JOURNAL OF SCIENCE OF THE HIROSHIMA UNIVERSITY, SER. A, VOL. 18, NO. 1, JUNE, 1954

On the Different Theorem in Complete Fields with Respect to a Discrete Valuation

By

Akira KINOHARA

(Received March 20, 1954)

§ **1.** Throughout this note we shall be dealing with finite separable extensions K of a field k which is complete under a discrete valuation. As usual, we shall denote by $\mathfrak{O}$, $\mathfrak{P}$, $\mathfrak{R}$ and $\mathfrak{o}$, $\mathfrak{p}$, $\mathfrak{k}$ the rings of integers, prime ideals, and residue class fields in K and k, respectively. The trace from K to k will be denoted by S. Then the *different* $D(K/k)$ of K/k is defined as the inverse of $\mathfrak{M}$ such that $\lambda \in \mathfrak{M} \Leftrightarrow S(\lambda\mathfrak{O}) \subset \mathfrak{o}$.

In this note, we shall show a proof of the different theorem different from the usual one.[1]

§ **2.** Throughout this note, let $f(x)$[2] be the canonical defining polynomial of $\theta \in \mathfrak{O}$ in $\mathfrak{o}[x]$, and $f'(x)$ the derivative of $f(x)$ with respect to x. Then, as is well known, the different $f'(\theta)$ of θ is divisible by $D(K/k)$. In particular, if, for example, k, K are $\mathfrak{p}$-adic number fields, $D(K/k)$ is the greatest common divisor of $(f'(\theta))$ for all θ in $\mathfrak{O}$. But, in our case, it is not always true.

LEMMA 1. *The following three statements are equivalent:*

A) $\mathfrak{O} = \mathfrak{o}[\theta]$

B) $D(K/k) = (f'(\theta))$

C) There exists an element $\eta \in \mathfrak{O}$ whose residue class modulo $\mathfrak{P}$ is a primitive element of $\mathfrak{R}/\mathfrak{k}$ and one of the prime elements of $\mathfrak{P}$ in $\mathfrak{O}$ belongs to $\mathfrak{o}[\eta]$.

PROOF. We have already proved[3]: A)$\Leftrightarrow$B). Here we shall show A)$\Leftrightarrow$C). We may take an element θ which satisfies the conditions required in C) and is one of the primitive elements of K/k. Then, if $[\mathfrak{R}:\mathfrak{k}]$[4] $=f$, we can choose $1, \theta, \cdots, \theta^{f-1}$ as a

1) See: E. Artin, Algebraic Numbers and Algebraic Functions I, Princeton Univ. and New York Univ., 1950–1951, Chap. 5, The Different, Theorem 2.

2) $f(x)$ is irreducible in $\mathfrak{o}[x]$ with the leading coefficient 1.

3) See: A. Kinohara, A Note on the Relative 2-Dimensional Cohomology Group in Complete Fields with Respect to a Discrete Valuation, this Journal, **18**, p. 2 (1954), Lemma 1.

4) $[\mathfrak{R}:\mathfrak{k}]$ denotes the degree of $\mathfrak{R}/\mathfrak{k}$.

representative in $\mathfrak{O}$ of a basis for $\mathfrak{R}/\mathfrak{k}$. Let $\mathfrak{O}\mathfrak{p}=\mathfrak{P}^e$, and Π one of the prime elements of $\mathfrak{P}$ in $\mathfrak{O}$ such that $\Pi\in\mathfrak{o}[\theta]$. Then $\theta^i\Pi^j(i=0, 1, \cdots, f-1; j=0, 1, \cdots, e-1)$, which are a minimal basis for K/k, belong to $\mathfrak{o}[\theta]$. Hence we have C)$\Rightarrow$A). Moreover, from the above statement, we have easily $\overline{\text{C}})^{1)}\Rightarrow\overline{\text{A}})$, q. e. d.

COROLLARY 1. *If $\mathfrak{R}/\mathfrak{k}$ is separable, then $\mathfrak{O}=\mathfrak{o}[\theta]$.*

COROLLARY 2. *If $[\mathfrak{R}:\mathfrak{k}]$ is a prime number, then $\mathfrak{O}=\mathfrak{o}[\theta]$.*

LEMMA 2. *Let $\mathfrak{O}=\mathfrak{o}[\theta]$. The irreducible factorization of $f(x)$ modulo $\mathfrak{p}$ is the following, if and only if $\mathfrak{O}\mathfrak{p}=\mathfrak{P}^e$:*

$$f(x)\equiv P(x)^e \qquad \textit{mod } \mathfrak{p},$$

where $(P(\theta))=\mathfrak{P}$ and $[\mathfrak{R}:\mathfrak{k}]=deg\ (P(x))$.

PROOF. Since $\mathfrak{O}=\mathfrak{o}[\theta]$, we have:

$$\mathfrak{O}/\mathfrak{O}\mathfrak{p}=\mathfrak{o}[\theta]/\mathfrak{O}\mathfrak{p}\cong\mathfrak{o}[x]/(\mathfrak{p}, f(x)) \quad (\cong\mathfrak{k}[x]/f(x)).$$

Hence, if $\mathfrak{O}\mathfrak{p}=\mathfrak{P}^e$, $f(x)$ must split into a power of an irreducible polynomial $P(x)$ modulo $\mathfrak{p}$ such that $(P(\theta))=\mathfrak{P}$ and $[\mathfrak{R}:\mathfrak{k}]=\deg\ (P(x))$, that is, $f(x)\equiv P(x)^e \bmod \mathfrak{p}$, and vice versa.

§ **3.** Now we shall prove the different theorem.

THEOREM (the different theorem). *$D(K/k)=\mathfrak{O}$, if and only if K/k is unramified and $\mathfrak{R}/\mathfrak{k}$ is separable.*

PROOF. We shall consider the following three cases.

Case 1. $\mathfrak{O}\mathfrak{p}=\mathfrak{P}^e$ and $\mathfrak{R}/\mathfrak{k}$ is separable. Then, by Corollary 1, there exists θ such that $\mathfrak{O}=\mathfrak{o}[\theta]$. Thus, by using the same notations as in Lemma 2, we have $f(x)\equiv P(x)^e \bmod \mathfrak{p}$, where $(P(\theta))=\mathfrak{P}$ and $P(x)$ is an irreducible polynomial modulo $\mathfrak{p}$. Then we have $f'(\theta)\equiv eP(\theta)^{e-1}P'(\theta) \bmod \mathfrak{P}^e$. However, since $\mathfrak{R}/\mathfrak{k}$ is separable, $P'(\theta)\not\equiv 0 \bmod \mathfrak{P}$. Hence, if K/k is unramified, i. e., $e=1$, we have $\text{D}(K/k)=\mathfrak{O}$.

Case 2. $e=1$ but $\mathfrak{R}/\mathfrak{k}$ is a purely inseparable extension of degree p where p (a prime number) is the characteristic of $\mathfrak{k}$. Then, by Corollary 2, there exists θ such that $\mathfrak{O}=\mathfrak{o}[\theta]$. Thus, by using the same notations as in Lemma 2, we hawe $f'(\theta)\equiv P'(\theta) \bmod \mathfrak{P}$. On the other hand, since $\mathfrak{R}/\mathfrak{k}$ is purely inseparable, $P'(\theta)\equiv 0 \bmod \mathfrak{P}$. Hence we have $D(K/k)\neq\mathfrak{O}$.

Case 3. $\mathfrak{R}/\mathfrak{k}$ is inseparable. In this case, by using Cases 1 and 2, we shall show that $D\ (K/k)\neq\mathfrak{O}$ holds.

Now let N be a finite separable and normal extension of k containing K. Let k_0 be

1) $\overline{\text{C}})$ denotes non-C).

the first ramification field of N/k, and the Galois group of N/k_0 is a p-group where p (a prime number) is the characteristic of $\mathfrak{k}$. Then, from the theory of the normalizer in the group theory and the Galois fundamental theorem, we can choose the following series of the fields:

$$k_0 \subset k_1 \subset \cdots\cdots \subset k_m = N,$$

where $[k_i : k_{i-1}] = p$ for $i = 1, 2, \cdots, m$.

From the structure of N/k[1], the residue class field $\mathfrak{k}_0/\mathfrak{k}$ of k_0/k is separable, and, k_i/k_{i-1} is either completely ramified or the residue class field $\mathfrak{k}_i/\mathfrak{k}_{i-1}$ of k_i/k_{i-1} is purely inseparable. Hence, if $\mathfrak{K}/\mathfrak{k}$ is inseparable, then it must be $1 < [Kk_0$[2]$: k_0]$.

Since $\mathfrak{k}_0/\mathfrak{k}$ is separable, there exists a primitive element α of k_0/k such that

$$D(k_0/k) = (g'(\alpha)), \tag{1}$$

where $g(x)$ is the canonical defining polynomial of α in $\mathfrak{o}[x]$. Since $k_0 = k(\alpha)$, we have $Kk_0 = K(\alpha)$. Let $g(x) = g_1(x)\,h(x)$ be the factorization of $g(x)$ in $\mathfrak{O}[x]$, where $g_1(\alpha) = 0$ and $g_1(x)$ is the irreducible polynomial. Then we have:

$$g'(\alpha) = g_1'(\alpha)\,h(\alpha) \quad \text{and} \quad h(\alpha) \not\equiv 0, \tag{2}$$

because N/k is separable. On the other hand, since $(g_1'(\alpha)) \subseteqq D(Kk_0/K)$, we have from (1) and (2):

$$D(k_0/k) \subseteqq D(Kk_0/K). \tag{3}$$

From the chain theorem,[3] we have:

$$D(K/k)\,D(Kk_0/K) = D(k_0/k)\,D(Kk_0/k_0). \tag{4}$$

Thus, we have from (3) and (4)

$$D(K/k) \subseteqq D(Kk_0/k_0). \tag{5}$$

Then, in the same manner as was used to obtain (3), we have also:

$$D(k_i/k_{i-1}) \subseteqq D(Kk_i/Kk_{i-1}) \quad \text{for} \quad i = 1, 2, \cdots, m. \tag{6}$$

Now, from the relation

$$[Kk_0 : k_0] \prod_{i=1}^{m} [Kk_i : Kk_{i-1}] = \prod_{i=1}^{m} [k_i : k_{i-1}], \tag{7}$$

where $k_m = Kk_m = N$, we have:

---

1) See: M. Deuring, Verzweigungstheorie bewerteter Körper, Math. Ann., **105** (1930), pp. 291–307.

2) Kk_0 denotes the composite field of K and k_0.

3) See: H. Hasse, Zahlentheorie, Berlin, 1949, pp. 316–317.

(8) $$Kk_i = Kk_{i-1} \quad \text{for some } i,$$

because $1 < [Kk_0 : k_0]$ and $[Kk_i : Kk_{i-1}] \leqq [k_i : k_{i-1}] = p$ (a prime number). Since k_i/k_{i-1} possesses the properties as described in p. 11, we have always, by using Cases 1 and 2:

(9) $$D(k_i/k_{i-1}) \neq \mathfrak{o}_i \quad \text{for all } i,$$

where $\mathfrak{o}_i$ is the ring of integers in k_i. Then, by considering the differents of fields on both sides of (7), we have from (6), (8), and (9):

(10) $$D(Kk_0/k_0) \neq \mathfrak{O}_0,$$

where $\mathfrak{O}_0$ is the ring of integers in Kk_0. Finally, from (5) and (10) we have $D(K/k) \neq \mathfrak{O}$.

This completes the proof of our theorem.

REMARK. Let k be such a quotient field that, in its integral domain, the fundamental theorem of the multiplicative ideal theory holds, and let K be the finite separable extensions of k, then the different theorem holds in K/k also.

Department of Mathematics,
Hiroshima University