On a factorization result of Ştefănescu

Sanjeev Kumar and Jitender Singh

Department of Mathematics, SGGS College, Chandigarh, India; Department of Mathematics, Guru Nanak Dev University, Amritsar, India

ABSTRACT

Ştefănescu proved an elegant factorization result for polynomials over discrete valuation domains [On the factorization of polynomials over discrete valuation domains, Versita 22:1 (2014), 273–280]. We generalize Ştefănescu’s result to include a larger class of polynomials over such domains.

ARTICLE HISTORY

Received 30 December 2021
Communicated by Alfred Geroldinger

KEYWORDS
Discrete valuation domain; Dumas irreducibility criterion; Eisenstein irreducibility criterion; factorization; irreducibility; Newton index; polynomials; Schönemann irreducibility criterion

2020 MATHEMATICS SUBJECT CLASSIFICATION
Primary: 30C10; 12E05; 11C08

The augean work of identifying irreducible polynomials in a prescribed domain is a classical yet exciting theme as is evident from the fact that the prolific irreducibility criteria due to Schönemann [4] and Eisenstein [2] have witnessed exquisite extensions and generalizations for decades. Recently, Weintraub [6] generalized Eisenstein’s criterion and also provided a correction to the false claim made by Eisenstein himself [2]. However, one of the earliest known generalization is credited to Dumas [1], who generalized the Schönemann-Eisenstein criteria by establishing an intimate connection between the valuation theoretic properties of the polynomials having integer coefficients and the associated geometric properties exhibited by the Newton polygons.

Let \((R, v)\) be a discrete valuation domain and \(f = a_0 + a_1 x + \cdots + a_n x^n \in R[x]\) be a nonconstant polynomial. For any index \(i \in \{0, 1, \ldots, n - 1\}\), let \(m_i(f)\) be the slope of the line segment joining the points \((n, v(a_n))\) and \((i, v(a_i))\), that is,

\[
m_i(f) = \frac{v(a_n) - v(a_i)}{n - i}.
\]

The Newton index \(e(f)\) of \(f\) is then defined to be the number \(\max_{0 \leq i \leq n-1} \{m_i(f)\}\) and the following identity

\[
\max\{e(f_1), e(f_2)\} = \max\{e(f_1 f_2)\} \text{ for all } f_1, f_2 \in R[x],
\]

is well acknowledged. In [5, Theorem 2.2], some factorization properties for polynomials over a discrete valuation ring \((R, v)\) were investigated and the following main result was established.

CONTACT Jitender Singh at jitender.math@gndu.ac.in; sonumaths@gmail.com

© 2022 Taylor & Francis Group, LLC
Theorem A. Let \((R, v)\) be a discrete valuation domain and \(f = a_0 + a_1x + \cdots + a_nx^n \in R[x]\). If there exists an index \(s \in \{0, \ldots, n - 1\}\) such that

(a) \(v(a_n) = 0\); \(m_i(f) < m_s(f)\) for all \(i = 0, 1, \ldots, n - 1, i \neq s\),

(b) \(n(n-s)(m_0(f) - m_s(f)) = -1\),

then the polynomial \(f\) is either irreducible in \(R[x]\), or has a factor whose degree is a multiple of \(n - s\).

From the hypothesis (a) in Theorem A we have \(v(a_n) = 0\), which in view of the hypothesis (b) in Theorem A implies that \(v(a_i)\) and \(n - s\) are coprime for \(s \neq 0\). Consequently, the hypotheses (a) and (b) in Theorem A together yield the factorization result of Weintraub [6], that is, if \(f(x) = g(x)h(x)\) is any factorization of the polynomial \(f\) in \(R[x]\), then \(\min\{\deg g, \deg h\} \leq s\) or equivalently

\[
\max\{\deg g, \deg h\} \geq (n - s).
\]

Moreover, the hypothesis (b) in Theorem A enables us to proceed one step ahead of the aforementioned inequality by asserting \(n - s\) as a divisor of \(\deg g\) or \(\deg h\).

However, in case if \(R = \mathbb{Z}\) and \(v = v_p\) the associated \(p\)-adic discrete valuation of \(\mathbb{Z}\) with \(s = 0\), then the assumption (b) in the hypothesis of Theorem A becomes void. So, in this particular context, an amelioration of the above result is necessary. In this article, we modify the hypothesis (b) of Theorem A in order to allow \(s = 0\) without ambiguity and then prove a mild generalization, which we hope paves the way for a significant criterion that rectifies an error Eisenstein made himself, that too with a weaker hypothesis. More precisely, we have the following result.

Theorem 1. Let \((R, v)\) be a discrete valuation domain and \(f = a_0 + a_1x + \ldots + a_nx^n \in R[x]\) with \(v(a_n) = 0\). Let there be an index \(s \in \{0, \ldots, n - 1\}\) such that

(a) \(m_i(f) < m_s(f)\) for all \(i = 0, 1, \ldots, n - 1, i \neq s\),

(b) \(d_s = \gcd(n - s, v(a_i))\) satisfies

\[
(-d_s) = \begin{cases} 
  n(n-s)(m_0(f) - m_s(f)), & \text{if } s \neq 0; \\
  -1, & \text{if } s = 0. 
\end{cases}
\]

Then any factorization \(f(x) = f_1(x)f_2(x)\) of \(f\) in \(R[x]\) has a factor whose degree is a multiple of \((n - s)/d_s\). In particular, if \(s = 0\), then \(f\) is irreducible.

To the best of our knowledge, all earlier investigations about factorization and irreducibility of polynomials have been based on the coprimality of \(v(a_i)\) and \(n - s\), which has now been relaxed in Theorem 1 above for the case \(s > 0\). The examples below justify that there exist polynomials whose factorization properties can be deduced using Theorem 1 wherein Theorem A fails to be applicable.

Examples. Let \(p\) be a prime number and \(v = v_p\), the discrete valuation on \(\mathbb{Z}\).

(1) Consider the polynomial

\[
X(x) = (a_0 + p^2(p - 1)a_2x^2)p^{n-2} + p^{n-3}a_1x + a_nx^n \in \mathbb{Z}[x], \quad n \geq 5,
\]

where \(n\) is odd, \(a_i > 0\) and \(v_p(a_i) = 0\) for \(i \in \{0, 1, 2, n\}\); \(a_i = 0\) for \(i \notin \{0, 1, 2, n\}\). Taking \(s = 1\), we observe that

\[
m_i(X) - m_1(X) \leq - \frac{n-2}{n} + \frac{n-3}{n-1} = \frac{-2}{n(n-1)} < 0,
\]
and also \( n(n - 1)(m_0(X) - m_1(X)) = -2 = -d_1 \). By Theorem 1 either \( X \) is irreducible or \( X \) has a factor whose degree is a multiple of \((n - 1)/2\).

(2) The polynomial

\[
Y(x) = (1 + p^2x^2)p^{n-2} + p^{n-4}x^2 + x^n \in \mathbb{Z}[x], \quad n \geq 6,
\]

where \( n \) is even satisfies the hypothesis of Theorem 1 with \( s = 2 \), \( a_0 = p^{n-2}, a_2 = p^{n-4}, a_3 = p^{n+1} \); \( a_i = 0 \) for \( i \not\in \{0, 2, 3, n\} \); \( m_1(Y) - m_2(Y) \leq \frac{-2}{n(n-2)} < 0 \), and \( n(n-1) \) \((m_0(Y) - m_1(Y)) = -2 = -d_1 \). So, either \( Y \) is irreducible or \( Y \) has a factor of degree equal to a multiple of \((n - 2)/2\).

(3) Let \( n > 2 \) and \( d \) be a divisor of \( n - 1 \). Now consider the polynomial

\[
Z(x, y) = a_0(x) + a_1(x)y + y^n \in \mathbb{Z}[x, y],
\]

where each of \( a_0(x) \) and \( a_1(x) \) is an irreducible polynomial of degree \( d \) in \( \mathbb{Z}[x] \). For non-zero \( g \in \mathbb{Z}[x] \), define \( v(g) = -\deg(g) \) and \( v(0) = \infty \). Taking \( s = 1 \), we have

\[
m_1(Z) - m_1(Z) \leq \frac{d}{n} - \frac{d}{n - 1} = \frac{-d}{n(n - 1)} < 0,
\]

and also \( n(n - 1)(m_0(Z) - m_1(Z)) = -d = -\gcd(v(a_0(x)), n - 1) \). By Theorem 1, \( Z \) has a factor (with respect to \( y \)) whose degree is a multiple of \((n - 1)/d \). This example can also be viewed in \( K[x, y] \) where \( K \) is any field of characteristic zero, and \( v \) is the discrete degree valuation on \( K \).

**Proof of Theorem 1.** For the case \( s = 0 \), Theorem 1 is precisely the well-known classical result of Dumas (See [5, p.273, Theorem 1.1]). So, let \( s > 0 \). Let \( k_i = \deg(f_i), x_i = v(f_i(0)) \) for \( i = 1, 2 \). Let \( y_i = v(a_i) \) for each \( j = 0, 1, ..., n - 1 \). With these notations, the hypothesis (b) in the theorem becomes

\[
(n - s)y_0 - ny_s = d_s. \tag{1}
\]

By hypothesis (a) in the theorem, we have \( e(f) = -v(a_s)/(n - s) = -y_s/(n - s) \) and since \( e(f) \geq e(f_i) \), we deduce that

\[-y_s/(n - s) = e(f) \geq e(f_i) \geq -v(f_i(0))/k_i = -x_i/k_i. \]

So we must have \( y_ik_i \leq (n - s)x_i \) for \( i = 1, 2 \). We also have

\[
y_0 = v(f(0)) = v(f_1(0)) + v(f_2(0)) = x_1 + x_2; \quad n = k_1 + k_2.
\]

Using these in (1), we get that

\[
0 \leq (n - s)x_2 - k_2y_s = (n - s)x_2 + k_1y_s - ny_s \leq (n - s)(x_2 + x_1) - ny_s = d_s.
\]

Consequently, if we let \( \kappa = ((n - s)/d_s)x_2 - k_2(y_s/d_s) \), then \( 0 \leq \kappa \leq 1 \), and so, either \( \kappa = 0 \) or \( \kappa = 1 \).

If \( \kappa = 0 \), then in view of (b), the number \((n - s)/d_s \) must divide \( k_2 \), and so, \( k_2 \) must be a multiple of \((n - s)/d_s \). On the other hand, if \( \kappa = 1 \), then

\[
((n - s)/d_s)(y_0 - x_1) - (n - k_1)(y_s/d_s) = 1,
\]

which in view of (1) gives \((n - s)/d_s)x_1 = k_1(y_s/d_s) \), and so, the number \((n - s)/d_s \) divides \( k_1 \). In this case, \( k_1 \) is a multiple of \((n - s)/d_s \). Thus, in either of the cases, the degree of one of \( f_1 \) or \( f_2 \) is a multiple of \((n - s)/d_s \). This completes the proof.

\[\square\]

Most of the factorization results on polynomials over a discrete valuation domain \((R, v)\) require to take \( v(a_i) \) and \( n - s \) to be coprime, whenever \( s \) is the smallest index for which the minimum
of the quantity $v(a_i)/(n - i)$, $0 \leq i \leq n - 1$ is $v(a_n)/(n - s)$ (See for example, Jhorar and Khanduja [3]). In the case when $v(a_i)$ and $n - s$ are not coprime, we have the following result.

Lemma 2. Let $(R, v)$ be a discrete valuation domain and $f = a_0 + a_1x + \ldots + a_nx^n \in R[x]$ with $v(a_n) = 0$. If $d_i = \gcd(n - s, v(a_i)) > 1$, then any factorization $f(x) = g(x)h(x)$ of $f$ in $R[x]$ has $\max\{\deg g, \deg h\} \geq (n - s)/d_i$.

**Proof.** Assume on the contrary that $\max\{\deg g, \deg h\} < (n - s)/d_i$. Then $\deg g < (n - s)/d_i$ and $\deg h < (n - s)/d_i$. Since $f(x) = g(x)h(x)$, we have

$$n = \deg f = \deg g + \deg h < 2(n - s)/d_i \leq 2n/d_i,$$

which yields $d_i < 2$, and so, $d_i = 1$. This contradicts the hypothesis. \qed

Theorem 3. Let $(R, v)$ be a discrete valuation domain and $f = a_0 + a_1x + \ldots + a_nx^n \in R[x]$ with $v(a_n) = 0$. Let there be an index $s \in \{0, \ldots, n - 1\}$ such that $m_i(f) < m_s(f)$ for all $i = 0, 1, \ldots, n - 1$, $i \neq s$ and $d_i = \gcd(n - s, v(a_i))$. Then any factorization $f(x) = g(x)h(x)$ of $f$ in $R[x]$ has $\max\{\deg g, \deg h\} \geq (n - s)/d_i$.

**Proof.** The theorem in the case $d_i = 1$ follows from a result proved in Jhorar and Khanduja [3, Theorem 1.2] for more general domains. On the other hand if $d_i > 1$, then the theorem follows from Lemma 2. \qed

**Acknowledgments**

The authors are highly indebted to the anonymous referees for useful comments.

**ORCID**

Sanjeev Kumar http://orcid.org/0000-0001-6882-4733

Jitender Singh http://orcid.org/0000-0003-3706-8239

**References**

[1] Dumas, G. (1906). Sur quelques cas d’irréducibilité des polynômes à coefficients rationnels. *J. de Math. Puers et Appl.* 12:191–258.

[2] Eisenstein, F. G. M. (1850). Über die Irreducibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt. *J. Reine Angew. Math.* 39:160–179.

[3] Jhorar, B., Khanduja, S. K. (2017). A generalization of the Eisenstein–Dumas–Schönemann irreducibility criteria. *Proc. Edinburgh Math. Soc.* 60(4):937–945. DOI: 10.1017/S0013091516000638.

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

[5] Ştefânescu, D. (2014). On the factorization of polynomials over discrete valuation domains. *Versita.* 22(1):273–280. DOI: 10.2478/auom-2014-0023.

[6] Weintraub, S. H. (2012). A mild generalization of Eisenstein’s criterion. *Proc. Amer. Math. Soc.* 141(4):1159–1160. DOI: 10.1090/S0002-9939-2012-10880-9.