Residually transcendental prolongations with application to factorization of polynomials over henselian valued fields

Sudesh K. Khanduja

Indian Institute of Science Education and Research,

Mohali (Chandigarh), India
Email: skhanduja@iisermohali.ac.in

Definition (Real valuation).

A mapping $v: \; K \longrightarrow \mathbb{R} \cup \{\infty\}$ is called a (real) valuation of a field K if the following hold for all $a, \; b$ in K.

(i) $v(a) = \infty \Leftrightarrow a = 0$
(ii) $v(ab) = v(a) + v(b)$
(iii) $v(a+b) \geq \min\{v(a), \; v(b)\}$.

Example: π-adic valuation

Let R be U.F.D with quotient field K and π be a prime element of R. We denote v_π the π-adic valuation of K defined for any non-zero $\alpha \in R$ by $v_\pi(\alpha) = r$, where $\alpha = \pi^r\beta, \beta \in R$, π does not divide β. It can be extended to K in a canonical manner.

In 1932, Krull extended the notion of a real valuation by replacing $v(K^{\times})$ by a totally ordered abelian group.

In 1932, Krull extended the notion of a real valuation by replacing $v(K^{\times})$ by a totally ordered abelian group.

Totally ordered abelian group

A totally ordered abelian group $(G, +, 0)$ is an abelian group together with a binary relation $\leq$ of G satisfying the following axioms for all $g, h, h_1 \in G$:
(i). $g \leq g$.
(ii). $g \leq h, h \leq g$ implies $g = h$.
(iii). $g \leq h, h \leq h_1$ implies $g \leq h_1$.
(iv). $g \leq h$ or $h \leq g$.
(v). $g \leq h$ implies $g + h_1 \leq h + h_1$.

A Krull valuation v is defined to be a mapping

$$v: \ K \stackrel{\text{onto}}{\longrightarrow} G \cup \{\infty\},$$

where G is a totally ordered additively written abelian group, such that for all $a, \ b$ in K the following hold :
(i) $v(a) = \infty \Leftrightarrow a = 0$
(ii) $v(ab) = v(a) + v(b)$
(iii) $v(a+b) \geq \min\{v(a), \ v(b)\}$.

A Krull valuation v is defined to be a mapping

$$v: \; K \overset{\text{onto}}{\longrightarrow} G \cup \{\infty\},$$

where G is a totally ordered additively written abelian group, such that for all $a, \; b$ in K the following hold :
(i) $v(a) = \infty \Leftrightarrow a = 0$
(ii) $v(ab) = v(a) + v(b)$
(iii) $v(a+b) \geq \min\{v(a), \; v(b)\}$.

With v as above
(K, v):= valued field

A Krull valuation v is defined to be a mapping

$$v: K \overset{\text{onto}}{\longrightarrow} G \cup \{\infty\},$$

where G is a totally ordered additively written abelian group, such that for all a, b in K the following hold :
(i) $v(a) = \infty \Leftrightarrow a = 0$
(ii) $v(ab) = v(a) + v(b)$
(iii) $v(a + b) \geq \min\{v(a), v(b)\}$.

With v as above
(K, v):= valued field
G := value group of v

A Krull valuation v is defined to be a mapping

$$v: \ K \overset{\text{onto}}{\longrightarrow} G \cup \{\infty\},$$

where G is a totally ordered additively written abelian group, such that for all $a, \ b$ in K the following hold :
(i) $v(a) = \infty \Leftrightarrow a = 0$
(ii) $v(ab) = v(a) + v(b)$
(iii) $v(a+b) \geq \min\{v(a), \ v(b)\}$.

With v as above
(K, v):= valued field
G := value group of v
$R_v := \{a \in K | \ v(a) \geqslant 0\}$ is called the valuation ring of v

A Krull valuation v is defined to be a mapping

$$v: \ K \xrightarrow{\text{onto}} G \cup \{\infty\},$$

where G is a totally ordered additively written abelian group, such that for all $a, \ b$ in K the following hold :
(i) $v(a) = \infty \Leftrightarrow a = 0$
(ii) $v(ab) = v(a) + v(b)$
(iii) $v(a+b) \geq \min\{v(a), \ v(b)\}$.

With v as above
(K, v):= valued field
G := value group of v
$R_v := \{a \in K | \ v(a) \geqslant 0\}$ is called the valuation ring of v
$\mathcal{M}_v := \{a \in K | \ v(a) > 0\}$
$R_v/\mathcal{M}_v$:= residue field of v.

A Krull valuation v is defined to be a mapping

$$v: \ K \overset{\text{onto}}{\longrightarrow} G \cup \{\infty\},$$

where G is a totally ordered additively written abelian group, such that for all $a, \ b$ in K the following hold :
(i) $v(a) = \infty \Leftrightarrow a = 0$
(ii) $v(ab) = v(a) + v(b)$
(iii) $v(a+b) \geq \min\{v(a), \ v(b)\}$.

With v as above
(K, v):= valued field
G := value group of v
$R_v := \{a \in K | \ v(a) \geqslant 0\}$ is called the valuation ring of v
$\mathcal{M}_v := \{a \in K | \ v(a) > 0\}$
$R_v/\mathcal{M}_v$:= residue field of v.
The order type of the chain of all convex subgroups of the value group G of v different from G is called the rank of v.

Example.(Krull valuation)

The ring $\mathbb{Q}[x]$ of polynomials in indeterminate x is U.F.D. Let v_x denote the valuation of the field $\mathbb{Q}(x)$ corresponding to the irreducible element x and v_p denote the p-adic valuation of $\mathbb{Q}$. For any non-zero polynomial $f(x)$ belonging to $\mathbb{Q}[x]$, we shall denote by f^* the constant term of the polynomial $f(x)/x^{v_x(f(x))}$. Let v be the mapping from non-zero elements of $\mathbb{Q}(x)$ to $\mathbb{Z}\times\mathbb{Z}$ (lexicographically ordered) defined on $\mathbb{Q}[x]$ by

$$v(f(x)) = (v_x(f(x)), v_p(f^*)).$$

Then v defines a valuation on $\mathbb{Q}(x)$.

Prolongation

If K'/K is an extension of fields and v is a valuation of K, then a valuation v' of K' is said to be an extension or a prolongation of v to K' if v' coincides with v on K. In this situation, the valued field (K', v') is said to be an extension of (K, v).

Prolongation

If K'/K is an extension of fields and v is a valuation of K, then a valuation v' of K' is said to be an extension or a prolongation of v to K' if v' coincides with v on K. In this situation, the valued field (K', v') is said to be an extension of (K, v).

Index of ramification and residual degree

For a valued field extension $(K', v')/(K, v)$, if $G \subseteq G'$ and R_v/M_v embedded in $R_{v'}/M_{v'}$ denote respectively the value groups and the residue fields of v, v', then the index $[G' : G]$ and the degree of the field extension $R_{v'}/M_{v'}$ over R_v/M_v are respectively called the index of ramification and the residual degree of v'/v.

Isomorphism of valued fields.

Two valued fields (K, v) and (K_1, v_1) are said to be isomorphic if there exists an isomorphism λ from K onto K_1 such that $v_1 \circ \lambda = v$.

Isomorphism of valued fields.

Two valued fields (K, v) and (K_1, v_1) are said to be isomorphic if there exists an isomorphism λ from K onto K_1 such that $v_1 \circ \lambda = v$.

Henselian valuation.

A valued field (K, v) or a valuation v of K is said to be henselian if v has a unique prolongation to the algebraic closure of K.

Isomorphism of valued fields.

Two valued fields (K, v) and (K_1, v_1) are said to be isomorphic if there exists an isomorphism λ from K onto K_1 such that $v_1 \circ \lambda = v$.

Henselian valuation.

A valued field (K, v) or a valuation v of K is said to be henselian if v has a unique prolongation to the algebraic closure of K.

Residually transcendental prolongation.

A prolongation (K', v') of (K, v) is called residually transcendental if the residue field of v' is transcendental over the residue field of v.

Main focus will be on residually transcendental prolongation of v to $K(x)$.

Background.

In 1894, Hensel proved that the prime ideals of the ring A_K of algebraic integers of an algebraic number field $K = \mathbb{Q}(\theta)$ with θ an algebraic integer having minimal polynomial $F(x)$ over $\mathbb{Q}$, occurring in the factorization of pA_K for any prime p are in one-to-one correspondence with the monic irreducible factors of $F(x)$ over the ring $\mathbb{Z}_p$ of p-adic integers and that the ramification index together with the residual degree of a prime ideal of A_K lying over p are same as those of a simple extension of the field $\mathbb{Q}_p$ of p-adic numbers obtained by adjoining a root of the corresponding irreducible factor of $F(x)$ belonging to $\mathbb{Z}_p[x]$.

If the factorization of $F(x)$ modulo p is given by

$$\overline{F}(x) = \overline{\phi_1}(x)^{e_1} \cdots \overline{\phi_r}(x)^{e_r}$$

as a product of powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ with $\phi_i(x)$ monic polynomials belonging to $\mathbb{Z}[x]$, then by Hensel's Lemma $F(x) = F_1(x) \cdots F_r(x)$, where $F_i(x)$ is a polynomial over $\mathbb{Z}_p$ with $F_i(x) \equiv \phi_i(x)^{e_i} \pmod{p}$.

In 1928, Ore in a series of papers described a method to further split $F_i(x)$ into a product of irreducible factors over $\mathbb{Z}_p$ using the notion of ϕ- Newton polygons.

Gaussian prolongation.

Let v be a valuation of a field K. We shall denote by v^x the Gaussian prolongation of v to a simple transcendental extension $K(x)$ of K defined on $K[x]$ by

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

The residue field of v^x is a simple transcendental extension of the residue field of v.

Gaussian prolongation.

Let v be a valuation of a field K. We shall denote by v^x the Gaussian prolongation of v to a simple transcendental extension $K(x)$ of K defined on $K[x]$ by

$$v^x\left(\sum_i a_i x^i\right) = \min_i \{v(a_i)\}, \quad a_i \in K.$$

The residue field of v^x is a simple transcendental extension of the residue field of v.

ϕ-expansion of a polynomial

If $\phi(x)$ is a fixed monic polynomial with coefficients from an integral domain R, then each $F(x) \in R[x]$ can be uniquely written as $\sum A_i(x)\phi(x)^i$, $\deg A_i(x) < \deg \phi(x)$, referred to as the ϕ-expansion of $F(x)$.

Definition (ϕ- Newton polygon.)

Let v be a real valuation of a field K.

Definition (ϕ- Newton polygon.)

Let v be a real valuation of a field K.
$\phi(x) :=$ A monic polynomial in $R_v[x]$ with $\overline{\phi}(x)$ irreducible over R_v/M_v.

Definition (ϕ- Newton polygon.)

Let v be a real valuation of a field K.
$\phi(x)$:= A monic polynomial in $R_v[x]$ with $\overline{\phi}(x)$ irreducible over R_v/M_v.
$F(x)$:= A polynomial in $K[x]$ not divisible by $\phi(x)$ with $\phi(x)$-expansion $\sum_{i=0}^{s} A_i(x)\phi(x)^i,\ A_s(x) \neq 0$.

Definition (ϕ- Newton polygon.)

Let v be a real valuation of a field K.
$\phi(x)$:= A monic polynomial in $R_v[x]$ with $\overline{\phi}(x)$ irreducible over R_v/M_v.
$F(x)$:= A polynomial in $K[x]$ not divisible by $\phi(x)$ with $\phi(x)$-expansion $\sum_{i=0}^{s} A_i(x)\phi(x)^i, \; A_s(x) \neq 0$.
$P_i := (i, v^x(A_{s-i}(x))$ when $A_{s-i}(x) \neq 0, 0 \leq i \leq s$.

Definition (ϕ- Newton polygon.)

Let v be a real valuation of a field K.
$\phi(x) :=$ A monic polynomial in $R_v[x]$ with $\overline{\phi}(x)$ irreducible over R_v/M_v.
$F(x) :=$ A polynomial in $K[x]$ not divisible by $\phi(x)$ with $\phi(x)$-expansion $\sum_{i=0}^{s} A_i(x)\phi(x)^i,\ A_s(x) \neq 0$.
$P_i := (i, v^x(A_{s-i}(x))$ when $A_{s-i}(x) \neq 0, 0 \leq i \leq s$.
For distinct points P_i, P_j, let μ_{ij} denote the slope of the line joining P_iP_j defined by

$$\mu_{ij} = \frac{v^x(A_{s-j}(x)) - v^x(A_{s-i}(x))}{j-i}.$$

i_1:=The largest index $0 < i_1 \leq s$ such that

$$\mu_{0i_1} = \min\{\ \mu_{0j} \mid 0 < j \leq s,\ A_{s-j}(x) \neq 0\}.$$

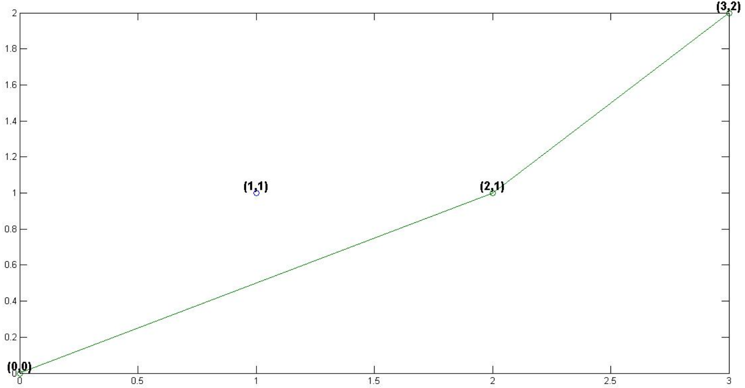
If $i_1 < s$, let i_2 be the largest index such that $i_1 < i_2 \leq s$ and

$$\mu_{i_1 i_2} = \min\{\ \mu_{i_1 j} \mid i_1 < j \leq s,\ A_{s-j}(x) \neq 0\}.$$

If $i_k = s$, then the ϕ-Newton polygon of $F(x)$(with underlying valuation v) is said to have k sides whose slopes are defined to be $\lambda_1 = \mu_{0i_1}, \lambda_2 = \mu_{i_1 i_2}, \cdots, \lambda_k = \mu_{i_{k-1} i_k}$ which are in strictly increasing order.

Example.

Consider $\phi(x) = x^2 + 2$. We calculate the ϕ-Newton polygon of the polynomial
$F(x) = (x^2+2)^3 + (5x+5)(x^2+2)^2 + 20x(x^2+2) + 25(x+5)$
with respect to the 5-adic valuation v_5. Its ϕ- Newton polygon consists of segments from (0, 0) to (2, 1) and (2, 1) to (3, 2).



Let $K = \mathbb{Q}(\theta)$ with θ an algebraic integer having minimal polynomial $F(x)$ over $\mathbb{Q}$. If the factorization of $F(x)$ modulo p is given by

$$\overline{F}(x) = \overline{\phi_1}(x)^{e_1} \cdots \overline{\phi_r}(x)^{e_r}$$

as a product of powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ with $\phi_i(x)$ monic polynomials belonging to $\mathbb{Z}[x]$, then by Hensel's Lemma $F(x) = F_1(x) \cdots F_r(x)$, where $F_i(x)$ is a polynomial over the ring $\mathbb{Z}_p$ of p-adic integers with $F_i(x) \equiv \phi_i(x)^{e_i} (\mod p)$.

Ore's method of factorization

For simplicity of notation, fix one i; denote $\phi_i(x)$ by $\phi(x)$, its degree by m and $F_i(x)$ by $g(x)$. Ore proved that if the ϕ-Newton polygon of $g(x)$ has k sides $S_1, \cdots, S_k$, then $g(x) = g_1(x) \cdots g_k(x)$ where each $g_j(x) \in \mathbb{Z}_p[x]$ is a monic polynomial whose ϕ-Newton polygon consists of a single side which is a translate of S_j and $\deg g_j(x) = ml_j$, l_j being the length of horizontal projection of the side S_j. Corresponding to S_j, he associated a polynomial $G_{S_j}(y)$ in an indeterminate y over the finite field $\mathbb{F}_q, q = p^{\deg \phi}$ to the polynomial $g_j(x)$. The factorization of $G_{S_j}(y)$ in $\mathbb{F}_q[y]$ leads to a further factorization of $g_j(x)$ over $\mathbb{Z}_p$. Finally Ore showed that if each of these polynomials $G_{S_j}(y), 1 \leq j \leq k$, decomposes into n_j distinct monic irreducible factors over $\mathbb{F}_q$, then all the $\sum_{j=1}^{k} n_j$ factors of $g(x)$ obtained in this way are irreducible over $\mathbb{Q}_p$ and their product equals $g(x)$.

Further the slopes of the sides of the ϕ_i-Newton polygon of $F_i(x)$ and the degrees of the irreducible factors of $(F_i)_S(y)$ over $\mathbb{F}_{q_i}$ for S ranging over all the sides of such a polygon lead to the explicit determination of the residual degrees and the ramification indices of all those prime ideals of A_K lying over p which correspond to the irreducible factors of $F_i(x)$.
In 2000, Cohen, Movahhedi and Salinier generalized Ore's method of factorization for polynomials with coefficients in complete discrete valued fields. In 2012, its scope was extended to complete valued fields of rank one and later in 2015, the analogues of Ore's results were proved for polynomials with coefficients in henselian valued fields of arbitrary rank (see [Manuscr. Math, 151, 223-241]).

Problem.

Given a monic polynomial $F(x)$ with coefficients in a valued field (K, v) of arbitrary rank, how to extend the result of Ore to further explore the possibility of obtaining more information about the irreducible factors of $F(x)$ over K replacing the Gaussian prolongation by arbitrary residually transcendental prolongation of v to $K(x)$ in the definition of ϕ-Newton polygon ?

Notation A.

$V_0 :=$ A henselian valuation of arbitrary rank of a field K

Notation A.

V_0 := A henselian valuation of arbitrary rank of a field K

G_0 := Value group of V_0. R_0 := Valuation ring of V_0.

Notation A.

V_0 := A henselian valuation of arbitrary rank of a field K
G_0 := Value group of V_0. R_0 := Valuation ring of V_0.
M_0 := maximal ideal of R_0.

Notation A.

V_0 := A henselian valuation of arbitrary rank of a field K

G_0 := Value group of V_0. R_0 := Valuation ring of V_0.

M_0 := maximal ideal of R_0.

$\widetilde{K}$:= an algebraic closure of K

Notation A.

V_0 := A henselian valuation of arbitrary rank of a field K

G_0 := Value group of V_0. R_0 := Valuation ring of V_0.

M_0 := maximal ideal of R_0.

$\widetilde{K}$:= an algebraic closure of K

$\widetilde{V}_0$:= A fixed prolongation of the valuation V_0 of K to $\widetilde{K}$.

Notation A.

V_0 := A henselian valuation of arbitrary rank of a field K
G_0 := Value group of V_0. R_0 := Valuation ring of V_0.
M_0 := maximal ideal of R_0.
$\widetilde{K}$:= an algebraic closure of K
$\widetilde{V}_0$:= A fixed prolongation of the valuation V_0 of K to $\widetilde{K}$.
$\widetilde{G}_0$:= The value group of $\widetilde{V_0}$.

Notation A.

V_0 := A henselian valuation of arbitrary rank of a field K
G_0 := Value group of V_0. R_0 := Valuation ring of V_0.
M_0 := maximal ideal of R_0.
$\widetilde{K}$:= an algebraic closure of K
$\widetilde{V}_0$:= A fixed prolongation of the valuation V_0 of K to $\widetilde{K}$.
$\widetilde{G}_0$:= The value group of $\widetilde{V_0}$.
For $f(x) \in R_0[x]$, $\bar{f}(x)$:= The polynomial over R_0/M_0 obtained by replacing each coefficient of $f(x)$ by its V_0-residue. For any subfield L of $\widetilde{K}$,

Notation A.

V_0 := A henselian valuation of arbitrary rank of a field K
G_0 := Value group of V_0. R_0 := Valuation ring of V_0.
M_0 := maximal ideal of R_0.
$\widetilde{K}$:= an algebraic closure of K
$\widetilde{V}_0$:= A fixed prolongation of the valuation V_0 of K to $\widetilde{K}$.
$\widetilde{G}_0$:= The value group of $\widetilde{V_0}$.
For $f(x) \in R_0[x]$, $\bar{f}(x)$:= The polynomial over R_0/M_0 obtained by replacing each coefficient of $f(x)$ by its V_0-residue. For any subfield L of $\widetilde{K}$,
$\overline{L}$:= the residue field of $(L, \widetilde{V}_0 \mid_L)$.

Notation A.

V_0 := A henselian valuation of arbitrary rank of a field K
G_0 := Value group of V_0. R_0 := Valuation ring of V_0.
M_0 := maximal ideal of R_0.
$\widetilde{K}$:= an algebraic closure of K
$\widetilde{V}_0$:= A fixed prolongation of the valuation V_0 of K to $\widetilde{K}$.
$\widetilde{G}_0$:= The value group of $\widetilde{V_0}$.
For $f(x) \in R_0[x]$, $\overline{f}(x)$:= The polynomial over R_0/M_0 obtained by replacing each coefficient of $f(x)$ by its V_0-residue. For any subfield L of $\widetilde{K}$,
$\overline{L}$:= the residue field of $(L, \widetilde{V}_0 |_L)$.
$G(L)$:= The value group of $(L, \widetilde{V}_0 |_L)$.

Definition (Minimal pair).

A pair $(\alpha, \delta) \in \widetilde{K} \times \widetilde{G}_0$ is said to be a minimal pair (more precisely a (K, V_0)-minimal pair) if whenever β belongs to $\widetilde{K}$ with $[K(\beta) : K] < [K(\alpha) : K]$, then $\widetilde{V}_0(\alpha - \beta) < \delta$, i.e., α has least degree over K in the closed ball $B(\alpha, \delta) = \{\beta \in \widetilde{K} \mid \widetilde{V}_0(\alpha - \beta) \geq \delta\}$.

Definition (Minimal pair).

A pair $(\alpha, \delta) \in \widetilde{K} \times \widetilde{G}_0$ is said to be a minimal pair (more precisely a (K, V_0)-minimal pair) if whenever β belongs to $\widetilde{K}$ with $[K(\beta) : K] < [K(\alpha) : K]$, then $\widetilde{V}_0(\alpha - \beta) < \delta$, i.e., α has least degree over K in the closed ball $B(\alpha, \delta) = \{\beta \in \widetilde{K} \mid \widetilde{V}_0(\alpha - \beta) \geq \delta\}$.

Example(Minimal pair).

If $\phi(x)$ belonging to $R_0[x]$ is a monic polynomial of degree $m \geq 1$ with $\overline{\phi}(x)$ irreducible over the residue field of V_0 and α is a root of $\phi(x)$ in the algebraic closure $\widetilde{K}$ of K, then (α, δ) is a (K, V_0)-minimal pair for each positive δ in G_0, because whenever β belongs to $\widetilde{K}$ with degree $[K(\beta) : K] < m$, then $\widetilde{V_0}(\alpha - \beta) \leq 0$, for otherwise $\overline{\alpha} = \overline{\beta}$, which in view of the Fundamental Inequality would imply that $[K(\beta) : K] \geq [\overline{K}(\overline{\beta}) : \overline{K}] = m$ leading to a contradiction.

Note that to the minimal pair $(0,0)$ belonging to $\widetilde{K} \times \widetilde{G}_0$, one can associate in a natural way, the Gaussian prolongation V_0^x of V_0 to a simple transcendental extension $K(x)$ of K defined on $K[x]$ by

$$V_0^x\Big(\sum_i a_i x^i\Big) = \min_i\{V_0(a_i)\}, a_i \in K.$$

Note that to the minimal pair $(0,0)$ belonging to $\widetilde{K} \times \widetilde{G}_0$, one can associate in a natural way, the Gaussian prolongation V_0^x of V_0 to a simple transcendental extension $K(x)$ of K defined on $K[x]$ by

$$V_0^x\big(\sum_i a_i x^i\big) = \min_i\{V_0(a_i)\}, a_i \in K.$$

In the same manner, for a (K, V_0)-minimal pair (α, δ), we can define a valuation $\widetilde{w}_{\alpha,\delta}$ of $\widetilde{K}(x)$ by

$$\widetilde{w}_{\alpha,\delta}\big(\sum_i c_i(x-\alpha)^i\big) = \min_i\{\tilde{V}_0(c_i) + i\delta\},\ c_i \in \widetilde{K};$$

its restriction to $K(x)$ will be denoted by $w_{\alpha,\delta}$. It is known that a prolongation W of V_0 to $K(x)$ is residually transcendental if and only if $W = w_{\alpha,\delta}$ for some (K, V_0)-minimal pair (α, δ).

Theorem B (Alexandru,Popescu, Zaharescu, 1988).

Let (K, V_0), $(\widetilde{K}, \widetilde{V}_0)$ be as in Notation A. Let (α, δ) be a (K, V_0)-minimal pair. Let $f(x)$ be the minimal polynomial of α over K of degree m with $w_{\alpha,\delta}(f(x)) = \mu$. Then the following hold:

(a) For any polynomial $g(x)$ belonging to $K[x]$ with f-expansion $\sum_i g_i(x)f(x)^i$, $\deg g_i(x) < m$, one has

$$w_{\alpha,\delta}(g(x)) = \min_i \{\widetilde{V}_0(g_i(\alpha)) + i\mu\}.$$

Theorem B (Alexandru,Popescu, Zaharescu, 1988).

Let (K, V_0), $(\widetilde{K}, \widetilde{V}_0)$ be as in Notation A. Let (α, δ) be a (K, V_0)-minimal pair. Let $f(x)$ be the minimal polynomial of α over K of degree m with $w_{\alpha,\delta}(f(x)) = \mu$. Then the following hold:

(a) For any polynomial $g(x)$ belonging to $K[x]$ with f-expansion $\sum_i g_i(x)f(x)^i$, $\deg g_i(x) < m$, one has

$$w_{\alpha,\delta}(g(x)) = \min_i \{\widetilde{V}_0(g_i(\alpha)) + i\mu\}.$$

(b) If $c(x)$ belonging to $K[x]$ is a non-zero polynomial of degree less than m, then the $\widetilde{w}_{\alpha,\delta}$-residue of $c(x)/c(\alpha)$ equals 1.

Theorem B (Alexandru,Popescu, Zaharescu, 1988).

Let (K, V_0), $(\widetilde{K}, \widetilde{V}_0)$ be as in Notation A. Let (α, δ) be a (K, V_0)-minimal pair. Let $f(x)$ be the minimal polynomial of α over K of degree m with $w_{\alpha,\delta}(f(x)) = \mu$. Then the following hold:

(a) For any polynomial $g(x)$ belonging to $K[x]$ with f-expansion $\sum_i g_i(x)f(x)^i$, $\deg g_i(x) < m$, one has

$$w_{\alpha,\delta}(g(x)) = \min_i \{\widetilde{V}_0(g_i(\alpha)) + i\mu\}.$$

(b) If $c(x)$ belonging to $K[x]$ is a non-zero polynomial of degree less than m, then the $\widetilde{w}_{\alpha,\delta}$-residue of $c(x)/c(\alpha)$ equals 1.

(c) Let e be the smallest positive integer such that $e\mu \in G(K(\alpha))$ and $h(x)$ belonging to $K[x]$ be a polynomial of degree less than m with $\widetilde{V}_0(h(\alpha)) = e\mu$, then the $w_{\alpha,\delta}$-residue z of $\dfrac{f(x)^e}{h(x)}$ is transcendental over $\overline{K(\alpha)}$ and the residue field of $w_{\alpha,\delta}$ is $\overline{K(\alpha)}(z)$.

As usual one can lift any monic polynomial $x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_0}$ with coefficients in R_0/M_0 to yield a monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ over R_0. In 1995, Popescu and Zaharescu extended this notion using (K, V_0)-minimal pairs as follows:

As usual one can lift any monic polynomial $x^n + \overline{a_{n-1}}x^{n-1} + \cdots + \overline{a_0}$ with coefficients in R_0/M_0 to yield a monic polynomial $x^n + a_{n-1}x^{n-1} + \cdots + a_0$ over R_0. In 1995, Popescu and Zaharescu extended this notion using (K, V_0)-minimal pairs as follows:

Definition (Lifting w.r.t. a minimal pair).

For a (K, V_0)-minimal pair (α, δ), let $f(x), m, \mu, e$ and $h(x)$ be as in Theorem B. A monic polynomial $F(x)$ belonging to $K[x]$ is said to be a lifting of a monic polynomial $T(y)$ in an indeterminate y belonging to $\overline{K(\alpha)}[y]$ having degree $t \geq 1$ with respect to (α, δ) if the following three conditions are satisfied:

(i) $\deg F(x) = etm$,

(ii) $w_{\alpha,\delta}(F(x)) = w_{\alpha,\delta}(h(x)^t) = et\mu$,

(iii) the $w_{\alpha,\delta}$-residue of $\dfrac{F(x)}{h(x)^t}$ is $T(z)$, where z is the $w_{\alpha,\delta}$-residue of $\dfrac{f(x)^e}{h(x)}$.

Keeping in mind that the valuation $w_{\alpha,\delta}$ is uniquely determined by $f(x)$ and $\mu = w_{\alpha,\delta}(f(x))$ in view of Theorem B(a), sometimes we avoid referring to the minimal pair (α, δ) and say that the above lifting is with respect to $f(x), \mu$ and $h(x)$ or more briefly with respect to $f(x), \mu$.

Definition (Nontrivial key polynomial).

Let W be a Krull valuation of $K(x)$. Two polynomials f and g belonging to $K[x]$ are said to be equivalent in W if $W(f-g) > W(f)$; f is said to be equivalence divisible by h belonging to $K[x]$ in W if there exists $q \in K[x]$ such that f is equivalent to qh in W.

Definition (Nontrivial key polynomial).

Let W be a Krull valuation of $K(x)$. Two polynomials f and g belonging to $K[x]$ are said to be equivalent in W if $W(f-g) > W(f)$; f is said to be equivalence divisible by h belonging to $K[x]$ in W if there exists $q \in K[x]$ such that f is equivalent to qh in W. A monic polynomial $\phi = \phi(x) \in K[x]$ is said to be a key polynomial over W if it satisfies the following two conditions: (i) ϕ is equivalence irreducible in W, i.e., whenever a product of two polynomials is equivalence divisible by ϕ in W, then one of the factors is equivalence divisible by ϕ in W; (ii) any non-zero polynomial of $K[x]$ equivalence divisible by ϕ in W has degree in x not less than the degree of $\phi(x)$.

Definition (Nontrivial key polynomial).

Let W be a Krull valuation of $K(x)$. Two polynomials f and g belonging to $K[x]$ are said to be equivalent in W if $W(f-g) > W(f)$; f is said to be equivalence divisible by h belonging to $K[x]$ in W if there exists $q \in K[x]$ such that f is equivalent to qh in W. A monic polynomial $\phi = \phi(x) \in K[x]$ is said to be a key polynomial over W if it satisfies the following two conditions: (i) ϕ is equivalence irreducible in W, i.e., whenever a product of two polynomials is equivalence divisible by ϕ in W, then one of the factors is equivalence divisible by ϕ in W; (ii) any non-zero polynomial of $K[x]$ equivalence divisible by ϕ in W has degree in x not less than the degree of $\phi(x)$. A key polynomial $\phi(x)$ over a residually transcendental prolongation $(K(x), W)$ of a valued field (K, V_0) is called nontrivial if there exists a (K, V_0)-minimal pair (α_1, δ_1) such that $W = w_{\alpha_1,\delta_1}$ and the minimal polynomial of α_1 over K is not equivalent to $\phi(x)$ in W.

It is known that if $W = w_{\alpha',\delta'}$ is a residually transcendental prolongation of V_0 to $K(x)$ defined by a (K, V_0)-minimal pair (α', δ'), then the minimal polynomial of α' over K is a key polynomial over W. We shall avoid working with such trivial key polynomials.

Example (Nontrivial key polynomial).

Any monic polynomial $\phi(x)$ having coefficients in the valuation ring of V_0 with $\bar{\phi}(x)$ is irreducible over the residue field of V_0 is a key polynomial over the Gaussian valuation V_0^x and in fact this key polynomial is nontrivial if $\bar{\phi}(x) \neq x$.

Theorem C. (L. Popescu and N. Popescu,1991)

Let $W = w_{(\alpha_1,\delta_1)}$ be a residually transcendental prolongation of a valued field (K, V_0). Assume that $deg(\phi(x))$ is strictly greater than the degree of the minimal polynomial of α_1 over K. Then $\phi(x) \in K[x]$ is a nontrivial key polynomial over W if and only if $\phi(x)$ is a lifting of an irreducible polynomial different from y with respect to the minimal pair (α_1, δ_1) belonging to $\overline{K(\alpha_1)}[y]$.

Definition (Generalized ϕ- Newton polygon).

Let W be a residually transcendental extension of V_0 to $K(x)$ and $\phi(x)$ be a key polynomial over W. Let $F(x)$ belonging to $K[x]$ be a polynomial not divisible by $\phi(x)$ with ϕ-expansion $\sum_{i=0}^{s} A_i(x)\phi(x)^i$, $A_s(x) \neq 0$. Let P_i stand for the pair $(i, W(A_{s-i}(x)\phi(x)^{s-i})$ when $A_{s-i}(x) \neq 0, 0 \leq i \leq s$. For distinct pairs P_i, P_j, let μ_{ij} denote the element of the divisible closure of G_0 defined by

$$\mu_{ij} = \frac{W(A_{s-j}(x)\phi(x)^{s-j}) - W(A_{s-i}(x)\phi(x)^{s-i})}{j-i}.$$

Let i_1 denote the largest index $0 < i_1 \leq s$ such that

$$\mu_{0i_1} = \min\{\ \mu_{0j} \mid 0 < j \leq s,\ A_{s-j}(x) \neq 0\}.$$

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

$$\mu_{i_1 i_2} = \min\{\ \mu_{i_1 j} \mid i_1 < j \leq s,\ A_{s-j}(x) \neq 0\}.$$

Proceeding in this way if $i_k = s$, then the ϕ-Newton polygon of $F(x)$ with respect to W is said to have r sides whose slopes are defined to be $\lambda_1 = \mu_{0i_1}, \lambda_2 = \mu_{i_1 i_2}, \cdots, \lambda_r = \mu_{i_{r-1} i_r}$ which are in strictly increasing order. The interval $[i_{j-1}, i_j]$ will be referred to as the interval of horizontal projection of the j-th side, $1 \leq j \leq r$ with $i_0 = 0$.

Theorem 1 (-, A. Jakhar, N. Sangwan, 2018).

Let (K, V_0) be a henselian valued field of arbitrary rank with value group G_0 and residue field $\overline{K}$. Let $\widetilde{K}$ be a fixed algebraic closure of K and $\widetilde{V}_0$ be the unique prolongation of V_0 to $\widetilde{K}$. Let W be a residually transcendental extension of V_0 to $K(x)$ and $\phi(x)$ be a nontrivial key polynomial of degree m over W having a root $\alpha \in \widetilde{K}$. Let $F(x)$ belonging to $K[x]$ be a monic polynomial not divisible by $\phi(x)$ with ϕ-expansion $\sum_{i=0}^{s} A_i(x)\phi(x)^i,\ A_s(x) = 1$. Suppose that the ϕ-Newton polygon of $F(x)$ with respect to W consists of r sides $S_1, \ldots, S_r$ having positive slopes $\lambda_1, \ldots, \lambda_r$. Then the following hold:

Theorem 1 (-, A. Jakhar, N. Sangwan, 2018).

Let (K, V_0) be a henselian valued field of arbitrary rank with value group G_0 and residue field $\overline{K}$. Let $\widetilde{K}$ be a fixed algebraic closure of K and $\widetilde{V}_0$ be the unique prolongation of V_0 to $\widetilde{K}$. Let W be a residually transcendental extension of V_0 to $K(x)$ and $\phi(x)$ be a nontrivial key polynomial of degree m over W having a root $\alpha \in \widetilde{K}$. Let $F(x)$ belonging to $K[x]$ be a monic polynomial not divisible by $\phi(x)$ with ϕ-expansion $\sum_{i=0}^{s} A_i(x)\phi(x)^i,\ A_s(x) = 1$. Suppose that the ϕ-Newton polygon of $F(x)$ with respect to W consists of r sides $S_1, \ldots, S_r$ having positive slopes $\lambda_1, \ldots, \lambda_r$. Then the following hold:

(i) $F(x) = F_1(x) \cdots F_r(x)$, where each $F_i(x)$ belonging to $K[x]$ is a monic polynomial of degree ml_i whose ϕ-Newton polygon with respect to W has a single side which is a translate of S_i and l_i is the length of the horizontal projection of S_i.

(ii) If θ_i is a root of $F_i(x)$, then $\widetilde{V}_0(\phi(\theta_i)) = W(\phi(x)) + \lambda_i = \mu_i'$ (say) and $G(K(\alpha)) \subseteq G(K(\theta_i))$. The index $[G(K(\theta_i)) : G(K(\alpha))]$ is divisible by e_i, where e_i is the smallest positive integer such that $e_i\mu_i' \in G(K(\alpha))$. The degree $[\overline{K(\theta_i)} : \overline{K}]$ is divisible by $[\overline{K(\alpha)} : \overline{K}]$.

(ii) If θ_i is a root of $F_i(x)$, then $\widetilde{V}_0(\phi(\theta_i)) = W(\phi(x)) + \lambda_i = \mu_i'$ (say) and $G(K(\alpha)) \subseteq G(K(\theta_i))$. The index $[G(K(\theta_i)) : G(K(\alpha))]$ is divisible by e_i, where e_i is the smallest positive integer such that $e_i\mu_i' \in G(K(\alpha))$. The degree $[\overline{K(\theta_i)} : \overline{K}]$ is divisible by $[\overline{K(\alpha)} : \overline{K}]$.

(iii) $F_i(x)$ is a lifting of a monic polynomial $T_i(y) \in \overline{K(\alpha)}[y]$ not divisible by y of degree l_i/e_i with respect to $\phi(x), \mu_i'$.

(ii) If θ_i is a root of $F_i(x)$, then $\widetilde{V}_0(\phi(\theta_i)) = W(\phi(x)) + \lambda_i = \mu'_i$ (say) and $G(K(\alpha)) \subseteq G(K(\theta_i))$. The index $[G(K(\theta_i)) : G(K(\alpha))]$ is divisible by e_i, where e_i is the smallest positive integer such that $e_i\mu'_i \in G(K(\alpha))$. The degree $[\overline{K(\theta_i)} : \overline{K}]$ is divisible by $[\overline{K(\alpha)} : \overline{K}]$.

(iii) $F_i(x)$ is a lifting of a monic polynomial $T_i(y) \in \overline{K(\alpha)}[y]$ not divisible by y of degree l_i/e_i with respect to $\phi(x), \mu'_i$.

(iv) If $U_{i1}(y)^{a_{i1}} \cdots U_{in_i}(y)^{a_{in_i}}$ is the factorization of $T_i(y)$ into powers of distinct monic irreducible polynomials over $\overline{K(\alpha)}$, then $F_i(x)$ factors as $F_{i1}(x) \cdots F_{in_i}(x)$ over K, each $F_{ij}(x)$ is a lifting of $U_{ij}(y)^{a_{ij}}$ with respect to $\phi(x), \mu'_i$ with degree $me_i a_{ij} \deg U_{ij}$ and $\widetilde{V}_0(\phi(\theta_{ij})) = \mu'_i$. If some $a_{ij} = 1$, then $F_{ij}(x)$ is irreducible over K and for any root θ_{ij} of $F_{ij}(x)$, the index $[G(K(\theta_{ij})) : G(K(\alpha))] = e_i$ and the degree $[\overline{K(\theta_{ij})} : \overline{K}] = \deg U_{ij}(y)[\overline{K(\alpha)} : \overline{K}]$ in this case.

First stage valuation.

Let V_0 be a Krull valuation of a field K with value group Γ_0 and μ be an element of a totally ordered abelian group containing Γ_0 as an ordered subgroup. Then the function V_1 defined on the polynomial ring $K[x]$ by

$$V_1(\sum c_i x^i) = \min_i \{V_0(c_i) + i\mu\}$$

gives a valuation of $K(x)$ and will be denoted by $V_1 = [V_0, V_1 x = \mu]$. It will be referred to as a first stage valuation of $K(x)$. In 1936, MacLane described a method by which any valuation W of $K(x)$ can be augmented to yield another valuation of $K(x)$ by means of a key polynomial.

Let $\phi(x)$ be a key polynomial over a valuation W of $K(x)$ having value group Γ and $\mu > W(\phi(x))$ be an element of a totally ordered abelian group containing Γ as an ordered subgroup. Then the function V defined for any $g(x) \in K[x]$ having ϕ-expansion $\sum_{i=0}^{n} g_i(x)\phi(x)^i$ with $\deg(g_i(x)) < \deg(\phi(x))$ by

$$V(f) = \min_i \{W(g_i(x)) + i\mu\},$$

gives a valuation of $K(x)$. The valuation V is called the augmented valuation over W associated with ϕ, μ and will be denoted by $V = [W, V\phi = \mu]$. With this notation, we now introduce the notion of k-th stage commensurable inductive valuation.

k-th stage inductive valuation.

A k-th stage inductive valuation V_k is a valuation of $K(x)$ obtained by a finite sequence of valuations $V_1, V_2, \cdots, V_k$ of $K(x)$ where $V_1 = [V_0, V_1 x = \mu_1]$ is a first stage valuation obtained from a valuation V_0 of K and each $V_i = [V_{i-1}, V_i\phi_i = \mu_i]$ is obtained by augmenting V_{i-1} with the key polynomials $\phi_i(x)$ satisfying the following two conditions for $2 \leq i \leq k$:

(*i*) $\phi_1(x) = x$, $\deg(\phi_i(x)) \geq \deg(\phi_{i-1}(x))$;

(*ii*) $\phi_i(x)$ is not equivalent to $\phi_{i-1}(x)$ in V_{i-1}.

The valuation V_k will be symbolized as $V_k = [V_0, V_1 x = \mu_1, V_2\phi_2 = \mu_2, \cdots, V_k\phi_k = \mu_k]$. The above valuation V_k with value group Γ_k is called *commensurable* if Γ_k/Γ_0 is a torsion group; Γ_0 being the value group of V_0.

The following theorem which plays a great role in the proof of the main result relates minimal pairs with key polynomials.

Theorem 2.

Let (K, V_0), $\Gamma_0, \widetilde{\Gamma}_0$ be as in Notation A. Let W be a valuation of $K(x)$ extending V_0 and $\phi(x)$ be a key polynomial over W. Let $V = [W, V\phi = \mu]$ with $\mu \in \widetilde{\Gamma}_0$ be an augmented valuation over W associated with ϕ, μ. Then V is a residually transcendental extension of V_0 to $K(x)$. Moreover there exists $\delta \in \widetilde{\Gamma}_0$ such that for any root α of $\phi(x)$, (α, δ) is a (K, V_0)-minimal pair and $V = w_{\alpha,\delta}$.

The above theorem immediately yields the following corollary.

Corollary 3.

Let (K, V_0) be as in Notation A and $V_k = [V_0, V_1 x = \mu_1, V_2\phi_2 = \mu_2, \cdots, V_k\phi_k = \mu_k]$ be a k-th stage commensurable inductive valuation. Then V_k is a residually transcendental extension of V_0 to $K(x)$. Moreover $V_k = w_{\alpha_k,\delta_k}$ where α_k is a root of ϕ_k with (α_k, δ_k) a (K, V_0)-minimal pair.

Corollary 4.

Let V_k be as in the above corollary with value group Γ_k. Let $\phi(x)$ be a key polynomial for an inductive valuation over V_k having a root α in $\widetilde{K}$, then $\Gamma_k = G(K(\alpha))$.

Proof of Corollary 4.

Fix an element $\mu > V_k(\phi(x))$ in the divisible closure $\widetilde{\Gamma}_0$ of Γ_0. Let V denote the augmented valuation $V = [V_k, V\phi = \mu]$. By Theorem 2, there exists $\delta \in \widetilde{\Gamma}_0$ such that (α, δ) is a (K, V_0)-minimal pair and $V = w_{\alpha,\delta}$. Note that for any polynomial $A(x) \in K[x]$ with $\deg(A(x)) < \deg(\phi(x)) = m$ (say), in view of Theorem B(b), we have

$$\widetilde{V}_0(A(\alpha)) = w_{\alpha,\delta}(A(x)) = V(A(x)) = V_k(A(x)); \qquad (1)$$

consequently $G(K(\alpha)) \subseteq \Gamma_k$.

To prove that $\Gamma_k \subseteq G(K(\alpha))$, it is enough to show that $V_k(\phi_k(x)) = \mu_k$ (say) belongs to $G(K(\alpha))$, because for any polynomial $g(x) \in K[x]$ with ϕ_k-expansion $\sum_i g_i(x)\phi_k(x)^i$, on using (1) and the fact that $\deg(\phi_k(x)) \leq m$ by definition of inductive valuation, we have

$$V_k(g(x)) = \min_i\{V_k(g_i(x)) + i\mu_k\} = \min_i\{\widetilde{V}_0(g_i(\alpha)) + i\mu_k\}.$$

If $\deg(\phi_k(x)) < m$, then again in view of (1), $\mu_k = V_k(\phi_k(x)) = \widetilde{V}_0(\phi_k(\alpha)) \in G(K(\alpha))$. So assume that $\deg(\phi_k(x)) = m$. In this situation, $\phi(x)$ has ϕ_k-expansion $\phi(x) = \phi_k(x) + r(x)$. By hypothesis $\phi(x)$ is a key polynomial for an inductive valuation over V_k and hence $\phi(x)$ is not equivalent to $\phi_k(x)$ in V_k, i.e., $V_k(\phi(x) - \phi_k(x)) \leq V_k(\phi_k(x))$. Indeed $V_k(r(x)) = V_k(\phi_k(x))$, for otherwise $V_k(r(x)) < V_k(\phi_k(x)) = V_k(\phi(x) - r(x))$ which implies that $\phi(x)$ is equivalent to $r(x)$ in V_k; this is impossible. Therefore by virtue of (1), we see that $V_k(\phi_k(x)) = V_k(r(x)) = \widetilde{V}_0(r(\alpha))$ belongs to $G(K(\alpha))$.

With α as in Corollary 4, the following theorem gives the degree of the extension $\overline{K(\alpha)}/\overline{K}$.

Theorem 5.

Let $V_k, \phi(x), \alpha$ be as in Corollary 4. For $1 \leq j \leq k$, let $V_j = [V_0, V_1 x = \mu_1, V_2\phi_2 = \mu_2, \cdots, V_j\phi_j = \mu_j]$ stand for the j-th stage inductive valuation and τ_j be the smallest positive integer such that $\tau_j\mu_j$ belongs to the value group Γ_{j-1} of V_{j-1}. Then degree of the extension $\overline{K(\alpha)}/\overline{K}$ equals $\deg(\phi(x))/\prod_{j=1}^{k}\tau_j$.

Remark 6.

It may be pointed out that in the particular case when V_k is as in Corollary 3 and $\phi(x)$ is a key polynomial for an inductive valuation over V_k, then $\phi(x)$ is a nontrivial key polynomial because in view of Corollary 3, we have $V_k = w_{\alpha_k,\delta_k}$ with α_k a root of $\phi_k(x)$ and $\phi(x)$ is not equivalent to $\phi_k(x)$ in V_k by definition of inductive valuation.

Application to Theorem 1.

Keeping in mind Corollary 4, Theorem 5 and Remark 6, the following Theorem can be easily deduced from Theorem 1.

Theorem 7.

Let (K, V_0) be a henselian valued field of arbitrary rank with value group Γ_0, residue field $\overline{K}$ and $(\widetilde{K}, \widetilde{V}_0)$ be as in Notation A. Let $V_k, \phi(x), \alpha, \tau_j$ be as in Theorem 5 and Γ_k denote the value group of V_k. Let $F(x)$ belonging to $K[x]$ be a monic polynomial not divisible by $\phi(x)$ with ϕ-expansion $\sum_{i=0}^{s} A_i(x)\phi(x)^i,\ A_s(x) = 1.$ Suppose that the ϕ-Newton polygon of $F(x)$ with respect to V_k consists of r sides $S_1, \ldots, S_r$ having positive slopes $\lambda_1, \ldots, \lambda_r$. Then the following hold:

[(*i*)] $F(x) = F_1(x) \cdots F_r(x)$, where each $F_i(x)$ belonging to $K[x]$ is a monic polynomial of degree $l_i(\deg(\phi(x))$ whose ϕ-Newton polygon with respect to V_k has a single side which is a translate of S_i and l_i is the length of the horizontal projection of S_i.

[(*ii*)] If θ_i is a root of $F_i(x)$, then $\widetilde{V}_0(\phi(\theta_i)) = V_k(\phi(x)) + \lambda_i$ and $\Gamma_k \subseteq G(K(\theta_i))$. The index $[G(K(\theta_i)) : \Gamma_0]$ is divisible by $e_i \prod_{j=1}^{k} \tau_j$, where e_i is the smallest positive integer such that $e_i\lambda_i \in \Gamma_k$. The degree $[\overline{K(\theta_i)} : \overline{K}]$ is divisible by $[\overline{K(\alpha)} : \overline{K}] = \frac{\deg(\phi(x))}{\prod_{j=1}^{k} \tau_j}$.

[(*iii*)] $F_i(x)$ is a lifting of a monic polynomial $T_i(y) \in \overline{K(\alpha)}[y]$ not divisible by y of degree l_i/e_i with respect to $\phi(x), V_k(\phi(x)) + \lambda_i$.

[(iv)] If $U_{i1}(y)^{a_{i1}} \cdots U_{in_i}(y)^{a_{in_i}}$ is the factorization of $T_i(y)$ into powers of distinct monic irreducible polynomials over $\overline{K(\alpha)}$, then $F_i(x)$ factors as $F_{i1}(x) \cdots F_{in_i}(x)$ over K, each $F_{ij}(x)$ is a lifting of $U_{ij}(y)^{a_{ij}}$ with respect to $\phi(x), V_k(\phi(x)) + \lambda_i$ with degree $e_i a_{ij} \deg U_{ij} \deg \phi$ and $\widetilde{V}_0(\phi(\theta_{ij})) = V_k(\phi(x)) + \lambda_i$. If some $a_{ij} = 1$, then $F_{ij}(x)$ is irreducible over K and for any root θ_{ij} of $F_{ij}(x)$, the index $[G(K(\theta_{ij})) : \Gamma_0] = e_i \tau_1 \tau_2 \cdots \tau_k$ and the degree $[\overline{K(\theta_{ij})} : \overline{K}] = \frac{\deg(U_{ij}(y)) \deg(\phi(x))}{\tau_1 \tau_2 \cdots \tau_k}$ in this case.

Corollary 8.

Let $(K, V_0), \phi(x), m, W$ and α be as in Theorem 1. Let $F(x)$ belonging to $K[x]$ be a polynomial having ϕ-expansion $\sum_{i=0}^{s} A_i(x)\phi(x)^i$ with $A_s(x) = 1$, $A_i(x) \neq 0$ for some $i < s$ and assume that all the sides in the ϕ-Newton polygon of $F(x)$ with respect to W have positive slopes. If l is the smallest non-negative integer for which

$$\min_{0 \leq i \leq s-1} \left\{ \frac{W(A_i(x)\phi(x)^i) - W(\phi(x)^s)}{s-i} \right\} = \frac{W(A_l(x)\phi(x)^l) - W(\phi(x)^s)}{s-l}$$

and $\frac{W(A_l(x))}{d}$ does not belong to $G(K(\alpha))$ for any number $d > 1$ dividing $s - l$, then for any factorization $G(x)H(x)$ of $F(x)$ over K, $\min\{\deg G(x), \deg H(x)\} \leq lm$.

Corollary 9.(Generalized Schönemann Irreducibility Criterion, R. Brown, 2008)

Let V_0 be a Krull valuation of arbitrary rank of a field K with value group G_0, valuation ring R_0 having maximal ideal M_0. Let $\phi(x) \in R_0[x]$ be a monic polynomial of degree m with $\overline{\phi}(x)$ irreducible over R_0/M_0. Let $F(x)$ belonging to $R_0[x]$ be a polynomial having $\phi(x)$-expansion $\sum_{i=0}^{s} A_i(x)\phi(x)^i$ with $A_s(x) = 1, A_0(x) \neq 0$. Assume that (i) $\frac{V_0^x(A_i(x))}{s-i} \geqslant \frac{V_0^x(A_0(x))}{s} > 0$ for $0 \leqslant i \leqslant s-1$ and (ii) $V_0^x(A_0(x)) \notin dG_0$ for any number $d > 1$ dividing s. Then $F(x)$ is irreducible over K.

Corollary 10.(Weintraub, 2013)

Let $F(x) = a_s x^s + \cdots + a_0$ belonging to $\mathbb{Z}[x]$ be a polynomial and suppose there is a prime p such that p does not divide a_s, p divides a_i for $i = 0, 1, \cdots, s-1$ and for some k with $0 \leq k \leq s-1, p^2$ does not divide a_k. Let k_0 be the smallest such value of k. If $F(x) = G(x)H(x)$ is a factorization in $\mathbb{Z}[x]$, then $\min(\deg G(x), \deg H(x)) \leq k_0$.

Example 1.

Let V_0 be a henselian valuation of arbitrary rank of a field K whose value group has a smallest positive element $\lambda_0 = V_0(\pi)$ for some π in the valuation ring R_0 of V_0. Let $\phi(x) \in R_0[x]$ be a monic polynomial with $\overline{\phi}(x) \neq x$ irreducible over the residue field of V_0. We factorize the polynomial $F(x) = (\phi(x)^s + \pi)^s + a\phi(x)$ into irreducible factors over K, where $V_0(a) = t\lambda_0$ and $t \geq s \geq 2$ are integers. Let V_2 denote the second stage inductive valuation defined by $V_2 = [V_0, V_1 x = 0, V_2\phi = \lambda_0/s]$. Take $\phi_3(x) = \phi(x)^s + \pi$. Keeping in mind Corollary 3, it can be easily verified using Theorem C that $\phi_3(x)$ is a key polynomial over V_2. Further $\phi_3(x)$ is not equivalent to $\phi(x)$ in V_2 because $V_2(\phi_3(x)) = \lambda_0 > V_2(\phi(x)) = \frac{\lambda_0}{s}$. So $\phi_3(x)$ is a key polynomial for an inductive valuation over V_2.

Example 1(contd.)

Since $F(x)$ has ϕ_3-expansion $\phi_3(x)^s + a\phi(x)$, the ϕ_3-Newton polygon of $F(x)$ with respect to V_2 consists of a single side with slope $\lambda = \frac{(t-s)\lambda_0}{s} + \frac{\lambda_0}{s^2}$. If e denotes the smallest positive integer such that $e\lambda$ belongs to the value group $\Gamma_0 + \frac{\lambda_0\mathbb{Z}}{s}$ of V_2, then by virtue of the hypothesis that λ_0 is the smallest positive element of Γ_0, we have $e = s$. Let α be a root of $\phi_3(x)$. Using assertions (i),(iii) of Theorem 7, we see that $F(x)$ is a lifting of a linear polynomial $T(y) \in \overline{K(\alpha)}[y]$ not divisible by y with respect to $\phi_3(x)$, $\lambda_0 + \lambda$. Hence in view of Theorem 7(iv), $F(x)$ is irreducible over K and for any root θ of $F(x)$,
$[G(K(\theta)) : \Gamma_0] = s^2$, $[\overline{K(\theta)} : \overline{K}] = \deg(\phi(x))$.

Example 2.

Let w_0 be the 2-adic valuation of the field $\mathbb{Q}$ of rational numbers defined by $w_0(2) = 1$. Let w_y denote the valuation of the field $\mathbb{Q}(y)$ of rational functions with coefficients from $\mathbb{Q}$ in an indeterminate y defined for any polynomial $f(y)$ belonging to $\mathbb{Q}[y]$ by $w_y(f(y))=$ the highest power of the monomial y dividing $f(y)$. For a non-zero polynomial $f(y) \in \mathbb{Q}[y]$, let f^* denote the constant term of the polynomial $f(y)/y^{w_y(f(y))}$. Let w be the mapping from $\mathbb{Q}[y]$ into the group $\mathbb{Z} \times \mathbb{Z}$ with lexicographic ordering defined for any non-zero polynomial $f(y)$ by $w(f(y)) = (w_y(f(y)), w_0(f^*))$ and $w(0) = \infty$. It can be easily checked that w gives a valuation of $\mathbb{Q}(y)$. Let (K, V_0) denote the henselization of $(\mathbb{Q}(y), w)$. Then the value group Γ_0 of V_0 is $\mathbb{Z} \times \mathbb{Z}$ (lexicographically ordered) with smallest positive element $(0, 1)$. Let $s \geq 2$ be any integer.

Example 2(contd.).

Consider the polynomial $F(x) = x^{2^s} - a$ belonging to $K(x)$ with $V_0(a-4) \geq (0,5)$. We show that $F(x)$ factors into a product of two irreducible polynomials over K each of degree 2^{s-1}. Let V_1 stand for the first stage valuation defined by
$V_1 = [V_0, V_1 x = (0, 1/2^{s-1})]$. Applying Theorem C, it can be easily checked that the polynomial $\phi_2(x) = x^{2^{s-1}} - 2$ is a key polynomial over V_1. Clearly $\phi_2(x)$ is not equivalent to x in V_1. Note that the ϕ_2-expansion of $F(x)$ is $(\phi_2(x))^2 + 4\phi_2(x) + 4 - a$. Denote $V_0(4-a)$ by μ and recall that by hypothesis $\mu \geq (0,5)$. So the ϕ_2-Newton polygon of $F(x)$ with respect to V_1 consists of two edges. The first edge has slope $\lambda_1 = (0,1)$; the second edge has slope $\lambda_2 = \mu - (0,3) \geq (0,2)$.

Example 2(contd.).

Let α be a root of $\phi_2(x)$. In view of assertions $(i), (iii)$ of Theorem 7, we see that $F(x) = F_1(x)F_2(x)$, where $F_i(x)$ belonging to $K[x]$ having degree 2^{s-1} is a lifting of a monic linear polynomial $T_i(y) \neq y$ belonging to $\overline{K(\alpha)}[y]$ with respect to $\phi_2(x)$,$\lambda_i + V_1(\phi_2) = \lambda_i + (0, 1)$. It now follows from Theorem 7(iv) that $F_i(x)$ is irreducible over K for $i = 1, 2$ and for any root θ_i of $F_i(x)$, $[G(K(\theta_i)) : \Gamma_0] = 2^{s-1}$. Thus for each root θ of $F(x)$, $K(\theta)$ is a totally ramified extension of (K, V_0).

Remark.

It may be pointed out that Theorem 1.2 of [Manuscr. Math, 151, 223-241] does not establish the irreducibility of $F(x)$ over K in Example 1 even when $s = t = 2$, for in this situation the ϕ-Newton polygon of $F(x)$ (with underlying valuation V_0) consists of a single edge having slope $\lambda_0/2$ with length of horizontal projection 4. So by Theorem 1.2 of [Manuscr. Math, 151, 223-241], $F(x)$ would be a lifting of a second degree polynomial belonging to $\overline{K(\beta)}[y]$ with respect to $\phi(x), \lambda_0/2$, where β is a root of $\phi(x)$.

Remark (contd.)

As regards Example 2, $\phi(x) = x$ is the only irreducible factor of $F(x)$ modulo the maximal ideal M_0 of the valuation ring of V_0 and the ϕ-Newton polygon of $F(x)$ consists of a single edge having slope $(0, 1/2^{s-1})$ with length of horizontal projection 2^s. So $F(x)$ will be a lifting of a square of a linear polynomial belonging to $\overline{K}[y]$ with $\overline{K}$ being the field of two elements. Therefore Theorem 1.2 of [Manuscr. Math, 151, 223-241] does not give any information regarding the factorization of $F(x)$ in this situation. Similarly in the last example the irreducibility of $F(x)$ cannot be established by the analogue of Ore's Theorem for Krull valuations.

References.

[APZ1] Alexandru, V., Popescu, N., Zaharescu, A. (1988). A theorem of characterization of residual transcendental extension of a valuation. *J. Math. Kyoto Univ.* 28:579-592.

[APZ2] Alexandru, V., Popescu, N., Zaharescu, A. (1990). Minimal pairs of definition of a residual transcendental extension of a valuation. *J. Math. Kyoto Univ.* 30:207-225.

[Cohen] Cohen, S.D., Movahhedi, A., Salinier, A. (2000). Factorization over local fields and the irreducibility of generalized difference polynomials. *Mathematika* 47:173-196.

[En-Pr] Engler, A.J., Prestel, A. (2005). *Valued Fields.* New York: Springer-Verlag.

[GMN] Guàrdia, J., Montes, J., Nart, E. (2012). Newton polygons of higher order in algebraic number theory. *Trans. Amer. Math. Soc.* 364:361–416.

[Hen] Hensel, K. (1894). Arithmetische Untersuchung über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung. *J. Reine Angew. Math.* 113:128-160.

[Edi] Jhorar, B., Khanduja, S.K. (2017). A generalization of Eisenstein-Dumas- Schönemann Irreducibility Criteria. *Proc. Edinburgh Math. Soc.* 61:19.

[Jh-Kh] Jhorar, B., Khanduja, S.K. (2016). Reformulation of Hensel's Lemma and extension of a theorem of Ore. *Manuscr. Math.* 151(1):223-241.

[Kh1] Khanduja, S.K. (2010). On Brown's constant associated with irreducible polynomials over henselian valued fields. *J. Pure Appl. Algebra* 214:2294-2300.

[Kh-Ku2] Khanduja, S.K., Kumar, M. (2010). Prolongations of valuations to finite extensions. *Manuscr. Math.* 131:323-334.

[Kh-Ku] Khanduja, S.K., Kumar, M. (2012). On prolongations of valuations via Newton polygons and liftings of polynomials. *J. Pure Appl. Algebra* 216:2648-2656.

[KH-SH] Khanduja, S.K., Saha, J. (1999). A generalized fundamental principle. *Mathematika* 46:83-92.

Kh-Po-Ro] Khanduja, S.K., Popescu, N., Roggenkamp, K.W. (2002). On minimal pairs and residually transcendental extensions of valuations. *Mathematika* 49:93-106.

[Mac] MacLane, S. (1936). A construction for absolute values in polynomial rings. *Trans. Amer. Math. Soc.* 40:363-395.

[Moy] Moyls, B.N. (1951). The structure of valuations of the rational function field $K(x)$. *Trans. Amer. Math. Soc.* 71:102-112.

[Ore1] Ore, Ø. (1923). Zur Theorie der algebraischen Körper. *Acta Mathematica* 44:219-314.

[Ore2] Ore, Ø. (1924-25). Weitere Untersuchungen zur Theorie der algebraischen Körper. *Acta Mathematica* 45:145-160.

[Ore3] Ore, Ø. (1925). Bestimmung der Diskriminanten algebraischer Körper. *Acta Mathematica* 45:303-344.

[Lp-Np] Popescu L., Popescu, N. (1991). On the residual transcendental extensions of a valuation, key polynomials and augmented valuation. *Tsukuba J. Math.* 15(1):57-78.

[Po-Za] Popescu N., Zaharescu, A. (1995). On the structure of the irreducible polynomials over local fields. *J. Number Theory* 52:98-118.

[Rib2] Ribenboim, P. (1999). *The Theory of Classical Valuations.* New York: Springer-Verlag.

[Wei] S.H. Weintraub, A mild generalization of Eisenstein's criterion, *Proc. Amer. Math. Soc.* **141** (2013) 1159–1160.

Thank You