ON THE DERIVATIONS AND THE RELATIVE DIFFERENTS IN ALGEBRAIC NUMBER FIELDS

By

Akira KINOHARA

(Received April 30, 1952)

Recently Prof. Y. Kawada [1][1] has developed by derivations the theory of the relative differents in algebraic number fields, and he has proved the equivalence of his new definition with the usual one which was introduced by R. Dedekind[2].

In this note I shall show the equivalence of both definitions in more direct way than that of Prof. Kawada.

Let k be an algebraic number field of finite degree over the rational number field and let K be a finite algebraic extension of k. Then the totalities of all algebraic integers in k and K will be denoted by $\mathfrak{o}$ and $\mathfrak{O}$ respectively. Now we consider for an ideal $\mathfrak{A}$ in $\mathfrak{O}$ the residue class ring $\mathfrak{O}/\mathfrak{A}$ and define a *derivation* modulo $\mathfrak{A}$ in a subring $\mathfrak{R}(\supseteq\mathfrak{o})$ of $\mathfrak{O}$ as a unique mapping of $\mathfrak{R}$ into $\mathfrak{O}/\mathfrak{A}$ with the following properties:

(1) D has $\mathfrak{O}$ as an operator domain i. e. for an arbitrary element λ in $\mathfrak{O}$ and every element α in $\mathfrak{R}$ the relation

$$(\lambda D)(\alpha)=\lambda D(\alpha)=\overline{\lambda}D(\alpha)$$

holds where $D(\alpha)$ denotes the image of α by D and $\overline{\lambda}$ the residue class mod $\mathfrak{A}$ containing λ;

(2) D is a module homomorphism of $\mathfrak{R}$ into $\mathfrak{O}/\mathfrak{A}$ i. e. for $\alpha, \beta\in\mathfrak{R}$

$$D(\alpha+\beta)=D(\alpha)+D(\beta)\ ;$$

(3) for $\alpha, \beta\in\mathfrak{R}$

$$D(\alpha\beta)=\beta D(\alpha)+\alpha D(\beta).$$

In the following we denote by $\mathfrak{D}(\mathfrak{R}, \mathfrak{o}; \mathfrak{O}/\mathfrak{A})$ the totality of all derivations modulo $\mathfrak{A}$ in $\mathfrak{R}$ which map $\mathfrak{o}$ onto the null element of $\mathfrak{O}/\mathfrak{A}$.

THEOREM 1. *Let* $\mathfrak{A}=\prod_{i=1}^{t}\mathfrak{P}_i^{e_i}$ *be the prime ideal decomposition of an ideal* $\mathfrak{A}$ *in* $\mathfrak{O}$. *Then we have a direct decomposition*:

1) The numbers in square brackets refer to the list of references at the end of this note.

2) See E. Hecke [1] 131-132.

$$\mathfrak{D}(\mathfrak{R}, \mathfrak{o}; \mathfrak{O}/\mathfrak{A}) \cong \sum_{i=1}^{t} \oplus \mathfrak{D}(\mathfrak{R}, \mathfrak{o}; \mathfrak{O}/\mathfrak{P}_i^{e_i}).$$

PROOF. See Y. Kawada [1] 308 Lemma 8.

LEMMA 1. *Let* $\mathfrak{A}, \mathfrak{B}$ *be ideals in* $\mathfrak{O}$ *and* $\mathfrak{A} \supseteqq \mathfrak{B}$. *Then* $\mathfrak{D}(\mathfrak{R}, \mathfrak{o}; \mathfrak{O}/\mathfrak{A})$ *is* $\mathfrak{O}$*-isomorphically mapped into* $\mathfrak{D}(\mathfrak{R}, \mathfrak{o}; \mathfrak{O}/\mathfrak{B})$.

PROOF. See Y. Kawada [1] 307 Lemma 7.

LEMMA 2. *Let* ξ *be an element in* $\mathfrak{O}$ *with the canonical defining equation* $\varphi(x)=0$[1] *in* $\mathfrak{o}$, *and let* $\mathfrak{o}[\xi]$ *be the ring of all polynomials of* ξ *with coefficients in* $\mathfrak{o}$. *Then, a necessary and sufficient condition in order that there exist a derivation* $D \in \mathfrak{D}(\mathfrak{o}[\xi], \mathfrak{o}; \mathfrak{O}/\mathfrak{A})$ *with* $D(\xi) \ni \lambda (\lambda \in \mathfrak{O})$ *is that the congruence*

$$\varphi'(\xi)\lambda \equiv 0 \pmod{\mathfrak{A}}$$

holds where $\varphi'(x)$ *denotes the derivative of* $\varphi(x)$ *by* x.

PROOF. This proof is easy by using properties of $\mathfrak{D}(\mathfrak{o}[\xi], \mathfrak{o}; \mathfrak{O}/\mathfrak{A})$ and A. Weil [2] 12 Proposition 15.

THEOREM 2. *Let* $\mathfrak{P}$ *be a prime ideal and* r *an arbitrary positive integer. Then,* $\mathfrak{D}(\mathfrak{o}[\xi], \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$ *is* $\mathfrak{O}$*-isomorphically mapped into* $\mathfrak{O}/(\varphi'(\xi))_{\mathfrak{P}}$ *where* $\varphi'(\xi)$ *has the same meaning as in Lemma 2 and* $(\varphi'(\xi))_{\mathfrak{P}}$ *denotes the* $\mathfrak{P}$*-component of the principal ideal* $(\varphi'(\xi))$ *in* $\mathfrak{O}$.

PROOF. (1) $\mathfrak{P}^r \subseteqq (\varphi'(\xi))_{\mathfrak{P}}$. In this case, the totality of all elements in $\mathfrak{O}$ which satisfy the congruence

$$\varphi'(\xi)\lambda \equiv 0 \pmod{\mathfrak{P}^r}$$

forms the ideal $\mathfrak{P}^r(\varphi'(\xi))_{\mathfrak{P}}^{-1}$. Now we may choose an element λ_0 such that $\varphi'(\xi)\lambda_0 \equiv 0 \bmod \mathfrak{P}^r$ and $\varphi'(\xi)\lambda_0 \not\equiv 0 \bmod \mathfrak{P}^{r+1}$. Then there exists for every solution λ of $\varphi'(\xi)\lambda \equiv 0 \bmod \mathfrak{P}^r$ an element μ in $\mathfrak{O}$ such that $\lambda \equiv \lambda_0\mu \bmod \mathfrak{P}^r$.

Let D_0 be a derivation in $\mathfrak{D}(\mathfrak{o}[\xi], \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$ with $D_0(\xi) \ni \lambda_0$. Then, by Lemma 2, $D=\mu D_0$ defines clearly the derivation $D(\xi) \ni \lambda$. Derivations $D=\mu D_0$ and $D'=\mu' D_0$ define the same derivation if and only if $\mu \equiv \mu' \bmod (\varphi'(\xi))_{\mathfrak{P}}$. Therefore, we obtain the $\mathfrak{O}$-isomorphic relation

$$\mathfrak{D}(\mathfrak{o}[\xi], \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r) \cong \mathfrak{O}/(\varphi'(\xi))_{\mathfrak{P}}.$$

(2) $\mathfrak{P}^r \supseteqq (\varphi'(\xi))_{\mathfrak{P}}$. By Lemma 1, $\mathfrak{D}(\mathfrak{o}[\xi], \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$ is $\mathfrak{O}$-isomorphically mapped into $\mathfrak{D}(\mathfrak{o}[\xi], \mathfrak{o}; \mathfrak{O}/(\varphi'(\xi)_{\mathfrak{P}})$, and, since by (1)

$$\mathfrak{D}(\mathfrak{o}[\xi], \mathfrak{o}; \mathfrak{O}/(\varphi'(\xi))_{\mathfrak{P}}) \cong \mathfrak{O}/(\varphi'(\xi))_{\mathfrak{P}},$$

1) $\varphi(x)$ is irreducible in $\mathfrak{o}[x]$ with the heighest coefficient 1 and $\varphi(\xi) = 0$.

$\mathfrak{D}(\mathfrak{o}[\xi], \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$ is $\mathfrak{O}$-isomorphically mapped into $\mathfrak{O}/(\varphi'(\xi))_{\mathfrak{P}}$.

COROLLARY. *The (set-theoretically) greatest ideal modulus* $\mathfrak{P}^r$ *for which* $\mathfrak{D}(\mathfrak{o}[\xi], \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r) \cong \mathfrak{O}/(\varphi'(\xi))_{\mathfrak{P}}$ *is* $(\varphi'(\xi))_{\mathfrak{P}}$.

It has been proved that for an ideal $\mathfrak{A}$ in $\mathfrak{O}$ the number of derivations in $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{A})$ is bounded[1]; this number is called the *dimension* of $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{A})$. Further, there exists the (set-theoretically) greatest ideal $\mathfrak{D}_0$ in $\mathfrak{O}$ such that $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{D}_0)$ has the maximal dimension. The ideal $\mathfrak{D}_0$ is called by A. Weil and Y. Kawada the *relative different* of K/k.

However, on the other hand, we know the *relative different* $\overline{\mathfrak{D}}$ of K/k defined by R. Dedekind. $\overline{\mathfrak{D}}$ is an ideal in $\mathfrak{O}$ such that $\overline{\mathfrak{D}}^{-1}=\{\mu;\ \mu \in K\}$ with $S_{K/k}(\mu\omega) \in \mathfrak{o}$ for every element ω in $\mathfrak{O}$ where $S_{K/k}(\quad)$ means the trace of an element in K with respect to k.

Let $\psi(x)=0$ be the canonical defining equation of an element α in $\mathfrak{O}$. Then $\psi'(\alpha)$—the different of α—is divisible by $\overline{\mathfrak{D}}$ and, moreover, $\overline{\mathfrak{D}}$ is the greatest common divisor of differents of all elements in $\mathfrak{O}$.

Now we shall prove the following theorem.

THEOREM 3. *Let* $\mathfrak{P}$ *be an arbitrary prime ideal in* $\mathfrak{O}$ *and* r *an arbitrary positive integer. Then there exists an integral primitive element* θ *of* K/k *such that the* $\mathfrak{O}$*-isomorphic relation*

$$\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r) \cong \mathfrak{D}(\mathfrak{o}[\theta], \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$$

holds.

PROOF. It is well-known that one can choose an integral primitive element θ such that for every element $\gamma \in \mathfrak{O}$ and for an arbitrary positive integer ν the congruence[2]

$$\gamma \equiv \gamma_\nu^* \pmod{\mathfrak{P}^\nu} \quad \gamma_\nu^* \in \mathfrak{o}[\theta]$$

holds and the ideal $(f'(\theta))\overline{\mathfrak{D}}^{-1}=\mathfrak{F}$ is prime to $\mathfrak{P}$ where $f(x)=0$ is the canonical defining equation of θ in $\mathfrak{o}$ and $\overline{\mathfrak{D}}$ is the relative different of K/k.

We shall show $D(\gamma)=0$ if $\gamma \in \mathfrak{P}^{r+1}$. For this purpose, we take a prime element Π of $\mathfrak{P}$. Then, γ is expressible in the form

$$\gamma = \Pi^{r+1}\frac{\mathfrak{A}}{\mathfrak{B}} \quad (\mathfrak{B}, \mathfrak{P}) = 1$$

where $\mathfrak{A}$, $\mathfrak{B}$ are ideals in $\mathfrak{O}$. Obviously, we can choose an ideal $\mathfrak{C}$ prime

1) See Y. Kawada [1] 308 Theorem 5.
2) See E. Hecke [1] 136 Hilfssatz c).

to $\mathfrak{P}$ such that $\mathfrak{BC}$ is a principal ideal (β) in $\mathfrak{O}$. Therefore we can put for some $\alpha \in \mathfrak{O}$

$$\gamma = \Pi^{r+1}\frac{\alpha}{\beta} \quad (\beta, \mathfrak{P}) = 1 .$$

Hence it follows

$$D(\beta\gamma) = \beta D(\gamma) + \gamma D(\beta) = (\gamma+1)\Pi^r \alpha D(\Pi) + \Pi^{r+1} D(\alpha) = 0 ;$$

since $\gamma D(\beta)=0$ and $(\beta, \mathfrak{P})=1$ we have

$$D(\gamma) = 0 .$$

1) Since $\mathfrak{o}[\theta]$ is a subring of $\mathfrak{O}$ every derivation D in $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$ induces the unique derivation D^* in $\mathfrak{D}(\mathfrak{o}[\theta], \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$. Putting for an arbitrary $\gamma \in \mathfrak{O}$ $\gamma=\gamma_0^* + \xi$ $(\gamma_0^* \in \mathfrak{o}[\theta], \xi \in \mathfrak{P}^{r+1})$, we obtain

$$D(\gamma) = D(\gamma_0^*) + D(\xi) = D(\gamma_0^*) = D^*(\gamma_0^*) ,$$

because $D(\xi)=0$. If $D(\gamma)\neq 0$, it follows obviously $D^*(\gamma_0^*)\neq 0$. Hence, by the correspondence $D \to D^*$, $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$ is $\mathfrak{O}$-isomorphically mapped into $\mathfrak{D}(\mathfrak{o}[\theta], \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$.

2) Conversely, let D^* be a derivation in $\mathfrak{D}(\mathfrak{o}[\theta], \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$ and let ξ^* be an element in $\mathfrak{o}[\theta]$ divisible by $\mathfrak{P}^{r+1}$. Then, since for a prime element Π of $\mathfrak{P}$ in $\mathfrak{O}$ there exists an element Π_0 in $\mathfrak{o}[\theta]$ with $\Pi \equiv \Pi_0 \bmod \mathfrak{P}^2$, Π_0 is also a prime element of $\mathfrak{P}$. As above proved, there exist α, β in $\mathfrak{O}$ such that $\beta\xi^* = \Pi_0^{r+1}\alpha$ with $(\beta, \mathfrak{P})=1$.

Since we can choose in the ideal $\mathfrak{F}$ an element η prime to $\mathfrak{P}$, $\alpha\eta$ and $\beta\eta$ belong to $\mathfrak{o}[\theta]$. Hence, it follows obviously

$$\eta\beta D^*(\xi^*) = 0$$

so that $D^*(\xi^*)=0$. Now, put for an arbitrary $\gamma \in \mathfrak{O}$

$$\gamma = \gamma_0^* + \xi \qquad \gamma_0^* \in \mathfrak{o}[\theta] , \quad \xi \in \mathfrak{P}^{r+1}$$

and define

$$D(\gamma) = D^*(\gamma_0^*) .$$

If we have $\gamma = \gamma_0^{*\prime} + \xi'$ with $\gamma_0^{*\prime} \in \mathfrak{o}[\theta]$ and $\xi' \in \mathfrak{P}^{r+1}$ then $\xi - \xi' = \gamma_0^{*\prime} - \gamma_0^* \in \mathfrak{o}[\theta]$ and $(\gamma_0^{*\prime} - \gamma_0^*) \in \mathfrak{P}^{r+1}$. Therefore, we obtain

$$D^*(\gamma_0^{*\prime}) - D^*(\gamma_0^*) = D(\xi - \xi') = 0$$

so that

$$D(\gamma) = D^*(\gamma_0^*) = D^*(\gamma_0^{*\prime}) .$$

Thus, D is uniquely determined by D^*. It is not difficult to see that

D is a derivation in $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$. Clearly, by definition, D induces D^* in $\mathfrak{D}(\mathfrak{o}[\theta], \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$. By 1) and 2), $\mathfrak{O}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$ is $\mathfrak{O}$-isomorphic to $\mathfrak{D}(\mathfrak{o}[\theta], \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$.

LEMMA 3. *If θ is taken as in proof of Theorem 3, then the $\mathfrak{P}$-component $\overline{\mathfrak{D}}_{\mathfrak{P}}$ of $\overline{\mathfrak{D}}$ coincides with that of $(f'(\theta))$. The maximal dimension of $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^i)$ $(i=0, 1, 2, \ldots\ldots)$ is the absolute value of the absolute norm $N\overline{\mathfrak{D}}_{\mathfrak{P}}$ of $\overline{\mathfrak{D}}_{\mathfrak{P}}$ and the greatest ideal modulus $\mathfrak{P}^r$ for which $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$ gives the maximal dimension $|N\overline{\mathfrak{D}}_{\mathfrak{P}}|$ is equal to $\overline{\mathfrak{D}}_{\mathfrak{P}}$.*

PROOF. By Theorem 2, the dimension of $\mathfrak{D}(\mathfrak{o}[\theta], \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^i)$ $(i=0, 1, 2, \ldots\ldots)$ is not greater than $|N(f'(\theta))_{\mathfrak{P}}|$, and, by Corollary of Theorem 2, the greatest ideal modulus $\mathfrak{P}^r$ for which $\mathfrak{D}(\mathfrak{o}[\theta], \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$ gives the maximal dimension $|N(f'(\theta))_{\mathfrak{P}}|$ is equal to $(f'(\theta))_{\mathfrak{P}}$.

Since, by assumption, $(f'(\theta))\overline{\mathfrak{D}}^{-1}$ is prime to $\mathfrak{P}$, then $(f'(\theta))_{\mathfrak{P}}=\overline{\mathfrak{D}}_{\mathfrak{P}}$. From Theorem 3 it follows that $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{D}_{\mathfrak{P}})$ has the maximal dimension $|N\overline{\mathfrak{D}}_{\mathfrak{P}}|$ and $\overline{\mathfrak{D}}_{\mathfrak{P}}$ is the greatest ideal modulus among the $\mathfrak{P}^r$'s for which the $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{P}^r)$'s have the maximal dimension.

REMARK. If $\mathfrak{Q}$ is no prime ideal divisor of $\overline{\mathfrak{D}}$, then, by Lemma 3, the maximal dimension of $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{Q}^r)$ $(r=1, 2, \ldots\ldots)$ is equal to 1.

THEOREM 4. *The relative different $\mathfrak{D}_0$ of K/k in the sense of A. Weil and Y. Kawada coincides with the relative different $\overline{\mathfrak{D}}$ defined by R. Dedekind.*

PROOF. Let $\mathfrak{D}_0=\mathfrak{P}_1^{e_1}\ldots\ldots\mathfrak{P}_t^{e_t}$ be the prime ideal decomposition of $\mathfrak{D}_0$. Then, by Theorem 1,

$$\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{D}_0) \cong \sum_{i=1}^{t} \oplus \mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{P}_i^{e_i}).$$

Since the dimension of $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{D}_0)$ is maximal, then for each $i(1\leqq i\leqq t)$ $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{P}_i^{e_i})$ is to have the maximal dimension $|N\overline{\mathfrak{D}}_{\mathfrak{P}_i}|$ (by Lemma 3). On the other hand, $\overline{\mathfrak{D}}_{\mathfrak{P}_i}$ is the greatest ideal modulus such that the dimension of $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{P}_i^r)$'s is equal to $|N\overline{\mathfrak{D}}_{\mathfrak{P}_i}|$. By definition, it must be

$$\mathfrak{D}_0 = \prod_{i=1}^{t} \overline{\mathfrak{D}}_{\mathfrak{P}_i}.$$

Let $\mathfrak{P}$ be a prime ideal divisor of $\overline{\mathfrak{D}}$ which is different from $\mathfrak{P}_i$ $(i=1, 2, \ldots\ldots, t)$. Then, by Lemma 3, the dimension of $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\overline{\mathfrak{D}}_{\mathfrak{P}})\geqq 2$ and $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{D}_0\overline{\mathfrak{D}}_{\mathfrak{P}})$ has a greater dimension than that of $\mathfrak{D}(\mathfrak{O}, \mathfrak{o}; \mathfrak{O}/\mathfrak{D}_0)$ but this gives a contradiction. Hence, it must be

$$\overline{\mathfrak{D}} = \prod_{i=1}^{t} \overline{\mathfrak{D}}_{\mathfrak{P}_i} = \mathfrak{D}_0, \quad \text{q. e. d.}$$

In conclusion I wish to express my sincere thanks to Professor M. Moriya for his kind guidance.

References

E. HECKE [1] Vorlesungen uber die Theorie der algebraischen Zahlen, Leipzig, (1923) 131-136.

Y. KAWADA [1] *On the derivations in number fields*, Ann. of Math. **54** (1951), 302-310.

A. WEIL [1] *Differentiation in algebraic number fields*, (Abstract), Bull. Amer. Math. Soc., **49** (1943), 41.

A. WEIL [2] Foundations of algebraic geometry, New York, (1946), 11-16.

DEPARTMENT OF MATHEMATICS,
HIROSHIMA UNIVERSITY.