

PRIME IDEAL FACTORIZATION IN QUARTIC NUMBER FIELDS

L. EL FADIL ^{1*}, A. CHILLALI ² AND I. AKHARRAZ³

ABSTRACT. For every prime integer p , and for every number field K defined by a p -regular polynomial, the form of the factorization of the principal ideal $p\mathbb{Z}_K$ into prime ideals of $\mathbb{Z}_K$ is given. To illustrate the potential applications of this factorization, we derive from this result an explicit description of the factorization of $p\mathbb{Z}_K$, where K is a quartic number field defined by an irreducible polynomial $X^4 + aX + b \in \mathbb{Z}[X]$.

1. INTRODUCTION

Let K be a number field defined by an irreducible polynomial $F(X) \in \mathbb{Z}[X]$, $\mathbb{Z}_K$ 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 the group $\mathbb{Z}[\alpha]$ in $\mathbb{Z}_K$. In [1], Llorente and Nart given the form of the prime ideal factorization in any cubic number field K . 21 years later, Alaca et al in [2], for every prime factor $\mathfrak{p}$ of $p\mathbb{Z}_K$, they given a p -generator of $\mathfrak{p}$, i.e., an integral element β of K such that $\mathfrak{p} = p\mathbb{Z}_K + \beta\mathbb{Z}_K$. In this paper, for every rational prime p , the form of the factorization of $p\mathbb{Z}_K$ into prime ideals of $\mathbb{Z}_K$; $p\mathbb{Z}_K = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$ is given, where K is a number field defined by a p -regular polynomial. In particular, for any quartic number field K defined by an irreducible polynomial $X^4 + aX + b \in \mathbb{Z}[X]$, and for every rational prime p , an explicit factorization of $p\mathbb{Z}_K$ into prime ideals of $\mathbb{Z}_K$ is given. In that last case, not only the form of the factorization is given, but for every prime factor $\mathfrak{p}$ of $p\mathbb{Z}_K$, a p -generator of $\mathfrak{p}$ will be constructed too.

First, for a prime integer p , $p\mathbb{Z}_K$ is said to be analogous to the factorization of $\bar{F}(X) \pmod{p}$ if $p\mathbb{Z}_K = \prod_{i=1}^r \mathfrak{p}_i^{e_i}$, where $\bar{F}(X) = \prod_{i=1}^r g_i(X)^{e_i}$ is the factorization of $\bar{F}(X)$ in $\mathbb{F}_p[X]$, where every $\mathfrak{p}_i = (p, g_i(\alpha))$. It is well known that if p does not divide the index $ind(F)$, then the Kummer's theorem says that $p\mathbb{Z}_K$ is analogous to the factorization of $\bar{F}(X) \pmod{p}$. R. Dedekind gave a criterion to test if p does not divide the index $ind(F)$, and in that case, we can apply Kummer's theorem(see for example [3, page 257]). In [2], the used method is based on the construction of a p -generator ϕ of $\mathbb{Z}_K$, when p is not a common divisor of K , i.e., p does not divide $[\mathbb{Z}_K : \mathbb{Z}[\phi]]$. But a such construction is not very easy. In

Date: Accepted: Oct 24, 2016.

* Corresponding author.

2010 *Mathematics Subject Classification.* 11Y40.

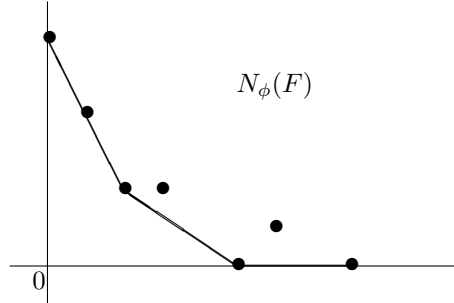
Key words and phrases. Prime ideal factorization, Newton polygons, p -regular polynomial, Quartic number fields.

this paper, based on Newton polygon techniques, the form of $p\mathbb{Z}_K$ will be given and for every prime factor $\mathfrak{p}$ of $p\mathbb{Z}_K$, a p -generator element $\beta \in \mathbb{Z}_K$ of $\mathfrak{p}$ will be constructed. A such β will satisfy $v_{\mathfrak{p}}(\beta) \geq 1$ and for every prime $\mathfrak{p}' \neq \mathfrak{p}$ above p , $v_{\mathfrak{p}'}(\beta) = 0$ and if the ramification index $e(\mathfrak{p}) \geq 2$, then the first condition will be replaced by $v_{\mathfrak{p}}(\beta) = 1$.

For every prime integer p , let v_p be the p -adic discrete valuation defined in $\mathbb{Q}_p$ by $v_p(p) = 1$. v_p is 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 remainder of the Euclidean division of x by m . For every odd prime p , denote $\left(\frac{\cdot}{p}\right)$ the Legendre symbol.

2. NEWTON POLYGONS

Let $F(X)$ be an irreducible polynomial in $\mathbb{Z}[X]$, $\phi \in \mathbb{Z}[X]$ a monic polynomial whose reduction modulo p is an irreducible factor of $\bar{F}(X)$ in $\mathbb{F}_p[X]$. Let $\mathbb{F}_{\phi}$ be the field $\frac{\mathbb{F}_p[X]}{(\phi)}$ and $F(X) = \sum_{i=0}^n a_i(X)\phi(X)^i = a_0(X) + \dots + a_{n-1}(X)\phi(X)^{n-1} + a_n(X)\phi(X)^n$ the ϕ -adic development of $F(X)$ (for every i , $\deg(a_i(X)) \leq \deg(\phi) - 1$). For every prime integer p , the ϕ -Newton polygon of $F(X)$, with respect to p , is the lower convex envelope of the set of points (i, u_i) , $u_i < \infty$, in the Euclidean plane, where $u_i = v_p(a_i(X))$. For example, let $F(X) = \sum_{i=0}^n a_i(X)\phi(X)^i$ and p a fixed prime integer such that $v_p(a_0(X)) = 6$, $v_p(a_1(X)) = 4$, $v_p(a_2(X)) = v_p(a_3(X)) = 2$, $v_p(a_4(X)) = 0$, $v_p(a_5(X)) = 1$ and $v_p(a_6(X)) = 0$.



The ϕ -Newton polygon is the union of different adjacent sides $S_0, \dots, S_g$ with increasing slope $\lambda_0 < \lambda_1 < \dots < \lambda_g$. We shall write $N_{\phi}(F) = S_0 + \dots + S_g$. The principal part of $N_{\phi}(F)$, denoted $N_{\phi}^+(F)$, is the polygon determined by the sides of negative slope of $N_{\phi}(F)$. For every $0 \leq i \leq n$, we attach to any abscissa the following *residual coefficient* $c_i \in \mathbb{F}_{\phi}$:

$$c_i = \begin{cases} 0, & \text{if } (i, u_i) \text{ lies strictly above } N \text{ or } u_i = \infty, \\ \text{red} \left(\frac{a_i(X)}{p^{u_i}} \right) \pmod{(p, \phi(X))}, & \text{if } (i, u_i) \text{ lies on } N. \end{cases}$$

Let S be one of the sides of N , with slope λ . Let $\lambda = -h/e$ such that h and e are positive coprime integers. Let $l = \ell(S)$ be the length of the projection of S to the x -axis and $d = \ell(S)/e$ the degree of S . Note that, if s is the initial abscissa of S , then S is divided into d segments by the points $(s, u_s), (s+e, u_s+h), \dots, (s+de, u_s+dh)$ of integer coordinates that lie on S . Let $F_S(Y) =$

$c_s Y^d + c_{s+e} Y^{d-1} + \cdots + c_{s+(d-1)e} Y + c_{s+de} \in \mathbb{F}_\phi[Y]$, the residual polynomial of $F(X)$ attached to S . For more details on Newton polygon see [4].

3. MAIN RESULTS

Let $F(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial, α a complex root of $F(X)$, p a prime integer, $\phi \in \mathbb{Z}[X]$ a monic polynomial whose reduction (mod p) is an irreducible factor of $\bar{F}(X)$, $N = S_k + \cdots + S_1 + S_0$ the ϕ -Newton polygon of $F(X)$ with respective slopes $\lambda_k < \cdots < \lambda_1 < \lambda_0$. $F(X)$ is said to be ϕ -regular if for every i , $F_{S_i}(Y)$ is square free. $F(X)$ is said to be p -regular if there exist $\phi_1, \dots, \phi_r$ such that $F(X) \equiv \prod_{i=1}^r \bar{\phi}_i^{\ell_i}(X) \pmod{p}$ is the factorization of $\bar{F}(X)$ in $\mathbb{F}_p[X]$ and for every $i := 1, \dots, r$, $F(X)$ is ϕ_i -regular.

3.1. Prime ideal Factorization number fields defined by p -regular polynomials

In this section, K is a number field defined by a p -regular irreducible polynomial $F(X) \in \mathbb{Z}[X]$. Using Newton polygon techniques, the form of the factorization $p\mathbb{Z}_K$ into prime ideals of $\mathbb{Z}_K$ will be given.

Recall the celebrated Hensel theorem:

Theorem 3.1. *Let $F(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial, p a prime integer, $\mathbb{Q}_p$ the p -adic completion of $\mathbb{Q}$ and $\mathbb{Z}_p$ its ring of integers. Let $F(X) = F_1(X) \cdots F_t(X)$ be the factorization into a product of monic irreducible polynomials in $\mathbb{Q}_p[X]$ and consider the local fields $K_i = \mathbb{Q}_p[X]/(F_i(X))$, for $i = 1, \dots, t$. The factorization of $p\mathbb{Z}_K$ into a product of prime ideals of $\mathbb{Z}_K$ is: $p\mathbb{Z}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_t^{e_t}$, where for every $i := 1..t$, $f(\mathfrak{p}_i) = f(K_i/\mathbb{Q}_p)$ and $e_i = \frac{\deg(F_i)}{f(\mathfrak{p}_i)}$.*

Lemma 3.2. *Let $F(X) \in \mathbb{Z}[X]$. If $F(X)$ is irreducible in $\mathbb{Z}_p[X]$, then $\bar{F}(X)$ is congruent to a power of an irreducible factor $\bar{\phi}(X) \pmod{p}$, $N_\phi F = S$ is only one side, and $F_S(Y)$ is congruent to a power of an irreducible factor in $\mathbb{F}_\phi[Y]$.*

Proof. It follows by Hensel Lemma, Theorem of the polygon, and Theorem of the residual polynomial. $\square$

Assume that $F(X)$ is irreducible in $\mathbb{Z}_p[X]$, then let $\mathbb{K}$ be the local field defined by $F(X)$ and $\mathfrak{p}$ prime ideal of $\mathbb{Z}_\mathbb{K}$. let $\phi(X) \in \mathbb{Z}[X]$ be a monic such that $\bar{\phi}(X) \pmod{p}$ is irreducible, $\bar{F}(X)$ is congruent to a power of $\bar{\phi}(X)$, $N_\phi F = S$ is only one side of slope $\lambda = -h/e$, where h and e are positive coprime integers, and assume that $F_S(Y)$ is irreducible in $\mathbb{F}_\phi[Y]$. The following proposition, gives as the ramification index, the residue degree, and a p -generator of $\mathfrak{p}$.

Proposition 3.3. *Under these hypothesis,*

- (1) *For every polynomial $P(X) \in \mathbb{Z}_p[X]$, $v_\mathfrak{p}(P(\alpha)) \geq e(\mathfrak{p})v(P(X))$. With equality if and only if $\bar{\phi}(X)$ does not divide $\bar{P}(X)$.*
- (2) *$e(\mathfrak{p}) = e$ is the ramification index of $\mathfrak{p}$ and $f(\mathfrak{p}) = \frac{n}{e} = \deg(\phi)d$, where $n = \deg(F)$ and $d = \deg(F_S)$.*
- (3) *$v_\mathfrak{p}(\phi(\alpha)) = h$ and if we denote $\gamma = \frac{\phi^e(\alpha)}{p^h}$, then $v_\mathfrak{p}(\gamma) = 0$ and $v_\mathfrak{p}(F_S(\gamma)) \geq 1$.*

- (4) Let n and k are two positive integers such that $hn - ek = 1$. Then $\beta = \frac{\phi(\alpha)^n}{p^k}$ is a generator of $\mathfrak{p}$.

Proof. (1) Consider the ring $i : \mathbb{F}_p[X] \longrightarrow \frac{\mathbb{Z}_K}{\mathfrak{p}}$ defined by $i(a(X)) = \overline{a(\alpha)} \pmod{\mathfrak{p}}$.

Dividing by $p^{v(P(X))}$, we can assume that $v(P(X)) = 0$. Since $\bar{\phi}(X)$ is the minimal polynomial of $\bar{\alpha} \pmod{\mathfrak{p}}$, we conclude that $P(\alpha) \in \mathfrak{p}$ if and only if $\bar{\phi}(X)$ divides $\bar{P}(X)$.

- (2) Let $F(X) = \sum_{i=0}^{\ell} a_{\ell-i}(X)\phi^i(X)$ be the ϕ -adic development of $F(X)$ and set $v_{\mathfrak{p}}(\phi(\alpha)) = u$. Since $N_{\phi}F$ is one side of slope λ , we have for every $i := 0.. \ell - 1$, $v(a_i(X)) \geq (i - \ell)\lambda$ and $v(a_0(X)) = -\ell\lambda$. Thus, for every $i := 0.. \ell - 1$, $v_{\mathfrak{p}}(a_i(\alpha)) \geq (i - \ell)\lambda$. Moreover, since $\deg(a_0(X)) < \deg(\phi(X))$, $v_{\mathfrak{p}}(a_0(\alpha)) = e(\mathfrak{p})v(a_0(X)) = -e(\mathfrak{p})\ell\lambda$. By using, $F(\alpha) = \phi^{\ell}(\alpha) + \dots + a_0(\alpha) = 0$, we conclude that $v_{\mathfrak{p}}(\phi(\alpha)^{\ell}) = v_{\mathfrak{p}}(a_0(\alpha)) = -e(\mathfrak{p})\ell\lambda$ and $v_{\mathfrak{p}}(\phi(\alpha)) = -e(\mathfrak{p})\lambda = \frac{e(\mathfrak{p})h}{e}$. Since e and h are coprime, e divides $e(\mathfrak{p})$. Let $\gamma = \frac{\phi(\alpha)^e}{p^h}$. Then $v_{\mathfrak{p}}(\gamma) = e\frac{e(\mathfrak{p})h}{e} - e(\mathfrak{p})h = 0$ and γ is integral over $\mathbb{Z}_p$. Consider the ring homomorphism: $\iota : \mathbb{F}_{\phi}[Y] \longrightarrow \mathbb{Z}_K/(\mathfrak{p})$, $a(Y) \mapsto \overline{a(\gamma)} \pmod{\mathfrak{p}}$. Then $\iota^{-1}(0)$ is the maximal ideal of $\mathbb{F}_{\phi}[Y]$ generated by the minimal polynomial $\psi(Y)$ of $\bar{\gamma}$ in $\mathbb{F}_{\phi}[Y]$ and $[\mathbb{F}_{\phi}[\gamma] : \mathbb{F}_p]$ divides $f(\mathfrak{p}) = [\frac{\mathbb{Z}_K}{\mathfrak{p}} : \mathbb{F}_p]$. Let $H(X) = X^n + b_{n-1}X^{n-1} + \dots + b_0$ be the minimal polynomial of $\phi(\alpha)^e$ over $\mathbb{Z}_p$ and $G(X) = H(\phi(X)^e) = \sum_{i=0}^{ne} a_{en-i}\phi(X)^{en-i}$, where $a_{(n-j)e}(X) = b_j$ and $a_i(X) = 0$ if $i \notin e\mathbb{N}$. As $v_{\mathfrak{p}}(\phi(\alpha)^e) = -e(\mathfrak{p})e\lambda = e(\mathfrak{p})h$, using the relation relating roots and coefficients of $H(X)$, $v_p(b_0) = \frac{v_{\mathfrak{p}}(b_0)}{e(\mathfrak{p})} = nh$ and for every $i = 1 \dots n - 1$, $v_p(b_{n-i}) \geq (n - i)h$. Thus $N_{\phi}G = T$ is one side of slope $-\frac{ne\lambda}{en} = -\frac{h}{e} = -\lambda$, $N_X(H) = S_0$ is one side of slope $-e\lambda = -h$, and $G_T(Y) = H_{S_0}(Y)$. As $H(X)$ is irreducible in $\mathbb{Z}_p[X]$, by Theorem of the residual polynomial $H_{S_0}(Y)$ and so $G_T(Y)$ is a power of an irreducible polynomial in $\mathbb{F}_{\phi}[Y]$. Since $G(\alpha) = 0$, by Theorem of the product, $F_S(Y)$ divides $G_T(Y)$. But by assumption, $F_S(Y)$ is irreducible, then $G_T(Y)$ is a power of $F_S(Y)$ in $\mathbb{F}_{\phi}[Y]$. On the other hand, $p^{en}H_{S_0}(\gamma) = H(\phi(\alpha)^e) = 0$. It follows that $\psi(Y)$ divides $H_{S_0}(Y)$ and $F_S(Y) = \psi(Y)$ up to a non-zero multiplicative constant element. Finally, $[\mathbb{F}_{\phi}[\gamma] : \mathbb{F}_p] = [\frac{\mathbb{F}_{\phi}[Y]}{(F_S(Y))} : \mathbb{F}_{\phi}][\mathbb{F}_{\phi} : \mathbb{F}_p] = d.m$ and $d.m$ divides $f(\mathfrak{p})$. The fact that e divides $e(\mathfrak{p})$ and $e(\mathfrak{p})f(p) = mde$ implies that $e(\mathfrak{p}) = e$ and $f(\mathfrak{p}) = d.m$.
- (3) Since $v_{\mathfrak{p}}(\phi(\alpha)^e) = e(\mathfrak{p})h$ and $e(\mathfrak{p}) = e$ and the rest follows from $F_S(Y) = \psi(Y)$ up to a non-zero multiplicative constant.
- (4) $v_{\mathfrak{p}}(\frac{\phi^n(\alpha)}{p^k}) = nh - ke = 1$.

□

The following theorem gives the form of the factorization of $p\mathbb{Z}_K$, when K is defined by a p -regular polynomial.

Theorem 3.4. Let $F(X) \in \mathbb{Z}[X]$ be a p -regular monic irreducible polynomial and $\bar{F}(X) \equiv \prod_{i=1}^r \bar{\phi}_i^{\ell_i} \pmod{p}$ the factorization into irreducible polynomials of $\mathbb{F}_p[X]$. For every $i := 1..r$, let $N_i = N_{\phi_i}^+(F) = S_1^i + \dots + S_{k_i}^i$ be the principal ϕ_i -Newton

polygon of $F(X)$. For every $j := 1..k_i$, 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 $\mathbb{F}_{\phi_i}[Y]$. If every $F_{S_j}(Y)$ is square free, i.e., every $n_{i,j,s} = 1$, then

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

and for every $i := 1..r$, $j := 1..k_i$ and $s := 1..r_{ij}$, $v_{\mathfrak{p}_{i,j,s}}(\phi_i(\alpha)) = -e(S_j^i)\lambda_j$, where $e(S_j^i)$ is the ramification index of the side S_j^i and λ_j^i is its slope.

Proof. By Hensel theorem, it suffices to factorize $F(X) = F_1(X) \cdots F_t(X)$ into irreducible polynomials of $\mathbb{Q}_p[X]$. By Hensel lemma, we can split $F(X)$ as a product $F_1(X) \times \cdots \times F_r(X)$ in $\mathbb{Q}_p[X]$ such that for every $i := 1..r$, $\bar{F}_i(X) \equiv \bar{\phi}_i(X)^{\ell_i} \pmod{p}$. Let $\mathcal{P}$ be the set of the prime ideals of $\mathbb{Z}_K$ above p . Then $\mathcal{P} = \bigcup_{i=1}^r \mathcal{P}_i$, where for every $i := 1..r$, $\mathcal{P}_i = \{\mathfrak{p} \in \mathcal{P}, \phi_i(\alpha) \in \mathfrak{p}\}$. Fix $i := 1..r$. From the theorem of the product, the ϕ_i -Newton polygon of $F_i(X)$ is $N_{\phi_i}(F_i) = N_{\phi_i}^+(F) = N_i$ up to a translation. So, we can assume that $r = 1$, $F = F_1$, $\bar{F}(X) \equiv \bar{\phi}(X)^{\ell} \pmod{p}$ and $N_{\phi} F = S_1 + \cdots + S_k$. By the theorem of the polygon, we can split $F(X)$ as a product $G_1(X) \times \cdots \times G_k(X)$ in $\mathbb{Q}_p[X]$ such that for every $i := 1..k$, $\bar{G}_i(X) \equiv \bar{\phi}(X)^{\ell(S_i)} \pmod{p}$, $N_{\phi}(G_i) = S_i$ up to a translation and $G_{iS_i}(Y) = F_{S_i}(Y)$, up to a non zero multiplicative constant. Therefore, we can assume that $k = 1$, $F(X) = G(X)$, $\bar{F}(X) \equiv \bar{\phi}(X)^{\ell} \pmod{p}$, $N_{\phi}(F) = S$ is only one side and $F_S(Y) = \prod_{s=1}^r \psi_s(Y)^{n_s}$ is the factorization of $F_S(Y)$ into irreducible polynomials of $\mathbb{F}_{\phi}[Y]$. By the theorem of the residual polynomial, we can split $F(X)$ as a product $K_1(X) \times \cdots \times K_s(X)$ in $\mathbb{Q}_p[X]$ such that for every $i := 1..s$, $\bar{K}_i(X)$ is a power of $\bar{\phi}(X) \pmod{p}$, $N_{\phi} K_i = T_i$ is only one side ($T_i \subset S_i$), and by the assumption of the Theorem, $(K_i)_{T_i}(Y)$ is irreducible in $\mathbb{F}_{\phi}[Y]$. Thus, for every $i := 1..s$, K_i is irreducible in $\mathbb{Q}_p[X]$. Using (3) of the Proposition 3.3, for every $i := 1..r$, $\mathcal{P}_i = \bigcup_{j=1}^k \mathcal{P}_{i,j}$, where for every $j := 1..k_i$, $\mathcal{P}_{i,j} = \{\mathfrak{p} \in \mathcal{P}_i, v_{\mathfrak{p}}(\phi_i(\alpha)) = h_j \text{ the hight of } S_j\}$ and $\mathcal{P}_{i,j} = \{\mathfrak{p}_{i,j,s}, s := 1..r_{ij}\}$, where for every s , $\mathfrak{p}_{i,j,s}$ is the prime ideal attached to the factor $\psi_{i,j,s}(Y)$ of the residual polynomial of $F_{S_{i,j}}(Y)$. $\square$

Example 3.5. Let $f(X) \in \mathbb{Z}[X]$ be an irreducible polynomial, α a complex root of $f(X)$ and $K = \mathbb{Q}[\alpha]$. For $f = x^9 + 48x^7 + 6x^6 + 24x^5 + 12x^4 + 3x^3 + 18x^2 + 48x + 24$, let $p = 2$, by Einstein criterion, f is irreducible over $\mathbb{Q}$ and $f \equiv x^3(x-1)^2(x^2+x+1)^2 \pmod{2}$. Let $\phi_1 = x$, $\phi_2 = x-1$, and $\phi_3 = x^2+x+1$. Then $f = (x-4)\phi_1^4 + (6x+6)\phi_3^3 - 9x\phi_3^2 + (4x-4)\phi_3 + 2$ and $f = \phi_2^9 + 9\phi_2^8 + 36\phi_2^7 + 84\phi_2^6 + 126\phi_2^5 + 126\phi_2^4 + 85\phi_2^3 + 39\phi_2^2 + 12\phi_2 + 2$. It follows that for every $i = 1, 2, 3$, the principal Newton polygon $N_{\phi_i}^+(f) = S_i$ is only one side with respective hight $H_1 = 3$, $H_2 = H_3 = 1$. Since $f_{S_1}(Y) = Y^3 + Y^2 + 1$ and $f_{S_2}(Y) = f_{S_3}(Y) = Y + 1$ are irreducible in $\mathbb{F}_2[Y]$, then $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2^2\mathfrak{p}_3^2$, where $f(\mathfrak{p}_1) = 3$, $f(\mathfrak{p}_2) = 1$, $f(\mathfrak{p}_3) = 2$, $\mathfrak{p}_1 = (2, \alpha)$, $\mathfrak{p}_2 = (2, \alpha - 1)$ and $\mathfrak{p}_3 = (2, \alpha^2 + \alpha + 1)$.

3.2. Prime ideal factorization in any quartic field defined by

$$X^4 + aX + b$$

In this section, let $F(X) = X^4 + aX + b \in \mathbb{Z}[X]$ be a monic irreducible polynomial such that for every prime p , $v_p(a) \leq 2$ or $v_p(b) \leq 3$. Note that this is not a restriction, because if there exists a prime p such that $v_p(a) \geq 3$ and $v_p(b) \geq 4$, then let q_1 and q_2 be respectively the quotient of $v_p(a)$ by 3 and of $v_p(b)$ by 4, and let $\theta = \frac{\alpha}{p^q}$, where $q = \text{Min}(q_1, q_2)$. Then θ is integral over $\mathbb{Z}$, with minimal polynomial $F(X) = X^4 + AX + B \in \mathbb{Z}[X]$, where $A = \frac{a}{p^{3q}}$ and $B = \frac{b}{p^{4q}}$. Repeat this process until to obtain $v_p(A) \leq 2$ or $v_p(B) \leq 3$. As $K = \mathbb{Q}[\theta] = \mathbb{Q}[\alpha]$, then up to replace α by $\theta = \frac{\alpha}{p^q}$, we can assume that for every prime p , $v_p(a) \leq 2$ or $v_p(b) \leq 3$.

Theorem 3.6. *In the following tables, the form of the factorization of $p\mathbb{Z}_K$ into prime ideals of $\mathbb{Z}_K$, and for every prime factor $\mathfrak{p}$ of $p\mathbb{Z}_K$ a p -generator element β of $\mathbb{Z}_K$, i.e, $\mathfrak{p} = (p, \beta)$, are given. If $p\mathbb{Z}_K = \prod_i \mathfrak{p}_i^{e_i}$, then for every i , a p -generator β_i of $\mathfrak{p}_i$ is an integral element defined by $v_{\mathfrak{p}_j} = (\beta_i) = 0$, for every $j \neq i$, and if $e_i = 1$, $v_{\mathfrak{p}_i} = (\beta_i) \geq 1$. If $e_i \geq 2$, then $v_{\mathfrak{p}_i} = (\beta_i) = 1$. For $p = 2$, $v_2(b) = 2$ and $v_2(a) \geq 2$. In TableA5, a monic polynomial ϕ_2 such that $t = (X, 1/2, \phi_2)$ is $F(X)$ -complete is given too.*

Table A				
Case	Conditions	p	$p\mathbb{Z}_K$	Generators
A1	$v_p(a) \geq 3, v_p(b) = 3$		$\mathfrak{p}^4$	$\mathfrak{p} = (p, \frac{\alpha^3}{p^2})$
A2	$v_p(a) = 2, v_p(b) \geq 3$		$\mathfrak{p}_1^3 \mathfrak{p}_2$	$\mathfrak{p}_1 = (p, \frac{\alpha^3+a}{p^2} + \frac{\alpha^2}{p}),$ $\mathfrak{p}_2 = (p, \frac{\alpha^3}{p^2} + \frac{\alpha^3+a}{p})$
A3	$v_p(a) = 1, v_p(b) \geq 2$		$\mathfrak{p}_1^3 \mathfrak{p}_2$	$\mathfrak{p}_1 = (p, \alpha + \frac{\alpha^3+a}{p}),$ $\mathfrak{p}_2 = (p, \frac{\alpha^3}{p} + p)$
A4	$v_p(a) \geq 1, v_p(b) = 1$		$\mathfrak{p}^4$	$\mathfrak{p} = (p, \alpha)$
A5	$v_p(a) \geq 2, v_p(b) = 2$	2		<i>Tab.A5</i>
A6	$v_p(a) \geq 2, v_p(b) = 2,$	$\neq 2$ $(\frac{-b_p}{p}) = -1$	$\mathfrak{p}^2$	$\mathfrak{p} = (p, \alpha)$
A7	$v_p(a) = 2, v_p(b) = 2$ $(\frac{-b_p}{p}) = 1$	$\neq 2$	$\mathfrak{p}_1^2 \mathfrak{p}_2^2$	$\mathfrak{p}_1 = (p, \frac{\alpha^2-pt\alpha}{p}),$ $\mathfrak{p}_2 = (p, \frac{\alpha^2+pt\alpha}{p})$ $v_p(t^2 + b_p) = v_p(a)$
A8	$v_p(a) \geq 3, v_p(b) = 2$ $(\frac{-b_p}{p}) = 1$	$\neq 2$	$\mathfrak{p}_1^2 \mathfrak{p}_2^2$	$\mathfrak{p}_1 = (p, \alpha + \frac{\alpha^2-pt\alpha}{p}),$ $\mathfrak{p}_2 = (p, \frac{\alpha^2+pt\alpha}{p} + \alpha)$ $v_p(t^2 + b_p) = v_p(a)$
A9	$v_p(a) \geq 1, v_p(b) = 0$	2		<i>Tab.A9</i>
A10	$v_p(a) \geq 1, v_p(b) = 0,$ $b \equiv 1 \pmod{3}$	3	$\mathfrak{p}_1 \mathfrak{p}_2$	$\mathfrak{p}_1 = (3, \alpha^2 - \alpha - 1),$ $\mathfrak{p}_2 = (3, \alpha^2 + \alpha - 1)$
A11	$v_p(a) \geq 1, v_p(b) = 0$ $b \equiv -1 \pmod{3}$	3	$\mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3$	$\mathfrak{p}_1 = (3, \alpha^2 + 1),$ $\mathfrak{p}_2 = (3, \alpha - 1),$ $\mathfrak{p}_3 = (3, \alpha + 1)$
A12	$v_p(a) \geq 1, v_p(b) = 0$	≥ 5		<i>Tab.A12</i>
A13	$v_p(a) = 0, v_p(b) \geq 1$	2	$\mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3$	$\mathfrak{p}_1 = (2, \alpha),$ $\mathfrak{p}_2 = (2, 1 + \alpha)$ $\mathfrak{p}_3 = (2, 1 + \alpha + \alpha^2)$
A14	$v_p(a) = 0, v_p(b) \geq 1$	3		<i>Tab.A14</i>
A15	$v_p(a) = 0, v_p(b) \geq 1,$ $-a \notin \mathbb{F}_p^3$	≥ 5	$\mathfrak{p}_1 \mathfrak{p}_2$	$\mathfrak{p}_1 = (p, \alpha),$ $\mathfrak{p}_2 = (p, a + \alpha^3)$
A16	$v_p(a) = 0, v_p(b) \geq 1$ $-a \in \mathbb{F}_p^3, (\frac{-3}{p}) = -1$	≥ 5	$\mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3$	$\mathfrak{p}_1 = (p, \alpha),$ $\mathfrak{p}_2 = (p, -u + \alpha)$ $\mathfrak{p}_3 = (p, u^2 + u\alpha + \alpha^2)$ $u^3 \equiv -a \pmod{p}$
A17	$v_p(a) = 0, v_p(b) \geq 1$ $-a \in \mathbb{F}_p^3, (\frac{-3}{p}) = 1$	≥ 5	$\mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \mathfrak{p}_4$	$\mathfrak{p}_1 = (p, \alpha),$ $\mathfrak{p}_2 = (p, -u + \alpha)$ $u^3 \equiv -a \pmod{p},$ $\mathfrak{p}_3 = (p, v_1 + \alpha)$ $\mathfrak{p}_4 = (p, -(u + v_1) + \alpha)$ $v^2 \equiv -3 \pmod{p},$ $2v_1 \equiv -u(1 + v) \pmod{p}$
A18	$v_p(ab) = 0$	2	$\mathfrak{p}$	$\mathfrak{p} = (2)$
A19	$v_p(ab) = 0$	≥ 5	<i>Tab.A19</i>	
A20	$v_p(ab) = 0, b \equiv -1 \pmod{3}$	3	$\mathfrak{p}$	$\mathfrak{p} = (3)$
A21	$v_p(ab) = 0,$ $a \equiv b \equiv 1 \pmod{3}$	3	$\mathfrak{p}_1 \mathfrak{p}_2$	$\mathfrak{p}_1 = (3, \alpha - 1),$ $\mathfrak{p}_2 = (3, \alpha^3 + \alpha^2 + \alpha - 1)$
A22	$v_p(ab) = 0,$ $a \equiv -1, b \equiv 1 \pmod{3}$	3	$\mathfrak{p}_1 \mathfrak{p}_2$	$\mathfrak{p}_1 = (3, \alpha - 1),$ $\mathfrak{p}_2 = (3, \alpha^3 - \alpha^2 + \alpha + 1)$

Table A5 : $v_2(b) = 2$ and $v_2(a) \geq 2$.

Table A5				
Case	conditions	$\phi_2(X)$	$2\mathbb{Z}_K$	Generators
A5.1	$v_2(b) = 2, v_2(a) = 2$	$X^2 + 2$	$\mathfrak{p}^4$	$\mathfrak{p} = (2, \frac{\phi_2(\alpha)}{2})$
A5.2	$b \equiv 12 \pmod{16}, v_2(a) = 3$	$X^2 + 2$	$\mathfrak{p}^4$	$\mathfrak{p} = (2, \alpha \frac{\phi_2(\alpha)}{4})$
A5.3	$b \equiv 4 \pmod{16}, v_2(a) = 3$	$X^2 + 2X + 2$	$\mathfrak{p}^4$	$\mathfrak{p} = (2, \alpha \frac{\phi_2(\alpha)}{4})$
A5.4	$b \equiv 4 \pmod{32}, v_2(a) = 4$	$X^2 + 2X + 2$	$\mathfrak{p}^4$	$\mathfrak{p} = (2, \frac{\phi_2(\alpha)}{4})$
A5.5	$b \equiv 20 \pmod{64}, v_2(a) = 4$	$X^2 + 2X - 2$	$\mathfrak{p}^2$	$\mathfrak{p} = (2, \alpha)$
A5.6	$b \equiv 52 \pmod{64},$ $a \equiv 16 \pmod{64}$	$X^2 + 2X - 2$	$\mathfrak{p}_1^2 \mathfrak{p}_2^2$	$\mathfrak{p}_1 = (2, \alpha + \alpha \frac{\phi_2(\alpha)+8-4\alpha}{8}),$ $\mathfrak{p}_2 = (2, \alpha + \alpha \frac{\phi_2(\alpha)}{8})$
A5.7	$b \equiv 52 \pmod{64},$ $a \equiv 48 \pmod{64}$	$X^2 + 2X - 2$	$\mathfrak{p}_1^2 \mathfrak{p}_2^2$	$\mathfrak{p}_1 = (2, \alpha \frac{\phi_2(\alpha)+8-4\alpha}{8}),$ $\mathfrak{p}_2 = (2, \alpha \frac{\phi_2(\alpha)}{8})$
A5.8	$b \equiv 12 \pmod{32}, v_2(a) \geq 4$	$X^2 + 2$	$\mathfrak{p}^2$	$\mathfrak{p} = (2, \alpha)$
A5.9	$b \equiv 28 \pmod{32}, v_2(a) \geq 4$	$X^2 + 2$	$\mathfrak{p}_1^2 \mathfrak{p}_2^2$	$\mathfrak{p}_1 = (2, \alpha \frac{\phi_2(\alpha)}{4} + \frac{\phi_2(\alpha)-4}{4}),$ $\mathfrak{p}_2 = (2, \frac{\phi_2(\alpha)}{4} + \alpha \frac{\phi_2(\alpha)-4}{4})$
A5.10	$b \equiv 4 \pmod{64}, v_2(a) = 5$	$X^2 + 2X + 2$	$\mathfrak{p}_1^2 \mathfrak{p}_2^2$	$\mathfrak{p}_1 = (2, \alpha + \alpha \frac{\phi_2(\alpha)-4\alpha}{8}),$ $\mathfrak{p}_2 = (2, \alpha \frac{\phi_2(\alpha)}{8})$
A5.11	$b \equiv 4 \pmod{64}, v_2(a) \geq 6$	$X^2 + 2X + 2$	$\mathfrak{p}_1^2 \mathfrak{p}_2^2$	$\mathfrak{p}_1 = (2, \alpha + \alpha \frac{\phi_2(\alpha)-4\alpha}{8}),$ $\mathfrak{p}_2 = (2, \alpha \frac{\phi_2(\alpha)}{8} + \alpha)$
A5.12	$b \equiv 36 \pmod{64}, v_2(a) \geq 5$	$X^2 + 2X + 2$	$\mathfrak{p}^2$	$\mathfrak{p} = (2, \alpha)$
A5.13	$b \equiv 20 \pmod{32}, v_2(a) \geq 5$	$X^2 + 2X - 2$	$\mathfrak{p}^4$	$\mathfrak{p} = (2, \frac{\phi_2(\alpha)}{4})$

Table A9 : $v_2(b) = 0, v_2(a) \geq 1$. We pose $A = 4 + a$, $B = 1 + a + b$ and $\theta = \alpha - 1$.

Table A9			
Case	Conditions	$2\mathbb{Z}_K$	Generators
A8.1	$v_2(B) = 1$	$\mathfrak{p}^4$	$\mathfrak{p} = (2, \theta)$
A9.2	$v_2(B) = 2, a \equiv 0 \pmod{4}$	$\mathfrak{p}^2$	$\mathfrak{p} = (2, \theta)$
A9.3	$v_2(B) \geq 2, a \equiv 2 \pmod{4}$	$\mathfrak{p}_1^3 \mathfrak{p}_2$	$\mathfrak{p}_1 = (2, \theta + \frac{\theta^3+4\theta^2+6\theta+A}{2}),$ $\mathfrak{p}_2 = (2, \frac{\theta^3}{2})$
A9.4	$v_2(B) = 3, a \equiv 0 \pmod{8}$	$\mathfrak{p}_1^2 \mathfrak{p}_2$	$\mathfrak{p}_1 = (2, \frac{\theta^2+4\theta+6}{2}),$ $\mathfrak{p}_2 = (2, \frac{\theta^2}{2})$
A9.5	$v_2(B) \geq 4, a \equiv 0 \pmod{8}$	$\mathfrak{p}_1^2 \mathfrak{p}_2 \mathfrak{p}_3$	$\mathfrak{p}_1 = (2, \frac{\theta^2+4\theta+6}{2}),$ $\mathfrak{p}_2 = (2, \frac{\theta^2}{2} + \frac{\theta^3+4\theta^2+6\theta+A}{4}),$ $\mathfrak{p}_3 = (2, \frac{\theta^2}{2} + \frac{\theta^3+4\theta^2+6\theta}{4})$
A9.6	$v_2(B) \geq 4, a \equiv 4 \pmod{8}$		Tab.A9.6

Table A9.6 : $b \equiv 3 \pmod{8}$ and $v_2(a) = 2$. We pose $t \in \mathbb{Z}$ where $3at \equiv -4b \pmod{2\Delta}$.
 $k = \lfloor \frac{v_2(\Delta)-9}{2} \rfloor$, $\theta = \alpha - t$, $s = t + 2^k$, $\omega = \alpha - s$, $A_t = 4t^3 + a$ and $A_s = 4s^3 + a$.

Table A9.6					
Case	Conditions	$2\mathbb{Z}_K$	β_3	β_2	β_1
A9.6.1	$v_2(\Delta) = 2k + 10$	$\mathfrak{p}_1^2 \mathfrak{p}_2^2$		$\frac{\theta^2}{2} + \frac{\theta^3 + 4t\theta^2 + 6t^2\theta + A_t}{2^{k+1}}$	$\frac{\theta^2 + 6t\theta + 4t^2}{2} + \theta$
A9.6.2	$v_2(\Delta) = 2k + 9$ $b\Delta_2 \equiv 3 \pmod{4}$	$\mathfrak{p}_1^2 \mathfrak{p}_2^2$		$\frac{\omega^2}{2} + \frac{\omega^3 + 4s\omega^2 + 6s^2\omega + A_s}{2^{k+1}}$	$\frac{\omega^2 + 6t\omega + 4t^2}{2} + \omega$
A9.6.3	$v_2(\Delta) = 2k + 9$ $b\Delta_2 \equiv 1 \pmod{8}$	$\mathfrak{p}_1^2 \mathfrak{p}_2$		$\frac{\omega^2}{2}$	$\frac{\omega^2 + 6s\omega + 4s^2}{2} + \omega$
A9.6.4	$v_2(\Delta) = 2k + 9$ $b\Delta_2 \equiv 5 \pmod{8}$	$\mathfrak{p}_1^2 \mathfrak{p}_2 \mathfrak{p}_3$	$\frac{\omega^3 + 4s\omega^2 + 6s^2\omega}{2^{k+2}} + \frac{\omega^2}{2}$	$\frac{\omega^3 + 4s\omega^2 + 6s^2\omega + A_s}{2^{k+2}} + \frac{\omega^2}{2}$	$\frac{\omega^2 + 4s\omega + 6s^2}{2} + \omega$

Table A14 : $v_3(b) \geq 1$ and $v_3(a) = 0$. We pose $A = a - 4a^3$, $B = a^4 - a^2 + b$ and $\theta = \alpha + a$.

Table A14				
Case	Conditions	$3\mathbb{Z}_K$	Generators	
A14.1	$v_3(B) = 1$	$\mathfrak{p}_1 \mathfrak{p}_2^3$	$\mathfrak{p}_1 = (3, \alpha)$, $\mathfrak{p}_2 = (3, \theta)$	
A13.2	$v_3(A) = 1$ $v_3(B) = 2$	$\mathfrak{p}_1 \mathfrak{p}_2^2 \mathfrak{p}_3$	$\mathfrak{p}_1 = (3, \alpha)$, $\mathfrak{p}_2 = (3, \frac{\theta^3 - 4a\theta^2 + 6a^2\theta + A}{3} + \theta^2)$ $\mathfrak{p}_3 = (3, \frac{\theta^3 - 4a\theta^2 + 6a^2\theta}{3} + \theta)$	
A14.3	$v_3(A) = 1$ $v_3(B) \geq 3$	$\mathfrak{p}_1 \mathfrak{p}_2^2 \mathfrak{p}_3$	$\mathfrak{p}_1 = (3, \alpha)$, $\mathfrak{p}_2 = (3, \frac{\theta^3 - 4a\theta^2 + 6a^2\theta + A}{3} + \theta)$ $\mathfrak{p}_3 = (3, \frac{\theta^3 - 4a\theta^2 + 6a^2\theta}{3} + \theta)$	
A14.4	$b \equiv 6 \pmod{9}$, $a^2 \not\equiv 4 \pmod{9}$	$\mathfrak{p}_1 \mathfrak{p}_2^3$	$\mathfrak{p}_1 = (3, \alpha)$, $\mathfrak{p}_2 = (3, \theta)$	
A14.5	$b \equiv 6 \pmod{9}$, $a^2 \equiv 4 \pmod{9}$ $v_3(B) = 2$	$\mathfrak{p}_1 \mathfrak{p}_2^2 \mathfrak{p}_3$	$\mathfrak{p}_1 = (3, \alpha)$, $\mathfrak{p}_2 = (3, \frac{\theta^3 - 4a\theta^2 + 6a^2\theta + A}{3} + \theta^2)$ $\mathfrak{p}_3 = (3, \frac{\theta^3 - 4a\theta^2 + 6a^2\theta}{3} + \theta)$	
A14.6	$b \equiv 6 \pmod{9}$, $a^2 \equiv 4 \pmod{9}$ $v_3(B) \geq 3$	$\mathfrak{p}_1 \mathfrak{p}_2^2 \mathfrak{p}_3$	$\mathfrak{p}_1 = (3, \alpha)$, $\mathfrak{p}_2 = (3, \frac{\theta^3 - 4a\theta^2 + 6a^2\theta + A}{3} + \theta)$ $\mathfrak{p}_3 = (3, \frac{\theta^3 - 4a\theta^2 + 6a^2\theta}{3} + \theta)$	
A14.7	$a^2 \not\equiv 7 \pmod{9}$, $b \equiv 3 \pmod{9}$	$\mathfrak{p}_1 \mathfrak{p}_2^3$	$\mathfrak{p}_1 = (3, \alpha)$, $\mathfrak{p}_2 = (3, \theta)$	
A14.8	$b \equiv 3 \pmod{9}$, $a^2 \equiv 7 \pmod{9}$ $v_3(B) = 2$	$\mathfrak{p}_1 \mathfrak{p}_2^3$	$\mathfrak{p}_1 = (3, \alpha)$, $\mathfrak{p}_2 = (3, \frac{\theta^3 - 4a\theta^2}{3})$	
A14.9	$b \equiv 3 \pmod{9}$, $a^2 \equiv 7 \pmod{9}$ $v_3(B) \geq 3$		Tab.A14.9	

Table A14.9: $b \equiv 3 \pmod{9}$, $a^2 \equiv 7 \pmod{9}$ and $v_3(b + a^4 - a^2) \geq 3$. We $s \in \mathbb{Z}$ such that $as \equiv -4b_3 \pmod{3\Delta}$, and let $\theta = \alpha - s$, $A = 4s^3 + a$ and $B = s^4 + as + b$.

Table A14.9			
Case	Conditions	$3\mathbb{Z}_K$	Generators
A14.9.1	$v_3(\Delta) = 6$, $B_3 \equiv 1 \pmod{3}$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_1 = (3, \alpha)$, $\mathfrak{p}_2 = (3, \theta)$
A14.9.2	$v_3(\Delta) = 6$, $B_3 \equiv -1 \pmod{3}$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1 = (3, \alpha)$, $\mathfrak{p}_2 = (3, \frac{(\theta+3s)(\theta+4s)}{3})$, $\mathfrak{p}_3 = (3, \frac{(s\theta^2+3\theta-9s)(s\theta+4s-3)}{9})$
A14.9.3	$v_3(\Delta) = 2r \geq 8$, $B_3 \equiv 1 \pmod{3}$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	$\mathfrak{p}_1 = (3, \alpha)$, $\mathfrak{p}_2 = (3, \frac{\theta^2+4s\theta}{3} + \frac{(\theta^2+4s\theta+6s^2)(\theta+3^{r-2})}{3^{r-1}})$, $\mathfrak{p}_3 = (3, \theta + \frac{\theta^2+4s\theta+6s^2}{3})$, $\mathfrak{p}_4 = (3, \frac{\theta^2+4s\theta}{3} + \frac{(\theta^2+4s\theta+6s^2)(\theta+3^{r-2})}{3^{r-1}})$
A14.9.3	$v_3(\Delta) = 2r \geq 8$, $B_3 \equiv -1 \pmod{3}$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_1 = (3, \alpha)$, $\mathfrak{p}_2 = (3, \theta + \frac{\theta^2+4s\theta+6s^2}{3})$, $\mathfrak{p}_3 = (3, \frac{\theta^2+4s\theta}{3})$
A14.9.3	$v_3(\Delta) = 2r + 1 \geq 7$, $B_3 \equiv 1 \pmod{3}$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$	$\mathfrak{p}_1 = (3, \alpha)$, $\mathfrak{p}_2 = (3, \frac{\theta^2+4s\theta}{3})$, $\mathfrak{p}_3 = (3, \frac{\theta^2+4s\theta}{3} + \frac{\theta^2+4s\theta+6s^2}{3^{r-1}})$

Table A18: $p \geq 5$, $v_p(ab) = 0$. We $pases \in \mathbb{Z}$ such that $3as + 4b \equiv 0 \pmod{p\Delta}$. Let $\theta = \alpha - s$, $A = 4s^3 + a$ and $B = s^4 + as + b$.

Conditions	$p\mathbb{Z}_K$	with generators
$v_p(\Delta) = 0$	analogous to $F(X)$	
$v_p(\Delta) = 1$ $(\frac{-2}{p}) = -1$	$\mathfrak{p}_1\mathfrak{p}_2^2$	$\mathfrak{p}_2 = (p, \theta)$, $\mathfrak{p}_1 = (p, \theta^2 + 4s\theta + 6s^2)$
$v_p(\Delta) = 1$ $(\frac{-2}{p}) = 1$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$	$\mathfrak{p}_3 = (p, \theta)$, $\mathfrak{p}_2 = (p, \theta + s(2 - u))$ $\mathfrak{p}_2 = (p, \theta + s(2 + u))$, $u^2 \equiv -2 \pmod{p}$
$v_p(\Delta) = 2r + 1$ $(\frac{-2}{p}) = -1$	$\mathfrak{p}_1\mathfrak{p}_2^2$	$\mathfrak{p}_2 = (p, \theta + \frac{\theta^3+4s\theta^2+6s^2\theta}{p^r})$, $\mathfrak{p}_1 = (p, \theta^2 + 4s\theta + 6s^2)$
$v_p(\Delta) = 2r + 1$ $(\frac{-2}{p}) = 1$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$	$\mathfrak{p}_3 = (p, \theta + \frac{\theta^3+4s\theta^2+6s^2\theta}{p^r})$, $\mathfrak{p}_2 = (p, \theta + s(2 - u))$ $\mathfrak{p}_2 = (p, \theta + s(2 + u))$, $u^2 \equiv -2 \pmod{p}$
$v_p(\Delta) = 2r$ $(\frac{-2}{p}) = -1$ $(\frac{-6B_p}{p}) = -1$	$\mathfrak{p}_1\mathfrak{p}_2$	$\mathfrak{p}_2 = (p, \theta)$, $\mathfrak{p}_1 = (p, \theta^2 + 4s\theta + 6s^2)$
$v_p(\Delta) = 2r$ $(\frac{-2}{p}) = 1$ $(\frac{-6B_p}{p}) = -1$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_3 = (p, \theta)$, $\mathfrak{p}_1 = (p, \theta + s(2 - u))$ $\mathfrak{p}_2 = (p, \theta + s(2 + u))$ $u^2 \equiv -2 \pmod{p}$
$v_p(\Delta) = 2r$ $(\frac{-2}{p}) = -1$ $(\frac{-6B_p}{p}) = 1$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$	$\mathfrak{p}_3 = (p, \theta + \frac{(\theta^2+4s\theta+6s^2)(\theta-p^r t)}{p^r})$, $\mathfrak{p}_1 = (p, \theta^2 + 4s\theta + 6s^2)$ $\mathfrak{p}_2 = (p, \theta + \frac{(\theta^2+4s\theta+6s^2)(\theta+p^r t)}{p^r})$ $6s^2 t^2 \equiv -B_p \pmod{p}$
$v_p(\Delta) = 2r$ $(\frac{-2}{p}) = 1$ $(\frac{-6B_p}{p}) = 1$	$\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$	$\mathfrak{p}_3 = (p, \theta + \frac{(\theta^2+4s\theta+6s^2)(\theta+p^r t)}{p^r})$, $\mathfrak{p}_1 = (p, \theta - s(2 - u))$ $\mathfrak{p}_2 = (p, \theta + s(2 + u))$, $\mathfrak{p}_4 = (p, \theta + \frac{(\theta^2+4s\theta+6s^2)(\theta-p^r t)}{p^r})$ $u^2 \equiv -2 \pmod{p}$, $6s^2 t^2 \equiv -B_p \pmod{p}$

Proof Theorem 3.6.

Notice that all cases, except $(p = 2, v_p(b) = 2 \text{ and } v_p(a) \geq 2)$, correspond to a situation where $F(X)$ is a p -regular polynomial. The case $p = 2, v_p(b) = 2$ and $v_p(a) \geq 2$ is handled in *Table A5* by using techniques of Newton polygons of second order.

First case: $v_p(a) \geq 1$ and $v_p(b) \geq 1$. Then $\bar{F}(X) \equiv X^4 \pmod{p}$. Let $N_X(F)$ be the X -Newton polygon of $F(X)$.

- (1) $v_p(a) \geq 3$ and $v_p(b) = 3$. Then $N_X(F) = S$ is only one side such that $F_S(Y)$ is of degree 1. Thus, $p\mathbb{Z}_K = \mathfrak{p}^4$, $v_{\mathfrak{p}}(\alpha) = 4 \times 3/4 = 3$, and $\mathfrak{p} = (p, \frac{\alpha^3}{p^2})$.
- (2) $v_p(a) = 2$ and $v_p(b) \geq 3$. Then $N_X(F) = S_1 + S_2$, where $F_{S_1}(Y)$ and $F_{S_2}(Y)$ are of degree 1. Thus, $p\mathbb{Z}_K = \mathfrak{p}_1^3 \mathfrak{p}_2$, $v_{\mathfrak{p}_1}(\alpha) = 2$ and $v_{\mathfrak{p}_2}(\alpha) = v_2(b) - 1$. So, $\mathfrak{p}_1 = (p, \frac{\alpha^2}{p} + \frac{\alpha^3+a}{p})$ and $\mathfrak{p}_2 = (p, \frac{\alpha^3}{p})$.
- (3) $v_p(a) = 1$ and $v_p(b) \geq 2$. Then $N_X(F) = S_1 + S_2$, where $F_{S_1}(Y)$ and $F_{S_2}(Y)$ are of degree 1. Thus, $p\mathbb{Z}_K = \mathfrak{p}_1^3 \mathfrak{p}_2$, $v_{\mathfrak{p}_1}(\alpha) = 1$ and $v_{\mathfrak{p}_2}(\alpha) = v_2(b) - 1$. So, $\mathfrak{p}_2 = (p, \frac{\alpha^3}{p} + p)$ and if $v_p(b) = 2$, then $\mathfrak{p}_1 = (p, \frac{\alpha^3+a}{p})$. If $v_p(b) \geq 3$, then $\mathfrak{p}_1 = (p, \alpha + \frac{\alpha^3+a}{p})$.
- (4) $v_p(b) = 1$ and $v_p(a) \geq 1$. Then $N_X(F) = S$ is only one side such that $F_S(Y)$ is of degree 1, $p\mathbb{Z}_K = \mathfrak{p}^4$, and $\mathfrak{p} = (p, \alpha)$.
- (5) If $v_p(b) = 2$ and $v_p(a) \geq 2$, then $N_X(F) = S$ is only one side such that $F_S(y) = Y^2 + b_p$. If $p \neq 2$, then we have the following cases:
 - (a) If $(\frac{-b_p}{p}) = -1$, then $p\mathbb{Z}_K = \mathfrak{p}^2$ such that $v_{\mathfrak{p}}(\alpha) = 1$ and $\mathfrak{p} = (p, \alpha)$.
 - (b) If $(\frac{-b_p}{p}) = 1$, then let $t \in \mathbb{Z}$ such that $v_p(t^2 + b_p) \geq v_p(a)$. So, $F_S(Y) = (Y - t)(Y + t)$, $p\mathbb{Z}_K = \mathfrak{p}_1^2 \mathfrak{p}_2^2$ and for every i , $v_{\mathfrak{p}_i}(\alpha) = 1$. Consider $F(X) = \phi_2^2 - 2tp\phi_2 + aX + b + t^2p^2$ the ϕ_2 -adic development of $F(X)$, where $\phi_2 = X^2 + pt$ (resp. $\phi_2 = X^2 - pt$). We have then $v_{\mathfrak{p}_1}(\alpha^2 + pt) = 2v_p(a) - 1$ and $v_{\mathfrak{p}_2}(\alpha^2 - pt) = 2v_p(a) - 1$. Since $Y - t$ and $Y + t$ are coprime, $v_{\mathfrak{p}_1}(\alpha^2 - pt) = 2$ and $v_{\mathfrak{p}_2}(\alpha^2 + pt) = 2$. Thus, if $v_p(a) = 2$, then $\mathfrak{p}_1 = (p, \frac{\alpha^2 - pt}{p})$ and $\mathfrak{p}_2 = (p, \frac{\alpha^2 + pt}{p})$. Else, then $\mathfrak{p}_1 = (p, \alpha + \frac{\alpha^2 - pt}{p})$ and $\mathfrak{p}_2 = (p, \alpha + \frac{\alpha^2 + pt}{p})$.
- (6) For $p = 2, v_2(b) = 2$ and $v_2(a) \geq 2$. In that case, using techniques of Newton polygons of second order, for every subcase, a monic polynomial $\phi_2 \in \mathbb{Z}[X]$ such that $t = (X, 1/2, \phi_2)$ is $F(X)$ -complete is given (see [4, Def 3.9, p 38]). Let $F(X) = \phi_2^2 + U(X)\phi_2 + V(X)$ be the ϕ_2 -adic development and N_2 the ϕ_2 -Newton polygon of second order of $F(X)$. From [4, Cor 3.8, p 38], if N_2 is one side, then $2\mathbb{Z}_K = \mathfrak{p}^e$, where $e = 2e_2$ and e_2 is the ramification index of N_2 . If N_2 is two sides, then for every side, $e_2 = 1$ and $2\mathbb{Z}_K = \mathfrak{p}_1^2 \mathfrak{p}_2^2$.
 - (a) If $v_2(a) = 2$ or $v_2(a) \geq 3$ and $b \equiv 12 \pmod{16}$, then for $\phi_2 = X^2 + 2$, $t = (X, 1/2, \phi_2)$ is $F(X)$ -complete, $U(X) = -4$, and $V(X) = aX + b + 4$. If $v_2(a) = 2$, then N_2 is one side with ramification index $e_2 = 2$. Thus, $2\mathbb{Z}_K = \mathfrak{p}^4$, $v_{\mathfrak{p}}(\phi_2(\alpha)) = 5$ and $\mathfrak{p} = (2, \frac{\phi_2(\alpha)}{2})$. If $v_2(a) = 3$ and $b \equiv 12 \pmod{16}$, then N_2 is one side with ramification index $e_2 = 2$, $2\mathbb{Z}_K = \mathfrak{p}^4$, $v_{\mathfrak{p}}(\phi_2(\alpha)) = 7$, and $\mathfrak{p} = (2, \alpha \frac{\phi_2(\alpha)}{4})$. If $v_2(a) \geq 4$ and $b \equiv 12 \pmod{32}$, then N_2 is one side with ramification index $e_2 = 1$, $2\mathbb{Z}_K = \mathfrak{p}^2$ and $\mathfrak{p} = (2, \alpha)$. If $v_2(a) \geq 4$ and $b \equiv 28 \pmod{32}$, then N_2 is two sides, $2\mathbb{Z}_K = \mathfrak{p}_1^2 \mathfrak{p}_2^2$ such that $v_{\mathfrak{p}_1}(\phi_2(\alpha)) = 4$ and $v_{\mathfrak{p}_2}(\phi_2(\alpha)) = v_{\mathfrak{p}_2}(V(\alpha)) - 4 \geq 5$. Therefore,

- $v_{\mathbf{p}_1}(\frac{\phi_2(\alpha)}{4}) = 0$, $v_{\mathbf{p}_2}(\frac{\phi_2(\alpha)}{4}) \geq 1$, $v_{\mathbf{p}_1}(\frac{\phi_2(\alpha)-4}{4}) \geq 1$, $v_{\mathbf{p}_2}(\frac{\phi_2(\alpha)-4}{4}) = 0$ and for every $i = 1, 2$, $v_{\mathbf{p}_i}(\alpha) = 1$. Thus, if $v_2(a) = 4$, then $\mathbf{p}_1 = (2, \frac{\phi_2(\alpha)-4}{4})$ and $\mathbf{p}_2 = (2, \frac{\phi_2(\alpha)}{4})$. If $v_2(a) \geq 5$, then $\mathbf{p}_1 = (2, \alpha + \frac{\phi_2(\alpha)-4}{4})$ and $\mathbf{p}_2 = (2, \alpha + \frac{\phi_2(\alpha)}{4})$.
- (b) If $v_2(a) = 3$ and $b \equiv 4 \pmod{16}$ or $(v_2(a) \geq 4$ and $b \equiv 4 \pmod{32})$, then for $\phi_2 = X^2 + 2X + 2$, $t = (X, 1/2, \phi_2)$ is $F(X)$ -complete, $U(X) = -4X$, and $V(X) = aX + b - 4$. It follows that:
 If $v_2(a) = 3$ and $b \equiv 4 \pmod{16}$, then N_2 is only one side and $2\mathbb{Z}_K = \mathbf{p}^4$ such that $v_{\mathbf{p}}(\phi_2(\alpha)) = 7$, $v_{\mathbf{p}}(\alpha) = 2$ and $\mathbf{p} = (2, \alpha \frac{\phi_2(\alpha)}{4})$.
 If $v_2(a) \geq 4$ and $b \equiv 4 \pmod{32}$, then N_2 is only one side and $2\mathbb{Z}_K = \mathbf{p}^4$ such that $v_{\mathbf{p}}(\phi_2(\alpha)) = 9$ and $\mathbf{p} = (2, \frac{\phi_2(\alpha)}{4})$.
 If $v_2(a) \geq 5$ and $b \equiv 4 \pmod{64}$, then N_2 is two sides, $2\mathbb{Z}_K = \mathbf{p}_1^2 \mathbf{p}_2^2$ such that $v_{\mathbf{p}_1}(\phi_2(\alpha)) = 5$ and $v_{\mathbf{p}_2}(\phi_2(\alpha)) = v_{\mathbf{p}_2}(V(\alpha)) - 5 \geq 6$. Hence $v_{\mathbf{p}_2}(\alpha \frac{\phi_2(\alpha)-4\alpha}{8}) = 0$, $v_{\mathbf{p}_1}(\alpha \frac{\phi_2(\alpha)-4\alpha}{8}) \geq 2$, $v_{\mathbf{p}_1}(\alpha \frac{\phi_2(\alpha)}{8}) = 0$, $v_{\mathbf{p}_2}(\alpha \frac{\phi_2(\alpha)}{8}) \geq 1$, and for every $i = 1, 2$, $v_{\mathbf{p}_i}(\alpha) = 1$. So, $\mathbf{p}_1 = (2, \alpha + \frac{\phi_2(\alpha)-4\alpha}{8})$ and if $v_2(a) = 5$, then $\mathbf{p}_2 = (2, \frac{\alpha \phi_2(\alpha)}{8})$. If $v_2(a) \geq 6$, then $\mathbf{p}_2 = (2, \alpha + \frac{\alpha \phi_2(\alpha)}{8})$.
- (c) If $v_2(a) \geq 4$ and $b \equiv 20 \pmod{32}$, then for $\phi_2 = X^2 + 2X - 2$, $t = (X, 1/2, \phi_2)$ is $F(X)$ -complete, $U(X) = -4X + 8$ and $V(X) = (a - 16)X + b + 12$. It follows that:
 If $v_2(a) \geq 5$, then N_2 is only one side, $2\mathbb{Z}_K = \mathbf{p}^4$, $v_{\mathbf{p}}(\phi_2(\alpha)) = 9$, and $\mathbf{p} = (2, \frac{\phi_2(\alpha)}{4})$.
 If $v_2(a) = 4$ and $b \equiv 20 \pmod{64}$, then N_2 is only one side $2\mathbb{Z}_K = \mathbf{p}^2$ and $\mathbf{p} = (2, \alpha)$.
 If $v_2(a) = 4$ and $b \equiv 52 \pmod{64}$, then N_2 is two sides, $2\mathbb{Z}_K = \mathbf{p}_1^2 \mathbf{p}_2^2$ such that $v_{\mathbf{p}_1}(\phi_2(\alpha)) = 5$ and $v_{\mathbf{p}_2}(\phi_2(\alpha)) = v_{\mathbf{p}_2}(V(\alpha)) - 5 \geq 6$. $v_{\mathbf{p}_1}(\alpha \frac{\phi_2(\alpha)}{8}) = 0$, $v_{\mathbf{p}_2}(\alpha \frac{\phi_2(\alpha)}{8}) \geq 1$, $v_{\mathbf{p}_2}(\alpha \frac{\phi_2(\alpha)+8-4\alpha}{8}) = 0$, $v_{\mathbf{p}_1}(\alpha \frac{\phi_2(\alpha)+8-4\alpha}{8}) \geq 2$, and for every $i = 1, 2$, $v_{\mathbf{p}_i}(\alpha) = 1$.

Second case: $v_p(a) = 0$ and $v_p(b) \geq 1$.

If $p \neq 3$, then $v_p(\text{ind}(F)) = 0$ and $p\mathbb{Z}_K$ is analogous to $\bar{F}(X) \pmod{p}$.

For $p = 3$, let $P(X) = F(X - a) = X^4 - 4aX^3 + 6a^2X^2 + AX + B$ and $\theta = \alpha + a$, where $A = -a(4a^2 - 1)$ and $B = (a^4 - a^2 + b)$.

- (1) If $v_3(B) = 1$, then $v_3(\text{ind}(F)) = 0$ and $3\mathbb{Z}_K = (3, \alpha)(3, \theta)^3$.
- (2) If $v_3(B) = 2$ and $v_3(A) \geq 2$, then $3\mathbb{Z}_K = \mathbf{p}_1 \mathbf{p}_2^3$, where $\mathbf{p}_1 = (3, \alpha)$ and $\mathbf{p}_2 = (3, \frac{\theta^3 - 4a\theta^2 + 6a^2\theta}{3})$.
- (3) If $v_3(A) = 1$ and $v_3(B) \geq 2$, then $3\mathbb{Z}_K = \mathbf{p}_1 \mathbf{p}_2^2 \mathbf{p}_3$, where $\mathbf{p}_1(3, \alpha)$, $v_{\mathbf{p}_1}(\theta) = 0$, $v_{\mathbf{p}_2}(\theta) = 1$, $v_{\mathbf{p}_3}(\theta) = v_3(B) - 1$. Thus, $v_{\mathbf{p}_3}(\frac{\theta^3 - 4a\theta^2 + 6a^2\theta}{3}) \geq 1$, $v_{\mathbf{p}_2}(\frac{\theta^3 - 4a\theta^2 + 6a^2\theta}{3}) = 0$ and $\mathbf{p}_3 = (3, \frac{\theta^3 - 4a\theta^2 + 6a^2\theta}{3})$. For $\mathbf{p}_2$, we have $v_{\mathbf{p}_3}(\frac{\theta^3 - 4a\theta^2 + 6a^2\theta + A}{3}) = 0$ and $v_{\mathbf{p}_2}(\frac{\theta^3 - 4a\theta^2 + 6a^2\theta + A}{3}) = 2v_3(B) - 3 \geq 1$. Therefore, If $v_3(B) = 2$, then $\mathbf{p}_2 = (3, \theta^2 + \frac{\theta^3 - 4a\theta^2 + 6a^2\theta + A}{3})$. Else, then $\mathbf{p}_2 = (3, \theta + \frac{\theta^3 - 4a\theta^2 + 6a^2\theta + A}{3})$.
- (4) If $v_3(A) \geq 2$ and $v_3(B) \geq 3$, i.e., $b \equiv 3 \pmod{9}$, $a^2 \equiv 7 \pmod{9}$ and $v_3(B) \geq 3$, then $v_3(\Delta) \geq 6$. Let $s \in \mathbb{Z}$ such that $as \equiv -4b_3 \pmod{3\Delta}$, $P(X) = F(X + s) = X^4 + 4sX^3 + 6s^2X^2 + AX + B$ and $\theta = \alpha - s$, where $A = 4s^3 + a$ and $B = s^4 + as + b$. In this case, we have $v_3(A) = v_3(B) = v_3(\Delta) - 3 \geq 3$. So,
 - (a) If $v_3(\Delta) = 6$, then $N_X(P) = S_0 + S_1$ such that $P_{S_1}(Y) = sY^3 - Y^2 + B_3$. Hence if $B_3 \equiv 1 \pmod{3}$, then $P_{S_1}(Y)$ is irreducible and $3\mathbb{Z}_K = \mathbf{p}_1 \mathbf{p}_2$,

where $\mathfrak{p}_1 = (3, \alpha)$ and $\mathfrak{p}_2 = (3, \theta)$.

If $B_3 \equiv -1 \pmod{3}$, then $P_{S_1}(Y) = (Y + s)(sY^2 + Y - s) = \psi_1(Y)\psi_2(Y)$ and $3\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, where $\mathfrak{p}_1 = (3, \alpha)$ and for every $i = 2, 3$, $v_{\mathfrak{p}_i}(\theta) = 1$. Form (3) of the Proposition 3.3, $v_{\mathfrak{p}_2}(\theta + 3s) \geq 2$ and $v_{\mathfrak{p}_3}(s\theta^2 + 3\theta - 3^2s) \geq 3$. As $(Y + s)$ and $sY^2 + Y - s$ are coprime, $v_{\mathfrak{p}_3}(\theta + 3s) = 1$ and $v_{\mathfrak{p}_2}(s\theta^2 + 3\theta - 3^2s) = 2$. Since $v_{\mathfrak{p}_1}(\theta + 4s) = 1$ and $X^3 + 4sX^2 + 6s^2X \equiv (sX^2 + 3X - 9s)(s^{-1}X + 4 - 3s^{-2} \pmod{9})$, we have $\mathfrak{p}_2 = (3, \frac{(\theta+4s)(\theta+3s)}{3})$ and $\mathfrak{p}_3 = (3, \theta + \frac{(\theta+4s-3s^{-1})(s\theta^2+3\theta-3^2s)}{9})$.

- (b) If $v_3(\Delta) = 2r \geq 8$, then $N_X(P) = S_0 + S_1 + S_2$ such that for $i = 0, 1$, $P_{S_i}(Y)$ is of degree 1 and $P_{S_2}(Y) = -Y^2 + B_3$. Thus, if $B_3 \equiv -1 \pmod{3}$, then $P_{S_2}(Y)$ is irreducible and $3\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, where $\mathfrak{p}_1 = (3, \alpha)$, $\mathfrak{p}_2 = (3, \theta + \frac{\theta^2+4s\theta+6s^2}{3})$ and $\mathfrak{p}_3 = (3, \frac{\theta^2+4s\theta}{3})$.

If $B_3 \equiv 1 \pmod{3}$, then $3\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$, where $\mathfrak{p}_1 = (3, \alpha)$, $\mathfrak{p}_2 = (3, \theta + \frac{\theta^2+4s\theta+6s^2}{3})$. For $\mathfrak{p}_3$ and $\mathfrak{p}_4$, since $P_{S_2}(Y) = (1 - Y)(1 + Y)$, and $\lambda_2 = r - 2$, from (3) of the Proposition 3.3, we have $v_{\mathfrak{p}_3}(\theta + 3^{r-2}) \geq r - 1$, $v_{\mathfrak{p}_4}(\theta - 3^{r-2}) \geq r - 1$, and $v_{\mathfrak{p}_3}(\theta - 3^{r-2}) = v_{\mathfrak{p}_4}(\theta + 3^{r-2}) = r - 2$. Hence $\mathfrak{p}_3 = (3, \frac{\theta^2+4s\theta}{3} + \frac{(\theta^2+4s\theta+6s^2)(\theta+3^{r-2})}{3^{r-1}})$ and $\mathfrak{p}_4 = (3, \frac{\theta^2+4s\theta}{3} + \frac{(\theta^2+4s\theta+6s^2)(\theta-3^{r-2})}{3^{r-1}})$.

- (c) If $v_3(\Delta) = 2r + 1 \geq 7$, then $N_X(P) = S_0 + S_1 + S_2$ such that for $i = 0, 1, 2$, $P_{S_i}(Y)$ is of degree 1 and then $3\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$, where $\mathfrak{p}_1 = (3, \alpha)$, $\mathfrak{p}_2 = (3, \theta + \frac{\theta^2+4s\theta+6s^2}{3})$ and $\mathfrak{p}_3 = (3, \frac{\theta^2+4s\theta}{3} + \frac{\theta^3+4s\theta^2+6s^2\theta}{3^{r-1}})$.

Third case: $sv_p(a) \geq 1$ and $v_p(b) = 0$.

If $p \neq 2$, then $v_p(\text{ind}(F)) = 0$ and $p\mathbb{Z}_K$ is analogous to $\bar{F}(X) \pmod{p}$. For $p = 2$, let $P(X) = F(X + 1) = X^4 + 4x^3 + 6X^2 + AX + B$ and $\theta = \alpha - 1$, where $A = 4 + a$ and $B = 1 + a + b$.

- (1) If $v_2(B) = 1$, then $2\mathbb{Z}_K = \mathfrak{p}^4$ and $\mathfrak{p} = (2, \theta)$.
- (2) If $v_2(a) = 1$ and $v_2(B) \geq 2$, then $v_2(A) = 1$, $2\mathbb{Z}_K = \mathfrak{p}_1^3\mathfrak{p}_2$, where $v_{\mathfrak{p}_1}(\theta) = 1$ and $v_{\mathfrak{p}_2}(\theta) = v_2(B) - 1$. Hence, $\mathfrak{p}_2 = (2, \frac{\theta^2}{2})$ and $\mathfrak{p}_1 = (2, \theta + \frac{\theta^3+4\theta^2+6\theta+A}{2})$.
- (3) If $v_2(B) = 2$ and $v_2(a) \geq 2$, then $N_X(P) = S$ is only one side such that $P_S(Y) = Y^2 + Y + 1$. Thus, $2\mathbb{Z}_K = \mathfrak{p}^2$ and $\mathfrak{p} = (2, \theta)$.
- (4) If $v_2(a) \geq 3$ and $v_2(B) = 3$, then $N_X(P) = S_1 + S_2$ such that $P_{S_1}(Y) = Y + 1$ and $P_{S_2}(Y) = Y^2 + Y + 1$. So, $2\mathbb{Z}_K = \mathfrak{p}_1^2\mathfrak{p}_2$, where $v_{\mathfrak{p}_2}(\theta) = v_{\mathfrak{p}_1}(\theta) = 1$. Hence $\mathfrak{p}_1 = (2, \frac{\theta^2+4\theta+6}{2})$ and $\mathfrak{p}_2 = (2, \frac{\theta^2}{2})$.
- (5) If $v_2(a) \geq 3$ and $v_2(B) \geq 4$, then $N_X(P) = S_1 + S_2 + S_3$ and $2\mathbb{Z}_K = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$, where $v_{\mathfrak{p}_1}(\theta) = 1$, $v_{\mathfrak{p}_2}(\theta) = 1$ and $v_{\mathfrak{p}_3}(\theta) = v_2(B) - 2$. Thus, $\mathfrak{p}_1 = (2, \frac{\theta^2+4\theta+6}{2})$, $\mathfrak{p}_2 = (2, \frac{\theta^2}{2} + \frac{\theta^3+4\theta^2+6\theta+A}{4})$, and $\mathfrak{p}_3 = (2, \frac{\theta^2}{2} + \frac{\theta^3+4\theta^2+6\theta}{4})$.
- (6) If $v_2(a) = 2$ and $v_2(B) \geq 3$, then $v_2(\Delta) \geq 11$. Let $t \in \mathbb{Z}$ such that $3at \equiv -4b \pmod{2\Delta}$. Let $k = \lfloor \frac{v_2(\Delta)-9}{2} \rfloor$, $A_t = (4t^3 + a)$, $B_t = t^4 + at + b$, $\theta = \alpha - t$, $\omega = \alpha - t - 2^k$, and $P(X) = F(X + t) = X^4 + 4tX^3 + 6t^2X^2 + A_tX + B_t$. Since $(3a)^4B_t \equiv b\Delta \pmod{2\Delta}$ and $(3a)^3A_t \equiv -\Delta \pmod{2\Delta}$, we have $v_2(A_t) = v_2(\Delta) - 6$ and $v_2(B_t) = v_2(\Delta) - 8$. It follows that:
 - (a) If $v_2(\Delta) = 2k + 10$, then $N_X(P) = S_1 + S_2$ and for every $i := 1, 2$, $P_{S_i}(Y) = Y + 1$. So, $2\mathbb{Z}_K = \mathfrak{p}_1^2\mathfrak{p}_2^2$ such that $v_{\mathfrak{p}_1}(\theta) = 1$ and $v_{\mathfrak{p}_2}(\theta) = 2k + 1$. Thus, $v_{\mathfrak{p}_1}(\frac{\theta^2+4t\theta+6t^2}{2}) \geq 2$, $v_{\mathfrak{p}_2}(\frac{\theta^2+4t\theta+6t^2}{2}) = 0$, $v_{\mathfrak{p}_1}(\frac{\theta^2}{2}) = 0$, and $v_{\mathfrak{p}_2}(\frac{\theta^3+4t\theta^2+6t^2\theta+A_t}{2^{k+1}}) = 1$. Therefore, $\mathfrak{p}_1 = (2, \theta + \frac{\theta^2+4t\theta+6t^2}{2})$ and $\mathfrak{p}_2 = (2, \frac{\theta^2}{2} + \frac{\theta^3+4t\theta^2+6t^2\theta+A_t}{2^{k+1}})$.

- (b) If $v_2(\Delta) = 2k + 9$, then $N_X(P) = S_1 + S_2$, where $P_{S_1}(Y) = Y + 1$ and $P_{S_2}(Y) = Y^2 + 1$. Let $s = t + 2^k$ and consider $K(X) = F(X + s) = X^4 + 4sX^3 + 6s^2X^2 + A_sX + B_s$. Since $A_s \equiv A_t + 12t^22^k \pmod{2^{2k+3}}$ and $B_s \equiv 6t^22^{2k} + B_t \pmod{2^{3k+2}}$, $(3a)^4B_s \equiv (3a)^4.6t^22^{2k} + b\Delta \pmod{2\Delta}$, $v_2(A_s) = k + 2$ and $v_2(B_s) = 2k + 1 + v_2(3(3a_2)^4t^2 + b\Delta_2)$. It follows that: If $b\Delta_2 \equiv 3 \pmod{4}$, then $v_2(B_s) = 2k + 2$ and $2\mathbb{Z}_K = \mathfrak{p}_1^2\mathfrak{p}_2^2$ such that $v_{\mathfrak{p}_1}(\omega) = 1$ and $v_{\mathfrak{p}_2}(\omega) = 2k + 1$. Therefore, $\mathfrak{p}_2 = (2, \frac{\omega^2}{2} + \frac{\omega^3 + 4s\omega^2 + 6s^2\omega + A_s}{2^{k+1}})$ and $\mathfrak{p}_1 = (2, \omega + \frac{\omega^2 + 4s\omega + 6s^2}{2})$.
 If $b\Delta_2 \equiv 1 \pmod{8}$, then $v_2(B_s) = 2k + 3$, and $2\mathbb{Z}_K = \mathfrak{p}_1^2\mathfrak{p}_2$ such that $v_{\mathfrak{p}_1}(\omega) = 1$ and $v_{\mathfrak{p}_2}(\omega) = k + 1$. Hence, $\mathfrak{p}_2 = (2, \frac{\omega^2}{2})$ and $\mathfrak{p}_1 = (2, \omega + \frac{\omega^2 + 4s\omega + 6s^2}{2})$.
 If $b\Delta_2 \equiv 5 \pmod{8}$, then $v_2(B_s) \geq 2k + 4$, and $2\mathbb{Z}_K = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3$ such that $v_{\mathfrak{p}_1}(\omega) = 1$, $v_{\mathfrak{p}_2}(\omega) = k + 1$, and $v_{\mathfrak{p}_3}(\omega) = v_2(B_s) - (k + 2) \geq k + 2$. So, $\mathfrak{p}_1 = (2, \theta + \frac{\omega^2 + 4s\omega + 6s^2}{2})$, $\mathfrak{p}_2 = (2, \frac{\omega^2}{2} + \frac{\omega^3 + 4s\omega^2 + 6s^2\omega + A_s}{2^{k+2}})$, and $\mathfrak{p}_3 = (2, \frac{\omega^2}{2} + \frac{\omega^3 + 4s\omega^2 + 6s^2\omega}{2^{k+2}})$.

Fourth case: $v_p(ab) = 0$.

If $p \in \{2, 3\}$, then $v_p(\text{ind}(F)) = 0$ and $p\mathbb{Z}_K$ is analogous to $\bar{F}(X) \pmod{p}$. For $p \geq 5$, let $s \in \mathbb{Z}$ such that $3as + 4b \equiv 0 \pmod{p\Delta}$, $\theta = \alpha - s$, $A = 4s^3 + a$, $B = s^4 + as + b$ and $P(X) = F(X + s) = X^4 + 4sX^3 + 6s^2X^2 + AX + B$. Then $v_p(A) = v_p(B) = v_p(\Delta)$.

If $v_p(\Delta) = 0$, then $p\mathbb{Z}_K$ is analogous to $\bar{F}(X)$.

If $v_p(\Delta) \geq 1$, then $N_X(P) = S_0 + S_1$, where $P_{S_0}(Y) = Y^2 + 4sY + 6s^2$.

If $v_p(\Delta) = 1$ and $(\frac{-2}{p}) = 1$, then $P_{S_1}(Y) = 6s^2Y + B_p$ and $p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$, where $\mathfrak{p}_3 = (p, \theta)$, $\mathfrak{p}_2 = (p, \theta - v_1)$, $\mathfrak{p}_1 = (p, \theta - v_2)$, $v_1 = -s(2 + u)$, $v_2 = -s(2 - u)$ and $u^2 \equiv -2 \pmod{p}$.

If $v_p(\Delta) = 1$ and $(\frac{-2}{p}) = -1$, then $p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2^2$, where $\mathfrak{p}_2 = (p, \theta)$ and $\mathfrak{p}_1 = (p, \theta^2 + 4s\theta + 6s^2)$.

If $v_p(\Delta) \geq 2$, then we have the following cases:

- (1) If $v_p(\Delta) = 2r + 1$, then $P_{S_2}(Y)$ is of degree 1. So, if $(\frac{-2}{p}) = 1$, then $p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3^2$, where $\mathfrak{p}_3 = (p, \theta + \frac{\theta^3 + 4s\theta^2 + 6s^2\theta}{p^r})$, $\mathfrak{p}_2 = (p, \theta - v_1)$, $\mathfrak{p}_1 = (p, \theta - v_2)$, $v_1 = -s(2 + u)$, $v_2 = -s(2 - u)$ and $u^2 \equiv -2 \pmod{p}$. If $(\frac{-2}{p}) = -1$, then $p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2^2$, where $\mathfrak{p}_2 = (p, \theta + \frac{\theta^3 + 4s\theta^2 + 6s^2\theta}{p^r})$ and $\mathfrak{p}_1 = (p, \theta^2 + 4s\theta + 6s^2)$.
- (2) If $v_p(\Delta) = 2r$, then $P_{S_2}(Y) = 6s^2Y^2 + B_p$. Hence, if $(\frac{-2}{p}) = 1$ and $(\frac{-6B_p}{p}) = -1$, then $p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, where $\mathfrak{p}_3 = (p, \theta)$, $\mathfrak{p}_2 = (p, \theta - v_1)$, $\mathfrak{p}_1 = (p, \theta - v_2)$, $v_1 = -s(2 + u)$, $v_2 = -s(2 - u)$ and $u^2 \equiv -2 \pmod{p}$.
 If $(\frac{-2}{p}) = -1$ and $(\frac{-6B_p}{p}) = -1$, then $p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_2 = (p, \theta)$ and $\mathfrak{p}_1 = (p, \theta^2 + 4s\theta + 6s^2)$.
 If $(\frac{-2}{p}) = -1$ and $(\frac{-6B_p}{p}) = 1$, then $F_{S_2}(Y) = 6s^2(Y - t)(Y + t)$, where $6s^2t^2 \equiv -B_p \pmod{p}$. Thus, $p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, where $\mathfrak{p}_1 = (p, \theta^2 + 4s\theta + 6s^2)$, $\mathfrak{p}_2 = (p, \theta + \frac{(\theta^2 + 4s\theta + 6s^2)(\theta + p^r t)}{p^r})$, and $\mathfrak{p}_3 = (p, \theta + \frac{(\theta^2 + 4s\theta + 6s^2)(\theta - p^r t)}{p^r})$. If $(\frac{-2}{p}) = 1$ and $(\frac{-6B_p}{p}) = 1$, then $p\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$.

Examples 3.7. Let $f(X) = X^4 + aX + b \in \mathbb{Z}[X]$ be an irreducible polynomial, α a complex root of $f(X)$ and $K = \mathbb{Q}[\alpha]$.

- (1) $a = 2^{10}.5$ and $b = 2^9.3.5$. Let $\theta = \frac{\alpha}{4}$. Then θ is integral with minimal polynomial $F(X) = X^4 + 80X + 30$ and $K = \mathbb{Q}[\theta]$. Thus $2\mathbb{Z}_K = (2, \theta)^4$, $3\mathbb{Z}_K = (3, \theta)(3, \theta - 1)^3$, $5\mathbb{Z}_K = (5, \theta)^4$ and for every $p \notin \{2, 3, 5\}$, $p\mathbb{Z}_K$ is analogous to $\bar{F}(X)$.
- (2) $a = 48$ and $b = 188$. From *TableA5*, row A5.9, we have $2\mathbb{Z}_K = \mathfrak{p}_1^2 \mathfrak{p}_2^2$, where $\mathfrak{p}_1 = (2, \alpha \frac{\phi_2(\alpha)}{4} + \frac{\phi_2(\alpha)-4}{4})$, $\mathfrak{p}_2 = (2, \frac{\phi_2(\alpha)}{4} + \alpha \frac{\phi_2(\alpha)-4}{4})$, and $\phi_2(\alpha) = \alpha^2 + 2$.
- (3) $a = 144$ and $b = 36$. From *TableA5*, row A5.4, we have $2\mathbb{Z}_K = (2, \frac{\alpha^2+2\alpha+2}{4})^4$. Since $(\frac{-b_3}{3}) = -1$, from *TableA*, row A6 $3\mathbb{Z}_K = \mathfrak{p}^2$, where $\mathfrak{p} = (3, \alpha)$. Since $\Delta = -2^{14}.3^6.971$, for every $p \notin \{2, 3, 5\}$, $p\mathbb{Z}_K$ is analogous to $\bar{P}(X)$.
- (4) $a = 28, b = 189$ and $p = 2$. Let $F(X) = P(X+1) = X^4 + 4X^3 + 6X^2 + 32X + 218$. Since $B = 218 = 2.109$, we have $2\mathbb{Z}_K = (2, \alpha - 1)^4$.
- (5) $a = 22$ and $b = 66$. Then $\Delta = 2^4.3^5.11^3.13$. We have $2\mathbb{Z}_K = (2, \alpha)^4$, $11\mathbb{Z}_K = (11, \alpha)^4$, $13\mathbb{Z}_K = (13, \alpha)(13, \alpha^3 + 9)$ and for every prime $p \notin \{2, 3, 11, 13\}$, $p\mathbb{Z}_K$ is analogous to $\bar{P}(X)$. For $p = 3$, since $a^2 \equiv 7 \pmod{9}$, $b \equiv 3 \pmod{9}$ and $b + a^4 - a^2 = 9.25982$, from *TableA14*, row A14.8, $3\mathbb{Z}_K = \mathfrak{p}_1 \mathfrak{p}_2^3$, where $P_1 = (3, \alpha - 5a)$ and $P_2 = (3, \frac{\theta^3 - 4a\theta^2}{3})$.
- (6) $a = 3^6.5^5.139$ and $b = 2^2.3^5.5^5.139$. Let $\theta = \frac{\alpha}{15}$. Then θ is integral with minimal polynomial $F(X) = X^4 + AX + B$ and $K = \mathbb{Q}[\theta]$, where $A = 3^3.5^2.139$ and $B = 2^2.3.5.139$. Thus $2\mathbb{Z}_K = (2, \theta + 1)(2, \theta^2 + \theta + 1)(2, \theta)$, $3\mathbb{Z}_K = (3, \theta)^4$, $5\mathbb{Z}_K = (5, \theta)^4$, $139\mathbb{Z}_K = (139, \theta)^4$. Since $\Delta = 2092367789117959822875 = 202317851.7.3^3.5^3.139^3.163$, for every $p \notin \{3, 5, 139\}$, $p\mathbb{Z}_K$ is analogous to $\bar{F}(X)$.

4. ACKNOWLEDGMENT

The first author is very very grateful to Professor Enric Nart, who communicated him the Newton polygon techniques, when he was a post-doc at CRM of Barcelona

REFERENCES

- [1] Llorente and E. Nart, Effective determination of the decomposition of the rational primes in a cubic field, *Proceedings of the American Mathematical Society* vol(4)1983, 579-585
- [2] S. Alaca, B. K. Spearman, and K. S. Williams, Explicit decomposition of a rational prime in a cubic c field, *Far East J. Math. Sci.* vol(12)2004, 137-168
- [3] H. Cohen, *A course in computational algebraic number theory*, GTM 138, Springer-Verlag Berlin Heidelberg, New York, Paris, Tokyo, second correction (1995).
- [4] J. Guardia, J. Montes and E. Nart, Newton polygons of higher order in algebraic number theory, *Trans. of ams* vol(1)364 (2012), 361-416

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

E-mail address: ¹lhouelfaduil2@gmail.com

^{2,3}DEPARTMENT OF MATHEMATICS, PHYSICS AND COMPUTING, LSI, FPT, UNIVERSITY S.M. BEN ABDELLAH, TAZA, BOX 1223, , MOROCCO.

E-mail address: ²abdelhakim.chillali@usmba.ac.ma, ³ismail.akharraz@usmba.ac.ma