



Miskolc Mathematical Notes
Vol. 15 (2014), No 2, pp. 317-325

HU e-ISSN 1787-2413
DOI: 10.18514/MMN.2014.723

Galois group for some class field

Abdelmalek Azizi and Mohammed Talbi



GALOIS GROUP FOR SOME CLASS FIELD

ABDELMALEK AZIZI AND MOHAMMED TALBI

Received 24 September, 2013

Abstract. For some imaginary quartic cyclic fields \mathbb{K} , we will study the capitulation problem of the 2-class ideals of \mathbb{K} and we will determine the structure of the Galois group of the second Hilbert 2-class field of \mathbb{K} over \mathbb{K} .

2010 *Mathematics Subject Classification:* 11R27; 11R37

Keywords: cyclic quartic fields, class group, Hilbert class field

1. INTRODUCTION

Let \mathbb{F}/\mathbb{L} a finite extension of number fields and $O_{\mathbb{L}}$ (resp. $O_{\mathbb{F}}$) the ring of integers of \mathbb{L} (resp. of \mathbb{F}). We say, since Hilbert, that an ideal of $O_{\mathbb{L}}$ capitulates in \mathbb{F} , if it becomes principal by extension of scalars to $O_{\mathbb{F}}$, and, of course, when an ideal \mathfrak{a} of $O_{\mathbb{L}}$ capitulates in \mathbb{F} , then the class $[\mathfrak{a}]$ of \mathfrak{a} capitulates in \mathbb{F} (ie. $[\mathfrak{a}O_{\mathbb{F}}]$ is trivial). Therefore, the study of the capitulation problem is precisely to describe the group of all classes of ideals of \mathbb{L} which capitulate in \mathbb{F} , where \mathbb{F} is an unramified abelian extension of \mathbb{L} .

Proposition 1 ([8]). *Let \mathbb{G} a 2-group of finite order 2^m and \mathbb{G}' its derived subgroup. Then \mathbb{G}/\mathbb{G}' is of type $(2, 2)$ if and only if \mathbb{G} is isomorphic to one of 2-groups:*

$$Q_m = \langle \sigma, \tau \rangle \quad \text{where} \quad \sigma^{2^{m-2}} = \tau^2 = a, a^2 = 1, \tau^{-1}\sigma\tau = \sigma^{-1};$$

$$D_m = \langle \sigma, \tau \rangle \quad \text{where} \quad \sigma^{2^{m-1}} = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^{-1};$$

$$S_m = \langle \sigma, \tau \rangle \quad \text{where} \quad \sigma^{2^{m-1}} = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma^{2^{m-2}-1};$$

$$(2, 2) = \langle \sigma, \tau \rangle \quad \text{where} \quad \sigma^2 = \tau^2 = 1, \tau^{-1}\sigma\tau = \sigma.$$

Where Q_m is the quaternionic group, D_m the dihedral group, S_m the semi-dihedral group of order 2^m and $(2, 2)$ is an abelian group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Suppose that \mathbb{G} is a 2-group of finite order 2^m such that \mathbb{G}/\mathbb{G}' is of type $(2, 2)$, then \mathbb{G} is isomorphic to Q_m , D_m , S_m or $(2, 2)$ defined in the Proposition 1. Let $\{\sigma, \tau\}$ generates \mathbb{G} such that the relationships cited in the Proposition 1 are verified, by a simple calculation we can see that the derived subgroup $\mathbb{G}' = [\mathbb{G}, \mathbb{G}] = \langle \sigma^2 \rangle$

and \mathbb{G} has three subgroups of index 2: $H_1 = \langle \sigma \rangle$, $H_2 = \langle \sigma^2, \tau \rangle$ and $H_3 = \langle \sigma^2, \sigma\tau \rangle$. Moreover if \mathbb{G} is of type (2, 2), then the subgroups H_i are cyclic of order 2, if $\mathbb{G} \simeq Q_3$, then the subgroups H_i are cyclic of order 4 and if \mathbb{G} is isomorphic to Q_m ($m > 3$), D_m or S_m , then H_1 is cyclic and H_2/H_2' and H_3/H_3' are of type (2, 2) where H_2' (resp. H_3') is the derived subgroup of H_2 (resp. H_3).

Throughout the remainder of this section we denote by \mathbb{M} a number field, $\mathbb{M}_2^{(1)}$ the first 2-Hilbert class field of \mathbb{M} , $\mathbb{M}_2^{(2)}$ the second 2-Hilbert class field of \mathbb{M} , $C_{\mathbb{M}}$ the class group of \mathbb{M} , $C_{2, \mathbb{M}}$ the 2-part of $C_{\mathbb{M}}$, \mathbb{G} the Galois group of $\mathbb{M}_2^{(2)}/\mathbb{M}$ and \mathbb{G}' its derived sub-group. Then $\mathbb{G}' \simeq \text{Gal}(\mathbb{M}_2^{(2)}/\mathbb{M}_2^{(1)})$ and $\mathbb{G}/\mathbb{G}' \simeq \text{Gal}(\mathbb{M}_2^{(1)}/\mathbb{M})$, and we know from the class field theory that $\text{Gal}(\mathbb{M}_2^{(1)}/\mathbb{M}) \simeq C_{2, \mathbb{M}}$, so $\mathbb{G}/\mathbb{G}' \simeq C_{2, \mathbb{M}}$.

Definition 1. Let \mathbb{F} be a cyclic unramified extension of \mathbb{M} and j is the mapping of $C_{\mathbb{M}}$ into $C_{\mathbb{F}}$ that maps to the class of an ideal \mathfrak{a} of \mathbb{M} the class of the ideal generated by \mathfrak{a} in \mathbb{F} . Then the extension \mathbb{F}/\mathbb{M} is called:

- of type (A) if and only if $\#\ker j \cap N_{\mathbb{F}/\mathbb{M}}(C_{\mathbb{F}}) > 1$;
- of type (B) if and only if $\#\ker j \cap N_{\mathbb{F}/\mathbb{M}}(C_{\mathbb{F}}) = 1$.

Now suppose that $C_{2, \mathbb{M}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then $\mathbb{G}/\mathbb{G}' \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and as \mathbb{G} is a 2-finite group, then \mathbb{G}' is cyclic. Thus the Hilbert 2-class field towers of \mathbb{M} ends in $\mathbb{M}_2^{(2)}$.

In addition, we know that if \mathbb{G} has order 2^m and $\mathbb{G}/\mathbb{G}' \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then \mathbb{G} is isomorphic to Q_m , D_m , S_m or to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In all these cases, we have $\mathbb{G}' = \langle \sigma^2 \rangle$ and the three subgroups of index 2 in \mathbb{G} are: $H_1 = \langle \sigma \rangle$, $H_2 = \langle \sigma^2, \tau \rangle$ and $H_3 = \langle \sigma^2, \sigma\tau \rangle$, and if $\mathbb{G}' \neq 1$, then $\mathbb{M}_2^{(1)} \neq \mathbb{M}_2^{(2)}$ and $\langle \sigma^4 \rangle$ is the only subgroup of \mathbb{G}' of index 2.

Let \mathbb{L} the subfield of $\mathbb{M}_2^{(2)}$ left fixed by $\langle \sigma^4 \rangle$, \mathbb{F}_i ($i = 1, 2, 3$) the subfield of $\mathbb{M}_2^{(2)}$ left fixed by H_i and j_i the mapping j defined for $\mathbb{F} = \mathbb{F}_i$.

Theorem 1 ([8]). *Assume that $\mathbb{G}/\mathbb{G}' \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, so we have*

- (1) *If $\mathbb{M}_2^{(1)} = \mathbb{M}_2^{(2)}$, then the fields \mathbb{F}_i are of type (A), $\#\ker j_i = 4$ for $i = 1, 2, 3$ and $\mathbb{G} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;*
- (2) *If $\text{Gal}(\mathbb{L}/\mathbb{M}) \simeq Q_3$, then the fields \mathbb{F}_i are of type (A), $\#\ker j_i = 2$ for $i = 1, 2, 3$ and $\mathbb{G} \simeq Q_3$;*
- (3) *If $\text{Gal}(\mathbb{L}/\mathbb{M}) \simeq D_3$, then the fields \mathbb{F}_2 and \mathbb{F}_3 are of type (B) and $\#\ker j_2 = \#\ker j_3 = 2$. Moreover, if \mathbb{F}_1 is of type (B) then $\#\ker j_1 = 2$ and $\mathbb{G} \simeq S_m$. If \mathbb{F}_1 is of type (A) and $\#\ker j_1 = 2$, then $\mathbb{G} \simeq Q_m$. Finally if \mathbb{F}_1 is of type (A) and $\#\ker j_1 = 4$, then $\mathbb{G} \simeq D_m$.*

Theorem 2 ([6]). *Let \mathbb{L}/\mathbb{M} be an unramified cyclic extension of prime degree, then the number of classes that capitulate in \mathbb{L}/\mathbb{M} is*

$$[\mathbb{L} : \mathbb{M}][E_{\mathbb{M}} : N_{\mathbb{L}/\mathbb{M}}(E_{\mathbb{L}})],$$

where $E_{\mathbb{M}}$ (resp. $E_{\mathbb{L}}$) is the group of units of \mathbb{M} (resp. of \mathbb{L}).

For more details about the capitulation problem see [8, 11, 12].

2. UNITS OF SOME NUMBER FIELDS

Proposition 2 ([1]). *Let \mathbb{K}_0 a number field, abelian real and β an algebraic integer in \mathbb{K}_0 , totally positive, without square factors. Assume that $\mathbb{F} = \mathbb{K}_0(\sqrt{-\beta})$ is a quadratic extension of \mathbb{K}_0 , abelian over \mathbb{Q} and $i = \sqrt{-1} \notin \mathbb{F}$. Let $\{\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r\}$ be a fundamental system of units of \mathbb{K}_0 . We choose, without limiting the generality, units ε_j positive. Then we have:*

- (1) *If there is a unit of \mathbb{K}_0 such that $\varepsilon = \varepsilon_1^{j_1} \varepsilon_2^{j_2} \dots \varepsilon_{r-1}^{j_{r-1}} \varepsilon_r$ (close to a permutation), where the $j_k \in \{0, 1\}$, such that $\beta\varepsilon$ is a square in \mathbb{K}_0 , then $\{\varepsilon_1, \dots, \varepsilon_{r-1}, \sqrt{-\varepsilon}\}$ is a fundamental system of units of \mathbb{F} ;*
- (2) *Otherwise $\{\varepsilon_1, \dots, \varepsilon_r\}$ is a fundamental system of units of \mathbb{F} .*

Corollary 1 ([2]). *Let $\mathbb{L} = \mathbb{Q}(\sqrt{-n\varepsilon\sqrt{d}})$ a cyclic extension of degree 4 over \mathbb{Q} , where ε is the fundamental unit of $\mathbb{Q}(\sqrt{d})$ with d a positive integer squarefree and n a positive integer, then $\{\varepsilon\}$ is a fundamental system of units of \mathbb{L} .*

Theorem 3 ([2]). *Let $\mathbb{K}_0 = \mathbb{Q}(\sqrt{p}, \sqrt{p'})$ where p and p' are two different primes such that $p \equiv p' \equiv 1 \pmod{4}$, ε_1 (resp. $\varepsilon_2, \varepsilon_3$) the fundamental unit of $\mathbb{Q}(\sqrt{p})$ (resp. $\mathbb{Q}(\sqrt{p'})$, $\mathbb{Q}(\sqrt{pp'})$) and $\mathbb{F} = \mathbb{K}_0(\sqrt{-n\varepsilon_1\sqrt{p}})$ where n is a positive integer square-free. Then we have:*

- (1) *If ε_3 has norm 1, then $\{\varepsilon_1, \varepsilon_2, \sqrt{\varepsilon_3}\}$ is a fundamental system of units of \mathbb{K}_0 and of \mathbb{F} ;*
- (2) *Otherwise, $\{\sqrt{\varepsilon_1\varepsilon_2\varepsilon_3}, \varepsilon_2, \varepsilon_3\}$ is a fundamental system of units of \mathbb{K}_0 and of \mathbb{F} .*

Now, using the results of M. N. Gras [4], we'll define a fundamental system of units of real cyclic extension of degree 4 over \mathbb{Q} . Let $\mathbb{L} = \mathbb{k}(\sqrt{\varepsilon_0\sqrt{l}})$ where l is a prime number congruent to 1 modulo 8 and ε_0 is the fundamental unit of $\mathbb{k} = \mathbb{Q}(\sqrt{l})$, then \mathbb{L}/\mathbb{Q} is a real cyclic extension of degree 4 with Galois group $H = \langle \gamma \rangle$ and quadratic subfield \mathbb{k} . Since \mathbb{L} has conductor $F_{\mathbb{L}} = l$, we have $\mathbb{L} \subset \mathbb{Q}^{(l)}$ and there exists a character χ' of $Gal(\mathbb{Q}^{(l)}/\mathbb{Q}) \simeq (\mathbb{Z}/l\mathbb{Z})^*$ such that $\ker \chi' = Gal(\mathbb{Q}^{(l)}/\mathbb{L})$. Let $\chi = \chi' + \chi'^{-1}$, then χ is a rational character of $\mathbb{Q}^{(l)}$ and \mathbb{L} is fixed by the common kernel of χ' and χ'^{-1} . Let $E_{\mathbb{L}}$ be the group of units of \mathbb{L} , E_{χ} the group of χ -relative units of \mathbb{L} , $|E_{\mathbb{L}}|$ (resp. $|E_{\chi}|$) the group of absolute values of $E_{\mathbb{L}}$ (resp.

E_χ), $|E^\mathbb{L}| = |E_\mathbb{L}| \oplus |E_\chi|$, $Q = [|E_\mathbb{L}| : |E^\mathbb{L}|]$ and ε_χ a generator of E_χ . Then we have the following result:

Theorem 4 ([4]). *Let $\mathbb{L} = k(\sqrt{\varepsilon_0 \sqrt{l}})$ where l is a prime number congruent to 1 modulo 8 and ε_0 the fundamental unit of $k = \mathbb{Q}(\sqrt{l})$, then:*

- (1) $Q = 2$;
- (2) *There exists ξ in $E_\mathbb{L}$ such that $\xi^2 = \pm \varepsilon_0 \varepsilon_\chi^{1-\sigma}$ and $\{\xi, \xi^\sigma, \xi^{\sigma^2}\}$ is a fundamental system of units of \mathbb{L} .*

Remark 1. Since $\xi^2 = \pm \varepsilon_0 \varepsilon_\chi^{1-\sigma}$, then:

- (1) $\xi^{1+\sigma} = \pm \varepsilon_\chi$;
- (2) $\xi^{1+\sigma^2} = \pm \varepsilon_0$;
- (3) $\xi^{1+\sigma+\sigma^2+\sigma^3} = \varepsilon_\chi^{1+\sigma^2} = \varepsilon_0^{1+\sigma}$;
- (4) $N_{k/\mathbb{Q}}(\varepsilon_0) = N_{\mathbb{L}/k}(\varepsilon_\chi) = N_{\mathbb{L}/\mathbb{Q}}(\xi) = -1$.

Lemma 1. *With the same notation of Theorem 4, $\{\xi, \xi^\sigma, \xi^{\sigma^2}\}$ is a fundamental system of units of $\mathbb{F} = \mathbb{L}(\sqrt{-n})$ where n is an integer different from 1, relatively prime to l and square-free.*

Proof. By Proposition 2, to show that $\{\xi, \xi^\sigma, \xi^{\sigma^2}\}$ is a fundamental system of units of \mathbb{F} it suffices to show that $n\mu$ is not a square in \mathbb{L} , for $\mu = \xi_1^{j_1} \xi_2^{j_2} \xi_3^{j_3}$ where $\{\xi_1, \xi_2, \xi_3\} = \{\xi, \xi^\sigma, \xi^{\sigma^2}\}$ and $j_1, j_2 \in \{0, 1\}$.

Indeed, if $\mu = \xi$, then if $n\xi = x^2$ in \mathbb{L} , so by calculating the norm in \mathbb{L}/k , we find that $\xi^{1+\sigma^2} = \pm \varepsilon_0$ is a square in k , which is impossible.

If $\mu = \xi^\sigma$, then if $n\xi^\sigma = \pm n \frac{\varepsilon_\chi}{\xi} = x^2$ in \mathbb{L} , so by using the norm in \mathbb{L}/k , we find that $\pm \frac{\varepsilon_0^{1+\sigma}}{\varepsilon_0} = \pm \varepsilon_0^{-1}$ is a square in k , which is absurd.

If $\mu = \xi^{\sigma^2}$, then if $n\xi^{\sigma^2} = \pm n \frac{\varepsilon_0}{\xi} = x^2$ in \mathbb{L} , so by calculating the norm in \mathbb{L}/k , we find that $\pm \frac{\varepsilon_0^2}{\varepsilon_0} = \pm \varepsilon_0$ is a square in k , which is not the case.

If $\mu = \xi^{1+\sigma} = \pm \varepsilon_\chi$, then if $\pm n \varepsilon_\chi = x^2$ in \mathbb{L} , so by calculating the norm in \mathbb{L}/k , we find that $\varepsilon_\chi^{1+\sigma^2} = \varepsilon_0^{1+\sigma} = -1$ is a square in k , which is absurd.

If $\mu = \xi^{1+\sigma^2} = \pm \varepsilon_0$, then $\pm n \varepsilon_0$ can not be a square in \mathbb{L} .

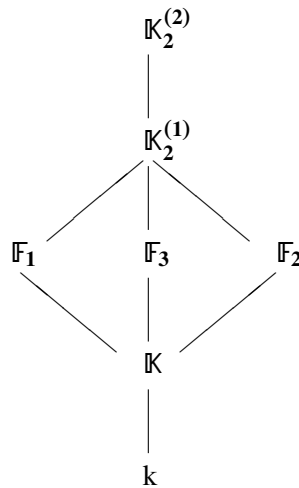
If $\mu = \xi^{\sigma+\sigma^2}$, then if $n\xi^{\sigma+\sigma^2} = x^2$ in \mathbb{L} , so by calculating the norm in \mathbb{L}/k , we find that $\xi^{1+\sigma+\sigma^2+\sigma^3} = -1$ is a square in k , which is not the case.

If $\mu = \xi^{1+\sigma+\sigma^2}$, then if $n\xi^{1+\sigma+\sigma^2} = x^2$ in \mathbb{L} , so by calculating the norm in \mathbb{L}/k , we find that $\xi^{1+\sigma+\sigma^2+\sigma^3} \xi^{1+\sigma^2} = \pm \varepsilon_0$ is a square in k , which is impossible, which completes the proof of the lemma. \square

3. CAPITULATION OF THE 2-IDEAL CLASS OF \mathbb{K} AND STRUCTURE OF \mathbb{G}_2

In the following, let $\mathbb{K} = k(\sqrt{-pq\varepsilon_0\sqrt{l}})$ where ε_0 is the fundamental unit of $k = \mathbb{Q}(\sqrt{l})$ with l is a prime number congruent to 1 modulo 8, p and q two prime numbers such that $p \equiv -q \equiv 1 \pmod{4}$ and $(\frac{p}{l}) = (\frac{q}{l}) = -1$, $\mathbb{K}_2^{(1)}$ the Hilbert 2-class field of \mathbb{K} , $\mathbb{K}_2^{(2)}$ the Hilbert 2-class field of $\mathbb{K}_2^{(1)}$, \mathbb{G}_2 the Galois group of $\mathbb{K}_2^{(2)}/\mathbb{K}$ and for an ideal \mathfrak{a} of \mathbb{K} , we note $[\mathfrak{a}]$ the class of \mathfrak{a} . Then, by [3], $C_{2,\mathbb{K}}$, the 2-class group of \mathbb{K} , is of type $(2, 2)$. Using the Results of [7] for the calculation of the genus fields of an extension of degree 2^s on \mathbb{Q} , we find that $\mathbb{K}_2^{(1)} = \mathbb{K}^{(*)} = \mathbb{K}(\sqrt{p}, \sqrt{-q})$, where $\mathbb{K}^{(*)}$ is the genus field of \mathbb{K} , whose quadratic subfields over \mathbb{K} are $\mathbb{F}_1 = \mathbb{K}(\sqrt{p})$, $\mathbb{F}_2 = \mathbb{K}(\sqrt{-q})$ and $\mathbb{F}_3 = \mathbb{K}(\sqrt{-pq})$.

We study the capitulation problem of the 2-ideal classes of \mathbb{K} in different sub-quadratic extension \mathbb{F}_i/\mathbb{K} of $\mathbb{K}_2^{(1)}/\mathbb{K}$, and hence we determine the structure of \mathbb{G}_2 .



Proposition 3. Let $\mathbb{K} = k(\sqrt{-pq\varepsilon_0\sqrt{l}})$, \mathcal{P} the prime ideal of \mathbb{K} above p and \mathcal{Q} that above q . Then the classes $[\mathcal{P}]$, $[\mathcal{Q}]$ and $[\mathcal{P}\mathcal{Q}]$ are of order 2 in \mathbb{K} , $C_{2,\mathbb{K}}$ is generated by the classes $[\mathcal{P}]$ and $[\mathcal{Q}]$. Also \mathcal{P} capitulates in \mathbb{F}_1 , \mathcal{Q} capitulates in \mathbb{F}_2 and $\mathcal{P}\mathcal{Q}$ capitulates in \mathbb{F}_3 .

Proof. The class $[\mathcal{P}]$ has order 2, indeed, since p is inert in k/\mathbb{Q} and p ramifies in \mathbb{K}/\mathbb{Q} , then $\mathcal{P}^2 = (p)$. Assume that $\mathcal{P} = (\alpha)$ for some α in \mathbb{K} , which is equivalent to $(\alpha^2) = (p)$ in \mathbb{K} . So there is therefore a unit ε of K such that $p\varepsilon = \alpha^2$, but there exist a and b in k such that $\alpha = a + b\sqrt{-pq\varepsilon_0\sqrt{l}}$, thus $p\varepsilon = a^2 - pq\varepsilon_0\sqrt{l}b^2 + 2ab\sqrt{-pq\varepsilon_0\sqrt{l}}$ and as $\{\varepsilon_0\}$ is a fundamental system of units of \mathbb{K} (Corollary 1) and

$i = \sqrt{-1} \notin \mathbb{K}$, then $p\varepsilon \in \mathbb{k}$, therefore a or $b = 0$. If $b = 0$, then $p\varepsilon = a^2$, thus, if ε has norm 1 (the norm in \mathbb{k}/\mathbb{Q}), p will be norm in \mathbb{k}/\mathbb{Q} which is not the case because $\left(\frac{p}{l}\right) = -1$, if ε has norm -1 we find that -1 is a square in \mathbb{Q} which is impossible. Similarly, if $a = 0$ we find that $\pm l$ is a square in \mathbb{Q} , thus $[\mathcal{P}]$ has order 2 and similarly one shows that $[\mathcal{Q}]$ and $[\mathcal{P}\mathcal{Q}]$ orders are 2, therefore $C_{2,\mathbb{K}}$ is generated by $[\mathcal{P}]$ and $[\mathcal{Q}]$. To show that \mathcal{P} capitulates in \mathbb{F}_1 , it suffices to see that $\sqrt{p} \in \mathbb{F}_1$ and $(\sqrt{p^2}) = (p)$ in \mathbb{F}_1 , so \mathcal{P} capitulated in \mathbb{F}_1 and even \mathcal{Q} capitulated in \mathbb{F}_2 and $\mathcal{P}\mathcal{Q}$ capitulated in \mathbb{F}_3 . \square

Proposition 4 ([5]). *Let \mathbb{M} a number field which contains the m -th roots of unity, \mathbb{L} a finite extension of \mathbb{M} , $\alpha \in \mathbb{M}^*$ and $\beta \in \mathbb{L}^*$. We denote by P a prime ideal of \mathbb{M} , and \mathcal{P} a prime ideal of \mathbb{L} above P . Then*

$$\prod_{\mathcal{P}} \left(\frac{\beta, \alpha}{\mathcal{P}}\right)_m = \left(\frac{N_{\mathbb{L}/\mathbb{M}}(\beta), \alpha}{P}\right)_m,$$

where the product is taken for all prime ideals of \mathbb{L} that are above P .

Theorem 5. *Let $\mathbb{K} = \mathbb{k}(\sqrt{-pq\varepsilon_0\sqrt{l}})$ where ε_0 is the fundamental unit of $\mathbb{k} = \mathbb{Q}(\sqrt{l})$ with l is a prime number congruent to 1 modulo 8, p and q be two prime numbers such that $p \equiv -q \equiv 1 \pmod{4}$ and $\left(\frac{p}{l}\right) = \left(\frac{q}{l}\right) = -1$, $\mathbb{F}_1 = \mathbb{K}(\sqrt{p})$, $\mathbb{F}_2 = \mathbb{K}(\sqrt{-q})$ and $\mathbb{F}_3 = \mathbb{K}(\sqrt{-pq})$. Then in each extension \mathbb{F}_i , $i \in \{1, 2, 3\}$, there exist exactly two classes of $C_{2,\mathbb{K}}$ which capitulate and the group \mathbb{G}_2 is quaternionic of order 2^m with $m > 3$.*

Proof. Let ε_2 (resp. ε_3) the fundamental unit of $\mathbb{Q}(\sqrt{p})$ (resp. $\mathbb{Q}(\sqrt{lp})$), \mathcal{P} the prime ideal of \mathbb{K} above p , \mathcal{Q} that above q , then, by Theorem 3, $\{\sqrt{\varepsilon_0\varepsilon_2\varepsilon_3}, \varepsilon_2, \varepsilon_3\}$ is a fundamental system of units of \mathbb{F}_1 , since $N_{\mathbb{F}_1/\mathbb{K}}(\sqrt{\varepsilon_0\varepsilon_2\varepsilon_3}) = \pm\varepsilon_0$ and $N_{\mathbb{F}_1/\mathbb{K}}(\varepsilon_2) = N_{\mathbb{F}_1/\mathbb{K}}(\varepsilon_3) = -1$, then $N_{\mathbb{F}_1/\mathbb{K}}(E_{\mathbb{F}_1}) = E_{\mathbb{K}}$, therefore, by Theorem 2, we found that only two classes of $C_{2,\mathbb{K}}$ capitulate in \mathbb{F}_1 , namely $[\mathcal{P}]$ and its square. Also the extension \mathbb{F}_1/\mathbb{K} is of type (B), indeed, let $\mathbb{K}' = \mathbb{k}(\sqrt{-q\varepsilon_0\sqrt{l}})$, then we have $\mathbb{K}\mathbb{K}' = \mathbb{F}_1$, since $N_{\mathbb{K}/\mathbb{k}}(\mathcal{P}) = p$ and p is unramified in \mathbb{K}'/\mathbb{k} , then to show that \mathcal{P} is inert in \mathbb{F}_1/\mathbb{K} , it suffices to show that p is inert in \mathbb{K}'/\mathbb{k} (translation theorem) and for this we compute the norm residue symbol $\left(\frac{p, -q\varepsilon_0\sqrt{l}}{p}\right)$. Since $p \in \mathbb{Q}$ is inert in \mathbb{k}/\mathbb{Q} and $-q\varepsilon_0\sqrt{l} \in \mathbb{k}$, therefore using the Proposition 4, we find

$$\left(\frac{p, -q\varepsilon_0\sqrt{l}}{p}\right) = \left(\frac{p, N_{\mathbb{k}/\mathbb{Q}}(-q\varepsilon_0\sqrt{l})}{p}\right) = \left(\frac{p, lq^2}{p}\right) = \left(\frac{l}{p}\right) = -1,$$

so p is inert in \mathbb{K}'/\mathbb{k} , which gives that \mathcal{P} is inert in \mathbb{F}_1/\mathbb{K} , then \mathbb{F}_1/\mathbb{K} is of type (B). Similarly, we show that extension \mathbb{F}_2/\mathbb{K} is of type (B), using Theorem 1, only two classes of $C_{2,\mathbb{K}}$ capitulate in \mathbb{F}_2 , namely $[\mathcal{Q}]$ and its square.

Using the notation of Theorem 4, we have that $\{\xi, \xi^\sigma, \xi^{\sigma^2}\}$ is a fundamental system

of units of \mathbb{F}_3 , since $N_{\mathbb{F}_3/\mathbb{K}}(\xi) = N_{\mathbb{F}_3/\mathbb{K}}(\xi^{\sigma^2}) = \pm \varepsilon_0$ and $N_{\mathbb{F}_3/\mathbb{K}}(\xi^\sigma) = \pm \varepsilon_0^{-1}$, then we have $N_{\mathbb{F}_3/\mathbb{K}}(E_{\mathbb{F}_3}) = E_{\mathbb{K}}$, using Theorem 2, we found that only two classes of $C_{2,\mathbb{K}}$ capitulate in \mathbb{F}_3 , namely $[\mathcal{P}\mathcal{Q}]$ and its square. Moreover, the extension \mathbb{F}_3/\mathbb{K} is of type (A), indeed, let $\mathbb{L} = k(\sqrt{\varepsilon_0\sqrt{l}})$, then we have $\mathbb{K}\mathbb{L} = \mathbb{F}_3$, $N_{\mathbb{K}/k}(\mathcal{P}) = p$ and p is unramified in \mathbb{L}/k , so to show that \mathcal{P} is inert in \mathbb{F}_3/\mathbb{K} , it suffices to show that p is inert in \mathbb{L}/k , for this, we compute the norm residue symbol $\left(\frac{p, \varepsilon_0\sqrt{l}}{p}\right)$. We have $p \in \mathbb{Q}$ is inert in k/\mathbb{Q} and $\varepsilon_0\sqrt{l} \in k$, so by Proposition 4, we have $\left(\frac{p, \varepsilon_0\sqrt{l}}{p}\right) = \left(\frac{p, N_{k/\mathbb{Q}}(\varepsilon_0\sqrt{l})}{p}\right) = \left(\frac{p, l}{p}\right) = \left(\frac{l}{p}\right) = -1$, therefore p is inert in \mathbb{L}/k , what gives that \mathcal{P} is inert in \mathbb{F}_3/\mathbb{K} , and similarly one shows that \mathcal{Q} remains inert in \mathbb{F}_3/\mathbb{K} and like $\mathcal{P}\mathcal{Q}$ capitulates in \mathbb{F}_3/\mathbb{K} , then by applying the Artin reciprocity law, we find that \mathbb{F}_3/\mathbb{K} is of type (A), therefore, using Theorem 1, the group \mathbb{G}_2 is isomorphic to Q_m with $m > 3$. \square

Example 1. Let $\mathbb{K} = \mathbb{Q}(\sqrt{-55(4 + \sqrt{17})\sqrt{17}})$, $\mathbb{F}_1 = \mathbb{K}(\sqrt{5})$, $\mathbb{F}_2 = \mathbb{K}(\sqrt{-11})$ and $\mathbb{F}_3 = \mathbb{K}(\sqrt{-55})$. By Theorem 5, in each extension \mathbb{F}_i there are exactly two classes of $C_{2,\mathbb{K}}$ which capitulate and $\mathbb{G}_2 \simeq Q_m$ with $m > 3$.

Corollary 2. *With the same notation of Theorem 5, we have $\#\mathbb{G}_2 = 4h_2(\mathbb{K}_0)$ where $\mathbb{K}_0 = \mathbb{Q}(\sqrt{l}, \sqrt{-pq})$ and $h_2(\mathbb{K}_0)$ its 2-class number.*

Proof. We have $\mathbb{K}_2^{(1)}/\mathbb{F}_3$ is an unramified extension and the extension \mathbb{F}_3/\mathbb{K} is of type (A), then, according to [8], C_{2,\mathbb{F}_3} is cyclic, thus \mathbb{F}_3 and $\mathbb{K}_2^{(1)}$ has the same Hilbert 2-class field which is $\mathbb{K}_2^{(2)}$, therefore $\#\mathbb{G}_2 = 2h_2(\mathbb{F}_3)$. Moreover \mathbb{F}_3/k is a biquadratic normal extension with Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and quadratic subfields \mathbb{K} , \mathbb{K}_0 and $\mathbb{L} = k(\sqrt{\varepsilon_0\sqrt{l}})$, so, by using [9], page 247, we find that

$$h_2(\mathbb{F}_3) = \frac{1}{2}q(\mathbb{F}_3/k)h_2(\mathbb{K})h_2(\mathbb{K}_0)h_2(\mathbb{L}),$$

where $q(\mathbb{F}_3/k)$ is the unit index of \mathbb{F}_3/k and $h_2(\mathbb{F})$ is the 2-class number of a number field \mathbb{F} . We have $h_2(\mathbb{K}) = 4$, according to [13] we have $h_2(\mathbb{L}) = 1$, by Corollary 1 we have $\{\varepsilon_0\}$ is a fundamental system of units of \mathbb{K} , using the Proposition 2 we show that $\{\varepsilon_0\}$ is a fundamental system of units of \mathbb{K}_0 , according to Lemma 1, we have $\{\xi, \xi^\sigma, \xi^{\sigma^2}\}$ is a fundamental system of units of \mathbb{L} and \mathbb{F}_3 , which gives that $q(\mathbb{F}_3/k) = 1$, thus $h_2(\mathbb{F}_3) = 2h_2(\mathbb{K}_0)$, therefore $\#\mathbb{G}_2 = 4h_2(\mathbb{K}_0)$. \square

Corollary 3. *Let $\mathbb{K} = k(\sqrt{-pq\varepsilon_0\sqrt{l}})$ where ε_0 is the fundamental unit of $k = \mathbb{Q}(\sqrt{l})$ with l a prime number congruent to 1 modulo 8, p and q be two primes such that $p \equiv -q \equiv 1 \pmod{4}$ and $\left(\frac{p}{l}\right) = \left(\frac{q}{l}\right) = \left(\frac{p}{q}\right) = -1$, then $\mathbb{G}_2 \simeq Q_4$.*

Proof. According to the Theorem 5, \mathbb{G}_2 is quaternionic of order 2^m with $m > 3$. Let $\mathbb{K}_0 = \mathbb{Q}(\sqrt{l}, \sqrt{-pq})$, since $\left(\frac{p}{l}\right) = \left(\frac{q}{l}\right) = \left(\frac{p}{q}\right) = -1$, then, according to [10], we have $h_2(\mathbb{K}_0) = 4$, so, using Corollary 2, we find that $\mathbb{G}_2 \simeq Q_4$. \square

Example 2. Let $\mathbb{K} = \mathbb{Q}(\sqrt{-15(4 + \sqrt{17})\sqrt{17}})$, $\mathbb{F}_1 = \mathbb{K}(\sqrt{5})$, $\mathbb{F}_2 = \mathbb{K}(\sqrt{-3})$ and $\mathbb{F}_3 = \mathbb{K}(\sqrt{-15})$. According to the Theorem 5, in each extension \mathbb{F}_i there exist exactly two classes of $C_{2,\mathbb{K}}$ which capitulate and the group \mathbb{G}_2 is quaternionic of order 2^m with $m > 3$. Furthermore, since $\left(\frac{5}{3}\right) = -1$, then, according to the Corollary 3, $\mathbb{G}_2 \simeq Q_4$.

REFERENCES

- [1] A. Azizi, "Sur les unités de certains corps de nombres de degré 8 sur \mathbb{Q} ," *Ann. Sci. Math. Québec*, vol. 29, no. 2, pp. 111–129, 2005.
- [2] A. Azizi and M. Talbi, "Capitulation dans certaines extensions non ramifiées de corps quartiques cycliques," *Archivum Mathematicum (BRNO)*, vol. 44, no. 4, pp. 271–284, 2008.
- [3] E. Brown and C. J. Parry, "The 2-class group of certain biquadratic number fields ii," *Pacific Journal of Mathematics*, vol. 78, no. 1, pp. 11–26, 1978.
- [4] M. N. Gras, "Table numérique du nombre de classes et des unités des extensions cycliques réelles de degré 4 de \mathbb{Q} ," *Publ. Math. Fac. Sciences de Besançon, Théorie des Nombres*, vol. 2, pp. 1–79, 1977–78.
- [5] H. Hasse, "Neue begründung und verallgemeinerung der theorie des normenrestsymbols," *J. Reine Angew. Math.*, vol. 162, pp. 134–144, 1930.
- [6] F. P. Heider and B. Schmithals, "Zur kapitulation der idealklassen in unverzweigten primzyklischen erweiterungen," *J. Reine Angew. Math.*, vol. 366, pp. 1–25, 1982.
- [7] M. Ishida, *The genus fields of algebraic number fields*, ser. Lecture notes in mathematics. London: Springer-Verlag, 1976, vol. 555.
- [8] H. Kisilevsky, "Number fields with class number congruent to 4 modulo 8 and hilbert's theorem 94," *J. Number Theory*, vol. 8, no. 3, pp. 271–279, 1976.
- [9] F. Lemmermeyer, "Kuroda's class number formula," *Acta Arithmetica*, vol. 66, no. 3, pp. 245–260, 1994.
- [10] T. M. McCall, C. J. Parry, and R. R. Ranalli, "Imaginary bicyclic biquadratic fields with cyclic 2-class group," *Journal of Number Theory*, vol. 53, no. 1, pp. 88–99, 1995.
- [11] K. Miyake, "Algebraic investigations of Hilbert's theorem 94, the principal ideal theorem and capitulation problem," *Expos. Math.*, vol. 7, no. 4, pp. 289–346, 1989.
- [12] H. Suzuki, "A generalisation of Hilbert's theorem 94," *Nagoya Math. J.*, vol. 121, pp. 161–169, 1991.
- [13] L. C. Washington, *Introduction to cyclotomic fields (Book 83)*, 2nd ed., ser. Graduate texts in mathematics. New York: Springer-Verlag, 1997.

Authors' addresses

Abdelmalek Azizi

Mohamed First University, Department of Mathematics and Computer Sciences, Faculty of Sciences, Oujda, Morocco

E-mail address: abdelmalekazizi@yahoo.fr

Mohammed Talbi

Regional Center of Education and Training, Oujda, Morocco

E-mail address: talbimm@yahoo.fr