# Imaginary Quadratic Fields $k$ with Cyclic $\mathrm{Cl}_2(k^1)$

E. Benjamin
Mathematics Department
Unity College

F. Lemmermeyer
Erwin-Rohde-Str. 19
D-69120 Heidelberg

C. Snyder
Department of Mathematics and Statistics
University of Maine
and
Research Institute of Mathematics, Orono

**Abstract**

Let $k$ be an imaginary quadratic number field. Let $k^1$ denote the Hilbert 2-class field of $k$. We characterize those $k$ whose 2-class fields have cyclic 2-class group.

## 1 Introduction

Let $k$ be an algebraic number field with $\mathrm{Cl}_2(k)$, the Sylow 2-subgroup of its ideal class group, $\mathrm{Cl}(k)$. Denote by $k^1$ the Hilbert 2-class field of $k$ (in the wide sense). Also let $k^n$ (for $n$ a nonnegative integer) be defined inductively as: $k^0 = k$ and $k^{n+1} = (k^n)^1$. Then

$$k^0 \subseteq k^1 \subseteq k^2 \subseteq \cdots \subseteq k^n \subseteq \cdots$$

is called the 2-class field tower of $k$. (Other types of class field towers have been studied, also.) If $n$ is the minimal integer such that $k^n = k^{n+1}$, then $n$ is called the length of the tower. If no such $n$ exists, then the tower is said to be of infinite length. One outstanding problem in nonabelian class field theory is to determine if a given field has finite or infinite class field tower.

By class field theory, $\mathrm{Gal}(k^1/k) \simeq \mathrm{Cl}_2(k)$; moreover, if $G = \mathrm{Gal}(k^n/k)$, then $G^{(j+1)} = \mathrm{Gal}(k^n/k^j)$ and $G/G^{(j+1)} \simeq \mathrm{Gal}(k^j/k)$ where $G^{(j)}$ denotes the $j$th derived subgroup of $G$, (see the next section for details). In particular, if $G = \mathrm{Gal}(k^2/k)$, then the commutator subgroup $G' = \mathrm{Gal}(k^2/k^1) \simeq \mathrm{Cl}_2(k^1)$ and $G/G' \simeq \mathrm{Gal}(k^1/k) \simeq \mathrm{Cl}_2(k)$.

Now, if $\mathrm{Cl}_2(k)$ is nontrivial and cyclic, then the 2-class field tower always is of length 1. Furthermore, if $\mathrm{Cl}_2(k) \simeq (2,2)$, then the 2-class field tower is of length 1 or 2. For particular types of fields $k$, for example, imaginary quadratic fields with $\mathrm{Cl}_2(k) \simeq (2,2)$, cf. [14], the structure of $\mathrm{Gal}(k^2/k)$ has been completely determined. The success in this case is in part due to the fact that, contrary to most other cases, 2-groups whose abelianization is $(2,2)$ are well understood, cf., e.g. the footnote on page 85 of [29] and also see [27].

If one considers the next simplest case, namely where $\mathrm{Cl}_2(k) \simeq (2,4)$, then the situation is very different when compared with the cases described above, even when $k$ is an imaginary quadratic number field. For example, if $k = \mathbb{Q}(\sqrt{})$, where $-d = 264, 260, 1443$, or $25355$, then $\mathrm{Cl}_2(k) \simeq (2,4)$ and the length of the 2-class field tower is $1, 2, 2, \infty$, respectively, see [16]. At present there is no known way to determine explicitly the length of the 2-class field tower. In particular, (to our knowledge) it is not even known if there exists such a field with finite 2-tower of length other than 1 and 2.

As implied above, part of the reason for this difficulty is that 2-groups, $G$, with $G/G' \simeq (2,4)$ are not well understood. However, it is known that if $G/G' \simeq (2,4)$, then the 2-rank of $G' \leq 3$, cf. [6]. Moreover, if the 2-rank of $G' \leq 2$, then $G'$ is abelian, c.f. [5]. Hence, if we let $G = \mathrm{Gal}(k^2/k)$ so that $G' = \mathrm{Gal}(k^2/k^1) \simeq \mathrm{Cl}_2(k^1)$, then the 2-rank of $\mathrm{Cl}_2(k^1)$ equals $0, 1, 2$, or $3$. Also, if $\mathrm{Cl}_2(k^1)$ has 2-rank $< 3$, then the 2-class field tower terminates at $k^2$. In the examples above, where $k = \mathbb{Q}(\sqrt{})$, the 2-ranks of $\mathrm{Cl}_2(k^1)$ are $0, 1, 2$, and $3$, respectively. One way of searching for fields with finite 2-class field tower of length at least 3, is to start by determining the 2-rank of $\mathrm{Cl}_2(k^1)$.

In this note, we begin this project by determining which imaginary quadratic fields $k$ have cyclic $\mathrm{Cl}_2(k^1)$. Since it is known precisely when $\mathrm{Gal}(k^2/k)$ is abelian or metacyclic (and so of course $\mathrm{Cl}_2(k^1)$ is cyclic) (cf. [19]), we shall concentrate on the nonmetacyclic case.

First we give some background on Schur multipliers and related results of Scholz and Tate on number knots. Then these results are applied to show that $\mathrm{Cl}_2(k)$ has type $(2, 2^m)$ if $\mathrm{Cl}_2(k^1)$ is cyclic. Next we use group theory to describe the Galois groups of $k^2/k$ of such fields, and finally we classify the imaginary quadratic number fields with cyclic $\mathrm{Cl}_2(k^1)$.

# 2 Schur Multipliers

The Schur Multiplier of a finite group $G$ is most easily defined as follows (cf. [30]): a group extension $E : 1 \longrightarrow A \longrightarrow \Gamma \longrightarrow G \longrightarrow 1$ is called central if $A \subseteq Z(\Gamma)$; $E$ is called a *covering* if $A \subseteq \Gamma'$. Schur [26] has shown that the order of the groups $A$ in central coverings is bounded. Moreover, the groups $A$ in any maximal central covering are mutually isomorphic. The isomorphism class of $A$ in a maximal central covering is called the Schur Multiplier of $G$ and will be denoted by $\mathcal{M}(G)$, the groups $\Gamma$ are called *covering groups* of $G$.

Schur multipliers occur naturally in class field theory. In fact, let $K/k$ denote a finite normal extension of number fields. Then the genus class field $K_{gen}$ is the maximal unramified extension of $K$ such that $K = KF$ for an abelian extension $F/k$. Clearly, $K_{gen}$ is contained in the central class field $K_{cen}$ which is defined as the maximal unramified central extension of $K$ with respect to $k$ (a tower $L/K/k$ is called central if the corresponding group extension $1 \longrightarrow \mathrm{Gal}\,(L/K) \longrightarrow \mathrm{Gal}\,(L/k) \longrightarrow \mathrm{Gal}\,(K/k) \longrightarrow 1$ is central). Therefore, if $K$ is the $p$-class field of $k$, then the group extension corresponding to the tower $L/K/k$ (where $L = K_{cen}^{(p)}$ denotes the central $p$-class field of $K$, i.e., the maximal $p$-extension contained in $K_{cen}/K$) is a central covering. In particular, $\mathrm{Gal}\,(L/K)$ is a factor group of $\mathcal{M}(\mathrm{Gal}\,(K/k))$.

The structure of $\mathcal{M}(G)$ for abelian groups $G$ has been known since Schur [26]:

**Proposition 1** *Let $G$ be an abelian $p$-group, and let $C(p^a)$ denote a cyclic group of order $p^a$. Write $G = C(p^{n_1}) \times \ldots \times C(p^{n_m})$ in such a way that $n_1 \geq n_2 \geq \ldots \geq n_m$. Then*

$$\mathcal{M}(G) \simeq C(p^{n_2}) \times C(p^{n_3})^2 \times \ldots \times C(p^{n_m})^{m-1}.$$

*In particular, the $p$-rank of $\mathcal{M}(G)$ is $\binom{m}{2}$.*

We will need the following simple result on Schur multipliers:

**Proposition 2** *Let $G$ be a finite group with normal subgroup $N$. Suppose that $G' \cap N = 1$. Then $\mathcal{M}(G/N)$ is a homomorphic image of $\mathcal{M}(G)$.*

This follows directly from results of Ganea (Thm. 2.5.6, [13]) or Jones (Thm. 2.5.2, [13]).

# 3 Scholz's Number Knots

The main references for this section are Jehne [11] and Lorenz [20]. Let $k$ be a number field; embedding $k^\times$ into the idele group $J_k$ gives rise to the exact sequence

$$1 \longrightarrow k^\times \longrightarrow J_k \longrightarrow C_k \longrightarrow 1,$$

where $C_k$ is called the idele class group of $k$. The kernel of the canonical map $J_k \longrightarrow I_k$ of the idele group onto the group of fractional ideals is the unit idele group $U_k$.

The number knot of a finite normal extension $K/k$ is defined as the factor group $\nu_{K/k} = k^\times \cap NJ_K/NK^\times$, where $N$ denotes the norm of $K/k$. For cyclic extensions $K/k$, Hasse has shown that $\nu_{K/k} = 1$, and Scholz introduced knots in order to study the validity of Hasse's norm theorem in noncyclic extensions. Scholz also defined the unit knot $\omega^0_{K/k} := E_k \cap NU_K/E_k \cap NK^\times$ and the divisor knot $\delta^0_{K/k}$; if we put $\delta_{K/k} := H_k \cap NI_K/NH_K$ (where $I_K \supseteq H_K$ denote the groups of fractional and principal fractional ideals, respectively), then the divisor knot is simply the image of the map $\nu_{K/k} \longrightarrow \delta_{K/k}$.

Scholz proved

**Theorem 1** *There is an exact sequence (the knot sequence)*

$$1 \longrightarrow \omega^0_{K/k} \longrightarrow \nu_{K/k} \longrightarrow \delta^0_{K/k} \longrightarrow 1,$$

*and* $\delta^0_{K/k} \simeq \mathrm{Gal}\,(K_{cen}/K_{gen})$.

The middle term of the exact knot sequence can also be related to the Schur Multiplier $\mathcal{M}(G)$ of the Galois group $G = \mathrm{Gal}\,(K/k)$, as the theorem of Scholz [24, 25] and Tate ([28], p. 198) shows:

**Theorem 2** *Let $K/k$ be a normal extension with Galois group $G$; for a prime ideal $\mathfrak{P}$ in $K$, let $\mathfrak{p}$ denote the prime ideal $\mathfrak{P} \cap k$ in $k$. Moreover, let $G_{\mathfrak{P}}$ denote the Galois group of the local extension $K_{\mathfrak{P}}/k_{\mathfrak{p}}$, where $K_{\mathfrak{P}}$ and $k_{\mathfrak{p}}$ are the completions of $K$ and $k$ at the prime ideals $\mathfrak{P}$ and $\mathfrak{p}$, respectively. Finally, let $A^\frown = \mathrm{Hom}\,(A, \mathbb{Q}/\mathbb{Z})$ denote the dual of a finite abelian group $A$. Then there is an exact sequence* $\coprod_{\mathfrak{P}} \mathcal{M}(G_{\mathfrak{P}})^\frown \longrightarrow \mathcal{M}(G)^\frown \longrightarrow \nu_{K/k} \longrightarrow 1$.

Thm. 2 contains Hasse's norm theorem as a corollary: the Schur multiplier of cyclic groups is trivial, so we conclude that $\nu_{K/k} = 1$. A slightly more general consequence of Theorem 2 is the following

**Corollary 1** *Let $K/k$ be a finite unramified normal extension with Galois group $G = \mathrm{Gal}\,(K/k)$; then $\nu_{K/k} \simeq \mathcal{M}(G)^\frown$.*

In fact, if $K/k$ is unramified then so is $K_{\mathfrak{P}}/k_{\mathfrak{p}}$; but unramified extensions of local fields are cyclic, hence $\mathcal{M}(G_{\mathfrak{P}}) = 1$ for all primes $\mathfrak{P}$.

We continue to assume that $K/k$ is unramified; then every unit in $E_k$ is a local norm, i.e. $E_k \cap NU_K = E_k$, and we find $\omega^0_{K/k} \simeq E_k/E_k \cap NK^\times$. Now Scholz's knot sequence implies

**Corollary 2** *Let $K/k$ be a finite unramified normal extension with Galois group $G = \mathrm{Gal}\,(K/k)$; then there is an exact sequence of abelian groups*

$$1 \longrightarrow E_k/E_k \cap NK^\times \longrightarrow \mathcal{M}(G)^\frown \longrightarrow \mathrm{Gal}\,(K_{cen}/K_{gen}) \longrightarrow 1.$$

For the applications we have in mind we do not need an explicit description of the maps in this sequence. In fact, all we use is the inequality

$$\mathrm{rank}\,\mathrm{Gal}\,(K_{cen}/K_{gen}) \ \geq\ \mathrm{rank}\,\mathcal{M}(G) - \mathrm{rank}\,E_k/E_k \cap NK^\times,$$

where we have used that $A \simeq A^\frown$ for finite abelian groups $A$.

# 4 The Reduction

Our aim is to show that imaginary quadratic number fields with cyclic $\mathrm{Cl}_2(k^1)$ must satisfy $\mathrm{Cl}_2(k) \subseteq (2, 2^m)$.

**Proposition 3** *If $k$ is an imaginary quadratic number field whose 2-class group contains a subgroup of type $(2,2,2)$, then $\mathrm{Cl}_2(k^1)$ has rank $\geq 2$.*

*Proof.* Here we only have to observe that $G = \mathrm{Gal}\,(k^1/k)$ is an abelian group with factor group $(2,2,2)$; therefore Prop. 2 guarantees that $\mathcal{M}(G)$ has $(2,2,2) = \mathcal{M}(2,2,2)$ as a homomorphic image. Now Cor. 2 shows that there exists an unramifed extension $K/k^1$ of type (2,2), proving our claim that $\mathrm{Cl}_2(k^1)$ has rank $\geq 2$.

Remark. The first author proved a special case of Prop. 3 in [1].

**Proposition 4** *If $k$ is an imaginary quadratic number field whose 2-class group contains a subgroup of type $(4,4)$, then $\mathrm{Cl}_2(k^1)$ has rank $\geq 2$.*

*Proof.* If $\mathrm{Cl}_2(k)$ has rank $\geq 3$ then the claim follows from Prop. 3. Assume therefore that $\mathrm{Cl}_2(k)$ has rank 2. Then $d = \mathrm{disc}\, k = d_1 d_2 d_3$ is the product of three prime discriminants, and since $\mathrm{Cl}_2(k)$ has full 4-rank, we must have $(d_i/p_j) = +1$ for all $i \neq j$ and $p_j \mid d_j$ (cf. Rédei-Reichardt [22] or Kaplan [12]). It was shown in [17] that these conditions imply the existence of an unramified quaternion extension of $k$. Its compositum with the unramified extension of type $(4,4)$ gives an unramified extension $K/k$ with $H = \mathrm{Gal}\,(K/k) \simeq 32.018$ (this is the $18^{th}$ group of order 32 in [23]); we observe that $H$ has Schur multiplier $\mathcal{M}(H) \simeq (2,2,2)$ (cf. [23]). Now consider $L = Kk^1$. $L$ is clearly a normal extension of $k$; let $G = \mathrm{Gal}\,(L/k)$ denote its Galois group. Let $N$ denote the normal subgroup which fixes $K$; then clearly $N \cap G' = 1$ since $L$ is the compositum of the fixed fields of $N$ and $G'$. Applying Prop. 2 we find that $\mathcal{M}(G)$ has $\mathcal{M}(G/N) = \mathcal{M}(H)$ as a homomorphic image, and in particular we see that $\mathcal{M}(G)$ has 2-rank $\geq 3$. Now Cor. 2 guarantees the existence of an unramified extension $M/L$ with a Galois group whose rank is $\geq \mathrm{rank}\,\mathcal{M}(G) - \mathrm{rank}\,(E_k/E_k \cap N_{L/k}L^\times) \geq 2$ (note that $E_k$ is cyclic). Thus we conclude that the 2-class group of $L$ is not cyclic. But this implies of course that the 2-class group of its subfield $k^1$ is not cyclic, and this was what we wanted to prove.

Taking both propositions together we find

**Corollary 3** *An imaginary quadratic number field with cyclic $\mathrm{Cl}_2(k^1)$ must satisfy $\mathrm{Cl}_2(k) \subseteq (2, 2^m)$.*

Remark. The first author has shown that if $Cl_2(k) \simeq (4,4)$, then $h_2(k^1) \geq 8$, see [2].

# 5 Results in Group Theory

Let $G$ be a group. If $x, y \in G$, then we let $[x, y] = x^{-1}y^{-1}xy$ denote the commutator of $x$ and $y$. If $A$ and $B$ are nonempty subsets of $G$, then $[A, B]$ shall denote the subgroup of $G$ generated by the set $\{[a, b] : a \in A, b \in B\}$. The lower central series $\{G_j\}$ of $G$ is defined inductively by: $G_1 = G$ and $G_{j+1} = [G, G_j]$ for $j \geq 1$. The derived series $\{G^{(n)}\}$ is defined inductively by: $G^{(1)} = G$ and $G^{(n+1)} = [G^{(n)}, G^{(n)}]$ for $n \geq 1$. Notice that $G^{(2)} = G_2 = [G, G]$ the commutator subgroup, $G'$, of $G$.

We now let $G$ be a (finite) 2-group such that $G^{ab} = G/G' \simeq (2, 2^m)$ with $m > 1$ and $G$ nonmetacyclic, i.e. there exists no normal cyclic subgroup $N$ of $G$ such that $G/N$ is cyclic. Since $G^{ab}$ has two generators, so does $G$ by the Burnside Basis Theorem. In addition, since $G$ is nonmetacyclic, we have that there exist $a, b \in G$ such that

$$a^2 \equiv b^{2^m} \equiv [a, b]^2 \equiv 1 \bmod G_0$$

where $G_0$ is the unique maximal subgroup of $G'$ normal in $G$, see [6] for details. But in the present situation, we claim that $G_0 = G_3$. For, $G' = \langle [a, b], G_3 \rangle$ (see [9]) and, moreover,

$$1 \equiv [a^2, b] = a^{-1}[a, b]a[a, b] \equiv [a, b]^2 \bmod G_3$$

(since $G_2/G_3 \subseteq Z(G/G_3)$, the center of $G/G_3$, see [9]). This establishes the claim.

**Lemma 1** *Let $G$ be a nonmetacyclic, metabelian (i.e. $G'$ abelian) 2-group such that $G^{ab} \simeq (2, 2^m)$. Let $G = \langle a, b \rangle$ with $a^2 \equiv b^{2^m} \equiv c^2 \equiv 1 \bmod G_3$ where $c = [a, b]$. Finally, let $c_2 = c$ and $c_{j+1} = [b, c_j]$ for $j > 1$. Then*

*a)* $[b, c_j^{2^k}] = c_{j+1}^{2^k}$, *for* $j \geq 2, k \geq 0$,

*b)* $[a, c_j^{2^k}] \equiv c_j^{2^{k+1}} \bmod G_{k+j+2}$, *for* $j \geq 2, k \geq 0$.

*Proof*. *a)* If $k = 0$, then result is obvious from the definition of $c_j$. Assume that $[b, c_j^{2^k}] = c_{j+1}^{2^k}$. Then $[b, c_j^{2^{k+1}}] = [b, (c_j^{2^k})^2] = [b, c_j^{2^k}]^2$, since $G'$ is abelian, and thus $[b, c_j^{2^k}]^2 = c_{j+1}^{2^{k+1}}$.

*b)* We use induction on $k$. For $k = 0$, we claim $[a, c_j] \equiv c_j^2 \bmod G_{j+2}$ for all $j \geq 2$. Let $j = 2$. Then since $a^2 \equiv 1 \bmod G_3$, we have

$$1 \equiv [a^2, b] \equiv a^{-1}c_2 a c_2 \equiv c_2[c_2, a]c_2 \bmod G_4.$$

Hence $[a, c_2] \equiv c_2^2 \bmod G_4$. Now suppose the claim is true for $j$, i.e. $[a, c_j] = c_j^2\gamma_{j+2}$ for some $\gamma_{j+2} \in G_{j+2}$. We want to show that $[a, c_{j+1}] \equiv c_{j+1}^2 \bmod G_{j+3}$. First notice that $G_2^2 \subseteq G_3$ and thus by [10], p.266, for example, $G_l^2 \subseteq G_{l+1}$ for all $l \geq 2$. In particular, $[a, c_{j+1}] \equiv [c_{j+1}, a] \bmod G_{j+3}$, since $[a, c_{j+1}] \in G_{j+2}$. By the Witt identity (c.f., e.g. [6]) $[[b, c_j], a] \equiv [[c_j, a], b] \bmod G_{j+3}$. Hence, by the induction assumption,

$$\begin{aligned} [[c_j, a], b] &= [c_j^{-2}\gamma_{j+2}^{-1}, b] = [c_j^{-2}, b][\gamma_{j+2}^{-1}, b] \\ &\equiv [c_j, b]^{-2} \equiv [b, c_j]^2 = c_{j+1}^2 \bmod G_{j+3}. \end{aligned}$$

This establishes *b)* when $k = 0$. Now suppose the result is true for $k$, i.e. $[a, c_j^{2^k}] = c_j^{2^{k+1}}\gamma_{k+j+2}$ for some $\gamma_{k+j+2} \in G_{k+j+2}$. We need to show that $[a, c_j^{2^{k+1}}] \equiv c_j^{2^{k+2}} \bmod G_{k+j+3}$. To this end,

$$[a, c_j^{2^{k+1}}] = [a, (c_j^{2^k})^2] = [a, c_j^{2^k}]^2 = c_j^{2^{k+2}}\gamma_{k+j+2}^2 \equiv c_j^{2^{k+2}} \bmod G_{k+j+3}.$$

This establishes part *b)* and thus the lemma.

**Lemma 2** *Assume all the hypotheses in Lemma 1. Then for all $j \geq 2$,*

$$G_j = \langle c_2^{2^{j-2}}, c_3^{2^{j-3}}, \cdots, c_{j-1}^2, c_j, c_{j+1}, \cdots \rangle.$$

*Proof*. We first claim that for all $j \geq 2$ that

$$G_j = \langle c_2^{2^{j-2}}, \cdots, c_{j-1}^2, c_j, G_{j+1} \rangle.$$

We prove this by induction on $j$. For $j = 2$, the claim is obvious since $G_2 = \langle c_2, G_3 \rangle$ for $G = \langle a, b \rangle$ (cf. [9]). Assume the claim is true for $j$, i.e.

$$G_j = \langle c_2^{2^{j-2}}, \cdots, c_j, G_{j+1} \rangle.$$

Then again by [9], we have

$$G_{j+1} = \langle [a, c_2^{2^{j-2}}], \cdots, [a, c_j], [b, c_2^{2^{j-2}}], \cdots, [b, c_j], G_{j+2} \rangle.$$

By the Lemma 1,

$$[a, c_j] \equiv c_j^2, [a, c_{j-1}^2] \equiv c_{j-1}^4, \cdots, [a, c_2^{2^{j-2}}] \equiv c_2^{2^{j-1}} \bmod G_{j+2},$$

and

$$[b, c_j] = c_{j+1}, [b, c_{j-1}^2] = c_j^2, \cdots, [b, c_2^{2^{j-2}}] = c_3^{2^{j-2}}.$$

This establishes the claim. But, since $G$ is nilpotent, there exists a $j$ such that $G_{j+1} = (1)$. From this, the lemma follows immediately.

**Proposition 5** *Let $G$ be a nonmetacyclic 2-group with $G^{ab} \simeq (2, 2^m)$, $m > 1$. Let $H$ and $K$ be the two maximal subgroups of $G$ such that $H/G', K/G'$ are cyclic. Then*

*$G'$ is cyclic and nonelementary*

*if, and only if,*

*$(G' : H') = 2$ and $(G' : K') > 2$ (without loss of generality).*

*Proof*. Assume the notation of the previous lemmas. Then, without loss of generality, let $H = \langle b, G' \rangle$, and $K = \langle ab, G' \rangle$.

Suppose $G'$ is cyclic and nonelementary. Hence $G' = \langle c \rangle$; but then $G_3 = \langle [ab, c], [b, c] \rangle = \langle c^2 \rangle$. Without loss of generality, assume $G_3 = \langle [b, c] \rangle = \langle c_3 \rangle$. Now $H' = \langle [b, c] \rangle = \langle c_3 \rangle$ and thus $(G' : H') = 2$. We now show that
$(G' : K') > 2$. First notice that since $G'$ is not elementary, $c^2 \neq 1$. We shall show that $K' \subseteq G_4$ from which the result follows since $(G' : G_4) = 4$. Without loss of generality, assume $G_4 = (1)$. We show $K' = (1)$. Since $G_4 = (1)$ and $G_3 = \langle c_3 \rangle = \langle c^2 \rangle$, $c_3 = c^2$. Now $K' = \langle [ab, c] \rangle$, and

$$[ab, c] = b^{-1}[a, c]bc_3 = [a, c]c_3$$

since $G_4 = (1)$ implies that $G_3 \subseteq Z(G)$, the center of $G$. But $[a, c] = c^2[b, a^2] = c^2$ because $a^2 \in G_3$. Hence, $[ab, c] = [a, c]c_3 = c^4 = 1$, as desired.

Conversely, suppose $(G' : H') = 2$ and $(G' : K') > 2$. First, assume that $G$ is metabelian. Since $(G' : H') = 2$, we see $H' = G_3$. Furthermore, since $H' = \langle c_3, c_4, \cdots \rangle$ and by Lemma 2, $G_3 = \langle c_2^2, c_3, c_4, \cdots \rangle$, we have $c_2^2 \in \langle c_3, c_4, \cdots \rangle$. From this, we claim that $c_j^{2^k} \in \langle c_{j+k}, c_{j+k+1}, \cdots \rangle$. We use induction on $k$. Let $k = 1$. Then if $j = 2$, the result follows from the above. Assume $c_j^2 \in \langle c_{j+1}, c_{j+2}, \cdots \rangle$. Hence $c_j^2 = c_{j+1}^m c_{j+2}^n \cdots$ from which $c_{j+1}^2 = [b, c_j^2] = [b, c_{j+1}^m][b, c_{j+2}^n] \cdots = c_{j+2}^m c_{j+3}^n \cdots \in \langle c_{j+2}, c_{j+3}, \cdots \rangle$. Now assume the claim for $k$, i.e. $c_j^{2^k} = c_{j+k}^m c_{j+k+1}^n \cdots$; then $c_j^{2^{k+1}} = (c_j^{2^k})^2 = (c_{j+k}^2)^m (c_{j+k+1}^2)^n \cdots \in \langle c_{j+k+1}, c_{j+k+2}, \cdots \rangle$. Hence the claim is established. From this claim and Lemma 2, we obtain

$$G_j = \langle c_j, c_{j+1}, \cdots \rangle.$$

Notice then that $(G_j : G_{j+1}) = 2$ for $j \geq 2$. Next we claim that $K' \subseteq G_4$. For first notice that since $K \lhd G$, $K' \lhd G$. Suppose $K' \not\subseteq G_4$. Then $K'G_4 \supseteq G_3$. Then by [9], Theorem 2.49ii), we see $K' \supseteq G_3$, which implies that $(G' : K') \leq (G' : G_3) = 2$ contrary to the assumption that $(G' : K') > 2$. The claim now follows. Now $K' = \langle [ab, c_2], [ab, c_3], \cdots \rangle \subseteq G_4$. Notice that (as above)

$$1 \equiv [ab, c_2] = b^{-1}[a, c_2]bc_3 \equiv [a, c_2]c_3 \bmod G_4.$$

This implies that $[a, c_2] \equiv c_3 \bmod G_4$. On the other hand,

$$1 \equiv [a^2, b] = a^{-1}c_2 a c_2 = c_2[c_2, a]c_2 \bmod G_4,$$

and this implies $[a, c_2] \equiv c_2^2 \bmod G_4$. Therefore, $c_3 \equiv c_2^2 \bmod G_4$. In particular, $c_2^2 \not\equiv 1 \bmod G_4$ since otherwise $G_3 = G_4$ which contradicts the assumption that $(G' : K') > 2$. Thus, $G'$ is not elementary. We next claim that $[a, c_2^{2^k}] \equiv c_2^{2^{k+1}} \bmod G_{k+4}$ and that $[b, c_2^{2^k}] \equiv c_2^{2^{k+1}} \bmod G_{k+4}$. For $k = 0$, then $[a, c_2] \equiv c_2^2 \bmod G_4$ and $c_3 = [b, c_2] \equiv c_2^2 \bmod G_4$ from above. Assume the claim is true for $k$. Then $[a, c_2^{2^k}] = c_2^{2^{k+1}} \gamma_{k+4}$ and $[b, c_2^{2^k}] = c_2^{2^{k+1}} \delta_{k+4}$, for some

$\gamma_{k+4}, \delta_{k+4} \in G_{k+4}$. Then $[a, c_2^{2^{k+1}}] = c_2^{2^{k+2}} \gamma_{k+4}^2 \equiv c_2^{2^{k+2}} \bmod G_{k+5}$ and similarly $[b, c_2^{2^{k+1}}] \equiv c_2^{2^{k+2}} \bmod G_{k+5}$. This establishes the claim. From this it follows that $G_j = \langle c_2^{2^{j-2}}, G_{j+1} \rangle$. As usual we use induction. It is obviously true for $j = 2$. Suppose it is true for $j$. Then $G_{j+1} = \langle [a, c_2^{2^{j-2}}], [b, c_2^{2^{j-2}}], G_{j+2} \rangle = \langle c_2^{2^{j-1}}, G_{j+2} \rangle$ by the above claim. Since for some $j$, $G_j = (1)$, it follows that $G_2 = \langle c_2 \rangle$. Thus the proposition is established for $G$ metabelian. The general case follows from the above argument applied to $G^{ab}$ which shows that $G'/G''$ is cyclic and nonelementary. But then the Burnside Basis Theorem implies that $G'$ itself is cyclic and nonelementary. Thus the proposition has been proved.

In the following proposition we show that under certain circumstances the subgroup $K$ above is abelian.

**Proposition 6** *Let $G$ be a nonmetacyclic 2-group with $G^{ab} \simeq (2, 2^m)$, $m > 1$, and such that $G'$ is cyclic and nonelementary. Let $K$ be the maximal subgroup of $G$ such that $(G' : K') > 2$, as in the previous proposition. Finally, assume that the kernel of the transfer map $V : G^{ab} \longrightarrow K^{ab}$ has order 2. Then $K$ is abelian.*

*Proof.* We assume all the previous notation. Then $G_2 = \langle c_2 \rangle$, and, more generally, $G_j = \langle c_2^{2^{j-2}} \rangle$, for $j = 2, 3, \cdots$. We have $H = \langle b, c_2 \rangle$ and $H' = \langle c_3 \rangle = G_3$, since $(G' : H') = 2$. From this it follows that $c_3 \equiv c_2^2 \bmod G_4$. Furthermore, $K = \langle ab, c_2 \rangle$ and $K' = \langle [ab, c_2] \rangle$. Let $K' = G_s = \langle c_2^{2^{s-2}} \rangle$; then $s \geq 4$, since $(G' : K') > 2$. We need to show that $K' = \langle 1 \rangle$, i.e. $c_2^{2^{s-2}} = 1$. Let $\overline{g} = gG'$ for any $g \in G$. Since $a, b \notin K$, then the transfer map is given by $V(\overline{a}) = a^2 K'$, $V(\overline{b}) = b^2 K'$, see [21] for information on transfer maps. Moreover, since $(G : K) = 2$, the exponent of the kernel of $V$ is equal to 2; and hence $\ker V \subset \{\overline{1}, \overline{a}, \overline{b}^{2^{m-1}}, \overline{a}\overline{b}^{2^{m-1}}\}$.

*Case 1*: Suppose $\overline{a} \notin \ker V$. Then $a^2 \notin K'$. However, since $a^2 \in G'$, $a^4 \in K'$. This all implies that $a^2 = c_2^{2^{s-3}} \gamma_s$ for some $\gamma_s \in G_s$. Then

$$1 = [a, a^2] = [a, c_2^{2^{s-3}} \gamma_s] = [a, c_2]^{2^{s-3}} [a, \gamma_s].$$

Thus, since $[a, c_2] \equiv c_2^2 \bmod G_4$, $1 \equiv c_2^{2^{s-2}} \bmod G_{s+1}$. This implies that $G_s = G_{s+1}$ and so $K' = G_s = \langle 1 \rangle$.

*Case 2*: Suppose $\overline{a} \in \ker V$. Then $\overline{b}^{2^{m-1}} \notin \ker V$. But then $b^{2^m} \notin K'$, whereas (as above) $b^{2^{m+1}} \in K'$. Thus $b^{2^m} = c_2^{2^{s-3}} \gamma_s$ for some $\gamma_s \in G_s$ and so

$$1 = [b, b^{2^m}] = [b, c_2]^{2^{s-3}} [b, \gamma_s] \equiv c_2^{2^{s-2}} \bmod G_{s+1},$$

since from above $[b, c_2] = c_3 \equiv c_2^2 \bmod G_4$. Therefore, $G_s$ is trivial as above. This establishes the proposition.

In the next proposition we determine the structure of the group $G$ in Proposition 6, as well as some of its subgroups and their abelianizations. First we isolate some lemmas which will be used in the proof of the proposition. We assume all the notation above.

**Lemma 3** *Suppose* $[a,b]=c, [a,c]=c^2, [ab,c]=1$; *then* $[b,c]=c^2$.

*Proof.* By the assumptions, $a^{-1}c^{-1}a = c, (ab)^{-1}c^{-1}ab = c^{-1}$ and thus $c^{-1} = b^{-1}a^{-1}c^{-1}ab = b^{-1}cb = c[b,c]^{-1}$. This implies that $[b,c]=c^2$.

**Lemma 4** *Assume the hypothesis of the previous lemma. Then*

$$(ab)^{2^l} = a^{2^l} b^{2^l} c^{2^{l-1}}, l \geq 1.$$

*Proof.* This follows by straightforward induction on $l$ once we observe that $c^{\pm 1}b = bc^{\mp 1}$ by Lemma 3.

**Lemma 5** *Assume the hypothesis of the previous lemma. Then*

$$ab^l c^s = b^l c^{-s} a, \text{ if } l \text{ is even}, \; ab^l c^s = b^l c^{-1-s} a, \text{ if } l \text{ is odd};$$

$$ba^j c^s = a^j c^{-s} b, \text{ if } j \text{ is even}, \; ba^j c^s = a^j c^{1-s} b, \text{ if } j \text{ is odd}.$$

The proof follows easily by induction on $l$ and $j$.

We now define two groups $\Gamma^j_{m,t}$ $(j=1,2)$ by their presentations

$$\begin{aligned} \Gamma^1_{m,t} &= \langle a,b : a^4 = b^{2^m} = 1, c=[a,b], a^2 = c^{2^{t-1}}, [a,c]=c^2, [ab,c]=1\rangle, \\ \Gamma^2_{m,t} &= \langle a,b : a^4 = 1, c=[a,b], a^2 = b^{2^m} = c^{2^{t-1}}, [a,c]=c^2, [ab,c]=1\rangle. \end{aligned}$$

**Proposition 7** *Let $G$ be as in Proposition 6. Assume $\sharp(G') = 2^t$, (and thus $t \geq 2$). Then $G$ has the following presentations depending on the make up of* $\ker V$*:*

*Case i)* $\ker V = \langle \bar{b}^{2^{m-1}} \rangle$. *Then* $G \simeq \Gamma^1_{m,t}$;

*Case ii)* $\ker V = \langle \bar{a}\bar{b}^{2^{m-1}} \rangle$. *Then* $G \simeq \Gamma^2_{m,t}$.

*Moreover, depending on the case given above, the structure of certain subgroups are given in the following table:*

| *subgroup* | $\simeq$ | *i)* | *ii)* |
|---|---|---|---|
| $Z(G) = \langle b^2, c^{2^{t-1}} \rangle$ | | $(2^{m-1}, 2)$ | $(2^m)$ |
| $J = \langle b^2, c \rangle$ | | $(2^{m-1}, 2^t)$ | $(2^{m-\omega}, 2^{t-1+\omega})$ |
| $K = \langle ab, c \rangle$ | | $(2^{m-\omega}, 2^{t+\omega})$ | $(2^{m-\epsilon}, 2^{t+\epsilon})$ |
| $H = \langle b, c \rangle$ | | $(2^t) \times_s (2^m)$ | $(2^t) \times_p (2^{m+1})$ |
| $M = \langle a, b^2, c \rangle$ | | $H_{2^{t+1}} \times (2^{m-1})$ | $H_{2^{t+1}} \times_{s,p} (2^{m-\omega})$ |

*In this table,* $\left\{ \begin{array}{ll} \omega = 1 & \text{if } t \geq m, \\ \omega = 0 & \text{if } t < m; \end{array} \right\}$, *and* $\left\{ \begin{array}{ll} \epsilon = 1 & \text{if } t > m, \\ \epsilon = 0 & \text{if } t = m, \\ \epsilon = -1 & \text{if } t < m. \end{array} \right\}$

*$H_l$ denotes the quaternion group of order $l$.*

*Also $\times_s$ denotes a semidirect product with the normal subgroup given on the left (as usual); $\times_p$ represents a partial direct or semidirect product. Finally $\times_{s,p}$ means $\times_s$, if $m \leq t$; and $\times_p$, if $m > t$. (See the proof below for more details.) We also note that $H^{ab} \simeq (2, 2^m)$ and $M^{ab} \simeq (2, 2, 2^{m-1})$.*

*Proof.* First of all, we verify the presentations of $G$. Consider *Case i)*. Then, as in the proof of Proposition 6, $a^2 = c^{2^{t-1}}$ and $b^{2^m} = 1$. Moreover, by definition $[a, b] = c$; by Proposition 6, $[ab, c] = 1$ since $K'$ is trivial. Finally, as in the proof of Lemma 1, since $a^2 \in Z(G)$ we have $[a, c] = c^2$. This establishes the presentation of $G$ is this first case. The other case follows in the same way. Furthermore, notice that if $\ker V = \langle \overline{a} \rangle$, then by using the presentation $\langle ab^{2^{m-1}} \rangle$ for $G$, we are reduced to *Case ii)*.

Next, we claim that $Z(G) = \langle b^2, c^{2^{t-1}} \rangle$. It is trivial to see that $Z(G) \supseteq \langle b^2, c^{2^{t-1}} \rangle$. On the other hand, suppose $z \in Z(G)$. Then $z = a^j b^l c^s$ for some nonnegative integers $j, l, s$. If $l$ is odd, then by Lemma 5 $za = az = a^j b^l c^{-1-s} a$, which implies $c$ has odd order, a contradiction. A similar argument shows that $j$ cannot be odd. Then $z \in \langle b^2, c^{2^{t-1}} \rangle$ since $a^2 \in \langle c^{2^{t-1}} \rangle$. It is also easy to see that $Z(G) \simeq (2^{m-1}, 2)$ in *Case i)*, but $Z(G) \simeq (2^m)$ in the other case.

Now consider $J = \langle b^2, c \rangle$, which is abelian since $b^2 \in Z(G)$. In *Case i)* we see that $J \simeq (2^{m-1}, 2^t)$. In the remaining case we have two possibilities: if $t \geq m$, then $J \simeq \langle b^2 c^{2^{t-m}} \rangle \times \langle c \rangle \simeq (2^{m-1}, 2^t)$; if $t < m$, then $J \simeq \langle b^2 \rangle \times \langle cb^{2^{m-t+1}} \rangle \simeq (2^m, 2^{t-1})$.

Consider $K = \langle ab, c \rangle$. Then, as already seen, $K' = \langle 1 \rangle$. In *Case i)*, suppose first that $m > t$; then $K \simeq \langle ab \rangle \times \langle c \rangle \simeq (2^m, 2^t)$. But if $m \leq t$, then $K \simeq \langle ab \rangle \times \langle b^2 c^{2^{t-m+1}} \rangle \simeq (2^{t+1}, 2^{m-1})$. In *Case ii)* we proceed in a similar way. If $m > t$, then $K \simeq \langle ab \rangle \times \langle cb^{2^{m-t+1}} \rangle \simeq (2^{m+1}, 2^{t-1})$. If $m = t$, then $K \simeq \langle ab \rangle \times \langle c \rangle \simeq (2^m, 2^t)$. Finally, if $m < t$, then $K \simeq \langle ab \rangle \times \langle b^2 c^{2^{t-m}} \rangle \simeq (2^{t+1}, 2^{m-1})$.

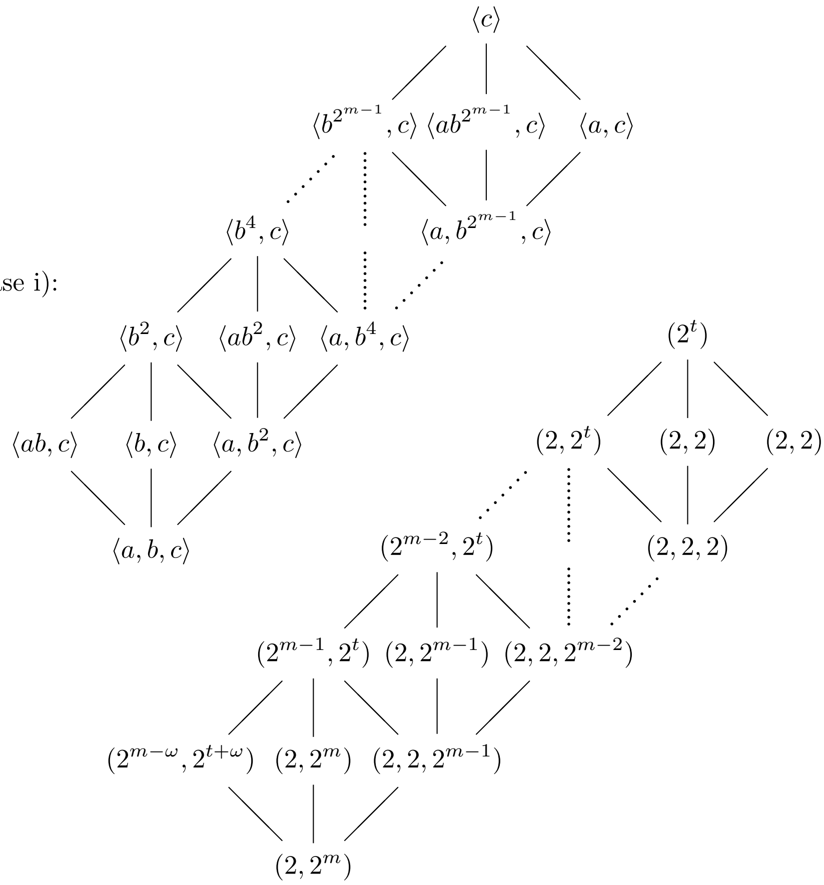
Next consider $H = \langle b, c \rangle$. Then $H' = \langle c^2 \rangle$ and thus $H^{ab} \simeq (2^m, 2)$. In the first case, $H \simeq \langle c \rangle \times_s \langle b \rangle \simeq (2^t) \times_s (2^m)$ and the action of $b$ on $c$ is given by inversion, namely, $b^{-1} c b = c^{-1}$. In the other case, $H \simeq \langle c \rangle \times_p \langle b \rangle$, the partial semidirect product of the two subgroups the intersection of $\langle c \rangle$ and $\langle b \rangle$ is $\langle c^{2^{t-1}} \rangle$ and the action of $b$ on $c$ is again given by inversion.

Finally, consider $M = \langle a, b^2, c \rangle$. Then $M' = \langle c^2 \rangle$ and thus $M^{ab} \simeq (2, 2^{m-1}, 2)$. In *Case i)* $M \simeq \langle a, c \rangle \times \langle b^2 \rangle \simeq H_{2^{t+1}} \times (2^{m-1})$. In *Case ii)* we have two possiblities. If $m \leq t$, then $M \simeq \langle a, c \rangle \times_s \langle b^2 c^{2^{t-m}} \rangle \simeq H_{2^{t+1}} \times_s (2^{m-1})$, a semidirect product; if $m > t$, then $M \simeq \langle a, c \rangle \times_p \langle b^2 \rangle \simeq H_{2^{t+1}} \times_p (2^m)$.

All this establishes the proposition.

The following diagrams give the subgroups of $G$ containing $\langle c \rangle$ (these are the groups fixing the subfields $L$ of $k^1/k$) as well as their abelianization type, which are isomorphic to the 2-class groups of these fields $L$.

Case i):




The situation in case ii) is similar: the diagrams of subgroups is the same, and the abelianization types can differ only for the chain of subgroups $\langle ab, c\rangle \subset \langle b^2, c\rangle \subset \ldots \subset \langle c\rangle$. The abelianization type for $\langle ab, c\rangle$ is given in Prop. 7, for the other groups we have

$$\langle b^{2^j}, c\rangle^{ab} \simeq \begin{cases} (2^{m-j+1}, 2^{t-1}) & \text{if} \quad j \le m-t+1 \\ (2^{m-j}, 2^t) & \text{if} \quad j \ge m-t+1 \end{cases}.$$

**Remark.** In [4] we proved that the 2-class field tower of a number field $k$ is abelian if $\mathrm{Cl}_2(k)$ has rank $\le 2$ and if there exists a quadratic unramified extension $K/k$ such that $h_2(K) = \frac{1}{2}h_2(k)$. The diagram shows (consider the fixed fields of $\langle a, b^2, c\rangle$ and $\langle ab^2, c\rangle$) that this fails to hold if $\operatorname{rank} \mathrm{Cl}_2(k) \ge 3$, even if the 2-class number *and* the 2-rank become smaller.

# 6 The 2-Class Field Tower

Armed with the proposition in the previous section, we come to the main result of this note. We determine those imaginary quadratic fields $k$ such that $\mathrm{Cl}_2(k^1)$ is cyclic. We start by translating Prop. 5 into the field theoretical language:

**Proposition 8** *Let $k$ be a number field such that $\mathrm{Cl}_2(k) \simeq (2, 2^m)$, and assume that $\mathrm{Gal}(k^2/k)$ is nonmetacyclic. Let $K_1$ and $K_2$ be the two quadratic unramified extensions of $k$ such that $N_{K_i/k}\mathrm{Cl}_2(K_i)$ is cyclic. Then $\mathrm{Cl}_2(k^1)$ is cyclic if and only if $h_2(K_1) = h_2(k)$ and $h_2(K_2) > h_2(k)$ (or vice versa).*

Now we claim

**Theorem 3** *Let $k$ be an imaginary quadratic number field with discriminant $d_k$. Let $G = \mathrm{Gal}(k^2/k)$ (recall then that $G' \simeq \mathrm{Cl}_2(k^1)$ and $G/G' \simeq \mathrm{Cl}_2(k)$). Then $G$ is nonmetacyclic and $G'$ is cyclic if, and only if, $d_k = d_1d_2d_3$ where $d_j$ are prime discriminants satisfying*

*i)* $d_1 < 0$, $d_2 > 0, d_3 > 0$,

*ii)* $(d_3/p_1) = (d_3/d_2) = -(d_2/p_1) = 1$, *where $p_1$ is the prime dividing $d_1$;*

*iii)* $(d_3/d_2)_4(d_2/d_3)_4 = -1$.

*Moreover, $G = \Gamma^1_{m,t}$ if $d_1 = -4$, and $G = \Gamma^2_{m,t}$ if $d_1 \neq -4$.*

*Proof*. Suppose $G$ is nonmetacyclic and $G'$ is cyclic; then $G \simeq (2, 2^m)$ for some $m > 1$ (use Cor. 3 and the fact that $m = 1$ only occurs for dihedral, semidihedral od quaternionic 2-groups, all of which are metacyclic). Then *i)* and *ii)* follow from the Tables and Lemma 4 of [3]. Moreover, by [3] $N(\epsilon_{d_2d_3}) = 1$, where $\epsilon_{d_2d_3}$ denotes a fundamental unit of $\mathbb{Q}(\sqrt{\nvDash\nvDash})$ and $N$ the norm from $\mathbb{Q}(\sqrt{\nvDash\nvDash})$ to $\mathbb{Q}$. Now consider $K_j = k(\sqrt{d_j})$ for $j = 1, 2, 3$. Let $H_j = \mathrm{Gal}(k^2/K_j)$ for $j = 1, 2, 3$. Then $H_j/G'$ is cyclic for $j = 1, 2$, whereas $H_3/G'$ is not, cf. [3]. Let $h_2(m)$ denote the 2-class number of the quadratic number field $\mathbb{Q}(\sqrt{>})$; then the 2-class numbers of $K_1$ and $K_2$ are given by

$$h_2(K_1) = \frac{1}{2} q(K_1) h_2(d_2d_3) h_2(d_1) h_2(k),$$

$$h_2(K_2) = \frac{1}{2} q(K_2) h_2(d_2) h_2(d_1d_3) h_2(k),$$

where $q(K_j)$ denotes the unit index of $K_j/\mathbb{Q}$, see [15] for details. But then $h_2(K_1) = 2^m h_2(d_2d_3)$ and $h_2(K_2) = 2^m h_2(d_1d_3)$, since, for example, by [18] (Example 4, p. 352), $q(K_j) = 1$, and also $h_2(d_1) = h_2(d_2) = 1$. Thus $h_2(d_2d_3) = (G' : H_1')$ and $h_2(d_1d_3) = (G' : H_2')$. By Proposition 8, we have $h_2(d_2d_3) = 2$ or $h_2(d_1d_3) = 2$. Since $4 \mid h_2(d_1d_3)$ (cf. [12]), we conclude that $h_2(d_2d_3) = 2$. But then *iii)* follows since $h_2(d_2d_3) = 2$ and $N(\epsilon_{d_2d_3}) = 1$ is equivalent to

$(d_2/d_3)_4(d_3/d_2)_4 = -1$, see, for example, [12].

The converse follows immediately from Proposition 8, since $G/G' \simeq (2, 2^m)$, $m > 1$, and $G$ is nonmetacyclic satisfying the conditions of the proposition (see [3]). This establishes the first part of the theorem.

In order to prove the presentation of $G$ we observe that we are in case i) of Prop. 7 if and only if the nontrivial ideal class capitulating in $K_2/k$ is a square. Now $c = [(d_2, \sqrt{d})]$ becomes principal in $K_2$, and $c$ is a square in $\mathrm{Cl}_2(k)$ if and only if the prime $d_2$ splits completely in $k_{gen}/k$, i.e. if and only if $(d_1/d_2) = (d_3/d_2) = +1$. Since $(d_2/p_1) = -1$, the first condition holds if and only if $d_1 = -4$, whereas the second condition is part of our assumptions.

Finally we summarize our knowledge on the Galois groups of 2-class field towers of imaginary quadratic number fields in Table 1 below. It contains results of Furtwängler [7], Kisilevsky [14], and the authors [3, 19].

The groups occuring in Table 1 have the following presentations ($-1$ always denotes a central involution, i.e. an element of order 2 contained in the center of the group):

| group | presentation | order |
|---|---|---|
| $D_m$ | $\langle a, b : a^m = b^2 = 1,\ [a, b] = a^{-2}\rangle$ | 2m |
| $H_{4m}$ | $\langle a, b : a^m = b^2 = -1,\ [a, b] = a^{-2}\rangle$ | 4m |
| $SD_{4m}$ | $\langle a, b : a^{2m} = b^2 = 1,\ [a, b] = a^{m-2}\rangle$ | 4m |
| $M_{4m}$ | $\langle a, b : a^m = b^2 = -1,\ [a, b] = -1\rangle$ | 4m |
| $\mathrm{MC}_m^-$ | $\langle a, b : b^{2^{m+1}} = 1, a^4 = b^{2^m},\ a^{-1}ba = b^{-1}\rangle$ | $2^{m+3}$ |
| $\mathrm{MC}_{m,t}^+$ | $\langle a, b : a^{2^{t+1}} = b^{2^m} = 1,\ b^{-1}ab = a^{-1}\rangle$ | $2^{m+t+1}$ |
| $\Gamma^1_{m,t}$ | $\langle a, b : a^4 = b^{2^m} = 1,\ c = [a, b],$ $a^2 = c^{2^{t-1}},\ [a, c] = c^2,\ [ab, c] = 1\rangle$ | $2^{m+t+1}$ |
| $\Gamma^2_{m,t}$ | $\langle a, b : a^4 = b^{2^{m+1}} = 1,\ c = [a, b],$ $a^2 = b^{2^m} = c^{2^{t-1}},\ [a, c] = c^2,\ [ab, c] = 1\rangle$ | $2^{m+t+1}$ |

In Table 1, $p$ and $p'$ represent positive prime discriminants, whereas $r$ denotes a negative prime discriminant $\neq -4$. Moreover, $d < 0$ prime stands for $d$ is a negative prime discriminant, and all factors (e.g. in $-rpp'$) are assumed to be relatively prime.

Table 1:

| disc $k$ | conditions | G | |
|---|---|---|---|
| $d$ | $d < 0$ prime | 1 | |
| $dd'$ | $d < 0$, $d' > 0$ prime, | $(2^m)$ | $2^m = h_2(k)$ |
| $dd'd''$ | $d, d', d'' < 0$ prime | $(2, 2^m)$ | $2^m = h_2(k)/2$ |
| $-rpp'$ | $(p/p') = (r/p) = (r/p') = -1$ | $H_8$ | |
| $-rpp'$ | $(p/p') = 1, (r/p) = (r/p') = -1$<br>$N\varepsilon_{pp'} = +1$ | $D_m$,<br>$m \geq 4$ | $m = 2h_2(pp')$ |
| $-rpp'$<br><br>$-rpp'$ | $(p/p') = 1, (r/p) = (r/p') = -1,$<br>$N\varepsilon_{pp'} = -1$<br>$(r/p) = +1$, $(p/p') = (r/p') = -1$ | $H_m$,<br>$m \geq 16$ | $m = 4h_2(pp')$<br><br>$m = 4h_2(-rp)$ |
| $-4pp'$ | $(p/p') = -1$, $p \equiv 1$, $p' \equiv 5 \bmod 8$ | $SD_m$ | $m = 4h_2(-4p)$ |
| $-4pp'$ | $p \equiv p' \equiv 5 \bmod 8, (p/p') = -1$ | $M_{4m}$ | $m = h_2(k)/2$ |
| $-4pp'$ | $p \equiv p' \equiv 5 \bmod 8, (p/p') = +1$<br>$N\varepsilon_{pp'} = -1$ | $\mathrm{MC}^{-}_{m}$ | $2^m = h_2(pp')$ |
| $-4pp'$ | $p \equiv p' \equiv 5 \bmod 8, (p/p') = +1,$<br>$N\varepsilon_{pp'} = +1$ | $\mathrm{MC}^{+}_{m,t}$ | $2^m = h_2(k)/2$<br>$2^t = h_2(pp')$ |
| $-4pp'$ | $p \equiv 1, p' \equiv 5 \bmod 8,$<br>$(p/p') = +1, (p/p')_4(p'/p)_4 = -1$ | $\Gamma^1_{m,t}$ | $2^m = h_2(k)/2$<br>$2^t = h_2(-4p)$ |
| $-rpp'$ | $(p/p') = (r/p) = 1,$<br>$(r/p') = (p/p')_4(p'/p)_4 = -1$ | $\Gamma^2_{m,t}$ | $2^m = h_2(k)/2$<br>$2^t = h_2(-rp)$ |

# References


[1] E. Benjamin, *Remarks Concerning the* 2*-Hilbert Class Field of Imaginary Quadratic Number Fields*, Bull. Austral. Math. Soc., **48** (1993), 379-383; Corrigenda, **50** (1994), 351–352.

[2] E. Benjamin, *Lower Bounds on the* 2*-Class Number of the Hilbert* 2*-Class Field of Quadratic Number Fields with* 2*-Class Number Greater than or Equal to* 16, Preprint (1996).

[3] E. Benjamin, C. Snyder, *Number Fields with* 2*-Class Group Isomorphic to* $(2, 2^m)$, Preprint (1993).

[4] E. Benjamin, F. Lemmermeyer, C. Snyder, *Real Quadratic Fields with Abelian* 2*-Class Field Tower*, submitted.

[5] N. Blackburn, *On Prime-Power Groups in which the Derived Group has Two Generators*, Proc. Cambridge Phil. Soc. **53** (1957), 19-27.

[6] N. Blackburn, *On Prime Power Groups with Two Generators*, Proc. Cambridge Phil. Soc. **54** (1958), 327-337.

[7] Ph. Furtwängler, *Über das Verhalten der Ideale des Grundkörpers im Klassenkörper*, Monatsh. Math. Phys. **27** (1916), 1–15.

[8] M. Hall, J. K. Senior, *The groups of order* $2^n$ $(n \le 6)$, Macmillan, New York 1964.

[9] P. Hall, *A Contribution to the Theory of Groups of Prime Power Order*, Proc. London Math. Soc. **36** (1933), 29-95.

[10] B. Huppert, *Endliche Gruppen I*, Springer Verlag, Heidelberg, 1967.

[11] W. Jehne, *On knots in algebraic number theory*, J. Reine Angew. Math. **311/312** (1979), 215–254.

[12] P. Kaplan, *Sur le* 2*-groupe des classes d'idéaux des corps quadratiques*, J. reine angew. Math. **283/284** (1974), 313–363.

[13] G. Karpilovsky, *Schur Multipliers* London Math. Soc. Monographs, Oxford, 1987.

[14] H. Kisilevsky, *Number Fields with Class Number Congruent to* 4 *mod* 8 *and Hilbert's Theorem* 94, J. Number Theory **8** (1976), 271-279.

[15] T. Kubota, *Über den bizyklischen biquadratischen Zahlkörper*, Nagoya Math. J. **10** (1956), 65-85.

[16] F. Lemmermeyer, *Hilbert Class Fields*, preprint Heidelberg 1996.

[17] F. Lemmermeyer, *Unramified quaternion extensions of quadratic number fields*, submitted.

[18] F. Lemmermeyer, *Ideal Class Groups of Cyclotomic Number Fields*, Acta Arith. **72.4** (1995), 347–359.

[19] F. Lemmermeyer, *On* 2*-Class Field Towers of Imaginary Quadratic Number Fields*, J. Théor. Nombres Bordeaux **6** (1994), 261–272.

[20] F. Lorenz, *Algebraische Zahlentheorie*, Bibl. Inst. Mannheim, 1993

[21] K. Miyake, *Algebraic investigations of Hilbert's Theorem* 94*, the principal ideal theorem and the capitulation problem*, Expo. Math. **7** (1989), 289–346.

[22] L. Rédei, H. Reichardt, *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. **170** (1933), 69–74

[23] T. W. Sag, J. Wamsley, *Minimal presentations for groups of order* $2^n$*,* $n \le 6$, J. Austral. Math. Soc. **15** (1973), 461–469.

[24] A. Scholz, *Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelscher Körpererweiterungen I*, J. Reine Angew. Math. **175** (1936), 100-107.

[25] A. Scholz, *Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelscher Körpererweiterungen II*, J. Reine Angew. Math. **182** (1940), 217–234.

[26] I. Schur, *Untersuchungen über die Darstellungen der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. Reine Angew. Math. **132** (1907), 85–137.

[27] J.-P. Serre, *Sur une question d'Olga Taussky*, J. Number Theory **2** (1970), 235–236; see also Œuvres II, 540–541.

[28] J. Tate, *Global Class Field Theory*, Algebraic Number Theory (Cassels, Fröhlich, eds.), London 1967, 162–203.

[29] O. Taussky, *A Remark on the Class Field Tower*, J. London Math. Soc. **12** (1937), 82-85.

[30] J. Wiegold, *The Schur multiplier: an elementary approach*, in Groups: St. Andrews 1981, LMS Lecture Note Series (C. M. Campbell, E. F. Robertson eds.) **71** Cambridge Univ. Press (1982), 137–154.