ACTA ARITHMETICA
179.2 (2017)

An example of a $\mathrm{PSL}_2(\mathbb{F}_7)$-maximal unramified extension of a quartic number field

by

Kwang-Seob Kim (Seoul)

1. Introduction. This work is a continuation of [3] and [4]. One of the current problems in algebraic number theory is to gain a deeper understanding of the Galois groups of various Galois extensions of number fields, especially maximal extensions of number fields with restricted ramifications. Such Galois groups can be regarded as étale fundamental groups of spectrums of algebraic integer rings punctured at some closed points, and they play an essential role in understanding the arithmetic of number fields, in analogy with the geometric fundamental groups of manifolds in geometry. In other words, we can write $\pi_1^{\text{ét}}(X) \simeq \mathrm{Gal}(K_{\mathrm{ur}}^f/K)$, where K_{ur}^f is the maximal extension of K that is unramified over all finite spaces. This fact provides one motivation for studying unramified extensions of number fields and their Galois groups.

In [3] and [4], we have already demonstrated that there exist real quadratic fields K such that the étale fundamental groups are isomorphic to A_5 under the assumption of the generalized Riemann hypothesis (GRH), i.e., $\mathrm{Gal}(K_{\mathrm{ur}}^f/K)$ is isomorphic to A_5 where K_{ur}^f is the maximal extension of K that is unramified over *all finite spaces*.

It is well known that A_5 is the smallest nonabelian simple group. Then, we can naturally ask whether there exists a number field K such that $\mathrm{Gal}(K_{\mathrm{ur}}^f/K)$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_7)$. Here, $\mathrm{PSL}_2(\mathbb{F}_7)$ is the second smallest non-abelian simple group. In this article, we will construct a finite nonabelian simple étale fundamental group that is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_7)$ under the GRH. (We require the GRH for the lower discriminant bound, and for the computation of some narrow class groups.)

2010 *Mathematics Subject Classification*: Primary 11R37; Secondary 11F80, 11R29.
Key words and phrases: nonsolvable unramified extensions of number fields, class number one problems.
Received 18 April 2016; revised 4 January 2017.
Published online 7 July 2017.

DOI: 10.4064/aa8506-2-2017

PROPOSITION 1.1. *Let K be the narrow Hilbert class field of the real quadratic field $\mathbb{Q}(\sqrt{1417})$. Then, under the assumption of the GRH,* $\mathrm{Gal}(K_{\mathrm{ur}}^f/K)$ *is isomorphic to the finite nonsolvable group* $\mathrm{PSL}_2(\mathbb{F}_7)$.

Here, we briefly summarize the structure of this article. First, we will find an unramified extension M/K such that $\mathrm{Gal}(M/K) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$. Second, we will demonstrate that the class number of M is one. Finally, we will show that no nonsolvable unramified extension of M exists, i.e., $K_{\mathrm{ur}}^f = M$.

2. Preliminaries

2.1. Discriminant bounds. In this section, we will demonstrate how to use the discriminant bound to determine that a field admits no nonsolvable unramified extensions.

2.1.1. *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 $L/K/F$ of number fields, we have the following equality for ideals of F:

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

where $d_{L/F}$ denotes the relative discriminant (see [8, Corollary 2.10]). We set $F = \mathbb{Q}$. It follows from (2.1) that if L is an extension of K, then $|d_K|^{1/n_K} \le |d_L|^{1/n_L}$, with equality holding if and only if $d_{L/K} = 1$, i.e., L/K is unramified over *all finite spaces.*

2.1.2. *Crucial proposition.* Let K_{ur} be the maximal extension of K that is unramified over all primes.

PROPOSITION 2.1 ([14, Proposition 1]). *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 admits an unramified normal extension L of degree m. If* $\mathrm{Cl}(L) = 1$ *and* $|d_K|^{1/n_K} < B(60mn_K, 60mr_1, 60mr_2)$, *then* $K_{\mathrm{ur}} = L$. (*Here,* $\mathrm{Cl}(L)$ *denotes the class number of* L.)

REMARK 2.2. Suppose that L/K is unramified over all finite primes. Let $\mathrm{Cl}^+(L)$ be the narrow class group of L. If $\mathrm{Cl}^+(L) = 1$ and $|d_K|^{1/n_K} < B(60mn_K, 0, 60mr_2)$, then $K_{\mathrm{ur}}^f = L$.

2.1.3. *Description of Table III of [7].* Table III of [7] describes the following. If K is an algebraic number field containing r_1 real and $2r_2$ complex conjugate fields, and d_K denotes the absolute value of the discriminant of K, then for any b,

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

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

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

Here, 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

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

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

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

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

in the GRH case.

2.2. $\mathbb{F}_2$-representations of C_7. In this section, we will consider $\mathbb{F}_2$-representations of C_7, which we will use later. We will deal with C_7-actions on $\mathbb{F}_2[C_7]$-modules $(\mathbb{F}_2)^n$, where $1 \le n \le 5$. Since the characteristic of $\mathbb{F}_2$ does not divide $\#G$, all $\mathbb{F}_2[C_7]$-modules $(\mathbb{F}_2)^n$ are *completely reducible*. Let us denote by ϕ_n any representation $C_7 \to \mathrm{Aut}((\mathbb{F}_2)^n)$. If n is equal to 1 or 2, there is only a trivial representation.

2.2.1. *Classification of ϕ_3.* We can check that $\mathrm{GL}_3(\mathbb{F}_2)$ has two conjugacy classes of order 7. They are

$$\begin{pmatrix} 0&1&0\\ 0&0&1\\ 1&0&1 \end{pmatrix} \text{ and } \begin{pmatrix} 0&1&0\\ 0&0&1\\ 1&1&0 \end{pmatrix}. \tag{2.6}$$

This implies that there are two nontrivial representations $C_7 \to \mathrm{GL}_3(\mathbb{F}_2)$.

2.2.2. *Classification of ϕ_4 and ϕ_5.* We can check that $\mathrm{GL}_4(\mathbb{F}_2)$ has two conjugacy classes of order 7:

$$\begin{pmatrix} 1&0&0&0\\ 0&0&1&0\\ 0&0&0&1\\ 0&1&1&0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1&0&0&0\\ 0&0&1&0\\ 0&0&0&1\\ 0&1&0&1 \end{pmatrix}. \tag{2.7}$$

This implies that there are two nontrivial representations $C_7 \to \mathrm{GL}_3(\mathbb{F}_2)$, and we know that they come from $C_7 \to \mathrm{GL}_3(\mathbb{F}_2) \hookrightarrow \mathrm{GL}_4(\mathbb{F}_2)$ because $\mathrm{GL}_3(\mathbb{F}_2)$ also has two conjugacy classes of order 7. This implies that a nontrivial $\mathbb{F}_2[C_7]$-module $(\mathbb{F}_2)^4$ is reducible and $(\mathbb{F}_2)^4 = (\mathbb{F}_2)^3 \oplus \mathbb{F}_2$.

Likewise, we can check that a nontrivial $\mathbb{F}_2[C_7]$-module $(\mathbb{F}_2)^5$ is reducible and $(\mathbb{F}_2)^5 = (\mathbb{F}_2)^3 \oplus \mathbb{F}_2 \oplus \mathbb{F}_2$.

2.2.3. *Classification of* ϕ_6. Let us consider the following subgroup of $\mathrm{GL}_6(\mathbb{F}_2)$:

$$\begin{pmatrix} \mathrm{GL}_3(\mathbb{F}_2) & 0 \\ 0 & \mathrm{GL}_3(\mathbb{F}_2) \end{pmatrix} \subset \mathrm{GL}_6(\mathbb{F}_2).$$

Thus, a nontrivial $\mathbb{F}_2[C_7]$-module $(\mathbb{F}_2)^6$ can be decomposed into two nontrivial $\mathbb{F}_2[C_7]$-modules $(\mathbb{F}_2)^3$, i.e., $(\mathbb{F}_2)^6 = (\mathbb{F}_2)^3 \oplus (\mathbb{F}_2)^3$. Therefore, there is a possibility that an $\mathbb{F}_2[C_7]$-module $(\mathbb{F}_2)^6$ has no trivial submodule.

2.3. Remark regarding the class field tower

LEMMA 2.3 ([11, Theorem 1]). *Let K be an algebraic number field of finite degree, 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.*

REMARK 2.4. The lemma above can be easily proved using elementary group theory. We can prove the case of the narrow p-Hilbert class field using the same method.

3. Some group theory.

In this section, we recall some facts from group theory. We will consider the theory of group extensions, which we will use later.

3.1. Central extensions of $\mathrm{PSL}_2(\mathbb{F}_7)$

LEMMA 3.1. *Let μ_{p^n} be the multiplicative cyclic group generated by the p^nth primitive root of unity in $\mathbb{C}^*$. If p is an odd prime, then $H^2(\mathrm{PSL}_2(\mathbb{F}_7), \mu_{p^n}) = 0$, whereas $H^2(\mathrm{PSL}_2(\mathbb{F}_7), \mu_{2^n}) \simeq C_2$ for all $n \geq 1$.*

Proof. This is a consequence of the $\mathrm{PSL}_2(\mathbb{F}_7)$ cohomology of the exponential sequence

$$1 \to \mu_{2^n} \to \mathbb{C}^* \xrightarrow{\tau} \mathbb{C}^* \to 1$$

in which τ is defined by $\alpha \mapsto \alpha^{p^n}$, along with the fact that $H^1(\mathrm{PSL}_2(\mathbb{F}_7), \mathbb{C}^*) = 0$ and $H^2(\mathrm{PSL}_2(\mathbb{F}_7), \mathbb{C}^*) = C_2$, by [13, 3.3]. ∎

PROPOSITION 3.2. *Let H be an abelian 2-group. Suppose that $1 \to H \to G \to \mathrm{PSL}_2(\mathbb{F}_7) \to 1$ is a central extension of $\mathrm{PSL}_2(\mathbb{F}_7)$ by H. If the order of H is greater than 2, then G has a nontrivial abelian quotient, whereas if H is of order 2, then G is isomorphic to $C_2 \times \mathrm{PSL}_2(\mathbb{F}_7)$ or $\mathrm{SL}_2(\mathbb{F}_7)$.*

Proof. By the above lemma, $H^2(\mathrm{PSL}_2(\mathbb{F}_7), \mu_{2^n}) \simeq C_2$ for all $n \geq 1$. It follows that the unique nontrivial extension of $\mathrm{PSL}_2(\mathbb{F}_7)$ by μ_{2^n} is given by the quotient of $\mu_{2^n} \times \mathrm{SL}_2(\mathbb{F}_7)$ and the subgroup generated by $\langle -1, -I \rangle$, where I is the identity matrix in $\mathrm{SL}_2(\mathbb{F}_7)$. Thus, G is isomorphic to $C_2 \times \mathrm{PSL}_2(\mathbb{F}_7)$ or $\mathrm{SL}_2(\mathbb{F}_7)$, when H is C_2.

We now write H as a sum of copies of cyclic groups of the form μ_{2^n}. By the above calculation, $H^2(\mathrm{PSL}_2(\mathbb{F}_7), H)$ is a sum of copies of C_2, indexed by the summands of H. All extension classes in $H^2(\mathrm{PSL}_2(\mathbb{F}_7), H)$ can be obtained using G. These are either $H \times \mathrm{PSL}_2(\mathbb{F}_7)$ (giving the trivial extension class), or the quotient of $H \times \mathrm{SL}_2(\mathbb{F}_7)$ and a central group of order 2 generated by $\langle h, -I\rangle$ for some nontrivial element $h \in H$. It follows that if G is not isomorphic to $H \times \mathrm{PSL}_2(\mathbb{F}_7)$, then there exists a normal subgroup of G that is isomorphic to $\mathrm{SL}_2(\mathbb{F}_7)$, and the quotient of G by this subgroup is abelian and of order $|H|/2$. ∎

3.2. Noncentral extensions of $\mathrm{PSL}_2(\mathbb{F}_7)$ by $(C_2)^3$. In the previous section, we considered the central extension of $\mathrm{PSL}_2(\mathbb{F}_7)$. Here, we will study the case of noncentral extensions. Let G be the noncentral group extension of $\mathrm{PSL}_2(\mathbb{F}_7)$ by $(C_2)^3$:

$$1 \to (C_2)^3 \to G \to \mathrm{PSL}_2(\mathbb{F}_7) \to 1.$$

First, let us consider the $\mathrm{PSL}_2(\mathbb{F}_7)$-action on $(C_2)^3$. Because $\mathrm{Aut}((C_2)^3) \simeq \mathrm{GL}_3(\mathbb{F}_2)$ and $\mathrm{PSL}_2(\mathbb{F}_7) \simeq \mathrm{GL}_3(\mathbb{F}_2)$, the nontrivial action of $\mathrm{PSL}_2(\mathbb{F}_7)$ on $(C_2)^3$ is uniquely determined by the isomorphism

$$\mathrm{PSL}_2(\mathbb{F}_7) \simeq \mathrm{GL}_3(\mathbb{F}_2).$$

By using Magma we can check that there are only two possibilities for G. One is the nonsplit extension of $(C_2)^3$ with $\mathrm{PSL}_2(\mathbb{F}_7) \simeq \mathrm{GL}_3(\mathbb{F}_2)$, and the other is the split extension. (Jürgen Klüners and Gunter Malle [5] denoted these as $14T33$ and $14T34$.) Here, 'nTr' denotes the rth transitive subgroup of S_n.)

Proposition 3.3. *Let G be the group extension of $\mathrm{PSL}_2(\mathbb{F}_7)$ by $(C_2)^3$:*

$$1 \to (C_2)^3 \to G \to \mathrm{PSL}_2(\mathbb{F}_7) \to 1.$$

If G does not act trivially on $(C_2)^3$, then G is isomorphic to either $14T33$ or $14T34$.

3.3. Structures of $14T33$ and $14T34$. We will now study some properties of subgroups of $14T33$ and $14T34$. For this, we will require computer calculations. These have been performed using Magma and a standard home computer.

Lemma 3.4. $\mathrm{PSL}_2(\mathbb{F}_7)$ *admits two different conjugacy classes of subgroups of order* 24.

Proof. $\mathrm{PSL}_2(\mathbb{F}_7)$ is isomorphic to a subgroup of S_8, and can be expressed as follows:

$$\mathrm{PSL}_2(\mathbb{F}_7) \simeq \langle (1,5,8,4,2,7,3), (1,6,8,7,3,4,2)\rangle$$

(see [6]). Using Magma, we can check that $\mathrm{PSL}_2(\mathbb{F}_7)$ admits the following two different conjugacy classes of subgroups of order 24:

$\langle (1,4)(2,8)(3,5)(6,7), (1,2,6)(4,8,5), (1,3)(2,6)(4,7)(5,8), (1,2)(3,6)(4,8)(5,7)\rangle$,
$\langle (1,5)(2,6)(3,4)(7,8), (1,8,3)(2,4,5), (1,8)(2,5)(3,6)(4,7), (1,3)(2,7)(4,5)(6,8)\rangle$. ∎

LEMMA 3.5. $14T33$ (*resp.* $14T34$) *has two conjugacy classes of subgroups of order* 192. *The orders of the derived groups of these subgroups are* 48 *and* 96.

Proof. From [6], $14T33$ is generated by

$(1,6,4,5,10,14,9)(2,8,13,11,12,3,7)$ and $(1,7,8,14)(2,11,12,6,9,4,5,13)$.

Then we can deduce the stated result by using a Magma program. In the case of $14T34$, we get the result in the same manner. ∎

3.4. Schur–Zassenhaus theorem

THEOREM 3.6 (Schur–Zassenhaus). *If G is a finite group and N is a normal subgroup whose order is coprime to the order of the quotient group G/N, then G is a semidirect product of N and G/N.*

3.5. Group extensions of groups with trivial centers. Let H and F be groups, and G a group extension of H by F:

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

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

LEMMA 3.7 ([10, (7.11)]). *Suppose H has trivial center ($Z(H) = \{1\}$). Then the structure of G is uniquely determined by the homomorphism ψ_G. For any group homomorphism $\psi : F \to \operatorname{Out} H$, 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 $\psi(F) = 1$.) Each extension is realized as a subgroup U of the direct product $F \times \operatorname{Aut} H$ satisfying the two conditions $U \cap \operatorname{Aut} H = \operatorname{Inn} H$ and $\pi(U) = F$, where π is the projection from $F \times \operatorname{Aut} H$ to F.*

From this result, we immediately obtain the following:

PROPOSITION 3.8. *Let H be a group with a trivial center.*

(i) *If H has a trivial outer automorphism group, then for any group F, any extension of H by F is the direct product $F \times H$.*
(ii) *If $\operatorname{Out} H \simeq C_2$, then for any group F with no quotient group of order two, any extension of H by F is the direct product $F \times H$. In particular, for any finite group F of odd order, any group extension of H by F is $F \times H$.*

DEFINITION 3.9. Let G, H be groups, and let $N \lhd G$ and $K \lhd H$. Let $G/N \cong H/K$ with $\theta : G/N \to H/K$ an isomorphism. The *pullback* $G \curlywedge H$ of G and H via θ is the subset of $G \times H$ consisting of elements of the form (g, h) with $\theta(gN) = hK$.

Let p be a prime number ≥ 5. Then $Z(\mathrm{PGL}_2(\mathbb{F}_p)) = Z(\mathrm{PSL}_2(\mathbb{F}_p)) = \{1\}$, $\mathrm{Out}\,\mathrm{PGL}_2(\mathbb{F}_p) = \{1\}$, and $\mathrm{Out}\,\mathrm{PSL}_2(\mathbb{F}_p) \cong C_2$. Therefore, we have the following results.

PROPOSITION 3.10. *Let p be a natural number with $p \geq 5$.*

(i) *For any group F, any extension of $\mathrm{PGL}_2(\mathbb{F}_p)$ by F is the direct product $F \times \mathrm{PGL}_2(\mathbb{F}_p)$.*
(ii) *For any group F without any quotient group of order two, any extension of $\mathrm{PSL}_2(\mathbb{F}_p)$ by F is the direct product $F \times \mathrm{PSL}_2(\mathbb{F}_p)$. Moreover, any extension of $\mathrm{PSL}_2(\mathbb{F}_p)$ by C_2 is isomorphic to $C_2 \times \mathrm{PSL}_2(\mathbb{F}_p)$ or $\mathrm{PGL}_2(\mathbb{F}_p)$. Furthermore, any extension of $\mathrm{PSL}_2(\mathbb{F}_p)$ by C_{2^m} is isomorphic to $C_{2^m} \times \mathrm{PSL}_2(\mathbb{F}_p)$ or $C_{2^m} \curlywedge \mathrm{PGL}_2(\mathbb{F}_p)$.*

4. $\mathrm{PSL}_2(\mathbb{F}_7)$-unramified extension of a quartic field. From this section on, we will assume that the GHR holds, in order to obtain a better discriminant bound, as explained in Section 2.1. Let $K' = \mathbb{Q}(\sqrt{1417})$. We can check that the narrow class number of K' is 2. Let K be the narrow Hilbert class field of K'. The narrow class number of K is 1, i.e., K admits no nontrivial solvable unramified extensions.

4.1. Example. Let L be the splitting field of

$$x^8 + x^7 + 11x^6 - 37x^5 + 10x^4 + 28x^3 - 12x^2 - 3x + 4, \tag{4.1}$$

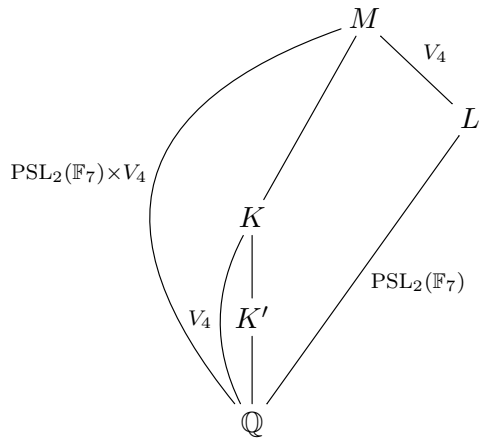
which is a polynomial with complex roots. We can find the polynomial (4.1) in the database of [5]. Its discriminant is $13^4 \cdot 109^4 = 1417^4$, and its factorizations modulo 13 and 109 are

$$(x^2 + 8x + 10)^2(x^2 + 12x + 5)^2 \bmod 13,$$
$$(x^2 + 12x + 86)^2(x^2 + 43x + 71)^2 \bmod 109.$$

Thus, L is a $\mathrm{PSL}_2(\mathbb{F}_7)$-extension of $\mathbb{Q}$ with ramification index 2 at both 13 and 109.

By Abhyankar's Lemma, LK/K is unramified over all finite spaces. Because $\mathrm{PSL}_2(\mathbb{F}_7)$ is a nonabelian simple group, we know that $L \cap K = \mathbb{Q}$. Hence, $\mathrm{Gal}(LK/K) \simeq \mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$. That is, LK is an unramified $\mathrm{PSL}_2(\mathbb{F}_7)$-extension of K over all finite spaces.

4.2. Bound of $[K_{\mathrm{ur}}^f : K]$. Define M to be LK.

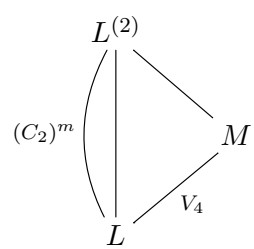


Because M/K is unramified over all finite primes, the root discriminant of M is $|d_M|^{1/n_M} = |d_K|^{1/n_K} = \sqrt{1417} = 37.643\ldots$. If we assume that the GRH holds, then $|d_M|^{1/n_M} = |d_K|^{1/n_K} = \sqrt{1417} = 37.643\ldots < 37.994\ldots = B(100000, 0, 50000)$ (see the table in [7]). This implies that $[K_{\mathrm{ur}}^f : M] < 100000/[M : \mathbb{Q}] = 148.809\ldots$.

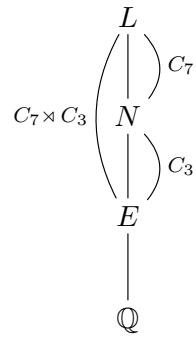
5. Class number of M. In this section, we will show that the class number of M is 1 under the assumption of the GRH. The first step is to show that the Hilbert 2-class field of L is M.

5.1. The 2-class group of L

5.1.1. *The elementary 2-class group of L.* Let $L^{(2)}$ be the maximal elementary abelian 2-class tower of L, i.e., $L^{(2)}/L$ is unramified and $\mathrm{Gal}(L^{(2)}/L) \simeq (C_2)^m$. By maximality, $L^{(2)}$ is also Galois over $\mathbb{Q}$. Because $[K_{\mathrm{ur}}^f : L] < 595.236\ldots$, we see that $m < 10$. Because M/L is unramified and $\mathrm{Gal}(M/L) \simeq V_4$, M is contained in $L^{(2)}$, i.e., $2 \le m \le 9$.



Let E be the octic number field defined by (4.1), and let N be the subfield of L fixed by a subgroup of $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{PSL}_2(\mathbb{F}_7)$ of order 7 that contains E.

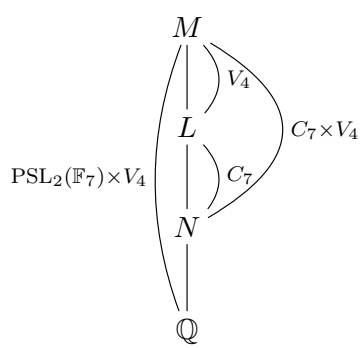


Because the discriminant of E is $13^4 \cdot 109^4$, $L/N/E$ is unramified over all finite spaces.

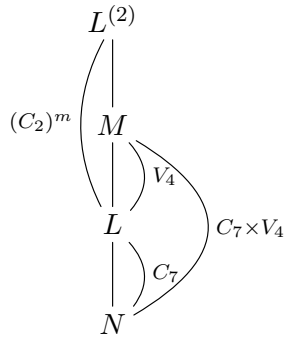
Using a computer calculation, we can check that N is defined by the following polynomial:

$$
\begin{aligned}
(5.1)\quad & x^{24} + 66x^{23} + 1514x^{22} + 13022x^{21} + 78158x^{20} + 2229546x^{19} \\
& + 17039958x^{18} - 114205156x^{17} + 1261675830x^{16} + 14442723470x^{15} \\
& - 206451271654x^{14} + 1601200893156x^{13} + 3183161315040x^{12} \\
& - 152141710405042x^{11} + 1772054344788451x^{10} - 11494744590768912x^{9} \\
& + 48852129137635664x^{8} - 91837569177842648x^{7} - 223335273618107650x^{6} \\
& + 244128682930806590 2x^{5} - 75357392100203430 32x^{4} \\
& + 71729687180320644 64x^{3} + 35762510379590386933x^{2} \\
& - 12890498836786052646 0x + 155328675599907155475.
\end{aligned}
$$

Using another computer calculation, we can check that the narrow class group of N is isomorphic to $C_7 \times V_4$ under the GRH. In other words, the narrow 2-class group of N is isomorphic to $V_4 \simeq (C_2)^2$.



Now let consider the action of $\mathrm{Gal}(L/N)$ on $\mathrm{Gal}(L^{(2)}/L) \simeq (C_2)^m$.



The action of $\mathrm{Gal}(L/N)$ on $\mathrm{Gal}(L^{(2)}/L) \simeq (C_2)^m$ can be thought of as the $\mathbb{F}_2$-representation of C_7. For $3 \leq m \leq 4$, we can easily see that $\mathrm{Gal}(L/N)$ acts trivially on $\mathrm{Gal}(L^{(2)}/L)$. (See Section 2.2.) In these cases, $\mathrm{Gal}(L^{(2)}/N)$ is isomorphic to $(C_2)^m \times C_7$ by Theorem 3.6. This contradicts the assumption that the narrow 2-class group of N is isomorphic to $(C_2)^2$. Similarly, for $m = 6, 7$ and 9, we arrive at the same conclusion (see Section 2.2.2). Thus, the remaining cases are $m = 5$ and $m = 8$. In these cases, $\mathrm{Gal}(L/N)$ $(\simeq C_7)$ nontrivially acts on $\mathrm{Gal}(L^{(2)}/M) \simeq (C_2)^{m-2}$ (see Section 2.2.3).

Case 1: $m = 5$. Then $\mathrm{Gal}(L^{(2)}/M) \simeq (C_2)^3$. The group $\mathrm{Gal}(L^{(2)}/K)$ is an extension of $\mathrm{Gal}(M/K)$ $(\simeq \mathrm{PSL}_2(\mathbb{F}_7))$ by $\mathrm{Gal}(L^{(2)}/M)$ $(\simeq (C_2)^3)$.

If $\mathrm{Gal}(M/K)$ acts trivially on $\mathrm{Gal}(L^{(2)}/M)$, then $\mathrm{Gal}(L^{(2)}/K)$ admits an abelian quotient by Proposition 3.2, which contradicts $|\mathrm{Cl}(K)| = 1$. Therefore, $\mathrm{Gal}(M/K)$ must act nontrivially on $\mathrm{Gal}(L^{(2)}/M)$. In conclusion, $\mathrm{Gal}(L^{(2)}/K)$ is isomorphic to $14T33$ or $14T34$. Suppose that $\mathrm{Gal}(L^{(2)}/K)$ is isomorphic to $14T33$.

By Lemma 3.4, L has two distinct nonisomorphic subfields of degree 7, and we check that these correspond to

$$x^7 - x^6 - 3x^5 + x^4 + 4x^3 - x^2 - x + 1 \tag{5.2}$$

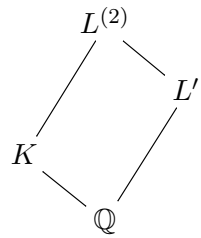
and

$$x^7 - 2x^6 - x^5 + 4x^4 - 3x^2 - x + 1 \tag{5.3}$$

(see [5]). Let E_1 (resp. E_2) be the number field defined by (5.2) (resp. the polynomial (5.3)). Let us consider the composite fields KE_1 and KE_2. By Lemma 3.5, two distinct nonisomorphic subfields of $L^{(2)}/K$ of degree 7 are KE_1/K and KE_2/K. Using computer calculations, we find that the narrow class group of KE_1 (resp. KE_2) is C_2 under the GRH. This contradicts Lemma 3.5, which states that one of these class groups should be of order 4.

Case 2: $m = 8$. In this case, $\mathrm{Gal}(L^{(2)}/M) \simeq (C_2)^6$. $L^{(2)}$ can be thought of as the composite of K and L' whose Galois group $\mathrm{Gal}(L'/\mathbb{Q})$ is an exten-

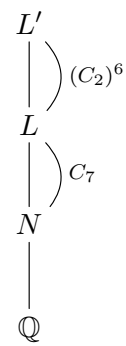
sion of $\mathrm{Gal}(L/\mathbb{Q})$ ($\simeq \mathrm{PSL}_2(\mathbb{F}_7)$) by $(C_2)^6$.



Let $\bar{\mathfrak{p}}$ (resp. $\mathfrak{p}$) be a prime ideal in L' (resp. L) satisfying $\bar{\mathfrak{p}} \mid 2$ (resp. $\mathfrak{p} \mid 2$). The factorization of the polynomial (4.1) modulo 2 is given by

$$x^8 + x^7 + 11x^6 - 37x^5 + 10x^4 + 28x^3 - 12x^2 - 3x + 4 \equiv x(x^7 + x^6 + x^5 + x^4 + 1) \bmod 2. \tag{5.4}$$

Thus, $\mathrm{Gal}(L_{\mathfrak{p}}/\mathbb{Q}_2)$ is isomorphic to C_7, where $L_{\mathfrak{p}}$ is the $\mathfrak{p}$-completion of L. Because L'/L is unramified, $\mathrm{Gal}(L'_{\bar{\mathfrak{p}}}/L_{\mathfrak{p}})$ is either trivial or C_2.



Because 2 is unramified in $L'/\mathbb{Q}$, $L'_{\bar{\mathfrak{p}}}/\mathbb{Q}_2$ should be a cyclic extension. Because the narrow class group of N is $C_7 \times V_4$, there exists no proper subgroup of $\mathrm{Gal}(L'/L)$ that is invariant under the action of the subgroup of order 7 (see Section 2.2.3). Thus, $\mathrm{Gal}(L'_{\bar{\mathfrak{p}}}/L_{\mathfrak{p}})$ is trivial, i.e., $\mathfrak{p}$ splits completely in L'. Then, for a number field $L'/\mathbb{Q}$, we have $f_2 = 7$, where f_2 is the inertia degree of 2.

Let $\bar{\mathfrak{q}}$ (resp. $\mathfrak{q}$) be a prime ideal in L' (resp. L) satisfying $\bar{\mathfrak{q}} \mid 3$ (resp. $\mathfrak{q} \mid 3$). The factorization of the polynomial (4.1) modulo 3 is given by

$$x^8 + x^7 + 11x^6 - 37x^5 + 10x^4 + 28x^3 - 12x^2 - 3x + 4 \equiv (x+2)(x^7 + 2x^6 + x^5 + x^3 + 2x^2 + 2x + 2) \bmod 3. \tag{5.5}$$

By a similar argument, we also know that $f_3 = 7$.

Let us recall equation (2.3):

$$f = 2\sum_{\mathfrak{p}}\sum_{m=1}^{\infty}\frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^{m/2}}F(\log N(\mathfrak{p})^m). \tag{5.6}$$

Because every term of f is greater than or equal to 0, the following holds for the number field L':

(5.7)
$$f \geq 2\Bigg(\sum_{j=1}^{1536}\sum_{i=1}^{100}\frac{\log N(\bar{\mathfrak{p}}_j)}{N(\bar{\mathfrak{p}}_j)^{i/2}}F(\log N(\bar{\mathfrak{p}}_j)^i) + \sum_{j=1}^{1536}\sum_{i=1}^{100}\frac{\log N(\bar{\mathfrak{q}}_j)}{N(\bar{\mathfrak{q}}_j)^{i/2}}F(\log N(\bar{\mathfrak{q}}_j)^i)\Bigg),$$

where the $\bar{\mathfrak{p}}_j$ (resp. $\bar{\mathfrak{q}}_j$) denote prime ideals of L' satisfying $\bar{\mathfrak{p}}_j \mid 2$ (resp. $\bar{\mathfrak{q}}_j \mid 3$). Because $f_2 = f_3 = 7$, we have $N(\bar{\mathfrak{p}}_j) = 2^7$ and $N(\bar{\mathfrak{q}}_j) = 3^7$ for all j. We set $b = 9.8$. Using a numerical calculation, we find that

$$\begin{aligned} f &\geq 2\cdot 1536\sum_{i=1}^{100}\left(\frac{\log 2^7}{2^{7i/2}}F(\log 2^{7i}) + \frac{\log 3^7}{3^{7i/2}}F(\log 3^{7i})\right) \\ &= 1292.96\ldots. \end{aligned} \tag{5.8}$$

Let us recall (2.2). For $b = 9.8$, we have

$$\begin{aligned} |d_{L'}|^{1/n_{L'}} &> 38.067\cdot e^{(f-1244.2)/10752} \\ &\geq 38.067\cdot e^{(1292.96-1244.2)/10752} \\ &= 38.2400\ldots. \end{aligned} \tag{5.9}$$

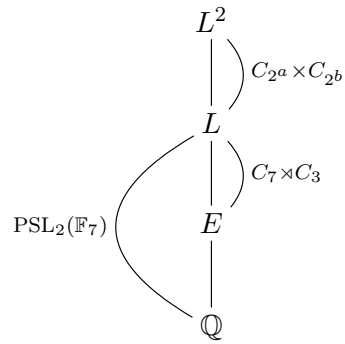
Because $|d_{L'}|^{1/n_{L'}} = |d_L|^{1/n_L} = \sqrt{1417}$, this contradicts the fact that $|d_{L'}|^{1/n_{L'}} = 37.643\ldots$.

In conclusion, $\mathrm{Gal}(L^{(2)}/L) \simeq (C_2)^2$, i.e., $L^{(2)} = M$.

5.1.2. *Determination of the 2-class group of L.* Let L^2 be the Hilbert 2-class field of L. Because $\mathrm{Gal}(L^{(2)}/L) \simeq (C_2)^2$, $\mathrm{Gal}(L^2/L)$ is an abelian 2-group with rank 2. By [2, Theorem 4.1], we know that $\mathrm{Aut}(\mathrm{Gal}(L^2/L))$ does not divide by 168, i.e., $\mathrm{Gal}(L/\mathbb{Q})$ acts trivially on $\mathrm{Gal}(L^2/L)$.

$$\begin{array}{c} L^2 \\ \Big| \big) C_{2^a}\times C_{2^b} \\ L \\ \Big| \big) \mathrm{PSL}_2(\mathbb{F}_7) \\ \mathbb{Q} \end{array}$$

Let us recall the octic number field E defined in (4.1):

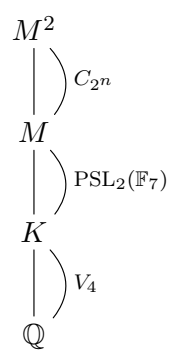


(Note that L^2/E is unramified over all finite spaces.) Because $\mathrm{Gal}(L/\mathbb{Q})$ acts trivially on $\mathrm{Gal}(L^2/L)$, so does $\mathrm{Gal}(L/E)$. By Theorem 3.6, $\mathrm{Gal}(L^2/E)$ is isomorphic to

$$\mathrm{Gal}(L^2/L) \times \mathrm{Gal}(L/E) \simeq (C_{2^a} \times C_{2^b}) \times C_7 \rtimes C_3,$$

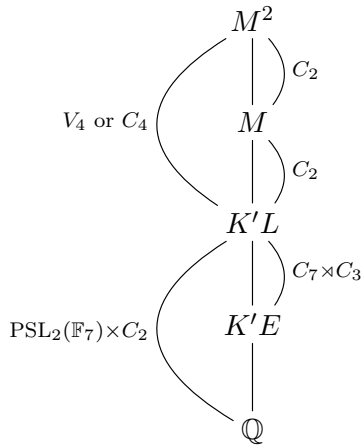
and its abelianization is given by $C_{2^a} \times C_{2^b} \times C_3$. We can check that the narrow class group of E is $C_6 \times C_2$ using computer calculations. Thus, $a = b = 1$, i.e., the 2-class group of L is V_4.

5.2. The 2-class group of M. Note that $M = L^2$. Let M^2 be the Hilbert 2-class field of M, and assume that M^2/M is a nontrivial extension. By Lemma 2.3, M^2/M is cyclic.



Because M^2/M is cyclic, we know that $\mathrm{Gal}(M/K)$ acts trivially on $\mathrm{Gal}(M^2/M)$. Because the narrow class number of K is one, $\mathrm{Gal}(M^2/K)$ does not admit any abelian quotients. Thus, $\mathrm{Gal}(M^2/M)$ should be C_2, by Proposition 3.2.

Let us recall $K' = \mathbb{Q}(\sqrt{1417})$, and consider $K'E$.



(Note that $M^2/K'E$ is unramified.) From computer calculations, we find that the narrow class group of $K'E$ is C_6. Using a similar argument to Section 5.1.2, the abelianization of $\mathrm{Gal}(M^2/K'E)$ is either $V_4 \times C_3$ or $C_4 \times C_3$. This is a contradiction.

In conclusion, the 2-class group of M is trivial.

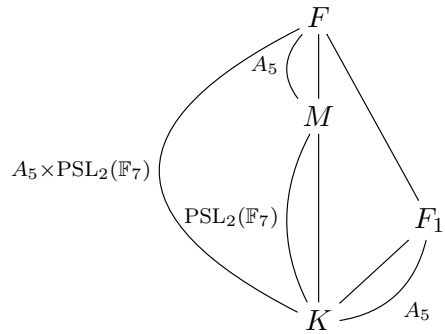
5.2.1. *The p-class group of M for an odd prime p.* Let $p = 3$, and let $M^{(3)}/M$ be the maximal elementary abelian 3-class tower of M. Then $\mathrm{Gal}(M^{(3)}/M) \simeq (C_3)^m$ with $1 \leq m \leq 4$. By [2, Theorem 4.1], $\mathrm{Aut}((C_3)^m)$ does not divide by 168 for $1 \leq m \leq 4$. This means that $\mathrm{Gal}(M^{(3)}/K)$ admits an abelian quotient, which contradicts the fact that the narrow class number of K is 1.

Using similar methods, we can verify that the p-class group of M is trivial for all odd prime p.

Proposition 5.1. *The class number of M is* 1*, under the assumption of the GRH.*

6. Determination of $\mathrm{Gal}(K_{\mathrm{ur}}^f/K)$**.** We have shown that the class number of M is 1 and $[K_{\mathrm{ur}}^f : M] < 168$ under the assumption of the GRH. Thus, 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. Since $[K_{\mathrm{ur}}^f : M] < 168$, F is the unique unramified A_5-extension of F, 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 Proposition 3.10, $\mathrm{Gal}(N/K) \simeq A_5 \times \mathrm{PSL}_2(\mathbb{F}_7)$, i.e., K admits an A_5-unramified extension F_1.



(Note that F_1 is also Galois over $\mathbb{Q}$.) Then, by Proposition 3.10, $\mathrm{Gal}(F_1/K')$ is isomorphic to either $A_5 \times C_2$ or S_5.

Case 1: $\mathrm{Gal}(F_1/K') \simeq A_5 \times C_2$. By a similar argument to 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 with ramification index 2 at 13 and 109. However, from the tables in [1] no such extension exists.

Case 1.2: $\mathrm{Gal}(N_2/\mathbb{Q}) \simeq S_5$. By the unramifiedness of F_2/K', a quintic subfield E of F_2 must have discriminant 1417. However, the smallest discriminant of quintic fields with Galois group S_5 is 1609, a contradiction.

Case 2: $\mathrm{Gal}(F_1/K') \simeq S_5$. By Proposition 3.10, $\mathrm{Gal}(F_1/\mathbb{Q}) \simeq S_5 \times C_2$. Consequently, F_1 is the compositum of K' and an S_5-extension F_2 of $\mathbb{Q}$. For F_1/K' to be unramified, the quintic subfield of $F_2/\mathbb{Q}$ must have discriminant 13, 109, $13 \cdot 109^2$, or $13^2 \cdot 109$. Such a quintic number field does not exist, from [9].

In conclusion, M admits no unramified A_5-extensions, i.e., $\mathrm{Gal}(K^f_{\mathrm{ur}}/K) \cong \mathrm{PSL}_2(\mathbb{F}_7)$ under the assumption that the GRH holds.

References

[1] J. Basmaji and I. Kiming, *A table of A_5-fields*, in: On Artin's Conjecture for odd 2-Dimensional Representations, Lecture Notes in Math. 1585, Springer, Berlin, 1994, 37–46, 122–141.

[2] C. J. Hillar and D. L. Rhea, *Automorphisms of finite abelian groups*, Amer. Math. Monthly 114 (2007), 917–923.

[3] K. Kim, *A construction of nonabelian simple étale fundamental groups*, Ramanujan J. 35 (2014), 111–120.

[4] K. Kim, *A construction of nonabelian simple étale fundamental groups II*, Ramanujan J. 39 (2016), 49–59.

[5] J. Klüners and G. Malle, http://galoisdb.math.upb.de/home.

[6] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, Home page of Galois groups http://www.lmfdb.org/GaloisGroup/, 2013 [online; accessed 16 September 2013].
[7] J. Martinet, *Petits discriminants des corps de nombres*, in: Number Theory Days, 1980 (Exeter, 1980), London Math. Soc. Lecture Note Ser. 56, Cambridge Univ. Press, Cambridge, New York, 1982, 151–193.
[8] J. Neukirch, *Algebraic Number Theory*, Grundlehren Math. Wiss. 322, Springer, Berlin, 1999.
[9] A. Schwarz, M. Pohst, and F. Diaz Y. Diaz, *A table of quintic number fields*, Math. Comp. 63 (1994), 361–376.
[10] M. Suzuki, *Group Theory. I*, Grundlehren Math. Wiss. 247, Springer, Berlin, 1982.
[11] O. Taussky, *A remark on the class field tower*, J. London Math. Soc. 12 (1937), 82–85.
[12] L. C. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer, New York, 1982.
[13] R. A. Wilson, *The Finite Simple Groups*, Grad. Texts in Math. 251, Springer London, London, 2009.
[14] K. Yamamura, *Maximal unramified extensions of imaginary quadratic number fields of small conductors*, J. Théor. Nombres Bordeaux 9 (1997), 405–448.

Kwang-Seob Kim
School of Mathematics
Korea Institute for Advanced Study
Seoul 130-722, Korea
E-mail: kwang12@kias.re.kr