degree 4 with 2-class group $[4, 32]$. We conclude that G must be isomorphic to one of 8 possible groups. Each one of these can be obtained by selecting $r, s, t \in \{0, 1\}$ and then considering the group generated by $\{x_i\}_{i=1}^{11}$ subject to the power commutator presentation

$$\begin{array}{lll}
[x_2, x_1] = x_3, & [x_4, x_3] = x_{10}, & [x_6, x_1] = x_9, \\
[x_3, x_1] = x_6, & [x_5, x_1] = x_6 x_7 x_8 x_9 x_{10}, & [x_8, x_1] = x_{10}, \\
[x_3, x_2] = x_7, & [x_5, x_3] = x_{10} x_{11}, & [x_8, x_2] = x_{10} x_{11}, \\
[x_4, x_2] = x_8, & [x_5, x_4] = x_{10} x_{11}, & [x_9, x_1] = x_{11}. \\
x_1^2 = x_4, & x_5^2 = x_6 x_9 x_{10}^s x_{11}^t, & \\
x_2^2 = x_5, & x_6^2 = x_9 x_{10} x_{11}, & \\
x_3^2 = x_6 x_8 x_9 x_{10}, & x_7^2 = x_{10} x_{11}, & \\
x_4^2 = x_7 x_{11}^r, & x_9^2 = x_{11}, &
\end{array}$$

Remark 1 about power commutator presentations applies here also.

The 8 groups defined by these presentations are very similar. They all have order 2^{11} and 2-class 5. They also possess derived series of the same length and with the same abelian factors. This allows us to deduce

Proposition 1. *The* 2*-class tower of the imaginary quadratic field* $k = \mathbb{Q}(\sqrt{-2379})$ *is finite of length* 2, *i.e.* $k = k_0 \subset k_1 \subset k_2 = k^{nr,2}$. *We have* $\mathrm{Gal}(k_1/k_0) \cong [4, 4]$ *and* $\mathrm{Gal}(k_2/k_1) \cong [2, 4, 16]$.

3.2. The field $k = \mathbb{Q}(\sqrt{-445})$

In this case $G/G' \cong [2,4]$ so we still have $G/P_1(G) \cong [2,2]$. The field $\mathbb{Q}(\sqrt{-1}, \sqrt{5}, \sqrt{89})$ is a degree 4 subextension of $k^{nr,2}/k$. We can calculate the 2-Sylow subgroup of the ideal class group of each intermediate field, and construct a representative of the pair $G_{(1)} = (G/P_1(G), \{\overline{G_i}\}_{i=1}^{5})$, where the groups G_i are the subgroups of G corresponding to the intermediate fields. Applying the method from Section 2 we are able to narrow down $G/P_2(G)$ to one of 3 groups. Two of these can be identified as $[2,4]$ and D_4 (the dihedral group of order 8). These can be eliminated as possibilities since it is easy to find examples of degree 8 subextensions of $k^{nr,2}/k$ with either of these groups as the Galois group. This implies that both groups must arise as quotients of $G/P_2(G)$. It follows that $G/P_2(G)$ must be isomorphic to the remaining group of order 16 which we will denote H_3. The group H_3 is actually isomorphic to the group H_4 in the previous example.

As before we now consider an unramified degree 8 extension L over k defined over $\mathbb{Q}$ by the polynomial

$$x^{16} + 12x^{14} + 4554x^{12} + 17928x^{10} + 2231251x^{8} + 13625880x^{6}$$
$$- 10866150x^{4} - 143437500x^{2} + 244140625.$$

We have $\mathrm{Gal}\,(L/k) \cong [2,4]$. The lattice of subfields of L/k together with the 2-Sylow subgroups of the corresponding ideal class groups can be seen in Fig. 3. The degree 2 extensions of k in this lattice (from left to right) are $k(\sqrt{5})$, $k(\sqrt{89})$ and $k(\sqrt{-1})$. The degree 4 extensions of k in this lattice (from left to right) are $k(\sqrt{-\mu})$, $\mathbb{Q}(\sqrt{-1}, \sqrt{5}, \sqrt{89})$ and $k(\sqrt{\mu})$ where $\mu = -3 + 4\sqrt{-5}$.

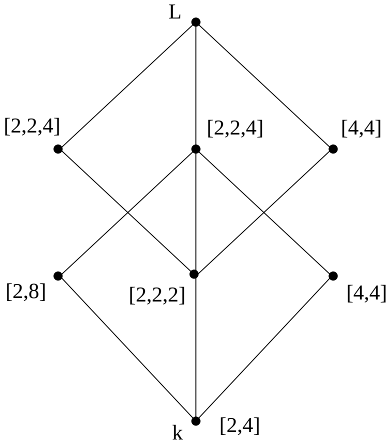

Fig. 3. A lattice of subfields and 2-class groups.

We construct $\mathbf{L}_2$ by adjoining all pairs of the form $(H_3, \{f^{-1}(R_i)\}_{i=1}^7)$, where f runs over all the surjective maps from H_3 to $[2,4]$ and $\{(R_i)\}_{i=1}^7$ are the subgroups of $[2,4]$ of index at most 4. When we apply the method starting with $\mathbf{L}_2$ the sequence of lists generated terminates and a total of 12 candidates for G are found. To try and determine which one is isomorphic to G we look again at the abelian quotient invariants of their index 4 subgroups. We find that only 2 of the 12 groups have an index 4 subgroup with invariants $[2,16]$. It can be checked that the field $k(\sqrt{v})$ where $v = 13 + 4\sqrt{5}$ is an unramified extension of k of degree 4 with 2-class group $[2,16]$. It follows that G must be isomorphic to one of these two groups. Each one of these can be obtained by selecting $r \in \{0,1\}$ and then considering the group generated by $\{x_i\}_{i=1}^8$ subject to the power commutator presentation

$$\begin{array}{lll}
[x_2,x_1] = x_3, & [x_5,x_2] = x_8, & x_1^2 = x_4, \\
[x_3,x_1] = x_5, & [x_5,x_3] = x_8, & x_2^2 = x_5x_7, \\
[x_3,x_2] = x_6, & [x_5,x_4] = x_8, & x_3^2 = x_6x_7, \\
[x_4,x_2] = x_5x_6x_7x_8, & [x_7,x_1] = x_8, & x_6^2 = x_8. \\
[x_4,x_3] = x_7, & [x_7,x_2] = x_8, & \\
[x_5,x_1] = x_7, & x_4^2 = x_8^r, &
\end{array}$$

Remark 1 about power commutator presentations applies here also.

Once again these groups are very similar. They both have order 2^8 and 2-class 5 and by looking at their derived series we deduce

Proposition 2. *The field* $k = \mathbb{Q}(\sqrt{-445})$ *has finite* 2*-class tower of length* 3, *i.e.* $k = k_0 \subset k_1 \subset k_2 \subset k_3 = k^{nr,2}$. *We have* $\mathrm{Gal}\,(k_1/k_0) \cong [2,4]$, $\mathrm{Gal}\,(k_2/k_1) \cong [2,2,4]$ *and* $\mathrm{Gal}\,(k_3/k_2) \cong [2]$.

Remark 2. We note that the finiteness of the towers in the propositions above is purely a group theoretic result. Any field k for which there exists a degree 8 subextension L of $k^{nr,2}/k$ such that the lattice of subfields and corresponding 2-class groups are the same as those in Figs. 2 and 3 must also have a finite 2-class tower.

Remark 3. In each of the previous examples a single unramified degree 8 extension of k was selected. The number theoretic information provided by this extension was sufficient for us to be able to show the finiteness of $\mathrm{Gal}\,(k^{nr,2}/k)$ in each case. One obvious way to extend the algorithm would be to incorporate the information from several such extensions at the same time. In some sense we were already doing this (in an ad hoc fashion) when we took the initial finite list of candidates in each of the previous examples and eliminated some of them using additional number theoretic information. More precisely we now consider pairs of the form $(H, \{\{H_i^{(j)}\}_{i=1}^n\}_{j=1}^t)$ where t is the number of extensions under consideration. Such a pair will be called a *representative* of $G_{(m)}$ if there exists a family of isomorphisms $\psi_j : H \to G/P_m(G)$ such that $\psi_j(H_i^{(j)}) = \overline{G_i}$ for each $i = 1, \dots, n$ and $j = 1, \dots, t$. As before given a list of pairs $\mathbf{L}_m$ containing a representative of $G_{(m)}$ we can use the p-group generation algorithm to compute a list $\mathbf{L}_{m+1}$ containing a representative of $G_{(m+1)}$.

3.3. *The fields $k = \mathbb{Q}(\sqrt{-1015})$ and $\mathbb{Q}(\sqrt{-1595})$*

In both cases $G/G' \cong [2,8]$ so we have $G/P_1(G) \cong [2,2]$. The fields $\mathbb{Q}(\sqrt{-7}, \sqrt{5}, \sqrt{29})$ and $\mathbb{Q}(\sqrt{-11}, \sqrt{5}, \sqrt{29})$ are degree 4 subextensions of $k^{nr,2}/k$ in each case. We can calculate the 2-Sylow subgroup of the ideal class group of each intermediate field, and construct a representative of the pair $G_{(1)} = (G/P_1(G), \{\overline{G_i}\}_{i=1}^{5})$ where the groups G_i are the subgroups of G corresponding to the intermediate fields. For both the given fields we get the same representative of $G_{(1)}$. Applying the method from Section 2 we are able to narrow down $G/P_2(G)$ to one of 4 groups. Two of these can be identified as $[2,4]$ and D_4 (the dihedral group of order 8). These can be eliminated as possibilities since it is easy to find examples of degree 8 subextensions of $k^{nr,2}/k$ with either of these groups as the Galois group (see below). This implies that both groups must arise as quotients of $G/P_2(G)$. It follows that $G/P_2(G)$ must be isomorphic to one of the remaining two groups of order 16 which we will denote H_3 and H_4. The group H_3 is actually isomorphic to the group H_3 in the previous example.

Now taking into account Remark 3 we consider several unramified degree 8 extensions L over k instead of only one. For $k = \mathbb{Q}(\sqrt{-1015})$ we consider the fields defined over $\mathbb{Q}$ by the polynomials

$$\begin{aligned} L_1 : x^{16} &+ 8302x^{14} + 29865815x^{12} + 60621449422x^{10} + 75762817738769x^{8} \\ &+ 59625975137422568x^{6} + 28858765154851072400x^{4} \\ &+ 7861191091575524181248x^{2} + 92418233297272071635353 6, \end{aligned}$$

$$\begin{aligned} L_2 : x^{16} &+ 68x^{14} - 26x^{13} + 1922x^{12} - 2316x^{11} + 29806x^{10} - 20958x^{9} + 335885x^{8} \\ &+ 62002x^{7} + 1639268x^{6} + 2747082x^{5} + 6227217x^{4} + 7583004x^{3} + 7628823x^{2}, \\ &+ 4664142x + 1486431, \end{aligned}$$

$$\begin{aligned} L_3 : x^{16} &+ 208250x^{14} + 6454080x^{13} + 84986985877x^{12} - 319881524440x^{11} \\ &+ 10504186175856042x^{10} + 3217249977395280x^{9} + 22312073535837591684 04x^{8} \\ &- 4165232197552629790668 0x^{7} + 162122207446267254901910082x^{6} \end{aligned}$$

$$\begin{aligned}
&- 44492763756606987561141601 20x^5 + 2316989620455845795444303772 1749x^4\\
&- 46682108626857407129924517175 3200x^3\\
&+ 796726493601047682437367297422156178x^2\\
&- 37902470874562381569855570165787116760x\\
&+ 815959853788268525135566273425211624405 21.
\end{aligned}$$

For $k = \mathbb{Q}(\sqrt{-1595})$ we consider the fields defined over $\mathbb{Q}$ by the polynomials

$$\begin{aligned}
L_1 : x^{16} &+ 75x^{14} + 3384x^{12} + 85875x^{10} + 1497421x^8 + 16831500x^6\\
&+ 129999744x^4 + 564715200x^2 + 1475789056,
\end{aligned}$$

$$\begin{aligned}
L_2 : x^{16} &+ 145x^{14} + 4721x^{12} - 336690x^{10} + 2932126x^8 + 22696270x^6\\
&+ 32760881x^4 - 90377775x^2 + 43046721,
\end{aligned}$$

$$\begin{aligned}
L_3 : x^{16} &- 2312x^{14} + 2359542x^{12} - 1183214812x^{10} + 276742820433x^8\\
&- 63131144780036x^6 + 6695155576703324 8x^4 - 13918403354887798784x^2\\
&+ 793394183478882017536.
\end{aligned}$$

In each case we obtain three lattices of subfields together with the 2-Sylow subgroups of the corresponding ideal class groups. These turn out to be the same for both $k = \mathbb{Q}(\sqrt{-1015})$ and $k = \mathbb{Q}(\sqrt{-1595})$ and are displayed in Fig. 4. Note that $\mathrm{Gal}\,(L_1/k) = D_4$, $\mathrm{Gal}\,(L_2/k) = [2,4]$ and $\mathrm{Gal}\,(L_3/k) = D_4$. A list $\mathbf{L}_2$ containing a representative of $G_{(2)}$ (see the modified definition in Remark 3) can be constructed by taking each group H_r ($r = 3$ or 4) and adjoining all pairs of the form $(H_r, \{\{f_j^{-1}(R_i^{(j)})\}_{i \in I_j}\}_{j=1}^{3})$ where f_j runs through all the surjective homomorphisms from H_r onto $\mathrm{Gal}(L_j/k)$ and $\{R_i^{(j)}\}_{i \in I_j}$ are the subgroups of $\mathrm{Gal}(L_j/k)$ of index at most 4. Here I_j is simply an indexing set for the subgroups, its size being determined by the structure of $\mathrm{Gal}(L_j/k)$. When the method from Section 2 is applied to $\mathbf{L}_2$ the sequence of lists generated terminates and a total of 2 candidates for G are found. Each one of these can be obtained by selecting $r \in \{0,1\}$ and then considering the

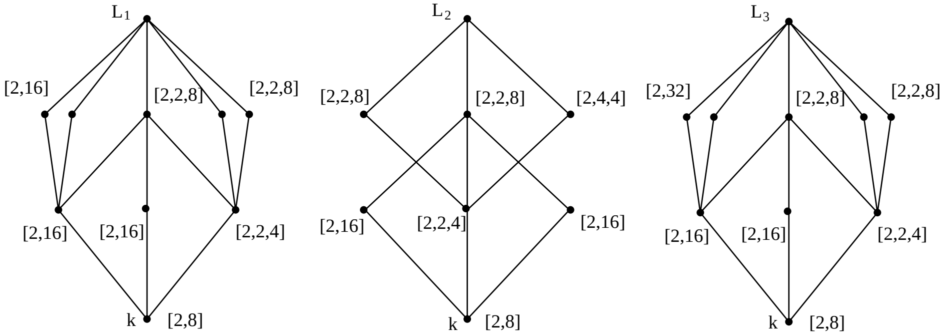

Fig. 4. Three subfield lattices and associated 2-class groups.

group generated by $\{x_i\}_{i=1}^{9}$ subject to the power commutator presentation

$$\begin{aligned}
&[x_2,x_1]=x_3, && [x_5,x_2]=x_9, && x_2^2=x_5x_7,\\
&[x_3,x_1]=x_5, && [x_5,x_3]=x_9, && x_3^2=x_7x_8x_9^{1-r},\\
&[x_3,x_2]=x_8x_9^{1-r}, && [x_5,x_4]=x_9, && x_4^2=x_6,\\
&[x_4,x_2]=x_5x_7x_8x_9^{r}, && [x_7,x_1]=x_9, && x_6^2=x_8,\\
&[x_4,x_3]=x_7, && [x_7,x_2]=x_9, && x_8^2=x_9.\\
&[x_5,x_1]=x_7, && x_1^2=x_4, &&
\end{aligned}$$

Remark 1 about power commutator presentations applies here also. Both of these groups have order 2^9 and 2-class 5. By looking at their derived series we deduce

Proposition 3. *The fields* $k=\mathbb{Q}(\sqrt{-1015})$ *and* $k=\mathbb{Q}(\sqrt{-1595})$ *have finite* 2-*class tower of length* 3, *i.e.* $k=k_0\subset k_1\subset k_2\subset k_3=k^{nr,2}$. *In both cases we have* $\mathrm{Gal}(k_1/k_0)\cong[2,8]$, $\mathrm{Gal}(k_2/k_1)\cong[2,2,4]$ *and* $\mathrm{Gal}(k_3/k_2)\cong[2]$.

Acknowledgments

The author thanks Nigel Boston for suggesting this problem and for many helpful discussions. He would also like to thank the referee who provided explicit descriptions of various subfields in the examples.

References

[1] E. Benjamin, F. Lemmermeyer, C. Snyder, Imaginary quadratic fields k with cyclic $Cl_2(k^1)$, J. Number Theory 67 (1997) 229–245.

[2] E. Benjamin, F. Lemmermeyer, C. Snyder, Imaginary quadratic fields with $Cl_2(k)\cong(2,2^m)$ and Rank $\mathrm{Cl}_2(k^1)=2$, preprint, 2000.

[3] W. Bosma, J.J. Cannon, Handbook of Magma Functions, School of Mathematics and Statistics, University of Sydney, 1996.

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

[5] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, K. Wildanger, KANT $V4$, J. Symbolic Comput. 24 (1997) 267–283.

[6] F. Hajir, C. Maire, Tamely ramified towers and discriminant bounds for number fields, Compositio Math. 128 (2001) 35–53.

[7] F. Lemmermeyer, On 2-class field towers of some imaginary quadratic number fields, Abh. Math. Sem. Univ. Hamburg 67 (1997) 205–214.

[8] E.A. O'Brien, The p-group generation algorithm, J. Symbolic Comput. 9 (5–6) (1990) 677–698.

[9] 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 (1) (1990) 119–141.

[10] H.M. Stark, private communication.

[11] K. Yamamura, Maximal unramified extensions of imaginary quadratic number fields of small conductors, J. Théorie Nombres Bordeaux 9 (2) (1990) 405–448.