Chapter

On the Irreducible Factors of a Polynomial and Applications to Extensions of Absolute Values

Lhoussain El Fadil and Mohamed Faris

Abstract

Polynomial factorization over a field is very useful in algebraic number theory, in extensions of valuations, etc. For valued field extensions, the determination of irreducible polynomials was the focus of interest of many authors. In 1850, Eisenstein gave one of the most popular criterion to decide on irreducibility of a polynomial over $\mathbb{Q}$. A criterion which was generalized in 1906 by Dumas. In 2008, R. Brown gave what is known to be the most general version of Eisenstein-Schönemann irreducibility criterion. Thanks to MacLane theory, key polynomials play a key role to extend absolute values. In this chapter, we give a sufficient condition on any monic plynomial to be a key polynomial of an absolute value, an irreducibly criterion will be given, and for any simple algebraic extension $L = K(\alpha)$, we give a method to describe all absolute values of L extending $||$, where $(K, ||)$ is a discrete rank one valued field.

Keywords: Irreducibly criterion, irreducible factors, Extensions of absolute values, Newton polygon's techniques

1. Introduction

Polynomial factorization over a field is very useful in algebraic number theory, for prime ideal factorization. It is also important in extensions of valuations, etc. For valued field extensions, the determination of irreducible polynomials was the focus of interest of many authors (cf. [1–7]). In 1850, Eisenstein gave one of the most popular criterion to decide on irreducibility of a polynomial over $\mathbb{Q}$ [1]. A criterion which was generalized in 1906 by Dumas in [8], who showed that for a polynomial $f(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{Q}[x]$ $(a_0 \neq 0)$, 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 $gcd\left(\nu_p(a_0), n\right) = 1$ for some prime integer p, then $f(x)$ is irreducible over $\mathbb{Q}$. In 2008, R. Brown gave what is known to be the most general version of Eisenstein-Schönemann irreducibility criterion [9]. He showed for a valued field (K, ν) and for a monic polynomial $f(x) = \phi^n(x) + a_{n-1}(x)\phi^{n-1}(x) + \dots + a_0(x) \in R_\nu[x]$, where R_ν is a valuation ring of a discrete rank one valuation and ϕ being a monic polynomial in $R_\nu[x]$ whose reduction $\overline{\phi}$ is irreducible over $\mathbb{F}_\nu$, $a_i(x) \in R_\nu[x]$, $\deg(a_i) < \deg(\phi)$ for every $i = 0, \dots, n-1$, if $\nu(a_i) \leq (1 - i/n)\nu(a_0)$ for every $i = 0, \dots, n-1$ and $\gcd(\nu(a_0), n) = 1$, then $f(x)$ is irreducible over the field K. In this paper, based on absolute value, we give an irreduciblity criterion of monic polynomials. More precisely, let $(K, ||)$ be a discrete rank one valued field, $R_{||}$ its valuation ring, $\mathbb{F}_{||}$, its residue field, and $\Gamma = |K^*|$ its value group, we show that for a monic polynomial $f(x) = \phi^n(x) + a_{n-1}(x)\phi^{n-1}(x) + \dots + a_0(x) \in R_{||}[x]$, where ϕ being a monic polynomial in $R_{||}[x]$ whose reduction $\overline{\phi}$ is irreducible over $\mathbb{F}_{||}$, $a_i(x) \in R_{||}[x]$, $\deg(a_i) < \deg(\phi)$ for every $i = 0, \dots, n-1$, if $|a_{n-i}|_\infty \geq \gamma^i$ for every $i = 0, \dots, n-1$ and n is the smallest integer satisfying $\gamma^n \in \Gamma$, where $\gamma = \left(|a_0|_\infty\right)^{1/n}$, then $f(x)$ is irreducible over K. Similarly for the results of extensions of valuations given in [10, 11], for any simple algebraic extension $L = K(\alpha)$, we give a method to describe all absolute values of L extending $||$, where $(K, ||)$ is a discrete rank one valued field. Our results are illustrated by some examples.

2. Preliminaries

2.1 Newton polygons

Let $L = \mathbb{Q}(\alpha)$ be a number field generated by a complex root α of a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ and $\mathbb{Z}_L$ the ring of integers of L. 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–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 factors [6]. These results were generalized in ([12], Proposition 8.2). Namely, for a rank one valued field (K, ν), R_ν its valuation ring, and $L = K(\alpha)$ a simple extension generated by $\alpha \in \overline{K}$ a root of a monic irreducible polynomial $f(x) \in R_\nu[x]$, the valuations of L extending ν are in one–one correspondence with monic irreducible factors of $f(x)$ in $K^h[x]$, where K^h is the henselization of $(K, ||)$ will be defined later. So, in order to describe all valuations of L extending ν, one needs to factorize the polynomial $f(x)$ into monic irreducible factors over K^h. The first step of the factorization was 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 residual polynomial say that we can factorize any factor provided by Hensel's lemma, with as many sides of the polygon and with as many of irreducible factors of the residual polynomial. For more details, we refer to [7, 13] for Newton polygons over p-adic numbers and [14, 15] for Newton polygons over rank one discrete valued fields. As our proofs are based on Newton polygon techniques, we recall some fundamental notations and techniques on Newton polygons. Let (K, ν) be a rank one discrete valued field ($\nu(K^*) = \mathbb{Z}$), R_ν its valuation ring, M_ν its maximal ideal, $\mathbb{F}_\nu$ its residue field, and $\left(K^h, \nu^h\right)$ its henselization; the separable closure of K in $\hat{K}$, where $\hat{K}$ is the completion of $(K, ||)$, and $||$ is an associated absolute value of 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 also ν be the Gauss's extension of ν to $K^h(x)$. For any monic polynomial $\phi \in R_\nu[x]$ whose reduction modulo M_ν is irreducible in $\mathbb{F}_\nu[x]$, let $\mathbb{F}_\phi$ be the field $\frac{\mathbb{F}_\nu[x]}{(\overline{\phi})}$.

Let $f(x) \in R_\nu[x]$ be a monic polynomial and assume that $\overline{f(x)}$ is a power of $\overline{\phi}$ in $\mathbb{F}_\nu[x]$, with $\phi \in R_\nu[x]$ a monic polynomial, whose reduction is irreducible in $\mathbb{F}_\nu[x]$. Upon the Euclidean division by successive powers of ϕ, we can expand $f(x)$ as follows $f(x) = \sum_{i=0}^{l} a_i(x)\phi(x)^i$, where $\deg(a_i) < \deg(\phi)$ for every $i = 0, \dots, l$. Such a ϕ-expansion is unique and called the ϕ-expansion of $f(x)$. The ϕ-Newton polygon of f, denoted by $N_\phi(f)$ is the lower boundary of the convex envelope of the set of points $\{(i, \nu(a_i)), i = 0, \dots, l\}$ in the Euclidean plane. For every edge S_j, of the polygon $N_\phi(f)$, let l_j be the length of the projection of S_j to the x-axis and H_j the length of its projection to the y-axis. l_j is called the length of S_j and H_j is its height. Let $d_j = \gcd(l_j, H_j)$ be the degree of S_j, $e_j = \frac{l_j}{d_j}$ the ramification degree of S_j, and $-\lambda_j = -\frac{H_j}{l_j} \in \mathbb{Q}$ the slope of S_j. Geometrically, we can remark that $N_\phi(f)$ is the process of joining the obtained edges $S_1, \dots, S_r$ ordered by increasing slopes, which can be expressed by $N_\phi(f) = S_1 + \dots + S_r$. The segments $S_1, \dots,$ and S_r are called the sides of $N_\phi(f)$. The principal ϕ-Newton polygon of $f(x)$, 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 $N_\phi^+(f)$ of slope $-\lambda$ and initial point (s, u_s), let l be its length, H its height and e the smallest positive integer satisfying $e\lambda \in \mathbb{Z}$. Since $l\lambda = H \in \mathbb{Z}$, we conclude that e divides l, and so $d = l/e \in \mathbb{Z}$ called the degree of S. Remark that $d = \gcd(l, H)$. For every $i = 0, \dots, l$, we attach the following residue coefficient $c_i \in \mathbb{F}_\phi$:

$$c_i = \begin{cases} 0, & \text{if } (s+i, u_{s+i}) \text{ lies strictly above } S \\ \left(\dfrac{a_{s+i}(x)}{\pi^{u_{s+i}}}\right) \pmod{(\pi, \phi)}, & \text{if } (s+i, u_{s+i}) \text{ lies on } S. \end{cases} \tag{1}$$

where (π, ϕ) is the maximal ideal of $R_\nu[x]$ generated by π and ϕ.

Let $\lambda = -h/e$ be the slope of S, where $h = H/d$ and $d = l/e$. Notice that, the points with integer coordinates lying in S are exactly $(s, u_s), (s+e, u_s - h), \dots, (s+de, u_s - dh)$. Thus, if i is not a multiple of e, then $(s+i, u_{s+i})$ does not lie on S, and so $c_i = 0$. It follows that the candidate abscissas which yield nonzero residue coefficient are $s, s+e, \dots,$ and $s+de$. Let $R_\lambda(f)(y) = t_d y^d + t_{d-1} y^{d-1} + \dots + t_1 y + t_0 \in \mathbb{F}_\phi[y]$ be the residual polynomial of $f(x)$ associated to the side S, where for every $i = 0, \dots, d$, $t_i = c_{ie}$. For every $\lambda \in \mathbb{Q}^+$, the λ-component of $N_\phi(f)$ is the largest segment of $N_\phi(f)$ of slope $-\lambda$. If $N_\phi(f)$ has a side S of slope $-\lambda$, then $T = S$. Otherwise, T is reduced to a single point; the end point of a side S_i, which is also the initial point of S_{i+1} if $\lambda_{i+1} < \lambda < \lambda_i$ or the initial point of $N_\phi(f)$ if $\lambda_i < \lambda$ for every side S_i of $N_\phi(f)$ or the end point of $N_\phi(f)$ if $\lambda_i < \lambda$ for every side S_i of $N_\phi(f)$. In the sequel, we denote by $R_\lambda(f)(y)$, the residual polynomial of $f(x)$ associated to the λ-component of $N_\phi(f)$.

The following are the relevant theorems from Newton polygon. Namely, theorem of the product and theorem of the polygon. For more details, we refer to [15].

Theorem 2.1. (theorem of the product) *Let $f(x) = f_1(x) f_2(x)$ in $R_\nu[x]$ be monic polynomials such that $\overline{f(x)}$ is a positive power of $\overline{\phi}$. Then for every $\lambda \in \mathbb{Q}^+$, if T_i is the λ-componenet of $N_\phi(f_i)$, then $T = T_1 + T_2$ is the λ-componenet of $N_\phi(f)$ and*

$$R_\lambda(f)(y) = R_\lambda(f_1)(y) R_\lambda(f_2)(y)$$

up to multiplication by a nonzero element of $\mathbb{F}_\phi$.

Theorem 2.2. (theorem of the polygon) *Let $f \in R_\nu[x]$ be a monic polynomial such that $\overline{f(x)}$ is a positive power of $\overline{\phi}$. If $N_\phi(f) = S_1 + \dots + S_g$ has g sides of slope $-\lambda_1, \dots, -\lambda_g$ respectively, then we can split $f(x) = f_1 \times \dots \times f_g(x)$ in $K^h[x]$, such that $N_\phi(f_i) = S_i$ and $R_{\lambda_i}(f_i)(y) = R_{\lambda_i}(f)(y)$ up to multiplication by a nonzero.*

Theorem 2.3. (theorem of the residual polynomial) *Let $f \in R_\nu[x]$ be a monic polynomial such that $N_\phi(f) = S$ has a single side of finite slope $-\lambda$. If $R_\lambda(f)(y) = \prod_{i=1}^t \psi_i(y)^{a_i}$ is the factorization in $\mathbb{F}_\phi[y]$, then $f(x)$ splits as $f(x) = f_1(x) \times \cdots \times f_t(x)$ in $K^h[x]$ such that $N_\phi(f_i) = S_i$ has a single side of slope $-\lambda$ and $R_\alpha(f_i)(y) = \psi_i(y)^{a_i}$ up to multiplication by a nonzero element of $\mathbb{F}_\phi$ for every $i = 1, \cdots, t$.*

2.2 Absolute values

Let $||$ be an absolute value of K; a map $|| : K \to \mathbb{R}^+$, which satisfies the following three axioms:

1. $|a| = 0$ if and only if $a \neq 0$,

2. $|ab| = |a||b|$, and

3. $|a + b| \leq |a| + |b|$. (triangular inequality)

for every $(a, b) \in K^2$.

If the triangular inequality is replaced by an ultra-inequality, namely $|a + b| \leq \max\{|a|, |b|\}$ for every $(a, b) \in K^2$, then the absolute value $||$ is called a non archimidean absolute value and we say that $(K, ||)$ is a non archimidean valued field.

Lemma 2.4. *Let $(K, ||)$ be a valued field. Then $||$ is a non archimidean absolute value if and only if the set $\{|n1_K|, n \in \mathbb{N}\}$ is bounded in $\mathbb{R}$.*

Proof. By induction if $||$ is a non archimidean absolute value, then the set $\{|n1_K|, n \in \mathbb{N}\}$ is bounded by 1.

Conversely, assume that there exists $M \in \mathbb{R}^+$ such that $|n1_K| \leq M$ for every $n \in \mathbb{N}$. Let $(a, b) \in K^2$, $n \in \mathbb{N}$, and set $m = sup(|a|, |b|)$. Then $|a + b|^n = |\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}|$, where $\binom{n}{k}$ is the binomial coefficient. As $||$ is a non archimidean absolute value, $|a + b|^n \leq \sup\{|\binom{n}{k} 1_K| \cdot |a^k b^{n-k}| \leq M m^n$. Thus $|a + b| \leq M^{1/n} m$. Go over the limit, we obtain $|a + b| \leq m = sup(|a|, |b|)$ as desired. □

Exercices 1. Let $(K, ||)$ be a valued field.

1. Show that if K is a finite field, then $||$ is a non archimidean absolute value.

2. More precisely, show that if K is a finite field, then $||$ is trivial; $|x| = 1$ for every $x \in K^*$.

3. Let $\nu : K^* \to \mathbb{R}$ be the map defined by $\nu(a) = -Ln(|a|)$ for every $a \in K^*$, where Ln is the Napierian logarithm defined on $\mathbb{R}^+$. Show that $||$ is a non archimidean absolute value if and only if ν is a valuation of K. ν is called an associated valuation to $||$.

4. Show that if $||$ is a non archimidean absolute value and $(a, b) \in K^2$ such that $|a| \neq |b|$, then $|a + b| = \max(|a|, |b|)$.

5. Let p be a prime integer and $||_p : \mathbb{Q} \to \mathbb{R}^+$, defined by $|a|_p = p^{-\nu_p(a)}$ for every $a \in K^*$, where ν_p is the p-adic valuation on $\mathbb{Q}$. Show that $||_p$ is a non archimidean absolute value of $\mathbb{Q}$.

2.3 Characteristic elements of an absolute value

Let $(K, ||)$ be a non archimedian valued field.

Let $R_{||} = \{a \in K, |a| \leq 1\}$ and $M_{||} = \{a \in K, |a| < 1\}$. Then $R_{||}$ is a valuation ring, called the valuation ring of $||$, $M_{||}$ its maximal ideal, and so $\mathbb{F}_{||} = R_{||}/M_{||}$ is a field, called the residue field of $||$.

Exercices 2. Let p be a prime integer and $||$ the p-adic absolute value of $\mathbb{Q}$, defined by $|a| = p^{-\nu_p(a)}$ for every $a \in \mathbb{Z}$, where $\nu_p(a)$ is the greatest integer satisfying $p^{\nu_p(a)}$ divides a for $a \neq 0$ and $\nu_p(0) = \infty$.

1. Show that $(\mathbb{Q}, ||)$ is a non archimidean valued field.

2. Determine the characteristic elements of $||$.

Exercices 3. Let $(K, ||)$ be a non archimidean valued field.

1. Show that $\Gamma = |K^*|$ is a sub-group of $(\mathbb{R}^*, .)$, called the value group of $||$.

2. For every polynomial $A = \sum_{i=0}^{n} a_i x^i \in K[x]$, let $|A|_\infty = \max\{|a_i|, i = 0, \dots, n\}$. Show that, extended by $|A/B|_\infty = |A|_\infty / |B|_\infty$ for every $(A, B) \in K[x]^2$ with $B \neq 0$, $||_\infty$ define an absolute value on $K(x)$ called the Gauss's extension of $||$.

3. For every polynomial $P = \sum_{i=0}^{n} p_i(x)\phi^i \in K[x]$, let $|P|_\phi = \max\left\{|p_i|_\infty, i = 0, \dots, n\right\}$. Show that, extended by $|A/B|_\phi = |A|_\phi / |B|_\phi$ for every $(A, B) \in K[x]^2$ with $B \neq 0$, $||_\phi$ define an absolute value on $K(x)$.

2.4 Completion and henselization

Let $(K, ||)$ be a valued field and consider the map $d : K \times K \to \mathbb{R}_{\geq 0}$, defined by $d(a, b) = |a - b|$. Then d is a metric on K.

Definition 1. A sequence $(u_n) \in K^{\mathbb{N}}$ is said to be a Cauchy sequence if for every positive real number ε, there exists an integer N such that for every natural numbers $m, n \geq N$, we have $|u_n - u_m| \leq \varepsilon$.

Example 1.

Any convergente sequence of $(K, ||)$ is a Cauchy sequence.

The converse is false, indeed, it suffices to consider the valued field $(\mathbb{Q}, ||_0)$ with $||_0$ is the usual absolute value of $\mathbb{Q}$ and $u_n = 1 + 1/1! + \dots + 1/n!$ for every natural integer n. Then (u_n) is a Cauchy sequence, which is not convergente.

Definition 2. A valued field $(K, ||)$ is said to be complete if every Cauchy sequence of $(K, ||)$ is convergente.

Example 2.

1. $(\mathbb{R}, ||_0)$ is a complete valued field.

2. $(\mathbb{Q}, ||_0)$ is not a complete valued field.

Definition 3. Let $(K, ||)$ be a valued field, L/K an extension of fields, and $||_L$ an absolute value of L.

1. We say that $||_L$ extends $||$ if $||_L$ and $||$ coincide on K. In this case $(L, ||_L)/(K, ||)$ is called a valued field extension.

2. Let $(L, ||_L)/(K, ||)$ be a valued field extension and $\Delta = |L^*|_L$. Then $e = |\Delta/\Gamma|$ the cardinal order of Δ/Γ, is called the ramification index of the extension and $f = [\mathbb{F}_{||_L} : F_{||}]$ is called its residue degree.

Definition 4. Let $(K_1, ||_1)$ and $(K_2, ||_2)$ be two valued fields and$f : K_1 \to K_2$ be an isomorphism of fields.f is said to be an isomorphism of valued fields if it preserves the absolute values.

Exercices 4. Let $(L, ||_L)/(K, ||)$ be a valued field extension.

1. Show that if $||$ is a non archimidean absolute value, then $||_L$ is a non archimidean absolute value.

2. Assume that $(K, ||)$ is a non archimidean valued field. Show that the convergence of a series in K is equivalent to the convergence of its general term to 0.

3. Let $\Gamma = |K^*|$ and $\Delta = |L^*|_L$. Show that if Γ is a discrete rank one Abelian group and L/K is a finite extension, then Δ is a discrete rank one Abelian group and $[L : K] = ef$, where e is the ramification index of the extension and$f$ is its residue degree.

Theorem 2.5. ([16], Theorem 1.1.4)

There exists a complete valued field $(L, ||_L)$*, which extends* $(K, ||)$.

Definition 5. The smallest complete valued field extending $(K, ||)$ is called the completion of $(K, ||)$ and denoted by $\hat{K}$.

Furtheremore, the completion is unique up to a valued fields isomorphism.

Now we come to an important property of complete fields. This theorem is widely known as Hensel's Lemma. For the proof, we refer to ([16], Lemma 4.1.3).

Theorem 2.6. (*Hensel's lemma*)

Let$f \in R_{||}[x]$ *be a monic polynomial such that* $\overline{f(x)} = g_1(x)g_2(x)$ *in* $\mathbb{F}_{||}[x]$ *and*$g_1(x)$ *and* $g_2(x)$ *are coprime in* $\mathbb{F}_{||}[x]$*. If* $(K, ||)$ *is a complete valued field valued field, then there exists two monic polynomials* $f_1(x)$ *and* $f_2(x)$ *in* $R_{||}[x]$ *such that*$\overline{f}_1(x) = g_1(x)$ *and*$\overline{f}_2(x) = g_2(x)$.

The following example shows that for any prime integer p, Hensel's lemma is not applicable in $(\mathbb{Q}, ||)$, with $||$ is the p-adic absolute value defined by $|a| = p^{-\nu_p(a)}$. Indeed, let q be a prime integer which is coprime to p, $n \geq 2$ an integer, and$f(x) = x^n + qx + pq \in Z[x]$. First$\overline{f}(x) = x(x^{n-1} + q)$ in $\mathbb{F}_{||}[x]$. As$f(x)$ is q-Eisenstein$f(x)$ is irreducible over $\mathbb{Q}$. Thus, we conclude that Hensel's lemma is not applicable in $(\mathbb{Q}, ||)$.

Definition 6. A valued field $(K, ||)$ is said to be Henselian if Hensel's lemma is applicable in $(K, ||)$. The smallest Henselian field extending $(K, ||)$ is called the henselization of $(K, ||$ and denoted by K^h.

Exercices 5. Let $(K, ||)$ be a valued field $(K, ||)$.

Show that $K \subset K^h \subset \hat{K}$. Furthermore, these three fields have the same value group and same residue fields.

We have the following apparently easier characterization of Henselian fields. For the proof, we refer to ([16], Lemma 4.1.1).

Theorem 2.7. *The valued field* $(K, ||)$ *is Henselian if and only if it extends uniquely to* K^s, where K^s is the separable closure of K.

In particular, we conclude the following characterization of the henselization K^h of $(K, ||)$.

Theorem 2.8. *Let* $(K, ||)$ *be a valued field. Then* K^h *is the separable closure of* K *in* K^s.

3. Main results

Let $(K, ||)$ be a non archimidean valued field, ν the associated valuation to $||$ defined by $\nu(a) = -Ln|a|$ for every $a \in K^*$, $R_{||}$ its valuation ring, $M_{||}$ its maximal ideal, $\mathbb{F}_{||}$ its residue field, and $\left(K^h, \nu^h\right)$ its henselization.

3.1 Key polynomials

The notion of key polynomials was introduced in 1936, by MacLane [17], in the case of discrete rank one absolute values and developed in [18] by Vaquié to any arbitrary rank valuation. The motivation of introducing key polynomials was the problem of describing all extensions of $||$ to any finite simple extension $K(\alpha)$. For any simple algebraic extension of K, MacLane introduced the notions of key polynomials and augmented absolute with respect to the gievn key.

Definition 7. Two nonzero polynomials f and g in $R_{||}[x]$,

1. f and g are said to be $||$-equivalent if $|f-g|_\infty < |f|_\infty$.

2. We say that g is $||$-divides f if there exists $q \in R_{||}[x]$ such that f and gq are $||$-equivalent.

3. We say that a polynomial $\phi \in R_{||}[x]$ is $||$-irreducible if for every f and g in $R_{||}[x]$, ϕ $||$-divides fg implies that ϕ $||$-divides f or ϕ $||$-divides g.

Definition 8. A polynomial $\phi \in R_{||}[x]$ is said to be a MacLane-Vaquié key polynomial of $||$ if it satisfies the following three conditions:

1. ϕ is monic,

2. ϕ is $||$-irreducible,

3. ϕ is $||$-minimal; for every nonzero polynomial $f \in R_{||}[x]$, ϕ $||$-divides f implies that $\deg(\phi) \le \deg(f)$.

It is easy to prove the following lemma:

Lemma 3.1. *Let $\phi \in R_{||}[x]$ be a monic polynomial. If $\overline{\phi}$ is irreducible over $\mathbb{F}_{||}$, then ϕ is a MacLane-Vaquié key polynomial of $||$.*

3.2 Augmented absolute values

Let $\phi \in R_{||}[x]$ be a MacLane-Vaquié key polynomial of $||$ and $\gamma \in \mathbb{R}^+$ with $\gamma \le |\phi|_\infty$. Let $\omega : K(x) \to \mathbb{R}_{\ge 0}$, defined by $\omega(P) = \max\left\{|p_i|_\infty \gamma^i, i = 0, \ldots, l\right\}$ for every $P \in K[x]$, with $P = \sum_{i=0}^{l} p_i \phi^i$ and $\deg(p_i) < \deg(\phi)$ for every $i = 0, \ldots, l$ and extended by $\omega(A/B) = \omega(A) - \omega(B)$ for every nozero A and B of $K(x)$.

Lemma 3.2 *Let $P = \sum_{i=0}^{n} b_i \phi^i$ be a ϕ-expansion of P, where the condition $deg(b_i) < deg(\phi)$ for every $i = 0, \ldots, n$ is omitted. If $\overline{\phi}$ does not divide $\overline{b_i(x)/b}$ for every $i = 0, \ldots, n$, then $\omega(P) = max\left\{|b_i|_\infty \gamma^i, i = 0, \ldots, n\right\}$, where $b \in R_\nu$ such that $|b_i|_\infty = |b|$. Such an expansion is called an admissible expansion.*

Theorem 3.3. *Let $\phi \in R_{||}[x]$ be MacLane-Vaquié key polynomial of $||$ and $\gamma \in \mathbb{R}^+$ with $\gamma \le |\phi|_\infty$. The map $\omega : K(x) \to \mathbb{R}_{\ge 0}$, defined by $\omega(P) = max\left\{|p_i|_\infty \gamma^i, i = 0, \ldots, l\right\}$*

for every $P \in K[x]$, *with* $P = \sum_{i=0}^{l} p_i \phi^i$ *and* $deg(p_i) < deg(\phi)$ *for every* $i = 0, \dots, l$, *and extended by* $\omega(A/B) = \omega(A)/\omega(B)$ *for every nonzero polynomials* $(A, B) \in K[x]^2$, *is an absolute value of* $K(x)$.

Proof. It suffices to check that ω satisfies the three proprieties of an absolute value in $K[x]$. Let $(A, B) \in K[x]$ be tow polynomials, $A = \sum_{i=0}^{k} a_i \phi^i$, and $B = \sum_{i=0}^{s} b_i \phi^i$ the ϕ-expansions.

1. $\omega(A) = 0$ if and only if $|a_i|_\infty \gamma^i = 0$ for every $i = 0, \dots, k$, which means $|a_i|_\infty = 0$ for every $i = 0, \dots, k$ (because $\gamma \in \mathbb{R}^+$). Therefore $A = 0$.

2. Let $A = \sum_{i=0}^{l} a_i \phi^i$ and $B = \sum_{i=0}^{t} b_i \phi^i$ be the ϕ-expansions of A and B, with $\deg(a_i) < \deg(\phi)$ and $\deg(b_i) < \deg(\phi)$ for every $i = 0, \dots, sup(l, t)$. For every $i = 0, \dots, L = l + t$, let $c_i = \sum_{j=0}^{i} a_j b_{i-j}$. Then $AB = \sum_{i=0}^{L} c_i \phi^i$. For every $i = 0, \dots, L$, upon the Euclidean division, let $c_i = q_i \phi + r_i$. Then $AB = \sum_{i=0}^{L} f_i \phi^i$ is the ϕ-expansion of AB, where $f_i = r_i + q_{i-1}$ with $q_{-1} = 0$. Since $|\phi|_\infty = 1$, we conclude that $|r_i|_\infty \le |c_i|_\infty$ and $|q_i|_\infty \le |c_i|_\infty$ for every $i = 0, \dots, L$. Let i_1 and i_2 be the smallest integers satisfying $\omega(A) = |a_{i_1}|_\infty \gamma^{i_1}$ and $\omega(B) = |b_{i_2}|_\infty \gamma^{i_2}$. Then by the ultra-metric propriety $\omega(c_i \phi^i) \le |a_{i_1}|_\infty \gamma^{i_1} |b_{i_2}|_\infty \gamma^{i_2}$ for every $i = 0, \dots, L$. For the equality, by definition of i_1 and i_2, $\omega(a_{i_1} b_j \phi^{i_1+j}) < |a_{i_1} b_j|_\infty \gamma^{i_1+j}$ for every $j < i_2$ and $\omega(a_j b_{i_2} \phi^{j+i_2}) < |a_j b_{i_2}|_\infty \gamma^{j+i_2}$ for every $j < i_1$. Thus by using the expression of $c_{i_1+i_2}$, we conclude the equality. For $i = i_1 + i_2$, let $(a, b) \in R_\nu^2$, with $|a_{i_1}|_\infty = |a|$ and $|b_{i_2}|_\infty = |b|$. If $|r_i|_\infty < |c_i|_\infty = |ab|$, then $|r_i/c|_\infty < |c_i/c|_\infty$, and so $|r_i/c|_\infty < 1$. By reducing modulo $M_{||}$, we deduce that $\overline{\phi}$ divides $\overline{c_i/c}$, which means that ϕ $||$-divides $(a_{i_1}/a)(b_{i_2}/b)$, which is impossible because ϕ is MacLane-Vaquié key polynomial of $||$, ϕ does not $||$-divide a_{i_1}/a, and ϕ does not $||$-divide $b_{i_2})/b$. Therefore, $|r_i|_\infty = |c_i|_\infty$. Hence $\omega(AB) = \max\{|a_i|_\infty \gamma^i, i = 0, \dots, l\} \cdot \max\{|b_i|_\infty \gamma^i, i = 0, \dots, t\}$ and $\omega(AB) = \omega(A)\omega(B)$ as desired.

3. Completing by zeros; $a_i = 0$ if $i > k$ and $b_i = 0$ if $i > s$, we have $\omega(A + B) = \max\{|a_i + b_i|_\infty \gamma^i, i = 0, \dots, \sup(k, s)\} \le \max\{|a_i|_\infty \gamma^i, i = 0, \dots, k\} + \max\{|b_i|_\infty \gamma^i, i = 0, \dots, s\} = \omega(A) + \omega(B)$. Thus, $\omega(A + B) \le \omega(A) + \omega(B)$.

□

Definition 9. The absolute value ω defined in Theorem 3.3 is denoted by $[||\phi, \gamma,]$ and called the augmented absolue value of $||$ associated to ϕ and γ.

Example 3. Let $|||$ be the 2-adic absolute value defined on $\mathbb{Q}$ by $|a| = e^{-\nu_2(a)}$, where for every integer b, $\nu_2(b)$ is the largest integer satisfying 2^k divides b in $\mathbb{Z}$. Let $\phi = x^2 + x + 1 \in \mathbb{Z}[x]$. By Lemma 3.1, ϕ is a MacLane-Vaquié key polynomial of $||$. Since $|\phi|_\infty = 1$, for every real γ, $0 < \gamma \le 1$, the map $\omega : \mathbb{Q}(x) \to \mathbb{R}_{\ge 0}$, defined by $\omega(P(\alpha)) = \max\{|p_i|_\infty \gamma^i, i = 0, \dots, l\}$ for every $P \in K[x]$, with $P = \sum_{i=0}^{l} p_i \phi^i$ and $\deg(p_i) < 2$.

3.3 Extensions of absolute values

The following Lemma makes a one–one correspondence between the absolute value of L and monic irreducible factors of $f(x)$ in $K^h[x]$ for any simple finite extension $L = K(\alpha)$ of K generated by a root $\alpha \in \overline{K}$ of a monic irreducible polynomial $f(x) \in K[x]$.

Lemma 3.4. ([19], Theorem 2.1)

Let $L = K(\alpha)$ generated by a root $\alpha \in \overline{K}$ of a monic irreducible polynomial $f(x) \in K[x]$ and $f(x) = \prod_{i=1}^{t} f_i^{e_i}(x)$ be the factorization into powers of monic irreducible factors of $K^h[x]$. Then $e_i = 1$ for every $i = 1, \ldots, t$ and there are exactly t distinct valuations $||_1, \ldots,$ and $||_t$ of L extending $||$. Furthermore for every absolute value $||_i$ of L associated to the irreducible factor f_i, $|P(\alpha)|_i = \overline{|P(\alpha_i)|}$, where $\overline{||}$ is the unique absolute value of $\overline{K^h}$ extending $||$ and $\alpha_i \in \overline{K}$ is a root of $f_i(x)$.

Lemma 3.5. ([16], Corollary 3.1.4)

Let L/K be a finite extension and R_L the integral closure of $R_{||}$ in L. Then

$$R_L = \cap_{||_L} R_{||_L};$$

for any elemnt $\alpha \in L$, $\alpha \in R_L$ if and only if $|\alpha|_L \leq 1$ for every absolute value $||_L$ of L extending $||$.

Lemma 3.6. *Let $f(x) \in R_{||}[x]$ be a monic irreducible polynomial such that $\overline{f(x)}$ is a power of $\overline{\phi}$ in $\mathbb{F}_{||}[x]$ for some monic polynomial $\phi \in R_{||}[x]$, whose reduction is irreducible over $\mathbb{F}_{||}$. Let $L = K(\alpha)$ with $\alpha \in \overline{K}$ a root of $f(x)$. Then for every absolute value $||_L$ of L extending $||$, for every nonzero polynomial $P \in K[x]$, $|P(\alpha)|_L \leq |P|_\infty$.*

The equality holds if and only if $\overline{\phi}$ does not divide $\overline{P_0}$, where $P_0 = \frac{P}{a}$, with $a \in K$ such that $|P|_\infty = |a|$.

In particular, $|\phi(\alpha)|_L < 1$ and $|P(\alpha)|_L = |P|_\infty$ for every polynomial $P \in K[x]$ such $deg(P) < deg(\phi)$.

Proof. Let $||_L$ be an absolute value of L extending $||$, $P \in K[x]$ a nonzero polynomial, and $a \in K$ with $|a| = |P|_\infty$. Then $|P_0|_\infty = 1$. Since α is integral over $R_{||}$, we conclude that $|P_0(\alpha)|_L \leq 1$. Thus, $|P(\alpha)|_L \leq |a| = |P|_\infty$.

Moreover, the inequality $|P(\alpha)|_L < |P|_\infty$ means that $P_0(\alpha) \in M_{||_L}$, which means that $P_0(\alpha) \equiv 0 \pmod{M_{||_L}}$. Consider the ring homomorphism $\varphi : \mathbb{F}_{||}[x] \to \mathbb{F}_{M_{||_L}}$, defined by $\varphi(\overline{P}) = P(\alpha) + M_{||_L}$. Then $P_0(\alpha) \not\equiv 0 \pmod{M_{||_L}}$ is equivalent to $\overline{\phi}$ does not divide $\overline{P_0}$.

In particular, since $\phi \in R_{||}[x]$, $|\phi|_\infty \leq 1$. Furthermore as $\overline{\phi}$ divide $\overline{\phi}$, we conclude that $|\phi|_\infty < 1$.

Let $P \in K[x]$ be a nonzero polynomial of degree less than degree of ϕ. Then $P_0(x) \in R_{||}[x]$ is a primitive polynomial; $|P_0|_\infty = 1$. As degree $\overline{P}_0$ is less than degree of $\overline{\phi}$, $\overline{\phi}$ does not divide $\overline{P_0}$. Thus $|P(\alpha)|_L = |P|_\infty$. □

Theorem 3.7. *Let $f(x) \in R_{||}[x]$ be a monic polynomial. If $f(x)$ is irreducible over K^h, then $\overline{f(x)}$ is a power of $\overline{\phi}$ in $\mathbb{F}_{||}[x]$ for some monic polynomial $\phi \in R_{||}[x]$, whose reduction is irreducible over $\mathbb{F}_{||}$. Moreover if we set $f(x) = \sum_{i=0}^{n} a_i(x)\phi^i(x)$ the ϕ-expansion of $f(x)$, then $|a_{n-i}|_\infty \leq \gamma^i$ for every $i = 0, \ldots, n$, where $\gamma = |a_0|_\infty^{1/n}$.*

Proof. The first point of the theorem is an immediate consequence of Theorem 2.6. For the second point, let $m = \deg(\phi)$.

1. For $m = 1$, let $f(x) = \prod_{i=1}^{k}(x - \alpha_i)$, where $\alpha_1, \ldots, \alpha_k$ be the roots of $f(x)$ in $\overline{K}$, the algebraic closure of K. Then the formula linking roots and coefficients of $f(x)$, we conclude that $f(x) = \sum_{i=0}^{k} s_i x^i$, where $s_k = 1$, $s_i = \sum \prod_{j_1 < \ldots < j_i} \alpha_{j_1} \cdots \alpha_{j_i}$. Keep the notation $||$ for the valuation of K^h extending $||$ and let $\overline{||}$ be the unique extension of $||$ to $\overline{K^h} = \overline{K}$. Then $\overline{|\alpha_1|} = \ldots = \overline{|\alpha_k|} = \tau$, $\overline{|s_{k-i}|} \leq \tau^i$, and $\tau = \gamma$.

2. For $m \geq 2$, let $Ł = K^h(\alpha)$, where $\alpha \in \overline{K}$ is a root of $f(x)$, $g(x) = x^t + b_{t-1}x^{t-1} + \ldots + b_0$ the minimal polynomial of $\phi(\alpha)$ over K^h, and $F(x) = g(\phi(x)) = \phi(x)^t + b_{t-1}\phi(x)^{t-1} + \ldots + b_0$. By the previous case, we conclude that $|b_{t-i}| \leq \tau^i$ for every $i = 0, \ldots, t$ with $\tau = |b_0|^{1/t}$, which means that $N_\phi(F) = S$ has a single side of slope $-\lambda = -\frac{\nu(b_0)}{t}$. Since $F(\alpha) = 0$, we conclude that $f(x)$ divides $F(x)$, and so $N_\phi(f)$ has a single side of the same slope $-\lambda$. Therefore, $|a_{n-i}|_\infty \leq \gamma^i$ for every $i = 0, \ldots, n$, where $\gamma = |a_0|_\infty^{1/n}$.

□

Exercices 6. Let $(K, ||)$ be a non archimidean valued field and $f(x) \in K^h[x]$. Set $f(x) = \sum_{i=0}^n a_i(x)\phi^i(x)$ the ϕ-expansion of $f(x)$.

Show that $|f(x)|_\infty = \max(|a_n|_\infty, |a_0|_\infty)$.

Based on absolute value, the following theorem gives an hyper bound of the number of monic irreducible factors of monic polynomials. In particular, Corollary 3.9 gives a criterion to test the irreducibility of monic polynomials.

Theorem 3.8. *Let $(K, ||)$ be a non archimidean valued field, $\Gamma = |K^*|$ its value group, and $f(x) \in K[x]$ a monic polynomial such that $\overline{f(x)}$ is a power of $\overline{\phi}$ in $\mathbb{F}_{||}[x]$. Let $f(x) = \sum_{i=0}^n a_i(x)\phi^i(x)$ be the ϕ-expansion of $f(x)$ and assume that $|a_{n-i}|_\infty \leq \gamma^i$ for every $i = 0, \ldots, n$, where $\gamma = |a_0|_\infty^{1/n}$. Let e be the smallest positive integer satisfying $\gamma^e \in \Gamma$. Then $f(x)$ has at most d irreducible monic factors in $K^h[x]$, where $d = n/e$ with degree at least em each, and $m = deg(\phi)$.*

Proof. By applying the map $-Ln$, the hypothesis $|a_{n-i}|_\infty \leq \gamma^i$ for every $i = 0, \ldots, n$ means that $\nu(a_{n-i}) \geq i\lambda$, where $\lambda = \frac{\nu(a_0)}{n}$, which means that $N_\phi(f) = S$ has a single side of slope $-\lambda$ with respect to ν. Let $f(x) = \prod_{i=1}^t f_i(x)$ be a non trivial factorization of monic polynomials in $K^h[x]$. Then by Theorem 2.2, $N_\phi(f_i) = S_i$ has a single side of slope $-\lambda$. Fix $i = 1, \ldots, t$ and let $f_i(x) = \sum_{j=0}^{l_i} a_{ij}(x)\phi^j$ be the ϕ-expansion of f_i. Then $\deg(f_i) = l_i m$ and $-Ln(\gamma) = -\lambda$ is the slope of S_i. Since e is the smallest positive integer satisfying $\gamma^e \in \Gamma$, we conclude that e is the smallest positive integer satisfying $e\lambda \in \nu(K^*)$. On the other hand, since $\lambda = \frac{a_{i0}}{l_i}$ is the slope of S_i, where l_i is the length of the side S_i, we conclude that e divides l_i. Thus $\deg(f_i) = d_i em$, where $d_i = \frac{l_i}{e}$. It follows that every non trivial factor $f_i(x)$ has degree at least em. Since $\deg(f) = \sum_{i=1}^t \deg(f_i) \geq tem$, we conclude that $t \leq \frac{n}{e} = d$. □

Corollary 3.9. *Under the hypothesis and notations of Theorem 3.8, if $e = n$, then $f(x)$ is irreducible over K^h.*

Proof. If $n = e$, then $d = 1$, and so there is a unique monique polynomial of $K[x]$ which divides $f(x)$ and this factor has the degree at least mn. As $\deg(f) = nm$, we conclude that $f(x)$ is this unique monic factor. □

Theorem 3.10. *Let $L = K(\alpha)$ be a simple extension generated by $\alpha \in \overline{K}$ a root of a monic irreducible polynomial $f(x) \in R_{||}[x]$ such that $\overline{f(x)} = \overline{\phi}^n$ in $\mathbb{F}_{||}[x]$. Let $f(x) = \sum_{i=0}^n a_i(x)\phi^i(x)$ be the ϕ-expansion of $f(x)$. Assume that $|a_{n-i}|_\infty \leq \gamma^i$ for every $i = 0, \ldots, n$, where $\gamma = |a_0|_\infty^{1/n}$. Then for every absolute value $||_L$ of L extending $||$, $|P(\alpha)|_L \leq max\left\{|p_i|_\infty \gamma^i, i = 0, \ldots, l\right\}$ for every $P \in K[x]$, with $P = \sum_{i=0}^l p_i\phi^i$ and $l < n$.*

Proof. Let $||_L$ be an absolute value of L extending $||$ and let us show that $|\phi(\alpha)|_L = \gamma$. For this reason, let $\tau = |\phi(\alpha)|_L$. By Lemma 3.6, $0 < \tau < 1$. By hypotheses and Lemma 3.6, $\left|a_i(\alpha)\phi(\alpha)^i\right|_L \le \gamma^{n-i}\tau^i$ for every $i = 0, \dots, n$. Thus, if $\tau \neq \gamma$, $\max\left\{\left|a_i(\alpha)\phi(\alpha)^i\right|_L, i = 0, \dots, n\right\} = \max(\tau^n, \gamma^n)$. Since $||$ is a non archimidean absolute value, we conclude that $||_L$ is a non archimidean absolute value, and so by the ultra-metric propriety, $|f(\alpha)|_L = \max(\tau^n, \gamma^n) > 0$, which is impossible because $f(\alpha) = 0$. Therefore $|\phi(\alpha)|_L = \gamma$.

Now, let $P = \sum_{i=0}^{l} p_i\phi^i$ be a polynomial in $K[x]$. By the ultra-metric propriety, $|P(\alpha)|_L \le \left|p_i(\alpha)\right|_L \gamma^i$. □

Theorem 3.11. *Let $L = K(\alpha)$ be a simple extension generated by $\alpha \in \overline{K}$ a root of a monic irreducible polynomial $f(x) \in R_{||}[x]$ such that $\overline{f(x)} = \overline{\phi}^n$ in $\mathbb{F}_{||}[x]$. Let $f(x) = \sum_{i=0}^{n} a_i(x)\phi^i(x)$ be the ϕ-expansion of $f(x)$. Assume that $|a_{n-i}|_\infty \le \gamma^i$ for every $i = 0, \dots, n$, where $\gamma = |a_0|_\infty^{1/n}$. If n is the smallest positive integer satisfying $\gamma^e \in \Gamma$, then there is a unique absolute value $||_L$ of L extending $||$. Moreover this absolute value is defined by $|P(\alpha)|_L = max\left\{\left|p_i\right|_\infty \gamma^i, i = 0, \dots, l\right\}$ for every $P \in K[x]$, with $P = \sum_{i=0}^{l} p_i\phi^i$ and $l < n$.*

Furthermore, its ramification index is n and its residue degree is $m = deg(\phi)$.

Proof. By Corollary 3.9, if $n = e$, then $f(x)$ is irreducible over K^h. Thus by Hensel's Lemma, there is a unique absolute value $||_L$ of L extending $||$. By Theorem 3.10, we conclude that $|\phi(\alpha)|_L = \gamma$ and $|P(\alpha)|_L \le \left|p_i(\alpha)\right|_L \gamma^i = \left|p_i\right|_\infty$ for every polynomial $P = \sum_{i=0}^{l} p_i\phi^i$ in $K[x]$. Let us show the equality. Let s be the smallest integer which satisfies $\omega(P) = \left|p_s\right|_\infty \gamma^s$. Let i be an integer satisfying $\omega(P) = \left|p_i\right|_\infty \gamma^i$. Then $\gamma^{s-i} = \left|p_i\right|_\infty / \left|p_s\right|_\infty \in \Gamma$. Thus n divides $i - s$ because n is the smallest positive integer satisfying $\gamma^e \in \Gamma$. Since $l < n$, then $i - s = 0$. Therefore, $|P(\alpha)|_L = \left|p_s\right|_\infty \gamma^s = \omega(P)$.

For the residue degree and ramification index, since $|\phi(\alpha)|_L = \gamma$ and $n = (\Gamma(\gamma) : \Gamma)$, we conclude that n divides the ramification index e of $||_L$. On the other hand, since $\mathbb{F}_{||} \subset \mathbb{F}_\phi \subset \mathbb{F}_{||_L}$, with $\mathbb{F}_\phi = \frac{\mathbb{F}_{||}[x]}{(\overline{\phi})}$, we have $m = \left[\mathbb{F}_\phi : \mathbb{F}_{||}\right]$ divides $\left[\mathbb{F}_{||_L} : \mathbb{F}_{||}\right]$. As $m \cdot n = \deg(f)$, we conclude the equality. □

Exercices 7. For every positive integer $n \ge 2$ and p a positive prime integer, let $f(x) = x^n - p$.

1. How that f is irreducible over $\mathbb{Q}$.

2. Conclude a new proof for $[\mathbb{R} : \mathbb{Q}] = \infty$.

3. Let $L = \mathbb{Q}(\alpha)$ with α a complex root of $f(x)$. Show that there is a unique absolute value of L extending the absolute $||_p$, defined on $\mathbb{Q}$ by $|a|_p = e^{-\nu_p(a)}$ for every $a \in \mathbb{Q}$, where ν_p is the p-adic valuation on $\mathbb{Q}$. Calculate its residue degree and its ramification index.

Combining Lemma 3.4 and Theorem 3.8, we conclude the following result:

Corollary 3.12. *Let $L = K(\alpha)$ be a simple extension generated by $\alpha \in \overline{K}$ a root of a monic irreducible polynomial $f(x) \in R_{||}[x]$. Let $\overline{f(x)} = \prod_{i=1}^{r} \overline{\phi_i}^{n_i}(x)$ be the factorization of $\overline{f(x)}$ in $\mathbb{F}_{||}[x]$, with every $\phi_i \in R_{||}[x]$ is a monic polynomial. For every $i = 1, \dots, r$, let $N_{\phi_i}^{+}(f) = S_{i1} + \dots + S_{ig_i}$ be the principal ϕ_i-Newton polygon of $f(x)$. Then L has t absolue value extending $||$ with $r \le t \le \sum_{i=1}^{r}\sum_{j=1}^{g_i} d_{ij}$, where $d_{ij} = \frac{l_{ij}}{e_{ij}}$ is the degree of S_{ij}, l_{ij} is the length of S_{ij}, and $e_{ij} = \frac{l_{ij}}{d_{ij}}$ for every $i = 1, \dots, r$ and $j = 1, \dots, g_i$.*

4. Applications

1. Let $||$ be the p-adic absolute value defined on $\mathbb{Q}$ by $|a| = p^{-\nu_p(a)}$ and $f(x) = x^n - p\mathbb{Z}[x]$. Show that $f(x)$ is irreducible over $\mathbb{Q}$. Let $L = \mathbb{Q}(\alpha)$ with α a complex root of $f(x)$. Determine all absolute value of L extending $||$.

   Answer. First $\varGamma = \{p^k, k \in \mathbb{Z}\}$ is the value group of $||$. Since $|p| = p^{-1}$, $\gamma = |a_0|^{1/n} = p^{-1/n}$, we conclude that the smallest integer satisfying $\gamma^e \in \Gamma$ is n. Thus, by Corollary 3.9, $f(x)$ is irreducible over $\mathbb{Q}^h$,and so is over $\mathbb{Q}$. Since $\overline{f(x)} = x^n$ in $\mathbb{F}_p[x]$, by Theorem 3.11, there is a unique absolute value of L extending $||$ and it is defined by $|P(\alpha)|_L = \max\{|p_i|\gamma^i, i = o, \dots, l\}$ for every polynomial $P = \sum_{i=0}^{l} x^i$ with $l < n$.

2. Let $||$ be the p-adic absolute value and $f(x) = x^{n^{-a}} \in \mathbb{Z}[x]$ such that p does not divide $\nu_p(a)$. Show that $f(x)$ is irreducible over $\mathbb{Q}$. Let $L = \mathbb{Q}(\alpha)$ with α a complex root of $f(x)$. Determine all absolute value of L extending $||$.

   Answer. First $\varGamma = \{p^k, k \in \mathbb{Z}\}$ is the value group of $||$. Since $|p| = p^{-1}$, $\gamma = |a_0|^{1/n} = p^{-1/n}$, we conclude that the smallest integer satisfying $\gamma^e \in \Gamma$ is n. Thus, by Corollary 3.9, $f(x)$ is irreducible over $\mathbb{Q}^h$,and so is over $\mathbb{Q}$. Since $\overline{f(x)} = x^n$ in $\mathbb{F}_p[x]$, by Theorem 3.11, there is a unique absolute value of L extending $||$ and it is defined by $|P(\alpha)|_L = \max\{|p_i|\gamma^i, i = o, \dots, l\}$ for every polynomial $P = \sum_{i=0}^{l} x^i$ with $l < n$.

3. Let $f(x) = \phi^6 + 24x\phi^4 + 24\phi^3 + 15(16x + 32)\phi + 48$ with $\phi \in \mathbb{Z}[x]$ a monic polynomial whose reduction is irreducible in $\mathbb{F}_2[x]$. In $\mathbb{Q}_2[x]$, how many monic irreducible factors $f(x)$ gets?, where $\mathbb{Q}_2$ is the completion of $(\mathbb{Q}, ||)$ and $||$ is the 2-adic absolute value.

   Answer. It is easy to check that $f(x)$ satisfies the conditions of Theorem 3.8; $|a_{6-i}|_\infty \le \gamma^i$ with $\gamma = 2^{-4/6} = \left(2^{-1/3}\right)^2$. Thus $e = 3$ and $d = 2$. By Theorem 3.8, $f(x)$ has at most 2 monic irreducible factors in $\mathbb{Q}_2[x]$.

Author details

Lhoussain El Fadil* and Mohamed Faris
Faculty of Sciences Dhar El Mahraz, Sidi Mohamed ben Abdellah University, Morocco

*Address all correspondence to: lhouelfadil2@gmail.com

References

[1] G. Eisenstein, *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.

[2] K. Girstmair, *On an irreducibility criterion of M. Ram Murty*, Amer. Math. Monthly 112 (2005) 269–270

[3] S. K. Khanduja and M. Kumar, *Prolongations of valuations to finite extensions*, Manus. Math. **131** (2010) 323–334.

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

[5] S. H. Weintraub, *A family of tests for irreducibility of polynomials*, Proc. Amer. Math. Soc. 144 (2016) 3331–3332.

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

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

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

[9] R. Brown, *Roots of generalized Schönemann polynomials in henselian extension fields*, Indian J. Pure Appl. Math. 39(5) (2008) 403–410

[10] A. Deajim and L. El Fadil, *On the extensions of discrete valuations in number fields*, Mathematica Slovaca 69(5) (2019), 1009–1022

[11] L. El Fadil, *On prolongations of rank one discrete valuations*, Comment. Math. Univ. Carolin. 60,3 (2019), 299–304

[12] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.

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

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

[15] L. El Fadil, *On Newton polygon's techniques and factorization of polynomial over henselian valued fields*, J. of Algebra and its Appl. 19(10) (2020) 2050188

[16] J. Engler and A. Prestel, Valued Fields, Springer Berlin Heidelberg New York, 2005.

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

[18] M. Vaquié, Extension d'une valuation, Trans. Amer. Math. Soc. 359 (7) (2007), 3439–3481

[19] A. Deajim, L. El Fadil, and A. Najim, *On a theorem of Dedekind* (arxiv preprint and to appear in Siberian Math. Journal)