2-CLASS FIELDS TOWERS OF
SOME IMAGINARY Biquadratic NUMBER FIELDS

Abdelmalek Azizi\textsuperscript{1}, Mohammed Rezzougui\textsuperscript{2}§
\textsuperscript{1,2}Department of Mathematics
Faculty of Science
Mohamed First University
Oujda, MOROCCO

Abstract: Let $K = \mathbb{Q}(\sqrt{d}, i)$, where $d$ is a positive square free integer and $i = \sqrt{-1}$. Our goal is to determine some fields $K$ have an infinite $S$-decomposing 2-class field tower, $S$ is a finite set of prime ideals of $K$.

AMS Subject Classification: 11R27, 11R37
Key Words: biquadratic fields, class group, capitulation, Hilbert class fields

1. Introduction

Let $K$ be a number field and let $p$ be a prime number. We denote by $K_p^{(1)}$ the $p$-class field of $K$, and for a positive integer $n$, $K_p^{(n+1)}$ the $p$-class field of $K_p^{(n)}$. The Hilbert $p$-class field tower is the sequence of fields:

$$K = K_p^{(0)} \subseteq K_p^{(1)} \subseteq K_p^{(2)} \subseteq \cdots \subseteq K_p^{(n)} \subseteq K_p^{(n+1)} \subseteq \cdots$$

If there exists $n \in \mathbb{N}$ such that $K_p^{(n-1)} \neq K_p^{(n)}$ and $K_p^{(n)} = K_p^{(n+1)}$, then we say that the $p$-class field tower is finite of length $n$, otherwise the tower is infinite.

Let $K$ be a number field and let $S$ be a finite set of prime ideals of $K$, the maximal abelian unramified $p$-extension of $K$ in which every prime ideal in $S$ splits completely, denoted $K_p^S$, is called the $S$-decomposing $p$-class field of $K$.

The $S$-decomposing $p$-class field tower of $K$ is the sequence of fields such that $K_0 = K$, $K_1 = K_p^S$ and for $n \geq 2$, $K_n = (K_{n-1})_p^{S_{n-1}}$, where $S_n$ is the set of prime ideals in $K_n$ lying above $S$. 

\textsuperscript{§}Correspondence author
Golod-Šafarevič theory gives a sufficient condition for the infinitude of the $S$-decomposing $p$-class field tower of some number field based on lower bounds on the $p$-rank of the ideal $S$-class group.

In this paper, we recall some definitions and theorems for extensions of number fields, and we give a sufficient condition for imaginary biquadratic extensions to have infinite $S$-decomposing 2-class field tower.

2. Hilbert $p$-Class Field Tower

Let $K$ be a number field, and $\mathcal{O}_K$ be its ring of integers. Let $I_K$ denote the group of fractional ideals of $K$. Let $P_K$ denote the subgroup of $I_K$ formed by the principal ideals. The quotient $C_K = I_K/P_K$ is called the ideal class group of $K$. Let $S$ be a finite set of prime ideals of $K$, $\#S = s$ the cardinal number of the set $S$ and $s_0$ the number of principal prime ideals of $S$. In the following, we denote by $p$ a prime number.

**Theorem 1** ([1]). Let $I$ be a fractional ideal of $K$. there exists a unique factorization

$$I = \prod_{i=1}^{g} p_i^{\nu_{p_i}(I)},$$

where the $p_i$ are distinct prime ideals of $\mathcal{O}_K$ and $\nu_{p_i}(I) \in \mathbb{Z} \setminus \{0\}$. Furthermore, $I$ is an integral ideal if and only if all the $\nu_{p_i}(I)$ are positive. In particular $p_0 = \mathcal{O}_K$.

**Corollary 2** ([1]). Let $p$ be a prime ideal of $\mathcal{O}_K$. The function $\nu_p : K \to \mathbb{Z} \cup \{\infty\}$ defined by $\nu_p(x) = \nu_p(x\mathcal{O}_K)$, with the convention $\nu_p(0) = +\infty$, satisfies the following properties:

1. $\nu_p(x) = +\infty \iff x = 0$.
2. $\nu_p(xy) = \nu_p(x) + \nu_p(y)$ for all $x, y \in K$.
3. $\nu_p(x + y) \geq \min\{\nu_p(x), \nu_p(y)\}$ for all $x, y \in K$ (with equality if $\nu_p(x) \neq \nu_p(y)$)

**Definition 3.** The ring of $S$-integers of $K$, denoted by $\mathcal{O}_{K,S}$, is defined by

$$\mathcal{O}_{K,S} = \{ x \in K; \nu_p(x) \geq 0 \text{ for all } p \not\in S \}$$

The group of invertible elements of $\mathcal{O}_{K,S}$ is called the group of $S$-units of $K$, denoted by $E_{K,S}$, and we have

$$E_{K,S} = \{ x \in K; \nu_p(x) = 0 \text{ for all } p \not\in S \}.$$  

**Definition 4.** Let $I_{K,S}$ be the group of fractional ideals nondivisible by prime ideal of $S$. Let $P_{K,S}$ be the subgroup of principal ideals of $I_{K,S}$. The quotient $C_{K,S} = I_{K,S}/P_{K,S}$ is called the ideal $S$-class group of $K$. 
Proposition 5 ([4]). Let $I^S_K$ be the group of ideals generated by prime ideal in $S$ and $\Phi$ the group homomorphism from $I^S_K$ into $C_K$ defined by

$$\Phi : I^S_K \rightarrow C_K$$

$I \mapsto [I]$ then the ideal $S$-class group $C_{K,S}$ is isomorphic to the quotient group $C_K/\text{Im}\Phi$.

Proposition 6. Let $M$ be an $A$-module and $I$ an ideal of $A$. We have the isomorphisms of $A$-modules:

$$A \otimes M \simeq M$$

and

$$A/I \otimes M \simeq M/IM.$$ Moreover, $M/IM$ is an $A/I$-module.

Definition 7. Let $p$ be a prime ideal of a ring $A$. The $p$-rank of an $A$-module $M$ is the rank of the $A/p$-module $A/p \otimes M \simeq M/pM$.

Definition 8. Let $G$ be an abelian group, the $p$-rank of the $\mathbb{Z}$-module $G$ is the rank of the vector space over the field $\mathbb{F}_p$

$$\mathbb{F}_p \otimes G \simeq G/\mathbb{G}^p$$

and denoted by $d_p(G) = \text{p-rank}(G) = \dim_{\mathbb{F}_p}(G/\mathbb{G}^p)$, where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Definition 9. the $p$-rank of group $G$ is the dimension of $G/\mathbb{G}^p[G : G]$ as a vector space over the field $\mathbb{F}_p$ and we have

$$d_p(G) = \dim_{\mathbb{F}_p}(G^{ab}/p) = \dim_{\mathbb{F}_p}(G/\mathbb{G}^p[G : G])$$


Theorem 10. Let $G$ be an abelian group and $H$ a subgroup of $G$, then

$$d_p(G/H) + d_p(H) = d_p(G) + d_p(H \cap G^p/H^p).$$

Proof. We have a short exact sequence of vector space over the field $\mathbb{F}_p$

$$1 \rightarrow H/H \cap G^p \rightarrow G/G^p \rightarrow (G/H)/(G/H)^p \rightarrow 1$$

and the following commutative diagram

$$\begin{array}{ccc}
H & \rightarrow & H/H \cap G^p \\
\downarrow & & \downarrow \\
H/H^p & \rightarrow & \\
\end{array}$$

by the rank theorem, we have $d_p(G/H) + d_p(H) = d_p(G) + d_p(H \cap G^p/H^p)$. \qed
Theorem 11 ([3]). Let $G$ be a finite $p$-group, then
\[
\frac{1}{4}(d_p(G))^2 - d_p(G) < d_p(H_2(G, \mathbb{Z}))
\]
where $H_2(G, \mathbb{Z})$ the second homology group of the group $G$, with integer coefficients.

Lemma 12 ([4]). If
\[
d_p(C_{K,S}) \geq 2 + 2\sqrt{d_p(E_{K,S})} + 1,
\]
then $K$ has an infinite $S$-decomposing $p$-class field tower.

Lemma 13 ([1]). The $p$-rank of the group of $S$-units of $K$ equals
\[
d_p(E_{K,S}) = r_1 + r_2 + \# S + \delta_p - 1,
\]
where $(r_1, r_2)$ the signature of $K$ and $\delta_p = 1$ if $K$ contains the $p^{th}$ root of unity, 0 otherwise.

Lemma 14. ([4]) We have
\[
d_p(C_{K,S}) \geq d_p(C_K) - s + s_0.
\]

Proposition 15. ([2]) The rank of the 2-class group of $K = \mathbb{Q}(\sqrt{d}, i)$ is:
\[
\begin{cases}
r + r_0 & \text{if } d \text{ is even and } p \equiv 1 \mod 8 \text{ for all } p \in Q_0, \\
r + r_0 - 1 & \text{if } d \text{ is even and there exists } p \in Q_0 \text{ such that } p \equiv 5 \mod 8, \\
r + r_0 - 2 & \text{if } d \text{ is odd and there exists } p \in Q_0 \text{ such that } p \equiv 5 \mod 8,
\end{cases}
\]
where $r = \# Q$ with $Q$ is the set of odd primes that ramify in $\mathbb{Q}(\sqrt{d})$, and $r_0 = \# Q_0$ with $Q_0$ is the subset of $Q$ consisting of those primes which split completely in $\mathbb{Q}(\sqrt{-1})$.

Theorem 16. Let $P = \{p_1, \ldots, p_s\}$ and $Q = \{q_1, \ldots, q_r\}$ be disjoint sets of odd primes. Consider an imaginary biquadratic extension $\mathbb{Q}(\sqrt{d}, i)/\mathbb{Q}$ that is ramified exactly at those primes in $\{2\} \cup Q$, and $P$ splits completely in $K = \mathbb{Q}(\sqrt{d}, i)$. Let $s_0$ be the number of primes in $P$ split into principal prime ideals in $K$. Let $Q_0$ be the subset of $Q$ consisting of those primes congruent to 1 modulo 4 and $r_0 = \# Q_0$. Let $S$ be the set of prime ideals of $K$ that lie above the primes in $P$. Suppose that one of the following properties is verified:

1. $d$ is even and $q \equiv 1 \mod 8$ for all $q \in Q_0$, and
\[
r + r_0 \geq 2 + s - s_0 + 2\sqrt{3 + s},
\]
2. \( d \) is even and there exists \( q \in \mathbb{Q}_0 \) such that \( q \equiv 5 \mod 8 \), and
\[
 r + r_0 \geq 3 + s - s_0 + 2\sqrt{3 + s},
\]

3. \( d \) is odd and \( q \equiv 1 \mod 8 \) for all \( q \in \mathbb{Q}_0 \), and
\[
 r + r_0 \geq 3 + s - s_0 + 2\sqrt{3 + s},
\]

4. \( d \) is odd and there exists \( q \in \mathbb{Q}_0 \) such that \( q \equiv 5 \mod 8 \), and
\[
 r + r_0 \geq 4 + s - s_0 + 2\sqrt{3 + s},
\]

then \( \mathbb{K} \) has an infinite \( S \)-decomposing 2-class field tower.

Proof. Let \( S' = \{p_1, \ldots, p_s\} \) be a set of prime ideals of \( \mathbb{K} = \mathbb{Q}(\sqrt{d}, i) \) that lie above the primes in \( P \) such that
\[
 N(p_j) = p_j \quad \text{for all } 1 \leq j \leq s.
\]

The imaginary biquadratic field \( \mathbb{K} = \mathbb{Q}(\sqrt{d}, i) \) has signature \((0, 2)\) and contains the 2\textsuperscript{nd} root of unity, then
\[
 d_2(E_{\mathbb{K}, S'}) = r_1 + r_2 + \delta_2 + s - 1 = 2 + s.
\]

From Lemma 14, we have
\[
 d_2(C_{\mathbb{K}, S'}) \geq d_2(C_{\mathbb{K}}) - s + s_0.
\]

If
\[
 d_2(C_{\mathbb{K}}) \geq 2 + s - s_0 + 2\sqrt{3 + s},
\]
then \( \mathbb{K} \) has an infinite \( S' \)-decomposing 2-class field tower. Using the Proposition 15, we obtain the results.

Since any Galois extension of \( \mathbb{K} \) is a Galois extension of \( \mathbb{Q} \), then the \( S \)-decomposing 2-class field tower of \( \mathbb{K} \) coincides with the \( S' \)-decomposing 2-class field tower of \( \mathbb{K} \). \( \square \)
Table 1: Examples of imaginary biquadratic fields $\mathbb{Q} (\sqrt{d}, i)$ have infinite $S$-decomposing 2-class field tower

| $\mathbb{K} = \mathbb{Q}(\sqrt{d}, i)$ | $rd_\mathbb{K} = |d_\mathbb{K}|^t$ | $P$ | $|Q|$ | $|Q_0|$ |
|----------------------------------|-----------------|-----|------|------|
| $d = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23$ | 5239.998473 | $\{13\}$ | 6 | 1 |
| $d = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23$ | 5239.998473 | $\{37\}$ | 6 | 1 |
| $d = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17$ | 609.3274981 | $\{37\}$ | 5 | 3 |
| $d = 2 \cdot 5 \cdot 13 \cdot 17 \cdot 41$ | 851.398849 | $\{37\}$ | 4 | 4 |
| $d = 3 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 31$ | 14587.53838 | $\{13\}$ | 7 | 1 |
| $d = 3 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 31$ | 14587.53838 | $\{37\}$ | 7 | 1 |
| $d = 3 \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ | 1664.73421 | $\{29\}$ | 6 | 3 |
| $d = 3 \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ | 1664.73421 | $\{37\}$ | 6 | 3 |
| $d = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 41$ | 33552.36123 | $\{29, 37\}$ | 7 | 2 |
| $d = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23 \cdot 41$ | 38952.91989 | $\{13, 37\}$ | 7 | 2 |
| $d = 2 \cdot 5 \cdot 13 \cdot 17 \cdot 29 \cdot 37$ | 4355.529819 | $\{53, 61\}$ | 5 | 5 |
| $d = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 37$ | 3706.394474 | $\{29, 41\}$ | 6 | 4 |
| $d = 17 \cdot 41 \cdot 73 \cdot 89 \cdot 97$ | 41916.85451 | $\{13, 53\}$ | 5 | 5 |
| $d = 3 \cdot 7 \cdot 17 \cdot 41 \cdot 73 \cdot 89$ | 19503.49599 | $\{13, 37\}$ | 6 | 4 |
| $d = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$ | 21123.10915 | $\{29, 41\}$ | 8 | 3 |
| $d = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 29$ | 5441.468552 | $\{37, 41\}$ | 7 | 3 |

References


