

# ON HILBERT 2-CLASS FIELDS AND 2-TOWERS OF IMAGINARY QUADRATIC NUMBER FIELDS

VICTOR Y. WANG

**ABSTRACT.** Inspired by the Odlyzko root discriminant and Golod–Shafarevich  $p$ -group bounds, Martinet (1978) asked whether an imaginary quadratic number field  $K/\mathbb{Q}$  must always have an infinite Hilbert 2-class field tower when the class group of  $K$  has 2-rank 4, or equivalently when the discriminant of  $K$  has 5 prime factors. No negative results are known. Benjamin (2001, 2002) and Sueyoshi (2004, 2009, 2010) systematically established infinite 2-towers for many  $K$  in question, by casework on the associated Rédei matrices. Others, notably Mouhib (2010), have also made progress, but still many cases remain open, especially when the class group of  $K$  has small 4-rank.

Recently, Benjamin (2015) made partial progress on several of these open matrices when the class group of  $K$  has 4-rank 1 or 2. In this paper, we partially address many open cases when the 4-rank is 0 or 2, affirmatively answering some questions of Benjamin. We then investigate barriers to our methods and ask an extension question (of independent interest) in this direction. Finally, we suggest places where speculative refinements of Golod–Shafarevich or group classification methods might overcome the “near miss” inadequacies in current methods.

## 1. INTRODUCTION

We first review some notation and background, and then outline our paper in Section 1.4.

**1.1. Rank, field inclusion, class group, and Hilbert class field notation.** For a prime power  $p^i > 1$  and a finitely generated abelian group  $A$ , let  $d_{p^i}(A) := \dim_{\mathbb{F}_p} A^{p^{i-1}}/A^{p^i} < \infty$  (which we will often abbreviate as  $d_{p^i}A$  for convenience) denote the (generalized)  $p^i$ -rank.

For fields  $F$  and  $E$ , we mean by  $F \leq E$  (or  $E \geq F$ ) the existence of a field embedding  $F \hookrightarrow E$ .

Given a number field  $K$ , let  $\text{Cl}(K)$  and  $\text{Cl}^+(K)$  denote the *wide* and *narrow* (or *strict*) ideal class groups, respectively. Specifically, let  $I_K$  denote its group of nonzero fractional ideals,  $P_K$  the subgroup of principal fractional ideals in  $I_K$ , and  $P_K^+$  the subgroup of *totally positive* fractional ideals in  $P_K$ . Then recall  $\text{Cl}(K) := I_K/P_K$  and  $\text{Cl}^+(K) := I_K/P_K^+$ . The notions coincide when  $K$  is totally imaginary, but in general, we only know that  $\text{Cl}(K)$  is the quotient  $\text{Cl}^+(K)/[P_K/P_K^+]$  of  $\text{Cl}^+(K)$ . In particular, if  $K/\mathbb{Q}$  is quadratic, then  $[P_K : P_K^+]$  equals 1 if and only if  $K$  is imaginary or  $x^2 - \Delta_K y^2 = -4$  has an integer solution; otherwise

---

*Date:* November 10, 2015.

*2010 Mathematics Subject Classification.* 11R37, 11R29, 11R32, 11R11, 11R27.

*Key words and phrases.* Hilbert 2-class field tower; 2-class group; Rédei matrix; class field theory; Golod–Shafarevich inequality.

v3: incorporated final referee suggestions and corrections; shorter version to appear as J. Number Theory 160 (2016), 492–515. v2: switched to unmarked formatting option in `versions.sty`, for better readability; now 24 pages. v1: Version for the arXiv, with 25 pages. Shorter version with 19 pages (currently available at <https://www.overleaf.com/read/rcfjpsqrxvgt>), with fewer details and SAGE code examples. Comments welcome on either.

it equals 2 (a sufficient, but not necessary, criterion being that  $\Delta_K$  has a 3 (mod 4) prime divisor).

Let  $K^1$  (resp.  $K_+^1$ ) be the (resp. *narrow*) *Hilbert class field* of a number field  $K$ , i.e. the maximal abelian extension of  $K$  unramified everywhere (resp. outside of infinity). The reciprocity law of ray class field theory gives abelian group isomorphisms  $\text{Gal}(K^1/K) \simeq \text{Cl}(K)$  and  $\text{Gal}(K_+^1/K) \simeq \text{Cl}^+(K)$ . Now fix a prime  $p$ . Let  $K_{(p)}^1 \leq K^1$  (resp.  $K_{+, (p)}^1 \leq K_+^1$ ) be the (resp. *narrow*) *Hilbert  $p$ -class field* of  $K$ , i.e. the maximal abelian  $p$ -extension (i.e. Galois extension with Galois group a  $p$ -group) of  $K$  unramified everywhere (resp. outside of infinity). Then looking at  $p$ -primary parts yields  $\text{Gal}(K_{(p)}^1/K) \simeq \text{Cl}_p(K)$  and  $\text{Gal}(K_{+, (p)}^1/K) \simeq \text{Cl}_p^+(K)$  by Galois theory.

**1.2. Background: Hilbert class field towers and Golod–Shafarevich.** One may iterate the Hilbert class field construction (i.e.  $K^0 := K$  and  $K^{i+1} := (K^i)^1$  for  $i \geq 0$ ) to obtain the  $n$ th *Hilbert class fields*  $K^n$  for  $n \geq 0$ , which together form the *Hilbert class field tower* (which we will refer to as the  $p$ -tower), with *top*  $K^\infty := \bigcup_{n \geq 0} K^n$ . We call the tower *finite* or *infinite* according as  $[K^\infty : K] < \infty$  or  $[K^\infty : K] = \infty$ ; by [45, Proposition 1], the tower is finite if and only if  $\text{Cl}(L) = 1$  for some (not necessarily unramified or Galois) finite extension  $L/K$ . We analogously define  $K_{(p)}^\infty$ , the  $p$ -class field tower, the *top*  $K_{(p)}^\infty$ , and *(in)finiteness*; here, the  $p$ -tower is finite if and only if  $\text{Cl}_p(L) = 1$  for some finite extension  $L/K$  [45, Proposition 2]. In particular, these towers are Galois by the maximality of Hilbert ( $p$ -)class fields. (For other properties of class field towers, we refer to Lemmermeyer’s survey [30], Ershov’s survey [11], and Koch’s book [25].) For use in Section 1.3 and Proposition 3.5, we state the following standard result, proved by induction.

**Proposition 1.1** (Cf. Roquette [45, proofs of Propositions 1 and 2]). *Fix a number field  $K$  and a prime  $p$ . Let  $F/\mathbb{Q}$  be a finite subfield of  $K_{(p)}^\infty/\mathbb{Q}$ . Then  $F_{(p)}^\infty \leq K_{(p)}^\infty$ .*

*Proof.* Field  $F/\mathbb{Q}$ , being a finite subfield of  $K_{(p)}^\infty/\mathbb{Q}$ , must be contained in some finite step  $K_{(p)}^n$  of the tower (i.e.  $F \leq K_{(p)}^n$  for some finite  $n \geq 0$ ). Then an inductive argument following [45, proofs of Propositions 1 and 2] shows that  $F_{(p)}^i \leq K_{(p)}^{n+i}$  for  $i \geq 0$ , so  $F_{(p)}^\infty \leq K_{(p)}^\infty$ . To illustrate the first step of induction, note that  $F_{(p)}^1/F$  is a  $p$ -extension (in particular, Galois), so  $F_{(p)}^1 K_{(p)}^n$  is a well-defined  $p$ -extension of  $K_{(p)}^n$ ; this “relativization” also preserves unramified-ness (for the nonarchimedean valuations, see e.g. Neukirch’s textbook [40, p. 153, Ch. II, Sec. 7, Proposition 7.2]).  $\square$

In the 1960s, Golod and Shafarevich gave a sufficient criterion—the contrapositive of the following theorem—for the infinitude of  $p$ -towers.

**Theorem 1.2** (Vinberg/Gaschütz refinement of the Golod–Shafarevich inequality [14]; see [45]). *Fix a number field  $K$  and a prime  $p$ . Suppose  $K$  has finite  $p$ -tower. Then  $d_p \text{Cl}(K) < 2 + 2\sqrt{1 + d_p \mathcal{O}_K^\times}$ , where  $\mathcal{O}_K^\times$  denotes the unit group of the ring of integers  $\mathcal{O}_K$ .*

*Side Remark 1.1.* Actually, if  $L := K_{(p)}^\infty$ , then  $\mathcal{O}_K^\times$  can be replaced by the quotient  $\mathcal{O}_K^\times/N_{L/K}\mathcal{O}_L^\times$ , which Roquette [45] calls the *norm factor group*. But in practice this seems unwieldy.

*Side Remark 1.2* (General class field towers). It would be interesting to try to find an infinite class field tower not “built” from an infinite  $p$ -class field tower for some prime  $p$ . (To the best of our knowledge, while there are examples of number fields with infinite class field tower

but finite  $p$ -class field tower for all primes  $p$ , these examples still depend on a *closely related*  $q$ -class field tower being infinite for some prime  $q$ .)

It directly follows from Theorem 1.2 that the 2-tower is infinite for any imaginary quadratic number field  $K$  with  $d_2 \text{Cl}(K) \geq 5$ . Martinet [36] (1978), inspired by the Odlyzko [42] (1976) root discriminant bounds, asked whether the same holds when  $d_2 \text{Cl}(K) = 4$ , or equivalently when  $K$  has 5 ramified primes, i.e. the discriminant  $\Delta_K$  factors into 5 prime discriminants  $p^*$  (reviewed in Section 2 along with 2-ranks and genus theory).

**1.3. Previous progress on Martinet's question.** No negative results are known. Currently, all of the best (positive) results on Martinet's question, to the author's knowledge, stem from applications of the Golod–Shafarevich bound to unramified 2-extensions of  $K$ , combined with genus theory bounds. The point is that  $K = \mathbb{Q}(\sqrt{d})$  has infinite 2-tower if (and only if) there exists a number field  $L/\mathbb{Q}$  satisfying both of the following conditions.

- (1) The well-defined compositum  $KL = L(\sqrt{d})$  has infinite 2-tower. This is guaranteed—in view of Corollary 2.2 (below) on relative genus theory—by Theorem 1.2 (above), if  $KL/L = L(\sqrt{d})/L$  is a sufficiently ramified quadratic extension.
- (2)  $KL \leq K_{(2)}^\infty$  (in which case  $K \leq KL \leq K_{(2)}^\infty$  yields  $K_{(2)}^\infty \leq (KL)_{(2)}^\infty \leq K_{(2)}^\infty$  by Proposition 1.1 (above), so  $(KL)_{(2)}^\infty = K_{(2)}^\infty$ ). This is equivalent to  $L \leq K_{(2)}^\infty$ .

*Remark 1.3.* The second condition is guaranteed, for instance, when  $KL/K$  is an everywhere unramified 2-extension—or equivalently (by solvability of 2-extensions), when  $KL/K$  is Galois (certainly guaranteed if  $L/\mathbb{Q}$  is Galois) and  $L \leq K_{(2)}^\infty$ . To our knowledge, all of the best results on Martinet's question choose Galois subfields  $L/\mathbb{Q}$  of  $K_{(2)}^\infty/K$ , so it might be fruitful to look at different choices of  $L$ .

These observations immediately lead to the extended criterion Proposition 3.1 (below) for infinite 2-towers. We are not aware of any particularly usable improvements, but we speculate some in Section 6. We now summarize the best previous (positive) results, in terms of the choice of  $L$  in Proposition 3.1.

- Mouhib [38] (2010), improving on Sueyoshi [48] (2004), gave a uniformly positive answer to Martinet's question when  $\Delta_K = p_1^* \cdots p_5^*$  (with  $p^*$  as defined in Section 2) has exactly 1 *negative* prime discriminant. Say  $p_5^* < 0$ ; then Mouhib took  $L$  to be—with modifications in some cases—the well-defined decomposition field of  $p_5$  in the elementary abelian 2-extension  $\mathbb{Q}(\sqrt{p_1^*}, \dots, \sqrt{p_4^*})$ . However, it seems difficult to extend the technique—which relies on the total realness of  $L$ —to the cases of 3 or 5 negative prime discriminants.

Recall that one may also categorize quadratic number fields by the Rédei matrix (see Section 2.2), motivated by the fact that a rational prime  $p$  unramified in  $\mathbb{Q}(\sqrt{p_1^*} \cdots p_n^*)$  splits if and only if  $\left(\frac{p_1^*}{p}\right) \cdots \left(\frac{p_n^*}{p}\right) = +1$  (even if  $p = 2$ ). The following results build on techniques of Martinet [36], with  $L$  a (Galois) subfield (usually quadratic or biquadratic) of the *narrow genus field*  $\mathbb{Q}(\sqrt{p_1^*}, \dots, \sqrt{p_5^*})/\mathbb{Q}$  of  $K/\mathbb{Q}$ .

- Hajir [16, 17] (1996, 2000), improving on a theorem of Koch [24] (1969), established infinite 2-towers when  $d_4 \text{Cl}(K) \geq 3$ , using Ramsey-type analysis of Rédei matrices with small rank. Lemmermeyer [29] used analogous methods to study *real* quadratic fields.

- Later, Benjamin [1, 2] (2001, 2002) and Sueyoshi [48, 49, 50] (2004, 2009, 2010 for one, five, three negative prime discriminants, respectively) systematically established infinite 2-towers for many  $5 \times 5$  Rédei matrix cases, but still left many cases open (see [3, Table 1] for details)—especially for small  $d_4 \text{Cl}(K)$ .

However, there seems to be more room for exploration. For example, in this paper we focus on Schmithals’ idea [46] (1980) of looking at  $L = F_{(2)}^1$  for a quadratic field  $F$ —see Proposition 3.5 below—motivated by the decomposition law of class field theory. Recently, by taking  $F$  with 4 prime discriminants (see [3, Lemma 9]—where the preceding text “ $K$  is the compositum of  $k^1$  and  $F$ ” should instead be “ $K$  is the compositum of  $k$  and  $F^1$ ”, and  $F$  should be specified to satisfy “ $d_F \mid d_k$  so that  $K/k$  is unramified”—and the more specific applications [3, Lemmas 10 and 11], where to correct a sign error it should say “ $\mathbb{Q}(\sqrt{-5.11.401})$ ” in the second listing of  $k$  in [3, Remark 6]), Benjamin [3] (2015) established infinite 2-towers in certain sub-cases of several of these open matrix cases with  $d_4 \text{Cl}(K) \in \{1, 2\}$ , and explained in particular the failure of his methods for  $d_4 \text{Cl}(K) = 0$ .

**1.4. Outline of paper.** In contrast to Benjamin [3], we take  $F$  (in Proposition 3.5) with 3 or 2 prime discriminants to make some progress when  $d_4 \text{Cl}(K) \in \{0, 2\}$ , in the hopes of identifying some of the “most difficult” remaining cases of Martinet’s question. Specifically, we give some new results in Section 3, and present our concrete applications to open Rédei matrices in Section 4. This provides affirmative answers to Benjamin’s questions [3, Questions 1, 2, and 5] on the existence of new (to the best of our knowledge) imaginary quadratic number fields  $K$  with  $d_2 \text{Cl}(K) = 4$  and  $d_4 \text{Cl}(K) \in \{0, 2\}$ .

*Remark 1.4.* In private correspondence, Benjamin informed us that [3, Question 5] has minor typos; the correct version is “Do there exist new imaginary quadratic number fields  $k$  with rank  $C_{k,2} = 4$  that have infinite 2-class field tower in the case when the 4-rank of  $C_k$  is 0...?” with a remark that “such new fields do not satisfy [3, Lemma 10].” Also, “Lemma 11” in [3, Question 4] should be replaced with “Lemma 10”.

Our attempts at applying the decomposition law (Proposition 3.3) to Proposition 3.5 naturally lead to Section 5, where we investigate barriers to our methods—specifically, “insufficient” prime splitting in 2-class fields—and establish them as consequences of the “classical principal genus theorem” over  $\mathbb{Q}$ . We also ask an extension question (of independent interest) in this direction.

Section 2 reviews, in particular, the usual relative genus theory estimates on 2-ranks of class groups, with an additional remark (Remark 2.3) on potentially helpful additional information from the ambiguous class number formula. Section 6 discusses further possible research directions.

## 2. BACKGROUND: PRIME DISCRIMINANTS, 2-CLASS GROUPS, AND GENUS THEORY

Experts can quickly skim this section for notation and review of prime discriminants, genus theory, and Rédei matrices.

Recall that for any quadratic number field  $K$  with discriminant  $\Delta_K$  (so that  $K = \mathbb{Q}(\sqrt{\Delta_K})$ ) and  $t$  (finite) ramified primes, we have a unique factorization  $\Delta_K = p_1^* \cdots p_t^*$  into  $t$  pairwise coprime *prime (power) discriminants*  $p_i^*$  (defined so that  $2^* \in \{+8, -8, -4\}$  and  $p^* = (-1)^{(p-1)/2} p \equiv 1 \pmod{4}$  for odd primes  $p$ ). By Gauss’ principal genus theorem, the 2-ranks of the narrow and wide class groups are simply  $d_2 \text{Cl}^+(K) = t - 1$  and  $d_2 \text{Cl}(K) =$

$t - 1 - [\Delta_K > 0 \text{ and } p_i^* < 0 \text{ for some } i]$ , where  $[*]$  is an indicator function (defined to be 1 if  $*$  holds, and 0 otherwise).

We now review a relative generalization of these results via the ambiguous class number formula, with an additional remark (Remark 2.3) on potentially helpful additional information.

## 2.1. Relative genus theory.

**Theorem 2.1** (Cf. Lemmermeyer [32], Gras [15, p. 180, Remark 6.2.3; p. 383, Remark 4.2.4], Emerton [10]). *If  $L/K$  is cyclic, then we have the ambiguous class number formula*

$$|\text{Cl}(L)^{\text{Gal}(L/K)}| = |\text{Cl}(K)| \cdot \frac{\prod_v e_v}{[L : K] \cdot [\mathcal{O}_K^\times : \mathcal{O}_K^\times \cap N_{L/K}(L^\times)]},$$

where the product of ramification indices  $e_v$  runs over all finite and infinite places  $v$  of  $K$ .

*Side Remark 2.1* (Resemblance with genus class number formula). We have the short exact sequence  $\text{Cl}(L)^{\text{Gal}(L/K)} \hookrightarrow \text{Cl}(L) \twoheadrightarrow \text{Cl}(L)^{1-\sigma}$  induced by the surjection  $I \pmod{P_L} \mapsto I/\sigma(I) \pmod{P_L}$ . It is important here that  $L/K$  is cyclic, so that a single generator  $\sigma$  generates  $\text{Gal}(L/K)$ . In particular,  $|\text{Cl}(L)|/|\text{Cl}(L)^{1-\sigma}| = |\text{Cl}(L)^{\text{Gal}(L/K)}|$ .

Let  $H_K, H_L$  denote Hilbert class fields of  $K, L$ , and  $H_{L/K}$  the relative genus field of  $L$  over  $K$  (which, when  $L/K$  is cyclic, hence abelian, is just the maximal everywhere unramified extension of  $L$  abelian over  $K$ ). Some Galois theory (as in Gras [15, Remark 4.2.4] or Cornell [8, Propositions 3 and 4]) shows that  $\text{Gal}(H_{L/K}/K)/\text{Cl}(L)^{1-\sigma}$  is the abelianization  $\text{Gal}(H_{L/K}/K)^{\text{ab}} = \text{Gal}(H_{L/K}/K)$ , so that  $H_{L/K}$  is the fixed field of (the normal subgroup)  $\text{Cl}(L)^{1-\sigma}$ . In particular,  $[H_{L/K} : K] = [H_L : K]/|\text{Cl}(L)^{1-\sigma}| = [L : K][H_L : L]/|\text{Cl}(L)^{1-\sigma}| = [L : K]|\text{Cl}(L)|/|\text{Cl}(L)^{1-\sigma}| = [L : K]|\text{Cl}(L)^{\text{Gal}(L/K)}|$ . Thus in relative genus field  $H_{L/K}$  language,  $|\text{Cl}(L)^G| = [H_{L/K} : K]/[L : K] = [H_{L/K} : H_K][H_K : K]/[L : K] = [H_{L/K} : H_K] \cdot |\text{Cl}(K)|/[L : K]$ —so the ambiguous class number formula becomes

$$[H_{L/K} : H_K] = \frac{\prod_v e_v}{[\mathcal{O}_K^\times : \mathcal{O}_K^\times \cap N_{L/K}(L^\times)]}.$$

This is close to the genus class number formula going back to Gauss, Hilbert, and Furtwängler, which holds for all abelian extensions  $L/K$ —see Lemmermeyer's survey [30, p. 11].

**Side Question 2.2.** *Is it true that  $H_{L/K}/H_K$  is an elementary abelian 2-extension if  $[L : K] = 2$ ? We would want to show that for any  $K$ -automorphism  $g : H_L \rightarrow H_L$  fixing  $K'$  (i.e.  $g|_{K'} = 1$  is trivial), that  $g^2$  fixes  $H_{L/K}$  (i.e.  $g^2|_{H_{L/K}}$  is trivial). We may need the map  $\text{Cl}(L) \simeq \text{Gal}(H_L/L) \hookrightarrow \text{Gal}(H_L/K) \twoheadrightarrow \text{Gal}(H_K/K) \simeq \text{Cl}(K)$  to be sufficiently canonical.*

We do not know the precise origins of the following classical 2-rank estimates. If  $L/K$  is cyclic with Galois group  $G$ , consider the norm map  $\phi : \text{Cl}(L) \rightarrow \text{Cl}(K)$  (sending  $I \pmod{P_L}$  to  $N_{L/K}(I) \pmod{P_K}$ ) and its restriction  $\psi := \phi|_{\text{Cl}(L)^G}$ . Then  $\ker \psi$  lies inside the  $[L : K]$ -torsion  $\text{Cl}(L)^G[[L : K]]$ . Restricting  $\psi$  further to the 2-primary part  $\text{Cl}(L)^G[2^\infty]$  induces an injection

$$\text{Cl}(L)^G[2^\infty]/(\ker \psi)[2^\infty] \hookrightarrow \text{Cl}_2(K).$$

Now assume in addition that  $L/K$  is quadratic. Then  $\text{Cl}(L)^G[[L : K]] = \text{Cl}(L)^G[2]$  is an elementary abelian 2-group, so one obtains the following result.

**Corollary 2.2** (Relative genus theory bounds on 2-rank, cf. Jehne [21, p. 230, Section 5], Lemmermeyer [30, Proposition 1.3.19]). *If  $L/K$  is quadratic with Galois group  $G$ , then*

$$(1) \quad d_2 \text{Cl}(L) \geq d_2 \text{Cl}(L)^G \geq d_2 \ker \psi \geq v_2(|\text{Cl}(L)^G|) - v_2(|\text{Cl}(K)|)$$

$$(2) \quad \underbrace{= \text{ram}(L/K) - 1 - d_2 \mathcal{O}_K^\times / \mathcal{O}_K^\times \cap N_{L/K}(L^\times)}_{\text{from Theorem 2.1 and } (K^\times)^{[L:K]=2} \leq N_{L/K}(L^\times)},$$

where  $\text{ram}(L/K)$  denotes the number of finite or infinite primes of  $K$  ramified in  $L$ . Furthermore,  $(\ker \phi^{|\text{Cl}(K)|/|\text{Cl}_2(K)|}[2] \leq \text{Cl}(L)^G$ . Note that  $\text{Cl}(L/K)[2] \leq (\ker \phi^{|\text{Cl}(K)|/|\text{Cl}_2(K)|}[2]$ , where  $\text{Cl}(L/K) := \ker \phi$  denotes the relative class group. In particular, if  $h_K$  is odd, i.e.  $v_2(|\text{Cl}(K)|) = 0$ , then  $\text{Cl}(L)[2] = \text{Cl}(L)^G[2] = \text{Cl}(L)^G[2^\infty]$  and equality holds everywhere in the inequality (1); when  $K = \mathbb{Q}$  we recover the classical formula for  $d_2 \text{Cl}(\mathbb{Q}(\sqrt{\Delta}))$ .

*Remark 2.3* (Additional information). Can one get better results (cf. Lemmermeyer [30, Questions 8 and 9])? For instance, in the equality case  $\text{rank}_2 \text{Cl}(L) = v_2(\#\text{Cl}(L)^G) - v_2(\#\text{Cl}(K))$ , we must have  $\ker \psi = \text{Cl}(L)^G[2]$  and  $\text{Cl}(L)^G[2^\infty]/\ker \psi \simeq \text{Cl}_2(K)$ , so  $d_4 \text{Cl}(L)^G = d_2 \text{Cl}(K)$  in particular, which could be helpful. We speculate further in Section 6.

*Side Remark 2.3.* See Lemmermeyer's survey [30, Proposition 1.3.19]: the kernel  $\ker \phi$  is called the relative class group  $\text{Cl}(L/K)$ . (There seems to be more than one definition in the literature, but this is one of them.) For  $K = \mathbb{Q}$  we have the usual class group, of course. See more facts, especially on the index of the image of  $\phi$  in  $\text{Cl}(K)$ , at [30, Theorem 1.2.5. Takagi's main theorem for Hilbert class fields] (specifically item 6).

*Proof of general injection.* An invariant ideal class  $I \pmod{P_L} \in \text{Cl}(L)^G$  lies in the kernel  $\ker \psi$  if and only if  $N_{L/K}(I) \in P_K$ . But for  $I \pmod{P_L} \in \text{Cl}(L)^G$  we have  $N_{L/K}(I)\mathcal{O}_L = I^{[L:K]}\mathcal{O}_L = I^{[L:K]}$ . So if  $N_{L/K}(I) \in P_K$ , then  $N_{L/K}(I)\mathcal{O}_L \in P_L$ , so  $I^{[L:K]} \in P_L$ . So  $\ker \psi$  lies inside the  $[L:K]$ -torsion subgroup  $\text{Cl}(L)^G[[L:K]]$  of  $\text{Cl}(L)^G$ . (It also lies inside  $\ker \phi$ , the relative class group  $\text{Cl}(L/K)$ .)

Consider the exact sequence  $1 \rightarrow \ker \psi \subseteq \text{Cl}(L)^G \rightarrow \text{Cl}(K)$ . Restrict  $\psi$  further to the 2-primary part  $\text{Cl}(L)^G[2^\infty]$ . Then the restriction  $\psi_2$  maps  $\text{Cl}(L)^G[2^\infty]$  into the  $2^\infty$ -torsion  $\text{Cl}_2(K)$  of  $\text{Cl}(K)$ . Clearly  $\ker \psi_2$  is just the  $2^\infty$ -torsion of  $\ker \psi$  (because  $\ker \psi \subseteq \text{Cl}(L)^G$ ). Thus  $\psi$  induces the desired injection  $\text{Cl}(L)^G[2^\infty]/(\ker \psi)[2^\infty] \hookrightarrow \text{Cl}_2(K)$ .  $\square$

*Proof of specialization to  $[L:K] = 2$ , including Inequality (1).* In this case  $\text{Cl}(L)^G[[L:K]] = \text{Cl}(L)^G[2]$  is an elementary abelian 2-group, so its subgroup  $\ker \psi$  is also elementary, and we obtain  $d_2 \text{Cl}(L) \geq d_2 \text{Cl}(L)^G \geq d_2 \ker \psi \geq v_2(\#\text{Cl}(L)^G) - v_2(\#\text{Cl}(K))$ , so Theorem 2.1 and  $(K^\times)^{[L:K]=2} \leq N_{L/K}(L^\times)$  (as well as  $[L:K] = 2$  and the fact that  $e_v \in \{1, 2\}$  for all  $v$ ) prove Inequality (1).

For the second part, consider  $[I] \in \text{Cl}(L)[2]$ , so that  $I^2 = a \cdot \mathcal{O}_L$  for some  $a$ . Then  $I/\sigma(I) = I^2/I\sigma(I) = a^2 N_{L/K}(I)^{-1} \mathcal{O}_L$ —somewhat abusing notation (as  $N_{L/K}(I) \in \mathcal{I}_K$ ). Raising to exponent of  $|\text{Cl}(K)|/|\text{Cl}_2(K)| \equiv 1 \pmod{2}$  gives  $I/\sigma(I) \in N_{L/K}(I^{|\text{Cl}(K)|/|\text{Cl}_2(K)|})^{-1} P_L$  (again somewhat abusing notation), since  $I^2 \in P_L$  (so also  $\sigma(I)^2 \in P_L$ ).

In particular, if  $[I] \in \text{Cl}(L)[2]$  and  $I \in \ker \phi^{|\text{Cl}(K)|/|\text{Cl}_2(K)|}$ , then  $I/\sigma(I) \in P_L$ , i.e.  $[I] = \sigma[I]$ , so  $[I] \in \text{Cl}(L)^G$ . In other words,  $(\ker \phi^{|\text{Cl}(K)|/|\text{Cl}_2(K)|}[2] \leq \text{Cl}(L)^G$ .  $\square$

*Proof of specialization to  $[L:K] = 2$  and  $h_K$  odd, including equality of Inequality (1).* If, in addition,  $h_K$  is odd, i.e.  $|\text{Cl}_2(K)| = 1$ , then  $\ker \phi^{|\text{Cl}(K)|/|\text{Cl}_2(K)|} = \text{Cl}(L)$ , so specializing gives

$\text{Cl}(L)[2] \leq \text{Cl}(L)^G$ , so that  $\text{Cl}(L)[2] = \text{Cl}(L)^G[2]$  in this case. But trivially  $v_2(\#\text{Cl}(K)) = 0$  and  $v_2(\#\text{Cl}(L)^G) \geq \text{rank}_2 \text{Cl}(L)^G$ , so equality indeed holds everywhere in Inequality (1).  $\square$

## 2.2. Rédei matrices and 4-ranks.

**Definition 2.4** (Cf. Rédei [44]; Rédei–Reichardt [43]). For a quadratic number field  $K$  with prime discriminant factorization  $\Delta_K = p_1^* \cdots p_t^*$ , let  $R_K$  denote the (additive) *Rédei matrix*  $[a_{ij}] \in \mathbb{F}_2^{t \times t}$  (up to re-labeling of the  $p_i^*$ ) with  $(-1)^{a_{ij}} := \left(\frac{p_i^*}{p_j}\right)$  when  $i \neq j$ , and  $(-1)^{a_{ii}} := \left(\frac{\Delta_K/p_i^*}{p_i}\right)$  (so that the row vectors sum to  $0 \in \mathbb{F}_2^t$ ). Here  $\left(\frac{\cdot}{\cdot}\right)$  denotes the Kronecker (not Legendre) symbol, so that  $a_{ij} = 0$  if and only if  $p_j$  splits in the quadratic field  $\mathbb{Q}(\sqrt{p_i^*})$  (even if  $p_j = 2$ ).

*Remark 2.5.* In this paper we will often draw Rédei matrices without the diagonal entries, which can be recovered by the fact that column sums are 0.

*Side Remark 2.4* (Relevant version of quadratic reciprocity). For our purposes, if  $p^*, q^*$  are prime discriminants with  $p, q$  distinct, then  $\left(\frac{p^*}{q}\right) = -\left(\frac{q^*}{p}\right)$  if  $p^*, q^* < 0$  are both negative and not equal to  $-4$ ; and  $\left(\frac{p^*}{q}\right) = \left(\frac{q^*}{p}\right)$  if at least one of  $p^*, q^*$  is positive, and neither equals  $-4$ . If, say,  $q^* = -4$ , then  $p$  is odd and it is easiest just to directly compute  $\left(\frac{p^*}{2}\right) = [p^* \equiv 1 \pmod{8}] = (-1)^{(p^*-1)/4} = (-1)^{(p^2-1)/8}$  and  $\left(\frac{-4}{p}\right) = [p \equiv 1 \pmod{4}] = (-1)^{(p-1)/2}$ .

**Theorem 2.6** (4-rank of narrow class group; cf. Rédei [44]; Rédei–Reichardt criterion [43]). *Let  $K/\mathbb{Q}$  be a quadratic number field with  $t$  rational primes dividing  $\Delta_K$ . Then  $d_4 \text{Cl}^+(K) = t - 1 - \text{rank}_{\mathbb{F}_2} R_K$ .*

For the connection between 4-rank and  $C_4$ -splitting/factorizations of  $\Delta_K$ , and related matters, see e.g. Lemmermeyer [30, 28, 29], Hurrelbrink [20], and Hajir [16, 17]. In a different direction, Waterhouse [51] gave an 8-rank criterion (see also Hasse [18] and Lu [34]), and Kolster [27] gave a criterion for all powers of 2. Yue [52] generalized the Rédei–Reichardt 4-rank criterion to relative quadratic extensions over a base field with odd class number.

## 3. KEY LEMMAS

We start by reviewing some background, but refer the reader to Section 3.2 for concrete new results, which we will apply to some open sub-cases of Martinet’s question in Section 4.

**3.1. Background.** Let  $K/\mathbb{Q}$  be an imaginary quadratic field extension with  $\Delta_K = p_1^* \cdots p_t^* < 0$  (recall  $t = 5$  in Martinet’s question) and  $L/\mathbb{Q}$  a finite subfield of  $K_{(2)}^\infty/\mathbb{Q}$  with  $\sqrt{\Delta_K} \notin L/\mathbb{Q}$ , so that  $KL = L(\sqrt{\Delta_K})$  is quadratic over  $L$ . Then

- $(KL)_{(2)}^\infty = K_{(2)}^\infty$  (from the beginning of Section 1.3), so  $[K_{(2)}^\infty : K] = \infty$  if and only if  $[(KL)_{(2)}^\infty : KL] = \infty$ .
- By Dirichlet’s unit theorem,  $d_2 \mathcal{O}_{KL}^\times = (\frac{1}{2}[KL : \mathbb{Q}] - 1) + 1 = [L : \mathbb{Q}]$ , as  $-1 \in \mathcal{O}_{KL}^\times$  and  $KL$  is always totally imaginary.
- Similarly,  $d_2 \mathcal{O}_L^\times$  equals  $\frac{1}{2}[L : \mathbb{Q}]$  if  $L$  is totally imaginary, and equals  $[L : \mathbb{Q}]$  if  $L$  is totally real.
- By Corollary 2.2 applied to the relative quadratic extension  $KL/L$ , we have

$$d_2 \text{Cl}(KL) \geq \text{ram}(L(\sqrt{\Delta_K})/L) - 1 - d_2(\mathcal{O}_L^\times / [\mathcal{O}_L^\times \cap N_{KL/L}((KL)^\times)]) \geq \text{ram}(L(\sqrt{\Delta_K})/L) - 1 - d_2 \mathcal{O}_L^\times.$$

Applying Theorem 1.2 to  $KL$  now yields the following main idea of most relevant papers.

**Proposition 3.1** (Cf. [36], [46], and [47]). *With notation as above, the field  $KL$ , and thus  $K$  by extension, has an infinite 2-tower if any of the following criteria hold:*

- $d_2 \text{Cl}(KL) \geq 2 + 2\sqrt{1 + [L : \mathbb{Q}]}$ ;
- $\text{ram}(L(\sqrt{\Delta_K})/L) - 1 - d_2(\mathcal{O}_L^\times / [\mathcal{O}_L^\times \cap N_{KL/L}((KL)^\times)]) \geq 2 + 2\sqrt{1 + [L : \mathbb{Q}]}$ ;
- $L/\mathbb{Q}$  is totally imaginary and  $\text{ram}(L(\sqrt{\Delta_K})/L) - 1 - \frac{1}{2}[L : \mathbb{Q}] \geq 2 + 2\sqrt{1 + [L : \mathbb{Q}]}$ ;
- $L/\mathbb{Q}$  is totally real and  $\text{ram}(L(\sqrt{\Delta_K})/L) - 1 - [L : \mathbb{Q}] \geq 2 + 2\sqrt{1 + [L : \mathbb{Q}]}$ .

*Remark 3.2.* Suppose  $L/\mathbb{Q}$  is unramified at  $m \geq 0$  primes dividing  $\Delta_K$ , say  $p_1, \dots, p_m$ . Then  $\text{ram}(L(\sqrt{\Delta_K})/L)$  equals  $\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid p_1 \cdots p_m\}$  if  $L$  is totally imaginary, and equals  $[L : \mathbb{Q}] + \#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid p_1 \cdots p_m\}$  if  $L$  is totally real (the  $[L : \mathbb{Q}]$  coming from ramification at the infinite places of  $L$ ).

*Side Remark 3.1.* The term  $d_2(\mathcal{O}_L^\times / [\mathcal{O}_L^\times \cap N_{KL/L}((KL)^\times)])$ —measuring the solvability of  $x^2 - \Delta_K y^2 = \epsilon$  in  $L$  for the various units  $\epsilon \in \mathcal{O}_L^\times$ —seems unwieldy in general (almost all papers use the trivial upper bound  $d_2 \mathcal{O}_L^\times$ ), though under certain hypotheses Schoof [47, Remark 3.5 and Theorem 3.7] and Lemmermeyer [29, Proof of Theorem 3] have been able to give stronger yet clean estimates this way, on different but related problems.

Schmithals [46] (1980) introduced the idea (Proposition 3.5) of looking at  $L = F_{(2)}^1$  for a (quadratic) field  $F$ . The motivation comes from the decomposition law of class field theory; we will use the following particular 2-extension version.

**Proposition 3.3** (Decomposition law and application, consult e.g. [30, Theorem 1.2.5]). *Set  $L := F_{(2)}^1$  for a number field  $F$ . A (nonzero) prime  $\mathfrak{p}$  of  $F$  splits into  $|\text{Cl}(F)| / \text{ord}_{\text{Cl}(F)}[\mathfrak{p}]$  primes in  $F^1$ , and hence (by Galois theory of  $F \leq L \leq F^1$ ) into  $|\text{Cl}_2(F)| / \text{ord}_{\text{Cl}(F)/\text{Cl}(F)[\mathbb{Z}\backslash 2\mathbb{Z}]}[\mathfrak{p}]$  primes in  $L$ ; note that  $\text{ord}_{\text{Cl}(F)/\text{Cl}(F)[\mathbb{Z}\backslash 2\mathbb{Z}]}[\mathfrak{p}]$  equals the largest power of 2 dividing  $\text{ord}_{\text{Cl}(F)}[\mathfrak{p}]$ . For  $m \geq 0$  distinct rational primes  $p_1, \dots, p_m$ , we have*

$$\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid p_1 \cdots p_m\} = \sum |\text{Cl}_2(F)| / (\text{largest power of 2 dividing } \text{ord}_{\text{Cl}(F)}[\mathfrak{p}]),$$

where the sum runs over the primes  $\mathfrak{p}$  of  $F$  dividing  $p_1 \cdots p_m$ .

*Remark 3.4* (See [46]). If a rational prime  $p$  is inert in  $F/\mathbb{Q}$ , then (perhaps surprisingly) we still have lots of splitting in  $L/\mathbb{Q}$ : the prime ideal  $p\mathcal{O}_F$  is *principal*, hence *totally split* in  $L/F$  (in fact, also in the extension  $F^1/F$ ). In fact, from a “random Rédei matrix” perspective (when  $F$  is quadratic), it is *harder* to guarantee lots of splitting in  $L/\mathbb{Q}$  when  $p$  splits in  $F/\mathbb{Q}$ , as discussed in Section 5.

*Side Remark 3.2.* There is an analogous decomposition law for narrow Hilbert class fields (and ray class fields in general), presented for instance in Neukirch’s textook [40, p. 409, Ch. VI, Sec. 6, Theorem 7.3] and <http://math.stackexchange.com/a/1264488/43100>.

**Proposition 3.5** (2-class field idea, cf. Schmithals [46] (1980) and Schoof [47] (1986)). *Let  $K/\mathbb{Q}$  be an imaginary quadratic field extension with  $\Delta_K = p_1^* \cdots p_t^*$  and  $F/\mathbb{Q}$  a finite subfield of  $K_{(2)}^\infty/\mathbb{Q}$ , with  $F/\mathbb{Q}$  unramified at  $m \geq 1$  primes dividing  $\Delta_K$ , say  $p_1, \dots, p_m$ . Then  $L := F_{(2)}^1$  is a finite subfield (by Proposition 1.1) of  $K_{(2)}^\infty/\mathbb{Q}$  unramified at  $p_1, \dots, p_m$ , with  $\sqrt{\Delta_K} \notin L/\mathbb{Q}$  (since  $m \geq 1$ ). By Proposition 3.1 and  $[L : \mathbb{Q}] = 2[L : F] = 2|\text{Cl}_2(F)|$ , the field  $K$  has an infinite 2-tower if any of the following criteria hold:*



- $d_2 \text{Cl}(KL) \geq 2 + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$ ;
- $\text{ram}(L(\sqrt{\Delta_K})/L) - 1 - d_2(\mathcal{O}_L^\times/[\mathcal{O}_L^\times \cap N_{KL/L}((KL)^\times)]) \geq 2 + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$ ;
- $L/\mathbb{Q}$  is totally imaginary and  $\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid p_1 \cdots p_m\} - 1 - |\text{Cl}_2(F)| \geq 2 + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$ ;
- $L/\mathbb{Q}$  is totally real and  $\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid p_1 \cdots p_m\} - 1 \geq 2 + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$ .

*Side Remark 3.3.* When  $F/\mathbb{Q}$  is Galois, the maximality of  $F_{(2)}^1/F = L/F$  proves that  $L/\mathbb{Q}$  is also Galois.

*Side Remark 3.4* (Relaxing to more general unramified solvable towers). If instead of strictly looking at 2-towers, one allows a few “steps” to be unramified, then it could turn out to be much easier to get uniform results on infinitude of class field towers. For instance, following Schoof [47], one could take  $L = F^1$  instead of  $L = F_{(2)}^1$ .

*Side Remark 3.5.* In view of Side Remark 3.2, it could in principle be useful to consider the variant with  $L := F_{+, (2)}^1$  instead the *narrow* Hilbert 2-class field. However, we have not yet managed to find a particularly fruitful application to (the open cases of) Martinet’s question, because if  $F/\mathbb{Q}$  is quadratic with  $\text{Cl}^+(F) \neq \text{Cl}(F)$  (so  $F$  must be real in particular), then  $F \leq F_{(2)}^1 \leq F^1$  is a tower of totally real fields—but one can then check that  $L$  becomes totally imaginary (in which case the criterion is stricter, due to lack of archimedean ramification).

**3.2. Concrete new lemmas.** We obtain the following Lemmas 3.6, 3.11, and 3.16 by applying Proposition 3.3 to some choice of quadratic field  $F/\mathbb{Q}$  in Proposition 3.5. Throughout this section, we denote by  $K/\mathbb{Q}$  an imaginary quadratic field with  $\Delta_K = \ell_1^* \cdots \ell_5^*$  (exactly 5 prime discriminants).

**3.2.1.  $F$ : imaginary quadratic field with three prime discriminants.** When  $\ell_3^* \ell_4^* \ell_5^* < 0$ , taking the imaginary quadratic field  $F = \mathbb{Q}(\sqrt{\ell_3^* \ell_4^* \ell_5^*}) \leq K_{(2)}^\infty$  in Proposition 3.5 yields Lemma 3.6.

**Lemma 3.6.** *If some three of the five prime discriminants, say  $\ell_3^*, \ell_4^*, \ell_5^*$ , have negative product, then the imaginary quadratic field  $K$  has infinite 2-tower if any of the following criteria hold:*

- (1)  $d_2 \text{Cl}(KL) \geq 2 + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$ ;
- (2)  $|\text{Cl}_2(F)| \geq 16$  and  $\ell_1, \ell_2$  are both inert in  $F/\mathbb{Q}$ , i.e.  $(\frac{\ell_3^*}{p})(\frac{\ell_4^*}{p})(\frac{\ell_5^*}{p}) = -1$  for both of  $p = \ell_1, \ell_2$ .

Here  $F = \mathbb{Q}(\sqrt{\ell_3^* \ell_4^* \ell_5^*})$  and  $L := F_{(2)}^1$  from Proposition 3.5 are totally imaginary.

*Remark 3.7.* Since  $F$  is imaginary, Gauss’ genus theory gives  $\text{Cl}_2(F) = \text{Cl}_2^+(F) \simeq C_{2^m} \oplus C_{2^n}$  for some  $m, n \geq 1$ , so the inequality  $|\text{Cl}_2(F)| \geq 8$  is equivalent to  $d_4 \text{Cl}_2(F) \geq 1$ , or  $\text{rank}_{\mathbb{F}_2} R_F \leq 1$  by Rédei–Reichardt. (When  $\ell_3^*, \ell_4^*, \ell_5^*$  are all negative and not equal to  $-4$ , this condition is particularly clean: in this case there are only 2 types of Rédei matrices  $R_F$  up to re-indexing, one with rank 1 and the other with rank 2.) Combined with Waterhouse’s determination of  $d_8 \text{Cl}_2^+(F)$  [51], one could in principle obtain a criterion for  $|\text{Cl}_2(F)| \geq 16$ .

*Remark 3.8.* In view of the group-theoretic success in (for instance) Koch [23], Maire [35], and Benjamin–Lemmermeyer–Snyder [4], it could potentially be enlightening to analyze the “near miss” or “borderline” cases  $\text{Cl}_2(F) \simeq (2, 4)$  or  $\text{Cl}_2(F) \simeq (2, 8)$ .

**Example 3.9.** For the reader's convenience, we now list our attempts at using Lemma 3.6, with the first column detailing the number of negative prime discriminants among  $\ell_3^*, \ell_4^*, \ell_5^*$  in the application of Lemma 3.6(2), and whether  $-4 \in \{\ell_3^*, \ell_4^*, \ell_5^*\}$ .

Application	Progress?	Examples	$R_K$	$\#\{p_i^* < 0\}$	$-4 \in \{p_i^*\}$ ?	$d_4 \text{Cl}(K)$
-	none	Ex. 4.5	$B$	5	no	0
3 neg., no $-4$	Thm. 4.6	Ex. 4.8	$A$	5	no	0
3 neg., no $-4$	Thm. 4.24	Ex. 4.25	28	3	no	0
3 neg., no $-4$	Thm. 4.11	Ex. 4.12	$C$	5	yes	0
3 neg., yes $-4$	Thm. 4.13	Ex. 4.14	$D_1$	5	yes	0
1 neg., yes $-4$	Thm. 4.1	Ex. 4.3	$\mathcal{D}_2$	3	yes	2

*Proof of Lemma 3.6(2).*  $L/\mathbb{Q}$  is totally imaginary, so by Proposition 3.5 it suffices to check  $\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid \ell_1 \ell_2\} - 1 - |\text{Cl}_2(F)| \geq 2 + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$ .

Since  $\ell_1, \ell_2$  are inert in  $F/\mathbb{Q}$ , the decomposition law (specifically, the inert trick of Remark 3.4) yields  $\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid \ell_i\} = [L : F] = |\text{Cl}_2(F)|$  for  $i = 1, 2$ . Thus

$$\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid \ell_1 \ell_2\} \geq \underbrace{|\text{Cl}_2(F)| + |\text{Cl}_2(F)|}_{\text{if } |\text{Cl}_2(F)| \geq 7 + 2\sqrt{11} = 13.6332 \dots} \geq 3 + |\text{Cl}_2(F)| + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$$

verifies the desired criterion when  $|\text{Cl}_2(F)| \geq 16$ .  $\square$

3.2.2.  $F$ : real quadratic field with exactly two positive prime discriminants. Alternatively, when  $\ell_4^*, \ell_5^* > 0$ , taking the real quadratic field  $F = \mathbb{Q}(\sqrt{\ell_4^* \ell_5^*}) \leq K_{(2)}^\infty$  in Proposition 3.5 gives Lemma 3.11.

*Remark 3.10.* This particular idea seems to originate from Schmithals [46] (and independently later by Hajir [16, p. 17, last paragraph] and Mouhib [38, Proposition 3.3], [39]), who took  $F = \mathbb{Q}(\sqrt{(+5)(+461)})$ —with class number 16—to show that  $\mathbb{Q}(\sqrt{(+5)(-11)(+461)})$ , an imaginary quadratic field with 2-class group  $C_4 \oplus C_2$ , has infinite 2-tower.

**Lemma 3.11.** *If some two of the five prime discriminants, say  $\ell_4^*, \ell_5^*$ , are positive, then the imaginary quadratic field  $K$  has infinite 2-tower if any of the following criteria hold:*

- (1)  $d_2 \text{Cl}(KL) \geq 2 + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$ ;
- (2)  $|\text{Cl}_2(F)| \geq 8$  and at least 1 of  $\ell_1, \ell_2, \ell_3$  is inert in  $F/\mathbb{Q}$ , i.e.  $(\frac{\ell_4^*}{p})(\frac{\ell_5^*}{p}) = -1$  for at least 1 of  $p = \ell_1, \ell_2, \ell_3$ ;
- (3)  $|\text{Cl}_2(F)| \geq 4$  and at least 2 of  $\ell_1, \ell_2, \ell_3$  is inert in  $F/\mathbb{Q}$ , i.e.  $(\frac{\ell_4^*}{p})(\frac{\ell_5^*}{p}) = -1$  for at least 2 of  $p = \ell_1, \ell_2, \ell_3$ .

Here  $F = \mathbb{Q}(\sqrt{p_4^* p_5^*})$  and (by non-ramification of  $L/F$  at  $\infty$ )  $L := F_{(2)}^1$  from Proposition 3.5 are totally real.

**Example 3.12.** When Lemma 3.11(2) fails, it is natural to ask (assuming  $K$  has infinite 2-tower) where the failure comes from: Golod–Shafarevich, or the genus theory input? For instance, take  $K = \mathbb{Q}(\sqrt{(-7)(-3)(-8)(+29)(+5)})$ , which has an open Rédei matrix

$$R_K = \#49 = \left[ \begin{array}{ccc|cc} - & 1 & 0 & 0 & 1 \\ 0 & - & 1 & 1 & 1 \\ 1 & 0 & - & 1 & 1 \\ \hline 0 & 1 & 1 & - & 0 \\ 1 & 1 & 1 & 0 & - \end{array} \right].$$

(For partial positive progress on matrix 49, see Theorem 4.17.) Here  $F := \mathbb{Q}(\sqrt{(+29)(+5)})$  has class number 4 (as well as narrow class number 4), so its Hilbert 2-class field  $L := F_{(2)}^1 = F^1$  coincides with its Hilbert class field, which can be computed in SAGE.

The genus theory input gives a lower bound

$$d_2 \text{Cl}(KL) \geq \#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid (-7)(-3)(-8)\} - 1 \geq 4 + 2 + 2 - 1 = 7$$

—here 7 is inert in  $F/\mathbb{Q}$ , and then splits completely into 4 primes in  $L/F$ , while 3, 2 split into 2 primes in  $F/\mathbb{Q}$  and then stay inert in  $L/F$ , due to Theorem 5.3. In fact, here the bound is tight: the class group  $\text{Cl}(KL)$  has cyclic direct sum decomposition  $(336, 336, 4, 4, 2, 2, 2)$  (under the `proof=False` flag in SAGE, i.e. assuming GRH for a reasonable run-time), so 2-rank exactly 7, which is just shy of the  $2 + 2\sqrt{8+1} = 8$  needed for Golod–Shafarevich. But Golod–Shafarevich doesn't take into account the 4-rank of 4, or the 8- and 16- ranks of 2, so it would be nice to have a strengthening incorporating such data; see Question 6.1 for further speculation.

```
R.<x> = PolynomialRing(QQ)
F.<d> = (x^2 - 5*29).splitting_field(); F
F.class_group(); F.narrow_class_group()

H.<a> = F.hilbert_class_field(); H
H.class_group(); H.narrow_class_group()

Z.<u> = H.extension(x^2 - 5*29*(-8)*(-3)*(-7)); Y.<v> = Z.
  absolute_field(); Y
Z.class_group(proof=False); #Z.class_group(proof=True)
```

Here is the output from SAGE.

```
Number Field in d with defining polynomial x^2 - 145
Class group of order 4 with structure C4 of Number Field in d
  with defining polynomial x^2 - 145
Multiplicative Abelian group isomorphic to C4
Number Field in a with defining polynomial x^4 - 6*x^2 - 5*x -
  1 over its base field
Class group of order 1 of Number Field in a with defining
  polynomial x^4 - 6*x^2 - 5*x - 1 over its base field
Trivial Abelian group
Number Field in v with defining polynomial x^16 + 193696*x^14 +
  20*x^13 + 16471863912*x^12 + 968240*x^11 + 803220850771478*
  x^10 - 61753673800*x^9 + 24564405504767344470*x^8 -
  5925738645060300*x^7 + 482450842595634923493592*x^6 -
  178917857880265611700*x^5 + 5942613705132902419583139177*x^4
  - 2412654792740884887465160*x^3 +
  41972919293354024066614415135974*x^2 -
  12387969691342454354951827720*x +
  130154117938774456595949675427812841
```

Class group of order 14450688 with structure C336 x C336 x C4 x C4 x C2 x C2 x C2 of Number Field in u with defining polynomial  $x^2 + 24360$  over its base field

*Remark 3.13.* Recall that whether  $|\text{Cl}_2^+(F)| = |\text{Cl}_2(F)|$  is subtle for real quadratic fields  $F$ . But at least both  $\text{Cl}_2^+(F)$  and  $\text{Cl}_2(F)$  are cyclic here, so by Rédei–Reichardt, the inequality  $|\text{Cl}_2^+(F)| \geq 4$  is equivalent to  $\left(\frac{\ell_4^*}{\ell_5^*}\right) = \left(\frac{\ell_5^*}{\ell_4^*}\right) = +1$ .

*Remark 3.14.* In view of the group-theoretic success in (for instance) Koch [23], Maire [35], and Benjamin–Lemmermeyer–Snyder [4], it could potentially be enlightening to analyze the “near miss” or “borderline” cases  $\text{Cl}_2(F) \simeq C_2$  and  $\text{Cl}_2(F) \simeq C_4$ .

**Example 3.15.** See the applications and examples under Theorem 4.17 (progress on matrices 34a and 49, using Lemma 3.11(2), with Example 4.18), in the case where  $\Delta_K \not\equiv 4 \pmod{8}$  has 3 negative prime discriminants and  $d_4 \text{Cl}(K) = 0$ .

*Proof of Lemma 3.11(2).*  $L/\mathbb{Q}$  is totally real, so by Proposition 3.5 it suffices to check  $\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid \ell_1 \ell_2 \ell_3\} - 1 \geq 2 + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$ .

Say  $\ell_1$  is inert in  $F/\mathbb{Q}$ , so  $\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid \ell_1\} = [L : F] = |\text{Cl}_2(F)|$  by the decomposition law (specifically, the inert trick of Remark 3.4). Furthermore, any prime  $p \nmid \ell_4^* \ell_5^*$  splits into 2 or 4 primes in  $\mathbb{Q}(\sqrt{\ell_4^*}, \sqrt{\ell_5^*})/\mathbb{Q}$ , hence at least that many in the extension  $L/\mathbb{Q}$  (inclusion due to  $\ell_4^*, \ell_5^* > 0$ ). Thus

$$\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid \ell_1 \ell_2 \ell_3\} \geq \underbrace{|\text{Cl}_2(F)| + 2 + 2}_{\text{if } |\text{Cl}_2(F)| \geq 3 + 2\sqrt{3} = 6.4641\dots} \geq 3 + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$$

verifies the desired criterion when  $|\text{Cl}_2(F)| \geq 8$ .  $\square$

*Proof of Lemma 3.11(3).*  $L/\mathbb{Q}$  is totally real, so by Proposition 3.5 it suffices to check  $\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid \ell_1 \ell_2 \ell_3\} - 1 \geq 2 + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$ .

Say  $\ell_1, \ell_2$  are inert in  $F/\mathbb{Q}$ , so  $\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid \ell_i\} = [L : F] = |\text{Cl}_2(F)|$  for  $i = 1, 2$  by the decomposition law (specifically, the inert trick of Remark 3.4). Furthermore, any prime  $p \nmid \ell_4^* \ell_5^*$  splits into 2 or 4 primes in  $\mathbb{Q}(\sqrt{\ell_4^*}, \sqrt{\ell_5^*})/\mathbb{Q}$ , hence at least that many in the extension  $L/\mathbb{Q}$  (inclusion due to  $\ell_4^*, \ell_5^* > 0$ ). This time

$$\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid \ell_1 \ell_2 \ell_3\} \geq \underbrace{|\text{Cl}_2(F)| + |\text{Cl}_2(F)| + 2}_{\text{if } |\text{Cl}_2(F)| \geq \frac{1}{2}(3 + 2\sqrt{3}) = 3.2320\dots} \geq 3 + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$$

verifies the desired criterion when  $|\text{Cl}_2(F)| \geq 4$ .  $\square$

**3.2.3.  $F$ : imaginary quadratic field with two prime discriminants.** On the other hand, when  $\ell_4^* \ell_5^* < 0$ , taking the imaginary quadratic field  $F = \mathbb{Q}(\sqrt{\ell_4^* \ell_5^*}) \leq K_{(2)}^\infty$  in Proposition 3.5 gives Lemma 3.16.

**Lemma 3.16.** *If some two of the five prime discriminants, say  $\ell_4^*, \ell_5^*$ , have opposite sign, then the imaginary quadratic field  $K$  has infinite 2-tower if any of the following criteria hold:*

- (1)  $d_2 \text{Cl}(KL) \geq 2 + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$ ;
- (2)  $|\text{Cl}_2(F)| \geq 16$  and at least 2 of  $\ell_1, \ell_2, \ell_3$  is inert in  $F/\mathbb{Q}$ , i.e.  $\left(\frac{\ell_4^*}{p}\right)\left(\frac{\ell_5^*}{p}\right) = -1$  for at least 2 of  $p = \ell_1, \ell_2, \ell_3$ ;

(3)  $|\text{Cl}_2(F)| \geq 4$ , at least 1 of  $\ell_1, \ell_2, \ell_3$  is inert in  $F/\mathbb{Q}$ , and at least 1 of  $\ell_1, \ell_2, \ell_3$  splits completely in  $L/\mathbb{Q}$ .

Here  $F = \mathbb{Q}(\sqrt{p_4^* p_5^*})$  and  $L := F_{(2)}^1$  from Proposition 3.5 are totally imaginary.

**Example 3.17.** See the applications and examples under Theorems 4.20 (progress on matrix 32, using Lemma 3.16(2), with Example 4.21) and 4.22 (progress on matrices 16 and 28, using Lemma 3.16(3), with Example 4.23), both in the case where  $\Delta_K \not\equiv 4 \pmod{8}$  has 3 negative prime discriminants and  $d_4 \text{Cl}(K) = 0$ .

*Remark 3.18.* Since  $F$  is imaginary,  $\text{Cl}_2(F) = \text{Cl}_2^+(F) \simeq C_{2^n}$  for some  $n \geq 1$ , so by Rédei–Reichardt, the inequality  $|\text{Cl}_2(F)| \geq 4$  is equivalent to  $(\frac{\ell_4^*}{\ell_5^*}) = (\frac{\ell_5^*}{\ell_4^*}) = +1$ .

*Proof of Lemma 3.16(2).*  $L/\mathbb{Q}$  is totally imaginary, so by Proposition 3.5 it suffices to check  $\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid \ell_1 \ell_2 \ell_3\} - 1 - |\text{Cl}_2(F)| \geq 2 + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$ .

Say  $\ell_1, \ell_2$  are inert in  $F/\mathbb{Q}$ , so  $\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid \ell_i\} = [L : F] = |\text{Cl}_2(F)|$  for  $i = 1, 2$  by the decomposition law (specifically, the inert trick of Remark 3.4). Furthermore, any prime  $p \nmid \ell_4^* \ell_5^*$  splits into 2 or 4 primes in  $\mathbb{Q}(\sqrt{\ell_4^*}, \sqrt{\ell_5^*})/\mathbb{Q}$ , hence at least that many in the extension  $L/\mathbb{Q}$  (inclusion due to  $F$  imaginary). Thus

$$\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid \ell_1 \ell_2 \ell_3\} \geq \underbrace{|\text{Cl}_2(F)| + |\text{Cl}_2(F)| + 2}_{\text{if } |\text{Cl}_2(F)| \geq 5 + 2\sqrt{7} = 10.2915 \dots} \geq 3 + |\text{Cl}_2(F)| + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$$

verifies the desired criterion when  $|\text{Cl}_2(F)| \geq 16$ . □

*Proof of Lemma 3.16(3).*  $L/\mathbb{Q}$  is totally imaginary, so by Proposition 3.5 it suffices to check  $\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid \ell_1 \ell_2 \ell_3\} - 1 - |\text{Cl}_2(F)| \geq 2 + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$ .

Say  $\ell_1$  is inert in  $F/\mathbb{Q}$  and  $\ell_2$  splits completely in  $L/\mathbb{Q}$ , so  $\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid \ell_1\} = [L : F] = |\text{Cl}_2(F)|$  by the decomposition law, and  $\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid \ell_2\} = [L : \mathbb{Q}] = 2|\text{Cl}_2(F)|$ . Furthermore, any prime  $p \nmid \ell_4^* \ell_5^*$  splits into 2 or 4 primes in  $\mathbb{Q}(\sqrt{\ell_4^*}, \sqrt{\ell_5^*})/\mathbb{Q}$ , hence at least that many in the extension  $L/\mathbb{Q}$  (inclusion due to  $F$  imaginary). Thus

$$\#\{\wp \in \text{Spec } \mathcal{O}_L : \wp \mid \ell_1 \ell_2 \ell_3\} \geq \underbrace{|\text{Cl}_2(F)| + 2|\text{Cl}_2(F)| + 2}_{\text{if } |\text{Cl}_2(F)| \geq \frac{1}{2}(3 + 2\sqrt{3}) = 3.2320 \dots} \geq 3 + |\text{Cl}_2(F)| + 2\sqrt{1 + 2|\text{Cl}_2(F)|}$$

verifies the desired criterion when  $|\text{Cl}_2(F)| \geq 4$ . □

#### 4. APPLICATION TO MARTINET'S QUESTION

We now apply the lemmas from Section 3.2 to several sub-cases of open Rédei matrices  $R_K$  of rank 2 or 4 (corresponding by Rédei–Reichardt to  $d_4 \text{Cl}(K) = 2$  or  $d_4 \text{Cl}(K) = 0$ , respectively). We will use the labeling of Rédei matrices from Sueyoshi [49, 50] and Benjamin [3]. In this section, we often write Rédei matrices without the diagonal entries, which can be recovered by the fact that column sums are 0.

**4.1. 4-rank 2.** When  $K$  (with five prime discriminants  $p_i^*$ ) has  $d_4 \text{Cl}(K) = 2$ , there is exactly one family of open Rédei matrices, referred to as “Family  $\mathcal{D}_2$ ” (we use a different font to avoid confusion with matrix  $D_2$  in Section 4.3) by Benjamin [3, pp. 127–128] (and falling under “Case 60” in Sueyoshi [50, p. 181, with discussion on p. 184]; note that Benjamin has a minor typo in his listing of the Kronecker symbols in the first paragraph of [3, p. 127, Section 4. Case 1]); this is originally due to Benjamin [2] (2002). More precisely, the family

$\mathcal{D}_2$  consists of  $K$  with exactly three negative discriminants  $p_1^*, p_2^*, p_3^*$  (up to re-indexing) and  $\Delta_K \equiv 4 \pmod{8}$ —so say  $p_1^* = -4$ , up to re-indexing—and Rédei matrix  $R_K$  of the form

$$\left[ \begin{array}{c|cc|cc} - & 1 & 1 & 0 & 0 \\ \hline a_{21} & - & 1 & 1 & 1 \\ a_{31} & 0 & - & 1 & 1 \\ \hline 1 & 1 & 1 & - & a_{45} \\ 1 & 1 & 1 & a_{54}(= a_{54}) & - \end{array} \right],$$

with four specific possibilities (following Benjamin [3, p. 128]):

- (a)  $(a_{45}, a_{54}) = (0, 0)$  and  $(a_{21}, a_{31}) = (1, 0)$  (so in particular,  $a_{11} = 1$ );
- (b)  $(a_{45}, a_{54}) = (0, 0)$  and  $(a_{21}, a_{31}) = (0, 1)$  (so in particular,  $a_{11} = 1$ );
- (c)  $(a_{45}, a_{54}) = (1, 1)$  and  $(a_{21}, a_{31}) = (1, 0)$  (so in particular,  $a_{11} = 1$ );
- (d)  $(a_{45}, a_{54}) = (1, 1)$  and  $(a_{21}, a_{31}) = (1, 1)$  (so in particular,  $a_{11} = 0$ ).

Benjamin makes (positive) progress on matrices (a) [3, p. 128, Example 3], (b) [3, p. 128, Example 4], and (c) [3, p. 128, Examples 1 and 2]—but not (d). We now present some further progress on the  $\mathcal{D}_2$  family.

**Theorem 4.1** (Further progress on family  $\mathcal{D}_2$ ). *Suppose  $R_K \in \mathcal{D}_2$ , and set  $F := \mathbb{Q}(\sqrt{p_1^* p_4^* p_5^*})$  (imaginary quadratic field, so  $\text{Cl}(F) = \text{Cl}^+(F)$ ). Then  $p_2, p_3$  are inert in  $F/\mathbb{Q}$ .*

*Rédei–Reichardt says  $d_4 \text{Cl}_2^+(F) = (3 - 1) - 1 = 1$  (since  $R_F = \begin{bmatrix} - & 0 & 0 \\ 1 & - & \alpha \\ 1 & \alpha & - \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & \alpha & \alpha \\ 1 & \alpha & \alpha \end{bmatrix}$ , where  $\alpha := a_{45} = a_{54}$ ), so by Gauss’ genus theory,  $\text{Cl}_2(F) \simeq C_2 \oplus C_{2^n}$  for some  $n \geq 2$ . By Lemma 3.6(2),  $K$  has infinite 2-tower if  $|\text{Cl}_2(F)| \geq 16$ , i.e.  $n \geq 3$ , holds.*

*Remark 4.2.* In the remaining case  $\text{Cl}_2(F) \simeq C_2 \oplus C_4$  (for family  $\mathcal{D}_2$ ), it is plausible that group-theoretic methods could give helpful additional structure for the 2-tower of  $K$ .

**Example 4.3** (Examples with  $R_K = (d) \in \mathcal{D}_2$ ). Start with any three prime discriminants  $p_1^* = -4$  and  $p_4^*, p_5^* > 0$  (necessarily  $p_4, p_5 \equiv 1 \pmod{4}$ ) such that  $R_F = \begin{bmatrix} - & 0 & 0 \\ 1 & - & 1 \\ 1 & 1 & - \end{bmatrix}$ . It is then standard (Chinese remainder theorem and Dirichlet’s theorem) to find primes  $p_2, p_3 \equiv 3 \pmod{4}$  such that  $p_2^*, p_3^* \equiv 1 \pmod{4}$  satisfy the correct Kronecker symbols with respect to each other and with respect to  $p_1, p_4, p_5$ .

For instance, based on <http://oeis.org/A046013> (listing imaginary  $F$  with  $\#\text{Cl}(F) = 16$ ), one could take  $F = \mathbb{Q}(\sqrt{-740})$ , i.e.  $(p_1^*, p_4^*, p_5^*) = (-4, +5, +37)$  (as  $(\frac{+5}{2}) = (\frac{+37}{2}) = -1$  and  $(\frac{+37}{5}) = -1$ ).

**4.2. Five negative prime discriminants, 4-rank 0, discriminant not 4 (mod 8).** When  $K$  has five negative prime discriminants  $p_i^*$  all not equal to  $-4$ , and  $d_4 \text{Cl}(K) = 0$ , there are two open Rédei matrices, called  $A$  (resp. (k)) and  $B$  (resp. (l)) in [3, p. 137, Section 8. Case 5] (resp. [49, p. 335]):

$$A = \begin{bmatrix} - & 1 & 1 & 0 & 1 \\ 0 & - & 1 & 1 & 0 \\ 0 & 0 & - & 1 & 1 \\ 1 & 0 & 0 & - & 1 \\ 0 & 1 & 0 & 0 & - \end{bmatrix}; \quad B = \begin{bmatrix} - & 1 & 1 & 0 & 0 \\ 0 & - & 1 & 1 & 0 \\ 0 & 0 & - & 1 & 1 \\ 1 & 0 & 0 & - & 1 \\ 1 & 1 & 0 & 0 & - \end{bmatrix}.$$

*Remark 4.4.* We have made progress on  $A$  (Theorem 4.6) but not  $B$ , which “looks harder” to us. Note that  $B$  is a circulant matrix, so it is certainly harder to exploit any asymmetries.

**Example 4.5** (Relatively small examples of  $B$ ).  $R_K = B$ , for instance, when the prime discriminant tuple  $(p_i^*)_{i \in \mathbb{Z}/5\mathbb{Z}}$  equals

- $(-3, -8, -23, -7, -19)$ ;
- $(-3, -11, -8, -7, -31)$ ; or
- $(-3, -11, -q, -7, -31)$ , where  $q$  denotes a prime  $107 \pmod{3 \cdot 11 \cdot 7 \cdot 31 \cdot 4}$ , e.g.  $q = 107 + n \cdot 3 \cdot 11 \cdot 7 \cdot 31 \cdot 4$  for  $n = 0, 1, 3, 9, 10, 21, 23, 33, 34, \dots$

Also, if  $F := \sqrt{(-31)(-3)(-11)} = \sqrt{-1023}$  or  $F := \sqrt{(-7)(-19)(-3)} = \sqrt{-399}$  accordingly (in the spirit of Proposition 3.5), then  $|\text{Cl}(F)| = 16$  (so  $\text{Cl}(F) \simeq C_2 \oplus C_8$ ) according to <http://oeis.org/A046013>, which may be helpful for computations.

**Theorem 4.6** (Progress on matrix  $A$ ). *Suppose  $R_K = A$ , and set  $F := \mathbb{Q}(\sqrt{p_3^* p_4^* p_5^*})$  (imaginary quadratic field, so  $\text{Cl}(F) = \text{Cl}^+(F)$ ). Then  $a_{3j} + a_{4j} + a_{5j} = 1$  (in  $\mathbb{F}_2$ ) for  $j = 1, 2$ , i.e.  $p_1, p_2$  are inert in  $F/\mathbb{Q}$ .*

*Rédei–Reichardt says  $d_4 \text{Cl}_2^+(F) = (3 - 1) - 1 = 1$  (since  $R_F = \begin{bmatrix} - & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & - \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$ ), so by Gauss' genus theory,  $\text{Cl}_2(F) \simeq C_2 \oplus C_{2^n}$  for some  $n \geq 2$ . By Lemma 3.6(2),  $K$  has infinite 2-tower if  $|\text{Cl}_2(F)| \geq 16$ , i.e.  $n \geq 3$ , holds.*

*Remark 4.7.* In the remaining case  $\text{Cl}_2(F) \simeq C_2 \oplus C_4$  (for matrix  $A$ ), it is plausible that group-theoretic methods could give helpful additional structure for the 2-tower of  $K$ .

**Example 4.8** (Examples with  $R_K = A$ ). Start with any three negative prime discriminants  $p_3^*, p_4^*, p_5^* \neq -4$  such that  $|\text{Cl}_2(F)| \geq 8$ , or equivalently  $\text{rank}_{\mathbb{F}_2} R_F \leq 1$ , i.e.  $R_F = \begin{bmatrix} - & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & - \end{bmatrix}$  up to re-indexing. It is then standard to find primes  $p_1, p_2 \equiv 3 \pmod{4}$  such that  $p_1^*, p_2^* \equiv 1 \pmod{4}$  satisfy the correct Kronecker symbols with respect to each other and with respect to  $p_3, p_4, p_5$ .

For instance, based on <http://oeis.org/A046013> (listing imaginary  $F$  with  $\#\text{Cl}(F) = 16$ ), one could take  $F = \mathbb{Q}(\sqrt{-399})$  (i.e.  $(p_3^*, p_4^*, p_5^*) = (-7, -19, -3)$ , as  $(\frac{-19}{-7}) = +1$ ,  $(\frac{-3}{-7}) = +1$ , and  $(\frac{-19}{-3}) = -1$ ) or  $F = \mathbb{Q}(\sqrt{-1023})$  (i.e.  $(p_3^*, p_4^*, p_5^*) = (-31, -3, -11)$ ).

**4.3. Five negative prime discriminants, 4-rank 0, discriminant 4 (mod 8).** When  $K$  has five negative prime discriminants  $p_i^*$  with  $p_1^* = -4$  (up to re-indexing), and  $d_4 \text{Cl}(K) = 0$ , there are three open Rédei matrices, called  $C$  (resp. (o)) and  $D$  (resp. (p)) in [3, p. 138, Section 8. Case 5] (resp. [49, p. 336]), with (following Benjamin)  $D$  split into two cases:

$$C = \begin{bmatrix} - & 1 & 1 & 1 & 1 \\ a_{21} & - & 1 & 0 & 1 \\ a_{31} & 0 & - & 1 & 1 \\ a_{41} & 1 & 0 & - & 1 \\ 1 & 0 & 0 & 0 & - \end{bmatrix}; \quad D_1 = \begin{bmatrix} - & 1 & 1 & 1 & 1 \\ a_{21} & - & 1 & 1 & 0 \\ 1 & 0 & - & 1 & 1 \\ 0 & 0 & 0 & - & 1 \\ 1 & 1 & 0 & 0 & - \end{bmatrix}; \quad D_2 = \begin{bmatrix} - & 1 & 1 & 1 & 1 \\ a_{21} & - & 1 & 1 & 0 \\ 0 & 0 & - & 1 & 1 \\ 1 & 0 & 0 & - & 1 \\ a_{51} & 1 & 0 & 0 & - \end{bmatrix}.$$

*Remark 4.9.* Benjamin has ambiguous typos in his  $D_1, D_2$ , with  $a_{31} = a_{41}$  (but see “(p) [ $d_4 \text{Cl}(K) = 1$ ] if and only if  $a_{31} = a_{41}$ ” from Sueyoshi), so our correction *arbitrarily* associates  $D_1$  with  $(a_{31}, a_{41}) = (1, 0)$  and  $D_2$  with  $(a_{31}, a_{41}) = (0, 1)$ . We thank the anonymous referee for observing that Sueyoshi [49, p. 337] has resolved the case  $(a_{31}, a_{41}, a_{51}) = (1, 0, 0)$  in matrix  $D$  (or (p) in Sueyoshi's terminology).

*Remark 4.10.* We have made progress on  $C$  (Theorem 4.11) and  $D_1$  (Theorem 4.13) but not  $D_2$ , which “looks hardest” to us. In some sense  $C$  and  $D_1$  closely resemble  $A$  from Section 4.2, while  $D_2$  closely resembles  $B$ .

**Theorem 4.11** (Progress on matrix  $C$ ). *Suppose  $R_K = C$  (in particular,  $p_1^* = -4$ ).*

- (1) *If  $a_{31} + a_{41} = 0$ , and we set  $F := \mathbb{Q}(\sqrt{p_3^* p_4^* p_5^*})$ , then  $p_1, p_2$  are inert in  $F/\mathbb{Q}$ , and  $R_F = \begin{bmatrix} - & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & - \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$  has rank 1.*
- (2) *If  $a_{21} + a_{41} = 0$ , and we set  $F := \mathbb{Q}(\sqrt{p_2^* p_4^* p_5^*})$ , then  $p_1, p_3$  are inert in  $F/\mathbb{Q}$ , and  $R_F = \begin{bmatrix} - & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & - \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}$  has rank 1.*
- (3) *If  $a_{21} + a_{31} = 0$ , and we set  $F := \mathbb{Q}(\sqrt{p_2^* p_3^* p_5^*})$ , then  $p_1, p_4$  are inert in  $F/\mathbb{Q}$ , and  $R_F = \begin{bmatrix} - & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & - \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$  has rank 1.*

*These three cases are not mutually exclusive, but for any  $K$  with  $R_K = C$ , at least one will apply, since it is impossible to have  $a_{u1} + a_{v1} = 1$  in  $\mathbb{F}_2$  for all pairs  $u, v \in \{2, 3, 4\}$ .*

*In each case,  $F$  is imaginary, so  $\text{Cl}(F) = \text{Cl}^+(F)$  has 4-rank  $(3 - 1) - 1 = 1$  by Rédei–Reichardt, and thus  $\text{Cl}_2(F) \simeq C_2 \oplus C_{2^n}$  for some  $n \geq 2$ . By Lemma 3.6(2),  $K$  has infinite 2-tower if  $|\text{Cl}_2(F)| \geq 16$ , i.e.  $n \geq 3$ , holds in any of the three cases applying to  $K$ .*

**Example 4.12** (Examples with  $R_K = C$ ). Start with any three negative prime discriminants  $p_3^*, p_4^*, p_5^* \equiv -3 \pmod{8}$  such that  $|\text{Cl}_2(F)| \geq 8$ , or equivalently  $\text{rank}_{\mathbb{F}_2} R_F \leq 1$ , i.e.  $R_F = \begin{bmatrix} - & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & - \end{bmatrix}$  up to re-indexing; then  $p_1^* = -4, p_3^*, p_4^*, p_5^*$  satisfy permitted Rédei sub-matrix (specifically, with  $a_{31} = a_{41} = 1$ , which lies in the first case of Theorem 4.11). It is then standard to find a prime  $p_2 \equiv 3 \pmod{4}$  such that  $p_2^* \equiv 1 \pmod{4}$  satisfies the correct Kronecker symbols with respect to  $p_1 = 2, p_3, p_4, p_5$ .

For instance, based on <http://mathworld.wolfram.com/ClassNumber.html> (listing imaginary  $F$  with  $\#\text{Cl}(F) = 16$ ), one could take  $F = \mathbb{Q}(\sqrt{-2211})$  (i.e.  $(p_3^*, p_4^*, p_5^*) = (-67, -3, -11)$ , as  $(\frac{-67}{3}) = -1$ ,  $(\frac{-67}{11}) = -1$ , and  $(\frac{-11}{3}) = +1$ ). We thank Ian Whitehead for providing this example.

**Theorem 4.13** (Progress on matrix  $D_1$ ). *Suppose  $R_K = D_1$  (in particular,  $p_1^* = -4$ ), and set  $F := \mathbb{Q}(\sqrt{p_1^* p_3^* p_4^*})$  (imaginary quadratic field, so  $\text{Cl}(F) = \text{Cl}^+(F)$ ). Then  $p_2, p_5$  are inert in  $F/\mathbb{Q}$ .*

*Rédei–Reichardt says  $d_4 \text{Cl}_2^+(F) = (3 - 1) - 1 = 1$  (since  $R_F = \begin{bmatrix} - & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & - \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$ ), so  $\text{Cl}_2(F) \simeq C_2 \oplus C_{2^n}$  for some  $n \geq 2$ . By Lemma 3.6(2),  $K$  has infinite 2-tower if  $|\text{Cl}_2(F)| \geq 16$ , i.e.  $n \geq 3$ , holds.*

**Example 4.14** (An infinite family with  $R_K = D_1$ ). Fix  $n \geq 2$ . Lopez [33, Proposition 1.1] proves that any imaginary quadratic field  $E = \mathbb{Q}(\sqrt{(-4)(-q_3)(-q_4)})$  with  $q_3 \equiv 11 \pmod{24}$ ,  $q_4 \equiv 7 \pmod{24}$ , and  $q_3 + q_4 = 2(3m^2)^{2^{n-1}}$  for some odd integer  $m$  has 2-class group exactly  $\text{Cl}_2(F) \simeq C_2 \oplus C_{2^n}$ , and also that there are infinitely many such quadratic fields  $E$  [33, Theorem 1.3]. For such  $E$  we easily check  $R_E = \begin{bmatrix} - & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & - \end{bmatrix}$ , so we may find  $K$  with  $(p_1^*, p_3^*, p_4^*) = (-4, -q_3, -q_4)$  (here  $F = E$ ).

Alternatively, based on <http://oeis.org/A046013> (listing imaginary  $F$  with  $\#\text{Cl}(F) = 16$ ), one could take  $F = \mathbb{Q}(\sqrt{-1876})$  (i.e.  $(p_1^*, p_3^*, p_4^*) = (-4, -67, -7)$ , as  $(\frac{-7}{2}) = +1$ ,  $(\frac{-67}{2}) = -1$ , and  $(\frac{-67}{7}) = (\frac{+3}{7}) = -1$ ) or  $F = \mathbb{Q}(\sqrt{-2004})$  (i.e.  $(p_1^*, p_3^*, p_4^*) = (-4, -3, -167)$ ).

It is then standard to find primes  $p_2, p_5 \equiv 3 \pmod{4}$  such that  $p_2^*, p_5^* \equiv 1 \pmod{4}$  satisfy the correct Kronecker symbols with respect to each other and  $p_1, p_3, p_4$ .

**4.4. Three negative prime discriminants, 4-rank 0, discriminant not 4 (mod 8).** When  $K$  has five prime discriminants  $p_i^*$  all not equal to  $-4$ , exactly three negative prime



discriminants (say  $p_1^*, p_2^*, p_3^* < 0 < p_4^*, p_5^*$ ), and  $d_4 \text{Cl}(K) = 0$ , there are seven open Rédei matrices, numbered 16, 28, 30, 32, 34, 49 (from [3, p. 140, Section 9. Case 6] or [50, pp. 179–180]), with (following Benjamin) 34 split into two cases:

$$\begin{aligned} \#16 &= \left[ \begin{array}{ccc|cc} - & 1 & 1 & 1 & 0 \\ 0 & - & 1 & 0 & 1 \\ 0 & 0 & - & 1 & 0 \\ \hline 1 & 0 & 1 & - & 1 \\ 0 & 1 & 0 & 1 & - \end{array} \right]; & \#28 &= \left[ \begin{array}{ccc|cc} - & 1 & 1 & 0 & 1 \\ 0 & - & 1 & 1 & 1 \\ 0 & 0 & - & 0 & 1 \\ \hline 0 & 1 & 0 & - & 1 \\ 1 & 1 & 1 & 1 & - \end{array} \right]; & \#32 &= \left[ \begin{array}{ccc|cc} - & 1 & 1 & 1 & 1 \\ 0 & - & 1 & 0 & 1 \\ 0 & 0 & - & 1 & 0 \\ \hline 1 & 0 & 1 & - & 1 \\ 1 & 1 & 0 & 1 & - \end{array} \right]; \\ \#34a &= \left[ \begin{array}{ccc|cc} - & 1 & 1 & 1 & 1 \\ 0 & - & 1 & 0 & 1 \\ 0 & 0 & - & 1 & 1 \\ \hline 1 & 0 & 1 & - & 0 \\ 1 & 1 & 1 & 0 & - \end{array} \right]; & \#49 &= \left[ \begin{array}{ccc|cc} - & 1 & 0 & 0 & 1 \\ 0 & - & 1 & 1 & 1 \\ 1 & 0 & - & 1 & 1 \\ \hline 0 & 1 & 1 & - & 0 \\ 1 & 1 & 1 & 0 & - \end{array} \right]; & \#30 &= \left[ \begin{array}{ccc|cc} - & 1 & 1 & 0 & 1 \\ 0 & - & 1 & 1 & 0 \\ 0 & 0 & - & 1 & 1 \\ \hline 0 & 1 & 1 & - & 1 \\ 1 & 0 & 1 & 1 & - \end{array} \right]; \\ & & & & \#34b &= \left[ \begin{array}{ccc|cc} - & 1 & 1 & 1 & 1 \\ 0 & - & 1 & 0 & 1 \\ 0 & 0 & - & 1 & 1 \\ \hline 1 & 0 & 1 & - & 1 \\ 1 & 1 & 1 & 1 & - \end{array} \right]. \end{aligned}$$

*Remark 4.15.* Benjamin has a single typo in matrix 16 ( $a_{15}$  should be 0, not 1) and several typos in matrix 32.

*Remark 4.16.* We have made progress on matrices 16 and 28 (Theorems 4.22 and 4.24), matrix 32 (Theorem 4.20), and matrices 34a and 49 (Theorem 4.17), but not matrices 30 and 34b.

**Theorem 4.17** (Progress on matrices 34a and 49). *Suppose  $R_K \in \{\#34a, \#49\}$ , and set  $F := \mathbb{Q}(\sqrt{p_4^* p_5^*})$  (real quadratic field). Then  $p_2$  is inert in  $F/\mathbb{Q}$  if  $R_K = \#34a$ , and  $p_1$  is inert in  $F/\mathbb{Q}$  if  $R_K = \#49$ .*

*Rédei-Reichardt says  $d_4 \text{Cl}_2^+(F) = (2 - 1) - 0 = 1$  (since  $R_F = \begin{bmatrix} - & 0 \\ 0 & - \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ ), so  $\text{Cl}_2^+(F) \simeq C_{2^n}$  for some  $n \geq 2$  (so  $\text{Cl}_2(F)$  is cyclic of order either  $2^n$  or  $2^{n-1}$ ). By Lemma 3.11(2),  $K$  has infinite 2-tower if  $|\text{Cl}_2(F)| \geq 8$  holds.*

**Example 4.18** (Examples for 34a and 49). Start with any two positive prime discriminants  $p_4^*, p_5^*$  such that  $\text{rank}_{\mathbb{F}_2} R_F = 0$ , i.e.  $R_F = \begin{bmatrix} - & 0 \\ 0 & - \end{bmatrix}$ . It is then standard to find primes  $p_1, p_2, p_3 \equiv 3 \pmod{4}$  such that (the three negative prime discriminants)  $p_1^*, p_2^*, p_3^* \equiv 1 \pmod{4}$  satisfy the correct Kronecker symbols with respect to each other and with respect to  $p_4, p_5$ .

For instance, based on <http://oeis.org/A081364> or <http://oeis.org/A218158> (to find suitable real  $F$  with  $\# \text{Cl}(F) = 8$ ), one could take  $F = \mathbb{Q}(\sqrt{906})$  (i.e.  $(p_4^*, p_5^*) = (+8, +113)$ ) or  $F = \mathbb{Q}(\sqrt{2605})$  (i.e.  $(p_4^*, p_5^*) = (+5, +521)$ ).

**Example 4.19** (Cf. Remark 3.10). Schmithals [46] (and independently, Hajir [16, p. 17, last paragraph] and Mouhib [38, Proposition 3.3], [39]) used  $F = \mathbb{Q}(\sqrt{(+5)(+461)})$  (note  $\left(\frac{+5}{+461}\right) = \left(\frac{+461}{5}\right) = +1$ ) with  $\# \text{Cl}(F) = 16$  (in particular  $|\text{Cl}_2(F)| \geq 16$ , a stronger assumption than  $|\text{Cl}_2(F)| \geq 8$ ) to prove that  $\mathbb{Q}(\sqrt{(-11)(+5)(+461)})$  has infinite 2-tower. As a corollary, cases 34a and 49 already had examples with proven infinite 2-towers at the time of Benjamin's paper [3], but still 34a and 49 remain open in general.

**Theorem 4.20** (Progress on matrix 32). *Suppose  $R_K = \#32$ , and set  $F := \mathbb{Q}(\sqrt{p_3^* p_5^*})$  (imaginary quadratic field, so  $\text{Cl}^+(F) = \text{Cl}(F)$ ). Then  $p_1, p_2$  are inert in  $F/\mathbb{Q}$ .*

*Rédei–Reichardt says  $d_4 \text{Cl}_2^+(F) = (2 - 1) - 0 = 1$  (since  $R_F = \begin{bmatrix} - & 0 \\ 0 & - \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ ), so  $\text{Cl}_2(F) \simeq C_{2^n}$  for some  $n \geq 2$ . By Lemma 3.16(2),  $K$  has infinite 2-tower if  $|\text{Cl}_2(F)| \geq 16$ , i.e.  $n \geq 4$ , holds.*

**Example 4.21** (An infinite family with  $R_K = \#32$ ). Fix  $n \geq 1$ . Dominguez–Miller–Wong [9] prove that any imaginary quadratic field  $E = \mathbb{Q}(\sqrt{(-q_3)(+q_5)})$  with  $q_3 \equiv 3 \pmod{8}$ ,  $q_5 \equiv 5 \pmod{8}$ , and  $q_5 + q_3 = 4(2M^2)^{2^{n-1}}$  for some odd integer  $M$  has 2-class group exactly  $\text{Cl}_2(F) \simeq C_{2^n}$ , and also that there are infinitely many such quadratic fields  $E$  [9, Theorem 3.1]. For such  $E$  we easily check that  $R_E = \begin{bmatrix} - & 0 \\ 0 & - \end{bmatrix}$  if and only if  $n \geq 2$ , so we may find  $K$  with  $(p_3^*, p_5^*) = (-q_3, +q_5)$  (here  $F = E$ ).

It is then standard to find primes  $p_1, p_2, p_4$  with  $p_1, p_2 \equiv 3 \pmod{4}$  and  $p_4 \equiv 1 \pmod{4}$  such that  $p_1^*, p_2^* < 0$  and  $p_4^* > 0$  satisfy the correct Kronecker symbols with respect to each other and with respect to  $p_3, p_5$ .

**Theorem 4.22** (Progress on matrices 16 and 28). *Suppose  $R_K \in \{\#16, \#28\}$ .*

- (1) *If  $R_K = \#16$ , then set  $F := \mathbb{Q}(\sqrt{p_3^* p_5^*})$ .*
- (2) *If  $R_K = \#28$ , then set  $F := \mathbb{Q}(\sqrt{p_3^* p_4^*})$ .*

*In each case,  $p_2$  is inert in  $F/\mathbb{Q}$ , the Rédei matrix  $R_F = \begin{bmatrix} - & 0 \\ 0 & - \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$  has rank 0, and  $F$  is imaginary, so  $\text{Cl}(F) = \text{Cl}^+(F)$  has 4-rank  $(2 - 1) - 0 = 1$  by Rédei–Reichardt, and thus  $\text{Cl}_2(F) \simeq C_{2^n}$  for some  $n \geq 2$ . By Lemma 3.16(3),  $K$  has infinite 2-tower if  $p_1$  splits completely in  $L := F_{(2)}^1$  (note that  $|\text{Cl}_2(F)| \geq 4$  automatically holds, from  $n \geq 2$ ).*

**Example 4.23.** We describe the method for  $R_K = \#16$ ; the case  $R_K = \#28$  is analogous. For  $R_K = \#16$ , one starts with any appropriate  $p_3^*, p_5^* \neq -4$  (so  $p_3^* < 0 < p_5^*$ ) satisfying  $\left(\frac{p_3^*}{p_5^*}\right) = \left(\frac{p_5^*}{p_3^*}\right) = +1$  (so  $|\text{Cl}_2(F)| \geq 4$  automatically), and then takes  $p_1 \equiv 3 \pmod{4}$  totally split in  $L$ , guaranteeing  $\left(\frac{p_3^*}{p_1}\right) = \left(\frac{p_5^*}{p_1}\right) = +1$  in view of the tower  $F \leq \mathbb{Q}(\sqrt{p_3^*}, \sqrt{p_5^*}) \leq L$ .

Such  $p_1$  exists by Chebotarev’s density theorem:  $\sqrt{-1} \notin F$  means  $\sqrt{-1} \notin F_{\text{gen}} = \mathbb{Q}(\sqrt{p_3^*}, \sqrt{p_5^*})$ , so  $F(\sqrt{-1})/F$  is ramified, so  $\sqrt{-1} \notin L$ . So  $L/\mathbb{Q} < L(i)/\mathbb{Q}$  is a *proper* inclusion of Galois extensions, whence by Neukirch [40, p. 548, Ch. VII, Sec. 13, Corollary 13.10] there exist infinitely many primes  $p_1$  splitting completely in  $L$  but *not* splitting completely in  $L(i)$ . (Of course, any prime splitting completely in  $L(i)$  must automatically split completely in  $L$ .) There is also a more direct approach:  $\text{Gal}(L(i)/\mathbb{Q}) = \text{Gal}(L/\mathbb{Q}) \times \text{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ , so we may apply Chebotarev to the conjugacy class of size 1 consisting of the generator of  $\text{Gal}(\mathbb{Q}(i)/\mathbb{Q})$ .

It is then standard to find primes  $p_2, p_4$  with  $p_2 \equiv 3 \pmod{4}$  and  $p_4 \equiv 1 \pmod{4}$  such that  $p_2^* < 0$  and  $p_4^* > 0$  satisfy the correct Kronecker symbols with respect to each other and with respect to  $p_1, p_3, p_5$ .

**Theorem 4.24** (Alternative progress on matrix 28, analogous to Theorem 4.6 for matrix A). *Suppose  $R_K = \#28$ , and set  $F := \mathbb{Q}(\sqrt{p_1^* p_2^* p_3^*})$  (imaginary quadratic field, so  $\text{Cl}(F) = \text{Cl}^+(F)$ ). Then  $p_4, p_5$  are inert in  $F/\mathbb{Q}$ .*

*Rédei–Reichardt says  $d_4 \text{Cl}_2^+(F) = (3 - 1) - 1 = 1$  (since  $R_F = \begin{bmatrix} - & 1 & 1 \\ 0 & 0 & - \end{bmatrix} = \begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \end{bmatrix}$ ), so  $\text{Cl}_2(F) \simeq C_2 \oplus C_{2^n}$  for some  $n \geq 2$ . By Lemma 3.6(2),  $K$  has infinite 2-tower if  $|\text{Cl}_2(F)| \geq 16$ , i.e.  $n \geq 3$ , holds.*

**Example 4.25.** The examples here are analogous to those (Example 4.8) for matrix  $A$  from the case of five negative discriminants.

## 5. PRIME SPLITTING BARRIER, AND EXTENSION QUESTION OF INDEPENDENT INTEREST

This section (including Question 5.5 of independent interest) is motivated by our failed attempts at applying (to the open cases of Martinet's question) Proposition 3.3 and Remark 3.4 on the decomposition law in Hilbert 2-class fields. The results in this section, as well as our extension question (Question 5.5), stem from the key “classical principal genus theorem” (CPGT) over the rationals.

**Theorem 5.1** (CPGT over  $\mathbb{Q}$ ; see [12, Proposition 2.12]). *Let  $K/\mathbb{Q}$  be a quadratic extension, and  $\sigma$  a generator of  $\text{Gal}(K/\mathbb{Q})$ . Fix a nonzero fractional ideal  $I$  of  $K$ . Then the ideal class  $[I] \in \text{Cl}(K)$  lies in  $\text{Cl}(K)^{1-\sigma}$  (which here coincides with  $\text{Cl}(K)^2$ ) if and only if the ideal norm  $N_{K/\mathbb{Q}}(I) = I\sigma(I) \cap \mathbb{Q}$  takes the form  $\alpha\mathcal{O}_{\mathbb{Q}}$  for some  $\alpha \in \mathbb{Q}^\times$  that is a local norm (or norm residue) at all (finite and infinite) ramified primes in  $K/\mathbb{Q}$ .*

*Remark 5.2.* Dominguez, Miller, and Wong [9] similarly used Hasse's “fundamental criterion” [18, p. 345] to prove the infinitude of imaginary quadratic fields  $K$  with cyclic 2-class groups  $C_{2^n}$  for any  $n \geq 1$ , and Lopez [33] extended their method to 2-class groups  $C_2 \oplus C_{2^n}$  for  $n \geq 1$ . Recall that these results give a wealth of examples in Examples 4.21 and 4.14, respectively.

We now fully work out two specific applications, originally motivated by some SAGE tests based on attempts at modifying Lemmas 3.11 (for a concrete example see Example 3.12) and 3.6.

**Theorem 5.3** (Cf. Dominguez–Miller–Wong [9, proof of Lemma 2.3]). *Fix distinct primes  $\ell_1, \ell_2 \equiv 1 \pmod{4}$ . Let  $F = \mathbb{Q}(\sqrt{\ell_1\ell_2})$ , so  $\text{Cl}_2(F) \simeq C_{2^n}$  for some  $n \geq 1$ . Let  $p$  be a prime with  $(\frac{\ell_1}{p}) = (\frac{\ell_2}{p}) = -1$ . Then  $(p)$  splits into exactly 2 primes in the extension  $F_{(2)}^1/\mathbb{Q}$ .*

*Proof.* The rational prime  $(p)$  splits into 2 primes  $\mathfrak{p}_1, \mathfrak{p}_2$  in  $F/\mathbb{Q}$ , of ideal norm  $p\mathbb{Z}$ . Using the Kronecker symbol conditions on  $\ell_1, \ell_2$ , it is standard to check that neither  $p$  nor  $-p$  is a local norm at either of the ramified primes  $\ell_1, \ell_2$ . By Theorem 5.1 applied to  $F/\mathbb{Q}$ , the ideal classes  $[\mathfrak{p}_i] \in \text{Cl}(F)$  must lie outside of  $\text{Cl}(F)^2$ , so their orders are divisible by  $2^n$ , the size of the largest cyclic 2-subgroup of  $\text{Cl}(F)$ . Thus  $\mathfrak{p}_1, \mathfrak{p}_2$  are inert in  $F_{(2)}^1/F$  by the decomposition law (Proposition 3.3).  $\square$

**Theorem 5.4** (Cf. Lopez [33, proof of Proposition 2.3]). *Fix distinct primes  $\ell_1, \ell_2, \ell_3 \equiv 3 \pmod{4}$ . Let  $F = \mathbb{Q}(\sqrt{\ell_1^*\ell_2^*\ell_3^*})$  be an imaginary quadratic field with  $\text{Cl}_2(F) = \text{Cl}_2^+(F) \simeq C_2 \oplus C_{2^n}$  for some  $n \geq 2$ ; by genus theory and Rédei–Reichardt, without loss of generality suppose  $R_F = \begin{bmatrix} - & 1 & 1 \\ 0 & 0 & - \end{bmatrix}$ . Take a prime  $p \nmid \Delta_F$  and any prime  $\mathfrak{p} \mid p$  of  $F$ . Then  $\mathfrak{p}$  splits into exactly 2 primes in the extension  $F_{(2)}^1/F$  if and only if  $((\frac{\ell_1^*}{p}), (\frac{\ell_2^*}{p}), (\frac{\ell_3^*}{p})) \in \{(+1, -1, -1), (-1, +1, -1)\}$ .*

*Proof.* By the decomposition law (Proposition 3.3),  $\mathfrak{p}$  splits into exactly 2 primes in  $F_{(2)}^1/F$  if and only if the ideal class  $[\mathfrak{p}] \in \text{Cl}(F)$  has order divisible by  $2^n$ ; if and only if the  $\text{Cl}(F)[2]$ -coset  $[\mathfrak{p}] \cdot \text{Cl}(F)[2]$  is disjoint from  $\text{Cl}(F)^2$ .

But since  $F$  is imaginary, genus theory says the 2-torsion  $\text{Cl}(F)[2] \leq \text{Cl}_2(F)$  is generated by the (ideal classes of the) ramified primes  $L_1, L_2, L_3$  of  $F$ , defined by  $(\ell_i) = L_i^2$ . So by Theorem 5.1,  $\mathfrak{p}$  (of ideal norm  $p\mathbb{Z}$  if  $(p)$  splits in  $F/\mathbb{Q}$ , and  $p^2\mathbb{Z}$  if  $(p)$  is inert) splits into exactly 2 primes in  $F_{(2)}^1/F$  if and only if  $(p)$  splits in  $F/\mathbb{Q}$  and  $\epsilon p \prod \ell_i^{\ell_i}$  is never (for any

choice  $\epsilon = \pm 1$  and  $t_i \in \mathbb{F}_2$ ) a local norm at all four ramified primes  $\infty, \ell_1, \ell_2, \ell_3$ . By standard computations (for instance, based on Hensel's lemma or Hilbert symbols), this is the case unless and only unless  $(p)$  is inert or  $((\frac{\ell_1^*}{p}), (\frac{\ell_2^*}{p}), (\frac{\ell_3^*}{p})) \in \{(+1, +1, +1), (-1, -1, +1)\}$ ; in other words, if and only if  $((\frac{\ell_1^*}{p}), (\frac{\ell_2^*}{p}), (\frac{\ell_3^*}{p})) \in \{(+1, -1, -1), (-1, +1, -1)\}$ , as desired.  $\square$

We now raise a natural extension question of independent interest.

**Question 5.5.** *Let  $F/\mathbb{Q}$  be a quadratic field with prime discriminant factorization  $\Delta_F = \ell_1^* \cdots \ell_t^*$ , with  $t \geq 1$ . Take a rational prime  $p \nmid \Delta_F$ , and any prime  $\mathfrak{p} \mid p$  in  $F$ . Then is it true that the condition “the ideal class  $[\mathfrak{p}]$  has order divisible by the largest possible 2-power order in  $\text{Cl}(F)$ ” depends only on the prime discriminants  $\ell_1^*, \dots, \ell_t^*$  and the Kronecker symbols  $(\frac{\ell_i^*}{p})$  for  $1 \leq i \leq t$ ? What if we work with the narrow class group  $\text{Cl}^+(F)$  instead of  $\text{Cl}(F)$ ? If this is false, is there an interesting correct statement along these lines?*

*Remark 5.6.* The methods from Theorems 5.3 and 5.4 only apply when the 2-class group  $\text{Cl}_2(F)$  is a direct sum of finitely many copies of  $C_2$  and  $C_{2^n}$ , for some  $n \geq 1$ , and the 2-torsion  $\text{Cl}(F)[2]$  is generated by the ideal classes of the ramified primes in  $F/\mathbb{Q}$ . In this special case, the order divisibility condition in question actually only depends on the Kronecker symbols  $(\frac{\ell_i^*}{p})$  and  $(\frac{\ell_j^*}{p})$  for distinct indices  $i, j \in \{1, \dots, t\}$ .

However, based on SAGE data (not assuming any conjectures such as GRH), this stronger correspondence does not hold in general; for example, take  $F$  with  $t = 4$  and  $(\ell_1^*, \ell_2^*, \ell_3^*, \ell_4^*) = (+5, +29, +109, \ell_4)$  with all  $\ell_i \equiv 1 \pmod{4}$ ; then the patterns differ for  $\ell_4 = 661$  and  $\ell_4 = 2609$  although the Rédei matrices  $R_F$  do not. (In both cases, SAGE says  $\text{Cl}(F) \simeq C_8 \oplus C_4 \oplus C_2$  and  $\text{Cl}^+(F) \simeq C_8 \oplus C_4 \oplus C_4$ .)

```
R.<x> = PolynomialRing(QQ)
p1 = +5; p2 = +29; p3 = +109
#p4 = +661
p4 = +2609
F.<d> = (x^2 - p1*p2*p3*p4).splitting_field(); F
print F.class_group(); print F.narrow_class_group()
Cl = F.class_group()

PrimeCount = 0; OrderCount = [0 for j in range(100)] #keep
    track of distribution of orders

for i in range(100000):
    p = i
    if is_prime(p) and (kronecker_symbol(p1,p) == +1) and (
        kronecker_symbol(p2,p) == -1) and (kronecker_symbol(p3,p)
        ) == -1) and (kronecker_symbol(p4,p) == +1): #exactly
        orders 2,4 occur for 661; exactly order 8 occurs for
        2609
        PrimeCount += 1
        J = F.ideal(p); #J
        I = J.prime_factors()[0]; #J.prime_factors()
```

```

OrderI = Cl(I).order(); #OrderI
OrderCount[OrderI] += 1

print PrimeCount
print OrderCount

```

*Remark 5.7.* It may be helpful to consider the criteria from Waterhouse [51] (see also Hasse [18] and Lu [34]) and Kolster [27] for ideal classes to be 4th powers, and so on.

## 6. FURTHER DIRECTIONS

Perhaps one can simply apply Propositions 3.1, 3.5, or close variants in cleverer ways, using constructions related to genus fields, relative genus fields (cf. Cornell [8]), decomposition fields (cf. Mouhib [38]), or narrow Hilbert class fields. Remark 1.3 suggests it may also help to choose non-Galois fields  $L/\mathbb{Q}$  in Proposition 3.1 or 3.5.

It may also be possible to use the group-theoretic classification methods of Benjamin–Lemmermeyer–Snyder [4]/Boston–Nover [6]/Bush [7] (see also Boston’s survey [5]), where the extra structure may help us push past the “near miss” Golod–Shafarevich failures encountered in (for instance) Sections 3 and 4.

Or perhaps we need better machinery: in view of older results of Koch–Venkov [26]/Schoof [47]/Maire [35], Koch [23, 24, 25] (see also Lemmermeyer [30, Section 1.9.4. Galois groups of class field towers]), and Gaschütz–Newman [13]—based on the Zassenhaus filtration of group algebras over  $\mathbb{F}_2$  (see also Jennings [22], the book [41], and McLeman [37]), and the study of central extensions (see also Fröhlich’s book [12] and Horie [19])—we ask the following.

**Question 6.1.** *Are there stronger yet usable versions of the Golod–Shafarevich inequality for a number field  $K$  cleanly incorporating, for instance, the 4-rank  $d_4 \text{Cl}(K)$ ? Results in special cases could still be useful.*

We now suggest how one might apply such a strengthening to Martinet’s question.

*Remark 6.2.* Recall, in the notation of Proposition 3.1, the failure of our methods in Example 3.12 due to  $\text{rank}_2 \text{Cl}(L(\sqrt{\Delta_K})) = 7 < 8 = 2 + 2\sqrt{8+1}$  (based on SAGE computations assuming GRH); it is not the exact example that matters, but rather that these “near misses” occur all the time when one tries to directly use Golod–Shafarevich, which is based only on 2-rank. So an affirmative answer to Question 6.1 might allow us to incorporate Remark 2.3 on 4-rank information from the ambiguous class number formula, or Yue’s generalized Rédei matrix 4-rank criterion [52] when  $L$  has odd class number.

## 7. ACKNOWLEDGEMENTS

This research was conducted at the University of Minnesota Duluth REU and was supported by NSF grant 1358695 and NSA grant H98230-13-1-0273. The author thanks Joe Gallian for suggesting the problem and a careful proofreading of the manuscript; Ian Whitehead for encouragement, a thorough reading of the paper, providing Example 4.12, and insightful mathematical and organizational comments; Elliot Benjamin for clarifying some typos in [3, Questions 4 and 5]; Farshid Hajir for sending a copy of [17]; David Moulton for helpful discussions; and Bjorn Poonen for teaching helpful algebraic number theory courses at MIT in the Fall 2014 and Spring 2015 semesters. The author is indebted to the anonymous referee for a thorough reading and many helpful corrections and suggestions, many of

which have been incorporated into this version of the paper. The author would also like to thank Yutaka Sueyoshi [49, 50] and Elliot Benjamin [3] for their thorough analysis of Rédei matrices (in some sense identifying the “hardest cases” remaining), and Franz Lemmermeyer for his excellent surveys and expositions on a wide variety of class field theory topics and his English translation of [23]. Finally, the author thanks SageMathCloud and SageMath-Cell for enabling class group computations, Google Scholar ‘allintitle: 2-class group’ for the serendipitous pointers to [9] and [33], and Overleaf for speeding up the writing process.

## REFERENCES

- [1] E. Benjamin, On imaginary quadratic number fields with 2-class group of rank 4 and infinite 2-class field tower, *Pacific J. Math.* 201 (2001), 257–266. <http://www.ams.org/mathscinet-getitem?mr=1875893>. [Cited on page 4.]
- [2] E. Benjamin, On a question of Martinet concerning the 2-class field tower of imaginary quadratic number fields, *Ann. Sci. Math. Québec* 26(1) (2002), 1–13. <http://www.ams.org/mathscinet-getitem?mr=1943908>. [Cited on pages 4 and 13.]
- [3] E. Benjamin, On the 2-class field tower conjecture for imaginary quadratic number fields with 2-class group of rank 4, *J. Number Theory* 118 (2015), 118–143. <http://www.ams.org/mathscinet-getitem?mr=3339569>. [Cited on pages 4, 13, 14, 15, 17, 21, and 22.]
- [4] E. Benjamin, F. Lemmermeyer, and C. Snyder, Imaginary quadratic fields with  $\text{Cl}_2(k) \simeq (2, 2, 2)$ , *J. Number Theory* 103 (2003), no. 1, 38–70. <http://www.ams.org/mathscinet-getitem?mr=2008065>. [Cited on pages 9, 12, and 21.]
- [5] N. Boston, Galois  $p$ -groups unramified at  $p$ —a survey, *Contemp. Math.*, 416 (2006), 31–40. <http://www.ams.org/mathscinet-getitem?mr=2276134>. [Cited on page 21.]
- [6] N. Boston and H. Nover, Computing pro- $p$  Galois groups, *Lecture Notes in Comput. Sci.*, 4076 (2006), 1–10. <http://www.ams.org/mathscinet-getitem?mr=2282911>. [Cited on page 21.]
- [7] M. R. Bush, Computation of Galois groups associated to the 2-class towers of some quadratic fields, *J. Number Theory* 100 (2003), no. 2, 313–325. <http://www.ams.org/mathscinet-getitem?mr=1978459>. [Cited on page 21.]
- [8] G. Cornell, Relative genus theory and the class group of  $l$ -extensions, *Trans. Amer. Math. Soc.* 277 (1983), no. 1, 421–429. <http://www.ams.org/mathscinet-getitem?mr=690061>. [Cited on pages 5 and 21.]
- [9] C. Dominguez, S. J. Miller, and S. Wong, Quadratic fields with cyclic 2-class groups, *J. Number Theory* 133 (2013), no. 3, 926–939. <http://www.ams.org/mathscinet-getitem?mr=2997776>. [Cited on pages 18, 19, and 22.]
- [10] M. Emerton, Genus theory, online handout (accessed August 2015), <http://math.uchicago.edu/~emerton/number-theory/genus.pdf>. [Cited on page 5.]
- [11] M. Ershov, Golod–Shafarevich groups: a survey, *Internat. J. Algebra Comput.* 22 (2012), no. 5, 1230001, 68 pp. <http://www.ams.org/mathscinet-getitem?mr=2949205>. [Cited on page 2.]
- [12] A. Fröhlich, Central extensions, Galois groups, and ideal class groups of number fields, *Contemporary Mathematics*, 24, American Mathematical Society (1983). <http://www.ams.org/mathscinet-getitem?mr=720859>. [Cited on pages 19 and 21.]
- [13] W. Gaschütz and M. F. Newman, On presentations of finite  $p$ -groups, *J. Reine Angew. Math.* 245 (1970), 172–176. <http://www.ams.org/mathscinet-getitem?mr=271225>. [Cited on page 21.]
- [14] E. S. Golod and I. R. Shafarevich, On the class field tower (Russian), *Izv. Akad. Nauk SSSR Ser. Mat.* 28 (1964), 261–272; English translation in *Amer. Math. Soc. Transl* 48 (1965), 91–102. <http://www.ams.org/mathscinet-getitem?mr=161852>. [Cited on page 2.]
- [15] G. Gras, *Class field theory: from theory to practice* (translated from the French manuscript by Henri Cohen), Springer Monographs in Mathematics, Springer-Verlag, Berlin (2003). <http://www.ams.org/mathscinet-getitem?mr=1941965>. [Cited on page 5.]
- [16] F. Hajir, On a theorem of Koch, *Pacific J. Math.* 176 (1996), no. 1, 15–18. <http://www.ams.org/mathscinet-getitem?mr=1433980>. [Cited on pages 3, 7, 10, and 17.]
- [17] F. Hajir, Correction to: “On a theorem of Koch”, *Pacific J. Math.* 196 (2000), no. 2, 507–508. <http://www.ams.org/mathscinet-getitem?mr=1800589>. [Cited on pages 3, 7, and 21.]

- [18] H. Hasse, An algorithm for determining the structure of the 2-Sylow-subgroups of the divisor class group of a quadratic number field, *Symposia Mathematica*, Vol. XV (Convegno di Strutture in Corpi Algebrici, INDAM, Rome, 1973), pp. 341–352, Academic Press, London (1975). <http://www.ams.org/mathscinet-getitem?mr=387239>. [Cited on pages 7, 19, and 21.]
- [19] M. Horie, On central extensions of elementary abelian fields, *J. Number Theory* 36 (1990), no. 1, 95–107. <http://www.ams.org/mathscinet-getitem?mr=1068676>. [Cited on page 21.]
- [20] J. Hurrelbrink, Circulant graphs and 4-ranks of ideal class groups, *Canad. J. Math.* 46 (1994), no. 1, 169–183, <http://cms.math.ca/cjm/a148551>. <http://www.ams.org/mathscinet-getitem?mr=1260342>. [Cited on page 7.]
- [21] W. Jehne, On knots in algebraic number theory, *J. Reine Angew. Math.* 311/312 (1979), 215–254. <http://www.ams.org/mathscinet-getitem?mr=549967>. [Cited on page 6.]
- [22] S. A. Jennings, The structure of the group ring of a  $p$ -group over a modular field, *Trans. Amer. Math. Soc.* 50, (1941), 175–185. <http://www.ams.org/mathscinet-getitem?mr=4626>. [Cited on page 21.]
- [23] H. Koch, Über den 2-Klassenkörperturn eines quadratischen Zahlkörpers. I (German), *J. Reine Angew. Math.* 214/215 (1964), 201–206, English translation by Franz Lemmermeyer available at <http://www.fen.bilkent.edu.tr/~franz/publ/koch2cft.pdf>. <http://www.ams.org/mathscinet-getitem?mr=164945>. [Cited on pages 9, 12, 21, and 22.]
- [24] H. Koch, Zum Satz von Golod–Schafarewitsch (German), *Math. Nachr.* 42 (1969), 321–333. <http://www.ams.org/mathscinet-getitem?mr=291286>. [Cited on pages 3 and 21.]
- [25] H. Koch, Galois theory of  $p$ -extensions (translated from the 1970 German original by Franz Lemmermeyer, with a postscript by the author and Lemmermeyer), *Springer Monographs in Mathematics*, Springer-Verlag, Berlin (2002). <http://www.ams.org/mathscinet-getitem?mr=1930372>. [Cited on pages 2 and 21.]
- [26] H. Koch and B. B. Venkov, Über den  $p$ -Klassenkörperturn eines imaginär-quadratischen Zahlkörpers (German), *Journées Arithmétiques de Bordeaux*, Astérisque 24/25 (1975), pp. 57–67. <http://www.ams.org/mathscinet-getitem?mr=392928>. [Cited on page 21.]
- [27] M. Kolster, The 2-part of the narrow class group of a quadratic number field, *Ann. Sci. Math. Qubec* 29 (2005), no. 1, 73–96. <http://www.ams.org/mathscinet-getitem?mr=2296831>. [Cited on pages 7 and 21.]
- [28] F. Lemmermeyer, Construction of Hilbert 2-class fields, undated preprint, available at <http://www.fen.bilkent.edu.tr/~franz/publ/consum.pdf>. [Cited on page 7.]
- [29] F. Lemmermeyer, The 4-class group of real quadratic number fields, undated preprint, available at <http://arxiv.org/abs/1310.6607>. [Cited on pages 3, 7, and 8.]
- [30] F. Lemmermeyer, Survey on class field towers, preprint (version of September 7, 2010), available at <http://www.rzuser.uni-heidelberg.de/~hb3/publ/pcf.pdf>. [Cited on pages 2, 5, 6, 7, 8, and 21.]
- [31] F. Lemmermeyer, The development of the principal genus theorem, in: *The shaping of arithmetic after C. F. Gauss's Disquisitiones arithmeticae*, 529–561, Springer, Berlin (2007), <http://www.math.uiuc.edu/Algebraic-Number-Theory/0354/dpgt.pdf>. <http://www.ams.org/mathscinet-getitem?mr=2308295>. [Not cited.]
- [32] F. Lemmermeyer, The ambiguous class number formula revisited, *J. Ramanujan Math. Soc.* 28 (2013), no. 4, 415–421. <http://www.ams.org/mathscinet-getitem?mr=3158989>. [Cited on page 5.]
- [33] A. Lopez, Imaginary quadratic fields with 2-class group of type  $(2, 2^\ell)$ , *Funct. Approx. Comment. Math.* 52 (2015), no. 1, 37–55. <http://www.ams.org/mathscinet-getitem?mr=2997776>. [Cited on pages 16, 19, and 22.]
- [34] Q. Lu, 8-rank of the class group and isotropy index, *Sci. China Math.* 58 (2015), no. 7, 1433–1444. <http://www.ams.org/mathscinet-getitem?mr=3353980>. [Cited on pages 7 and 21.]
- [35] C. Maire, Un raffinement du théorème de Golod–Safarevic (French) [A sharpening of the Golod–Shafarevich theorem], *Nagoya Math. J.* 150 (1998), 1–11, <https://zbmath.org/?q=an:0923.11158>. <http://www.ams.org/mathscinet-getitem?mr=1633138>. [Cited on pages 9, 12, and 21.]
- [36] J. Martinet, Tours de corps de classes et estimations de discriminants (French), *Invent. Math.* 44 (1978), 65–73. <http://www.ams.org/mathscinet-getitem?mr=460281>. [Cited on pages 3 and 8.]
- [37] C. McLeman, A Golod–Shafarevich equality and  $p$ -tower groups, *J. Number Theory* 129 (2009), no. 11, 2808–2819. <http://www.ams.org/mathscinet-getitem?mr=2549535>. [Cited on page 21.]
- [38] A. Mouhib, Infinite Hilbert 2-class field tower of quadratic number fields, *Acta Arith.* 145 (2010), no. 3, 267–272. <http://www.ams.org/mathscinet-getitem?mr=2733088>. [Cited on pages 3, 10, 17, and 21.]

- [39] A. Mouhib, Acknowledgment of priority: “Infinite Hilbert 2-class field tower of quadratic number fields”, *Acta Arith.* 167 (2015), no. 3, 299. <http://www.ams.org/mathscinet-getitem?mr=3316463>. [Cited on pages 10 and 17.]
- [40] J. Neukirch, Algebraic number theory (translated from the 1992 German original, with a note by Norbert Schappacher and foreword by G. Harder), Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322, Springer-Verlag, Berlin (1999). <http://www.ams.org/mathscinet-getitem?mr=1697859>. [Cited on pages 2, 8, and 18.]
- [41] J. Neukirch, A. Schmidt, and K. Wingberg, Cohomology of number fields (second edition), Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 323, Springer-Verlag, Berlin (2008). <http://www.ams.org/mathscinet-getitem?mr=2392026>. [Cited on page 21.]
- [42] G. Poitou, Minorations de discriminants (d’après A. M. Odlyzko), *Séminaire Bourbaki*, Vol. 1975/76 28ème année, Exp. No. 479, 136–153. <http://www.ams.org/mathscinet-getitem?mr=435033>. [Cited on page 3.]
- [43] L. Rédei, H. Reichardt, Die Anzahl der durch vier teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, *J. Reine Angew. Math.* 170 (1934), 69–74. <http://www.ams.org/mathscinet-getitem?mr=1581397>. [Cited on page 7.]
- [44] L. Rédei, Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper (German), *J. Reine Angew. Math.* 171 (1934), 55–60. <http://www.ams.org/mathscinet-getitem?mr=1581419>. [Cited on page 7.]
- [45] P. Roquette, On class field towers, in: J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, Academic Press (1967), pp. 231–249. <http://www.ams.org/mathscinet-getitem?mr=218331>. [Cited on page 2.]
- [46] B. Schmithals, Konstruktion imaginärquadratischer Körper mit unendlichem Klassenkörperturm (German), *Arch. Math. (Basel)* 34 (1980), no. 4, 307–312. <http://www.ams.org/mathscinet-getitem?mr=593948>. [Cited on pages 4, 8, 10, and 17.]
- [47] R. Schoof, Infinite class field towers of quadratic fields, *J. Reine Angew. Math.* 372 (1986), 209–220. <http://www.ams.org/mathscinet-getitem?mr=863524>. [Cited on pages 8, 9, and 21.]
- [48] Y. Sueyoshi, Infinite 2-class field towers of some imaginary quadratic number fields, *Acta Arith.* 113 (2004), no. 3, 251–257. <http://www.ams.org/mathscinet-getitem?mr=2069114>. [Cited on pages 3 and 4.]
- [49] Y. Sueyoshi, On 2-class field towers of imaginary quadratic number fields, *Far East J. Math. Sci. (FJMS)* 34 (2009), no. 3, 329–339, available online at <http://hdl.handle.net/10069/28861>. <http://www.ams.org/mathscinet-getitem?mr=2583339>. [Cited on pages 4, 13, 14, 15, and 22.]
- [50] Y. Sueyoshi, On the infinitude of 2-class field towers of some imaginary quadratic number fields, *Far East J. Math. Sci. (FJMS)* 42 (2010), no. 2, 175–187, available online at <http://hdl.handle.net/10069/28862>. <http://www.ams.org/mathscinet-getitem?mr=2743347>. [Cited on pages 4, 13, 17, and 22.]
- [51] Waterhouse, Pieces of eight in class groups of quadratic fields, *J. Number Theory* 5 (1973), 95–97. <http://www.ams.org/mathscinet-getitem?mr=319944>. [Cited on pages 7, 9, and 21.]
- [52] Q. Yue, The generalized Rédei-matrix, *Math. Z.* 261 (2009), no. 1, 23–37. <http://www.ams.org/mathscinet-getitem?mr=2452635>. [Cited on pages 7 and 21.]

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA 02139, UNITED STATES

*E-mail address:* [vywang@mit.edu](mailto:vywang@mit.edu)