RELATIVELY COMPLETE FIELDS

by F. J. RAYNER
(Received 14th June 1958)

Let K be a valued field, let v denote its valuation and B its valuation ring. Let P denote the valuation ideal. For each a in B, let $\bar{a}$ denote the residue class $a+P$ in the field B/P; for $f(x)=\Sigma a_r x^r$ in $B[x]$, let $\bar{f}(x)$ denote $\Sigma \bar{a}_r x^r$ in $B/P[x]$. Let Λp denote the leading coefficient of a polynomial p, and ∂p the degree of a non-zero polynomial.

Hensel's lemma will be said to hold for K **in the strong form** *if, given any triple of polynomials f, g, h in $B[x]$ for which* (i) $\bar{f}=\bar{g}\bar{h}$; (ii) $(\bar{g}, \bar{h})=1$; (iii) $\Lambda g=1$, $\partial g \neq 0_2$; (iv) $\partial h \leqslant \partial f - \partial g$, *there exists a pair of polynomials G, H such that $f=GH$, $\bar{g}=\bar{G}$, $\partial g=\partial G$, $\Lambda G=1$, $\bar{h}=\bar{H}$.*

If this conclusion follows when (iii) and (iv) are replaced by the requirement that f, g and h be monic (i.e. that Λf, Λg and Λh be units of B), we shall say that *the weak form of Hensel's lemma* holds for K.

K will be said to be *strongly (weakly) relatively complete* if Hensel's lemma holds for K in the strong (weak) form.

A valued field K is said to have the *unique extension property* if any algebraic extension K_1 of K admits one and only one valuation which agrees on K with the valuation of K. Krull (1) proved that a strongly relatively complete field has the unique extension property. Dock Sang Rim (2) has stated the theorem that the unique extension property is equivalent to relative completeness. He appears, however, to have overlooked the difference between strong and weak relative completeness, for he proves only that a field with the unique extension property is weakly relatively complete. The purpose of the present note is to show that the unique extension property implies strong relative completeness.

LEMMA 1. *Let K be a field with the unique extension property. Let σ be any automorphism of $\hat{K}$ (the algebraic closure of K) over K. Then σ leaves the valuation invariant.*

Proof: Suppose that $a \in \hat{K} \smallsetminus K$, and that $v(a) \neq v(a^\sigma)$. Then if $w(x)=v(x^\sigma)$ for each x in $\hat{K}$, it is clear that w is a valuation of $\hat{K}$ distinct from v. Hence the valued field K does not have the unique extension property, contrary to hypothesis. Thus Lemma 1 is proved.

For the discussion of the strong form of Hensel's lemma, it suffices to consider polynomials over B which are primitive (in the sense that the corresponding polynomials over B/P are non-zero). Accordingly, I suppose all polynomials to be primitive, unless otherwise indicated.

LEMMA 2. *Let l be an irreducible polynomial of degree v over the valuation ring of a field with the unique extension property. Then either (i) $l = \alpha x^v$ (α in B/P); or (ii) $l = \beta$ (β in B/P); or (iii) Λl is a unit of B, and $l(0)$ is a unit of B.*

Proof: Let $\hat{K}$ denote the algebraic closure of K. Then, over $\hat{K}$, l may be represented in the form $\prod\limits_{i=1}^{v} (ax + b_i)$. Then $\{b_i/a\}$ is a set of conjugates over K, and so for each i, $v(b_i/a) = \gamma$, say ; so that $v(b_i) = \gamma + v(a)$. Hence either for each i, $\bar{b}_i = 0$, or for each i, $\bar{b}_i \neq 0$. Thus if $\bar{b}_i = 0$, $l = \Pi \bar{a} x = \alpha x^v$, or if $\bar{b}_i \neq 0$, but $\bar{a} = 0$, $l = \Pi \bar{b}_i = \beta$, say. (We cannot have both $\bar{a} = 0$ and $\bar{b}_i = 0$, since we are assuming that l is primitive.) In the remaining case, $l = \prod\limits_{i=1}^{v} (\bar{a} x + \bar{b}_i)$ with $\bar{a} \neq 0$, $\bar{b}_i \neq 0$, and so Λl and $l(0)$ are units of B.

LEMMA 3. *Let l, m, n be elements of $B[x]$ such that $l | \bar{m}\bar{n}$, $\Lambda m = 1$, $\partial m \neq 0$, $(\bar{m}, \bar{n}) = 1$, and l is irreducible over K. Then l divides at least one of $\bar{m}$ and $\bar{n}$.*

Proof: By Lemma 2, either $l = \alpha x^v$ or $l = \beta (\neq 0$, in $B/P)$ or $l = \prod\limits_{i=1}^{v} (ax + b_i)$, $\bar{a} \neq 0$, $\bar{b}_i \neq 0$.

In the first case, since $(\bar{m}, \bar{n}) = 1$, x^v divides either $\bar{m}$ or $\bar{n}$, and so also l divides either $\bar{m}$ or $\bar{n}$.

In the second case ($l = \beta$), clearly $l | \bar{m}$ and $l | \bar{n}$.

For the third case, we have that each irreducible factor of l divides either $\bar{m}$ or $\bar{n}$. Since $(\bar{m}, \bar{n}) = 1$, any repeated factor of l will divide either $\bar{m}$ or $\bar{n}$ in its full multiplicity. Thus if each factor of l divides $\bar{m}$ it follows that l divides $\bar{m}$ (and similarly for $\bar{n}$). I now use a method due to Schilling ((3), p. 60), to show that l cannot have two distinct relatively prime factors, the one dividing $\bar{m}$ and the other dividing $\bar{n}$. Suppose that this occurred. Then we may write (over $\hat{K}$) $l = a\Pi(x + c_i)$; we have for some i_0, $x + \bar{c}_{i0} | \bar{m}$, and for some i_1, $x + \bar{c}_{i1} | \bar{n}$. However, there is an automorphism σ of $\hat{K}$ over K which carries c_{i0} into c_{i1}. This induces an automorphism $\bar{\sigma}$ of the residue class field $\hat{B}/\hat{P}$ over B/P which carries $x + \bar{c}_{i0}$ into $x + \bar{c}_{i1}$. $\bar{\sigma}$ leaves $\bar{m}$ and $\bar{n}$ invariant, and so $\bar{\sigma}(x + \bar{c}_{i0}) | \bar{m}$, i.e. $x + \bar{c}_{i1}$ is a common factor of $\bar{m}$ and $\bar{n}$. This is contrary to hypothesis. Hence either each irreducible factor of l divides $\bar{m}$, or each divides $\bar{n}$. The conclusion of Lemma 3 now follows : in each of the three cases, either $l | \bar{m}$ or $l | \bar{n}$ or both.

LEMMA 4. *If l is irreducible over a field with the unique extension property, then l is a constant multiple of a power of an irreducible polynomial.*

Proof: Suppose l is not a constant multiple of a power of an irreducible polynomial. Then l may be written in the form $\bar{m}\bar{n}$ where $(\bar{m}, \bar{n}) = 1$ and $\partial \bar{m} \neq 0$, $\partial \bar{n} \neq 0$. Further, we may take $\Lambda m = \Lambda \bar{m} = 1$, so that $\partial \bar{m} = \partial m$. Then the hypotheses of Lemma 3 will be satisfied, so that l divides either $\bar{m}$ or $\bar{n}$ (or both). In each of these cases the remaining factor must be a constant (i.e. $\bar{n}$ or $\bar{m}$ or both), contrary to hypothesis. Hence the lemma is proved.

THEOREM 1. *If l is an irreducible polynomial of degree n over the valuation ring of a field with the unique extension property, then either* (i) $\bar{l} = \alpha x^n$; *or* (ii) $\bar{l} = \beta$; *or* (iii) $\bar{l} = k\{\alpha_0 x^r + \alpha_1 x^{r-1} + \ldots + \alpha_r\}^s$, *where* $\alpha_0 x^r + \alpha_1 x^{r-1} + \ldots + \alpha_r$ *is irreducible over B/P, $\alpha_0 \neq 0$, and $rs = n$.*

Proof: This follows from Lemma 2 and Lemma 4.

Note: The property of irreducible polynomials given in Theorem 1 is the corollary of Hensel's lemma (strong form) which Krull used. I prove, finally, that this property is equivalent to the strong form of Hensel's lemma.

LEMMA 5. *Let K be a valued field such that each irreducible polynomial l of degree n over the valuation ring has either $\bar{l} = \alpha x^n$, or $\bar{l} = \beta$, or*
$$\bar{l} = k\{\alpha_0 x^r + \alpha_1 x^{r-1} + \ldots + \alpha_r\}^s,$$
where $\alpha_0 x^r + \alpha_1 x^{r-1} + \ldots + \alpha_r$ is irreducible over B/P, $\alpha_0 \neq 0$, and $rs = n$. Then Hensel's lemma in the strong form holds for K.

Proof: Let f, g, h be a triple of polynomials over B for which (i) $\bar{f} = \bar{g}\bar{h}$; (ii) $(\bar{g}, \bar{h}) = 1$; (iii) $\Lambda g = 1$, $\partial g \neq 0$; (iv) $\partial h \leqslant \partial f - \partial g$. Let the irreducible factors of f be $f_1, \ldots, f_p$ (we may have $p = 1$). Then for each $i = 1, \ldots, p$, f_i is primitive, and $\bar{f}_i$ is either a constant, or a power of an irreducible monic polynomial such that $\partial \bar{f}_i = \partial f_i$.

Clearly, we may take each such f_i to have leading coefficient 1. By Lemma 3, each of the $\bar{f}_i$ must divide at least one of $\bar{g}$, $\bar{h}$, and those corresponding to monic f_i of non-zero degree can divide only one. Let G denote the product of such monic f_i for which $\bar{f}_i | \bar{g}$. We take $G = 1$, if there are no such f_i. It is readily seen that $\bar{G} = \bar{g}$, and (since $\Lambda G = \Lambda g = 1$) that $\partial G = \partial g$. Finally, if $H = f/G$, then $\bar{H} = \bar{h}$, so that the conclusion of Hensel's lemma holds for K.

As a consequence we have the following theorem.

THEOREM 2. *If the valued field K has the unique extension property, then K is strongly relatively complete.*

REFERENCES

(1) W. KRULL, Allgemeine Bewertungstheorie, *J. fur Math.*, **167** (1932), 160-96
(2) DOCK SANG RIM, Relatively complete fields, *Duke Math. J.*, **24** (1957), 197-200.
(3) O. F. G. SCHILLING, *Theory of Valuations*, New York, 1950.

DEPARTMENT OF MATHEMATICS
THE UNIVERSITY
GLASGOW, W. 2