

# ANNALES MATHÉMATIQUES



## BLAISE PASCAL

CHRISTIAN MAIRE & CAM MCLEMAN

On  $p^2$ -Ranks in the Class Field Tower Problem

Volume 21, n° 2 (2014), p. 57-68.

<[http://ambp.cedram.org/item?id=AMBP\\_2014\\_\\_21\\_2\\_57\\_0](http://ambp.cedram.org/item?id=AMBP_2014__21_2_57_0)>

© Annales mathématiques Blaise Pascal, 2014, tous droits réservés.

L'accès aux articles de la revue « Annales mathématiques Blaise Pascal » (<http://ambp.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://ambp.cedram.org/legal/>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

*Publication éditée par le laboratoire de mathématiques  
de l'université Blaise-Pascal, UMR 6620 du CNRS  
Clermont-Ferrand — France*

**cedram**

*Article mis en ligne dans le cadre du  
Centre de diffusion des revues académiques de mathématiques  
<http://www.cedram.org/>*

# On $p^2$ -Ranks in the Class Field Tower Problem

CHRISTIAN MAIRE  
CAM MCLEMAN

## Abstract

Much recent progress in the 2-class field tower problem revolves around demonstrating infinite such towers for fields – in particular, quadratic fields – whose class groups have large 4-ranks. Generalizing to all primes, we use Golod-Safarevic-type inequalities to analyse the source of the  $p^2$ -rank of the class group as a quantity of relevance in the  $p$ -class field tower problem. We also make significant partial progress toward demonstrating that all real quadratic number fields whose class groups have a 2-rank of 5 must have an infinite 2-class field tower.

## *$p^2$ -rangs et $p$ -tours de Hilbert*

### Résumé

Les récents progrès sur le problème de la 2-tour de Hilbert des corps de nombres portent sur l'infinitude – en particulier pour les corps quadratiques – quand le groupe des classes a un grand 4-rang. Généralisant à tout nombre premier  $p$ , nous utilisons les inégalités de type Golod-Safarevic afin d'analyser la contribution du  $p^2$ -rang du groupe des classes à l'étude de la  $p$ -tour de Hilbert. Nous apportons également des résultats partiels en direction de l'infinitude de la 2-tour de Hilbert des corps quadratiques réels lorsque que le 2-rang du groupe des classes vaut 5.

## 1. Introduction

The  *$p$ -class field tower* problem for a number field  $K$  is the question of whether the maximal unramified  $p$ -extension  $\tilde{K}/K$  is an infinite extension, or equivalently, whether  $G = \text{Gal}(\tilde{K}/K)$  is infinite. The first positive answer to the class field tower problem, demonstrating number fields for which  $\tilde{K}/K$  is infinite, came from the landmark paper of Golod and Safarevic [2]. This is done via what is now known as (one of many forms of) the Golod-Shafarevich inequality, dictating that if  $G$  is finite, then for

---

Keywords: Hilbert class field towers.

Math. classification: 11R29, 11R34, 11R37.

all  $t \in (0, 1)$  we have the polynomial inequality

$$\sum_{k=2}^{\infty} r_k t^k - dt + 1 > 0.$$

Here,  $d = d_p \text{Cl}(K)$  denotes the  $p$ -rank of the class group of  $K$ , and the various  $r_k$  are invariants of  $G$  defined from the Magnus embedding of  $G$  into the ring of formal power series over  $\mathbb{F}_p$  in  $d$  non-commuting variables. We will not need the precise definitions of these  $r_k$ , but note that while difficult to compute, they were computable enough to permit the first demonstrations of infinite class field towers. For example, from this it can be deduced that a quadratic field whose class group satisfies  $d_2 \text{Cl}(K) \geq 6$  has an infinite class field tower. A variant of this result due to Schoof [4] gives the same inequality but with the  $r_k$  replaced by certain cohomologically-defined invariants  $r'_k$ . These new invariants, while still difficult to compute, greatly expanded the collection of number fields for which we could affirmatively answer the class field tower problem.

The central tool of the current paper is a third version of the inequality, due to Maire [3]. Here, the invariants  $r_k$  or  $r'_k$  are replaced by yet another set,  $m_k$ , which thanks to their concrete arithmetic interpretation can be explicitly computed for many examples. Our main result (Theorem 2.2) is an explicit formula for the second such invariant,  $m_2$ , in terms of the arithmetic of  $K$  and that of its maximal elementary abelian unramified  $p$ -extension  $L$ . This calculation affords us several significant corollaries, two of which we mention here. The first is a correction of a claim in [3] about the effect of the  $p^2$ -rank of the class group on the class field tower problem. The second is an application to 2-class field towers over real quadratic fields: We recall that the original argument of Golod and Shafarevich proves that such towers are infinite when  $d_2 \text{Cl}(K) \geq 6$ . The article [1] asks if this requirement can be relaxed to  $d_2 \text{Cl}(K) \geq 5$ . Corollary 4.2 gives significant partial progress toward an affirmative answer to this question, showing that it is true under any of a wide range of additional arithmetic hypotheses. Finally, while explicit relationships between the sequences  $m_k$ ,  $r_k$ , and  $r'_k$  are in general hard to come by, Section 4.3 demonstrates examples where they are provably not all equal.

## Notation and Setup

For a group  $A$ , we denote its  $p$ -rank by

$$d_p A = \dim_{\mathbb{F}_p} A/A^p[A, A] = \dim_{\mathbb{F}_p} H_1(A, \mathbb{F}_p)$$

and define its  $p^2$ -rank by  $d_{p^2} A = d_p(A^p)$ . Let  $K$  be a number field and  $p$  a prime. We denote by  $K^{(1)}$  the Hilbert  $p$ -class field of  $K$ , the maximal unramified abelian  $p$ -extension of  $K$ , and define the  $p$ -class field tower over  $K$  recursively by  $K^{(n)} = (K^{(n-1)})^{(1)}$  for  $n \geq 2$ . We let  $\tilde{K}$  denote the top of the tower:  $\tilde{K} = \cup K^{(n)}$ . It is easily verified that  $\tilde{K}/K$  is Galois, and we put  $G = \text{Gal}(\tilde{K}/K)$  for the remainder of the paper. Let  $L_i = \tilde{K}^{G_i}$  denote the fixed field of  $\tilde{K}$  corresponding to the  $i$ -th lower central subgroup  $G_i$  of  $G$ , defined recursively by  $G_1 = G$  and  $G_i = G_{i-1}^p[G_{i-1}, G]$ . Let  $L = L_2$ , the maximal unramified  $p$ -extension of  $K$  whose Galois group is elementary abelian. Let  $E_K$  and  $A_K = \text{Cl}_p(K)$  respectively denote the unit group and  $p$ -class group of  $K$ , and we define the generator and relation rank of  $G$  respectively by

$$d = d_p(G) = d_p A_K = d_p H_1(G, \mathbb{F}_p) \quad \text{and} \quad r = d_p H_2(G, \mathbb{F}_p).$$

## 2. Statement of the Main Theorem

We now turn to the construction of the invariants  $m_i$ , which form the foundation for the third variant of the Golod-Shafarevich inequality mentioned in the introduction. For each  $i \geq 1$ , define

$$\Lambda_i = \{x \in L_i^\times \mid (x) = \mathfrak{Q}^p \text{ for some ideal } \mathfrak{Q} \text{ of } L\}.$$

Then when  $G$  is finite, i.e.,  $K$  has a finite  $p$ -class field tower, there is an isomorphism ([3], Proposition 4.2)

$$\Delta_i := \frac{\Lambda_i}{L_i^{\times p} N_{\tilde{K}/L_i}(E_{\tilde{K}})} \approx H_2(G_i, \mathbb{F}_p),$$

giving a concrete arithmetic interpretation to the relation rank. We then filter  $\Delta_1$  by the images of the higher  $\Delta_i$ , setting:

$$M_i = \frac{\text{Im}(\Delta_{i-1} \rightarrow \Delta_1)}{\text{Im}(\Delta_i \rightarrow \Delta_1)}$$

for  $i \geq 2$ , where the arrows are the obvious norm maps. Finally, we define the invariants  $m_i$  by  $m_i = \dim_{\mathbb{F}_p} M_i$  and note that by the filtration,  $\sum_{i \geq 2} m_i = r$ .

We can now state the main result of [3]:

**Theorem 2.1.** *If  $G$  is finite, then for all  $t \in (0, 1)$  we have*

$$\sum_{i \geq 2} m_i t^i - dt + 1 > 0.$$

Theorem 2.1 can be used to prove class field towers infinite using the same type of argument as used in the original Golod-Shafarevich examples: For example, we can re-derive the famous inequality  $r > \frac{d^2}{4}$  for finite towers from the standard argument that the inequality

$$0 < \sum_{i \geq 2} m_i t^i - dt + 1 \leq \left( \sum_{i \geq 2} m_i \right) t^2 - dt + 1 = r t^2 - dt + 1 \quad (2.1)$$

is violated at  $t = \frac{d}{2r}$  if  $r \leq \frac{d^2}{4}$ .

The goal of the current article is to use the invariants  $m_i$  to prove certain class field towers infinite, analogously to how refinements of the Golod-Shafarevich theorem (e.g., the refinements of Koch-Venkov [6] and Schoof [4]) provided new examples of infinite class field towers. In particular, whereas Koch-Venkov and Schoof used symmetry arguments to prove that the even invariants vanish ( $r_{2k} = r'_{2k} = 0$  for  $k \geq 1$ ), we will compute the early  $m$ -invariants (in this article, specifically  $m_2$ ) in terms of the arithmetic of  $K$  and  $L$ .

The algebra behind the subsequent numerical results is then rather straight-forward, as in (2.1): Since  $t^k \leq t^2$  for all  $k \geq 2$  and all  $t \in (0, 1)$ , stronger results come from Theorem 2.1 if we can bound  $m_2$  from above. The article's main result follows this path, culminating in an explicit computation of  $m_2$  in terms of the arithmetic of  $K$  and  $L$ .

**Theorem 2.2.** *With  $L/K$  as above, we have*

$$m_2 = d + d_p \frac{E_K}{E_K^p(E_L \cap N(\Lambda_L))} - d_p N(A_L[p]).$$

Here and elsewhere, we abuse notation in using the symbol  $N = N_{L/K}$  for all of the obvious norm maps from  $L$  to  $K$  (e.g., norms of units, ideals, ideal classes,...). This calculation corrects an earlier attempt to bound  $m_2$  from above, namely, the claim given in [3] that we have

$$m_2 \leq d + d_p E_k - d_{p^2} A_K. \quad (2.2)$$

As a consequence of the theorem, we can see that this inequality does not in general hold without further assumptions, and demonstrate other bounds to replace it. For example, we can deduce the following:

**Corollary 2.3.** *We have*

$$m_2 \leq d + d_p E_K - d_p N(A_L[p]).$$

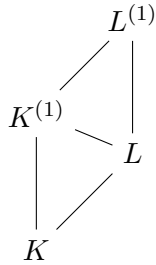
*If  $N: A_L[p] \rightarrow A_K^p[p]$  is surjective, then inequality (2.2) holds, i.e.,*

$$m_2 \leq d + d_p E_K - d_{p^2} A_K.$$

We will give the explicit counter-example of  $K = \mathbb{Q}(\sqrt{-3 \cdot 13 \cdot 61})$  to inequality (2.2) in the case that this restricted norm map is not surjective in Example 4.1.

### 3. Proof of the main theorem

We begin with the following easily-verified diagram of fields and their Galois groups. In particular, we note that since  $L/K$  is the maximal elementary abelian sub-extension of  $K^{(1)}/K$ , the Galois group  $\text{Gal}(L/K)$  is the maximal elementary abelian quotient of  $A_K$ , isomorphic to  $(\mathbb{Z}/p\mathbb{Z})^d$ .



with Galois groups:

$$\text{Gal}(K^{(1)}/K) \approx A_K$$

$$\text{Gal}(L^{(1)}/L) \approx A_L$$

$$\text{Gal}(K^{(1)}/L) \approx A_K^p$$

$$\text{Gal}(L/K) \approx (\mathbb{Z}/p\mathbb{Z})^d$$

We begin by identifying the kernel and image of the norm map on ideal classes.

**Lemma 3.1.** *For  $N: A_L \rightarrow A_K$ , we have*

$$\ker(N) \approx \text{Gal}(L^{(1)}/K^{(1)}) \quad \text{and} \quad \text{im}(N) = A_K^p.$$

*Proof.* This follows from the fact that under Artin reciprocity, the norm map on ideal class groups corresponds to the restriction map on Galois groups. That is, we have the following commutative diagram:

$$\begin{array}{ccc} A_L & \xrightarrow{N} & A_K \\ \downarrow \cong & & \downarrow \cong \\ \text{Gal}(L^{(1)}/L) & \xrightarrow{\text{res}} & \text{Gal}(K^{(1)}/K) \end{array}$$

Now, via the Artin map, we have

$$\ker(N) \cong \ker(\text{res}) \cong \text{Gal}(L^{(1)}/K^{(1)})$$

and

$$\text{im}(N) \cong \text{im}(\text{res}) \cong \text{Gal}(K^{(1)}/K^{(1)} \cap L) = \text{Gal}(K^{(1)}/L) \cong A_K^p.$$

□

**Lemma 3.2.** *Given a commutative diagram of vectors spaces with exact rows as below,*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & V_1 & \longrightarrow & V_2 & \longrightarrow & V_3 & \longrightarrow & 1 \\ & & \downarrow f_1 & & \downarrow f_2 & & \downarrow f_3 & & \\ 1 & \longrightarrow & W_1 & \longrightarrow & W_2 & \longrightarrow & W_3 & \longrightarrow & 1 \end{array}$$

we have

$$\dim \text{im}(f_2) = \dim \text{im}(f_1) + \dim \text{im}(f_3) + \dim(\partial(\ker(f_3))),$$

where  $\partial: \ker(f_3) \rightarrow \text{cok}(f_1)$  denotes the connecting homomorphism from the snake lemma.

*Proof.* From the snake lemma we have an exact sequence

$$\begin{array}{ccccccc} 1 & \longrightarrow & \ker(f_1) & \longrightarrow & \ker(f_2) & \longrightarrow & \ker(f_3) \\ & & & & & & \downarrow \\ & & & & & & \partial \\ & & & & \text{cok}(f_1) & \longrightarrow & \text{cok}(f_2) & \longrightarrow & \text{cok}(f_3) & \longrightarrow & 1 \end{array}$$

where  $\partial$  is the standard connecting homomorphism. From this we obtain the following short exact sequence:

ON  $p^2$ -RANKS AND  $p$ -CLASS FIELD TOWERS

$$1 \longrightarrow \frac{\text{cok}(f_1)}{\partial(\ker(f_3))} \longrightarrow \text{cok}(f_2) \longrightarrow \text{cok}(f_3) \longrightarrow 1$$

Taking an alternating sum of dimensions of this sequence gives the result.  $\square$

Next, for any subfield  $F \subset \tilde{K}$ , recall/define

$$\Delta_F = \frac{\Lambda_F}{F \times_p N_{\tilde{K}/F}(E_{\tilde{K}})} \quad \text{and} \quad E'_F = \frac{E_F}{E_F^p N_{\tilde{K}/F}(E_{\tilde{K}})}$$

and consider the following commutative diagram:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & E'_L & \longrightarrow & \Delta_L & \xrightarrow{\phi_L} & A_L[p] & \longrightarrow & 1 \\ & & \downarrow N & & \downarrow N & & \downarrow N & & \\ 1 & \longrightarrow & E'_K & \longrightarrow & \Delta_K & \xrightarrow{\phi_K} & A_K[p] & \longrightarrow & 1 \end{array}$$

Here the two rows are the well-known exact sequences stemming from the morphism  $\phi_L$  defined by  $\phi_L([x]) = [\mathfrak{Q}]$ , where  $\mathfrak{Q}$  is an ideal of  $L$  chosen so that  $\mathfrak{Q}^p = (x)$ , and the two rows are connected by the appropriate norm maps  $N = N_{L/K}$ . In anticipation of applying Lemma 3.2, we note that the connecting map  $\partial$  can be made explicit in our context as follows: For  $\mathfrak{c} \in \ker(N) \subset A_L[p]$ , choose  $[x] \in \Delta_L$  such that  $(x) = \mathfrak{Q}^p$  for some  $\mathfrak{Q} \in \mathfrak{c}$ . Then by commutativity of the rightmost square,  $N([x]) = [N(x)] \in \Delta_K$  is in the kernel of  $\phi_K$ , so by exactness  $\partial(\mathfrak{c}) := [N(x)] \in E'_K$ . It is now easy to characterize the subgroup of elements of

$$\text{cok}(N: E'_L \rightarrow E'_K) \cong \frac{E_K}{E_K^p N(E_L)}$$

which are in the image of  $\partial$ . Namely,  $[u] \in E'_K$  is in the image of  $\partial$  if and only if there exists  $x \in \Lambda_L$  whose class  $[x] \in \Delta_L$  satisfies  $N([x]) = [u]$ . That is,

$$\partial(\ker(N: A_L[p] \rightarrow A_K[p])) \cong \frac{E_K \cap N(\Lambda_L)}{E_K^p N(E_L)}.$$

This is the last ingredient needed to apply Lemma 3.2 to the commutative diagram above, which yields the following formula for the key dimension of interest:

$$d_p(\text{Im}(\Delta_L \rightarrow \Delta_K)) = d_p N(E'_L) + d_p N(A_L[p]) + d_p \frac{E_K \cap N(\Lambda_L)}{E_K^p N(E_L)}.$$



This calculation reduces the proof of the main theorem to combining a collection of established identities:

*Proof of Theorem 2.2.* The isomorphism  $\Delta_K \approx H_2(G, \mathbb{F}_p)$  provides via the bottom row of the diagram above that  $r - d = d_p E'_K$ . By definition of  $m_2$  we have  $m_2 = r - \dim(\text{Im}(\Delta_L \rightarrow \Delta_K))$ . Finally, we note that we have  $d_p E'_K - d_p N(E'_L) = d_p \frac{E_K}{E_K^p N(E_L)}$ . Combining these gives

$$\begin{aligned} m_2 &= r - \dim(\text{Im}(\Delta_L \rightarrow \Delta_K)) \\ &= d + d_p E'_K - (d_p N(E'_L) + d_p N(A_L[p]) + d_p \frac{E_L \cap N(\Lambda_L)}{E_K^p N(E_L)}) \\ &= d + d_p \frac{E_K}{E_K^p N(E_L)} - d_p N(A_L[p]) - d_p \frac{E_L \cap N(\Lambda_L)}{E_K^p N(E_L)} \\ &= d + d_p \frac{E_K}{E_K^p N(E_L)(E_K \cap N(\Lambda_L))} - d_p N(A_L[p]) \\ &= d + d_p \frac{E_K}{E_K^p (E_K \cap N(\Lambda_L))} - d_p N(A_L[p]), \end{aligned}$$

completing the argument. □

The theorem and Lemma 3.1 combine to explain the appearance of the  $p^2$ -rank in the  $p$ -class field tower problem. Namely, since  $N(A_L) = A_K^p$ , we have  $N(A_L[p]) \subset A_K^p[p]$ , and so the dimension of this norm group is bounded above by the  $p^2$ -rank of  $A_K$ . In cases where this norm map on the  $p$ -torsion ideal classes is surjective, we can thus get a lot of mileage from Golod-Shafarevich type arguments by using a large  $p^2$ -rank to demonstrate a small value of  $m_2$ . Unfortunately, this norm map is not always surjective, as we shall see in the next section.

## 4. Consequences

Before turning to explicit corollaries of the main theorem, we pause for the brief general remark that the theorem implies that the ultimate goal of bounding  $m_2$  from above can be achieved via two principal routes:

- Finding elements of  $A_K[p]$  which are norms from  $A_L[p]$ ; and
- Finding elements of  $E_K$  which are norms from  $\Lambda_L$  (including, in particular, norms from  $E_L$ ).

This illuminates the perspective that the likelihood of a number field  $K$  having an infinite  $p$ -class field tower increases directly with the non-triviality of the norm maps on ideal classes and units from  $L$ .

#### 4.1. A Counter-Example to Inequality (2.2)

All computations were done in SAGE [5].

*Example 4.1.* Consider the number field  $K = \mathbb{Q}(\sqrt{-3 \cdot 13 \cdot 61})$  and let  $p = 2$ . We have  $A_K \cong (4, 4)$ , so  $d = d_2 A_K = d_4 A_K = 2$ , and  $d_2 E_K = 1$ . Then the claim of inequality (2.2) predicts that

$$m_2 \leq d + d_p E_K - d_{p^2} A_K = 2 + 1 - 2 = 1.$$

We will show that, to the contrary,  $m_2 = 2$ , but first note that verifying that  $m_2 \geq 2$  is easier. We simply compute in SAGE that both norm maps  $N: E_L \rightarrow E_K$  and  $N: A_L[2] \rightarrow A_K[2]$  are the trivial map. Then the Main Theorem gives

$$m_2 = d + d_2 \frac{E_K}{E_K^2(E_K \cap N(\Delta_L))} - d_2 N(A_L[p]) = 2 + d_2 \frac{E_K}{E_K \cap N(\Delta_L)} - 0 \geq 2.$$

We include some auxiliary calculations to show that in fact  $m_2 = 2$  by showing that  $-1 \in N(\Delta_L)$ . The genus field  $L$  of  $K$  is given by  $L = K(\sqrt{13}, \sqrt{-3})$ , and  $A_L \cong (8, 8, 4)$ . We have SAGE choose a basis  $\{\mathfrak{c}_i\}_{i=1}^3$  of  $A_L[2]$ , choose representative ideals  $I_i \in \mathfrak{c}_i$ , and let  $x_i$  be a generator for  $I_i^2$ . We check that for SAGE's particular choice of  $x_1, x_2$ , and  $x_3$ , we have

$$\begin{aligned} N_{L/K}(x_1) &= 729 = 3^6 \\ N_{L/K}(x_2) &= -729 = -3^6 \\ N_{L/K}(x_3) &= -764411904 = -2^{20} \cdot 3^6. \end{aligned}$$

From this we see that the image of  $N_{L/K} \Lambda_L \bmod \text{squares}$  is  $\{\pm 1\} = E_K$ , so  $-1 \in N(\Lambda_L)$  and  $m_2 = 2$ .

Incidentally, this computation makes clear the oversight which led to the inequality. The claim in the proof of [3, Corollary 3.2] that we can find the described elements  $\sigma_1, \dots, \sigma_4$  is tantamount to the claim that the surjection  $A_L \rightarrow A_K^2$  necessarily restricts to a surjection  $A_L[2] \rightarrow A_K^2[2]$  on 2-torsion. The example above shows how this can be false from a purely group-theoretic perspective: Taking abstract groups  $G = (8, 8, 4)$

and  $H = (4, 4)$  as in the class groups of the example above, there is no surjection from  $G$  to  $H^2$  which restricts to a surjection  $G[2] \rightarrow H^2[2]$ .

#### 4.2. Real Quadratic Fields with $d = 5$ .

Next, we return to the application from the introduction concerning real quadratic fields. Suppose  $K$  is real quadratic with fundamental unit  $\varepsilon$ , and  $d = d_2 A_K = 5$ . Then as in the first sentence of the proof of the main theorem, we have

$$r - 5 \leq d_2 \frac{E_K}{E_K^2 N(E_{\tilde{K}})} =: e$$

and so  $r \leq 5 + e$ . Now by Theorem 2.1, if  $K$  has a finite 2-class field tower, then for all  $t \in (0, 1)$ , we have

$$\begin{aligned} 0 &< \sum_{i \geq 2} m_i t^i - 5t + 1 \\ &\leq (r - m_2)t^3 + m_2 t^2 - 5t + 1 \\ &\leq (5 + e - m_2)t^3 + m_2 t^2 - 5t + 1. \end{aligned}$$

It is trivial to verify that for each possible value of  $e$  (note  $e \leq 2$  for real quadratic fields), this inequality is violated for some  $t \in (0, 1)$  if  $m_2 \leq 7 - e$ . Using Theorem 2.2 to compute  $m_2$ , this is equivalent to

$$5 + d_2 \frac{E_K}{E_K^2 N(E_L)} - d_2 N(A_L[2]) \leq 7 - e,$$

or

$$d_2 \frac{E_K}{E_K^2 (E_K \cap N(\Lambda_L))} + d_2 \frac{E_K}{E_K^2 N(E_{\tilde{K}})} \leq 2 + d_2 N(A_L[2]). \quad (*)$$

This inequality thus provides a sufficient condition for  $K$  to have an infinite 2-class field tower. We continue to develop this expression. In particular, note that since  $E_L \subset \Lambda_L$ , we have

$$N_{\tilde{K}/K}(E_{\tilde{K}}) \subset N_{L/K}(E_L) \subset E_K \cap N_{L/K}(\Lambda_L),$$

and so

$$0 \leq d_2 \frac{E_K}{E_K^2 (E_K \cap N(\Lambda_L))} \leq d_2 \frac{E_K}{E_K^2 N_{\tilde{K}/K}(E_{\tilde{K}})} \leq 2. \quad (**)$$

It is easy to enumerate the list of possible dimensions of the three  $\mathbb{F}_2$ -vector spaces appearing in  $(*)$  for which the inequalities in  $(*)$  and  $(**)$  are all satisfied, providing the next corollary.

**Corollary 4.2.** *Suppose  $K$  is a real quadratic field with  $d_2 A_K = 5$ . Then  $K$  has an infinite 2-class field tower if either*

$$d_2 \frac{E_K}{E_K^2 N_{\tilde{K}/K}(E_{\tilde{K}})} < 2$$

or

$$d_2 \frac{E_K}{E_K^2 N_{\tilde{K}/K}(E_{\tilde{K}})} = 2 \quad \text{and} \quad d_2 \frac{E_K}{E_K^2 (E_K \cap N(\Lambda_L))} \leq d_2 N(A_L[2]).$$

It is desirable to have a version of this result which does not depend on knowing anything about  $N_{\tilde{K}/K}(E_{\tilde{K}})$ . To that end, we extract from the previous corollary a slightly weaker sufficient condition that is in practice vastly simpler to evaluate.

**Corollary 4.3.** *Suppose  $K$  is a real quadratic field with  $d_2 A_K = 5$ . Then  $K$  has an infinite 2-class field tower if*

$$d_2 \frac{E_K}{E_K^2 (E_K \cap N(\Lambda_L))} \leq d_2 N(A_L[2]).$$

Even more directly, we note that this condition is satisfied, and hence  $K$  has an infinite 2-class field tower, if any of the following hold:

- $d_2(N(A_L[2])) \geq 2$ ;
- $d_2(N(A_L[2])) = 1$  and at least one of  $-1$  or  $\varepsilon$  are norms from  $\Lambda_L$ .
- Both  $-1$  and  $\varepsilon$  are norms from  $\Lambda_L$ .

Finally, to return to the topic of  $p^2$ -ranks, recall that  $d_2 N(A_L[2])$  is bounded above by the 4-rank of  $A_K$ . This tells us, for example, that if  $d_4 A_K = 0$ , only the third of the three conditions in the above list will be viable as an argument to show that  $K$  has an infinite 2-class field tower via this method.

### 4.3. A Comparison of Invariants

While the computation of  $m_2$  does not improve upon the result of Koch-Venkov for quadratic imaginary number fields and  $p$  odd, the simplicity of Theorem 2.2 in this case permits us to demonstrate a distinction between the  $m$ -invariants and the two types of  $r$ -invariants in this case. Namely, by Koch-Venkov [6] and Schoof [4] respectively, we have  $r_2 = 0$  and  $r'_2 = 0$ . Applying Theorem 3, since  $E_K = E_K^p = \{\pm 1\}$ , we conclude simply that  $m_2 = d - d_p N(A_L[p])$ . But since  $N(A_L[p]) \subset A_K^p[p]$ , we conclude  $m_2 = d$  if, for example,  $K$  has a cyclic class group.

*Example 4.4.* For  $\mathbb{Q}(\sqrt{-23})$ , of class number 3, we have  $r_2 = r'_2 = 0$  but  $m_2 = 1$ .

## Acknowledgements

The authors would like to acknowledge an anonymous referee for a careful reading and some helpful suggestions regarding the exposition.

## References

- [1] E. BENJAMIN, F. LEMMERMEYER & C. SNYDER – “Real quadratic fields with abelian 2-class field tower”, *J. Number Theory* **73** (1998), no. 2, p. 182–194.
- [2] E. S. GOLOD & I. R. ŠAFAREVIČ – “On the class field tower”, *Izv. Akad. Nauk SSSR Ser. Mat.* **28** (1964), p. 261–272.
- [3] C. MAIRE – “Un raffinement du théorème de Golod-Safarevic”, *Nagoya Math. J.* **150** (1998), p. 1–11.
- [4] R. SCHOOF – “Infinite class field towers of quadratic fields”, *J. Reine Angew. Math.* **372** (1986), p. 209–220.
- [5] W. A. STEIN et al. – *Sage Mathematics Software (Version 5.11)*, The Sage Development Team, Y2013, <http://www.sagemath.org>.
- [6] B. B. VENKOV & H. KOH – “The  $p$ -tower of class fields for an imaginary quadratic field”, *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)* **46** (1974), p. 5–13, 140, Modules and representations.

CHRISTIAN MAIRE  
Laboratoire de Mathématiques  
UMR 6623  
CNRS - Université de Franche-Comté  
16, Route de Gray  
25030 Besançon cedex  
FRANCE  
[christian.maire@univ-fcomte.fr](mailto:christian.maire@univ-fcomte.fr)

CAM MCLEMAN  
Mathematics Department  
University of Michigan - Flint  
303 E. Kearsley St.  
Flint, MI, 48502  
USA  
[mclemanc@umflint.edu](mailto:mclemanc@umflint.edu)