International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 6, No. 3 (2013)

International Electronic Journal of Pure and Applied Mathematics

Volume 6 No. 3 2013, 127-132
ISSN: 1314-0744
url: http://www.e.ijpam.eu
doi: http://dx.doi.org/10.12732/iejpam.v6i3.3

2-CLASS FIELDS TOWERS OF SOME IMAGINARY BIQUADRATIC NUMBER FIELDS

Abdelmalek Azizi[1], Mohammed Rezzougui[2] §

[1,2]Department of Mathematics
Faculty of Science
Mohamed First University
Oujda, MOROCCO

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

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 ${\rm K_p}^{(1)}$ the p-class field of K, and for a positive integer n, ${\rm K_p}^{(n+1)}$ the p-class field of ${\rm K_p}^{(n)}$. The Hilbert p-class field tower is the sequence of fields:

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

If there exists $n \in \mathbb{N}$ such that ${\rm K_p}^{(n-1)} \neq {\rm K_p}^{(n)}$ and ${\rm K_p}^{(n)} = {\rm K_p}^{(n+1)}$, 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 ${\rm K_p}^{S}$, 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 $\mathrm{K}_0 = \mathrm{K}$, $\mathrm{K}_1 = {\rm K_p}^{S}$ and for $n \geq 2$, $\mathrm{K}_n = (\mathrm{K}_{n-1})_{\rm p}^{S_{n-1}}$, where S_n is the set of prime ideals in K_n lying above S.

Received: November 22, 2013 © 2013 Academic Publications, Ltd.

§Correspondence author

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 6, No. 3 (2013)

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 $\mathcal{O}_{\mathrm{K}}$ 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 $C_{\mathrm{K}} = I_{\mathrm{K}}/P_{\mathrm{K}}$ 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 $\mathcal{I}$ be a fractional ideal of* K. *there exists a unique factorization*

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

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

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

1. $\nu_{\mathfrak{p}}(x) = +\infty \Leftrightarrow x = 0$.
2. $\nu_{\mathfrak{p}}(xy) = \nu_{\mathfrak{p}}(x) + \nu_{\mathfrak{p}}(y)$ *for all* $x, y \in \mathrm{K}$.
3. $\nu_{\mathfrak{p}}(x + y) \geq \min\{\nu_{\mathfrak{p}}(x), \nu_{\mathfrak{p}}(y)\}$ *for all* $x, y \in \mathrm{K}$. (*with equality if* $\nu_{\mathfrak{p}}(x) \neq \nu_{\mathfrak{p}}(y)$)

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

$$\mathcal{O}_{\mathrm{K},S} = \{x \in \mathrm{K}; \nu_{\mathfrak{p}}(x) \geq 0 \text{ for all } \mathfrak{p} \notin S\}$$

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

$$E_{\mathrm{K},S} = \{x \in \mathrm{K}; \nu_{\mathfrak{p}}(x) = 0 \text{ for all } \mathfrak{p} \notin S\}.$$

Definition 4. Let $I_{\mathrm{K},S}$ be the group of fractional ideals nondivisible by prime ideal of S. Let $P_{\mathrm{K},S}$ be the subgroup of principal ideals of $I_{\mathrm{K},S}$. The quotient $C_{\mathrm{K},S} = I_{\mathrm{K},S}/P_{\mathrm{K},S}$ is called the ideal S-class group of K.

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 6, No. 3 (2013)

Proposition 5 ([4]). *Let I_{K}^{S} be the group of ideals generated by prime ideal in S and Φ the group homomorphism from I_{K}^{S} into C_{K} defined by*

$$\begin{array}{ccccc} \Phi & : & I_{\mathrm{K}}^{S} & \to & C_{\mathrm{K}} \\ & & I & \mapsto & [I] \end{array}$$

then the ideal S-class group $C_{\mathrm{K},S}$ is isomorphic to the quotient group $C_{\mathrm{K}}/Im\Phi$.

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 $\mathfrak{p}$ be a prime ideal of a ring A. The $\mathfrak{p}$-rank of an A-module M is the rank of the $A/\mathfrak{p}$-module $A/\mathfrak{p} \otimes M \simeq M/\mathfrak{p}M$.

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

$$\mathbb{F}_{\mathrm{p}} \otimes \mathcal{G} \simeq \mathcal{G}/\mathcal{G}^{\mathrm{p}}$$

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

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

$$d_{\mathrm{p}}(\mathcal{G}) = \dim_{\mathbb{F}_{\mathrm{p}}}(\mathcal{G}^{ab}/\mathrm{p}) = \dim_{\mathbb{F}_{\mathrm{p}}}(\mathcal{G}/\mathcal{G}^{\mathrm{p}}[\mathcal{G} : \mathcal{G}])$$

where $[\mathcal{G} : \mathcal{G}]$ the commutator subgroup of $\mathcal{G}$ and $\mathcal{G}^{ab} = \mathcal{G}/[\mathcal{G} : \mathcal{G}]$.

Theorem 10. *Let $\mathcal{G}$ be an abelian group and $\mathcal{H}$ a subgroup of $\mathcal{G}$, then*

$$d_{\mathrm{p}}(\mathcal{G}/\mathcal{H}) + d_{\mathrm{p}}(\mathcal{H}) = d_{\mathrm{p}}(\mathcal{G}) + d_{\mathrm{p}}(\mathcal{H} \cap \mathcal{G}^{\mathrm{p}}/\mathcal{H}^{\mathrm{p}}).$$

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

$$1 \longrightarrow \mathcal{H}/\mathcal{H} \cap \mathcal{G}^{\mathrm{p}} \overset{i}{\longrightarrow} \mathcal{G}/\mathcal{G}^{\mathrm{p}} \overset{\pi}{\longrightarrow} (\mathcal{G}/\mathcal{H})/(\mathcal{G}/\mathcal{H})^{\mathrm{p}} \longrightarrow 1$$

and the following commutative diagram

$$\begin{array}{ccc} \mathcal{H} & \longrightarrow & \mathcal{H}/\mathcal{H} \cap \mathcal{G}^{\mathrm{p}} \\ \downarrow & \nearrow & \\ \mathcal{H}/\mathcal{H}^{\mathrm{p}} & & \end{array}$$

by the rank theorem, we have $d_{\mathrm{p}}(\mathcal{G}/\mathcal{H}) + d_{\mathrm{p}}(\mathcal{H}) = d_{\mathrm{p}}(\mathcal{G}) + d_{\mathrm{p}}(\mathcal{H} \cap \mathcal{G}^{\mathrm{p}}/\mathcal{H}^{\mathrm{p}})$. □

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 6, No. 3 (2013)

Theorem 11 ([3]). *Let $\mathcal{G}$ be a finite* p*-group, then*

$$\frac{1}{4}(d_{\mathrm{p}}(\mathcal{G}))^2 - d_{\mathrm{p}}(\mathcal{G}) < d_{\mathrm{p}}(H_2(\mathcal{G}, \mathbb{Z}))$$

where $H_2(\mathcal{G}, \mathbb{Z})$ the second homology group of the group $\mathcal{G}$, with integer coefficients.

Lemma 12 ([4]). *If*

$$d_{\mathrm{p}}(C_{\mathrm{K},S}) \geq 2 + 2\sqrt{d_{\mathrm{p}}(E_{\mathrm{K},S}) + 1},$$

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*

$$d_{\mathrm{p}}(E_{K,S}) = r_1 + r_2 + \#\ S + \delta_{\mathrm{p}} - 1,$$

where (r_1, r_2) the signature of K *and $\delta_{\mathrm{p}} = 1$ if K contains the p^{th} root of unity, 0 otherwise.*

Lemma 14. *[[4]] We have*

$$d_{\mathrm{p}}(C_{K,S}) \geq d_{\mathrm{p}}(C_K) - s + s_0.$$

Proposition 15. *[[2]] The rank of the 2-class group of $\mathbb{K} = \mathbb{Q}(\sqrt{d}, i)$ is :*

$$\begin{cases} r + r_0 & \text{if } d \text{ is even and } p \equiv 1 \bmod 8 \text{ for all } p \in Q_0, \\ r + r_0 - 1 & \text{if } d \text{ is even and there exists } p \in Q_0 \text{ such that } p \equiv 5 \bmod 8, \\ & \text{ or } d \text{ is odd and } p \equiv 1 \bmod 8 \text{ for all } p \in Q_0, \\ r + r_0 - 2 & \text{if } d \text{ is odd and there exists } p \in Q_0 \text{ such that } p \equiv 5 \bmod 8, \end{cases}$$

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 $\mathbb{K} = \mathbb{Q}(\sqrt{d}, i)$. Let s_0 be the number of primes in P split into principal prime ideals in $\mathbb{K}$. 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 $\mathbb{K}$ that lie above the primes in P. Suppose that one of the following properties is verified :*

1. *d is even and $q \equiv 1 \bmod 8$ for all $q \in Q_0$, and*

$$r + r_0 \geq 2 + s - s_0 + 2\sqrt{3 + s},$$

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 6, No. 3 (2013)

2. *d is even and there exists $q \in Q_0$ such that $q \equiv 5 \bmod 8$, and*

$$r + r_0 \geq 3 + s - s_0 + 2\sqrt{3+s},$$

3. *d is odd and $q \equiv 1 \bmod 8$ for all $q \in Q_0$, and*

$$r + r_0 \geq 3 + s - s_0 + 2\sqrt{3+s},$$

4. *d is odd and there exists $q \in Q_0$ such that $q \equiv 5 \bmod 8$, 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 $S' = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ be a set of prime ideals of $\mathbb{K} = \mathbb{Q}(\sqrt{d}, i)$ that lie above the primes in P such that

$$N(\mathfrak{p}_j) = p_j \quad \text{for all } \; 1 \leq j \leq s.$$

The imaginary biquadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{d}, i)$ has signature $(0, 2)$ and contains the 2^{nd} root of unity , then

$$\begin{aligned} d_2(E_{\mathbb{K},S'}) &= r_1 + r_2 + \delta_2 + s - 1 \\ &= 2 + s. \end{aligned}$$

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 $\mathbb{K}$. □

International Electronic Journal of Pure and Applied Mathematics – IEJPAM, Volume 6, No. 3 (2013)

$\mathbb{K} = \mathbb{Q}(\sqrt{d}, i)$	$rd_{\mathbb{K}} = \mid d_{\mathbb{K}} \mid^{\frac{1}{4}}$	P	$\mid Q \mid$	$\mid Q_0 \mid$
$d = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 23$	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
$d = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 17 \cdot 19 \cdot 31 \cdot 41$	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

Table 1: Examples of imaginary biquadratic fields $\mathbb{Q}(\sqrt{d}, i)$ have infinite S-decomposing 2-class field tower

References

[1] G.J. Janus, *Algebric Number Fields*, Academic Press, New-York–London (1973).

[2] T.M. McCall, C.J. Parry, R.R. Ranalli, On imaginary bicyclic biquadratic fields with cyclic 2-class group, *J. Number Theory*, **53** (1995), 88-99.

[3] P. Roquette, On class field towers, In: *Algebraic Number Theory* (Ed-s: J.W.S. Cassels, A. Frölich), Academic Press (1967), 231-249.

[4] M.A. Tsfasman, S.G. Vlăduţ, Infinite global fields and the generalized Brauer-Siegel theorem, *Moscow Mathematical Journal, Dedicated to Yuri I. Manin on the occasion of his 65-th birthday* (2002), 65-69.