Bol. Soc. Paran. Mat.
©SPM –ISSN-2175-1188 on line
SPM: www.spm.uem.br/bspm

(3s.) **v. 2022 (40)** : 1–7.
ISSN-0037-8712 in press
doi:10.5269/bspm.42373

On Power Integral Bases for Certain Pure Sextic Fields

Lhoussain El Fadil

Abstract: In their paper [1], Shahzad Ahmad et. al. gave a characterization on any pure sextic number field $\mathbb{Q}(m^{1/6})$ with square-free integers $m \neq 1$ satisfying $m \not\equiv \pm 1 (\text{mod } 9)$ to have a power integral bases or to do not. In this paper, for these results, we give a new easier proof than that given in [1]. We further investigate the cases $m \equiv 1 (\text{mod } 4)$ independently to the satisfaction of $m^2 \equiv 1 (\text{mod } 9)$, $m \equiv 1 (\text{mod } 9)$, and the number fields defined by $x^{2^r 3^t} - m$, where r, t are two non-negative integers with $1 \leq r + t$, and m is a square free integer are investigated. The proposed proofs are based on Dedekind's criterion and on prime ideal factorization.

Key Words: Power integral basis, Sextic number field, Dedekind's criterion, Prime ideal factorization.

Contents

1. Introduction

Let K be a number field defined by a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$. We denote by $\mathbb{Z}_K$ its ring of integers . For any element $\theta \in \mathbb{Z}_K$, we said that θ generates a power integral basis of K if $(1, \theta, \cdots, \theta^{n-1})$ is a $\mathbb{Z}$-basis of $\mathbb{Z}_K$, where n is the degree $[K : \mathbb{Q}]$; $\mathbb{Z}_K = \mathbb{Z}[\theta]$. When a field K has a power integral basis, the field K is said to be monogenic, and not monogenic otherwise. It is called a problem of Hasse to characterize whether the ring of integers of an algebraic number field has a power integral basis or does not [6,10,9]. Let $K = \mathbb{Q}(m^{1/6})$ be a pure sextic field such that m is a square-free integer. In [12], It was proved that for $m \equiv 1 (\text{mod } 4)$ satisfying $m \not\equiv \pm 1 (\text{mod } 9)$, K is not monogenic. In [1], if $m \not\equiv 1 (\text{mod } 4)$ and $m \not\equiv \pm 1 (\text{mod } 9)$, then based on the existence of power relative integral bases of their quadratic and cubic subfields, it was shown that K is monogenic. In this paper, based on prime ideal factorization, we prove that if m is a square free integer such that $m \equiv 1 (\text{mod } 4)$ or $m \equiv 1 (\text{mod } 9)$, then K is not monogenic. If $m \not\equiv 1 (\text{mod } 4)$ and $m \not\equiv \pm 1 (\text{mod } 9)$, then we show that K is monogenic.

2. Main results

Our below main theorem gives a precise test on any square free integer $m \neq 1$ for the integral closedness of $\mathbb{Z}[\alpha]$, where α is a complex root of $f(x) = x^n - m \in \mathbb{Z}[x]$.

Theorem 2.1. *Let $K = \mathbb{Q}(\alpha)$ be a number field, where α is a root of an irreducible polynomial $f(x) = x^n - m \in \mathbb{Z}[x]$, with $m \neq 1$ is a square free integer.*
If for every rational prime integer p dividing n and not dividing m, $\nu_p(m^{p-1} - 1) = 1$, then $\mathbb{Z}[\alpha]$ is integrally closed.

Corollary 2.2. *Under the hypothesis of Theorem 2.1,*

1. *Let $f(x) = x^{2^r} - m \in \mathbb{Z}[x]$, where r is a natural integer. If $m \equiv 2$ or $3 (\text{mod } 4)$, then $\mathbb{Z}[\alpha]$ is the ring of integers of K.*

2. *Let $f(x) = x^{3^r} - m \in \mathbb{Z}[x]$, where r is a natural integer. If $m \not\equiv \mp 1 (\text{mod } 9)$, then $\mathbb{Z}[\alpha]$ is the ring of integers of K.*

2010 *Mathematics Subject Classification:* 11R04, 11R16, 11R21.
Submitted April 14, 2018. Published November 10, 2020

Typeset by $\mathcal{B}^{\mathcal{S}}_{\mathcal{M}}\mathcal{P}$ style.
© Soc. Paran. de Mat.

3. *Let* $f(x) = x^{2^r 3^t} - m \in \mathbb{Z}[x]$, *where* r *and* t *are natural integers. If* $m \equiv 2$ *or* $3 (\text{mod } 4)$ *and* $m \not\equiv \mp 1 (\text{mod } 9)$, *then* $\mathbb{Z}[\alpha]$ *is the ring of integers of* K.

Proposition 2.3. *Under the above hypothesis, let* $f(x) = x^6 - m \in \mathbb{Z}[x]$. *If* $m \not\equiv 1 (\text{mod } 4)$ *and* $m \not\equiv \mp 1 (\text{mod } 9)$, *then* K *is monogenic. Especially,* α *generates a power integral basis of* $\mathbb{Z}_K$.

Theorem 2.4. *Under the above hypothesis, let* $f(x) = x^6 - m \in \mathbb{Z}[x]$. *If* $m \equiv 1 (\text{mod } 4)$ *or* $m \equiv 1 (\text{mod } 9)$, *then number* K *is not monogenic.*

Remark 2.1. 1. *In [1], it was shown that if* $m \equiv 1 (\text{mod } 4)$ *satisfying* $m \not\equiv \mp 1 (\text{mod } 9)$, *then* $\mathbb{Z}_K$ *is not monogenic. Here in Theorem 2.4, we show that if* $m \equiv 1 (\text{mod } 4)$, *then* $\mathbb{Z}_K$ *is not monogenic independently to the satisfaction of the condition* $m \not\equiv \mp 1 (\text{mod } 9)$.

2. *The investigation given in [1] does not cover the case* $m \equiv \mp 1 (\text{mod } 9)$.

3. Proofs

Now, we tackle the proofs of our main theorem:

Proof: of Theorem 2.1.
Since the discriminant of $f(x)$ is $\triangle(f) = \mp n^n m^{n-1}$, thanks to the formula linking the discriminant, the index and $\triangle(f)$, $\mathbb{Z}[\alpha]$ is integrally closed if and only if p does not divide the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$ for every rational prime factor p dividing nm. Let p be a rational prime integer dividing m. Then according to Dedekind's criterion notations [14,3], $f(x) \equiv x^n (\text{mod } p)$ holds and $M(x) = \frac{f(x)-x^n}{p} = \frac{-m}{p}$. As m is square free, $\bar{x}$ does not divide $\overline{M(x)}$ modulo p. Thus p does not divide the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. Now, let p be a rational prime integer dividing n and not dividing m. Set $n = p^r q$, where $q \in \mathbb{N}$ such that p does not divide q. Then by the little Fermat's theorem, $f(x) \equiv (x^{qp^{r-1}} - m)^p (\text{mod } p)$ and $f(x) = ((x^{qp^{r-1}} - m) + m)^p - m = \sum_{k=0}^{p-1} C_k^p m^k (x^{qp^{r-1}} - m)^{p-k} + m^p - m$, where C_k^p is the k^{th} binomial coefficient. As $m^p - m \equiv 0 (\text{mod } p)$, $f(x) \equiv ((x^{qp^{r-1}} - m)^p$. Let $\overline{(x^{qp^{r-1}} - m)} = \prod_{i=1}^t \bar{g_i}^{e_i}(x)$ be the factorization of $\overline{(x^{qp^{r-1}} - m)}$ into powers of irreducible polynomials in $\mathbb{F}_p[x]$, where every $g_i(x) \in \mathbb{Z}[x]$ is a monic polynomial. As p divides all coefficients except the leading one, of $f(x)$ with respect to $(x^{qp^{r-1}} - m)$, it follows that if $\nu_p(m^{p-1} - 1) = 1$, then p does not divide the index $(\mathbb{Z}_K : \mathbb{Z}[\alpha])$. □

Lemma 3.1. *Under the hypothesis and notations of Theorem 2.4,*

1. *If* $m \equiv 1 (\text{mod } 8)$, *then* $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$ *is the factorization into product of prime ideals of* $\mathbb{Z}_K$, *with* $f_1 = f_2 = 1$ *and* $f_3 = f_4 = 2$ *being the respective residue degrees.*

2. *If* $m \equiv 5 (\text{mod } 8)$, *then* $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ *is the factorization into product of prime ideals of* $\mathbb{Z}_K$, *with* $f_1 = f_2 = f_3 = 2$ *being the respective residue degrees.*

3. *If* $m \equiv 1 (\text{mod } 9)$, *then* $3\mathbb{Z}_K = (\mathfrak{p}_1\mathfrak{p}_2)^2\mathfrak{p}_3\mathfrak{p}_4$ *is the factorization into product of prime ideals of* $\mathbb{Z}_K$, *with* $f_1 = f_2 = f_3 = f_4 = 1$ *being the respective residue degrees.*

In order to show Lemma 3.1, we recall some fundamental notions on Newton polygon techniques. In 1894, K. Hensel developed a powerful approach by showing that the primes of $\mathbb{Z}_K$ lying above a prime p are in one-to-one correspondence with irreducible factors of $f(x)$ in $\mathbb{Q}_p[x]$. For every prime ideal corresponding to any irreducible factor in $\mathbb{Q}_p[x]$, the ramification index and the residue degree together are the same as those of the local field defined by the irreducible factor [8]. So, in order to describe all prime ideals of $\mathbb{Z}_K$ lying above p, we have to factorize the polynomial $f(x)$ into irreducible factors in $\mathbb{Q}_p[x]$. The first step of the factorization is based on Hensel's lemma. Unfortunately, the factors provided by Hensel's lemma are not necessarily irreducible in $\mathbb{Q}_p[x]$. The Newton polygon's techniques could refine the factorization. Namely, the theorem of the polygon and the theorem of the residual polynomial say that we can factorize any factor provided by Hensel's lemma, with as many sides of the polygon and as many irreducible factors of each residual polynomial. For more details, see [7, Th. 1.15 and Th. 1.19].

For any rational prime integer p and for any monic polynomial $\phi \in \mathbb{Z}[x]$ *whose reduction* modulo p is irreducible in $\mathbb{F}_p[x]$, let $\mathbb{F}_\phi$ be the field $\frac{\mathbb{F}_p[x]}{(\bar{\phi})}$. For any monic polynomial $f(x) \in \mathbb{Z}[x]$, upon to the

Euclidean division by successive powers of ϕ, we can expand $f(x)$ as follows : $f(x)=\sum_{i=0}^{l} a_i(x)\phi(x)^{l-i}$, called the ϕ-expansion of $f(x)$ (for every i, $deg(a_i(x)) < deg(\phi)$).

For every $i \neq j = 0,\dots,l$, let $a_i = a_i(x)$ and $\mu_{ij} = \frac{\nu_p(a_i)-\nu_p(a_j)}{i-j} \in \mathbb{Q}$. Let us construct by induction the following integers $i_0 = 0$, $i_1 =$ max $\{j = 1,\dots l,\ \mu_{0i_1} \le \mu_{0j}\}$, if $i_j < l$, then $i_{j+1} =$ max $\{i = i_j+1,\dots l,\ \mu_{i_j i_{j+1}} \le \mu_{i_j i}\}$. Repeat this process until to get $i_r = l$. For every $j = 1,\dots r$, let S_j be the segment joining the points $A_{j-1} = (i_{j-1}, \nu(a_{i_{j-1}}))$ and $A_j = (i_j, \nu(a_{i_j}))$ in the euclidean plane. The rational number $\lambda_j = \frac{\nu_p(a_{i_j})-\nu_p(a_{i_{j-1}})}{i_j - i_{j-1}} \in \mathbb{Q}$ is called the slope of S_j, $l(S_j) = i_j - i_{j-1}$ is its length, and $h(S_j) = \lambda_j l(S_j)$ is its height. In what follows $\nu(a_{i_j}) = \nu(a_{i_{j-1}}) + l_j\lambda_j$. The ϕ-Newton polygon of f, denoted by $N_\phi(F)$, is the process of joining the segments $S_1,\dots,S_r$ ordered by the increasing slopes, which can be expressed as $N_\phi(f) = S_1 + \cdots + S_t$. Notice that $N_\phi(f) = S_0 + \cdots + S_t$ is only a notation and not the sum in the Euclidean plane. The segments $S_1,\dots,$ and S_r are called the sides of $N_\phi(f)$. For every side S of the polygon $N_\phi(f)$, $l(S)$ is the length of its projection to the x-axis and $h(S)$ is the length of its projection to the y-axis. The principal part of $N_\phi(f)$, denoted ${N_\phi}^{+}(f)$, is the part of the polygon $N_\phi(f)$, which is determined by joining all sides of positive slopes. For instance, for $p = 3$, $\phi = x^2 + x - 1$ which is irreducible modulo 3, and $f(x) = \phi^7 + (x-1)\phi^5 + 12x\phi^4 + (27x+6)\phi^3 + 9(x-2)\phi^2 + (18x+162)\phi + 3^3$,

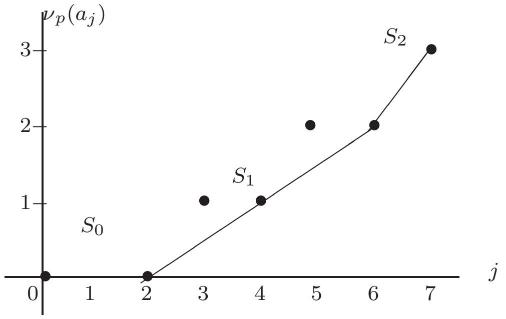

Figure 1

So, $i_0 = 0$, $i_1 = 2$, $i_2 = 6$, and $i_3 = 7$, $N_\phi(f) = S_0 + S_1 + S_2$ (has 3 sides S_0, S_1, and S_2) with respective slopes $\lambda_0 = 0$, $\lambda_1 = 1/2$, and $\lambda_2 = 1$. Thus ${N_\phi}^{+}(f) = S_1 + S_2$.

For every side S of $N_\phi(f)$, with initial point (s, u_s) and length l, let $d = l/e$, called the degree of S. For every $0 \le i \le l$, we attach the following residual coefficient $c_i \in \mathbb{F}_\phi$:

$$c_i = \begin{cases} 0, & \text{if } (s+i, u_{s+i}) \text{ lies strictly above } S \text{ or } u_{s+i} = \infty, \\ \left(\dfrac{a_{s+i}(x)}{p^{u_{s+i}}}\right) \pmod{(p, \phi(x))}, & \text{if } (s+i, u_{s+i}) \text{ lies on } S. \end{cases}$$

where $(p, \phi(x))$ is the maximal ideal of $\mathbb{Z}[x]$ generated by p and ϕ. That means if $(s+i, u_{s+i})$ lies on S, then $c_i = \overline{\dfrac{a_{s+i}(\beta)}{p^{u_{s+i}}}}$, where β is a root of ϕ.

Let $\lambda = h/e$ be the slope of S, where h and e are positive coprime integers, and let $d = l/e$ be the degree of S. Notice that, the points with integer coordinates lying in S are exactly $(s, u_s), (s+e, u_s + h), \cdots, (s+de, u_s+dh)$. Thus, if i is not a multiple of e, then $(s+i, u_{s+i})$ does not lie in S, and so, $c_i = 0$. Let $f_S(y) = t_0 y^d + t_1 y^{d-1} + \cdots + t_{d-1}y + t_d \in \mathbb{F}_\phi[y]$ be the residual polynomial of $f(x)$ associated to the side S, where for every $i = 0,\dots,d$, $t_i = c_{ie}$.

Remark 3.1. *Note that if $\nu(a_{s+i}(x)) = 0$ and $\phi = x$, then $\mathbb{F}_\phi = \mathbb{F}_p$ and $c_i = \overline{a_{s+i}}(\text{mod } p)$. Thus this notion of residual coefficient generalizes the reduction modulo a maximal ideal. If $\lambda = 0$, then for every $i = 0,\dots,d$, $(s+i, u_{s+i})$ lies on S if and only if $\nu(a_{s+i}(x)) = 0$. Thus if $\lambda = 0$ and $\phi = x$, then $c_i = \overline{a_{s+i}}(\text{mod } p)$ and $f_S(y) \in \mathbb{F}_p[y]$ coincides with the reduction of $f(x)$ modulo the maximal ideal (p).*

In our example for $S = S_1$, its initial point is $(2, 0)$ with length 4 and height 2. Thus, $e = 2$, $d = 2$, $t_0 = a_2(x)(\text{mod } 3, \phi) = x - 1(\text{mod } 3, \phi) = z - 1$, $t_1 = a_4(x)/3(\text{mod } 3, \phi) = 12/3(\text{mod } 3, \phi) = 1$, and

$t_2 = a_6(x)/9(\mathrm{mod}\ 3,\phi) = (18x+162)/3^2(\mathrm{mod}\ 3,\phi) = 2z$, where z is a root of ϕ in an algebraic closure of $\mathbb{F}_3$. Thus $f_{S_1}(y) = (z-1)y^2 + y + 2z$ in $\mathbb{F}_\phi[y]$.

In [4, Theorem 3.4, p: 5], we showed that:

Theorem 3.2. *For any monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ such that $\overline{f(x)} = \prod_{i=1}^r \overline{\phi_i}^{l_i}(x)(\mathrm{mod}\ p)$ is the factorization in $\mathbb{F}_p[x]$. For every $i = 1, \dots, r$, let $N_i = N_{\phi_i}(f) = S_1^i + \cdots + S_{k_i}^i$ be the principal part $N_{\phi_i}^+(f)$ and for every $j = 1, \dots, k_i$, let $f_{S_j}(y) = \prod_{s=1}^{r_{ij}} \psi_{i,j,s}(y)^{n_{i,j,s}}$ be the factorization of $f_{S_j}(y)$ into irreducible polynomials of $\mathbb{F}_{\phi_i}[y]$. Then if every $f_{S_j}(y)$ is square free, i.e., every $n_{i,j,s} = 1$, then*

$$p\mathbb{Z}_K = \prod_{i=1}^{r}\prod_{j=1}^{k_i}\prod_{s=1}^{r_{ij}} \mathfrak{p}_{i,j,s}^{e_{ij}},$$

where $e_{ij} = e(S_{ij})$ is the ramification index of the side S_{ij}.

Proof: of Lemma 3.1.

1. If $m \equiv 1(\mathrm{mod}\ 8)$, then $f(x) \equiv (x-1)^2(x^2+x+1)^2(\mathrm{mod}\ 2)$. Let $F(x) = f(x+1) = x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1 - m$. As $m \equiv 1(\mathrm{mod}\ 8)$, $\nu_2(1-m) \geq 3$, and $N_x^+(f) = S_1 + S_2$ has two sides with the same length 1, and so of degree 1. Thus their residual polynomials are of degree 1. Especially $F_{S_2}(y) = F_{S_1}(y) = y+1$ in $\mathbb{F}_2[y]$. Again let $f(x) = \phi^3 - 3x\phi^2 + (2x-2)\phi + 1 - m$ be the ϕ-adic development, where $\phi = x^2+x+1$. As $m \equiv 1(\mathrm{mod}\ 8)$, $N_\phi{}^+(f) = S_1 + S_2$ with the same length 1 and so their residual polynomials are $f_{S_2}(y) = f_{S_1}(y) = y+1$ in $\mathbb{F}_\phi[y]$. Hence by Theorem 3.2, $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$, where $f_1 = f_2 = 1$ and $f_3 = f_4 = \deg(\phi) = 2$.

2. If $m \equiv 5(\mathrm{mod}\ 8)$, then $f(x) \equiv (x-1)^2(x^2+x+3)^2(\mathrm{mod}\ 2)$. Let $F(x) = f(x+1) = x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1 - m$. $m \equiv 5(\mathrm{mod}\ 8)$, $\nu_2(1-m) = 2$ and $N_x^+(f) = S$ has only one side of degree 2, with residual polynomial $F_S(y) = y^2 + y + 1$, which is irreducible in $\mathbb{F}_2[y]$. Again let $f(x) = \phi^3 - (6+3x)\phi^2 + (14x+10)\phi - (16x+3+m)$ be the ϕ-adic development, where $\phi = x^2+x+3$. As $m \equiv 5(\mathrm{mod}\ 8)$, $\nu_2(16x+3+m) \geq 3$ and so $N_\phi{}^+(f) = S_1 + S_2$ (see Figure 2 below).

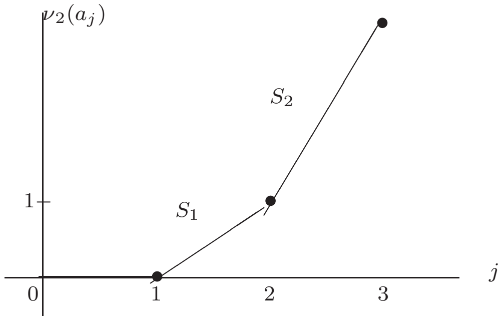

Figure 2

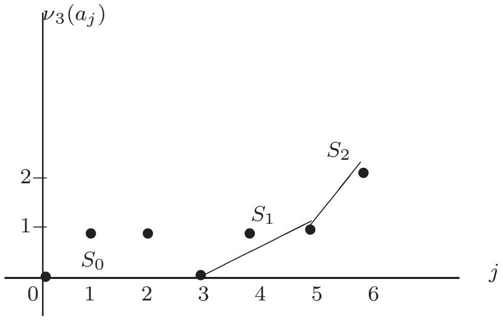

Figure 3

As the length of every S_i is 1 and so of degree 1, the residual polynomial $f_{S_i}(y)$ is of degree 1 and so is irreducible in $\mathbb{F}_\phi[y]$ (see Figure 1). Therefore, by Theorem 3.2, $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ with $f_1 = \deg\,(f_S(y)) = 2$ and $f_3 = f_4 = \deg(\phi) = 2$.

3. If $m \equiv 1(\text{mod } 9)$, then $f(x) \equiv ((x-1)(x+1))^3(\text{mod } 3)$. Let $F(x) = f(x+1) = x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1 - m$ and $G(x) = f(x-1) = x^6 - 6x^5 + 15x^4 - 20x^3 + 15x^2 - 6x + 1 - m$. Then $N_x^+(F) = S_1 + S_2$ (see Figure 3) has two sides with respective residual polynomials $F_{S_1}(y) = y + 1$ and $F_{S_2}(y) = y + c$ ($c \in \mathbb{F}_3^*$), with respective degrees $f_1 = f_3 = 1$. Also $N_x^+(G) = S_1 + S_2$ (see $Figure$3) has two sides with respective residual polynomials $G_{S_1}(y) = -y - 1$ and $F_{S_2}(y) = -y + b$ ($b \in \mathbb{F}_3^*$). By Theorem 3.2, $3\mathbb{Z}_K = (\mathfrak{p}_1\mathfrak{p}_2)^2\mathfrak{p}_3\mathfrak{p}_4$, with $f_1 = f_2 = f_3 = f_4 = 1$.

□

As the proof of the above lemma depends on Theorem 3.2, which could be difficult for some readers, and following the suggestion of the referee, we give below a new proof based on Kronecker's method for $m \equiv 1(\text{mod } 9)$. We recall that the well known Dedekind's factorization method of $p\mathbb{Z}_K$ is applicable only when p does not divide the index $[\mathbb{Z}_K : \mathbb{Z}[\alpha]]$. Thanks to Kronecker's theory of forms [2, Section 17.B], an alternative method can be applied even when Dedekind's criterion conditions failed. Namely, Let $(w_1, \ldots, w_n)$ be a $\mathbb{Z}$-basis of $\mathbb{Z}_K$ and $\Xi = \sum_{i=1}^n t_i w_i$ be a fundamental form of $\mathbb{Z}_K$, where $t = (t_1, \ldots, t_n)$, and every t_i is an indeterminate. For every $\mathbb{Q}$-isomorphism σ of K in $\mathbb{C}$, let $\Xi^\sigma = \sum_{i=1}^n t_i \sigma(w_i)$ and $f(x,t) = \prod_{i=1}^n (x - \Xi^{\sigma_i})$, where $\sigma_1, \ldots, \sigma_n$ are the distinct $\mathbb{Q}$-isomorphisms of K in $\mathbb{C}$. If $f(x,t) \equiv \prod_{i=1}^g g_i^{e_i}(x,t)(\text{mod } p)$ is the factorization of $\overline{f(x,t)}$ in $\mathbb{F}_p[t_1, \ldots, t_n, x]$, where every $g_i(x,t) \in \mathbb{Z}[t_1, \ldots, t_n, x]$ is a monic polynomial whose reduction modulo p is irreducible of degree f_i, then p factorizes as follows : $p\mathbb{Z}_K = \prod_{i=1}^g \mathfrak{p}_i^{e_i}$, where every $\mathfrak{p}_i$ is a prime ideal of $\mathbb{Z}_K$ lying above p with residue degree f_i. In our case, let $m \neq 1$ be a square free integer such that $m \equiv 1(\text{mod } 9)$, θ a complex root of $f(x) = x^6 - m$, $\alpha = \theta^2$, $w = \theta^3$, and $\gamma = \frac{1+\alpha+\alpha^2}{3}$. As we saw in the proof of Lemma 3.1, $f(x) \equiv (x-1)^3(x+1)^3(\text{mod } 3)$, with the associated residual polynomial of any side of any Newton polygon of f is square free, then by Theorem of index (see for instance [5, Th. 1.9] and [13]), $ind_3(f) = \nu_3((\mathbb{Z}_K : \mathbb{Z}[\alpha])) = ind_{x-1}(f) + ind_{x+1}(f) = 1 + 1 = 2$ (see Figure 2 and Figure 3), where $ind_\phi(f)$ is the ϕ-index of f, which is defined in [5, Def. 1.3] by $ind_\phi(f)$ is $\deg(\phi)$ times the number of points with integer coordinates that lie below or on the polygon $N_\phi^+(f)$, strictly above the horizontal axis, and strictly before the vertical axis of equation $x = l$. Let $B_1 = (1, \theta, \alpha, \theta\alpha, \gamma, \theta\gamma)$ and M be the $\mathbb{Z}$-module generated by B_1. Then $\nu_3((M : \mathbb{Z}[\alpha])) = 2$, and so $\nu_3((\mathbb{Z}_K : M)) = 0$. Thus B_1 is a 3-integral basis of $\mathbb{Z}_K$. Let $B_2 = (1, \alpha, \gamma, w, w\alpha, w\gamma)$. Since the determinant of the transition matrix of B_1 to B_2 is $\begin{vmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & \frac{m-1}{3} \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 1 \end{vmatrix} = 1 - (m-1) = -m$ and $m \equiv 1(\text{mod } 9)$, B_2 is a 3-integral basis of $\mathbb{Z}_K$. Thus $\Xi = \sum_{i=1}^n t_i w_i$ is a fundamental form of $\mathbb{Z}_K$, where $w_1, \ldots, w_6$ are the elements of B_2. Let $H = \mathbb{Q}(w)$. Then $f(x,t) = N_{K/\mathbb{Q}}(x - \Xi) = N_{H/\mathbb{Q}}(N_{K/H}(x - \Xi)) = N_{H/\mathbb{Q}}(N_{K/H}((x - t_1 - t_2\alpha - t_3\gamma) - (t_4 + t_5\alpha + t_6\gamma)w) = N_{H/\mathbb{Q}}((x - t_1 - t_2\alpha - t_3\gamma)^2 - m(t_4 + t_5\alpha + t_6\gamma)^2 \equiv N_{H/\mathbb{Q}}((x - t_1 - t_2\alpha - t_3\gamma)^2 - (t_4 + t_5\alpha + t_6\gamma)^2 \equiv N_{H/\mathbb{Q}}((x - (t_1 + t_4 - (t_2 + t_5)\alpha - (t_3 + t_6)\gamma))N_{H/\mathbb{Q}}((x - (t_1 - t_4 - (t_2 - t_5)\alpha - (t_3 - t_6)\gamma))$. Set $a = x - (t_1 + t_4)$, $b = -(t_2 + t_5)$, and $c = -(t_3 + t_6)$. Recall that $N_{H/\mathbb{Q}}(a + b\alpha + c\gamma)$ is the determinant of the matrix of the endomorphism of H defined by the multiplication by $(a + b\alpha + c\gamma)$. As $\alpha^2 = 3\gamma - \alpha - 1 \equiv -\alpha - 1(\text{mod } 3)$, $\alpha\gamma = \frac{\alpha^3+\alpha^2+\alpha}{3} = \frac{m-1}{3} + \frac{1+\alpha^2+\alpha}{3} \equiv \gamma(\text{mod } 3)$ (because $m \equiv 1(\text{mod } 9)$, and $\gamma^2 = \frac{m-1}{9}(\alpha+2) + \gamma = 2K + K\alpha + \gamma$ ($m = 1 + 9K$), $N_{H/\mathbb{Q}}(a + b\alpha + c\gamma) \equiv \begin{vmatrix} a & -b & 2K \\ b & a-b & K \\ c & c & a+b+c \end{vmatrix} \equiv (a+b+c)(a+b)^2 \equiv (x - s_1(t))(x - s_2(t))^2(\text{mod } 3)$, where $s_1(t) = t_1 + t_2 + t_3 + t_4 + t_5 + t_6$ and $s_2(t) = t_1 + t_2 + t_4 + t_5$. Similarly, $N_{H/\mathbb{Q}}((x - (t_1 - t_4 - (t_2 - t_5)\alpha - (t_3 - t_6)\gamma)) \equiv (x - s_3(t))(x - s_4(t))^2(\text{mod } 3)$, where $s_3(t)=t_1+t_2+t_3-(t_4+t_5+t_6)$ and $s_4(t)=t_1+t_2-(t_4+t_5)$. Since for every $i\neq j$, $s_i(t)\neq s_j(t)$, $\overline{f(x,t)}=(x-s_1(t))(x-s_3(t))(x-s_2(t))^2(x-s_4(t))^2$ is the factorization of $\overline{f(x,t)}$ over $\mathbb{F}_3$. Finally, $3\mathbb{Z}_K=\mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_4$, where for every i, $f(\mathfrak{p}_i)=1$.

Proof: of Corollaries 2.2 and Proposition 2.3,
Since m is square free, by Theorem 2.1, it suffices to evaluate $\nu_2(m-1)$ and $\nu_3(m^2-1)$. But as by assumption, $m\not\equiv 1 (\text{mod } 4)$ and $m\not\equiv \mp 1(\text{mod } 9)$, we have $m-1\not\equiv 0(\text{mod } 4)$ and $m^2-1\not\equiv 0(\text{mod } 9)$. Hence $\nu_2(m-1)=1$ and $\nu_3(m^2-1)=1$. Finally, α generates a power integral basis of $\mathbb{Z}_K$. □

Proof: of Theorem 2.4. In every case, we will show that K is not monogenic.

1. Assume that $m\equiv 1(\text{mod } 8)$. If there exists $\theta\in\mathbb{Z}_K$ such that 2 does not divide the index $(\mathbb{Z}_K:\mathbb{Z}[\theta])$, then thanks to Kummer's Theorem, the factorization of $2\mathbb{Z}_K$ is 2-analogous to the factorization of $\overline{F}(x)$ modulo 2, where $F(x)$ is the minimal polynomial of θ over $\mathbb{Q}$. More precisely $2\mathbb{Z}_K=\prod_{k=1}^r \mathfrak{p}_i^{e_i}$, where $\overline{F}(x)=\prod_{k=1}^r \overline{g_i^{e_i}}(x)$ is the factorization of $\overline{F}(x)$ into powers of monic irreducible polynomials of $\mathbb{F}_2[x]$. As there is only one monic irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$, namely x^2+x+1, the factorization $2\mathbb{Z}_K=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$, with $f_3=f_4=2$ is impossible.

2. Assume that $m\equiv 5(\text{mod } 8)$. If there exists $\theta\in\mathbb{Z}_K$ such that 2 does not divide the index $(\mathbb{Z}_K:\mathbb{Z}[\theta])$, then thanks to Kummer's Theorem, the factorization of $2\mathbb{Z}_K$ is 2-analogous to the factorization of $\overline{F}(x)$ modulo 2, where $F(x)$ is the minimal polynomial of θ over $\mathbb{Q}$. More precisely, $2\mathbb{Z}_K=\prod_{k=1}^r \mathfrak{p}_i^{e_i}$, where $\overline{F}(x)=\prod_{k=1}^r \overline{g_i^{e_i}}(x)$ is the factorization of $\overline{F}(x)$ into powers of monic irreducible polynomials of $\mathbb{F}_2[x]$. As there is only one monic irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$, namely x^2+x+1, the factorization $2\mathbb{Z}_K=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, with $f_1=f_2=f_3=2$ is impossible, which contradicts Lemma 3.1. Hence for every $\theta\in\mathbb{Z}_K$, 2 divides the index $(\mathbb{Z}_K:\mathbb{Z}[\theta])$ and $\mathbb{Z}_K$ can not have a power integral basis.

3. Similarly, if $m\equiv 1(\text{mod } 9)$ and there exists $\theta\in\mathbb{Z}_K$ such that 3 does not divide the index $(\mathbb{Z}_K:\mathbb{Z}[\theta])$, then the factorization of $3\mathbb{Z}_K$ is 3-analogous to the factorization of $\overline{F}(x)$ modulo 3, where $F(x)$ is the minimal polynomial of θ over $\mathbb{Q}$. As there is only three monic irreducible polynomials of degree 1 in $\mathbb{F}_3[x]$, namely $x+1$, $x-1$, and x, the factorization $3\mathbb{Z}_K=(\mathfrak{p}_1\mathfrak{p}_2)^2\mathfrak{p}_3\mathfrak{p}_4$, with $f_1=f_2=f_3=f_4=1$ is impossible, which contradicts Lemma 3.1. Hence for every $\theta\in\mathbb{Z}_K$, 3 divides the index $(\mathbb{Z}_K:\mathbb{Z}[\theta])$ and $\mathbb{Z}_K$ can not have a power integral basis.

□

Acknowledgments

The author is deeply grateful to the Editor Marcelo Escudeiro Hernandes for his patience and professionalism during the review process of this manuscript. Also, he is very grateful to the anonymous referee for his patience too and for his suggestions which improved the quality of this paper. As well as for Professor Enric Nart who introduced him to Newton polygon's techniques.

References

1. S. Ahmad, T. Nakahara, and S. M. Husnine *Power integral bases for certain pure sextic fields*, Int. J. of Number Theory 10(8) (2014) 2257– 2265.
2. H. Cohn, *A classical invitation to algebraic numbers and class fields*, With two appendices by Olga Taussky: "Artin's 1932 Göttingen lectures on class field theory" and "Connections between algebraic number theory and integral matrices". Universitext. Springer-Verlag, New York-Heidelberg (1978).
3. H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM 138, Springer-Verlag Berlin Heidelberg (1993).
4. L. El Fadil, A. Chillali, and I. Akharaz *Prime ideal factorization in quartic number fields*, Gulf journal of Mathematics 4(4) (2016) 1–15.
5. L. El Fadil, J. Montes and E. Nart, *Newton polygons and p-integral bases of quartic number fields*, J. Algebra and Appl. 11(4)(2012).
6. T. Funakura, *On integral bases of pure quartic fields*, Math. J. Okayama Univ. 26 (1984) 27-–41.

7. J. Guardia, J. Montes, and E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. 364 (1) (2012) 361–416.

8. K. Hensel, *Untersuchung der Fundamentalgleichung einer Gattung reine reelle Primzahl als Modul und Bestimmung der Theiler ihrer Discriminante*, J. Reine Angew. Math. 113 (1894) 61–83.

9. Y. Motoda, T. Nakahara and S. I. A. Shah, *On a problem of Hasse*, J. Number Theory 96 (2002) 326—334.

10. Y. Motoda, T. Nakahara, S. I. A. Shah and T. Uehara, *On a problem of Hasse for certain imaginary abelian fields*, RIMS Kokyuroku Bessatsu B12 (2009) 209—221.

11. A. Hameed, T. Nakahara, S. M. Husnine and S. Ahmad, *On existence of canonical number system in certain classes of pure algebraic number fields*, J. Prime Res. Math. 7 (2011) 19—24.

12. S. Ahmad, T. Nakahara and S. M. Husnine, *Non-monogenesis of a family of pure sextic fields*, Arch. Sci. (Geneva) 65(7) (2012) 42—49.

13. O. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann., 99 (1928) 84–117.

14. R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Göttingen Abhandlungen 23 (1878) 1–23.

L. El Fadil,
Department of Mathematics,
Faculty of Sciences Dhar El Mahraz,
Sidi mohamed ben Abdellah University,
Morocco.
E-mail address: lhouelfadil2@gmail.com