ON THE DECOMPOSITION THEORY FOR KRULL VALUATIONS

BY

P. Ribenboim

Let K be a field endowed with a Krull valuation v, $L \mid K$ a finite Galoisian extension, $\mathcal{V} = \{w = w_1, w_2, \cdots, w_g\}$ the set of distinct prolongations of v to L. We define and study the decomposition field and decomposition group associated with a *distinguished set* $\mathcal{E}$ of valuations, $\mathcal{E} \subseteq \mathcal{V}$.

Among other results, we obtain a new proof that the value group $w(Z)$ and the residue-class field Z/w of the decomposition field Z of w in $L \mid K$ are respectively the same as those of the ground field K: $w(Z) = v(K)$, $Z/w = K/v$; cf. [1], [4, pp. 70 ff.].

Finally, the theory is applied to define the decomposition field of a prolongation of the valuation v to a finite extension of K, which may be neither normal nor separable.

An example is given to show that the results indicated cannot be improved.

1. Known results and a technical lemma

Let w_1, w_2 be valuations of a field L, and x_1, x_2 nonzero elements of L. We say that the pair (w_1, x_1) is *compatible* with the pair (w_2, x_2) in case

$$(w_1 \wedge w_2)(x_1) = (w_1 \wedge w_2)(x_2),$$

where $w_1 \wedge w_2$ denotes the greatest lower bound of w_1, w_2 in the ordered set of valuations of L (cf. [4, p. 43] or [3]).

This relation is transitive: If (w_1, x_1) is compatible with (w_2, x_2), and if (w_2, x_2) is compatible with (w_3, x_3), let us consider $w_1 \wedge w_2$ and $w_2 \wedge w_3$. Since both valuations are coarser than w_2, one is coarser than the other, say $w_1 \wedge w_2 \geqq w_2 \wedge w_3$; hence $w_1 \wedge w_3 = w_2 \wedge w_3$. Thus, if either $(w_1 \wedge w_2)(y) = 0$ or $(w_2 \wedge w_3)(y) = 0$, we have $(w_1 \wedge w_3)(y) = 0$. This implies that

$$(w_1 \wedge w_3)(x_1/x_3) = (w_1 \wedge w_3)(x_1/x_2) + (w_1 \wedge w_3)(x_2/x_3) = 0,$$

showing that (w_1, x_1) is compatible with (w_3, x_3).

More generally, the set $\{(w_1, x_1), (w_2, x_2), \cdots, (w_g, x_g)\}$ is said to be *compatible* when (w_i, x_i) is compatible with (w_j, x_j), for any $i \neq j$.

The following theorems will be used (cf. [3]):

Approximation Theorem. *If $w_1, \cdots, w_g$ are pairwise incomparable valuations of L, if $x_1, \cdots, x_g \in L$ are such that*

$$\{(w_1, x_1), (w_2, x_2), \cdots, (w_g, x_g)\}$$

Received July 18, 1961; received in revised form January 4, 1962.

is compatible, then there exists $x \in L$ *such that*

$$w_i(x) = w_i(x_i) \qquad \textit{for every } i = 1, \cdots, g.$$

STRONG APPROXIMATION THEOREM. *Let* $w_1, \cdots, w_g$ *be pairwise incomparable valuations of* L, *let* $x_1, \cdots, x_g \in L$ *be such that* $\{(w_1, x_1), \cdots, (w_g, x_g)\}$ *is compatible, and let* $b_1, \cdots, b_g \in L$. *Then, in order that there exist an element* $x \in L$ *such that*

$$w_i(x - b_i) = w_i(x_i) \qquad \textit{for every } i = 1, \cdots, g,$$

it is necessary and sufficient that the following condition hold:

If $w_i(b_i - b_j) < w_i(x_i)$, *for indices* $i \neq j$, *then*

$$(w_i \wedge w_j)(x_i) = (w_i \wedge w_j)(b_i - b_j).$$

The following technical result will be used in the proof of Theorem 2:

LEMMA 1. *Let* $L \mid K$ *be an algebraic extension,* v *a valuation of* K, *and* $w_1, \cdots, w_g$ *a set of distinct prolongations of* v *to* L. *Given an element* $x_1 \in L$, $x_1 \neq 0$, *there exist elements* $x_2, \cdots, x_g \in L$ *such that* $\{(w_1, x_1), \cdots, (w_g, x_g)\}$ *is compatible and*[1]

$$w_1(x_1) < w_i(x_i) \qquad \textit{for every } i = 2, \cdots, g.$$

Proof. By the transitivity property of the compatibility relation, it is sufficient to consider the case where $g = 2$.

If $w_1(x_1) < w_2(x_1)$, we take $x_2 = x_1$.

If $w_1(x_1) = w_2(x_1)$, we take $x_2 = x_1 y$, with $(w_1 \wedge w_2)(y) = 0, w_2(y) > 0$, observing that such an element $y \in L$ exists, since $w_1 \wedge w_2 \neq w_2$.

If $w_2(x_1) < w_1(x_1)$, let m be an integer such that $m \cdot w_1(L) \subseteq v(K)$, $m \cdot w_2(L) \subseteq v(K)$; hence, there exist elements $y_1, y_2 \in K$ such that $m \cdot w_1(x_1) = v(y_1)$, $m \cdot w_2(x_1) = v(y_2)$, and hence $v(y_2) < v(y_1)$. Taking $x_2 = x_1 \cdot (y_1/y_2)^2$, we have

$$(w_1 \wedge w_2)(y_2) = m \cdot (w_1 \wedge w_2)(x_1) = (w_1 \wedge w_2)(y_1);$$

hence $(w_1 \wedge w_2)(x_1) = (w_1 \wedge w_2)(x_2)$, so (w_1, x_1) is compatible with (w_2, x_2).

Finally,

$$w_2(x_2) = w_2(x_1) + 2 \cdot [v(y_1) - v(y_2)] > w_2(x_1) + (1/m)[v(y_1) - v(y_2)]$$
$$= w_2(x_1) + w_1(x_1) - w_2(x_1) = w_1(x_1).$$

2. New results

Let $L \mid K$ be a finite Galoisian extension, $\mathcal{K} = \mathrm{Gal}(L \mid K)$; let v be a valuation of K, and $\mathcal{E}$ a nonempty set of prolongations of v to L.

[1] Since the value groups of the valuations $w_1, \cdots, w_g$ may be considered as subgroups of the divisible group generated by $v(K)$, we may compare the values $w_1(x_1)$, $w_i(x_i)$.

The set

$$\mathcal{Z}_{L|K}(\mathcal{E}) = \mathcal{Z}(\mathcal{E}) = \{\sigma \in \mathcal{K} \mid w \circ \sigma \in \mathcal{E} \text{ for every } w \in \mathcal{E}\}$$

is clearly a subgroup of $\mathcal{K}$, called the *decomposition group of the set* $\mathcal{E}$ *in* $L \mid K$. The field of invariants of $\mathcal{Z}(\mathcal{E})$ is denoted by $Z_{L|K}(\mathcal{E}) = Z(\mathcal{E})$, and it is called the *decomposition field of the set* $\mathcal{E}$ *in* $L \mid K$.

The special case where $\mathcal{E}$ is reduced to only one prolongation w of v is already well known; corresponding notations $\mathcal{Z}(w)$, $Z(w)$ will be used.

A nonempty set $\mathcal{E}$ of valuations of L, prolongations of the valuation v of K, is called *a distinguished set* whenever there exists an intermediate field F, $K \subseteq F \subseteq L$, such that

(1) all the valuations $w \in \mathcal{E}$ have the same restriction w^F to F;

(2) $\mathcal{E}$ is the set of all the prolongations of w^F to L.

Trivial distinguished sets are $\mathcal{V}$ (the set of all the prolongations of v to L) and each set $\{w\}$, where w is any prolongation of v to L.

In general, there may exist sets $\mathcal{E}$ which are not distinguished, because

If $\mathcal{E}$ *is a distinguished set, then the number of elements in* $\mathcal{E}$ *divides the degree* $[L:K]$ (a more precise assertion will be made later).

Indeed, if $\mathcal{E}$ is a distinguished set of valuations of L, if F is a field such that $\mathcal{E}$ is the set of all prolongations to L of some valuation u of F, then $[L:F] = e \cdot f \cdot t \cdot \chi^q$ (cf. [4, p. 78]), where

e is the ramification index of any $w \in \mathcal{E}$ in $L \mid F$,

f is the inertial degree of any $w \in \mathcal{E}$ in $L \mid F$,

t is the number of valuations in $\mathcal{E}$,

χ is the characteristic exponent of the residue-class field K/v, $q \geqq 0$.

Hence, t divides $[L:K] = [L:F] \cdot [F:K]$.

THEOREM 1. *Let* $\mathcal{E}$ *be a nonempty set of prolongations of* v *to* L.

(a) *If* $w \in \mathcal{V}$, $w \notin \mathcal{E}$, *then the restriction of* w *to* $Z(\mathcal{E})$ *is distinct from the restriction to* $Z(\mathcal{E})$ *of any valuation in* $\mathcal{E}$.

(b) $Z(\mathcal{E})$ *is the smallest intermediate field with property* (a).

(c) *If, moreover,* $\mathcal{E}$ *is a distinguished set, then all the valuations in* $\mathcal{E}$ *have the same restriction to* $Z(\mathcal{E})$.

Proof. (a) If $w \in \mathcal{V}$ has the same restriction to $Z(\mathcal{E})$ as a valuation $w' \in \mathcal{E}$, then w, w' are conjugate valuations in the extension $L \mid Z(\mathcal{E})$, having Galois group $\mathcal{Z}(\mathcal{E})$; so there exists $\sigma \in \mathcal{Z}(\mathcal{E})$ such that $w = w' \circ \sigma \in \mathcal{E}$.

(b) Let F be a field, $K \subseteq F \subseteq L$, $\mathcal{F} = \mathrm{Gal}(L \mid F)$, and assume that F satisfies property (a) of $Z(\mathcal{E})$; we want to show that $F \supseteq Z(\mathcal{E})$, or equivalently, $\mathcal{F} \subseteq \mathcal{Z}(\mathcal{E})$. Let $\sigma \in \mathcal{F}$, $w \in \mathcal{E}$; then $w \circ \sigma$ is a valuation of L having the same restriction to F as w; by property (a) of F, we must have $w \circ \sigma \in \mathcal{E}$. This shows that $\sigma \in \mathcal{Z}(\mathcal{E})$, and hence $\mathcal{F} \subseteq \mathcal{Z}(\mathcal{E})$.

(c) There exists an intermediate field F such that $\mathcal{E}$ is the set of all the prolongations to L of a valuation of F. Hence, F satisfies property (a) above;

by (b), $F \supseteq Z(\mathcal{E})$; hence all the valuations in $\mathcal{E}$ have the same restriction to $Z(\mathcal{E})$.

THEOREM 2. (a) *If $\mathcal{E}$ is any nonempty set of prolongations of v to L, then, for every $w \in \mathcal{E}$, $(w(Z(\mathcal{E})):v(K))$ divides*

$$(\mathcal{Z}(w):\mathcal{Z}(\mathcal{E}) \cap \mathcal{Z}(w)) = [Z(\mathcal{E})\cdot Z(w):Z(w)];$$

in particular, if $\mathcal{E} = \{w\}$, then $w(Z(w)) = v(K)$.

(b) *$Z(w)/w = K/v$ for every prolongation w of v to L.*

Proof. (a) We may assume that $Z(\mathcal{E}) \neq K$. Let us denote $H = Z(\mathcal{E})\cdot Z(w)$, $\mathcal{H} = \mathrm{Gal}(L \mid H) = \mathcal{Z}(\mathcal{E}) \cap \mathcal{Z}(w)$, $m = (\mathcal{Z}(w):\mathcal{H}) = [H:Z(w)]$.

To show that $(w(Z(\mathcal{E})):v(K))$ divides m, it is sufficient to establish that if $\alpha \in w(Z(\mathcal{E}))$, then $m\alpha \in v(K)$. Indeed, this implies that the totally ordered abelian group $w(Z(\mathcal{E})) \subseteq (1/m)v(K)$, so it must be of type $(1/m')v(K)$, where m' divides m.

Let $\alpha \in w(Z(\mathcal{E})) \subseteq w(H)$. Denote by $u_1 = w^H$ the restriction of w to H; u_1 is not the only prolongation of v to H, for otherwise $\mathcal{E} = \mathcal{V}$ by Theorem 1 (a), and $Z(\mathcal{E}) = K$ by Theorem 1 (b).

Let $u_2, \cdots, u_s$ be the other valuations of H extending v. If $x_1 \in H$ is such that $\alpha = u_1(x_1)$, by Lemma 1, there exist $x_2, \cdots, x_s \in H$ such that

$$\{(u_1, x_1), \cdots, (u_s, x_s)\}$$

is compatible and $u_1(x_1) < u_i(x_i)$ for every $i = 2, \cdots, s$. As the valuations $u_1, u_2, \cdots, u_s$ are pairwise incomparable (since they are prolongations of v), by the Approximation Theorem there exists $c \in H$ such that $u_i(c) = u_i(x_i)$ for every $i = 1, 2, \cdots, s$.

Let

$$b = N_{H \mid Z(w)}(c) = \textstyle\prod_\sigma \sigma(c) \in Z(w)$$

(where σ runs through a set of representatives of right cosets of $\mathcal{H}$ in $\mathcal{Z}(w)$). We observe that for every such σ we have $w \circ \sigma = w$; on the other hand, their number is $m = (\mathcal{Z}(w):\mathcal{H})$. Then

$$w(b) = \textstyle\sum_\sigma w(\sigma(c)) = \sum_\sigma w(c) = m\alpha.$$

Let now

$$a = \mathrm{Tr}_{Z(w) \mid K}(b) = \textstyle\sum_\tau \tau(b) \in K$$

(where τ runs through a set of representatives of right cosets of $\mathcal{Z}(w)$ in $\mathcal{K}$); we have $v(a) = w(a) \geqq \min_\tau \{w \circ \tau(b)\}$, and we want to compute the exact value of a.

If $\tau \in \mathcal{Z}(w)$, then $w \circ \tau = w$, and hence $w(\tau(b)) = w(b) = m\alpha$.

If $\tau \notin \mathcal{Z}(w)$, then $\tau\sigma \notin \mathcal{Z}(w)$ (for each $\sigma \in \mathcal{Z}(w)$). Hence $(w \circ \tau\sigma)^H \neq w^H$, since otherwise the valuations $w \circ \tau\sigma$, w would be conjugate in the extension $L \mid H$, and thus there would exist $\varphi \in \mathcal{H}$ such that $w \circ \tau\sigma = w \circ \varphi$, $\tau\sigma\varphi^{-1} \in \mathcal{Z}(w)$

and $\tau\sigma \in \mathcal{Z}(w)\cdot\mathcal{H} = \mathcal{Z}(w)$, a contradiction. It follows that $w \circ \tau\sigma(c) = u_i(c) = u_i(x_i) > \alpha$, for some $u_i \neq u_1$.

It follows that if $\tau \notin \mathcal{Z}(w)$, then

$$w \circ \tau(b) = w \circ \tau(\textstyle\prod_\sigma \sigma(c)) = \sum_\sigma w \circ \tau\sigma(c) > m\alpha.$$

We conclude that there exists precisely one τ such that $w \circ \tau(b) = m\alpha$ is the minimum possible. Hence, $v(a) = w(a) = \min_\tau \{w \circ \tau(b)\} = m\alpha$, so $m\alpha \in v(K)$.

(b) We know that $Z(w)/w$ is an extension of K/v (after a canonical identification). We must show that if $b \in A_w \cap Z(w)$ (valuation ring of the restriction of w to $Z(w)$) there exists $a \in A$ (valuation ring of v) such that $b \equiv a \pmod{P_w \cap Z(w)}$ (prime ideal of the restriction of w to $Z(w)$).

We may assume $b \neq 0$ and $Z(w) \neq K$.

Let u_1 be the restriction of w to $Z(w)$. u_1 is not the only prolongation of v to $Z(w)$, for otherwise v has only one prolongation to L, by Theorem 1 (a) applied to $\mathcal{E} = \{W\}$; then $Z(w) = K$.

Let $u_2, \cdots, u_s$ be the other prolongations of v to $Z(w)$. We want to apply the Strong Approximation Theorem.

Let j be an index such that $u_1 > u_1 \wedge u_j \geqq u_1 \wedge u_i$, for every $i = 2, \cdots, s$; hence, there exists an element $x_1 \in Z(w)$ such that $u_1(x_1) > 0$, but

$$(u_1 \wedge u_j)(x_1) = (u_1 \wedge u_i)(x_1) = 0$$

for every $i = 2, \cdots, s$.

By Lemma 1, there exist elements $x_2, \cdots, x_s \in Z(w)$ such that

$$\{(u_1, x_1), \cdots, (u_s, x_s)\}$$

is compatible and $0 < u_1(x_1) < u_i(x_i)$ for every $i = 2, \cdots, s$; hence $(u_i \wedge u_1)(x_i) = (u_i \wedge u_1)(x_1) = 0$. Considering the elements $b, 1, \cdots, 1$, we now verify the condition of the Strong Approximation Theorem.

If $u_1(b - 1) < u_1(x_1)$, from $0 \leqq u_1(b - 1)$ we deduce that

$$0 \leqq (u_i \wedge u_1)(b - 1) \leqq (u_i \wedge u_1)(x_1) = 0.$$

If $u_i(b - 1) < u_i(x_i)$ and $0 \leqq u_i(b - 1)$, then

$$0 \leqq (u_i \wedge u_1)(b - 1) \leqq (u_i \wedge u_1)(x_i) = 0;$$

if, however, $u_i(b - 1) < 0$, then $u_i(b) = u_i(b - 1)$, so from $u_1(b) \geqq 0$ it follows that

$$(u_1 \wedge u_i)(b - 1) = (u_1 \wedge u_i)(b) = 0 = (u_1 \wedge u_i)(x_i).$$

By the Strong Approximation Theorem, there exists an element $z \in Z(w)$ such that $u_1(z - b) = u_1(x_1) > 0$, $u_i(z - 1) = u_i(x_i) > 0$, for every $i = 2, \cdots, s$. So $u_1(z) \geqq 0$ (because $u_1(b) \geqq 0$), $u_i(z) = 0$ for $i \neq 1$, and

$$z \equiv b \pmod{P_w \cap Z(w)}.$$

Now, let $a = N_{Z(w)|K}(z) \in K$, so $a = \prod_\tau \tau(z)$ (where τ runs through a set of representatives of the right cosets of $\mathcal{Z}(w)$ in $\mathcal{K}$).

It follows that $a \in A$, since

$$v(a) = w(a) = w(\textstyle\prod_\tau \tau(z)) = \sum_\tau w \circ \tau(z) \geqq 0,$$

because each valuation $w \circ \tau$ induces one of the valuations $u_1, u_2, \cdots, u_s$, and $u_i(z) \geqq 0$ for every $i = 1, \cdots, s$.

We finish the proof as in part (a), by showing that $a \equiv b \pmod{P_w \cap Z(w)}$; in fact, it is sufficient to show that $a \equiv z \pmod{P_w \cap Z(w)}$. For that purpose, we remark that if $\tau \notin \mathcal{Z}(w)$, then $w \circ \tau \not\asymp w$; hence its restriction to $Z(w)$ is some $u_i \not\asymp u_1$, so

$$w(\tau(z) - 1) = w(\tau(z - 1)) = u_i(z - 1) = u_i(x_i) > 0,$$

and $\tau(z) \equiv 1 \pmod{P_w}$. Therefore

$$a = \textstyle\prod_\tau \tau(z) = z \cdot \prod_{\tau \neq \varepsilon} \tau(z) \equiv z \pmod{P_w \cap Z(w)}.$$

THEOREM 3. *If F is any intermediate field, $\mathfrak{F} = \text{Gal}(L \mid F)$, and w is any prolongation of v to L, then*

(a) $[Z(w) \cdot F : Z(w)] = e_{F|K}(w) \cdot f_{F|K}(w) \cdot \chi$, *where $r \geqq 0$ and χ is the characteristic exponent of K/v;*

(b) *if $\mathcal{E}$ denotes the set of valuations of L having the same restriction to F as w, then the number t of valuations in $\mathcal{E}$ is equal to*

$$t = (\mathfrak{F} : \mathcal{Z}(w) \cap \mathfrak{F}) = [Z(w) \cdot F : F],$$

and the number g of prolongations of v to L is equal to

$$g = \frac{t \cdot [F:K]}{[Z(w) \cdot F : Z(w)]},$$

where

$$\frac{[F:K]}{[Z(w) \cdot F : Z(w)]} = \frac{[Z(w):K]}{[Z(w) \cdot F : F]}$$

is equal to the number of distinct prolongations of v to F; in particular, t divides g.

Proof. (a) Let $H = Z(w) \cdot F$; by standard results, or Theorem 1 (a) applied to $\mathcal{E} = \{w\}$, the restriction of w to $Z(w)$ has only one prolongation to L; the same is true of the restriction of w to H, since $H \supseteq Z(w)$. Hence

$$[L : Z(w)] = e_{L|Z(w)} \cdot f_{L|Z(w)} \cdot \chi^q,$$

$$[L : H] = e_{L|H} \cdot f_{L|H} \cdot \chi^{q'},$$

where $q \geqq 0$, $q' \geqq 0$, and the indices e, f are computed for w. By the transitivity of e and f, we have

$$[H : Z(w)] = e_{H|Z(w)} \cdot f_{H|Z(w)} \cdot \chi^{q-q'}.$$

Since $e_{H|Z(w)} \cdot f_{H|Z(w)} \leqq [H : Z(w)]$ (cf. [4, p. 55]), we have $q - q' \geqq 0$.

Finally, since $Z(w)$ is the decomposition field of w over K, and $H = Z(w) \cdot F$ is the decomposition field of w over F, we have

$$e_{Z(w)|K} = f_{Z(w)|K} = e_{H|F} = f_{H|F} = 1$$

by Theorem 2, so that $e_{H|Z(w)} = e_{H|K} = e_{F|K}$, and similarly for f.

(b) Since $H = Z(w) \cdot F$ is the decomposition field of w in $L \mid F$, the number t of valuations in the set $\mathcal{E}$ is equal to $t = [H:F]$ (cf. [4, p. 74]). Similarly, $g = [Z(w):K]$; hence, by transitivity of degrees,

$$g = \frac{t \cdot [F:K]}{[H:Z(w)]}.$$

We show now that the prolongations of v to F correspond in a one-to-one way to the double cosets $\mathcal{Z}(w)\sigma\mathfrak{F}$ (for $\sigma \in \mathcal{K}$). Indeed, if u is any prolongation of v to F, let $w' = w \circ \sigma$ be any prolongation of u to L; if $w_1' = w \circ \sigma_1$ is another prolongation of u, then w', w_1' are conjugate with respect to $\mathfrak{F}$; hence $w_1' = w' \circ \xi$, $\xi \in \mathfrak{F}$, so $w \circ \sigma_1 = w \circ \sigma\xi$ and $\sigma_1 \in \mathcal{Z}(w)\sigma\mathfrak{F}$. The mapping that associates with u the double coset $\mathcal{Z}(w)\sigma\mathfrak{F}$ is well defined, onto the set of double cosets, and one-to-one.

Hence the number of prolongations of v to F is equal to the number of double cosets $\mathcal{Z}(w)\sigma\mathfrak{F}$, that is,

$$\frac{(\mathcal{K}:\mathfrak{F})}{(\mathcal{Z}(w):\mathcal{Z}(w) \cap \mathfrak{F})} = \frac{[F:K]}{[H:Z(w)]} = \frac{[Z(w):K]}{[H:F]} = \frac{g}{t}.$$

We now apply the preceding considerations to define the decomposition field of a valuation w in an extension which may be neither separable nor normal.

Let $M \mid K$ be a finite (algebraic) extension, v a valuation of K, and $w = w_1, \cdots, w_g$ its prolongations to M. Let S be the separable closure of K in M, and L the normal extension of K, generated by S; hence $L \mid K$ is a finite Galoisian extension, whose group will be denoted by $\mathcal{K}$. Let $\mathcal{E}$ be the set of prolongations to L of the restriction w^S of w to S; hence $\mathcal{E}$ is a distinguished set of valuations of L.

DEFINITION. The decomposition field $Z_{L|K}(\mathcal{E})$ of the set $\mathcal{E}$ in $L \mid K$ is called the *decomposition field of w in $M \mid K$* and denoted by $Z_{M|K}(w) = Z(w)$.

Since all the valuations in $\mathcal{E}$ have the same restriction to S, by Theorem 1 (b), we deduce that $Z(w) = Z_{L|K}(\mathcal{E}) \subseteq S$.

The restriction of each valuation $w_i \neq w$ to $Z(w)$ is different from the restriction of w to $Z(w)$.

This follows from the facts that $M \mid S$ is a purely inseparable extension (hence the restrictions w_i^S, w^S are distinct) and that the restriction of w to $Z(w)$ has only one prolongation to L.

$Z(w)$ is the smallest field between K and M with the above property.

Let F be an intermediate field such that $w_i^F \neq w^F$ for every $i = 2, \cdots, g$; since $F \mid (F \cap S)$ is a purely inseparable extension, $w_i^{F \cap S} \neq w^{F \cap S}$. All the valuations in $\mathcal{E}$ have the same restriction w^S to S, and hence also the same restriction $w^{F \cap S}$ to $F \cap S$. On the other hand, if u is a prolongation of $w^{F \cap S}$ to L, then $u \in \mathcal{E}$, for otherwise $u^S = w_i^S$ for some $i > 1$, and hence $w^{F \cap S} = w_i^{F \cap S}$, a contradiction. By Theorem 1 (b), we conclude that

$$F \supseteq F \cap S \supseteq Z(\mathcal{E}) = Z(w).$$

Similarly, for every $u \in \mathcal{E}$ we have

$$[Z(u) \cdot Z(w) : Z(u)] = e_{Z(w)|K}(w) \cdot f_{Z(w)|K}(w) \cdot \chi^q$$

(with $q \geqq 0$), and the number of distinct prolongations of v to M is equal to

$$\frac{[S:K]}{[Z(u) \cdot S : Z(u)]},$$

where u is any prolongation of v to L.

This last assertion follows at once from Theorem 3 (b), applied to the extension $L \mid K$ and the intermediate field $F = S$, if we observe that each valuation of S has only one prolongation to M.

The following example shows that the results of Theorem 3 are, in a sense, the best ones to be expected.

Example. There exists a field K, endowed with a discrete valuation v, of rank 1, such that, given any two integers $\mu > 1$, $\nu > 1$, there exists a finite Galoisian extension L of K, with the following property: There exists a distinguished set $\mathcal{E}$ of valuations, prolongations of v to L, such that if u is the restriction of any $w \in \mathcal{E}$ to the decomposition field $Z(\mathcal{E})$, then

$$e_{Z(\mathcal{E})|K}(u) = \mu, \qquad f_{Z(\mathcal{E})|K}(u) = \nu.$$

In this construction, we shall use Krull's existence theorem (cf. [2]).

Given μ, ν, let p be any prime number such that $\mu\nu < p$, and let $t = (p - \mu\nu) + 1 > 1$.

Let K be a field of characteristic zero, with a discrete valuation v such that K/v has also characteristic zero, and let us assume that K admits at least one more nonequivalent discrete valuation v'. We may take, for example, $K = \mathbf{Q}(X)$, v being that prolongation of the trivial valuation of $\mathbf{Q}$ such that $v(X) = 1$; then $K/v = \mathbf{Q}$; moreover, we may take v' equal to the natural prolongation of the 2-adic valuation of $\mathbf{Q}$ to $\mathbf{Q}(X) = K$, so v' is also discrete.

By Krull's existence theorem, there exists a separable extension $F \mid K$, of degree p, such that v admits t prolongations $u_1, u_2, \cdots, u_t$ to F, for which we have $e_{F|K}(u_1) = \mu$, $f_{F|K}(u_1) = \nu$, $e_{F|K}(u_i) = 1$, $f_{F|K}(u_i) = 1$, for every $i = 2, \cdots, t$.

Let $L \mid K$ be the smallest normal extension of K containing F, and let $\mathcal{E}$ be the set of all the prolongations of u_1 to L.

We show now that $Z(\mathcal{E}) = F$. Indeed, $Z(\mathcal{E})$ is the smallest subfield of L

such that all the valuations of $\mathcal{E}$ have the same restriction to $Z(\mathcal{E})$, but some valuation of L, extending v and not in $\mathcal{E}$, has distinct restriction to $Z(\mathcal{E})$. As F has this property, then $F \supseteq Z(\mathcal{E})$. As $[F:K] = p$ prime, if $F \neq Z(\mathcal{E})$, then $Z(\mathcal{E}) = K$; this means that $\mathfrak{Z}(\mathcal{E}) = \mathfrak{K} = \text{Gal}\,(L \mid K)$, so $\mathcal{E} = \mathcal{V}$ (set of all the prolongations of v to L), which is impossible, since any prolongation of u_i, $i \geqq 2$, to L does not belong to $\mathcal{E}$.

The same example shows us that there may exist cases in which $Z(w) \cdot Z(\mathcal{E})$ contains strictly $Z(w)$, that is, $Z(w)$ does not contain $Z(\mathcal{E})$, for some $w \in \mathcal{E}$.

Similarly, if in the previous example we take p such that $p \neq 2\mu\nu - 1$, then $t \neq \mu\nu$. Let $w \in \mathcal{E}$; since $[Z(w) \cdot Z(\mathcal{E}):Z(w)] = \mu\nu$, then the number g of prolongations of v to L is

$$g = \frac{t \cdot [Z(\mathcal{E}):K]}{[Z(w) \cdot Z(\mathcal{E}):Z(w)]} \neq [Z(\mathcal{E}):K] .$$

Hence, contrary to the case where $\mathcal{E}$ is reduced to only one valuation, in general we have $[Z(\mathcal{E}):K] \neq g$.

Bibliography

1. Wolfgang Krull, *Allgemeine Bewertungstheorie*, J. Reine Angew. Math., vol. 167 (1932), pp. 160–196.
2. ———, *Über eine Existenzsatz der Bewertungstheorie*, Abh. Math. Sem. Univ. Hamburg, vol. 23 (1959), pp. 29–35.
3. P. Ribenboim, *Le théorème d'approximation pour les valuations de Krull*, Math. Zeitschrift, vol. 68 (1957), pp. 1–18.
4. Oscar Zariski and Pierre Samuel, *Commutative algebra, Vol. II*, Princeton, Van Nostrand, 1960.

University of Illinois
Urbana, Illinois