ON A THEOREM OF A. WEIL

ON DERIVATIONS IN NUMBER FIELDS

BY

W. NARKIEWICZ (WROCŁAW)

Let $L/K$ be a finite extension of an algebraic number field $K$, and let $R_L$ and $R_K$ be the rings of integers in $L$ and $K$, respectively. Let $I$ be an ideal in $R_L$. A mapping $D: R_L \to R_L/I$ is said to be an $I$-derivation over $K$ if it satisfies the following conditions:

$$D(x+y) = D(x) + D(y), \quad D(xy) = xD(y) + yD(x)$$

and

$$D(x) = 0 \quad \text{for } x \in R_K.$$

An $I$-derivation $D$ over $K$ is said to be essential if its image contains at least one element which is not a zero-divisor.

In [2] A. Weil stated without proof the following

**Theorem.** An ideal $I$ divides the different of the extension $L/K$ if and only if there exists an essential $I$-derivation over $K$.

A proof of this theorem was given by Kawada [1] with the use of $p$-adic considerations. The purpose of this note is to give a proof which does not use $p$-adicities.

**Proof.** Observe first that it suffices to prove the result for powers of prime ideals only. In fact, if $I = P_1^{q_1} \cdots P_t^{q_t}$ and there exists an essential $I$-derivation over $K$, then there exist also $P_i^{q_i}$-derivations over $K$ which are essential, namely those defined by $D_i(x) \equiv D(x) \pmod{P_i^{q_i}}$, $i = 1, 2, \ldots, t$. Conversely, if $D_i(x)$, $i = 1, 2, \ldots, t$, are essential $P_i^{q_i}$-derivations over $K$, and $y(x) \equiv D_i(x) \pmod{P_i^{q_i}}$, then putting $D(x) \equiv y(x) \pmod{I}$ one obtains an essential $I$-derivation over $K$.

So assume that $D$ is an essential $P^m$-derivation over $K$. Observe first that $a - b \in P^{m+1}$ implies $D(a) = D(b)$. In fact, if $x \in P^{m+1}$ and $t \notin P$, then $x = t^{m+1}A/B$ with $A, B \in R_L$ and $B \notin P$, whence $Bx = At^{m+1}$, which implies

$$BD(x) + xD(B) = (1 + m)t^{m}D(t)A + t^{1+m}D(A),$$
and so $BD(x) = 0$, whence $D(x) = 0$. By the linearity of $D$ our observation follows.

Now let $a$ be chosen in such a way that $P$ does not divide the conductor of $R_K[a]$, and every number from $R_L$ is congruent to a number from $R_K[a] \pmod{P^{m+1}}$. If $b \equiv V(a) \pmod{P^{m+1}}$, then $D(b) = D(V(a)) = V'(a)D(a)$. Note that $D(a)$ cannot be a zero-divisor as otherwise by the last equality we would infer that $D(b)$ is a zero-divisor for every $b$, against our assumption. If now $f(X)$ is the minimal polynomial for $a$ over $K$, then from $f(a) = 0$ we easily obtain $f'(a)D(a) = 0$, thus $f'(a) \equiv 0 \pmod{P^m}$, and so $P^m$ divides the different of the extension $L/K$.

To prove the converse implication assume that $P^m$ divides the different, and choose $a \in R_L$ in such a way that $P$ does not divide the conductor $f$ of $R_K[a]$. Let $b \in f, b \notin P$. Let $V(X)$ be a polynomial over $R_K$ such that $V(a) = b$, and define $c$ as the residue class $\pmod{P^m}$ satisfying $cV(a) \equiv 1 \pmod{P^m}$. Every number from $R_L$ can be put in the form

$$x = F(a)/V(a)$$

with $F(X) \in R_K[X]$. We define now the mapping $D : R_L \to R_L/P^m$ by means of

$$D(x) \equiv (F'(a)V(a) - F(a)V'(a))c^a \pmod{P^m}.$$ 

This is well-defined, as $F(a)/V(a) = F_1(a)/V(a)$ easily implies the equality $F'(a) \equiv F_1'(a) \pmod{P^m}$.

The linearity of $D$ is evident, the equality $D(xy) = xD(y) + yD(x)$ follows by a simple calculation. Moreover,

$$D(a) = D(aV(a)/V(a)) \equiv \left(\left(V(a) + aV'(a) \right)V(a) - aV(a)V'(a)\right)c^a$$

$$\equiv 1 \pmod{P^m}$$

and so $\text{Im}D$ contains 1. Finally, $D(x) = 0$ for $x \in R_K$, whence $D$ is an essential $P^m$-derivation over $K$, as needed.

REFERENCES


INSTITUTE OF MATHEMATICS OF THE WROCLAW UNIVERSITY

*Reçu par la Rédaction le 14.11.1967*