Ramanujan J (2020) 51:205–228
https://doi.org/10.1007/s11139-018-0046-3

Some examples of quadratic fields with finite non-solvable maximal unramified extensions II

Kwang-Seob Kim[1] · **Joachim König**[2]

Received: 12 April 2018 / Accepted: 24 May 2018 / Published online: 10 September 2018

Abstract Let K be a number field and K_{ur} be the maximal extension of K that is unramified at all places. In a previous article (Kim, J Number Theory 166:235–249, 2016), the first author found three real quadratic fields K such that $\mathrm{Gal}(K_{\mathrm{ur}}/K)$ is finite and non-abelian simple under the assumption of the generalized Riemann hypothesis (GRH). In this article, we extend the methods of Kim (2016) and identify more quadratic number fields K such that $\mathrm{Gal}(K_{\mathrm{ur}}/K)$ is a finite nonsolvable group and also explicitly calculate their Galois groups under the assumption of the GRH. In particular, we find the first imaginary quadratic field with this property.

Keywords Nonsolvable unramified extensions of number fields · Class number one problems

Mathematics Subject Classification Primary 11R37 · Secondary 11F80 and 11R29

The second author was supported by the Israel Science Foundation (Grant No. 577/15).

✉ Kwang-Seob Kim
kwang12@chosun.ac.kr

Joachim König
jkoenig@kaist.ac.kr

[1] Department of Mathematics, Chosun University, 309 Pilmun-daero, Dong-gu, Kwangju 61452, South Korea

[2] Department of Mathematical Sciences, KAIST, 291 Daehak-ro, Yuseong-gu, Taejon 34141, South Korea

1 Introduction

Let K be a number field and K_{ur} be the maximal extension of K that is unramified at *all places*. In [13], Yamamura showed that $K_{\mathrm{ur}} = K_1$, where K denotes an imaginary quadratic field with absolute discriminant value $|d_K| \leq 420$, and K_1 is the top of the class field tower of K and also computed $\mathrm{Gal}(K_{\mathrm{ur}}/K)$. Hence, we can find examples of abelian or solvable étale fundamental groups. It is then natural to wonder whether we can find examples with the property that $\mathrm{Gal}(K_{\mathrm{ur}}/K)$ is a finite nonsolvable group. In [3], we presented three explicit examples that provide an affirmative answer.

In this article, we will refine the previously used methods and identify two more quadratic number fields K such that $\mathrm{Gal}(K_{\mathrm{ur}}/K)$ is a finite nonsolvable group and also explicitly calculate their Galois groups under the generalized Riemann hypothesis (GRH). Under the assumption of GRH, we will show that $\mathrm{Gal}(K_{\mathrm{ur}}/K)$ is isomorphic to a finite nonsolvable group when $K = \mathbb{Q}(\sqrt{22268})$ (Theorem 4.1) and when $K = \mathbb{Q}(\sqrt{-1567})$ (Theorem 5.1).

In particular, to the best of the authors' knowledge, $K = \mathbb{Q}(\sqrt{-1567})$ is the first example of an imaginary quadratic field which has a nonsolvable unramified extension and for which $\mathrm{Gal}(K_{\mathrm{ur}}/K)$ is explicitly calculated.

Tools used for the proof to identify certain unramified extensions with nonsolvable Galois groups, we use the database of number fields created by Klüners and Malle [4]. To exclude further unramified extensions, we use a wide variety of tools, including class field theory, Odlyzko's discriminant bounds, results about low degree number fields with small discriminants, and various group-theoretical results. In particular, our examples demonstrate how to combine the methods of the previous paper [3] with more involved group-theoretical arguments to obtain conclusions for fields whose class numbers and discriminants do not yield immediate results via application of discriminant bounds.

2 Preliminaries

2.1 The action of Galois groups on class groups

If A is a finite abelian p-group, then $A \simeq \oplus \mathbb{Z}/p^{a_i}\mathbb{Z}$ for some integers a_i. Let

$$\begin{aligned} n_a &= \text{ number of } i \text{ with } a_i = a, \\ r_a &= \text{ number of } i \text{ with } a_i \geq a. \end{aligned}$$

Then

$$r_1 = p\text{-rank } A = \dim_{\mathbb{Z}/p\mathbb{Z}} \left(A/A^p\right)$$

and, more generally,

$$r_a = \dim_{\mathbb{Z}/p\mathbb{Z}} \left(A^{p^{a-1}}/A^{p^a}\right).$$

The action of Galois groups on class groups can often be used to obtain useful information on the structure of class groups. We review the following lemma, often called p-rank theorem. By $\mathrm{cl}(K)$ we denote the class number of the number field K.

Lemma 2.1 (Theorem 10.8 of [11]) *Let L/K be a cyclic extension of degree n. Let p be a prime, $p \nmid n$ and assume that all fields E with $K \subsetneqq E \subsetneqq L$ satisfy $p \nmid \mathrm{Cl}(E)$. Let A be the p-Sylow subgroup of the ideal class group of L, and let f be the order of p mod n. Then*

$$r_a \equiv n_a \equiv 0 \bmod f$$

for all a, where r_a and n_a are as above. In particular, if $p|\mathrm{Cl}(L)$ then the p-rank of A is at least f and $p^f|\mathrm{Cl}(L)$.

2.2 A remark on the class field tower

Lemma 2.2 (Theorem 1 of [10]) *Let K be a number field and p any prime number. If the p-class group, i.e., the p-part of the class group of K is cyclic, then the p-class group of the Hilbert p-class field of K is trivial. Moreover, if $p = 2$ and the 2-class group of K is isomorphic to V_4, then the 2-class group of the Hilbert 2-class field of K is cyclic.*

2.3 Root discriminant

Let K be a number field. We define the *root discriminant* of K to be $|d_K|^{1/n_K}$, where n_K is $[K : \mathbb{Q}]$. Given a tower of number fields $L/K/F$, we have the following equality for the ideals of F:

$$d_{L/F} = \left(d_{K/F}\right)^{[L:K]} N_{K/F}\left(d_{L/K}\right), \tag{2.1}$$

where $d_{L/F}$ denotes the relative discriminant (see [7, Corollary 2.10]). Set $F = \mathbb{Q}$. It follows from (2.1) that, if L is an extension of K, $|d_K|^{1/n_K} \leq |d_L|^{1/n_L}$, with equality if and only if $d_{L/K} = 1$, i.e., L/K is unramified at *all finite places*.

2.4 Discriminant bounds

In this section, we describe how the discriminant bound is used to determine that a field has no nonsolvable unramified extensions.

2.4.1 Crucial proposition

Consider the following proposition, in which K_{ur} is the maximal extension of K that is unramified over all primes.

Proposition 2.3 (Proposition 1 of [13]) *Let $B(n_K, r_1, r_2)$ be the lower bound for the root discriminant of K of degree n_K with signature (r_1, r_2). Suppose that K has an*

unramified normal extension L of degree m. If $\mathrm{Cl}(L) = 1$, *where* $\mathrm{Cl}(L)$ *is the class number of* L, *and* $|d_K|^{1/n_K} < B(60mn_K, 60mr_1, 60mr_2)$, *then* $K_{\mathrm{ur}} = L$.

If the GRH is assumed, much better bounds can be obtained. The lower bounds for number fields are stated in Martinet's expository paper [6].

2.4.2 Description of [6, Table III]

Table III of [6] describes the following. If K is an algebraic number field with r_1 real and $2r_2$ complex conjugate embeddings, and d_K denotes the absolute value of the discriminant of K, then, for any b, we have

$$d_K > A^{r_1} B^{2r_2} \mathrm{e}^{f-E}, \tag{2.2}$$

where A, B, and E are given in the table, and

$$f = 2 \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^{m/2}} F\left(\log N(\mathfrak{p})^m\right), \tag{2.3}$$

where the outer sum is taken over all prime ideals of K, N is the norm from K to $\mathbb{Q}$, and

$$F(x) = G(x/b)$$

in the GRH case, where the even function $G(x)$ is given by

$$G(x) = \left(1 - \frac{x}{2}\right) \cos \frac{\pi}{2} x + \frac{1}{\pi} \sin \frac{\pi}{2} x \tag{2.4}$$

for $0 \le x \le 2$ and $G(x) = 0$ for $x > 2$.

The values of A and B are lower estimates; the values of E have been rounded up from their true values, which are

$$8\pi^2 b \left(\frac{\mathrm{e}^{b/2} + \mathrm{e}^{-b/2}}{\pi^2 + b^2} \right)^2 \tag{2.5}$$

in the GRH case.

3 Some group theory

In this section, we recall some facts from group theory.

3.1 Schur multipliers and central extensions

Definition 3.1 The *Schur multiplier* is the second homology group $H_2(G, \mathbb{Z})$ of a group G.

Definition 3.2 A *stem extension* of a group G is an extension

$$1 \to H \to G_0 \to G \to 1, \tag{3.1}$$

where $H \subset Z(G_0) \cap G_0'$ is a subgroup of the intersection of the center of G_0 and the derived subgroup of G_0.

If the group G is finite and one considers only stem extensions, then there is a largest size for such a group G_0, and for every G_0 of that size the subgroup H is isomorphic to the Schur multiplier of G. Moreover, if the finite group G is perfect as well, then G_0 is unique up to isomorphism and is itself perfect. Such G_0 are often called *universal perfect central extensions* of G, or *covering groups*.

Proposition 3.3 *Let H be a finite abelian group, and let $1 \to H \to G_0 \to G \to 1$ be a central extension of G by H. Then either this extension is a stem extension, or G_0 has a non-trivial abelian quotient.*

Proof By definition, if the extension is not a stem extension, then $H \nsubseteq G_0'$, and thus G_0/G_0' is a non-trivial abelian quotient. □

Lemma 3.4 *The Schur multiplier of A_n is C_2 for $n = 5$ or $n > 7$ and it is C_6 for $n = 6$ or 7.*

Proof See [12, 2.7] □

Lemma 3.5 *The Schur multiplier of $\mathrm{PSL}_n(\mathbb{F}_{p^d})$ is a cyclic group of order $\gcd(n, p^d - 1)$ except for $\mathrm{PSL}_2(\mathbb{F}_4)$ (order 2), $\mathrm{PSL}_2(\mathbb{F}_9)$ (order 6), $\mathrm{PSL}_3(\mathbb{F}_2)$ (order 2), $\mathrm{PSL}_3(\mathbb{F}_4)$ (order 48, product of cyclic groups of orders 3, 4, 4) and $\mathrm{PSL}_4(\mathbb{F}_2)$ (order 2).*

Proof See [12, 3.3]. □

3.2 Group extensions of groups with trivial centers

Let H and F be groups, with G a group extension of H by F:

$$1 \to H \to G \to F \to 1.$$

Then, it is well known that G acts on H by conjugation, and this action induces a group homomorphism $\psi_G : F \to \mathrm{Out}\ H$, which depends only on G.

Lemma 3.6 ((7.11) of [9]) *Suppose that H has trivial center ($Z(H) = \{1\}$). Then, the structure of G is uniquely determined by the homomorphism ψ_G. For any group homomorphism ψ from F to* Out H, *there exists an extension G of H by F such*

that $\psi_G = \psi$. Moreover, the isomorphism class of G is uniquely determined by ψ. [In particular, the class of $F \times H$ is determined by ψ with $\psi(F) = 1$]. All of the extensions are realized as a subgroup U of the direct product $F \times \mathrm{Aut}\, H$ satisfying the two conditions $U \cap \mathrm{Aut}\, H = \mathrm{Inn}\, H$ and $\pi(U) = F$, where π is the projection from $F \times \mathrm{Aut}\, H$ to F.

3.3 Prerequisites on $\mathrm{GL}_n(\mathbb{F}_q)$

3.3.1 General prerequisites

The following lemma is well known.

Lemma 3.7 *Let $n \geq 2$, q be a prime power, and let $U \leq \mathrm{GL}_n(\mathbb{F}_q)$ act irreducibly on $(\mathbb{F}_q)^n$. Then the centralizer of U in $\mathrm{GL}_n(\mathbb{F}_q)$ is cyclic.*

Proof This follows immediately from Schur's lemma. □

Lemma 3.8 *Let $n \geq 2$, q be a prime power and let $U \leq \mathrm{GL}_n(\mathbb{F}_q)$ be cyclic, of order coprime to q. Assume that U acts irreducibly on $(\mathbb{F}_q)^n$. Then the centralizer of U in $\mathrm{GL}_n(\mathbb{F}_q)$ is cyclic of order $q^n - 1$.*

Proof This follows from [2, Hilfssatz II.3.11]. Namely, setting $G := C_{\mathrm{GL}_n(\mathbb{F}_q)}$, the centralizer of U in $\mathrm{GL}_n(\mathbb{F}_q)$, that theorem states that G is isomorphic to $\mathrm{GL}_1(\mathbb{F}_{q^n})$, and thus in particular cyclic of order $q^n - 1$. □

An important special case of the previous lemma is the following:

Lemma 3.9 *Let $n \geq 2$, q be a prime power and let p be a primitive prime divisor of $q^n - 1$, that is p divides $q^n - 1$, but does not divide any of the numbers $q^k - 1$ with $1 \leq k < n$. Then the following hold*:

(i) *There is a unique non-trivial linear action of C_p on $(\mathbb{F}_q)^n$, and this action is irreducible.*
(ii) *The centralizer of a subgroup of order p in $\mathrm{GL}_n(\mathbb{F}_q)$ is cyclic, of order $q^n - 1$.*

Proof Let $U < \mathrm{GL}_n(\mathbb{F}_q)$ be any subgroup isomorphic to C_p. From Maschke's theorem, it follows immediately that U acts irreducibly on $(\mathbb{F}_n)^q$. From Lemma 3.8, the centralizer of U in $\mathrm{GL}_n(\mathbb{F}_q)$ is then cyclic, of order $q^n - 1$. Finally, every such U is the unique subgroup of order p of some p-Sylow subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ [note that, by assumption, the p-Sylow subgroups are of order dividing $q^n - 1$, and then in fact cyclic, since $\mathrm{GL}_1(\mathbb{F}_{q^n}) \leq \mathrm{GL}_n(\mathbb{F}_q)$ is cyclic]. Therefore, all such subgroups U are conjugate in $\mathrm{GL}_n(\mathbb{F}_q)$, proving the uniqueness in (i). □

In the following sections, we collect some results about more specific linear groups.

3.3.2 Structure of $\mathrm{GL}_2(\mathbb{F}_p)$

Lemma 3.10 $\mathrm{GL}_2(\mathbb{F}_p)$ *does not contain any non-abelian simple subgroups for any prime p.*

Proof Let S be non-abelian simple. Then it is known that S contains a non-cyclic abelian subgroup (see e.g., [5, Corollary 6.6]), and therefore even some subgroup $C_r \times C_r$ for some prime r. On the other hand, as a direct consequence of Schur's lemma, any subgroup $C_r \times C_r$ of $\mathrm{GL}_2(\mathbb{F}_p)$ must intersect the center of $\mathrm{GL}_2(\mathbb{F}_p)$ non-trivially.[1] Since S has trivial center, it follows that S cannot be contained in $\mathrm{GL}_2(\mathbb{F}_p)$. □

3.3.3 Structure of $\mathrm{GL}_4(\mathbb{F}_2)$

This article uses the structure of $\mathrm{GL}_4(\mathbb{F}_2)$. Thus, we recall several structural properties of this group.

Proposition 3.11 *A_8 is isomorphic to* $\mathrm{PSL}_4(\mathbb{F}_2) = \mathrm{GL}_4(\mathbb{F}_2)$.

Lemma 3.12 *A_8 does not contain a subgroup isomorphic to $A_5 \times C_2$ or* $\mathrm{SL}_2(\mathbb{F}_5)$.

Proof Both $A_5 \times C_2$ and $\mathrm{SL}_2(\mathbb{F}_5)$ contain an element of order 10, but there is no element of order 10 in A_8. □

Lemma 3.13 *The class of* (12345) *is the unique conjugacy class of elements of order 5 in A_8. In particular, there is a unique non-trivial linear C_5-action on $(\mathbb{F}_2)^4$. This action is irreducible.*

Proof This is a special case of Lemma 3.9, with $q = 2$ and $n = 4$. □

3.3.4 Structure of $\mathrm{GL}_4(\mathbb{F}_3)$

We also make use of the structure of $\mathrm{GL}_4(\mathbb{F}_3)$ in this article. So we recall several structural properties of this group. We proved the following lemmas, partially aided by the computer program Magma.

Lemma 3.14 $\mathrm{GL}_4(\mathbb{F}_3)$ *contains a unique conjugacy class of subgroups isomorphic to $A_5 \times C_2$.*

Proof By computer calculation, we can check that $\mathrm{GL}_4(\mathbb{F}_3)$ has four conjugacy classes of subgroups of order 120. They are

$$\left\langle \begin{pmatrix} 0&0&2&0\\0&2&0&1\\1&0&0&0\\0&1&0&1 \end{pmatrix}, \begin{pmatrix} 1&1&1&2\\2&0&0&2\\2&1&0&0\\1&0&2&0 \end{pmatrix}, \begin{pmatrix} 2&0&0&0\\0&2&0&0\\0&0&2&0\\0&0&0&2 \end{pmatrix} \right\rangle, \quad \left\langle \begin{pmatrix} 1&1&0&2\\0&2&0&0\\2&1&2&2\\0&0&0&2 \end{pmatrix}, \begin{pmatrix} 2&0&1&1\\1&2&0&1\\0&0&1&0\\0&0&1&2 \end{pmatrix} \right\rangle$$
$$\left\langle \begin{pmatrix} 2&1&2&2\\2&0&1&1\\1&1&2&0\\1&1&0&2 \end{pmatrix}, \begin{pmatrix} 0&0&0&2\\2&1&0&2\\2&2&0&1\\0&2&2&0 \end{pmatrix}, \begin{pmatrix} 2&0&0&0\\0&2&0&0\\0&0&2&0\\0&0&0&2 \end{pmatrix} \right\rangle \text{ and } \left\langle \begin{pmatrix} 2&2&0&1\\0&1&0&0\\1&2&1&1\\0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&2&2\\2&1&0&2\\0&0&2&0\\0&0&2&1 \end{pmatrix} \right\rangle. \tag{3.2}$$

We use Magma to check that $\left\langle \begin{pmatrix} 2&1&2&2\\2&0&1&1\\1&1&2&0\\1&1&0&2 \end{pmatrix}, \begin{pmatrix} 0&0&0&2\\2&1&0&2\\2&2&0&1\\0&2&2&0 \end{pmatrix}, \begin{pmatrix} 2&0&0&0\\0&2&0&0\\0&0&2&0\\0&0&0&2 \end{pmatrix} \right\rangle$ is the only the conjugacy class of subgroup of order 120 which is isomorphic to $A_5 \times C_2$. □

[1] To apply Schur's lemma here, we have used that $p \neq r$, which is obvious, since p^2 does not divide $|\mathrm{GL}_2(\mathbb{F}_p)|$.

Lemma 3.15 $\mathrm{GL}_4(\mathbb{F}_3)$ *does not contain a subgroup isomorphic to* $A_5 \times V_4$.

Proof $A_5 \times V_4$ contains an abelian subgroup isomorphic to $C_{10} \times C_2$. As a special case of Lemma 3.9 (with $q = 3$, $n = 4$), the centralizer of a cyclic group of order 5 in $\mathrm{GL}_4(\mathbb{F}_3)$ is cyclic, of order $3^4 - 1 = 80$. Now of course, if $\mathrm{GL}_4(\mathbb{F}_3)$ contained a subgroup isomorphic to $C_{10} \times C_2$, then the centralizer of a respective subgroup of order 5 would be non-cyclic. This ends the proof. □

Lemma 3.16 *There exist a unique conjugacy class of elements of order* 5 *in* $\mathrm{GL}_4(\mathbb{F}_3)$. *Furthermore, there is a unique non-trivial linear action of* C_5 *on* $(\mathbb{F}_3)^4$, *and this action is irreducible.*

Proof This again follows directly from Lemma 3.9, with $q = 3$ and $n = 4$. □

3.3.5 Structure of $\mathrm{GL}_3(\mathbb{F}_5)$

We will also use the structures of $\mathrm{GL}_3(\mathbb{F}_5)$.

Lemma 3.17 $\mathrm{GL}_3(\mathbb{F}_5)$ *contains a unique conjugacy class of subgroups isomorphic to* $A_5 \times C_2$.

Proof By computer calculation, we can check that $\mathrm{GL}_4(\mathbb{F}_3)$ has four conjugacy classes of subgroups of order 120. They are

$$\begin{gathered}\left\langle \begin{pmatrix} 2&1&2\\3&0&0\\2&3&4 \end{pmatrix}, \begin{pmatrix} 0&1&1\\3&4&1\\4&2&1 \end{pmatrix}, \begin{pmatrix} 1&3&2\\1&3&1\\1&4&0 \end{pmatrix} \right\rangle, \quad \left\langle \begin{pmatrix} 4&0&1\\0&4&0\\4&1&0 \end{pmatrix}, \begin{pmatrix} 2&3&1\\3&0&3\\3&4&4 \end{pmatrix} \right\rangle, \\ \left\langle \begin{pmatrix} 1&0&0\\0&1&0\\1&4&4 \end{pmatrix}, \begin{pmatrix} 1&0&4\\2&1&1\\3&0&3 \end{pmatrix}, \begin{pmatrix} 4&0&0\\0&4&0\\0&0&4 \end{pmatrix} \right\rangle, \quad \text{and} \quad \left\langle \begin{pmatrix} 1&0&4\\0&1&0\\1&4&0 \end{pmatrix}, \begin{pmatrix} 3&2&4\\2&0&2\\2&1&1 \end{pmatrix} \right\rangle. \end{gathered} \tag{3.3}$$

We use Magma to check that $\left\langle \begin{pmatrix} 1&0&0\\0&1&0\\1&4&4 \end{pmatrix}, \begin{pmatrix} 1&0&4\\2&1&1\\3&0&3 \end{pmatrix}, \begin{pmatrix} 4&0&0\\0&4&0\\0&0&4 \end{pmatrix} \right\rangle$ is the only the conjugacy class of subgroup of order 120 which is isomorphic to $A_5 \times C_2$.

Lemma 3.18 $\mathrm{GL}_3(\mathbb{F}_5)$ *does not contain a subgroup isomorphic to* $A_5 \times V_4$.

Proof By Lemma 3.10, any subgroup $A_5 \leq \mathrm{GL}_3(\mathbb{F}_5)$ has to act irreducibly. Since $A_5 \times V_4$ has non-cyclic center, the claim now follows immediately from Lemma 3.7. □

3.3.6 Structures of $\mathrm{GL}_5(\mathbb{F}_2)$ *and* $\mathrm{GL}_6(\mathbb{F}_2)$

Lemma 3.19 $\mathrm{GL}_5(\mathbb{F}_2)$ *does not contain a subgroup isomorphic to* $\mathrm{PSL}_2(8)$.

Proof The group $\mathrm{PSL}_2(\mathbb{F}_8) = \mathrm{SL}_2(\mathbb{F}_8)$ contains cyclic subgroups of order $\frac{8^2-1}{8-1} = 9$. However, $\mathrm{GL}_5(\mathbb{F}_2)$ does not contain any such subgroups. Indeed, since 9 is a prime power, Maschke's theorem implies that the existence of such a cyclic subgroup would enforce the existence of an irreducible cyclic subgroup of order 9 in some $\mathrm{GL}_d(\mathbb{F}_2)$ with $d \leq 5$. Then $2^d - 1$ would have to be divisible by 9, which is not the case for any such d. This concludes the proof. □

Lemma 3.20 $\mathrm{GL}_6(\mathbb{F}_2)$ *contains a unique conjugacy class of subgroups isomorphic to* $\mathrm{PSL}_2(\mathbb{F}_8)$.

Proof Since $\mathrm{PSL}_2(\mathbb{F}_8) = \mathrm{SL}_2(\mathbb{F}_8) \leq \mathrm{GL}_2(\mathbb{F}_8)$, the existence follows immediately from the well-known fact that $\mathrm{GL}_{n\cdot d}(\mathbb{F}_q)$ contains subgroups isomorphic to $\mathrm{GL}_n(\mathbb{F}_{q^d})$. The uniqueness can once again be verified with Magma. □

Lemma 3.21 $\mathrm{GL}_6(\mathbb{F}_2)$ *does not contain subgroups isomorphic to* $\mathrm{PSL}_2(\mathbb{F}_8) \times C_2$.

Proof By Maschke's theorem (and using the proof of Lemma 3.19), any cyclic subgroup of order 9 in $\mathrm{GL}_6(\mathbb{F}_2)$ has to act irreducibly. By Lemma 3.8, the centralizer of such a subgroup is then cyclic of order $2^6 - 1 = 63$. However, the centralizer of an order-9 subgroup in $\mathrm{PSL}_2(\mathbb{F}_8) \times C_2$ is of course of even order. This concludes the proof. □

4 Example: $K = \mathbb{Q}(\sqrt{22268})$

Let K be the real quadratic number field $\mathbb{Q}(\sqrt{22268})$. We determine the Galois group of the maximal unramified extension of K.

Theorem 4.1 *Let K be the real quadratic field $\mathbb{Q}(\sqrt{22268})$. Then, under the assumption of GRH, $\mathrm{Gal}(K_{\mathrm{ur}}/K)$ is isomorphic to $A_5 \times C_2$.*

The class number of K is 2, i.e., $\mathrm{Cl}(K) \simeq C_2$. Let K_1 be the Hilbert class field of K. Then K_1 can be written as $\mathbb{Q}(\sqrt{76}, \sqrt{293})$. By computer calculation, we know that the class group of K_1 is trivial, i.e., K_1 has no non-trivial solvable unramified extensions.

4.1 An unramified A_5-extension of K_1

Let $K = \mathbb{Q}(\sqrt{22268})$ and let L be the splitting field of

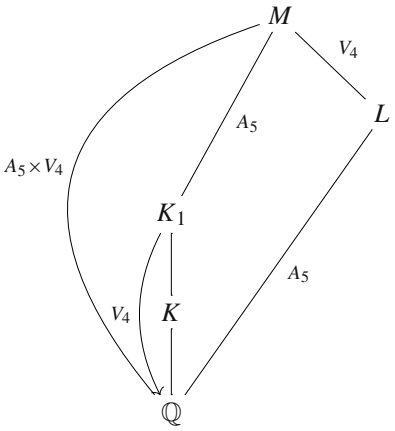
$$x^6 - 10x^4 - 7x^3 + 15x^2 + 14x + 3, \tag{4.1}$$

a totally real polynomial with discriminant $19^2 \cdot 293^2$. We can also find the polynomial (4.1) from the database of [4] and check that the discriminant of a root field of the polynomial (4.1) is also $19^2 \cdot 293^2$. Then, L is an A_5-extension over $\mathbb{Q}$ which is only ramified at 19 and 293. The factorizations of the above polynomial modulo 19 and 293 are

$$x^6 - 10x^4 - 7x^3 + 15x^2 + 14x + 3 = (x+12)^2(x+15)^2\left(x^2+3x+12\right) \bmod 19,$$
$$x^6 - 10x^4 - 7x^3 + 15x^2 + 14x + 3 = (x+66)^2(x+103)(x+160)(x+242)^2 \bmod 293.$$

Thus, 19 and 293 are the only primes ramified in this field with ramification index 2. By Abhyankar's lemma, LK_1/K_1 is unramified at all primes, and 2, 19, and 293 are the only primes ramified in $LK_1/\mathbb{Q}$ with ramification index 2 (note that $22268 = 4 \cdot$

19·293). Since A_5 is a non-abelian simple group, $L \cap K_1 = \mathbb{Q}$. Thus, $\mathrm{Gal}(LK_1/K_1) \simeq \mathrm{Gal}(L/\mathbb{Q}) \simeq A_5$, i.e., LK_1 is an unramified A_5-extension of K_1. We also know that $\mathrm{Gal}(LK_1/\mathbb{Q}) \simeq V_4 \times A_5$. Define M as LK_1.



4.2 Determination of $\mathrm{Gal}(K_{\mathrm{ur}}/K)$

To prove Theorem 4.1, it suffices to show that M possesses no non-trivial unramified extensions. Since M/K is unramified, the root discriminant of M is $|d_M|^{1/n_M} = |d_K|^{1/n_K} = \sqrt{22268} = 149.2246\ldots$ If we assume GRH, then $|d_M|^{1/n_M} = |d_K|^{1/n_K} = \sqrt{22268} = 149.2246\cdots < 153.252 \leq B(31970, 31970, 0)$ (see [6, Table]). This implies that $[K_{\mathrm{ur}} : M] < \frac{31,970}{[M:\mathbb{Q}]} = 133.2083\ldots$

We now first exclude the existence of non-trivial unramified abelian extensions of M. Suppose M possesses such an extension T/M. Without loss, T/M can be assumed cyclic of prime degree. Let T' be its normal closure over $\mathbb{Q}$. Then T' is unramified and elementary-abelian over K_1, and $\mathrm{Gal}(M/K_1) \simeq A_5$ acts on $\mathrm{Gal}(T'/M)$. The following intermediate result is useful.

Lemma 4.2 *If T/M is an unramified cyclic C_p-extension, then the action of A_5 on $\mathrm{Gal}(T'/M)$ is faithful or $[T' : M] = 2$.*

Proof Since A_5 is simple, it suffices to exclude the case that the action of A_5 on $\mathrm{Gal}(T'/M)$ is trivial. In that case, the extension $1 \to \mathrm{Gal}(T'/M) \to \mathrm{Gal}(T'/K_1) \to A_5 \to 1$ would be a central extension. Assume that this extension is not a stem extension. In this case, $\mathrm{Gal}(T'/K_1)$ has a non-trivial abelian quotient by Proposition 3.3. Since T'/K_1 is unramified, this contradicts the fact that K_1 has class number 1. So the extension is a stem extension, whence Lemma 3.4 yields $\mathrm{Gal}(T'/M) \simeq C_2$. □

Corollary 4.3 *If T/M is an unramified cyclic C_p-extension, then $\mathrm{Gal}(T'/M)$ is one of $(C_2)^k$ with $k \in \{1, 4, 5, 6, 7\}$, or $(C_3)^4$, or $(C_5)^3$.*

Proof Lemma 4.2 shows that either $[T' : M] = 2$, or A_5 embeds into $\mathrm{Aut}(\mathrm{Gal}(T'/M))$. Furthermore, we already know $[T' : M] \leq 133$. Now it is easy to check that only the above possibilities for $\mathrm{Gal}(T'/M)$ remain (see in particular Lemma 3.10). □

We now treat the remaining cases one by one.

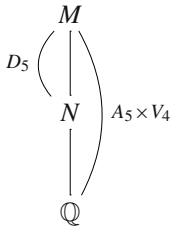
4.2.1 2-Class group of M

With the above notation, suppose that $\mathrm{Gal}(T/M) \simeq C_2$. Then, T'/M is unramified and $\mathrm{Gal}(T'/M)$ is isomorphic to $(C_2)^m$ $(1 \leq m \leq 7)$.

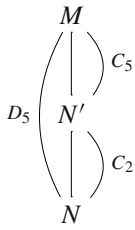
Let $E \subset L$ be a root field of the polynomial (4.1) and N be the compositum of E and K_1, i.e., $N = EK_1$. Then E can be defined by the composite of three polynomials: $x^2 - 19$, $x^2 - 293$ and the polynomial (4.1). By computer calculation, N is a root field of the following polynomial:

$$\begin{aligned}
&x^{24} - 3784x^{22} - 28x^{21} + 6404076x^{20} + 53312x^{19} - 6401641814x^{18} \\
&\quad - 31411548x^{17} + 4204260566526x^{16} - 5837238288x^{15} \\
&\quad - 1908791963697448x^{14} + 18501271313028x^{13} \\
&\quad + 613640140988085895x^{12} - 11975084172112012x^{11} \\
&\quad - 1406165162711839659 10x^{10} + 4264300576327196748x^9 \\
&\quad + 22779186389906647652933x^8 - 932994735936411884988x^7 \\
&\quad - 25427928013219963729128 90x^6 \\
&\quad + 12439363325568612791 7612x^5 \\
&\quad + 18559861964135953618092 4174x^4 \\
&\quad - 92373973101998964634611 64x^3 \\
&\quad - 79513244897969392700270 88092x^2 \\
&\quad + 29146425273178784072288 3096x \\
&\quad + 15117431604557742461676 9218057.
\end{aligned} \tag{4.2}$$

We also know that $\mathrm{Gal}(M/N)$ is isomorphic to D_5.



By computer calculation, we know that the class group of N is isomorphic to C_2 under GRH. Let N' be the Hilbert class field of N. (Note that, N' is a subfield of M, since M/N is unramified.)



By Lemma 2.2, the 2-class group of N' is trivial. Thus the rank m of the 2-class group of M is a multiple of 4 by Lemma 2.1, i.e., m is equal to 0 or 4.

Suppose that $m = 4$. Then, $\mathrm{Gal}(T'/K_1)$ is an extension of A_5 by $(C_2)^4$. By Lemma 4.2, $\mathrm{Gal}(M/K_1)$ acts faithfully on $\mathrm{Gal}(T'/M)$. Consider $\mathrm{Gal}(T'/K)$. This group is an extension of $\mathrm{Gal}(M/K)(\simeq A_5 \times C_2)$ by $\mathrm{Gal}(T'/M)(\simeq (C_2)^4)$ and an extension of $\mathrm{Gal}(K_1/K)(\simeq C_2)$ by $\mathrm{Gal}(T'/K_1)$ simultaneously. Therefore, it is natural to examine how $\mathrm{Gal}(K_1/K)$ acts on $\mathrm{Gal}(T'/M)(\simeq (C_2)^4)$. By Lemma 3.12, $\mathrm{Gal}(M/K)(\simeq A_5 \times C_2)$ does not act faithfully on $\mathrm{Gal}(T'/M)(\simeq (C_2)^4)$. Since $\mathrm{Gal}(M/K_1)(\simeq A_5)$ acts non-trivially on $\mathrm{Gal}(T'/M)$, we obtain that $\mathrm{Gal}(K_1/K)(\simeq \mathrm{Gal}(M/LK))$ acts trivially on $\mathrm{Gal}(T'/M)(\simeq (C_2)^4)$.
$\mathrm{Gal}(T'/LK) \simeq (C_2)^5$ Since $\mathrm{Gal}(M/LK)$ acts trivially on $\mathrm{Gal}(T'/M)$, $\mathrm{Gal}(T'/LK)$ is $(C_2)^3 \times C_4$ or $(C_2)^5$. Let $\mathrm{Gal}(T'/LK)$ be $(C_2)^3 \times C_4$. Then, $\mathrm{Gal}(T''/LK)$ is isomorphic to $(C_2)^4$, where T''/LK is the maximal elementary abelian 2-subextension of T'/LK. By the maximality of T'', T'' is also Galois over $\mathbb{Q}$ and $\mathrm{Gal}(T''/K)$ is an extension of A_5 by $(C_2)^4$. By restriction, this A_5-actions on $(C_2)^4$ comes from the $\mathrm{Gal}(M/K)$-actions on $\mathrm{Gal}(T'/M)$ mentioned above. Since $\mathrm{Gal}(T'/K_1)$ does not have any abelian quotient, $\mathrm{Gal}(T''/K)$ also has no abelian quotients, i.e., $T'' \cap K_1 = K$. Thus, $\mathrm{Gal}(T'/K)$ is a direct product of $\mathrm{Gal}(T''/K)$ and $\mathrm{Gal}(K_1/K)$, i.e., $\mathrm{Gal}(T'/LK)$ is a direct product of $\mathrm{Gal}(T''/LK) \simeq (C_2)^4$ and $\mathrm{Gal}(K_1/K) \simeq C_2$. This contradicts the fact that $\mathrm{Gal}(T'/LK)$ is $(C_2)^3 \times C_4$. Thus, $\mathrm{Gal}(T'/LK)$ is isomorphic to $(C_2)^5$, and there exists some $S/LK/K$ such that $SK_1 = T'$ and $\mathrm{Gal}(S/K) \simeq (C_2)^4 \rtimes A_5$.

In a similar manner, we can prove that there exists some $S'/L/\mathbb{Q}$ such that $S'K_1 = T'$ and $\mathrm{Gal}(S'/\mathbb{Q}) \simeq (C_2)^4 \rtimes A_5$.

Since $S'K$ is contained in T', $S'K/K$ is an unramified extension. Therefore, the only ramified primes in $S'/L/\mathbb{Q}$ are 2, 19, and 293 with ramification index 2. Since 19 and 293 are already ramified in $L/\mathbb{Q}$, the only ramified prime in S'/L is 2.

Unramifiedness of S'/L Suppose that 2 is ramified in S'/L. The ramification index of 2 should then be 2. Let $\bar{\mathfrak{p}}$ (resp. $\mathfrak{p}$) be a prime ideal in S' (resp. L) satisfying $\bar{\mathfrak{p}}|2$ (resp. $\mathfrak{p}|2$). The factorization of the polynomial (4.1) modulo 2 is

$$x^6 - 10x^4 - 7x^3 + 15x^2 + 14x + 3 \equiv (x+1)\left(x^5 + x^4 + x^3 + x + 1\right) \bmod 2. \tag{4.3}$$

Thus, we know that $\mathrm{Gal}(L_{\mathfrak{p}}/\mathbb{Q}_2)$ is isomorphic to $C_5 \simeq \langle(12345)\rangle$, where $L_{\mathfrak{p}}$ is the $\mathfrak{p}$-completion of L. Consider $\mathrm{Gal}(S'_{\bar{\mathfrak{p}}}/L_{\mathfrak{p}})$. Since the ramification index of $\mathfrak{p}$ is 2, $\mathrm{Gal}(S'_{\bar{\mathfrak{p}}}/L_{\mathfrak{p}})$ is C_2 or $(C_2)^2$, i.e., the proper subgroup of $(C_2)^4$. Hence, $\mathrm{Gal}(S'_{\bar{\mathfrak{p}}}/\mathbb{Q}_3) = \mathrm{Gal}(S'_{\bar{\mathfrak{p}}}/L_{\mathfrak{p}}) \rtimes \langle(12345)\rangle \subsetneq (C_2)^4 \rtimes \langle(12345)\rangle$. This contradicts the statement that

there is no proper subgroup of $(C_2)^4$ that is invariant under the action of $\langle(12345)\rangle$ (see Lemma 3.13). Thus, S'/L should be unramified at all places. In conclusion, $S'/\mathbb{Q}$ is a $(C_2)^4 \rtimes A_5$-extension of $\mathbb{Q}$ that has ramification index 2 at only 19 and 293. Let us now consider the root discriminant of S'. Since S'/L is unramified at all places,

$$|d_{S'}|^{1/n_{S'}} = |d_L|^{1/n_L} = \left(19^{30} \cdot 293^{30}\right)^{1/60} = \sqrt{19 \cdot 293} = 74.6123\ldots$$

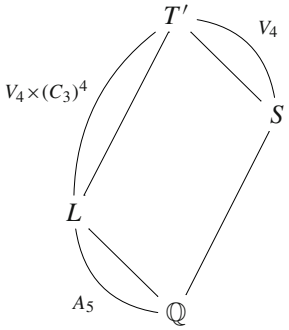
This implies that $|d_{S'}|^{1/n_{S'}} < 106.815\cdots \leq B(960,\ 960,\ 0)$ under the GRH (see [6, Table]). This contradicts the definition of the lower bound for the root discriminant. Thus, the 2-class group of M is trivial.

4.2.2 3-Class group of M

Suppose that T/M is an unramified C_3-extension. Then, as seen above, T' is unramified over M and $\mathrm{Gal}(T'/M)$ is isomorphic to $(C_3)^4$. Then, $\mathrm{Gal}(T'/\mathbb{Q})$ is an extension of $\mathrm{Gal}(M/\mathbb{Q}) \simeq A_5 \times V_4$ by $(C_3)^4$. Therefore, it is natural to examine how $\mathrm{Gal}(M/\mathbb{Q})$ acts on $\mathrm{Gal}(T'/M) \simeq (C_3)^4$. By Lemmas 3.14 and 3.15, we know that there are three possibilities of the actions of $\mathrm{Gal}(M/\mathbb{Q})$ on $\mathrm{Gal}(T'/M)$. [Note that $\mathrm{Aut}((C_3)^4) \simeq \mathrm{GL}_4(\mathbb{F}_3)$]. Each action is induced by the following three group homomorphisms $\psi : A_5 \times V_4 \to \mathrm{GL}_4(\mathbb{F}_3)$:

- ψ is trivial.
- $\psi(A_5 \times V_4) \simeq A_5$.
- $\psi(A_5 \times V_4) \simeq A_5 \times C_2$.

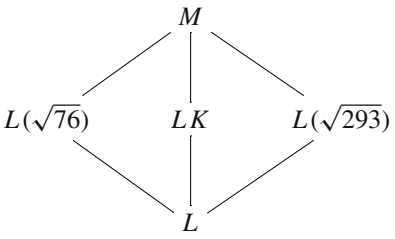
By Lemma 4.2, $\mathrm{Gal}(M/K_1)$ acts faithfully on $\mathrm{Gal}(T'/M)$. Therefore, ψ cannot be trivial.
$\psi(A_5 \times V_4) \simeq A_5$ This means that $\mathrm{Gal}(M/K_1)(\simeq A_5)$ acts non-trivially on $\mathrm{Gal}(T'/M)$ and $\mathrm{Gal}(M/L) \simeq V_4$ acts trivially on $\mathrm{Gal}(T'/M)$. Since $|\mathrm{Gal}(T'/M)|$ and $|\mathrm{Gal}(M/L)|$ are coprime, $\mathrm{Gal}(T'/L)$ is isomorphic to $V_4 \times (C_3)^4$. Let S be the subfield of T' fixed by V_4. Then $\mathrm{Gal}(S/\mathbb{Q})$ is a group extension of A_5 by $(C_3)^4$.



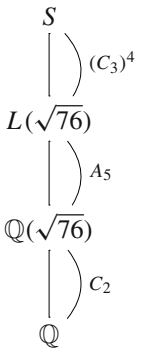
Since 19 and 293 are already ramified in $L/\mathbb{Q}$, the only ramified prime in S/L is 2. If 2 is ramified in S/L, its ramification index should be 2. But it is impossible, because the degree of $[S : L]$ is odd. Thus S/L is unramified over all places. By a similar

argument as in Sect. 4.2.2.1, we can check that this contradicts the definition of the lower bound for the root discriminant.

$\psi(A_5 \times V_4) \simeq A_5 \times C_2$ First of all, let us see the intermediate fields in M/L. Since $\mathrm{Gal}(M/L)$ is isomorphic to V_4, there are three proper intermediate fields in M/L.



Suppose that $\mathrm{Gal}(M/L(\sqrt{76}))$ acts trivially on $\mathrm{Gal}(T'/M)$. This means that $\mathrm{Gal}(T'/L(\sqrt{76}))$ is isomorphic to $C_2 \times (C_3)^4$, i.e., there exists a subfield S in $T'/L(\sqrt{76})$ such that $\mathrm{Gal}(S/L(\sqrt{76}))$ is isomorphic to $(C_3)^4$.



We easily check that $S/L(\sqrt{76})$ is unramified over all places. Let $\bar{\mathfrak{p}}$ (resp. $\mathfrak{p}'$, $\mathfrak{p}$) be a prime ideal in S [resp. $L(\sqrt{76})$, $\mathbb{Q}(\sqrt{76})$] satisfying $\bar{\mathfrak{p}}|2$ (resp. $\mathfrak{p}'|2$, $\mathfrak{p}|2$). We had already show that the factorization of the polynomial (4.1) modulo 2 is

$$x^6 - 10x^4 - 7x^3 + 15x^2 + 14x + 3 \equiv (x+1)\left(x^5 + x^4 + x^3 + x + 1\right) \bmod 2. \tag{4.4}$$

Thus, we know that $\mathrm{Gal}(L(\sqrt{76})_{\mathfrak{p}'}/\mathbb{Q}(\sqrt{76})_{\mathfrak{p}})$ is isomorphic to $C_5 \simeq \langle(12345)\rangle$, where $L(\sqrt{76})_{\mathfrak{p}'}$ [resp. $\mathbb{Q}(\sqrt{76})_{\mathfrak{p}}$] is the $\mathfrak{p}'$-completion of $L(\sqrt{76})$ [resp. the $\mathfrak{p}$-completion of $\mathbb{Q}(\sqrt{76})_{\mathfrak{p}}$].

Let us consider $\mathrm{Gal}(S_{\bar{\mathfrak{p}}}/L(\sqrt{76})_{\mathfrak{p}'})$. We know that $S/L(\sqrt{76})$ is unramified. Thus, $S_{\bar{\mathfrak{p}}}/L(\sqrt{76})_{\mathfrak{p}'}$ is a cyclic extension, i.e., $\mathrm{Gal}(S_{\bar{\mathfrak{p}}}/L(\sqrt{76})_{\mathfrak{p}'})$ is isomorphic to C_3 or a trivial group.

Suppose that $\mathrm{Gal}(S_{\bar{\mathfrak{p}}}/L(\sqrt{76})_{\mathfrak{p}'})$ is isomorphic to C_3. Then $\mathrm{Gal}(S_{\bar{\mathfrak{p}}}/\mathbb{Q}(\sqrt{76})_{\mathfrak{p}}) = \mathrm{Gal}(S_{\bar{\mathfrak{p}}}/L(\sqrt{76})_{\mathfrak{p}'}) \rtimes \langle(12345)\rangle \subsetneq (C_3)^4 \rtimes \langle(12345)\rangle$. This contradicts the statement

that there is no proper subgroup of $(C_3)^4$ that is invariant under the action of $\langle(12345)\rangle$ (see Lemma 3.16). In conclusion, $\mathrm{Gal}(S_{\bar{\mathfrak{p}}}/L(\sqrt{76})_{\mathfrak{p}'})$ is trivial.

Thus, for a number field $S/\mathbb{Q}$, $e_2 = 2$ and $f_2 = 5$ where e_2 is the ramification index of 2 and f_2 is the inertia degree for 2. Let us recall the function (2.3)

$$f = 2\sum_{\mathfrak{p}}\sum_{m=1}^{\infty}\frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^{m/2}}F\left(\log N(\mathfrak{p})^m\right).$$

Since every term of f is greater than or equal to 0, the following holds for the number field S.

$$f \geq 2\sum_{j=1}^{972}\sum_{i=1}^{100}\frac{\log N(\bar{\mathfrak{q}}_j)}{N(\bar{\mathfrak{q}}_j)^{i/2}}F\left(\log N\left(\bar{\mathfrak{q}}_j\right)^i\right), \tag{4.5}$$

where the $\bar{\mathfrak{q}}_j$ denote the prime ideals of S satisfying $\bar{\mathfrak{q}}_j|2$. Since $f_2 = 5$, $N(\bar{\mathfrak{q}}_j) = 2^5$ for all j. Set $b = 8.8$. By a numerical calculation, we have

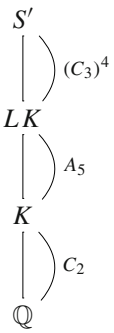
$$f \geq 2\cdot 972\sum_{i=1}^{100}\frac{\log 2^5}{2^{5i/2}}F\left(\log 2^{5i}\right) = 1111.46\ldots \tag{4.6}$$

Let us recall (2.2). For $b = 8.8$, we have

$$\begin{aligned}|d_S|^{1/n_S} &> 149.272\cdot \mathrm{e}^{(f-604.89)/9720}\\ &\geq 149.272\cdot \mathrm{e}^{(1111.46-604.89)/9720} = 157.258\ldots\end{aligned} \tag{4.7}$$

$|d_S|^{1/n_S} = |d_K|^{1/n_K} = \sqrt{22268}$ contradicts the fact that $|d_S|^{1/n_S} = 149.2246\ldots$

Next, suppose that $\mathrm{Gal}(M/LK)$ acts trivially on $\mathrm{Gal}(T'/M)$. This means that $\mathrm{Gal}(T'/LK)$ is isomorphic to $C_2\times(C_3)^4$, i.e., there exists a subfield S' in T'/LK such that $\mathrm{Gal}(S'/LK)$ is isomorphic to $(C_3)^4$.

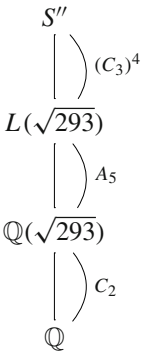


By the same argument as in the above, we can get

$$|d_{S'}|^{1/n_S} > 157.258\ldots \tag{4.8}$$

and this contradicts the fact that $|d_S|^{1/n_S} = 149.2246\ldots$

Finally, suppose that $\mathrm{Gal}(M/L(\sqrt{293}))$ acts trivially on $\mathrm{Gal}(T'/M)$. This means that $\mathrm{Gal}(T'/L(\sqrt{293}))$ is isomorphic to $C_2 \times (C_3)^4$, i.e., there exists a subfield S'' in $T'/L(\sqrt{293})$ such that $\mathrm{Gal}(S''/L(\sqrt{293}))$ is isomorphic to $(C_3)^4$.



We easily know that 19 and 293 are the only ramified primes in $S''/\mathbb{Q}$. By a similar argument as in Sect. 4.2.1.2, we can check that this contradicts the definition of the lower bound for the root discriminant.

In conclusion, the 3-class group of M is trivial.

4.2.3 5-Class group of M

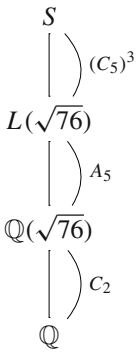
Suppose that T/M is an unramified C_5-extension. Then, T' is unramified over M and $\mathrm{Gal}(T'/M)$ is isomorphic to $(C_5)^3$. Thus, $\mathrm{Gal}(T'/\mathbb{Q})$ is an extension of $\mathrm{Gal}(M/\mathbb{Q}) \simeq A_5 \times V_4$ by $(C_5)^3$. Therefore, it is natural to examine how $\mathrm{Gal}(M/\mathbb{Q})$ acts on $\mathrm{Gal}(T'/M) \simeq (C_5)^3$. By Lemmas 3.17 and 3.18, we know that there are three possibilities of the actions of $\mathrm{Gal}(M/\mathbb{Q})$ on $\mathrm{Gal}(T'/M)$. Each action is induced by the following three group homomorphisms $\psi : A_5 \times V_4 \to \mathrm{GL}_3(\mathbb{F}_5)$:

- ψ is trivial.
- $\psi(A_5 \times V_4) \simeq A_5$.
- $\psi(A_5 \times V_4) \simeq A_5 \times C_2$.

By a similar argument as in Sect. 4.2.2, we just need to think about the case $\psi(A_5 \times V_4) \simeq A_5 \times C_2$.

$\psi(A_5 \times V_4) \simeq A_5 \times C_2$ Consider again the intermediate fields of M/L as in Sect. 4.2.2.2. Suppose that $\mathrm{Gal}(M/L(\sqrt{76}))$ acts trivially on $\mathrm{Gal}(T'/M)$. This means that $\mathrm{Gal}(T'/L(\sqrt{76}))$ is isomorphic to $C_2 \times (C_5)^3$, i.e., there exists a subfield S in

$T'/L(\sqrt{76})$ such that $\mathrm{Gal}(S/L(\sqrt{76}))$ is isomorphic to $(C_5)^3$.

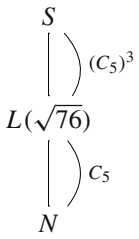


From [4], we know that L can also be defined as the splitting field of following polynomial, corresponding to an imprimitive degree-12 action of A_5:

$$\begin{aligned} x^{12} + 11x^{11} - 59x^{10} - 647x^9 - 295x^8 + 5446x^7 + 4294x^6 \\ - 14727x^5 - 4960x^4 + 16477x^3 - 4028x^2 - 1813x + 324. \end{aligned} \tag{4.9}$$

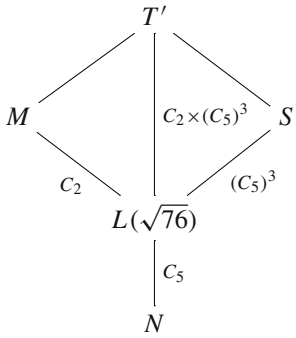
Let $E \subset L$ be a root field of the polynomial (4.9). We know that the discriminant d_E of E is $19^6 \cdot 293^6$. Since $|d_E|^{1/n_E} = |d_L|^{1/n_L}$, L/E is unramified.

Define N as the compositum of E and $\mathbb{Q}(\sqrt{76})$. Then N is a subfield of $L(\sqrt{76})$ and $\mathrm{Gal}(L(\sqrt{76})/N)$ is isomorphic to C_5.



By Abhyankar's lemma, we easily know that $L(\sqrt{76})/N$ is unramified. Using a computer calculation, we can check that N is a root field of the following polynomial:

$$\begin{aligned} x^{24} - 111x^{22} + 4394x^{20} - 83286x^{18} + 818659x^{16} - 4122356x^{14} \\ + 9878557x^{12} - 10688099x^{10} + 5561624x^8 - 1360039x^6 \\ + 130854x^4 - 2499x^2 + 1. \end{aligned} \tag{4.10}$$



By the calculation of Sage, we can check that the class group of N is equal to C_{10}, i.e., 5-class group of N is C_5 and Hilbert 5-class field of N is $L(\sqrt{76})$. We know that $\mathrm{Gal}(T'/L(\sqrt{76}))$ is isomorphic to $C_2 \times (C_3)^5$, i.e., 5-class group of $L(\sqrt{76})$ is not trivial. This contradicts Lemma 2.2.

Suppose that $\mathrm{Gal}(M/LK)$ acts trivially on $\mathrm{Gal}(T'/M)$. Define N' as the compositum of E and K. Then N can be defined by the following polynomial:

$$\begin{aligned} & x^{24} - 98x^{22} + 4073x^{20} - 94,476x^{18} + 1354898x^{16} - 12553566x^{14} \\ & \quad + 76075696x^{12} - 297782263x^{10} + 723063287x^8 - 1000608193x^6 \\ & \quad + 654400814x^4 - 110097135x^2 + 3818116. \end{aligned} \tag{4.11}$$

By a computer calculation with Magma, we can check, assuming GRH, that the class group of N is equal to C_{10}, i.e., the 5-class group of N is C_5 and the Hilbert 5-class field of N is LK. By the same argument as above, we obtain a contradiction.

Suppose that $\mathrm{Gal}(M/L(\sqrt{293}))$ acts trivially on $\mathrm{Gal}(T'/M)$. This means that $\mathrm{Gal}(T'/L(\sqrt{293}))$ is isomorphic to $C_2 \times (C_5)^3$, i.e., there exists a subfield S'' in $T'/L(\sqrt{293})$ such that $\mathrm{Gal}(S''/L(\sqrt{293}))$ is isomorphic to $(C_5)^3$, and such that 19 and 293 are the only ramified primes in $S''/\mathbb{Q}$. By a similar argument as in Sect. 4.2.2.1, we can check that this contradicts the lower bound for the root discriminant.

In conclusion, 5-class group of M is also trivial under the assumption of the GRH. We have therefore obtained:

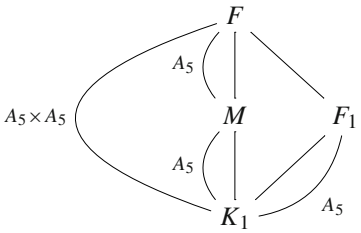
Proposition 4.4 *The class number of M is* 1, *under the assumption of the GRH.*

4.2.4 A_5-unramified extension of M

Since the class number of M is one, there is no solvable unramified extension over M. The last thing we have to do is to show that there is no nonsolvable unramified extension over M. Since $[K_{\mathrm{ur}} : M] < 133.2083\ldots$, our task is to show that K does not admit an unramified A_5-extension.

Suppose that M admits an unramified A_5-extension F. Because $[K_{\mathrm{ur}} : M] < 134$, F is the unique unramified A_5-extension of M, i.e., F is Galois over $\mathbb{Q}$. It is well known that A_5 is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_5)$ and S_5 is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_5)$. By

Lemma 3.6, $\mathrm{Gal}(F/K_1) \simeq A_5 \times A_5$, i.e., K_1 admits another A_5-unramified extension F_1.



(Note that, F_1 is also Galois over $\mathbb{Q}$, or otherwise K_1 would have further unramified A_5-extensions, contradicting Odlyzko's bound.) Then, by Lemma 3.6, there are only two possibilities for $\mathrm{Gal}(F_1/K)$: $A_5 \times C_2$ or S_5.

Case 1: $\mathrm{Gal}(F_1/K) \simeq A_5 \times C_2$ By a similar argument in the above, K admits an A_5-unramified extension F_2. Then, $\mathrm{Gal}(F_2/\mathbb{Q})$ is also isomorphic to $A_5 \times C_2$ or S_5.

Case 1.1: $\mathrm{Gal}(F_2/\mathbb{Q}) \simeq A_5 \times C_2$ This implies that there exists an A_5-extension $F_3/\mathbb{Q}$ with all ramification indices ≤ 2 and unramified outside of $\{2,\ 19,\ 293\}$. Assume first that 19 is unramified in $F_3/\mathbb{Q}$. Let E be a quintic subfield of $F_3/\mathbb{Q}$. Then, by a well known result of Dedekind, we get the upper bound $|d_E| \leq 2^6 \cdot 293^2 < 5.5 \cdot 10^6$ for the discriminant of E. However, from [8, Table 2 in Sect. 4.1] no extension with this discriminant bound and ramification restrictions exists. We may therefore assume that 19 is ramified in $F_3/\mathbb{Q}$. Since its inertia group is generated by a double transposition in A_5, the inertia degree of 19 in the extension $F_2/\mathbb{Q}$ (with Galois group $A_5 \times C_2$) is at most 2. The same holds for the inertia degree of 19 in the extension $L/\mathbb{Q}$, and therefore eventually also in the compositum $LF_2/\mathbb{Q}$.

Let us recall the function (2.3)

$$f = 2 \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^{m/2}} F\left(\log N(\mathfrak{p})^m\right).$$

Since every term of f is greater than or equal to 0, the following holds for the number field LF_2.

$$f \geq 2 \sum_{j=1}^{1800} \sum_{i=1}^{100} \frac{\log N(\bar{\mathfrak{q}}_j)}{N(\bar{\mathfrak{q}}_j)^{i/2}} F\left(\log N(\bar{\mathfrak{q}}_j)^i\right), \tag{4.12}$$

where the $\bar{\mathfrak{q}}_j$ denote the prime ideals of LF_2 satisfying $\bar{\mathfrak{q}}_j | 19$. Since $f_{19} = 2$, $N(\bar{\mathfrak{q}}_j) = 19^2$ for all j. Set $b = 8.8$. By a numerical calculation, we have

$$f \geq 2 \cdot 1800 \sum_{i=1}^{100} \frac{\log 19^2}{19^i} F\left(\log 19^{2i}\right) = 683.225\ldots \tag{4.13}$$

Let us recall (2.2). For $b = 8.8$, we have

$$\begin{aligned} \left|d_{LF_2}\right|^{1/n_{LF_2}} &> 149.272 \cdot \mathrm{e}^{(f-604.89)/7200} \\ &\geq 149.272 \cdot \mathrm{e}^{(683.225-604.89)/7200} = 150.905\ldots \end{aligned} \tag{4.14}$$

$|d_{LF_2}|^{1/n_{LF_2}} = |d_K|^{1/n_K} = \sqrt{22268}$ contradicts the fact that $|d_{LF_2}|^{1/n_{LF_2}} = 149.2246\ldots$

Case 1.2: $\mathrm{Gal}(F_2/\mathbb{Q}) \simeq S_5$ By the unramifiedness of F_2/K, and since the only involutions of S_5 not contained in A_5 are the transpositions, a quintic subfield E of F_2 must have the discriminant 22268. However, such a quintic number field does not exist, from [8]. This is a contradiction.

Case 2: $\mathrm{Gal}(F_1/K) \simeq S_5$ By Lemma 3.6, $\mathrm{Gal}(F_1/\mathbb{Q}) \simeq S_5 \times C_2$. Consequently, F_1 is the compositum of K and an S_5-extension F_2 of $\mathbb{Q}$. Furthermore, $F_2/\mathbb{Q}$ has a quadratic subextension contained in K_1, but linearly disjoint from K. Therefore, it is either $\mathbb{Q}(\sqrt{293})$ or $\mathbb{Q}(\sqrt{76})$. Consider now a quintic subfield E of $F_2/\mathbb{Q}$. Of course, $E/\mathbb{Q}$ is unramified outside $\{2,\ 19,\ 293\}$. Furthermore, all non-trivial inertia subgroups are generated either by transpositions or by double transpositions. Finally, the inertia subgroups at those primes which ramify in the quadratic subfield of $F_2/\mathbb{Q}$ are generated by transpositions. By a similar argument as in Sect. 4.2.4.2, we then get one of the following two upper bounds for the discriminant of E: either $|d_E| \leq 2^3 \cdot 19 \cdot 293^2$ [namely, if the quadratic subfield is $\mathbb{Q}(\sqrt{76})$], or $|d_E| \leq 2^6 \cdot 19^2 \cdot 293$. Such a quintic number field does not exist, from [8, Sect. 4.1]. This is a contradiction.

In conclusion, M admits no unramified A_5-extensions, i.e., we have that $\mathrm{Gal}(K_{ur}/K_1) \cong A_5$ under the assumption that the GRH holds. This concludes the proof of Theorem 4.1.

5 Example: $K = \mathbb{Q}(\sqrt{-1567})$

Until now, we dealt with real quadratic fields. In this section, we will give the first case of an imaginary quadratic field.

Let K be the imaginary quadratic number field $\mathbb{Q}(\sqrt{-1567})$. We show the following:

Theorem 5.1 *Let K be the imaginary quadratic field $\mathbb{Q}(\sqrt{-1567})$ and K_{ur} be its maximal unramified extension. Then $\mathrm{Gal}(K_{\mathrm{ur}}/K)$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_8) \times C_{15}$ under the assumption of the GRH.*

The class number of K is 15, i.e., $\mathrm{Cl}(K) \simeq C_{15}$. Let K_1 be the Hilbert class field of K.

5.1 Class number of K_1

The first thing we have to do is show that the class number of K_1 is one. It can be computed that K_1 is the splitting field of the polynomial

$$x^{15} + 14x^{14} + 56x^{13} + 105x^{12} + 497x^{11} + 832x^{10} + 1157x^9 + 1274x^8 + 644x^7 - 971x^6 - 2582x^5 - 177x^4 + 7x^3 + 1187x^2 - 20x + 1. \tag{5.1}$$

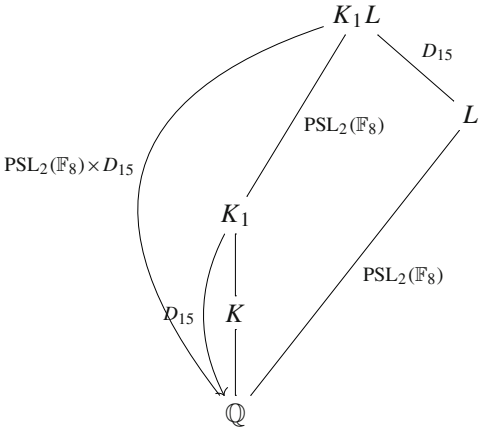
We can then check with Magma that the class number of K_1 is 1, under GRH.

5.2 An unramified $\mathrm{PSL}_2(\mathbb{F}_8)$-extension of K_1

Let $K = \mathbb{Q}(\sqrt{-1567})$ and let L be the splitting field of

$$x^9 - 2x^8 + 10x^7 - 25x^6 + 34x^5 - 40x^4 + 52x^3 - 45x^2 + 20x - 4, \tag{5.2}$$

a polynomial with complex roots. Then L is a $\mathrm{PSL}_2(\mathbb{F}_8)$-extension of $\mathbb{Q}$ and 1567 is the only prime ramified in this field with ramification index two. By Abhyankar's lemma, LK/K is unramified at all primes. Since $\mathrm{PSL}_2(\mathbb{F}_8)$ is a non-abelian simple group, $L \cap K_1 = \mathbb{Q}$. So $\mathrm{Gal}(LK_1/K_1) \simeq \mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{PSL}_2(\mathbb{F}_8)$, i.e., LK_1 is a $\mathrm{PSL}_2(\mathbb{F}_8)$-extension of K_1 which is unramified over all places. It follows that $\mathrm{Gal}(LK_1/\mathbb{Q})$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_8) \times D_{15}$.



5.3 The determination of $\mathrm{Gal}(K_{\mathrm{ur}}/K)$

Define M as LK_1. Since M/K is unramified at all places, the root discriminant of M is $|d_M|^{1/|M|} = |d_K|^{1/|K|} = \sqrt{1567} = 39.5853\ldots$ If we assume GRH, then $|d_M|^{1/|M|} = |d_K|^{1/|K|} = \sqrt{1567} = 39.5853 < 39.895\cdots = B(1000000, 0, 500000)$ (see [6, Table]). This implies that $[K_{\mathrm{ur}} : M] < \frac{1{,}000{,}000}{[M:\mathbb{Q}]} = 66.1375\ldots$ We now proceed similarly as in Sect. 4. Let T be a non-trivial unramified C_p-extension of M, and let T' be its Galois closure over $\mathbb{Q}$. First, we obtain the following analog of Lemma 4.2.

Lemma 5.2 *If T/M is a non-trivial unramified cyclic C_p-extension, then the action of* $\mathrm{PSL}_2(\mathbb{F}_8)$ *on* $\mathrm{Gal}(T'/M)$ *is faithful.*

Proof As in Lemma 4.2, and using additionally that $\mathrm{PSL}_2(\mathbb{F}_8)$ has trivial Schur multiplier (see Lemma 3.5). □

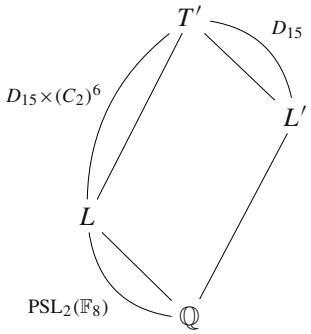
Corollary 5.3 *If T/M is a non-trivial unramified cyclic C_p-extension, then $p = 2$ and $\mathrm{Gal}(T'/M) \simeq (C_2)^6$.*

Proof Use Lemma 5.2, the bound $[T' : M] \leq 66$, and Lemmas 3.10 and 3.19 in order to obtain that $(C_2)^6$ is the only elementary-abelian group in the relevant range which allows a non-trivial $\mathrm{PSL}_2(\mathbb{F}_8)$-action. □

We deal with the remaining case below.

5.3.1 2-Class group of M

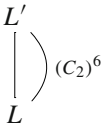
Suppose that M has an unramified C_2-extension T and let T' be its normal closure over $\mathbb{Q}$. As shown above, T' is unramified over M and $\mathrm{Gal}(T'/M)$ is isomorphic to $(C_2)^6$.



Let $\bar{\mathfrak{p}}$ (resp. $\mathfrak{p}$) be a prime ideal in L' (resp. L) satisfying $\bar{\mathfrak{p}}|2$ (resp. $\mathfrak{p}|2$). The factorization of the polynomial (5.2) modulo 2 is

$$x^2\left(x^7 + x^4 + 1\right) \bmod 2. \tag{5.3}$$

Since $\mathrm{PSL}_2(\mathbb{F}_8)$ contains no elements of order 14, we thus know that $\mathrm{Gal}(L_{\mathfrak{p}}/\mathbb{Q}_2)$ is isomorphic to C_7, where $L_{\mathfrak{p}}$ is the $\mathfrak{p}$-completion of L. Consider $\mathrm{Gal}(L'_{\bar{\mathfrak{p}}}/L_{\mathfrak{p}})$. Because L'/L is unramified, $\mathrm{Gal}(L'_{\bar{\mathfrak{p}}}/L_{\mathfrak{p}})$ is either trivial or C_2.



By Lemma 3.20, there is a unique class of subgroups $\mathrm{PSL}_2(\mathbb{F}_8)$ inside $\mathrm{GL}_6(\mathbb{F}_2)$. The cyclic subgroups of order 7 in these subgroups act fixed-point-freely on $(C_2)^6$ (in fact, the vector space decomposes into a direct sum of two irreducible modules of

dimension 3 under their action). Therefore, the corresponding group extension of C_7 by $(C_2)^6$ has trivial center, and in particular contains no element of order 14. Thus, $\mathrm{Gal}(L'_{\bar{\mathfrak{p}}}/L_{\mathfrak{p}})$ is trivial, i.e., $\mathfrak{p}$ splits completely in L'.

Define S to be the compositum $L'K$. Since $-1567 \equiv 1$ modulo 8, 2 splits completely in K. Then, for the number field $S/\mathbb{Q}$, we have that $f_2 = 7$, where f_2 is the inertia degree of 2. Let us recall the function (2.3) again.

$$f = 2\sum_{\mathfrak{p}}\sum_{m=1}^{\infty}\frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^{m/2}}F\left(\log N(\mathfrak{p})^m\right).$$

Since every term of f is greater than or equal to 0, the following holds for the number field S.

$$f \geq 2\sum_{j=1}^{9216}\sum_{i=1}^{100}\frac{\log N(\bar{\mathfrak{q}}_j)}{N(\bar{\mathfrak{q}}_j)^{i/2}}F\left(\log N\left(\bar{\mathfrak{q}}_j\right)^i\right), \tag{5.4}$$

where the $\bar{\mathfrak{q}}_j$ denote the prime ideals of S satisfying $\bar{\mathfrak{q}}_j|2$. Since $f_2 = 7$, $N(\bar{\mathfrak{q}}_j) = 2^7$ for all j. Set $b = 11.6$. By a numerical calculation, we have

$$f \geq 2\cdot 9216\sum_{i=1}^{100}\frac{\log 2^7}{2^{7i/2}}F\left(\log 2^{7i}\right) = 6814.41\ldots \tag{5.5}$$

Let us recall (2.2). For $b = 11.6$, we have

$$\begin{aligned}|d_S|^{1/n_S} &> 39.619\cdot \mathrm{e}^{(f-4790.3)/64{,}512}\\ &\geq 39.619\cdot \mathrm{e}^{(6814.41-4790.3)/64{,}512} = 40.8818\ldots\end{aligned} \tag{5.6}$$

Since S/K is unramified, $|d_S|^{1/n_S} = |d_K|^{1/n_K} = \sqrt{1567} = 39.5853\ldots$ This is a contradiction. Therefore, the 2-class group of M is trivial. In conclusion, the class number of M is one.

5.3.2 A_5-unramified extension of M

Since $[K_{\mathrm{ur}} : M] < 66.1375\ldots$, our final task is to show that M does not admit an unramified A_5-extension. By an analogous argument as in Sect. 4.2.4, K admits an A_5-extension F and $\mathrm{Gal}(F/\mathbb{Q})$ is also isomorphic to $A_5 \times C_2$ or S_5.

Case 1: $\mathrm{Gal}(F/\mathbb{Q}) \simeq A_5 \times C_2$ This implies that there exists an A_5-extension $F_1/\mathbb{Q}$ with ramification index 2 at 1567, and unramified at all other finite primes. However, from [1, Tables] no such extensions exists. This is a contradiction.

Case 2: $\mathrm{Gal}(F/\mathbb{Q}) \simeq S_5$ By the unramifiedness of F/K, a quintic subfield E of F must have the discriminant -1567. However, the minimal negative discriminant of quintic fields with Galois group S_5 is -4511 [8, Table 3]. This is a contradiction.

Therefore, we know that $K_{\mathrm{ur}} = M$ under the assumption of the GRH. This concludes the proof of Theorem 5.1.

References

1. Basmaji, J., Kiming, I.: A table of A_5 fields. In: On Artin's Conjecture for Odd 2-Dimensional Representations. Lecture Notes in Mathematics, vol. 1585, pp. 37–46, 122–141. Springer, Berlin (1994)
2. Huppert, B.: Endliche Gruppen I. Springer, Berlin (1967)
3. Kim, K.: Some examples of real quadratic fields with finite nonsolvable maximal unramified extensions. J. Number Theory **166**, 235–249 (2016)
4. Klüners, J., Malle, G. http://galoisdb.math.upb.de/home
5. König, J., Legrand, F., Neftin, D.: On the local behaviour of specializations of function field extensions. Preprint (2017). https://arxiv.org/pdf/1709.03094.pdf
6. Martinet, J.: Petits discriminants des corps de nombres. Number Theory Days, 1980 (Exeter, 1980). London Mathematical Society Lecture Note Series 56, pp. 151–193. Cambridge University Press, Cambridge (1982)
7. Neukirch, J.: Algebraic number theory. Grundlehren der Mathematischen Wissenschaften, vol. 322. Springer, Berlin (1999)
8. Schwarz, A., Pohst, M., Diaz, F., Diaz, Y.: A table of quintic number fields. Math. Comput. **63**(207), 361–376 (1994)
9. Suzuki, M.: Group theory. I. Grundlehren der Mathematischen Wissenschaften, vol. 247. Springer, Berlin (1982)
10. Taussky, O.: A remark on the class field tower. J. Lond. Math. Soc. **12**, 82–85 (1937)
11. Washington, L.C.: Introduction to Cyclotomic Fields. Graduate Texts in Mathematics, vol. 83. Springer, New York (1982)
12. Wilson, R.A.: The Finite Simple Groups. Graduate Texts in Mathematics, vol. 251. Springer, London (2009)
13. Yamamura, K.: Maximal unramified extensions of imaginary quadratic number fields of small conductors. J. Théor. Nr. Bordx **9**(2), 405–448 (1997)