HIROSHIMA MATH. J.
34 (2004), 161–176

Irreducibility over valued fields in the presence of a secondary valuation

Alexandru ZAHARESCU

(Received May 6, 2003)
(Revised January 17, 2004)

ABSTRACT. We provide an irreducibility criterion for polynomials in one variable over a valued field K, in the presence of a secondary valuation defined on K.

1. Introduction

The problem of understanding the structure of irreducible polynomials over a local field is simpler than the corresponding problem over a global field. In [6] it is shown how one can construct all the irreducible polynomials in one variable over a local field. This is done with the aid of the so-called saturated distinguished chains of polynomials, introduced in [6] and studied also in [1], [4] and [5]. In this paper we are concerned with an irreducibility criterion for polynomials in one variable over a field equipped with two valuations. A classical fact concerning irreducible polynomials over a field K which is complete with respect to a nonarchimedean absolute value $|.|$, is that if $f(X) = X^d + a_1X^{d-1} + \cdots + a_d \in K[X]$ is irreducible over K, then there exists an $\varepsilon > 0$ such that any polynomial $g(X) = X^d + b_1X^{d-1} + \cdots + b_d \in K[X]$, with $|b_j - a_j| < \varepsilon$ for any $j \in \{1, \ldots, d\}$, is also irreducible over K. A more precise result in this direction is provided by a well known lemma of Krasner. By pursuing this kind of ideas, Krasner (see [3]) computed explicitly the number of extensions of a given degree of a p-adic field. In this paper we present an irreducibility result as above, which is applicable to some valued fields K that are not necessarily complete with respect to the given absolute value. As we shall see, the lack of completeness of the field K is compensated by the existence of a secondary valuation on K, which satisfies a certain property in connection with the given, primary valuation. In Section 2 below we consider the case where $K = K_0(t)$, where K_0 is a finite extension of $\mathbf{Q}_p$ for some prime number p, and t is an indeterminate. By examining this example we identify a certain property, which we then take as a starting point in the more general

2000 *Mathematics Subject Classification*. 11C08, 11S99.
Key words and phrases: valued fields, irreducible polynomials, secondary valuations.

case treated in Section 3. In the last section we consider the case of an algebraic function field of one variable over a p-adic field. It would be interesting to find more instances where properties which are known to hold true for complete fields can be shown to be satisfied by some valued fields which are not necessarily complete, and where the lack of completeness is compensated by the existence of one, or several secondary valuations.

2. The case $K = K_0(t)$

Let p be a prime number, $\mathbf{Q}_p$ the field of p-adic numbers, K_0 a finite extension of $\mathbf{Q}_p$, t an indeterminate and $K = K_0(t)$ the field of rational functions in t with coefficients in K_0. Denote by $|.|$ the p-adic absolute value on K_0, normalized by $|p| = \frac{1}{p}$, say. If π_0 is a uniformizing element of K_0 and $e(K_0/\mathbf{Q}_p)$ denotes the ramification index of K_0 over $\mathbf{Q}_p$, then $|\pi_0| = \left(\frac{1}{p}\right)^{1/e(K_0/\mathbf{Q}_p)}$. We consider the Gauss extension of $|.|$ to K. This absolute value, which we continue to denote by $|.|$, is defined as follows. If $P(t) = c_0 t^n + c_1 t^{n-1} + \cdots + c_n$, with $c_0, \ldots, c_n \in K_0$, then

$$|P(t)| = \max_{0 \le j \le n} |c_j|. \tag{2.1}$$

Next, $|.|$ is extended from $K_0[t]$ to K by multiplicativity, thus if $r(t) = \frac{P(t)}{Q(t)} \in K$ with $P(t), Q(t) \in K_0[t]$, then

$$|r(t)| = \frac{|P(t)|}{|Q(t)|}. \tag{2.2}$$

Note that K is not complete with respect to the absolute value $|.|$. We now take a polynomial in one variable

$$f(X) = X^d + a_1 X^{d-1} + \cdots + a_d, \tag{2.3}$$

with $a_1, \ldots, a_d \in K_0[t]$, such that $f(X)$ is irreducible over K, and approximate $f(X)$ with polynomials

$$g(X) = X^d + b_1 X^{d-1} + \cdots + b_d, \tag{2.4}$$

with $b_1, \ldots, b_d \in K_0[t]$. Suppose that

$$|b_j - a_j| < \varepsilon \qquad \text{for any } j \in \{1, \ldots, d\}, \tag{2.5}$$

for a given $\varepsilon > 0$. One can not conclude that for ε small enough, any such polynomial $g(X)$ is irreducible. To see this, consider the following example. Let p be an odd prime and $f(X) = X^2 - (1 + pt)$. For each positive integer m, let

$$g_m(X) = X^2 - \left(\sum_{k=0}^{m} \binom{1/2}{k} p^k t^k\right)^2, \tag{2.6}$$

where

$$\binom{1/2}{k} = \frac{\frac{1}{2}\left(\frac{1}{2}-1\right)\ldots\left(\frac{1}{2}-k+1\right)}{k!}. \tag{2.7}$$

The elements $A_m(t) := \sum_{k=0}^{m} \binom{1/2}{k} p^k t^k \in K_0[t]$ are partial sums of the Taylor series expansion of $\sqrt{1+pt}$. Hence $1 + pt - A_m(t)^2$, as a polynomial in t, has only terms of degree $> m$. These terms are of the form $\binom{1/2}{i}\binom{1/2}{j} p^{i+j} t^{i+j}$ and are small in our absolute value $|.|$ as $(i+j) \to \infty$. Thus $g_m(X)$ approaches $f(X)$ as $m \to \infty$. At the same time, each polynomial $g_m(X)$ is reducible over K, while the limiting polynomial $f(X)$ is irreducible over K.

At this point we would say that this was an expected phenomenon, simply due to the fact that the field K is not complete with respect to the absolute value $|.|$. Observe that in the above example the coefficients of the polynomials $g_m(X)$ are elements of $K_0[t]$ of higher and higher degree as polynomials in t over K_0. Let us then restrict to the case when the irreducible polynomial $f(X)$ given by (2.3) is approximated by polynomials $g(X)$ as in (2.4) and (2.5), with the additional constraint that the degrees of all the coefficients $b_0, \ldots, b_d$, as polynomials in t over K_0, are bounded by a given number D. Then we do have an irreducibility result. For $\varepsilon > 0$ small enough, depending on $K_0, f(X)$ and D, any polynomial $g(X)$ as above is irreducible over K. Indeed, if this fails, then there is a sequence of polynomials $(g_n(X))_{n \in \mathbf{N}}$,

$$g_n(X) = X^d + b_{1,n} X^{d-1} + \cdots + b_{d,n},$$

with $b_{1,n}, \ldots, b_{d,n} \in K_0[t]$, for which

$$|b_{j,n} - a_j| \leq \frac{1}{n}, \tag{2.8}$$

for any $n \in \mathbf{N}$ and any $j \in \{1, \ldots, d\}$, and such that each polynomial $g_n(X)$ is reducible over K. Say

$$g_n(X) = G_n(X) H_n(X),$$

for any $n \in \mathbf{N}$, with $G_n(X), H_n(X) \in K_0[t][X]$, $\deg G_n(X) \geq 1$, $\deg H_n(X) \geq 1$. Restricting if necessary to a subsequence, we may assume that $\deg G_n(X) = r$ is constant. Denote

$$G_n(X) = X^r + C_{1,n} X^{r-1} + \cdots + C_{r,n},$$

where each $C_{j,n}$, $1 \le j \le r$, is a polynomial in t over K_0, of degree at most D,

$$C_{j,n} = c_{j,0,n} + c_{j,1,n}t + \cdots + c_{j,D,n}t^D.$$

If we extend the absolute value $|.|$ to an absolute value, also denoted by $|.|$, on a fixed algebraic closure $\overline{K_0(t)}$ of $K_0(t)$, then from (2.8) we see that the coefficients, and therefore also the roots of all the polynomials $g_n(X)$, are uniformly bounded in the absolute value $|.|$. In particular the roots of the polynomials $G_n(X)$, and thus also their coefficients $C_{j,n}$, are uniformly bounded in the absolute value $|.|$. Since for any j and any n we have

$$|C_{j,n}| = \max_{0 \le s \le D} |c_{j,s,n}|,$$

we deduce that for any $j \in \{1, \ldots, r\}$ and any $s \in \{0, \ldots, D\}$, the sequence $(c_{j,s,n})_{n \in \mathbf{N}}$ is bounded. The field K_0 is locally compact, and so each such sequence has a subsequence which converges in K_0. Therefore there is a subsequence $n_1 < n_2 < \cdots < n_k < \cdots$ for which

$$\lim_{k \to \infty} c_{j,s,n_k} = c_{j,s} \in K_0, \tag{2.9}$$

for $1 \le j \le r$ and $0 \le s \le D$. If we denote

$$C_j = c_{j,0} + c_{j,1}t + \cdots + c_{j,D}t^D,$$

then from (2.9) it follows that

$$\lim_{k \to \infty} C_{j,n_k} = C_j,$$

for $1 \le j \le r$. This means that the sequence of polynomials $(G_{n_k}(X))_{k \in \mathbf{N}}$ converges to the polynomial

$$G(X) := X^r + C_1 X^{r-1} + \cdots + C_r.$$

Similarly, along a subsequence of this sequence, we have that $H_n(X)$ approaches a polynomial $H(X) \in K_0[t][X]$. Then clearly $g_n(X)$ will converge along this last subsequence, to $G(X)H(X)$. Thus $f(X) = G(X)H(X)$, which contradicts our assumption that $f(X)$ is irreducible.

The above familiar reasoning uses two special properties, particular to this situation, namely the fact the ring $K_0[t]$ containing the coefficients of the given polynomial $f(X)$ is a polynomial ring in one variable over a field K_0, and the fact that K_0 is locally compact with respect to the given absolute value $|.|$. We would like to find an alternative way of proving a result as above, assuming less restrictive properties of the rings and absolute values under consideration, and which will then have a larger area of possible applications.

Let us also remark that in the above example we have a second absolute value, namely the one given by the degree of elements from $K_0[t]$ viewed as polynomials in t, whose properties were tacitly used in the proof.

In the next section we consider a more general situation, in which $K_0[t]$ is replaced by a ring A on which we have two absolute values, or, more generally, two valuations v_1 and v_2. The valuation v_1, which we view as the primary valuation, will play the role of the above absolute value $|.|$, and the valuation v_2, which we see as a secondary valuation, will play the role of the degree with respect to t in the above result. Thus the role of the secondary valuation v_2 will be to compensate the lack of completeness of the given field with respect to our primary valuation v_1.

3. An axiomatic treatment

Let K be a field of characteristic zero, equipped with two non-archimedean valuations v_1 and v_2. For general definitions and basic properties of valuations we refer the reader to [7]. For $i = 1, 2$, let O_i denote the valuation ring of v_i, let M_i be the maximal ideal of O_i, and let $k_i = O_i/M_i$, the residue field of v_i. We also denote by Γ_i the value group of the valuation v_i.

Let now A be a subring of K, with field of fractions K, and which is integrally closed in K.

Denote by $\overline{K}$ a fixed algebraic closure of K, and let us fix two valuations $\bar{v}_1$ and $\bar{v}_2$ on $\overline{K}$, which are extensions of the given valuations v_1 and respectively v_2. For $i = 1, 2$, denote by $\overline{O}_i, \overline{M}_i, \overline{k}_i = \overline{O}_i/\overline{M}_i$ and $\overline{\Gamma}_i$ the valuation ring, the maximal ideal of the valuation ring, the residue field, and respectively the value group of the valuation $\bar{v}_i$ on $\overline{K}$.

So far the valuations v_1 and v_2 had a symmetric role. We now introduce a condition which is not symmetric in v_1 and v_2, and from now on we call v_1 the *primary valuation*, and we call v_2 the *secondary valuation* on K.

Denote by $\bar{A}$ the integral closure of A in $\overline{K}$. Since A is integrally closed in K, we have $\bar{A} \cap K = A$.

We introduce the following condition. We require that no element from $\bar{A} \setminus A$ can be approximated, with respect to $\bar{v}_1$, by a (generalized) sequence of elements from A which is bounded with respect to the secondary valuation v_2. Thus, we ask that for any $\alpha \in \bar{A} \setminus A$, and any $\gamma_2 \in \Gamma_2$, there exists an element $\gamma_1 \in \Gamma_1 \subseteq \overline{\Gamma}_1$, such that

$$\bar{v}_1(u - \alpha) \leq \gamma_1, \qquad \text{for any } u \in A \text{ with } v_2(u) \geq \gamma_2. \tag{3.1}$$

Note that (3.1) holds if K is complete with respect to the primary valuation v_1, regardless of the choice of v_2.

Note also that (3.1) holds with K as in the previous section, $K = K_0(t)$, K_0

finite extension of $\mathbf{Q}_p$, $A = K_0[t]$, v_1 the Gauss extension to $K_0(t)$ of the p-adic valuation on K_0, and v_2 defined by

$$v_2\left(\frac{P(t)}{Q(t)}\right) = \deg Q(t) - \deg P(t),$$

for any $P(t), Q(t) \in K_0[t]$, $Q(t) \neq 0$. In this case, (3.1) says that no element $\alpha \in \bar{A} \backslash A$ can be approximated by a sequence of elements from $K_0[t]$ whose degrees with respect to t are uniformly bounded. This happens simply because any sequence of polynomials in t, of bounded degree, with coefficients in K, which is a Cauchy sequence in the Gauss valuation, will converge to an element from $K_0[t] = A$.

Of course, if one would ignore the secondary valuation here and would only ask whether elements $\alpha \in \overline{K_0[t]} \backslash K_0[t]$ can be limits with respect to the Gauss valuation of sequences of elements from $K_0[t]$, we already know that this does happen indeed. We have seen for instance in the previous section that the algebraic function $\alpha = \sqrt{1+pt} \in \overline{K_0[t]} \backslash K_0[t]$ is approximated in the Gauss valuation by the partial sums of its Taylor expansion.

Returning to the general case, let us remark that (3.1) only depends on the ring A, which also determines the field K, and on the two valuations v_1 and v_2 on K, and does not depend on the particular choice of the extension $\bar{v}_1$ of v_1 to $\bar{K}$.

To see this, let us assume that (3.1) holds for a particular extension $\bar{v}_1$ of v_1 to $\bar{K}$, and let us choose any other valuation w on $\bar{K}$, whose restriction to K coincides with v_1. Fix elements $\alpha \in \bar{A} \backslash A$ and $\gamma_2 \in \Gamma_2$. We need to show that there exists an element $\gamma_1 \in \Gamma_1$ such that

$$w(u - \alpha) \leq \gamma_1, \qquad \text{for any } u \in A \text{ with } v_2(u) \geq \gamma_2. \tag{3.2}$$

Let

$$f_\alpha(X) = X^d + c_1 X^{d-1} + \cdots + c_d \in A[X]$$

be the minimal polynomial of α over K, and denote by $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$ the roots of $f_\alpha(X)$ in $\bar{K}$. We apply (3.1), with α replaced by α_i, $1 \leq i \leq d$. It follows that there are elements $\gamma_{1,1}, \ldots, \gamma_{1,d} \in \Gamma_1$ such that

$$\bar{v}_1(u - \alpha_i) \leq \gamma_{1,i}, \tag{3.3}$$

for any $u \in A$ with $v_2(u) \geq \gamma_2$, and any $i \in \{1, \ldots, d\}$. As a consequence,

$$\bar{v}_1(f_\alpha(u)) = \sum_{1 \leq i \leq d} \bar{v}_1(u - \alpha_i) \leq \sum_{1 \leq i \leq d} \gamma_{1,i}, \tag{3.4}$$

for any $u \in A$ with $v_2(u) \geq \gamma_2$. Since for any such $u, f_\alpha(u)$ belongs to A, we have that

$$\bar{v}_1(f_\alpha(u)) = v_1(f_\alpha(u)) = w(f_\alpha(u)) = \sum_{1 \leq i \leq d} w(u - \alpha_i).$$

Therefore,

$$\sum_{1 \leq i \leq d} w(u - \alpha_i) \leq \sum_{1 \leq i \leq d} \gamma_{1,i}. \tag{3.5}$$

On the other hand,

$$\sum_{1 \leq i \leq d} w(u - \alpha_i) \geq w(u - \alpha) + \sum_{2 \leq j \leq d} \min\{w(u - \alpha), w(\alpha - \alpha_j)\}. \tag{3.6}$$

Fix an element $\gamma' \in \Gamma_1$ such that

$$\gamma' \geq w(\alpha - \alpha_j), \tag{3.7}$$

for any $j \in \{2, \ldots, d\}$. We distinguish two cases.

I. If u is such that $w(u - \alpha) \leq \gamma'$, then (3.2) will hold true for such elements u, provided that γ_1 is chosen to be larger than or equal to γ'.

II. If u is such that $w(u - \alpha) \geq \gamma'$, then from (3.6) and (3.7) we obtain

$$\sum_{1 \leq i \leq d} w(u - \alpha_i) \geq w(u - \alpha) + \sum_{2 \leq j \leq d} w(\alpha - \alpha_j). \tag{3.8}$$

Fix an element $\gamma'' \in \Gamma_1$ for which

$$\gamma'' \geq \sum_{1 \leq i \leq d} \gamma_{1,i} - \sum_{2 \leq j \leq d} w(\alpha - \alpha_j). \tag{3.9}$$

By (3.5), (3.8) and (3.9) we find that

$$w(u - \alpha) \leq \gamma'',$$

for any $u \in A$ for which $v_2(u) \geq \gamma_2$ and $w(u - \alpha) \geq \gamma'$.

In conclusion, if we let

$$\gamma_1 := \max\{\gamma', \gamma''\} \in \Gamma_1,$$

then (3.2) will hold true for any $u \in A$ with $v_2(u) \geq \gamma_2$. This shows that the above property (3.1) is independent indeed of the particular choice of the valuation $\bar{v}_1$ on $\overline{K}$ which extends v_1.

We prove the following irreducibility result.

THEOREM 1. *Let K be a field of characteristic zero, equipped with two non-archimedean valuations v_1 and v_2, and let A be a subring of K, with field of fractions K, and which is integrally closed in K. Denote by Γ_1 and Γ_2 the value groups of v_1 and respectively v_2, and assume that* (3.1) *holds true. Then, for any polynomial*

$$f(X) = X^d + a_1 X^{d-1} + \cdots + a_d \in A[X],$$

which is irreducible over K, and for any $\gamma_2 \in \Gamma_2$, there exists $\gamma_1 \in \Gamma_1$ such that, for any $b_1, \dots, b_d \in A$ for which

$$v_1(b_i - a_i) \geq \gamma_1, \qquad 1 \leq i \leq d, \tag{3.10}$$

and

$$v_2(b_i) \geq \gamma_2, \qquad 1 \leq i \leq d, \tag{3.11}$$

the polynomial

$$g(X) = X^d + b_1 X^{d-1} + \cdots + b_d, \tag{3.12}$$

is irreducible over K.

PROOF. Let $\bar{v}_1$ and $\bar{v}_2$ be valuations on $\overline{K}$ whose restrictions to K coincide with v_1 and respectively v_2, and denote by $\overline{\Gamma}_1$ and $\overline{\Gamma}_2$ respectively, the value groups of $\bar{v}_1$ and $\bar{v}_2$.

We first work inside the group $\overline{\Gamma}_2$.

Note first that for any polynomial $g(X)$ as in (3.12), with $b_1, \dots, b_d$ satisfying (3.11), and any root θ of $g(X)$ in $\overline{K}$, we have

$$\begin{aligned} d\bar{v}_2(\theta) = \bar{v}_2(\theta^d) &= \bar{v}_2\left(- \sum_{1 \leq i \leq d} b_i \theta^{d-i} \right) \\ &\geq \min_{1 \leq i \leq d} \{ v_2(b_i) + (d-i)\bar{v}_2(\theta) \} \geq \gamma_2 + \min_{1 \leq i \leq d} \{ (d-i)\bar{v}_2(\theta) \}. \end{aligned}$$

Thus there is an $i \in \{1, \dots, d\}$ for which

$$\bar{v}_2(\theta) \geq \frac{\gamma_2}{i}. \tag{3.13}$$

According as to whether γ_2 is a positive or a negative element of Γ_2, we let $\gamma_2' \in \overline{\Gamma}_2$ be defined by the equality $\gamma_2' = \gamma_2/d$, and respectively by the equality $\gamma_2' = \gamma_2$. Then, in both cases it follows from (3.13) that

$$\bar{v}_2(\theta) \geq \gamma_2', \tag{3.14}$$

for any root θ of any polynomial $g(X)$ as in (3.12), with coefficients $b_1, \dots, b_d$ satisfying (3.11).

Let us also remark that in case such a polynomial $g(X)$ is reducible, say

$$g(X) = G(X)H(X),$$

with $G(X), H(X) \in A[X]$, then from (3.14) one obtains bounds for all the coefficients of $G(X)$ and $H(X)$, with respect to the valuation v_2. More precisely, if

$$G(X) = X^r + C_1X^{r-1} + \cdots + C_r, \tag{3.15}$$

and if $\theta_1, \ldots, \theta_r \in \bar{K}$ are the roots of $G(X)$, then $\bar{v}_2(\theta_j) \geq \gamma_2'$, $1 \leq j \leq r$, and from the expressions of $C_1, \ldots, C_r$ as symmetric functions of $\theta_1, \ldots, \theta_r$, we see that

$$v_2(C_i) \geq i\gamma_2', \qquad 1 \leq i \leq r, \tag{3.16}$$

and similarly for the coefficients of $H(X)$.

We now return to the given polynomial $f(X)$, and apply (3.1) for various symmetric functions of proper subsets of the set of roots of $f(X)$. Thus, if $\alpha_1, \ldots, \alpha_d$ are the roots of $f(X)$ in $\bar{K}$, then for any $r \in \{1, \ldots, d-1\}$, and any subset S of $\{1, \ldots, d\}$ having exactly r elements, we consider the symmetric sums

$$\sigma_{S,1} = \sum_{j \in S} \alpha_j, \qquad \sigma_{S,2} = \sum_{\substack{i,j \in S \\ i<j}} \alpha_i\alpha_j, \ldots, \sigma_{S,r} = \prod_{j \in S} \alpha_j.$$

Clearly, $\sigma_{S,j} \in \bar{A}$, $1 \leq j \leq r$, and if we consider the polynomial $f_S(X) \in \bar{A}[X]$,

$$f_S(X) := X^r - \sigma_{S,1}X^{r-1} + \sigma_{S,2}X^{r-2} + \cdots + (-1)^r\sigma_{S,r},$$

then $f_S(X)$ factors over $\bar{A}$, as

$$f_S(X) = \prod_{j \in S} (X - \alpha_j).$$

Since $f(X)$ was assumed to be irreducible over K, it follows that for $1 \leq r \leq d-1$, and any subset S of $\{1, \ldots, d\}$ having exactly r elements, at least one of the coefficients of $f_S(X)$ belongs to $\bar{A} \backslash A$. For any such S, let us denote by $j_S \in \{1, \ldots, r\}$ the smallest positive integer for which $\sigma_{S,j_S} \in \bar{A} \backslash A$. We now apply (3.1), with α replaced by σ_{S,j_S}, and γ_2 replaced by $j_s\gamma_2'$. It follows that there is an element of Γ_1, call it $\gamma_{1,S}$, for which

$$\bar{v}_1(u - \sigma_{S,j_S}) \leq \gamma_{1,S}, \tag{3.17}$$

for any $u \in A$ with $v_2(u) \geq j_S\gamma_2'$.

We now fix an element $\gamma_1 \in \Gamma_1$. The actual choice of γ_1 will be made explicit later. We will choose γ_1 to be large enough so that it satisfies certain inequalities which will appear in what follows.

Let $g(X)$ be as in (3.12), with $b_1, \dots, b_d$ satisfying (3.10) and (3.11), and let us assume that $g(X)$ is not irreducible over K. Say $g(X) = G(X)H(X)$, with $G(X), H(X) \in A[X]$, $\deg G \geq 1$, $\deg H \geq 1$. Denote by $\theta_1, \dots, \theta_d$ the roots of $g(X)$ in $\overline{K}$. Here we order these roots so that θ_1 is one of the roots of $g(X)$ that are closest to α_1, that is,

$$\bar{v}_1(\theta_1 - \alpha_1) = \max_{1 \leq j \leq d} \bar{v}_1(\theta_j - \alpha_1).$$

After θ_1 is chosen, we denote by θ_2 one of the remaining roots of $g(X)$, which is closest to α_2, so

$$\bar{v}_1(\theta_2 - \alpha_2) = \max_{2 \leq j \leq d} \bar{v}_1(\theta_j - \alpha_2).$$

Then continue in the same way with $\theta_3, \dots, \theta_d$. Thus for any $1 \leq i < j \leq d$ we have that

$$\bar{v}_1(\theta_i - \alpha_i) \geq \bar{v}_1(\theta_j - \alpha_i).$$

For any $i \in \{1, \dots, d\}$, one has

$$\begin{aligned} \sum_{1 \leq j \leq d} \bar{v}_1(\theta_j - \alpha_i) &= \bar{v}_1(g(\alpha_i)) = \bar{v}_1(g(\alpha_i) - f(\alpha_i)) \\ &= \bar{v}_1\left(\sum_{1 \leq s \leq d} (b_s - a_s)\alpha_i^{d-s} \right) \\ &\geq \min_{1 \leq s \leq d} \{ v_1(b_s - a_s) + (d-s)\bar{v}_1(\alpha_i) \} \\ &\geq \gamma_1 + \min_{1 \leq s \leq d} \{ (d-s)\bar{v}_1(\alpha_i) \} = \gamma_1 + \delta_i, \end{aligned} \tag{3.18}$$

where $\delta_i \in \overline{\Gamma}_1$ is given by $\delta_i = 0$ if $\bar{v}_1(\alpha_i) \geq 0$, and respectively by $\delta_i = (d-1)\bar{v}_1(\alpha_i)$, if $\bar{v}_1(\alpha_i) < 0$. Let us denote

$$\omega = \max_{1 \leq i \neq j \leq d} \bar{v}_1(\alpha_i - \alpha_j).$$

We assume that γ_1 is chosen such that

$$\gamma_1 > d\omega - \delta_i, \tag{3.19}$$

for any $i \in \{1, \dots, d\}$. By (3.18) and (3.19) we see that

$$\sum_{1 \leq j \leq d} \bar{v}_1(\theta_j - \alpha_i) > d\omega,$$

which further implies that

$$\max_{1 \leq j \leq d} \bar{v}_1(\theta_j - \alpha_i) > \omega, \tag{3.20}$$

for any $i \in \{1, \ldots, d\}$. For $i = 1$, we know that the maximum on the left side of (3.20) is attained for $j = 1$, so

$$\bar{v}_1(\theta_1 - \alpha_1) > \omega. \tag{3.21}$$

Since $\bar{v}_1(\alpha_1 - \alpha_2) \leq \omega < \bar{v}_1(\theta_1 - \alpha_1)$, we have

$$\bar{v}_1(\theta_1 - \alpha_2) = \bar{v}_1(\alpha_1 - \alpha_2) \leq \omega. \tag{3.22}$$

By (3.22) and the choice of θ_2, it follows that for $i = 2$, the maximum on the left side of (3.20) is attained for $j = 2$, hence

$$\bar{v}_1(\theta_2 - \alpha_2) > \omega. \tag{3.23}$$

As before we find that $\bar{v}_1(\theta_1 - \alpha_3) = \bar{v}_1(\alpha_1 - \alpha_3) \leq \omega$, and $\bar{v}_1(\theta_2 - \alpha_3) = \bar{v}_1(\alpha_2 - \alpha_3) \leq \omega$, from which we derive that $\bar{v}_1(\theta_3 - \alpha_3) > \omega$. By repeating the above reasoning, we conclude that

$$\bar{v}_1(\theta_i - \alpha_i) > \omega, \tag{3.24}$$

for any $i \in \{1, \ldots, d\}$. It also follows that

$$\bar{v}_1(\theta_j - \alpha_i) = \bar{v}_1(\alpha_j - \alpha_i), \tag{3.25}$$

for any $1 \leq i \neq j \leq d$. Using (3.18), (3.25) and the equality

$$\bar{v}_1(f'(\alpha_i)) = \sum_{\substack{1 \leq j \leq d \\ j \neq i}} \bar{v}_1(\alpha_i - \alpha_j),$$

we deduce that for any $i \in \{1, \ldots, d\}$,

$$\bar{v}_1(\theta_i - \alpha_i) \geq \gamma_1 - \bar{v}_1(f'(\alpha_i)) + \delta_i. \tag{3.26}$$

Assume in what follows that for any $i \in \{1, \ldots, d\}$,

$$\gamma_1 > \bar{v}_1(f'(\alpha_i)) - \delta_i + \bar{v}_1(\alpha_i). \tag{3.27}$$

By (3.26) and (3.27) it follows that

$$\bar{v}_1(\theta_i) = \bar{v}_1(\alpha_i), \tag{3.28}$$

for any $i \in \{1, \ldots, d\}$. Denote by S the subset of $\{1, \ldots, d\}$ which corresponds to the roots of $G(X)$, in the sense that

$$G(X) = \prod_{j \in S} (X - \theta_j).$$

Consider the polynomial

$$f_S(X) = \prod_{j \in S} (X - \alpha_j).$$

By (3.26) we see that for γ_1 large enough, the corresponding coefficients in the polynomials $G(X)$ and $f_S(X)$ are close to each other. One of the coefficients of $f_S(X)$ is

$$\sigma_{S,j_S} = \sum_{\substack{i_1,\dots,i_{j_S}\in S\\ i_1<\cdots<i_{j_S}}} \alpha_{i_1}\alpha_{i_2}\dots\alpha_{i_{j_S}}. \tag{3.29}$$

The corresponding coefficient in $G(X)$, call it u, is given by

$$u = \sum_{\substack{i_1,\dots,i_{j_S}\in S\\ i_1<\cdots<i_{j_S}}} \theta_{i_1}\theta_{i_2}\dots\theta_{i_{j_S}}. \tag{3.30}$$

Note that for any $1 \le i_1,\dots,i_k \le d$, one has

$$\begin{aligned}\theta_{i_1}\dots\theta_{i_k} - \alpha_{i_1}\dots\alpha_{i_k} &= \theta_{i_1}\dots\theta_{i_{k-1}}(\theta_{i_k}-\alpha_{i_k}) + \theta_{i_1}\dots\theta_{i_{k-2}}(\theta_{i_{k-1}}-\alpha_{i_{k-1}})\alpha_{i_k}\\ &\quad + \theta_{i_1}\dots\theta_{i_{k-3}}(\theta_{i_{k-2}}-\alpha_{i_{k-2}})\alpha_{i_{k-1}}\alpha_{i_k} + \cdots + (\theta_{i_1}-\alpha_{i_1})\alpha_{i_2}\dots\alpha_{i_k}.\end{aligned}$$

Combining this with (3.26) and (3.28), we find that

$$\begin{aligned}\bar{v}_1(\theta_{i_1}\dots\theta_{i_k}-\alpha_{i_1}\dots\alpha_{i_k}) &\ge \bar{v}_1(\alpha_{i_1}\dots\alpha_{i_k})\\ &\quad + \min_{1\le l\le k}\{\gamma_1 - \bar{v}_1(f'(\alpha_{i_l})) + \delta_{i_l} - \bar{v}_1(\alpha_{i_l})\}.\end{aligned} \tag{3.31}$$

Using (3.31) together with (3.29) and (3.30), we obtain

$$\begin{aligned}\bar{v}_1(\sigma_{S,j_S}-u) &\ge \gamma_1 + \min_{\substack{i_1,\dots,i_{j_S}\in S\\ i_1<\cdots<i_{j_S}}}\Bigg\{\bar{v}_1(\alpha_{i_1}\dots\alpha_{i_{j_S}})\\ &\qquad + \min_{1\le l\le j_S}\{-\bar{v}_1(f'(\alpha_{i_l})) + \delta_{i_l} - \bar{v}_1(\alpha_{i_l})\}\Bigg\} = \gamma_1 + \rho_S,\end{aligned} \tag{3.32}$$

where $\rho_S \in \bar{\Gamma}_1$ denotes the minimum above.

Now $\sigma_{S,j_S} \in \bar{A}\backslash A$, while $u \in A$. By (3.16) we also know that $v_2(u) \ge j_S\gamma_2'$. Thus (3.17) is applicable, and we get

$$\bar{v}_1(\sigma_{S,j_S}-u) \le \gamma_{1,S}. \tag{3.33}$$

The inequalities (3.32) and (3.33) imply that

$$\gamma_1 \le \gamma_{1,S} - \rho_S. \tag{3.34}$$

It follows that if we start with an element γ_1 of Γ_1 satisfying (3.19), (3.27) and such that

$$\gamma_1 > \gamma_{1,S} - \rho_S, \tag{3.35}$$

for any nonempty, proper subset S of $\{1, \ldots, d\}$, then no polynomial $g(X) \in A[X]$ as in (3.10), (3.11) and (3.12), can be reducible over K. This completes the proof of the theorem.

4. The case of an algebraic function field over a p-adic field

We conclude this paper with an example. Let K_0 be a p-adic field, as in Section 2. Denote by O the ring of p-adic integers in K_0, and let K be an algebraic function field of one variable over K_0. Choose any prime divisor $\mathscr{P}$ (i.e. any valuation on K which is trivial on K_0), and let t be any element of K whose only pole is at $\mathscr{P}$. The existence of such an element t follows from the Riemann-Roch theorem (see Chapter II of [2]). Denote by A the integral closure of $O[t]$ in K. Then A is integrally closed in K, and K is the field of fractions of A. Also, K is a finite extension of $K_0(t)$. On $K_0(t)$ we have an absolute value, as in Section 2, which is the Gauss extension of the p-adic absolute value on K_0. We fix an extension of this absolute value to K, and denote it by $|.|_1$. This is our primary absolute value. Next, fix any real number $\rho > 1$, and put

$$|P(t)|_2 = \rho^{\deg P(t)}, \tag{4.1}$$

for any $P(t) \in K_0[t]$. Then extend this absolute value to an absolute value on K, which we continue to denote by $|.|_2$. This is our secondary absolute value on K. By the above construction, the extension of the secondary absolute value from $K_0[t]$ to K is unique. Indeed, any two such extensions would correspond to distinct prime divisors which are poles for t, contrary to our assumption that the only pole of t is at $\mathscr{P}$. Note that if we extend the absolute value $|.|_2$ to an absolute value on a fixed algebraic closure $\overline{K}$ of K, which we also denote by $|.|_2$, then for any automorphism $\sigma \in Gal(\overline{K}/K_0(t))$, the map defined on $\overline{K}$ by $z \mapsto |\sigma(z)|_2$ is also an absolute value on $\overline{K}$, and its restriction to $K_0(t)$ coincides with the absolute value $|.|_2$. Since $|.|_2$ has a unique extension to K, it follows that the two absolute values also coincide on K. Therefore,

$$|\sigma(z)|_2 = |z|_2, \tag{4.2}$$

for any $\sigma \in Gal(\overline{K}/K_0(t))$ and any $z \in K$. This shows that for any $z \in K$, $|z|_2$ is given by

$$|z|_2 = |\mathrm{Norm}_{K/K_0(t)}\, z|_2^{1/[K:K_0(t)]}. \tag{4.3}$$

Note also that

$$|z|_2 \geq 1, \qquad \text{for any } 0 \neq z \in A. \tag{4.4}$$

Let us check that property (3.1) holds in the present context. We choose an extension of the primary absolute value $|.|_1$ to $\overline{K}$, and continue to denote it by $|.|_1$. Let $\bar{A}$ denote the integral closure of A in $\overline{K}$. Property (3.1) states in our case that for any $\alpha \in \bar{A} \backslash A$, and any $L > 0$, there exists a $\delta > 0$ such that

$$|u - \alpha|_1 \geq \delta, \qquad \text{for any } u \in A \text{ with } |u|_2 \leq L. \tag{4.5}$$

Suppose that (4.5) fails for some $\alpha \in \bar{A} \backslash A$ and $L > 0$. Then there is a sequence $(u_n)_{n \in \mathbf{N}}$ of elements from A, with $|u_n|_2 \leq L$ for any $n \in \mathbf{N}$, and such that

$$\lim_{n \to \infty} |u_n - \alpha|_1 = 0. \tag{4.6}$$

Denote by $\tilde{A}$ the integral closure of $K_0[t]$ in K, and fix an integral basis $B = \{\eta_1, \ldots, \eta_m\}$ of $\tilde{A}$ over $K_0[t]$, where $m = [K : K_0(t)]$. Each u_n belongs to A, and hence it also belongs to $\tilde{A}$. We write u_n in terms of this basis,

$$u_n = c_{1,n}\eta_1 + \cdots + c_{m,n}\eta_m, \tag{4.7}$$

with $c_{1,n}, \ldots, c_{m,n} \in K_0[t]$, for any $n \in \mathbf{N}$. Denote by $B^* = \{\eta_1^*, \ldots, \eta_m^*\}$ the dual basis of B. Then each coefficient $c_{j,n}$ can be written as a trace,

$$c_{j,n} = \mathrm{Trace}_{K/K_0(t)}(u_n \eta_j^*), \qquad 1 \leq j \leq m,\ n \in \mathbf{N}. \tag{4.8}$$

On the other hand, from (4.2) we know that for any automorphism $\sigma \in Gal(\overline{K}/K_0(t))$ we have

$$|\sigma(u_n \eta_j^*)|_2 = |u_n \eta_j^*|_2 = |u_n|_2 \cdot |\eta_j^*|_2 \leq L|\eta_j^*|_2. \tag{4.9}$$

It follows that

$$|c_{j,n}|_2 \leq L|\eta_j^*|_2, \tag{4.10}$$

for any $n \in \mathbf{N}$ and any $1 \leq j \leq m$. Therefore, for any fixed $j \in \{1, \ldots, m\}$, the sequence $(c_{j,n})_{n \in N}$ is a sequence of polynomials in t over K_0, of bounded degree, say

$$c_{j,n} = c_{j,n,0} + c_{j,n,1}t + \cdots + c_{j,n,D}t^D,$$

where $c_{j,n,0}, \ldots, c_{j,n,D} \in K_0$ for any $n \in \mathbf{N}$ and any $1 \leq j \leq m$. We claim that for any $1 \leq j \leq m$ and any $0 \leq d \leq D$, the sequence $(c_{j,n,d})_{n \in N}$ is bounded in the p-adic absolute value. Indeed, each u_n belongs to A, so u_n is a root of a polynomial of the form

$$P_n(X) = X^{l_n} + a_1 X^{l_n - 1} + \cdots + a_{l_n}$$

with $a_1, \ldots, a_{l_n} \in O[t]$. Since $|a_1|_1 \leq 1, \ldots, |a_{l_n}|_1 \leq 1$, it follows immediately that $|u_n|_1 \leq 1$, and also $|\sigma(u_n)|_1 \leq 1$ for any $\sigma \in Gal(\overline{K}/K_0(t))$. Therefore

$$|c_{j,n}|_1 = |\mathrm{Trace}_{K/K_0(t)}(u_n \eta_j^*)|_1 \leq \max\{|\sigma(\eta_j^*)|_1 : \sigma \in Gal(\overline{K}/K_0(t))\},$$

which in turn implies that

$$|c_{j,n,d}|_1 \leq \max\{|\sigma(\eta_j^*)|_1 : \sigma \in Gal(\overline{K}/K_0(t))\}$$

for all $d \in \{0, 1, \ldots, D\}$. Hence for any $1 \leq j \leq m$ and any $0 \leq d \leq D$ the sequence $(c_{j,n,d})_{n \in N}$ is bounded, as claimed. Since K_0 is locally compact, it follows that the sequence $(c_{j,n,0})_{n \in N}$ has a subsequence which converges with respect to the absolute value $|\cdot|_1$ to an element $\mu_{j,0}$ of K_0. This subsequence has a subsequence along which $c_{j,n,1}$ converges to an element $\mu_{j,1}$ of K_0, and so on. We conclude that there is a subsequence along which we simultaneously have that $c_{j,n,0} \to \mu_{j,0}$, $c_{j,n,1} \to \mu_{j,1}, \ldots, c_{j,n,D} \to \mu_{j,D}$. This means that along this subsequence $c_{j,n}$ converges in the Gauss absolute value $|\cdot|_1$ to the element

$$c_j := \mu_{j,0} + \mu_{j,1}t + \cdots + \mu_{j,D}t^D$$

of $K_0[t]$. This further implies that there is a subsequence $n_1 < n_2 < \cdots < n_k < \cdots$ for which we simultaneously have

$$\lim_{k \to \infty} |c_{j,n_k} - c_j|_1 = 0, \qquad \text{for } 1 \leq j \leq m.$$

Combining this with (4.6) and (4.7), we obtain

$$\left|\alpha - \sum_{1 \leq j \leq m} c_j \eta_j\right|_1 \leq |\alpha - u_{n_k}|_1 + \sum_{1 \leq j \leq m} |c_{j,n_k} - c_j|_1 \cdot |\eta_j|_1 \to 0,$$

as $k \to \infty$. Thus

$$\alpha = \sum_{1 \leq j \leq m} c_j \eta_j \in K.$$

Therefore $\alpha \in \bar{A} \cap K = A$, which contradicts our assumption that $\alpha \in \bar{A} \backslash A$. In conclusion, property (4.5) holds true.

Theorem 1 is then applicable in our case, and it gives the following result.

THEOREM 2. *Let K_0 be a p-adic field, O its ring of integers, and let K be an algebraic function field of one variable over K_0. Choose any prime divisor $\mathscr{P}$ and any element $t \in K$ whose only pole is at $\mathscr{P}$. Denote by A the integral closure of $O[t]$ in K. Let $|.|_1$ be an absolute value on K whose restriction to $K_0[t]$ coincides with the Gauss extension to $K_0[t]$ of the p-adic absolute value on K_0. Choose a real number $\rho > 1$, and denote by $|.|_2$ the unique absolute value on K given by* (4.1) *and* (4.3). *Then, for any polynomial*

$$f(X) = X^d + a_1 X^{d-1} + \cdots + a_d \in A[X],$$

which is irreducible over K, and for any $L > 0$, there exists a $\delta > 0$ such that, for any $b_1, \ldots, b_d \in A$ for which

$$|b_i - a_i|_1 \leq \delta, \qquad 1 \leq i \leq d,$$

and

$$|b_i|_2 \leq L, \qquad 1 \leq i \leq d,$$

the polynomial

$$g(X) = X^d + b_1 X^{d-1} + \cdots + b_d,$$

is irreducible over K.

References

[1] V. Alexandru, N. Popescu and A. Zaharescu, On the closed subfields of $\mathbf{C}_p$. Journal of Number Theory **68** (1998), no. 2, 131–150.

[2] C. Chevalley, Introduction to the theory of algebraic functions of one variable, Mathematical Surveys, No. VI. American Mathematical Society, Providence, R.I. 1963.

[3] M. Krasner, Nombre des extensions d'un degré donné d'un corps p-adique, 1966 Les Tendances Géom. en Algébre et Théorie des Nombres pp. 143–169 Editions du Centre National de la Recherche Scientifique, Paris.

[4] K. Ota, On saturated distinguished chains over a local field, J. Number Theory **79** (1999), no. 2, 217–248.

[5] A. Popescu, N. Popescu, M. Vajaitu and A. Zaharescu, Chains of metric invariants over a local field, Acta Arith. **103** (2002), no. 1, 27–40.

[6] N. Popescu and A. Zaharescu, On the structure of the irreducible polynomials over local fields, J. Number Theory **52** (1995), no. 1, 98–118.

[7] O. F. G. Schilling, The Theory of Valuations, Mathematical Surveys, No. 4. American Mathematical Society, New York, N.Y., 1950.

Alexandru Zaharescu
Department of Mathematics
University of Illinois at Urbana-Champaign
1409 *W. Green Street*
Urbana, IL, 61801, *USA*
E-mail address: zaharesc@math.uiuc.edu