Math. J. Okayama Univ. 25 (1984), 91—99

COMMUTATIVITY OF HOPF GALOIS EXTENSIONS WITH HOPF ALGEBRAS OF DERIVATION TYPE

Dedicated to Professor Hirosi Nagao on his 60th birthday

ATSUSHI NAKAJIMA and KENJI YOKOGAWA

Introduction. Let R be a commutative ring with identity of prime characteristic $p \neq 0$. We recall that an R-Hopf algebra $H(p^m)$ called as a *Hopf algebra of derivation type of degree* p^m is defined as follows : $H(p^m)$ is an R-algebra freely generated by d with relation $d^{p^m} = 0$ and its Hopf algebra structure is given by

$$\Delta(d) = d \otimes 1 + 1 \otimes d, \ \varepsilon(d) = 0 \text{ and } \lambda(d) = -d,$$

where Δ, ε and λ are diagonalization, augmentation and antipode respectively. (Hereafter, the letter "d" will always mean the above generator.) Also we denote $H(p) \otimes_R \ldots \otimes_R H(p)$ (m-times) as $H(p)^m$ and its generators $1 \otimes \ldots \otimes 1 \otimes d \otimes 1 \otimes \ldots \otimes 1$ (d in the i-th position) as d_i. In the previous paper [7] Theorem 7, the authors showed that a commutative R-algebra is an $H(p^m)$-Hopf Galois extension of R if and only if it is an $H(p)^m$-Hopf Galois extension. But the concepts of Hopf Galois extensions are extended to the case of non-commutative ring extensions, especially to that of algebras, which is natural from cohomological view-points cf. [3], [11], [12] etc.

In this paper we adopt the concepts of Hopf Galois extensions in the case of algebras, namely an R-algebra A (not necessarily commutative) is called to be an H-Hopf Galois extension of R for a finite R-Hopf algebra H if A is a finitely generated faithful projective R-module and is an H-module algebra and the natural homomorphism from the smash product algebra $A \# H$ to the endomorphism algebra $\mathrm{End}_R(A)$ is an isomorphism. And we shall show that there is a difference between $H(p^m)$-Hopf Galois extensions and $H(p)^m$-Hopf Galois extensions. More precisely, we shall determine the structure of $H(p^2)$-Hopf Galois extensions of R, especially we shall show that if R is a field then $H(p^2)$-Hopf Galois extensions are necessarily commutative—— this is done in § 1. In § 2, we shall show that they are commutative ring extensions of R or R-Azumaya algebras.

Throughout this paper, $R\langle X, Y\rangle$ means a polynomial ring with non-commutative variables X, Y and $R\langle x,y\rangle$ means an algebra (not necessarily commutative) generated by x, y with certain relations. Unadorned $\otimes$ and Hom etc. are taken over R and every map is R-linear. All modules and algebra homomorphisms considered are unitary.

1. $H(p^2)$-Hopf Galois extensions of R. Let A be an R-algebra not necessarily commutative and in this section we always assume that A is an $H(p^2)$-Hopf Galois extension of R unless otherwise stated. By the similar way as [6] Lemma 1.1, there exists $c \in A$ such that $d^{p^2-1}(c) = 1$. Setting $x = d^{p^2-2}(c)$, we get $d(x) = 1$. As to $R[x]$, we have the following.

Proposition 1. *$R[x] = \{a \in A \mid d^p(a) = 0\}$, and A is an $R[d]$-Hopf Galois extension of $R[x]$.*

Proof. Since $d^p(x^i) = 0$, the inclusion $R[x] \subset \{a \in A \mid d^p(a) = 0\}$ is clear. Noting that $R = A^{\{d\}} = \{a \in A \mid d(a) = 0\}$, we get easily that if $d^p(a) = 0$ then $d^{p-1}(a) \in R$. We put $d^{p-1}(a) = r_1$, so we get $d^{p-2}(a) = r_1 x + r_0 = d\left(\frac{r_1 x^2}{2} + r_0 x\right)$ for some $r_0 \in R$. Repeating this processes, we get $a \in R[x]$. Moreover by [11] Proposition 1.6, the latter assertion follows.

Next we shall set $y' = d^{p^2-p-1}(c)$. Then we get $d^{p-1}(y') = x = d\left(\frac{x^2}{2}\right)$. Repeating this processes we get $d(y') = \frac{1}{(p-1)!}x^{p-1} + f(x)$, where $f(x)$ is an element of $R[x]$ with degree less than $p-1$. Since $\deg f(x) < p-1$, there exists $g(x) \in R[x]$ such that $d(g(x)) = f(x)$ (cf. [7] Lemma 8). Setting $y = y' - g(x)$, we get the following.

Lemma 2. *Under the above notations, we have*
$$d(y) = \frac{1}{(p-1)!}x^{p-1} = -x^{p-1},\ d^{p-1}(y) = x,\ yx - xy = r \in R$$
and $R\langle x, y'\rangle = R\langle x, y\rangle$.

Proof. It suffices to prove that $yx - xy \in R$. Since $d(y) \in R[x]$, $d(y)x = xd(y)$. Hence $d(yx - xy) = d(y)x + yd(x) - d(x)y - xd(y) = d(y)x + y - y - xd(y) = 0$. Combining with the fact $R = A^{\{d\}}$, we get $yx - xy \in R$.

With the same notations in Lemma 2, we have the following.

Lemma 3.

$yx^n = x^n y + nrx^{n-1}$ *and*

$$y^n d(y) = \frac{1}{(p-1)!}\left(x^{p-1}y^n + \sum_{i=1}^{n} \binom{n}{i}(p-1)\cdots(p-i)r^i x^{p-i-1}y^{n-i}\right).$$

Proof. Using the relation $yx - xy = r \in R$, the first relation is easily seen by induction. So we shall prove the second relation by induction on n. For $n = 1$, the assertion is clear by the first relation. We assume that the assertion is valid for n. For $n+1$, we have

$$\begin{aligned} y^{n+1}d(y) &= y(y^n d(y)) \\ &= \frac{1}{(p-1)!}\left((yx^{p-1})y^n + \sum_{i=1}^{n} \binom{n}{i}(p-1)\cdots(p-i)r^i yx^{p-i-1}y^{n-i}\right) \\ &= \frac{1}{(p-1)!}\Big((x^{p-1}y + (p-1)rx^{p-2})y^n + \sum_{i=1}^{n} \binom{n}{i}(p-1)\cdots(p-i)\cdot \\ &\quad r^i(x^{p-i-1}y + (p-i-1)rx^{p-i-2})y^{n-i}\Big) \\ &= \frac{1}{(p-1)!}\Big(x^{p-1}y^{n+1} + r(p-1)(1+\tbinom{n}{1})x^{p-2}y^n + \cdots \\ &\quad + r^i(p-1)\cdots(p-i)(\tbinom{n}{i} + \tbinom{n}{i-1})x^{p-i-1}y^{n-i+1} + \cdots \\ &\quad + (p-1)\cdots(p-(n+1))r^{n+1}x^{p-1-(n+1)}\Big) \\ &= \frac{1}{(p-1)!}\left(x^{p-1}y^{n+1} + \sum_{i=1}^{n+1} \binom{n+1}{i}(p-1)\cdots(p-i)r^i x^{p-i-1}y^{n+1-i}\right). \end{aligned}$$

This completes the proof.

The following lemma is well-known.

Lemma 4. $\binom{n}{i} + \binom{n-1}{i} + \cdots + \binom{i}{i} = \binom{n+1}{i+1}$ *for* $1 \leqq i \leqq n$. *Especially* $\binom{p-1}{i} + \binom{p-2}{i} + \cdots + \binom{i}{i} \equiv 0 \pmod{p}$ *for* $1 \leqq i \leqq p-2$.

Lemma 5. *Let y be the element of A defined in* Lemma 2. *Then we have* $d(y^n) = \sum_{k=1}^{n} y^{n-k}d(y)y^{k-1}$ *and* $d(y^p) = r^{p-1}$.

Proof. Since d is a derivation, the first relation is proved by easy induction. We shall prove the second relation. By the first relation we have

$$
\begin{aligned}
d(y^p) &= \textstyle\sum_{i=1}^{p} y^{p-i}d(y)y^{i-1} \\
&= \frac{1}{(p-1)!}((x^{p-1}y^{p-1}+ \textstyle\sum_{i=1}^{p-1} \binom{p-1}{i}(p-1)\cdots(p-i)r^i x^{p-i-1}y^{p-1-i}) \\
&\quad +(x^{p-1}y^{p-2}+ \textstyle\sum_{i=1}^{p-2} \binom{p-2}{i}(p-1)\cdots(p-i)r^i x^{p-i-1}y^{p-2-i})y+\cdots \\
&\quad +(x^{p-1}y^{p-n}+ \textstyle\sum_{i=1}^{p-n} \binom{p-n}{i}(p-1)\cdots(p-i)r^i x^{p-i-1}y^{p-n-i})y^{n-1}+\cdots \\
&\quad +x^{p-1}y^{p-1}) \qquad \text{(by Lemma 3)} \\
&= \frac{1}{(p-1)!}(px^{p-1}y^{p-1}+(\tbinom{p-1}{1}+\tbinom{p-2}{1}+\cdots+\tbinom{1}{1})(p-1)rx^{p-2}y^{p-2} \\
&\quad +(\tbinom{p-1}{2}+\tbinom{p-2}{2}+\cdots+\tbinom{2}{2})(p-1)(p-2)r^2x^{p-3}y^{p-3}+\cdots \\
&\quad +(\tbinom{p-1}{i}+\tbinom{p-2}{i}+\cdots+\tbinom{i}{i})(p-1)\cdots(p-i)r^i x^{p-i-1}y^{p-i-1}+\cdots \\
&\quad +(\tbinom{p-1}{p-2}+\tbinom{p-2}{p-2})(p-1)\cdots 2r^{p-2}xy+(p-1)!r^{p-1}) \\
&= r^{p-1} \qquad \text{(by Lemma 4).}
\end{aligned}
$$

In [5] Proposition 2.12, it is shown that A is freely generated by $\{c, d(c),\ldots,d^{p^2-2}(c) = x, d^{p^2-1}(c) = 1\}$ as R-module. The algebra structure of A is given by the following theorem.

Theorem 6. *An R-algebra A is an $H(p^2)$-Hopf Galois extension of R if and only if $A = R\langle X,Y\rangle/(X^p-r_1,\ Y^p-r^{p-1}X-r_0,\ YX-XY-r)$, ($r_1, r_0, r \in R$) as $H(p^2)$-module algebra, where the $H(p^2)$-module structure of a right hand side algebra is given by $d(x) = 1$, $d(y) = \frac{1}{(p-1)!}x^{p-1} = -x^{p-1}$, x, y residue classes of X, Y respectively.*

Proof. We first prove if part. Let $A' = R\langle X, Y\rangle/(X^p-r_1,\ Y^p-r^{p-1}X-r_0,\ YX-XY-r)$. Then by Lemmas 3 and 5, A' is an $H(p^2)$-module algebra. Now let $\phi : A' \# H(p^2) \longrightarrow \mathrm{End}(A')$ be the natural homomorphism defined by $\phi(\sum_{i=0}^{p^2-1} a_i' \# d^i)(a') = \sum_{i=0}^{p^2-1} a_i' d^i(a')$. Substituting $1,x,\ldots,x^{p-1}$, $y, xy, x^2y,\ldots,x^{p-1}y^{p-1}$ for a' inductively, we get easily that ϕ is a monomorphism. The homomorphism $\bar{\phi}$ induced by passing to residue class fields is also a monomorphism as is easily seen. Counting ranks, we get that $\bar{\phi}$ is an isomorphism. So ϕ is an isomorphism. Thus A' is an $H(p^2)$-Hopf Galois extension of R. Next we shall prove only if part. Let A be an $H(p^2)$-Hopf Galois extension of R, and x, y elements of A chosen as Lemma 2. Then by if part $R\langle x,y\rangle$ is also an $H(p^2)$-Hopf Galois extension of R. So $A = R\langle x,y\rangle$ by the similar manner as if part. This completes the proof.

Corollary 7. *If R is a field then any $H(p^2)$-Hopf Galois extension of R is a commutative algebra.*

Proof. Let $A = R\langle x, y\rangle$ be an $H(p^2)$-Hopf Galois extension of R, where $x^p = r_1$, $y^p - r^{p-1}x = r_0$ and $yx - xy = r$, $r_1, r_0, r \in R$. If $r = 0$ there is nothing to prove. If $r \neq 0$, r is a unit, so $x \in R[y^p]$. Thus $R\langle x, y\rangle = R\langle y, y^p\rangle$. But this is impossible since $R\langle y, y^p\rangle$ is a commutative ring.

The assumption of Corollary 7 would be too strong. The following is due to the referee.

Remark. If R is reduced, then the assertion of Corollary 7 holds. In fact, from the relation $y^p - r^{p-1}x = r_0$, we get $y^{p+1} - r^{p-1}yx = r_0 y = y^{p+1} - r^{p-1}xy$. Hence we have $r^{p-1}(yx - xy) = r^p = 0$, and so $r = 0$.

2. $H(p)^2$-Hopf Galois extensions of R. The structure of a commutative $H(p)^2$-Hopf Galois extension is completely determined in [7] Corollary 4. So in this section we mainly consider a non-commutative Hopf Galois extension (of course if there exists).

Theorem 8. *Let A be an R-algebra. Then A is an $H(p)^2$-Hopf Galois extension of R if and only if $A = R\langle X, Y\rangle/(X^p - r_1, Y^p - r_2, XY - YX - r)$, $r_1, r_2, r \in R$, as $H(p)^2$-module algebra, where the $H(p)^2$-module structure of right hand side algebra is defined by $d_1(x) = 1$, $d_2(x) = 0$, $d_1(y) = 0$ and $d_2(y) = 1$, and x, y are residue classes of X, Y respectively.*

Proof. Only if part. It is easily seen that the integral

$$H(p)^{2^{H(p)^2}} = \{h \in H(p)^2 \mid gh = \varepsilon(g)h \text{ for any } g \in H(p)^2\}$$

is freely generated by $d_1^{p-1}d_2^{p-1}$ over R. Now let A be an $H(p)^2$-Hopf Galois extension of R. Then by similar way as [6] Lemma 1.1, there exists an element $c \in A$ such that $d_1^{p-1}d_2^{p-1}(c) = 1$. We set $x = d_1^{p-2}d_2^{p-1}(c)$ and $y = d_1^{p-1}d_2^{p-2}(c)$. Then $d_1(x) = 1$, $d_2(x) = 0$, $d_1(y) = 0$ and $d_2(y) = 1$. Since $d_1(xy - yx) = d_1(x)y + xd_1(y) - d_1(y)x - yd_1(x) = 0$ and similarly $d_2(xy - yx) = 0$, we get $xy - yx \in A^{H(p)^2} = R$. Next by Lemma 5, $d_1(x^p) = \sum_{k=1}^{p} x^{p-k}d_1(x)x^{k-1} = px^{p-1} = 0$, and $d_2(x^p) = \sum_{k=1}^{p} x^{p-k}d_2(x)x^{k-1} = 0$. Hence $x^p \in R$. Similary $y^p \in R$. Now we shall show that $\{x^i y^j\}_{0 \leq i,j \leq p-1}$ is linearly independent over R. Assume that $\sum_{i,j=0}^{p-1} r_{ij}x^i y^j = 0$. Applying d_1, we get

$$\begin{aligned}&\textstyle\sum_{i,j=0}^{p-1} r_{ij}d_1(x^iy^j)\\ &= \textstyle\sum_{i,j=0}^{p-1} r_{ij}d_1(x^i)y^j + \sum_{i,j=0}^{p-1} r_{ij}x^id_1(y^j)\\ &= \textstyle\sum_{i,j=0}^{p-1}\sum_{k=1}^{i} r_{ij}x^{i-k}d_1(x)x^{k-1}y^j + \sum_{i,j=0}^{p-1}\sum_{k=1}^{i} r_{ij}x^iy^{i-k}d_1(y)y^{k-1}\\ &= \textstyle\sum_{j=0}^{p-1}\sum_{i=1}^{p-1} r'_{ij}x^{i-1}y^j = 0,\end{aligned}$$

where $r'_{ij} = ir_{ij}$. Further applying d_1, we get $\sum_{j=0}^{p-1}\sum_{i=2}^{p-1} r''_{ij}x^{i-2}y^j = 0$, where $r''_{ij} = i(i-1)r_{ij}$. And finally we get $\sum_{j=0}^{p-1}(p-1)!r_{p-1j}y^j = 0$. Next applying d_2, $(p-1)$-times, we get $r_{p-1\,p-1} = 0$. Hence inductively we get $r_{p-1\,j} = 0$ for all j. Again inductively, we get $r_{ij} = 0$ for all i, j. Thus $\{x^iy^j\}_{0\le i,j\le p-1}$ is linearly independent over R. Usual arguments of passing to residue class fields and counting ranks, we get that $A = R\langle x,y\rangle$.

If part. Let A be an R-algebra generated by x and y with the relation $x^p = r_1$, $y^p = r_2$ and $xy-yx = r$, $r_1, r_2, r \in R$. We define the action of d_1 and d_2 as follows ; $d_1(x) = 1$, $d_1(y) = 0$, $d_2(x) = 0$ and $d_2(y) = 1$, and then extend the actions of d_1, d_2 to A as R-derivation. Since $xy-yx \in R$, $d_1d_2(xy) = d_1d_2(yx)$, A is an $H(p)^2$-module algebra as is easily seen. We define an homomorphism $\phi: A \# H(p)^2 \longrightarrow \mathrm{End}(A)$ by $\phi(\sum a_{ij} \# d_1^i \otimes d_2^j)(a) = \sum a_{ij}d_1^id_2^j(a)$. If $\phi(\sum a_{ij} \# d_1^i \otimes d_2^j) = 0$, then substituting $\{x^iy^j\}_{0\le i,j\le p-1}$ for a, we get inductively $a_{ij} = 0$. Thus ϕ is a monomorphism. By the usual way of passing to the residue class fields and counting ranks, we get ϕ is an isomorphism. Thus A is an $H(p)^2$-Hopf Galois extension of R.

In the case of R is a field, we have the following normal form of $H(p)^2$-Hopf Galois extensions.

Theorem 9. *Assume that R is a field and A is an R-algebra which is non-commutative. If A/R is an $H(p)^2$-Hopf Galois extension, then we can define a new $H(p)^2$-action on A (of course if necessary) such that A/R is an $H(p)^2$-Hopf Galois extension and $A = R\langle x,y\rangle$ where x, y satisfies the following relations ; $x^p, y^p \in R$, $xy-yx = 1$, $d_1(x) = 1$, $d_1(y) = 0$, $d_2(x) = 0$ and $d_2(y) = 1$ —— this means that d_1 is an inner derivation afforded by $-y$ and d_2 is an inner derivation afforded by $-x$.*

Proof. Let $x,y \in A$ be an element which satisfies the relations of Theorem 8 (say $xy-yx = r \neq 0$). We set $y' = r^{-1}y$, and define a new $H(p)^2$-action on $A = R\langle x,y\rangle = R\langle x,y'\rangle$ by $d_1(x) = 1$, $d_1(y') = 0$, $d_2(x) = 0$ and $d_2(y') = 1$. By this new $H(p)^2$-module structure, A is an $H(p)^2$-Hopf Galois extension of R. This completes the proof.

Proposition 10. *Let R be a field and $A = R\langle x, y\rangle$ an $H(p)^2$-Hopf Galois extension of R, where x, y is chosen to satisfy $x^p, y^p \in R$, $xy - yx = 1$, $d_1(x) = 1$, $d_2(x) = 0$, $d_1(y) = 0$ and $d_2(y) = 1$ as* Theorem 9. *Then A is a central simple R-algebra.*

Proof. Let H be a Hopf algebra generated by d_1. Then $R[x]/R$ is an H-Hopf Galois extension as is easily seen. We define a homomorphism $f : H \longrightarrow A$ by $f(d_1^j) = (-1)^j y^j$, $0 \leqq j \leqq p-1$. We note that f is an invertible element in the convolution algebra $\mathrm{Hom}(H, A)$ — f^{-1} is given by $f^{-1}(d_1^j) = y^j$. We want to show that f gives an A-inner action of H extending the action on $R[x]$. To this end we must show that $d_1^j(z) = \sum_{(d_1^j)} f(d^j_{1(1)}) z f^{-1}(d^j_{1(2)})$ for $z \in R[x]$. We proceed by induction on j. For $j = 0, 1$ the assertion is valid and we assume that the assertion holds for $j < p-1$. Then

$$\begin{aligned} d_1^{j+1}(z) &= d_1(d_1^j(z)) = d_1\big(\textstyle\sum_{(d_1^j)} f(d^j_{1(1)}) z f^{-1}(d^j_{1(2)})\big) \\ &= -y \textstyle\sum_{(d_1^j)} f(d^j_{1(1)}) z f^{-1}(d^j_{1(2)}) + \sum_{(d_1^j)} f(d^j_{1(1)}) z f^{-1}(d^j_{1(2)}) y \\ &= -y \textstyle\sum_{k=0}^{j} \binom{j}{k}(-y)^k z y^{j-k} + \sum_{k=0}^{j} \binom{j}{k}(-y)^k z y^{j-k+1} \\ &= \textstyle\binom{j}{j}(-y)^{j+1} z + \sum_{k=1}^{j} \big(\binom{j}{k-1} + \binom{j}{k}\big)(-y)^k z y^{j+1-k} + \binom{j}{0} z y^{j+1} \\ &= \textstyle\sum_{k=0}^{j+1} \binom{j+1}{k}(-y)^k z y^{j+1-k} \\ &= \textstyle\sum_{(d_1^{j+1})} f({d_1^{j+1}}_{(1)}) z f^{-1}({d_1^{j+1}}_{(2)}). \end{aligned}$$

Thus f gives a desired A-inner action. Next we shall consider the 2-cocycle σ associated of f. We formulate as the following lemma.

Lemma 11. *Let $0 \leqq i, j \leqq p-1$. Then $\sigma(d_1^i \otimes d_1^j) = 1$ when $i = j = 0$, $\sigma(d_1^i \otimes d_1^j) = -y^p$ when $i+j = p$, and $\sigma(d_1^i \otimes d_1^j) = 0$ otherwise.*

Proof. By definition $\sigma(d_1^i \otimes d_1^j) = \sum_{(d_1^j)} \sum_{(d_1^i)} f(d^i_{1(1)}) f(d^j_{1(1)}) f^{-1}(d^i_{1(2)} d^j_{1(2)})$. So for $0 \leqq i+j < p$,

$$\begin{aligned} \sigma(d_1^i \otimes d_1^j) &= \textstyle\sum_{s=0}^{i} \sum_{t=0}^{j} \binom{i}{s}\binom{j}{t} f(d_1^s) f(d_1^t) f^{-1}(d_1^{i-s} d_1^{j-t}) \\ &= \textstyle\sum_{s=0}^{i} \sum_{t=0}^{j} \binom{i}{s}\binom{j}{t} (-y)^{s+t} y^{i+j-s-t} \\ &= \textstyle\sum_{s=0}^{i} \sum_{t=0}^{j} \binom{i}{s}\binom{j}{t} (-1)^{s+t} y^{i+j} \\ &= (1-1)^i (1-1)^j y^{i+j} = 1 \end{aligned}$$

if $i = j = 0$ or $\sigma(d_1^i \otimes d_1^j) = 0$ if $0 < i+j < p$. Next we consider the case $i+j \geqq p$. Noting that $f^{-1}(d_1^{i+j-s-t}) = 0$ if $s+t \leqq i+j-p$, we get

$$\sigma(d_1^i \otimes d_1^j) = \textstyle\sum_{s=0}^{i} \sum_{t=0}^{j} \binom{i}{s}\binom{j}{t}(-1)^{s+t} y^{i+j} - \sum_{s+t \leqq i+j-p} \binom{i}{s}\binom{j}{t}(-1)^{s+t} y^{i+j}.$$

We know that $\sum_{s=0}^{i} \sum_{t=0}^{j} \binom{i}{s}\binom{j}{t}(-1)^{s+t} y^{i+j} = (1-1)^i (1-1)^j y^{i+j} = 0$ and $\sum_{s+t \leqq i+j-p} \binom{i}{s}\binom{j}{t}(-1)^{s+t} =$ sum of coefficients of the polynomial

$(1-X)^i(1-Y)^j=(1-X^p)(1-X)^{i+j-p}$ degree less than or equal to $i+j-p$, which is equal to $(1-1)^{i+j-p}$. Thus $\sigma(d_1^i \otimes d_1^j) = -y^p$ if $i+j=p$, or $\sigma(d_1^i \otimes d_1^j)=0$ otherwise. Since A is associative, σ is indeed a 2-cocycle. This completes the proof.

Now we return to the proof of Proposition 10. Since the associated 2-cocycle σ is R-valued, the smash product $R[x] \#_\sigma H$ is a simple ring (cf. [8] Proposition 9.1 or [10] Proposition 1.2). We define a homomorphism $\rho: R[x] \#_\sigma H \longrightarrow A$ by $\rho(a \# d^i) = af(d^i)$. ρ is a non-zero algebra homomorphism, hence a monomorphism. $\{\rho(x \# 1) = x, \rho(1 \# (-d_1)) = y\}$ is a generator of A over R, so ρ is an epimorphism. This completes the proof of proposition 10.

Corollary 12. *An $H(p)^2$-Hopf Galois extension A of R is a commutative algebra or an Azumaya algebra.*

Proof. We assume that A is non-commutative. By Theorem 8, A is central as is easily seen. Also by [4] Proposition 1.1, A is a separable R-algebra if and only if A/mA is a separable R/m-algebra for any maximal ideal m of R. So we may assume that R is a field. Since the ring structure is not changed in Theorem 9, we get the assertion by Proposition 10.

REFERENCES

[1] M. AUSLANDER and O. GOLDMAN: The Brauer group of a commutative ring, Trans. Amer. Math. Soc. 97 (1960), 367–409.

[2] S.U. CHASE and M.E. SWEEDLER: Hopf Algebras and Galois Theory, Lecture Notes in Math. 97, Springer-Verlag, Berlin, Berlin, 1969.

[3] T.E. EARLY and H.F. KREIMER: Galois algebras and Harrison cohomology, J. Alg. 58 (1979), 136–147.

[4] S. ENDO and Y. WATANABE: On separable algebras over a commutative ring, Osaka J. Math. 4 (1967), 233–242.

[5] H.F. KREIMER and M. TAKEUCHI: Hopf algebras and Galois extensions of an algebra, Indiana Univ. Math. J. 30 (1981), 675–692.

[6] A. NAKAJIMA: A certain type of commutative Hopf Galois extensions and their groups, Math. J. Okayama Univ. 24 (1982), 137–152.

[7] A. NAKAJIMA and K. YOKOGAWA: Hopf Galois extensions with Hopf algebras of derivation type, Math. J. Okayama Univ. 25 (1983), 49–55.

[8] M.E. SWEEDLER: Cohomology of algebras over Hopf algebras, Trans. Amer. Math. Soc. 133 (1968), 209–239.

[9] M.E. SWEEDLER: Hopf Algebras, Benjamin, New York, 1969.

[10] K. YOKOGAWA: On $S \otimes_R S$-module structure of S/R-Azumaya algebras, Osaka J. Math. 12 (1975), 673–690.

[11] K. YOKOGAWA: Non-commutative Hopf Galois extensions, Osaka J. Math. 18 (1981), 67–73.

[12] K. YOKOGAWA : The cohomological aspect of Hopf Galois extensions over a commutative ring, Osaka J. Math. 18 (1981), 75—93.

OKAYAMA UNIVERSITY
SCIENCE UNIVERSITY OF OKAYAMA

(Received September 22, 1983)