On the irreducible factors of a polynomial II

Anuj Jakhar, Srinivas Kotyada

Institute of Mathematical Sciences, HBNI, CIT Campus, Taramani,
Chennai - 600113, Tamil Nadu, India.
anujjakhar@imsc.res.in, srini@imsc.res.in

Abstract

We give a lower bound for the degree of an irreducible factor of a given polynomial. This improves and generalizes the results obtained in [4, On the irreducible factors of a polynomial, to appear in Proc. Amer. Math. Soc., 2019].

Keywords : Irreducibility; Newton Polygon; Polynomials; Valued fields.

2010 Mathematics Subject Classification : 12E05; 11R09; 12J10.

1 Introduction

In [4, Theorem 1.1], the following result was proved for polynomials having integer coefficients.

Theorem 1.1. *Let p be a prime number and let $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with integer coefficients. Suppose that p does not divide a_s for some $s \leq n$, and that $a_j \neq 0$ for some j with $0 \leq j < s$. For $0 \leq i < s$, let r_i be the largest positive integer such that p^{r_i} divides a_i (where $r_i = \infty$ if $a_i = 0$). Let $k(< s)$ be the smallest non-negative integer such that $\min\limits_{0 \leq i < s} \frac{r_i}{s-i} \geq \frac{r_k}{s-k}$. Suppose further that r_k and $(s-k)$ are coprime. Then $f(x)$ has an irreducible factor of degree at least $s-k$ over $\mathbb{Q}$.*

In this paper, we show that the above coprimality condition of r_k and $s-k$ can be weakened. Moreover, invoking the theory of Newton polygon (defined below), we improve the lower bound for the degree of an irreducible factor. Furthermore, we shall prove the theorem for polynomials having coefficients from the valuation ring of an arbitrary valued field and indicate how to derive it for polynomials with integer coefficients.

Let v be a Krull valuation of a field K with value group G_v and valuation ring R_v having maximal ideal M_v. We shall denote by v^x the Gaussian prolongation of v to $K(x)$ defined on $K[x]$ by

$$v^x\big(\sum_i a_i x^i\big) = \min_i\{v(a_i)\}, \quad a_i \in K. \tag{1.1}$$

For a polynomial $h(x) \in R_v[x]$, $\bar{h}(x)$ will stand for the polynomial over R_v/M_v obtained by replacing each coefficient of $h(x)$ by its v-residue. Below we define the notion of Newton polygon (see [3, Section 6.4], [5, Definition 1.D] for details).

Definition 1.2. Let (K, v) be a valued field with value group G_v and valuation ring R_v having maximal ideal M_v. Let $\phi(x) \in R_v[x]$ be a monic polynomial with $\bar{\phi}(x)$ irreducible over R_v/M_v and v^x be the Gaussian prolongation defined by (1.1). Let $f(x) \in R_v[x]$ be a polynomial not divisible by $\phi(x)$ with ϕ-expansion[1] $\sum\limits_{i=0}^{n} a_i(x)\phi(x)^i, a_n(x) \neq 0$. Let P_i stand for the pair $(i, v^x(a_{n-i}(x)))$ when $a_{n-i}(x) \neq 0,\ 0 \leq i \leq n$. For distinct pairs P_i, P_j, let μ_{ij} denote the element of the divisible closure of G_v defined by

$$\mu_{ij} = \frac{v^x(a_{n-j}(x)) - v^x(a_{n-i}(x))}{j - i};$$

in case v is a real valuation, μ_{ij} is the slope of the line segment joining P_i and P_j. Let i_1 denote the largest index $0 < i_1 \leq n$ such that

$$\mu_{0i_1} = \min_j \{\mu_{0j} : 0 < j \leq n, a_{n-j}(x) \neq 0\}.$$

If $i_1 < n$, let i_2 be the largest index such that $i_1 < i_2 \leq n$ and

$$\mu_{i_1 i_2} = \min_j \{\mu_{i_1 j} : i_1 < j \leq n, a_{n-j}(x) \neq 0\}.$$

Proceeding in this way if $i_\ell = n$, then the ϕ-Newton polygon of $f(x)$ is said to have ℓ many edges whose slopes are defined to be $\mu_{0i_1}, \mu_{i_1 i_2}, \cdots, \mu_{i_{\ell-1} i_\ell}$ which are in strictly increasing order. The pairs $P_0, P_{i_1}, P_{i_2}, \cdots, P_{i_\ell}$ are called the successive vertices of the ϕ-Newton polygon of $f(x)$ with respect to the valuation v.

We now state our main result.

Theorem 1.3. *Let v be a Krull valuation of a field K with value group G_v and valuation ring R_v having maximal ideal M_v. Let $\phi(x) \in R_v[x]$ be a monic polynomial of degree*

[1] On dividing by successive powers of $\phi(x)$, every polynomial $f(x) \in K[x]$ can be uniquely written as a finite sum $\sum_{i \geq 0} f_i(x)\phi(x)^i$ with $\deg(f_i(x)) < \deg(\phi(x))$, called the ϕ-expansion of $f(x)$.

m which is irreducible modulo M_v. Let $f(x) \in R_v[x]$ be a polynomial not divisible by $\phi(x)$. Assume that the ϕ-Newton polygon of $f(x)$ has ℓ many edges with positive slopes λ_j, $1 \leq j \leq \ell$. If $\mathfrak{d}_j$ is the smallest positive number such that $\mathfrak{d}_j\lambda_j \in G_v$ for $1 \leq j \leq \ell$, then $f(x)$ has an irreducible factor of degree at least $\max\limits_{1\leq j\leq \ell}\{\mathfrak{d}_j m\}$ over K.

With the notations as in the above theorem, the following corollary is an immediate consequence of Theorem 1.3.

Corollary 1.4. *Let the notations and assumptions be as in the above theorem. Then for any factorization $f_1(x)f_2(x)$ of $f(x)$ over K, we have*

$$\min\{\deg f_1(x), \deg f_2(x)\} \leq \deg f(x) - \max_{1\leq j\leq \ell}\{\mathfrak{d}_j m\}.$$

When $G_v = \mathbb{Z}$, Theorem 1.3 immediately gives the following result.

Theorem 1.5. *Let p be a prime number and $f(x) = \sum\limits_{i=0}^{n} a_i x^i$ with $a_0 \neq 0$ be a polynomial having integer coefficients. Assume that the x-Newton polygon of $f(x)$ with respect to the p-adic valuation v_p has ℓ many edges with positive slopes λ_j, $1 \leq j \leq \ell$. If $\lambda_j = \frac{r_j}{s_j}$ with* $\gcd(r_j, s_j) = 1$, *then $f(x)$ has an irreducible factor of degree at least $\max\limits_{1\leq j\leq \ell}\{s_j\}$ over $\mathbb{Q}$.*

Remark 1.6. It may be noted that Theorem 1.1 follows from Theorem 1.5 because in Theorem 1.1, the x-Newton polygon of $f(x)$ with respect to v_p has an edge having positive slope $\frac{r_k}{s-k}$ with $\gcd(r_k, s-k) = 1$.

For the history of the problem and related literature, the reader may refer to [4]. Before we get down to the proof of the theorem, an example may illustrate the importance of the result.

Example 1.7. Let a, b be integers with $b \neq 0$. Let q be a prime number and s, r denote the highest power of q dividing a, b respectively. Let n, m be positive integers with $n > m$ and $(n-m)r > ns > 0$. Then by Theorem 1.5, $f(x) = x^n + ax^m + b$ has an irreducible factor of degree at least $\max\{\frac{m}{\gcd(m,r-s)}, \frac{n-m}{\gcd\,(n-m,s)}\}$ over $\mathbb{Q}$. In the particular cases, when either $n = m+1$ with $\gcd(n-1, r-s) = 1$ or $m = 1$ with $\gcd\,(n-1, s) = 1$, then $f(x)$ has an irreducible of degree at least $n-1$ over $\mathbb{Q}$. Therefore, in these cases, if $f(x)$ does not have a linear factor, then $f(x)$ is irreducible over $\mathbb{Q}$. However, Theorem 1.1 provides no information about the irreducible factor of $f(x)$ when $n = m+1$.

2 Proof of Theorem 1.3.

2.1 Some Notations and Definitions.

Let v be a Krull valuation of a field K with value group G_v and valuation ring R_v having maximal ideal M_v. We fix a prolongation $\tilde{v}$ of v to an algebraic closure $\widetilde{K}$ of K. For an element α belonging to the valuation ring $R_{\tilde{v}}$ of $\tilde{v}$, $\bar{\alpha}$ will denote its $\tilde{v}$-residue, i.e., the image of α under the canonical homomorphism from $R_{\tilde{v}}$ onto its residue field $R_{\tilde{v}}/M_{\tilde{v}}$.

Definition 2.1. Let v be a henselian Krull valuation of a field K and $\tilde{v}$ the unique prolongation of v to the algebraic closure $\widetilde{K}$ of K with value group $G_{\tilde{v}}$. A pair (α, δ) belonging to $\widetilde{K} \times G_{\tilde{v}}$ is called a minimal pair (more precisely (K, v)-minimal pair) if whenever β belongs to $\widetilde{K}$ with $[K(\beta) : K] < [K(\alpha) : K]$, then $\tilde{v}(\alpha - \beta) < \delta$.

Example 2.2. If $\phi(x)$ is a monic polynomial of degree $m \geq 1$ with coefficients in R_v such that $\bar{\phi}(x)$ is irreducible over the residue field of v and α is a root of $\phi(x)$, then (α, δ) is a (K, v)-minimal pair for each positive δ in $G_{\tilde{v}}$, because whenever $\beta \in \widetilde{K}$ has degree less than m, then $\tilde{v}(\alpha - \beta) \leq 0$, for otherwise $\bar{\alpha} = \bar{\beta}$, which in view of the Fundamental Inequality [2, Theorem 3.3.4] would lead to $[K(\beta) : K] \geq m$.

Definition 2.3. Let $(K, v), (\widetilde{K}, \tilde{v})$ be as in the above definition and (α, δ) belonging to $\widetilde{K} \times G_{\tilde{v}}$ be a (K, v)-minimal pair. The valuation $\widetilde{w}_{\alpha,\delta}$ of a simple transcendental extension $\widetilde{K}(x)$ of $\widetilde{K}$ defined on $\widetilde{K}[x]$ by

$$\widetilde{w}_{\alpha,\delta}\big(\sum_i c_i(x-\alpha)^i\big) = \min_i\{\tilde{v}(c_i) + i\delta\}, \quad c_i \in \widetilde{K} \tag{2.1}$$

will be referred to as the valuation with respect to the minimal pair (α, δ); the restriction of $\widetilde{w}_{\alpha,\delta}$ to $K(x)$ will be denoted by $w_{\alpha,\delta}$. For more details on the classification of extensions of a valuation from a base field K to rational function fields, the reader may refer to the paper [7] and references therein.

With (α, δ) as above, if $\phi(x)$ is the minimal polynomial of α over K, then it is well known [1, Theorem 2.1] that for any polynomial $f(x) \in K[x]$ with ϕ-expansion $\sum_i a_i(x)\phi(x)^i$, one has

$$w_{\alpha,\delta}(f(x)) = \min_i\{\tilde{v}(a_i(\alpha)) + i w_{\alpha,\delta}(\phi(x))\}. \tag{2.2}$$

Remark 2.4. In particular, if (α, δ) is a minimal pair of the type described in Example 2.2 with $\phi(x)$ as the minimal polynomial of α over K, then for any polynomial $h(x) =$

$\sum_{i=0}^{m-1} a_i x^i \in K[x]$ having degree less than $m = \deg \phi(x)$, one has

$$\tilde{v}(h(\alpha)) = v^x(h(x)). \tag{2.3}$$

Clearly (2.3) needs to be verified when $m > 1$. Keeping in mind that $\bar{\phi}(x)$ is irreducible over R_v/M_v of degree $m > 1$, it follows that $\tilde{v}(\alpha) = 0$. If (2.3) were false, then the triangle inequality would imply that $\tilde{v}(h(\alpha)) > \min_i\{\tilde{v}(a_i\alpha^i)\} = v(a_j)$ (say), which yields $\sum_{i=0}^{m-1} \left(\overline{\frac{a_i}{a_j}}\right)(\bar{\alpha})^i = \bar{0}$, contradicting the fact that $\bar{\alpha}$ is a root of an irreducible polynomial $\bar{\phi}(x)$ of degree m. Hence (2.3) is proved.

Notation 2.5. Let (α, δ) be as in Definition 2.3 and $\phi(x)$ be the minimal polynomial of α having degree m over K. Let $w_{\alpha,\delta}$ be as in (2.2). For any non-zero polynomial $f(x) \in K[x]$ with ϕ-expansion $\sum_i a_i(x)\phi(x)^i$, we shall denote by $I_{\alpha,\delta}(f), S_{\alpha,\delta}(f)$ respectively the minimum and the maximum integers belonging to the set $\{i \mid w_{\alpha,\delta}(f(x)) = \tilde{v}(a_i(\alpha)) + iw_{\alpha,\delta}(\phi(x))\}$.

With the above notation, the following result proved in [6, Lemma 2.1] will be used in the sequel.

Theorem 2.A. For any non-zero polynomials $g(x), h(x)$ in $K[x]$, one has

(i) $I_{\alpha,\delta}(g(x)h(x)) = I_{\alpha,\delta}(g(x)) + I_{\alpha,\delta}(h(x))$,

(ii) $S_{\alpha,\delta}(g(x)h(x)) = S_{\alpha,\delta}(g(x)) + S_{\alpha,\delta}(h(x))$.

Proof of Theorem 1.3.

Let $f(x) = \sum_{i=0}^{n} a_i(x)\phi(x)^i$ be the ϕ-expansion of $f(x)$. Let the set $\{(n-k_0, v^x(a_{k_0}(x))), (n-k_1, v^x(a_{k_1}(x))), \cdots, (n-k_\ell, v^x(a_{k_\ell}(x)))\}$ denote the successive vertices corresponding to all the edges having positive slopes in the ϕ-Newton polygon of $f(x)$ where the k_j's are integers with $k_0 > k_1 > \cdots > k_\ell$. By the definition of the ϕ-Newton polygon of $f(x)$, the last vertex of the Newton polygon is $(n, v^x(a_0(x)))$. So we have $k_l = 0$. Observe that the slope λ_j is given by

$$\lambda_j = \frac{v^x(a_{k_j}(x)) - v^x(a_{k_{j-1}}(x))}{k_{j-1} - k_j}, \quad 1 \leq j \leq \ell. \tag{2.4}$$

We may assume that (K, v) is henselian because the value group and the residue field remain the same on replacing (K, v) by its henselization; moreover, if there is an irreducible factor of degree $\geq d$ in the factorization of $f(x)$ over the henselization, then there is an irreducible factor of degree $\geq d$ in the factorization of $f(x)$ over K. Let $\tilde{v}$ denote the unique prolongation of v to the algebraic closure $\widetilde{K}$ of K. Let α be a root of $\phi(x)$ in $\widetilde{K}$. Write $\phi(x) = c_m(x-\alpha)^m + \cdots + c_1(x-\alpha),\ c_m = 1$. Define a positive element δ_j in the divisible closure $G_{\tilde{v}}$ of G_v by

$$\delta_j = \max_{1\leq i\leq m}\left\{\frac{\lambda_j - \tilde{v}(c_i)}{i}\right\}.$$

Note that δ_j is positive in view of the fact that $c_m = 1$ and $\lambda_j > 0$. So (α, δ_j) is a (K, v)-minimal pair in view of Example 2.2. Let $\widetilde{w}_{\alpha,\delta_j}$ denote the valuation of $\widetilde{K}(x)$ defined by (2.1). Then by the choice of δ_j, we have

$$\widetilde{w}_{\alpha,\delta_j}(\phi(x)) = \min_i\{\tilde{v}(c_i) + i\delta_j\} = \lambda_j.$$

Keeping in mind (2.2) and (2.3), we see that

$$w_{\alpha,\delta_j}(f(x)) = \min_{0\leq i\leq n}\{v^x(a_i(x)) + i\lambda_j\}. \tag{2.5}$$

Let $I_{\alpha,\delta_j}(f)$ and $S_{\alpha,\delta_j}(f)$ be as in Notation 2.5. We claim that

$$I_{\alpha,\delta_j}(f) = k_j, \qquad S_{\alpha,\delta_j}(f) = k_{j-1}. \tag{2.6}$$

Recall that λ_j is the positive slope of the ϕ-Newton polygon of $f(x)$ connecting the vertices $(n-k_{j-1}, v^x(a_{k_{j-1}}(x)))$, $(n-k_j, v^x(a_{k_j}(x)))$. By virtue of Definition 1.2, we see that

$$\min_{0\leq i<k_{j-1}}\left\{\frac{v^x(a_i(x)) - v^x(a_{k_{j-1}}(x))}{k_{j-1}-i}\right\} \geq \frac{v^x(a_{k_j}(x)) - v^x(a_{k_{j-1}}(x))}{k_{j-1}-k_j} = \lambda_j, \tag{2.7}$$

$$\min_{k_{j-1}\leq i\leq n}\left\{\frac{v^x(a_{k_j}(x)) - v^x(a_i(x))}{i-k_j}\right\} \leq \frac{v^x(a_{k_j}(x)) - v^x(a_{k_{j-1}}(x))}{k_{j-1}-k_j} = \lambda_j. \tag{2.8}$$

Note that the smallest index i for which equality in (2.7) holds is $i = k_j$. On the other hand, $i = k_{j-1}$ is the largest index such that equality holds in (2.8). Therefore keeping in mind (2.5), it follows that

$$w_{\alpha,\delta_j}(f(x)) = \min_{0\leq i\leq n}\{v^x(a_i(x)) + i\lambda_j\} = v^x(a_{k_j}(x)) + k_j\lambda_j = v^x(a_{k_{j-1}}(x)) + k_{j-1}\lambda_j \tag{2.9}$$

and $I_{\alpha,\delta_j}(f) = k_j,\ S_{\alpha,\delta_j}(f) = k_{j-1}$.

Let $f(x) = f_1(x)f_2(x)\cdots f_t(x)$ be the factorization of $f(x)$ into irreducible factors over K. Denote $I_{\alpha,\delta_j}(f_r)$ by $k_j^{(r)}$ and $S_{\alpha,\delta_j}(f_r)$ by $k_{j-1}^{(r)}$ for $1 \leq r \leq t$. Applying Theorem 2.A together with (2.6), we see that

$$k_j = k_j^{(1)} + \cdots + k_j^{(t)}, \quad k_{j-1} = k_{j-1}^{(1)} + \cdots + k_{j-1}^{(t)}.$$

Since $k_{j-1} > k_j$ and $k_{j-1} - k_j = k_{j-1}^{(1)} - k_j^{(1)} + \cdots + k_{j-1}^{(t)} - k_j^{(t)}$, it follows that $k_{j-1}^{(r)} - k_j^{(r)} > 0$ for some r, $1 \leq r \leq t$. Without loss of generality, we may assume that

$$k_{j-1}^{(1)} - k_j^{(1)} > 0.$$

Let $f_1(x) = \sum_{u=0}^{d_1} b_u(x)\phi(x)^u$ be the ϕ-expansion of $f_1(x)$. Then we have

$$w_{\alpha,\delta_j}(f_1(x)) = v^x(b_{k_j^{(1)}}(x)) + k_j^{(1)}\lambda_j = v^x(b_{k_{j-1}^{(1)}}(x)) + k_{j-1}^{(1)}\lambda_j.$$

The above equality implies that $(k_{j-1}^{(1)} - k_j^{(1)})\lambda_j \in G_v$. Since $\mathfrak{d}_j$ is the smallest positive element such that $\mathfrak{d}_j\lambda_j \in G_v$, it follows that

$$(k_{j-1}^{(1)} - k_j^{(1)}) \geq \mathfrak{d}_j.$$

As $S_{\alpha,\delta_j}(f_1) = k_{j-1}^{(1)}$, the above inequality shows that

$$\deg f_1(x) \geq k_{j-1}^{(1)} m \geq (k_{j-1}^{(1)} - k_j^{(1)})m \geq \mathfrak{d}_j m.$$

As j is arbitrary, we therefore conclude that $f(x)$ has an irreducible factor of degree at least $\max\limits_{1\leq j\leq \ell}\{\mathfrak{d}_j m\}$ over K.

Acknowledgements. The authors are thankful to SERB MATRICS Project No. MTR /2017/00100 and IMSc for financial support. The authors express their gratitude to the anonymous referees for some important suggestions which improved the exposition of this paper.

References

[1] V. Alexandru, N. Popescu, A. Zaharescu, A theorem of characterization of residual transcendental extension of a valuation, J. Math. Kyoto Univ., 28 (1988) 579–592.
[2] A. J. Engler, A. Prestel, Valued Fields, Springer-Verlag, New York, 2005.
[3] F. Q. Gouvêa, p-adic Numbers: An Introduction, Springer-Verlag, New York, 2003.

[4] A. Jakhar, On the irreducible factors of a polynomial, Proc. Amer. Math. Soc., 148 (2020) 1429–1437.
[5] B. Jhorar, S. K. Khanduja, Reformulation of Hensel's Lemma and extension of a theorem of Ore, Manuscripta Math., 151 (2016) 223–241.
[6] S. K. Khanduja, M. Kumar, Prolongations of valuations to finite extensions, Manuscripta Math., 131 (2010) 323–334.
[7] F. V. Kuhlmann, Value groups, residue fields and bad places of rational function fields, Trans. Amer. Math. Soc., 356 (2004) 4559–4600.