Siman Wong

The maximal unramified extensions of certain complex Abelian number fields

2015, p. 93-104.

<http://pmb.cedram.org/item?id=PMB_2015____93_0>
THE MAXIMAL UNRAMIFIED EXTENSIONS OF CERTAIN COMPLEX ABELIAN NUMBER FIELDS

by

Siman Wong

Abstract. — We combine root discriminant bounds with a ramification argument to show unconditionally that $\mathbb{Q}(\sqrt{-7}, \sqrt{61})$ has no nontrivial unramified extension, a result first proved by Yamamura under the generalized Riemann hypothesis (GRH). This renders unconditional his determination of the maximal unramified extensions of the complex quadratic fields with class number 2. Assuming the GRH, we prove an analogous result for the degree 14 subfield of the cyclotomic field $\mathbb{Q}(\zeta_{49})$, a case previously not handled by conditional root discriminant bounds alone.

Résumé. — Nous combinons les minorations des discriminants avec des considérations portant sur la ramification pour montrer, inconditionnellement, que le corps $\mathbb{Q}(\sqrt{-7}, \sqrt{61})$ n'a pas d'extension non-ramifiée non-triviale (ce résultat a été montré par Yamamura avec l'aide de GRH). Cela rend inconditionnelle la détermination des extensions non-ramifiées maximales des corps quadratiques complexes de nombre de classes 2. Sous GRH, nous montrons un résultat analogue pour le sous-corps de degré 14 de $\mathbb{Q}(\zeta_{49})$ (corps non étudié même sous GRH).

1. Introduction

There are many examples of real quadratic fields with class number one that admit non-trivial extensions unramified at all finite places (for examples and discussion see [8, p.121], [16], [19], [22]), but we have no analogous example of complex Abelian number fields with class number one [17, p. 914ff]. Yamamura [17] shows that there are 172 complex Abelian number fields with class number one. Using the unconditional Odlyzko bound of root discriminants [10], we find that 132 of these fields $K$ are unramified-closed, i.e. $K = K^{ur}$, the maximal unramified extension of $K$. The stronger form of the Odlyzko bound under the generalized Riemann hypothesis for zeta functions of number fields (GRH) shows that an additional 23 of these 172 fields are also unramified-closed. Combining root discriminant bounds with the theory of group extensions, Yamamura [21] has since verified unconditionally that five additional


Key words and phrases. — Abelian fields, group extensions, root discriminants, unramified extensions.

Acknowledgements. — Siman Wong’s work is supported in part by NSF grant DMS-0901506.
complex Abelian fields are unramified-closed (and two more under GRH). In this paper we augment this approach with a ramification argument to study $K^{ur}$ for two additional cases.

**Theorem 1.** — (a) Unconditionally the complex Abelian number field $\mathbb{Q}(\sqrt{-7}, \sqrt{61})$ is unramified-closed.
(b) Assume the generalized Riemann hypothesis for the zeta functions of number fields. Then the degree 14 subfield of the cyclotomic field $\mathbb{Q}(\zeta_{49})$ is unramified closed.

Note that $\mathbb{Q}(\sqrt{-7}, \sqrt{61})$ is the Hilbert class field of $\mathbb{Q}(\sqrt{-427})$. By [9], there are 18 complex quadratic fields $\mathbb{Q}(\sqrt{-d})$ with class number 2; specifically


In a later work, Yamamura [18] shows that except for $-d = 115, 235, 403$ and 427, the Hilbert class field $H_{-d}$ of these quadratic fields (which turn out to be the genus fields) are unramified closed, and that for each of $-d = 115, 235$ and 403, the second Hilbert class field of $\mathbb{Q}(\sqrt{-d})$ (i.e. the Hilbert class fields of $H_{-d}$) is unramified closed. Finally, using the GRH form of the Odlyzko bound, he shows that $H_{-427}$ is unramified-closed. Thanks to theorem 1 we can now remove this GRH condition.

**Theorem 2.** — The Hilbert class field of $\mathbb{Q}(\sqrt{-427})$ has no nontrivial unramified extension, whence the maximal unramified extensions of imaginary quadratic fields of class number 2 as determined by Yamamura are valid unconditionally.

We now give an outline of the proof. Thanks to the unconditional Odlyzko bound, $[K^{ur} : K]$ is finite for $\mathbb{Q}(\sqrt{-7}, \sqrt{61})$; the same is true for the field in theorem 1(b) under GRH, thanks to the conditional Odlyzko bound. Suppose $K^{ur} \neq K$. Since $K$ has class number one and is complex, $\text{Gal}(K^{ur}/K)$ must admit a *simple* quotient. From the root discriminant of $K$ we find that $\text{Gal}(K^{ur}/K)$ is either $A_5$ or $\text{PSL}_2(\mathbb{F}_7)$. Using the theory of group extensions and explicit knowledge of the groups $\text{Gal}(K^{ur}/K)$ and $\text{Gal}(K/\mathbb{Q})$, we deduce from the hypothesis $K^{ur} \neq K$ the existence of a subfield $k/\mathbb{Q}$ of degree $\leq 8$ and with known Galois closure. For the two fields in Theorem 1, careful analysis of their ramification data leads to a sharp bound of $|\text{Disc}(k/\mathbb{Q})|$. For the degree 14 field, the bound is sharp enough that we can rule out the existence of $k/\mathbb{Q}$ by looking up tables of number fields [7]. For $\mathbb{Q}(\sqrt{-7}, \sqrt{61})$, we are led to a hypothetical field $k$ of degree 8 and of discriminant $\pm 7^4 61^4 \sim \pm 3.3 \times 10^{10}$, which lies outside the range of [7]. To eliminate this remaining case we combine our construction with an argument of Roberts [13].

There are four more fields in [17] which are known to be unramified closed only under GRH, and 17 more which are not known to be unramified closed even conditionally. To handle these fields requires new ideas; see Section 6 for details.

### 2. Preliminaries on group theory

In this section we recall the basic theory of group extensions and perform a calculation for later use. For more details, see [14, Chap. 11].

For any integer $n > 0$, denote by $C_n$ the cyclic group of order $n$. For any positive integers $n_1, \ldots, n_k$, set $C_{n_1, \ldots, n_k} := C_{n_1} \times \cdots \times C_{n_k}$. All groups will be written multiplicatively. In
such that $1 \rightarrow N \rightarrow E \rightarrow H \rightarrow 1$.

A computation using the theory of group extensions and outer automorphisms of finite simple groups yields the following result [18, Prop. 2, Prop. 3].

**Proposition 1 (Yamamura).** — (a) For each of the following pairs of groups $N, H$, the isomorphism classes of groups $G$ which are extensions of $N$ by $H$ are as follows:

<table>
<thead>
<tr>
<th>$N = A_5$</th>
<th>$N = PSL_2(\mathbb{F}_7)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$H$</td>
<td>$C_{2,2}$</td>
</tr>
<tr>
<td></td>
<td>$A_5 \times C_{2,2}$</td>
</tr>
<tr>
<td>$G$</td>
<td>$A_5 \times C_7$</td>
</tr>
<tr>
<td></td>
<td>$S_5 \times C_2$</td>
</tr>
<tr>
<td></td>
<td>$S_5 \times C_7$</td>
</tr>
</tbody>
</table>

(b) With the notation as above,

- if $N \simeq A_5$ then $G$ always contains an index 5 subgroup;
- if $G \simeq PSL_2(\mathbb{F}_7) \times C_{2,2}$ or $PSL_2(\mathbb{F}_7) \times C_7$ then $G$ contains an index 7 subgroup;
- if $G \simeq PGL_2(\mathbb{F}_7) \times C_2$ or $PGL_2(\mathbb{F}_7) \times C_7$ then $G$ contains an index 8 subgroup.

The following elementary facts about $PGL_2(\mathbb{F}_7)$ will be needed later on.

**Lemma 1.** — (a) $PGL_2(\mathbb{F}_7)$ has two conjugacy classes of order 2 elements. One of the two classes is contained in $PSL_2(\mathbb{F}_7)$. The other class is disjoint from $PSL_2(\mathbb{F}_7)$, has size 28, and the normalizer of any one of them is conjugate to

$$H := \langle (0 \ 1), (0 \ 1) \rangle \subset PGL_2(\mathbb{F}_7).$$

(b) $PGL_2(\mathbb{F}_7)$ has 28 $C_6$ subgroups. They are pairwise conjugate.

(c) Let $B \subset PGL_2(\mathbb{F}_7)$ be the projective image of a Borel subgroup. For any $C_6$ subgroup $S \subset PGL_2(\mathbb{F}_7)$, either $S \subset B$ or $S \cap B$ is trivial.

(d) $PGL_2(\mathbb{F}_7)$ has 42 $C_{2,2}$ subgroups not contained in $PSL_2(\mathbb{F}_7)$; they are pairwise conjugate. Every order 2 element in $PGL_2(\mathbb{F}_7) - PSL_2(\mathbb{F}_7)$ is contained in three $C_{2,2}$ subgroups.

**Proof.** — (a) Every order 2 element in $PGL_2(\mathbb{F}_7)$ is represented by a matrix $m \in GL_2(\mathbb{F}_7)$ such that $m^2 = \pm I$. So the possible choices for eigenvalues of $m$ are $\pm 1, \pm \sqrt{-1} \in \mathbb{F}_{7^2}$. Since $m$ is not a scalar matrix and $\sqrt{-1} \notin \mathbb{F}_7$, the characteristic polynomial of $m$ (necessarily $\mathbb{F}_7$-rational) must be one of $x^2 \pm 1$. Both cases occur: Consider for example the matrices $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $\gamma := \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Thus we get two $PGL_2(\mathbb{F}_7)$-conjugacy classes of order 2 elements, one of which is in $PSL_2(\mathbb{F}_7)$ and the other one is disjoint from $PSL_2(\mathbb{F}_7)$. The latter contains the projective image of $\gamma$ which as a matrix in $GL_2(\mathbb{F}_7)$ is contained in a split Cartan subgroup. So the $PGL_2(\mathbb{F}_7)$-normalizer of $\gamma$ is (2) above (cf. [15, prop. 17]). Since $\#H = 12$, the $PGL_2(\mathbb{F}_7)$-class of $\gamma$ has size 336/12 = 28.

(b) The $C_6$ subgroups of $PGL_2(\mathbb{F}_7)$ are projective image of split Cartan subgroups. Thus they are pairwise conjugate, and the number of such subgroups is equal to the number of unordered pairs of distinct lines through the origin of a 2-dimensional $\mathbb{F}_7$-vector space. There are 8 such lines, so there are $8 \cdot (8 - 1)/2 = 28$ such unordered pairs.
(c) Let $S'$ be a non-trivial subgroup of a $C_6$ subgroup $S \subset PGL_2(F_7)$. Then $S'$ is the projective image of a non-trivial, non-cyclic subgroup $\bar{S}'$ of a split Cartan subgroup $\bar{S} \subset GL_2(F_7)$ (whose projective image is $S$). Now, $\bar{S}$ corresponds to a unique, unordered pair of distinct lines $\{\ell_1, \ell_2\}$ of $F_7^2$ (and two $\bar{S}$ correspond to the same unordered pair if and only if both subgroups are contained in the same (maximal) split Cartan subgroup). Since $\bar{S}'$ is not cyclic, with respect to the ordered basis $\{\ell_1, \ell_2\}$ the only Borel subgroups $\bar{B} \subset GL_2(F_7)$ that contain $\bar{S}'$ are $\langle (\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}) \rangle$ and $\langle (\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}) \rangle$, in which case $\bar{S} \subset \bar{B}$ as well, whence $S \subset B$.

(d) Let $T$ be a $C_{2,2}$ subgroup of $PGL_2(F_7)$ not contained in $PSL_2(F_7)$. By part (a), $T$ contains a conjugate of $\gamma = (\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix})$, and hence $T$ is conjugate to a $C_{2,2}$ subgroup of the centralizer of $\gamma$. Since $\gamma$ has order 2, this centralizer is in fact the normalizer of $\gamma$. We readily check that (2) contains the following three $C_{2,2}$ subgroups:

$$(3) \quad \{ (\begin{smallmatrix} \pm 1 & 0 \\ 0 & 1 \end{smallmatrix}) , (\begin{smallmatrix} 0 & \pm 1 \\ 1 & 0 \end{smallmatrix}) \} ; \quad \{ (\begin{smallmatrix} \pm 1 & 0 \\ 0 & 1 \end{smallmatrix}) , (\begin{smallmatrix} 0 & \pm 2 \\ 1 & 0 \end{smallmatrix}) \} ; \quad \{ (\begin{smallmatrix} \pm 1 & 0 \\ 0 & 1 \end{smallmatrix}) , (\begin{smallmatrix} 0 & \pm 4 \\ 1 & 0 \end{smallmatrix}) \} .$$

So every order 2 element in $PGL_2(F_7) - PSL_2(F_7)$ is contained in three $C_{2,2}$ subgroups.

Finally, from the description (3) we see that the $C_{2,2}$ subgroups not in $PSL_2(F_7)$ are the projective image of a split Cartan subgroup, and hence they are pairwise conjugate. $\square$

### 3. Proof of the theorem: Basic setup

Let $K$ be one of the fields in Theorem 1. Denote by $K^{ur}$ the maximal unramified extension of $K$. In the table below we list the root discriminant of $K$, as well as an upper bound of the degree of $K^{ur}/Q$ furnished by the unconditional (resp. conditional) Odlyzko bound ([4, §2.2]; [10]). For odd $m$ and for $n|\varphi(m)$, denote by $L_m^n$ the degree $n$ subfield of $Q(\zeta_m)$, so $L_m^n$ is the degree 14 subfield of $Q(\zeta_{49})$.

<table>
<thead>
<tr>
<th>$K$</th>
<th>Gal($K/Q$)</th>
<th>root discriminant</th>
<th>$[K^{ur}:Q]$</th>
<th>$[K^{ur}:K]$</th>
<th>Odlyzko bound</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Q(\sqrt{-7}, \sqrt{61})$</td>
<td>$C_{2,2}$</td>
<td>$\sqrt{7} \cdot 61 = 20.664$</td>
<td>$&lt; 786$</td>
<td>$&lt; 196$</td>
<td>unconditional</td>
</tr>
<tr>
<td>$L_m^{49}$</td>
<td>$C_{14}$</td>
<td>$7^{25/14} = 32.293$</td>
<td>$&lt; 4800$</td>
<td>$&lt; 343$</td>
<td>conditional</td>
</tr>
</tbody>
</table>

By Galois theory, $Gal(K^{ur}/K)$ is an extension of $Gal(K^{ur}/K)$ by $Gal(K/Q)$. The next result puts restrictions on $Gal(K^{ur}/K)$ (cf. also [18, Prop. 2]).

**Lemma 2.** — Let $K$ be one of the fields in the table. Assume GRH if $K = L_m^{49}$.

(a) Let $K'/K$ be a non-Abelian, simple, unramified finite Galois extension. Then $K'/Q$ is Galois.

(b) Suppose the extensions $K'/K$ in part (a) do not exist. Then $K^{ur} = K$.

**Proof.** — (a) Suppose otherwise; denote by $M/Q$ the Galois closure of $K'/Q$. The simplicity of $Gal(K'/K)$ then implies that the intersection of any two conjugates of $K'/Q$ is exactly $K$, so $[M:Q] \geq [K':K][K:Q]$. But $M$ is the compositum of all conjugates of $K'/Q$ and $K'/K$ is unramified, so $M/K$ is also unramified. Thus $M$ has the same root discriminant as
Let \( K \) be one of the Abelian number fields in the table above, so \([K^\text{ur} : K] < 343\). So if \( K^\text{ur} \neq K \) then \( \text{Gal}(K^\text{ur}/K) \) is either \( A_5 \) or \( PSL_2(\mathbb{F}_7) \). Thanks to Proposition 1 and Lemma 2, we are reduced to study number fields \( k/\mathbb{Q} \) unramified outside the bad primes of \( K/\mathbb{Q} \), such that

\[
[k : \mathbb{Q}] = \begin{cases} 
5 & \text{if } [K^\text{ur} : K] = 60, \\
7 & \text{if } \text{Gal}(K^\text{ur}/\mathbb{Q}) \text{ contains a direct factor of } PSL_2(\mathbb{F}_7), \\
8 & \text{otherwise.}
\end{cases}
\]

Moreover, when \( [k : \mathbb{Q}] = 8 \) the Galois group of \( k/\mathbb{Q} \) is \( PGL_2(\mathbb{F}_7) \). In each case we exploit the arithmetic of \( K \) and the group theoretical properties of the Galois group of these hypothetical fields \( k \) to show that \( k \) cannot exist, and hence \( K \) must be unramified-closed.

### 4. The case of \( L_{49}^{14} \)

**Lemma 3.** — Let \( F/\mathbb{Q} \) be a degree 7 number field with Galois group \( PSL_2(\mathbb{F}_7) \). Then \( \text{Disc}(F/\mathbb{Q}) \) is a perfect square.

**Proof.** — By [3], \( S_7 \) contains a single conjugacy class of transitive subgroups isomorphic to \( PSL_2(\mathbb{F}_7) \). Furthermore, such subgroups are all contained in \( A_7 \). So if \( f \in \mathbb{Q}[x] \) is a septic polynomial with \( F \) as its splitting field, then \( \text{disc}(f) \) is a perfect square. Polynomial discriminant differs from the field discriminant by a square, so we are done. \( \square \)

For the rest of this section we will focus on the case \( K = L_{49}^{14} \). This \( C_{14} \) extension is totally ramified at 7 and is unramified at all other finite primes. Suppose \( K \neq K^\text{ur} \), and consider the associated extension \( k/\mathbb{Q} \) in (4) (furnished under GRH). If \( [k : \mathbb{Q}] = 5 \) then \( \text{Disc}(k/\mathbb{Q}) \) must divide \( 7^4 \). By the database of Jones and Roberts [7] (where the result is proven complete in this case), there is no such quintic field. Next, suppose \( [k : \mathbb{Q}] > 5 \) and that 7 is tamely ramified in \( k/\mathbb{Q} \). Then the ramification index of any prime of \( k \) lying above 7 is \( \leq 2 \), whence \( \text{Disc}(k/\mathbb{Q}) \) divides \( 7^4 \). Again this is not possible, thanks to [7].

Finally, suppose \( [k : \mathbb{Q}] = 7 \) or 8 and that 7 is wildly ramified. Then exactly one prime \( p \) in \( k/\mathbb{Q} \) lying above 7 ramifies, with ramification index 7. The completion \( k_p \) of \( k \) at \( p \) is contained in the completion of \( L_{49}^{14} \) at its unique prime above 7, so \( k_p/\mathbb{Q}_7 \) is a degree 7 Abelian extension with conductor \( 7^2 \). The conductor-discriminant formula then says that this Abelian degree 7 extension \( k_p/\mathbb{Q}_7 \) has discriminant \((7^2)^6\), and hence \( |\text{Disc}(k/\mathbb{Q})| = 7^{12} \). By the database of Jones and Roberts [7] (where the result is proven complete in this case), there is no such field of degree of 7. To handle the case where \( [k : \mathbb{Q}] = 8 \) we now give an argument applicable to the case \( [k : \mathbb{Q}] = 7 \) as well.

Denote by \( L/\mathbb{Q} \) the Galois closure of \( k/\mathbb{Q} \). Since \( \text{Gal}(L/\mathbb{Q}) \subset PGL_2(\mathbb{F}_7) \), that means \( \text{Gal}(L/\mathbb{Q}) \) has no order 14 element. Since \( k/\mathbb{Q} \) already has a prime with ramification index 7 and the inertia group of any ramified prime in \( K^\text{ur}/\mathbb{Q} \) is \( C_{14} \), the inertia group of any ramified prime in \( L/\mathbb{Q} \) is \( C_7 \). Since \( \mathbb{Q} \) has no non-trivial extension unramified at all finite places, the Galois group of any finite Galois extension of over \( \mathbb{Q} \) is generated by the inertia
groups of the extension. Since the order 7 subgroups of $\text{PSL}_2(\mathbb{F}_7)$ are transvections and they generate $\text{PSL}_2(\mathbb{F}_7)$, it follows that $\text{Gal}(L/\mathbb{Q}) \cong \text{PSL}_2(\mathbb{F}_7)$. Thus $[k : \mathbb{Q}] = 7$ and $L_{49}/L/k$ is unramified, whence the root discriminant of $L_{49}/L/\mathbb{Q}$ is $7^{12/7} = 28.102$. That is too small, by the GRH Odlyzko bound [11]. Thus $k/\mathbb{Q}$ does not exist, whence $K^{ur} = K$.

**Remark 1.** — Recall that in the outset we need to use the GRH Odlyzko bound to deduce that $[K^{ur} : K]$ is finite for $K = L_{49}$, so even if we replace the last line above with the database search as at the end of the previous paragraph, our argument for $K = L_{49}$ would still be conditional.

5. The case of $\mathbb{Q}(\sqrt{-7}, \sqrt{61})$

For the rest of this section we take $K = \mathbb{Q}(\sqrt{-7}, \sqrt{61})$. Suppose $K \neq K^{ur}$. Let $k/\mathbb{Q}$ be as in (4). Then $K^{ur}/K$ is unramified, and the ramification index of 7 or 61 in $K/\mathbb{Q}$ is 2. Consequently,

$$\tag{5} \text{the ramification index of each ramified prime in } k \text{ lying above } 7 \text{ or } 61 \text{ is } 2.$$  

When $[k : \mathbb{Q}] = 5$, by (5) we see that $k$ has either at most two ramified primes of residual degree 1 lying above $p$, or it has exactly one ramified prime of residual degree 2. Thus $\text{Disc}(k/\mathbb{Q})$ divides $7^261^2$. When $[k : \mathbb{Q}] = 7$, Lemma 3 plus (5) together imply that $\text{Disc}(k/\mathbb{Q})$ divides $7^261^2$ as well. There is no such quintic or septic field, by [7].

Finally, suppose $[k : \mathbb{Q}] = 8$. The argument above shows that $\text{Disc}(k/\mathbb{Q})$ divides $7^461^4$, which is too large for us to handle. By Proposition 1, $K^{ur}/\mathbb{Q}$ has Galois group $\text{PSL}_2(\mathbb{F}_7) \times C_2$. It has a unique $\text{PSL}_2(\mathbb{F}_7)$ subfield $L/\mathbb{Q}$ which is the Galois closure of $k/\mathbb{Q}$. To get a sharper estimate of $\text{Disc}(k/\mathbb{Q})$ we now analyze closely the ramification of $L/\mathbb{Q}$.

**Lemma 4.** — Let $p \subset \mathcal{O}_L$ be a prime lying above $p \in \{7, 61\}$.

(a) The inertia group $I(p)$ has order 2 and is not contained in $\text{PSL}_2(\mathbb{F}_7)$.

(b) The decomposition group $D(p)$ is isomorphic to one of $C_2, C_{2,2}$ or $C_6$.

**Proof.** — (a) Let $p \subset \mathcal{O}_L$ be a prime lying above $p \in \{7, 61\}$. Since $L \subset K^{ur}$ and $K^{ur}/K$ is unramified, so $\# I(p) = 2$. Inertia groups of conjugate primes are $\text{PSL}_2(\mathbb{F}_7)$-conjugate, so $I(p) \subset \text{PSL}_2(\mathbb{F}_7)$ if and only if $I(p') \subset \text{PSL}_2(\mathbb{F}_7)$ for every $p'$ lying above $p$. But $\text{Gal}(K^{ur}/K) \cong \text{PSL}_2(\mathbb{F}_7)$ and $\text{Gal}(K^{ur}/\mathbb{Q}) \cong \text{PSL}_2(\mathbb{F}_7)$, so if $I(p) \subset \text{PSL}_2(\mathbb{F}_7)$ then $p$ is unramified in $K/\mathbb{Q}$, a contradiction. Thus $I(p) \not\subset \text{PSL}_2(\mathbb{F}_7)$.

(b) $D(p)$ normalizes $I(p) \cong C_2$ and $I(p) \not\subset \text{PSL}_2(\mathbb{F}_7)$, so by Lemma 1(a), it is conjugate to a subgroup of $H := \langle (\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}), (\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}) \rangle \subset \text{PSL}_2(\mathbb{F}_7)$. In particular, $\# D(p) = 2m$ where $m = 1, 2, 3, \text{ or } 6$. Since $D(p)/I(p)$ is cyclic and $I(p) \cong C_2$, we see that $D(p)$ is one of the following subgroups of the order 12 dihedral group $H$:

<table>
<thead>
<tr>
<th>$m$</th>
<th>$D(p)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$C_2$</td>
</tr>
<tr>
<td>2</td>
<td>$C_{2,2}, C_4$</td>
</tr>
<tr>
<td>3</td>
<td>$C_6$</td>
</tr>
</tbody>
</table>

Since $I(p) \not\subset \text{PSL}_2(\mathbb{F}_7)$ and $\text{PSL}_2(\mathbb{F}_7) - \text{PSL}_2(\mathbb{F}_7)$ contains no order 4 element, we can rule out $C_4$. □
Lemma 5. — We have \( \text{Disc}(k/\mathbb{Q}) = \pm \tau^3 61^3 \).

Proof. — Let \( p \in \{7, 61\} \), and let \( p \subset \mathcal{O}_L \) be a prime lying above \( p \). Note that we can take \( \text{Gal}(L/k) \) to be the normalizer of \( \langle 1, 1 \rangle \) in \( PGL_2(\mathbb{F}_7) \), i.e. a projective Borel subgroup. Such a subgroup has at least one prime in \( \mathcal{O}_L \) but not all \( C_6 \) subgroups, so by Lemma 1(c), if \( D(p) \simeq C_6 \) then at least one prime in \( k \) lying above \( p \) has inertia degree 1 and ramification index 1, and at least one other prime in \( k \) has inertia degree 3 and ramification index 2. As \( [k : \mathbb{Q}] = 8 \), that means \( p \mathcal{O}_k = \mathcal{P}_0^2 \mathcal{P}_1 \mathcal{P}_2 \) with \( \text{Norm}(\mathcal{P}_0) = p^3 \) and \( \text{Norm}(\mathcal{P}_1) = \text{Norm}(\mathcal{P}_2) = p \), whence \( p^3 || \text{Disc}(k/\mathbb{Q}) \).

To handle the two remaining cases of \( D(p) \), we use the classical fact (cf. [6, Lemma 5]) that if

\[
PGL_2(\mathbb{F}_7) = \prod_{\tau \in T} \text{Gal}(L/k) \tau I(p),
\]

(6)
is the double-coset decomposition of \( PGL_2(\mathbb{F}_7) \) by \( \text{Gal}(L/k) \) and \( I(p) \), then there are exactly \#\( T \) primes in \( k \) lying above \( p \), and that the ramification index of the prime corresponding to \( \tau \in T \) is the index

\[
[\tau I(p) \tau^{-1} : \text{Gal}(L/k) \cap \tau I(p) \tau^{-1}] = (6, 8) 7 (2687453) = (13867542).
\]

To compute this double-coset decomposition, we will use the fact [2, p. 213] that \( PGL_2(\mathbb{F}_7) \) is realizable as a subgroup of \( S_8 \) generated by the permutations \( \gamma := (2687453) \) and \( \delta := (13867542) \).

First, take \( D(p) = I(p) \simeq C_2 \). Using the computer algebra package \textsc{GAP} [5] we find that \( N \), the normalizer of the 7-cycle \( \gamma \) in \( \langle \gamma, \delta \rangle \), contains the order two element \( \mu := (16)(24)(58) \).

Since \( PSL_2(\mathbb{F}_7) \) is the commutator subgroup of \( PGL_2(\mathbb{F}_7) \), and hence necessarily even, while \( \mu \) is odd, it follows that \( \mu \not\subseteq PSL_2(\mathbb{F}_7) \). By Lemma 1(d), the order 2 elements in \( PGL_2(\mathbb{F}_7) - PSL_2(\mathbb{F}_7) \) are pairwise conjugate, so we can \( \mu \) take to be the generator of \( I(p) = D(p) \). Using this explicit description

\[
PGL_2(\mathbb{F}_7) = \langle \gamma, \delta \rangle, \text{Gal}(L/k) = N, \text{ and } D(p) = I(p) = \langle \mu \rangle,
\]

we use \textsc{GAP} to find that the double coset decomposition (6) has size 5. Thus there are exactly five primes in \( k \) lying above \( p \), each with inertia degree 1 and ramification index \( \leq 2 \). Since \( [k : \mathbb{Q}] = 8 \), the only possibility is that \( p \mathcal{O}_k = \mathcal{P}_0^2 \mathcal{P}_1^2 \mathcal{P}_2 \) with every \( \text{Norm}(\mathcal{P}_i) = p \), whence \( p^3 || \text{Disc}(k/\mathbb{Q}) \). Note that we do not need to invoke (7).

Finally, suppose \( D(p) \simeq C_{2,2} \). Using \textsc{GAP} we find that the centralizer of \( \mu \) contains the permutation \( \omega := (14)(26)(37) \). Taking \( \langle \mu, \omega \rangle \) as a model of \( D(p) \) we now find that the double coset decomposition has size 3, with representatives

\[
\tau_1 = (\), \tau_2 = (13)(27)(58), \tau_3 = (15628473).
\]

Using (7), we check that the ramification indices of the corresponding primes of \( k \) are 1, 2 and 2, respectively. Since \( [k : \mathbb{Q}] = 8 \) and each such prime has inertia degree \( \leq 2 \), the only possibility is that \( p \mathcal{O}_k = \mathcal{P}_0 \mathcal{P}_1^2 \mathcal{P}_2^2 \) with \( \text{Norm}(\mathcal{P}_1) = \text{Norm}(\mathcal{P}_2) = p^2 \) and \( \text{Norm}(\mathcal{P}_3) = p \), whence \( p^3 || \text{Disc}(k/\mathbb{Q}) \). This completes the proof of the lemma. \( \square \)

Lemma 5 improves the trivial estimate \( \text{Disc}(k/\mathbb{Q})/(7^3 61^4) \), but it still lies outside the range of the database [7]. We now augment this with an argument of Roberts [13] to eliminate \( k \). Fix an order 2 element \( \sigma \in PGL_2(\mathbb{F}_7) - PSL_2(\mathbb{F}_7) \), and denote by \( L_\sigma \) the fixed field of \( L \) by \( \sigma \).
Lemma 6. — (a) The field discriminant of \( L_{\sigma}/\mathbb{Q} \) is \( \pm 7^{78}61^{81}, \pm 7^{81}61^{78}, \) or \( \pm 7^{81}61^{81}. \)  
(b) Suppose \( L_{\sigma} \) is not totally real and that the unique quadratic subfield of \( L/\mathbb{Q} \) is complex quadratic. Then \( L_{\sigma} \) has at least six distinct real places.

Proof. — (a) Let \( p \) be either 7 or 61, and let \( \mathfrak{p} \subset \mathcal{O}_L \) be a prime lying above \( p. \) First, suppose \( D(\mathfrak{p}) = C_2. \) By Lemma 1(a), \( PGL_2(\mathbb{F}_7) \) has 28 order 2 subgroups not contained in \( PSL_2(\mathbb{F}_7). \) For any one of them, call it \( J_2, \) there are \( (336/2)/28 = 6 \) primes in \( L \) with \( J_2 \) as its inertia group. Exactly one of the 28 choices of \( J_2 \) is \( \text{Gal}(L/L_{\sigma}). \) Thus there are \( (28 - 1) \cdot 6 \cdot \frac{1}{2} = 81 \) ramified primes in \( L_{\sigma} \) lying above \( \mathfrak{p}, \) each with ramification index 2 and inertia degree 1. Thus the \( p \)-part of the field discriminant of \( L_{\sigma} \) is \( p^{81}. \) 
Next, suppose \( D(\mathfrak{p}) = C_6. \) By Lemma 1(b), there are 28 \( C_6 \) subgroups \( J_6, \) each one being the decomposition group of \( (336/6)/28 = 2 \) primes in \( L. \) Thus there are \( (28 - 1) \cdot 2 \cdot \frac{1}{2} = 27 \) ramified primes in \( L_{\sigma} \) lying above \( \mathfrak{p}, \) each with ramification index 2 and inertia degree 3. Thus the \( p \)-part of the field discriminant of \( L_{\sigma} \) is \( (p^2)^{27} = p^{78}. \) 
Finally, suppose \( D(\mathfrak{p}) = C_{2,2}. \) By Lemma 1(d), there are \( (336/4)/42 = 2 \) primes in \( L \) with a given \( C_{2,2} \) as its decomposition group, and three of the 42 \( C_{2,2} \) contain \( \sigma. \) Thus there are \( (42 - 3) \cdot 2 \cdot \frac{1}{2} = 39 \) ramified primes in \( L_{\sigma} \) lying above \( \mathfrak{p}, \) each with ramification index 2 and inertia degree 2. Thus the \( p \)-part of the field discriminant of \( L_{\sigma} \) is \( (p^3)^{39} = p^{78}. \) 
(b) Since the unique quadratic subfield of \( L/\mathbb{Q} \) is complex, complex conjugation gives rise to an order 2 element in \( \text{Gal}(L/\mathbb{Q}) \cong PGL_2(\mathbb{F}_7) \) not contained in \( PSL_2(\mathbb{F}_7). \) Conjugate number fields have the same number of real places, and the conjugates of \( L_{\sigma} \) are precisely \( L_{\sigma'}. \) where \( \sigma' \) are \( PGL_2(\mathbb{F}_7) \)-conjugate to \( \sigma. \) Recall Lemma 1(a) and we see that to prove part (b) we can take \( \sigma \in \text{Gal}(L/\mathbb{Q}) \) to be complex conjugation. Then \( L_{\sigma} \subset \mathbb{R}, \) and we are reduced to find six distinct field automorphisms of \( L_{\sigma}. \) 
In the course of proving the \( D(\mathfrak{p}) \cong C_2 \) case of Lemma 5, we saw that \( PGL_2(\mathbb{F}_7) \) is realizable as a subgroup of \( S_8 \) generated by the permutations \( (2687453) \) and \( (13867543), \) and that \( \mu := (16)(24)(58) \) is an order 2 element of this permutation representation of \( PGL_2(\mathbb{F}_7) \) not contained in \( PSL_2(\mathbb{F}_7). \) Using the computer algebra system GAP, we find that the centralizer of \( \mu \) has order 12. That means there are twelve elements \( \alpha_1, \ldots, \alpha_{12} \) in \( \text{Gal}(L/\mathbb{Q}) \) that commute with \( \sigma. \) 
Fix a a normal basis of \( L/\mathbb{Q}, \) i.e. fix an element \( \omega \in L \) so that \( \{g \omega : g \in \text{Gal}(L/\mathbb{Q})\} \) is a \( \mathbb{Q} \)-basis of \( L. \) Let \( g_1, \ldots, g_{168} \) be a complete set of right coset representatives of \( \langle \sigma \rangle \subset \text{Gal}(L/\mathbb{Q}). \) Then the elements

\[
(8) \quad g_i \omega + \sigma g_i \omega \quad (1 \leq i \leq 168)
\]

are \( \mathbb{Q} \)-linearly independent, and hence they form a \( \mathbb{Q} \)-basis of \( L_{\sigma}/\mathbb{Q}. \) Since each \( \alpha_i \) above commutes with \( \sigma, \) left-multiplication by \( \alpha_i \) takes the set of elements in (8) to itself. We claim that

\[
(9) \quad \alpha_m \text{ and } \alpha_n \text{ induce the same action on the elements (8)} \iff \alpha_m = \sigma^i \alpha_n \text{ for some } i \in \{0, 1\}.
\]

The set of \( \alpha_i, \) being the centralizer of \( \sigma, \) is closed under multiplication by \( \sigma. \) It then follows that the restriction of these twelve \( \alpha_i \in \text{Gal}(L/\mathbb{Q}) \) to \( L_{\sigma} \) define six pairwise distinct field automorphisms of \( L_{\sigma} \subset \mathbb{R}, \) and hence \( L_{\sigma} \) has at least six distinct real embeddings.
It remains to verify the claim (9). To say that $\alpha_m$ and $\alpha_n$ induce the same action on the elements (8) is to say that

$$(\alpha_m + \alpha_m \sigma - \alpha_n - \alpha_n \sigma)(g_i \omega) = 0 \quad \text{for all } i.$$  

Since $\sigma$ has order 2, it follows that

$$(\alpha_m + \alpha_m \sigma - \alpha_n - \alpha_n \sigma)(g_i \sigma \omega) = 0 \quad \text{for all } i.$$  

Recall that the $g_i$ is a complete set of right coset representatives of $\langle \sigma \rangle \subset \text{Gal}(L/Q)$ and that $\{g \omega : g \in \text{Gal}(L/Q)\}$ is a $Q$-basis of $L/Q$, that means

$$(\alpha_m + \alpha_m \sigma - \alpha_n - \alpha_n \sigma)(x) = 0 \quad \text{for all } x \in L.$$  

By the linear independence of field automorphisms [1, Cor. on p. 84], that means $\alpha_m = \sigma^i \alpha_n$ for some $i \in \{0, 1\}$, as desired. \hfill \Box

Finally, we apply Roberts' argument [13] to deduce a contradiction from Lemma 6, and therefore $Q(\sqrt{-7}, \sqrt{61})$ must be unramified-closed.

First, suppose $|\text{Disc}(L_\sigma/Q)| \neq \pm 7^{81}1^{81}$. Then the root discriminant of $L_\sigma$ is $\leq 17.912$. This is not possible, since Diaz y Diaz [4] shows unconditionally that a degree 168 extension has root discriminant $\geq 17.98$.

Next, suppose $L_\sigma/Q$ has field discriminant $\pm 7^{81}1^{81}$. Note that $L_\sigma$ has a unique quadratic subfield which is one of $Q(\sqrt{-7} \times 61), Q(\sqrt{61})$ or $Q(\sqrt{-7})$. In the first two cases, $L_\sigma/Q$ is linearly disjoint from $Q(\sqrt{-7})$, and hence $L_\sigma(\sqrt{-7})/Q(\sqrt{-7})$ is unramified at the prime of $Q(\sqrt{-7})$ above 7. Then in these two cases the root discriminant of $L_\sigma(\sqrt{-7})/Q$ is

$$(7^{168}61^{162})^{1/336} = 19.20\ldots$$  

This is not possible, since Diaz y Diaz [4] shows unconditionally that a degree 336 extension has root discriminant $\geq 19.47$, so we are done.

Finally, suppose $|\text{Disc}(L_\sigma/Q)| = 7^{81}1^{81}$ and that $Q(\sqrt{-7})$ is the unique quadratic subfield of the $PGL_2(F_7)$-extension $L/Q$. Then lemma 6(b) says that $L_\sigma/Q$ has at least six distinct real places. For any degree 168 field with $r_1$ real places and $r_2$ pairs of complex places, using $b = 9.000$ in [11, Table 4] yields the unconditional root discriminant lower bound (see [11, description of tables] for details)

$$> 53.047^{r_1/168}20.710^{2r_2/168}e^{-24.001/168}.$$  

In particular, if $r_1 \geq 6$ then the root discriminant is $\geq 18.566$, contradicting our hypothesis $|\text{Disc}(L_\sigma/Q)|^{1/168} = (7^{81}1^{81})^{1/168} = 18.5456$. This completes the proof of the theorem.

6. Remaining cases

As we pointed out in the introduction, among the 172 complex Abelian number fields with class number one, 132 of them are known to be unramified closed under the unconditional Odlyzko, 23 of them are known to be unramified closed under the conditional Odlyzko bound (we will call these GRH fields), and the status of the 17 remaining fields are open (we will call these unknown fields). In this paper we determine the unramified closure of three of the 23 GRH fields and three of the 17 unknown field. We now discuss the remaining fields.

The unconditional Odlyzko bound for the root discriminant of a degree $n$ field is $|D|^{1/n} > 22.3816^{1+o(1)}$ [12, (2.5)]. The root discriminant of 16 of the GRH fields exceed this value, so
for these 16 fields we do not even know unconditionally if $[K^{ur} : \mathbb{Q}]$ is finite. Of the seven remaining GRH fields, Yamamura [21] has since verified unconditionally that $K^{ur} = K$ for $\mathbb{Q}(\sqrt{-53} - 2\sqrt{53})$, $\mathbb{Q}(\sqrt{-3}, \sqrt{-11}, \cos(2\pi/7))$, and $\mathbb{Q}(\sqrt{-61} - 6\sqrt{61})$. Theorem 1(a) handles the case $\mathbb{Q}(\sqrt{-7}, \sqrt{163})$. The three remaining GRH fields are as follows (in this table the degree $[K^{ur} : \mathbb{Q}]$ is computed using the unconditional Odlyzko bound):

<table>
<thead>
<tr>
<th>$K$</th>
<th>$\text{Gal}(K/\mathbb{Q})$</th>
<th>root discriminant</th>
<th>$[K^{ur} : \mathbb{Q}]$</th>
<th>$[K^{ur} : K]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$L_{43}^3(\sqrt{-3})$</td>
<td>$C_6$</td>
<td>$(3^34^3)^{1/4} = 21.26$</td>
<td>$&lt; 1524$</td>
<td>$&lt; 254$</td>
</tr>
<tr>
<td>$\mathbb{Q}(\sqrt{-3}, \sqrt{-163})$</td>
<td>$C_{2,2}$</td>
<td>$\sqrt{3} \cdot 163 = 22.11$</td>
<td>$&lt; 13538$</td>
<td>$&lt; 3384$</td>
</tr>
<tr>
<td>$\mathbb{Q}(\sqrt{-11}, i \sin(2\pi/8))$</td>
<td>$C_{2,4}$</td>
<td>$(2^{22}11^{4})^{1/8} = 22.31$</td>
<td>$&lt; 102183$</td>
<td>$&lt; 12772$</td>
</tr>
</tbody>
</table>

The smallest case above, $L_{43}^3(\sqrt{-3})$, is almost reachable by the techniques here. The remaining cases seem to be out of reach by current technology.

We now turn to the 17 unknown fields. Four of them, $\mathbb{Q}(\sqrt{-43}, \sqrt{-67})$, $\mathbb{Q}(\sqrt{-19}, \sqrt{-163})$, $\mathbb{Q}(\sqrt{-43}, \sqrt{-163})$, $\mathbb{Q}(\sqrt{-67}, \sqrt{-163})$ have root discriminants that exceed the GRH Odlyzko bound [12, (2.6)]. For these fields we do not even know if $K^{ur}$ is a finite extension. Yamamura [21] has since verified unconditionally that $K^{ur} = K$ for $\mathbb{Q}(\sqrt{-1}, \sqrt{-163})$ and $\mathbb{Q}(\sqrt{-11}, \sqrt{-67})$, and under GRH, the field $L_{37}^4(\sqrt{-1})$. Theorem 1(b) resolves the case $L_{43}^1$ under GRH, and we list the nine remaining unknown fields in the table below. In this table the degree $[K^{ur} : \mathbb{Q}]$ is computing using the conditional Odlyzko bound; specifically, for root discriminant up to 41.122 we use [11, Table 1], and for root discriminant $> 41.122$ we use the bound

$$|\text{Disc}(M/\mathbb{Q})|^{1/[M: \mathbb{Q}]} > B\cdot E^{[M: \mathbb{Q}]}$$

where $B = 43.426$ and $E = 3.5263 \times 10^8$ are given by [11, Table 3] using $b = 25$ (see [11, description of tables] for details.) These fields seem to be beyond current technology.

<table>
<thead>
<tr>
<th>$K$</th>
<th>$\text{Gal}(K/\mathbb{Q})$</th>
<th>root discriminant</th>
<th>$[K^{ur} : \mathbb{Q}]$</th>
<th>$[K^{ur} : K]$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathbb{Q}(\sqrt{-7}, \sqrt{-163})$</td>
<td>$C_{2,2}$</td>
<td>$\sqrt{7} \cdot 163 = 33.78$</td>
<td>$&lt; 10000$</td>
<td>$&lt; 2500$</td>
</tr>
<tr>
<td>$\mathbb{Q}(\sqrt{-19}, \sqrt{-67})$</td>
<td>$C_{2,2}$</td>
<td>$\sqrt{19} \cdot 67 = 35.68$</td>
<td>$&lt; 31970$</td>
<td>$&lt; 7993$</td>
</tr>
<tr>
<td>$\mathbb{Q}(\sqrt{-11}, \sqrt{-163})$</td>
<td>$C_{2,2}$</td>
<td>$\sqrt{11} \cdot 163 = 43.34$</td>
<td>$&lt; 10^{12}$</td>
<td>$&lt; 10^{12}/4$</td>
</tr>
<tr>
<td>$L_{67}^6$</td>
<td>$C_6$</td>
<td>$67^{5/6} = 33.25$</td>
<td>$&lt; 4800$</td>
<td>$&lt; 800$</td>
</tr>
<tr>
<td>$L_{29}^4(\sqrt{-2})$</td>
<td>$C_{2,4}$</td>
<td>$29^{3/4}2^{3/2} = 35.35$</td>
<td>$&lt; 31970$</td>
<td>$&lt; 3997$</td>
</tr>
<tr>
<td>$L_{61}^{12}$</td>
<td>$C_{12}$</td>
<td>$61^{11/12} = 43.31$</td>
<td>$&lt; 10^{12}$</td>
<td>$&lt; 10^{12}/5$</td>
</tr>
<tr>
<td>$L_{43}^6(\sqrt{-3})$</td>
<td>$C_{2,6}$</td>
<td>$43^{5/6}3^{1/2} = 39.79$</td>
<td>$&lt; 10^6$</td>
<td>$&lt; 83334$</td>
</tr>
<tr>
<td>$L_{13}^7L_3^3(\sqrt{-2})$</td>
<td>$C_{2,2,3}$</td>
<td>$(7^{6}8^{13})^{1/12} = 41.37$</td>
<td>$&lt; 10^{12}$</td>
<td>$&lt; 10^{12}/9$</td>
</tr>
<tr>
<td>$L_{43}^1$</td>
<td>$C_{14}$</td>
<td>$43^{13/14} = 32.97$</td>
<td>$&lt; 4800$</td>
<td>$&lt; 343$</td>
</tr>
</tbody>
</table>
Acknowledgment. — I would like to thank Professor Ken Yamamura for sending me a reprint of [18] and for detailed comments and references; Professor Farshid Hajir for useful discussions; and Professor David Roberts for showing us the beautiful argument in [13].

References


[22] K. Yamamura, Unpublished table titled *Examples of real quadratic number fields with class number one having an unramified nonsolvable Galois extension*.

June 11, 2014

Siman Wong, Department of Mathematics & Statistics, University of Massachusetts. Amherst, MA 01003

E-mail: siman@math.umass.edu