Hattori, A.
Osaka J. Math.
7 (1970) 307-312

AN APPLICATION OF INNER-EXTENSION OF HIGHER DERIVATIONS TO p-ALGEBRAS

Dedicated to Professor Keizo Asano on his 60th birthday

AKIRA HATTORI

(Received April 2, 1970)

Let A be a central separable algebra over a field K, and assume that it contains a normal extension L of K as a maximal commutative subalgebra. When L/K is moreover separable, one obtains a description of A as a crossed product by extending automorphisms of L to inner automorphisms of A. When L/K is purely inseparable of exponent 1, one obtains similarly a concrete description of A by extending derivations of L to inner derivations of A (e.g. Jacobson [5]). Here we apply a similar procedure using higher derivations in case L is purely inseparable of exponent 2, and derive the normal form $(\alpha | \beta_0, \beta_1]$ for A given by Schmid [7] and Witt [9]. For this purpose we prove in §1 some facts about inner-extension of higher derivations.

1. Inner-extension of higher derivations

Let A be an algebra over a commutative ring R. Let $A[T]_q = A[T]/(T^{q+1})$, where T is an indeterminate. We denote $T(\text{mod } T^{q+1})$ by t, so that any element of $A[T]_q$ is written uniquely as $a_0 + a_1 t + \cdots + a_q t^q$ $(a_i \in A)$. Let B be an R-algebra containing A. A *higher derivation* D of A into B of rank q is a sequence $\{D_1, \cdots, D_q\}$ of R-linear maps D_i: $A \to B$ such that

$$D_t\colon A \to B[T]_q; \quad D_t(a) = a + D_1(a)t + \cdots + D_q(a)t^q \qquad (a \in A)$$

is an algebra homomorphism, or what is the same thing, D_t defines an algebra homomorphism $A[T]_q \to B[T]_q$ over $R[T]_q$. If $D = \{D_1, \cdots, D_q\}$ is a higher derivation of rank q, $\{D_1, \cdots, D_k\}$ $(k \leqq q)$ is a higher derivation of rank k, which will be called the *k-section* of D.

For any $d_1, \cdots, d_q \in A$, the polynomial

$$d_t = 1 + d_1 t + \cdots + d_q t^q$$

is invertible in $A[T]_q$. It yields a higher derivation $\tilde{d}$ of A, via inner automorphism of $A[T]_q$, i.e.

$$\tilde{d}_t(a) = d_t a d_t^{-1} \qquad (a \in A)$$

We call such $\tilde{d}$ an *inner higher derivation* of A determined by $\{d_1, \cdots, d_q\}$. In other words, a higher derivation D is inner if there exist $d_1, \cdots, d_q \in$ A such that for any $a \in A$

$$d_k a = D_k(a) + D_{k-1}(a) d_1 + \cdots + D_1(a) d_{k-1} + a d_k \qquad (k = 1, \cdots, q)\,.$$

EXAMPLE 1. Embed A into End(A) as the set of left multiplications. Any higher derivation D: $A \to A$ is then extended to the inner higher derivation of End(A) defined by $D_1, \cdots, D_q \in$ End(A).

EXAMPLE 2. Let $1, \cdots, q$ be invertible in R. A derivation δ: $A \to A$ gives rise to a higher derivation $e_q(\delta)$ defined by

$$e_q(\delta)_t(a) = a + \delta(a)t + \frac{1}{2!}\delta^2(a)t^2 + \cdots + \frac{1}{q!}\delta^q(a)t^q \qquad (a \in A)$$

If δ is an inner derivation defined by $d \in A$, then $e_q(\delta)$ is an inner higher derivation defined by

$$e_q(d)_t = 1 + dt + \frac{1}{2!}d^2t^2 + \cdots + \frac{1}{q!}d^qt^q\,.$$

Let B be a subalgebra of A, and D: $B \to A$ a higher derivation. If there exists an inner higher derivation $\tilde{d}$ of A which coincides on B with D, we say that $\tilde{d}$ is an *inner-extension* of D.

Theorem 1. *If B is a separable algebra* [2] *over R, any higher derivation D: $B \to A$ has an inner-extension $A \to A$.*

Proof. There exist $u_i, v_i \in B$ $(i=1, \cdots, n)$ such that

i) $\sum u_i v_i = 1$, and
ii) $\sum b u_i \otimes v_i = \sum u_i \otimes v_i b \qquad$ (in $B \otimes B$).

Set

$$d_t = \sum_i D_t(u_i) v_i = 1 + (\sum_i D_1(u_i) v_i) t + \cdots\,.$$

For $b \in B$, we have

$$\begin{aligned} D_t(b) d_t = \sum D_t(b) D_t(u_i) v_i &= \sum D_t(b u_i) v_i \\ &= \sum D_t(u_i)(v_i b) = d_t b \end{aligned}$$

This shows that $\tilde{d}$ is an inner-extension of D.

Theorem 2. *Let A be a central separable algebra over R, and B be a left* (*or right*) *semisimple subalgebra* [3] *of A. Then any higher derivation D of B into*

A has an inner-extension $A \to A$.

REMARK. A special case is proved in Jacobson [5], and the theorem itself is essentially a special case of Sweedler [8, Th. 9. 5].

Proof. We proceed by induction on q. The case $q=1$ is proved in the following manner (after Hochschild [4]). Let A^0 be an anti-isomorphic copy of A. The direct sum $(A, A)=A\oplus A$ is considered as a $B\otimes A^0$-module by setting

$$b(a_1, a_2)a = (ba_1a,\ D_1(b)a_1a+ba_2a)\,.$$

The map $(a_1, a_2)\mapsto a_1$ defines an R-split $(B\otimes A^0)$-epimorphism $A\oplus A\to A$, where A is considered naturally as a $B\otimes A^0$-module. Since $B\otimes A^0$ is left semisimple [3, Prop. 2. 4], there exists a $B\otimes A^0$-monomorphism $\alpha\colon A\to A\oplus A$ such that $(A, A)=(0, A)\oplus\mathrm{im}\,(\alpha)$. If $\alpha(1)=(u, v)$, u is invertible, and we have $D(b)=(vu^{-1})b-b(vu^{-1})$ (*cf.* [4]). Let $q>1$ and assume that $d_1, \cdots, d_{q-1}\in A$ give an inner-extension of the $(q-1)$-section $D=\{D_1, \cdots, D_{q-1}\}$ of D. Set

$$d_t' = 1+d_1t+\cdots+d_{q-1}t^{q-1}\in A[T]_q\,.$$

For every $b\in B$, the terms of degree $<q$ in $D_t(b)d_t'-d_t'b$ all vanish. So there exists $f(b)\in A$ such that

$$f(b)t^q = D_t(b)d_t'-d_t'b\,.$$

We have

$$\begin{aligned} f(b_1b_2)t^q &= D_t(b_1)D_t(b_2)d_t'-d_t'b_1b_2 \\ &= (D_t(b_1)f(b_2)+f(b_1)b_2)t^q\,, \end{aligned}$$

whence

$$f(b_1b_2) = b_1f(b_2)+f(b_1)b_2\,.$$

Hence there exists $d_q\in A$ such that $f(b)=d_qb-bd_q(^{\forall}b\in B)$.
Setting

$$d_t = d_t'+d_qt^q\,,$$

we have

$$d_tb = D_t(b)d_t \qquad (^{\forall}b\in B)\,. \qquad\qquad \text{q. e. d.}$$

If both $\tilde{d}$ and $\tilde{d}'$ are inner-extensions of $D\colon B\to A$, then it is clear that $d_t^{-1}d_t'\in V_A(B)[T]_q$, where $V_A(B)$ denotes the commuter of B in A.

Proposition 3. *Let D be a higher derivation $B\to A$ which admits an inner-extension $A\to A$. If the k-section of D $(k\leqq q)$ has an inner-extension $A\to A$ determined by $d_1, \cdots, d_k$, then we can find $d_{k+1}, \cdots, d_q\in A$ so that D is extended to the inner higher derivation defined by $\{d_1, \cdots, d_k, d_{k+1}, \cdots, d_q\}$.*

Proof. Let the inner higher derivation by $\{d_1', \cdots, d_q'\}$ yields D when restricted to B. Then there exist $c_1, \cdots, c_k \in V_A(B)$ such that

$$1+d_1t+\cdots+d_kt^k \equiv d_t'(1+c_1t+\cdots+c_kt^k) \qquad (\text{mod } t^{k+1})$$

Determine $d_{k+1}, \cdots, d_q \in A$ by the identity (in $A[T]_q$)

$$1+d_1t+\cdots+d_kt^k+d_{k+1}t^{k+1}+\cdots+d_qt^q = d_t'(1+c_1t+\cdots+c_kt^k).$$

It is clear that $\{d_1, \cdots, d_k, d_{k+1}, \cdots, d_q\}$ induces the higher derivation D of B.

2. p-algebras of exponent 2

Let A be a central separable algebra over a field K of characteristic $p \neq 0$, and assume that there exists a maximal commutative subalgebra L which is a purely inseparable extension of K such that

$$(1) \qquad L = K(u), \qquad u^{p^2} = \alpha \in K$$

Since $L \cong K[X]/(X^{p^2}-\alpha)$, a higher derivation $D: L \to A$ of rank q is determined by assigning to u a polynomial $D_t(u) \in A[T]_q$ such that $D_t(u)^{p^2} = \alpha$. It follows that for $q < p^2$, there exists a (unique) higher derivation $D = \{D_1, \cdots, D_q\}: L \to L$ such that $D_i(u) = a_i$, $i = 1, \cdots, q$, for any preassigned values $a_1, \cdots, a_q \in L$.

In particular, there exists a higher derivation $D: L \to L$ of rank p such that

$$D_i(u) = \frac{1}{i!}D_1^i(u) = \frac{1}{i!}u, \qquad i = 1, \cdots, p-1,$$
$$D_p(u) = 0.$$

By Theorem 2, D has an inner-extension $A \to A$. If D_1 is given by the inner derivation by $d_1 \in A$, $\{D_1, \cdots, D_{p-1}\}$ is given by $\{d_1, \cdots, d_{p-1}\}$ where $d_i = (1/i!)d_1^i$ $(i = 1, \cdots, p-1)$. Hence, by proposition 3, D is extended to an inner higher derivation defined by

$$d_1, \cdots, d_p; \quad \text{where} \quad d_i = \frac{1}{i!}d_1^i, \qquad i = 1, \cdots, p-1.$$

In particular we have

$$(2) \qquad u^{-1}d_1u = d_1+1,$$

$$(3) \qquad u^{-1}d_pu = d_p + \sum_{i=1}^{p-1} \frac{1}{i!(p-i)!}d_1^i.$$

By (2) we have

$$(2') \qquad u^{-1}d_1^pu = d_1^p+1.$$

Hence $d_1^p - d_1$ commutes with u, and $d_1^p - d_1 \in L$. It commutes moreover with d_1. Hence $d_1^p - d_1 \in K(u^p)$. It follows that

$$(d_1^p)^p - d_1^p = (d_1^p - d_1)^p \in K\,.$$

By (2′) we may start with d_1^p instead of d_1. So we may assume

$$d_1^p - d_1 = \beta_0 \in K\,. \tag{4}$$

Set $v=[d_1, d_p]=d_1 d_p - d_p d_1$. We have

$$u^{-1}vu = (d_1+1)(d_p+S)-(d_p+S)(d_1+1) = v\,,$$

since $S=u^{-1}d_p u - d_p$ commutes with d_1 (cf. (3)). Hence $v \in L$.
We have

$$d_1^p d_p - d_p d_1^p = [\overbrace{d_1, \cdots, [d_1}^{p}, d_p]\cdots] = D_1^{p-1}(v)\,.$$

This together with (4) shows

$$d_1 d_p - d_p d_1 = D_1^{p-1}(v) = d_1 D_1^{p-2}(v) - D_1^{p-2}(v)\, d_1\,.$$

This means that $d_p' = d_p - D_1^{p-2}(v)$ commutes with d_1. Since d_p' satisfies (3), we can use this d_p' in place of d_p.

Hence we may assume

$$d_1 d_p = d_p d_1 \tag{5}$$

d_1 and d_p generate a commutative subalgebra P. Let $W_2(P)$ be the group of Witt vectors of length 2 in P. By definition, we have

$$(b_0, b_1)+\underline{1} = \left(b_0+1,\ b_1+\sum_{i=1}^{p-1}\frac{1}{i!(p-i)!}b_0^i\right)$$

where $\underline{1}=(1, 0)$. (Notice $(p-1)! \equiv -1 \pmod p$.) Hence (2) and (3) mean

$$u^{-1}(d_1, d_p)u = (d_1, d_p)+\underline{1} \tag{6}$$

Similarly, (2′) and the identity

$$u^{-1}d_p^p u = d_p^p + \sum_{i=1}^{p-1}\frac{1}{i!(p-i)!}d_1^{pi} \tag{3′}$$

which is derived from (3), mean

$$u^{-1}(d_1^p, d_p^p)u = (d_1^p, d_p^p)+\underline{1} \tag{6′}$$

Putting

$$\wp(d_1, d_p) = (d_1^p, d_p^p)-(d_1, d_p) = (\beta_0, \beta_1) \tag{7}$$

we have (by (6) and (6′))

$$u^{-1}(\beta_0, \beta_1)u = (\beta_0, \beta_1)$$

Since β_1 (as well as β_0) commutes with d_1, d_p and u, it must lie in K. Finally it is clear that d_1, d_p and u generate the whole algebra. A. The structure of A is thus completely determined by (1), (5), (6) and (7), and we have arrived to the normal form $(\alpha | \beta_0, \beta_1]$ given by Schmid [7] and Witt [9].

UNIVERSITY OF TOKYO, COLLEGE OF GENERAL EDUCATION

References

[1] A.A. Albert: Structure of Algebras, Amer. Math. Soc. Colloq. Publ. 24, Providence, 1939.

[2] M. Auslander and O. Goldman: *The Brauer group of a commutative ring*, Trans. Amer. Math. Soc. **97** (1960), 367–409.

[3] A. Hattori: *Semisimple algebras over a commutative ring*, J. Math. Soc. Japan **15** (1963), 404–419.

[4] G. Hochschild: *Simple algebras with purely inseparable splitting fields of exponent* 1, Trans. Amer. Math. Soc. **79** (1955), 477–489.

[5] N. Jacobson: *Generation of separable and central simple algebras*, J. Math. Pures Appl. **36** (1957), 217–227.

[6] N. Jacobson: Lectures in Abstract Algebra, vol. III, van Nostrand, 1964.

[7] H.L. Schmid: *Zyklische algebraische Funktionenkörper vom Grad p^n über endlichen Konstantenkörper der Charakteristik p*, Crelles J. **175** (1936), 108–123.

[8] M.E. Sweedler: *Cohomology of algebras over Hopf algebras*, Trans. Amer. Math. Soc. **133** (1968), 205–239.

[9] E. Witt: *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n*, Crelles J. **176** (1937), 31–44.