ON THE IDEAL GENERATED BY THE VALUES OF A POLYNOMIAL

Jean-Luc CHABERT and Sabine EVRARD

Laboratoire Amiénois de Mathématiques Fondamentale et Appliquée, UMR 6140, Université de Picardie, 33 rue Saint Leu, 80039 Amiens, France
jean-luc.chabert@u-picardie.fr, sabined.evrard@laposte.net

1. Introduction

Let D be a Dedekind domain with quotient field K and let

$$f = \sum_{k=0}^{n} a_k X^k \in K[X] \tag{1}$$

be a polynomial of degree n. We denote by $\mathcal{C}(f)$ the content of f, that is, the ideal of D generated by the coefficients of f and by $\mathcal{D}(f)$ the divisor of f, that is, the ideal generated by the values of f on D.

In this introduction we assume that f is primitive, that is, $\mathcal{C}(f) = D$. When $f \in \mathbb{Z}[X]$, it is well known that the gcd of the values of f on $\mathbb{Z}$ divides $n!$. For Dedekind domains, this result was generalized by Pólya [8, §4] in the following way (see also [5, II.3.3]): the ideal $\mathcal{D}(f)$ divides the n^{th} factorial ideal $n!_D$ where $n!_D$ is defined by

$$n!_D = \prod_{\mathfrak{m} \in \max(D),\ N(\mathfrak{m}) \le n} \mathfrak{m}^{w_{N(\mathfrak{m})}(n)} \tag{2}$$

with

$$N(\mathfrak{m}) = \mathrm{Card}(D/\mathfrak{m}) \tag{3}$$

and

$$w_q(n) = \sum_{l \ge 1} \left[\frac{n}{q^l} \right]. \tag{4}$$

Writing the ideal $\mathcal{D}(f)$ in the following form

$$\mathcal{D}(f) = \prod_{\mathfrak{m} \in \max(D)} \mathfrak{m}^{d_{\mathfrak{m}}(f)}, \tag{5}$$

this divisibility relation may be written as inequalities. For each maximal ideal $\mathfrak{m}$ of D, one has:

$$d_{\mathfrak{m}}(f) \le w_{N(\mathfrak{m})}(n). \tag{6}$$

The aim of this paper is to state another divisibility relation making use of the number of coefficients of f not belonging to $\mathfrak{m}$ instead of the degree of f. More precisely, let

$$\mu_{\mathfrak{m}}(f) = \text{Card}\,\{a_k \mid a_k \notin \mathfrak{m}\}, \tag{7}$$

we are going to prove that

$$d_{\mathfrak{m}}(f) < \mu_{\mathfrak{m}}(f). \tag{8}$$

But this inequality holds only for small values of $n = \deg(f)$, namely:

$$\deg(f) \leq char(D/\mathfrak{m}) \times (N(\mathfrak{m}) - 1). \tag{9}$$

Vâjâitu [9, Theorem 2] proved Inequality (8) when $D = \mathbb{Z}$. Here, we generalize it to every Dedekind domain D (Proposition 4.1). Then, we extend it to the ideal $\mathcal{D}(f, E)$ generated by the values of f on a subset E of D when $D = V$ is a discrete valuation domain (Proposition 5.4).

2. Technical preliminaries

Notation. For every polynomial f, we denote by $\mu(f)$ the number of nonzero coefficients of f.

The following technical result is implicitly contained in the proof of [9, Thm 2].

Lemma 2.1. *Let k be a field with characteristic $p > 0$ such that $k^p = k$ (for instance, a finite field). Let $f \in k[X]$ be a nonzero polynomial and let $z \in k$ be a nonzero root of f with multiplicity m. If $m < p$, then $m < \mu(f)$.*

In order to prove this lemma we associate to every polynomial f an integer $s(f) < \mu(f)$ defined by means of the following algorithm:

Algorithm A.

$s \leftarrow 0\ ,\ f_s \leftarrow f$
while $\mu(f_s) > 1$ do
  begin
    $s \leftarrow s + 1$
    $f_s \leftarrow \left(\frac{f_s}{X^{v_X(f_s)}}\right)'$
  end
$s(f) = s$

where $v_X(g)$ denotes the least degree of the monomials of g and the symbol $'$ denotes the formal derivation of polynomials.

It is clear that the procedure is finite since, for every $g \neq 0$, one has:

$$\mu\left(\left(\frac{g}{X^{v_X(g)}}\right)'\right) < \mu(g).$$

Consequently,

$$s(f) < \mu(f).$$

Proof. of Lemma 2.1. Assume that $m \geq \mu(f)$. Then z is a root of all the polynomials f_s constructed in Algorithm A with multiplicity

$$m - s \geq m - s(f) > m - \mu(f) \geq 0.$$

By definition of $s(f)$, one has $\mu(f_{s(f)}) \leq 1$. If $\mu(f_{s(f)}) = 1$, then $f_{s(f)}$ is of the form bX^h and z cannot be a root of $f_{s(f)}$. Consequently, $f_{s(f)} = 0$, and hence,

$$f_{s(f)-1}(X) = b_1 X^{h_1} + \ldots + b_l X^{h_l}$$

with

$$l \geq 2,\ b_j \in k^*,\ h_1 < h_2 < \cdots < h_l,\ h_j - h_1 = pm_j \text{ with } m_j \in \mathbb{N}^*.$$

By hypothesis, for $j = 1, \ldots, l$, $b_j = c_j^p$ with $c_j \in k^*$. Thus,

$$f_{s(f)-1}(X) = X^{h_1} \sum_{j=1}^{l} c_j^p X^{pm_j} = X^{h_1} \left(\sum_{j=1}^{l} c_j X^{m_j} \right)^p.$$

Since z is a root of $f_{s(f)-1}$, z is a root of $\sum_{j=1}^{l} c_j X^{m_j}$. Consequently, the multiplicity of z as a root of $f_{s(f)-1}$ is a nonzero multiple of p. But this multiplicity is $m - s(f) + 1$, so $m \geq p$, which contradicts the hypothesis. □

Corollary 2.2. *Let k be a field of characteristic $p > 0$ such that $k^p = k$ and let f be a nonzero polynomial in $k[X]$. If $x \in k$ is a root of f with multiplicity $m_x < p$ then, for every $y \in k$, $y \neq x$, one has :*

$$m_x < \mu(f(X + y)).$$

Proof. It suffices to use Lemma 2.1 with the polynomial $g(X) = f(X + y)$ and its root $z = x - y$. □

3. Polynomials with coefficients in a discrete valuation domain

Hypotheses and notation for Section 3. Let V be a discrete valuation domain with finite residue field. Denote by K the quotient field of V, v the corresponding valuation of K, $\mathfrak{m}$ the maximal ideal of V, π a generator of $\mathfrak{m}$, $k = V/\mathfrak{m}$ the residue field, p the characteristic of k, and $q = p^f$ its cardinality.

For every nonzero polynomial

$$f(X) = \sum_{i=0}^{n} a_i X^i \in K[X], \tag{10}$$

we consider the following integers:

$$v(f) = \inf_{0 \leq i \leq n} v(a_i), \tag{11}$$

$$d(f) = \inf_{a \in V} v(f(a)), \tag{12}$$

$$\nu(f) = \#\{i \mid v(a_i) = v(f)\} \tag{13}$$

Note that $\nu(f) = \mu(\tilde{f})$ where $\tilde{f}$ denotes the image of $\frac{1}{\pi^{v(f)}} f$ in $k[X]$.

Clearly,

$$v(f) \leq d(f), \tag{14}$$

and we also know that (see for instance [8] or [5, Corollary II.2.13])

$$d(f) \leq v(f) + w_q(\deg(f)) \tag{15}$$

where w_q is defined by:

$$w_q(n) = \sum_{l \geq 1} \left[\frac{n}{q^l} \right]. \tag{16}$$

In particular, if $\deg(f) < q$, then $d(f) = v(f)$. Here we prove another inequality for $d(f)$:

Proposition 3.1. *With the previous hypotheses and notation, for every nonzero polynomial f in $K[X]$ such that*

$$\deg(f) \leq p(q-1) + 1, \tag{17}$$

one has:

$$v(f) \leq d(f) < v(f) + \nu(f). \tag{18}$$

Proof. We may replace f by $\pi^{-v(f)} f$ and assume that f is primitive in $V[X]$, that is, $v(f) = 0$. Note that $\nu(f) \geq 1$ and, if $\nu(f) = 1$, then necessarily $d(f) = 0$. Consequently, one may also assume that $d(f) \geq 2$.

First, we recall some classical results concerning the values of a polynomial. Let $u_0 = 0, u_1, \ldots, u_{q-1}$ be a complete system of representatives of V modulo $\mathfrak{m}$. We extend the sequence u_r in the following way: for

$$r = r_0 + r_1 q + \ldots + r_l q^l \quad \text{where } 0 \leq r_i < q,$$

we let

$$u_r = u_{r_0} + u_{r_1}\pi + \ldots + u_{r_l}\pi^l.$$

Clearly, the following sequence of polynomials

$$g_i(X) = \prod_{j=0}^{i-1} (X - u_j)\ ,\ i \in \mathbb{N}$$

is a basis of the V-module $V[X]$. Then let

$$f(X) = \sum_{i=0}^{n} b_i g_i(X) \quad \text{with } b_i \in V.$$

We know, and this is easy to check, that the ideal generated by the values of f on V is equal to the ideal generated by the values of f on $u_0, u_1, \ldots, u_n$ where $n = \deg(f)$ [5, Corollary II.2.9], that is, the ideal generated by the $b_i \prod_{j<i} (u_i - u_j)$ for $0 \leq i \leq n$. Since $v(\prod_{j<i} (u_i - u_j)) = w_q(i)$ [5, Lemma II.2.6], one has:

$$d(f) = \inf_{0 \leq i \leq n} (v(b_i) + w_q(i)).$$

Let i_0 be the least integer i such that $v(b_i) = 0$ (f is assumed to be primitive). The hypothesis on $n = \deg(f)$ implies that

$$\left[\frac{i_0}{q^2}\right] \leq \frac{i_0}{q^2} < \frac{i_0}{p(q-1)} \leq \frac{i_0}{n} \leq 1,$$

and hence,

$$d(f) \leq w_q(i_0) = \sum_{l \geq 1} \left[\frac{i_0}{q^l}\right] = \left[\frac{i_0}{q}\right] \leq \frac{i_0}{q}.$$

Finally,

$$i_0 \geq q\, d(f).$$

We denote by $\overline{b}$ the canonical image in k of an element b of V and by $\overline{g}$ the canonical image in $k[X]$ of an element g of $V[X]$. It follows from the choice of i_0 and from the construction of the g_i's that

$$\overline{f}(X) = \sum_{i=0}^{n} \overline{b_i}\overline{g_i}(X) = \sum_{i=i_0}^{n} \overline{b_i}\overline{g_i}(X) = \overline{g_{i_0}}(X)\overline{h}(X) \text{ where } \overline{h}(X) \in k[X].$$

Since $\overline{u}_r = \overline{u}_s$ as soon as q divides $r-s$ and $i_0 \geq d(f)$, the q elements of $k = V/\mathfrak{m}$ are roots of $\overline{g_{i_0}}$, and hence of $\overline{f}$, with multiplicity $\geq d(f)$. On the other hand, there exists at least one root of $\overline{f}$ in k^* with a multiplicity $< p$ since otherwise we would have:

$$n = \deg(f) \geq \deg(\overline{f}) \geq d(f) + (q-1)p \geq 2 + (q-1)p > n.$$

Thus, there exists a root $z \in k^*$ of $\overline{f}$ with a multiplicity m such that $d(f) \leq m < p$. It follows from Lemma 2.1 that $m < \mu(\overline{f})$, and hence, $d(f) < \nu(f)$. □

Example 3.2. Let p be a prime number. For

$$f(X) = X(X^{(p-1)(q-1)} - 1) + \pi,$$

one has

$$d(f) = 1 = \nu(f) - 1$$

while

$$w_q(n) = p - 2 \ (> \nu(f) - 1 \text{ as soon as } p \geq 5 \ ).$$

Let us introduce another notation: for each $a \in V$, let $\nu_a(f) = \nu(f(X+a))$. In particular, $\nu_0(f) = \nu(f)$. Let

$$\tilde{\nu}(f) = \inf_{a \in V} \nu_a(f) = \inf_{a \in V} \nu(f(X+a)).$$

Of course, $v(f(X)) = v(f(X+a))$ and $d(f(X)) = d(f(X+a))$. Consequently,

Corollary 3.3. *If* $\deg(f) \leq p(q-1)+1$, *then*

$$v(f) \leq d(f) < v(f) + \tilde{\nu}(f). \tag{19}$$

Example 3.4. Let p be a prime number ≥ 5, let $V = \mathbb{Z}_{(p)}$, and let $f(X) = (X-1)^{p-1} - 1$. Then, on the one hand, for every $a \in \mathbb{Z}$,

$$f(X+a) \equiv (X + (a-1))^{p-1} - 1 \pmod{p}.$$

If $a \not\equiv 1 \pmod{p}$, then $\nu_a(f) = p - 1$. If $a \equiv 1 \pmod{p}$, then $\nu_a(f) = 2$. On the other hand, $f(1) = -1$, and hence, $d(f) = 0$. Finally,

$$d(f) = 0 < \tilde{\nu}(f) - 1 = 1 < \nu(f) - 1 = p - 2.$$

Thus, we may have strict inequalities. Nevertheless:

Remark. For $n \leq p(q-1) < q^2$, one has $w_q(n) = [\frac{n}{q}] \leq p-1$, and hence, it follows from Inequalities (15) and (18) that, if $f \in V[X]$ is primitive of degree

$$n \leq p(q-1) + 1, \tag{20}$$

then

$$d(f) \leq \min\left(\left[\frac{n}{q}\right], \nu(f) - 1\right). \tag{21}$$

Moreover, both inequalities are sharp. Inequality (20) is sharp as shown by the following example:

$$f(X) = X^2(X^{q-1} - 1)^p \ , \ \deg(f) = p(q-1) + 2 \ , \ \nu(f) \leq 2 \ , \ d(f) = 2.$$

Inequality (21) is sharp in the following sense: for every integer ν between 1 and p, there exists a polynomial f primitive in $V[X]$ of degree $n \leq p(q-1) + 1$ such that $d(f) = \nu(f) - 1 = \nu - 1$:

For $0 \leq k \leq p-1$, the polynomial $f_k(X) = (X^q - X)^k$ satisfies $d(f_k) = k$ and $\nu(f_k) = k + 1$ with $\deg(f_k) = kq \leq (p-1)q \leq p(q-1) + 1$.

4. Polynomials with coefficients in a Dedekind domain

Now we globalize the previous results.

Hypotheses and notation for section 4. Let D be a Dedekind domain with quotient field K. For every maximal ideal $\mathfrak{m}$ of D, we denote by $v_{\mathfrak{m}}$ the corresponding valuation of K, by $p_{\mathfrak{m}}$ the characteristic of the residue field $D/\mathfrak{m}$, and by $q_{\mathfrak{m}}$ its cardinality (finite or infinite).

For every polynomial

$$f = \sum_{i=0}^{n} a_i X^i \in K[X], \tag{22}$$

$\mathcal{C}(f)$ denotes the *content* of f, that is, the fractional ideal of D generated by the coefficients of f and $\mathcal{D}(f)$ denotes the *divisor* of f, that is, the fractional ideal generated by the values of f on D.

For every maximal ideal $\mathfrak{m}$ of D, we introduce the following integers:

$$v_{\mathfrak{m}}(f) = \inf_{0 \leq i \leq n} v_{\mathfrak{m}}(a_i), \tag{23}$$

$$d_{\mathfrak{m}}(f) = \inf_{a \in D} v_{\mathfrak{m}}(f(a)), \tag{24}$$

$$\nu_{\mathfrak{m}}(f) = \#\{i \mid v_{\mathfrak{m}}(a_i) = v_{\mathfrak{m}}(f)\}. \tag{25}$$

Obviously,

$$\mathcal{C}(f) = \prod_{\mathfrak{m} \in \max(D)} \mathfrak{m}^{v_{\mathfrak{m}}(f)}, \tag{26}$$

$$\mathcal{D}(f) = \prod_{\mathfrak{m} \in \max(D)} \mathfrak{m}^{d_{\mathfrak{m}}(f)}. \tag{27}$$

Clearly, the ideal $\mathcal{C}(f)$ divides the ideal $\mathcal{D}(f)$ and it is known [5, Proposition II.3.3] that $\mathcal{D}(f)$ divides $\mathcal{C}(f) \times n!_D$ where the ideal $n!_D$ is defined by Formula (2), in other words, for every maximal ideal $\mathfrak{m}$ of D, analogously to Formulas 14 and 15, one has the inequalities:

$$v_{\mathfrak{m}}(f) \leq d_{\mathfrak{m}}(f) \leq v_{\mathfrak{m}}(f) + w_{N(\mathfrak{m})}(\deg(f)) \tag{28}$$

where $N(\mathfrak{m})$ and $w_{N(\mathfrak{m})}$ are defined by Formulas (3) and (4).

Proposition 3.1 may be globalized in the following way:

Proposition 4.1. *Let D be a Dedekind domain with quotient field K and let $f \in K[X]$ be a nonzero polynomial of degree n. With the previous notation, for every maximal ideal $\mathfrak{m}$ of D such that*

$$n \leq p_{\mathfrak{m}}(q_{\mathfrak{m}} - 1) + 1, \tag{29}$$

one has:

$$d_{\mathfrak{m}}(f) < v_{\mathfrak{m}}(f) + \nu_{\mathfrak{m}}(f). \tag{30}$$

This proposition is the extension of Theorem 2 of Vâjâitu [9] from $\mathbb{Z}$ to every Dedekind domain D. Theorem 3 of [9] corresponds to the first example below.

Examples 4.2. In these three examples, f denotes a polynomial of degree n primitive in $D[X]$.
1) Let $D = \mathbb{Z}$ and denote by $\mathbb{P}$ the set of prime integers. Then, a generator of $\mathcal{D}(f)$ divides the integer

$$\prod_{p\in\mathbb{P},\, p<\sqrt{n-\frac{3}{4}}+\frac{1}{2}} p^{w_p(n)} \times \prod_{p\in\mathbb{P},\, \sqrt{n-\frac{3}{4}}+\frac{1}{2}\leq p\leq n} p^{\min([\frac{n}{p}],\nu_p(f)-1)}.$$

2) Let $D = \mathbb{Z}[i]$, $p_0 = \inf\{p \in \mathbb{P} \mid p(p^2-1)+1 \geq n\}$ and $p_1 = \inf\{p \in \mathbb{P} \mid p(p-1)+1 \geq n\}$. For each $p \in \mathbb{P}$, $\nu_p(f)$ denotes the number of coefficients of f that are not divisible by p. Then, the ideal $\mathcal{D}(f)$ divides the following ideal of $\mathbb{Z}[i]$

$$\mathbb{Z}[i]\ (1+i)^{w_2(n)} \times \prod_{p\equiv 1\,(4),\, p<p_1} p^{w_p(n)} \times \prod_{p\equiv 1\,(4),\, p_1\leq p\leq n} p^{\inf([\frac{n}{p}],\nu_p(f)-1)}$$
$$\times \prod_{p\equiv 3\,(4),\, p<p_0} p^{w_{p^2}(n)} \times \prod_{p\equiv 3\,(4),\, p_0\leq p\leq n} p^{\inf([\frac{n}{p^2}],\nu_p(f)-1)}.$$

3) Let $D = \mathbb{F}_q[T]$ and denote by $\mathbb{P}_q$ the set of monic irreducible polynomials of $\mathbb{F}_q[T]$. For $\mathfrak{m} = (Q)$ where $Q \in \mathbb{P}_q$, one has $q_{\mathfrak{m}} = q^{\deg(Q)}$. Then, a generator of $\mathcal{D}(f)$ divides the polynomial

$$\prod_{\deg(Q)<\frac{\ln n}{\ln q}-\frac{\ln\frac{pn}{n+p-1}}{\ln q}} Q^{w_{q^{\deg Q}}(n)} \times \prod_{\frac{\ln n}{\ln q}-\frac{\ln\frac{pn}{n+p-1}}{\ln q}\leq\deg(Q)\leq\frac{\ln n}{\ln q}} Q^{\min\left(\left[\frac{n}{q^{\deg(Q)}}\right],\nu_Q(f)-1\right)}.$$

Remark. Recall Theorem 1 of [9]: if the characteristic of D is 0 and if $f \in D[X]$ is primitive with degree n and leading coefficient a, then

$$Card(D/\mathcal{D}(f)) \leq Card(D/(a.n!D)^{n2^{n+1}}.$$

In fact, we have just recalled a stronger result: $\mathcal{D}(f)$ divides $n!_D$ and $n!_D$ divides $n!D$ because of the containment $\mathbb{Z} \subseteq D$. Thus, $\mathcal{D}(f)$ divides $n!D$, and hence,

$$Card(D/\mathcal{D}(f)) \leq Card(D/n!D).$$

5. The ideal generated by the values on a subset

In this paragraph we extend the previous results to the ideal $\mathcal{D}(f, E)$ generated by the values of a polynomial $f \in K[X]$ on a subset E of D. We will give the statement for the main result (Proposition 5.4) in the case when D is a discrete valuation domain. Then, by using a specific example, we will show what happens in the more general case of a Dedekind domain.

Hypotheses and notation for section 5 are those of Section 3. Hence, the domain $D = V$ is a discrete valuation domain, and we denote by E a subset of V.
We introduce the integer

$$d(f, E) = \inf_{x \in E} v(f(x)). \tag{31}$$

Obviously,

$$\mathcal{D}(f, E) = \mathfrak{m}^{d(f,E)}. \tag{32}$$

Definition 5.1 ([1], [2])**.** A v-ordering of E is a sequence $\{u_k\}_{k \in \mathbb{N}}$ of elements of E such that, for every $s \geq 1$, one has

$$v\left(\prod_{t=0}^{s-1}(u_s - u_t)\right) = \inf_{x \in E} v\left(\prod_{t=0}^{s-1}(x - u_t)\right).$$

There always exist v-orderings and, for every $s \geq 1$, the integer

$$w_E(s) = v\left(\prod_{t=0}^{s-1}(u_s - u_t)\right) \tag{33}$$

does not depend on the choice of the v-ordering $\{u_s\}_{s \in \mathbb{N}}$ of E (see for instance [1] or [6]).

Definition 5.2. The s^{th} factorial ideal of E with respect to V is the ideal

$$s!_E^V = \mathfrak{m}^{w_E(s)}.$$

It is easy to see that if $E \subseteq F \subseteq V$, then $s!_F^V$ divides $s!_E^V$, that is,

$$E \subseteq F \Rightarrow w_E(s) \geq w_F(s) \quad \forall s \in \mathbb{N}. \tag{34}$$

In particular,

$$w_E(s) \geq w_q(s) \quad \forall s \in \mathbb{N}. \tag{35}$$

Let $\{u_s\}_{s \in \mathbb{N}}$ be a v-ordering of E and, for $i \in \mathbb{N}$, let

$$g_i(X) = \prod_{s=0}^{i-1}(X - u_s).$$

Then, every polynomial $f \in K[X]$ of degree n may be written in the following way:

$$f(X) = \sum_{i=0}^{n} b_i g_i(X) \quad \text{with } b_i \in K.$$

It is known (and this is easy to check) that $\mathcal{D}(f, E)$ is also the ideal generated by the values $f(u_0), f(u_1), \ldots, f(u_n)$ [6, Corollary 2.8]. Thus, $\mathcal{D}(f, E)$ is generated by the $b_i \prod_{j<i}(u_i - u_j)$ $(0 \leq i \leq n)$. Consequently,

$$d(f, E) = \inf_{0 \leq i \leq n}(v(b_i) + w_E(i)). \tag{36}$$

In particular,

$$d(f, E) \leq \inf_{0 \leq i \leq n} v(b_i) + \sup_{0 \leq i \leq n} w_E(i),$$

that is,

Proposition 5.3. *For every $f \in K[X]$ with degree n, one has:*

$$d(f,E) \leq v(f) + w_E(n), \tag{37}$$

where $d(f,E)$, $v(f)$, and $w_E(n)$ are defined by (31), (11) and (33).

This well-known inequality generalizes Inequality (15). But our next goal is to extend Inequality (18) under some condition on the degree n of f.

Proposition 5.4. *Let E be a subset of V which contains at least $r \geq 2$ distinct classes modulo $\mathfrak{m}$ and let $f \in K[X]$ be a polynomial of degree n. If*

$$n \leq p(r-1)+1, \tag{38}$$

then

$$d(f,E) < v(f) + \nu_{\mathfrak{m}}(f). \tag{39}$$

Moreover, the previous inequality also holds as soon as

1. *$n < pr$ when $\mathfrak{m} \not\subseteq E$,*
2. *$n \leq pr$ when $\emptyset \neq E \cap \mathfrak{m} \neq \mathfrak{m}$.*

Proof. Since $E \subseteq F$ implies $d(f,E) \geq d(f,F)$, in order to prove Inequality (39) one may assume that E is exactly the union of r classes modulo $\mathfrak{m}$. Analogously to the proof of Proposition 3.1, one may also assume that f is primitive, that is, $v(f) = 0$, and that $d(f,E) \geq 2$.

We still consider a v-ordering $\{u_s\}_{s\in\mathbb{N}}$ of E, the basis of the V-module $V[X]$ formed by the polynomials $g_i = \prod_{0\leq s<i}(X-u_s)$, and the coefficients b_i $(0 \leq i \leq n)$ of f with respect to this basis. Then, $\inf_i v(b_i) = 0$; let i_0 be the least integer i such that $v(b_i) = 0$. It follows from (36) that

$$d(f,E) \leq w_E(i_0).$$

When E is a union of r distinct classes modulo $\mathfrak{m}$, then (cf. [4] or [3, Prop. 2.4]):

$$w_E(i) = \sum_{l\geq 0} \left[\frac{i}{rq^l}\right].$$

It follows from the hypothesis that

$$\left[\frac{i_0}{rq}\right] \leq \frac{n}{rq} < 1.$$

Thus, $w_E(i_0) = \left[\frac{i_0}{r}\right]$, and hence,

$$i_0 \geq r\, d(f,E).$$

Because of the fact that E is a union of r classes modulo $\mathfrak{m}$ and from the previous inequality, the image $\overline{g}_{i_0}$ of g_{i_0} in $(V/\mathfrak{m})[X]$ has a root in each class of E modulo $\mathfrak{m}$ with a mutiplicity at least equal to $d(f,E)$. The image $\overline{f}$ of f has the same property. Moreover, if each root of $\overline{f}$ distinct from the class $\mathfrak{m}$ had multiplicity $\geq p$, we would have the following inequalities:

$$n = \deg(f) \geq \deg(\overline{f}) \geq \deg(\overline{g}_{i_0}) = i_0 \geq d(f,E) + (r-1)p \geq 2 + p(r-1) > n. \tag{40}$$

Consequently, there is at least one root of $\overline{f}$ distinct from the class $\mathfrak{m}$ and with multiplicity $m < p$. It follows from Lemma 2.1 that $m < \mu(\overline{f}) = \nu_{\mathfrak{m}}(f)$. Finally,

$$d(f,E) \leq m < \nu_{\mathfrak{m}}(f).$$

When $\mathfrak{m} \not\subseteq E$, it follows from the proof and inequalities analogous to (40) that the condition $n < pr$ is enough.

Finally, assume that $\mathfrak{m} \not\subseteq E$ and that there is $t \in \mathfrak{m} \cap E$. We may assume that $E = E_0 \cup \{t\}$ where E_0 is exactly the union of r classes modulo $\mathfrak{m}$ distinct from $\mathfrak{m}$. Then, choosing t as first element of a v-ordering $\{u_s\}$ of E, we easily see that

$$w_E(s) = w_{E_0}(s) = \sum_{l \geq 0} \left[\frac{s-1}{rq^l}\right].$$

Consequently, we the previous notation i_0, one has $i_0 - 1 \geq r\ d(f, E)$. Then, $\overline{f}$ admits each class of E modulo $\mathfrak{m}$ as root with mutiplicity at least equal to $d(f, E)$. Moreover, if each root of $\overline{f}$ had a multiplicity $\geq p$, we would have:

$$n = \deg(f) \geq \deg(\overline{f}) \geq \deg(\overline{g}_{i_0}) = i_0 \geq 1 + rp > n.$$

We conclude in the same manner. □

Example 5.5. Let $p \in \mathbb{P}$, $V = \mathbb{Z}_{(p)}$, and $E = \{p\} \cup \mathbb{N} \setminus p\mathbb{N}$ $(r = p - 1)$. For every $f \in \mathbb{Q}[X]$, we have

$$n \leq p(p-1) \ \Rightarrow \ d(f, E) < v_p(f) + \nu_p(f).$$

Globalization. We discuss the extension of Proposition 5.4 to any Dedekind domain by showing what happens for a specific example. This seems to us a more efficient way in order to understand the general case rather than proving a general result.

Let $D = \mathbb{Z}$, $E = \mathbb{P}$, and f be a primitive polynomial in $\mathbb{Z}[X]$ of degree n. Recall that, if $f(\mathbb{P}) \subseteq \mathbb{Z}$ then, for every $p \in \mathbb{P}$, $f(\{p\} \cup \mathbb{Z} \setminus p\mathbb{Z}) \subseteq \mathbb{Z}_{(p)}$ [7]. Consequently, on the one hand, for every $p \in \mathbb{P}$, one has:

$$d_p(f, \mathbb{P}) \leq \sum_{l \geq 0} \left[\frac{k-1}{(p-1)p^l}\right],$$

on the other hand, for every $p \in \mathbb{P}$ such that $p(p-1) \geq n-1$, that is, $\sqrt{n - \frac{3}{4}} + \frac{1}{2} \leq p$, one has:

$$d_p(f, \mathbb{P}) < \nu_p(f),$$

and hence,

$$d_p(f, \mathbb{P}) \leq \inf\left(\frac{n-1}{p-1}, \nu_p(f) - 1\right).$$

Remark. A priori we have $d(f, \mathbb{P}) \geq d(f, \mathbb{Z})$, but the fact that the inequality $d_p(f, \mathbb{P}) < \nu_p(f)$ holds as soon as $n \leq p(p-1)$ is exactly the assertion given by Proposition 3.1 for $d_p(f, \mathbb{Z})$.

References

[1] M. Bhargava, *P*-orderings and polynomial functions on arbitrary subsets of Dedekind rings, *J. reine angew. Math.* **490** (1997), 101–127.

[2] M. Bhargava, Generalized Factorials and Fixed Divisors over Subsets of a Dedekind Domain, *J. Number Theory* **72** (1998), 67–75.

[3] J. Boulanger and J.-L. Chabert, Asymptotic behavior of characteristic sequences of integer-valued polynomials, *J. Number Theory* **80** (2000), 238-259.

[4] J. Boulanger, J.-L. Chabert, S. Evrard, and G. Gerboud, The Characteristic Sequence of Integer-Valued Polynomials on a Subset, in *Advances in Commutative Ring Theory*, 161-174, Lecture Notes in Pure and Appl. Math. **205**, Dekker, New York, 1999.

[5] P.-J. Cahen and J.-L. Chabert, *Integer-Valued Polynomials*, Amer. Math. Soc. Surveys and Monographs, **48**, Providence, 1997.

[6] J-L. Chabert, Generalized factorial ideals, *The Arabian Journal for Science and Engineering*, t. **26** (2001), 51–68.

[7] J.-L. Chabert, S. Chapman and W. Smith, Basis for the Ring of Polynomials Integer-Valued on Prime Numbers, in *Factorization in integral domains*, 271-284, Lecture Notes in Pure and Appl. Math. **189**, Dekker, New York, 1997.

[8] G. Pólya, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. reine angew. Math.* **149** (1919), 97–116.

[9] M. Vâjâitu, The ideal generated by the values of a polynomial over a Dedekind domain, *Rev. Roumaine Math. Pures Appl.* **42** (1997), 155-161.