ON IRREDUCIBLE FACTORS OF POLYNOMIALS OVER COMPLETE FIELDS

Sudesh K. Khanduja [1]
Indian Institute of Science Education and Research,(IISER,Mohali)
Sector-81,S.A.S. Nagar-140306, Punjab, India.
skhanduja@iisermohali.ac.in

Sanjeev Kumar
Department of Mathematics, Panjab University,Chandigarh-160014, India.
sanjeev_kumar_19@yahoo.co.in

Abstract. Let (K, v) be a complete rank-1 valued field. In this paper, we extend classical Hensel's Lemma to residually transcendental prolongations of v to a simple transcendental extension $K(x)$ and apply it to prove a generalization of Dedekind's theorem regarding splitting of primes in algebraic number fields. We also deduce an irreducibility criterion for polynomials over rank-1 valued fields which extends already known generalizations of Schönemann Irreducibility Criterion for such fields. A refinement of Generalized Akira criterion proved in [*Manuscripta Math.,* **134:1-2** (2010) 215-224] is also obtained as a corollary of the main result.

Keywords : Valued fields; Non-Archimedean valued fields; Irreducible polynomials.

2011 Mathematics Subject Classification : 12J10; 12J25; 12E05.

[1] All correspondence may be addressed to this author.

1 Introduction

Let (K, v) be a complete rank-1 valued field with valuation ring R_v, maximal ideal M_v and residue field $\overline{K} = R_v/M_v$. For a polynomial $f(x)$ belonging to $R_v[x]$, $\bar{f}(x)$ will denote its image under the canonical homomorphism from $R_v[x]$ onto $\overline{K}[x]$. The well-known Hensel's Lemma which is the foundation stone of the theory of p-adic numbers has several equivalent statements (cf. [5, Theorem 4.1.3], [14]). In all versions of Hensel's Lemma, there appears although not explicitly the Gaussian valuation v^x defined on a simple transcendental extension $K(x)$ of K given by

$$v^x\Big(\sum_i a_i x^i\Big) = \min_i \{v(a_i)\}, \quad a_i \in K. \tag{1}$$

The classical Hensel's Lemma, after bringing in v^x can be stated as follows. Let $F(x), G_0(x), H_0(x)$ in $R_v[x]$ be such that (i) $v^x(F(x) - G_0(x)H_0(x)) > 0$, (ii) the leading coefficient of $G_0(x)$ is a unit in R_v, (iii) $\overline{G_0}(x), \overline{H_0}(x)$ are coprime polynomials in $\overline{K}[x]$. Then there exist polynomials $G(x), H(x)$ belonging to $R_v[x]$ satisfying (a) $F(x) = G(x)H(x)$, (b) $\deg G(x) = \deg \overline{G_0}(x)$, (c) $v^x(G(x) - G_0(x)) > 0, v^x(H(x) - H_0(x)) > 0$.

A major characteristic of v^x is that its residue field is a transcendental extension of the residue field of v. In general, a prolongation of v to $K(x)$ whose residue field is a transcendental extension of that of v is referred to as a residually transcendental prolongation of v. It is known that if w is a residually transcendental extension of v to $K(x)$, then the residue field of w is $\overline{L}(Y)$, where $\overline{L}$ is the residue field of a finite extension L of (K, v) and Y is transcendental over $\overline{L}$ (cf. [1]).

In this paper, we give an extension of Hensel's Lemma to residually transcendental prolongations of v to $K(x)$. It may be remarked that Khanduja, Saha [11] and Perdry [13] have already formulated and proved a different generalization of Hensel's Lemma to residually transcendental extensions using a slightly stronger hypothesis and arriving at a different conclusion. The present extended version yields some interesting applications which donot follow from the already known generalizations.

We introduce some notations and definitions before stating the results precisely. Let v be a henselian Krull valuation of arbitrary rank of a field K and $\tilde{v}$

be the unique prolongation of v to a fixed algebraic closure $\widetilde{K}$ of K with value group $G_{\tilde{v}}$. For an element α in $\widetilde{K}$, $\deg\alpha$ will stand for the degree of the extension $K(\alpha)/K$. When α belongs to the valuation ring of $\tilde{v}$, then $\overline{\alpha}$ will denote its $\tilde{v}$-residue, i.e., the image of α under the canonical homomorphism from the valuation ring of $\tilde{v}$ onto its residue field. As in [6, §2], a pair (α,δ) belonging to $\widetilde{K}\times G_{\tilde{v}}$ will be called a minimal pair (more precisely a (K,v)-minimal pair) if whenever β belongs to $\widetilde{K}$ with $\deg\beta<\deg\alpha$, then $\tilde{v}(\alpha-\beta)<\delta$. For example, if $f(x)$ belonging to $R_v[x]$ is a monic polynomial with $\bar{f}(x)$ irreducible over the residue field of v and α is a root of $f(x)$, then as in [6, §2], it can be easily verified that (α,δ) is a (K,v)-minimal pair for each positive δ in $G_{\tilde{v}}$.

Let (α,δ) be a (K,v)-minimal pair. The valuation $\widetilde{w}_{\alpha,\delta}$ of $\widetilde{K}(x)$ defined on $\widetilde{K}[x]$ by

$$\widetilde{w}_{\alpha,\delta}\big(\sum_i c_i(x-\alpha)^i\big)=\min_i\{\tilde{v}(c_i)+i\delta\},\ c_i\in\widetilde{K} \qquad (2)$$

will be referred to as the valuation with respect to the minimal pair (α,δ). The valuation obtained by restricting $\widetilde{w}_{\alpha,\delta}$ to $K(x)$ will be denoted by $w_{\alpha,\delta}$. It is known that a prolongation w of v to $K(x)$ is residually transcendental if and only if $w=w_{\alpha,\delta}$ for some (K,v)-minimal pair (α,δ) (cf. [2]). The description of $w_{\alpha,\delta}$ and its residue field is given by the theorem stated below, the proof of which is omitted (see [1, Theorem 2.1]).

Theorem 1.A. *Let $(K,v),(\widetilde{K},\tilde{v})$ be as above and (α,δ) be a (K,v)-minimal pair. Let $f(x)$ be the minimal polynomial of α over K of degree m with $w_{\alpha,\delta}(f(x))=\lambda$. Let v_1 denote the valuation obtained by restricting $\tilde{v}$ to $K(\alpha)$ with value group G_{v_1} and residue field $\overline{K(\alpha)}$. Then the following hold:*
(a) For any polynomial $g(x)$ belonging to $K[x]$ with $f(x)$-expansion $\sum_i g_i(x)f(x)^i$, $\deg g_i(x)<\deg f(x)$, one has $w_{\alpha,\delta}(g(x))=\min_i\{\tilde{v}(g_i(\alpha))+i\lambda\}$.
(b) If $h(x)$ belonging to $K[x]$ is a polynomial of degree less than m, then the $\widetilde{w}_{\alpha,\delta}$-residue of $h(x)/h(\alpha)$ equals 1.
(c) Let e be the smallest positive integer such that $e\lambda\in G_{v_1}$. If $h(x)$ belonging to $K[x]$ is any polynomial of degree less than m with $w_{\alpha,\delta}(h(x))=e\lambda$, then the $w_{\alpha,\delta}$-residue Y of $\frac{f(x)^e}{h(x)}$ is transcendental over $\overline{K(\alpha)}$ and the residue field of $w_{\alpha,\delta}$ is canonically isomorphic to $\overline{K(\alpha)}(Y)$.

In this paper, we prove

Theorem 1.1. *Let (K, v) be a complete rank-1 valued field with value group G_v and $(\widetilde{K}, \tilde{v})$, (α, δ), $w_{\alpha,\delta}$, $f(x)$, m, λ and e be as in Theorem 1.A. Assume that $e\lambda$ belongs to G_v with $e\lambda = v(h)$ for some h in K. Let Y denote the $w_{\alpha,\delta}$-residue of $\frac{f(x)^e}{h}$ and $F(x)$ belonging to $K[x]$ be such that $w_{\alpha,\delta}(F(x)) = 0$. If the $w_{\alpha,\delta}$-residue of $F(x)$ is the product of two coprime polynomials $T(Y), U(Y)$ belonging to $\overline{K(\alpha)}[Y]$ with $T(Y)$ monic of degree $t \geq 1$, then there exist $G(x), H(x) \in K[x]$ such that $F(x) = G(x)H(x), \deg G(x) = etm$ and the $w_{\alpha,\delta}$-residue of $G(x), H(x)$ are $T(Y), U(Y)$ respectively. Further if $T(Y) \neq Y$ is irreducible over $\overline{K(\alpha)}$, then $G(x)$ is irreducible over K.*

As an application of above theorem[2], we shall prove Theorem 1.2 which extends Generalized Schönemann Irreducibility Criterion [3] and infact Theorem 1.1 of [6] in the rank-1 case; moreover it yields Dedekind's theorem as well as a slightly more general result regarding splitting of primes in algebraic number fields proved in [8, Corollary 1.2]. An extended version of the Generalized Akira Criterion proved in [6, Corollary 1.4] is also obtained using Theorem 1.2.

Theorem 1.2. *Let (K, v) be a complete rank-1 valued field with value group G_v and $(\widetilde{K}, \tilde{v})$ be as in the above theorem. Let $f(x)$ belonging to $R_v[x]$ be a monic polynomial of degree m having a root α in $\widetilde{K}$ such that $\bar{f}(x)$ is irreducible over $\overline{K}$. Let $g(x)$ belonging to $R_v[x]$ be a polynomial with $f(x)$-expansion $A_n(x)f(x)^n + A_{n-1}(x)f(x)^{n-1} + \cdots + A_0(x)$, $\deg A_i(x) < m$ and v^x be the Gaussian valuation defined by (1). Assume that there exists an index $s \leq n-1$ such that the following properties are satisfied:*
(i) $v^x(A_s(x)) = 0$, $\dfrac{v^x(A_i(x))}{s-i} \geq \lambda = \dfrac{v^x(A_0(x))}{s} > 0$ for $0 \leq i \leq s-1$.
(ii) Let e be the smallest positive integer for which $e\lambda \in G_v$ with $e\lambda = v(h), h \in K$ and t denote the number $\frac{s}{e}$. The polynomial $\overline{A_s(\alpha)}x^t + \overline{C_{t-1}(\alpha)}x^{t-1} + \cdots + \overline{C_0(\alpha)}$ is irreducible over $\overline{K(\alpha)}$, where $C_i(\alpha) = \dfrac{A_{ei}(\alpha)}{h^{t-i}}$, $0 \leq i \leq t-1$.
Then $g(x)$ has a monic irreducible factor $\phi(x)$ of degree sm over R_v and $\overline{\phi}(x) = \overline{f}(x)^s$. Further for any root β of $\phi(x)$, $\tilde{v}(f(\beta)) = \lambda$. If v_2 denotes the valuation of $K(\beta)$ obtained by restricting $\tilde{v}$ to $K(\beta)$, then the index of ramification of v_2/v is divisible by e and its residual degree is divisible by m.

[2] It will be an interesting problem to investigate the validity of Theorem 1.1 when (K, v) is a henselian valued field of arbitrary rank.

Corollary 1.3. *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with θ in the ring A_K of algebraic integers of K and $F(x)$ be the minimal polynomial of θ over $\mathbb{Q}$. Let p be a rational prime and $\bar{F}(x) = \bar{g}_1(x)^{e_1} \cdots \bar{g}_r(x)^{e_r}$, be the factorization of $F(x)$ modulo p as a product of powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ with each $g_i(x)$ monic. Let $F(x) = \sum_{j\geq 0} F_{ij}(x)g_i(x)^j$ be the $g_i(x)$-expansion of $F(x)$ and r_{ij} denote the highest power of p dividing the content of the polynomial $F_{ij}(x)$. Assume* that for $1 \leq i \leq r$, e_i and r_{i0} are coprime and $\frac{r_{ij}}{e_i - j} \geqslant \frac{r_{i0}}{e_i}$ when $1 \leq j \leq e_i - 1$. Then $pA_K = \wp_1^{e_1} \cdots \wp_r^{e_r}$, where $\wp_1, \ldots, \wp_r$ are distinct prime ideals of A_K with residual degree of $\wp_i/p$ equal to $\deg g_i(x)$.*

By virtue of Theorem 1.3 of [8] and Dedekind Criterion (cf. [4, Theorem 6.1.4]), the assumption* of the above corollary is weaker than the condition $p \nmid [A_K : \mathbb{Z}[\theta]]$ used for proving Dedekind's Theorem (see [4, Theorem 4.8.13], [7, Theorem 1.1]).

Corollary 1.4 (Extended Akira Criterion)**.** *Let R_0 be an integrally closed domain with quotient field K and v be a discrete valuation of K with valuation ring R_v containing R_0. Let $F(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with coefficients in R_0 satisfying the following conditions for an index $s \leq n-1$.*
(i) $v(a_s) = 0$, $\dfrac{v(a_i)}{s-i} \geq \dfrac{v(a_0)}{s} > 0$ for $0 \leq i \leq s-1$.
(ii) Let t denote the $\gcd(v(a_0), s)$, e the number $\frac{s}{t}$ and $h \in K$ be such that $v(h) = \dfrac{v(a_0)}{t}$. If c_i denotes the element of R_v given by $c_i = \dfrac{a_{ei}}{h^{t-i}}$, then the polynomial $\overline{a_s}x^t + \overline{c_{t-1}}x^{t-1} + \cdots + \overline{c_0}$ is irreducible over the residue field $\overline{K}$ of v.
(iii) The polynomial $x^{n-s} + \overline{a_{n-1}}x^{n-s-1} + \cdots + \overline{a_s}$ is irreducible over $\overline{K}$.
(iv) $\overline{d} \neq \overline{a_s}$ for any divisor d of a_0 in R_0.
Then $F(x)$ is irreducible over K.

It may be pointed out that the above corollary is proved in [6, Corollary 1.4] when $v(a_0) = 1$.

2 Preliminary Results

As in [9, Lemma 2.A], the following lemma can be easily proved. Its proof is omitted.

Lemma 2.A. *Let v be a valuation of a field K and v' a prolongation of v to a finite extension $K(\theta)$ of K. Let $f(x)$ belonging to $R_v[x]$ be a monic polynomial of* *degree m with $\bar{f}(x)$ irreducible over R_v/M_v having the v'-residue of θ as a root. Then for any polynomial $B(x) = \sum\limits_{i\geqslant 0} b_i x^i$ belonging to $K[x]$ of degree less than m, one has $v'(B(\theta)) = v^x(B(x)) = \min\limits_i\{v(b_i)\}$.*

With notations as in the preceding section, we prove

Lemma 2.1. *Let (K,v) be a henselian valued field of arbitrary rank, (α,δ) be a (K,v)-minimal pair and $f(x), \lambda, v_1, e, Y$ be as in Theorem 1.A. Let $G(x)$ belonging to $K[x]$ be a polynomial of degree etm such that $w_{\alpha,\delta}(G(x)) = 0$ and the $w_{\alpha,\delta}$-residue of $G(x)$ is a polynomial of degree $t \geq 1$ in Y over $\overline{K(\alpha)}$. If $F(x) = G(x)q(x) + r(x)$ belonging to $K[x]$ is any polynomial with $\deg r(x) < \deg G(x)$, then $w_{\alpha,\delta}(r(x)) \geq w_{\alpha,\delta}(F(x))$.*

Proof. Let $\sum\limits_{i\geq 0} q_i(x)f(x)^i$ and $\sum\limits_{j\geq 0} r_j(x)f(x)^j$ be the $f(x)$-expansions of $q(x)$ and $r(x)$ respectively. Suppose to the contrary that $w_{\alpha,\delta}(r(x)) < w_{\alpha,\delta}(F(x))$. Using the hypothesis $w_{\alpha,\delta}(G(x)) = 0$ and the strong triangle law, we see that $w_{\alpha,\delta}(q(x)) = w_{\alpha,\delta}(r(x))$. It now follows from Theorem 1.A(a) that

$$\min_i \{\tilde{v}(q_i(\alpha)) + i\lambda\} = \min_j \{\tilde{v}(r_j(\alpha)) + j\lambda\}.$$

Let k be the smallest index such that $w_{\alpha,\delta}(q(x)) = w_{\alpha,\delta}(r(x)) = \tilde{v}(s_k(\alpha)) + k\lambda$, where $s_k(\alpha) = r_k(\alpha)$ or $q_k(\alpha)$. Keeping in mind that e is the smallest positive integer such that $e\lambda \in G_{v_1}$ and using Theorem 1.A, it can be easily seen that the $w_{\alpha,\delta}$-residue of $\frac{q(x)}{s_k(x)f(x)^k}, \frac{r(x)}{s_k(x)f(x)^k}$ are non-zero polynomials in Y over $\overline{K(\alpha)}$, say $d_1(Y), d_2(Y)$. Now on dividing $F(x) = G(x)q(x) + r(x)$ by $s_k(x)f(x)^k$ and taking the $w_{\alpha,\delta}$-residues, we see that $\bar{0} = \psi(Y)d_1(Y) + d_2(Y)$, where the polynomial $\psi(Y)$ is the $w_{\alpha,\delta}$-residue of $G(x)$ having degree t by hypothesis. This leads to a contradiction as $\deg d_2(Y) < t$ in view of the fact that $\deg r(x) < \deg G(x) = etm$. Hence the lemma.

Lemma 2.2. *Let $w_{\alpha,\delta}, f(x), e, \lambda$ and Y be as in Theorem 1.A. Assume that $e\lambda = v(h)$ belongs to G_v for some h in K. If $d(Y)$ belonging to $\overline{K(\alpha)}[Y]$ is a polynomial of degree $t \geq 0$ in Y, then there exists a polynomial $g(x)$ with coefficients in K belonging to the valuation ring of $w_{\alpha,\delta}$ having degree $\leq etm + m - 1$ whose $w_{\alpha,\delta}$-residue is $d(Y)$. Further if $d(Y)$ is monic, then such a polynomial $g(x)$ of degree etm can be chosen.*

Proof. Write $d(Y) = \overline{d_0(\alpha)} + \overline{d_1(\alpha)}Y + \cdots + \overline{d_t(\alpha)}Y^t, d_i(x) \in K[x], \deg d_i(x) < m$. On taking $g(x) = d_0(x) + d_1(x)\frac{f(x)^e}{h} + \cdots + d_t(x)\big(\frac{f(x)^e}{h}\big)^t$, the lemma follows.

The following already known results will be used in the sequel (see [11, Lemma 2.3] for Lemma 2.B and [12, Proposition 6.1] for Theorem 2.C).

Lemma 2.B. *Let (K, v) be a complete rank-1 valued field and $\widetilde{w}_{\alpha,\delta}$ be a valuation of $\widetilde{K}(x)$ defined by a minimal pair (α, δ). Let $\{G_n(x)\} \subseteq K[x]$ be a sequence of polynomials with bounded degrees. Suppose that $\widetilde{w}_{\alpha,\delta}(G_n(x) - G_m(x)) \to \infty$ as $n, m \to \infty$. Then there exists $G(x) \in K[x]$ such that $\widetilde{w}_{\alpha,\delta}(G(x) - G_n(x)) \to \infty$ as $n \to \infty$. Moreover, if each $G_n(x)$ has the same degree d and leading coefficient l, then $G(x)$ also has degree d and leading coefficient l.*

Theorem 2.C. *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with θ in the ring of algebraic integers A_K of K. Let $F(x)$ be the minimal polynomial of θ over $\mathbb{Q}$. For a rational prime p, let $F(x) = \phi_1(x) \cdots \phi_r(x)$ be the factorization of $F(x)$ into distinct, monic irreducible polynomials over the field $\mathbb{Q}_p$ of p-adic numbers. Then $pA_K = \wp_1^{e_1} \cdots \wp_r^{e_r}$, where $\wp_i$ are distinct prime ideals of A_K. If f_i is the residual degree of $\wp_i/p$, then for each i, the product $e_i f_i$ equals the degree of $\phi_i(x)$. Moreover for $1 \leq i \leq r$, the completion $K_{\wp_i} = \mathbb{Q}_p(\beta_i)$ with $\phi_i(\beta_i) = 0$.*

3 Proof of Theorem 1.1

Since $T(Y)$ and $U(Y)$ are given to be coprime, there exist $a(Y)$ and $b(Y)$ in $\overline{K(\alpha)}[Y]$ such that $a(Y)T(Y) + b(Y)U(Y) = \overline{1}$. In view of Lemma 2.2 and the fact that $T(Y)$ is monic, one can choose $A(x), B(x), G_1(x), H_1(x)$ belonging to $K[x]$ having $w_{\alpha,\delta}$-residues $a(Y), b(Y), T(Y), U(Y)$ respectively and $\deg G_1(x) = etm$. Define polynomials $C_0(x), P_0(x)$ by $C_0(x) = A(x)G_1(x) + B(x)H_1(x) - 1, P_0(x) = F(x) - G_1(x)H_1(x)$ and set

$$\mu = \min\{w_{\alpha,\delta}(C_0(x)), w_{\alpha,\delta}(P_0(x))\}$$

which is positive because the $w_{\alpha,\delta}$-residue of $F(x)$ is $T(Y)U(Y)$. Let N denote the maximum of the degrees of $F(x), P_0(x)$. Observe that $\deg H_1(x) \leq N - etm$. The proof is split into two steps.

Step I. We construct polynomials $G_i(x), H_i(x)$ in $K[x], i = 1, 2, 3, \ldots$ such that the following conditions are satisfied:

(i) $\deg G_i(x) = \deg G_1(x), \deg H_i(x) \leq N - etm$ and the leading coefficient of $G_i(x)$ is same as that of $G_1(x)$.
(ii) $w_{\alpha,\delta}(G_i(x) - G_{i-1}(x)) \geq (i-1)\mu,\ w_{\alpha,\delta}(H_i(x) - H_{i-1}(x)) \geq (i-1)\mu$.
(iii) $w_{\alpha,\delta}(F(x) - G_i(x)H_i(x)) \geq i\mu$.
(iv) $w_{\alpha,\delta}(A(x)G_i(x) + B(x)H_i(x) - 1) \geq \mu$.
Clearly $G_1(x), H_1(x)$ satisfy conditions (i) - (iv) with condition (ii) being void. As induction hypothesis, assume that there are polynomials $G_i(x), H_i(x)$ for $1 \leq i \leq n$ satisfying the above properties. To construct $G_{n+1}(x), H_{n+1}(x)$, define

$$C_{n-1}(x) = A(x)G_n(x) + B(x)H_n(x) - 1, \tag{3}$$

$$P_{n-1}(x) = F(x) - G_n(x)H_n(x).$$

By division algorithm, write

$$B(x)P_{n-1}(x) = G_n(x)q_{n+1}(x) + r_{n+1}(x), \deg r_{n+1}(x) < \deg G_n(x), \tag{4}$$

$$C_{n-1}(x)P_{n-1}(x) = G_n(x)Q(x) + R(x), \deg R(x) < \deg G_n(x). \tag{5}$$

Multiply both sides of (3) by $P_{n-1}(x)$; on substituting for $B(x)P_{n-1}(x)$ from (4) and using (5), we obtain

$$s_{n+1}(x)G_n(x) + r_{n+1}(x)H_n(x) = P_{n-1}(x) + R(x), \tag{6}$$

where $s_{n+1}(x) = A(x)P_{n-1}(x) + q_{n+1}(x)H_n(x) - Q(x)$. Set

$$G_{n+1}(x) = G_n(x) + r_{n+1}(x), \tag{7}$$

$$H_{n+1}(x) = H_n(x) + s_{n+1}(x). \tag{8}$$

Then $\deg G_{n+1}(x) = \deg G_n(x) = etm$. Using the fact that $\deg R(x), \deg r_{n+1}(x)$ are less than etm and that degrees of $P_{n-1}(x), G_n(x)H_n(x)$ do not exceed N in view of induction hypothesis, it follows immediately from (6) that

$$\deg(s_{n+1}(x)G_n(x)) \leq \max\{\deg P_{n-1}(x), \deg R(x), \deg(r_{n+1}(x)H_n(x))\} \leq N$$

and hence $\deg s_{n+1}(x) \leq N - etm$ which in view of (8) proves that $\deg H_{n+1}(x) \leq N - etm$. Thus property (i) of the sequence is proved for $i = n+1$.

Keeping in mind (7), applying Lemma 2.1 to (4) and using condition (iii) of the induction hypothesis, we see that

$$w_{\alpha,\delta}(G_{n+1}(x) - G_n(x)) = w_{\alpha,\delta}(r_{n+1}(x)) \geq w_{\alpha,\delta}(B(x)P_{n-1}(x)) \geq n\mu. \quad (9)$$

Since $w_{\alpha,\delta}(G_n(x)) = w_{\alpha,\delta}(G_1(x)) = 0$, it follows from (8) and (6) that

$$\begin{aligned} w_{\alpha,\delta}(H_{n+1}(x) - H_n(x)) &= w_{\alpha,\delta}(s_{n+1}(x)) = w_{\alpha,\delta}(s_{n+1}(x)G_n(x)) \\ &\geq \min\{w_{\alpha,\delta}(P_{n-1}(x)), w_{\alpha,\delta}(R(x)), w_{\alpha,\delta}(r_{n+1}(x)H_n(x))\}. \quad (10) \end{aligned}$$

Applying Lemma 2.1 to (5) and using conditions (iii) and (iv) of the induction hypothesis, we have

$$w_{\alpha,\delta}(R(x)) \geq w_{\alpha,\delta}(C_{n-1}(x)P_{n-1}(x)) \geq (n+1)\mu; \quad (11)$$

consequently (10), by virtue of (9) and (11), shows that $w_{\alpha,\delta}(H_{n+1}(x) - H_n(x)) \geq n\mu$. So condition (ii) of the sequence is satisfied for $i = n+1$.

For verifying condition (iii), set $P_n(x) = F(x) - G_{n+1}(x)H_{n+1}(x)$. Substituting for $G_{n+1}(x), H_{n+1}(x)$ from (7),(8) and using (6), a simple calculation shows that $P_n(x) = -R(x) - r_{n+1}(x)s_{n+1}(x)$. Hence

$$w_{\alpha,\delta}(P_n(x)) \geq \min\{w_{\alpha,\delta}(R(x)), w_{\alpha,\delta}(r_{n+1}(x)) + w_{\alpha,\delta}(s_{n+1}(x))\}.$$

It now follows from (11) and property (ii) of the sequence proved above for $i = n+1$, that $w_{\alpha,\delta}(P_n(x)) \geq \min\{(n+1)\mu,\ 2n\mu\} \geq (n+1)\mu$ and hence condition (iii) holds for $i = n+1$. Using property (ii) of the sequence for $i = n+1$ and property (iv) for $i = n$, it can be easily seen that $w_{\alpha,\delta}(A(x)G_{n+1}(x) + B(x)H_{n+1}(x) - 1) \geq \mu$ as desired. This completes the proof of Step I.

Step II. We show that there exist polynomials $G(x)$ and $H(x)$ in $K[x]$ with the desired properties. In view of property (ii), the sequences $\{G_n(x)\}, \{H_n(x)\}$ are Cauchy with respect to the $w_{\alpha,\delta}$-valuation. By Lemma 2.B, there exist polynomials $G(x)$ and $H(x)$ belonging to $K[x]$ with $\deg G(x) = etm$ such that both $w_{\alpha,\delta}(G_n(x) - G(x))$ and $w_{\alpha,\delta}(H_n(x) - H(x))$ tend to ∞ as $n \to \infty$. Property (iii) of the induction hypothesis implies that the sequence $\{G_n(x)H_n(x)\}$ converges to $F(x)$ with respect to the $w_{\alpha,\delta}$-valuation, thereby proving that $F(x) = G(x)H(x)$. Further $w_{\alpha,\delta}(G(x) - G_1(x)) \geq \mu > 0$ and $w_{\alpha,\delta}(H(x) - H_1(x)) \geq \mu > 0$ as desired.

If the $w_{\alpha,\delta}$-residue $T(Y) \neq Y$ of $G(x)$ is irreducible over $\overline{K(\alpha)}$, then it quickly follows from [10, Theorem 2.2] that $G(x)$ is irreducible over K.

4 Proof of Theorem 1.2, Corollaries 1.3, 1.4

Proof of Theorem 1.2. Denote $\frac{v^x(A_0(x))}{s}$ by λ. Write $f(x) = \sum_{i=1}^{m} a_i(x-\alpha)^i,\ a_i \in K(\alpha)$. Determine δ in $G_{\tilde{v}}$ so that

$$\lambda = \min_{1\leqslant i\leqslant m}\{\tilde{v}(a_i) + i\delta\},\ i.e.,\quad \delta = \max_{1\leqslant i\leqslant m}\{(\lambda - \tilde{v}(a_i))/i\}.$$

Note that $\delta > 0$, in view of the fact that $a_m = 1$ and $\lambda > 0$ by hypothesis. As remarked in §1, (α, δ) is a (K, v)-minimal pair. In view of (2) and the choice of δ, it is clear that $\widetilde{w}_{\alpha,\delta}(f(x)) = \min_{1\leq i\leq m}\{\tilde{v}(a_i)+i\delta\} = \lambda$. Therefore by Theorem 1.A and Lemma 2.A, we have

$$w_{\alpha,\delta}(F(x)) = \min_i\{\tilde{v}(A_i(\alpha)) + i\lambda\} = \min_i\{v^x(A_i(x)) + i\lambda\}.$$

By virtue of assumption (i) of the theorem $w_{\alpha,\delta}(F(x)) = s\lambda = v^x(A_0(x)) = v(h^t)$, where t is as in assumption (ii). Let Y denote the $w_{\alpha,\delta}$-residue of $\frac{f(x)^e}{h}$. Using Theorem 1.A(b), it follows that the $w_{\alpha,\delta}$-residue of $\frac{F(x)}{h^t}$ is $\overline{A_s(\alpha)}Y^t + \overline{C_{t-1}(\alpha)}Y^{t-1} + \cdots + \overline{C_0(\alpha)} = \overline{A_s(\alpha)}T(Y)$ (say). Note that $\tilde{v}(C_0(\alpha)) = v^x(C_0(x)) = v^x(\frac{A_0(x)}{h^t}) = 0$. So $T(Y) \neq Y$. By assumption (ii), $T(Y)$ is irreducible over $\overline{K(\alpha)}$. Therefore by Theorem 1.1, $F(x)$ has an irreducible factor $G(x)$ of degree $etm = sm$ with $T(Y)$ as its $w_{\alpha,\delta}$-residue. Let c denote the leading coefficient of $G(x)$ and set $\phi(x) = c^{-1}G(x)$. We first prove that $\phi(x) \in R_v[x]$ and $\overline{\phi}(x) = \overline{f}(x)^s$.

Let $G(x) = \sum_{i=0}^{s} G_i(x)f(x)^i$ be the $f(x)$-expansion of $G(x)$. Note that $G_s(x) = c$ as $\deg G(x) = sm$. Keeping in mind that the $w_{\alpha,\delta}$-residue of $G(x)$ is a polynomial of degree t in Y with non-zero constant term, it follows from Theorem 1.A and Lemma 2.A that

$$0 = w_{\alpha,\delta}(G(x)) = \min_i\{v^x(G_i(x)) + i\lambda\} = v(c) + s\lambda = v^x(G_0(x)); \tag{12}$$

consequently

$$v^x(c^{-1}G_i(x)) \geq -v(c) - i\lambda = (s-i)\lambda > 0 \quad for \quad 0 \leq i \leq s-1. \tag{13}$$

Therefore

$$\phi(x) = c^{-1}G(x) \in R_v[x] \text{ and } v^x(\phi(x) - f(x)^s) \geq \min_{0\leq i\leq s-1}\{v^x(c^{-1}G_i(x))\} > 0$$

which proves that $\overline{\phi}(x) = \overline{f}(x)^s$. Let β be a root of $\phi(x)$. Clearly the assertions regarding the index of ramification and the residual degree of v_2/v are proved as soon as we show that

$$\tilde{v}(f(\beta)) = \lambda > 0. \tag{14}$$

Since $\overline{\beta}$ is a root of $\overline{f}(x)$, it follows from Lemma 2.A and (13) that

$$\tilde{v}(c^{-1}G_i(\beta)) = v^x(c^{-1}G_i(x)) \geq (s-i)\lambda,\ 0 \leq i \leq s-1. \tag{15}$$

If $\tilde{v}(f(\beta)) > \lambda$, then (15) would imply that

$$\tilde{v}\big(c^{-1}G_i(\beta)f(\beta)^i\big) \geq (s-i)\lambda + i\tilde{v}(f(\beta)) > s\lambda,\ 1 \leq i \leq s;$$

consequently by the strong triangle law and the fact that $v^x(G_0(x)) = 0$, as pointed out in (12) we shall have,

$$\tilde{v}(\phi(\beta)) = \tilde{v}(c^{-1}G_0(\beta)) = v^x(c^{-1}G_0(x)) = s\lambda,$$

which is impossible as $\phi(\beta) = 0$. On the other hand if $\tilde{v}(f(\beta)) < \lambda$, then arguing as above, we shall have $\tilde{v}(c^{-1}G_i(\beta)f(\beta)^i) \geq (s-i)\lambda + i\tilde{v}(f(\beta)) > s\tilde{v}(f(\beta))$ for $0 \leq i \leq s-1$, which in turn leads to $\tilde{v}(\phi(\beta)) = s\tilde{v}(f(\beta))$, another contradiction. This proves (14) and hence the theorem.

Proof of Corollary 1.3. Fix any $g_i(x)$ and apply Theorem 1.2 with $f(x)$ replaced by $g_i(x)$. It can be easily seen that assumption (i) of Theorem 1.2 is satisfied with $s = e_i$ in view of the hypothesis $\frac{r_{ij}}{e_i - j} \geqslant \frac{r_{i0}}{e_i}$ when $1 \leq j \leq e_i - 1$. Since r_{i0} and e_i are coprime, it follows with notations as in Theorem 1.2 that in this situation $e = s = e_i$ and $t = 1$. Therefore assumption (ii) is trivially satisfied. So by Theorem 1.2, $F(x)$ has an irreducible factor $\phi_i(x)$ with coefficients in the ring of p-adic integers having degree $e_i \deg g_i(x)$ and $\phi_i(x) \equiv g_i(x)^{e_i} \mod p$. Further if β_i is a root of $\phi_i(x)$ and v_i denotes the unique prolongation of the p-adic valuation v_p of the field $\mathbb{Q}_p$ of p-adic numbers to $\mathbb{Q}_p(\beta_i)$, then the index of ramification of $v_i/v_p \geq e_i$ and the residual degree of $v_i/v_p \geq \deg g_i(x)$ with equality at both the places in view of the fundamental inequality [5, Theorem 3.3.4]. Keeping in mind the degrees of $F(x)$ and $\phi_i(x)$, it is clear that $F(x) = \phi_1(x) \cdots \phi_r(x)$. The corollary now follows immediately from Theorem 2.C.

Proof of Corollary 1.4. Let $\hat{K}$ denote the completion of (K, v). We first show that $F(x)$ has an irreducible factor belonging to $\hat{K}[x]$ of degree s. Consider the $(\hat{K}, \hat{v})$-minimal pair $(0, \delta)$ with $\delta = \frac{v(a_0)}{s}$. Using condition (i) of the hypothesis, it can be easily seen that $w_{0,\delta}(F(x)) = \min\limits_{0 \leq i \leq n}\{v(a_i) + i\lambda\} = s\delta = v(h^t)$. In the notations of Theorem 1.2, here $e = \frac{s}{t}$. We denote the $w_{0,\delta}$-residue of $\frac{x^e}{h}$ by Y. Then the $w_{0,\delta}$-residue of $\frac{F(x)}{h^t}$ is the polynomial $\overline{a_s}Y^t + \overline{c_{t-1}}Y^{t-1} + \cdots + \overline{c_0}$ which is irreducible over $\overline{K}$ by condition (ii) of the hypothesis. Therefore by Theorem 1.2, $F(x)$ has an irreducible monic factor $\phi(x)$ of degree s over $R_{\hat{v}}$ and $\overline{\phi}(x) = x^s$. Now write $F(x) = \phi(x)H(x)$, where $H(x) \in R_{\hat{v}}[x]$. Then $\overline{F}(x) = \overline{\phi}(x)\overline{H}(x) = x^s(x^{n-s} + \overline{a_{n-1}}x^{n-s-1} + \cdots + \overline{a_s})$. Keeping in mind that $\overline{\phi}(x) = x^s$ and hence $\overline{H}(x) = x^{n-s} + \overline{a_{n-1}}x^{n-s-1} + \cdots + \overline{a_s}$, which is given to be irreducible over $\overline{K}$, it follows that $H(x)$ is irreducible over $\hat{K}$. If $F(x)$ were reducible over K, then $\phi(x)$ and $H(x)$ would belong to $K[x]$ and consequently would belong to $R_0[x]$ as R_0 is integrally closed. On multiplying the constant terms of $\phi(x)$ and $H(x)$, we see that condition (iv) of the corollary is violated and hence $F(x)$ is irreducible over K.

Acknowledgements. The authors are highly thankful to Mr. Anuj Bishnoi of the Department of Mathematics, Panjab University, Chandigarh for several helpful suggestions. The financial support by National Board for Higher Mathematics, Mumbai and CSIR(grant no. 09/135(0598)/2010-EMR-I) is gratefully acknowledged.

References

[1] V. Alexandru, N. Popescu and A. Zaharescu, A theorem of characterization of residual transcendental extension of a valuation, *J. Math. Kyoto Univ.,* **28**, (1988), 579-592.

[2] V. Alexandru, N. Popescu and A. Zaharescu, Minimal pairs of definition of a residual transcendental extension of a valuation, *J. Math. Kyoto Univ.,* **30**, (1990), 207-225.

[3] R. Brown, Roots of generalized Schönemann polynomials in henselian extension fields, *Indian J. Pure Appl. Math.,* **39 (5)**, (2008), 403-410.

[4] Henri Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag, Berlin Heidelberg, 1993.

[5] A. J. Engler and A. Prestel, Valued Fields, Springer-Verlag, New York 2005.

[6] S. K. Khanduja and R. Khassa, A generalization of Eisenstein-Schönemann Irreducibility Criterion, *Manuscripta Math.,* **134:1-2**, (2010), 215-224.

[7] S. K. Khanduja and M. Kumar, On a theorem a Dedekind, International Journal of Number Theory, **4 (6)**, (2008), 1019-1025.

[8] S. K. Khanduja and M. Kumar, Prolongations of valuations to finite extensions, *Manuscripta Math.*, **131 (2)**, (2010), 323-334.

[9] S. K. Khanduja and M. Kumar, On Dedekind's Criterion and simple extension of valuation rings, *Comm. Algebra.*, **38**, (2010), 684-696.

[10] S. K. Khanduja and J. Saha, On a generalization of Eisenstein's irreducibility criterion, *Mathematika,* **44**, (1997), 37-41.

[11] S. K. Khanduja and J. Saha, Generalized Hensel's Lemma, *Proc. Edinb. Math. Soc.,* **42**, (1999), 469-480.

[12] W. Narkewicz, Elementary and Analytic Theory of Algebraic Numbers, (Third edition), Springer-Verlag, Berlin Heidelberg, 2004.

[13] Herve Perdry, A generalization of Hensel's Lemma, *Fields Institute communications,* **33**, (2003), 241-249.

[14] P. Ribenboim, Equivalent forms of Hensel's Lemma, *Expo. Math.,* **3**, (1985), 3-24.