

A PAIR OF SUBALGEBRAS IN AN AZUMAYA ALGEBRA

KENJI YOKOGAWA

(Received January 26, 1981)

Introduction

It was shown by A.A. Albert [1] that a cyclic central simple (Azumaya) p -algebra has a purely inseparable extension field as a subalgebra. Hence such algebra contains a cyclic extension and a purely inseparable extension as subalgebras. On the other hand, a quaternion algebra $\mathbf{R}(i, j)$ contains two cyclic extensions $\mathbf{R}(i)$ and $\mathbf{R}(j)$ as subalgebras. These subalgebras are related by inner actions.

In this paper, we shall generalize the above results using Hopf algebras since we must treat separable and inseparable extensions simultaneously. Under certain conditions we shall show that if an Azumaya algebra A over a field K contains an H -Hopf Galois extension (in the sense of [3], [15]) of K as a maximal commutative subalgebra then A contains an H^* -Hopf Galois extension of K as a subalgebra. This is done in §1. In §2, we shall treat typical Hopf algebras and show that the classical results are typical examples of our results.

Throughout this paper, K will denote a field and H will denote a finite commutative co-commutative Hopf algebra over K . ε (resp. Δ , resp. λ) will denote augmentation (resp. diagonalization, resp. antipode) of H . Unadorned \otimes and Hom will mean \otimes_K and Hom_K . We shall denote by $-^*$ the functor $\text{Hom}_K(-, K)$. For Hopf algebras and Hopf Galois extensions we shall refer to [3], [10], [15] and [16].

1. Hopf Galois extension $v(H)$

Let A be a K -Azumaya algebra which contains an H -Hopf Galois extension L of K as a maximal commutative subalgebra. Then the H -action on L is extended innerly to the action on A and A is a smash product algebra $L \#_\sigma H$ (c.f. [14] cor. 3.7 and 3.8). But in general A would not become an H -module if we extend the H -action on L innerly to A . The following Proposition is fundamental.

Proposition 1. *The following conditions are equivalent.*

- (i) A becomes an H -module algebra.

(ii) *The value of 2-cocycle σ is contained in K , i.e. $\sigma(g \otimes h) \in K$ for any $g, h \in H$.*

Proof. (i) \Rightarrow (ii). This follows essentially from F.W. Long [8]. Let $v: H \rightarrow A$ be a homomorphism which gives an A -inner action. Thus v satisfies $h \cdot s = \sum_{(h)} v(h_{(1)})s v^{-1}(h_{(2)})$, $s \in L$ or equivalently $v(h)s = \sum_{(h)} (h_{(1)} \cdot s)v(h_{(2)})$, and $v(l_H) = l_A$, v^{-1} is the inverse of v in a convolution algebra $\text{Hom}(H, A)$. Since A is an H -module algebra, $(gh) \cdot a = g \cdot (h \cdot a)$, $a \in A$. Using this relation we get

$$\sum_{(g), (h)} v(g_{(1)}h_{(1)})av^{-1}(g_{(2)}h_{(2)}) = \sum_{(g), (h)} v(g_{(1)})v(h_{(1)})av^{-1}(h_{(2)})v^{-1}(g_{(2)}).$$

Thus

$$\sum_{(g), (h)} av^{-1}(g_{(1)}h_{(1)})v(g_{(2)})v(h_{(2)}) = \sum_{(g), (h)} v^{-1}(g_{(1)}h_{(1)})v(g_{(2)})v(h_{(2)})a \text{ for any } a \in A.$$

Since A is K -central, we get

$$\sum_{(g), (h)} v^{-1}(g_{(1)}h_{(1)})v(g_{(2)})v(h_{(2)}) \in K.$$

Thus the associated 2-cocycle

$$\begin{aligned} \sigma(g \otimes h) &= \sum_{(g), (h)} v(g_{(1)})v(h_{(1)})v^{-1}(g_{(2)}h_{(2)}) \\ &= \sum_{(g), (h)} v(g_{(1)}h_{(1)})v^{-1}(g_{(2)}h_{(2)})v(g_{(3)})v(h_{(3)})v^{-1}(g_{(4)}h_{(4)}) \end{aligned}$$

is K -valued.

(ii) \Rightarrow (i). Let σ be a K -valued 2-cocycle and $\bar{\sigma}$ be the associated normal cocycle defined by

$$\bar{\sigma}(g \otimes h) = \sum_{(g)} \sigma(g_{(1)} \otimes h) \sigma^{-1}(g_{(2)} \otimes 1).$$

Then $\bar{\sigma}$ is cohomologous to σ , $\bar{\sigma}$ is also K -valued and $\bar{\sigma}(1 \otimes h) = \bar{\sigma}(h \otimes 1) = \varepsilon(h)$, $h \in H$. Thus we may assume that σ itself is a normal 2-cocycle. Let $v: H \rightarrow A = L \#_{\sigma} H$ be the homomorphism defined by $v(h) = 1 \# h$. Then v gives an A -inner action and carries 1_H to $1_A = 1 \# 1$. Reversing the proof of (i) \Rightarrow (ii), we get that A is an H -module algebra. This completes the proof.

REMARK. If H is a group ring or a Hopf algebra whose simple subcoalgebras are of the form Kh for $h \in H$ and L is only a simple subalgebra (not necessarily commutative), then by Skolem-Noether and Sweedler [9], the action of H on L is A -inner (say by $v: H \rightarrow A$). From the proof of Proposition 1, we get that A becomes an H -module algebra is equivalent to $\sum_{(g), (h)} v^{-1}(g_{(1)}h_{(1)})v(g_{(2)})v(h_{(2)}) \in K$.

Corollary 2. *Under the equivalent conditions of Proposition 1, let v be a homomorphism which gives an A -inner action and makes A an H -module algebra. Then the K -module $v(H) \subset A$ forms a K -subalgebra.*

Proof. We have

$$\begin{aligned}
v(g)v(h) &= \sum_{(\mathcal{E}), (h)} v(g_{(1)})v(h_{(1)})v^{-1}(g_{(2)}h_{(2)})v(g_{(3)}h_{(3)}) \\
&= \sum_{(\mathcal{E}), (h)} \sigma(g_{(1)} \otimes h_{(1)})v(g_{(2)}h_{(2)}) \\
&= v\left(\sum_{(\mathcal{E}), (h)} \sigma(g_{(1)} \otimes h_{(1)})g_{(2)}h_{(2)}\right).
\end{aligned}$$

Hence $v(H)$ is closed under multiplication and $v(H)$ has an identity $v(1_H)=1_A$. This completes the proof.

REMARK. If H is a group ring then the converse of Corollary 2 holds as is easily proved.

From now, we shall always assume the equivalent conditions of Proposition

1. We shall define an H^* -action on $v(H)$ by

$$x \cdot v(h) = \sum_{(h)} x(h_{(1)})v(h_{(2)}), \quad x \in H^*.$$

Proposition 3. *Through the natural isomorphism $v(H) \cong H$, the H^* -action on $v(H)$ is the canonical left H^* -structure of H and $v(H)$ becomes an H^* -module algebra.*

Proof. Let σ be an associated 2-cocycle, then

$$\begin{aligned}
x \cdot (v(g)v(h)) &= x \cdot \left(\sum_{(\mathcal{E}), (h)} \sigma(g_{(1)} \otimes h_{(1)})v(g_{(2)}h_{(2)})\right) \\
&= \sum_{(h), (h)} \sigma(g_{(1)} \otimes h_{(1)})x(g_{(2)}h_{(2)})v(g_{(3)}h_{(3)}) \\
&= \sum_{(\mathcal{E}), (h)} x(g_{(1)}h_{(1)})\sigma(g_{(2)} \otimes h_{(2)})v(g_{(3)}h_{(3)}) \\
&= \sum_{(\mathcal{E}), (h), (x)} x_{(1)}(g_{(1)})x_{(2)}(h_{(1)})v(g_{(2)})v(h_{(2)}) \\
&= \sum_{(\mathcal{E}), (h), (x)} x_{(1)}(g_{(1)})v(g_{(2)})x_{(2)}(h_{(1)})v(h_{(2)}) \\
&= \sum_{(x)} (x_{(1)} \cdot v(g)) (x_{(2)} \cdot v(h)).
\end{aligned}$$

$$\begin{aligned}
\text{And } (xy) \cdot v(h) &= \sum_{(h)} (xy)(h_{(1)})v(h_{(2)}) = \sum_{(h)} x(h_{(1)})y(h_{(2)})v(h_{(3)}) \\
&= x \cdot \left(\sum_{(h)} y(h_{(1)})v(h_{(2)})\right) = x \cdot (y \cdot v(h)), \quad x, y \in H^*.
\end{aligned}$$

$$\text{And } x \cdot 1 = x \cdot v(1) = x(1)v(1) = x(1) = \varepsilon_{H^*}(x).$$

Thus $v(H)$ forms an H^* -module algebra. That this structure is a canonical one follows easily. This completes the proof.

Proposition 4. *Let $v': H \rightarrow A$ be another homomorphism such that $v'(1_H)=1_A$. Then v' gives an A -inner action, if and only if, there exists a unit $\rho \in \text{Hom}(H, L)$ such that $v' = \rho v$. Further if $\rho \in \text{Hom}(H, K)$ then $v(H) \cong v'(H)$ as H -module algebras.*

Proof. “if part” is easy, we shall prove “only if part”. Put $\rho(h) =$

$\sum_{\langle h \rangle} v'(h_{(1)})v^{-1}(h_{(2)})$. Since $v^{-1}(h) = v(\lambda(h))$ we have for any $s \in L$, $\rho(h)s = \sum_{\langle h \rangle} v'(h_{(1)})v^{-1}(h_{(2)})s = \sum_{\langle h \rangle} v'(h_{(1)})v(\lambda(h_{(2)}))s = \sum_{\langle h \rangle} v'(h_{(1)}) (\lambda(h_{(2)}) \cdot s) v(\lambda(h_{(3)})) = \sum_{\langle h \rangle} s v'(h_{(1)})v^{-1}(h_{(2)}) = s\rho(h)$. L is a maximal commutative subalgebra, so $\rho \in \text{Hom}(H, L)$. Further if $\rho \in \text{Hom}(H, K)$, then the homomorphism $v'(H) \ni v'(h) \mapsto \sum_{\langle h \rangle} v(\rho(h_{(1)})h_{(2)}) \in v(H)$ is a desired isomorphism. This completes the proof.

Until now, we have not used the commutativity of H . Next we shall utilize the commutativity of H and show that $v(H)$ is an H^* -Hopf Galois extension in the sense of [15], [16]. As before, let σ be the associated normal 2-cocycle. Then σ is an element of $\text{Hom}(H \otimes H, K) \cong H^* \otimes H^*$. Since σ is a 2-cocycle, we have

$$\begin{aligned} & \sum_{\langle f \rangle, \langle g \rangle} \sigma(f_{(1)}g_{(1)} \otimes h) \sigma(f_{(2)} \otimes g_{(2)}) \\ &= \sum_{\langle f \rangle, \langle g \rangle, \langle h \rangle} (f_{(1)} \cdot \sigma(g_{(1)} \otimes h_{(1)})) \sigma(f_{(2)} \otimes g_{(2)}h_{(2)}) \\ &= \sum_{\langle f \rangle, \langle g \rangle, \langle h \rangle} \varepsilon(f_{(1)}) \sigma(g_{(1)} \otimes h_{(1)}) \sigma(f_{(2)} \otimes g_{(2)}h_{(2)}) \\ &= \sum_{\langle g \rangle, \langle h \rangle} \sigma(g_{(1)} \otimes h_{(1)}) \sigma(f \otimes g_{(1)}h_{(1)}). \end{aligned}$$

Thus

$$((\Delta_{H^*} \otimes 1)\sigma)(\sigma \otimes 1) = (1 \otimes \sigma)((1 \otimes \Delta_{H^*})\sigma).$$

This means that $\sigma \in H^* \otimes H^*$ is a unit-valued Harrison 2-cocycle. In $v(H)$, multiplication is given by the formula;

$$v(g)v(h) = \sum_{\langle g \rangle, \langle h \rangle} \sigma(g_{(1)} \otimes h_{(1)})v(g_{(2)}h_{(2)}).$$

Thus $v(H) = H(\sigma)$ in the sense of [16] §2. Since K is a field and $\text{Hom}(H \otimes H, L)$ is finite dimensional, $\sigma^{-1} \in \text{Hom}(H \otimes H, L)$ is integral over $\text{Hom}(H \otimes H, K)$. Hence $\sigma^{-1} \in \text{Hom}(H \otimes H, K)$. By [16] Theorem 2.3, we get

Theorem 5. *Under the equivalent conditions of Proposition 1, $v(H)$ is an H^* -Hopf Galois extension of K .*

Next we shall consider the A -innerization of H^* -Hopf Galois extension $v(H)$ of K . For this purpose, we first consider the normalization of 2-cocycles. Let $u = \sum_i u_i \otimes u_{2i} \in H \otimes H$ be a unit-valued Harrison 2-cocycles. We shall call u is a *normal 2-cocycle* if $\varepsilon(\sum_i u_i u_{2i}) = 1$. As to this, we have the following;

Lemma 6. *Let $u = \sum_i u_i \otimes u_{2i} \in H \otimes H$ be a unit-valued Harrison 2-cocycle, then*

$$\varepsilon(\sum_i u_i u_{2i}) = \sum_i \varepsilon(u_{1i})u_{2i} = \sum_i u_{1i} \varepsilon(u_{2i}).$$

Further we have

$$\sum_i \lambda(u_{1_i})u_{2_i} = \sum_i u_{1_i}\lambda(u_{2_i}), \text{ where } \lambda \text{ is antipode of } H.$$

Proof. Since u is a 2-cocycle,

$$\begin{aligned} (*) & \quad \left(\sum_i 1 \otimes u_{1_i} \otimes u_{2_i} \right) \left(\sum_{i, (u_{1_i})} u_{1_i} \otimes u_{2_{i(1)}} \otimes u_{2_{i(2)}} \right) \\ & = \left(\sum_{i, (u_{1_i})} u_{1_{i(1)}} \otimes u_{1_{i(2)}} \otimes u_{2_i} \right) \left(\sum_i u_{1_i} \otimes u_{2_i} \otimes 1 \right). \end{aligned}$$

Applying $\varepsilon \otimes \varepsilon \otimes 1$ on both sides of (*), we get

$$\left(\sum_i \varepsilon(u_{1_i})u_{2_i} \right) \left(\sum_i \varepsilon(u_{1_i})u_{2_i} \right) = \left(\sum_i \varepsilon(u_{1_i})u_{2_i} \right) \left(\varepsilon \left(\sum_i u_{1_i}u_{2_i} \right) \right).$$

Hence

$$\sum_i \varepsilon(u_{1_i})u_{2_i} = \varepsilon \left(\sum_i u_{1_i}u_{2_i} \right).$$

Next applying $1 \otimes \varepsilon \otimes \varepsilon$ on both sides of (*), we get

$$\varepsilon \left(\sum_i u_{1_i}u_{2_i} \right) \left(\sum_i u_{1_i}\varepsilon(u_{2_i}) \right) = \left(\sum_i u_{1_i}\varepsilon(u_{2_i}) \right) \left(\sum_i u_{1_i}\varepsilon(u_{2_i}) \right).$$

Hence we get

$$\varepsilon \left(\sum_i u_{1_i}u_{2_i} \right) = \sum_i u_{1_i}\varepsilon(u_{2_i}).$$

Finally applying $1 \otimes \lambda \otimes 1$ to (*) and then applying a contraction map, we get

$$\left(\sum_i \lambda(u_{1_i})u_{2_i} \right) \left(\sum_i u_{1_i}\varepsilon(u_{2_i}) \right) = \left(\sum_i \varepsilon(u_{1_i})u_{2_i} \right) \left(\sum_i u_{1_i}\lambda(u_{2_i}) \right).$$

Hence we get the last relation. This completes the proof.

In an H -Hopf Galois extension $H^*(u)$ (in the sense of [16] §2) of K , an identity element is $\varepsilon \left(\left(\sum_i u_{1_i}u_{2_i} \right)^{-1} \right) \varepsilon$ ([16] Theorem 2.3). Let $w = \sum_i u_{1_i}\varepsilon(u_{2_i})$ and put $u' = (w \otimes w)^{-1} u \Delta(w)$. Then u is cohomologous to u' and $H^*(u) \cong H^*(u')$ by [16] Theorem 2.4. Moreover u' is a normal 2-cocycle and the identity of $H^*(u')$ is ε . Now we are ready to consider an inner action of an H^* -Hopf Galois extension $v(H)$ of K and from now we shall always consider normal cocycles. We shall write an H -Hopf Galois extension L which is a maximal commutative subalgebra of A as $H^*(u)$.

The following is necessary later.

Lemma 7. $\varepsilon(\lambda(h)) = \varepsilon(h)$ for all $h \in H$.

Proof. We have $\varepsilon(\lambda(h)) = \varepsilon \left(\lambda \left(\sum_{(h)} h_{(1)} \varepsilon(h_{(2)}) \right) \right) = \sum_{(h)} \varepsilon(\lambda(h_{(1)})) \varepsilon(h_{(2)})$
 $= \varepsilon \left(\sum_{(h)} \lambda(h_{(1)}) h_{(2)} \right) = \varepsilon(\varepsilon(h)) = \varepsilon(h).$

Let $V: H^* \rightarrow H^*(u) \subset A$ be the homomorphism defined by

$$(V(f))(h) = f(\lambda(h)), f \in H^*.$$

Then Lemma 7 ensures that V carries an identity ε of H^* to an identity ε of $H^*(u)$. We remark that $H^*(u) = H^*$ as a left H -module, multiplication is given by $(f \cdot g)(h) = \sum_{i, (h)} f(u_i, h_{(1)}) \cdot g(u_i, h_{(2)})$, $f, g \in H^*$, $h \in H$. We shall show that V gives an A -inner action of an H^* -Hopf Galois extension $v(H)$ of K . Since v gives an A -inner action of $L = H^*(u)$ of K , we have

$$v(h)f' = \sum_{(h)} (h_{(1)} \cdot f')v(h_{(2)}), f' \in H^*(u).$$

Thus for $f \in H^*$;

$$\begin{aligned} \sum_{(f)} (f_{(1)} \cdot v(h))V(f_{(2)}) &= \sum_{(f), (h)} f_{(1)}(h_{(1)})v(h_{(2)})V(f_{(2)}) \\ &= \sum_{(f), (h)} f_{(1)}(h_{(1)}) (h_{(2)} \cdot V(f_{(2)}))v(h_{(3)}) \\ &= \sum_{(f), (h)} f_{(1)}(h_{(1)}) (V(f_{(2)})(h_{(2)}))V(f_{(3)})v(h_{(3)}) \\ &= \sum_{(f), (h)} f_{(1)}(h_{(1)})f_{(2)}(\lambda(h_{(2)}))V(f_{(3)})v(h_{(3)}) \\ &= \sum_{(f), (h)} f_{(1)}(h_{(1)}\lambda(h_{(2)}))V(f_{(2)})v(h_{(3)}) \\ &= \sum_{(f), (h)} f_{(1)}(\varepsilon(h_{(1)}))V(f_{(2)})v(h_{(2)}) \\ &= \sum_{(f)} f_{(1)}(1)V(f_{(2)})v(h) = V(f)v(h). \end{aligned}$$

Next we shall show that V is invertible. Let $V': H^* \rightarrow H^*(u) \subset A$ be the homomorphism defined by

$$(V'(f))(h) = f((\sum u_i \lambda_{2_i}(u_{2_i}))^{-1}h), f \in H^*.$$

Then

$$\begin{aligned} ((V' * V)(f))(h) &= (\sum_{(f)} V'(f_{(1)}) \cdot V(f_{(2)}))(h) \\ &= \sum_{(f), i, (h)} V'(f_{(1)})(u_i, h_{(1)})V(f_{(2)})(u_i, h_{(2)}) \\ &= \sum_{(f), i, (h)} f_{(1)}((\sum_j u_{1_j} \lambda(u_{2_j}))^{-1}u_i, h_{(1)})f_{(2)}(\lambda(h_{(2)})\lambda(u_{2_i})) \\ &= f(\sum_{i, (h)} (\sum_j u_{1_j} \lambda(u_{2_j}))^{-1}u_i, h_{(1)}\lambda(h_{(2)})\lambda(u_{2_i})) \\ &= f(1)\varepsilon(h). \\ ((V * V')(f))(h) &= \sum_{(f)} (V(f_{(1)}) \cdot V'(f_{(2)}))(h) \\ &= \sum_{(f), (h), i} V(f_{(1)})(u_i, h_{(1)})V'(f_{(2)})(u_i, h_{(2)}) \\ &= \sum_{(f), (h), i} f_{(1)}(\lambda(h_{(1)})\lambda(u_{1_i}))f_{(2)}((\sum_j u_{1_j} \lambda(u_{2_j}))^{-1}u_i, h_{(2)}) \\ &= f(\varepsilon(h) (\sum_i \lambda(u_{1_i})u_{2_i}) \cdot (\sum_j u_{1_j} \lambda(u_{2_j}))^{-1}), \end{aligned}$$

which is equal to $f(1)\varepsilon(h)$ by Lemma 6. Thus V is invertible. That $V(H^*) =$

$H^*(u)$ is clear.

Finally we shall consider the 2-cocycle τ arising from V . Since τ is defined by the formula;

$$\tau(f \otimes g) = \sum_{(f), (g)} V(f_{(1)}) \cdot V(g_{(1)}) \cdot V^{-1}(f_{(2)}g_{(2)}), f, g \in H^*,$$

we get

$$\begin{aligned} (\tau(f \otimes g))(h) &= \left(\sum_{(f), (g)} (V(f_{(1)}) \cdot V(g_{(1)}) \cdot V^{-1}(f_{(2)}g_{(2)})) \right) (h) \\ &= \sum_{(f), (g), (h), i} (V(f_{(1)}) \cdot V(g_{(1)})) (u_i h_{(1)}) (V^{-1}(f_{(2)}g_{(2)})) (u_2 h_{(2)}) \\ &= \sum_{(f), (g), (h), (u_{1_i}), i, j} (V(f_{(1)})) (u_{1_j} u_{1_{(1)}} h_{(1)}) (V(f_{(2)})) (u_{2_j} u_{1_{(2)}} h_{(2)}) \\ &\quad \times (V^{-1}(f_{(2)}g_{(2)})) (u_2 h_{(3)}) \\ &= \sum_{(f), (g), (h), (u_{1_i}), i, j} f_{(1)}(\lambda(u_{1_j})\lambda(u_{1_{(1)}})\lambda(h_{(1)}))g_{(1)}(\lambda(u_{2_j})\lambda(u_{1_{(2)}})\lambda(h_{(2)})) \\ &\quad \times (f_{(2)}g_{(2)}) \left(\left(\sum_k u_{1_k} \lambda(u_{2_k}) \right)^{-1} u_2 h_{(3)} \right) \\ &= \sum_{(g), (h), (u_{1_i}), (u_{2_i}), (M), i, j} f_{(1)}(\lambda(u_{1_j})\lambda(u_{1_{(1)}})\lambda(h_{(3)}))g_{(1)}(\lambda(u_{2_j})\lambda(u_{1_{(2)}})\lambda(h_{(2)})) \\ &\quad \times f_{(2)}(M_{(1)}u_{2_{i(1)}}h_{(3)})g_{(2)}(M_{(2)}u_{2_{i(2)}}h_{(4)}), \quad \text{where we put} \\ M &= \left(\sum_k u_{1_k} \lambda(u_{2_k}) \right)^{-1} \\ &= \sum_{(h), (u_{1_i}), (u_{2_i}), (M), i, j} f(\lambda(u_{1_j})\lambda(u_{1_{(1)}})\lambda(h_{(1)}))M_{(1)}u_{2_{i(1)}}h_{(2)}g(\lambda(u_{2_j})\lambda(u_{1_{(2)}})) \\ &\quad \times \lambda(h_{(3)})M_{(2)}u_{2_{i(2)}}h_{(4)}) \\ &= \sum_{(u_{1_i}), (u_{2_i}), (M), i, j} f(\lambda(u_{1_j}u_{1_{(1)}}))M_{(1)}u_{2_{i(1)}}g(\lambda(u_{2_j}u_{1_{(2)}}))M_{(2)}u_{2_{i(2)}}\varepsilon(h). \end{aligned}$$

In $H^*(u)$, K is contained as $K\varepsilon$. Thus τ is also K -valued. Summing up, we get the following

Theorem 8. *Let A be a K -Azumaya algebra which contains an H -Hopf Galois extension $H^*(u)$ of K as a maximal commutative subalgebra and assume that the associated 2-cocycle is K -valued. Then there exists a subalgebra $v(H)$ which is an H^* -Hopf Galois extension of K . $H^*(u)$ and $v(H)$ are related as follows; there exist homomorphisms $v : H^*(u) \rightarrow v(H)$ and $V : v(H) \rightarrow H^*(u) \subset A$ such that v gives an A -inner action which extends the H -action of an H -Hopf Galois extension $H^*(u)$ of K and V gives an A -inner action which extends the H^* -action of an H^* -Hopf Galois extension $v(H)$ of K .*

2. Dual of Hopf algebras

First we shall prove two lemmas which exhibit the structure of dual of group rings as Hopf algebras.

Lemma 9. *Let p be a prime number which is not equal to the characteristic*

of a field K and G be a cyclic group of order p^n . We assume that K contains a primitive p^n -th root of 1. Then $(KG)^* \cong KG$ as Hopf algebras.

Proof. Let G^* be the character group of G , then $(KG)^* \cong KG^* \cong KG$ and this isomorphism is in fact an isomorphism of Hopf algebras as is easily seen.

REMARK. Theorem 8 combined with Lemma 9 explains the well-known phenomenon on quaternion algebras.

Next we shall review a Hopf algebra H_n introduced by A. Hattori [4] and K. Kosaki [7].

Let K be a field of characteristic $p \neq 0$. Then

$H_n = K[X_0, X_1, \dots, X_{n-1}] / (X_0^p - X_0, X_1^p - X_1, \dots, X_{n-1}^p - X_{n-1})$ as a K -algebra, we shall write the class of X_i as x_i .

$$\Delta(x_i) = S_i(x_0 \otimes 1, \dots, x_i \otimes 1; 1 \otimes x_0, \dots, 1 \otimes x_i)$$

$$\varepsilon(x_i) = 0$$

$$\lambda(x_i) = -x_i$$

where S_0, \dots, S_{n-1} are polynomials which define the additive structure of Witt vectors.

In particular,

$$\Delta(x_0) = x_0 \otimes 1 + 1 \otimes x_0$$

$$\Delta(x_1) = x_1 \otimes 1 + 1 \otimes x_1 + \sum_{k=1}^{p-1} \frac{1}{k!(p-1)!} x_0^k \otimes x_0^{p-k}.$$

A. Hattori first defined H_n as a dual of a cyclic group ring. Here for completeness we shall prove the following;

Lemma 10. *Let K be a field of characteristic $p \neq 0$ and $G = \{1, \theta, \dots, \theta^{p^n-1}\}$ be a cyclic group of order p^n . Then $(KG)^* \cong H_n$ as Hopf algebras.*

Proof. Let $\{e_i\} \subset (KG)^*$, $i=0, 1, \dots, p^n-1$, be a K -basis of $(KG)^*$ defined by $e_i(\theta^j) = \delta_{i,j}$ (Kronecker delta). We shall define a homomorphism $\phi: H_n \rightarrow (KG)^*$ as follows;

$$\phi(x_j) = \sum_{i=1}^{p^n-1} a_{ji} e_i, \quad j = 0, 1, \dots, n-1$$

where coefficients $a_{ji} \in \mathbf{Z}/p\mathbf{Z}$ are defined by

$$\begin{cases} a_{j0} = 0 & \text{for all } j \\ (a_{01}, a_{11}, \dots, a_{n-1,1}) = (1, 0, \dots, 0) \\ (a_{0,i}, a_{1,i}, \dots, a_{n-1,i}) = \underbrace{(1, 0, \dots, 0) + \dots + (1, 0, \dots, 0)}_{i \text{ terms}} \end{cases}$$

where “+” means the sum of Witt vectors.

We shall show that ϕ is a Hopf algebra isomorphism step by step. That $(\phi(x_j))^p = \phi(x_j)$ is an immediate consequence of $a_{j_i} \in \mathbf{Z}/p\mathbf{Z}$. Hence ϕ is an algebra homomorphism.

To see that ϕ is an epimorphism, we shall prove $K[\phi(x_0), \dots, \phi(x_j)] \cong K[\phi(x_0), \dots, \phi(x_j), \phi(x_{j+1})]$, then the dimension arguments will ensure that ϕ is an epimorphism. But $(a_{0\ p^m}, a_{1\ p^m}, \dots, a_{n-1\ p^m}) = \underbrace{(1, 0, \dots, 0) + \dots + (1, 0, \dots, 0)}_{p^m \text{ terms}} = \underbrace{(0, 0, \dots, 0, 1, 0, \dots, 0)}_{m+1}$

Thus the above inclusion is strict.

Next let Δ^* be a diagonal map of $(KG)^*$, then

$$(\Delta^*(\phi(x_j))) (\theta^k \otimes \theta^m) = \phi(x_j) (\theta^{k+m}) = a_{j\ k+m}.$$

On the other hand

$$\begin{aligned} ((\phi \otimes \phi)\Delta(x_j)) (\theta^k \otimes \theta^m) &= ((\phi \otimes \phi)(S_j(x_0 \otimes 1, \dots, x_j \otimes 1; 1 \otimes x_0, \dots, 1 \otimes x_j))) (\theta^k \otimes \theta^m) \\ &= S_j(a_{0\ k}, \dots, a_{j\ k}; a_{0\ m}, \dots, a_{j\ m}). \end{aligned}$$

But

$$\begin{aligned} (a_{0\ k+m}, a_{1\ k+m}, \dots, a_{n-1\ k+m}) &= \underbrace{(1, 0, \dots, 0) + \dots + (1, 0, \dots, 0)}_{k+m \text{ terms}} \\ &= (a_{0\ k}, \dots, a_{n-1\ k}) + (a_{0\ m}, \dots, a_{n-1\ m}) \\ &= (S_0(a_{0\ k}; a_{0\ m}), S_1(a_{0\ k}, a_{1\ k}; a_{0\ m}, a_{1\ m}), \dots, S_{n-1}(a_{0\ k}, a_{1\ k}, \dots, a_{n-1\ k}; a_{0\ m}, a_{1\ m}, \\ &\quad \dots, a_{n-1\ m})) \end{aligned}$$

Thus

$$\Delta^*((x_j)) = (\phi \otimes \phi)\Delta(x_j).$$

Let ε^* be an augmentation of $(KG)^*$, then $\varepsilon^*(\phi(x_j)) = 0$ follows easily from $a_{j\ 0} = 0$. Hence

$$\varepsilon^*(\phi(x_j)) = 0 = \phi(\varepsilon(x_j)).$$

Finally let λ^* be an antipode of $(KG)^*$, then

$$\begin{aligned} (\lambda^*(\phi(x_j))) (\theta^m) &= (\phi(x_j)) (\theta^{p^n-m}) = a_{j\ p^n-m} \\ (\phi(\lambda(x_j))) (\theta^m) &= (\phi(-x_j)) (\theta^m) = -a_{j\ m} \end{aligned}$$

But

$$\begin{aligned} (S_0(a_{0\ m}; a_{0\ p^n-m}), S_1(a_{0\ m}, a_{1\ m}; a_{0\ p^n-m}, a_{1\ p^n-m}), \dots, \\ S_{n-1}(a_{0\ m}, \dots, a_{n-1\ m}; a_{0\ p^n-m}, \dots, a_{n-1\ p^n-m})) \\ = (a_{0\ m}, a_{1\ m}, \dots, a_{n-1\ m}) + (a_{0\ p^n-m}, a_{1\ p^n-m}, \dots, a_{n-1\ p^n-m}) \\ = (1, 0, \dots, 0) + \underbrace{\dots + (1, 0, \dots, 0)}_{m \text{ terms}} + \underbrace{\dots + (1, 0, \dots, 0)}_{p^n-m \text{ terms}} \end{aligned}$$

$$\begin{aligned}
&= \underbrace{(1, 0, \dots, 0) + \dots + (1, 0, \dots, 0)}_{p^n \text{ terms}} \\
&= (0, 0, \dots, 0)
\end{aligned}$$

From this, we can get easily by induction that

$$a_{j \ m} + a_{j \ p^n - m} = 0.$$

This completes the proof.

REMARK. In Lemma 10, if $n=1$ then $\phi(x_0) = \sum_{k=1}^{p-1} \bar{k}e_k$, $\bar{k} \in \mathbf{Z}/p\mathbf{Z}$. This is proved in different ways by F.W. Long [8] Proposition 5.1.

Next we shall prove the following proposition in two ways. One uses Witt vector computations and another utilizes the fact that H_n is a dual of a group ring. The latter is due to Prof. A. Hattori, who kindly informed me such a proof.

Proposition 11. *Let K be a field of characteristic $p \neq 0$ and L be a commutative K -algebra. If L/K is an H_n -Hopf Galois extension, then L is a purely inseparable K -algebra in the sense of M.E. Sweedler [11].*

Proof I. We shall show that $s^{p^n} \in K$ for any $s \in L$, then by [11] Lemma 1 we shall easily get the assertion. To this, we shall show that $x_j \cdot s^{mp^{j+1}} = 0$ by induction.

$$\begin{aligned}
x_0 \cdot s^{mp} &= x_0(s^{mp-1}) = S_0((x_0 \cdot s)^{s^{mp-1}}; s(x_0 \cdot s^{mp-1})) \\
&= (x_0 \cdot s)^{s^{mp-1}} + s(x_0 \cdot s^{mp-1}) = (x_0 \cdot s)^{s^{mp-1}} + s((x_0 \cdot s)^{s^{mp-2}} + s(x_0 \cdot s^{mp-2})) \\
&= \dots = \underbrace{(x_0 \cdot s)^{s^{mp-1}} + \dots + (x_0 \cdot s)^{s^{mp-1}}}_{mp \text{ terms}} = 0.
\end{aligned}$$

Next we assume that the assertion is valid for numbers smaller than j , then

$$\begin{aligned}
x_j \cdot s^{mp^{j+1}} &= x_j \cdot (s^{p^j} s^{p^j(m p-1)}) = S_j((x_0 \cdot s^{p^j})^{s^{p^j(m p-1)}}, \dots, \\
&\quad (x_j \cdot s^{p^j})^{s^{p^j(m p-1)}}, s^{p^j}(x_0 \cdot s^{p^j(m p-1)}), \dots, s^{p^j}(x_j \cdot s^{p^j(m p-1)})) \\
&= S_j(0, 0, \dots, 0, (x_j \cdot s^{p^j})^{s^{p^j(m p-1)}}, s^{p^j}(x_0 \cdot s^{p^j(m p-1)}), \dots, s^{p^j}(x_j \cdot s^{p^j(m p-1)})) \\
&= (x_j \cdot s^{p^j})^{s^{p^j(m p-1)}} + s^{p^j}(x_j \cdot s^{p^j(m p-1)}) \\
&= (x_j \cdot s^{p^j})^{s^{p^j(m p-1)}} + s^{p^j}((x_j \cdot s^{p^j})^{s^{p^j(m p-2)}} + s^{p^j}(x_j \cdot s^{p^j(m p-2)})) \\
&= \dots = \underbrace{(x_j \cdot s^{p^j})^{s^{p^j(m p-1)}} + \dots + (x_j \cdot s^{p^j})^{s^{p^j(m p-1)}}}_{mp \text{ terms}} \\
&= 0.
\end{aligned}$$

In particular,

$$x_j \cdot s^{\rho^n} = 0 \text{ for any } s \in L, j = 0, 1, \dots, n-1.$$

Since $\varepsilon(x_j) = 0$,

$$x_j \cdot s^{\rho^n} = 0 = \varepsilon(x_j) s^{\rho^n}.$$

This means $s^{\rho^n} \in L^{\rho^n}$ which is equal to K since L/K is assumed to be an H_n -Hopf Galois extension. This completes the proof.

Proof II. Since L/K is an H_n -Hopf Galois extension, we have isomorphisms: $L \otimes L \cong \text{Hom}(H, L) \cong H^* \otimes L \cong KG \otimes L \cong K[X]/(X^{\rho^n}) \otimes L \cong L[X]/(X^{\rho^n})$ where G is a cyclic group of p^n . Comparing the number of idempotents of both sides, we see that L has no non-trivial idempotents. Hence $L/\text{rad}(L) = \bar{L}$ is a field ($\text{rad}(L)$ means Jacobson radical of L). Let Ω be an algebraic closure of K , then we have an isomorphism $(L \otimes \Omega) \otimes_{\Omega} (L \otimes \Omega) \cong (L \otimes \Omega)[X]/(X^{\rho^n})$. By the similar arguments, $(L \otimes \Omega)/\text{rad}(L \otimes \Omega)$ and $\bar{L} \otimes \Omega/\text{rad}(\bar{L} \otimes \Omega)$ are fields (necessarily isomorphic to Ω). If there are m distinct K -embeddings $\sigma_i: \bar{L} \rightarrow \Omega$ then there are m distinct Ω -homomorphisms: $\bar{L} \otimes \Omega \ni a \otimes b \mapsto \sigma_i(a)b \in \Omega$. Thus $\bar{L} \otimes \Omega/\text{rad}(\bar{L} \otimes \Omega)$ must contain a direct sum of m copies of Ω . Hence $m=1$, this means that \bar{L}/K is a purely inseparable extension. By [11] Corollary 13, we get the Proposition.

REMARK. Theorem 8 combined with Lemma 10 and Proposition 11 explains the results of A.A. Albert.

References

- [1] A.A. Albert: Structure of algebras, Amer. Math. Soc. Colloq. Publ. XXIV, 1939.
- [2] M. Beattie: *A direct sum decomposition for the Brauer group of H -module algebras*, J. Algebra **43** (1976), 686–693.
- [3] S.U. Chase and M.E. Sweedler: Hopf algebras and Galois theory, Lect. Note in Math. 97, Springer, 1968.
- [4] A. Hattori: *On higher derivations and related topics*, Seminar on Derivations and Cohomology of algebras (in Japanese), Research Institute for Mathematical Sciences, Kyoto University, 1970.
- [5] A. Hattori: *An application of inner-extension of higher derivations to p -algebras*, Osaka J. Math. **7** (1970), 307–312.
- [6] J.M. Hood: *Central simple p -algebras with purely inseparable subfields*, J. Algebra **17** (1971), 299–301.
- [7] K. Kosaki: *On Schmid-Witt's normal form from the Hopf algebra theoretic viewpoint*, Osaka J. Math. **8** (1971), 281–290.
- [8] F.W. Long: *The Brauer group of dimodule algebras*, J. Algebra **31** (1974), 559–601.
- [9] M.E. Sweedler: *Cohomology of algebras over Hopf algebras*, Trans. Amer. Math.

- Soc. **133** (1968), 209–239.
- [10] M.E. Sweedler: *Hopf algebras*, Benjamin, 1969.
- [11] M.E. Sweedler: *Purely inseparable algebras*, *J. Algebra* **35** (1975), 342–355.
- [12] M. Weisfeld: *Purely inseparable extensions and higher derivations*, *Trans. Amer. Math. Soc.* **116** (1965), 435–449.
- [13] E. Witt: *Zyklische Körper und Algebren der Charakteristik p von Grad p^n* , *J. Reine Angew. Math.* **176** (1937), 31–44.
- [14] K. Yokogawa: *On $S \otimes_R S$ -module structure of S/R -Azumaya algebras*, *Osaka J. Math.* **12** (1975), 673–690.
- [15] K. Yokogawa: *Non-commutative Hopf Galois extensions*, *Osaka J. Math.* **18** (1981), 63–73.
- [16] K. Yokogawa: *The cohomological aspect of Hopf Galois extensions over a commutative ring*, *Osaka J. Math.* **18** (1981), 75–93.

Department of Fundamental Natural Science
Okayama University of Science
Ridai-cho, Okayama 700
Japan