The important change that we have decided to bring in here is that we no lo
insist on what the level of the articles should be. We had previously empha
that the articles should be accessible to beginning research students. This
tation has turned out to be neither very clearly defined nor very effective. We
now that it is best to be flexible on this point and to let each author (anc
subject) determine his level of exposition. Needless to say, we continue to insis
the clarity of the exposition – whatever the level chosen.

Thus, in summing up, our goal remains the same as before, although some de
of presentation have been rearranged. If we had to describe our goal in a p
motto, we should say that it has always been and continues to be: Mehr L
(Goethe).

S.D. Chatterj
Managing Ed

EXPOSITIONES
MATHEMATICAE

Expo. Math. 3 (1985), 3-24

Equivalent forms of Hensel's lemma

Paulo Ribenboim

Dedicated to the memory of my friend Professor Robert A. Smith

Introduction

The celebrated Hensel's lemma, which is the cornerstone of the theory of p-adic numbers, has been the object of extensive studies. On the one hand, its scope has been broadened, first from the p-adic numbers to discrete valuation rings, then to rank one valuation rings, and later by Krull ([4]) to arbitrary valuation rings. On the other hand, it has also been formulated in the context of noetherian (and even non-noetherian) local domains, as well as in more general ring-theoretic situations. This proposition has found applications in number theory and in algebraic geometry and the process of henselization, which bears a resemblance with completion is of an algebraic nature, which makes it appropriate to be an important tool in model theory.

However, our aim in this paper is not to describe the development of ideas and applications centered around Hensel's lemma, but rather to examine closely the various formulations found in the literature.

We place ourselves in the framework of the theory of valued fields and show that Hensel's lemma is logically equivalent to many propositions concerning the number of the extensions of the valuation to algebraic extensions, or the lifting of polynomials from the residue field, or the determination of zeroes of a polynomial by a method which dates back to Newton, or still to a geometric formulation concerning the mutual distance between the zeroes of polynomials.

These facts are of a "folkloric" nature, yet no complete proof of their equivalence has appeared in any one paper (Nagata's paper [5] contains the proof of the equivalence of the so-called Hensel's strong condition).

This article is written at the level of research students. We have included in § 1, the definitions and the statement of all facts which are necessary for the subsequent sections; their proofs may be found in the papers or books listed in the bibliography. In the remaining sections, the proofs are complete and spelled out in detail.

§ 1 Recalling results from valuation theory

Let K be a field and v a *valuation* of K; v is a mapping from K onto a set $\Gamma \cup \{\infty\}$, such that the following properties are satisfied:

0723-0869/85/010003-22$ 5.90

(i) Γ is a totally ordered abelian additive group, ∞ is a symbol, $\infty \notin \Gamma$; $\alpha < \infty$ for every $\alpha \in \Gamma$, $\alpha + \infty = \infty + \alpha = \infty + \infty = \infty$ for every $\alpha \in \Gamma$

(ii) $v(x) = \infty$ if and only if $x = 0$

(iii) $v(x\,y) = v(x) + v(y)$

(iv) $v(x+y) \geq \min\{v(x), v(y)\}$, for every $x, y \in K$.

It follows easily that if $v(x) < v(y_i)$ (for $i = 1, \ldots, n$), then $v(x + y_1 + \ldots + y_n) = v(x)$.

The pair (K, v) is called a *valued field.*

$\Gamma = \Gamma_v$ is called the *value group* of v. If $\Gamma = \{0\}$ then v is called the *trivial* valuation.

The set $A_v = \{x \in K | v(x) \geq 0\}$ is a subring of K, called the *valuation ring* of v; K is the field of quotients of A_v and $A_v = K$ exactly when v is the trivial valuation.

The set $P_v = \{x \in K | v(x) > 0\}$ is the only maximal ideal of A_v; it is called the *valuation ideal* of v and $P_v = \{0\}$ exactly when v is the trivial valuation.

The elements of $A_v \backslash P_v$ are the *units* of A_v, i.e., their inverses belong to A_v.

The field A_v/P_v is called the *residue field* of the valuation v and it is often denoted by K_v; or also by $\bar{K}$.

For every $a \in A_v$ we shall denote by $\bar{a} = a + P_v$ the residue class of a modulo P_v. If $f = \sum_{i=0}^{m} a_i X^{m-i} \in A_v[X]$ we denote $\bar{f} = \sum_{i=0}^{m} \bar{a}_i X^{m-i} \in \bar{K}[X]$.

The valuations v, v' of K are said to be *equivalent* when $A_v = A_{v'}$. This happens if and only if there exists an isomorphism θ between the totally ordered groups Γ_v, $\Gamma_{v'}$ such that $v' = \theta \circ v$. Usually, we do not distinguish between equivalent valuations.

If K is a subfield of K' and v' is a valuation of K', then the restriction $v = v'|K$ of v' to K. is a valuation of K. v' is said to be an *extension* of v to K' and $A_v = A_{v'} \cap K$, $P_v = P_{v'} \cap K$, K_v is a subfield of $K'_{v'}$, Γ_v is a subgroup of $\Gamma_{v'}$. The extension is said to be *immediate* when $\Gamma_{v'} = \Gamma_v$, $K'_{v'} = K_v$. For the reader's convenience, we recall several facts from the theory of valuations, some of which will not be explicitly needed in this paper.

(A) The structure of the valuation ring

(A1) Krull's characterization of valuation rings: let R be an integral domain, K its field of quotients; there exists a valuation v of K such that $R = A_v$ if and only if R satisfies the following property: if $x \in K \backslash R$ then $x^{-1} \in R$.

(A2) Every finitely generated fractional ideal of A_v is a principal ideal.

(A3) The set of ideals of A_v is totally ordered by inclusion.

(A4) A_v is an integrally closed domain.

The prime ideals of A_v may be described in terms of the structure of the value group of v. A subgroup Δ of Γ_v is *isolated* (or *convex*) when the following condition is satisfied: if $0<\gamma<\delta\in\Delta$, $\gamma\in\Gamma$ then $\gamma\in\Delta$.

The collection of all isolated subgroups of Γ is totally ordered by inclusion. The quotient group Γ/Δ, consisting of the cosets $\bar{\gamma}=\gamma+\Delta$ (for $\gamma\in\Gamma$) is naturally totally ordered, by letting $\bar{\gamma}_1\leq\bar{\gamma}_2$ when there exists $\delta\in\Delta$ such that $\gamma_1\leq\gamma_2+\delta$. It follows that $\bar{\gamma}_1<\bar{\gamma}_2$ when $\gamma_1<\gamma_2+\delta$ for every $\delta\in\Delta$.

(A5) For every isolated subgroup Δ of Γ, let

$$P_\Delta=\{x\in A_v \mid v(x)\notin\Delta\};$$

then P_Δ is a prime ideal of A_v and Δ is the subgroup of Γ generated by $\{v(x) \mid x\in A_v\setminus P_v\}$. This establishes a bijection, reversing the inclusion, between the set of isolated subgroups of Γ and the set of prime ideals of A_v. We write also Δ_P for the isolated subgroup of Γ corresponding to the prime ideal P.

If A_v has $n\geq1$ distinct non-zero prime ideals (or equivalently, Γ has n distinct proper isolated subgroups) then the valuation v is said to be of *rank n*. It may be easily shown that v has rank 1 if and only if Γ_v is isomorphic to a subgroup of $\mathbb{R}$ (the additive group of real numbers).

(A6) An isolated subgroup Δ of Γ_v may be of two different types: either Δ is a limit isolated subgroup, that is, the union of all isolated subgroups properly contained in Δ; or there exists an immediate predecessor Δ' (Δ' is properly contained in Δ and there is no isolated subgroup properly between Δ and Δ'). In this second case, Δ/Δ' has no non-zero proper isolated subgroup, so it is isomorphic to a subgroup of $\mathbb{R}$.

Correspondingly, if P is any prime ideal of A_v, then either P is the intersection of all prime ideals of A_v properly containing P; or there exists an immediate successor P' (P' contains properly P and there is no prime ideal properly between P and P'). In particular, for every $a\in P_v$ there exists the smallest prime ideal P_1 of A_v containing a and the largest prime ideal P_2 of A_v not containing a; P_1 is the immediate successor of P_2.

(A7) For every prime ideal P of $A=A_v$ the ring of fractions $A_P=\left\{\frac{a}{b}\,\middle|\, a,b\in A, b\notin P\right\}$ is the ring of a valuation of K, denoted by v_P. It has maximal ideal equal to P, its residue field is A_P/P and its value group is Γ/Δ_P. Explicitly, $v_P=\theta\circ v$, where $\theta:\Gamma\to\Gamma/\Delta_P$ is the canonical homomorphism.

If v,v' are valuations of K and $A_v\subseteq A_{v'}$ then v is said to be *finer* than v or v' is said to be *coarser* than v, and we write $v\geq v'$. If v,v' are valuations of K and no one is coarser than the other, we say that v, v' are *incomparable*.

(A8) If R is a subring of K containing the valuation ring A_v then R is itself the ring of a valuation v' of K, which is therefore coarser than v, and there exists a prime ideal P of A_v such that $R=(A_v)_P$. The set of all valuations of K coarser than v is totally ordered by the relation $\geq$.

(A9) If $P\subset P'$ are distinct prime ideals of the valuation ring $A=A_v$ and $\Delta_P\supset\Delta_{P'}$ are the corresponding isolated subgroups of Γ_v, then $A_{P'}/P$ is the ring of a valuation, denoted by $v_{P',P}$, of the field A_P/P. It has maximal ideal P'/P, residue field $A_{P'}/P'$ and value group $\Delta_P/\Delta_{P'}$. Explicitly, if $x\in A_{P'}$ and $\bar{x}=x+P=A_{P'}/P$ then

$$v_{P',P}(\bar{x})=\begin{cases} v_P(x)+\Delta_{P'}\in\Delta_P/\Delta_{P'} & \text{when } x\notin P\\ \infty \quad \text{when } x\in P. \end{cases}$$

In particular, if $a\in P$, if P_1 is the smallest prime ideal of A_v containing a and P_2 is the largest prime ideal of A_v not containing a, then $\bar{v}=v_{P_1,P_2}$ is a valuation of rank 1 of $\bar{K}=A_{P_2}/P_2$ with valuation ring A_{P_1}/P_2.

(A10) If $\varphi: A_v\to A_v/P_v=K_v$ is the canonical homomorphism to the residue field, if B is any valuation ring with field of fractions K_v, then $\varphi^{-1}(B)$ is a valuation ring with field of fractions K. This establishes a bijection between the set of valuations of K_v and the set of valuations of K, which are finer than v.

(B) Intersection of finitely many valuation rings

We shall need the following result, which is a corollary of the approximation theorem:

(B1) Let $v_1,\dots,v_s$ be pairwise incomparable valuations of the field K, let $A=\bigcap_{i=1}^{s} A_{v_i}$. Then K is the field of quotients of A; the maximal ideals of A are $P_{v_i}\cap A$ and $A_{v_i}=A_{(P_{v_i}\cap A)}$

$$P_{v_i}=\left\{\frac{a}{b}\,\middle|\, a\in P_{v_i}\cap A,\ b\in A\backslash(P_{v_i}\cap A)\right\}$$

for every $i=1,\dots,s$. Moreover, for every $i=1,\dots,s$ $\bigcap_{j\neq i} P_{v_j}\nsubseteq P_{v_i}$.

(C) Extension of valuations from K to $K(X)$

If $f=\sum_{i=0}^{n} a_i X^{n-i}\in K[X]$, $n\geq 0$, any generator $c(f)$ of the principal fractional ideal $A_v a_0+\dots+A_v a_n$ defined by the coefficients of f, is called a *content of f*; $c(f)$ is defined up to units of A_v. A polynomial f is *primitive* when its content is a unit of A_v; in particular, $f\in A_v[X]$.

The analogue of Gauss' lemma states:

(C1) If $f,g\in K[X]$ then $A_v c(fg)=A_v c(f)\cdot A_v c(g)$.

Thus, the product of primitive polynomials is primitive.

It follows at once:

(C2) If $f \in A_v[X]$, $\deg(f) \geq 1$, then f is irreducible in $K[X]$ if and only if it is irreducible in $A_v[X]$.

(C3) If $f \in A_v[X]$, $\deg(f) \geq 1$, then f is a product of irreducible factors in $A_v[X]$ (which are unique up to constant factors).

(C4) The valuation v of K admits a *natural extension* to a valuation $\tilde{v}$ of $K(X)$, which is defined as follows: for every $f \in K[X]$, $\tilde{v}(f) = v(c(f))$; for every $\frac{f}{g} \in K(X)$ (with $f, g \in K[X]$, $g \neq 0$), $\tilde{v}\left(\frac{f}{g}\right) = \tilde{v}(f) - \tilde{v}(g)$. To simplify the notation, we shall write v for the natural extension $\tilde{v}$ of v.

(D) Extensions of valuations from K to algebraic extensions $\tilde{K}|K$

Let (K, v) be a valued field, let $\tilde{K}|K$ be any algebraic extension.

(D1) v has at least one extension to a valuation of $\tilde{K}$.

(D2) If $\tilde{v}$ is any extension of v to K, then $\tilde{K}_{\tilde{v}}$ is an algebraic extension of K_v, while $\Gamma_{\tilde{v}}$ is a subgroup of the divisible group generated by Γ_v, that is, for every $\gamma \in \Gamma_v$ there exists an integer $m \neq 0$ such that $m\gamma \in \Gamma_v$. Hence the prime ideals P and $\tilde{P}$ of A_v and $A_{\tilde{v}}$ correspond bijectively to each other by intersection: $\tilde{P} \cap K = P$.

(D3) Any two extensions from v to $\tilde{K}$ are incomparable valuations.

(D4) If $\tilde{K}|K$ is a purely inseparable extension then v has only one extension to $\tilde{K}$.

(D5) If $\tilde{K}|K$ has finite degree $[\tilde{K}:\mathrm{K}]$ then v has at most $[\tilde{K}:K]$ distinct extension to $\tilde{K}$.

We denote by $\mu_{\tilde{K}|K}(v)$ the number of such extensions.

Similarly, if $P' \supset P$ are prime ideals of A_v, if $\tilde{v}$ is an extension of v to $\tilde{K}$, if $\tilde{P}' \supset \tilde{P}$ are the prime ideals of $A_{\tilde{v}}$ such that $\tilde{P}' \cap K = P'$, $\tilde{P} \cap K = P$, then $\tilde{K}_{\tilde{v}_{\tilde{P}}}|K_{v_{\tilde{P}}}$ is a finite extension and so the number of extensions of $v_{P',P}$ to $\tilde{K}_{\tilde{v}_{\tilde{P}}}$ is finite, and in accordance with our notation, it is written $\mu_{\tilde{K}_{\tilde{v}_{\tilde{P}}}|K_{v_{\tilde{P}}}}(v_{P',P})$. Let $\mathscr{V}_P$ be the set of all valuations $\tilde{v}_{\tilde{P}}$ of $\tilde{K}$, which are extensions of v_P; so $\mathscr{V}_P$ has $\mu_{\tilde{K}|K}(v_P)$ elements.

(D6) If $P' \supset P$ we have the formula

$$\mu_{\tilde{K}|K}(v_{P'}) = \sum_{\tilde{v}_{\tilde{P}} \in \mathscr{V}_P} \mu_{\tilde{K}_{\tilde{v}_{\tilde{P}}}|K_{v_P}}(v_{P',P}).$$

In particular, if $\mu_{\tilde{K}|K}(v) = 1$ then $\mu_{\tilde{K}|K}(v_P) = 1$ and $\mu_{\tilde{K}_{\tilde{v}_{\tilde{P}}}|K_{v_P}}(v_{P',P}) = 1$.

We shall also need:

(D7) Let (K, v) be a valued field, let $L|K_v$ be any finite extension. Then there exists a finite extension $\tilde{K}|K$ and an extension $\tilde{v}$ of v to $\tilde{K}$ such that $\tilde{K}_{\tilde{v}} = L$.

Now we assume that $\tilde{K}|K$ is a Galois extension, with Galois group $\mathscr{H}$. We have the following results:

(D8) If $\tilde{v}$ is any extension of v to $\tilde{K}$, then for every $\sigma\in\mathscr{H}$, $\tilde{v}\circ\sigma$ is an extension of v to $\tilde{K}$ and every extension of v is of this form. In this situation, $\sigma(A_{\tilde{v}\circ\sigma})=A_{\tilde{v}}$, $\sigma(P_{\tilde{v}\circ\sigma})=P_{\tilde{v}}$ and therefore every $\sigma\in\mathscr{H}$ induces a K_v-isomorphism $\bar{\sigma}$ from the residue field $\tilde{K}_{\tilde{v}\circ\sigma}$ to $\tilde{K}_{\tilde{v}}$.

It is in general possible to have $\tilde{v}\circ\sigma=\tilde{v}\circ\tau$ for distinct $\sigma,\tau\in\mathscr{H}$.

The set $\mathscr{Z}=\mathscr{Z}_{\tilde{v}}=\{\sigma\in\mathscr{H}\,|\,\tilde{v}\circ\sigma=\tilde{v}\}$ is a subgroup of $\mathscr{H}$, called the *decomposition group* of $\tilde{v}$ (in the extension $\tilde{K}|K$).

The subfield $Z=Z_{\tilde{v}}=\{x\in\tilde{K}|\sigma(x)=x$ for every $\sigma\in\mathscr{Z}\}$ is called the *decomposition field* of $\tilde{v}$ (in the extension $\tilde{K}|K$).

(D9) If $\tau\in\mathscr{H}$ then $\mathscr{Z}_{\tilde{v}\circ\tau}=\tau^{-1}\mathscr{Z}_{\tilde{v}}\tau$ and $\tau^{-1}(Z_{\tilde{v}})=Z_{\tilde{v}\circ\tau}$.

(D10) The restriction of $\tilde{v}$ to $Z_{\tilde{v}}$ is distinct from the restriction to $Z_{\tilde{v}}$ of every other extension $\tilde{v}\circ\sigma\neq\tilde{v}$, and $Z_{\tilde{v}}$ is the smallest field between K and $\tilde{K}$ with the above property. If $\tilde{K}|K$ is of finite degree, the number of distinct extensions from v to $\tilde{K}$ is equal to the degree $[Z_{\tilde{v}}:K]$. The restriction $\tilde{v}|Z_{\tilde{v}}$ is an immediate extension of the valuation v of K.

(E) Complete valued fields

Let (K,v) be a valued field where the valuation v has rank 1. For every $\gamma\in\Gamma_v\subseteq\mathbb{R}$, let $N_\gamma=\{x\in K|v(x)>\gamma\}$. The family $\{N_\gamma\}$ is a fundamental system of neighborhoods of 0 for a topology on K, for which the operations of addition, multiplication and inverse (of non-zero elements) are continuous; thus K becomes a topological field.

(E1) The completion $\hat{K}$ of K is again a topological field, the valuation v extends by continuity to a valuation $\hat{v}$ of $\hat{K}$, $A_{\hat{v}}\cap K=A_v$, $P_{\hat{v}}\cap K=P_v$, so K is dense in $\hat{K}$; moreover $\Gamma_{\hat{v}}=\Gamma_v$ and $\hat{K}_{\hat{v}}\cong K_v$ (natural isomorphism), so $(\hat{K},\hat{v})$ is an immediate extension of (K,v).

(K,v) is a *complete valued* field, when the topological field K is complete, that is $\hat{K}=K$, $\hat{v}=v$.

(F) The resultant of polynomials

Let K be a field, let $f=\sum_{i=0}^{m}a_iX^{m-i}$, $g=\sum_{j=0}^{n}b_jx^{n-j}$ (with $m\geq0$, $n\geq0$, a_i, $b_j\in K$ and $a_0\neq0$, $b_0\neq0$).

We exclude the following situations: 1) $f=0$, $\deg(g)=0$; 2) $\deg(f)=0$, $g=0$. If $m>0$, $n>0$ the *resultant of f,g* is the following determinant:

$$R(f,g)=\begin{pmatrix} a_0 & a_1 & \dots & a_m & & \\ & a_0 & a_1 & \dots & a_m & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ b_0 & b_1 & \dots & b_n & & \\ & b_0 & b_1 & \dots & b_n & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}\begin{array}{l} \left.\begin{array}{l} \\ \end{array}\right\} n \text{ rows} \\ \\ \left.\begin{array}{l} \\ \end{array}\right\} m \text{ rows} \\ \\ \end{array}$$

(with entries equal to 0 in all other places).

This definition is completed as follows:

$$R(f,b_0)=b_0^m, \qquad R(a_0,g)=a_0^n.$$

It is clear that $R(g,f)=\pm R(f,g)$. Moreover, if the coefficients of f,g belong to the subring A of K then $R(f,g)\in A$.

If $f=\sum_{i=0}^{m} a_i X^{m-i}$ ($a_i \in K$, $m\geq 0$, $a_0\neq 0$) let $f'=\sum_{i=0}^{m-1}(m-i)\,a_i X^{m-1-i}$ be the derivative of f. If $\deg(f)>0$ we define the *discriminant of f* to be $\operatorname{discr}(f)=R(f,f')$.

To fix our terminology, we recall that the non-zero polynomials $f,g\in K[X]$ are relatively prime when there does not exist a non-constant polynomial in $K[X]$ which divides f and g. In particular, this happens if f or g has degree zero.

(F1) Let $f,g\in K[X]$ be non-zero polynomials. Then the following conditions are equivalent:

a) if f_1, g_1 are non-zero polynomials in $K[X]$ such that $\deg(f_1)<\deg(f)$, $\deg(g_1)<\deg(g)$ then $f_1 g+g_1 f\neq 0$

b) f,g are relatively prime

c) $R(f,g)\neq 0$.

(F2) Let $f\in K[X]$ be a polynomial with non-zero derivative. Then the following conditions are equivalent:

a) there exists $h\in K[X]$, non-constant, such that h^2 divides f

b) $\operatorname{discr}(f)=0$.

The resultant is expressible in terms of the roots as follows:

(F3) If $f=a_0\prod_{i=1}^{m}(X-\alpha_i)\neq 0$, $g=b_0\prod_{j=0}^{n}(X-\beta_j)\neq 0$ (with $m\geq 0$, $n\geq 0$) then

$$R(f,g)=a_0^n b_0^m \prod_{i=1}^{m}\prod_{j=1}^{n}(\alpha_i-\beta_j)$$

$$=a_0^n\prod_{i=1}^{m} g(\alpha_i)=(-1)^{mn} b_0^m \prod_{j=1}^{n} f(\beta_j).$$

(F4) If $f=a_0\prod_{i=1}^{m}(X-\alpha_i)$ and $\deg(f)>0$ then

$$\operatorname{discr}(f)=(-1)^{\frac{m(m-1)}{2}}a_0^{2m-1}\prod_{i<j}(\alpha_i-\alpha_j)^2.$$

(F5) If $f,g\in K[X]$, $\deg(f)=m>0$, $\deg(g)=n>0$ then

$$\operatorname{discr}(fg)=(-1)^{mn}\operatorname{discr}(f)\cdot\operatorname{discr}(g)\cdot[R(f,g)]^2.$$

(F6) If (K,v) is a valued field, if $f,g\in A_v[X]$, if $\bar{f}\neq 0$, $\bar{g}\neq 0$, $\deg(\bar{f})=\deg(f)$, $\deg(\bar{g})=\deg(g)$, then $\overline{R(f,g)}=R(\bar{f},\bar{g})$.

§ 2 The Henselization of a valued field

Definition 1. The valued field (K^H,v^H) is called a *henselization* of the valued field (K,v) when the following conditions are satisfied:

(H1) $K^H|K$ is an algebraic extension, $v^H|K=v$

(H2) if $\tilde{K}|K^H$ is an algebraic extension, then v^H has only one extension to $\tilde{K}$

(H3) if (K',v') is a valued field with properties (H1), (H2) then there exists a K-isomorphism ϱ from K^H into K' such that $v'\circ\varrho=v^H$.

The first theorem tells that the henselization exists, it is unique, and shows how to construct it.

Theorem 1. *Every valued field (K,v) has a henselization (K^H,v^H), which is unique up to a K-isomorphism. Moreover, $K^H|K$ is a separable extension.*

Proof. We begin showing the uniqueness. If (K^H,v^H) and (K',v') are henselizations of (K,v), by (H3) there exist K-isomorphisms ϱ from K^H into K' and ϱ' from K' into K^H such that $v'\circ\varrho=v^H$ and $v^H\circ\varrho'=v'$. Hence $\varrho\circ\varrho'$ is a K-isomorphism from K' into itself. Since $K'|K$ is an algebraic extension then $\varrho\circ\varrho'$ is a K-automorphism of K'. Hence $\varrho(K^H)=K'$ and $v'\circ\varrho=v^H$, showing the uniqueness of the henselization, up to a K-isomorphism.

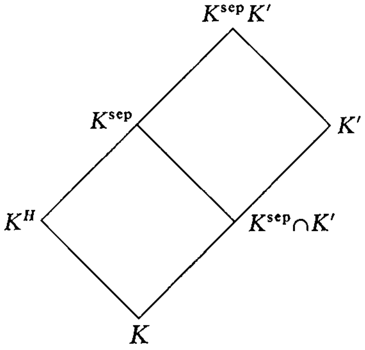
Now we show the existence of the henselization.

Let K^{sep} denote the separable closure of K, hence $K^{\text{sep}}|K$ is a Galois extension. Let $\mathscr{K}=\operatorname{Gal}(K^{\text{sep}}|K)$ be its Galois group. Let $\tilde{v}$ be any extension of v to K^{sep} and $\mathscr{Z}=\mathscr{Z}_{\tilde{v}}=\{\sigma\in\mathscr{K}\,|\,\tilde{v}\circ\sigma=\tilde{v}\}$ the decomposition group of $\tilde{v}$ in $K^{\text{sep}}|K$. Let K^H be the fixed field of $\mathscr{Z}$, v^H the restriction of $\tilde{v}$ to K^H.

We show that (K^H,v^H) is a henselization of (K,v).

Clearly, condition (H1) is satisfied. Let $L|K^H$ be any algebraic extension; we show that v^H has only one extension to L. First we note that by (D10) v^H has only one extension to K^{sep}. A fortiori, v^H has only one extension to $L^{\text{sep}}=L\cap K^{\text{sep}}$ and since $L|L^{\text{sep}}$ is a purely inseparable extension then v^H has also only one extension to L, as follows from (D4).

Now we show condition (H3). If (K', v') is a valued field satisfying conditions (H1) and (H2), let v'^{sep} denote the restriction of v' to $K^{\text{sep}} \cap K'$; since $K'|(K^{\text{sep}} \cap K')$ is a purely inseparable extension, then v' is the only extension of v'^{sep} to K'.



Then v'^{sep} has only one extension to K^{sep}. Indeed, if w_1, w_2 are valuations of K^{sep} extending v'^{sep}, since $K^{\text{sep}}K'|K^{\text{sep}}$ is purely inseparable, then w_1, w_2 have each only one extension to $K^{\text{sep}}K'$, which we denote by $\tilde{w}_1, \tilde{w}_2$; the restrictions of $\tilde{w}_1, \tilde{w}_2$ to K' are equal to v', since they are extensions of v'^{sep}. By hypothesis (H2) on (K', v'), it follows that $\tilde{w}_1 = \tilde{w}_2$ hence $w_1 = w_2$.

Since $w_1|K = v'|K = v$, by (D8) there exists $\varrho \in \mathscr{K}$ such that $\tilde{v} = w_1 \circ \varrho$. Therefore $\varrho \mathscr{Z}_{\tilde{v}} \varrho^{-1} = \mathscr{Z}_{w_1}$ (by (D9)). By (D10) $\operatorname{Gal}(K^{\text{sep}}|K^{\text{sep}} \cap K') \subseteq \mathscr{Z}_{w_1}$, because w_1 is the only extension of v'^{sep} to K^{sep}. Then the decomposition field of w_1 is contained in $K^{\text{sep}} \cap K'$, hence $\varrho(K^H) \subseteq K^{\text{sep}} \cap K' \subseteq K'$ and for every $x \in K^H$ we have

$$v'(\varrho(x)) = v'^{\text{sep}}(\varrho(x)) = w_1(\varrho(x)) = \tilde{v}(x) = v^H(x).$$

This shows that (K^H, v^H) is a henselization and by construction, $K^H|K$ is a separable extension. □

Definition 2. The valued field (K, v) is *henselian* if $K^H = K$.

Theorem 2. *Let (K, v) be a valued field. The following conditions are equivalent:*

(0) *(K, v) is henselian.*

(1) *v has only one extension to every algebraic extension of K*

(1′) *v has only one extension to every separable extension of K.*

Proof. (0)→(1): If (K, v) is henselian, by property (H2) v has only one extension to every algebraic extension of K.

(1)→(0): If the condition (1) is satisfied, by (H3) there exists a K-isomorphism ϱ from K^H to K, such that $v \circ \varrho = v^H$. Hence ϱ is injective then $K^H = K$, ϱ is the identity mapping and $v^H = v$.

(1)↔(1′): The equivalence of these conditions follows from (D4). □

We note the following corollaries:

Corollary 1. *If (K, v) is a henselian valued field, if $\tilde{K}|K$ is an algebraic extension, $\tilde{v}$ the only valuation of $\tilde{K}$ extending v, then the valued field $(\tilde{K}, \tilde{v})$ is henselian.*

Proof. This follows immediately from theorem 2. □

Corollary 2. *The henselization of (K, v) is an immediate extension.*

Proof. Indeed, by theorem 1, K^H is the decomposition field of any extension of v to K^{sep}. By (D10) (K^H, v^H) is an immediate extension of (K, v). □

Corollary 3. *If (K, v) satisfies property* (1) *and $P' \supset P$ are prime ideals of the valuation ring A_v, then $(K_{v_P}, v_{P',P})$ also satisfies property* (1). *In particular, for every prime ideal P of A_v, (K, v_P) satisfies property* (1).

Proof. It suffices to show that if $L|K_{v_P}$ is any finite extension then $v_{P',P}$ has only one extension to L. By (D7) there exists a finite extension $\tilde{K}|K$ and an extension $\tilde{v}_{\tilde{P}}$ of v_P such that $\tilde{K}_{\tilde{v}_{\tilde{P}}} = L$. By theorem 2, the number of extensions of v to $\tilde{K}$ is $\mu_{\tilde{K}|K}(v) = 1$, hence by (D6) $\mu_{\tilde{K}|K}(v_P) = 1$ and also $\mu_{\tilde{K}|K}(v_{P'}) = 1$, hence $\mu_{L|K_{v_P}}(v_{P',P}) = 1$. □

§ 3 The lifting of polynomials

In this section, we shall indicate several characterizations of henselian valued fields, involving the lifting of polynomials from the residue field.

It is convenient to begin proving the following

Lemma 1. *Let (K, v) be a valued field, let $\tilde{K}|K$ be a finite Galois extension and assume that v has $s \geq 2$ extensions $\tilde{v}_1, \ldots, \tilde{v}_s$ to $\tilde{K}$.* Then there exists *$a \in Z_{\tilde{v}_1}$ such that $\tilde{v}_1(a) = 0$, $\tilde{v}_j(a) > 0$, for $j = 2, \ldots, s$.*

Proof. By (D10), if $j \neq 1$ the restriction of $\tilde{v}_j$ to $Z_{\tilde{v}_1}$ is distinct from $\tilde{v}_1 | Z_{\tilde{v}_1}$. These valuations are extensions of v, hence by (D3) they are incomparable. By (B1) there exists $a \in Z_{\tilde{v}_1}$ such that $\tilde{v}_1(a) = 0$, $\tilde{v}_j(a) > 0$ for $j = 2, \ldots, s$. □

We consider the following statements:

(2) If $f \in A_v[X]$ is an irreducible polynomial of degree $n \geq 1$, then $\bar{f}$ is of one of the following types: $\bar{f} \in \bar{K}$ or $\bar{f} = \bar{a}\varphi^s$, where $\bar{a} \in \bar{K}$, $\bar{a} \neq 0$, $\varphi \in \bar{K}[X]$ is an irreducible polynomial, $s \geq 1$ and $s \deg(\varphi) = n$.

(3) If f, g, $h \in A_v[X]$ are such that $\deg(g) > 0$, g is monic, $\bar{g}$, $\bar{h}$ are nonzero relatively prime polynomials of $\bar{K}[X]$ and $\bar{f} = \bar{g}\bar{h}$ then there exist g^*, $h^* \in A_v[X]$ such that $\bar{g}^* = \bar{g}$, $\bar{h}^* = \bar{h}$, g^* is monic and $f = g^* h^*$.

(4) If $f, g, h \in A_v[X]$ are monic polynomials such that $\deg(g) > 0$, $\deg(h) > 0$, with $\bar{g}, \bar{h}$ relatively prime in $\bar{K}[X]$ and $\bar{f} = \bar{g}\bar{h}$ then there exist monic polynomials $g^*, h^* \in A_v[X]$ such that $\bar{g}^* = \bar{g}$, $\bar{h}^* = \bar{h}$ and $f = g^* h^*$.

(5) If $f \in A_v[X]$, $a \in A_v$ and $\bar{f} = (X - \bar{a})\psi$, where $\psi \in \bar{K}[X]$, $\deg(\psi) \neq 0$, $\psi(\bar{a}) \neq 0$, then there exists $a' \in A_v$, such that $\overline{a'} = \bar{a}$ and $f(a') = 0$.

(6) If $f = X^n + a_1 X^{n-1} + a_2 X^{n-2} + \ldots + a_n \in A_v[X]$, $\bar{a}_1 \neq \bar{0}$, $\bar{a}_2 = \ldots = \bar{a}_n = \bar{0}$, then f has a linear factor $X + a'_1$, with $a'_1 \in A_v$, $\overline{a'_1} = \bar{a}_1$.

We show:

Theorem 3. *Let* (K, v) *be a valued field. Then the statements* (1), (2), (3), (4), (5), (6) *are equivalent.*

Proof. (1)→(2)*): Let K^{alg} denote the algebraic closure of K. Let $f = a_0 X^n + a_1 X^{n-1} + \ldots + a_n \in A_v[X]$ be an irreducible polynomial over K, $a_0 \neq 0$. We write

$$f = a_0 \prod_{i=1}^{n} (X - b_i)$$

where each $b_i \in K^{\mathrm{alg}}$ and $b_i \neq 0$, since f is irreducible. By hypothesis, v has only one extension v^* to K^{alg}. We denote by $\overline{K^{\mathrm{alg}}}$ the residue field of K^{alg} with respect to v^*; if $c \in A_{v^*}$ we denote by $\bar{c}$ its image in $\overline{K^{\mathrm{alg}}}$. If $\sigma \in \mathrm{Gal}(K^{\mathrm{alg}} | K)$ then by hypothesis $v^* \circ \sigma = v^*$ so $\sigma(A_{v^*}) = A_{v^*}$, $\sigma(P_{v^*}) = P_{v^*}$, hence σ induces $\bar{\sigma} \in \mathrm{Gal}(\overline{K^{\mathrm{alg}}} | \bar{K})$.

First we assume that $v(a_n) \geq v(a_0)$. Since f is irreducible, the roots b_i are conjugate over K, say $b_i = \sigma(b_1)$, where $\sigma \in \mathrm{Gal}(K^{\mathrm{alg}} | K)$; then $v^*(b_i) = v^*(\sigma(b_1)) = v^*(b_1)$, because $v^* \circ \sigma = v^*$. Therefore from

$$a_0(-1)^n \prod_{i=1}^{n} b_i = a_n \quad \text{it follows that}$$

$$v^*(b_i) = \frac{v(a_n) - v(a_0)}{n} \geq 0.$$

If $v^*(b_i) > 0$ for every $i = 1, \ldots, n$, then from

$$a_j = a_0(-1)^j \sum b_{i_1} b_{i_2} \ldots b_{i_j}$$

it follows that $v(a_j) > v(a_0) \geq 0$ for $j = 1, \ldots, n$, and therefore $\bar{f} = \bar{a}_0 X^n$.

If $v^*(b_i) = 0$ for every $i = 1, \ldots, n$ and $v(a_0) > 0$ then again $v(a_j) \geq v(a_0) > 0$ for $j = 1, \ldots, n$, hence $\bar{f} = \bar{0}$.

If $v^*(b_i) = 0$ for every $i = 1, \ldots, n$ and $v(a_0) = 0$ then we show that $\bar{f} = \bar{a}_0 \varphi^s$ where $\varphi \in \bar{K}[X]$ is irreducible of degree $s \geq 1$ and $s \deg(\varphi) = n$. Otherwise, $\bar{f} = \bar{a}_0 \psi_1 \psi_2$ where $\psi_1, \psi_2 \in \bar{K}[X]$, $\deg(\psi_1) > 0$, $\deg(\psi_2) > 0$ and ψ_1, ψ_2 are relatively prime in $\bar{K}[X]$. Suppose that $\bar{b}_1$ is a root of, say, ψ_1. For every $j \neq 1$ there exists $\sigma \in \mathrm{Gal}(K^{\mathrm{alg}} | K)$ such that $b_j = \sigma(b_1)$, thus $\bar{b}_j = \bar{\sigma}(\bar{b}_1)$, so $\bar{b}_j$ is a conjugate of $\bar{b}_1$ over $\bar{K}$, hence also a root of ψ_1. This implies that $\deg(\bar{f}) \leq \deg(\psi_1) < \deg(\bar{f})$, which is a contradiction.

*) Rayner [7].

Now we assume that $v(a_0)\geq v(a_n)$. Let

$$g(X)=X^n f\left(\frac{1}{X}\right)=a_n X^n+a_{n-1}X^{n-1}+\ldots+a_0,$$

so $g\in A_v[X]$ and it is also irreducible. By the first part of the proof, either $\bar{g}=\bar{a}_n X^n$, or $\bar{g}=\bar{0}$, or $\bar{g}=\bar{a}_n\varphi^s$, where $\bar{a}_n\neq\bar{0}$, $s\geq 1$, $\varphi\in\bar{K}[X]$ is an irreducible polynomial, $s\deg(\varphi)=n$.

If $\bar{g}=\bar{a}_n X^n$ then $\bar{a}_i=0$ for $i=0,1,\ldots,n-1$, hence $\bar{f}=\bar{a}_n$.

If $\bar{g}=\bar{0}$ then $\bar{f}=\bar{0}$. Finally, if $\bar{g}=\bar{a}_n\varphi^s$ then

$$\bar{f}=X^n\bar{g}\left(\frac{1}{X}\right)=\bar{a}_n\left[X^{\frac{n}{s}}\varphi\left(\frac{1}{X}\right)\right]^s=\bar{a}_n\psi^s$$

where $\psi(X)=X^{\frac{n}{s}}\varphi\left(\frac{1}{X}\right)$ is irreducible and $s\deg(\psi)=n$.

(2)→(3)[*]: Let f, g, h satisfy the hypotheses of condition (3). It follows that $\bar{f}\neq 0$, $\deg(f)\geq\deg(\bar{f})\geq\deg(\bar{g})=\deg(g)$. Let $f_1,\ldots,f_p$ be the irreducible factors of f in $K[X]$; by (C3) we may assume, $f_i\in A_v[X]$ (for each $i=1,\ldots,p$). By (2), $\bar{f}_i\in\bar{K}$ or $\bar{f}_i=\bar{a}_i\varphi_i^{s_i}$ where φ_i is an irreducible polynomial in $K[X]$, $s_i\geq 1$, $s_i\deg(\varphi_i)=\deg(f_i)$, and $\bar{a}_i\in\bar{K}$, $\bar{a}_i\neq 0$. Thus if $\bar{f}_i\notin\bar{K}$ then $\deg(\bar{f}_i)=\deg(f_i)$ so the leading coefficient of f_i is a unit of A_v. From $\bar{g}\bar{h}=\bar{f}=\bar{f}_1\bar{f}_2\ldots\bar{f}_p$, if $\deg(\bar{f}_i)\neq 0$ then $\bar{f}_i$ divides exactly one of the polynomials $\bar{g}$, $\bar{h}$, since they are relatively prime. Let $I=\{i\,|\,1\leq i\leq p,\ \bar{f}_i\notin\bar{K},\ \bar{f}_i$ divides $\bar{g}\}$. Then $\bar{g}=\overline{c^{-1}}\prod_{i\in I}\bar{f}_i$, where $c\in A_v$ is the product of the leading coefficients of f_i (for all $i\in I$). Let $g^*=c^{-1}\prod_{i\in I}f_i$, and let $h^*=c\prod_{j\notin I}f_j$. Then g^*, $h^*\in A_v[X]$, $f=g^*h^*$, g^* is monic, $\bar{g}^*=\bar{g}$, $\bar{h}^*=h$.

(3)→(4): This is trivial.

(4)→(5): By hypothesis $f\equiv X^{n-1}(X+a_1)(\bmod P_v[X])$. Hence by condition (4) there exists $a_1'\in A_v$ such that $X+a_1'$ divides f in $A_v[X]$, and $\overline{a_1'}=\overline{a_1}$.

(5)→(6): This is trivial.

(6)→(1')[**]: We assume that v has more than one extension to some separable extension $\tilde{K}|K$.

We may also assume that $\tilde{K}|K$ is a finite Galois extension; let $\mathscr{K}$ denote its Galois group, let $\tilde{v}_1,\ldots,\tilde{v}_s$ ($s\geq 2$) be the extensions of v to $\tilde{K}$, Z the decomposition field of $\tilde{v}_1$ in $\tilde{K}|K$. By lemma 1, there exists $a\in Z$ such that $\tilde{v}_1(a)=0$, $\tilde{v}_j(a)>0$ for every $j=2,\ldots,s$. Thus $a\notin K$ and if $\sigma\in\mathscr{K}$, $\sigma(a)\neq a$ then $\tilde{v}_1(\sigma(a))=\tilde{v}_j(a)>0$ for some $j\geq 2$. Hence $\max\{\tilde{v}_1(\sigma(a)-a)|\sigma(a)\neq a\}=0$, therefore the minimal polynomial of a

[*] Rayner [7].

[**] Nagata [5].

over K is of the form $f=X^n+a_1X^{n-1}+\ldots+a_n\in A_v[X]$, with $a_1\equiv a(\mathrm{mod}\,P_{\tilde{v}_1})$, $a_i\in P_{\tilde{v}_1}$ for $i=2,\ldots,s$. This contradicts the hypothesis (6). □

§ 4 The characterization of Krasner

Now we consider Krasner's condition:

(7) If v^s is any extension of v to K^{sep}, if $x,y\in K^{\mathrm{sep}}$ and $v^s(y-x)>v^s(\sigma(x)-x)$ for every $\sigma\in\mathrm{Gal}(K^{\mathrm{sep}}|K)$ such that $\sigma(x)\neq x$, then $K(x)\subseteq K(y)$.

We show:

Theorem 4. *If* (K,v) *is a valued field then conditions* (1′) *and* (7) *are equivalent.*

Proof. (1′)→(7)[*]: We may assume that $x\notin K$. In order to show that $x\in K(y)$ it suffices to prove that if σ is any $K(y)$-automorphism of K^{sep} then $\sigma(x)=x$; therefore

$$\mathrm{Gal}(K^{\mathrm{sep}}|K(y))\subseteq\mathrm{Gal}(K^{\mathrm{sep}}|K(x))$$

hence $K(x)\subseteq K(y)$. By (1′) we have $v^s\circ\sigma=v^s$. Suppose, on the contrary, that there exists $\tau\in\mathrm{Gal}(K^{\mathrm{sep}}|K(y))$ such that $\tau(x)\neq x$.

From $\tau(x-y)=\tau(x)-y$ we have

$$\begin{aligned} v^s(\tau(x)-y)&=(v^s\circ\tau)(x-y)=v^s(x-y)>\alpha\\ &=\max\{v^s(\sigma(x)-x)|\sigma\in\mathrm{Gal}(K^{\mathrm{sep}}|K)\text{ with }\sigma(x)\neq x\}.\end{aligned}$$

Thus $v^s(\tau(x)-x)\geq\min\{v^s(\tau(x)-y),\ v^s(y-x)\}>\alpha$ hence $\tau(x)=x$ which is a contradiction, concluding the proof.

(7)→(1′): We proceed as in the proof of the implication (6)→(1′). We assume that v has more than one extension to some separable extension $\tilde{K}|K$; we may also assume that $\tilde{K}|K$ is a finite Galois extension. Let $\mathscr{K}$ denote its Galois group, let $\tilde{v}_1,\ldots,\tilde{v}_s$ $(s\geq 2)$ be the extensions of v to $\tilde{K}$, Z the decomposition field of $\tilde{v}_1$ in $\tilde{K}|K$. By lemma 1 there exists $a\in Z$ such that $\tilde{v}_1(a)=0$, $\tilde{v}_j(a)>0$ for every $j=2,\ldots,s$. Thus $a\notin K$ and if $\sigma\in\mathscr{K}$, $\sigma(a)\neq a$ then $\tilde{v}_1(\sigma(a))=\tilde{v}_j(a)>0$ for some $j\geq 2$. Hence $\max\{\tilde{v}_1(\sigma(a)-a)|\sigma(a)\neq a\}=0$. On the other hand, by (D10), $(Z,\tilde{v}_1|Z)$ is an immediate extension of (K,v), so there exists $b\in A_v$ such that $\bar{b}=\bar{a}$, that is $\tilde{v}_1(b-a)>0$. By the hypothesis (7) $K(a)\subseteq K(b)=K$, which is absurd. □

§ 5 The strong form of Hensel's condition and Newton's lemma

In order to consider the so-called strong form of Hensel's lemma we need to establish some preliminary results concerning the resultant and the discriminant of polynomials in $A_v[X]$.

[*] Krasner [3].

Lemma 2. *Let $f, g \in A_v[X]$ be non-zero polynomials, with* $\max\{\deg(f), \deg(g)\} \geq 1$, *which are relatively prime (so $R=R(f,g) \neq 0$, by* (F1)*). If $h \in A_v[X]$, $h \neq 0$, $v(h) \geq v(R)$ and* $\deg(h) < \deg(f) + \deg(g)$ *then h may be written in unique way as $h=g_1 f + f_1 g$, with f_1, $g_1 \in A_v[X]$, $\deg(f_1) < \deg(f)$, $\deg(g_1) < \deg(g)$, $v(f_1) \geq v(h)-v(R)$, $v(g_1) \geq v(h)-v(R)$ (with the convention that the degree of the zero polynomial is $-\infty$).*

Proof. Let $f=\sum_{i=0}^{m} a_i X^{m-i}$, $g=\sum_{j=0}^{n} b_j X^{n-j}$, with $a_i, b_j \in A_v$, $a_0 \neq 0$, $b_0 \neq 0$, $\max\{m,n\} \geq 1$. If, for example, $m \geq 1$, $n=0$ then $R(f,g)=b_0^m$, $v(h) \geq m v(b_0)$ and so $h=b_0 f_1$ with $f_1 \in A_v[X]$; in this case, we take $g_1=0$.

Let $m \geq 1$, $n \geq 1$ and $h=\sum_{i=1}^{m+n} e_i X^{m+n-i} \in A_v[X]$. We wish to determine $f_1 = \sum_{i=0}^{m-1} c_i X^{m-1-i} \in A_v[X]$, $g_1=\sum_{j=0}^{n-1} d_j X^{n-1-j} \in A_v[X]$ such that $h=g_1 f + f_1 g$.

Comparing the coefficients, we have a linear system of $m+n$ linear equations in the $m+n$ unknowns c_i, d_j, having determinant equal to $R(f,g)$, up to sign. By hypothesis $R(f,g) \neq 0$ so the system has a unique solution which is not trivial.

The coefficients c_i, d_j may be computed by Cramer's rule. The numerators are linear forms in the coefficients e_i, with coefficients in A_v (because $f, g \in A_v[X]$) and the denominator is equal to $R=R(f,g)$. From $v(e_i) \geq v(h) \geq v(R)$ then $v(c_i) \geq 0$, $v(d_j) \geq 0$ for all c_i, d_j. So $f_1, g_1 \in A_v[X]$ and $v(f_1) \geq v(h)-v(R)$, $v(g_1) \geq v(h)-v(R)$. □

Lemma 3. *If $f, g, f_1, g_1 \in A_v[X]$ are non-zero polynomials and* $\max\{\deg(f), \deg(g)\} \geq 1$, $\max\{\deg(f_1), \deg(g_1)\} \geq 1$ *then*

$$v(R(f_1, g_1) - R(f,g)) \geq \min\{v(f_1 - f), v(g_1 - g)\}.$$

Proof. Let $a \in A_v$ be such that $v(a)=\min\{v(f_1-f), v(g_1-g)\}$. Then $f_1=f+ah$, $g_1=g+ak$ where $h, k \in A_v[X]$. Thus $R(f_1, g_1)=R(f+ah, g+ak)=R(f,g)+ad$, where $d \in A_v$ is a sum of products of elements equal to a or to coefficients of f, g, h, k. Thus $v(R(f_1, g_1)-R(f,g)) \geq v(a)$. □

Lemma 4. *If f, $f_1 \in A_v[X]$ and* $\deg(f)>0$, $\deg(f_1)>0$ *then* $v(\operatorname{discr}(f)-\operatorname{discr}(f_1)) \geq v(f-f_1)$.

Proof. It suffices to note that if $g \in A_v[X]$ then $v(g') \geq v(g)$. In particular $v(f'-f_1') \geq v(f-f_1)$ hence, by lemma 3, $v(\operatorname{discr}(f)-\operatorname{discr}(f_1)) \geq v(f-f_1)$. □

Now we consider the following Hensel's strong condition (also attributed to Rychlik):

(8) Let $f, g, h \in A_v[X]$ be non-zero polynomials such that:

i) $\deg(g)>0$, $\deg(f)=\deg(g)+\deg(h)$, g is monic, f is primitive and f, h have the same leading coefficient,

ii) $v(R(g,h))=\varrho<\infty$,
iii) $v(f-gh)=\alpha\gg 2\varrho$.[*]

Then there exist polynomials $g^*, h^*\in A_v[X]$ such that:

a) $v(g^*-g)>\varrho$, $v(h^*-h)>\varrho$
b) $\deg(g^*)=\deg(g)$, $\deg(h^*)=\deg(h)$, g^* is monic
c) $f=g^*h^*$.

In order to show that condition (8) follows from (1′), we first establish some facts for the special case when v has rank 1.

Theorem 5. *If* (K,v) *is a complete valued field, when the valuation* v *has rank* 1, *then it satisfies* (8).

Proof[**]. Let f, g, $h\in A_v[X]$ be such that $\deg(g)=m>0$, $\deg(h)=n\geq 0$, $\deg(f)=m+n$, g is monic, f is primitive and f,h have the same leading coefficient $v(R(g,h))=\varrho<\infty$ and $v(f-gh)=\alpha>2\varrho$. If $f=gh$, we take $g^*=g$, $h^*=h$, so we may assume $f\neq gh$.

Let $g_0=g$, $h_0=h$ and note that $\deg(f-gh)<\deg(f)$. We let $j\geq 0$ and we assume already defined non-zero polynomials g_j, $h_j\in A_v[X]$ such that $\deg(g_j)=m$, $\deg(h_j)=n$, g_j is monic, f, h_j have the same leading coefficient, $f=g_jh_j$ or $\deg(f-g_jh_j)<\deg(f)$, $v(g_j-g)>\varrho$, $v(h_j-h)>\varrho$, $v(R(g_j,h_j))=\varrho<\infty$ and $v(f-g_jh_j)\geq\alpha+j(\alpha-2\varrho)>\varrho$.

If $f=g_jh_j$ we take $g^*=g_j$, $h^*=h_j$ and the required conditions are satisfied.

Let $f\neq g_jh_j$ then $\deg(f-g_jh_j)<\deg(f)=\deg(g_j)+\deg(h_j)$. Since $R(g_j,h_j)\neq 0$ then g_j, h_j are relatively prime. By lemma 2, $f-g_jh_j$ may be written uniquely in the form $f-g_jh_j=h_j^*g_j+g_j^*h_j$ with h_j^*, $g_j^*\in A_v[X]$, $\deg(g_j^*)<m$, $\deg(h_j^*)<n$,

$$v(g_j^*)\geq v(f-g_jh_j)-\varrho\geq\alpha+j(\alpha-2\varrho)-\varrho>\varrho \quad\text{and}$$
$$v(h_j^*)\geq v(f-g_jh_j)-\varrho\geq\alpha+j(\alpha-2\varrho)-\varrho>\varrho.$$

Let $g_{j+1}=g_j+g_j^*$ and $h_{j+1}=h_j+h_j^*$ so g_{j+1}, $h_{j+1}\in A_v[X]$, g_{j+1}, h_{j+1} are not equal to 0, $\deg(g_{j+1})=m$, $\deg(h_{j+1})=n$, g_{j+1} is monic, f,h_{j+1} have the same leading coefficient, $f=g_{j+1}h_{j+1}$ or $\deg(f-g_{j+1}h_{j+1})<\deg(f)$,

$$v(g_{j+1}-g)=v(g_j-g+g_j^*)>\varrho,$$
$$v(h_{j+1}-h)=v(h_j-h+h_j^*)>\varrho,$$
$$v(R(g_{j+1},h_{j+1}))=v(R(g_j,h_j))=\varrho$$

because

[*] If α, $\beta\in\Gamma_v$, $\alpha\geq 0$, $\beta\geq 0$, we write $\alpha\gg 0$ when $\alpha>0$ and $\alpha\gg\beta>0$ when $\alpha>\beta$ and $\alpha-\beta\notin\Delta_\beta$ (the largest isolated subgroup of Γ_v not containing β). Thus if Γ_v is archimedean then $\alpha\gg\beta$ is equivalent to $\alpha>\beta$.

[**] The proofs is similar to that of the classical Hensel's lemma: if (K,v) is complete, and the value group of v is $\mathbb{Z}$, then it satisfies condition (4).

$$v(R(g_{j+1},h_{j+1})-R(g_j,h_j))\geq\min\{v(g_j^*),v(h_j^*)\}\geq\alpha+j(\alpha-2\varrho)-\varrho>\varrho$$

since $\alpha>2\varrho$. Finally

$$\begin{aligned}v(f-g_{j+1}h_{j+1})&=v(f-g_jh_j-g_j^*h_j-h_j^*g_j-g_j^*h_j^*)\\&=v(g_j^*h_j^*)\geq 2\alpha+2j(\alpha-2\varrho)-2\varrho\geq\alpha+(j+1)(\alpha-2\varrho)\end{aligned}$$

since $\alpha>2\varrho$.

Thus either there exists $j\geq 0$ such that $f=g_jh_j$ and the proof is concluded, or there exist infinite sequences $(g_j)_{j\geq 0}$, $(h_j)_{j\geq 0}$ of polynomials of degrees m, n respectively. We have $\lim\limits_{j\to\infty}v(g_{j+1}-g_j)=\lim\limits_{j\to\infty}v(g_j^*)=\infty$ and similarly $\lim\limits_{j\to\infty}v(h_{j+1}-h_j)=\infty$, hence these are Cauchy sequences of polynomials. Since (K,v) is complete, there exist polynomials g^*, $h^*\in A_v[X]$ with $\deg(g^*)=m$, $\deg(h^*)=n$, g^* is monic, f and h^* have the same leading coefficient,

$$v(g^*-g)=\lim_{j\to\infty}v(g_j-g)>\varrho,\quad v(h^*-h)=\lim_{j\to\infty}v(h_j-h)>\varrho,\quad\text{and}$$

$$v(f-g^*h^*)=\lim_{j\to\infty}v(f-g_jh_j)=\infty$$

so $f=g^*h^*$. □

If v has rank 1, let $(\hat{K},\hat{v})$ be the completion of the valued field. Ostrowski considered the following property:

$(\mathcal{O})$ K is separably closed in its completion $\hat{K}$ (when v has rank 1).

He showed:

Theorem 6. *If v has rank 1 then (7) implies $(\mathcal{O})$.*

Proof. Let $x\in\hat{K}\cap K^{\text{sep}}$ and let $x=x_1, x_2,\ldots,x_n$ be the conjugates of x over K (so they are distinct and each $x_i\in K^{\text{sep}}$); let v^s be an extension of v to K^{sep} and $\alpha=\max\{v^s(x_i-x)\mid i\neq 1\}$. Since K is topologically dense in $\hat{K}$, there exists $a\in K$ such that $v^s(a-x)>\alpha$. Hence by (7), we have $K(x)\subseteq K(a)=K$, so $x\in K$. □

For the next theorem, we need first to establish two lemmas from the theory of fields.

Lemma 5. *Let $\tilde{K}|K$ be an algebraic extension let $f\in\tilde{K}[X]$. Then the following statements are equivalent:*

a) *the coefficients of f are separable over K*
b) *every root x of f has multiplicity which is divisible by the inseparability degree of $K(x)|K$.*

Proof. We may assume $\operatorname{char}(K)=p\neq 0$.

Let K' be the subfield of $\tilde{K}$, obtained by adjoining to K all the coefficients of f. So $f\in K'[X]$.

(a)→(b): By hypothesis $K'|K$ is separable.

First we assume that f is irreducible in $K'[X]$. The multiplicity of x is p^e, where $e \geq 0$ is the largest integer such that $f \in K'[X^{p^e}]$. Since f is irreducible then $p^e = [K'(x) : K']_{\text{ins}}$ (inseparability degree of $K'(x) \mid K'$). Then

$$\begin{aligned} [K'(x) : K]_{\text{ins}} &= [K'(x) : K(x)]_{\text{ins}} \times [K(x) : K]_{\text{ins}} \\ &= [K'(x) : K']_{\text{ins}} \times [K' : K]_{\text{ins}}. \end{aligned}$$

But $K' \mid K$ is separable, so is $K'(x) \mid K(x)$, hence $p^e = [K(x) : K]_{\text{ins}}$.

If f is arbitrary, let $f = f_1^{s_1} \dots f_k^{s_k}$ where each f_i is irreducible in $K'[X]$. $f_1, \dots, f_k$ are distinct and each $s_i \geq 1$. If x is a root of f, there exists a unique j, $1 \leq j \leq k$, such that $f_j(x) = 0$. Then the multiplicity of x as a root of f_i is $[K(x) : K]_{\text{ins}}$, hence as a root of f it is equal to $s_j[K(x) : K]_{\text{ins}}$.

(b)→(a): Let f be irreducible in $K'[X]$, let p^e be the multiplicity of the roots x_j of f. Let $p^{e_j} = [K(x_j) : K]_{\text{ins}}$, so by hypothesis p^{e_j} divides p^e. Thus $x_j^{p^e} = (x_j^{p^{e_j}})^{p^{e - e_j}}$ is separable over K. Since

$$f = \prod (X - x_j)^{p^e} = \prod (X^{p^e} - x_j^{p^e})$$

then its coefficients are separable over K.

If $f = f_1^{s_1} \dots f_k^{s_k}$, with each f_i is irreducible in $K'[X]$, $f_1, \dots, f_k$ are distinct, and each $s_i \geq 1$, then the coefficients of each f_i are separable over K, hence the same is true for the coefficients of f. □

Lemma 6. *Let $\tilde{K} \mid K$ be any extension, let $f \in K[X]$, $g, h \in \tilde{K}[X]$ and $f = gh$. If g, h have no common root (in any field containing $\tilde{K}$) then the coefficients of g, h are algebraic separable over K.*

Proof. We first show that the coefficients of g, h are algebraic over K. Let K^* be any algebraically closed field containing $\tilde{K}$. We write $gh = f = \prod_{i=1}^{k} (X - x_i)^{e_i}$, $e_i \geq 1$, where $x_1, \dots, x_k$ are the distinct roots of f in K^*. Each x_i is algebraic over K, and g, h are products of factors of the type $X - x_i$. So each coefficient of g, h is algebraic over K.

So $g, h \in K'[X]$ where K' is the subfield of $\tilde{K}$ consisting of the elements algebraic over K. Since f has coefficients in K, by lemma 5, every root x of f has multiplicity divisible by $[K(x) : K]_{\text{ins}}$. Since $f = gh$ and g, h have no common root, every root x of g (or of h) has the same multiplicity when considered as a root of f, hence it has multiplicity divisible by $[K(x) : K]_{\text{ins}}$. Again by lemma 5 the coefficients of g (and of h) are separable over K. □

Theorem 7. *If v has rank 1 and (K, v) satisfies condition $(\mathcal{O})$ then it satisfies condition* (8).

Proof. Let $f, g, h \in A_v[X]$ satisfy (i), (ii) and (iii) of condition (8). By theorem 5, the completion $(\hat{K}, \hat{v})$ of (K, v) satisfies condition (8), hence there exist non-zero polynomials $g^*, h^* \in A_{\hat{v}}[X]$ such that the corresponding properties (a), (b), (c) are satisfied: $\hat{v}(g^*-g)>\varrho$, $\hat{v}(h^*-h)>\varrho$, $\deg(g^*)=\deg(g)$, $\deg(h^*)=\deg(h)$, g^* is monic and $f=g^*h^*$. It suffices to show that $g^*, h^* \in A_v[X]$.

By lemma 3,

$$\hat{v}(R(g^*,h^*)-R(g,h)) \geq \min\{v(g^*-g), v(h^*-h)\} > \varrho.$$

Since $v(R(g,h))=\varrho$ then $\hat{v}(R(g^*,h^*))=\varrho$ so $R(g^*,h^*)\neq 0$, and therefore g^*, h^* have no common root (in any field containing $\hat{K}$). By lemma 6, the coefficients of g^*, h^* are algebraic separable over K, so they belong to $K^{\text{sep}} \cap \hat{K}$. By hypothesis $(\mathcal{O})$, $K^{\text{sep}} \cap \hat{K}=K$, so $g^*, h^* \in K[X]$, hence $g^*, h^* \in (A_{\hat{v}} \cap K)[X]=A_v[X]$. □

The following theorem holds for valuations of arbitrary rank:

Theorem 8. *If* (K, v) *satisfies* (1′) *then it satisfies condition* (8).

Proof*). If v has rank 1, by theorems 4, 6 and 7, the condition (8) follows from (1′).
Now we assume that v has arbitrary rank. Let $f, g, h \in A_v[X]$ be non-zero polynomials such that $\deg(g)=m>0$, $\deg(h)=n \geq 0$, $\deg(f)=m+n$, g is monic, f is primitive and f, h have the same leading coefficient c. Let $R=R(f,g) \in A_v$ and $v(R)=\varrho<\infty$, in particular $R \neq 0$. We assume also that $v(f-gh)=\alpha \gg 2\varrho$.

If $f=gh$ it is trivial, so we may assume $f \neq gh$.

First Case. cR is a unit of A_v.

Let $\bar{K}=A_v/P_v$ be the residue field of (K, v). By theorem 3 (K, v) satisfies condition (3). Let $\bar{f}, \bar{g}, \bar{h} \in \bar{K}[X]$ be the canonical images of f, g, h; since $\bar{c} \neq 0$ then $\bar{f}, \bar{g}, \bar{h}$ are non-zero polynomials, $R(\bar{g}, \bar{h})=\overline{R(g,h)}=\bar{R}$ and $R \notin P_v$ hence $\bar{R} \neq \bar{0}$; so $\bar{g}, \bar{h}$ are relatively prime polynomials. Moreover $v(f-gh)>0$ so $\bar{f}=\bar{g}\bar{h}$. Thus by (3) there exist polynomials $g^*, h^* \in A_v[X]$ such that $\overline{g^*}=\bar{g}$, $\bar{h}^*=\bar{h}$, g^* is monic and $f=g^*h^*$. Hence $v(g^*-g)>0=\varrho$, $v(h^*-h)>0=\varrho$, $\deg(g^*)=\deg(g)$, and $\deg(h^*)=\deg(h)$.

Second Case. cR is not a unit of A_v.

In this case $cR \in P_v$. Let P_1 be the smallest prime ideal of A_v such that $cR \in P_1$; let P_2 be the largest prime ideal of $A=A_v$ such that $cR \notin P_2$, thus $P_2 \subset AcR \subseteq P_1$. Let Δ_1, Δ_2 be the isolated subgroups of Γ_v corresponding to P_1, P_2 respectively. Let $\tilde{K}=A_{P_2}/P_2$, $\tilde{A}=A_{P_1}/P_2$, so $\tilde{A}$ is the ring of the valuation $\tilde{v}=v_{P_1,P_2}$, which has maximal ideal $\tilde{P}=P_1/P_2$ and rank 1 with value group isomorphic to Δ_2/Δ_1 (see § 1, (A9)). By corollary 3 to theorem 2, $(\tilde{K}, \tilde{v})$ satisfies (1′) and since $\tilde{v}$ has rank 1, then it satisfies (8). Let $\tilde{f}$, $\tilde{g}$, $\tilde{h} \in \tilde{K}[X]$ be the canonical images of f, g, h by the homomorphism extending $A_{P_2} \to A_{P_2}/P_2=\tilde{K}$. Thus $\tilde{f}$, $\tilde{g}$, $\tilde{h} \in \tilde{A}[X]$, $\tilde{g}$ is monic, $\deg(\tilde{g})=m$. Since $c \notin P_2$, then $\tilde{f} \neq 0$, $h \neq 0$, both have leading coefficient $\tilde{c}$ (image of c in $\tilde{K}$), $\deg(\tilde{h})=n$, $\deg(\tilde{f})=m+n$. Since f is primitive then $f \notin P_1[X]$ so $\tilde{f} \notin \tilde{P}[X]$, that is $\tilde{f}$ is primitive.

*) Nagata [5].

Let $\tilde{R}=R(\tilde{g},\tilde{h})$ so $\tilde{R}$ is the image of R in $\tilde{K}$; from $R\notin P_2$ it follows that $\tilde{R}\neq 0$ and $\tilde{v}(\tilde{R})=\tilde{\varrho}$, where $\tilde{\varrho}=\varrho+\Delta_1\in\Delta_2/\Delta_1$. Similarly $\tilde{v}(\tilde{f}-\tilde{g}\tilde{h})=\tilde{\alpha}=\alpha+\Delta_1$ (it is not excluded that $f-gh\in P_2$ so $\tilde{\alpha}$ may be infinite).

By hypothesis $\tilde{\alpha}>2\tilde{\varrho}$ since $\alpha>2\varrho+\delta$ for every $\delta\in\Delta_1$.

By (8) there exist non-zero polynomials $g_1, h_1\in A_{P_1}[X], g_1$ monic, $\deg(g_1)=m$, $\tilde{v}(\tilde{g}_1-\tilde{g})>\tilde{\varrho}$, $\tilde{v}(\tilde{h}_1-\tilde{h})>\tilde{\varrho}$, $\tilde{f}=\tilde{g}_1\tilde{h}_1$. Then the leading coefficient of $\tilde{h}_1$ is $\tilde{c}$, and $\deg(\tilde{h}_1)=\deg(\tilde{h})=n$.

By corollary 3 to theorem 2 (K, v_{P_2}) satisfies (1′), hence by theorem 3, it satisfies also (3). We show that $\tilde{g}_1, \tilde{h}_1\in\tilde{K}[X]$ are relatively prime polynomials. Indeed, by lemma 3

$$\hat{v}(R(\tilde{g}_1,\tilde{h}_1)-R(\tilde{g},\tilde{h}))\geq\min\{\tilde{v}(\tilde{g}_1-\tilde{g}),\tilde{v}(\tilde{h}_1-\tilde{h})\}>\varrho;$$

since $\tilde{v}(R(\tilde{g},\tilde{h}))=\tilde{\varrho}$ then $\tilde{v}(R(\tilde{g}_1,\tilde{h}_1))=\tilde{\varrho}$ and in particular $R(\tilde{g}_1,\tilde{h}_1)\neq 0$. Applying (3), there exist polynomials $g^*, h^*\in A_{P_2}[X]$ such that $\tilde{g}^*=\tilde{g}_1$, $\tilde{h}^*=\tilde{h}_1$, g^* is monic and $f=g^*h^*$. So $\deg(g^*)=m$, $\deg(h^*)=n$. We have also $v_{P_2}(g^*-g_1)>0$ so $v(g^*-g_1)>\delta$ for every $\delta\in\Delta_2$; in particular since $R\notin P_2$ then $\varrho\in\Delta_2$ thus $v(g^*-g_1)>\varrho$; but $v(g_1-g)>\varrho+\delta'$ for every $\delta'\in\Delta_1$, thus

$$v(g^*-g)\geq\min\{v(g^*-g_1), v(g_1-g)\}>\varrho.$$

Similarly $v(h^*-h)>\varrho$. Finally, the above inequalities imply that $g^*-g_1\in P_2[X]$ (since P_2 is the maximal ideal of the valuation ring of v_{P_2}) and $g_1-g\in P_1[X]$ (since P_1 is the maximal ideal of the valuation ring of v_{P_1}) so $g^*-g\in P_1[X]\subseteq A_v[X]$ hence also $g^*\in A_v[X]$; similarly $h^*\in A_v[X]$, and this concludes the proof. □

Now we consider the following modified form of Hensel's strong condition, which involves the discriminant:

(9) Let f, g, $h\in A_v[X]$ be non-zero polynomials such that:

(i) $\deg(g)>0$, $\deg(f)=\deg(g)+\deg(h)$, g is monic, f, h have the same leading coefficient, f is primitive
(ii) $\mathrm{discr}(f)\neq 0$,
(iii) $v(f-gh)\gg v(\mathrm{discr}(f))$.

Then there exist polynomials g^*, $h^*\in A_v[X]$ such that:

a) $\overline{g^*}=\bar{g}$, $\overline{h^*}=\bar{h}$
b) $\deg(g^*)=\deg(g)$, $\deg(h^*)=\deg(h)$, g^* is monic
c) $f=g^*h^*$.

Theorem 9. *If* (K, v) *satisfies condition* (8) *then it satisfies condition* (9).

Proof. As indicated in § 1, (F 5)

$$\mathrm{discr}(gh)=\pm\mathrm{discr}(g)\,\mathrm{discr}(h)\,[R(g,h)]^2.$$

By lemma 4,

$$v(\operatorname{discr}(f) \mp \operatorname{discr}(g) \operatorname{discr}(h) \cdot [R(g,h)]^2)$$
$$= v(\operatorname{discr}(f) - \operatorname{discr}(gh)) \geq v(f-gh) > v(\operatorname{discr}(f)),$$

then

$$v(\operatorname{discr}(g) \operatorname{discr}(h) \cdot [R(g,h)]^2) = v(\operatorname{discr}(f))$$

hence $2v(R(g,h)) \leq v(\operatorname{discr}(f)) \ll v(f-gh)$, showing in particular that $v(R(g,h)) < \infty$. By (8), there exist polynomials g^*, $h^* \in A_v[X]$ such that the conditions (a), (b), (c) of (8) hold. In particular, $v(g^*-g)>0$, $v(h^*-h)>0$ then $\overline{g^*} = \bar{g}$, $\overline{h^*} = \bar{h}$. □

Now we consider the following special condition, which in essence, goes back to Newton:

(10) Let $f \in A_v[X]$, with $\deg(f)>0$ and assume f primitive.

Let $a \in A_v$ be such that $v(f(a)) \gg v(\operatorname{discr}(f))$. Then there exists $a' \in A_v$ such that $\overline{a'} = \bar{a}$ and $f(a')=0$.

Theorem 10. *If* (K, v) *satisfies condition* (9) *then it satisfies condition* (10).

Proof. We assume that the hypothesis of (10) is satisfied by $f \in A_v[X]$ and $a \in A_v$.

If $\deg(f)=1$, $f=cX+b$, with $b, c \in A_v$, $f'=c \neq 0$, $\operatorname{discr}(f)=c$. Let $a \in A_v$ be such that $v(ca+b) \gg v(c)$, then

$$v(b) = v(ca+b-ca) \geq \min\{v(ca+b), v(ca)\} \geq v(c).$$

Let $a' = -\dfrac{b}{c} \in A_v$ then $f(a')=0$ and $v(a-a') = v\left(a+\dfrac{b}{c}\right) > 0$, so $\overline{a'} = \bar{a}$.

Now let $\deg(f)>1$ and we write $f-f(a)=(X-a)h$ with $h \in K[X]$. Since $v(h) = v(h)+v(X-a) = v(f-f(a)) \geq 0$ then $h \in A_v[X]$. So the polynomials f, $X-a$, h satisfy the hypothesis of (9). We take $a'=a$ if $f(a)=0$. More generally, by (9) there exists $g^* = X-a'$, with $a' \in A_v$, such that $\overline{a'} = \bar{a}$ and $f(a')=0$. □

The next condition is similar and very useful in the practical determination of roots.

(11) Let $f \in A_v[X]$, with $\deg(f)>0$. Let $a \in A_v$ be such that $f'(a) \neq 0$ and $v(f(a)) > 2v(f'(a))$. Then there exists $a' \in A_v$ such that $\overline{a'} = \bar{a}$ and $f(a')=0$.

Theorem 11. *If* (K, v) *satisfies condition* (10) *then it satisfies condition* (11).

*Proof**). Let $f \in A_v[X]$, $\deg(f)=n>0$, $a \in A_v$ satisfying the hypothesis of (11), let $d = \dfrac{f(a)}{(f'(a))^2}$ so $v(d)>0$. We have

$$f(a+X) = d(f'(a))^2 + f'(a)X + \sum_{i=2}^{n} b_i X^i$$

*) van den Dries [12].

where each $b_i \in A_v$. Replacing X by $df'(a)\,Y$ we obtain

$$f(a+df'(a)\,Y)$$
$$=d(f'(a))^2\left[1+Y+d\sum_{i=2}^{n} b_i d^{i-2}(f'(a))^{i-2}\,Y^i\right].$$

Let

$$g=1+Y+d\sum_{i=2}^{n} b_i d^{i-2}(f'(a))^{i-2}\,Y^i \in A_v[Y].$$

By lemma 4 $v(\mathrm{discr}(g)-\mathrm{discr}(1+Y)) \geq v(g-1-Y) \geq v(d) > 0$ and since $\mathrm{discr}(1+Y) = 1$ then $v(\mathrm{discr}(g))=0$. On the other hand, $v(g(-1)) \geq v(d) > 0 = v(\mathrm{discr}(g))$. By (10) there exists $y \in A_v$ such that $\bar{y} = -\bar{1}$ and $g(y)=0$. Let $a'=a+df'(a)\,y$. Then $f(a')=0$ and $v(a'-a) \geq v(d) > 0$, concluding the proof. □

Theorem 12. *If* (K, v) *satisfies condition* (11) *then it satisfies condition* (6), *hence the conditions* (8), (9), (10) *and* (11) *are equivalent to each other and hold if and only if* (K, v) *is a henselian field.*

Proof. (11)→(6): This implication is trivial. Indeed, if

$$f=X^n+a_1X^{n-1}+a_2X^{n-2}+\ldots+a_n \in A_v[X],$$

with $\bar{a}_1 \neq \bar{0}$, $\bar{a}_2=\ldots=\bar{a}_n=\bar{0}$, $n \geq 1$, then $\bar{f}=X^{n-1}(X+\bar{a}_1)$, so $\bar{f}(-\bar{a}_1)=0$. Thus $v(f(-a_1))>0$. But

$$f'=nX^{n-1}+(n-1)\,aX^{n-2}+\ldots+a_{n-1},$$

so $\bar{f}'=(nX+(n-1)\bar{a}_1)X^{n-2}$ and so $\bar{f}'(-\bar{a}_1) \neq \bar{0}$, hence $v(f'(-a_1))=0$. By (11) there exists $a' \in A_v$ such that $\bar{a}'=-\bar{a}_1$ and $f(a')=0$. So $X-a'$ is a linear factor of f.

It follows from theorems 2, 3, 4, 8, 9, 10, 11 and the implication (11)→(6) that the conditions (8), (9), (10) and (11) are equivalent to each other and to the fact that (K, v) is a henselian field. □

Acknowledgement

This paper was written to answer a question from R.A. Smith, whose untimely and sudden death we all deplore.

I'm thankful to Françoise Delon, who called my attention to an error in a preprint of this paper.

Bibliography

[1] Endler, O.: *Valuation Theory.* Springer Verlag, Berlin, 1972.

[2] Hensel, K.: *Theorie der algebraischen Zahlen.* Teubner, Leipzig, 1908.

[3] Krasner, M.: Séminaire d'Algèbre. Institut Henri Poincaré, Paris, 1964.
[4] Krull, W.: Allgemeine Bewertungstheorie. J. reine u. angew. Math., 167, 1931, 160–196.
[5] Nagata, M.: On the theory of Henselian rings, I. Nagoya Math. J., 5, 1953, 45–57.
[6] Ostrowski, A.: Untersuchungen zur arithmetischen Theorie der Körper. Math. Zeits., 39, 1934, 269–404.
[7] Rayner, F.J.: Relatively complete fields. Proc. Edinburgh Math. Soc., 11, 1958, 131–133.
[8] Ribenboim, P.: *Théorie des Valuations.* Presses Univ. Montréal, Montréal, 1964.
[9] Rim, D.S.: Relatively complete fields. Duke Math. J., 24, 1957, 197–200.
[10] Rychlik, K.: Zur Bewertungstheorie der algebraischen Körper. J. reine u. angew. Math., 153, 1923, 94–107.
[11] Schilling, O.F.G.: *The Theory of Valuations.* Amer. Math. Soc., New York, 1950.
[12] van den Dries, L.: *Model Theory of Fields, Decidability and Bounds for Polynomial Ideals.* Thesis, Utrecht, 1978.

Received 6. 12. 82
Revised 15. 9. 83

Department of Mathematics and Statistics
Queen's University at Kingston
Kingston, Ontario, K7L 3N6, Canada

EXPOSITIONES
MATHEMATICAE

Expo. Math. 3 (1985), 25-39
© Bibliographisches Institut 1985

On explicit bases in Sobolev spaces

C. Deninger and H. Lange

1. Introduction

It is well known that the Sobolev spaces $W^{k,p}(\Omega)$ and $\mathring{W}^{k,p}(\Omega)$ for $1<p<\infty$ have Schauder bases under some weak assumption on the regularity of a domain $\Omega \subset \mathbb{R}^n$ (s. [4]). The proofs for this statement however are non-constructive in general. Only for the case of an n-dimensional cube I^n, $I=[0,1]$ Z. Ciesielski & J. Domsta [2] gave an explicit construction of such a basis using spline functions; this basis is orthonormal relative to the usual inner product

$$(f,g)=\int_{\Omega} f(t)\overline{g(t)}\,dt$$

in $L^2(\Omega)$. By the way, the situation is nearly the same in the case of the $C^k(\Omega)$-spaces. Furthermore it is known that the eigenfunctions of the Dirichlet or Neumann problems for the Laplace operator (or other 2nd order strongly elliptic operators) in a bounded domain form orthonormal bases for $H^1(\Omega)$ and $\mathring{H}^1(\Omega)$ resp. ($H^1(\Omega)=W^{1,2}(\Omega)$, $\mathring{H}^1(\Omega)=\mathring{W}^{1,2}(\Omega)$; s. J.L. Lions [5]; see also H. Triebel [6] for the appropriate theorem from functional analysis).

In these notes we started from quite another point of view, namely the question whether the natural orthonormal basis $B=\{e^{\text{int}}\}_{n\in\mathbb{Z}}$ for $L^2[-\pi,\pi]$ gives rise to an orthonormal basis for $H^1(-\pi,\pi)$. Although B is orthogonal in the inner product

$$(u,v)_1=(u,v)+(u',v')$$

of $H^1(-\pi,\pi)$ the answer to this question clearly is negative. But then is it possible to complete B by known elementary functions to an orthonormal basis for $H^1(-\pi,\pi)$? In 2. we give an answer to this problem for we can show that $B_1=B\cup\{\sinh(t)\}$ is a complete orthogonal system for $H^1(-\pi,\pi)$ (Theorem (2.1)).

In the next sections we consider the generalization to higher order Sobolev spaces $H^k(-\pi,\pi)=W^{k,2}(-\pi,\pi)$ of the problem treated in 2.: we try to extend the orthogonal set of functions $\{e^{inx}\}_{n\in\mathbb{Z}}$ to an orthogonal basis of $H^k(-\pi,\pi)$ by adjoining a finite number of functions.

Before we explain the details let us introduce some notation:

0723-0869/85/010025-15 $4.50