The Narrow 2-Class Field Tower of

Some Real Quadratic Number Fields with

2-Class Group Isomorphic to Z/2Z X Z/2Z

by **Elliot Benjamin**

(based upon joint work with **Chip Snyder**)

Let k be an algebraic number field. We define k^1 to be the Hilbert 2-class field of k, which is the maximal abelian unramified extension of k such that the degree of k^1 over k is a power of 2. Similarly, we define k^2 to be the Hilbert 2-class field of k^1. We let $C_2(k)$ denote the 2-class group of k, $G = Gal(k^2/k)$, and G' be the commutator subgroup of G. Then

$$G/G' \simeq Gal(k^1/k),\ G' \simeq Gal(k^2/k^1),$$

and from class field theory we know that

$$C_2(k) \simeq Gal(k^1/k) \text{ and } C_2(k^1) \simeq Gal(k^2/k^1).$$

We define the 2-class field tower of k to be the sequence $k^0 = k \subseteq k^1 \subseteq k^2 \subseteq . . . \subseteq k^i \subseteq k^{i+1} \subseteq . . .$ where k^{i+1} is the Hilbert 2-class field of k^i, for any positive integer i. If $k^n = k^{n+1}$ for some positive integer n with n minimal, then the sequence ends at k^n and we say that the tower has finite length n.

If not we say that k has infinite 2-class field tower length. Analogously, we can define the standard class field tower of k without any restrictions on the degree of k^1 over k, and the p-class field tower of k for any prime p, such that the degree of k^1 over k is a power of p. All these class fields have been studied extensively. We define k_+^1 to be the narrow Hilbert 2-class field of k, which is the maximal abelian extension of k that is unramified at the finite prime ideals of k, with the degree of k_+^1 over k a power of 2. Thus there may be ramification from k to k_+^1 at the infinite real primes of k. We define the narrow 2-class field tower of k as follows: $k_+^0 = k \subseteq k_+^1 \subseteq k_+^2 \subseteq . . . \subseteq k_+^i \subseteq k_+^{i+1} \subseteq . . .$, analogously to the definition of the 2-class field tower of k. Furthermore, we define

the narrow 2-class group of k, $C_2^+(k)$, to be the 2-Sylow subgroup of the ideals in the ring of algebraic integers of k mod its principal ideals generated by totally positive elements. Denoting $G_+ = Gal(k_+^2/k)$ we obtain (again with the above generalizations) that $G_+/G_+^1 \simeq Gal(k_+^1/k) \simeq C_2^+(k)$, and $G_+^1 \simeq Gal(k_+^2/k_+^1) \simeq C_2^+(k_+^1)$.

We now let $k = Q(\sqrt{d})$ be a real quadratic number field with $d > 0$ square-free, such that $C_2(k) \simeq Z/2Z \times Z/2Z$ (which we denote as (2, 2), etc). We observe that $C_2^+(k_+^1) = C_2(k_+^1)$ since k_+^1 is totally imaginary, and we utilize the following notation.

--ε is the fundamental unit of k

--N(ε) denotes the norm of ε from k to the rational numbers Q

--t denotes the length of the narrow 2-class field tower of k

--"rank" refers to the minimal number of generators.

We have the following narrow 2-class group results.

1) If $N(\varepsilon) = -1$ then $C_2(k) = C_2^+(k) = (2, 2)$ and $t = 1$ or 2.

2) If $N(\varepsilon) = 1$ and d is a sum of two squares, then $C_2^+(k) = (2, 4)$.

3) If $N(\varepsilon) = 1$ and d is not a sum of two squares (i.e., d is divisible by a prime $q \equiv 3 \mod 4$), then $C_2^+(k) = (2, 2, 2)$.

When $N(\varepsilon) = -1$, since $C_2^+(k)$ (resp. $C_2(k)$) $= (2, 2)$, from group theory we know G_+ (resp. G) is dihedral, semidihedral, quaternion, or abelian and consequently G_+' (resp. G') is cyclic.

Couture & Derhem (1992) have determined completely the above types of G and G_+ in this case.

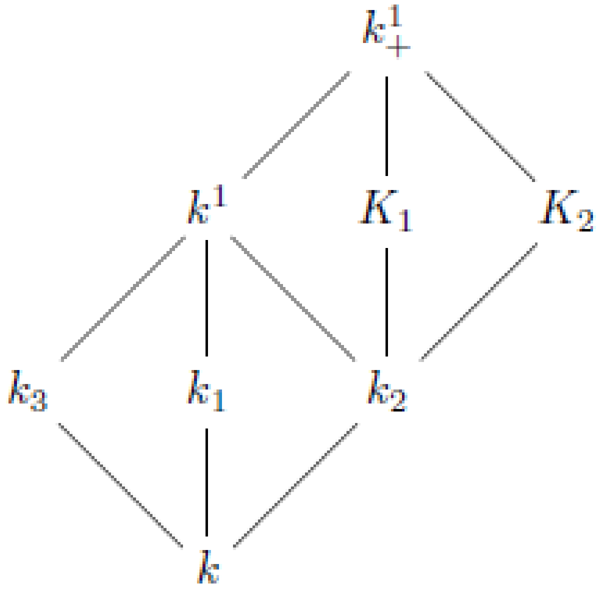
However, in the case when $N(\varepsilon) = 1$, although the type of G has been completely determined (Couture & Derhem, 1992; Benjamin & Snyder, 1995) neither G_+ nor t has been determined. In this talk we focus on the case when $N(\varepsilon) = 1$ and d is a sum of two squares, and we state the following main result.

Theorem (Benjamin & Snyder, to appear)**:**

Let k be a real quadratic number field with discriminant $d_k = d_1.d_2.d_3$ for positive prime discriminants d_j such that $C_2(k) = (2, 2)$ and $N(\varepsilon) = 1$, which all implies (wlog) that the Kronecker symbols $(d_1/d_2) = (d_2/d_3) = 1$, $(d_1/d_3) = -1$, and biquadratic residue symbols $(d_1/d_2)_4.(d_2/d_1)_4 = -1$, and $(d_2/d_3)_4.(d_3/d_2)_4 = 1$. If $(d_2/d_3)_4 = -1$ then $\mathrm{rank}(C_2(k_+^1)) = 2$ and $t = 2$.

If $(d_2/d_3)_4 = 1$ then $\mathrm{rank}(C_2(k_+^1)) = 3$ and $t \geq 3$. Furthermore, $C_2(k_+^1)$ is not elementary.

Rough Sketch of Proof: We first note that if $\mathrm{rank}(C_2(k_+^1) = 2$ then it is immediate by group theory that $t = 2$ (Blackburn, 1957). Let $k_i = k(\sqrt{d_i})$, $i = 1, 2, 3$, be the three unramified quadratic extensions of k. We know there are two cyclic quartic extensions of k that are unramified outside of ∞, which we denote as K_1 and K_2, and that $k_2 \subseteq K_i \subseteq k_+^1$, $i = 1, 2$. We have the following diagram:



k_+^1
k^1
K_1
K_2
k_3
k_1
k_2
k

To obtain our results for rank($C_2(k_+^1)$) we make use of the following table from Benjamin & Snyder (2019), where h_2^+ ( ) denotes the narrow 2-class number, and $C_2(K_i) = C_2^+(K_i)$ since K_i is totally imaginary.

Row	$h_2^+(k_2)$	$h_2^+(k_\mu)$	$h_2^+(k_\nu)$	$h_2^+(k^1)$	$C_2(K_i)$	$C_2(K_j)$	$C_2(k_+^1)$
1	$=4$	$=4$	$=4$	$=2$	(2)	(2)	$\simeq (1)$
2	$=8$	$=8$	$=8$	$=4$	$\# = 4$	$\# = 4$	$\simeq (2)$
3	≥ 16	$=8$	$=8$	≥ 8	$\# \geq 4$	$\# \geq 4$	$\simeq (4^*)$
4	$=8$	$=8$	≥ 16	≥ 8	$\# \geq 4$	$\# \geq 4$	$\simeq (4^*)$
5	$=8$	≥ 16	≥ 16	≥ 8	$\# = 8$	$\# = 8$	$d = 2$
6	$=8$	≥ 16	≥ 16	≥ 8	$\# \geq 16$	$\# \geq 16$	$d = 3$
7	$=8$	$=8$	$=8$	≥ 8	$\# = 8$	$\# = 8$	$\simeq (2,2)$
8	$=8$	$=8$	$=8$	≥ 8	$\simeq (2,4)$	$\# \geq 16$	$d = 3$
9	$=8$	$=8$	$=8$	≥ 8	$\simeq (2,2,2)$	$\# \geq 16$	$d = 2$

We use the Kuroda Class Number Formula, the Ambiguous Class Number Formula, and Capitulation theory to establish the following four results to show that if $(d_2/d_3)_4 = -1$ then we are in Row 9 of our table and therefore $\text{rank}(C_2(k_+^1)) = 2$; if $(d_2/d_3)_4 = 1$ then we are in Row 6 of our table and thus $\text{rank}(C_2(k_+^1)) = 3$.

1) $h_2^+(k_2) = 8$, $h_2^+(k_3) = 8$ or 16 (depending on the values of some relative norms of units), and if $(d_2/d_3)_4 = -1$ then $h_2^+(k_1) = 8$; if $(d_2/d_3)_4 = 1$ then $h_2^+(k_1) \geq 16$

2) $h_2^+(k_1) \equiv h_2^+(k_3) \bmod 16$

3) $h_2(K_1) \geq 16$ or $h_2(K_2) \geq 16$; consequently $h_2(k_+^1) \geq 8$

4) $h_2^+(k^1) \geq 8$

5) If $(d_2/d_3)_4 = -1$ and $h_2(K_i) = 8$ then $C_2(K_i) = (2, 2, 2)$

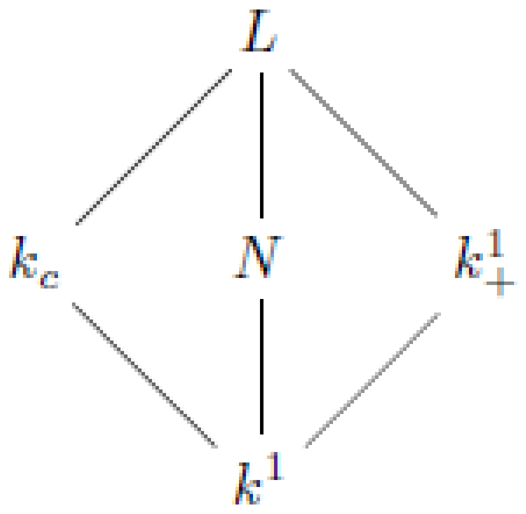
If $(d_2/d_3)_4 = -1$ then since rank$(C_2(k_+^1)) = 2$ we know by Result 3 that $C_2(k_+^1)$ is not elementary.

If $(d_2/d_3)_4 = 1$ then we show that $(k^2. K_+^1)/k_+^1$ is a cyclic extension of k_+^1 in k_+^2 of degree ≥ 4, and therefore $C_2(k_+^1)$ is not elementary. To prove that if rank$(C_2(k_+^1)) = 3$ then $t \geq 3$, we make use of the following formulation and subsequent results, where ε_{12} is the fundamental unit of $Q(\sqrt{(d_1 d_2)}) = F_{12}$.

Since $(d_1/d_2)_4 \neq (d_2/d_1)_4$ we know that $h_2^+(F_{12}) = 4$ and $N(\varepsilon_{12}) = 1$ (Scholz, 1934). Furthermore, $(F_{12})_+^1 = F_{12}(\sqrt{a})$ where $a = x+y\sqrt{d_2}$ for some half-integers $x, y, z \in ((½)Z)^3$ satisfying $x^2 - y^2d_2 - z^2d_1 = 0$, and such that $a \in O(F_2)$ (the ring of algebraic integers in $F_2 = Q(\sqrt{d_2})$) and is not divisible in $O(F_2)$ by any rational prime (Lemmermeyer, 1995).

We let k_c be the fixed field of the third term G_3 in the lower central series of $G = Gal(k^2/k)$. Then k_c is the unramified (everywhere) quadratic extension of k^1.

We let L be the compositum $k_c.k_+^1$ of k_c with k_+^1. Then L/k^1 is a V_4 extension unramified outside ∞, and thus $L \subseteq k_+^2$. This implies that there is a third quadratic extension of k^1 in L, which we refer to as N. We have the following diagram.


L
k_c
N
k^1_+
k^1

We show that when $(d_2/d_3)_4 = 1$, $h_2(L) \geq 2h_2(k_+^1)$, which implies that k_+^2 is not contained in L^1 and consequently that $t \geq 3$.

To prove this we make use of the following three results, which we obtained through applications of the Kuroda Class Number Formula, the Ambiguous Class Number Formula, and Kummer extensions, where

$F = Q(\sqrt{(d_3 a)})$ and we are assuming that $(d_2/d_3)_4 = 1$.

5) $h_2(L)/h_2(k_+^1) = h_2(N)/8h_2(k^1)$

6) $h_2(N)/h_2(k^1) = ((½)h_2(F))^2$

7) $h_2(F) \geq 8$

Thus our calculations are reduced to the 2-class number of a quartic extension of Q.

The following examples were obtained with the help of pari, utilizing our above formulations applied to any finitely unramified cyclic quartic extension of a quadratic number field (Lemmermeryer, 1995).

Example 1: $k = Q(\sqrt{1885})$, $d_k = d_1.d_2.d_3$ where $d_1 = 13$, $d_2 = 29$, and $d_3 = 5$. The fundamental unit $\varepsilon_k = 521+12\sqrt{1885}$ and $N(\varepsilon_k) = 1$

We have $(13/5) = -1$, $(29/13) = (29/5) = 1$, $(13/29)_4.(29/13)_4 = -1$, $(29/5)_4.(5/29)_4 = 1$, and $(29/5)_4 = -1$. We obtain $k_+^1 = Q(\sqrt{13}, \sqrt{5}, \sqrt{(-23+4\sqrt{29})})$. By our theorem, we conclude that $rank(C_2(k_+^1)) = 2$, and by pari we found that $C_2(k_+^1) = (4, 8)$.

Example 2: $k = Q(\sqrt{2938})$, $d_k = d_1.d_2.d_3$ where $d_1 = 13$, $d_2 = 113$, and $d_3 = 8$. $\varepsilon_k = 786707+14514\sqrt{1885}$ and $N(\varepsilon_k) = 1$, $(13/8) = -1$, $(113/8) = (113/13) = 1$,

$(13/113)_4.(113/13)_4 = -1$, $(113/8)_4.(8/113)_4 = 1$, and $(113/8)_4 = 1$. We obtain $k_+^1 = Q(\sqrt{13}, \sqrt{2}, \sqrt{(-23+\sqrt{113})})$.

By our theorem, we conclude that $\mathrm{rank}(C_2(k_+^1)) = 3$, and by pari we found that $C_2(k_+^1) = (4, 4, 4)$.

Remark: By our theorem we also know that since $C_2(k_+^1)$ is not elementary, if $(d_2/d_3)_4 = -1$ then $h_2(k_+^1) \geq 8$, and if $(d_2/d_3)_4 = 1$ then $h_2(k_+^1) \geq 16$. However, notice that in Example 1 we obtained the result that $h_2(k_+^1) = 32$ and in Example 2 we obtained the result that $h_2(k_+^1) = 64$. These greater narrow 2-class numbers as lower bounds for k_+^1 are consistent with all our heuristic investigations (Benjamin, 2019).

Open Question: We note that although our theorem distinguishes between $t = 2$ and $t \geq 3$, it does not distinguish between finite narrow 2-class field tower length and infinite 2-class field tower length, and we thus leave this as an open question.

References

1) E. Benjamin, Some 2-Class Groups Related to the Narrow 2-Class Field of Some Real Quadratic Number Fields: A Preliminary Heuristic Investigation, *Pinnacle Mathematics & Computer Science*, *3*(1), (2019), 1422-1428.

2) E. Benjamin & C. Snyder, Real Quadratic Number Fields with 2-Class Groups of Type (2, 2), *Math. Scan.*, *70*, (1995), 161-178.

3) E. Benjamin & C. Snyder, Classification of Metabelian 2-Groups G with $G^{ab} \approx (2, 2^n)$, $n \geq 2$, and Rank d(G') = 2; Applications to Real Quadratic Number Fields, Journal of Pure and Applied Algebra, 223(1), (2019), 108-130.

4) E. Benjamin, & C. Snyder, The Narrow 2-Class Field Tower of Some Real Quadratic Number Fields, *Acta Arithmetica* (to appear).

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

6) R. Couture & A. Derhem, Un Problem de Capitulation, C. R. Acad. Sci. Paris, 314 Serie 1. (1992), 785-788.

7) Lemmermeyer, Die Konstruktion von Klassenkoerpern, Diss. Univ. Heilderberg (1995).

8) A. Scholz, Ueber die Losbarkeit der Gleichung $t^2 - Du^2 = 4$, *Math. Z.*, *39,* (1934), 95-111.