Note on Relatively Complete Fields

Eizi Inaba (稲葉栄次)
Department of Mathematics, Faculty of Science,
Ochanomizu University

(*Received April 30, 1952*)

A real-valued function $V(a)$ of a field k is a non-archimedean valuation V of k, if the relations $V(ab)=V(a)+V(b)$ and $V(a+b)\geqq \text{Min}\{V(a), V(b)\}$ hold, where we put $V(0)=\infty$. The set of all elements a with $V(a)\geqq 0$ is the valution ring R in k. All elements a with $V(a)>0$ form a prime ideal P in R. A polynomial $f(x)$ with coefficients from R is called primitive, if among these coefficients there exists at least one unit. By Ostrowski the field k is termed relatively complete with respect to V, if Hensel's lemma holds for every primitive polynomial. The present note aims to reveal some characteristic properties of this field.

Lemma 1. *Let $f(x)$ be an irreducible polynomial over k and α_i, $i=1, \cdots, n$ be all roots of $f(x)$. If V has a unique prolongation to every algebraic extension of k, then the values $V(\alpha_i)$ are all equal.*

Proof. We consider the extension $K=k(\alpha_1)$ over k. If $V(\alpha_1)\neq V(\alpha_2)$, let σ be the isomorphism of K over k such that $\sigma\alpha_1=\alpha_2$. Putting $W(\beta)=V(\sigma\beta)$ for $\beta\in K$, we obtain another prolongation of V for K. Since $W(\alpha_1)=V(\alpha_2)\neq V(\alpha_1)$, one would obtain two different prolongation, contrary to the hypothesis.

Theorem 1. *A field k is relatively complete with respect to a non-archimedean valuation V, if and only if V has a unique prolongation to every algebraic extension of k.*

Proof. It is well known that the prolongation of V is unique, if k is relatively complete.[1] We prove the converse as follows. First we show that every primitive irreducible polynomial $f(x)$ is congruent modulo P to a unit in R or to a product of a unit and a power of a polynomial irreducible modulo P. Let $\alpha_i, i=1, \cdots, n$ be all roots of $f(x)$. The values $V(\alpha_i)$ are all equal by Lemma 1. For the case, where $V(\alpha_i)$ are negative, every coefficient of the polynomial $\left(\frac{x}{\alpha_1}-1\right)\cdots\left(\frac{x}{\alpha_n}-1\right)$ except the constant term belongs to P. Hence $f(x)$ is congruent to a unit modulo P. Next consider the case, where $V(\alpha_i)\geqq 0$. In this case every coefficient of $f(x)$ is divisible by the leading coefficient and hence we can assume that $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$. If $f(x)$ had two different monic irreducible factors $g(x)$ and $h(x)$ modulo P, it would follow that $g(\alpha_\lambda)\in\overline{P}$ and $h(\alpha_\mu)\in\overline{P}$, where $\overline{P}$ is the prime ideal of the

[1] We refer to Schilling, theory of valuations.

valuation ring in $K=k(\alpha_1, \cdots, \alpha_n)$. Since the prolongation of V is unique, $\overline{P}$ is invariant under any automorphism of K/k as can be seen from the proof of Lemma 1. Consequently we have $g(\alpha_\mu) \in \overline{P}$. Now, by virtue of the relation $g(x)A(x)+h(x)B(x) \equiv 1 \bmod. P$, we have $g(\alpha_\mu) A(\alpha_\mu)+h(\alpha_\mu)B(\alpha_\mu) \in \overline{P}$ and hence $1 \in \overline{P}$, which yields a contradiction. Thus $f(x)$ is a power of a polynomial irreducible modulo P. Next we consider the general case, where $f(x)$ is assumed to be primitive. If $f(x) \equiv g(x)h(x) \bmod. P$ and $g(x)A(x)+h(x)B(x) \equiv 1 \bmod. P$, then we can put $f(x)=\Pi f_i^{(1)}(x) \, \Pi f_j^{(2)}(x)$, where, $f_i^{(1)}$ and $f_j^{(2)}$ being primitive irreducible over k, $f_i^{(1)}(x) \equiv \varepsilon_i \bmod. P$ holds with a unit ε_i and $f_j^{(2)}(x)$ is congruent modulo P to a power of a polynomial irreducible mod. P. Further we can assume that $g(x)$ is monic with degree $m \geqq 1$. By virtue of the uniqueness of factorization modulo P, we can find polynomials $G(x)$ and $H(x)$ such that

$$G(x) \equiv g(x) \bmod. P, \qquad H(x) \equiv h(x) \bmod. P,$$

and $f(x)=G(x)H(x)$, the degree of $G(x)$ being m. Hence Hensel's lemma holds for k.

Corollary. *Every algebraic extension of a field, which is relatively complete with respect to a non-archimedean valuation V, is also relatively complete with respect to the prolongation of V.*

Ostrowski's criterion asserts that a field k is relatively complete with respect to a non-archimedean valuation V, if and only if k is separably algebraically closed in the completion k^* of k.[2] We shall show that this criterion follows from Theorem 1. Let k be relatively complete with respect to V and $K=k(\alpha)$ be a finite separable extension over k, which is contained in k^*. Let $f(x)$ be the irreducible polynomial over k with the root α. $f(x)$ being separable, there exists another root β of $f(x)$, which is different from α. Since α belongs to k^*, there exists a sequence $\{c_i\}$ of elements $c_i \in k$ such that $\lim V(c_i-\alpha)=\infty$. By Lemma 1 and Theorem 1 we have $V(c_i-\beta)=V(c_i-\alpha)$. This implies $V(\alpha-\beta)=\infty$, which yields a contradiction. Hence k has no separable extension, which is contained in k^*. In order to prove the converse, it suffices to show by Theorem 1 that V has a unique prolongation to every finite separable normal extension K over k. For the prolongation is always unique for every purely inseparable extension.[3] Since k is separably algebraically closed in k^*, it follows that $K \frown k^*=k$. Let $f(x)$ be the monic irreducible polynomial over k, which has $\alpha \in K$ as a root. Then this becomes $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$ with $\alpha_i \in K$, where $\alpha_1=\alpha$. Now we observe that $f(x)$ is irreducible over k^*. In fact, if $f(x)$

[2] A. Ostrowski, Untersuchungen zur arithmetischen Theorie der Körper, Math. Zeitschr. 39 (1935).

[3] Schilling, l. c.

$=g(x)h(x)$ with $g(x)\in k^*[x]$ and $h(x)\in k^*[x]$, then all coefficients of $g(x)$ and $h(x)$ would belong to $K\frown k^*=k$. Hence $V(\alpha)$ is uniquely determined as the value $\frac{1}{n}V(c)$, where c is the constant term of $f(x)$.

Corollary. *A field k is relatively complete with respect to a non-archimedean valuation V, if and only if every separable irreducible polynomial over k is also irreducible over the completion k^* of k.*

Proof. It was shown in the proof of Ostrowski's criterion that any separable irreducible polynomial over k is also irreducible over k^*, if k is relatively complete. The converse can be proved as follows. If an element α from k^* is separable over k, then the irreducible polynomial over k with the root α is also irreducible over k^*. Hence the degree of the polynomial is one and α belongs to k. The proof is now complete by Ostrowski's criterion, since k is separably algebraically closed in k^*,

Theorem 2. *A field k is relatively complete with respect to a non-archimedean valuation V, if and only if the following condition is satisfied: for every separable irreducible polynomial $f(x)$ over k with degree larger than one, the set of values $V(f(a))$ for all $a\in k$ is upper bounded.*

Proof. Let k be relatively complete with respect to V and put $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$, $K=k(\alpha_1,\cdots,\alpha_n)$, If there exists a sequence $\{a_i\}$ with $a_i\in k$ such that $V(f(a_i))=\lambda_i$ and $\lim\lambda_i=\infty$, then we obtain a subsequence $\{b_i\}$ of $\{a_i\}$ such that

$$\lim_{i\to\infty} V(b_i-\alpha_s)=\infty$$

for a certain α_s. Then α_s belongs to the completion k^* of k. This yields $\alpha_s\in K\frown k^*$ and consequently $\alpha_s\in k$ by Ostrowski's criterion, since α_s is separable over k. Then $f(x)$ is of degree one, contrary to the hypothesis. Next we prove that k is relatively complete, if the condition is satisfied. By Ostrowski's criterion it suffices to show that k is separably algebraically closed in the completion k^*. Let $K=k(\alpha)$ be a finite separable extension over k, which is contained in k^*. The relation $\lim V(c_i-\alpha)=\infty$ holds for a sequence $\{c_i\}$ with $c_i\in k$. We consider the separable irreducible polynomial $f(x)$ over k with the root α. Then we have $\lim V(f(c_i))=\infty$. Hence $f(x)$ must be of degree one by virtue of the condition, whence $K=k$.

Remark. For an irreducible polynomial $f(x)$ of the second degree over the field of all real numbers there exists a positive real number c such that $f(a)\geqq c$ for all real numbers a. Theorem 2 is an analogy of this fact.

Let k be a field with a non-archimedean valuation V. For a polynomial $f(x)=a_0+a_1x+\cdots+a_nx^n$ over k we put $V(f(x))=\mathrm{Min}\,\{V(a_0), V(a_1), \cdots, V(a_n)\}$. We define the set of all polynomials $g(x)$ with $V(g(x)-f(x))\geqq\lambda$ as a neighborhood of $f(x)$. By a neighborhood of an element

c from k we understand the set of all elements d from k with $V(d-c) \geqq \lambda$ as usual.

Theorem 3. *A field k is relatively complete with respect to a non-archimedean valuation V, if and only if the following condition is satisfied: for any separable polynomial $f(x)$, which has no root from k, there exists a neighborhood of $f(x)$ such that every polynomial in the neighborhood has no root from k.*

Proof. We can assume without loss of generality that $f(x)$ is monic with coefficients from R. If k is relatively complete, there exists a positive real number λ such that $V(f(a)) \leqq \lambda$ for all $a \in R$ by Theorem 2, since $f(x)$ is a product of separable irreducible polynomials with degree larger than one. We consider a polynomial $g(x)$ with $V(g(x)-f(x)) \geqq \lambda+1$. Then all coefficients of $g(x)$ belong to R, the leading coefficient being a unit. Since $V(g(a)-f(a)) \geqq \lambda+1$ for all $a \in R$, we have $V(g(a) \leqq \lambda$ for all $a \in R$. If $g(x)$ had a root b from k, it would necessarily belong to R and $V(g(b))=\infty$. This yields a contradiction. Next we prove the converse. Let $f(x)$ be a separable irreducible polynomial over k of degree larger than one with a root $\alpha \in k^*$. We put $f(x)=(x-\alpha)h(x)$, where $h(x)$ is a polynomial over $k(\alpha)$. If we choose an element c from k such that $V(\alpha-c)$ is sufficiently large, then we can find a polynomial $F(x)=(x-c)H(x)$ with $H(x)$ over k in every neighborhood of $f(x)$. This contradicts with the condition. Hence k is separably algebraically closed in k^* and relatively complete by Ostrowski's criterion.

Theorem 4. *If a field k is relatively complete with respect to a non-archimedean valuation V, and if $f(x)$ is a polynomial over k, which has a simple root a from k, then there exists a neighborhood of $f(x)$ such that every polynomial in the neighborhood has a simple root in any given neighborhood of a.*

Proof. Let k be relatively complete with respect to V. We can assume without loss of generality that all coefficients of $f(x)$ belong to the valuation ring R in k and the leading coefficient is 1. Then it is evident that the root a belongs to R. Putting $f(x)=(x-a)F(x)$, we have $f'(a)=F(a) \neq 0$ by hypothesis. If we put $V(F(a))=e$, then $e \geqq 0$, since $F(x)$ is a polynomial over R. Let $g(x)$ be a polynomial with $V(g(x)-f(x)) \geqq \lambda+e$, where $\lambda \geqq 1+e$. Then $g(x)$ is a polynomial over R. Now we shall show that we can construct a sequence $\{a_i\}$ of elements a_i from R such that $V(a_i-a) \geqq \lambda$ and $V(g(a_i)) \geqq \lambda+e+i-1$. For $i=1$, we put $a_1=a$ and we have $V(g(a_1)) \geqq \lambda+e$, $V(a_1-a)=V(o) \geqq \lambda$, since $V(g(a_1)-f(a_1)) \geqq \lambda+e$ and $f(a_1)=0$. If a_i satisfies the above relations, then we have $V(F(a_i))=e$, since $F(a_i)=F(a)+(a_i-a)h_i$ with $h_i \in R$ and $e=V(F(a))<\lambda \leqq V((a_i-a)h_i)$. If we put

$$a_{i+1}=a_i-\frac{g(a_i)}{F(a_i)},$$

it follows that $V(a_{i+1}-a_i)\geqq\lambda+i-1$ and hence $V(a_{i+1}-a)\geqq\lambda$. Further we have

$$g(a_{i+1})=g(a_i)+(a_{i+1}-a_i)g'(a_i)+(a_{i+1}-a_i)^2\theta_i,$$

where $\theta_i\in R$ and this amounts to

$$(1)\qquad g(a_{i+1})=\frac{g(a_i)}{F(a_i)}(F(a_i)-g'(a_i))+(a_{i+1}-a_i)^2\theta_i.$$

For the derivative of the polynomial $g(x)-f(x)$ we have $V(g'(x)-f'(x))\geqq\lambda+e$ and hence $V(g'(a)-f'(a))\geqq\lambda+e$. Then $V(g'(a_i)-F(a_i))\geqq\lambda$ by virtue of the relation $V(a_i-a)\geqq\lambda$. Consequently the relation (1) yields $V(g(a_{i+1}))\geqq\lambda+i+e$, since $\lambda\geqq e+1$. Thus we have a sequence $\{a_i\}$ such that $\lim V(g(a_i))=\infty$ and $V(a_{i+1}-a_i)\geqq\lambda+i-1$. This implies that there exists an element α in the completion k^* of k such that $g(\alpha)=0$, $V(\alpha-a)\geqq\lambda$ with $\lim V(\alpha-a_i)=\infty$. Since $V(g'(a)-f'(a))\geqq\lambda$ and $V(f'(a))=e$, we have $V(g'(\alpha))=e$. Then $g'(\alpha)\neq 0$ and α is a simple root of $g(x)$, which lies in the neighborhood of a with $V(\alpha-a)\geqq\lambda$. Since α is separable over k and contained in k^*, it must be an element from k by Ostrowski's criterion.

Corollary. *If k is relatively complete with respect to a non-archimedean valuation V, and if n is a positive integer, which is not divisible by the characteristic of k, then there exists a positive real number λ such that every element $a\in k$ with $V(a-1)\geqq\lambda$ is an n-th power of an element from k.*

Proof. The unity is a simple root of the polynomial x^n-1, since n is not divisible by the characteristic of k. By Theorem 4 we can find λ such that every polynomial x^n-a with $V(a-1)\geqq\lambda$ has a root from k. This completes the proof.

It is to be remarked that the above corollary is a precision of a lemma by Schilling. If k is a p-adic number field, this is important in class field theory and its usual proof is based upon the use of exponential and logarithmic functions.