J. Sci. HIROSHIMA UNIV. SER. A-I
34 (1970), 17-27

High Order Derivations II.

Yoshikazu NAKAI, Kôtaro KOSAKI and Yasunori ISHIBASHI

(Received February 20, 1970)

This is a suite of the previous paper [3]. In that paper the senior author developed the fundamental calculus on high order derivations and proved some functorial properties of high order differentials. In this paper we shall apply these results to the theory of fields, in particular to a purely inseparable field extension of finite exponent. In §1 it will be shown that a purely inseparable extension of finite degree over a field K will be characterized by the fact that the derivation algebra $\mathcal{D}(L/K)$ coincides with the endomorphismring of L over K. If L is an extension of infinite degree over K this is not the case. But when L is of finite exponent over K we can introduce a suitable topology so as to get a bijective correspondence between the intermediate fields of L and K and the closed subrings of $\mathcal{D}(L/K)$ containing L. §3 is devoted to the representation theory of high order derivations. In the case of characteristic $p(>0)$ the high derivations of orders $1, p, p^2, \cdots$ are fundamental while in the case of characteristic zero every high order derivation can be represented as the sum of products of ordinary derivations.

Notations and terminologies: Let k and A be commutative rings such that A is a k-algebra and let M be an A-module. The set of q-th order derivations of A/k into M will be denoted by $\mathcal{D}_0^{(q)}(A/k, M)$. $\mathcal{D}_0^{(q)}(A/k, M)$ has a natural structure of left A-module. When $M=A$ we shall use the notation $\mathcal{D}_0^{(q)}(A/k)$ instead of $\mathcal{D}_0^{(q)}(A/k, A)$. We shall set $\mathcal{D}_0(A/k)=\bigcup_{q=1}^{\infty}\mathcal{D}_0^{(q)}(A/k)$. The derivation algebra $\mathcal{D}(A/k)$ is the direct sum of homotheties by elements of A and $\mathcal{D}_0(A/k)$, i.e., $\mathcal{D}(A/k)=A\oplus\mathcal{D}_0(A/k)$. $\mathcal{D}(A/k)$ is a subring of $\mathrm{Hom}_k(A, A)$. The module of q-th order differentials of A over k will be denoted by $\Omega_k^{(q)}(A)$ and the canonical q-th order derivation will be denoted by $\delta_{A/k}^{(q)}$. $\Omega_k^{(q)}(A)$ is a representing module for the functor $\mathcal{D}_0^{(q)}(A/k)$. Let B be an A-algebra. Then we have the canonical homomorphism $B\otimes_A\Omega_k^{(q)}(A)\to\Omega_k^{(q)}(B)$. The cokernel of this homomorphism will be denoted by $\Omega_k^{(q)}(B/A)$. The readers are expected to refer the paper [3] for details. In this paper we shall make frequent use of the results in [3] and the Proposition (or Theorem) 12 of Chapter I in [3], for example, will be quoted as I-12.

§ 1. Structure theorems for derivation algebras

Let k and A be commutative rings such that A is a k-algebra. Let φ be the contraction homomorphism $A\otimes_k A\to A$ and let I be the kernel of φ. We endow $A\otimes_k A$ with a structure of A-module by $a(b\otimes c)=ab\otimes c$. Then the exact sequence of A-modules

$$0\longrightarrow I\longrightarrow A\otimes_k A\xrightarrow{\varphi} A\longrightarrow 0$$

splits since there exists an A-homomorphism of A into $A\otimes A$ such that $\psi(a)=a\otimes 1$. Identifying A with $\psi(A)$ we have a direct sum decomposition $A\otimes_k A=A\oplus I$. Hence there exists a canonical isomorphism of A-modules

$$A\otimes_k A/I^{n+1}\cong A\oplus I/I^{n+1}\cong A\oplus\Omega_k^{(n)}(A).$$

These consideration yields at once the

PROPOSITION 1. *There is a canonical isomorphism of left A-modules:*

$$\tau\colon \mathrm{Hom}_A(A\otimes_k A/I^{n+1},\ M)\cong M\oplus\mathcal{D}_0^{(n)}(A/k,\ M)$$

where M is an arbitrary A-module. If f is an element of $\mathrm{Hom}_A(A\otimes_k A/I^{n+1},$ $M)$, *then* $\tau(f)=f(1)+\tau_0(f)$ *where* $\tau_0(f)(\delta_{A/k}^{(n)}(a))=f(1\otimes a-a\otimes 1)$.

COROLLARY 1. 1. *Let us assume that A is a purely inseparable extension of finite degree of a field k. Then we have the canonical isomorphism $\mathcal{D}(A/k)\cong\mathrm{Hom}_A(A\otimes_k A,\ A)$.*

PROOF. Under the assumption $A\otimes_k A$ is an artinian local ring with the maximal ideal I. Hence I is nilpotent and we have $D_0^{(n)}(A/k)=D_0(A/k)$ for large n.

In the sequel we shall denote by L and K two fields of characteristic p such that $L\supset K$.

THEOREM 2. *Assume that L is a purely inseparable extension of finite exponent e over K and let x be an element of L not contained in K. Then there exists a high order derivation D of order p^{e-1} of L/K such that $D(x)\neq 0$.*

PROOF. By assumption we have $K\subset L\subset K^{p^{-e}}$. Let $\{x_\lambda,\ \lambda\varepsilon\Lambda\}$ be a p-basis of $K^{p^{-e}}$ over $K^{p^{-e+1}}$. Then we have $K^{p^{-e}}=\bigotimes_{\lambda\varepsilon\Lambda}K(x_\lambda)$. Let x be a given element of L and let f be the exponent of $x(f\leq e)$. Then $x_0=x^{f-e}$ is an element of $K^{p^{-e}}$ and of exponent e. We can supplement x_0 to a p-basis of $K^{p^{-e}}$ over $K^{p^{-e+1}}$ and hence we can assume that x_0 is a member of a p-basis $\{x_\lambda,$ $\lambda\varepsilon\Lambda\}$. In particular we see that there exists a field F such that $F(x_0)=K^{p^{-e}}$ and $[F(x_0)\colon F]=p^e$. Let us set $q=p^{e-1}$. Then $\Omega_F^{(q)}(F(x_0))$ is a free module with the basis $\delta(x_0),\ \delta(x_0^2),\dots,\ \delta(x_0^q)$ by II–15 where $\delta=\delta_{F(x_0)/F}^{(q)}$. We have then $\delta(x)=\delta(x_0^{p^{e-f}})\neq 0$ and there exists a p^{e-1}-th order derivation $\hat{D}$ of $K^{p^{-e}}$ over F (hence over K). The restriction of $\hat{D}$ to L gives rise to an element

Δ of $\mathcal{D}_0^{(p^{e-1})}(L/K, K^{p^{-e}})$ such that $\Delta(x) \neq 0$. Hence we must have $\delta_{L/K}^{(p^{e-1})}(x) \neq 0$. From this we immediately get the assertion.

Remark 1. If the exponent is not finite there could exist an element x of L not contained in K such that for any high order derivation D of L/K we have $D(x)=0$. Take for example $K=k(x)$, a purely transcendental extension of k, and let $L=K^{p^{-\infty}}$. Then $x^{p^{-1}} \notin K$ and if D is of order n $D(x^{p^{-1}}) = D((x^{p^{-n-1}})^{p^n}) = 0$ by I–7.1.

Remark 2. Theorem 1 implies among others that the notion of high order derivation is much broader than that of higher derivation. In fact let L be a purely inseparable extension of K which is not modular over K. Let F be the field of constants for higher derivations of L over K. Then by [5], F is strictly bigger than K. Let x be an element of F not contained in K. Then a high order derivation D of L/K such that $D(x) \neq 0$ can not be a component of any higher derivation of L/K.

Theorem 3. *Let L and K be as in Theorem 2. Then the center of $\mathcal{D}(L/K)$ is equal to K.*

Proof. It is clear that K is contained in the center of $\mathcal{D}(L/K)$. Conversely let $a+\Delta(a \in L, \Delta \in \mathcal{D}_0^{(n)}(L/K))$ be a central element of $\mathcal{D}(L/K)$. Then first we must have $\Delta x = x\Delta$ for any x in L, thence we have $\Delta(x)=0$ for any x in L, i.e. $\Delta=0$. Theorem 3 now follows from Theorem 2, since an element x of L can be a central element of $\mathcal{D}(L/K)$ only when $\Delta(x)=0$ for any high order derivation Δ. q.e.d.

Let $\mathfrak{A}$ be a subring of $\mathcal{D}(L/K)$. Henceforce we shall denote by $Z(\mathfrak{A})$ the center of $\mathfrak{A}$.

Theorem 4. *Let L be a purely inseparable extension of finite degree over K. Then we have $\mathcal{D}(L/K) \cong \mathrm{Hom}_K(L, L)$.*

Proof. By definition $\mathcal{D}(L/K)$ is a subring of $\mathrm{Hom}_K(L, L)$. By Corollary 1.1 we have $\mathcal{D}(L/K) \cong \mathrm{Hom}_L(L \otimes_K L, L) \cong \mathrm{Hom}_K(L, L)$ as left L-modules. Hence $\mathcal{D}(L/K)$ has the same dimension as $\mathrm{Hom}_K(L, L)$ and we must have the assertion. q.e.d.

This property of $\mathcal{D}(L/K)$ characterizes a purely inseparable extension of finite degree. In fact we have

Theorem 5. *Let L be a finite extension of K. Then L is a purely inseparable extension of K if and only if $[\mathcal{D}(L/K): L] = [L: K]$.*

Proof. Let K_s be the separable closure of K in L. Then as will be seen in the following proposition we have $\mathcal{D}(L/K) = \mathcal{D}(L/K_s)$. By Theorem 4 we know that $[\mathcal{D}(L/K_s): L] = [L: K_s]$. Hence the assumption implies that $K = K_s$, i.e., L is a purely inseparable extension of K.

PROPOSITION 6. *Let K_s be the separable closure of K in L. Then we have* $\mathcal{D}(L/K_s) = \mathcal{D}(L/K)$.

PROOF. As is well known $\Omega_K^{(1)}(K_s) = 0$. From this we easily deduce that $\Omega_K^{(n)}(K_s) = 0$ for any $n \geq 1$. It follows from II-12, (3) $\Omega_K^{(n)}(L) \cong \Omega_{K_s}^{(n)}(L)$ for $n \geqq 1$. The assertion then follows immediately.

§ 2. A purely inseparable extension of finite exponent

In this paragraph we shall assume that L is a purely inseparable extension of finite exponent e over a field K.

In this case $\mathcal{D}(L/K)$ cannot be a finite dimensional vector space, so we shall introduce a suitable topology. Since $\mathcal{D}(L/K)$ is a subring of $\mathrm{Hom}_K(L, L)$ we shall introduce first in the latter set the following topology which we shall refer to as the Krull topology in the sequel.

DEFINITION. *Let E be an intermediate field of L and K such that $[E: K] < \infty$. Then the fundamental system of neighborhoods of zero consists of the set of the element f in* $\mathrm{Hom}_K(L, L)$ *such that* $f|E = 0$.

In other words, two elements f, g of $\mathrm{Hom}_K(L, L)$ are said to be near if and only if there exist finite elements $x_1, \cdots, x_n$ of L such that $f(x_i) = g(x_i)$, $i = 1, 2, \cdots, n$. With this topology $\mathrm{Hom}_K(L, L)$ becomes a topological ring as one can see easily.

THEOREM 7. *Let L be a purely inseparable extension of finite exponent e. Let $\mathfrak{A}$ be a subring of* $\mathrm{Hom}_K(L, L)$ *containing L such that $Z(\mathfrak{A}) = K$. Then $\mathfrak{A}$ is a dense subset of* $\mathrm{Hom}_K(L, L)$. *In particular $\mathcal{D}(L/K)$ is a dense subspace of* $\mathrm{Hom}_K(L, L)$.

For the proof we need the following.

DENSITY THEOREM. *Let A be a ring and let M be a semi-simple left A-module and b an element of bicommutant B of M. Then for every finite set of elements $x_1, x_2, \cdots, x_n$ of M there exists an element a of A such that $ax_i = bx_i$ for $i = 1, 2, \cdots, n$.*

For the proof we refer to [1], Chap. 8, §4, $n^\circ 2$.

PROOF OF THEOREM. 7. We view L as a left $\mathfrak{A}$-module and we shall find its commutant C and bicommutant B. By our assumption the homotheties by elements of L are contained in $\mathfrak{A}$. Hence L is a simple $\mathfrak{A}$-module, and an element c of C must be an L-linear endomorphism of L. This implies that c is a homothety by an element of L and we can consider c as an element of L. Then the assumption $Z(\mathfrak{A}) = K$ implies that c is contained in K, hence, $C = K$.

The bicommutant B is then equal to $\mathrm{Hom}_K(L, L)$. The assertion now follows immediately from Density Theorem. The last assertion is a consequence of Theorem 3 that we have $Z(\mathfrak{D}(L/K)) = K$.

REMARK 3. When L is of finite degree over K, the topology introduced above is discrete. Hence we have again $\mathfrak{D}(L/K) = \mathrm{Hom}_K(L, L)$ (cf. Theorem 4)

PROPOSITION 8. *Let L and K be as in Theorem 7 and let F be an intermediate field of L and K. Then $\mathrm{Hom}_F(L, L)$ is closed in $\mathrm{Hom}_K(L, L)$.*

PROOF. Let f be an element adherent to $\mathrm{Hom}_F(L, L)$. We have to show that f is an element of $\mathrm{Hom}_F(L, L)$. Let a, x be arbitrary but fixed elements of F and L respectively. Then there exists an element g in $\mathrm{Hom}_F(L, L)$ such that $f = g$ on the subfield $K(x, ax)$. Then we have $f(ax) = g(ax) = ag(x) = af(x)$, i.e., f is F-linear. q.e.d.

We are now well prepared to establish a Galois correspondence between intermediate fields of L/K and the closed subrings of $\mathfrak{D}(L/K)$ containing L.

THEOREM 9. *Let L be a purely inseparable extension of finite exponent over K. If we endow $\mathfrak{D}(L/K)$ with the Krull topology we have a bijective correspondence between intermediate fields of L/K and closed subrings of $\mathfrak{D}(L/K)$ containing L. The corresponding intermediate field F and the subring $\mathfrak{A}$ are related by the formula*

$$F = Z(\mathfrak{A}), \qquad \mathfrak{A} = \mathfrak{D}(L/F).$$

PROOF. Assume a field F is given. Then $\mathfrak{D}(L/F) = \mathfrak{D}(L/K) \cap \mathrm{Hom}_F(L, L)$. Hence by Proposition 8, $\mathfrak{D}(L/F)$ is a closed subring of $\mathfrak{D}(L/K)$ and we have $Z(\mathfrak{D}(L/F)) = F$ by Theorem 3. Conversely let a closed subring $\mathfrak{A}$ (containing L) be given. It is easily seen that $Z(\mathfrak{A}) = F$ is a field between L and K. Moreover $\mathfrak{A} \subset \mathrm{Hom}_F(L, L)$ and is a dense subset of $\mathrm{Hom}_F(L, L)$ by Theorem 7. Hence $\mathfrak{A}$ is dense and closed in $\mathfrak{D}(L/K) \cap \mathrm{Hom}_F(L, L) = \mathfrak{D}(L/F)$ i.e., $\mathfrak{A} = \mathfrak{D}(L/F)$.

THEOREM 10. *Let L be a purely inseparable extension of finite exponent over K. Let $E_i (i = 1, 2)$ be intermediate fields of L and K. Then we have*

$$\mathfrak{D}(L/E_1 \cap E_2) = \mathfrak{D}(L/E_1) \cup \mathfrak{D}(L/E_2), \tag{1}$$

$$\mathfrak{D}(L/E_1 \cup E_2) = \mathfrak{D}(L/E_1) \cap \mathfrak{D}(L/E_2). \tag{2}$$

Conversely let $\mathfrak{A}_i$ $(i = 1, 2)$ be closed subrings of $\mathfrak{D}(L/K)$ containing L. Then we have

$$Z(\mathfrak{A}_1 \cap \mathfrak{A}_2) = Z(\mathfrak{A}_1) \cup Z(\mathfrak{A}_2), \tag{3}$$

$$Z(\mathfrak{A}_1 \cup \mathfrak{A}_2) = Z(\mathfrak{A}_1) \cap Z(\mathfrak{A}_2). \tag{4}$$

PROOF. (2) and (4) are immediate. (1) follows from (4) as follows. Let $\mathfrak{A}_i = \mathcal{D}(L/E_i)(i = i, 2)$. Then by (4), $Z(\mathfrak{A}_1 \cup \mathfrak{A}_2) = Z(\mathfrak{A}_1) \cap Z(\mathfrak{A}_2) = E_1 \cap E_2$. Hence by Theorem 9 $\mathcal{D}(L/E_1 \cap E_2) = \mathfrak{A}_1 \cup \mathfrak{A}_2$. Similarly (3) follows from (2). q.e.d.

In the following we shall give some applications of Theorem 7.

PROPOSITION 11. *Let L and K be as in Theorem 9, and let I be the kernel of the contraction homomorphism $L \otimes_k L \to L$. Then we have $\bigcap_{n=1}^{\infty} I^n = \{0\}$.*

Before we go to the proof we need

LEMMA 12. *Let M be a left L-subspace of $L \otimes L$. Then $\mathrm{Hom}_L(L \otimes_K L/M, L) = N$ is a closed subspace of $\mathrm{Hom}_K(L, L)$ where we identified $\mathrm{Hom}_K(L, L)$ with $\mathrm{Hom}_L(L \otimes_K L, L)$ by the isomorphism φ: $\mathrm{Hom}_L(L \otimes_K L, L) \cong \mathrm{Hom}_K(L, L)$ with $\varphi(f)(x) = f(1 \otimes x)$.*

PROOF. Let $f \in \mathrm{Hom}_K(L, L)$ and $f^* = \varphi^{-1}(f)$. Assume that $f \in \overline{\varphi(N)}$. We shall show $f^*(M) = 0$. Let $\sum_{i=1}^{n} x_i \otimes y_i$ be an arbitrary element of M. Then by definition $f \in \overline{\varphi(N)}$ implies the existence of an element $g \in \varphi(N)$ such that $f(y_i) = g(y_i) (i = 1, \cdots, n)$. Hence $f^*(\sum x_i \otimes y_i) = \sum x_i f(y_i) = \sum x_i g(y_i) = g^*(\sum x_i \otimes y_i) = 0$.

PROOF OF PROPOSITION 11. Let us set $M = \bigcap_{n=1}^{\infty} I^n$. By the identification φ defined above we have $\mathcal{D}(L/K) \subset \varphi(\mathrm{Hom}_L(L \otimes_k L/M, L)) \subset \mathrm{Hom}_K(L, L)$. Since $\mathcal{D}(L/K)$ is dense in $\mathrm{Hom}_K(L, L)$, $\varphi(\mathrm{Hom}_L(L \otimes_k L/M, L))$ is also dense in $\mathrm{Hom}_K (L, L)$. On the other hand this is closed by the previous Lemma. Hence we must have $\mathrm{Hom}_L(L \otimes_K L/M, L) = \mathrm{Hom}_L(L \otimes L, M)$. This implies that $M = 0$.

PROPOSITION 13. *Let L/K be a purely inseparable extension of finite exponent and let F be an intermediate field such that $[F: K] < \infty$ and let M be a finite L-module. Then any element D of $\mathcal{D}_0^{(n)}(F/K, M)$ can be extended to a high order derivation of L/K into M.*

PROOF. It suffices to show the case where $M = L$. Since F is a direct summand of L as a K-vector space D can be extended to an element f of $\mathrm{Hom}_K(L, L)$. Since $\mathcal{D}(L/K)$ is dense in $\mathrm{Hom}_K(L, L)$ and $[F: K] < \infty$ there exists an element Δ of $\mathcal{D}(L/K)$ such that $\Delta | F = f | F = D$. Δ is the desired extension.

REMARK 4. In general the order of extended high derivation should be much bigger than that of original high derivation. For instance if $K(x)$ is a rational function field over K an ordinary derivation of $K(x^p)$ over $K(x^{p^2})$ can be extended to a p-th order derivation of $K(x)$ over $K(x^{p^2})$, but not to an ordinary derivation.

§ 3. Generators of $\mathcal{D}_0^{(n)}(K/k)$.

In what follows most fields in consideration will be of characteristic p unless otherwise specified.

We shall first remind ourselves that if D is a q-th order derivation of K/k, then for any element α of kK^{p^i}, $[D, \alpha]$ is a high derivation of order $\leqq q-p^i$ by I-11. 2. In particular if $q \leq p^i$, we have $[D, \alpha]=0$. This implies among others that $D(\alpha a)=\alpha D(a)+aD(\alpha)$ for any $a \in K$.

LEMMA 14. *Let D be a q-th order derivation of K/k. If $q<p^i$, D is kK^{p^i}-linear.*

PROOF. For any element α of kK^{p^i} we have $[D, \alpha]=0$ and $D(\alpha)=0$ by I-10. Hence we have $D\alpha=\alpha D$.

Let K/k be a purely inseparable extension of finite degree and of exponent e. Let us consider a sequence of subfields

$$k \subset K_{e-1} \subset K_{e-2} \subset \cdots \subset K_1 \subset K,$$

where $K_i = kK^{p^i}$ $(i=1,\cdots, e-1)$. For convenience we set $K=K_0$, $k=K_e$.

We shall set

$$\mathcal{A}_i(K/k)=\{D \in \mathcal{D}_0^{(p^i)}(K/k) \mid D(K_i)=0\} \; (i=0, 1,\cdots, \mathrm{e}-1).$$

It should be noted that $\mathcal{A}_0=\{0\}$. We shall also set

$$\mathcal{G}_i(K/k)=\mathcal{D}_0^{(p^i)}(K/k)/\mathcal{A}_i(K/k) \; (i=0, 1,\ldots, e-1).$$

$\mathcal{A}_i(K/k)$, hence $\mathcal{G}_i(K/k)$ is a left vector space over K. When we speak of dimensions of $\mathcal{A}_i$, $\mathcal{G}_i$, etc., we mean the dimensions of left K-vector spaces $\mathcal{A}_i$, $\mathcal{G}_i$, etc.

PROPOSITION 15. *There exists an isomorphism of K-vector space $\mathcal{G}_i(K/k) \simeq \mathcal{D}_0^{(1)}(K_i/k, K)$. In particular $[\mathcal{G}_i(K/k): K]=\log_p[K_i: K_{i+1}]$.*

PROOF. Let D be an element of $\mathcal{D}_0^{(p^i)}(K/k)$. Then the restriction of D to K_i gives a K-module homomorphism of $\mathcal{D}_0^{(p^i)}(K/k)$ into $\mathcal{D}_0^{(1)}(K_i/k, K)$ with the kernel $\mathcal{A}_i$. Hence to prove the assertion it is necessary to show that every derivation of K_i/k into K is induced in this way and it suffices to show that every K_{i+1}-derivation Δ_0 of K_i into $K_{i+1}^{p^{-i}}$ can be extended to a p^i-th order derivation of $K_{i+1}^{p^{-i}}$ into $K_{i+1}^{p^{-i}}$. Let now $\{x_t\}_{1\leq t\leq s}$ be a p-basis of K_i/K_{i+1}. Let $\{z_t\}_{1\leq t\leq s}$ be elements of $K_{i+1}^{p^{-i}}$ such that $z_t^{p^{i-1}}=x_t (t=1,\cdots, s)$. Then we have $\bigotimes_{t=1}^{s} K_{i+1}(z_t) \otimes_{K_{i+1}} F \cong K_{i+1}^{p^{-i}}$ for a suitable field F, since $K_{i+1}^{p^{-i}}$ is modular over K_{i+1}. $K_{i+1}(z_t)$ is of exponent i over K_{i+1}. Let d_t be a p^i-th order derivation of $K_{i+1}^{p^{-i}}$ over K_{i+1} such that $ad_t = d_t a$ for any a in $\bigotimes_{t' \neq t} K_{i+1}(z_{t'}) \otimes F$, and $d_t(x_t) = \Delta_0(x_t)$, $d_t(x_t^2) = \Delta_0(x_t^2), \cdots, d_t(x_t^{p^i}) = \Delta_0(x_t^{p^i})$. The existence of such a high derivation is assured in II–15. It is easily seen that the p^i-th order derivation $\sum_{t=1}^{s} d_t$ answers the question.

Let $T = \{\Delta_1, \cdots, \Delta_s\}$ be a set of high order derivations of K/k. The set of K-linear combinations of the non-commutative monomials of $\Delta_1, \cdots, \Delta_s$ will be denoted by $K < T >$ or $K < \Delta_1, \cdots, \Delta_s >$. We say that $\mathcal{D}_0(K/k)$ is generated over K by $T = \{\Delta_1, \cdots, \Delta_s\}$ if we have $\mathcal{D}_0(K/k) = K < T >$.

PROPOSITION 16. *Let K/k be a finite purely inseparable extension of exponent e, $T^{(i)} = \{\Delta_j^{(p^i)}\}_{1 \leq j \leq s_i}$ be a set of high order derivations of K/k such that the residue class $\{\bar{\Delta}_j^{(p^i)}\}_{1 \leq j \leq s_i}$ forms a K-basis for $\mathcal{Q}_i(K/k)$ $(0 \leq i \leq e-1)$. Then $\mathcal{D}_0(K/k)$ is generated over K by $\{T^{(i)}, 0 \leq i \leq e-1\}$.*

PROOF. Since $\mathcal{D}_0^{(1)}(K/k) = \mathcal{D}_0^{(1)}(K/K_1)$ and K/K_1 is of exponent 1, $\mathcal{D}_0(K/K_1)$ is generated by $T^{(0)}$ over K. By induction we assume that $\mathcal{D}_0(K/K_i)$ is generated by $T^{(0)}, T^{(1)}, \cdots, T^{(i-1)}$ over K. Then we shall show that $\mathcal{D}_0(K/K_{i+1})$ is generated over K by $T^{(0)}, T^{(1)}, \cdots, T^{(i)}$.

Let $\mathfrak{A}_0 = K < T^{(0)}, \cdots, T^{(i)} >$. We shall first prove that $\mathfrak{A} = K \oplus \mathfrak{A}_0$ is a subring of $\mathfrak{L}(K)$, the set of additive homomorphisms of K into itself. For this purpose, it suffices to prove that $\Delta_*^{(p^j)} a \in \mathfrak{A}$ $(a \in K, 0 \leq j \leq i)$. For $a \in K$, $[\Delta_*^{(p^j)}, a]$ is a $(p^j - 1)$-th order derivation, and so $[\Delta_*^{(p^j)}, a]$ is K_j-linear by Lemma 14. Hence by induction assumption $[\Delta_*^{(p^j)}, a]$ is contained in $K < T^{(0)}, T^{(1)}, \cdots, T^{(j-1)} >$. Since $\Delta_*^{(p^j)} a = [\Delta_*^{(p^j)}, a] + a\Delta_*^{(p^j)} + \Delta_*^{(p^j)}(a)$, we have $\Delta_*^{(p^j)} a \in \mathfrak{A}$ and $\mathfrak{A}$ is a subring of $\mathfrak{L}(K)$. On the other hand we have $\{a \in K \mid \Delta_*^{(1)} a = a\Delta_*^{(1)}, \cdots, \Delta_*^{(p^i)} a = a\Delta_*^{(p^i)}\} = K_{i+1}$, by Proposition 15, thence $Z(\mathfrak{A}) = K_{i+1}$. Since $\mathfrak{A}$ is a subring of $\mathfrak{L}(K)$ and $Z(\mathfrak{A}) = K_{i+1}$, we have $\mathfrak{A} = \mathrm{Hom}_{K_{i+1}}(K, K)$ by Jacobson-Bourbaki Theorem (cf. [2]). Hence we have $\mathfrak{A} = \mathcal{D}(K/K_{i+1})$ by Theorem 4 and so $\mathfrak{A}_0 = \mathcal{D}_0(K/K_{i+1})$.

REMARK 5. Let the situation be as in Proposition 16. If $p^{f-1} \leq n < p^f$, an n-th order derivation of K/k is contained in $K < T^{(0)}, T^{(1)}, \cdots, T^{(f-1)} >$. This follows immediately from the facts that we have $\mathcal{D}_0^{(n)}(K/k) = \mathcal{D}_0^{(n)}(K/K_f)$, $\mathcal{D}_0^{(p^i)}(K/k) = \mathcal{D}_0^{(p^i)}(K/K_f)$, $\mathcal{A}_i(K/k) = \mathcal{A}_i(K/K_f)$ for $0 \leq i < f$.

Hitherto we were interested in the case of a purely inseparable extension K/k of finite degree. There the high derivations of orders $p^i (i = 0, 1, \cdots)$ are key stones for the construction of high order derivations. When K/k is a separably algebraic extension there is no non-trivial high order derivation over k. So we shall go to the case where K is a finitely generated separable extension of k. In this case there is a finite number of independent variables $x_1, \cdots, x_n$ over k such that K is a finite separable extension of $k(x_1, \cdots, x_n) = k(x)$. Then the essential theory of high order derivations of K/k is reduced to that of $k(x)/k$ owing to the following

THEOREM 17. *Let K, F be over fields of k such that K is separably algebraic over F. Then any q-th order derivation of F/k into a K-module M can be extended in a unique way to a q-th order derivation of K/k into M.*

PROOF. First we shall prove the uniqueness. From II-11 we have the following two exact sequences

(1) $\qquad K\otimes\Omega_k^{(q)}(F)\longrightarrow\Omega_k^{(q)}(K)\longrightarrow\Omega_k^{(q)}(K/F)\longrightarrow 0,$

(2) $\qquad \Omega_k^{(q-1)}(F)\otimes_F\Omega_k^{(q-1)}(K/F)\longrightarrow\Omega_k^{(q)}(K/F)\longrightarrow\Omega_F^{(q)}(K)\longrightarrow 0.$

Since K is separably algebraic over F we see easily $\Omega_F^{(q)}(K)=0\,(q\geq 1)$. Then the repeated use of (2) yields at once $\Omega_k^{(q)}(K/F)=0\,(q\geq 1)$. Hence from (1) we get an epimorphism

$$K\otimes\Omega_k^{(q)}(F)\xrightarrow{\varphi}\Omega_k^{(q)}(K)\longrightarrow 0,$$

and the dual monomorphism

$$0\longrightarrow\mathcal{D}_0^{(q)}(K/k,\ M)\xrightarrow{\varphi^*}\mathcal{D}_0^{(q)}(F/k,\ M).$$

This sequence implies that the extension is unique.

Next we shall prove that the extension is possible. For that purpose we have to show that φ^* is surjective and it suffices to prove that φ is injective. This is well known in case $q=1$(cf. [4]). The proof will be carried out by induction on q.

We denote by τ the mapping $K\otimes_F F\otimes_k F\to K\otimes_k K$ such that $\tau(x\otimes y\otimes z)=xy\otimes z$. Let ω be an element of $K\otimes_F I_F\subset K\otimes_F F\otimes_k F$ satisfying $\tau(\omega)\in I_K^{q+1}$. We shall show that $\omega\in K\otimes_F I_F^{q+1}$. Let us now consider the following commutative diagram of exact sequences

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \uparrow & & \uparrow & & & & \\
0 & \longrightarrow & J & \longrightarrow & K\otimes_F K & \xrightarrow{\alpha} & K & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & \| & & \\
0 & \longrightarrow & I_K & \longrightarrow & K\otimes_k K & \xrightarrow{\beta} & K & \longrightarrow & 0 \\
 & & \uparrow & & \uparrow & & & & \\
 & & \hat{I}_F & = & \hat{I}_F & & & & \\
 & & \uparrow & & \uparrow & & & & \\
 & & 0 & & 0 & & & &
\end{array}$$

where α and β are contraction homomorphisms and $\hat{I}_F$ denotes the ideal of $K\otimes_k K$ generated by elements of the form $\{1\otimes y-y\otimes 1,\ y\in F\}$. Since K is a finite separable extension of F we have $J=J^2$, and J has a finite basis. Hence there exists an element γ such that $\gamma\equiv 1$ (mod. J) and $\gamma J=0$. Let c be an element of $K\underset{k}{\otimes}K$ which is mapped on γ. Then $c-1=b$ is contained in $\hat{I}_F$, and $cI_K\equiv 0$ (mod $\hat{I}_F$). Then the assumption $\tau(\omega)\equiv 0(I_K^{q+1})$ implies that $c^{q+1}\tau(\omega)$ is contained in $\hat{I}_F^{q+1}$. On the other hand $\tau(\omega)$ is contained in $\hat{I}_F^q$ by induction assumption. Hence

$$\tau(\omega)\equiv(1+b)^{q+1}\tau(\omega)=c^{q+1}\tau(\omega)\equiv 0(\hat{I}_F^{q+1}).$$

This result completes the proof since we have

$$\tau^{-1}(\hat{I}_F^{q+1})\subset K\otimes I_F^{q+1}.$$

Let us go back to our original situation. Let K be a finitely generated separable extension of k and let $t_1,\cdots,t_n$ be a separating transcendence basis of K/k. Then we have

$$\Omega_k^{(q)}(K)\cong K\otimes\Omega_k^{(q)}(k(t)).$$

From II–10 it follows that

$$\Omega_k^{(q)}(k(t))\cong k(t)\otimes_{k[t]}\Omega_k^{(q)}(k[t]).$$

Hence we have

$$\Omega_k^{(q)}(K)\cong K\otimes_{k[t]}\Omega_k^{(q)}(k[t]).$$

Thus to find q-th order derivations of K/k it is sufficient to find q-th order derivations of $k[t_1,\cdots,t_n]/k$. From II–2 it follows that $\Omega_k^{(q)}(k[t])$ is a free module over $k[t]$ with the basis $\delta^{(q)}(M_\lambda)$ where $\delta^{(q)}=\delta^{(q)}_{k[t]/k}$ and $\{M_\lambda,\ \lambda\in\Lambda\}$ are all monomials of degree $\leq q$.

Now we divide the case into two cases.

(I) The characteristic of K is zero: Let us denote by ∂_i the partial derivation with respect to t_i. Then any high order derivation of order $\leq q$ is represented as $\partial_1^{a_1}\partial_2^{a_2}\cdots\partial_n^{a_n}$ with $\sum a_i\leq q$. The proof is quite easy. For example to every monomial $M_\lambda=t_1^{a_1}\cdots t_n^{a_n}$ of degree $\leq q$ we associate a q-th order derivation

$$D_\lambda=\frac{1}{a_1!\cdots a_n!}\partial_1^{a_1}\cdots\partial_n^{a_n}.$$

Then we see easily that D_λ form a $k[t]$-basis of $\mathcal{D}_0^{(q)}(k[t]/k)$.

(II) The characteristic of K is a positive prime p. Let us denote by

$D_{(a_1,\dots,a_n)}$ the high order derivation defined by $D_{(a_1,\dots,a_n)}(t_1^{m_1}\cdots t_n^{m_n})=\binom{m_1}{a_1}\cdots\binom{m_n}{a_n}$ $t_1^{m_1-a_1}\cdots t_n^{m_n-a_n}$. $D_{(a_1,\dots,a_n)}$ is a high derivation of order $\sum_{i=1}^n a_i$. Since we have $D_{(a_1,\dots,a_n)}(t_1^{a_1}\cdots t_n^{a_n})=1$ and $D_{(a_1,\dots,a_n)}(t_1^{m_1}\cdots t_n^{m_n})=0$ if $a_i>m_i$ for some i, we see easily that $D_{(a_1,\dots,a_n)}$ are independent and so $D_{(a_1,\dots,a_n)}(1\leq\sum_i a_i\leq q)$ form a $k[t]$-basis of $\mathcal{D}_0^{(q)}(k[t]/k)$. Let us set $D_{(0,\dots,0,\overset{i}{p^s},0,\dots,0)}=\partial_{si}(1\leq i\leq n)$. Let $a_i=\sum_{j=0}^{r_i}\alpha_{ij}p^j\,(1\leq i\leq n)$ be the p-adic expansion of a_i. Then we can see by a simple calculation that we have

$$D_{(a_1,\dots,a_n)}=\frac{1}{(\prod_{j=0}^{r_1}\alpha_{1j})\cdots(\prod_{j=0}^{r_n}\alpha_{nj})}\prod_{j=0}^{r_1}(\partial_{j1})^{\alpha_{1j}}\cdots\prod_{j=0}^{r_n}(\partial_{jn})^{\alpha_{nj}}.$$

In other words $D_0(K/k)$ is generated by high derivations of orders $1, p, p^2,\cdots\cdots$

PROPOSITION 18. *Let K be a finitely generated separable extension of a field k. Then if the characteristic of K is zero $\mathcal{D}_0(K/k)$ is generated by $\mathcal{D}_0^{(1)}(K/k)$. If the characteristic of K is a positive prime p, $\mathcal{D}_0(K/k)$ is generated by high order derivations of orders $p^i(i=0, 1,\cdots)$.*

Bibliography

[1] N. Bourbaki, Algèbre, Hermann, Paris.
[2] N. Jacobson, Lectures in abstract algebra III, Van Nostrand, Princeton, New Jersey 1964.
[3] Y. Nakai, High order derivations I, Osaka Journal of Mathematics **7** (1970), 1-27.
[4] Y. Nakai, On the theory of differentials in commutative rings, J. M. S. of Japan, **3** (1961), 63-84.
[5] M. E. Sweedler, Structure of inseparable extensions, Ann. Math. **87** (1968), 401-410.

Department of Mathematics
Faculty of Science
Osaka University