Proceedings of the Edinburgh Mathematical Society (1999) **42**, 469–480 ©

GENERALIZED HENSEL'S LEMMA

by SUDESH K. KHANDUJA and JAYANTI SAHA*

(Received 14th July 1997)

Let (K, v) be a complete, rank-1 valued field with valuation ring R_v and residue field k_v. Let v^x be the Gaussian extension of the valuation v to a simple transcendental extension $K(x)$ defined by $v^x(\sum_i a_i x^i) = \min_i\{v(a_i)\}$. The classical Hensel's lemma asserts that if polynomials $F(x)$, $G_0(x)$, $H_0(x)$ in $R_v[x]$ are such that (i) $v^x(F(x) - G_0(x)H_0(x)) > 0$, (ii) the leading coefficient of $G_0(x)$ has v-valuation zero, (iii) there are polynomials $A(x), B(x)$ belonging to the valuation ring of v^x satisfying $v^x(A(x)G_0(x) + B(x)H_0(x) - 1) > 0$, then there exist $G(x), H(x)$ in $K[x]$ such that (a) $F(x) = G(x)H(x)$, (b) $\deg G(x) = \deg G_0(x)$, (c) $v^x(G(x) - G_0(x)) > 0$, $v^x(H(x) - H_0(x)) > 0$. In this paper, our goal is to prove an analogous result when v^x is replaced by any prolongation w of v to $K(x)$, with the residue field of w a transcendental extension of k_v.

1991 *Mathematics subject classification:* 12D05, 12J10.

0. Introduction

Let (K, v) be a complete, rank-1 valued field with valuation ring R_v and residue field k_v. Let v^x be the Gaussian extension of the valuation v to a simple transcendental extension $K(x)$ defined by $v^x(\sum_i a_i x^i) = \min\{v(a_i)\}$. The classical Hensel's lemma [**2**, Thm. 16.7] asserts that if polynomials $F(x)$, $G_0(x)$, $H_0(x)$ in $R_v[x]$ are such that (i) $v^x(F(x) - G_0(x)H_0(x)) > 0$, (ii) the leading coefficient of $G_0(x)$ has v-valuation zero, (iii) there are polynomials $A(x), B(x)$ belonging to the valuation ring of v^x satisfying $v^x(A(x)G_0(x) + B(x)H_0(x) - 1) > 0$, then there exist $G(x), H(x)$ in $K[x]$ such that (a) $F(x) = G(x)H(x)$, (b) $\deg G(x) = \deg G_0(x)$, (c) $v^x(G(x) - G_0(x)) > 0$, $v^x(H(x) - H_0(x)) > 0$.

In this paper, our goal is to prove an analogous result when v^x is replaced by any prolongation w of v to $K(x)$, with the residue field of w a transcendental extension of k_v. Such a valuation will be referred to as a residually transcendental prolongation of v. A generalization of Hensel's Lemma dealing with residually transcendental prolongations of v has already been formulated and proved by Elena-Liliana Popescu [**6**]. However, there is an error in her proof. We state her result in the last section as it involves cumbersome notation and give an example to show that it is false. Our proof of the generalized Hensel's Lemma holds for all real valuations v, whereas the proof

* Research was partially supported by CSIR, New Delhi, vide grant No. 25(0072)/93/EMR-II & Q/135/(245)/93/EMR-I.

https://doi.org/10.1017/S0013091500020460 Published online by Cambridge University Press

in [6] uses strongly the hypothesis that v is discrete. Moreover our construction of the necessary sequences of polynomials used in the proof is completely different from the one given in [6].

1. Notation, definition and statement of results

Throughout, $\bar{v}$ will stand for a fixed prolongation of the henselian valuation v defined on K to an algebraic closure $\bar{K}$ of K with value group $\bar{G}_v$. A pair $(a,\delta) \in \bar{K} \times \bar{G}_v$ will be called *minimal* (with respect to (K,v)) if for every $b \in \bar{K}$, the condition $\bar{v}(a-b) \geq \delta$ implies $[K(a):K] \leq [K(b):K]$. The valuation $\bar{w}$ of $\bar{K}(x)$, given on $\bar{K}[x]$ by

$$\bar{w}\left(\sum_i c_i(x-a)^i\right) = \min_i\{\bar{v}(c_i) + i\delta\} \tag{1}$$

will be referred to as the valuation defined by the pair (a,δ).

Let w be a residually transcendental extension of v to $K(x)$. Let $\bar{w}$ be a prolongation of w to $\bar{K}(x)$. By virtue of [1, Prop. 2.1, Thm. 2.2], there exists a minimal pair (a,δ) such that the valuation defined by it coincides with w on $K(x)$; moreover, if (a',δ') is another minimal pair with the above property then $\delta = \delta'$. The element δ will be referred to as the defining value of w. Observe that the defining value of the Gaussian extension v^x is zero. We shall prove:

Theorem 1.1. *Suppose that (K,v) is a complete, rank-1 valued field. Let w be a residually transcendental prolongation of v to a simple transcendental extension $K(x)$ with defining value δ. Let $F(x)$, $G_0(x)$, $H_0(x)$ be polynomials over K, each having w-valuation zero and satisfying*

(i) $w(F(x) - G_0(x)H_0(x)) > 0$,

(ii) *the leading coefficient α of $G_0(x)$ has v-valuation $-m\delta$, where m is the degree of $G_0(x)$,*

(iii) *there are polynomials $A(x)$, $B(x)$ in the valuation ring of w with $w(A(x)G_0(x) + B(x)H_0(x) - 1) > 0$.*

Then there exist $G(x)$, $H(x) \in K[x]$ such that

(a) $F(x) = G(x)H(x)$,

(b) *degree $G(x) = m$ and the leading coefficient of $G(x)$ is α,*

(c) $w(G(x) - G_0(x)) > 0$, $w(H(x) - H_0(x)) > 0$.

An example given in the last section shows that the hypothesis (ii) in the above theorem cannot be removed. We shall deduce from this theorem the following.

https://doi.org/10.1017/S0013091500020460 Published online by Cambridge University Press

Corollary 1.2. *Let (K, v) be a complete, rank-1 valued field with value group G_v and $F(x) = a_0 + a_1x + \ldots + a_nx^n$ be a polynomial over K. If there exists an element δ in the divisible closure of G_v such that* (i) $v(a_n) + n\delta > 0$, (ii) $v(a_i) + i\delta \geq 0$ *for all i,* (iii) *there exists j, $1 \geq j \leq n-1$ with $v(a_j) + j\delta = 0$, then $F(x)$ is reducible over K.*

Corollary 1.3. *Let $\mathbb{Q}_p$ be the field of p-adic numbers (i.e. the completion of the field of rational numbers with respect to the p-adic valuation) with valuation v characterized by $v(p) = 1$. Let $n \geq 2$ be an integer which is not divisible by p. If a_i, b_i are p-adic integers for $0 \leq i \leq p-1$ and $a_{p-1} \equiv b_{p-1} \not\equiv 0$(modulo p), then the polynomial*

$$F_0(x) = (a_0x^{p-1} + a_1x^{p-2} + \ldots + a_{p-1})(x^p - p)^{(p-1)n} - (b_0x^{p-1} + b_1x^{p-2} + \ldots + b_{p-1})p^{pn}$$

is reducible over $\mathbb{Q}_p$.

The result of Corollary 1.3 does not hold in general when $n = 1$; this can be visualized on taking the ground field to be the field $\mathbb{Q}_2$ of 2-adic numbers and $F_0(x)$ to be $x^2 - 6 = (x^2 - 2) - 2^2$ which clearly is a polynomial of the type discussed in the above corollary (when $n = 1$) and is irreducible over $\mathbb{Q}_2$, because 6 is not a square in $\mathbb{Q}_2$.

2. Some preliminary results

Lemma 2.1. *Let a be an element of a field K_1 with valuation v_1 and δ be in the divisible closure of the value group of v_1. Let w_1 be a prolongation of v_1 to a simple transcendental extension $K_1(x)$ defined by*

$$w_1\left(\sum_i c_i(x-a)^i\right) = \min_i\{v_1(c_i) + i\delta\},\ c_i \in K_1.$$

Suppose that $G(x) = \sum_{i=0}^m b_i(x-a)^i \in K_1[x]$ is a polynomial of degree $m \geq 1$ with $w_1(G(x)) = 0$ and $v_1(b_m) = -m\delta$. If any polynomial $F(x) \in K_1[x]$ is written as

$$F(x) = G(x)q(x) + r(x), \deg r(x) < \deg G(x), q(x), r(x) \in K_1[x],$$

then we have $w_1(r(x)) \geq w_1(F(x))$.

Proof. If $\deg F(x) < \deg G(x)$, then $r(x) = F(x)$ and there is nothing to prove.

Suppose that $\deg F(x) = n \geq m$ and $F(x) = \sum_{i=0}^n a_i(x-a)^i$, $a_i \in K_1$. The polynomial $F_1(x) = F(x) - a_nb_m^{-1}G(x)(x-a)^{n-m}$ has degree less than n. Keeping in view that $w_1(b_m) = -m\delta$ and $w_1(G(x)) = 0$, it can be easily seen that

$$w_1(a_nb_m^{-1}G(x)(x-a)^{n-m}) = v_1(a_n) + n\delta \geq w_1(F(x)).$$

The desired assertion now follows by induction on the degree of $F(x)$.

https://doi.org/10.1017/S0013091500020460 Published online by Cambridge University Press

Lemma 2.2. *Let v be a valuation on a field K, a be an element of K and λ be in the divisible closure of the value group of v. Suppose that $G(x) = \sum_j b_j x^j = \sum_j c_j(x-a)^j$ is a polynomial over K of degree n such that $v(c_j) \geq \lambda$ for each $j, 0 \leq j \leq n$. Then $v(b_j) \geq \min\{\lambda, \lambda + (n-j)v(a)\}$ for all j.*

Proof. Keeping in view the Taylor's expansion for the polynomial $G(x)$ in powers of $(x-a)$, we see that

$$c_n = b_n, c_{n-1} = b_{n-1} + nb_n a, \ldots, c_0 = \sum_{i=0}^{n} b_i a^i.$$

On taking the v-valuations of $c_n, c_{n-1}, \ldots, c_0$ respectively, the desired assertions can be quickly verified.

Lemma 2.3. *Let (K, v) be a complete, rank-1 valued field with respect to a real valuation v and $\overline{w}$ be a valuation of $\overline{K}(x)$ defined by a minimal pair (a, δ). Let $\{G_n(x)\} \subseteq K[x]$ be a sequence of polynomials with bounded degrees. Suppose that $\overline{w}(G_n(x) - G_m(x)) \to \infty$ as $n, m \to \infty$. Then there exists a polynomial $G(x) \in K[x]$ such that $\overline{w}(G(x) - G_n(x)) \to \infty$ as $n \to \infty$.*

Proof. Suppose that $\deg G_n(x) \leq N$ for all n. Write

$$G_n(x) = \sum_{j=0}^{N} b_{n_j} x^j = \sum_{j=0}^{N} c_{n_j}(x-a)^j, \quad b_{n_j} \in K, \quad c_{n_j} \in \overline{K}.$$

By virtue of the definition of $\overline{w}$, we have for $0 \leq j \leq N$

$$\overline{w}(c_{n_j}) \geq \overline{w}(G_n(x)) - N|\delta|,$$

where $|\delta| = \max\{\delta, -\delta\}$. Applying Lemma 2.2 to $G_n(x) - G_m(x)$, it can be easily seen that

$$v(b_{n_j} - b_{m_j}) \geq \overline{w}(G_n(x) - G_m(x)) - N|\delta| - N|\overline{v}(a)|$$

for $0 \leq j \leq N$. Since $\overline{w}(G_n(x) - G_m(x)) \to \infty$ as $n, m \to \infty$, it follows that $\{b_{n_j}\}_{n_j}$ is a Cauchy sequence of elements in the complete field (K, v) and hence converges to an element b_j (say) of K. If we set $G(x) = \sum_{j=0}^{N} b_j x^j$, then clearly $\overline{w}(G(x) - G_n(x)) \to \infty$ as $n \to \infty$.

3. Proof of Theorem 1.1 and Corollary 1.2

By virtue of the hypothesis, the polynomials $P(x)$, $C(x)$ defined by

$$P(x) = F(x) - G_0(x)H_0(x) \tag{2}$$

$$C(x) = A(x)G_0(x) + B(x)H_0(x) - 1 \tag{3}$$

have w-valuation greater than zero. Set

$$\mu = \min\{w(P(x)), w(C(x))\} > 0. \tag{4}$$

Let N denote the maximum of the degrees of the polynomials $F(x)$ and $P(x)$. It is immediate from (2) that $\deg H_0(x) \leq N - m$.

We shall construct $G_n(x)$, $H_n(x)$ in $K[x]$ ($n = 0, 1, 2, \ldots$) satisfying

(I) $\deg G_n(x) = m$, $\deg H_n(x) \leq N - m$ and the leading coefficient of $G_n(x)$ is α,

(II) $w(G_n(x) - G_{n-1}(x)) \geq n\mu$, $w(H_n(x) - H_{n-1}(x)) \geq n\mu$,

(III) $w(F(x) - G_n(x)H_n(x)) \geq (n+1)\mu$.

Observe that the polynomials $G_0(x), H_0(x)$ in $K[x]$ clearly satisfy these conditions (condition (II) being void). To obtain the polynomials $G_1(x), H_1(x)$ with these properties, divide $B(x)P(x)$ and $C(x)P(x)$ respectively by $G_0(x)$ and write

$$B(x)P(x) = G_0(x)q_1(x) + r_1(x), \quad \deg r_1(x) < m, \tag{5}$$

$$C(x)P(x) = G_0(x)q(x) + r(x), \quad \deg r(x) < m. \tag{6}$$

Multiply both sides of (3) by $P(x)$ and then substituting for $B(x)P(x)$ and $C(x)P(x)$ from (5) and (6), we obtain

$$\{A(x)P(x) + q_1(x)H_0(x) - q(x)\}G_0(x) + r_1(x)H_0(x) = P(x) + r(x).$$

If the expression between { } is denoted by $s_1(x)$, then the above equation can be rewritten as

$$s_1(x)G_0(x) = P(x) + r(x) - r_1(x)H_0(x). \tag{7}$$

Set

$$G_1(x) = G_0(x) + r_1(x), \tag{8}$$

$$H_1(x) = H_0(x) + s_1(x). \tag{9}$$

Since $\deg r_1(x) < m$, it follows that the polynomial $G_1(x)$ is of degree m, with leading coefficient the same as that of $G_0(x)$. Our claim is that $\deg H_1(x) \leq N - m$. To prove the claim, observe first that by virtue of (9), we have

$$\deg(G_0(x)H_1(x)) \leq \max\{\deg(G_0(x)H_0(x)), \deg(G_0(x)s_1(x))\}. \tag{10}$$

It is clear from (2) that $\deg(G_0(x)H_0(x)) \leq N$. Using the fact that the degrees of $r(x)$ and $r_1(x)$ do not exceed the degree of $G_0(x)$, it quickly follows from (7) that

https://doi.org/10.1017/S0013091500020460 Published online by Cambridge University Press

$$\begin{aligned}\deg(s_1(x)G_0(x)) &\le \max\{\deg(r_1(x)H_0(x)), \deg r(x), \deg P(x)\}\\ &\le \max\{\deg(G_0(x)H_0(x)), \deg P(x)\} \le N.\end{aligned}$$

Thus in view of (10), the claim is proved.

We now prove that $G_1(x), H_1(x)$ satisfy (II) for $n=1$. By (5), (6) and Lemma 2.1, we have

$$w(r_1(x)) \ge w(B(x)P(x)) \quad \text{and} \quad w(r(x)) \ge w(C(x)P(x)).$$

Keeping in view (4) and the fact that $w(B(x)) \ge 0$, we conclude that

$$w(r_1(x)) \ge w(P(x)) \ge \mu, \tag{11}$$

$$w(r(x)) \ge w(C(x)P(x)) \ge w(P(x)) + \mu. \tag{12}$$

Taking into consideration that $w(G_0(x)) = w(H_0(x)) = 0$, it quickly follows from (7), (11) and (12) that

$$w(s_1(x)) = w(s_1(x)G_0(x)) \ge w(P(x)) \ge \mu. \tag{13}$$

It is immediate from (8), (9), (11) and (13) that

$$w(G_1(x) - G_0(x)) \ge \mu \quad \text{and} \quad w(H_1(x) - H_0(x)) \ge \mu$$

as desired.

Now it remains to be shown that $w(F(x) - G_1(x)H_1(x)) \ge 2\mu$. Define

$$P_1(x) = F(x) - G_1(x)H_1(x). \tag{14}$$

Substituting the expressions for $F(x), G_1(x), H_1(x)$ from (2), (8) and (9) respectively in (14) and then using (7), we obtain

$$P_1(x) = -r(x) - r_1(x)s_1(x). \tag{15}$$

Since $w(r(x)) \ge 2\mu$ by (12) and $w(r_1(x)s_1(x)) \ge 2\mu$ by (11) and (13), it follows from (15) that $w(P_1(x)) \ge 2\mu$.

Thus we have obtained polynomials $G_1(x), H_1(x)$ satisfying the conditions (I), (II) and (III). Furthermore, a simple calculation shows that $A(x)G_1(x) + B(x)H_1(x) = 1 + C_1(x)$, where

$$C_1(x) = C(x) + A(x)r_1(x) + B(x)s_1(x)$$

is such that $w(C_1(x)) \ge \mu$. On replacing $G_0(x)$, $H_0(x)$ and $P(x)$ by $G_1(x)$, $H_1(x)$ and $P_1(x)$, and arguing as above, we can construct polynomials $G_2(x), H_2(x)$ in $K[x]$ such that

https://doi.org/10.1017/S0013091500020460 Published online by Cambridge University Press

$G_2(x) = G_1(x) + r_2(x)$, $H_2(x) = H_1(x) + s_2(x)$, where $r_2(x)$ is a polynomial of degree less than m, $w(r_2(x)) \geq w(P_1(x)) \geq 2\mu$, $H_2(x)$ is a polynomial of degree not exceeding $N - m$, $w(s_2(x)) \geq w(P_1(x))$ and $w(F(x) - G_2(x)H_2(x)) \geq w(P_1(x)) + \mu \geq 3\mu$. Using induction, we obtain polynomials $G_n(x), H_n(x) (n = 0, 1, 2, \ldots)$ satisfying (I), (II) and (III).

By virtue of (II), the sequences $\{G_n(x)\}$ and $\{H_n(x)\}$ are Cauchy with respect to w. So by Lemma 2.3, there exist polynomials $G(x), H(x) \in K[x]$ such that the sequences $\{G_n(x)\}, \{H_n(x)\}$ converge to $G(x), H(x)$ respectively with respect to w. But (III) implies that the sequence $\{G_n(x)H_n(x)\}$ converges to $F(x)$; therefore $F(x) = G(x)H(x)$. Clearly $w(G(x) - G_0(x)) \geq \mu > 0$ and $w(H(x) - H_0(x)) \geq \mu > 0$. Since each $G_n(x)$ is a polynomial of degree m with leading coefficient α, it follows from the proof of Lemma 2.3 that $G(x)$ is a polynomial of degree m with leading coefficient α. Thus the polynomials $G(x), H(x)$ satisfy the requirements (a), (b) and (c).

4. A note on Popescu's result

In this section, we give an example to show that a generalization of Hensel's lemma proved in [6] for discrete, complete, rank-1 valued fields does not hold. Before stating the result referred to above, we give some of the notation used in [6].

Let (K, v) be a complete, discrete, rank-1 valued field with unique prolongation $\bar{v}$ to an algebraic closure $\bar{K}$ of K and w be a residually transcendental extension of v to $K(x)$. Let (a, δ) be a minimal pair with respect to K such that the valuation defined by it (see equation (1)) on $\bar{K}(x)$ coincides with w on $K(x)$. For any ξ in the valuation ring of w, ξ^* will stand for its w-residue, i.e., the image of ξ under the canonical homomorphism from the valuation ring of w onto the residue field of w. Also $f(x)$ will stand for the minimal polynomial of the element a over K of degree n and γ will stand for the w-valuation of $f(x)$. Let e be the smallest natural number such that $e\gamma$ belongs to the value group of the valuation v' obtained by restricting $\bar{v}$ to $K(a)$. For any $F(x) = \sum_i F_i(x)[f(x)]^i \in K[x]$, where each $F_i(x) \in K[x]$ is of degree less than n, the formula

$$w(F(x)) = \min_i \{v'(F_i(a)) + i\gamma\} \tag{16}$$

holds (see [4]). Let $h(x) \in K[x]$ be a polynomial of degree less than n such that $w(h(x)) = v'(h(a)) = e\gamma$. We denote $[f(x)]^e/h(x)$ by $r(x)$. Then the residue field of w is the simple transcendental extension $k_{v'}(r^*)$ of the residue field $k_{v'}$ of v' (cf. [4] or [5]). As in [5,Cor.1.5], it can be easily verified that if $F(x) \in K[x]$ is such that $w(F(x)) = 0$, then $F^* \in k_{v'}[r^*]$.

With the above notation, Elena-Liliana Popescu has proved the following generalization of Hensel's lemma.

Theorem A. *Let (K, v) be a complete, discrete, rank-1 valued field. Let w be a residually transcendental prolongation of v to $K(x)$ and $F(x) \in K[x]$ be a polynomial such that $w(F(x)) = 0$. Assume that $F^* = \phi\psi$, where the polynomials ϕ and ψ belonging to*

https://doi.org/10.1017/S0013091500020460 Published online by Cambridge University Press

$k_{v'}[r^*]$ have no common factor. Then we can write $F(x) = G(x)H(x)$, where $G(x)$ and $H(x)$ belonging to $K[x]$ are such that $w(G(x)) = w(H(x)) = 0$, $G^* = \phi$, $H^* = \psi$ and the degree of $G(x)$ is equal to en(deg ϕ).

The following example shows that Theorem A is false.

Example. Let (K, v) be the completion of the field $\mathbb{Q}$ of rational numbers with respect to the valuation v of $\mathbb{Q}$ characterized by $v(7) = 1$. Let $\bar{v}$ be the unique prolongation of v to the algebraic closure $\bar{K}$ of K with value group contained in the group of rationals. It can be easily seen that $(\sqrt{7}, 1)$ is a minimal pair with respect to (K, v). Let w be the restriction to $K(x)$ of the valuation $\bar{w}$, defined on $\bar{K}(x)$ by the pair $(\sqrt{7}, 1)$.

In the present situation, one can easily see that $f(x) = x^2 - 7$, which is the minimal polynomial of $\sqrt{7}$, has w-valuation $3/2$ and $e = 1$. Since $\bar{w}(x - \sqrt{7}) = 1$, i.e., $\bar{w}((x/\sqrt{7}) - 1) = 1/2 > 0$, it follows that the $\bar{w}$-residue $(x/\sqrt{7})^*$ of $(x/\sqrt{7})$ is 1^* (to be denoted by 1). In particular, $w(x) = w(\sqrt{7}) = 1/2$. So one can take $h(x) = 7x$ and $r(x) = (x^2 - 7)/7x$. Consider the polynomial

$$F(x) = ((x^2 - 7)^2/7^3) - 1.$$

By virtue of (16), we see that $w(F(x)) = 0$. On writing $F(x)$ as $((x^2 - 7)/7x)^2(x^2/7) - 1$ and keeping in view that $(x^2/7)^* = 1$, we have

$$[F(x)]^* = (r^*)^2 - 1 = (r^* + 1)(r^* - 1).$$

Our claim is that there do not exist any polynomials $G(x), H(x) \in K[x]$ with w-valuation zero such that

$$F(x) = G(x)H(x), [G(x)]^* = (r^* + 1), [H(x)]^* = (r^* - 1). \tag{17}$$

To prove the claim, observe first that if $((x - c)/d)$ is any linear polynomial over K of w-valuation zero, then $((x - c)/d)^*$ is not transcendental over the residue field of v. For if it were so, then as proved in [3, Prop. 4.3], it can be easily seen that the valuation w on $K(x)$ would be given by

$$w\left(\sum_i a_i(x - c)^i\right) = \min_i\{v(a_i) + iv(d)\},$$

which in turn implies that

$$1 = w(x - \sqrt{7}) = \min\{v(d), \bar{v}(c - \sqrt{7})\}.$$

Thus $\bar{v}(c - \sqrt{7}) \geq 1$. This gives $v(c) = v(\sqrt{7}) = 1/2$, which is impossible as $c \in K$.

Now suppose that there exist polynomials $G(x), H(x) \in K[x]$, each with w-valuation

https://doi.org/10.1017/S0013091500020460 Published online by Cambridge University Press

zero and satisfying (17). Then in view of the above observation $\deg G(x) \geq 2$, $\deg H(x) \geq 2$ and hence both are of degree 2 as the degree of $F(x)$ is 4. Write $G(x) = s(x^2 - 7) + tx + u$, where $s, t, u \in K$. By virtue of (16),

$$O = w(G(x)) = \min\{v(s) + 3/2, \bar{v}(t\sqrt{7} + u)\}.$$

The desired contradiction is obtained as soon as we show that $v(s) + 3/2 = 0$. If $v(s) + 3/2 > 0$, then $(r^* + 1) = [G(x)]^* = (tx + u)^*$, which contradicts the fact that no linear polynomial over K has its w-residue transcendental over the residue field of v.

Remark 4.1. Incidentally the above example can be used to show that the hypothesis (ii) in Theorem 1.1 can not be removed. Let $w, F(x), r(x)$ be as above. Take

$$G_0(x) = (x(x^2 - 7)/7^2) + 1, H_0(x) = (x(x^2 - 7)/7^2) - 1.$$

Since $(x^2/7)^* = 1$, we have

$$[G_0(x)]^* = (r^* + 1), \quad [H_0(x)]^* = (r^* - 1).$$

A simple calculation shows that

$$w(F(x) - G_0(x)H_0(x)) = w((x^2 - 7)^3/7^4) = 1/2,$$

and hence condition (i) of Theorem 1.1 is satisfied. Since $1/2[G_0(x)] - 1/2[H_0(x)] = 1$, the condition (iii) is also satisfied. But as shown in the above example, $F(x)$ can not be factored over K as $G(x)H(x)$ with $[G(x)]^* = [G_0(x)]^*$ and $[H(x)]^* = [H_0(x)]^*$.

Remark 4.2. The error in the proof of Theorem 2.1 of [6] creeps into the seventh line of the proof as the choice of the polynomial G_1 therein with the desired properties is not always possible.

5. Proof of Corollaries 1.2, 1.3

Proof of Corollary 1.2. Let w be a valuation of $K(x)$ defined by

$$w\left(\sum_i c_i x^i\right) = \min_i \cdot \{v(c_i) + i\delta\}.$$

Clearly w is defined by the minimal pair $(0, \delta)$ and is a residually transcendental extension of v to $K(x)$. Let j be the largest index, $1 \leq j \leq n - 1$, such that $v(a_j) + j\delta = 0$. Consider

$$G_0(x) = a_j x^j + a_{j-1} x^{j-1} + \ldots + a_0,$$

$$H_0(x) = 1.$$

https://doi.org/10.1017/S0013091500020460 Published online by Cambridge University Press

By virtue of the hypothesis and the choice of j, we see that $w(F(x)) = w(G_0(x)) = 0$,

$$w(F(x) - G_0(x)H_0(x)) = w(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_{j+1}x^{j+1}) > 0.$$

So by Theorem 1.1, there exist polynomials $G(x), H(x) \in K[x]$ with $\deg G(x) = j$ such that $F(x) = G(x)H(x)$. Thus $F(x)$ is reducible over K.

Proof of Corollary 1.3. Let $\overline{K}$ denote the algebraic closure of $K = \mathbb{Q}_p$ and $\bar{v}$ the unique extension of v to $\overline{K}$. We first show that $(p^{1/p}, 1/(p-1))$ is a minimal pair with respect to K and $\bar{v}$. If $\beta \in \overline{K}$ is such that $\bar{v}(p^{1/p} - \beta) \geq 1/(p-1)$, then $\bar{v}(\beta) = \bar{v}(p^{1/p}) = 1/p$. So the index of ramification of $K(\beta)/K$ is not less than p and consequently

$$[K(\beta) : K] \geq p = [K(p^{1/p}) : K].$$

Let $\overline{w}$ denote the valuation of $\overline{K}(x)$ defined by the minimal pair $(p^{1/p}, 1/(p-1))$ and w be the valuation of $K(x)$ obtained by restricting $\overline{w}$. Let ζ be the primitive p^{th}-root of unity. Then

$$\prod_{i=1}^{p-1}(x - \zeta^i) = x^{p-1} + x^{p-2} + \ldots + 1;$$

in particular

$$\prod_{i=1}^{p-1}(1 - \zeta^i) = p.$$

As the factors of the product on the left hand side of the above equation are conjugates of each other, we have

$$\bar{v}(1 - \zeta^i) = \bar{v}(1 - \zeta^j), \quad 1 \leq i, j \leq p - 1.$$

Consequently

$$\bar{v}(1 - \zeta^i) = \frac{v(p)}{p-1} = \frac{1}{p-1} \quad \text{for } 1 \leq i \leq p - 1.$$

It follows that for $1 \leq i \leq p - 1$,

$$\begin{aligned}\overline{w}(x - p^{1/p}\zeta^i) &= \min\{\overline{w}(x - p^{1/p}), \overline{w}(p^{1/p}(1 - \zeta^i))\}\\ &= \min\{1/(p-1), 1/p + 1/(p-1)\}\\ &= 1/(p-1).\end{aligned}$$

https://doi.org/10.1017/S0013091500020460 Published online by Cambridge University Press

Therefore

$$\overline{w}(x^p - p) = \sum_{i=1}^{p} \overline{w}(x - p^{1/p}\zeta^i) = p/(p-1).$$

By virtue of (16), for any $g(x) \in K[x]$ with $(x^p - p)$-expansion

$$\sum_i g_i(x)(x^p - p)^i, \quad \deg g_i(x)) < p,$$

we have

$$w(g(x)) = \min_i\{\bar{v}(g_i(p^{1/p}) + ip/(p-1)\}. \tag{‡}$$

If v' is the valuation obtained by restricting $\bar{v}$ to $K(p^{1/p})$, then clearly the index of ramification of v'/v is p and consequently the residual degree of v'/v is 1. Clearly, $p-1$ is the smallest positive integer such that $(p-1)w(x^p - p)$ is in the value group of v'. So by the result stated in the paragraph preceding Theorem A in Section 4, the residue field of w is the simple transcendental extension $k_v(r^*)$ of the residue field k_v of v, where r^* is the w-residue of $r(x) = (x^p - p)^{p-1}/p^p$. Set

$$F(x) = F_0(x)/p^{pn},$$

$$G_0(x) = ((x^p - p)^{p-1}/p^p) - 1 = r(x) - 1,$$

$$H_0(x) = b_{p-1}[r(x)^{n-1} + r(x)^{n-2} + \ldots + 1].$$

It is enough to show that $F(x), G_0(x), H_0(x)$ satisfy the three conditions of Theorem 1.1.

Keeping in view (‡) and the fact that $v(b_{p-1}) = 0$, $v(a_i) \geq 0$ and $v(b_i) \geq 0$, it can be easily seen that

$$w(F(x)) = w(G_0(x)) = w(H_0(x)) = 0.$$

Since $w(x^p - p) > 0$, it follows that $w(x) > 0$, i.e., the w-residue of x is 0. Therefore by virtue of the fact that $a_{p-1} \equiv b_{p-1}$(modulo p), we have

$$(a_0x^{p-1} + a_1x^{p-2} + \ldots + a_{p-1})^* = a^*_{p-1}$$
$$= b^*_{p-1} = (b_0x^{p-1} + b_1x^{p-2} + \ldots + b_{p-1})^*,$$

where * stands for w-residue.

It is now clear that

https://doi.org/10.1017/S0013091500020460 Published online by Cambridge University Press

$$[F(x)]^* = b^*_{p-1}(r^{*^n} - 1),$$
$$pt\ [G_0(x)]^* = r^* - 1,$$
$$[H_0(x)]^* = b^*_{p-1}[(r^{*^{n-1}} + r^{*^{n-2}} + \ldots + 1)].$$

Therefore

$$[F(x)]^* = [G_0(x)]^*[H_0(x)]^*$$

and the first condition of Theorem 1.1 is satisfied.

It only remains to verify the third condition, as the second is trivially true.

If Y is an indeterminate, then on dividing $Y^{n-1} + Y^{n-2} + \ldots + 1$ by $(Y - 1)$, we see that

$$[Y^{n-1} + Y^{n-2} + \ldots + Y + 1] = (Y - 1)[Y^{n-2} + 2Y^{n-3} + \ldots + n - 1] + n,$$

i.e.,

$$[Y^{n-1} + Y^{n-2} + \ldots + 1]/n - [(Y - 1)/n][Y^{n-2} + 2Y^{n-3} + \ldots + n - 1] = 1.$$

Keeping in view the hypothesis that $v(n) = 0$, it is now clear that is we take

$$A(x) = -(1/n)[(r(x))^{n-2} + 2(r(x))^{n-3} + \ldots + n - 1],$$
$$B(x) = 1/nb_{p-1},$$

then

$$[A(x)]^*[G_0(x)]^* + [B(x)]^*[H_0(x)]^* = 1,$$

which implies condition (iii) of Theorem 1.1 and hence the corollary.

REFERENCES

1. 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.

2. O. Endler, *Valuation Theory* (Springer-Verlag, New York, 1972).

3. J. Ohm, Simple transcendental extensions of valued fields, *J. Math. Kyoto Univ.* **22** (1982), 201–221.

4. Liliana Popescu and Nicolae Popescu, Sur la definition des prolongements résiduels transcendents d'une valuation sur un corps K à $K(x)$, *Bull. Math. Soc. Sci. Math. R. S. Roumaine* **33(81)** (1989), 257–264.

5. Liliana Popescu and Nicolae Popescu, On the residual transcendental extensions of a valuation, Key polynomials and augmented valuation, *Tsukuba J. Math.* **15** (1991), 57–78.

6. Elena-Liliana Popescu, A generalization of Hensel's Lemma, *Rev. Roumaine Math. Pures Appl.* **38** (1993), 801–805.

Centre for Advanced Study in Mathematics
Panjab University
Sector – 14
Chandigarh – 160014
India

https://doi.org/10.1017/S0013091500020460 Published online by Cambridge University Press