Kosaki, K.
Osaka J. Math.
8 (1971), 281-290

ON SCHMID-WITT'S NORMAL FORM FROM THE HOPF ALGEBRA THEORETIC VIEW-POINT

Kotaro KOSAKI

(Received October 20, 1970)

Introduction

Let K be a field of characteristic p and $L=K[u]$, $u^{p^2}=a\in K$, a simple purely inseparable extension of exponent 2 and let A be a central separable algebra over K which contains L as a maximal commutative subalgebra. Let D_1, D_2, $\cdots$, D_p be the higher derivation of L/K defined by

$$D_i(u)=\frac{1}{i!}u \quad (0<i<p),\ D_p(u)=0\,.$$

Then A. Hattori showed in [2] the existence of the elements d_i $(0<i\leq p)$ of A making the above higher derivation inner in such a way that $d_1d_p=d_pd_1$ and in the group of Witt vectors of length 2, we have

$$u^{-1}(d_1,\ d_p)u=(d_1,\ d_p)+(1,\ 0)\,,$$
$$(d_1^p,\ d_p^p)-(d_1,\ d_p)=(\beta_0,\ \beta_1),\ \beta_i\in K\,.$$

Thus u, d_1, d_p are the canonical generators of Schmid-Witt type for A.

Furthermore to extend this result to arbitrary exponent case, he introduced in [3] a Galois Hopf algebra $\mathfrak{D}$ for a simple purely inseparable extension $L=K[u]$, $u^{p^n}=a\in K$ $(n\geq 1)$. He conjectured that if A is a central separable algebra over K with L as a maximal commutative subalgebra, then making use of this Hopf algebra, one could find the canonical generators of Schmid-Witt type for A.

The purpose of this note is to answer this problem affirmatively. In Section 1, we clarify the structure of the Hopf algebra introduced in [3]. In Section 2, we give an answer to the above problem. Finally in Section 3, we give an another proof following the idea of A.A. Albert in [1].

0. Preliminaries

We quote for the sake of convenience some definitions, notations and fundamental facts on Hopf algebras. For the details the reader will be expected to refer M.E. Sweedler [4], [5].

We fix a ground field K. Let H be a Hopf algebra. Then we shall denote its comultiplication by Δ_H (or simply Δ), augmentation by ε_H (or ε), antipode by ι_H (or ι). Furthermore we use the abbreviation

$\Delta h = \sum h_{(1)} \otimes h_{(2)}$, $(I \otimes \Delta)\Delta h = \sum h_{(1)} \otimes h_{(2)} \otimes h_{(3)}$ and so on. With this notation $h = \sum \varepsilon(h_{(1)}) h_{(2)} = \sum \varepsilon(h_{(2)}) h_{(1)}$. Thus $\varepsilon(h) = \sum \varepsilon(h_{(1)}) \varepsilon(h_{(2)})$.

An element g of H is called a group-like element, if $\Delta g = g \otimes g$. We denote by $G(H)$ the set of all group-like elements of H.

In the sequel H will denote a Hopf algebra. A subspace I of H is called a coideal if $\varepsilon(I)=0$ and $\Delta I \subset H \otimes I + I \otimes H$. If I is furthermore a two-sided ideal of H, we can form the quotient Hopf algebra H/I.

If A is an algebra, Hom (H, A) has a natural algebra structure defined by

$$(f \cdot g)(h) = \sum f(h_{(1)}) g(h_{(2)}),\ f, g \in \mathrm{Hom}\,(H, A),\ h \in H,$$
$$1(h) = \varepsilon(h) 1_A\,,\quad h \in H\,.$$

Let A and B be algebras, and ω: $\mathrm{H} \otimes A \to B$ a K-linear mapping. We say ω measures A to B if

$$\omega(h \otimes 1) = \varepsilon(h) 1 \quad \text{and} \quad \omega(h \otimes xy) = \sum \omega(h_{(1)} \otimes x) \omega(h_{(2)} \otimes y),$$
$$h \in H,\ x, y \in A\,.$$

We abbreviate $\omega(h \otimes a)$ by $h \cdot a$. If $g \in G(H)$, then g induces an algebra homomorphism. Let us set

$$A^H = \{a \in A \mid h \cdot a = \varepsilon(h) a \,\forall h \in H\}\,.$$

Then A^H is a subalgebra of A. If in particular $A=B$ and A is an H-module with this action, we say that A is an H-module algebra.

Let H be a finite dimensional Hopf algebra and L a field extension of K, which is an H-module algebra. Then we say that L/K is a Galois extension with Galois Hopf algebra H, if

(1) $L^H = K$,

(2) $[L: K] = [H: K]$,

(3) the elements of $G(H)$ induce all automorphisms of L/K. In this case, L is a faithful H-module and for any K-algebra A, an element f of Hom (H, A) is invertible if and only if for every $g \in G(H)\, f(g)$ is invertible in A.

Let H be a Hopf algebra, A and B algebras. Suppose that H measures A to B. We say that the measuring is B-inner if there is an invertible element f of Hom (H, B) where $f(h) a = \sum (h_{(1)} \cdot a) f(h_{(2)})$ for all $h \in H$, $a \in A$. We say that f gives the B-inner action.

1. Hopf algebras H over K

In the sequel Z will denote the ring of rational integers. In this section we fix a ground field K of characteristic p>0.

For every ring (commutative with identity) of characteristic p, we denote by $W(A)$ (resp. $W_n(A)$) the ring of Witt vectors (resp. Witt vectors of length n) with coefficients in A. Let $S_0(X_0; Y_0)$, $S_1(X_0, X_1; Y_0, Y_1)$, $\cdots$, be the polynomials which define the additive structure of Witt vectors. Thus we have $(X_0, X_1, \cdots)+(Y_0, Y_1, \cdots)=(S_0, S_1, \cdots)$ in $W(Z/pZ[X_0, X_1, \cdots, Y_0, Y_1, \cdots])$. Then we can make the algebra $K[X_0, X_1, \cdots, X_{n-1}]=A_n$ into a Hopf algebra by

$$\begin{array}{lll}\text{comultiplication:} & \Delta X_i=S_i(X_0\otimes 1, \cdots, X_i\otimes 1; 1\otimes X_0, \cdots, 1\otimes X_i) & \\ \text{augmentation:} & \varepsilon(X_i)=0 & (0\leq i\leq n-1)\,. \\ \text{antipode:} & \iota(X_i)=-X_i & (0\leq i\leq n-1)\,. \end{array}$$

In particular,

$$\Delta X_0 = X_0\otimes 1+1\otimes X_0\,,$$
$$\Delta X_1 = X_1\otimes 1+1\otimes X_1+\sum_{i=1}^{p-1}\frac{1}{i!(p-i)!}X_0^i\otimes X_0^{p-i}\,.$$

In general,

$$\Delta X_i \equiv X_i\otimes 1+1\otimes X_i$$

modulo the ideal generated by $X_s\otimes X_t$ $(0\leq s, t\leq i)$.

Lemma. *The ideal I_n of A_n generated by $X_0^p-X_0, X_1^p-X_1, \cdots, X_{n-1}^p-X_{n-1}$ is a coideal of the above Hopf algebra A_n.*

Proof. Since the coefficients of S_i are in the prime field, we have $X_i^p=S_i(X_0^p\otimes 1, X_1^p\otimes 1, \cdots; 1\otimes X_0^p, 1\otimes X_1^p, \cdots)$. From this we can easily see that $\Delta(X_i^p-X_i)\subset A_n\otimes I_n+I_n\otimes A_n$.

From this lemma we obtain the quotient Hopf algebra $H_n=A_n/I_n$ which will play an essential role. Since A_n can be considered as a sub-Hopf algebra of A_{n+1} by the natural injection: $A_n\ni X_i\mapsto X_i\in A_{n+1}$, H_n also is a sub-Hopf algebra of H_{n+1}. We define H_0 as the trivial Hopf algebra K. We denote by δ_i the class of X_i in A_n. Though δ_i depends on n this will not cause confusions because of the above remark. In the sequel we use the vector notations

$$\delta^e = \delta_0^{e_0}\delta_1^{e_1}\cdots\delta_{n-1}^{e_{n-1}}\ (e=(e_0, e_1, \cdots, e_{n-1}),\ 0\leq e_i<p)\,.$$

These form the basis of H_n over K.

Let $L=K[u]$, $u^{p^n}=a\in K$ be a simple purely inseparable extension of exponent n. We are going to show that defining a suitable action of H_n on L, L/K is a Galois extension with Galois Hopf algebra H_n. For this purpose, we will introduce certain notational conventions. In every ring with indentity 1, 0^0 equals 1. For every integer $\alpha\in Z$, $\bar{\alpha}$ denotes its class in Z/p^nZ. Denote by $(\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$ the element of $W_n(Z/pZ)$ corresponding to $\bar{\alpha}$ by the ring isomorphism $Z/p^nZ \rightleftarrows W_n(Z/pZ)$. For two integers $0\leq\alpha, \beta<p^n$, define

$$(\alpha, \beta)=\begin{cases}0 & \text{if } \alpha+\beta<p^n\\ 1 & \text{if } \alpha+\beta\geq p^n\,.\end{cases}$$

Finally, for $\bar{\alpha}\in Z/p^nZ$ define $u^{\bar{\alpha}}$ by $u^{\bar{\alpha}}=u^{\alpha}$ $(0\leq\alpha<p^n)$. With these notations we have the following:

Proposition 1. (A. Hattori, [3]) *Define the action of H_n on L by*

$$\delta^e\cdot u^{\alpha}=\alpha_0^{e_0}\alpha_1^{e_1}\cdots\alpha_{n-1}^{e_{n-1}}u^{\alpha} \quad \textit{where} \quad e=(e_0, e_1, \cdots, e_{n-1}),$$

$$0\leq e_i<p,\ 0\leq\alpha<p^n\,.$$

Then L/K is a Galois extension with Galois Hopf algebra H_n.

Proof. That L is an H_n-module is clear since $\alpha_i^p=\alpha_i$. To prove that H_n measures L to L, it sufficies to show that

$$\delta_i\cdot(u^{\alpha}u^{\beta})=\mu(S_i(\delta_0\otimes 1, \cdots, \delta_i\otimes 1; 1\otimes\delta_0, \cdots, 1\otimes\delta_i)u^{\alpha}\otimes u^{\beta})\,.$$

where μ is the multiplication $L\otimes L\rightarrow L$. The left hand side is equal to $\delta_i\cdot(a^{(\alpha,\beta)}u^{\overline{\alpha+\beta}})=a^{(\alpha,\beta)}(\alpha+\beta)_i u^{\overline{\alpha+\beta}}=(\alpha+\beta)_i u^{\alpha+\beta}$. The right hand side is equal to

$$\mu(S_i(\alpha_0\otimes 1, \cdots, \alpha_i\otimes 1; 1\otimes\beta_0, \cdots, 1\otimes\beta_i)u^{\alpha}\otimes u^{\beta})=$$
$$S_i(\alpha_0, \cdots, \alpha_i; \beta_0, \cdots, \beta_i)u^{\alpha+\beta}\,.$$

Since $Z/p^nZ\rightleftarrows W_n(Z/pZ)$, $S_i(\alpha_0, \cdots, \alpha_i; \beta_0, \cdots, \beta_i)=(\alpha+\beta)_i$. Thus we get the above equality. We see easily that $L^{H_n}=K$. On the other hand $[H_n\colon K]=p^n$. Thus $[H_n\colon K]=[L\colon K]$. It remains to show that the group-like elements of H_n induce all automorphisms of L/K. But this is clear because L/K is purely inseparable and $1\in G(H_n)$.

Corollary 1. *The group-like elements of H_n consist only of the identity element 1 of H_n.*

Corollary 2. *For any algebra A, $f\in Hom\,(H_n, A)$ is invertible if and only if $f(1)$ is invertible in A.*

We state two lemmas which we use in the next section.

Lemma 1. *Let H be a Hopf algebra, A and B algebras, H measures A to B, and let J be the two-sided ideal of A generated by $f_1, f_2, \cdots, f_n$ $(f_i \in A)$. Assume $H \cdot f_i = 0$ for every i. Then H induces naturally a measuring of A/J to B.*

A non-commutative polynomial ring in n variables over K is a K-algebra characterized by the following properties.

(1) It is generated as a K-algebra by n elements $X_1, X_2, \cdots, X_n$

(2) For any K-algebra A and n elements $a_1, a_2, \cdots, a_n$ of A, there exists a unique K-algebra homomorphism g, such that $g(X_i) = a_i$ for $1 \leq i \leq n$. We denote this algebra by $K\langle X_1, \cdots, X_n \rangle$.

Lemma 2. *Let H be a Hopf algebra with basis $\delta_1, \cdots, \delta_n$, A an algebra and $K\langle X_1, X_2, \cdots, X_m \rangle$ a non-commutative polynomial ring. Then for every family $\{a_{i,j}\}$ $1 \leq i \leq n$, $1 \leq j \leq m$ of elements of A, there exists a unique measuring of $K\langle X_1, \cdots, X_m \rangle$ to A defined by*

$$\delta_i \cdot X_j = a_{i,j} \quad (1 \leq i \leq n,\ 1 \leq j \leq m)\,.$$

Proof. Define the action of H on X_i and K by $(\sum \alpha_i \delta_i) \cdot X_j = \sum_i \alpha_i a_{i,j}$, $h \cdot 1 = \varepsilon(h)$ where $\alpha_i \in K$. To get a measuring, it needs only to define $h \cdot (X_{i_1} X_{i_2} \cdots X_{i_s}) = \sum (h_{(1)} \cdot X_{i_1})(h_{(2)} \cdot X_{i_2}) \cdots (h_{(s)} \cdot X_{i_s})$.

2. Schmid-Witt's normal form

Let L/K be as in Section 1 and A a central separable algebra over K with L as a maximal commutative subalgebra. Then the action of H_n on L defined in Proposition 1 is A-inner. ([4])

Proposition 2. *We can choose $f: H_n \rightarrow A$ giving the inner action in such a way that f satisfies the following conditions*

$$f(\delta_i) = d_i \quad (0 \leq i \leq n-1) \textit{ are mutually commutative, and}$$
$$f(\delta^e) = d_0^{e_0} d_1^{e_1} \cdots d_{n-1}^{e_{n-1}} \quad (e = (e_0, e_1, \cdots, e_{n-1})\ 0 \leq e_i < p)\,.$$

In particular $f(1) = 1$, and in the group of Witt vectors

$$(d_0^p, d_1^p, \cdots, d_{n-1}^p) - (d_0, d_1, \cdots, d_{n-1}) = (\beta_0, \beta_1, \cdots, \beta_{n-1})$$

with $\beta_i \in K$.

Proof. We shall construct f step by step. Assume we have already constructed f_i: $H_i \rightarrow A$ giving the inner action of H_i on L such that

$$f_i(\delta_0) = d_0, \cdots, f_i(\delta_{i-1}) = d_{i-1} \text{ are mutually commutative,}$$
$$f_i(\delta_0^{e_0}\delta_1^{e_1}\cdots\delta_{i-1}^{e_{i-1}}) = d_0^{e_0}d_1^{e_1}\cdots d_{i-1}^{e_{i-1}}, \quad 0 \leq e_j < p$$
$$(d_0^p, d_1^p, \cdots, d_{i-1}^p) - (d_0, d_1, \cdots, d_{i-1}) = (\beta_0, \beta_1, \cdots, \beta_{i-1})$$

with $\beta_j \in K$.

Then, since $\Delta\delta_j = S_j(\delta_0 \otimes 1, \cdots, \delta_j \otimes 1; 1 \otimes \delta_0, \cdots, 1 \otimes \delta_j)$, $\delta_0 \cdot u = u$, $\delta_1 \cdot u = 0, \cdots,$ and $\delta_{i-1} \cdot u = 0$, we get the relations

$$d_j u = u S_j(1, 0, \cdots, 0; d_0, d_1, \cdots, d_j)\,,$$

or equivalently

$$u^{-1}(d_0, d_1, \cdots, d_{i-1})u = (d_0, d_1, \cdots, d_{i-1}) + (1, 0, \cdots, 0)\,.$$

Thus if we put D_i the subalgebra of A generated by u, d_0, $d_1, \cdots, d_{i-1}$. Then D_i is a central separable algebra over $K[u^{p^i}]$ by E. Witt [6]. Hence in particular D_i is simple. Now we prove the following:

Lemma. *There exists a measuring by $H = H_n$ of D_i to D_i extending the measuring of L to L, in such a way that*

$$h \cdot d_j = \varepsilon(h) d_j \quad (0 \leq j \leq i-1)\,.$$

Proof. Consider the non-commutative polynomial ring $C = K\langle U, X_0, X_1, \cdots, X_{i-1}\rangle$. Then by Lemma 2, we have a measuring of C to D_i defined by

$$h \cdot U = h \cdot u \quad \text{(original action)}\,,$$
$$h \cdot X_j = \varepsilon(h) d_j \quad (0 \leq j \leq i-1)\,.$$

Denote by I the ideal of C generated by the elements $X_s X_t - X_t X_s$ $(0 \leq s, t \leq i-1)$. We first show that $H \cdot (X_s X_t - X_t X_s) = 0$. In fact, for every element $h \in H$, $h \cdot (X_s X_t) = \sum (h_{(1)} \cdot X_s)(h_{(2)} \cdot X_t) = \sum \varepsilon(h_{(1)}) d_s \varepsilon(h_{(2)}) d_t = \varepsilon(h) d_s d_t$. Thus $h \cdot (X_s X_t - X_t X_s) = \varepsilon(h)(d_s d_t - d_t d_s) = 0$. Hence, if we denote the classes of U, X_t in C/I by the same letters, H induces a measuring such that

$$h \cdot U = h \cdot u, \quad \text{and} \quad h \cdot X_j = \varepsilon(h) d_j\,.$$

Next we consider the ideal J of C/I generated by

$$\begin{cases} U^{p^n} - a\,, & \\ X_j U - U S_j(X_0, X_1, \cdots, X_j; 1, 0, 0, \cdots, 0) & (0 \leq i \leq i-1) \\ g_j(X_0, X_1, \cdots, X_j) & (0 \leq j \leq i-1)\,, \end{cases}$$

where g_j are defined by $(X_0^p, X_1^p, \cdots, X_{i-1}^p) - (X_0, X_1, \cdots, X_{i-1}) - (\beta_0, \beta_1, \cdots, \beta_{i-1}) = (g_0, g_1, \cdots, g_{i-1})$ in the group $W_i(K[X_0, \cdots, X_{i-1}])$.

To complete the proof of the lemma it suffices to show that

$$H\cdot J=0\,.$$

We shall verify this relation for every generator.

(1) Take an element h of H. Then, since H measures C/I and L to D_i and $h\cdot U=h\cdot u$, we have $h\cdot U^{p^n}=h\cdot u^{p^n}$. Thus $h\cdot(U^{p^n}-a)=h\cdot(u^{p^n}-a)=0$.

(2) For any $h\in H$, $h\cdot(X_tU)=\sum(h_{(1)}\cdot X_t)(h_{(2)}\cdot U)=\sum\varepsilon(h_{(1)})d_t(h_{(2)}\cdot u)$ $=d_t((\sum\varepsilon(h_{(1)})h_{(2)})\cdot u)=d_t(h\cdot u)$ and $h\cdot(US_t(X_0, X_1, \cdots, X_t; 1, 0, \cdots, 0))=$ $\sum(h_{(1)}\cdot u)\varepsilon(h_{(2)})S_t(d_0, d_1, \cdots, d_t; 1, 0, \cdots, 0)=(h\cdot u)S_t(d_0, d_1, \cdots, d_t; 1, 0, 0, \cdots,$ $0)$. On the other hand, $h\cdot u=$bu with $b\in K$. Thus $h\cdot(X_tU-US_t(X_0, \cdots,$ $Y_t; 1, 0, \cdots, 0))=0$.

(3) For any $h\in H$, $h\cdot g_j(X_0, X_1, \cdots, X_j)=\varepsilon(h)g_j\,(d_0, d_1,\cdots, d_{i-1})=0$. Proof of the lemma is thus completed.

Now we return to the proof of the proposition. Consider A, $A\otimes H_i$, $A\otimes H_{i+1}$ as left $A\otimes D_i^0$-modules by

$$b\circ a\circ d=bad,$$

$$b\circ(a\otimes h)\circ d=\sum ba(h_{(1)}\cdot d)\otimes h_{(2)}\,,$$

where D_i^0 is the opposite ring of D_i and a, $b\in A$, $d\in D_i$, $h\in H_i$ or H_{i+1}. Then the homomorphism p_i: $A\otimes H_i\to A$ defined by $p_i(a\otimes\delta^e)=ad^e=af_i(\delta^e)$ (where $e=(e_0, e_1, \cdots, e_{i-1})$, $\delta^e=\delta_0^{e_0}\cdots\delta_{i-1}^{e_{i-1}}$, $d^e=d_0^{e_0}d_1^{e_1}\cdots d_{i-1}^{e_{i-1}}$, $0\leq e_j<p$) is an $A\otimes D_i^0$-homomorphism. In fact, for every $h\in H_i$, and $d=d_0^{k_0}d_1^{k_1}\cdots d_{i-1}^{k_{i-1}}$,

$$(a\otimes h)\circ d=\sum a(h_{(1)}\cdot d)\otimes h_{(2)}=ad\otimes(\sum\varepsilon(h_{(1)})h_{(2)})=ad\otimes h\,.$$

On the other hand, since f_i gives the inner action of H_i on L,

$$p_i((a\otimes\delta^e)\circ u^{\alpha})=\sum a[(\delta^e)_{(1)}\cdot u^{\alpha}]f_i((\delta^e)_{(2)})=af_i(\delta^e)u^{\alpha}=ad^eu^{\alpha}=p_i(a\otimes\delta^e)u^{\alpha}.$$

Thus $p_i((a\otimes\delta^e)\circ(du^{\alpha}))=p_i(ad\otimes\delta^e)u^{\alpha}=p_i(a\otimes\delta^e)du^{\alpha}$.

Since $A\otimes D_i^0$ is semi simple, there exists a projection q: $A\otimes H_{i+1}\to A\otimes H_i$ of $A\otimes D_i^0$-modules. If we put $p=p_iq$, and define f: $H_{i+1}\to A$ by $f(h)=p(1\otimes h)$, then f gives the A-inner action of H_{i+1} on D_i, because $f(h)d=p(1\otimes h)d$ $=p(\sum h_{(1)}\cdot d\otimes h_{(2)})=\sum(h_{(1)}\cdot d)f(h_{(2)})$. Since f gives the A-inner action, if we set $f(\delta_i)=d_i$,

$$(*)\quad d_id_j=d_jd_i\quad(0\leq j\leq i-1),$$

and $d_iu=uS_i(1, 0, \cdots, 0; d_0, d_1, \cdots, d_i)$, or equivalently

$$(**)\quad u^{-1}(d_0, d_1, \cdots, d_i)u=(d_0, d_1, \cdots, d_i)+(1, 0, \cdots, 0)$$

in the group of Witt vectors.

From the second relation, we get $u^{-1}(d_0^p, d_1^p, \cdots, d_i^p)u=(d_0^p, d_1^p, \cdots, d_i^p)+(1, 0, \cdots, 0)$. Thus if we put $(d_0^p, d_1^p, \cdots, d_i^p)-(d_0, d_1, \cdots, d_i)=(\gamma_0, \gamma_1, \cdots, \gamma_i)$, γ_j's are contained in $V_A(L)$, the commutor of L in A, hence in L. Replacing d_t by $d_t^{p^n}$, we obtain elements $d_0, d_1, \cdots, d_i$ of A which are mutually commutative, satisfy the relation $(**)$, such that $(d_0^p, d_1^p, \cdots, d_i^p)-(d_0, d_1, \cdots, d_i)\in W_{i+1}(K)$.

Define a linear mapping $f_{i+1}\colon H_{i+1}\rightarrow A$ by

$$f_{i+1}(\delta_0^{e_0}\delta_1^{e_1}\cdots\delta_i^{e_i}) = d_0^{e_0}d_1^{e_1}\cdots d_i^{e_i} \quad (0\leq e_j<p)\,.$$

Then we see easily, using the relation $(**)$, that f_{i+1} gives the A-inner action of H_{i+1} on L. Since the induction assumption is trivial for $i=0$, this completes the proof of the proposition.

Corollary. *The elements $d_0, d_1, \cdots, d_{n-1}$ in Proposition 2 together with u form the canonical generators of Schmid-Witt type for A.*

3. Appendix

As we have remarked in the last part of the proof of Proposition 2, to prove Proposition 2, it needs only to show the existence of the mutually commutative elements $d_0, d_1, \cdots, d_{n-1}$ of A, satisfying in the group of Witt vectors the relations

$$u^{-1}(d_0, d_1, \cdots, d_{n-1})u = (d_0, d_1, \cdots, d_{n-1})+(1, 0, 0, \cdots, 0)\,,$$
$$(d_0^p, d_1^p, \cdots, d_{n-1}^p)-(d_0, d_1, \cdots, d_{n-1})\in W_n(K)\,.$$

Lemma. *Let $K[d_0, d_1, \cdots, d_{i-1}]/K$ be a cyclic extension of degree p^i whose Galois group is generated by σ such that*

$$(d_0^\sigma, d_1^\sigma, \cdots, d_{i-1}^\sigma) = (d_0, d_1, \cdots, d_{i-1})+(1, 0, 0, \cdots, 0)$$

in $W_i(K[d_0, d_1, \cdots, d_{i-1}])$.

Then if we define γ_i by

$$(d_0, d_1, \cdots, d_{i-1},0)+(1, 0, 0, \cdots, 0, 0) = (d_0, d_1, \cdots, d_{i-1}, \gamma_i)\,,$$

Trace $\gamma_i=1$.

Proof. The assertion is a direct consequence of the relation

$$p^i\underbrace{(1, 0, 0, \cdots, 0)}_{i+1-\text{factors}} = (0, 0, 0, \cdots, 1)$$

Proof of the existence of $d_0, d_1, \cdots, d_{n-1}$ with the given properties. We shall divide into two steps.

(1) L$=K[u]$ splits A, but $M=K[u^p]$ does not.

Consider the derivation D of L/K defined by $D(u) = u$. Then D is A-inner.

Thus there exists an elements d_0 of A such that $d_0u-ud_0=u$, or equivalently $u^{-1}d_0u=d_0+1$. Raising to p-th power, $u^{-1}d_0^pu=d_0^p+1$. Hence $d_0^p-d_0$ is in L. Replacing d_0 by $d_0^{p^n}$, we get an element d_0 of A, such that

$$\begin{cases} u^{-1}d_0u = d_0+1\,, \\ d_0^p-d_0\in K\,. \end{cases}$$

From the first relation, we have $d_0\in V_A(M)$. On the other hand, $V_A(M)$ is similar to $A\otimes M$ as M-algebra, and $[V_A(M):M]=p^2$. Since, by hypothesis, $A\otimes M$ is not a total matrix algebra, $V_A(M)$ is a division algebra. Thus $K[d_0]$ is a field, and in fact a cyclic extension of degree p of K.

Suppose we have already obtained mutually commutative elements d_0, d_1, $\cdots$, d_{i-1} of A, such that $K[d_0, d_1, \cdots, d_{i-1}]$ is a cyclic extension of degree p^i and in the group of Witt vectors the relations

$$u^{-1}(d_0, d_1, \cdots, d_{i-1})u = (d_0, d_1, \cdots, d_{i-1})+(1, 0, 0, \cdots, 0),$$
$$(d_0^p, d_1^p, \cdots, d_{i-1}^p)-(d_0, d_1, \cdots, d_{i-1})\in W_i(K)$$

hold. From the first relation, if we put $N=K[d_0, d_1, \cdots d_{i-1}]$, $v=u^{p^i}$ is contained in $V_A(N)$. On the other hand, $[N[v]:N]=p^{n-i}$ and $[V_A(N):N]=p^{2(n-i)}$. Thus $N[v]$ is a maximal commutative subalgebra of the N-algebra $V_A(N)$. Because of the linear disjointness, $N[v]$ is in fact a field. Let us now consider the derivation S of $N[v]/N$ defined by $S(v)=v$. Then, since S is $V_A(N)$-inner, there exists an element x of $V_A(N)$, such that $v^{-1}xv=x+1$. Since $u^{-1}Nu=N$, we have $u^{-1}V_A(N)u=V_A(N)$, and $\omega=u^{-1}xu-x\in V_A(N)$. Furthermore $v^{-1}\omega v=\omega$. Thus $\omega\in N$. We get inductively $x=u^{-1}xu-\omega=u^{-2}xu^2-\omega-u^{-1}\omega u=\cdots=v^{-1}xv-\omega-u^{-1}\omega u-\cdots-u^{-(p^i-1)}\omega u^{p^i-1}$. If we take into account that the inner automorphism by u induces a generator of the Galois group of N/K, we have Trace ${}_{N/K}\omega=1$. On the other hand, by the above lemma, Trace ${}_{N/K}\gamma_i=1$. Thus Trace $(\gamma_i-\omega)=0$. Hence there exists an element β of N, such that $\gamma_i-\omega=u^{-1}\beta u-\beta$. Thus if we put $d_i=x+\beta$, we have $u^{-1}d_iu-d_i=\gamma_i$. Thence d_i satisfies in the group of Witt vectors the relation

$$u^{-1}(d_0, d_1, \cdots, d_i)u = (d_0, d_1, \cdots, d_i)+(1, 0, \cdots, 0)\,.$$

By the similar procedure as above, we may assume that

$$(d_0^p, d_1^p, \cdots, d_i^p)-(d_0, d_1, \cdots, d_i)\in W_{i+1}(K)\,.$$

There remains to show that $N[d_i]$ is a field. From the above relation, $d_i^p-d_i=\lambda\in N$. Thus, to prove that $N[d_i]$ is a field, it suffices to show that the polynomial $X^p-X-\lambda$ is irreducible over N, or equivalently, that $\lambda\notin N^p-N$. Suppose on the contrary that $\lambda=\mu^p-\mu$ with $\mu\in N$. Then $d_i^p-d_i=\mu^p-\mu$. Now $0=u^{-1}(d_i^p-d_i)u-u^{-1}(\mu^p-\mu)u=(d_i+\gamma_i)^p-(d_i+\gamma_i)-(u^{-1}\mu u)^p-u^{-1}\mu u=$

$(\gamma_i - u^{-1}\mu u + \mu)^p - (\gamma_i - u^{-1}\mu u + \mu)$. Since we have $\gamma_i - u^{-1}\mu u + \mu \in N$, it is contained in the prime field. Thus Trace γ_i=Trace $(u^{-1}\mu u - \mu) = 0$. Contradiction! This completes the induction step, hence the proof is completed.

(2) $K[u^{p^i}]$ $(i>0)$ splits A, but $K[u^{p^{i+1}}]$ does not.

Take an algebra similar to A which contains $K[u^{p^i}]$ as a maximal commutative subalgebra. Then from the first part, there exist $\beta_0, \beta_1, \cdots, \beta_{i-1} \in K$ such that $B \overset{\sim}{\to} (a|\beta_0, \beta_1, \cdots, \beta_{i-1}]$. On the other hand, $(a|\beta_0, \beta_1, \cdots, \beta_{i-1}] \sim (a|0, 0, 0, \cdots, 0, \beta_0, \beta_1, \cdots, \beta_{i-1}]$. Thus $A \overset{\sim}{\to} (a|\underbrace{0, 0, \cdots, 0}_{n-i-\text{factors}}, \beta_0, \beta_1, \cdots, \beta_{i-1}]$.

From this we can easily construct $d_0, d_1, \cdots, d_{n-1}$.

Osaka University

References

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

[2] A. Hattori: *An application of inner-extension of higher derivations to p-algebras*, Osaka J. Math. **7** (1970), 307-312.

[3] ——————: *On higher derivations and related topics*, Seminar on Derivations and Cohomology of algebras (in Japanese), Research Institute for Mathematical Sciences, Kyoto University, 1970.

[4] M.E. Sweedler: *Cohomology of algebras over Hopf algebras*, Trans. Amer. Math. Soc. **133** (1968), 209-239.

[5] ——————: Hopf Algebras, Benjamin, 1969.

[6] E. Witt: *Zyklische Körper und Algebren der Characteristik p von Grad p^n*, Crelles J. **176** (1937), 31-44.