RAMIFICATION IN QUARTIC CYCLIC NUMBER FIELDS K GENERATED BY $x^4 + px^2 + p$

Julio Pérez-Hernández, Mario Pineda-Ruelas, Mexico City

Received September 9, 2019. Published online February 11, 2021.
Communicated by Clemens Fuchs

Abstract. If K is the splitting field of the polynomial $f(x) = x^4 + px^2 + p$ and p is a rational prime of the form $4+n^2$, we give appropriate generators of K to obtain the explicit factorization of the ideal $q\mathcal{O}_K$, where q is a positive rational prime. For this, we calculate the index of these generators and integral basis of certain prime ideals.

Keywords: ramification; cyclic quartic field; discriminant; index

MSC 2020: 11S15, 11R16

1. Introduction

Let K be a number field of degree n and $\mathcal{O}_K$ the ring of integers K. We choose $\alpha \in \mathcal{O}_K$ such that $K = \mathbb{Q}(\alpha)$, and denote by δ_K the discriminant of K and $D(\alpha)$ the discriminant of the basis $\{1, \alpha, \ldots, \alpha^{n-1}\}$. We associate to α the positive integer $\operatorname{ind}(\alpha) = \sqrt{D(\alpha)/\delta_K}$ called the *index of* α. We know that δ_K and $D(\alpha)$ are related by $D(\alpha) = \det(C)^2\delta_K$, where C is the coefficient matrix that maps the basis $1, \alpha, \ldots, \alpha^{n-1}$ to some fixed integral basis of K. Since $D(\alpha) = \operatorname{ind}(\alpha)^2\delta_K$, then $\operatorname{ind}(\alpha) = |\det(C)|$. According to the Theorem 9.1.2 of [2] we have $\operatorname{ind}(\theta) = [\mathcal{O}_K : \mathbb{Z}[\alpha]]$, so that $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = |\det(C)|$. Let p be a positive rational prime and let $P_1, \ldots, P_g$ be prime ideals in $\mathcal{O}_K$ such that

$$p\mathcal{O}_K = P_1^{e_1} \ldots P_g^{e_g}.$$

If $I \neq \{o\}$ is any ideal of $\mathcal{O}_K$, we denote by $N(I) = |\mathcal{O}_K/I|$ the norm of the ideal I. Moreover, if $\alpha_1, \ldots, \alpha_n$ is an integral basis of I, then $N(I) = \sqrt{D(\alpha_1, \ldots, \alpha_n)/\delta_K}$.

The first author has been supported by CONACyT (México) 291197.

DOI: 10.21136/MB.2021.0131-19

Particularly, $N(P_i) = |\mathcal{O}_K/P_i| = p^{f_i}$ for $i = 1, \ldots, n$ and some $f_i \in \mathbb{N}$. If $K/\mathbb{Q}$ is a Galois extension, then $e = e_1 = \ldots = e_g$, $f = f_1 = \ldots = f_g$ and $efg = n$. If $G = \mathrm{Gal}(K/\mathbb{Q})$ and $\alpha \in \mathcal{O}_K$, we denote the norm of α by $N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$. If $f(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + x^n = \mathrm{Irr}(\alpha, \mathbb{Z})$, then $N(\alpha) = (-1)^n a_0$.

An old problem in algebraic number theory consists in explicitly giving prime ideals P_i with generators and positive integers e_i such that $p\mathcal{O}_K = P_1^{e_1} \ldots P_g^{e_g}$. If p is a prime number such that $p \nmid \mathrm{ind}(\alpha)$ then we can decompose theoretically $p\mathcal{O}_K$ as Dedekind's theorem ensures. Conrad has a comprehensive exposition of Dedekind's theorem in [4].

Theorem 1.1 (Dedekind)**.** *Let $K = \mathbb{Q}(\alpha)$ be a number field with $\alpha \in \mathcal{O}_K$, p be a rational prime and $f(x) = \mathrm{Irr}(\alpha, \mathbb{Q}) \in \mathbb{Z}[x]$. Let us consider the natural map $\overline{}\colon \mathbb{Z}[x] \to \mathbb{F}_p[x]$, where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Let $\overline{f}(x) = g_1(x)^{e_1} \ldots g_r(x)^{e_r}$, where $g_1(x), \ldots, g_r(x)$ are distinct irreducible polynomials in $\mathbb{F}_p[x]$ and $e_1, \ldots, e_r$ are positive integers. For $i = 1, \ldots, r$ let $f_i(x)$ be any polynomial of $\mathbb{Z}[x]$ such that $\overline{f}_i(x) = g_i(x)$ and $\deg(f_i(x)) = \deg(g_i(x))$. Set*

$$P_i = \langle p, f_i(\alpha) \rangle.$$

If $p \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$, then $P_1, \ldots, P_r$ are distinct prime ideals of $\mathcal{O}_K$ with

$$p\mathcal{O}_K = P_1^{e_1} \ldots P_r^{e_r} \quad \text{and} \quad N(P_i) = p^{\deg(f_i(x))}.$$

But if $p \mid \mathrm{ind}(\alpha)$ or $p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ we have the question: can we factorize $p\mathcal{O}_K$? Obviously we can't factorize $p\mathcal{O}_K$ using Dedekind's theorem, unless we could change α for another $\alpha' \in \mathcal{O}_K$ such that $p \nmid \mathrm{ind}(\alpha')$ and $K = \mathbb{Q}(\alpha')$. Remember that $\mathrm{ind}(K) = \gcd\{\mathrm{ind}(\alpha)\colon \alpha \in \mathcal{O}_K, K = \mathbb{Q}(\alpha)\}$, so, if $p \mid \mathrm{ind}(K)$, we can't find α' as we wish.

In cubic number fields K, Llorente and Nart (see [12]) give the factorization of $p\mathcal{O}_K$ for any prime p, but don't give generators of the prime ideal factors. Following the cubic case, Alaca et al. (see [1]) give the explicit factorization of $2\mathcal{O}_K$, where $\mathrm{ind}(K) = 2$. Guàrdia et al. (see [7]) build an algorithm to compute generators for the prime ideals P_i and the discriminant of any number field. This algorithm is a p-adic factorization method based on Newton polygons of higher order. The theory of Newton polygons of higher order is developed by Montes in [13] and revised in [8]. We suggest the interested reader to delight in reading [7]; we also suggest reading Chapter 6 in [3], where the reader can find an introduction to this subject and, especially, a version of Dedekind's theorem without using the hypothesis $p \nmid \mathrm{ind}(\alpha)$.

In this paper we are interested in getting the factorization of $q\mathcal{O}_K$ with $K=\mathbb{Q}(\alpha)$, where $f(\alpha)=0$, $f(x)=x^4+px^2+p$ and, for some $n\in\mathbb{N}$, $p=4+n^2$ is a rational prime. We don't use Newton polygons; we use explicitly the integral basis of cyclic quartic fields (see [10]), we calculate the integral basis of some prime ideals and we make calculation of the index of generators of K. In our case, it is relatively easy to factorize $q\mathcal{O}_K$, when $q>2$. For this reason, we start Section 3 by factoring $q\mathcal{O}_K$ for any prime $q\neq p$ such that $q\neq 2$ and $q\nmid n$, this includes the first case of the factorization of $q=3$. We finish Section 3 by factoring $q=2$. In Section 4 we study the case when K has index 3 and $q=3$.

2. Preliminaries

In this paper we shall consider a quartic field $K=\mathbb{Q}(\alpha)$ with

$$\alpha=\sqrt{-\frac{1}{2}(p-n\sqrt{p})}$$

and $p=4+n^2\in\mathbb{N}$ being a prime number. If $f(x)=x^4+bx^2+d\in\mathbb{Z}[x]$ is irreducible, then the Galois group of $f(x)$ can be V, C_4 or D_4, where V is the Klein 4-group, C_4 is the cyclic group of order 4, and D_4 is the dihedral group of order 8. If $f(x)=x^4+px^2+p$ with p a prime number and $\alpha^4+p\alpha^2+p=0$, then, according to Theorem 3 in [11], $K=\mathbb{Q}(\alpha)/\mathbb{Q}$ is cyclic if and only if $p=4+n^2$. Hardy et al. (see [9]) show that any cyclic quartic field can be expressed in a unique way as

$$\mathbb{Q}\Big(\sqrt{A(D+B\sqrt{D})}\Big),$$

where $A,B,C,D\in\mathbb{Z}$ are such that A is an odd squarefree integer, $D=B^2+C^2$ is squarefree, $B>0$, $C>0$ and A, D are relatively prime. Hudson and Williams (see [10]) give an integral basis for the integer ring of $K=\mathbb{Q}\Big(\sqrt{A(D+B\sqrt{D})}\Big)$. In our case, $K=\mathbb{Q}(\alpha)$. Since

$$\alpha'=\frac{n+2}{2}\alpha+\frac{\sqrt{p}}{2}\alpha,$$

then $\mathbb{Q}(\alpha')\subset\mathbb{Q}(\alpha)$. But $\mathrm{Irr}(\alpha',\mathbb{Q})=x^4+2px^2+n^2p$, so

$$K=\mathbb{Q}(\alpha)=\mathbb{Q}(\alpha'),\quad \alpha'=\sqrt{-(p+2\sqrt{p})},\quad \beta'=\sqrt{-(p-2\sqrt{p})},$$

where $p=4+n^2$ is a rational prime. According to the unique theorem in [10], an integral basis for $\mathcal{O}_K$ is as follows: if $n\equiv 3 \pmod 4$ then

$$\omega_1=1,\quad \omega_2=\frac{1+\sqrt{p}}{2},\quad \omega_3=\frac{1+\sqrt{p}+\alpha'+\beta'}{4},\quad \omega_4=\frac{1-\sqrt{p}+\alpha'-\beta'}{4}$$

and if $n \equiv 1 \pmod 4$ then

$$\omega_1 = 1, \quad \omega_2 = \frac{1+\sqrt{p}}{2}, \quad \omega_3 = \frac{1+\sqrt{p}+\alpha'-\beta'}{4}, \quad \omega_4 = \frac{1-\sqrt{p}+\alpha'+\beta'}{4}.$$

In any case $\delta_K = p^3$, and so p is the only ramified prime.

Theorem 2.1. *Let $K = \mathbb{Q}(\alpha)$ with*

$$\alpha = \sqrt{-\frac{1}{2}(p - n\sqrt{p})}.$$

Then $p\mathcal{O}_K = \langle\alpha\rangle^4$.

Proof. We have

$$\operatorname{ind}(\alpha) = \sqrt{\frac{D(\alpha)}{\delta_K}} = \sqrt{\frac{2^4 n^4 p^3}{p^3}} = 2^2 n^2,$$

then $\operatorname{ind}(\alpha) \not\equiv 0 \pmod p$. Since $\operatorname{Irr}(\alpha, \mathbb{Q}) = x^4 + px^2 + p$, by Theorem 1.1, $p\mathcal{O}_K = \langle p, \alpha\rangle^4 = \langle\alpha\rangle^4$. □

Since K is a Galois extension, then any prime $q \neq p$ does not ramify, i.e. $e = 1$ and $fg = 4$, so we have $g = 1$, $g = 2$ or $g = 4$.

On the other hand, Engstrom in [6] shows that for any quartic number field K, $\operatorname{ind}(K) = 1, 2, 3, 4, 6, 12$. Sperman and Williams in Theorem A (see [14]) show that, in the cyclic case, $\operatorname{ind}(K)$ assumes all of these values and give necessary and sufficient conditions for each to occur. In our case, according to Theorem A of [14], $\operatorname{ind}(K) = 1, 3$.

Theorem 2.2. *Let $K = \mathbb{Q}(\alpha)$ with $p = 4 + n^2$ be a rational prime. Then $\operatorname{ind}(K) = 3$ if and only if $3 \mid n$.*

Proof. By Theorem A of [14], we have that if $p \equiv 2 \pmod 3$, then $\operatorname{ind}(K) = 1$; and if $p \equiv 1 \pmod 3$, then $\operatorname{ind}(K) = 3$. If $\operatorname{ind}(K) = 3$, then $p \not\equiv 2 \pmod 3$. Since $p = 4 + n^2 \geqslant 5$, then $p \equiv 1 \pmod 3$. Therefore $n \equiv 0 \pmod 3$. If $n = 3t$ for some $t \in \mathbb{Z}$, we have

$$p = 4 + 9t^2 \equiv 1 \pmod 3,$$

so $\operatorname{ind}(K) = 3$. □

3. Factoring $q \neq p$

Let $q \in \mathbb{N}$ be a rational prime number. To use Dedekind's theorem to factorize $q\mathcal{O}_K$ in $\mathcal{O}_K$ where $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\alpha')$, we need that $\operatorname{ind}(\alpha) \not\equiv 0 \pmod q$ or $\operatorname{ind}(\alpha') \not\equiv 0 \pmod q$, but if

$$\operatorname{ind}(\alpha) = 2^2 n^2, \quad \operatorname{ind}(\alpha') = 2^6 n,$$

then we can factorize any prime $q \neq 2$, $q \neq p$ and $q \nmid n$.

Theorem 3.1. *Let $K = \mathbb{Q}(\alpha)$ and q be a rational prime such that $q \neq 2$ and $q \nmid n$. Then:*

(1) *If $\left(\frac{p}{q}\right) = -1$, then $q\mathcal{O}_K = \langle q, \alpha^4 + p\alpha^2 + p\rangle$ is a prime ideal of $\mathcal{O}_K$.*
(2) *If $p \equiv t^2 \pmod q$ for some $t \in \mathbb{Z}$ and $\left(\frac{-p-2t}{q}\right) = -1$, then*

$$q\mathcal{O}_K = \langle q, \alpha^2 + a_1\alpha + a_0\rangle\langle q, \alpha^2 + b_1\alpha + b_0\rangle,$$

where $a_1, a_0, b_1, b_0 \in \mathbb{Z}$ satisfy

$$x^4 + px^2 + p \equiv (x^2 + a_1x + a_0)(x^2 + b_1x + b_0) \pmod q.$$

(3) *If $p \equiv t^2 \pmod q$ for some $t \in \mathbb{Z}$ and $\left(\frac{-p-2t}{q}\right) = 1$, then*

$$q\mathcal{O}_K = \langle q, \alpha + a_0\rangle\langle q, \alpha + b_0\rangle\langle q, \alpha + a_1\rangle\langle q, \alpha + b_1\rangle,$$

where $a_1, a_0, b_1, b_0 \in \mathbb{Z}$ satisfy

$$x^4 + px^2 + p \equiv (x + a_0)(x + b_0)(x + a_1)(x + b_1) \pmod q.$$

Proof. We prove only the first assertion, the others are similar. As $\operatorname{ind}(\alpha) \not\equiv 0 \pmod q$, we can use Dedekind's theorem. Since

$$\left(\frac{p}{q}\right) = -1,$$

then

$$\left(\frac{p^2 - 4p}{q}\right) = -1,$$

so by Theorem 3 (iv) in [5], we have that $x^4 + px^2 + p$ is irreducible in $\mathbb{F}_q[x]$. Therefore $q\mathcal{O}_K = \langle q, \alpha^4 + p\alpha^2 + p\rangle$. □

Note that if $3 \nmid n$, then $\operatorname{ind}(K) = 1$. By (1) above, we have $3\mathcal{O}_K = \langle 3 \rangle$. If $q \mid n$, then $\operatorname{ind}(\alpha) \equiv \operatorname{ind}(\alpha') \equiv 0 \pmod{q}$. So we need to find new generators that satisfy the hypothesis of Theorem 1.1.

Proposition 3.1. *Let $K = \mathbb{Q}(\alpha')$ be with $\alpha' = \sqrt{-(p+2\sqrt{p})}$ and $\beta' = \sqrt{-(p-2\sqrt{p})}$. Then:*

(i) *$\mathbb{Q}(\alpha') = \mathbb{Q}(\alpha' + t\beta')$ for all $t \in \mathbb{Z}$;*

(ii) *$\operatorname{ind}(\alpha' + t\beta') = 2^6(4t - n(1-t^2))(t^2 - 1 - tn)^2$.*

Proof. Since $\alpha', \beta' \in \mathbb{Q}(\alpha')$, then $\mathbb{Q}(\alpha' + t\beta') \subseteq \mathbb{Q}(\alpha')$. By Theorem 2 (iii) in [11] we have that

$$h(x) = x^4 + 2p(1+t^2)x^2 + p(4t - n(1-t^2))^2$$

is irreducible in $\mathbb{Q}[x]$. Since $h(\alpha' + t\beta') = 0$, then $h(x) = \operatorname{Irr}(\alpha' + t\beta', \mathbb{Q})$. Therefore $[\mathbb{Q}(\alpha' + t\beta') : \mathbb{Q}] = 4$ and so $\mathbb{Q}(\alpha') = \mathbb{Q}(\alpha' + t\beta')$.

For the second assertion we know that $\operatorname{ind}(\alpha' + t\beta') = \sqrt{D(\alpha' + t\beta')/\delta_K}$ and $D(\alpha' + t\beta') = N(h'(\alpha' + t\beta'))$, where $h'(x)$ is the derivative of $h(x)$. Since

$$h'(\alpha' + t\beta') = 4(\alpha' + t\beta')((\alpha' + t\beta')^2 + p(1+t^2)) = 4(\alpha' + t\beta')(2t^2 - 2 - 2tn)\sqrt{p},$$

then $N(h'(\alpha' + t\beta')) = 4^4 p(4t - n(1-t^2))^2(2t^2 - 2 - 2tn)^4 p^2$.

Thus

$$\operatorname{ind}(\alpha' + t\beta') = 2^6(4t - n(1-t^2))(t^2 - 1 - tn)^2.$$

$\square$

We note that if $q \mid n$, then $q \mid \operatorname{ind}(\alpha' + t\beta')$ if and only if $q \mid t-1$, $q \mid t$ or $q \mid t+1$.

Theorem 3.2. *Let $K = \mathbb{Q}(\alpha')$ and q be a rational prime such that $q \neq 2, 3$ and $q \mid n$. If $\theta_1 = \alpha' + 2\beta'$, then:*

(1) *If $q \equiv 5, 7 \pmod 8$, then $q\mathcal{O}_K = \langle q, \theta_1^2 + a_1\theta_1 + a_0 \rangle \langle q, \theta_1^2 + b_1\theta_1 + b_0 \rangle$, where $a_1, a_0, b_1, b_0 \in \mathbb{Z}$ satisfy*

$$x^4 + 10px^2 + p(8+3n)^2 \equiv (x^2 + a_1x + a_0)(x^2 + b_1x + b_0) \pmod{q}.$$

(2) *If $q \equiv 1, 3 \pmod 8$, then $q\mathcal{O}_K = \langle q, \theta_1 + a_0 \rangle \langle q, \theta_1 + b_0 \rangle \langle q, \theta_1 + a_1 \rangle \langle q, \theta_1 + b_1 \rangle$, where $a_1, a_0, b_1, b_0 \in \mathbb{Z}$ satisfy*

$$x^4 + 10px^2 + p(8+3n)^2 \equiv (x + a_0)(x + b_0)(x + a_1)(x + b_1) \pmod{q}.$$

Proof. We note that for θ_1 it follows that $K = \mathbb{Q}(\theta_1)$ and $\operatorname{ind}(\theta_1) \not\equiv 0 \pmod{q}$. The proof is similar to that of Theorem 3.1. $\square$

Now we factorize $q = 2$ no matter what $\operatorname{ind}(K)$ is.

Proposition 3.2. *Let $K = \mathbb{Q}(\alpha')$ as in Proposition 3.1. Then:*

(i) *$\mathbb{Q}(\alpha') = \mathbb{Q}(\theta)$ with $\theta = \frac{1}{2}(1+\alpha')$;*

(ii) *$\operatorname{ind}(\theta) = n$, where $p = 4 + n^2 = 4k+1$.*

Proof. First note that $\mathbb{Q}(\theta) \subset \mathbb{Q}(\alpha')$. Let us consider

$$h(x) = x^4 - 2x^3 + 2(k+1)x^2 - (2k+1)x + k^2.$$

By Theorem 2 (iii) in [11],

$$h\Big(x + \frac{1}{2}\Big) = x^4 + \Big(-\frac{3}{2} + 2(k+1)\Big)x^2 + \Big(-\frac{3}{16} - \frac{k}{2} + k^2\Big)$$

is irreducible in $\mathbb{Q}[x]$. Therefore $h(x)$ is irreducible. Since $h(\theta) = 0$, we have

$$\operatorname{Irr}(\theta, \mathbb{Q}) = x^4 - 2x^3 + 2(k+1)x^2 - (2k+1)x + k^2$$

and $\mathbb{Q}(\alpha') = \mathbb{Q}(\theta)$. For the assertion (ii) remember that

$$D(\theta) = \det\begin{pmatrix} 4 & 2 & 1-p & \dfrac{1-3p}{2} \\ 2 & 1-p & \dfrac{1-3p}{2} & \dfrac{(p-1)^2}{4} \\ 1-p & \dfrac{1-3p}{2} & \dfrac{(p-1)^2}{4} & \dfrac{1+10p+5p^2}{8} \\ \dfrac{1-3p}{2} & \dfrac{(p-1)^2}{4} & \dfrac{1+10p+5p^2}{8} & \dfrac{1+45p+3p^2-p^3}{16} \end{pmatrix},$$

so $D(\theta) = n^2p^3$. Therefore $\operatorname{ind}(\theta) = \sqrt{n^2p^3/p^3} = n$. $\square$

As a consequence of (ii) above we have $2 \nmid \operatorname{ind}(\theta)$.

Theorem 3.3. *Let K be as in Proposition 3.1 and $\theta = \frac{1}{2}(1+\alpha')$. Then $2\mathcal{O}_K = \langle 2 \rangle$.*

Proof. Note that $\operatorname{Irr}(\theta) = x^4 - 2x^3 + 2(k+1)x^2 - (2k+1)x + k^2 \equiv x^4 + x + 1 \pmod{2}$ and $x^4 + x + 1$ is irreducible in $\mathbb{F}_2[x]$. Therefore by Dedekind's theorem $2\mathcal{O}_K = \langle 2, \theta^4 + \theta + 1 \rangle$. Finally $N(\langle 2, \theta^4 + \theta + 1 \rangle) = 2^4$, $N(\langle 2 \rangle) = N(2) = 2^4$ and $\langle 2 \rangle \subseteq \langle 2, \theta^4 + \theta + 1 \rangle$, so $2\mathcal{O}_K = \langle 2, \theta^4 + \theta + 1 \rangle = \langle 2 \rangle$ is principal. $\square$

4. Factoring 3 with $\operatorname{ind}(K) = 3$

In Section 3 we obtained the factorization of $3\mathcal{O}_K$ in the case $\operatorname{ind}(K) = 1$. Remember that $3 \mid n$ if and only if $\operatorname{ind}(K) = 3$. If 3 is a common index divisor of K, we can't use Dedekind's theorem. We find new generators.

Lemma 4.1. *Let $K = \mathbb{Q}(\alpha')$ with $\alpha' = \sqrt{-(p + 2\sqrt{p})}$ and $\{\omega_1, \omega_2, \omega_3, \omega_4\}$ be the integral basis as in Section 2. Then:*

(i) $\frac{1}{2}(3 + \alpha') = 1 + \omega_3 + \omega_4$;
(ii) $\frac{1}{2}(5 - \alpha') = 3 - \omega_3 - \omega_4$;
(iii) $\frac{1}{2}(5 + \alpha') = 2 + \omega_3 + \omega_4$.

Proof. We prove only one case, the others are similar. If $n \equiv 3 \pmod 4$, then

$$\omega_1 = 1, \quad \omega_2 = \frac{1 + \sqrt{p}}{2}, \quad \omega_3 = \frac{1 + \sqrt{p} + \alpha' + \beta'}{4}, \quad \omega_4 = \frac{1 - \sqrt{p} + \alpha' - \beta'}{4}.$$

Therefore $1 + \omega_3 + \omega_4 = \frac{1}{2}(3 + \alpha')$. □

Proposition 4.1. *Let $K = \mathbb{Q}(\alpha')$ be as in Lemma 4.1. The ideals*

$$M = \left\langle 3, \frac{3 + \alpha'}{2} \right\rangle, \quad P_1 = \left\langle 3, \frac{5 - \alpha'}{2} \right\rangle, \quad P_2 = \left\langle 3, \frac{5 + \alpha'}{2} \right\rangle$$

satisfy:

(i) $M = 3\mathbb{Z} + (3 + 3\omega_3)\mathbb{Z} + (-4 + \omega_2 - 3\omega_3)\mathbb{Z} + (1 + \omega_3 + \omega_4)\mathbb{Z}$;
(ii) $P_1 = 3\mathbb{Z} + (-17 + \omega_3)\mathbb{Z} + (-8 + \omega_2 + \omega_3)\mathbb{Z} + (-3 + \omega_3 + \omega_4)\mathbb{Z}$;
(iii) $P_2 = 3\mathbb{Z} + (-1 + \omega_3)\mathbb{Z} + (\omega_2 + 3\omega_3)\mathbb{Z} + (2 + \omega_3 + \omega_4)\mathbb{Z}$.

Proof. Only we comment the proof of assertion (i). Since $1+\omega_3+\omega_4 = \frac{1}{2}(3+\alpha')$, then $M \subset 3\mathbb{Z} + (3+3\omega_3)\mathbb{Z} + (-4+\omega_2-3\omega_3)\mathbb{Z} + (1+\omega_3+\omega_4)\mathbb{Z}$. The other statement is obtained by solving a linear equation system. The other assertions are similar. □

Corollary 4.1. *Let $K = \mathbb{Q}(\alpha')$, M, P_1 and P_2 be as in Proposition 4.1. Then $N(M) = 9$, $N(P_1) = N(P_2) = 3$.*

Proof. Proposition 4.1 provides an integral basis. Next calculate the discriminant. □

Since $N(P_1) = N(P_2) = 3$ we have that P_1 and P_2 are prime ideals of $\mathcal{O}_K$ and $P_1 \cap \mathbb{Z} = P_2 \cap \mathbb{Z} = 3\mathbb{Z}$. Also it is clear that $P_1 \neq P_2$ and $M \neq \mathcal{O}_K$.

Theorem 4.1. *Let $K = \mathbb{Q}(\alpha')$ with $\alpha' = \sqrt{-(p + 2\sqrt{p})}$. Let us consider*

$$M = \Big\langle 3, \frac{3+\alpha'}{2} \Big\rangle, \quad P_1 = \Big\langle 3, \frac{5-\alpha'}{2} \Big\rangle, \quad P_2 = \Big\langle 3, \frac{5+\alpha'}{2} \Big\rangle.$$

Then

$$3\mathcal{O}_K = MP_1P_2.$$

P r o o f. First we show that

$$P_1P_2 = \Big\langle 9, 6 + 3\omega_3 + 3\omega_4, 9 - 3\omega_3 - 3\omega_4, \frac{23+p}{4} + \omega_2 \Big\rangle = \langle 3, -\omega_2 \rangle,$$

where $\{1, \omega_2, \omega_3, \omega_4\}$ is an integral basis as in Section 2, no matter if $n \equiv 1$ or $3 \pmod 4$.

In our case, $\operatorname{ind}(K) = 3$ and $p = 4k + 1$ implies that $k = 3m$ for some $m \in \mathbb{Z}$. Since $\frac{1}{4}(23 + p) + \omega_2 = 3(2 + m) + \omega_2 \in \langle 3, -\omega_2 \rangle$, we have $P_1P_2 \subset \langle 3, -\omega_2 \rangle$. Likewise

$$3 = 2(9) - 3\Big(\frac{5+\alpha'}{2}\Big) - 3\Big(\frac{5-\alpha'}{2}\Big)$$

and

$$\frac{23+p}{4} = 3(2+m),$$

then

$$\omega_2 = \Big(\frac{23+p}{4} + \omega_2\Big) - \Big(\frac{23+p}{4}\Big) \in P_1P_2$$

and therefore, $\langle 3, -\omega_2 \rangle \subset P_1P_2$.

Finally, as $-\omega_2 = \frac{1}{4}(\alpha'^2 + (p-2))$ then

$$MP_1P_2 = \Big\langle 9, 3\frac{3+\alpha'}{2}, 3\frac{\alpha'^2 + (p-2)}{4}, \frac{3+\alpha'}{2}\frac{\alpha'^2 + (p-2)}{4} \Big\rangle.$$

The following numbers are in $3\mathcal{O}_K$:

$$\frac{3+\alpha'}{2}\frac{\alpha'^2 + (p-2)}{4}, \quad 9, \quad 3\frac{\alpha'^2 + (p-2)}{4}, \quad 3\frac{3+\alpha'}{2},$$

so $MP_1P_2 \subseteq 3\mathcal{O}_K$. Since $N(MP_1P_2) = N(3\mathcal{O}_K) = 3^4$, then $MP_1P_2 = 3\mathcal{O}_K$. $\square$

In the next result we give an integral basis of some prime ideals that will help us to decompose the ideal M.

Proposition 4.2. *Let K be as in Theorem 4.1. If $n \equiv 3 \pmod 4$ let's consider the ideals $Q_1 = \langle 3, \omega_2 - \omega_3 \rangle$, $Q_2 = \langle 3, -\omega_3 \rangle$ and if $n \equiv 1 \pmod 4$, let's consider the ideals $Q_1' = \langle 3, -1 - \omega_4 \rangle$, $Q_2' = \langle 3, 2 - \omega_2 - \omega_4 \rangle$. Then:*

(i) $Q_1 = 3\mathbb{Z} + (1 - \omega_3)\mathbb{Z} + (\omega_2 - \omega_3)\mathbb{Z} + (1 + \omega_2 + \omega_4)\mathbb{Z}$;

(ii) $Q_2 = 3\mathbb{Z} + (2 + \omega_2 - \omega_3)\mathbb{Z} + (\omega_2 + \omega_4)\mathbb{Z} - \omega_3\mathbb{Z}$;

(iii) $Q_1' = 3\mathbb{Z} + (-1 - \omega_4)\mathbb{Z} + \omega_3\mathbb{Z} + (3 - \omega_2 - \omega_4)\mathbb{Z}$;

(iv) $Q_2' = 3\mathbb{Z} + (1 - \omega_4)\mathbb{Z} + (2 + \omega_3)\mathbb{Z} + (-2 + \omega_2 + \omega_4)\mathbb{Z}$.

Proof. The proof is similar to the proof of Proposition 4.1. $\square$

By Proposition 4.2 it is clear that $N(Q_1) = N(Q_2) = N(Q_1') = N(Q_2') = 3$ and therefore Q_1, Q_2, Q_1', Q_2' are prime ideals.

Theorem 4.2. *Let $K = \mathbb{Q}(\alpha')$ with $\alpha' = \sqrt{-(p + 2\sqrt{p})}$ and Q_1, Q_2, Q_1', Q_2' be as in Proposition 4.2. Then*

$$M = \begin{cases} Q_1 Q_2 & \text{if } n \equiv 3 \pmod 4, \\ Q_1' Q_2' & \text{if } n \equiv 1 \pmod 4. \end{cases}$$

Proof. If $n \equiv 3 \pmod 4$, we show that $Q_1 Q_2 = \langle 3, 1 + \omega_3 + \omega_4 \rangle = M$. First we note that 9, $-3\omega_3$, $3\omega_2 - 3\omega_3 \in \langle 3,\ 1 + \omega_3 + \omega_4 \rangle$. As $n = 4l + 3$ for some $l \in \mathbb{Z}$, we have $-\omega_3(\omega_2 - \omega_3) = (-3l^2 - 4l - 2) - (1 + l)\omega_2$. By Proposition 4.1, $\{3, 3 + 3\omega_3, -4 + \omega_2 - 3\omega_3, 1 + \omega_3 + \omega_4\}$ is an integral basis of M and

$$(-3l^2 - 4l - 2) - (1 + l)\omega_2 = 3x_1 + (3 + 3\omega_3)x_2 + (-4 + \omega_2 - 3\omega_3)x_3 + (1 + \omega_3 + \omega_4)x_4,$$

where $x_1 = \frac{1}{3}(-3l^2 - 5l - 3)$, $x_2 = -l - 1$, $x_3 = -l - 1$, $x_4 = 0 \in \mathbb{Z}$. Therefore $-\omega_3(\omega_2 - \omega_3) \in M$ and $Q_1 Q_2 \subseteq M$. Since $N(Q_1 Q_2) = N(M) = 9$ we conclude that $Q_1 Q_2 = M$. The factorization $M = Q_1' Q_2'$ in the case $n \equiv 1 \pmod 4$ is similar. $\square$

Acknowledgement. We thank the referee for the valuable comments, which improved the presentation of this work.

References

[1] *Ş. Alaca, B. K. Spearman, K. S. Williams*: The factorization of 2 in cubic fields with index 2. Far East J. Math. Sci. (FJMS) *14* (2004), 273–282. zbl MR

[2] *Ş. Alaca, K. S. Williams*: Introductory Algebraic Number Theory. Cambridge University Press, Cambridge, 2004. zbl MR doi

[3] *H. Cohen*: A Course in Computational Algebraic Number Theory. Graduate Texts in Mathematics 138. Springer, Berlin, 1993. zbl MR doi

[4] *K. Conrad*: Factoring after Dedekind. Available at `https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekindf.pdf`, 7 pages.

[5] *E. Driver, P. A. Leonard, K. S. Williams*: Irreducible quartic polynomials with factorizations modulo p. Am. Math. Mon. *112* (2005), 876–890. zbl MR doi

[6] *H. T. Engstrom*: On the common index divisors of an algebraic field. Trans. Am. Math. Soc. *32* (1930), 223–237. zbl MR doi

[7] *J. Guàrdia, J. Montes, E. Nart*: Higher Newton polygons in the computation of discriminants and prime ideals decomposition in number fields. J. Théor. Nombres Bordx. *23* (2011), 667–696. zbl MR doi

[8] *J. Guàrdia, J. Montes, E. Nart*: Newton polygons of higher order in algebraic number theory. Trans. Am. Math. Soc. *364* (2012), 361–416. zbl MR doi

[9] *K. Hardy, R. H. Hudson, D. Richman, K. S. Williams, N. M. Holtz*: Calculation of the Class Numbers of Imaginary Cyclic Quartic Fields. Carleton-Ottawa Mathematical Lecture Note Series 7. Carleton University, Ottawa, 1986. zbl

[10] *R. H. Hudson, K. S. Williams*: The integers of a cyclic quartic field. Rocky Mt. J. Math. *20* (1990), 145–150. zbl MR doi

[11] *L.-C. Kappe, B. Warren*: An elementary test for the Galois group of a quartic polynomial. Am. Math. Mon. *96* (1989), 133–137. zbl MR doi

[12] *P. Llorente, E. Nart*: Effective determination of the decomposition of the rational primes in a cubic field. Proc. Am. Math. Soc. *87* (1983), 579–585. zbl MR doi

[13] *J. Montes*: Polígonos de Newton de orden superior y aplicaciones aritméticas: Dissertation Ph.D. Universitat de Barcelona, Barcelona, 1999. (In Spanish.)

[14] *B. K. Spearman, K. S. Williams*: The index of a cyclic quartic field. Monatsh. Math. *140* (2003), 19–70. zbl MR doi

Authors' address: *Julio Pérez-Hernández*, *Mario Pineda-Ruelas*, Departamento de Matemáticas, Universidad Autónoma Metropolitana-Iztapalapa, Avenida San Rafael Atlixco No. 186, Col. Vicentina, CP 09340, Ciudad de México, Mexico, e-mail: `galois60@gmail.com`, `mpr@xanum.uam.mx`.