sciendo

Tatra Mountains Mathematical Publications
DOI: 10.2478/tmmp-2023-0005
Tatra Mt. Math. Publ. **83** (2023), 51–60

A GENERALIZATION OF EISENSTEIN-SCHÖNEMANN'S IRREDUCIBILITY CRITERION

Lhoussain El Fadil

Université of Sidi Mohamed Ben Abdellah, Fez-MOROCCO

This paper is dedicated to István Gaál

ABSTRACT. The Eisenstein criterion is a particular case of the Schönemann's irreducibility criterion stated in 1846. In 1906, based on Newton polygon techniques, Dumas gave a generalization of the Eisenstein criterion. In this paper, we extend this last generalization. Some applications on factorization of polynomials, and prime ideal factorization will be given, too.

1. Introduction

Factorization of monic polynomials over a henselian field is very useful in algebraic number theory; it plays a crucial role in prime ideal factorization. It is also very important in the study of extensions of valuations. For a valued field extension, the determination of irreducible polynomials is the focus of interest of many authors (cf. [1, 3, 5, 10]). In 1850, Eisenstein gave one of the most popular criteria to determine irreducible polynomials [5]. A criterion which was generalized in 1906 by Dumas in [3], who showed that for a polynomial

$$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x] \ \ (a_0 \neq 0),$$

if $\nu_p(a_n) = 0$, $n\nu_p(a_i) \geq (n-i)\nu_p(a_0) > 0$ for every $0 = i, \dots, n-1$, and $\gcd\big(\nu_p(a_0), n\big) = 1$ for some prime integer p, then f is irreducible over $\mathbb{Q}$, where ν_p is the p-adic valuation of $\mathbb{Q}$. In 2008, R. Brown gave what is known to be the most general version of Eisenstein-Schönemann's irreducibility criterion [1]. Namely, let (K, ν) be a rank one discrete valued field, with R_ν its valuation

2020 Mathematics Subject Classification: 11R09, 12R21, 13A18.
Keywords: irreducibility criterion, irreducible factors, valued field, Henselian fields.

ring and k_ν the residue field. For every polynomial $f = a_n\phi^n + a_{n-1}\phi^{n-1} + \cdots + a_0 \in R_\nu[x]$, with ϕ a monic polynomial in $R_\nu[x]$, $\overline{\phi}$ irreducible over k_ν, $a_i \in R_\nu[x]$, $\deg(a_i) < \deg(\phi)$, $\nu(a_n) = 0$, and $n\nu(a_i) \geq (n-i)\nu(a_0) > 0$ for every $0 = i, \ldots, n-1$. If $\gcd\big(n, \nu(a_0)\big) = 1$, then f is irreducible over the field K. In this paper, based on Newton polygon techniques, we extend this last version of Eisenstein-Schönemann's irreducibility criterion. Some applications to the factorization of polynomials, and prime ideal factorization will be given, too. Our results are illustrated by some applications and examples.

2. Notations

For any number field $L = \mathbb{Q}(\alpha)$ generated by a complex root α of a monic irreducible polynomial $f \in \mathbb{Z}[x]$, in 1894, K. Hensel developed a powerful approach by showing that the prime ideals of $\mathbb{Z}_L$ lying above a prime p are in one-to-one correspondence with monic irreducible factors of f in $\mathbb{Q}_p[x]$, where $\mathbb{Z}_L$ is the ring of integers of L. 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 associated to the prime ideal (see for instance [8]). Let (K, ν) be a rank one discrete valued field, R_ν its valuation ring, M_ν its maximal ideal, k_ν its residue field, (K_ν, ν) its completion, and K^h its henselization; the separable closure of K in K_ν. By normalization, we can assume that $\nu(K^*) = \mathbb{Z}$, and so M_ν is a principal ideal of R_ν generated by an element $\pi \in K$ satisfying $\nu(\pi) = 1$. Let $L = K(\alpha)$ be a simple extension generated by $\alpha \in \overline{K}$ a root of a monic irreducible polynomial $f \in R_\nu[x]$, where $\overline{K}$ is a fixed algebraic closure of K. By [13, Chapter I, Proposition 8.3], the Hensel's correspondence, given in [8], remains valid. By [4], it was suggested that we can replace K_ν by K^h. So, in order to describe all prime ideals of $\mathbb{Z}_L$ lying above the maximal ideal (π), we need to factorize the polynomial $f(x)$ into monic irreducible polynomials of $K^h[x]$. The first step of the factorization is based on Hensel's lemma. Unfortunately, the factors provided by Hensel's lemma are not necessarily irreducible over K^h. The Newton polygon techniques could refine the factorization. Namely, theorem of the product, theorem of the polygon, and theorem of the residual polynomial say that we can factorize any factor provided by Hensel's lemma, with as many sides of the polygon and as many irreducible factors of every residual polynomial. For more details, see [7,14] for Newton polygons over p-adic numbers and [2,6] for Newton polygons over rank one discrete valuations. As our proof is based on Newton polygon techniques, we recall some fundamental facts on Newton polygons. For a monic polynomial $\phi \in R_\nu[x]$ whose reduction modulo M_ν is irreducible in $k_\nu[x]$, let k_ϕ be the residue field $\frac{k_\nu[x]}{(\overline{\phi})}$.

Let $f \in R_\nu[x]$ be a monic polynomial. Upon the Euclidean division by successive powers of ϕ, we can expand $f(x)$ as follows

$$f = \sum_{i=0}^{l} a_i \phi^i,$$

called the ϕ-expansion of f (for every i, $\deg(a_i) < \deg(\phi)$). The ϕ-Newton polygon of f, denoted by $N_\phi(f)$ is the lower boundary of the convex envelop of the set of points $\{(i, \nu(a_i)),\ i = 0, \ldots, n\}$ in the Euclidean plane. For every edge S_j, of the polygon, let $A_{j-1} = (i_{j-1}, \nu(a_{i_{j-1}}))$ its initial point and $A_j = (i_j, \nu(a_{i_j}))$ its end point. Let $l_j = i_j - i_{j-1}$ be its length, $-\lambda_j = \frac{\nu(a_{i_j}) - \nu(a_{i_{j-1}})}{i_j - i_{j-1}} \in \mathbb{Q}$ its slope, and $H_j = \lambda_j l(S_j) = \nu(a_{i_{j-1}}) - \nu(a_{i_j})$ its height. Remark that l_i is the length of the projection of S_i to the x-axis and H_i is the length of its projection to the y-axis. Geometrically, $N_\phi(f)$ is the process of joining the obtained edges $S_1, \ldots, S_r$ ordered by the increasing slopes, which can be expressed by $N_\phi(f) = S_1 + \cdots + S_r$. The segments $S_1, \ldots,$ and S_r are called the sides of $N_\phi(f)$. The principal ϕ-Newton polygon of f, denoted by $N_\phi^+(f)$, is the part of the polygon $N_\phi(f)$, which is determined by joining all sides of negative slopes. For every side S of the polygon $N_\phi(f)$ with initial point (s, u_s), let l be its length, H its height, $d = \gcd(l, H)$, and $e = \frac{l}{d}$. For every $i = 0, \ldots, l$, we attach the following residual coefficient $c_i \in k_\phi$:

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

where (π, ϕ) is the maximal ideal of $R_\nu[x]$ generated by π and ϕ. That means if $(s+i, u_{s+i})$ lies on S, then

$$c_i = \overline{\frac{a_{s+i}(\beta)}{\pi^{u_{s+i}}}}, \quad \text{where } \beta \in \overline{K} \text{ is a root of } \phi.$$

Let $-\lambda = -h/e$ be the slope of S, where h and e are two non-negative integers with $-h/e$ an irreducible fraction. Then $d = l/e$ is called the degree of S. Notice that, the points with integer coordinates lying in S are exactly (s, u_s), $(s+e, u_s - h), \ldots, (s+de, u_s - dh)$. Thus, if i is not a multiple of e, then $(s+i, u_{s+i})$ does not lie in S, and so, $c_i = 0$. Let $R_\lambda(f)(y) = t_d y^d + t_{d-1} y^{d-1} + \cdots + t_1 y + t_0 \in k_\phi[y]$ be the residual polynomial of f associated to the side S, where for every $i = 0, \ldots, d$, $t_i = c_{ie}$.

Remark 1.

(1) If $\phi = x$, then $k_\phi = k_\nu$.

(2) If $\nu(a_{s+l})=0$ and $\nu(a_s)=0$ ($\lambda=0$), then $c_i=\overline{a_{s+i}}$ (mod π). Thus this notion of residual coefficient generalizes the reduction modulo a maximal ideal. In this case, for every $i = 0, \dots, d$, $(s+i, u_{s+i})$ lies on S if and only if $\nu(a_{s+i}) = 0$.

(3) If $\lambda = 0$ and $\phi = x$, then $c_i = \overline{a_{s+i}}$ (mod π) and $R_\lambda(f)(y) \in k_\nu[y]$ coincides with the reduction of f modulo the maximal ideal $M_\nu = (\pi)$.

If for some factor provided by the applications of Hensel's lemma and Ore's work, namely theorem of the polygon and theorem of the residual polynomial is reducible, then Guardia, Montes, and Nart introduced the notion of high order Newton polygon over p-adic number fields. In this paper, we partially extend this technique to any discrete rank one valued field: Let $\phi \in R_\nu[x]$ be a monic with $\overline{\phi}$ irreducible over k_ν. Then ϕ is a key polynomial of ν. Thus according to MacLane notations and terminologies [12], for every $\lambda \in \mathbb{Q}^+$, ϕ induces a valuation V of $K(x)$, called the augmented valuation of ν with respect to ϕ and $\lambda \in \mathbb{Q}$. V is defined on $K[x]$ by $V(P) = \min\{e\nu(p_i) + ih, i = 0, \dots, n\}$ for every $P = \sum_{i=0}^{n} p_i\phi^i$ with $\deg(p_i) < m$ and extended by $V(A/B) = V(A) - V(B)$ for every nonzero polynomials A and B of $K[x]$, where $m =\deg(\phi)$, $\lambda = \frac{h}{e}$, h and e are two coprime positive integers. The valuation V is denoted by $[\nu, \phi, \lambda]$. This is exactly what the authors of [7], called the valuation of second order Newton polygon. Let $\psi \in k_\phi[y]$ be a monic irreducible factor of $R_\lambda(f)(y)$. Then we can construct a monic polynomial $\phi_2 \in R_\nu[x]$ such that $N_\phi(\phi_2)$ has a single side T of slope $-\lambda$ and $R_\lambda(\phi_2) = \psi$. Such a polynomial exists and called a lifting of ψ with respect to ϕ and λ. Indeed, let $\psi(y) = y^t + c_{t-1}y^{t-1} + \cdots + c_0$, where $c_i \in k_\phi$ for every $i = 0, \dots, t-1$. For every $i = 0, \dots, t-1$, let $A_i \in R_\nu[x]$ with $\deg(A_i) < m =\deg(\phi)$, and $c_i \equiv A_i$ (mod π, ϕ). As ψ is irreducible over k_ϕ, $c_0 \neq 0$, and so $\overline{\phi}$ does not divide $\overline{A_0}$. The fact that $\deg(A_0) < m$ implies that $\nu(A_0) = 0$. Now, let e be the smallest positive integer satisfying $e\lambda \in \mathbb{Z}$, $u \in R_\nu$ such that $\nu(u) = e\lambda$, and $\phi_2 = \phi^{et} + uA_{t-1}\phi^{t-1} + u^2A_{t-2}\phi^{t-2} + \cdots + u^tA_0$. Then $\phi_2 \in R_\nu[x]$, $\overline{\phi_2} = \overline{\phi}^{et}$, $N_\phi(\phi_2) = T$ has a single side of slope $-\frac{t\nu(u)}{te} = -\lambda$, and $R_\lambda(\phi_2) = \psi$. Now, let $f = \sum_{i=0}^{l_2} A_i\phi_2^i$ be the ϕ_2-expansion of f. For every $i = 0, \dots, l_2$, let $\mu_i = V(A_i\phi_2^i)$. According to Nart's terminology in [7], the second order Newton polygon of f, with respect to ϕ_2 and V, denoted by $N_2(f)$, is the lower convex envelope of the set of points $\{(i, \mu_i), i = 0, \dots, l_2\}$ in the Euclidean plane.

3. Main results

Let $f(x) \in R_\nu[x]$ be a monic polynomial. If $\overline{f}$ is not a power of an irreducible polynomial of $k_\nu[x]$, then Hensel's lemma assures that f is not irreducible over K^h. Thus, in the remainder of this paper, we assume that $\overline{f}$ is a power of $\overline{\phi}$ for some monic polynomial $\phi \in R_\nu[x]$, with $\overline{\phi}$ irreducible over k_ν.

We start by the following theorem, which relaxes the condition $\phi = x$ required in [9, Theorem 1.1 and Theorem 1.2].

Theorem 3.1. *Assume that $\overline{f}$ is a power of $\overline{\phi}$ for some monic polynomial $\phi \in R_\nu[x]$, with $\overline{\phi}$ irreducible over k_ν. Let $f = \phi^n + a_{n-1}\phi^{n-1}(x) + \cdots + a_0$ be the ϕ-expansion of $f(x)$. If $\nu(a_i) \geq \nu(a_0) - i\lambda$ for every $i = 0, \ldots, n-1$, with $\lambda = \frac{\nu(a_0)}{n}$, then $f(x)$ has at most $d = \gcd(\nu(a_0), n)$ irreducible factors over the field K^h and each irreducible factor has degree at least $e \cdot m$, where $e = n/d$ and $\deg(\phi) = m$.*

According to the notations and terminologies of Section 2, Eisenstein-Schönemann's irreducibility criterion could be reformulated as follows:

Let $f \in R_\nu[x]$ be a polynomial. If $\overline{f} = \overline{\phi}^l$ for some monic polynomial $\phi \in R_\nu[x]$, whose reduction is irreducible over k_ν, and $N_\phi(f) = S$ has a single side of degree $d = 1$, with respect to ν, then f is irreducible over K.

Note that in [11], Khanduja gave a generalization of Eisenstein-Schönemann's irreducibility criterion over a valued field of arbitrary rank. The meaning of this generalization is if $N_\phi(f) = S$ has a single side of degree 1, then f is irreducible over K. The problem is what happens when $N_\phi(f)$ has a single side of degree $d \geq 2$?

The following theorem gives a partial answer, it drops the condition $d = 1$ required in the Eisenstein-Schönemann's irreducibility criterion.

Theorem 3.2. *Let $f(x) \in R_\nu[x]$ be a monic polynomial, $f = \phi^n + a_{n-1}\phi^{n-1} + \cdots + a_0$ the ϕ-expansion of f, and $n\nu(a_{n-i}) \geq i\nu(a_0)$ for every $i = 0, \ldots, n-1$.*

(1) *If $R_\lambda(f) = \psi_1\psi_2$ with ψ_1 and ψ_2 are two coprime polynomials of $k_\phi[y]$, then f is not irreducible over K^h.*
(2) *Assume that $R_\lambda(f) = c\psi^a$ for some $c \in k_\phi^*$ and some monic irreducible polynomial $\psi \in k_\phi[y]$ of degree t. Let ϕ_2 be a lifting of ψ with respect to ϕ and λ and let $f = \phi_2^a + A_{a-1}\phi_2^{a-1} + \cdots + A_0$ be the ϕ_2-expansion of f. Then if $a\big(V(A_{a-i}) - aeth\big) \geq i\big(V(A_0) - aeth\big)$ for every $i = 0, \ldots, a-1$ and $\gcd\big(V(A_0), a\big) = 1$, then f is irreducible over K^h, where $\lambda = \frac{\nu(a_0)}{n} = \frac{h}{e}$, h and e are two coprime integers, and $V = [\nu, \phi, \lambda]$.*

Remark 2. Under the hypothesis and notations of Theorem 3.2,

(1) If $R_\lambda(f)$ is irreducible over k_ϕ, then $R_\lambda(f) = c\psi^a$ with $a = 1$. Thus $\gcd\big(a, V(A_0)\big) = 1$, and so f is irreducible over K^h.
(2) In particular, if $\gcd\big(n, \nu(a_0)\big) = 1$, then $\deg\big(R_\lambda(f)\big) = 1$, and so $R_\lambda(f)$ is irreducible over k_ϕ. Thus, by the first point, f is irreducible over K^h. As a result, Theorem 3.2 generalizes the Eisenstein-Schönemann irreducibility criterion given in [1].

Let $L = K(\alpha)$ be a simple extension of K generated by $\alpha \in \overline{K}$ a root of a monic irreducible polynomial $f \in R_\nu[x]$. Thanks to the one-one correspondence between monic irreducible factors of f in $K^h[x]$ and distinct prime ideals of R_L lying above π, where R_L is the integral closure of R_ν in L, we have the following corollary

Corollary 3.3. *Under the hypothesis and notations of Theorem 3.2, if* $\gcd\big(a, V(A_0)\big) = 1$, *then there is a unique prime ideal* $\mathfrak{p}$ *of* R_L *lying above* π. *Furthermore,* $\pi R_L = \mathfrak{p}^{ea}$, *where* $\mathfrak{p} = \left(\pi, \frac{\phi(\alpha)^u}{\pi^v}\right)$, $(u, v) \in \mathbb{Z}^2$ *is the unique solution of* $hu - ve = 1$, $0 \le u < e$, *and* $f(\mathfrak{p}) = mt$ *is the residue degree of* $\mathfrak{p}$. *In particular, if* $\gcd(\nu(a_0), n) = 1$, *then* $\pi R_L = \mathfrak{p}^n$, *where* $\mathfrak{p} = \left(\pi, \frac{\phi(\alpha)^u}{\pi^v}\right)$ *is the unique prime ideal of* R_L *lying above* π *(because* $e = n$ *and* $a = 1$*).*

4. Proofs

Proof of Theorem 3.1. Under the hypothesis of Theorem 3.1, let $f = f_1 \times \cdots \times f_t$ be the factorization of f in $K^h[x]$, with f_i a monic polynomial for every $i = 1, \ldots, t$. As R_{ν^h} is integrally closed and $f \in R_{\nu^h}[x]$ is monic, by Gauss's lemma, every $f_i \in R_{\nu^h}[x]$. Let $i = 1, \ldots, t$. Since $\overline{f_i}$ divides $\overline{f}$, then $\overline{f_i} = \overline{\phi^{l_i}}$ for some natural integer l_i. The hypothesis of Theorem 3.1, implies that $N_\phi(f) = S$ has a single side of slope $-\lambda$. By the theorem of the product [6], for every $i = 1, \ldots, t$, $N_\phi(f_i) = S_i$ has a single side of slope $-\lambda$, $S = S_1 + \cdots + S_t$, and $R_\lambda(f) = \prod_{i=1}^{t} R_\lambda(f_i)$ up to multiplication by a nonzero element of k_ϕ. Since $\deg(R_\lambda(f)) = d$ and $\deg\big(R_\lambda(f_i)\big) \ge 1$ for every $i = 1, \ldots, t$, we get $t \le d$. Fix $i = 1, \ldots, t$. As $N_\phi(f_i) = S_i$, $\overline{f_i} = \overline{\phi}^{l_i}$, with $l_i = d_i e$ and $d_i = \deg\big(R_\lambda(f_i)\big)$. Thus $\deg\big(f_i(x)\big) = m \cdot e \cdot d_i$. As $\deg\big(R_\lambda(f_i)\big) = d_i \ge 1$, $\deg(f_i) \ge m \cdot e$ as desired. □

In order to show Theorem 3.2, we need the following lemma:

Lemma 4.1. *Under the hypothesis and notations of* (*ii*) *of Theorem 3.2, assume that* $R_\lambda(f) = \psi^a$ *for some monic irreducible polynomial* $\psi \in k_\phi[y]$ *and* $a \in \mathbb{N}$. *Let* $\phi_2 \in R_\nu[x]$ *be a lifting of* ψ *with respect to* ϕ *and* λ *and* $f = \sum_{i=0}^{l_2} A_i \phi_2^i$ *the* ϕ_2*-expansion of* f. *Then* $l_2 = a$, $A_a = 1$, $V(f) = aeth$, *and* $V(A_i \phi_2^i) > V(f)$ *for every* $i = 0, \ldots, a-1$.

Proof. First, by using the ϕ-expansion of f, we conclude $\deg(f) = mn$. Also the ϕ_2-expansion of f shows that $nm = l_2 \deg(\phi_2)$. The expression of ϕ_2 implies that $nm = l_2 etm$.

Secondly, as $R_\lambda(f) = \psi^a$, we have $\deg(f) = me\deg\big(R_\lambda(f)\big) = meat$. Thus $l_2 = a$ and $\deg(A_a) = 0$. Since f and ϕ_2 are monic, $A_a = 1$. On the other hand, since $N_\phi(f)$ has a single side of slope $-\lambda$, $\nu(a_{n-i}) \ge i\lambda$ for every $i = 0,\dots,n$ and $\lambda = \frac{a_0}{n}$. So, $e\nu(a_{n-i}) + (n-i)h \ge nh$ for every $i = 0,\dots,n$, and so $V(f) = nh = aeth$ (because $\frac{n}{e} = d\deg\big(R_\nu(f)\big) = at$).

For the last point, let $I = \{i = 0,\dots,a,\ V(A_i\phi_2^i) = V(f)\}$. Then I is a non empty finite set. Let i_0 be its smallest element and L_λ the line of slope $-\lambda$, which contains $\big(a, V(f)\big)$. For every $i = 0,\dots,a$, set $j = a-i$. If

$$V(A_{a-j}\phi_2^{a-j}) = V(f) = aeth,$$

then

$$\nu(A_{a-j}\phi_2^{a-j}) = aeth - (a-j)eth = jeth.$$

Thus, the point $\big(i_0, \nu(A_{i_0}\phi_2^{i_0})\big)$ lies on the line L_λ (because $i_0 = a - j_0$) and by definition of i_0, the point $\big(i, \nu(A_i\phi_2^i)\big)$ lies strictly above the line L_λ for every $i < i_0$. So, $R_\lambda(A_i\phi_2^i) = 0$ for every $i < i_0$ and $R_\lambda(A_{i_0}\phi_2^{i_0}) = c\psi^{i_0}$ for some nonzero element $c \in k_\phi$. It follows that $R_\lambda(f) = \psi^{i_0}g$ for some $g \in k_\phi[y]$, with ψ does not divide g. Hence $i_0 = \nu_\psi\big(R_\lambda(f)\big) = a$. By definition of i_0, $V(A_i\phi_2^i) > V(f)$ for every $i = 0,\dots,a-1$. □

Proof of Theorem 3.2.

(1) The first point of Theorem 3.2 is an immediate application of Theorem 3.7 in [6].

(2) For the second point, assume that $\gcd(V(A_0), a) = 1$, and show that f is irreducible over K^h. If not, suppose that $f = f_1f_2$ in $K^h[x]$, with $\deg(f_i) \ge 1$ for every $i = 1,2$. Again, as R_{ν^h} is integrally closed and f is monic, we can assume that every $f_i \in R_{\nu^h}[x]$ is a monic polynomial, $N_\phi(f_i) = S_i$ has a single side of slope $-\lambda$, and $R_\lambda(f_i) = c_i\psi^{a_i}$ for some nonzero constant $c_i \in k_\phi$, $a_i \in \mathbb{N}$ with $a_1 + a_2 = a$, and $S_1 + S_2 = S$. Thus, the ϕ_2-expansion of f_i has the form $f_i = \phi_2^{a_i} + \dots + A_0^i$, with $V(A_j^i\phi_2^j) > V(\phi_2^{a_i}) = a_ih$ for every $j = 0,\dots,a_i - 1$ and $i = 1,2$. Let us show that $N_2(f_i)$ has a single side of slope $-\lambda_2$ with $\lambda_2 = \frac{V(A_0)-aeth}{a}$. For this reason, let $\mu_j^i = \frac{V(A_{a_i}-j)-jeth}{j}$, $\mu^i = \min\{\mu_j^i, j = 1,\dots,a_i\}$ for every $j = 1,\dots,a_i$, and $\mu = \min(\mu^1,\mu^2)$. We claim that $\mu \ge \lambda_2 = \frac{V(A_0)-aeth}{a}$. Suppose the opposite; $\mu < \lambda_2$. Let j_i be the greatest index such that $\mu_{j_i}^i = \mu^i$. For every $j \ge 0$ and $c_j = \sum_{k=0}^{j} A_k^1 A_{j-k}^2$ with $A_k^i = 0$ if $k < 0$ or $k > a_i$. For every $i = 0,\dots,a$, let r_i and q_i be, respectively, the remainder and the quotient of the Euclidean division of $c_i + q_{i-1}$ by ϕ_2, where $q_{-1} = 0$. Then for every $i = 0,\dots,a$, $r_i = A_i$ and $f = \sum_{i=0}^{a} r_i\phi_2^i$ is the ϕ_2-expansion of f.

Assume that $\mu^1 \le \mu^2$ and consider

$$c_{j_1+a_2}\phi_2^{j_1+a_2} = (A_{j_1}^1 A_{a_2}^2 + A_{j_1+1}^1 A_{a_2-1}^2 + \cdots)\phi_2^{j_1+a_2}.$$

By the definition of j_1, $V(c_{j_1+a_2}\phi_2^{j_1+a_2}) = V(A^1_{j_1}\phi_2^{j_1}) + a_2feh$. Thus

$$V(c_{j_1+a_2}\phi_2^{j_1+a_2}) - aefh = V(A^1_{j_1}\phi_2^{j_1}) + (a_2-a)feh = V(A^1_{j_1}\phi_2^{j_1}) - a_2feh$$
$$= (a_1 - j_1)\mu^1 < (a_1 - j_1)\lambda_2. \qquad (1)$$

Also, by definition of j_1, $V(c_{j_1+a_2-k} > V(c_{j_1+a_2})$ for every $k \geq 1$. As $c_{j_1+a_2} + q_{j_1+a_2-1} = q_{j_1+a_2}\phi_2 + r_{j_1+a_2}$ and ϕ_2 is monic,

$$V(q_{j_1+a_2}) = V(c_{j_1+a_2} + q_{j_1+a_2-1}) = V(c_{j_1+a_2})$$

because

$$V(q_{j_1+a_2-1}) = V(c_{j_1+a_2-1}) > V(c_{j_1+a_2}).$$

Thus $V(r_{j_1+a_2}) \geq V(c_{j_1+a_2})$. If $V(r_{j_1+a_2}) > V(c_{j_1+a_2})$, then the point $\big(j_1 + a_2, \nu(r_{j_1+a_2})\big)$ lies strictly above the line L_λ of slope $-\lambda$ and contains the point $\big(j_1+a_2, \nu(c_{j_1+a_2})\big)$, and thus $R_\lambda(c_{j_1+a_2}) = R_\lambda(q_{j_1+a_2})\psi + 0$. This implies that ψ divides $R_\lambda(c_{j_1+a_2})$, which is a contradiction because $\deg(c_{j_1+a_2}) < \deg(\phi_2)$. Therefore, $V(r_{j_1+a_2}) = V(c_{j_1+a_2})$. Since $N_2(F) = T$ has a single side of slope $-\lambda_2$,

$$V(c_{j_1+a_2}\phi_2^{j_1+a_2}) - aefh\lambda \geq \big(a - (a_2 + j_1)\big)\lambda_2 \qquad (2)$$

(1) and (2) imply that

$$(a_1 - j_1)\lambda_2 > V(c_{j_1+a_2}\phi_2^{j_1+a_2}) - aefh \geq (a_1 - j_1)\lambda_2,$$

which is a contradiction. Consequently,

$$\mu \geq \lambda_2, \quad \text{and so} \quad \frac{V(A^i_0) - a_iefh}{a_i} \geq \lambda_2 \quad \text{for every} \quad i = 1, 2.$$

As $V(A_0) = V(c_0) = V(A^1_0) + V(A^2_0)$, we have

$$\mu^i_{a_i} = \frac{V(A^i_0) - a_iefh}{a_i} = \lambda_2 \quad \text{for every } i = 1, 2.$$

Thus $N_2(f_1)$ has a single side of slope $-\lambda_2$, and so $a_1\lambda_2 \in \mathbb{Z}$, which is impossible because $a > a_1$ and as by assumption $\gcd(V(A_0), a) = 1$, we have $\gcd(V(A_0) - aeth, a) = 1$, and so a is the smallest positive integer satisfying $k\lambda_2 \in \mathbb{Z}$. Therefore, f is irreducible over K^h. □

5. Examples

(1) Let $K = \mathbb{F}_2((x))$ be the fraction field of the formal power series ring over $\mathbb{F}_2$. It is well known that (K, ν) is a valued field with valuation ring $\mathbb{F}_2[[x]]$, maximal ideal $M_\nu = (x)$, $K^h = K$ and $\mathbb{F}_\nu = \mathbb{F}_2$. Let $\phi = y^2 + y + 1$ and $f = \phi^6 + x^k\phi^4 + x^s\phi^2 + x^3 + x^4 \in K[y]$ with k and s are two non--negative integers. We need to test the irreducibility of f over $K^h = K$. First, if $s = 0$, then by Hensel's lemma, f is reducible over K^h. If $s \in \{0, 1\}$ or $k = 0$, then $N_\phi(f)$ has at least two distinct sides, and so by theorem of the

polygon f is reducible K^h. Now assume that $k \geq 1$ and $s \geq 2$. In this case, $N_\phi(f) = S$ has a single side of height 3 and length 6. As $\gcd(3,6) = 3 \neq 1$, the Eisenstein-Schönemann irreducibility criterion failed. So, we have to use the generalized version proposed in Theorem 3.2. As $\overline{\phi}$ is irreducible over $\mathbb{F}_\nu$, ϕ is a key polynomial of ν, and so ϕ induces an extension of ν to $K[y]$ defined by $V(P) = \min\{e\nu(p_i) + ih,\ i = 0, \dots, n\}$ for every positive coprime integers e, and h and for every $P \in K[y]$, where $P = \sum_{i=0}^{n} p_i \phi^i$ is the ϕ-expansion of P. Extended by $V(A/B) = V(A) - V(B)$ for every A and B in $K[y]^*$, V is a valuation of $K(y)$. We have to investigate the following cases:

(a) If $k > 1$ and $s > 2$, then $R\lambda(f) = z^3 + 1 = (z+1)(z^2+z+1)$. Thus by (1) of Theorem 3.2, we conclude that f is reducible over K^h.

(b) If $k = 1$ and $s > 2$, then $R\lambda(f) = z^3 + z^2 + 1$ is irreducible over k_ϕ. Thus by (1) of Remark 2, f is irreducible over K. Let $L = K(\alpha)$, where $\alpha \in \overline{K}$ is a root of f. Then $xR_L = \mathfrak{p}^2$, where $f(\mathfrak{p}) = 2 \cdot 3 = 6$ is the residue degree of $\mathfrak{p}$.

(c) Similarly, if $k > 1$ and $s = 2$, then $R\lambda(f) = z^3 + z + 1$ is irreducible over k_ϕ. Thus by (1) of Remark 2, f is irreducible over K. Let $L = K(\alpha)$, where $\alpha \in \overline{K}$ is a root of f. Then $xR_L = \mathfrak{p}^2$, where $f(\mathfrak{p}) = 2 \cdot 3 = 6$ is the residue degree of $\mathfrak{p}$.

(d) If $k = 1$ and $s = 2$, then $R\lambda(f) = z^3 + z^2 + z + 1 = (z+1)^3$. Then $\psi = z + 1$, $t = 1$, $h = 1$, and $e = 2$. Let V be the augmented valuation of ν with respect to ϕ and $\lambda = 1/2$ and let $\phi_2 = \phi^2 + x$ be a lifting of ψ with respect to ϕ and λ. Then $f = \phi^3 + x^4$. Since $V(\phi) = h = 1$ and $V(x) = e0 = 2$, $V(\phi_2) = 2$, $V(\phi_2^3) = 6$, and $V(x^4) = 8$. Thus $N_2(f) = T$ has a single side. As also $\gcd(V(x^4), 3) = \gcd(8, 3) = 1$, by (2) of Theorem 3.2, f is irreducible over K. Let $L = K(\alpha)$, where $\alpha \in \overline{K}$ is a root of f. Then $xR_L = \mathfrak{p}^6$, where $f(\mathfrak{p}) = 2 \cdot 1 = 2$ is the residue degree of $\mathfrak{p}$.

(2) Let $f(x) = \phi^6 + 24x\phi^4 + 12\phi^3 + 15(16x + 32)\phi + 48$ and $\phi \in \mathbb{Z}[x]$ be a monic polynomial of degree at least 2, whose reduction is irreducible in $\mathbb{F}_2[x]$.
For $p = 2$, $N_\phi(f) = S$ has a single side of length $l = 6$, height $H = 4$, and so $d = 2$. By Theorem 3.1, $f(x)$ has at most 2 irreducible factors in $\mathbb{Q}_2[x]$. As $f_S(y) = y^2 + y + 1$ is irreducible over $\mathbb{F}_2[x]$, then for $\phi = x^3 + x + 1$, $f_S(y)$ is irreducible over $k_\phi \simeq \mathbb{F}_2$. Thus by Theorem 3.2, $f(x)$ is irreducible over $\mathbb{Q}_2$. Let $L = \mathbb{Q}(\alpha)$ and R_L its ring of integers, where α is a complex root of $f(x)$. Since $f(x)$ is irreducible over $\mathbb{Q}_2$, there is a single prime ideal $\mathfrak{p}$ of R_L lying above 2. Furthermore, $2R_L = \mathfrak{p}^3$ and $f(\mathfrak{p}) = 6$ is the residue degree of $\mathfrak{p}$.

(3) Let $f(x) = \phi^6 + 12x\phi^3 + 9(16x+32)\phi + 3(16x+16)$ and $\phi = x^2 + x - 1 \in \mathbb{Z}[x]$. For $p = 2$, $\overline{\phi}$ is irreducible over $\mathbb{F}_2$, $N_\phi(f) = S$ has a single side of length $l = 6$, height $H = 4$, and $d = 2$. By Theorem 3.1, $f(x)$ has at most 2 irreducible factors in $\mathbb{Q}_2[x]$. As $f_S(y) = y^2 + jy + j + 1 = (y-1)(y-j-1)$ in $k_\phi[y]$, then $f(x)$ has exactly two irreducible factors over $\mathbb{Q}_2$.
For $p = 3$, $\overline{\phi}$ is irreducible over $\mathbb{F}_3$. Since $f(x)$ satisfies the Eisenstein--Schönemann irreducibility criterion conditions, $f(x)$ is irreducible over $\mathbb{Q}_3$. Let $K = \mathbb{Q}(\alpha)$, where α is a complex root of $f(x)$. By Corollary 3.3, $2R_K = \mathfrak{p}_1^3\mathfrak{p}_2^3$, with respective residue degree 2 each prime ideal factor and $3R_K = \mathfrak{p}^6$ with residue degree 2.

REFERENCES

[1] BROWN, R.: *Roots of generalized Schönemann polynomials in Henselian extension fields*, Indian J. Pure Appl. Math. **39** (2008), no. 5, 403–410.

[2] COHEN, D.—MOVAHHEDI, A.—SALINIER, A.: , *Factorization over local fields and the irreducibility of generalized difference polynomials*, Mathematika, **47** (2000), 173–196.

[3] DUMAS, G.: *Sur quelques cas d'irréductibilité des polynômes à coefficients rationnels*, J. Math. Pures Appl. **6** (1906), 191–258.

[4] DEAJIM, A.—EL FADIL, L.—NAJIM, A.: *On a theorem of Dedekind* (submitted).

[5] EISENSTEIN, G.: *Über die Irreduztibilität und einige andere Eigenschaften der Gleichungen, von welcher die Theilung der ganzen Lemniscate abhängt*, J. reine angew. Math. **39** (1850), 160–179.

[6] EL FADIL, L.: *On Newton polygons techniques and factorization of polynomial over Henselian valued fields*, J. of Algebra and its Appl. **19** (2020), DOI: S0219498820501881.

[7] GUARDIA, J.—MONTES, J.—NART, E.: *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. **364** (2012), no. 1, 361–416.

[8] HENSEL, K.: *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.

[9] JAKHAR, A.: *On the factors of a polynomial*, Bull. London Math. Soc. **52** (2020) 158–160.

[10] MURTY, M. R.: *Prime numbers and irreducible polynomials*, Amer. Math. Monthly **109** (2002), 452–458.

[11] KHANDUJA, S. K.—SAHA, J.: *On a generalization of Eisenstein's irreducibility criterion*, Mathematika **44** (1997), 37–41.

[12] MACLANE, S.: *A construction for absolute values in polynomial rings*, Trans. Amer. Math. Soc. **40** (1936), 363–395.

[13] NEUKIRCH, J.: *Algebraic Number Theory*. Springer-Verlag, Berlin, 1999.

[14] ORE, O.: *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann. **99** (1928), 84–117.

Received November 12, 2022

Faculty of Sciences Dhar El Mahraz
Université of Sidi Mohamed Ben Abdellah
Fez-MOROCCO
E-mail: lhoussain.elfadil@usmba.ac.ma