Canad. Math. Bull. 2026, pp. 1–13
http://dx.doi.org/10.4153/S0008439526101775
© The Author(s), 2026. Published by Cambridge University Press on behalf of Canadian Mathematical Society

On class groups of abelian extensions

Anuj Jakhar and Mahesh Kumar Ram

Abstract. Let K be an absolutely abelian number field, and t be a positive integer relatively prime to $[K:\mathbb{Q}]$. We provide a method to use the t-rank of the class group of K to obtain a lower bound on the t-rank of class groups of any cyclotomic fields (or real cyclotomic fields) that contain this K. As an application, for any odd integer $t > 1$, we provide a family of cyclotomic fields whose class groups have t-rank at least 2. Furthermore, we prove that the class number of $\mathbb{Q}(\zeta_{p^e} + \zeta_{p^e}^{-1})$ cannot be equal to 2, where p is a prime, $e \geq 1$ is an integer, and ζ_{p^e} denotes a primitive p^e-th root of unity. We also provide an upper bound for the class number of a real cyclotomic field.

1 Introduction

For a number field K, we denote its class group, class number, discriminant, and Hilbert class field by $C\ell(K)$, h_K, D_K, and $H(K)$, respectively. If K/F is a Galois extension of number fields, we write $G_{K/F}$ for its Galois group. For any integer $n > 1$, let ζ_n denote a primitive nth root of unity, and define the maximal real subfield of $\mathbb{Q}(\zeta_n)$ as $\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$, called a real cyclotomic field. For any group G, we write $|G|$ to denote its cardinality.

Given an integer $t > 1$, we say that the t-rank of the class group of a number field K is r if $C\ell(K)$ contains exactly r-copies of $\mathbb{Z}/t\mathbb{Z}$. The 2-rank of class groups of quadratic fields is completely known by Gauss's genus theory, and using this one can easily construct quadratic fields whose class group has a large 2-rank. Motivated by this, many researchers have explored families of number fields whose class groups have large t-rank for integers $t > 1$. Several works [1, 11, 15, 21, 23, 28, 33] provide a family of quadratic fields whose class groups contain $\mathbb{Z}/t\mathbb{Z}$ as a subgroup.

The main objective of this article is to use the known results regarding the t-rank of class group of a field K to obtain a lower bound on the t-rank of class groups of any cyclotomic fields (or real cyclotomic fields) that contain this K. In this context, we prove the following theorem.

Theorem 1.1 *Let $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$ be a product of powers of distinct odd primes p_i with $e_i \geq 1$, and set $d = p_1 p_2 \dots p_s$. Define*

$$K = \begin{cases} \mathbb{Q}(\sqrt{d}), & \text{if } d \equiv 1 \pmod 4, \\ \mathbb{Q}(\sqrt{-d}), & \text{if } d \equiv 3 \pmod 4. \end{cases}$$

Received by the editors September 22, 2025; accepted January 28, 2026.
Published online on Cambridge Core February 4, 2026.
AMS subject classification: **11R29**, **11R18**.
Keywords: Cyclotomic extensions, class numbers, class groups.

https://doi.org/10.4153/S0008439526101775 Published online by Cambridge University Press

Let $m > 1$ be the largest odd divisor of h_K, and suppose $t > 1$ divides m such that the t-rank of $C\ell(K)$ is r. Then:

(1) *If $d \equiv 1 \pmod 4$, the t-rank of the class groups of $\mathbb{Q}(\zeta_n)^+$ and $\mathbb{Q}(\zeta_n)$ is at least r, and m divides the class number of both fields.*
(2) *If $d \equiv 3 \pmod 4$, the t-rank of the class group of $\mathbb{Q}(\zeta_n)$ is at least r, and m divides its class number.*

Theorem 1.1 highlights the important role of class groups of quadratic fields in deducing arithmetic information about the class groups of cyclotomic fields. For instance, by combining Theorem 1.1 of [4] with Theorem 1.1, one can conclude that there exist infinitely many primes $p \equiv q \equiv 3 \pmod 4$ such that the class number of $\mathbb{Q}(\zeta_{pq})^+$ is divisible by 3.

Furthermore, for any odd integer $t > 1$, Theorem 1.1 provides lower bounds on the t-rank of class groups of various fields of the form $\mathbb{Q}(\zeta_n)^+$. Even though for any odd integer $t > 5$, no infinite family of quadratic fields is currently known whose class groups have t-rank at least 3. However, Theorem 1.1 can be used to construct cyclotomic (or real cyclotomic) fields whose class groups have large t-rank. For example, one can find square-free positive integers $d_1, d_2, \ldots, d_s$ such that $(d_i, d_j) = 1$ for $i \neq j$ and $d_i \equiv 3 \pmod 4$. For each i, the class group of $K_i = \mathbb{Q}(\sqrt{-d_i})$ contains at least one copy of $\mathbb{Z}/t\mathbb{Z}$. Theorem 1.1, together with Proposition 2.9, then implies that the class group of $\mathbb{Q}(\zeta_{d_1 d_2 \ldots d_s})$ has t-rank at least s. We prove one such application of Theorem 1.1, which is the following result.

Corollary 1.2 *Let $t > 1$ and $a > 1$ be two odd integers, and let $u \geq 2$ be an integer. Assume that $-d_{u,t}$ and $d'_{a,t}$ are the square-free parts of $1 - 4u^t$ and $a^{2t} + 4$, respectively. Suppose $a = 17b$ and $u = a^2$, where $b \geq 1$ is an integer. Then, the t-rank of the class group of $\mathbb{Q}(\zeta_{d_{u,a,t}})$ is at least 2, where $d_{u,a,t} = d_{u,t} \cdot d'_{a,t}$, and the class group of $\mathbb{Q}(\zeta_{d'_{a,t}})^+$ has a subgroup isomorphic to $\mathbb{Z}/t\mathbb{Z}$.*

There are many results providing families of fields $\mathbb{Q}(\zeta_n)^+$ whose class numbers are greater than one. For example, Ankeny, Chowla, and Hasse [2] proved that if $n = (2vq)^2 + 1$ is prime, where q is prime and $v > 1$ is an integer, then the class number of $\mathbb{Q}(\zeta_n)^+$ is greater than one. For more results in this direction, see [6, 8, 10, 13, 24, 25, 29, 32]. In Corollary 1.2, we provide a family of maximal real subfields $\mathbb{Q}(\zeta_{d'_{a,t}})^+$ whose class groups contain a subgroup isomorphic to $\mathbb{Z}/t\mathbb{Z}$.

The next theorem shows that there exist infinitely many real cyclotomic fields whose class numbers are even. In particular, we establish the following result.

Corollary 1.3 *Let s be a positive integer relatively prime to 3. Then, there exist infinitely many real cyclotomic fields whose class numbers are divisible by s.*

Combining Corollaries 1.2 and 1.3, we obtain the following remarkable conclusion:

There are infinitely many real cyclotomic fields and cyclotomic fields whose class numbers are divisible by any given positive integer m not divisible by 6.

https://doi.org/10.4153/S0008439526101775 Published online by Cambridge University Press

We remark that this conclusion also follows from [22], although our methods are different.

Studying class numbers of cyclotomic fields and the class numbers of maximal real subfields of cyclotomic fields is still a difficult and mysterious problem after a long research era. However, there is a nice result on the class numbers of cyclotomic fields, which is the following.

Let $n \not\equiv 2 \pmod 4$ be a positive integer. Then, the class number of $\mathbb{Q}(\zeta_n)$ is one if and only if

$$n \in \left\{ \begin{matrix} 1, 3, 4, 5, 7, 8, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 24, \\ 25, 27, 28, 32, 33, 35, 36, 40, 44, 45, 48, 60, 84 \end{matrix} \right\}. \tag{1.1}$$

In [17], Masley proved that the class number of $\mathbb{Q}(\zeta_n)$ equals 2 if and only if $n = 39$ or $n = 56$, provided $n \not\equiv 2 \pmod 4$. For more results on class numbers of cyclotomic fields, we refer the reader to [16, 18–20, 27].

In this context, we prove the following theorem, which provides a restriction on possible values of the class number of certain real cyclotomic fields.

Theorem 1.4 *Let $K = \mathbb{Q}(\zeta_{p^e})^+$, where p is a prime and $e \geq 1$ is an integer. Suppose q is a prime such that $q - 1$ is relatively prime to $\frac{p^{e-1}(p-1)}{2}$. Then, $h_K \neq q$.*

As an immediate consequence, we obtain the following corollary.

Corollary 1.5 *Let p be a prime and $e \geq 1$ be an integer. Then, the class number of $\mathbb{Q}(\zeta_{p^e})^+$ is not equal to 2.*

Finally, we provide an upper bound for the class number of real cyclotomic fields in terms of the relative Pólya group, as defined by Chabert in [5].

Theorem 1.6 *Let $n \not\equiv 2 \pmod 4$ be a positive integer, and let $L = \mathbb{Q}(\zeta_n)$ and $K = \mathbb{Q}(\zeta_n)^+$. Then,*

$$h_K \leq \begin{cases} |\mathcal{P}o(L/K)| & \text{if } n \text{ is a prime power,} \\ 2|\mathcal{P}o(L/K)| & \text{otherwise,} \end{cases}$$

where $\mathcal{P}o(L/K)$ denotes the relative Pólya group of the extension L/K. Moreover, if $h_K = 1$, then $\mathcal{P}o(L/K)$ is trivial. The converse of the last assertion holds provided h_L is odd.

Theorem 1.6 ensures the following asymptotic behavior:

As $h_K \to \infty$, the size of the relative Pólya group $\mathcal{P}o(L/K)$ also tends to infinity.

The structure of the article is as follows: In Section 2, we present some preliminary results. Section 3 is devoted to the proof of Theorem 1.1. In Section 4, we establish Corollaries 1.2 and 1.3. Finally, Sections 5 and 6 contain the proofs of Theorems 1.4 and 1.6, respectively.

https://doi.org/10.4153/S0008439526101775 Published online by Cambridge University Press

2 Preliminaries

The purpose of this section is to present the necessary background results that will be used in the proofs of the results. We begin with the following theorem due to Louboutin [15].

Theorem 2.1 *Let $t > 1$ be an odd integer. Then, for any integer $u \geq 2$, the ideal class group of the imaginary quadratic field $\mathbb{Q}\left(\sqrt{1-4u^t}\right)$ contains an element of order t.*

We now recall a result due to Ichimura [11].

Theorem 2.2 *Let $t \geq 2$ be an integer, and let $a \geq 3$ be an odd integer. Then, the class group of the real quadratic field $\mathbb{Q}(\sqrt{a^{2t}+4})$ contains an element of order t.*

We next present a well-known result regarding Galois extensions.

Lemma 2.3 *If $K/\mathbb{Q}$ is a Galois extension, then the Hilbert class field $H(K)$ over $\mathbb{Q}$ is also a Galois extension.*

For a Galois extension $K/\mathbb{Q}$, there exists an exact sequence:

$$1 \longrightarrow \mathrm{C}\ell(K) \longrightarrow \mathrm{G}_{H(K)/\mathbb{Q}} \longrightarrow \mathrm{G}_{K/\mathbb{Q}} \longrightarrow 1. \tag{2.1}$$

This sequence is said to split if there exists a group homomorphism $\psi : \mathrm{G}_{K/\mathbb{Q}} \to \mathrm{Aut}(\mathrm{C}\ell(K))$ such that

$$\mathrm{G}_{H(K)/\mathbb{Q}} \simeq \mathrm{C}\ell(K) \rtimes_{\psi} \mathrm{G}_{K/\mathbb{Q}}.$$

Regarding the splitting of the sequence (2.1), the following result was proved by Gold [9].

Theorem 2.4 *Let $K/\mathbb{Q}$ be a Galois extension of number fields. Suppose s is the least common multiple of the ramification indices of all finite primes in the extension $K/\mathbb{Q}$. If $s = [K : \mathbb{Q}]$, then the exact sequence*

$$1 \longrightarrow \mathrm{C}\ell(K) \longrightarrow \mathrm{G}_{H(K)/\mathbb{Q}} \longrightarrow \mathrm{G}_{K/\mathbb{Q}} \longrightarrow 1$$

splits.

We now state the following result from Ankeny, Chowla, and Hasse [2].

Theorem 2.5 *Let L/K be an extension of number fields. Suppose there exists no intermediate field $F \neq K$ such that F/K is abelian and unramified at all primes of K. Then, the class number h_K divides h_L.*

We next recall a result from [31, Proposition 2.15], useful for identifying ramified primes in real cyclotomic subfields.

https://doi.org/10.4153/S0008439526101775 Published online by Cambridge University Press

Proposition 2.6 *Let $n \not\equiv 2 \pmod 4$ be a positive integer. If $n = p^a$ for some prime p and integer $a \geq 1$, then the extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ is ramified only at the prime of $\mathbb{Q}(\zeta_n)^+$ lying above p and at the infinite primes of $\mathbb{Q}(\zeta_n)^+$. If n is not a prime power, then only the infinite primes of $\mathbb{Q}(\zeta_n)^+$ are ramified in $\mathbb{Q}(\zeta_n)$.*

We also record the following result from [31, Lemma 6.15].

Theorem 2.7 *Let $m \not\equiv 2 \pmod 4$ and $n \not\equiv 2 \pmod 4$ be two positive integers greater than 1 such that $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_n)$. Suppose K is a number field with $\mathbb{Q}(\zeta_m) \subseteq K \subseteq \mathbb{Q}(\zeta_n)$. If $K/\mathbb{Q}(\zeta_m)$ is unramified at all primes of $\mathbb{Q}(\zeta_m)$, then $K = \mathbb{Q}(\zeta_m)$.*

Following the proof of Theorem 1.1 in [26] (or see also [7, p. 2]), one can obtain the next result.

Proposition 2.8 *Let $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s} \not\equiv 2 \pmod 4$, where $p_1, p_2, \dots, p_s$ are distinct primes and $e_i \in \mathbb{N}$. Then, the class group of $\mathbb{Q}(\zeta_n)$ contains a subgroup isomorphic to $C\ell(K_1) \oplus C\ell(K_2) \oplus \cdots \oplus C\ell(K_s)$, where $K_i = \mathbb{Q}(\zeta_{p_i^{e_i}})$ for $1 \leq i \leq s$.*

Moreover, the following result holds.

Proposition 2.9 *Let d_1, d_2 be two coprime positive integers with $d_1 \not\equiv 2 \pmod 4$ and $d_2 \not\equiv 2 \pmod 4$. Then, the class group of $\mathbb{Q}(\zeta_{d_1 d_2})$ contains a subgroup isomorphic to $C\ell(\mathbb{Q}(\zeta_{d_1})) \oplus C\ell(\mathbb{Q}(\zeta_{d_2}))$.*

Finally, we recall a classical result concerning the genus field of an abelian extension from [14] (or see [12, p. 52]). The Genus field of a number field K, denoted by $G(K)$, is defined as the maximal abelian extension of K that is unramified at all finite primes of K and is the compositum of K with an abelian extension of $\mathbb{Q}$.

Theorem 2.10 *Let $K/\mathbb{Q}$ be an abelian extension, and let $G(K)$ be the genus field of K. Then,*

$$[G(K) : K] = \frac{\prod_p e(p)}{[K : \mathbb{Q}]},$$

where the product runs over all rational primes p, and $e(p)$ denotes the ramification index of p in K.

3 Proof of Theorem 1.1

We begin this section with the following result, which will be used in the next result. It is of independent interest as well.

Theorem 3.1 *Let $K/\mathbb{Q}$ be an abelian extension of number fields. Suppose $m > 1$ is the largest positive divisor of h_K such that $\gcd(m, [K : \mathbb{Q}]) = 1$. Consider the subfield L of the Hilbert class field $H(K)$ containing K with $[L : K] = m$. Then, $L/\mathbb{Q}$ is not abelian. Moreover, for any intermediate field L' with $K \subsetneq L' \subseteq L$, the extension $L'/\mathbb{Q}$ is also not abelian.*

https://doi.org/10.4153/S0008439526101775 Published online by Cambridge University Press

Proof (Theorem 3.1) Assume, by contradiction, that $L/\mathbb{Q}$ is abelian. Let $G(K)$ be the genus field of K. Since $L \subset H(K)$ and L contains K, it follows that $L \subset G(K)$. Hence, $[L : K]$ divides $[G(K) : K]$. By Theorem 2.10, we know that

$$[G(K) : K] = \frac{\prod_p e(p)}{[K : \mathbb{Q}]},$$

where the product is over all primes p, and $e(p)$ denotes the ramification index of p in K. Therefore, m divides $\frac{\prod_p e(p)}{[K:\mathbb{Q}]}$, contradicting the assumption that $m > 1$ and $\gcd(m, [K : \mathbb{Q}]) = 1$. Thus, $L/\mathbb{Q}$ cannot be abelian.

A similar argument shows that the same conclusion holds for any proper intermediate field L' with $K \subsetneq L' \subset L$, thereby completing the proof. ∎

Note that in Theorem 3.1, such a subfield L of $H(K)$ is unique. If $L'/\mathbb{Q}$ is not a Galois extension, then we do not need to show that $L'/\mathbb{Q}$ is non-abelian.

Using the above theorem, we establish the following result, which will be used in the sequel. Although it can be obtained from [34], we present a self-contained proof here using a different approach for the sake of completeness.

Theorem 3.2 *Let $L/\mathbb{Q}$ be an abelian extension of number fields containing a proper subfield $K \neq \mathbb{Q}$. Let $m > 1$ be the largest positive divisor of h_K such that $\gcd(m, [K : \mathbb{Q}]) = 1$. If $t > 1$ divides m and the t-rank of the class group of K is r, then the t-rank of $C\ell(L)$ is at least r. Moreover, m divides h_L.*

Proof (Theorem 3.2) It is known that $C\ell(K)$ is a finite abelian group, and from class field theory, we have $C\ell(K) \simeq G_{H(K)/K}$. Hence, the Galois group $G_{H(K)/K}$ has a unique subgroup H of order h_K/m. Let L' denote the fixed field of H in $H(K)$. Then, L' is the unique subfield of $H(K)$ containing K such that $[L' : K] = m$.

Since L'/K is abelian and unramified at all primes of K, it follows that the extension LL'/L is also abelian and unramified at all primes of L. Therefore, the class group $C\ell(L)$ contains a subgroup isomorphic to $G_{LL'/L}$.

As L/K and L'/K are both finite Galois extensions, we have

$$[LL' : K] = \frac{[L : K] \cdot [L' : K]}{[L \cap L' : K]}. \tag{3.1}$$

By hypothesis, $L/\mathbb{Q}$ is an abelian extension and $L \cap L'$ is a subfield of both L and L' containing K, Theorem 3.1 implies that $L \cap L' = K$. Consequently, (3.1) becomes

$$[LL' : K] = [L : K] \cdot [L' : K]. \tag{3.2}$$

On the other hand, we also have

$$[LL' : K] = [LL' : L] \cdot [L : K]. \tag{3.3}$$

Comparing (3.2) and (3.3), we deduce

$$[LL' : L] = [L' : K] = m. \tag{3.4}$$

Thus, $G_{LL'/L}$ is a group of order m, and as noted earlier, is isomorphic to a subgroup of $C\ell(L)$. Hence, m divides h_L.

https://doi.org/10.4153/S0008439526101775 Published online by Cambridge University Press

Define the map

$$\psi : G_{LL'/L} \longrightarrow G_{L'/K} \quad \text{by} \quad \sigma \mapsto \sigma|_{L'}.$$

This map is clearly an injective group homomorphism. Therefore, by (3.4), it is a group isomorphism:

$$G_{LL'/L} \simeq G_{L'/K}.$$

Now, since $t \mid m$ and $C\ell(K)$ contains a unique subgroup of order m isomorphic to $G_{L'/K}$, it follows that the t-rank of $G_{L'/K}$ is r; because $C\ell(K)$ has t-rank r by assumption. Therefore, $G_{LL'/L}$ contains at least r copies of $\mathbb{Z}/t\mathbb{Z}$, implying that $C\ell(L)$ also contains at least r copies of $\mathbb{Z}/t\mathbb{Z}$. This completes the proof. ∎

Proof (Theorem 1.1) Let $L = \mathbb{Q}(\zeta_n)$ and let $L^+ = \mathbb{Q}(\zeta_n)^+$ denote its maximal real subfield.

We first consider the case where $d \equiv 1 \pmod 4$, so that $K = \mathbb{Q}(\sqrt{d})$. In this case, K is contained in L^+, and since $[K : \mathbb{Q}] = 2$, it follows that $K/\mathbb{Q}$ is a nontrivial abelian extension.

Given that m is odd, it is relatively prime to $[K : \mathbb{Q}] = 2$. Therefore, by applying Theorem 3.2 with $K \subset L^+$, we conclude that the t-rank of the class group of L^+ is at least r, and that m divides the class number of L^+. Since $C\ell(L^+)$ is isomorphic to a subgroup of $C\ell(L)$, these conclusions also hold for L. This completes the proof for the case $d \equiv 1 \pmod 4$.

Next, consider the case where $d \equiv 3 \pmod 4$, so that $K = \mathbb{Q}(\sqrt{-d})$. Then, K is contained in L, and as before, $[K : \mathbb{Q}] = 2$, implying that $K \neq \mathbb{Q}$ and $K/\mathbb{Q}$ is abelian. Since m is odd, m is again coprime with $[K : \mathbb{Q}]$. Applying Theorem 3.2 with $K \subset L$, we obtain that the t-rank of the class group of L is at least r, and that m divides the class number of L. This completes the proof of the theorem. ∎

4 Proof of Corollaries 1.2 and 1.3

Combining Theorems 1.1, 2.5, and 2.7, we obtain the following result.

Theorem 4.1 *Let $d \not\equiv 2 \pmod 4$ be a square-free positive integer. Define*

$$K = \begin{cases} \mathbb{Q}(\sqrt{d}) & \text{if } d \equiv 1 \pmod 4, \\ \mathbb{Q}(\sqrt{-d}) & \text{if } d \equiv 3 \pmod 4. \end{cases}$$

Suppose $m > 1$ is the largest odd divisor of h_K, and let $t > 1$ be a divisor of m such that the t-rank of $C\ell(K)$ is r. Let $n > 1$ be any integer such that $d \mid n$. Then, the class group of $\mathbb{Q}(\zeta_n)$ contains at least r copies of $\mathbb{Z}/t\mathbb{Z}$.

Proof (Corollary 1.2) From Theorem 2.2, we know that the class group of $\mathbb{Q}(\sqrt{d'_{a,t}})$ contains a subgroup isomorphic to $\mathbb{Z}/t\mathbb{Z}$. Hence, the t-rank of the class group of $\mathbb{Q}(\sqrt{d'_{a,t}})$ is at least 1.

Since a is odd and $d'_{a,t}$ is the square-free part of $a^{2t} + 4$, it follows that $d'_{a,t} \equiv 1 \pmod 4$. Moreover, as t is assumed to be odd, t is relatively prime to $[\mathbb{Q}(\sqrt{d'_{a,t}}) :$

https://doi.org/10.4153/S0008439526101775 Published online by Cambridge University Press

$\mathbb{Q}] = 2$. Therefore, by Theorem 1.1, we conclude that both the fields $\mathbb{Q}(\zeta_{d'_{a,t}})$ and $\mathbb{Q}(\zeta_{d'_{a,t}})^+$ have class groups containing a subgroup isomorphic to $\mathbb{Z}/t\mathbb{Z}$.

Similarly, Theorem 2.1 implies that the class group of $\mathbb{Q}(\sqrt{-d_{u,t}})$ also contains a subgroup isomorphic to $\mathbb{Z}/t\mathbb{Z}$, so the t-rank of its class group is at least 1. Since $-d_{u,t}$ is the square-free part of $1 - 4u^t$, it follows that $d_{u,t} \equiv 3 \pmod 4$. Given that t is odd, t is again relatively prime to $[\mathbb{Q}(\sqrt{-d_{u,t}}) : \mathbb{Q}] = 2$. Therefore, Theorem 1.1 applies, and we conclude that the class group of $\mathbb{Q}(\zeta_{d_{u,t}})$ contains a subgroup isomorphic to $\mathbb{Z}/t\mathbb{Z}$.

Now, since $a = 17b$ and $u = a^2$, it follows that $d'_{a,t}$ and $d_{u,t}$ are relatively prime. Applying Proposition 2.9, we deduce that the class group of $\mathbb{Q}(\zeta_{d_{u,a,t}})$ contains a subgroup isomorphic to $C\ell\big(\mathbb{Q}(\zeta_{d'_{a,t}})\big) \oplus C\ell\big(\mathbb{Q}(\zeta_{d_{u,t}})\big)$. We have already shown that each of the above groups contains a subgroup isomorphic to $\mathbb{Z}/t\mathbb{Z}$. Therefore, the class group of $\mathbb{Q}(\zeta_{d_{u,a,t}})$ contains a subgroup isomorphic to $\mathbb{Z}/t\mathbb{Z} \oplus \mathbb{Z}/t\mathbb{Z}$. This completes the proof. ∎

Remark 4.2 Theorem 4.1 further implies that if a cyclotomic field contains $\mathbb{Q}(\zeta_{d_{u,a,t}})$ as a subfield, then the t-rank of its class group is also at least 2.

The following result, cited from [30], will be used to prove Corollary 1.3.

Theorem 4.3 *Let m and a be positive integers such that a is coprime to 6, and a has a prime factor q for which either 2 or 3 is not a quadratic residue modulo q. Furthermore, for every odd prime divisor ℓ of m, assume that a has two prime factors q_1 and q_2 such that:*

- *2 is not an ℓ-th power residue modulo q_1 and modulo q_2, and*
- *3 is an ℓ-th power residue modulo q_1 but not modulo q_2.*

Let $K = \mathbb{Q}(\theta)$, where θ is a root of the polynomial

$$f(x) = x^3 + ux^2 + 2ux + u,$$

with integer $u = \frac{a^{2m}+27}{4}$. Then, $K/\mathbb{Q}$ is a cyclic cubic extension, and its class number is divisible by m. Moreover, there are infinitely many such fields K.

Proof (Corollary 1.3) Let m, a, and K be as in Theorem 4.3. From Theorem 4.3, we know that the class number h_K is divisible by m. Let s be a positive divisor of m such that $\gcd(s, 3) = 1$. Since $K/\mathbb{Q}$ is an abelian extension, the Kronecker–Weber theorem implies that $K \subset \mathbb{Q}(\zeta_f)$ for some positive integer f. Let f be the minimal such positive integer. Therefore, keeping in mind the fact that $[K : \mathbb{Q}] = 3$, we see that $K \subset \mathbb{Q}(\zeta_f)^+$.

Define $L = \mathbb{Q}(\zeta_f)^+$. Applying Theorem 3.2 for the fields L, K, and the integer s, we conclude that s divides h_L. Consequently, s divides the class number of $\mathbb{Q}(\zeta_f)$.

By Theorem 4.3, there are infinitely many such fields K, and thus infinitely many corresponding fields $L = \mathbb{Q}(\zeta_f)^+$ whose class numbers are divisible by s. This completes the proof. ∎

5 Proof of Theorem 1.4

We first prove an auxiliary result, analogous to Theorem 2.7, which will be used in the proof of Theorem 1.4.

https://doi.org/10.4153/S0008439526101775 Published online by Cambridge University Press

Proposition 5.1 *Let $m \not\equiv 2 \pmod 4$ and $n \not\equiv 2 \pmod 4$ be two positive integers greater than* 1 *such that $\mathbb{Q}(\zeta_m)^+ \subset \mathbb{Q}(\zeta_n)$. Suppose K is a number field with*

$$\mathbb{Q}(\zeta_m)^+ \subseteq K \subseteq \mathbb{Q}(\zeta_n),$$

and the extension $K/\mathbb{Q}(\zeta_m)^+$ is unramified at all primes of $\mathbb{Q}(\zeta_m)^+$. Then, $K = \mathbb{Q}(\zeta_m)^+$.

Proof (Proposition 5.1) Assume, by contradiction, that $K/\mathbb{Q}(\zeta_m)^+$ is a nontrivial extension unramified at all primes of $\mathbb{Q}(\zeta_m)^+$ and

$$\mathbb{Q}(\zeta_m)^+ \subset K \subseteq \mathbb{Q}(\zeta_n).$$

Then, the compositum $K\mathbb{Q}(\zeta_m)$ is contained in $\mathbb{Q}(\zeta_n)$, since both K and $\mathbb{Q}(\zeta_m)$ are subfields of $\mathbb{Q}(\zeta_n)$. Moreover, since $K/\mathbb{Q}(\zeta_m)^+$ is unramified at all primes of $\mathbb{Q}(\zeta_m)^+$, so is $K\mathbb{Q}(\zeta_m)/\mathbb{Q}(\zeta_m)$ at all primes of $\mathbb{Q}(\zeta_m)$. By Theorem 2.7, we conclude that $K\mathbb{Q}(\zeta_m) = \mathbb{Q}(\zeta_m)$. Hence, $K \subseteq \mathbb{Q}(\zeta_m)$, and since $\mathbb{Q}(\zeta_m)^+ \subset K$, we must have

$$\mathbb{Q}(\zeta_m)^+ \subset K \subseteq \mathbb{Q}(\zeta_m).$$

But $[\mathbb{Q}(\zeta_m) : \mathbb{Q}(\zeta_m)^+] = 2$, so the only possibility is $K = \mathbb{Q}(\zeta_m)$. This is not possible, otherwise the assumption that $K/\mathbb{Q}(\zeta_m)^+$ is unramified at all primes of $\mathbb{Q}(\zeta_m)^+$ contradicts Proposition 2.6. This contradiction proves that $K = \mathbb{Q}(\zeta_m)^+$, thereby completing the proof. ∎

One can prove the following result using a similar approach as in the proof of Proposition 5.1.

Proposition 5.2 *Let $m \not\equiv 2 \pmod 4$ and $n \not\equiv 2 \pmod 4$ be positive integers greater than* 1 *such that $\mathbb{Q}(\zeta_m)^+ \subset \mathbb{Q}(\zeta_n)^+$. Suppose K is a number field satisfying*

$$\mathbb{Q}(\zeta_m)^+ \subseteq K \subseteq \mathbb{Q}(\zeta_n)^+.$$

If the extension $K/\mathbb{Q}(\zeta_m)^+$ is unramified at all primes of $\mathbb{Q}(\zeta_m)^+$, then $K = \mathbb{Q}(\zeta_m)^+$.

We can now deduce the following result as a direct consequence of Theorem 2.5 and Proposition 5.2.

Proposition 5.3 *Let $n \not\equiv 2 \pmod 4$ be a positive integer, and let p be a prime divisor of n. Then, the class number of $\mathbb{Q}(\zeta_p)^+$ divides the class number of $\mathbb{Q}(\zeta_n)^+$. Moreover, for any positive divisor d of n, the class group of $\mathbb{Q}(\zeta_n)^+$ contains a subgroup isomorphic to the class group of $\mathbb{Q}(\zeta_d)^+$.*

In particular, from Corollary 1.2 and Proposition 5.3, we observe that if $d'_{a,t}$ is a divisor of a positive integer n, then the class group of $\mathbb{Q}(\zeta_n)^+$ has a subgroup isomorphic to $\mathbb{Z}/t\mathbb{Z}$.

Proof (Theorem 1.4) Assume, by contradiction, that the class number $h_K = q$. Since $K/\mathbb{Q}$ is a Galois extension and p is the only ramified prime in $K/\mathbb{Q}$ with ramification index equal to $[K : \mathbb{Q}]$, we apply Theorem 2.4, which gives a group homomorphism

$$\psi\colon G_{K/\mathbb{Q}} \to \mathrm{Aut}(C\ell(K))$$

https://doi.org/10.4153/S0008439526101775 Published online by Cambridge University Press

such that

$$G_{H(K)/\mathbb{Q}} \simeq C\ell(K) \rtimes_{\psi} G_{K/\mathbb{Q}}. \tag{5.1}$$

Since $C\ell(K)$ is of order q, a prime, we have that the order of $\mathrm{Aut}(C\ell(K))$ is $q-1$. The assumption that $\gcd(q-1, \frac{p^{e-1}(p-1)}{2}) = 1$ implies that ψ is a trivial homomorphism. Consequently, the semidirect product becomes a direct product:

$$C\ell(K) \rtimes_{\psi} G_{K/\mathbb{Q}} \simeq C\ell(K) \times G_{K/\mathbb{Q}}. \tag{5.2}$$

Since both $G_{K/\mathbb{Q}}$ and $C\ell(K)$ are abelian groups, it follows that $C\ell(K) \times G_{K/\mathbb{Q}}$ is also abelian. So, by (5.1) and (5.2), we see that $G_{H(K)/\mathbb{Q}}$ is abelian, and hence the Hilbert class field $H(K)/\mathbb{Q}$ is an abelian extension.

Therefore, there exists a positive integer v such that $H(K) \subseteq \mathbb{Q}(\zeta_v)$. Since the extension $H(K)/\mathbb{Q}(\zeta_{p^e})^+$ is unramified at all primes of $\mathbb{Q}(\zeta_{p^e})^+$ and satisfies

$$\mathbb{Q}(\zeta_{p^e})^+ \subset H(K) \subseteq \mathbb{Q}(\zeta_v),$$

by Proposition 5.1, it follows that $H(K) = \mathbb{Q}(\zeta_{p^e})^+$. Hence, $h_K = 1$, leading to a contradiction. This completes the proof. ∎

Remark 5.4 Using Corollary 1.5 and Proposition 5.3, we observe the following: if there exist infinitely many positive integers $n \not\equiv 2 \pmod 4$ such that the class number of $\mathbb{Q}(\zeta_n)^+$ is 2, then we obtain infinitely many primes p for which the class number of $\mathbb{Q}(\zeta_p)^+$ is 1. Determining the density of such primes p for which $h_{\mathbb{Q}(\zeta_p)^+} = 1$ remains an open problem. Therefore, exploring whether there exist infinitely many positive integers n with $h_{\mathbb{Q}(\zeta_n)^+} = 2$ might be a promising direction for further research.

Along similar lines to the proof of Theorem 1.4, one can establish the following result.

Theorem 5.5 *Let p be a prime and $e \geq 1$ be an integer. Then, the class number of $\mathbb{Q}(\zeta_{p^e})$ cannot be equal to 2.*

Remark 5.6 Using the list in (1.1), Proposition 2.8, and Theorem 5.5, we observe the following: for any positive integer $n \not\equiv 2 \pmod 4$, if $h_{\mathbb{Q}(\zeta_n)} = 2$, then every prime divisor p of n must lie in the set $\{2, 3, 5, 7, 11, 13, 17, 19\}$. By applying Theorem 1.1, Theorems 2.5–2.7, Proposition 2.9, and Theorem 5.5, along with the known data regarding the class numbers of cyclotomic fields $\mathbb{Q}(\zeta_v)$ for $1 \leq v \leq 160$ and performing some computations, one can conclude that

$$h_{\mathbb{Q}(\zeta_n)} = 2 \quad \text{if and only if} \quad n = 39 \text{ or } n = 56.$$

This conclusion was also obtained by Masley in [17].

6 Proof of Theorem 1.6

We first state two results which will be used in the proof of Theorem 1.6. The following proposition is taken from [3, Proposition 3.2].

https://doi.org/10.4153/S0008439526101775 Published online by Cambridge University Press

Theorem 6.1 *Let L/K be a Galois extension of number fields of prime degree p. Suppose w is the number of infinite primes of K that are unramified in L. Then, the order of the first cohomology group $H^1(G_{L/K}, \mathcal{O}_L^\times)$ divides p^{w+1}.*

The next result describes the size of the first cohomology group (cf. [5, Proposition 4.4]).

Theorem 6.2 *Let L/K be a Galois extension of number fields. Then*

$$|\mathcal{P}o(L/K)| = \frac{h_K \times \prod_{\mathfrak{p}} e(\mathfrak{p})}{|H^1(G_{L/K}, \mathcal{O}_L^\times)|},$$

where the product runs over all the finite prime ideals $\mathfrak{p}$ of K that ramify in L, and $e(\mathfrak{p})$ denotes the ramification index of $\mathfrak{p}$ in the extension L/K.

Proof (Theorem 1.6) Applying Proposition 2.6, we obtain

$$\prod_{\mathfrak{p}} e(\mathfrak{p}) = \begin{cases} 2 & \text{if } n \text{ is a prime power,} \\ 1 & \text{otherwise,} \end{cases}$$

where the product runs over all finite prime ideals $\mathfrak{p}$ of K that ramify in L, and $e(\mathfrak{p})$ denotes the ramification index of $\mathfrak{p}$ in the extension L/K.

Since L/K is a Galois extension of degree 2 and all infinite primes of K ramify in L, Theorem 6.1 implies that $|H^1(G_{L/K}, \mathcal{O}_L^\times)|$ divides 2. Thus, by Theorem 6.2, we conclude

$$h_K \leq \begin{cases} |\mathcal{P}o(L/K)| & \text{if } n \text{ is a prime power,} \\ 2 \cdot |\mathcal{P}o(L/K)| & \text{otherwise.} \end{cases} \tag{6.1}$$

Now assume that $h_K = 1$. We aim to show that the relative Pólya group $\mathcal{P}o(L/K)$ is trivial.

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ with residue degree f in the extension L/K. Define

$$\prod_{\mathfrak{p}^f}(L/K) = \prod_{\substack{\mathfrak{P} \in \mathrm{Max}(\mathcal{O}_L) \\ \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}}} \mathfrak{P},$$

where $\mathrm{Max}(\mathcal{O}_L)$ denotes the set of all maximal ideals (i.e., prime ideals) of $\mathcal{O}_L$. Since L/K is a Galois extension of degree 2, it follows that the residue degree f is either 1 or 2.

Case I: Suppose $n = p^a$ is a prime power. Then, by Proposition 2.6, we have

$$\prod_{\mathfrak{p}^f}(L/K) = \begin{cases} \mathfrak{P} & \text{if } p \in \mathfrak{p} \text{ and } f = 1, \\ \mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2 & \text{if } p \notin \mathfrak{p} \text{ and } f = 1, \\ \mathfrak{p}\mathcal{O}_L & \text{if } p \notin \mathfrak{p} \text{ and } f = 2. \end{cases}$$

Case II: Suppose n is not a prime power. Again, by Proposition 2.6, we have

$$\prod_{\mathfrak{p}^f}(L/K) = \begin{cases} \mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2 & \text{if } f = 1, \\ \mathfrak{p}\mathcal{O}_L & \text{if } f = 2. \end{cases}$$

https://doi.org/10.4153/S0008439526101775 Published online by Cambridge University Press

Since $h_K = 1$, the ideal $\mathfrak{p}\mathcal{O}_L$ is principal in $\mathcal{O}_L$ for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Also, $\mathfrak{P}$ is principal due to L being a Pólya field. Using these facts in both cases, it follows that $\prod_{\mathfrak{p}^f}(L/K)$ is a principal ideal of $\mathcal{O}_L$ for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, but the relative Pólya group $\mathcal{P}o(L/K)$ is generated by the ideal classes containing the ideals of the form $\prod_{\mathfrak{p}^f}(L/K)$. Therefore, we see that the group $\mathcal{P}o(L/K)$ is trivial.

Now assume that $\mathcal{P}o(L/K)$ is trivial and the class number h_L is odd. Using inequality (6.1), we deduce that $h_K \in \{1, 2\}$. However, since h_K divides h_L and h_L is odd, h_K must be odd. Hence, $h_K \neq 2$, so $h_K = 1$. This completes the proof. ∎

References

[1] N. C. Ankeny and S. Chowla, *On the divisibility of the class number of quadratic fields*. Pacific J. Math. **5**(1955), 321–324.
[2] N. C. Ankeny, S. Chowla, and H. Hasse, *On the class number of the maximal real subfield of a cyclotomic field*. J. Reine Angew. Math. **217**(1965), 217–220.
[3] A. Brumer and M. Rosen, *Class number and ramification in number fields*. Nagoya Math. J. **23**(1963), 97–101.
[4] D. Byeon, *Real quadratic fields with odd class number divisible by* 3. Ramanujan J. **62**(2023), 755–759.
[5] J.-L. Chabert, *From Pólya fields to Pólya groups (I): Galois extensions*. J. Number Theory **203**(2019), 360–375.
[6] K. Chakraborty and A. Hoque, *Pell-type equations and class number of the maximal real subfield of a cyclotomic field*. Ramanujan J. **46**(2018), 727–742.
[7] G. Cornell, *A note on the class group of composita*. J. Number Theory **39**(1991), 1–4.
[8] G. Cornell and L. C. Washington, *Class numbers of cyclotomic fields*. J. Number Theory **21**(1985), 260–274.
[9] R. Gold, *Hilbert class fields and split extensions*. Illinois J. Math. **21**(1977), 66–69.
[10] A. Hoque and H. K. Saikia, *On the class number of the maximal real subfield of a cyclotomic field*. Quaest. Math. **39**(2016), 889–894.
[11] H. Ichimura, *Note on the class numbers of certain real quadratic fields*. Abh. Math. Sem. Univ. Hamburg **73**(2003), 281–288.
[12] M. Ishida, *The genus fields of algebraic number fields*, Lecture Notes in Mathematics, 555, Springer-Verlag, Berlin–Heidelberg, 1976.
[13] S. D. Lang, *Note on the class number of the maximal real subfield of a cyclotomic field*. J. Reine Angew. Math. **290**(1977), 70–72.
[14] H. W. Leopoldt, *Zur Geschlechtertheorie in abelschen Zahlkörpern*. Math. Nachr. **9**(1953), 351–362.
[15] S. R. Louboutin, *On the divisibility of the class number of imaginary quadratic number fields*. Proc. Amer. Math. Soc. **137**(2009), 4025–4028.
[16] J. M. Masley, *On the class number of cyclotomic fields*. Ph.D. Thesis, Princeton University, 1972.
[17] J. M. Masley, *Solution of the class number two problem for cyclotomic fields*. Invent. Math. **28**(1975), 243–244.
[18] J. M. Masley, *Solution of small class number problems for cyclotomic fields*. Compos. Math. **33**(1976), 179–186.
[19] J. M. Masley, *Class numbers of real cyclic number fields with small conductor*. Compos. Math. **37**(1978), 297–319.
[20] J. M. Masley and H. L. Montgomery, *Cyclotomic fields with unique factorization*. J. Reine Angew. Math. **286**–287(1976), 248–256.
[21] J.-F. Mestre, *Corps quadratiques dont le* 5*-rang du groupe des classes est* ≥ 3. C. R. Acad. Sci. Paris Sér. I Math. **315**(1992), 371–374.
[22] M. Mishra, R. Schoof, and L. C. Washington, *Class groups of real cyclotomic fields*. Monatsh. Math. **195**(2021), no. 3, 489–496.
[23] M. R. Murty, *Exponents of class groups of quadratic fields*. In: Topics in number theory, S. D. Ahlgren, G. E. Andrews, and K. Ono (eds.), Mathematics and its Applications, 467, Kluwer Academic Publishers, Dordrecht, 1999, pp. 229–239.
[24] H. Osada, *Note on the class number of the maximal real subfield of a cyclotomic field*. Manuscripta Math. **58**(1987), 215–227.

https://doi.org/10.4153/S0008439526101775 Published online by Cambridge University Press

[25] M. K. Ram, *On the class number of the maximal real subfields of a family of cyclotomic fields*. Czechoslovak Math. J. **73**(2023), 937–940.
[26] M. K. Ram, *Class groups of large ranks in biquadratic fields*. Czechoslovak Math. J. **74**(2024), 429–436.
[27] M. K. Ram, *Determination of class numbers of imaginary cyclic quartic number fields and cyclotomic fields*. Ramanujan J. **67**(2025).
[28] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*. J. London Math. Soc. **61**(2000), 681–690.
[29] H. Takeuchi, *On the class number of the maximal real subfield of a cyclotomic field*. Canad. J. Math. **33**(1981), 55–58.
[30] K. Uchida, *Class numbers of cubic cyclic fields*. J. Math. Soc. Japan **26**(1974), 447–453.
[31] L. C. Washington, *Introduction to cyclotomic fields*. 2nd ed., Springer-Verlag, New York, 1991.
[32] I. Yamaguchi, *On the class number of the maximal real subfield of a cyclotomic field*. J. Reine Angew. Math. **272**(1974), 217–220.
[33] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*. Osaka J. Math. **7**(1970), 57–76.
[34] A. Yokoyama, *On class numbers of finite algebraic number fields*. Tohoku Math. J. **17**(1965), 349–357.

Indian Institute of Technology (IIT) Madras, India
e-mail: anujjakhar@iitm.ac.in maheshkumarram621@gmail.com

https://doi.org/10.4153/S0008439526101775 Published online by Cambridge University Press