

P-INTEGRAL BASES AND PRIME IDEAL FACTORIZATION IN QUINTIC FIELDS

LHOUSSAIN EL FADIL ^{1*} AND OMAR BOUGHALEB ²

ABSTRACT. Based on Newton polygon techniques, for every prime integer p , a p -integral basis of $\mathbb{Z}_K$, and the factorization of the principal ideal $p\mathbb{Z}_K$ into prime ideals of $\mathbb{Z}_K$ are given, where K is a quintic number field defined by an irreducible trinomial $X^5 + aX^2 + b \in \mathbb{Z}[X]$.

1. INTRODUCTION

Let K be a quintic number field defined by an irreducible trinomial $f(X) = X^5 + aX^2 + b \in \mathbb{Z}[X]$, $\mathbb{Z}_K$ its ring of integers, d_K its discriminant, α a complex root of $f(X)$, Δ the discriminant of $f(X)$ and $ind(f) = [\mathbb{Z}_K : \mathbb{Z}[\alpha]]$ the index of $\mathbb{Z}[\alpha]$. In this paper, based on Newton polygon techniques, for every prime integer p , a p -integral basis is proposed. This method provides also the factorization of $p\mathbb{Z}_K$ into prime ideals of $\mathbb{Z}_K$; The form $p\mathbb{Z}_K = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$ and for every prime factor $\mathfrak{p}_i$, a p -generator β_i of $\mathfrak{p}_i$ is given too; $\mathfrak{p}_i = p\mathbb{Z}_K + \beta_i\mathbb{Z}_K$. A such p -generator is characterized by $v_{\mathfrak{p}_i}(\beta_i) = 1$ and for every $\mathfrak{p} \neq \mathfrak{p}_i$, $v_{\mathfrak{p}}(\beta_i) = 0$. If the ramification index $e_i = 1$, then the first condition could be replaced by $v_{\mathfrak{p}_i}(\beta_i) \geq 1$. Let p be a prime integer. It is well known that if p does not divide $ind(f)$, then thanks to a theorem of Kummer the factorization of $p\mathbb{Z}_K$ can be derived directly from the factorization of $\bar{f}(X)$ modulo p ; $p\mathbb{Z}_K = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$, where every $\mathfrak{p}_i = (p, g_i(\alpha))^{e_i}$ and $\bar{f}(X) = \prod_{i=1}^r \bar{g}_i^{e_i}$ is the factorization of $f(X)$ in $\mathbb{F}_p[X]$ (see, for example [2, page 257]). In this case, we said that the factorization of $p\mathbb{Z}_K$ is p -analogous to the factorization of $\bar{f}(X)$ modulo p . Dedekind gave a criterion to detect if p does not divide $ind(f)$ or not (see [3]). If p divides $ind(f)$, then the previous theorem of Kummer failed. In that case, using Newton polygon techniques, the index $v_p(ind(f))$ is calculated, a p -integral basis, the form of $p\mathbb{Z}_K = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$, and for every prime factor $\mathfrak{p}_i$, a p -generator of $\mathfrak{p}_i$ are given. Throughout this paper, the following notations are used: For every prime p , v_p is the p -adic discrete valuation defined in $\mathbb{Q}_p$ by $v_p(p) = 1$, extended to $\mathbb{Q}_p[X]$ by $v_p(A(X)) := \min\{v_p(a_i), 0 \leq i \leq r\}$, where $A(X) = \sum_{i=0}^r a_i X^i$. For every $(x, m) \in \mathbb{Z}^2$, denote $x_p = \frac{x}{p^{v_p(x)}}$, $x \pmod{m}$ the residue class of x modulo m and $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol.

Date: Accepted: Oct 24, 2016.

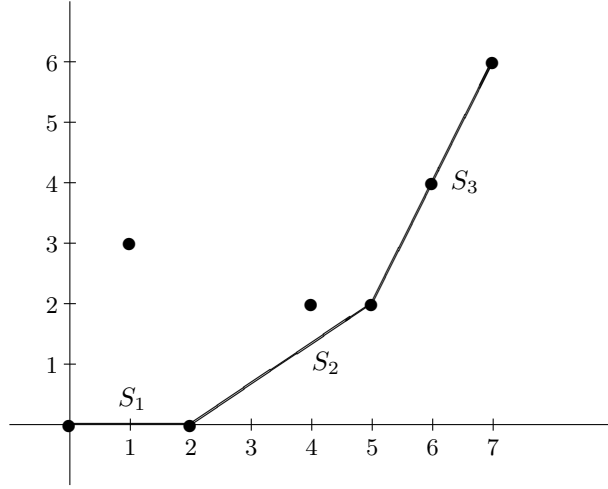
* Corresponding author.

2010 *Mathematics Subject Classification.* 11Y40.

Key words and phrases. p -integral basis, Newton polygons, Quintic fields.

2. NEWTON POLYGONS

In this section, we briefly review the notions of Newton polygons. Let p be a prime integer such that p^2 divides Δ . Let $\phi(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree m such that $\bar{\phi}(X)$ is an irreducible divisor of $f(X)$ modulo p . Let $f(X) = a_0(X)\phi(X)^r + a_1(X)\phi(X)^{r-1} + \cdots + a_r(X)$ be the $\phi(X)$ -adic development of $f(X)$ (every $a_i(X) \in \mathbb{Z}[X]$ and $\deg a_i(X) < m$). To any coefficient $a_i(X)$, we attach $u_i = v_p(a_i(X))$. If $u_i < \infty$, then let P_i be the point in the Euclidean plane defined by (i, u_i) . The ϕ -Newton polygon of $f(X)$ is the lower convex envelope of the set of points $P_i = (i, u_i)$, $u_i < \infty$, in the Euclidean plane. This open polygon is denoted by $N_\phi f$. For instance, for a ϕ -development of degree 7 with $u_i = 0, 3, 0, \infty, 2, 2, 4, 6$ for $i = 0, 1, \dots, 7$, the polygon is



Let N be the $\phi(X)$ -Newton polygon of $f(X)$. The *length* $\ell(N_\phi f)$ and the *height* $h(N_\phi f)$ of the polygon are the respective lengths of the projection to the horizontal and vertical axis. Clearly, $\deg f(X) = m\ell(N_\phi f) + \deg a_0(X)$, where $m = \deg \phi$. The ϕ -Newton polygon is the union of different adjacent *sides* $S_1, \dots, S_t$ with increasing slopes $\lambda_1 < \lambda_2 < \cdots < \lambda_t$. We shall write $N_\phi f = S_1 + \cdots + S_t$. The points joining two different sides are called the *vertices* of the polygon. The polygon determined by the sides of positive slopes of $N_\phi f$ is called the *principal ϕ -polygon* of $f(X)$ and denoted by $N_\phi^+ f$. The length and the height of $N_\phi^+ f$ are respectively the lengths of its orthogonal projections to the horizontal and vertical axis. For instance, the polygon of the figure has three sides S_1, S_2, S_3 with slopes $0 < 2/3 < 2$ and $N_\phi^+ f = S_2 + S_3$. For every side S of the principal part $N_\phi^+ f$, the *length* $\ell(S)$ and the *height* $h(S)$, of S , are the respective lengths of the projection to the horizontal and vertical axis. The *slope* of S is the quotient $h(S)/\ell(S)$. The positive integer $d(S) := \gcd(h(S), \ell(S))$ is called the *degree* of S . Denote $d := d(S)$ the degree of S , $h := h(S)/d$ and $e := \ell(S)/d$. $\lambda := h/e$ is the slope of S and e is its ramification index. Let $l = \ell(N_\phi f)$ be the length of $N_\phi f$. For any $j := 1..l$, let $H_j \in \mathbb{Q}$ be the ordinate of the point of $N_\phi(f)$ of abscissa j , h_j its integral part and $t_j = \text{red} \left(\frac{a_j(X)}{p^{h_j}} \right)$, where *red* is the canonical map defined on $\mathbb{Z}[X]$ by reduction modulo p . Note that If $P_j \notin S$, then $t_j = 0$ and if $P_j \in S$, then

$t_j \neq 0$. If i is the abscissa of the initial point of S , let $f_S(Y)$ be the *residual polynomial* attached to S : $f_S(Y) := t_i Y^d + t_{i+e} Y^{d-1} + \dots + t_{i+(d-1)e} Y + t_{i+de} \in \mathbb{F}_\phi[Y]$. Let $\bar{f}(X) \equiv \prod_{i=1}^r \bar{\phi}_i^{l_i}(X)$ modulo p be the factorization of $\bar{f}(X)$ in $\mathbb{F}_p[X]$, where $\phi(X) \in \mathbb{Z}[X]$ is monic. Let $N_\phi^+ f = S_1^i + \dots + S_t^i$. $f(X)$ is said to be ϕ_i -regular if for every $j := 1..t$, $f_{S_j^i}(Y)$ is square free in $\mathbb{F}_p[Y]$. Let $N_i := N_\phi f$. Define $\text{ind}_{N_i}(f) := m_i \sum_{j=i_0^i+1}^{l_i-1} h_j$ the N_i -index of $f(X)$, where $i_0^i = \prod_{k \neq i} \bar{\phi}_k^{l_k}(X)$, l_i is the length of N_i and $m_i = \deg(\phi_i)$. For every $j := 0..l_i - 1$, let $q_j^i(X)$ be the quotient of the Euclidean division of $f(X)$ by $\phi_i^j(X)$. For every $j := 0..l_i - 1$ and for every $k := 0..m_i - 1$, let $Q_{i,j,k}(\alpha) = \alpha^{k \frac{q_j^i(\alpha)}{p_j^{h_j}}}$, where h_j is the integral part of H_j and H_j is the ordinate of the point $P_j \in N_i$ of abscissa j . Then we have the following results:

Proposition 2.1. [4, Pr. 2.3 and Th. 2.6]

- (1) If $\bar{f}(X) \equiv \bar{\phi}_1^{l_1} \bar{H}(X) \pmod{p}$ such that $\bar{H}(X)$ is square free and $f(X)$ is $\phi_1(X)$ -regular, then $v_p(\text{ind}(f)) = m_1 \times \text{ind}_{N_1}(f)$ and $\{Q_{1,j,k}(\alpha) \mid j := 0..l_1 - 1, k := 0..m_1 - 1\}$ is a p -integral basis of $\mathbb{Z}_K$.
- (2) If $\bar{f}(X) \equiv \bar{\phi}_1^{l_1} \bar{\phi}_2^{l_2} \pmod{p}$ such that for every $i := 1, 2$, $f(X)$ is $\phi_i(X)$ -regular, then $v_p(\text{ind}(f)) = m_1 \times \text{ind}_{N_1}(f) + m_2 \times \text{ind}_{N_2}(f)$ and $\{Q_{1,j,k}(\alpha) \mid j := i_0^1 + 1..l_1 - 1, k := 0..m_1 - 1\} \cup \{Q_{2,j,k}(\alpha) \mid j := i_0^2 + 1..l_2 - 1, k := 0..m_2 - 1\}$ is a p -integral basis of $\mathbb{Z}_K$.

3. MAIN RESULTS

Let $K = \mathbb{Q}[\alpha]$ be a quintic number field generated by α a complex root of an irreducible polynomial $f(X) = X^5 + aX^2 + b \in \mathbb{Z}[X]$. Note that if there exists a prime p such that $v_p(a) \geq 3$ and $v_p(b) \geq 5$, then $K = \mathbb{Q}[\theta]$, where $\theta = \frac{\alpha}{p^q}$, $q := \text{Min}(q_1, q_2)$, q_1 the quotient of $v_p(b)$ by 5 and q_2 is the quotient of $v_p(a)$ by 3. Since $P(X) = X^5 + AX^2 + B$ is the minimal polynomial of θ and $v_p(A) \leq 2$ and $v_p(B) \leq 4$, up to replace α by θ , we can assume that $v_p(a) \leq 2$ or $v_p(b) \leq 4$. First, we describe an iterative process that converges, in some special cases, to an integer $s \in \mathbb{Z}$ such that $f(X)$ is $(X - s)$ -regular. We say that an integer s is *regular* if $f(X)$ is $(X - s)$ -regular. Otherwise, we say that s is *irregular*. Let s be an integer, and denote $u_5 := v_p(f(s))$, $u_4 := v_p(f'(s))$, $u_3 := v_p(\frac{f''(s)}{2})$, $u_2 := v_p(\frac{f^{(3)}(s)}{6})$, $u_1 := v_p(\frac{f^{(4)}(s)}{24})$, $\sigma_1 := \frac{f^{(4)}(s)}{p^{u_2}}$, $\sigma_2 := \frac{f^{(3)}(s)}{p^{u_2}}$, $\sigma_3 := \frac{f''(s)}{p^{u_3}}$, $\sigma_4 := \frac{f'(s)}{p^{u_4}}$, $\sigma_5 := \frac{f(s)}{p^{u_5}}$.

The $(X - s)$ -adic development of $f(X)$ is $f(X) = (X - s)^5 + \frac{f^{(4)}(s)}{24}(X - s)^4 + \frac{f^{(3)}(s)}{6}(X - s)^3 + \frac{f''(s)}{2}(X - s)^2 + f'(s)(X - s) + f(s)$, and the $(X - s)$ -Newton polygon of $f(X)$ is the lower convex envelope of the points: $(0, 0)$, $(1, u_1)$, $(2, u_2)$, $(3, u_3)$, $(4, u_4)$ and $(5, u_5)$.

Let us show an efficient way to find a regular s .

Lemma 3.1. For $p = 3$, $a^2 \equiv 4 \pmod{9}$ and $v_3(-a^5 - a^3 + b) \geq 3$, let $s = -a$.

- (1) If $v_3(f(s)) \leq 2$, then s is regular, and the process is done.

- (2) If $v_3(f(s)) = 3$, $v_3(f'(s)) = 2$ and $f_S(Y)$ is square free, then s is regular, and the process is done too.
- (3) If $v_3(f(s)) \geq 4$, $v_3(f'(s)) = 2$ and $\sigma_3^2 - \sigma_2\sigma_4 \not\equiv 0 \pmod{3}$, then s is regular, and the process is done too.
- (4) If $v_3(f(s)) = 3$, $v_3(f'(s)) = 2$ and $\sigma_2Y^3 + \sigma_3Y^2 + \sigma_4Y + \sigma_5$ is inseparable in $\mathbb{F}_3[Y]$, then let $t \in \mathbb{Z}$ such that $\bar{t}$ is the square root of $\sigma_2t^3 + \sigma_3t^2 + \sigma_4t + \sigma_5$. Replace s by $s + 3t$ and go to the next step.
- (5) If $v_3(f(s)) \geq 4$, $v_3(f'(s)) = 2$ and $\sigma_3^2 - \sigma_2\sigma_4 \equiv 0 \pmod{3}$, then let $t \in \mathbb{Z}$ such that $\bar{t}$ is the root of $\sigma_2t^2 + \sigma_3t + \sigma_4$. Replace s by $s + 3t$ and go to the next step.
- (6) If $v_3(f(s)) \geq 4$, $v_3(f'(s)) \geq 3$, $2u_4 = u_5 + 1$ and $\sigma_4^2 - \sigma_3\sigma_5 \equiv 0 \pmod{3}$, then replace s by $s + 3^{u_4-1}t$, where t is a root of $\sigma_3t^2 + \sigma_4t + \sigma_5$. Compute the new corresponding $u_2, u_3, u_4, u_5, \sigma_3, \sigma_4$ and σ_5 , and then repeat this step until to obtain $2u_4 \neq u_5 + 1$ or $(2u_4 = u_5 + 1$ and $\sigma_4^2 - \sigma_3\sigma_5 \equiv 0 \pmod{3})$.
- (7) If $v_3(f(s)) \geq 4$, $v_3(f'(s)) \geq 3$, $2u_4 = u_5 + 1$ and $\sigma_4^2 - \sigma_3\sigma_5 \not\equiv 0 \pmod{3}$, then s is regular.
- (8) If $v_3(f(s)) \geq 4$, $v_3(f'(s)) \geq 3$, $2u_4 \neq u_5 + 1$, then s is regular.

Proof. For $s = -a$, we have $u_2 = 0$, $u_3 = 1$, $u_4 \geq 2$ and $u_5 \geq 1$. Thus, we have the following situations:

- (1) If $u_5 \leq 3$, then $N_{(X-s)}^+(f) = S$ is one side. If $u_5 \leq 2$, then $f_S(Y)$ is of degree 1, and then s is regular.
If $u_5 = 3$, $u_4 = 2$ and $f_S(Y)$ is square free, then s is regular too.
If $u_5 = 3$, $u_4 = 2$ and $\sigma_2Y^3 + \sigma_3Y^2 + \sigma_4Y + \sigma_5$ is inseparable in $\mathbb{F}_3[Y]$, then let $t \in \mathbb{Z}$ such that $\bar{t}$ is the square root of $f_S(t)$. Let $s_0 = -a$, $s_1 = s + 3t$ and for every i , $f(X - s_i) = X^5 - 5s_iX^4 + 10s_i^2X^3 + A_iX^2 + B_iX + C_i$. Then $A_1 = -10s_1^3 + a \equiv A_0 \pmod{9}$, $B_1 = s_1(5s_1^3 - 2a) \equiv B_0 + 9 \cdot 2t\sigma_3 \pmod{27}$ and $C_1 = C_0 + 27t\sigma_4 + 27t^2\sigma_3 + 27t^3\sigma_5$. Since t is the square root of $f_S(t)$, $f'_S(t) = \sigma_4 + 2t\sigma_3 \equiv 0 \pmod{3}$ and $f_S(t) \equiv 0 \pmod{3}$. Thus, $u_5 \geq 4$ and $u_4 \geq 3$. Go to the next step.
- (2) If $u_5 \geq 4$, $u_4 = 2$ and $\sigma_3^2 - \sigma_2\sigma_4 \equiv 0 \pmod{3}$, then $N^+(f) = S_1 + S_2$ such that $f_{S_1}(Y) \equiv \sigma_2Y^2 + \sigma_3Y + \sigma_4 \pmod{3}$ and $f_{S_2}(Y)$ is of degree 1. Let $t \in \mathbb{Z}$ such that $\bar{t}$ is the root of $f_{S_1}(t)$ and $s_1 = s_0 - 3t$. As in the previous step $u_3 = 1$, $u_4 \geq 3$ and $u_5 \geq 4$. Go to the next step.
- (3) If $u_5 \geq 4$, $u_4 \geq 3$ and $2u_4 = u_5 + 1$, then $N^+(f) = S_1 + S_2$ such that $f_{S_1}(Y)$ is of degree 1 and $f_{S_2}(Y) \equiv \sigma_3Y^2 + \sigma_4Y + \sigma_5 \pmod{3}$. As $\sigma_4^2 - \sigma_3\sigma_5 \equiv 0 \pmod{3}$, let $t \in \mathbb{Z}$ such that $\bar{t}$ is the root of $f_{S_2}(t)$. Let $s_0 = s$, $s_1 = s_0 - 3t^{u_4-1}$ and $f(X - s_i) = X^5 - 5s_iX^4 + 10s_i^2X^3 + A_iX^2 + B_iX + C_i$. As in the previous, $v_3(A_1) = 1$, $v_3(B_1) \geq u_4 + 1$ and $v_3(C_1) \geq u_5 + 1$. Replace s by s_1 , compute the new corresponding $u_2, u_3, u_4, u_5, \sigma_3, \sigma_4$ and σ_5 , and then repeat this step until to obtain $2u_4 \neq u_5 + 1$ or $(2u_4 = u_5 + 1$ and $\sigma_4^2 - \sigma_3\sigma_5 \equiv 0 \pmod{3})$. Go to the next step.

Remark that for every iteration i , if s_{i+1} is irregular, then $u_4^i + 2 \leq u_4^{i+2}$ and $u_5^i + 2 \leq u_5^{i+2}$. Thus, $v_3(\text{ind}_{N_{i+2}}(f)) > v_3(\text{ind}_{N_i}(f))$, where $N_i := N_{(X-s_i)}(f)$. As the index $v_3(\text{ind}(f))$ is finite, after a finite number of iterations, this process will done.

- (4) If $u_5 \geq 4$, $u_4 \geq 3$ and $2u_4 = u_5 + 1$, then $N^+(f) = S_1 + S_2$ such that $f_{S_1}(Y)$ is of degree 1 and $f_{S_2}(Y) \equiv \sigma_3 Y^2 + \sigma_4 Y + \sigma_5 \pmod{3}$. As $\sigma_4^2 - \sigma_3 \sigma_5 \not\equiv 0 \pmod{3}$, then $f_{S_2}(Y)$ is square free. Thus, s is regular.
- (5) If $v_3(f(s)) \geq 4$, $v_3(f'(s)) \geq 3$ and $2u_4 > u_5 + 1$, then $N^+(f) = S_1 + S_2$ such that every $i := 1, 2$, $f_{S_i}(Y)$ is square free, and then s is regular.
- (6) If $v_3(f(s)) \geq 4$, $v_3(f'(s)) \geq 3$ and $2u_4 < u_5 + 1$, then $N^+(f) = S_1 + S_2 + S_3$ such that every $i := 1, 2, 3$, $f_{S_i}(Y)$ is of degree 1, and then s is regular.

□

By analogous, we have the followings:

Lemma 3.2. For $p = 5$, $v_5(b) = 0$, $v_5(b^4 - ab - 1) \geq 2$ and $v_5(5b^3 + 2a) \geq 2$, let $s = -b$. Then

- (1) If $2u_4 = u_5 + 1$ and $\sigma_4^2 - \sigma_3 \sigma_5 \not\equiv 0 \pmod{5}$, then s is regular.
- (2) If $2u_4 = u_5 + 1$ and $\sigma_4^2 - \sigma_3 \sigma_5 \equiv 0 \pmod{5}$, then replace s by $s + 5^{u_4-1}t$, where $t \in \mathbb{Z}$ and $\bar{t}$ is the root of $\sigma_3 Y^2 + \sigma_4 Y + \sigma_5$. Compute the new corresponding $u_2, u_3, u_4, u_5, \sigma_3, \sigma_4$ and σ_5 and resume the process.

Theorem 3.3. In Table A, B, C and D, $v_p(\Delta)$, a p -integral basis of $\mathbb{Z}_K$ is given, where $K = \mathbb{Q}[\alpha]$ is a quintic number field generated by α a complex root of an irreducible polynomial $f(X) = X^5 + aX^2 + b \in \mathbb{Z}[X]$ such that $v_p(a) \leq 2$ or $v_p(b) \leq 4$.

Table A : $v_p(a) \geq 1$ and $v_p(b) \geq 1$

case	conditions	p	p -integral basis
1	$v_p(b) = 4, v_p(a) \geq 3$	$\neq 5$	$(1, \alpha, \frac{\alpha^2}{p}, \frac{\alpha^3}{p^2}, \frac{\alpha^4}{p^3})$
2	$v_p(b) = 3, v_p(a) \geq 2$		$(1, \alpha, \frac{\alpha^2}{p}, \frac{\alpha^3}{p}, \frac{\alpha^4}{p^2})$
3	$v_p(b) = 2, v_p(a) \geq 2$		$(1, \alpha, \alpha^2, \frac{\alpha^3}{p}, \frac{\alpha^4}{p})$
4	$v_p(b) \geq 3, v_p(a) = 2$	$\neq 2$	$(1, \alpha, \frac{\alpha^2}{p}, \frac{\alpha^3}{p^2}, \frac{\alpha^4 + a\alpha}{p^{r+1}})$ $r = \lfloor \frac{v_p(b)}{2} \rfloor$
5	$v_2(b) = 2k + 1 \geq 4, v_2(a) = 2$	2	$(1, \alpha, \frac{\alpha^2}{2}, \frac{\alpha^3}{2^2}, \frac{\alpha^4 + a\alpha}{2^{k+1}})$
6	$v_2(b) = 2k \geq 4, v_2(a) = 2$ $a_2 + b_2 \equiv 2 \pmod{4}$	2	$(1, \alpha, \frac{\alpha^2}{2}, \frac{\alpha^3}{2^2}, \frac{\alpha^4 + a\alpha}{2^{k+1}})$
7	$v_2(b) = 2k \geq 4, v_2(a) = 2$ $a_2 + b_2 \equiv 0 \pmod{4}$	2	$(1, \alpha, \frac{\alpha^2}{2}, \frac{\alpha^3}{2^2}, \frac{\theta^4 + 5 \cdot 2^{k-1} \theta^3 + a\theta}{2^{k+2}})$ $t = \alpha - 2^{k-1}$
8	$v_p(b) \geq 2, v_p(a) = 1$	$\neq 2$	$(1, \alpha, \alpha^2, \frac{\alpha^3}{p}, \frac{\alpha^4 + a\alpha}{p^r})$ $r = \lfloor \frac{v_3(b)}{2} \rfloor$
9	$v_p(b) = 2k, v_p(a) = 1$	2	$(1, \alpha, \alpha^2, \frac{\alpha^3}{2}, \frac{\alpha^4 + a\alpha}{2^k})$
10	$v_p(b) = 2k + 1 \geq 3, v_p(a) = 1$ $a_2 + b_2 \equiv 2 \pmod{4}$	2	$(1, \alpha, \alpha^2, \frac{\alpha^3}{2}, \frac{\alpha^4 + a\alpha}{2^{k+1}})$
11	$v_p(b) = 2k + 1 \geq 3, v_p(a) = 1$ $a_2 + b_2 \equiv 0 \pmod{4}$	2	$(1, \alpha, \alpha^2, \frac{\alpha^3}{2}, \frac{\theta^4 + 5 \cdot 2^k \theta^3 + a\theta}{2^{k+2}})$ $t = \alpha - 2^k$
12	$v_p(b) = 1, v_p(a) \geq 1$		$(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$

TableB : $v_p(b) = 0$ and $v_p(a) \geq 1$

Let $\theta = \alpha + b$

Case	Conditions	p	p -integral basis of $\mathbb{Z}_K$
<i>B1</i>		$p \neq 5$	$(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$
<i>B2</i>	$v_p(b^4 - 1 + ab) = 1$	5	$(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$
<i>B3</i>	$v_5(b^4 - 1 + ab) \geq 2, v_5(5b^3 - 2a) = 1$	5	$(1, \alpha, \alpha^2, \alpha^3, \frac{\theta^4}{5})$
<i>B4</i>	$v_5(b^4 - 1 + ab) = 2, a \equiv 15b^3 \pmod{25}$	7	$(1, \alpha, \alpha^2, \frac{\theta^3}{5}, \frac{\theta^4}{5})$
<i>B5</i>	$v_5(b^4 - 1 + ab) \geq 3, a \equiv 15b^3 \pmod{25}$	5	go to <i>TableB5</i>

If $a \equiv 15b^3 \pmod{25}$ and $v_5(b^4 - 1 + ab) \geq 3$, then let s be a regular integer defined by Lemma 3.2.

TableB5 : $a \equiv 15b^3 \pmod{25}$ and $v_5(b^4 - 1 + ab) \geq 3$

Let $\theta = \alpha - s$, $A = 10s^3 + a$, $u_4 = v_5(f'(s))$ and $u_5 = v_5(f(s))$.

Case	Conditions	5-integral basis of $\mathbb{Z}_K$
<i>B5.1</i>	$2u_4 \geq u_5 + 1$	$(1, \alpha, \alpha^2, \frac{\theta^3}{5}, \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta}{5^\mu})$ $\mu = \lfloor \frac{u_5 + 1}{2} \rfloor$
<i>B5.2</i>	$2u_4 < u_5 + 1$	$(1, \alpha, \alpha^2, \frac{\theta^3}{5}, \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta}{5^{u_4}})$

TableC : $v_p(a) = 0$ and $v_p(b) \geq 1$

Case	Conditions	p	p -integral basis of $\mathbb{Z}_K$
<i>C1</i>		$p \notin \{2, 3\}$	$(1, \alpha, \alpha^2, \alpha^3, \frac{\alpha^4 + a\alpha}{p^\mu})$ $\mu = \lfloor \frac{v_p(b)}{2} \rfloor$
<i>C2</i>	$v_2(b) = 2k + 1$	2	$(1, \alpha, \alpha^2, \alpha^3, \frac{\alpha^4 + a\alpha}{2^k})$
<i>C3</i>	$v_2(b) = 2k, a \equiv -b_2 \pmod{4}$	2	$(1, \alpha, \alpha^2, \alpha^3, \frac{\theta^4 + 5.2^k\theta^3 + a\theta}{2^{k+1}})$ $\theta = \alpha - 2^k$
<i>C4</i>	$v_2(b) = 2k, a \equiv 2 - b_2 \pmod{4}$	2	$(1, \alpha, \alpha^2, \alpha^3, \frac{\alpha^4 + a\alpha}{2^k})$
<i>C5</i>		3	go to <i>TableC5</i>

TableC5 : $p = 3, v_3(a) = 0$ and $v_3(b) \geq 1$

Let s be a regular integer defined by using Lemma 3.1, $A = 10s^3 + a$, $B = s(2a + 5s^3)$, $C = b + as^2 + s^4$ and $\theta = \alpha - s$.

Case	Conditions	a 3-integral basis of $\mathbb{Z}_K$
<i>C5.1</i>	$v_3(-a^5 + a^3 + b) = 1, v_3(b) = 1$	$(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$
<i>C5.2</i>	$v_3(-a^5 + a^3 + b) = 1, v_3(b) \geq 2$	$(1, \alpha, \alpha^2, \alpha^3, \frac{\alpha^4 + a\alpha}{3^\mu})$ $\mu = \lfloor \frac{v_3(b)}{2} \rfloor$
<i>C5.3</i>	$v_3(-a^5 + a^3 + b) \geq 2, v_3(b) \geq 2$ $a^2 \not\equiv 4 \pmod{9}$	$(1, \alpha, \alpha^2, \frac{\alpha^3 - a\alpha^2 + \alpha - a}{3}, \frac{\alpha^4 - a\alpha^3 + a^2 + a}{3^\mu})$ $\mu = \lfloor \frac{v_3(b)}{2} \rfloor$
<i>C5.4</i>	$v_3(-a^5 + a^3 + b) \geq 2, a^2 \equiv 4 \pmod{9}$	go to <i>TableC5.6</i>

TableC5.6 : $a^2 \equiv 4 \pmod{9}$ and $v_3(-a^5 + a^3 + b) \geq 2$

Let s be a regular integer defined by using Lemma 3.1, $A = 10s^3 + a$, $\theta = \alpha - s$, $u_4 = v_3(f'(s))$ and $u_5 = v_3(f(s))$.

Case	Conditions	3-integral basis of $\mathbb{Z}_K$
1	$2u_4 \geq u_5 + 1$	$(1, \alpha, \alpha^2, \frac{\theta^3 + a\theta^2 + \theta}{3}, \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta}{3^\mu})$ $\mu = \lfloor \frac{u_5 + 1}{2} \rfloor$
2	$2u_4 \leq u_5$	$(1, \alpha, \alpha^2, \frac{\theta^3 + a\theta^2 + \theta}{3}, \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta}{3^{u_4}})$

TableD : $v_p(ab) = 0$

Case	Conditions	p	p -integral basis of $\mathbb{Z}_K$
D1		$p \in \{2, 3, 5\}$	$(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$
D2	$v_p(\Delta) \leq 1$		$(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$
D3	$v_p(\Delta) \geq 2$	$p \geq 7$	$(1, \alpha, \alpha^2, \alpha^3, \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + (10s^3 + a)\theta}{p^r})$ $r = \lfloor \frac{v_p(\Delta)}{2} \rfloor$

Proof. (1) $v_p(b) \geq 1$, $v_p(a) \geq 1$. All cases, except 3, correspond to a situation where $f(X)$ is X -regular. In the case 13, $f(X)$ is $(X + 2^k)$ -regular.

(2) $v_p(b) = 0$ and $v_p(a) \geq 1$. If $p \neq 5$, then $\bar{f}(X \equiv X^5 + \bar{b} \pmod{p})$ is square free, and then $v_p(\text{ind}(f)) = 0$.

For $p = 5$, we have $\bar{f}(X) \equiv (X + b)^5 \pmod{5}$. Let $f(X - b) = X^5 - 5bX^4 + 10b^2X^3 + AX^2 + BX + C$ and $\theta = \alpha + b$, where $A = a - 10b^3$, $B = b(5b^3 - 2a)$ and $C = -b(b^4 - 1 + a)$. It follows that:

(a) If $v_5(C) = 1$, then $v_5(\text{ind}(f)) = 0$.

(b) If $a \not\equiv 15b^3 \pmod{25}$, then $v_5(B) = 1$, $v_5(A) \geq 1$ and $v_5(C) \geq 1$. Thus if $v_5(C) \geq 2$, then $v_5(\text{ind}(f)) = 1$ and $(1, \alpha, \alpha^2, \alpha^3, \frac{\theta^4}{5})$ is an integral basis of K .

(c) If $a \equiv 15b^3 \pmod{25}$ and $v_5(C) = 2$, then $v_5(\text{ind}(f)) = 2$ and $(1, \alpha, \alpha^2, \frac{\theta^3}{5}, \frac{\theta^4}{5})$ is a 5-integral basis of K .

(d) If $a \equiv 15b^3 \pmod{25}$ and $v_5(C) \geq 3$, then $v_5(A) = 1$. Let s be a regular integer defined by Lemma 3.2, $f(X + s)$, $A = 10s^3 + a$ and $\theta = \alpha - s$. It follows that: If $2u_4 \geq u_5 + 1$, then $v_5(\text{ind}(f)) = 2 + \mu$, $(1, \alpha, \alpha^2, \frac{\theta^3}{5}, \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta}{5^\mu})$ is an integral basis of K and $v_5(\Delta) = 6 + u_5$, where $\mu = \lfloor \frac{u_5 + 1}{2} \rfloor$.

If $2u_4 < u_5 + 1$, then $v_5(\text{ind}(f)) = 1 + u_4$, $(1, \alpha, \alpha^2, \frac{\theta^3}{5}, \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta}{5^{u_4}})$ is an integral basis of K and $v_5(\Delta) = 4 + 2u_4$.

(3) $v_p(a) = 0$ and $v_p(b) \geq 1$. Then $\bar{f}(X) \equiv X^2(X^3 + a) \pmod{p}$. By Hensel's Lemma, $f(X) = F_1(X)F_2(X)$ in $\mathbb{Z}_p[X]$, where $\bar{F}_1(X) \equiv X^2 \pmod{p}$, $\bar{F}_2(X) \equiv (X^3 + a) \pmod{p}$. If $p \neq 3$, then $\bar{F}_2(X)$ is square free, $v_p(\text{ind}(F_2)) = 0$ and $v_p(\text{ind}(f)) = v_p(\text{ind}(F_1))$. Thus,

(a) If $p \notin \{2, 3\}$, then $v_p(\text{ind}(f)) = r = \lfloor \frac{v_p(b)}{2} \rfloor$ and $(1, \alpha, \alpha^2, \alpha^3, \frac{\alpha^4 + a\alpha}{p^r})$ is a p -integral basis of K .

(b) If $p = 2$ and $v_2(b) = 2k + 1$, then $v_p(\text{ind}(f)) = k$ and $(1, \alpha, \alpha^2, \alpha^3, \frac{\alpha^4 + a\alpha}{2^k})$ is a 2-integral basis of K .

If $p = 2$ and $v_2(b) = 2k$, then let $P(X) = f(X + 2^k) = X^5 + 5 \cdot 2^k X^4 + 5 \cdot 2^{2k+1} X^3 + AX^2 + BX + C$ and $\theta = \alpha - 2^k$. Then $v_2(A) = 0$, $B = 2^{k+1}(5 \cdot 2^{3k-1} + a)$ and $C = 2^{2k}(2^{3k} + a + b_2)$. Thus, $v_2(B) = k + 1$ and $v_2(C) = 2k + r$, where $r = 1$, if $a + b_2 \equiv 2 \pmod{4}$ and $r \geq 2$, if $a + b_2 \not\equiv 2 \pmod{4}$. Therefore, if $a + b_2 \equiv 2 \pmod{4}$, then $(1, \alpha, \alpha^2, \alpha^3, \frac{\alpha^4 + a\alpha}{2^k})$ is a 2-integral basis of K . If $a + b_2 \not\equiv 2 \pmod{4}$, then $(1, \alpha, \alpha^2, \alpha^3, \frac{\theta^4 + 2^k \theta^3 + a\theta}{2^{k+1}})$ is a 2-integral basis of K .

- (c) For $p = 3$, we have $v_3(\text{ind}(f)) = v_3(\text{ind}(F_1)) + v_3(\text{ind}(F_2))$. As in the previous case, $v_3(\text{ind}(F_1)) = r = \lfloor \frac{v_3(b)}{2} \rfloor$.

For $v_3(\text{ind}(F_2))$, let s be a regular integer given Lemma 3.1, and consider $f(X + s)$.

If $a^2 \not\equiv 4 \pmod{9}$, then $s = -a$, $v_3(A) \geq 1$ and $v_3(B) = 1$. Thus, if $v_3(C) = 1$, then $v_3(\text{ind}(F_2)) = 0$ and $(1, \alpha, \alpha^2, \alpha^3, \frac{\alpha^4 + a\alpha}{3^r})$ is a 3-integral basis of K .

If $v_3(C) \geq 2$, then $v_3(\text{ind}(F_2)) = 1$ and $(1, \alpha, \alpha^2, \frac{\alpha^3 + \alpha^2}{3}, \frac{\alpha^4 + a\alpha}{3^r})$ is a 3-integral basis of K .

If $a^2 \equiv 4 \pmod{9}$, for a regular integer s , $u_3 = 1$ and $u_4 \geq 2$. It follows that:

If $u_5 = 1$, then $v_3(\text{ind}(F_2)) = 0$ and $(1, \alpha, \alpha^2, \alpha^3, \frac{\alpha^4 + a\alpha}{3^r})$ is a 3-integral basis of K .

If $u_5 = 2$, then $v_3(b) = 1$, $v_3(\text{ind}(f)) = v_3(\text{ind}(F_2)) = 2$ and $(1, \alpha, \alpha^2, \frac{\theta^3 + a\theta^2 + \theta}{3}, \frac{\theta^4 + a\theta^3 + \theta^2}{3})$ is a 3-integral basis of K .

If $u_5 \geq 3$, then $v_3(b) = 1$, $v_3(\text{ind}(f)) = v_3(\text{ind}(F_2)) = 1 + \mu$, where $\mu = \text{Min}(u_4, \lfloor \frac{u_5 + 1}{2} \rfloor)$. So, $(1, \alpha, \alpha^2, \frac{\theta^3 + a\theta^2 + \theta}{3}, \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta}{3^\mu})$ is a 3-integral basis of K .

- (4) $v_p(ab) = 0$. Since $\Delta = b(5^5 b^3 + 2^2 \cdot 3^3 a^5)$, if $p \in \{2, 3, 5\}$, then $v_p(\Delta) = 0$, and then $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. If $p \geq 7$ and $v_p(\Delta) \leq 1$, then $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. For $p \geq 7$ and $v_p(\Delta) \geq 2$, using the Euclid's algorithm, we have $25bX - 6a^2 \pmod{p}$ is the greatest common divisor of $\bar{f}(X)$ and $\bar{f}'(X) \pmod{p}$. Let $s \in \mathbb{Z}$ such that $25bs \equiv 6a^2 \pmod{p^{v_p(\Delta)+1}}$ and $P(X) = f(X + s) = X^5 - 5sX^4 + 10s^2X^3 + AX^2 + BX + C$, where $A = 10s^3 + a$, $B = 5s^4 + 2as$ and $C = s^5 + as^2 + b$. Then $(25b)^3 B \equiv s((6a^2)^3 + 2a(25b)^3) \equiv 10as(5^5 b^3 + 2^2 \cdot 3^3 a^5) \pmod{p^{v_p(\Delta)+1}}$ and $(5^5 b^3 + 2^2 \cdot 3^3 a^5)^2 - (25b)^5 C \equiv 4.9(5^5 b^3 + 2^2 \cdot 3^3 a^5) \pmod{p^{v_p(\Delta)+1}}$. The fact $v_p(\Delta) = v_p(5^5 b^3 + 2^2 \cdot 3^3 a^5)$ implies that $v_p(B) = v_p(C) = v_p(\Delta)$. As $sA - 2B = -as$, then $v_p(A) = 0$. It follows that $v_p(\text{ind}(f)) = r$ and $(1, \alpha, \alpha^2, \alpha^3, \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta}{p^r})$ is a p -integral basis of K , where $r = \lfloor \frac{v_p(\Delta)}{2} \rfloor$.

□

4. PRIME IDEAL FACTORIZATION

In this section, for every prime integer p , an explicit factorization of the principal ideal $p\mathbb{Z}_K$ into prime ideals of $\mathbb{Z}_K$ is given. Note only the form is given, but two element generators of each prime ideal factor are given.

Theorem 4.1. *Let p be a prime integer. In the following tables, the form of $p\mathbb{Z}_K$ as a product of prime ideals of $\mathbb{Z}_K$, and for every prime factor P of $p\mathbb{Z}_K$ an integral element β of K such that $P = (p, \beta)$ are given.*

Table A : $v_p(a) \geq 1$ and $v_p(b) \geq 1$

case	conditions	p	the form of $p\mathbb{Z}_K$	generators
1	$v_p(b) = 4, v_p(a) \geq 3$		P^5	$\beta = \frac{\alpha^4}{p^3}$
2	$v_p(b) = 3, v_p(a) \geq 2$		P^5	$\beta = \frac{\alpha^2}{p}$
3	$v_p(b) = 2k + 1 \geq 4, v_p(a) = 2$		$P_1^3 P_2^2$	$\beta_1 = \frac{\alpha^2}{p} + \frac{\alpha^3 + a}{p^2}$ $\beta_2 = \frac{\alpha^3}{p^2} + \frac{\alpha^4 + a\alpha}{p^{k+1}}$
4	$v_p(b) = 2k \geq 4, v_p(a) = 2$ $(\frac{-a_p b_p}{p}) = -1$	$\neq 2$	$P_1^3 P_2$	$\beta_1 = \frac{\alpha^4 + a\alpha}{p} + \frac{\alpha^3 + a}{p^2}$ $\beta_2 = \frac{\alpha^3}{p^2} + \frac{\alpha^4 + a\alpha}{p^{k+1}}$
5	$v_p(b) = 2k \geq 4, v_p(a) = 2$ $(\frac{-a_p b_p}{p}) = 1$	$\neq 2$	$P_1^3 P_2 P_3$	$\beta_1 = \frac{\alpha^4 + a\alpha}{p} + \frac{\alpha^3 + a}{p^2}$ $\beta_2 = \frac{\alpha^3}{p^2} + \frac{(\alpha^3 + a)(\alpha + tp^{k-1})}{p^{k+1}} \quad (v_p(a_p t^2 + b_p) = 1)$ $\beta_3 = \frac{\alpha^3}{p^2} + \frac{(\alpha^3 + a)(\alpha - tp^{k-1})}{p^{k+1}}$
6	$v_2(b) = 2k \geq 4, v_2(a) = 2$ $a_2 + b_2 \equiv 2 \pmod{4}$	2	$P_1^3 P_2^2$	$\beta_1 = \frac{\alpha^4 + a\alpha}{2} + \frac{\alpha^3 + a}{2^2}$ $\beta_2 = \frac{\alpha^3}{2^2} + \frac{\alpha^4 + a\alpha}{2^{k+1}}$
7	$v_2(b) = 2k \geq 4, v_2(a) = 2$ $a_2 + b_2 \equiv 4 \pmod{8}$	2	$P_1^3 P_2$	$\beta_1 = \frac{\alpha^4 + a\alpha}{2} + \frac{\alpha^3 + a}{2^2}$ $\beta_2 = \frac{\alpha^3}{2^2} + \frac{\theta^4 + 5 \cdot 2^{k-1} \theta^3 + a\theta}{2^{k+1}} \quad (t = \alpha - 2^{k-1})$
8	$v_2(b) = 2k \geq 4, v_2(a) = 2$ $a_2 + b_2 \equiv 0 \pmod{8}$	2	$P_1^3 P_2 P_3$	$\beta_1 = \frac{\alpha^4 + a\alpha}{2} + \frac{\alpha^3 + a}{2^2}$ $\beta_2 = \frac{\alpha^3}{2^2} + \frac{\theta^4 + 5 \cdot s \theta^3 + a\theta + 2as}{2^{k+2}}$ $(t = \alpha - s, s = 2^{k-1}(1 - (2 + 4t), v_2(b_2 + a_2(1 + 8t)) = 3)$ $\beta_3 = \frac{\alpha^3}{2^2} + \frac{\theta^4 + 5 \cdot s \theta^3 + a\theta}{2^{k+2}}$
9	$v_p(b) = 2, v_p(a) \geq 1$		P^5	$\beta = \frac{\alpha^3}{p}$
10	$v_p(b) = 2k \geq 3, v_p(a) = 1$		$P_1^3 P_2^2$	$\beta_1 = \frac{\alpha^4}{p} + \frac{\alpha^3 + a}{p^2}$ $\beta_2 = \frac{\alpha^3}{p} + \frac{\alpha^4 + a\alpha}{p^k}$
11	$v_p(b) = 2k + 1 \geq 3, v_p(a) = 1$ $(\frac{-a_p b_p}{p}) = -1$	$\neq 2$	$P_1^3 P_2$	$\beta_1 = \frac{\alpha^4}{p} + \frac{\alpha^3 + a}{p^2}$ $\beta_2 = \frac{\alpha^3}{p} + \frac{\alpha^4 + a\alpha}{p^k}$
12	$v_p(b) = 2k + 1 \geq 3, v_p(a) = 1$ $(\frac{-a_p b_p}{p}) = 1$	$\neq 2$	$P_1^3 P_2 P_3$	$\beta_1 = \frac{\alpha^4}{p} + \frac{\alpha^3 + a}{p^2}$ $\beta_2 = \frac{\alpha^3}{p} + \frac{(\alpha^3 + a)(\alpha + tp^k)}{p^{k+1}} \quad (v_p(a_p t^2 + b_p) = 1)$ $\beta_3 = \frac{\alpha^3}{p} + \frac{(\alpha^3 + a)(\alpha - tp^k)}{p^{k+1}}$
13	$v_p(b) = 2k + 1 \geq 3, v_p(a) = 1$ $a_2 + b_2 \equiv 2 \pmod{4}$	2	$P_1^3 P_2^2$	$\beta_1 = \frac{\alpha^4}{2} + \frac{\alpha^3 + a}{2}$ $\beta_2 = \frac{\alpha^3}{2} + \frac{\theta^4 + a\theta}{2^{k+1}} \quad (\theta = \alpha - 2^k)$
14	$v_p(b) = 2k + 1 \geq 3, v_p(a) = 1$ $a_2 + b_2 \equiv 4 \pmod{8}$	2	$P_1^3 P_2$	$\beta_1 = \frac{\alpha^4}{2} + \frac{\alpha^3 + a}{2}, \theta = \alpha - 2^k$ $\beta_2 = \frac{\theta^3}{2} + \frac{\theta^4 + A\theta}{2^{k+1}} \quad (\theta = \alpha - 2^k)$
15	$v_p(b) = 2k + 1 \geq 3, v_p(a) = 1$ $a_2 + b_2 \equiv 0 \pmod{8}$	2	$P_1^3 P_2 P_3$	$\beta_1 = \frac{\alpha^4}{2} + \frac{\alpha^3 + a}{2}, \theta = \alpha - 2^k$ $\beta_2 = \frac{\alpha^3}{2} + \frac{\theta^4 + 5 \cdot s \theta^3 + a\theta + 2as}{2^{k+2}}$ $(t = \alpha - s, s = 2^k(1 - (2 + 4t), v_2(b_2 + a_2(1 + 8t)) = 3)$ $\beta_3 = \frac{\alpha^3}{2} + \frac{\theta^4 + 5 \cdot 2^k \theta^3 + a\theta}{2^{k+2}}$
16	$v_p(b) = 1, v_p(a) \geq 1$		P^5	$\beta = \alpha$

Table B : $v_p(b) = 0$ and $v_p(a) \geq 1$

Let $\theta = \alpha + b$

Case	Conditions	p	the form of $p\mathbb{Z}_K$	generators
B1		$p \geq 7$	p -analogous to $f \pmod{p}$	
B2		2	$P_1 P_2$	$\beta_1 = \alpha + 1$ $\beta_2 = \alpha^4 + \alpha^3 + \alpha^3 + \alpha + 1$
B3	$b \equiv 1 \pmod{3}$	3	$P_1 P_2$	$\beta_1 = \alpha + 1$ $\beta_2 = \alpha^4 - \alpha^3 + \alpha^3 - \alpha + 1$
B4	$b \equiv -1 \pmod{3}$	3	$P_1 P_2$	$\beta_1 = \alpha - 1$ $\beta_2 = \alpha^4 + \alpha^3 + \alpha^3 + \alpha + 1$
B5	$v_5(b^4 - 1 + ab) = 1$	5	P^5	$\beta = \alpha + b$
B6	$v_5(b^4 - 1 + ab) \geq 2, v_5(5b^3 - 2a) = 1$	5	$P_1^4 P_2$	$\beta_1 = \theta + \frac{\theta^4 + (5b^4 - 2ab)\theta}{5}, \beta_2 = 5 + \frac{\theta^4}{5}$
B7	$v_5(b^4 - 1 + ab) = 2, a \equiv 15b^3 \pmod{25}$	5	$P_1^3 P_2^2$	$\beta_1 = \theta + \frac{\theta^3 + (5b^4 - 2ab)}{5}, \beta_2 = \frac{\theta^3}{5}$
B5	$v_5(b^4 - 1 + ab) \geq 3, a \equiv 15b^3 \pmod{25}$	5	go to Table B5	

If $a \equiv 15b^3 \pmod{25}$ and $v_5(b^4 - 1 + ab) \geq 3$, then let s be a regular integer defined by Lemma 3.2.

Table B5 : $a \equiv 15b^3 \pmod{25}$ and $v_5(b^4 - 1 + ab) \geq 3$

Let $\theta = \alpha - s, A = -5s^3 + a, B = 5s^4 + 2as, C = f(s), u_4 = v_5(B)$ and $u_5 = v_5(C)$.

Case	Conditions	the form $p\mathbb{Z}_K$	generators
B5.1	$2u_4 \geq u_5 + 1$ $u_5 = 2k$	$P_1^3 P_2^2$ $\mu = \lfloor \frac{u_5 + 1}{2} \rfloor$	$\beta_1 = \frac{\theta^3 + A}{5}$ $\beta_2 = \frac{\theta^3}{5} + \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta}{5^k}$
B5.2	$2u_4 > 4$ $u_5 = 3, (\frac{A_5 C_5}{5}) = -1$	$P_1^3 P_2$	$\beta_1 = \frac{\theta^3 + A}{5}$ $\beta_2 = \frac{\theta^3}{5} + \theta$
B5.3	$2u_4 > u_5 + 1$ $u_5 = 2k + 1 \geq 5, (\frac{A_5 C_5}{5}) = -1$	$P_1^3 P_2$	$\beta_1 = \frac{\theta^3 + A}{5}$ $\beta_2 = \frac{\theta^3}{5} + \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta}{5^k}$
B5.4	$2u_4 > u_5 + 1$ $u_5 = 2k + 1, (\frac{A_5 C_5}{5}) = 1$	$P_1^3 P_2 P_3$	$\beta_1 = \frac{\theta^3 + A}{5}$ $\beta_2 = \frac{\theta^3}{5} + \frac{(\theta^3 + 5s\theta^2 + 10s^2\theta + A)(\theta + tp^k)}{5^{k+1}} (v_5(A_5 t^2 + C_5) = 1)$ $\beta_3 = \frac{\theta^3}{5} + \frac{(\theta^3 + 5s\theta^2 + 10s^2\theta + A)(\theta - tp^k)}{5^{k+1}}$
B5.5	$2u_4 = u_5 + 1$ $u_5 = 2k + 1, (\frac{B_5^2 + A_5 C_5}{5}) = -1$	$P_1^3 P_2$	$\beta_1 = \frac{\theta^3 + A}{5}$ $\beta_2 = \frac{\theta^3}{5} + \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta}{5^k}$
B5.6	$2u_4 = u_5 + 1$ $u_5 = 2k + 1, (\frac{B_5^2 + A_5 C_5}{5}) = 1$	$P_1^3 P_2 P_3$	$\beta_1 = \frac{\theta^3 + A}{5}$ $\beta_2 = \frac{\theta^3}{5} + \frac{(\theta^3 + 5s\theta^2 + 10s^2\theta + A)(\theta + tp^k)}{5^{k+1}} (v_5(A_5 t^2 + B_5 t + C_5) = 1)$ $\beta_3 = \frac{\theta^3}{5} + \frac{(\theta^3 + 5s\theta^2 + 10s^2\theta + A)(\theta - tp^k)}{5^{k+1}}$
B5.7	$2u_4 = u_5$	$P_1^3 P_2 P_3$	$\beta_1 = \frac{\theta^3 + A}{5}$ $\beta_2 = \frac{\theta^3}{5} + \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta + B}{5^{u_4}}$ $\beta_3 = \frac{\theta^3}{5} + \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta}{5^{u_4}}$
B5.8	$2u_4 < u_5$	$P_1^3 P_2 P_3$	$\beta_1 = \frac{\theta^3 + A}{5}$ $\beta_2 = \frac{\theta^3}{5} + \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta + B}{5^{u_4}} + 5$ $\beta_3 = \frac{\theta^3}{5} + \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta}{5^{u_4}} + 5$

TableC : $v_p(a) = 0$ and $v_p(b) \geq 1$

Case	Conditions	p	the form of $p\mathbb{Z}_K$	generators
C1	$v_p(b) = 2k + 1$	$p \notin \{2, 3\}$	$I.P^2$	I is p -analogous to $X^3 + a$ $\beta = \frac{\alpha(\alpha^3+a)}{p^k}$
C2	$v_p(b) = 2k \geq 2$ $(\frac{-b_p a_p}{p}) = -1$	$p \notin \{2, 3\}$	$I.P$	I is p -analogous to $X^3 + a$ $\beta = \frac{\alpha(\alpha^3+a)}{p^{k-1}}$
C3	$v_p(b) = 2k \geq 2$ $(\frac{-b_p a_p}{p}) = 1$	$p \notin \{2, 3\}$	$I.P_1P_2$	I is p -analogous to $X^3 + a$ $\beta_1 = \frac{(\alpha^3+a)(\alpha+tp^k)}{p^k}$ ($v_p(at^2 + b_p) = 1$) $\beta_2 = \frac{(\alpha^3+a)(\alpha-tp^k)}{p^k}$
C4	$v_2(b) = 1$	2	$P_1P_2P_3^2$	$\beta_1 = \alpha + 1, \beta_12 = \alpha^2 + \alpha + 1$ $\beta_3 = \alpha$
C5	$v_2(b) = 2k + 1$ $k \geq 1$	2	$P_1P_2P_3^2$	$\beta_1 = \alpha + 3, \beta_2 = \alpha^2 + \alpha + 3$ $\beta_3 = \frac{\alpha^4+a\alpha}{2^k}$
C6	$v_2(b) = 2k, a \equiv -b_2 \pmod{8}$	2	$P_1P_2P_3P_4$	$\beta_1 = \alpha + 3, \beta_2 = \alpha^2 + \alpha + 3$ $\beta_3 = \frac{\alpha^4+a\alpha}{2^k}$ ($\theta = \alpha - 2^k$) $\beta_4 = \frac{\alpha^4+a\alpha}{2^k}$
C6	$v_2(b) = 2k, a \equiv 4 - b_2 \pmod{8}$	2	$P_1P_2P_3$	$\beta_1 = \alpha + 3, \beta_2 = \alpha^2 + \alpha + 3$ $\beta_3 = \theta + 2$ ($\theta = \alpha - 2^k$)
C7	$v_2(b) = 2k, a \equiv 2 - b_2 \pmod{4}$	2	$P_1P_2P_3^2$	$\beta_1 = \alpha + 3, \beta_2 = \alpha^2 + \alpha + 3$ $\beta_3 = \frac{\theta^4+a\theta}{2^k}$ ($\theta = \alpha - 2^k$)
C8		3	go to TableC5	

TableC5 : $p = 3$, $v_3(a) = 0$ and $v_3(b) \geq 1$

Let $A = -10a^3 + a$, $B = -a^2(2 - 5a^2)$, $C = b + a^3 - a^5$ and $\theta = \alpha + a$.

Case	Conditions	the form of $3\mathbb{Z}_K$	generators
C5.1	$v_3(-a^5 + a^3 + b) = 1$, $v_3(b) = 1$	$P_1^2 P_2^3$	$\beta_1 = \alpha$, $\beta_2 = \theta$
C5.2	$v_3(-a^5 + a^3 + b) = 1$, $v_3(b) = 2k + 1 \geq 3$	$P_1^2 P_2^3$	$\beta_1 = \alpha + \frac{\alpha^4 + a\alpha}{3^k}$ $\beta_2 = \theta$
C5.3	$v_3(-a^5 + a^3 + b) = 1$, $v_3(b) = 2k \geq 2$ $(\frac{ab_3}{3}) = -1$	$P_1 P_2^3$	$\beta_1 = \alpha + \frac{\alpha^4 + a\alpha}{3^{k-1}}$ $\beta_2 = \theta$
C5.4	$v_3(-a^5 + a^3 + b) = 1$, $v_3(b) = 2k \geq 2$ $(\frac{ab_3}{3}) = 1$	$P_1 P_2 P_3^3$	$\beta_1 = \alpha + \frac{(\alpha^3 + a)(\alpha + 3^k t)}{3^k}$ $\beta_2 = \alpha + \frac{(\alpha^3 + a)(\alpha - 3^k t)}{3^k}$ ($v_3(at^2 + b_3) = 1$) $\beta_3 = \theta$
C5.5	$v_3(-a^5 + a^3 + b) = 2$, $v_3(b) = 2k + 1 \geq 3$ $a^2 \not\equiv 4 \pmod{9}$	$P_1^2 P_2^2 P_3$	$\beta_1 = \alpha + \frac{\alpha^4 + a\alpha}{3^k}$ $\beta_2 = \alpha + \frac{(\alpha^3 + a)(\alpha - 3^k t)}{3^k}$ ($v_3(at^2 + b_3) = 1$) $\beta_3 = \theta + \frac{\theta^4 - 5a\theta^3 + 10a^2\theta^2 + A\theta + B}{3}$ $\beta_4 = \theta + \frac{\theta^4 - 5a\theta^3 + 10a^2\theta^2}{3}$
C5.6	$v_3(-a^5 + a^3 + b) \geq 3$, $v_3(b) = 2k + 1 \geq 3$ $a^2 \not\equiv 4 \pmod{9}$	$P_1^2 P_2^2 P_3$	$\beta_1 = \alpha + \frac{\alpha^4 + a\alpha}{3^k}$ $\beta_2 = \alpha + \frac{(\alpha^3 + a)(\alpha - 3^k t)}{3^k}$ ($v_3(at^2 + b_3) = 1$) $\beta_3 = \theta + \frac{\theta^4 - 5a\theta^3 + 10a^2\theta^2 + A\theta + B}{3}$ $\beta_4 = \theta + 3 + \frac{\theta^4 - 5a\theta^3 + 10a^2\theta^2}{3}$
C5.7	$v_3(-a^5 + a^3 + b) = 2$, $v_3(b) = 2k \geq 2$ $a^2 \not\equiv 4 \pmod{9}$, $(\frac{ab_3}{3}) = 1$	$P_1 P_2 P_3^2 P_4$	$\beta_1 = \alpha + \frac{(\alpha^3 + a)(\alpha + 3^k t)}{3^k}$ $\beta_2 = \alpha + \frac{(\alpha^3 + a)(\alpha - 3^k t)}{3^k}$ ($v_3(at^2 + b_3) = 1$) $\beta_3 = \theta + \frac{\theta^4 - 5a\theta^3 + 10a^2\theta^2 + A\theta + B}{3}$ $\beta_4 = \theta + \frac{\theta^4 - 5a\theta^3 + 10a^2\theta^2}{3}$
C5.8	$v_3(-a^5 + a^3 + b) \geq 3$, $v_3(b) = 2k \geq 2$ $a^2 \not\equiv 4 \pmod{9}$, $(\frac{ab_3}{3}) = 1$	$P_1 P_2 P_3^2 P_4$	$\beta_1 = \alpha + \frac{(\alpha^3 + a)(\alpha + 3^k t)}{3^k}$ $\beta_2 = \alpha + \frac{(\alpha^3 + a)(\alpha - 3^k t)}{3^k}$ ($v_3(at^2 + b_3) = 1$) $\beta_3 = \theta + \frac{\theta^4 - 5a\theta^3 + 10a^2\theta^2 + A\theta + B}{3}$ $\beta_4 = \theta + \frac{\theta^4 - 5a\theta^3 + 10a^2\theta^2}{3} + 3$
C5.9	$v_3(-a^5 + a^3 + b) = 2$, $v_3(b) = 1$ $a^2 \not\equiv 4 \pmod{9}$	$P_1 P_2^2 P_3$	$\beta_1 = \alpha$ $\beta_2 = \theta + \frac{\theta^4 - 5a\theta^3 + 10a^2\theta^2 + A\theta + B}{3}$ $\beta_3 = \theta + \frac{\theta^4 - 5a\theta^3 + 10a^2\theta^2}{3}$
C5.10	$v_3(-a^5 + a^3 + b) \geq 3$, $v_3(b) = 1$ $a^2 \not\equiv 4 \pmod{9}$	$P_1 P_2^2 P_3$	$\beta_1 = \alpha$ $\beta_2 = \theta + \frac{\theta^4 - 5a\theta^3 + 10a^2\theta^2 + A\theta + B}{3}$ $\beta_3 = \theta + \frac{\theta^4 - 5a\theta^3 + 10a^2\theta^2}{3} + 3$
C5.11	$v_3(-a^5 + a^3 + b) = 2$ $a^2 \equiv 4 \pmod{9}$	$P_1^2 P_2^3$	$\beta_1 = \alpha$ $\beta_2 = \theta + \frac{\theta^4 - 5a\theta^3 + 10a^2\theta^2 + A\theta + B}{3}$
C5.12	$v_3(-a^5 + a^3 + b) \geq 3$, $a^2 \equiv 4 \pmod{9}$	go to tableC5.12	

TableC5.12 : $a^2 \equiv 4 \pmod{9}$ and $v_3(-a^5 + a^3 + b) \geq 3$

Let s be a regular integer, $A = 10s^3 + a$, $B = f'(s)$, $C = f(s)$ $\theta = \alpha - s$, $u_4 = v_3(B)$ and $u_5 = v_3(C)$.

Case	Conditions	the form of $3\mathbb{Z}_K$	generators
1	$u_4 \geq 3, u_5 = 3$ $A_3 \equiv -C_3 \pmod{3}$	$P_1^2 P_2$	$\beta_1 = \alpha, \beta_2 = \theta$
2	$u_4 \geq 3, u_5 = 3$ $A_3 \equiv C_3 \pmod{3}$	$P_1^2 P_2 P_3$	$\beta_1 = \alpha, \beta_2 = \theta + \frac{(\theta^2 + 5s\theta + 10s^2)(\theta + 3t)}{9} \pmod{v_3(A_3 t^2 + C_3) = 1}$ $\beta_3 = \theta + \frac{(\theta^2 + 5s\theta + 10s^2)(\theta^2 + 9u)}{9} \pmod{A_3 u - C_3 \equiv 0 \pmod{3}}$
3	$u_4 = 2, u_5 = 3$ $A_3 B_3 C_3 \equiv -1 \pmod{3}$	$P_1^2 P_2$	$\beta_1 = \alpha, \beta_2 = \theta$
3	$u_4 = 2, u_5 = 3$ $A_3 \equiv C_3 \equiv B_3 \equiv 1 \pmod{3}$	$P_1^2 P_2 P_3$	$\beta_1 = \alpha$ $\beta_2 = \theta + \frac{(\theta^2 + 5s\theta + 10s^2)(\theta + 3t)}{3} \pmod{t^3 - t^2 A_3 + t B_3 - C_3 \equiv 0 \pmod{9}}$ $\beta_3 = \theta + \frac{(\theta^2 + 5s\theta + 10s^2)(\theta^2 + 9)}{3}$
3	$u_4 = 2, u_5 = 3$ $A_3 \equiv C_3 \equiv -1 \pmod{3}, B_3 \equiv 1 \pmod{3}$	$P_1^2 P_2 P_3$	$\beta_1 = \alpha$ $\beta_2 = \theta + \frac{(\theta^2 + 5s\theta + 10s^2)(\theta + 3t)}{3} \pmod{t^3 - t^2 A_3 + t B_3 - C_3 \equiv 0 \pmod{9}}$ $\beta_3 = \theta + \frac{(\theta^2 + 5s\theta + 10s^2)(\theta^2 + 9)}{3}$
3	$u_4 = 2, u_5 = 3$ $A_3 \equiv C_3 \equiv -1 \pmod{3}, B_3 \equiv 1 \pmod{3}$	$P_1^2 P_2$	$\beta_1 = \alpha, \beta_2 = \theta$
4	$u_4 = 2, u_5 = 3$ $A_3 \equiv C_3 \pmod{3}$	$P_1^2 P_2 P_3$	$\beta_1 = \alpha, \beta_2 = \theta + \frac{(\theta^2 + 5s\theta + 10s^2)(\theta + 3t)}{9} \pmod{v_3(A_3 t^2 + C_3) = 1}$ $\beta_3 = \theta + \frac{(\theta^2 + 5s\theta + 10s^2)(\theta^2 + 9u)}{9} \pmod{A_3 u - C_3 \equiv 0 \pmod{3}}$
	$A_3 B_3 C_3 \equiv -1 \pmod{3}$		$\beta_3 = \theta + \frac{(\theta^2 + 5s\theta + 10s^2)(\theta^2 + 9u)}{9} \pmod{A_3 u - C_3 \equiv 0 \pmod{3}}$
1	$u_4 \geq 3, u_5 = 3$ $A_3 \equiv -C_3 \pmod{3}$	$P_1^2 P_2$	$\beta_1 = \alpha, \beta_2 = \theta$
3	$2u_4 > u_5 + 1$ $u_5 = 2k + 1 \geq 5, A_3 C_3 \equiv -1 \pmod{3}$	$P_1^2 P_2 P_3$	$\beta_1 = \alpha, \beta_2 = \theta + \frac{\theta^3 + 5s\theta^2 + 10s^2\theta + A}{3}$ $\beta_3 = \theta + \frac{\theta^3 + 5s\theta^2 + 10s^2\theta}{3} + 3$
4	$2u_4 > u_5 + 1$ $u_5 = 2k + 1 \geq 5, A_3 C_3 \equiv 1 \pmod{3}$	$P_1^2 P_2 P_3 P_4$	$\beta_1 = \alpha, \beta_2 = \theta + \frac{\theta^3 + 5s\theta^2 + 10s^2\theta + A}{3}$ $\beta_3 = \theta + \frac{(\theta^2 + 5s\theta + 10s^2)(\theta + t3^k)}{3^k} \pmod{v_3(A_3 t^2 + C_3) = 1}$ $\beta_4 = \theta + \frac{(\theta^2 + 5s\theta + 10s^2)(\theta - t3^k)}{3^k}$
5	$2u_4 \geq u_5 + 1$ $u_5 = 2k \geq 4$	$P_1^2 P_2 P_3^2$	$\beta_1 = \alpha, \beta_2 = \theta + \frac{\theta^3 + 5s\theta^2 + 10s^2\theta + A}{3^k}$ $\beta_3 = \theta + \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2}{3^k}$
6	$2u_4 - 1 = u_5 \geq 5$	$P_1^2 P_2 P_3$	$\beta_1 = \alpha, \beta_2 = \theta + \frac{\theta^3 + 5s\theta^2 + 10s^2\theta + A}{3}$ $\beta_3 = \theta + \frac{\theta^3 + 5s\theta^2 + 10s^2\theta}{3} + 3$

TableD : $v_p(ab) = 0$

For $p \geq 7$ and $v_p(\Delta) \geq 2$, let $s \in \mathbb{Z}$ such that $25bs \equiv 6a^2 \pmod{p^{v_p(\Delta)+1}}$, $A = 10s^3 + a$, $B = f'(s)$ and $C = f(s)$.

Case	Conditions	p	the form of $p\mathbb{Z}_K$	generators
D1		$p \in \{2, 3, 5\}$	p -analogous to $f(X)$	
D2	$v_p(\Delta) = 0$	$p \geq 7$	p -analogous to $f(X)$	
D3	$v_p(\Delta) = 1$	$p \geq 7$	IP^2	I is p -analogous to $\overline{X^3 + 5sX^2 + 10s^2X + A}$ $\beta = \theta$
D4	$v_p(\Delta) \geq 2$ $v_p(\Delta) = 2k + 1$	$p \geq 7$	IP^2	I is p -analogous to $\overline{X^3 + 5sX^2 + 10s^2X + A}$ $\beta = \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta}{p^k}$
D5	$v_p(\Delta) \geq 2$ $v_p(\Delta) = 2k, (\frac{-AC_p}{p}) = -1$	$p \geq 7$	IP	I is p -analogous to $\overline{X^3 + 5sX^2 + 10s^2X + A}$ $\beta = \frac{\theta^4 + 5s\theta^3 + 10s^2\theta^2 + A\theta}{p^{k-1}}$

Let $p\mathbb{Z}_K = \prod_i^r P_i^{e_i}$. If $r = 1$, then it suffices to find an integral element β such that $v_{P_1}(\beta) = 1$. If $r \geq 2$, then for every $i \neq j$, an element $\beta_i \in K$ such that $v_{P_i}(\beta_i) = 1$ and $v_{P_j}(\beta_i) = 0$ will be calculated. If $v_p(ab) = 0$, $v_p(\Delta) = 2k$ and $(\frac{-AC_p}{p}) = 1$, then $p\mathbb{Z}_K = IP_1P_2$, where I is p -analogous to $\overline{X^3 - 5sX^2 + 10s^2X + A}$ and for every $i := 1, 2$, $v_{P_i}(\theta) = k$. Let $t \in \mathbb{Z}$ such that $v_p(C_p + t^2A) = 1$ (up to replace t by $t + p$, such a t exists), $\phi = X + tp^k$ and

consider the ϕ -adic development of $f(X + s)$, where $25bs \equiv 6a^2 \pmod{p^{2k}}$. Then $v_{P_1}(\theta + tp^k) = k + 1$ and $v_{P_2}(\theta - tp^k) = k + 1$. Thus $\beta_1 = \frac{(\theta^3 - 5s\theta^2 + 10s^2\theta + A)(\theta + tp^k)}{p^{k+1}}$ and $\beta_2 = \frac{(\theta^3 - 5s\theta^2 + 10s^2\theta + A)(\theta - tp^k)}{p^{k+1}}$.

5. EXAMPLES

- (1) $a = 2^4.5^2.11$ and $b = 2^7.5.13^2$. As $v_2(a) = 4$ $v_2(b) = 7$, let us replace a by $2.5^2.11$, b by $b = 2^2.5.13^2$ and α by $\theta = \frac{\alpha}{2}$. Then $\Delta = 2^8.5^9.13^2.109.2038951$. For $p = 2$, we have $(1, \theta, \theta^2, \frac{\theta^3}{2}, \frac{\theta^4}{2})$ is a 2-integral basis of K and $v_2(d_K) = 8 - 4 = 4$. For $p = 5$, since $v_5(b) = 1$ and $v_5(a) \geq 1$, we have $(1, \theta, \theta^2, \theta^3, \theta^4)$ is a 5-integral basis of K and $v_5(d_K) = 9$. For $p = 13$, since $v_{13}(a) = 0$, $v_{13}(b) = 2$ and $a \equiv 4 \pmod{13}$, $(1, \theta, \theta^2, \theta^3, \frac{\theta^4 + 4\theta}{13})$ is a 13-integral basis of K and $v_{13}(d_K) = 0$. As for every prime $p \notin \{2, 5, 13\}$, $v_p(\Delta) \leq$, we have $d_K = 2^4.5^7.13^2.109.2038951$ and $(1, \theta, \theta^2, \frac{\theta^3}{2}, \frac{\theta^4 + 4\theta}{26})$ is an integral basis of K .
- (2) $a = 390$ and $b = 736$. Then $\Delta = 2^{12}.5^9.23.1489.2621$. For $p = 2$, since $v_2(b) = 1$ and $v_2(a) \geq 1$, $v_2(\text{ind}(f)) = 0$ and $v_2(d_K) = 2^{12}$. For $p = 5$, we have $v_5(5b^3 - 2a) = 3$ and $v_5(b^4 - 1 - ab) = 4$. Then $(1, \alpha, \alpha^2, \frac{\alpha^3}{5}, \frac{\alpha^4 - 5\theta^3 + 10\theta^2 + 5\theta}{5^2})$ is a 5-integral basis of K and $v_5(d_K) = 9 - 6 = 3$. The fact that for every prime $p \notin \{2, 5\}$, $v_p(\Delta) \leq 1$ implies that $d_K = 2^{12}.5^3.23.1489.2621$ and $(1, \alpha, \alpha^2, \frac{\alpha^3}{5}, \frac{\alpha^4 - 5\theta^3 + 10\theta^2 + 5\theta}{5^2})$ is an integral basis of K .

6. ACKNOWLEDGMENT

The authors would like to thank Sidi Mohamed Ben Abdellah University (USMBA), LSI and FP of Taza in MOROCCO for their valued supports.

REFERENCES

- [1] A. Alaca and S. Alaca, An integral basis and the discriminant of a quintic field defined by a trinomial $X^5 + aX + b$ (Preprint), (September, 2003).
- [2] H. Cohen, A course in computational algebraic number theory, GTM 138, Springer-Verlag Berlin Heidelberg, New York, Paris, Tokyo, second correction (1995).
- [3] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Abhandlungen der Königl. Gesellschaft der Wissenschaften zu Göttingen 23(1878), 1-23
- [4] L. El Fadil, J. Montes and E. Nart, *Newton polygons and p-Integral Bases of Quartic Number Fields*, J. of Algebra and Its Applications Vol. 11(4) (2012), (33 pages).
- [5] J. Guardia, J. Montes and E. Nart, *Newton polygons of higher order in algebraic number theory*, J. trans. of ams Vol 364(1) (2012), 361416
- [6] K. Hensel, *Untersuchung der Fundamentalgleichung einer Gattung für eine reelle Primzahl als Modul und Bestimmung der Theiler ihrer Discriminante*, J. Reine Angew. Math. 113 (1894), 61-83
- [7] P. Llorente, E. Nart and N. Vila, Decomposition of primes in number fields defined by trinomials, J. Théorie des nombres de Bourdeaux, t1, 1(1991), 27-41.

¹DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCES POLYDISCIPLINARY FACULTY OF OUARZAZAT, P.O. BOX 638-OUARZAZT 45000, IBN ZOHR UNIVERSITY, MOROCCO.

E-mail address: ¹lhouelfaduil2@gmail.com

²SIDI MOHAMED BEN ABDELLAH UNIVERSITY, FSDM, FEZ , MOROCCO.

E-mail address: ²boughaleb01@gmail.com

COMMUNICATED BY:

A. CHILLALI, SIDI MOHAMED BEN ABDELLAH UNIVERSITY, FP, LSI, TAZA, MOROCCO.

E-mail address: abdelhakim.chillali@usmba.ac.ma