Czechoslovak Mathematical Journal, 71 (146) (2021), 529–543

PRIME IDEAL FACTORIZATION IN A NUMBER FIELD VIA NEWTON POLYGONS

Lhoussain El Fadil, Fès

Received December 2, 2019. Published online March 8, 2021.

Abstract. Let K be a number field defined by an irreducible polynomial $F(X) \in \mathbb{Z}[X]$ and $\mathbb{Z}_K$ its ring of integers. For every prime integer p, we give sufficient and necessary conditions on $F(X)$ that guarantee the existence of exactly r prime ideals of $\mathbb{Z}_K$ lying above p, where $\overline{F}(X)$ factors into powers of r monic irreducible polynomials in $\mathbb{F}_p[X]$. The given result presents a weaker condition than that given by S. K. Khanduja and M. Kumar (2010), which guarantees the existence of exactly r prime ideals of $\mathbb{Z}_K$ lying above p. We further specify for every prime ideal of $\mathbb{Z}_K$ lying above p, the ramification index, the residue degree, and a p-generator.

Keywords: prime factorization; valuation; φ-expansion; Newton polygon

MSC 2020: 11Y05, 11Y40, 11S05

1. Introduction

For every prime p of $\mathbb{Z}$ let ν_p be the p-adic valuation on $\mathbb{Q}$ and $\mathbb{F}_p$ the finite field $\mathbb{Z}/(p)$. The Gaussian valuation of $\mathbb{Q}_p[X]$ which extends ν_p is defined by $\nu_p\Big(\sum_{i=0}^{l} a_i X^{l-i}\Big) = \min\{\nu_p(a_i),\, 0 \leqslant i \leqslant l\}$. Let $K = \mathbb{Q}(\alpha)$ be a number field, where α is a complex root of a monic irreducible polynomial $F(X) \in \mathbb{Z}[X]$, $\mathbb{Z}_K$ its ring of integers, and $\operatorname{ind}(\alpha) = [\mathbb{Z}_K : \mathbb{Z}[\alpha]]$ the index of the group $\mathbb{Z}[\alpha]$ in $\mathbb{Z}_K$. If a prime integer p does not divide $\operatorname{ind}(\alpha)$, then a theorem of Dedekind says: The factorization of $p\mathbb{Z}_K$ can be derived directly from the decomposition $\overline{F}(X) = \prod_{i=1}^{r} \bar{\varphi}_i(X)^{l_i} \pmod p$. Namely, $p\mathbb{Z}_K = \prod_{i=1}^{r} \mathfrak{p}_i^{l_i}$, where every $\mathfrak{p}_i = (p, \varphi_i(\alpha))$, $e(\mathfrak{p}_i) = l_i$ is the ramification index, $f(\mathfrak{p}_i) = \deg(\varphi_i)$ is the residue degree. Also, Dedekind's criterion in [4] allows to test whether p divides $\operatorname{ind}(\alpha)$ or not. It is known that there exist number fields with at least one prime integer p for which Dedekind's criterion fails, that is, p divides

DOI: 10.21136/CMJ.2021.0516-19

the index $[\mathbb{Z}_K : \mathbb{Z}[\alpha]]$ for all primitive elements α of $\mathbb{Z}_K$ (see for example [1]). For such primes and number fields it is not possible to obtain the prime factorization of $p\mathbb{Z}_K$ by Dedekind's theorem. An alternative approach towards obtaining the factorization of $p\mathbb{Z}_K$ for these primes was initiated by Bauer in [2] using Newton polygons. This method has been further developed by several mathematicians, starting by Ore in 1923. In 2009, Khanduja and Kumar in [8] asked whether it is possible to find a weaker condition in order to have exactly r prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of $\mathbb{Z}_K$ lying above p, with ramification indices, and residue degrees all as above. In the same paper, they gave a weaker sufficient condition, a result which we state in Section 3. Besides, in 1894, Hensel developed a powerful approach by showing that the primes of $\mathbb{Z}_K$ lying above a prime p are in one-to-one correspondence with monic irreducible factors of $F(X)$ in $\mathbb{Q}_p[X]$. For every prime ideal corresponding to any irreducible factor in $\mathbb{Q}_p[X]$, the ramification index and the residue degree together are the same as those of the local field defined by the irreducible factor, see [7]. The main goal of this paper is to give an improvement of the result given in [8], by giving a weaker sufficient condition, which is also necessary to get exactly r prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of $\mathbb{Z}_K$ lying above p. A result which appears in our main results: Proposition 3.2, Lemma 3.6 and Theorem 3.8. We further specify for every prime ideal $\mathfrak{p}_i$, the ramification index, the residue degree and a p-generator; i.e., an integral element $\beta_i \in \mathbb{Z}_K$ such that $\mathfrak{p}_i$ is generated by p and β_i.

2. Preliminaries

After Hensel's work for every prime integer p the prime ideals of $\mathbb{Z}_K$ lying above p are in one-one correspondence with the monic irreducible factors of $F(X)$ in $\mathbb{Q}_p[X]$. Hensel's lemma allows then to get the first step of the factorization of $F(X)$ in $\mathbb{Q}_p[X]$. First order Newton polygon techniques (Ore's work) can be used to refine this factorization namely, the theorem of the polygon and the theorem of the residual polynomial, see for instance [6]. If all these techniques do not provide all irreducible factors of $F(X)$ in $\mathbb{Q}_p[X]$, then in 2012, Guardia, Montes, and Nart (see [6]) introduced an alternative technique, namely high order Newton polygon. In each order, the theorem of the polygon and the theorem of the residual polynomial could be used again to refine the factorization.

Let p be a prime integer, $\varphi \in \mathbb{Z}_p[X]$ a monic polynomial *whose reduction* modulo p is irreducible. Let $\mathbb{F}_\varphi$ be the finite field defined by p and φ; $\mathbb{F}_\varphi = \mathbb{Z}_p[X]/(p, \varphi)$ and $\operatorname{red}\colon \mathbb{Z}_p[X] \to \mathbb{F}_\varphi$ the canonical projection. For any polynomial $F(X) \in \mathbb{Z}_p[X]$, by the Euclidean division by successive powers of φ, we can expand $F(X)$ as $F(X) = a_n(X)\varphi(X)^n + a_{n-1}(X)\varphi(X)^{n-1} + \ldots + a_0(X)$; this is called the *$\varphi$-expansion* of $F(X)$ ($a_i(X) \in \mathbb{Z}_p[X]$ and $\deg a_i(X) < \deg \varphi$ for every $i := 0, \ldots, n$). 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 $u_i = \nu_p(a_i(X))$. The φ-Newton polygon is obtained by joining all sides $S_0, \ldots, S_g$ ordered by increasing slopes. We express this construction as $N_\varphi(F) = S_0 + \ldots + S_g$. Note that the sum here is only a notation to express that the sides are joining in the order of increasing slopes. The principal φ-Newton polygon of F, denoted by $N_\varphi^+(F)$, is the polygon determined by the sides of negative slopes of $N_\varphi(F)$. For every $i = 0, \ldots, n$, we attach the following *residue coefficient* $t_i \in \mathbb{F}_\varphi$ defined by

$$t_i = \begin{cases} 0 & \text{if } (i, u_i) \text{ lies strictly above } N_\varphi(F), \\ \operatorname{red}\Big(\dfrac{a_i(X)}{p^{u_i}}\Big) & \text{if } (i, u_i) \text{ lies on } N_\varphi(F). \end{cases}$$

For every side S of $N_\varphi^+(F)$, let $l = \ell(S)$ be the length of its projection to the x-axis and $H = h(S)$ the length of its projection to the y-axis. Then l is called the *length* of S and H is called its *height*. Let $d = \gcd(l, H)$. Then d is called the *degree* of S and $-\lambda = -h/e$ is the slope of S, where h and e are two positive coprime integers; $h = H/d$ and $e = l/d$. Note that if s is the abscissa of the initial point of S, then the points with integer coordinates lying on S are exactly $(s, u_s), (s + e, u_s - h), \ldots, (s + de, u_s - dh)$ and the abscissa candidates to provide nonzero residue coefficients are exactly $s, s + e, \ldots, s + de$. Let

$$F_S(Y) = c_d Y^d + c_{d-1} Y^{d-1} + \ldots + c_1 Y + c_0 \in \mathbb{F}_\varphi[Y]$$

be the residual polynomial of $F(X)$ attached to S, where for every $i = 0, \ldots, d$, $c_i = t_{s+ie}$ is the residue coefficient. The following are the relevant theorems from Ore's work (first order Newton polygon):

Theorem 2.1 (Theorem of the polygon)**.** *Let $F \in \mathbb{Z}_p[X]$ be a monic polynomial such that $\overline{F(X)}$ is a positive power of $\bar{\varphi}$. If $N_\varphi^+(F) = S_1 + \ldots + S_t$, then we can split $F(X) = F_1(X) \times \ldots \times F_t(X)$ in $\mathbb{Z}_p[X]$, such that $N_\varphi^+(F_i) = S_i$ and $F_{iS_i}(Y) = F_{S_i}(Y)$ up to multiplication by a nonzero element of $\mathbb{F}_\varphi$ for every $i = 1, \ldots, r$.*

Theorem 2.2 (Theorem of the residual polynomial)**.** *Let $F \in \mathbb{Z}_p[X]$ be a monic polynomial such that $F(X)$ is congruent to a positive power of $\varphi(x) \pmod p$, $N_\varphi^+(F) = S$ has a single side of slope $-\lambda$. If $F_S(Y) = \prod_{i=1}^{g} \psi_i(Y)^{t_i}$ is the factorization in $\mathbb{F}_\varphi[Y]$, then $F(X)$ splits as follows: $F(X) = F_1(X) \times \ldots \times F_g(X)$ in $\mathbb{Z}_p[X]$ such that $N_\varphi(F_i) = S_i$ has a single side of slope $-\lambda$ and $F_{iS_i}(Y) = c_i \psi_i(Y)^{t_i}$ for some $c_i \in \mathbb{F}_\varphi^*$ for every $i = 1, \ldots, r$.*

The following example illustrates the first order Newton polygon's techniques. Let $p = 2$, $\varphi = X^2 + X - 1$ and $F = \varphi^5 + (12X + 6)\varphi^3 + (12X + 12)\varphi^2 + 72$. As φ is irreducible modulo 3, $\overline{F} = \bar{\varphi}^5 \pmod 3$, and $\nu_3(72X + 48) = 1$, then $N_\varphi(F) = S$, with respect to $p = 3$, has a single side of height 1, and so its residual polynomial is irreducible over $\mathbb{F}_\varphi$. Thus, F is irreducible over $\mathbb{Q}_3$. Let $K = \mathbb{Q}(\alpha)$ be the number field defined by F. Then there is a unique prime ideal of $\mathbb{Z}_K$ lying above 3. For $p = 2$, $\bar{\varphi}$ is irreducible in $\mathbb{F}_2[X]$, $\overline{F} = \bar{\varphi}^5$ in $\mathbb{F}_2[X]$, and $N_\varphi(F) = N_\varphi^+(F) = S_1 + S_2$ (see Figure 1). By the theorem of the polygon, $F(X) = F_1(X)F_2(X)$, where $N_\varphi(F_i) = S_i$, and $F_{iS_i}(Y) = F_{S_i}(Y)$ up to multiplication by a nonzero element of $\mathbb{F}_\varphi$ for $i = 1, 2$. As $d(S_2) = 1$, $F_{S_2}(Y)$ is irreducible, and so F_2 is irreducible over $\mathbb{Q}_2$. Thus, F_2 provides a unique prime ideal of $\mathbb{Z}_K$ lying above 2. For F_1, $N_\varphi(F_1) = S_1$ and $F_{1S_1}(Y) = (Y + 1)^2$ is a power of an irreducible factor, then we have to use second order Newton polygon techniques. We recall here some fundamental techniques of Newton polygon of high order. For more details, we refer to [6]. As introduced in [6], a type of order $r - 1$ is a data $\mathbf{t} = (g_1(X), -\lambda_1, g_2(X), -\lambda_2, \ldots, g_{r-1}(X), -\lambda_{r-1}, \psi_{r-1}(X))$, where every $g_i(X)$ is a monic polynomial in $\mathbb{Z}_p[X]$, $\lambda_i \in \mathbb{Q}^+$, and $\psi_{r-1}(Y)$ is a polynomial over a finite field of p^α elements, with $\alpha = \prod_{i=0}^{r-2} f_i$, $f_i = \deg(\psi_i(X))$, satisfying the following recursive properties:

(1) $g_1(X)$ is irreducible modulo p, $\psi_0(Y) \in \mathbb{F}[Y]$ ($\mathbb{F} = \mathbb{F}_p$) is the polynomial obtained by reduction of $g_1(X)$ modulo p, and $\mathbb{F}_1 := \mathbb{F}[Y]/(\psi_0(Y))$.

(2) For every $i = 1, \ldots, r-1$, the Newton polygon of the ith order $N_i(g_{i+1}(X))$ has a single side of slope $-\lambda_i$.

(3) For every $i = 1, \ldots, r-1$, the residual polynomial of the ith order $R_i(g_{i+1})(Y)$ is an irreducible polynomial in $\mathbb{F}_i[Y]$, $\psi_i(Y) \in \mathbb{F}_i[Y]$ is the monic polynomial determined by $R_i(\varphi_{i+1})(Y) \simeq \psi_i(Y)$ (are equal up to multiplication by a nonzero element of $\mathbb{F}_i$, and $\mathbb{F}_{i+1} = \mathbb{F}_i[Y]/(\psi_i(Y))$).

(4) For every $i = 1, \ldots, r-1$, $g_{i+1}(X)$ has minimal degree among all monic polynomials in $\mathbb{Z}_p[X]$ satisfying (2) and (3).

(5) $\psi_{r-1}(Y) \in \mathbb{F}_{r-1}[Y]$ is a monic irreducible polynomial, $\psi_{r-1}(Y) \neq Y$, and $\mathbb{F}_r = \mathbb{F}_{r-1}[Y]/(\psi_{r-1}(Y))$.

Here the field $\mathbb{F}_i$ should not be confused with the finite field of i elements. As for every $i = 1, \ldots, r-1$, the residual polynomial of the ith order $R_i(g_{i+1})(Y)$ is an irreducible polynomial in $\mathbb{F}_i[Y]$, by theorem of the product in order i, the polynomial $g_i(X)$ is irreducible in $\mathbb{Z}_p[X]$. Let $\omega_0 = [\nu_p, x, 0]$ be the Gauss's extension of ν_p to $\mathbb{Q}_p(X)$. As for every $i = 1, \ldots, r-1$, the residual polynomial of the ith order $R_i(g_{i+1})(Y)$ is an irreducible polynomial in $\mathbb{F}_i[Y]$, then according to MacLane notations and definitions (see [9]), $g_{i+1}(X)$ induces a valuation on $\mathbb{Q}_p(X)$, denoted by

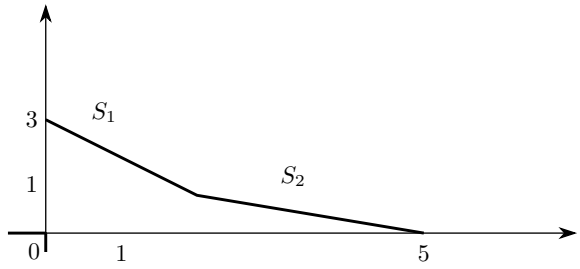

Figure 1. $N_\varphi(F)$.

$\omega_{i+1} = e_i[\omega_i, g_{i+1}, \lambda_{i+1}]$, where $\lambda_i = h_i/e_i$, e_i and h_i are positive coprime integers. The valuation ω_{i+1} is called the *augmented valuation* of ν_p with respect to φ and λ is defined over $\mathbb{Q}_p[X]$ as follows:

$$\omega_{i+1}(F(X)) = \min\{e_{i+1}\omega_i(a_j^{i+1}(X)) + jh_{i+1},\, j = 0, \ldots, n_{i+1}\},$$

where $F(X) = \sum_{j=0}^{n_{i+1}} a_j^{i+1}(X) g_{i+1}^j(X)$ is the $g_{i+1}(X)$-expansion of $F(X)$. According to the terminology in [6], the valuation ω_r is called the rth-order valuation associated to the data $\mathbf{t}$. For every order $r \geqslant 1$, the g_r-Newton polygon of $F(X)$ with respect to the valuation ω_r, is the lower boundary of the convex envelope of the set of points $\{(i, \mu_i),\, i = 0, \ldots, n_r\}$ in the Euclidean plane, where $\mu_i = \omega_r(a_i^r(X) g_r^i(X))$. The following are the relevant theorems from Montes-Guardia-Nart's work (high order Newton polygon):

Theorem 2.3 ([6], Theorem 3.1)**.** *Let $F \in \mathbb{Z}_p[X]$ be a monic polynomial such that $\overline{F(X)}$ is a positive power of $\bar{\varphi}$. If $N_r(F) = S_1 + \ldots + S_g$ has g sides, then we can split $F(X) = F_1 \times \ldots \times F_g(X)$ in $\mathbb{Z}_p[X]$, such that $N_r(F_i) = S_i$ and $R_r(F_i)(Y) = R_r(F)(Y)$ up to multiplication by a nonzero element of $\mathbb{F}_r$ for every $i = 1, \ldots, g$.*

Theorem 2.4 ([6], Theorem 3.7)**.** *Let $F \in \mathbb{Z}_p[X]$ be a monic polynomial such that $N_r(F) = S$ has a single side of finite slope $-\lambda_r$. If $F_S(Y) = \prod_{i=1}^{t} \psi_i(Y)^{a_i}$ is the factorization in $\mathbb{F}_r[Y]$, then $F(X)$ splits as $F(X) = F_1(X) \times \ldots \times F_t(X)$ in $\mathbb{Z}_p[X]$ such that $N_r(F_i) = S$ has a single side of slope $-\lambda_r$ and $R_r(F_i)(Y) = \psi_i(Y)^{a_i}$ up to multiplication by a nonzero element of $\mathbb{F}_r$ for every $i = 1, \ldots, t$.*

The following example illustrates the high order Newton polygon's techniques. Let $p = 2$, $\varphi = X$, and $F = X^4 + aX^2 + bX + c \in \mathbb{Z}[X]$ be an irreducible polynomial over $\mathbb{Q}$ such that $\nu_2(a) \geqslant 2$, $\nu_2(b) \geqslant 2$, and $\nu_2(c) = 2$. Then modulo 2, $\overline{F} = X^4$, $N_1(F) = S$ has a single side of slope $-\frac{1}{2}$, and $R_1(F) = (Y+1)^2$. So, with Ore's

works, we can not conclude the factorization of F in $\mathbb{Q}_2[X]$. Let $\varphi_2 = X^2 + 2$. Then $F = \varphi_2^2 + (a-4)\varphi_2 + (bX + c + 4 - 2a)$ is the φ_2-expansion of F. Let $\omega_2 = 2[\nu_2, X, \frac{1}{2}]$ be the augmented valuation of ν_2 with respect to X and $\lambda = \frac{1}{2}$. As $\omega_2(X) = 2\lambda = 1$, $\omega_2(\varphi_2) = 2$, $\omega_2((a-4)\varphi_2) \geqslant 6$, and $\omega_2(bX + c + 4 - 2a) \geqslant 5$, the second order Newton polygon of F is as follows:

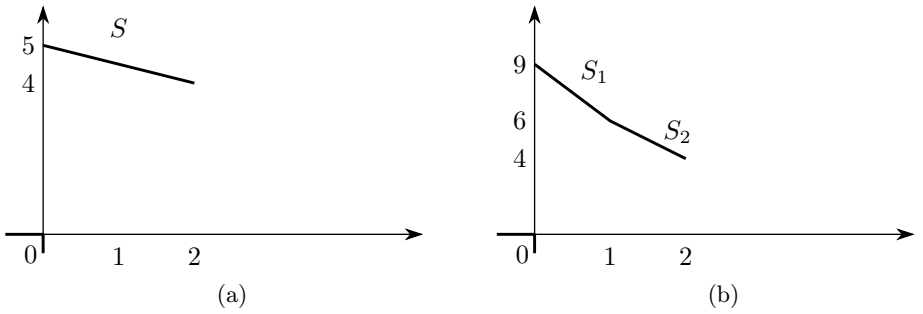

Figure 2. $N_2(F)$ with (a) $\nu_2(b) = 2$; (b) $\nu_2(b) = 4$, $\nu_2(c + 4 - 2a) \geqslant 5$ and $\nu_2(a) \geqslant 3$).

If $\nu_2(b) = 2$, then $N_2(F) = S$ has a single side with height 1 and length 2 (see Figure 2 (a)). In this case, there is a unique prime ideal of $\mathbb{Z}_K$ lying above 2 with ramification index $e_1 e_2 = 4$ and residue degree 1. If $\nu_2(b) = 4$, $\nu_2(c + 4 - 2a) \geqslant 5$ and $\nu_2(a) \geqslant 3$, then $N_2(F) = S_1 + S_2$ has two sides with length 1 each one (see Figure 2 (b)). In this case, there is two prime ideals of $\mathbb{Z}_K$ lying above 2 with ramification index 2 and residue degree 1 each one. Thanks to the index formula (see [6], Theorem 4.18), after a finite number of iterations, this process will provide $\mathrm{ind}_{j+1}^{i}(F) = 0$; the index of $(j+1)$th-order associated to the factor $g_1(X)$. In this case, the data $\mathbf{t} = (g_1(X), \lambda_1, g_2(X), \lambda_2, \ldots, g_j(X), \lambda_j, g_{j+1}(Y))$ is said to be F-complete. Thus, all factors of $F(X)$, provided by applying factorization of each order from 1 to r, are irreducible in $\mathbb{Q}_p[X]$. So, thanks to Hensel's correspondence, we deduce all maximal ideals of $\mathbb{Z}_K$ lying above p (their number, in particular). In the third example, we exhibit an example, where we have to use high order Newton polygon to achieve the factorization of $F(X)$ in $\mathbb{Q}_p[X]$, and so the number of maximal ideals of $\mathbb{Z}_K$ lying above p.

3. Main results

Throughout this paper, $F(X) \in \mathbb{Z}[X]$ is a monic irreducible polynomial, α a complex root of $F(X)$, K the number field generated by α, $\mathbb{Z}_K$ its ring of integers and p a prime integer such that $F(X) \equiv \prod_{i=1}^{r} \varphi_i^{l_i}(X) \pmod{p}$, where every $\varphi_i \in \mathbb{Z}_p[X]$ is

a monic polynomial and whose reduction modulo p is irreducible, φ_i and φ_j are not congruent modulo p for all $i \neq j$. For every $i = 1, \ldots, r$ let $F(X) = \sum_{j=0}^{L_i} a_j^i(X)\varphi_i^j(X)$ be the φ_i-expansion of $F(X)$ and $N_i = N_{\varphi_i}^+(F)$ the φ_i-principal polygon of $F(X)$.

According to Newton polygon notations and terminology (see [8], Corollary 1.2) can be reformulated as follows: *If for every $i = 1, \ldots, r$ either $l_i = 1$ or $l_i \geqslant 2$ and N_i has a single side of degree $d_i = 1$, then there are exactly r prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of $\mathbb{Z}_K$ lying above p.*

Proposition 3.2 gives a much weaker sufficient condition on $F(X)$ that guarantees the existence of exactly r prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of $\mathbb{Z}_K$ lying above p and for every prime ideal $\mathfrak{p}_i$, the ramification index $e(\mathfrak{p}_i)$, the residue degree $f(\mathfrak{p}_i)$ and a p-generator of $\mathfrak{p}_i$ are given too; an element $\omega_i \in \mathbb{Z}_K$ such that $\mathfrak{p} = p\mathbb{Z}_K + \omega\mathbb{Z}_K$.

For a p-generators of $\mathfrak{p}_i$ we need the following lemma:

Lemma 3.1. *An element $\omega \in K$ being a p-generator of $\mathfrak{p}$ is characterized in the following way: If $e(\mathfrak{p}) \geqslant 2$, then $\omega \in \mathbb{Z}_K$, $\nu_{\mathfrak{p}}(\omega) = 1$ and $\nu_{\mathfrak{p}'}(\omega) = 0$ for every other prime ideal $\mathfrak{p}'$ lying above p. If $e(\mathfrak{p}) = 1$, then the condition $\nu_{\mathfrak{p}}(\omega) = 1$ can be replaced by $\nu_{\mathfrak{p}}(\omega) \geqslant 1$, where $\nu_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic valuation on K.*

P r o o f. Let $\mathfrak{p}$ be a maximal ideal of $\mathbb{Z}_K$ lying above p. If $\mathfrak{p} = (p, \omega) = p\mathbb{Z}_K + \omega\mathbb{Z}_K$, then $\omega \in \mathfrak{p}$ and $\nu_{\mathfrak{p}}(\omega) \geqslant 1$. If $e(\mathfrak{p}) \geqslant 2$ and $\nu_{\mathfrak{p}}(\omega) \geqslant 2$, then ω and p are both in $\mathfrak{p}^2$, which is impossible because $\mathfrak{p} \not\subset \mathfrak{p}^2$. Hence, if $e(\mathfrak{p}) \geqslant 2$, then $\nu_{\mathfrak{p}}(\omega) = 1$ and if $e(\mathfrak{p}) = 1$, then condition $\nu_{\mathfrak{p}}(\omega) = 1$ can be replaced by $\nu_{\mathfrak{p}}(\omega) \geqslant 1$. If $p\mathbb{Z}_K \neq \mathfrak{p}$, then let $\mathfrak{p}' \neq \mathfrak{p}$ be an other maximal ideal of $\mathbb{Z}_K$ lying above p and set $s = \nu_{\mathfrak{p}'}(\omega)$. If $s \geqslant 1$, then $\mathfrak{p}'^s \subset (p, \omega) = \mathfrak{p}$, which is impossible because $\mathfrak{p}'^s$ and $\mathfrak{p}$ are coprime ideals. □

Proposition 3.2. *Suppose that for every $i = 1, \ldots, r$, either $l_i = 1$ or $l_i \geqslant 2$, N_i has a single side and $F_{N_i}(Y)$ is irreducible. Then there are exactly r prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of $\mathbb{Z}_K$ lying above p.*

Moreover, for every $i = 1, \ldots, r$, $f(\mathfrak{p}_i) = m_i d_i$, $e(\mathfrak{p}_i) = l_i/d_i$, where $m_i = \deg(\varphi_i)$, $d_i = \gcd(\nu_p(a_0^i(X)), l_i)$, and if $e(\mathfrak{p}_i) = 1$, then $\mathfrak{p}_i = (p, \varphi_i(\alpha))$, otherwise $\mathfrak{p}_i = (p, G_i(\alpha)(\varphi_i^{x_i}(\alpha)/p^{y_i}) + \varphi_i(\alpha))$, where h_i and e_i are two positive coprime integers such that $-h_i/e_i$ is the slope of N_i, x_i and y_i are two integers solution of $h_i x_i - e_i y_i = 1$ with $0 \leqslant x_i < e_i$ and $G_i(X) = \prod_{j \neq i} \varphi_j(X)^{y_i}$.

P r o o f. If for every $i = 1, \ldots, r$, $l_i = 1$, then by Dedekind's criterion, p does not divide $\mathrm{ind}(\alpha)$ and $p\mathbb{Z}_K = \prod_{i=1}^{r} \mathfrak{p}_i$. Else, as $F(X) \equiv \prod_{i=1}^{r} \varphi_i^{l_i}(X) \pmod p$, by Hensel's lemma we can split $F(X) = \prod_{i=1}^{r} F_i(X)$ in $\mathbb{Z}_p[X]$, where for every $i = 1, \ldots, r$, $F_i(X)$ is monic and $F_i(X) \equiv \varphi_i^{l_i}(X) \pmod p$. So, in order to have exactly r prime

ideals of $\mathbb{Z}_K$ lying above p, it suffices that every $F_i(X)$ is irreducible in $\mathbb{Z}_p[X]$, see [7]. Fix $i = 1, \ldots, r$. By theorem of the polygon (see [6], Theorem 1.15, page 372) and by assumption, $N_{\varphi_i}(F_i) = N^+_{\varphi_i}(F) = N_i$ has a single side up to a translation and $F_{iN_i}(Y) = F_{N_i}(Y)$ up to multiplication by a nonzero constant. As $F_{N_i}(Y)$ is irreducible in $\mathbb{F}_{\varphi_i}[Y]$, $F_{iN_i}(Y)$ is irreducible in $\mathbb{F}_{\varphi_i}[Y]$. By [3], Theorem 1.6, $F_i(X)$ is irreducible in $\mathbb{Z}_p[X]$. Finally, for every $i = 1, \ldots, r$, $F_i(X)$ is irreducible in $\mathbb{Z}_p[X]$. Thus, by [7] there are exactly r prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of $\mathbb{Z}_K$ lying above p.

We next calculate the ramification index, the residue degree and a p-generator of each prime ideal $\mathfrak{p}_i$. To simplify notations, fix $i = 1, \ldots, r$ and set $f(X) = F_i(X)$, $\varphi(X) = \varphi_i(X)$, $S = N_i$, β a root of $f(X) = F_i(X)$, $\mathbb{K} = \mathbb{Q}_p(\beta)$ the local field, $\mathfrak{p}$ its maximal ideal, and $\mathbb{Z}_\mathbb{K}$ its ring of integers. As $\overline{f}(X) = \bar{\varphi}^l(X) \pmod p$, the φ-expansion of $f(X)$ is $f(X) = \varphi(X)^l + b_{l-1}(X)\varphi(X)^{l-1} + \ldots + b_0(X)$. Let $\nu = \nu_p(a_0^i(X))$. As $S = N_{\varphi_i}(F_i) = N^+_{\varphi_i}(F)$, $\nu = \nu_p(b_0(X))$. Moreover, the fact that S has a single side of slope $-\lambda$ implies that $\nu = l\lambda$. Since $0 = f(\beta) \equiv \varphi^l(\beta)$ modulo $\mathfrak{p}$, let $\overline{\beta}$ be the projection of β in $\mathbb{Z}_\mathbb{K}/(\mathfrak{p})$. So, $\overline{\varphi(X)}$ is the minimal polynomial of $\overline{\beta}$ over $\mathbb{F}_p$. Since $\overline{\varphi(X)}$ does not divide $\overline{(b_0(X)/p^\nu)}$, we have $\overline{(b_0(\beta)/p^\nu)} \neq \bar{0}$ modulo $\mathfrak{p}$. So $\nu_\mathfrak{p}(b_0(\beta)) = e(\mathfrak{p})\nu_p(b_0(X)) = e(\mathfrak{p})\nu = e(\mathfrak{p})l\lambda$. We now show that $\nu_\mathfrak{p}(\varphi(\beta)) = e(\mathfrak{p})\lambda$. Note that as S has a single side, $\nu_p(b_j(X)) \geqslant (l-j)\lambda$ for every $j = 0, \ldots, l$. So, $\nu_\mathfrak{p}(b_j(\beta)) \geqslant (l-j)\lambda e(\mathfrak{p})$ (since β is integral over $\mathbb{Z}_p$). Thus, for every $j = 0, \ldots, l$, $\nu_\mathfrak{p}(b_j(\beta))\varphi(\beta)^j) \geqslant (l-j)\lambda e(\mathfrak{p}) + jw$, where $w = \nu_\mathfrak{p}(\varphi(\beta))$. If $w \neq e(\mathfrak{p})\lambda$, then it follows from the φ-expansion of $f(X)$ that $\nu_\mathfrak{p}(f(\beta)) = \min(l\omega, le(\mathfrak{p})\lambda)$, which is impossible since $\nu_\mathfrak{p}(f(\beta)) = \nu_\mathfrak{p}(0) = \infty$. Thus, $w = e(\mathfrak{p})\lambda$. Let $d = \gcd(l, \nu_p(a_0^i(X)))$, $e = l/d$, $h = \nu_p(a_0^i(X))/d$ and $\gamma = \varphi(\beta)^e/p^h$. Let us show that $e(\mathfrak{p}) = e$. As $\nu_\mathfrak{p}(\varphi(\beta)) = e(\mathfrak{p})\lambda = e(\mathfrak{p})h/e$ and e and h are coprime, we conclude that e divides $e(\mathfrak{p})$. Moreover, as $\nu_\mathfrak{p}(\gamma) = 0$, γ is integral over $\mathbb{Z}_p$ and $\gamma \not\equiv 0 \pmod \mathfrak{p}$. Consider the ring homomorphism

$$\iota\colon\ \mathbb{F}_\varphi[Y] \to \mathbb{Z}_\mathbb{K}/\mathfrak{p}, \quad \bar{a}(Y) \mapsto \overline{a(\gamma)}.$$

Its kernel is the maximal ideal of $\mathbb{F}_\varphi[Y]$ generated by the minimal polynomial of $\overline{\gamma}$ over $\mathbb{F}_\varphi$. Since $f_S(Y)$ is irreducible over $\mathbb{F}_\varphi$, in order to show that $[\mathbb{F}_\varphi[\gamma] : \mathbb{F}_\varphi] = \deg(f_S(Y))$, it suffices to show that $f_S(\gamma) = 0$. Recall that $f_S(Y) = \sum\limits_{i=0}^{d} c_i Y^{d-i}$, where $c_i = \operatorname{red}(b_{ie}(X)/p^{ih}) \pmod{p, \varphi} = \pi(b_{ie}(X)/p^{ih})$ with π being the canonical projection defined by $\pi\colon\ \mathbb{Z}_p[X] \to \mathbb{Z}_\mathbb{K}/\mathfrak{p}$, $X \mapsto \overline{\beta}$.

Now, let us show that $f_S(\gamma) = 0$. As

$$\frac{f(X)}{p^{hd}} = \frac{\sum_{j=0}^{l} b_j(X)\varphi^j(X)}{p^{hd}} = \sum_{i=0}^{d} \frac{b_{ie}(X)}{p^{(d-i)h}} \Big(\frac{\varphi^e(X)}{p^h}\Big)^i + \sum_{j \notin e\mathbb{N}} \frac{b_j(X)}{p^{(dh - \lfloor j\lambda \rfloor - 1)}} \frac{\varphi^j(X)}{p^{1+\lfloor j\lambda \rfloor}},$$

$y_j = dh - j\lambda$ is the ordinate of the point $A = (j, y_j) \in N_\varphi(f)$ with abscissa j, and so if $j \notin e\mathbb{N}$, then $\lfloor y_j \rfloor = dh - \lfloor j\lambda \rfloor - 1 < dh - j\lambda < \nu_p(b_j(X))$. By applying the projection π, we conclude that

$$\begin{aligned} 0 = \pi(f(\beta)) &= \sum_{i=0}^{d} \frac{b_{ie}(\overline{\beta})}{p^{ih}} \Big(\frac{\varphi^e(\overline{\beta})}{p^h} \Big)^{d-i} + \sum_{j \notin e\mathbb{N}} \frac{b_j(\overline{\beta})}{p^{(dh - \lfloor j\lambda \rfloor - 1)}} \frac{\varphi^j(\overline{\beta})}{p^{1+\lfloor j\lambda \rfloor}} \\ &= \sum_{i=0}^{d} \frac{b_{ie}(\overline{\beta})}{p^{ih}} \Big(\frac{\varphi^e(\overline{\beta})}{p^h} \Big)^{d-i} + 0 = f_S(\gamma). \end{aligned}$$

It follows that

$$f(\mathfrak{p}) = \Big[\frac{\mathbb{Z}_{\mathbb{K}}}{\mathfrak{p}} : \mathbb{F}_p \Big] = \Big[\frac{\mathbb{Z}_{\mathbb{K}}}{\mathfrak{p}} : \mathbb{F}_\varphi[\gamma] \Big] \cdot [\mathbb{F}_\varphi[\gamma] : \mathbb{F}_\varphi] \cdot [\mathbb{F}_\varphi : \mathbb{F}_p].$$

Thus, $m \cdot d = [\mathbb{F}_\varphi[\gamma] : \mathbb{F}_\varphi][\mathbb{F}_\varphi : \mathbb{F}_p] \cdot \deg(f_S(Y)) \cdot \deg(\varphi(X))$ and $m \cdot d$ divides $f(\mathfrak{p})$. As $e \cdot d \cdot m = \deg(f(X)) = e(\mathfrak{p}) \cdot f(\mathfrak{p})$, $d \cdot m$ divides $f(\mathfrak{p})$, and e divides $e(\mathfrak{p})$, we conclude that $e(\mathfrak{p}) = e$ and $f(\mathfrak{p}) = d \cdot m$.

For generators, first notice that under the hypothesis of the lemma, there is a one-one correspondence between maximal ideals of $\mathbb{Z}_K$ lying above p and $\varphi_1(X), \ldots, \varphi_r(X)$. So, if $i \neq j$, then $\nu_{\mathfrak{p}_i}(\varphi_i(\alpha)) \geqslant 1$ and $\nu_{\mathfrak{p}_i}(\varphi_j(\alpha)) = 0$. Thus, if $e_i = 1$, then $\mathfrak{p}_i = (p, \varphi_i(\alpha))$. If $e_i \geqslant 2$, then as $\gcd(e_i, h_i) = 1$, let (x_i, y_i) be nonnegative integers with $x_i h_i - y_i e_i = 1$ such that $0 \leqslant x_i < e_i$ and set $G_i(X) = \prod_{j \neq i} \varphi_j(X)^{y_i}$. Then for every $j \neq i$, $\nu_{\mathfrak{p}_j}(\varphi_i(\alpha)) = 0$ we have $\nu_{\mathfrak{p}_j}(G_i(\alpha)) = \nu_{\mathfrak{p}_j}(\varphi_j^{y_i}(\alpha)) \geqslant y_i$, $\nu_{\mathfrak{p}_j}(G_i(\alpha)(\varphi_i^{x_i}(\alpha)/p^{y_i})) \geqslant 0$, and so $G_i(\alpha)(\varphi_i^{x_i}(\alpha)/p^{y_i}) \in \mathbb{Z}_K$. Together with $\nu_{\mathfrak{p}_i}(\varphi_i^{x_i}(\alpha)/p^{y_i}) = 1$ and $\nu_{\mathfrak{p}_j}(\varphi_i(\alpha)) = 0$ we conclude that $G_i(\alpha)(\varphi_i^{x_i}(\alpha)/p^{y_i}) + \varphi_i(\alpha)$ is a p-generator of $\mathfrak{p}_i$. □

Remark 3.3. By applying the theorem of Ore [3], Theorem 1.8, page 179 and [5], Theorem 1 if for every $i := 1, \ldots, r$, N_i has a single side, then $p\mathbb{Z}_K = \prod_{i=1}^{r} \mathfrak{a}_i$, where $\mathfrak{a}_i$ are coprime ideals of $\mathbb{Z}_K$. In order to have $\mathfrak{a}_i$ a power of a maximal ideal $\mathfrak{p}_i$ of $\mathbb{Z}_K$ lying above p, a condition is missing, namely the irreducibility in $\mathbb{Z}_p[X]$ of the factor $F_i(X)$ associated to the single side N_i. This is also mentioned in the paper [3], page 174, between lines 22–24.

It is very important to consider the possibility of a converse of Proposition 3.2.

Lemma 3.4. *If $F(X)$ is irreducible in $\mathbb{Z}_p[X]$, then $\overline{F}(X)$ is a power of an irreducible factor $\bar{\varphi}(X)$ and $N_\varphi(F)$ has a single side.*

P r o o f. If we can split $\overline{F}(X) = \overline{F}_1(X) \cdot \overline{F}_2(X)$ such that $\overline{F}_1(X)$ and $\overline{F}_2(X)$ are coprime modulo p, then by Hensel's lemma, $F(X) = f_1(X) \cdot f_2(X)$ in $\mathbb{Z}_p[X]$ such that for every $i = 1, 2$, $f_i(X) \equiv F_i(X) \pmod{p}$. But as $F(X)$ is irreducible in $\mathbb{Z}_p[X]$, we conclude that $\overline{F}(X)$ is a power of an irreducible factor $\bar{\varphi}(X)$. Let $F(X) = \sum_{i=0}^{l_1} a_i(X)\varphi(X)^i$ be the φ-expansion of $F(X)$, α a root of $F(X)$, $g(X) = X^l + b_{l-1}X^{l-1} + \ldots + b_0$ the minimal polynomial of $\varphi(\alpha)$ over $\mathbb{Q}_p$, and $G(X) = g(\varphi(X))$. As $F(X)$ is irreducible in $\mathbb{Z}_p[X]$, by Hensel's correspondence (see [7]), there is only one prime $\mathfrak{p}$ of $\mathbb{Z}_K$ lying above p. Let $w = \nu_{\mathfrak{p}}(\varphi(\alpha))$. The fact that the $\mathfrak{p}$-adic valuations are invariant under Galois actions over the Henselian field $\mathbb{Q}_p$, by using the formulas linking roots and coefficients of the polynomial $g(X)$, we have $\nu_{\mathfrak{p}}(b_0) = l \cdot w$ and $\nu_{\mathfrak{p}}(b_i) \geqslant (l-i) \cdot w$ for every $i = 1, \ldots, l-1$. Thus, $\nu_p(b_0) = l\lambda$ and $\nu_p(b_i) \geqslant (l-i)\lambda$ for every $i = 1, \ldots, l-1$, where $\lambda = w/e(\mathfrak{p})$ and $e(\mathfrak{p})$ is the ramification index of $\mathfrak{p}$. So, $N_X(g) = S$ has a single side of slope $-\lambda$ and $N_\varphi(G) = S$. Since $G(\alpha) = 0$ and $F(X)$ is the minimal polynomial of α over $\mathbb{Q}_p$, $F(X)$ divides $G(X)$, and by theorem of the product (see [6]), $N_\varphi(F)$ has a single side of slope $-\lambda$. □

Remark 3.5.

(1) By Theorem of the polygon (see [6], Theorem 1.15, page 372), in order to have exactly r prime ideals of $\mathbb{Z}_K$ lying above p the condition that $N^+_{\varphi_i}(F) = N_{\varphi_i}(F_i)$ has a single side for every $i = 1, \ldots, r$, is a necessary condition for a converse of Proposition 3.2.

(2) For every $i = 1, \ldots, r$, let $\lambda_i = \nu_p(a_0^i(X))/l_i$. If l_i is the smallest positive integer such that $l_i \cdot \lambda_i \in \mathbb{Z}$, then $\nu_p(a_0^i(X))$ and l_i are two coprime integers. Thus, $d_i = 1$ and $F_{N_i}(X)$ is irreducible. It follows that Proposition 3.2 improves Corollary 1.2 given in [8].

(3) The following example shows that a full converse of Proposition 3.2 is impossible. Let $p = 2$, $\varphi = X$ and $F = X^4 + aX^2 + bX + c \in \mathbb{Z}[X]$ be an irreducible polynomial over $\mathbb{Q}$ such that $\nu_2(a) \geqslant 2$, $\nu_2(b) = \nu_2(c) = 2$ and let $K = \mathbb{Q}(\alpha)$. Then modulo 2, $\overline{F} = X^4$, $N_1(F) = S$ has a single side of slope $-\frac{1}{2}$, and $R_1(F) = (Y+1)^2$. For $\varphi_2 = X^2 + 2$, we have that $F = \varphi_2^2 + (a-4)\varphi_2 + (bX + c + 4 - 2a)$ is the φ_2-expansion of F. Let $\omega_2 = 2[\nu_2, \varphi, \frac{1}{2}]$. As $\omega_2(X) = 2\lambda = 1$, $\omega_2(\varphi_2) = 2$, $\omega_2((a-4)\varphi_2) \geqslant 6$ and $\omega_2(bX + c + 4 - 2a) = 5$, the second order Newton polygon $N_2(F)$ has a single side of degree 1 (see Figure 2 (b)). Thus, there is a unique prime ideal of $\mathbb{Z}_K$ lying above 2 even if $F_S(Y)$ is not irreducible over $\mathbb{F}_\varphi$.

Lemma 3.6. *Suppose that there are exactly r prime ideals of $\mathbb{Z}_K$ lying above p. Then N_i has a single side and $F_{N_i}(Y)$ is a power of an irreducible polynomial of $\mathbb{F}_{\varphi_i}[Y]$ for every $i = 1, \ldots, r$. Moreover, $m_i | f(\mathfrak{p}_i) | d_i \cdot m_i$ and $e_i | e(\mathfrak{p}_i) | l_i$ for every*

$i = 1, \dots, r$, where N_i has a single side of degree $d_i = l_i/e_i$ and slope $-\lambda_i = -h_i/e_i$, h_i and e_i are positive coprime integers, and $a \mid b$ means that a divides b. In particular, if $F_{N_i}(Y)$ is not a power of an irreducible polynomial of $\mathbb{F}_{\varphi_i}[Y]$ for some $i = 1, \dots, r$, then there are more than r prime ideals of $\mathbb{Z}_K$ lying above p.

P r o o f. As $F(X) \equiv \prod_{i=1}^{r} \varphi_i^{l_i}(X) \pmod p$, let $F(X) = \prod_{i=1}^{r} F_i(X)$ in $\mathbb{Z}_p[X]$, where $F_i(X) \equiv \varphi_i^{l_i}(X) \pmod p$ for every $i = 1, \dots, r$. Then every $F_i(X)$ yields at least one prime ideal $\mathfrak{p}_i$ lying above p. If we assume that there are exactly r prime ideals of $\mathbb{Z}_K$ lying above p, then by Hensel's correspondence (see [7]), every $F_i(X)$ is irreducible in $\mathbb{Z}_p[X]$. Fix $i = 1, \dots, r$ and let $\mathbb{K} = \mathbb{Q}_p[\alpha_i]$ be the local field defined by the polynomial $F_i(X)$ and $\mathfrak{p}_i$ the prime ideal of $\mathbb{Z}_{\mathbb{K}}$. Let $F_i(X) = \sum_{j=0}^{L_i} a_j^i(X)\varphi_i^j(X)$ be the φ_i-expansion of $F_i(X)$, $H_i = \nu_p(a_0^i(X))$ and $\lambda_i = H_i/l_i$. As $F_i(X) \equiv \varphi_i^{l_i}(X) \pmod p$, $L_i = l_i$. Moreover, in the proof of Proposition 3.2, that $\nu_{\mathfrak{p}_i}(\varphi_i(\alpha_i)) = e(\mathfrak{p}_i)\lambda_i = e(\mathfrak{p}_i)h_i/e_i$, where e_i and h_i are positive coprime integers, and that e_i divides $e(\mathfrak{p}_i)$ too. Let $\gamma_i = (\varphi_i(\alpha_i))^{e_i}/p^{h_i}$ and $g(X) = X^l + b_{l-1}X^{l-1} + \ldots + b_0$ its minimal polynomial over $\mathbb{Q}_p$. Since $\nu_{\mathfrak{p}_i}(\gamma_i) = 0$, γ_i is integral over $\mathbb{Z}_p$, $g(X) \in \mathbb{Z}_p[X]$, $\nu_p(b_j) \geqslant 0$ for every $j = 1, \dots, l-1$, and $\nu_p(b_0) = 0$. Let $G(X) = p^{lh_i} g((\varphi_i(X)))^{e_i}/p^{h_i})$. Then $G(X) = \sum_{j=0}^{l} A_j^i(X)\varphi_i^j(X)$, where for every $j = 0, \dots, l$, $A_{e_ij}^i(X) = p^{jh_i}b_j$ and $A_j^i(X) = 0$ if $j \notin e_i\mathbb{N}$. As $G(\alpha_i) = 0$ and $F_i(X)$ is the minimal polynomial of α_i, $F_i(X)$ divides $G(X)$. Since $\nu_p(b_0) = 0$, $N_{\varphi_i}(G) = S$ has a single side of slope $-lh_i/le_i = -\lambda_i$. By theorem of the product (see [6]), $N_{\varphi_i}(F_i) = N_i$ has a single side of slope $-\lambda_i$. By theorem of the residual polynomial (see [6]), $F_{N_i}(Y)$ is a power of an irreducible factor in $\mathbb{F}_{\varphi_i}[Y]$ (since $F_i(X)$ is irreducible in $\mathbb{Z}_p[X]$). As we showed in the proof of Proposition 3.2, if we consider the homomorphism of rings $\iota\colon \mathbb{F}_{\varphi_i}[Y] \to \mathbb{Z}_{\mathbb{K}}/\mathfrak{p}$, $\bar{a}(Y) \mapsto \overline{a(\gamma_i)}$, its kernel is the maximal ideal of $\mathbb{F}_{\varphi_i}[Y]$ generated by the minimal polynomial $\psi_i(Y)$ of γ_i over $\mathbb{F}_{\varphi_i}$ and $f_S(\gamma_i) = 0$. As by assumption $f_S(Y)$ is a power of an irreducible factor, $f_S(Y) = \psi_i(Y)^{r_i}$ and $d_i = r_i \cdot k_i$, where $k_i = \deg(\psi_i)$. Thus, $m_i \cdot k_i = [\mathbb{F}_{\varphi_i} : \mathbb{F}_p]$ divides $f(\mathfrak{p}_i)$ and $e_i \cdot r_i \cdot k_i \cdot m_i = e_i \cdot d_i \cdot m_i = l_i \cdot m_i = \deg(F_i(X)) = e(\mathfrak{p}_i) \cdot f(\mathfrak{p}_i)$. Since e_i divides $e(\mathfrak{p}_i)$, we have $f(\mathfrak{p}_i) = k_i \cdot m_i \cdot \mu_i$ and $e(\mathfrak{p}_i) = e_i \cdot \tau_i$, where $\tau_i \cdot \mu_i = r_i$. □

Remark 3.7. The condition "N_i has a single side of degree $d_i = 1$ for every $i = 1, \dots, r$" is not a necessary condition for having exactly r primes of $\mathbb{Z}_K$ lying above p such that $e(\mathfrak{p}_i) = l_i$ and $f(\mathfrak{p}_i) = m_i$ for every $i = 1, \dots, r$.

Indeed, it suffices to have for some i, $\deg(\psi_i) = 1$ and $r_i = \tau_i$ as shown in the previous proof. For example let $F(X) = X^4 + aX^2 + bX + c \in \mathbb{Z}[X]$ be an irreducible polynomial such that $\nu_2(a) \geqslant 2$, $\nu_2(b) = 2$ and $\nu_2(c) = 2$. Then for $p = 2$ we

have $F(X) \equiv X^4 \pmod 2$, $N_X(F) = S$ has a single side, and $F_S(Y) = (Y+1)^2$. Then neither Proposition 3.2 nor Lemma 3.6 can provide the number of prime ideals of $\mathbb{Z}_K$ lying above 2. We next use Newton polygon techniques of higher order. For $\varphi_2 = X^2 + 2$, $F(X) = \varphi_2^2 + (a-4)\varphi_2 + bX + c + 4 - 2a$. Let $\omega_2 = 2[\nu_2, \varphi, \frac{1}{2}]$ be the augmented valuation of ν_2 with respect to φ and $\lambda = \frac{1}{2}$. Then $\omega_2(\varphi_2^2) = 4$, $\omega_2((a-4)\varphi_2) \geqslant 6$ and $\omega_2(bX + c + 4 - 2a) = 5$ (because $\nu_2(c + 4 - 2a) \geqslant 3$, $\omega_2(c + 4 - 2a) \geqslant 6$ and $\omega_2(bX) = 5$). It follows that the φ_2-Newton polygon of the second order of $F(X)$ has a single side of degree 1, i.e., its residual polynomial is of degree 1, and so there is only one prime ideal $\mathfrak{p}$ of $\mathbb{Z}_K$ lying above 2 with ramification index $e(\mathfrak{p}) = e_1.e_2 = 4$ and residue degree $f(\mathfrak{p}) = 1$. Especially, $2\mathbb{Z}_K = (2, \frac{1}{2}(\alpha^2+2))^4$ (because $\nu_{\mathfrak{p}}(\varphi_2^2(\alpha)) = \nu_{\mathfrak{p}}(b\alpha + c + 4 - 2a) = 10$, $\nu_{\mathfrak{p}}(\varphi_2(\alpha)) = 5$ and $\nu_{\mathfrak{p}}(\frac{1}{2}\varphi_2(\alpha)) = 1$).

Theorem 3.8. *There are exactly r prime ideals of $\mathbb{Z}_K$ lying above p if and only if for every $j \geqslant 1$ and for every $i = 1, \ldots, r$, N_i^j has a single side and $F_{N_i^j}(Y)$ is a power of an irreducible factor, where N_i^j is the principal Newton polygon of order j attached to $(\varphi_i^1(X), \lambda_i^1, \varphi_i^2(X), \lambda_i^2, \ldots, \varphi_i^j(X), \lambda_i^j)$ and $F_{N_i^j}(Y)$ is the residual polynomial of order j as defined in* [6], *Section* 2.

P r o o f. By Lemma 3.6, it suffices to show the converse. By Hensel's Lemma, let $F(X) = F_1(X) \cdot \ldots \cdot F_r(X)$ be in $\mathbb{Z}_p[X]$ such that F_i is a monic polynomial and $F_i(X) \equiv \varphi_i^{e_i}(X) \pmod p$ for every $i = 1, \ldots, r$. So, in order to prove that there are exactly r prime ideals of $\mathbb{Z}_K$ lying above p, it suffices to show that $F_i(X)$ is irreducible in $\mathbb{Z}_p[X]$ for every $i = 1, \ldots, r$. Fix $i = 1, \ldots, r$. If we can split $F_i(X) = H_i(X)G_i(X)$ in $\mathbb{Z}_p[X]$ as a product of two nonconstant polynomials, then by [6], Theorem 2.26, page 390, we can split $F_{N_i^j}(Y)$ as a product of at least two nonconstant polynomials. The fact that $\mathrm{ind}_{j+1}^i(F) = 0$ implies that N_i^{j+1} has a single side of degree $d_i^j = 1$; length 1 or height 1 (see [6], Remark 4.13, page 405). Thus $F_{N_i^{j+1}}(Y)$ is of degree $d_i^j = 1$ and $F_i(X)$ is irreducible in $\mathbb{Z}_p[X]$. □

Recall that thanks to the index formula (see [6], Theorem 4.18) after a finite number of iterations, we get $\mathrm{ind}_{j+1}^i(F) = 0$. So the verification process is completed after a finite number of iterations.

Remark 3.9. Let $F \in \mathbb{Z}[X]$ be a monic irreducible polynomial which is congruent to a power of a monic irreducible polynomial $\bar{\varphi}$ in $\mathbb{F}_p[X]$ with $\varphi \in \mathbb{Z}[X]$ being monic. Then according to the notations and definitions of [6], Section 2, there is only a unique prime ideal of $\mathbb{Z}_K$ lying above p if and only if the jth-order Newton polygon N^j of F has a single side for every $j \geqslant 1$.

Indeed, if for some $j \geqslant 1$, $F_{N_i^j}(Y)$ has two coprime irreducible factors, namely g_j and h_j, in the finite field $\mathbb{F}_j[Y]$, then by [6], Lemma 2.17 (2), the length $l(N_j^+(F))$ is

the greatest power of g_j which divides $R_j(F)$, and so $N_j(F) \neq N_j^+(F)$. Thus, $N_j(F)$ has at least two distinct sides S_{0j} and S_{1j} with respective slopes $-\lambda_0^j$ and λ_1^j with $\lambda_0^j \leqslant 0$ and $\lambda_1^j > 0$.

4. Examples

Example 4.1. Let $F(X) = X^7 + 3X^5 + 24X^4 + 3X^3 + 18X^2 + 24X + 24$. It is clear that $F(X)$ is 3-Eisenstein and so is irreducible over $\mathbb{Q}$. Let $K = \mathbb{Q}(\alpha)$, where α is a complex root of $F(X)$. We want to see the factorization of 2 in $\mathbb{Z}_K$. First $F(X) \equiv X^3(X^2 + X + 1)^2 \pmod 2$. Let $\varphi_1 = X$ and $\varphi_2 = X^2 + X + 1$. Then

$$\begin{aligned} F(X) &= \ldots + 3\varphi_1^3 + 18\varphi_1^2 + 24\varphi_1 + 24 \\ &= (X-3)\varphi_2^3 + (6X+23)\varphi_2^2 - (46X+2)\varphi_2 + (28X+6). \end{aligned}$$

We can check that for every $i = 1, 2$, $N_{\varphi_i}(F) = S_i$ has only one side with respective slopes $-\lambda_1 = -1$ and $-\lambda_2 = -\frac{1}{2}$. Now, for $i = 1$, $F_{S_1}(Y) = Y^3 + Y^2 + 1$ is irreducible over $\mathbb{F}_2 \cong \mathbb{F}_{\varphi_1}$. For $i = 2$, since $\nu_2(28X + 6) = 1$, S_2 is of degree $d_2 = 1$, and thus $F_{S_2}(Y) = (j-1)Y + 1$, which is irreducible over $\mathbb{F}_{\varphi_2}$, where $j \in \bar{\mathbb{F}}_2$ is a root of $X^2 + X + 1$. Hence, $2\mathbb{Z}_K = \mathfrak{p}_1\mathfrak{p}_2^2$, where $\mathfrak{p}_1 = (2, \alpha)$, $\mathfrak{p}_2 = (2, \alpha^2 + \alpha + 1)$, $f(\mathfrak{p}_1) = 3$ and $f(\mathfrak{p}_2) = 2$.

Example 4.2. Let $F(X) = X^9 + 48X^7 + 6X^6 + 24X^5 + 12X^4 + 3X^3 + 18X^2 + 48X + 24$. It is clear that $F(X)$ is 3-Eisenstein and hence, is irreducible over $\mathbb{Q}$. Let $K = \mathbb{Q}(\alpha)$, where α is a complex root of $F(X)$. We have $F(X) \equiv X^3(X-1)^2 \times (X^2 + X + 1)^2 \pmod 2$. Set $\varphi_1 = X$, $\varphi_2 = X - 1$ and $\varphi_3 = X^2 + X + 1$. Then

$$\begin{aligned} F(X) &= \ldots + 3\varphi_1^3 + 18\varphi_1^2 + 48\varphi_1 + 24 = \ldots + 1473\varphi_2^2 + 642\varphi_2 + 184 \\ &= \ldots + (141X + 204)\varphi_3^2 - (174X + 36)\varphi_3 + (66X - 8). \end{aligned}$$

Thus, for $i = 1, 3$, $N_{\varphi_i}^+(F) = S_i$ has a single side of slope $-\lambda_1 = -1$ and $-\lambda_3 = -\frac{1}{2}$. For $i = 1$, $F_{S_1}(Y) = Y^3 + Y^2 + 1$, which is irreducible over $\mathbb{F}_{\varphi_1} \cong \mathbb{F}_2$. For $i = 3$, S_3 is of degree $d_3 = 1$, and thus $F_{S_3}(Y)$ is irreducible over $\mathbb{F}_{\varphi_3}$. But for $i = 2$, since $\nu_2(642) = 1$ and $\nu_2(184) = 3$, $N_{\varphi_2}^+(F) = S_1 + S_2$ has two sides and so φ_2 provides two prime ideals of $\mathbb{Z}_K$ lying above 2. Hence, there are 4 prime ideals of $\mathbb{Z}_K$ lying above 2.

Example 4.3. Let $F(X) = X^4 + aX^2 + bX + c \in \mathbb{Z}[X]$ be an irreducible polynomial, α a complex root of $F(X)$ and K the quartic number field generated by α. For $p = 2$, $\nu_2(c) = 2$, $\nu_2(b) \geqslant 2$ and $\nu_2(a) \geqslant 2$, $F(X) \equiv X^4 \pmod 2$,

$N_X(F) = S$ has a single side and $F_S(Y) = (Y+1)^2$. Notice that neither Proposition 3.2 nor Lemma 3.6 can provide the number of maximal ideals of $\mathbb{Z}_K$lying above 2. So, we next have to use Newton polygon techniques of high order. Let $\mathbf{t} = (X, \frac{1}{2}, \varphi_2(X), \lambda_2, \psi_2(Y))$, where $\varphi_2(X) = X^2+2$, λ_2 and ψ_2 will be defined in every case. As $-\frac{1}{2}$ is the slope of the side S, $\omega_2(a) = 2\nu_2(a)$ for every $a \in \mathbb{Z}$, $\omega_2(x) = 1$, and $\omega_2(\varphi_2(X)) = e = 2$, where $\omega_2 = 2[\nu_2, \varphi, \frac{1}{2}]$.

(1) For $\nu_2(b) = 2$, $F(X) = \varphi_2^2(X) + (a-4)\varphi_2(X) + bX + c + 4 - 2a$ is the $\varphi_2(X)$-expansion of $F(X)$. As $\omega_2(\varphi_2^2) = 4$, $\omega_2((a-4)\varphi_2) = 2 + 2\nu_2(a-4) \geqslant 6$ and $\omega_2(bX+c+4-2a) = 5$, $N^2(F) = S$ has a single side of degree 1, $-\lambda_2 = -\frac{1}{2}$ and $\psi_2(Y) = Y+1$. Thus, $2\mathbb{Z}_K = \mathfrak{p}^4$, where $\omega_2(\frac{1}{2}\varphi_2(\alpha)) = 1$.

(2) For $\nu_2(a) \geqslant 3$, $\nu_2(b) \geqslant 4$ and $\nu_2(c+4-2a) = 4$, $\omega_2((a-4)\varphi_2) = 6$ and $\omega_2(bX+c+4-2a) = 8$. Thus, $N^2(F) = S$ has a single side of slope, $-\lambda_2 = -1$, degree 2, and $\psi_2(Y) = F_S(Y) = Y^2+Y+1$, which is irreducible. Thus, $2\mathbb{Z}_K = \mathfrak{p}^2$, where $\omega_2(\alpha) = 1$.

(3) For $\nu_2(a) \geqslant 3$, $\nu_2(b) \geqslant 4$ and $\nu_2(c+4-2a) \geqslant 5$, $\omega_2((a-4)\varphi_2) = 6$ and $\omega_2(bX+c+4-2a) \geqslant 9$. Thus, $N^2_{\varphi_2}(F) = S_1 + S_2$ has two distinct sides. Thus, there are two different maximal ideals of $\mathbb{Z}_K$ lying above 2. More precisely, $2\mathbb{Z}_K = \mathfrak{p}_1^2\mathfrak{p}_2^2$.

Acknowledgements. The author is deeply grateful to the anonymous referee, their valuable comments and suggestions have tremendously improved the quality of the paper. Also, he is very grateful to Professor Enric Nart for introducing him to Newton polygon's techniques when he was a post-doc at CRM of Barcelona, Spain (2007–2008).

References

[1] *M. Bauer*: Über die ausserwesentliche Diskriminantenteiler einer Gattung. Math. Ann. *64* (1907), 573–576. (In German.) zbl MR doi

[2] *M. Bauer*: Zur allgemeinen Theorie der algebraischen Grösen. J. Reine Angew. Math. *132* (1907), 21–32. (In German.) doi

[3] *S. D. Cohen, A. Movahhedi, A. Salinier*: Factorization over local fields and the irreducibility of generalized difference polynomials. Mathematika *47* (2000), 173–196. zbl MR doi

[4] *R. Dedekind*: Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen. Abh. Math. Klasse Königlichen Gesellsch. Wiss. Göttingen *23* (1878), 3–37. (In German.)

[5] *L. El Fadil, J. Montes, E. Nart*: Newton polygons and p-integral bases of quartic number fields. J. Algebra Appl. *11* (2012), Article ID 1250073, 33 pages. zbl MR doi

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

[7] *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. (In German.) zbl MR doi

[8] *S. K. Khanduja, M. Kumar*: Prolongations of valuations to finite extensions. Manuscr. Math. *131* (2010), 323–334. zbl MR doi
[9] *S. MacLane*: A construction for absolute values in polynomial rings. Trans. Am. Math. Soc. *40* (1936), 363–395. zbl MR doi

Author's address: Lhoussain El Fadil, Faculty of Sciences Dhar El Mahraz, Sidi Mohamed Ben Abdellah University, P.O. Box 1874 Atlas-Fes, Fès, Morocco, e-mail: lhouelfadil2@gmail.com.