DOI: 10.2478/auom-2014-0023
An. Şt. Univ. Ovidius Constanţa VERSITA **Vol. 22(1),2014, 273–280**

On the factorization of polynomials over discrete valuation domains

Doru Ştefănescu

Abstract

We study some factorization properties for univariate polynomials with coefficients in a discrete valuation domain (A, v). We use some properties of the Newton index of a polynomial $F(X) = \sum_{i=0}^{d} a_i X^{d-i} \in A[X]$ to deduce conditions on $v(a_i)$ that allow us to find some information on the degree of the factors of F.

1 Introduction

One of the oldest irreducibility criterion for univariate polynomials with coefficients in a valuation domain was given by G. Dumas [10] as a valuation approach to Schönemann-Eisenstein's criterion for polynomials with integer coefficients ([21] and [11]).

Theorem 1.1. *Let $F(X) = \sum_{i=0}^{d} a_i X^{d-i}$ be a polynomial over a discrete valuation domain A, with valued field (K, v). If the following conditions are fulfilled*

i) $v(a_0) = 0$,

ii) $\frac{v(a_d)}{d} < \frac{v(a_i)}{i}$ *for all* $i \in \{1, 2, \ldots, d-1\}$,

iii) $(v(a_d), d) = 1$,

then the polynomial $F(X)$ is irreducible in $K[X]$.

Key Words: irreducible polynomials, valuation, Newton polygon
2010 Mathematics Subject Classification: Primary 11R09; Secondary 11C08.
Received: November, 2013.
Accepted: November, 2013.

There are many recent results that provide irreducibility conditions for various classes of polynomials by using techniques coming from valuation theory (see for instance [23], [24], [2], [3], [4], [8], [5] and [9]), or Newton polygon method (see for instance [12], [13], [14], [15], [16], [17], [18], [1], [6], [7], [22] and [25]).

In this paper we will consider univariate polynomials $F(X) = \sum_{i=0}^{d} a_i X^{d-i}$ with coefficients in a discrete valuation domain (A, v), and we will study some of their factorization properties by using information on the quotients $\frac{v(a_0)-v(a_i)}{i}$. The results obtained for such polynomials are related to the irreducibility criteria of Schönemann, Eisenstein, Dumas and their generalizations, but also to the irreducibility of generalized difference polynomials (see for instance [20] and [19]).

Throughout this paper we will suppose that $v(a_0) = 0$. Our results will require the use of the *Newton index* of the polynomial F, which is defined by

$$e(F) \;=\; \max_{1\le i\le d} \frac{v(a_0)-v(a_i)}{i}.$$

We note here that the value of the Newton index in Dumas' theorem and its extensions is attained for the couple $(d, v(a_d))$, so the Newton index of the polynomial F is in this case $-v(a_d)/d$. In this paper we will also consider the case in which the maximum in the definition of $e(F)$ may be attained for an index $i \neq d$.

2 Main results

With the notations in previous section, we have

Proposition 2.1. *If* $F_1\, F_2 \in A[X] \setminus A$ *then*

$$e(F_1F_2) \;=\; \max\left(e(F_1), e(F_2)\right) .$$

Proof: We remind that one may associate to the polynomial F its Newton polygon $N(F)$ defined as the lower convex hull of the set of points

$$\{(0, v(a_d)), (1, v(a_{d-1})), \ldots, (d, v(a_0))\}$$

By the celebrated theorem of Dumas [10], we know that if $F = F_1F_2$ is a nontrivial factorization of F in $A[X]$, then the edges of the Newton polygon of F can be constructed through translates of those of the Newton polygons $N(F_1)$ and $N(F_2)$, using exactly one translate for each edge, in such a way as to form a polygonal path with the slopes of the edges increasing.

Using this result, it will be sufficient to observe that the quotient $\frac{v(a_0)-v(a_i)}{i}$ is the slope of the line joining the points $(d, v(a_0))$ and $(d-i, v(a_i))$. □

In the following result we will suppose that the Newton index of F is attained for an index $i \in \{1, \ldots, d\}$, fact that will not necessarily imply the irreducibility of F, but will allow us in case F is reducible to obtain some information on the degree of one of its factors.

Theorem 2.2. *Let (A, v) be a discrete valuation domain, and let*

$$F(X) = a_0X^d + a_1X^{d-1} + \cdots + a_{d-1}X + a_d \in A[X].$$

Suppose that $v(a_0) = 0$ and that there exists an index $s \in \{1, 2, \ldots, d\}$ such that the following conditions are satisfied:

(a) $\dfrac{v(a_s)}{s} < \dfrac{v(a_i)}{i}$ for $i \in \{1, 2, ..., d\}, i \neq s$;

(b) $sv(a_d) - dv(a_s) = 1$.

(c) $(s, v(a_s)) = 1$;

Then the polynomial F is either irreducible in $A[X]$, or has a factor whose degree is a multiple of s.

Proof: Let us assume that there exists a nontrivial factorization $F = F_1F_2$ of the polynomial F in $A[X]$, and let us denote

$$d = \deg F,\ d_1 = \deg(F_1) \geq 1,\ d_2 = \deg(F_2) \geq 1,$$

and

$$m = v(a_d),\ a = v(a_s).$$

We also put

$$m_1 = v(F_1(0)) \quad \text{and} \quad m_2 = v(F_2(0)).$$

With these notations, condition (b) reads

$$sm - ad = 1. \tag{1}$$

Now, since condition (a) shows that $e(F) = -\frac{v(a_s)}{s}$, and by Proposition 2.1 we have $e(F) = \max\{e(F_1), e(F_2)\}$, we first deduce that

$$-\frac{a}{s} = -\frac{v(a_s)}{s} = e(F) \geq e(F_1) \geq -\frac{v(F_1(0))}{d_1} = -\frac{m_1}{d_1},$$

so we must have

$$ad_1 \leq sm_1. \tag{2}$$

On the other hand, since

$$d = \deg(F_1F_2) = \deg(F1) + \deg(F_2) = d_1 + d_2$$

and

$$m = v(F_1(0)F_2(0)) = v(F_1(0)) + v(F_2(0)) = m_1 + m_2,$$

we see by (1) and (2) that

$$sm_2 - ad_2 \leq sm - ad = 1.$$

Now, since

$$-\frac{a}{s} = e(F) \geq e(F_2) \geq -\frac{m_2}{d_2},$$

we deduce that $ad_2 \leq sm_2$, so we must have

$$0 \leq sm_2 - ad_2 \leq 1. \tag{3}$$

Next, since $sm_2 - ad_2$ is an integer, (3) shows that it can only take the value 0 or 1, so we distinguish two cases:

Case 1: $sm_2 - ad_2 = 0$. Here, since condition (b) implies in particular the fact that a and s are coprime, we see that d_2 must be divisible by s.

Case 2: $sm_2 - ad_2 = 1$. In this case we have $s(m - m_1) - a(d - d_1) = 1$, which in view of (1) shows that $sm_1 = ad_1$, and since a and s are coprime, we see now that d_1 must be divisible by s.

Therefore, if the polynomial F is reducible, the degree of one of its factors must be a multiple of s. ∎

With the notations in Theorem 2.2, one has the following result.

Corollary 2.3. *If $d \geq 4$ and $s > d/2$, then the polynomial F is either irreducible, or has a divisor of degree s.*

Proof: If F would have a factor of degree ks, with $k \geq 2$, then we would obtain

$$d > ks > k\frac{d}{2} \geq d,$$

a contradiction. ∎

3 Examples

1) Let $F(X)=X^d+p^d(p-1)X^2+p^{d-2}X+p^{d-1}\in\mathbb{Z}[X]$, with $d\geq 3$ and p a prime number, and let us consider the usual p–adic value on $\mathbb{Z}$, denoted by v. Since

$$\frac{v(a_{d-1})}{d-1}=\frac{d-2}{d-1}<\frac{d}{d-2}=\frac{v(a_{d-2})}{d-2}$$

and

$$\frac{v(a_{d-1})}{d-1}=\frac{d-2}{d-1}<\frac{d-1}{d}=\frac{v(a_d)}{d},$$

we may take $s=d-1$, and since $sv(a_d)-dv(a_s)=(d-1)^2-d(d-2)=1$, we conclude by Theorem 2.2 that F is either irreducible, or has a factor of degree $d-1$, and hence also a linear factor. On the other hand, one may easily check that F has no integer solutions, and hence is an irreducible polynomial.

2) Let $F(X,Y)=Y^d+q(X)Y+r(X)\in\mathbb{Z}[X,Y]$, where $q,r\in\mathbb{Z}[X]$ with $\deg(q)=\deg(r)=1$. Using now the discrete valuation on $\mathbb{Z}[X]$ given by $v(h)=-\deg(h)$ for $h\in\mathbb{Z}[X]$, we see that

$$\frac{v(q)}{d-1}=\frac{-1}{d-1}<\frac{-1}{d}=\frac{v(r)}{d},$$

so with the notation in Theorem 2.2 we have $s=d-1$. On the other hand, using the same notation we observe that

$$sv(a_d)-dv(a_s)=(d-1)v(r)-dv(q)=1.$$

It follows that F is either irreducible in $\mathbb{Z}[X,Y]$, or has a linear factor with respect to Y.

3) Let K be a field of characteristic zero, $d\geq 4$ an integer, and let

$$F(X,Y)=Y^d+(X^{d-2}+1)Y^2+(X^d+X+1)Y+X^{d+1}+X^2+1\in K[X,Y].$$

We represent the polynomial F as

$$F(X,Y)\;=\;Y^d+a_{d-2}(X)Y^2+a_{d-1}(X)Y+a_d(X)$$

with $a_{d-2}(X)=X^{d-2}+1$, $a_{d-1}(X)=X^d+X+1$ and $a_d(X)=X^{d+1}+X^2+1$. Using now the discrete valuation on $K[X]$ given by $v(h)=-\deg(h)$ for $h\in K[X]$, we observe that

$$\frac{v(a_{d-2})}{d-2}=-1,\quad \frac{v(a_{d-1})}{d-1}=-\frac{d}{d-1}\quad\text{and}\quad\frac{v(a_d)}{d}=-\frac{d+1}{d}.$$

Therefore $\frac{v(a_{d-1})}{d-1}<\frac{v(a_{d-2})}{d-2}$ and $\frac{v(a_{d-1})}{d-1}<\frac{v(a_d)}{d}$, so we may take $s=d-1$, and since $sv(a_d)-dv(a_s)=1$, we conclude by Theorem 2.2 that F is either irreducible in $K[X,Y]$, or has a factor whose degree with respect to Y is a multiple of $d-1$, that is F is either irreducible, or has a linear factor in Y.

Acknowledgement. The publication of this paper was supported by the grants PN-II-ID-WE-2012-4-161 and PN-II-ID-WE-2012-4-169.

References

[1] A. Bishnoi, S. K. Khanduja, K. Sudesh, *Some extensions and applications of the Eisenstein irreducibility criterion*, Developments in Mathematics 18 (2010), 189–197.

[2] A.I. Bonciocat, N.C. Bonciocat, *Some classes of irreducible polynomials*, Acta Arith. 123 (2006), no. 4, 349-360.

[3] A.I. Bonciocat, N.C. Bonciocat, *A Capelli type theorem for multiplicative convolutions of polynomials*, Math. Nachr. 281 (2008), no. 9, 1240-1253.

[4] N.C. Bonciocat, *On an irreducibility criterion of Perron for multivariate polynomials*, Bull. Math. Soc. Sci. Math. Roumanie 53 (101) No. 3 (2010), 213-217.

[5] N.C. Bonciocat, *From prime numbers to irreducible multivariate polynomials*, An. Ştiint. Univ. Ovidius Constanţa Ser. Mat. 19 (2011) no. 2, pag. 37 - 53.

[6] N.C. Bonciocat, *Schönemann-Eisenstein-Dumas-type irreducibility conditions that use arbitrarily many prime numbers*, arXiv:1304.0874v1.

[7] N.C. Bonciocat, Y. Bugeaud, M. Cipu, M. Mignotte, *Irreducibility criteria for sums of two relatively prime polynomials*, Int. J. Number Theory 9 (6) (2013), 1529–1539.

[8] N.C. Bonciocat, A. Zaharescu, *Irreducible multivariate polynomials obtained from polynomials in fewer variables*, J. Pure Appl. Algebra 212 (2008), no. 10, 2338-2343.

[9] N.C. Bonciocat, A. Zaharescu, *Irreducible multivariate polynomials obtained from polynomials in fewer variables, II*, Proc. Indian Acad. Sci. Math. Sci. 121 (2011) no. 2, 133-141.

[10] G. Dumas, *Sur quelques cas d'irréducibilité des polynômes à coefficients rationnels*, Journal de Math. Puers et Appl., 12 (1906), 191-258.

[11] G. Eisenstein, *Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt*, J. Reine Angew. Math. 39 (1850), 160–182.

[12] M. Filaseta, *On the irreducibility of almost all Bessel Polynomials*, Acta Math. 174 (1995), no. 2, 383–397.

[13] M. Filaseta, *A generalization of an irreducibility theorem of I. Schur*, in: Analytic Number Theory, Proc. Conf. in Honor of Heini Halberstam, vol. 1, (B.C. Berndt, H.G. Diamond, and A.J. Hildebrand, eds.), Birkhäuser, Boston, 1996, pp. 371–395.

[14] M. Filaseta, T. Kidd, O. Trifonov, *Laguerre polynomials with Galois group A_m for each m*, J. Number Theory 132 (2012), 776–805.

[15] M. Filaseta, C. Finch, J.R. Leidy, *T.N. Shorey's influence in the theory of irreducible polynomials*, Diophantine Equations (ed. N. Saradha), Narosa Publ.House, New Delhi, 2005, pp. 77–102.

[16] M. Filaseta and T.-Y. Lam, *On the irreducibility of the Generalized Laguerre polynomials*, Acta Arith. 105 (2002), no. 2, 177–182.

[17] M. Filaseta and O. Trifonov, *The irreducibility of the Bessel Polynomials*, J. Reine Angew. Math. 550 (2002), 125–140.

[18] M. Filaseta and R. L. Williams, Jr., *On the irreducibility of a certain class of Laguerre polynomials*, J. Number Theory 100 (2003), no. 2, 229–250.

[19] L. Panaitopol, D. Ştefănescu, *On the generalized difference polynomials*, Pacific J. Math. 143 (1990), 341–348.

[20] L.A. Rubel, A. Schinzel, H. Tverberg, *On difference polynomials and hereditary irreducible polynomials*, J. Number Theory 12 (1980), 230–235.

[21] T. Schönemann, *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*, J. Reine Angew. Math. 32 (1846), 93–105.

[22] D. Ştefănescu, *On the irreducibility of bivariate polynomials*, Bull. Math. Soc. Sci. Math. Roumanie, 56 (104) (2013), 377–384.

[23] A. Zaharescu, *Irreducibility over valued fields in the presence of a secondary valuation*, Hiroshima Math. J. 34 (2004), 167–176.

[24] A. Zaharescu, *Residual transcendental extentions of valuations, irreducible polynomials and trace series over p–adic fields*, Bull. Math. Soc. Sci. Math. Roumanie, 56 (104) (2013), 125-131.

[25] S.H. Weintraub, *A mild generalization of Eisenstein's criterion*, Proc. Amer. Math. Soc. 141 (2013), no. 4, 1159–1160.

Doru Ştefănescu
Department of Theoretical Physics and Mathematics,
University of Bucharest
Bdul M. Kogălniceanu 36–46, Bucharest, Romania
Email: stef@rms.unibuc.ro