Czechoslovak Mathematical Journal

Mahesh Kumar Ram

Class groups of large ranks in biquadratic fields

Czechoslovak Mathematical Journal, Vol. 74 (2024), No. 2, 429–436

Persistent URL: http://dml.cz/dmlcz/152450

Czechoslovak Mathematical Journal, 74 (149) (2024), 429–436

CLASS GROUPS OF LARGE RANKS IN BIQUADRATIC FIELDS

Mahesh Kumar Ram, Bhubaneswar

Received August 4, 2023. Published online April 15, 2024.

Abstract. For any integer $n > 1$, we provide a parametric family of biquadratic fields with class groups having n-rank at least 2. Moreover, in some cases, the n-rank is bigger than 4.

Keywords: ideal class group; biquadratic field

MSC 2020: 11R11, 11R29

1. Introduction

For any number field K, we use notations $Cl(K)$, h_K, D_K and $H(K)$ to denote the class group, class number, discriminant and the Hilbert class field of K, respectively. We employ the symbol $\mathrm{Gal}(K/F)$ to denote the Galois group of a Galois extension K/F of number fields. For any group G and integer $n > 1$, we define $G^n = \{a^n \colon a \in G\}$.

Understanding the class groups of number fields is at the forefront of research in algebraic number theory. However, barring the cases of fields of small degree and small discriminants, it is extremely difficult to give precise information on the class group of a number field K.

An active trend of research is to understand the behaviour of class groups of number fields coming from certain families. For example, if $d > 1$ and G is a finite abelian group, then it is natural to ask if there are infinitely many number fields K of degree d such that the class group $Cl(K)$ contains a subgroup isomorphic to G. Cohen-Lenstra and Cohen-Martinet heuristics provide some conjectural answers in this regard, see [3], [4]. These conjectures have not witnessed much progress. For any integer $n > 1$, there are many beautiful works showing $\mathbb{Z}/n\mathbb{Z}$ as subgroups of class groups of lots of fields among fields of a given degree d, see [1], [10], [11], [12], [15], [16].

The author expresses gratitude to the National Institute of Science Education and Research, Bhubaneswar, India, for supporting the postdoctoral research.

DOI: 10.21136/CMJ.2024.0356-23

However, for an arbitrary integer $r > 1$, it is difficult to show the existence of many number fields of degree d whose class group contains r-copies of $\mathbb{Z}/n\mathbb{Z}$. We refer the reader to consult [6] to know the recent status in this regard. The recent article (see [5]) improves upon the records mentioned in [6].

We prove the following theorem.

Theorem 1.1. *Let $K_1/\mathbb{Q}$ be a Galois extension of number fields, and let $K_2/\mathbb{Q}$ be any extension of number fields such that D_{K_1} is relatively prime to D_{K_2}. If the n-rank of $Cl(K_1)$ and $Cl(K_2)$ is r_1 and r_2, respectively, then the n-rank of the class group of K_1K_2 is at least $r_1 + r_2$.*

Note that Theorem 1.1 can be used to produce many more biquadratic fields whose class group has a large n-rank for any integer $n > 1$. We use Theorem 1.1 to prove the following result.

Corollary 1.2. *Let $u \geqslant 3$ be an odd integer such that u has a prime factor congruent to 3 modulo 4. Let $n > 1$ be an integer and $a > 1$ be an odd integer. Assume that $d_{u,n}$ and $d'_{a,n}$ are the square-free parts of $1-4u^n$ and $a^{2n}+4$, respectively. If $a = 17b$ and $u = a^2$, where $b > 1$ is an integer having a prime factor congruent to 3 modulo 4, then the class group of $L = \mathbb{Q}(\sqrt{d_{u,n}}, \sqrt{d'_{a,n}})$ has n-rank at least 2.*

Now, we use an idea of [9] to show that using quadratic fields of large rank class groups we can obtain biquadratic fields with class groups of even larger rank. More precisely, we prove the following theorem.

Theorem 1.3. *Let $n > 1$ be an odd integer and p, q be distinct odd primes such that $p \equiv 3 \pmod 4$ and $q^2 < p^n$. Assume that $d_{q,p,n}$ is the square-free part of $q^2 - p^n$ and $q \not\equiv \pm 1 \pmod{|d_{q,p,n}|}$. Suppose $K_{q,p,n} = \mathbb{Q}(\sqrt{q^2 - p^n}) = \mathbb{Q}(\sqrt{d_{q,p,n}})$ and $K_{u,n} = \mathbb{Q}(\sqrt{d_{u,n}})$, where $d_{u,n}$ is the square-free part of $1-4u^n$ for any integer $u \geqslant 2$. Then the class group of $L = K_{q,p,n}K_{u,n}$ has n-rank at least 2.*

Note that using Theorem 1.1, we can show that Theorem 1.3 holds for any odd integer $n > 1$ if the discriminants of $K_{q,p,n}$ and $K_{u,n}$ are relatively prime. Analogously to Theorem 1.3, we prove the following theorem.

Theorem 1.4. *Let $n > 1$ and $a > 1$ be two odd integers, and let $u \geqslant 2$ be any integer. Assume that $d_{u,n}$ and $d'_{a,n}$ are the square-free parts of $1 - 4u^n$ and $a^{2n} + 4$, respectively. Consider the fields $K_{u,n} = \mathbb{Q}(\sqrt{d_{u,n}})$ and $K'_{a,n} = \mathbb{Q}(\sqrt{d'_{a,n}})$. Then the class group of $L = K_{u,a}K'_{a,n} = \mathbb{Q}(\sqrt{d_{u,n}}, \sqrt{d'_{a,n}})$ has n-rank at least 2.*

Note that for the family of biquadratic fields in Theorem 1.4, the result of Nakano (see [12]) only guarantees a copy of $\mathbb{Z}/n\mathbb{Z}$ in the class group. In Section 4, we provide some examples of Theorems 1.3 and 1.4 with the help of SageMath.

In [13], Schoof provided a quadratic field whose class group has 5-rank 4. As far as we know, this is the only known example of a quadratic field in which 5-rank of the class group is 4. We use this quadratic field to find a large 5-rank in biquadratic fields. More precisely, we prove the following theorem.

Theorem 1.5. *Let $K = \mathbb{Q}(\sqrt{-258559351511807})$ and $K_u = \mathbb{Q}(\sqrt{1-4u^5})$ be two number fields, where $u \geqslant 2$ is an integer. Suppose $L = KK_u$. Then*

(i) *if $u \equiv 2 \pmod 3$, then the class group of L has 5-rank at least 5,*

(ii) *if $u \not\equiv 2 \pmod 3$, then the class group of L has 5-rank at least 5 except for finitely many values of u.*

We end the section with the remark that it is possible to obtain class groups of larger n-rank by taking more compositums.

2. Preliminaries

We begin this section with a result of Louboutin, see [8].

Theorem 2.1.

(1) *If $n > 1$ is an odd integer, then for any integer $u \geqslant 2$ the ideal class groups of the imaginary quadratic fields $\mathbb{Q}(\sqrt{1-4u^n})$ contain an element of order n.*

(2) *Let $u \geqslant 3$ be an odd integer such that u has a prime factor congruent to 3 modulo 4. Then for any integer $n > 1$, the ideal class groups of the imaginary quadratic fields $\mathbb{Q}(\sqrt{1-4u^n})$ contain an element of order n.*

Now, we record the following theorem of Ichimura, see [7].

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

The next theorem we record from [2] is the following result.

Theorem 2.3 ([2])**.** *Let $n \geqslant 3$ be an odd integer and p, q be distinct odd primes such that $q^2 < p^n$. Suppose d is the square-free part of $q^2 - p^n$ and $q \not\equiv \pm 1 \pmod{|d|}$. Moreover, we assume $p^{n/3} \neq \frac{1}{3}(2q+1), \frac{1}{3}(q^2+2)$ whenever both $d \equiv 1 \pmod 4$ and $3 \mid n$. Then the class groups of $K_{q,p,n} = \mathbb{Q}(\sqrt{q^2-p^n}) = \mathbb{Q}(\sqrt{d})$ contain an element of order n.*

Let K be any number field and S be a finite set of valuations on K containing all the archimedean valuations. Then the set

$$R_S = \{\alpha \in K\colon\ \nu(\alpha) \geqslant 0\ \forall\, \nu \notin S\}$$

is said to be the set of S-integers of K.

Now we state Siegel's theorem (see [14], Chapter IX, Theorem 4.3), which helps us in proving the second part of Theorem 1.5.

Theorem 2.4. *Let K be a number field and $f(x) \in K[x]$ be a polynomial of degree not less than 3 with distinct roots in the algebraic closure $\overline{K}$ of K. Then the equation $y^2 = f(x)$ has only finitely many solutions (x, y) in $R_S \times R_S$.*

One can readily obtain the following lemma.

Lemma 2.5. *For any number field K, the set of S-integers R_S of K contains $\mathbb{Z}$.*

We recall a lemma of Mishra, Schoof and Washington, see [9].

Lemma 2.6. *Let F_1 and F_2 be Galois extensions of $\mathbb{Q}$ with $F_1 \cap F_2 = \mathbb{Q}$. Suppose $m = [F_1 : \mathbb{Q}]$ and $n = [F_2 : \mathbb{Q}]$. Then $Cl(F_1F_2)$ contains a subgroup isomorphic to $Cl(F_1)^n \oplus Cl(F_2)^m$.*

We end this section by mentioning the following elementary group theoretic lemma.

Lemma 2.7. *If G is an abelian group of odd order, then $G^2 = G$, where $G^2 = \{g^2 \colon g \in G\}$.*

3. Proofs

We begin this section with the following proposition.

Proposition 3.1. *Let $f(x) = (1 - 4x^n)/D$ be a polynomial over $\mathbb{Q}$, where $n \geqslant 3$ and $D \neq 0$ are integers. Then the equation*

$$y^2 = f(x)$$

has finitely many solutions (x, y) in $\mathbb{Z} \times \mathbb{Z}$.

P r o o f. Clearly, $f(x) \in \mathbb{Q}(x)$ and the degree of $f(x)$ is greater than or equal to 3. As $f(x)$ has no multiple roots in the algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$, Theorem 2.4 and Lemma 2.5 imply that the equation $y^2 = f(x)$ has finitely many solutions in $\mathbb{Z} \times \mathbb{Z}$. □

Now we are in a position to prove all the results of this article.

P r o o f of Theorem 1.1. Let $L = H(K_1)H(K_2)$ and $K = K_1K_2$. Since $H(K_1)$ is the Hilbert class fields of K_1, $H(K_1)/K_1$ is abelian and is unramified at all primes of K_1. Similarly, $H(K_2)/K_2$ is abelian and is unramified at all primes of K_2. From this, we obtain that L/K is abelian and is unramified at all primes of K. From class field theory, this shows that $Cl(K)$ has a subgroup isomorphic to $\mathrm{Gal}(L/K)$. Now, to prove the claim of the theorem, it suffices to show that $\mathrm{Gal}(L/K) \simeq Cl(K_1) \oplus Cl(K_2)$.

Since $H(K_1)/\mathbb{Q}$ is a Galois extension and $H(K_2)/\mathbb{Q}$ is a finite extension, it follows that

$$[L : \mathbb{Q}] = \frac{[H(K_1) : \mathbb{Q}][H(K_2) : \mathbb{Q}]}{[H(K_1) \cap H(K_2) : \mathbb{Q}]}. \tag{3.1}$$

We also have

$$[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}]. \tag{3.2}$$

We know that $Cl(K_1) \simeq \mathrm{Gal}(H(K_1)/K_1)$. Using this, we get $[H(K_1) : \mathbb{Q}] = h_{K_1}[K_1 : \mathbb{Q}]$. Similarly, we have $[H(K_2) : \mathbb{Q}] = h_{K_2}[K_2 : \mathbb{Q}]$. As D_{K_1} is relatively prime to D_{K_2}, it implies that $H(K_1) \cap H(K_2) = \mathbb{Q}$. Substituting these in (3.1), we obtain

$$[L : \mathbb{Q}] = h_{K_1}h_{K_2}[K_1 : \mathbb{Q}][K_2 : \mathbb{Q}]. \tag{3.3}$$

One can easily obtain

$$[K : \mathbb{Q}] = [K_1 : \mathbb{Q}][K_2 : \mathbb{Q}].$$

Thus, (3.2) becomes

$$[L : \mathbb{Q}] = [L : K][K_1 : \mathbb{Q}][K_2 : \mathbb{Q}]. \tag{3.4}$$

From (3.3) and (3.4), we get that $[L : K] = h_{K_1}h_{K_2}$. Define a map

$$\Psi\colon\ \mathrm{Gal}(L/K) \to \mathrm{Gal}(H(K_1)/K_1) \oplus \mathrm{Gal}(H(K_2)/K_2)$$

by

$$\sigma \mapsto (\sigma|_{H(K_1)}, \sigma|_{H(K_2)}).$$

It is immediately evident that Ψ is an injective group homomorphism. We have established that $[L : K] = h_{K_1}h_{K_2}$. This proves that Ψ is surjective. Thus, $\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(H(K_1)/K_1) \oplus \mathrm{Gal}(H(K_2)/K_2)$. This completes the proof. □

Along the same lines, as we have proved Theorem 1.1, one can prove the next result.

Theorem 3.2. *Let $K_1/\mathbb{Q}$ and $K_2/\mathbb{Q}$ be Galois extensions of number fields. Assume that $[K_1 : \mathbb{Q}]$ and $[K_2 : \mathbb{Q}]$ are relatively prime. If the n-rank of $Cl(K_1)$ and $Cl(K_2)$ is r_1 and r_2, respectively, then the n-rank of the class group of K_1K_2 is at least $r_1 + r_2$.*

P r o o f of Corollary 1.2. Theorem 2.1 implies that the class group of the field $\mathbb{Q}(\sqrt{d_{u,n}})$ has n-rank at least 1, and Theorem 2.2 gives that the n-rank of the class group of the field $\mathbb{Q}(\sqrt{d'_{a,n}})$ is at least 1. Using the hypothesis $a = 17b$ and $u = a^2$, where $b > 1$ is an integer having a prime factor congruent to 3 modulo 4, we find that $d_{u,n}$ and $d'_{a,n}$ are relatively prime, and we note that $d_{u,n} \equiv 1 \pmod 4$. Consequently, we conclude that the discriminants of $\mathbb{Q}(\sqrt{d_{u,n}})$ and $\mathbb{Q}(\sqrt{d'_{a,n}})$ are relatively prime. Applying Theorem 1.1 for $\mathbb{Q}(\sqrt{d_{u,n}})$ and $\mathbb{Q}(\sqrt{d'_{a,n}})$, we obtain the required result. This completes the proof. □

P r o o f of Theorem 1.3. Since $[K_{u,n} : \mathbb{Q}] = 2$ and $[K_{q,p,n} : \mathbb{Q}] = 2$, it implies that $K_{u,n}$ and $K_{q,p,n}$ are Galois extensions of $\mathbb{Q}$. It follows from $1-4u^n \equiv 1 \pmod 4$ and $q^2-p^n \equiv 2 \pmod 4$ that $d_{u,n} \equiv 1 \pmod 4$ and $d_{q,p,n} \equiv 2 \pmod 4$, respectively. This shows that $K_{u,n} \cap K_{q,p,n} = \mathbb{Q}$. Thus, Lemma 2.6 implies that $Cl(L)$ contains a subgroup isomorphic to $Cl(K_{u,n})^2 \oplus Cl(K_{q,p,n})^2$.

From Theorems 2.1 and 2.3, we find that $Cl(K_{u,n})$ and $Cl(K_{q,p,n})$ contain an element of order n, respectively. Using Lemma 2.7, we obtain that $Cl(K_{u,n})^2$ and $Cl(K_{q,p,n})^2$ also contain an element of order n. Consequently, $Cl(K_{u,n})^2 \oplus Cl(K_{q,p,n})^2$ contains a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. Thus, $Cl(L)$ has a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. This completes the proof of Theorem 1.3. □

P r o o f of Theorem 1.4. Since $K_{u,n}$ and $K'_{a,n}$ are quadratic number fields, they are Galois over $\mathbb{Q}$. As $K_{u,n}$ is an imaginary quadratic field and $K'_{a,n}$ is a real quadratic field, it follows that $K_{u,n} \cap K'_{a,n} = \mathbb{Q}$. From Lemma 2.6, the class group $Cl(L)$ has a subgroup isomorphic to $Cl(K_{u,n})^2 \oplus Cl(K'_{a,n})^2$.

Using Theorems 2.1, 2.2 and Lemma 2.7, we obtain that each group $Cl(K_{u,n})^2$ and $Cl(K'_{a,n})^2$ has an element of order n. Thus, $Cl(K_{u,n})^2 \oplus Cl(K'_{a,n})^2$ contains a subgroup isomorphic to $\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. This proves the claim of Theorem 1.4. □

P r o o f of Theorem 1.5. (i) As $[K : \mathbb{Q}] = 2$ and $[K_u : \mathbb{Q}] = 2$, K and K_u are Galois over $\mathbb{Q}$. From $-258559351511807 \equiv 1 \pmod 3$ and $1 - 4u^5 \equiv 2 \pmod 3$, we have $K \cap K_u = \mathbb{Q}$. Thus, by Lemma 2.6, $Cl(L)$ contains a subgroup isomorphic to $Cl(K)^2 \oplus Cl(K_u)^2$. Since $Cl(K)$ contains a subgroup H isomorphic to $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ (see [13]), using Lemma 2.7 we get that $Cl(K)^2$ also contains H. Further, from Theorem 2.1, $Cl(K_u)$ contains an element of order 5. Lemma 2.7

implies that $Cl(K_u)^2$ has an element of order 5. Thus, we find that $Cl(K)^2 \oplus Cl(K_u)^2$ has a subgroup isomorphic to $H \oplus \mathbb{Z}/5\mathbb{Z}$. This completes the proof of the first part of Theorem 1.5.

(ii) It follows from Proposition 3.1 that $K \cap K_u = \mathbb{Q}$ for all values of u except for finitely many values of u. Now the rest of the proof will go along the same lines as the proof of the first part. □

4. Some computations and concluding remarks

Now, we list some quadratic fields whose class group contains at least 2-copies of $\mathbb{Z}/3\mathbb{Z}$ with the help of SageMath.

u	$d_{u,3}$	3-rank
131	-8992363	3
305	-113490499	3
395	-246519499	3
478	-436861407	3
587	-809048011	3
865	-2588858499	3
902	-2935483231	3
917	-3084380851	3
998	-3976047967	3
1013	-4158036787	3

Table 1. Let $d_{u,3}$ be the square-free part of $1 - 4u^3$.

q	p	$d_{q,p,3}$	3-rank
3	107	-1225034	2
3	127	-2048374	2
3	331	-36264682	2
3	379	-54439930	2
3	683	-318611978	3
5	43	-79482	2
5	71	-357886	2
7	23	-12118	2
7	71	-387862	2
7	103	-1092678	2

Table 2. Let $d_{q,p,3}$ be the square-free part of $q^2 - p^3$.

Now we apply Theorem 1.3 for the values of Table 1 and Table 2, we obtain 100 biquadratic fields L whose class groups having 3-rank at least 5.

a	$d'_{a,3}$	3-rank
67	90458382173	3
83	326940373373	3
99	941480149405	3
119	2839760855285	3
223	122978496247493	3
257	288136807515653	3

Table 3. Let $d'_{a,3}$ be the square-free part of $a^6 + 4$.

Now we apply Theorem 1.4 for the values of Table 1 and Table 3, we obtain 60 biquadratic fields L whose class groups have 3-rank at least 6.

Let K_1 and K_2 be two distinct quadratic number fields and let $L = K_1K_2$. Then L contains a quadratic number field K_3 such that $K_3 \neq K_1$, $K_3 \neq K_2$ and $L = K_1K_3 = K_2K_3 = K_1K_2K_3$. Further, the class group of L contains a subgroup isomorphic to $Cl(K_1)^2 \oplus Cl(K_2)^2 \oplus Cl(K_3)^2$. So, if the class group of each K_i for $i = 1, 2, 3$ contains at least a copy of $\mathbb{Z}/n\mathbb{Z}$, where $n > 1$ is odd, then the class group of L has n-rank at least 3.

Acknowledgements. We express our gratitude to the anonymous referee for a thorough reading of the article and making many suggestions to improve the overall presentation considerably.

References

[1] *N. C. Ankeny, S. Chowla*: On the divisibility of the class number of quadratic fields. Pac. J. Math. *5* (1955), 321–324. zbl MR doi

[2] *K. Chakraborty, A. Hoque, Y. Kishi, P. P. Pandey*: Divisibility of the class numbers of imaginary quadratic fields. J. Number Theory *185* (2018), 339–348. zbl MR doi

[3] *H. Cohen, H. W. Lenstra, Jr.*: Heuristics on class groups of number fields. Number Theory. Lecture Notes in Mathematics 1068. Springer, Berlin, 1984, pp. 33–62. zbl MR doi

[4] *H. Cohen, J. Martinet*: Heuristic study of the class groups of number fields. J. Reine Angew. Math. *404* (1990), 39–76. (In French.) zbl MR doi

[5] *J. Gillibert, P. Gillibert*: Galois covers of $\mathbb{P}^1$ and number fields with large class groups. Int. J. Number Theory *18* (2022), 1261–1288. zbl MR doi

[6] *J. Gillibert, A. Levin*: A geometric approach to large class groups: A survey. Class Groups of Number Fields and Related Topics. Springer, Singapore, 2020, pp. 1–15. zbl MR doi

[7] *H. Ichimura*: Note on the class numbers of certain real quadratic fields. Abh. Math. Sem. Univ. Hamb. *73* (2003), 281–288. zbl MR doi

[8] *S. R. Louboutin*: On the divisibility of the class number of imaginary quadratic number fields. Proc. Am. Math. Soc. *137* (2009), 4025–4028. zbl MR doi

[9] *M. Mishra, R. Schoof, L. C. Washington*: Class groups of real cyclotomic fields. Monatsh. Math. *195* (2021), 489–496. zbl MR doi

[10] *M. R. Murty*: Exponents of class groups of quadratic fields. Topics in Number Theory. Mathematics and its Applications 467. Kluwer Academic, Dordrecht, 1999, pp. 229–239. zbl MR doi

[11] *T. Nagell*: Über die Klassenzahl imaginär-quadratischer Zahlkörper. Abh. Math. Semin. Univ. Hamb. *1* (1922), 140–150. (In German.) zbl MR doi

[12] *S. Nakano*: On ideal class groups of algebraic number fields. J. Reine Angew. Math. *358* (1985), 61–75. zbl MR doi

[13] *R. J. Schoof*: Class group of complex quadratic fields. Math. Comput. *41* (1983), 295–302. zbl MR doi

[14] *J. H. Silverman*: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics 106. Springer, Dordrecht, 2009. zbl MR doi

[15] *K. Soundararajan*: Divisibility of class numbers of imaginary quadratic fields. J. Lond. Math. Soc., II. Ser. *61* (2000), 681–690. zbl MR doi

Author's address: Mahesh Kumar Ram, National Institute of Science Education and Research, Jatni, Bhubaneswar, Odisha-752050, India, e-mail: `maheshkumarram621@gmail.com`.