Math. J. Okayama Univ. 24 (1982), 137—152

A CERTAIN TYPE OF COMMUTATIVE HOPF GALOIS EXTENSIONS AND THEIR GROUPS

ATSUSHI NAKAJIMA

Let R be a commutative ring with identity, H a finite Hopf algebra over R, and $H^*=\mathrm{Hom}_R(H, R)$. In [1], Chase and Sweedler introduced the notion of a Galois H-object of R as a generalization of a commutative Galois extension of R. A Galois H-object is nothing but an H^*-Hopf Galois extension of R in the sense of [8]. In this paper we consider a certain type of Hopf algebra H. We shall characterize commutative H-Hopf Galois extensions of R and determine the group of isomorphism classes of such extensions for some special cases.

Now, let R be a commutative algebra over the prime field $GF(p)$ ($p\neq 0$), u an element in R, and m a positive integer. We denote by $H(u,p^m)$, the free Hopf algebra over R with basis $\{1, \delta, \cdots, \delta^{p^m-1}\}$ whose Hopf algebra structure is defined by

$$\delta^{p^m}=0,\quad \Delta(\delta)=\delta\otimes 1+1\otimes\delta+u(\delta\otimes\delta),\quad \varepsilon(\delta)=0 \quad\text{and}$$
$$\lambda(\delta)=\textstyle\sum_{i=1}^{p^m-1}(-1)^i u^{i-1}\delta^i,$$

where Δ, ε and λ are the comultiplication, counit and antipode of $H(u,p^m)$, respectively. In §1, we characterize commutative $H(u,p^m)$-Hopf Galois extensions of R. Using this characterization, we show that a commutative $H(u,p^m)$-Hopf Galois extension is a cyclic p^m-extension [2], a purely inseparable extension [6], or a strongly radicial extension [7] according as u is invertible, or $u=0$, or u is nilpotent. In §2, for $H(u,p^2)$-Hopf Galois extensions A and B of R, we determine $H(u,p^2)$-module algebra isomorphisms from A to B and give a system of generators of the $H(u,p^2)$-Hopf Galois extension $A\cdot B$ of R. In §3, using results in §1 and §2, we determine the group of $H(u,p^m)$-Hopf Galois extensions in the following two cases: (1) p is an arbitrary prime and $m=1$. (2) $p=2$ and $m=2$.

Throughout the following, R is a commutative algebra over $GF(p)$ ($p\neq 0$), each $\otimes$, Hom, etc. is taken over R and each map is R-linear unless otherwise stated. By an R-algebra A we always assume that A is a ring extension of R with the same identity. All R-algebra homomorphisms are unitary. We freely use the notations, terminologies and the results of Hopf algebras and Galois H-objects in Sweedler [5] and Chase-Sweedler [1].

0. Preliminaries. Let H be a finite cocommutative Hopf algebra over R. Let A be an H-module. Then $A\otimes A$ and R are H-modules via, respectively,

$$(0.1)\qquad h(a\otimes b)=\sum_{(h)}h_{(1)}a\otimes h_{(2)}b, \quad \text{where} \quad \Delta(h)=\sum_{(h)}h_{(1)}\otimes h_{(2)}$$

and

$$(0.2)\qquad h(r)=\varepsilon(h)r.$$

An R-algebra A is called an *H-module algebra* if A is an H-module such that the multiplication map and the unit map of A are H-module homomorphisms. These conditions say that

$$(0.3)\qquad h(ab)=\sum_{(h)}(h_{(1)}a)(h_{(2)}b) \quad \text{and} \quad h(1)=\varepsilon(h)1.$$

If A and B are H-module algebras and $f\in \mathrm{Hom}(A, B)$, then f is called an *H-module algebra homomorphism* if it is an H-module homomorphism and an R-algebra homomorphism. For an H-module algebra A, the *smash product* $A\# H$ is equal to $A\otimes H$ as an R-module with multiplication

$$(0.4)\qquad (a\# h)(b\# k)=\sum_{(h)}a(h_{(1)}b)\# h_{(2)}k \quad (a,\ b\in A,\ h,\ k\in H).$$

A commutative H-module algebra A is called an *H-Hopf Galois extension* of R if A is a finitely generated projective R-module and the map ϕ: $A\# H\rightarrow \mathrm{Hom}(A, A)$ defined by $\phi(a\# h)(x)=ah(x)$ is an isomorphism. Then by [1, Th.9.3], A is an H-Hopf Galois extension if and only if A is a Galois H^*-object. When this is the case $A^H=\{a\in A|ha=\varepsilon(h)a$ for all $h\in H\}$ is equal to R. Moreover if H has a constant rank n, then A has the same rank n.

Let A be a commutative $H(u,p^m)$-module algebra. Then by (0.3), we have

$$(0.5)\qquad \delta(ab)=\delta(a)b+a\delta(b)+u\delta(a)\delta(b) \quad \text{and} \quad \delta(1)=0.$$

Note that the formula (0.5) depends only on the coalgebra structure of δ. Moreover by (0.4) and the coalgebra structure of δ, we have

$$(0.6)\qquad (1\#\delta)(a\# 1)=\delta(a)\# 1+a\#\delta+u\delta(a)\#\delta.$$

In the rest of this section, assume that $H=H(u,p^m)$ and A is a commutative H-module algebra. First, we formulate the operation of δ on A. By inductions, the following two lemmas are proved by (0.5).

Lemma 0.1. *For any $a\in A$, we have the following*:
(1) $\delta(a^n)=\sum_{i=1}^{n}\binom{n}{i}u^{i-1}a^{n-i}\delta(a)^i$ $(1\leq n\leq p-1)$.
(2) $\delta(a^p)=u^{p-1}\delta(a)^p$.

(3) *If* $\delta(a)=1$, *then* $\delta^n(a^n)=n!$.

Lemma 0.2. *Suppose that there exist* $\delta_1, \cdots, \delta_s$ *in* H *and* $u_1, \cdots, u_s$ *in* R *such that*

$$(0.7)\qquad \Delta(\delta_i)=\delta_i\otimes 1+1\otimes\delta_i+u_i(\delta_i\otimes\delta_i) \text{ and } \varepsilon(\delta_i)=0 \quad (1\leqq i\leqq s).$$

If there exist $x_1, \cdots, x_s$ *in* A *such that* $\delta_i(x_j)=0$ *and* $\delta_i(x_i)=1$ $(1\leqq j<i\leqq s)$, *then the followings hold for any non-negative integer* $j_1, \cdots, j_k\leqq p-1$:

(1) $\delta_k(x_1^{j_1}\cdots x_n^{j_n})=0$ *for* $1\leqq n<k$.

(2) $\delta_k^l(x_1^{j_1}\cdots x_k^{j_k})=x_1^{j_1}\cdots x_{k-1}^{j_{k-1}}\delta_k^l(x_k^{j_k})$ *for* $1\leqq l<j_k$.

(3) $\delta_k^l(x_1^{j_1}\cdots x_k^{j_k})=0$ *for* $l>j_k$.

Note that if we set $\delta_i=\delta^{p^{i-1}}$ and $u_i=u^{p^{i-1}}$, then $\delta_1, \cdots, \delta_m$ in H and $u_1, \cdots, u_m$ in R satisfies the assumption (0.7).

Lemma 0.3. *Let* $\delta_j\in H$ *and* $u_j\in R$ *be as in Lemma* 0.2, *and* $R_j=\{a\in A\mid \delta_j(a)=0\}$. *If there exists* $a\in A$ *such that* $\delta_j(a)=1$, *then* $1, a, \cdots, a^{p-1}$ *are linearly independent over* R_j, *and* $a^p-u_j^{p-1}a\in R_j$.

Proof. Suppose that $\sum_{i=0}^{p-1}r_ia^i=0$ $(r_i\in R_j)$. By $\delta_j(r_i)=0$ $(0\leqq i\leqq p-1)$ and Lemma 0.1 (3),

$$0=\delta_j^{p-1}(\textstyle\sum_{i=0}^{p-1}r_ia^i)=r_{p-1}\delta_j^{p-1}(a^{p-1})=r_{p-1}(p-1)!.$$

Since $0\neq(p-1)!\in GF(p)$, we have $r_{p-1}=0$, and by induction, $r_{p-2}=\cdots=r_0=0$. Moreover by Lemma 0.1 (2), we have $\delta_j(a^p-u_j^{p-1}a)=0$. This proves the lemma.

Lemma 0.4. *Suppose that there exists* $\delta_1\in H$ *and* $u_1\in R$ *such that*

$$\Delta(\delta_1)=\delta_1\otimes 1+1\otimes\delta_1+u_1(\delta_1\otimes\delta_1) \text{ and } \varepsilon(\delta_1)=0.$$

If there exists $x\in A$ *such that* $\delta_1(x)=1$, *then for any* $n(1\leqq n\leqq p-1)$, *there exist a polynomial* $f_n(X)\in R_1[X]$ *with* deg $f_n(X)=n$ *such that* $\delta_1(f_n(x))=x^{n-1}$, *where* $R_1=\{a\in A|\delta_1(a)=0\}$. *Moreover* $f_n(X)$ *is uniquely determined by* x^{n-1} *except the constant term.*

Proof. For $n=1$, the lemma is clear by $\delta_1(x)=1$. Assume that there holds the assertion for any $k\leqq n-1$. By Lemma 0.1 (1), we have

$$\begin{aligned}x^n&=\{1/(n+1)\}\{\delta_1(x^{n+1})-\textstyle\sum_{i=2}^{n+1}\binom{n+1}{i}u^{i-1}x^{n+1-i}\}\\&=\{1/(n+1)\}\{\delta_1(x^{n+1})-\textstyle\sum_{i=2}^{n+1}\binom{n+1}{i}u^{i-1}\delta_1(f_{n+2-i}(x))\}\\&=\delta_1\{(1/(n+1))(x^{n+1}-\textstyle\sum_{i=2}^{n+1}\binom{n+1}{i}u^{i-1}f_{n+2-i}(x))\}.\end{aligned}$$

If $\delta_1(f_n(x))=\delta_1(g_n(x))=x^{n-1}$, then $\delta_1(f_n(x)-g_n(x))=0$ and so $f_n(x)-g_n(x) \in R_1$. Therefore $f_n(X)$ is uniquely determined by x^{n-1} except the constant term.

By the above lemma, the following is easily seen.

Corollary 0.5. *Under the same assumptions of Lemma* 0.4, *for any* $g(X) \in R_1[X]$ *with* $\deg g(X) \leqq p-2$, *there exists* $h(X) \in R_1[X]$ *such that* $\deg h(X)=\deg g(X)+1$ *and* $\delta_1(h(x))=g(x)$. *Moreover* $h(X)$ *is uniquely determined by* $g(X)$ *except the constant term.*

Note that if $g(X)$ is a monic polynomial, then the highest coefficient of $h(X)$ is invertible in R.

1. $H(u,p^m)$-Hopf Galois extensions. In this section we characterize $H(u,p^m)$-Hopf Galois extensions of R. The following lemma is a special case of [8, Prop.2.1], but it is useful in our studies.

Lemma 1.1. *Let* $H=H(u,p^m)$, *A an H-Hopf Galois extension of R, and* $\phi: A\# H \to \mathrm{Hom}(A, A)$ *an isomorphism defined by* $\phi(a\# h)(x)=ah(x)$. *Then* ϕ *induces an R-module isomorphism* $(1\#\delta^{p^m-1})(A\# R)=A^*=\mathrm{Hom}(A, R)$. *In particular, there exists* $a \in A$ *such that* $\delta^{p^m-1}(a)=1$.

Proof. We set $H^H=\{h \in H | gh=\varepsilon(g)h$ for all $g \in H\}$. Since $A\# H$ is an H-progenerator by [8, Cor.1.4], we can apply [8, Prop.2.1] to our case. By $H^H=R\delta^{p^m-1}$, ϕ induces a requested isomorphism. Moreover by [1, Th.9.3] R is an R-direct summand of A, there exists a projection ρ with $\rho(1)=1$. Thus there exists $a \in A$ such that $\phi\{(1\#\delta^{p^m-1})(a\#1)\}=\rho$, and therefore $1=\rho(1)=\delta^{p^m-1}(a)$.

Now, for an $H(u,p^m)$-Hopf Galois extension A of R, we set

$$\delta_i=\delta^{p^{i-1}} \text{ and } x_i=\delta^{q_i}(a),$$

where $q_i=p^m-p^{i-1}-1$ $(1 \leqq i \leqq m)$ and a is an element in A such that $\delta^{p^m-1}(a)=1$. Then under the above notations, we have the following

Lemma 1.2. *Let A be an* $H(u,p^m)$*-Hopf Galois extension of R and* $R_i=\{a \in A | \delta_i(a)=0\}$. *Then* $R_1=R$, $R_i=R[x_1, \cdots, x_{i-1}]$ *and* $\delta(x_i) \in R[x_1, \cdots, x_{i-1}]$ $(2 \leqq i \leqq m)$.

Proof. By definitions of δ_i and x_i, it suffices to prove that R_i is contained in $R[x_1, \cdots, x_{i-1}]$. We prove this fact by induction on i. Since

A is an $H(u,p^m)$-Hopf Galois extension, $R_1=R$ is clear. Assume that it is true for any $n \leqq i$. If $\delta_{i+1}(a)=0\,(a \in A)$, then $0=\delta_{i+1}(a)=\delta_i^p(a)=\delta_i\delta_i^{p-1}(a)$ and so $\delta_i^{p-1}(a) \in R[x_1, \cdots, x_{i-1}]$ by our induction assumption. Thus we have

$$\delta_i(\delta_i^{p-2}(a)-f_1x_i)=0 \quad \text{for some} \quad f_1 \in R[x_1, \cdots, x_{i-1}],$$

and so

$$\delta_i^{p-2}(a)=f_1x_i+f_0 \text{ for some } f_0 \in R[x_1, \cdots, x_{i-1}].$$

Since $\Delta(\delta_i)=\delta_i \otimes 1+1 \otimes \delta_i+u^{p^{i-1}}\delta_i \otimes \delta_i$, $\varepsilon(\delta_i)=0$ and $\delta_i(x_i)=1$, we can apply Lemma 0.4 to $f_1x_i+f_0$ and thus there exists $g_2(X) \in R[x_1, \cdots, x_{i-1}][X]$ such that deg $g_2(X)=2$ and $\delta_i(g_2(x_i))=f_1x_i+f$. Hence we have $\delta_i(\delta_i^{p-3}(a)-g_2(x_i))=0$. Repeating these processes, we consequently have $a=g_{p-1}(x_i) \in R[x_1, \cdots, x_i]$. This shows that R_{i+1} is contained in $R[x_1, \cdots, x_i]$. Since $\delta_i\delta(x_i)=\delta^{p^m}(a)=0$, $\delta(x_i) \in R[x_1, \cdots, x_{i-1}]$, so that Lemma 1.2 is proved.

Now, we prove the main theorem in this section.

Theorem 1.3. *Let $H=H(u,p^m)$, and A an H-Hopf Galois extension of R. Let $\delta_i=\delta^{p^{i-1}}$, $R_i=\{a \in A \mid \delta_i(a)=0\}$, and H_i an R-Hopf subalgebra generated by δ_i $(1 \leqq i \leqq m)$. Then there exist $x_1, \cdots, x_m$ in A which satisfy the following conditions:*

(1) $\delta_i(x_i)=1$, $\delta_i(x_j)=0$ *and* $(\delta_k)^{p-1}(x_{k+1})=x_k$ $(1 \leqq j < i \leqq m$, $1 \leqq k \leqq m-1)$.

(2) $\{x_1^{j_1} \cdots x_m^{j_m}\}_{0 \leqq j_i \leqq p-1}$ *is a free basis of A.*

(3) *R_i is generated by $x_1, \cdots, x_{i-1}$ as an R-algebra and A is an H_i-Hopf Galois extension of R_i.*

(4) $x_1^p-u^{p-1}x_1 \in R$ *and* $x_i^p=(u^{p^{i-1}})^{p-1}x_i+f_{i-1}(x_{i-1})$ *for some* $f_{i-1}(X) \in R_{i-1}[X]$ *with* deg $f_{i-1}(X) \leqq p-1$ $(2 \leqq i \leqq m)$.

Proof. By Lemma 1.1, there exists $a \in A$ such that $\delta^{p^m-1}(a)=1$. We set $q_i=p^m-p^{i-1}-1$ and $x_i=\delta^{q_i}(a)$ $(1 \leqq i \leqq m)$. Then (1) is trivial, and by Lemma 1.2 and [8, Prop.1.6], (3) is clear. Now we prove (2). By Lemmas 0.3 and 1.2, $1, x_m, \cdots, x_m^{p-1}$ are linearly independent over $R_m=R[x_1, \cdots, x_{m-1}]$ and so $\{x_1^{j_1} \cdots x_m^{j_m}\}$ is linearly independent over R. Thus the R-subalgebra $B=R[x_1, \cdots, x_m]$ of R is a free R-module of rank p^m. We show that the inclusion map $i: B \to A$ is an epimorphism. To this purpose, we may assume that R is a local ring with maximal ideal M. Then we can easily see that $i \otimes 1: B \otimes R/M \to A \otimes R/M$ is an epimorphism. Thus i is an epimorphism, because A is a free R-module of rank p^m. This proves (2). By Lemmas 0.3 and 1.2, (4) is easily seen. This completes the proof.

If $u=0$, then δ is an R-derivation on A and so $\delta(x_i^p)=0$. Hence $x_i^p \in A^H=R$. Thus we have the following

Corollary 1.4. *Let A be an $H(0,p^m)$-Hopf Galois extension of R. Then there exist $x_1, \cdots, x_m$ in A such that $\delta_i(x_i)=1$. Further we have $x_i^p \in R$ and $R[x_1, \cdots, x_m]=A$; and there exists an R-algebra isomorphism*

$$A \cong R[X_1]/(X_1^p - x_1^p) \otimes \cdots \otimes R[X_m]/(X_m^p - x_m^p).$$

Proposition 1.5. *If u is invertible, then an $H(u,p^m)$-Hopf Galois extension A of R is a cyclic p^m-extension in the sense of [2].*

Proof. We set $\sigma=u\delta+1$. Then $\Delta(\sigma)=\sigma\otimes\sigma$, $\varepsilon(\sigma)=1$ and $\delta^{p^m}=1$. Thus σ is an R-algebra automorphism of A of order p^m, because u is invertible. Moreover $H(u,p^m)=R\langle\sigma\rangle$, $\langle\sigma\rangle$ the cyclic group generated by σ.

The following is a generalization of [2, Ths.1.1 and 1.2].

Corollary 1.6. *Let A be an $H(u,p)$-Hopf Galois extension of R. Then there exists $x \in A$ such that $\delta(x)=1$. When this is the case, there holds that $x^p - u^{p-1}x \in R$ and $A=R[x]$; and there exists an isomorphism $A \cong R[X]/(X^p - u^{p-1}X - x^p - u^{p-1}x)$ of $H(u,p)$-Hopf Galois extensions of R. Conversely, let $f(X)=X^p - u^{p-1}X - r \in R[X]$. Then $R[X]/(f(X))$ is an $H(u,p)$-Hopf Galois extension of R with a suitable action of δ.*

Proof. It suffices to prove the converse part. Define $\delta(r)=0$ ($r \in R$), $\delta(x)=1$ and inductively $\delta(x^{i+1})=x^i+\delta(x^i)x+u\delta(x^i)$ ($1 \leqq i \leqq p-1$), where $x=X+(f(X))$. Then it is easy to see that $R[x]$ is an $H(u,p)$-module algebra. We have to show that the map $\phi\colon R[x]\# H(u,p) \to \mathrm{Hom}(R[x], R[x])$ defined by $\phi(a\# h)(b)=ah(b)$ is an isomorphism. Since $R[x]$ and $H(u,p)$ are free R-modules of rank p, it suffices to show that ϕ is an epimorphism. Passing to residue class field, this is proved easily by Cor.1.4 and Prop.1.5. But here we show that ϕ is indeed an epimorphism. Let $\rho_k\colon R[x] \to R[x]$ be the map defined by $\rho_k(x^k)=1$ and $\rho_k(x^j)=0$ ($j \neq k$). We note that $\delta^k(x^l)=0$ ($l < k$), $\delta^k(x^k)=k!$ and $\delta^k(x^l) \in R[x]$ ($l > k$) by Lemma 0.1. We put

$$a_0= \cdots =a_{k-1}=0,\ a_k=1/k!,\ a_{k+1}=-(1/(k+1)!)a_k\delta^k(x^{k+1}),$$
$$\cdots\cdots$$
$$a_{p-1}=-(1/(p-1)!)\{a_{p-2}\delta^{p-2}(x^{p-1})+ \cdots +a_k\delta^k(x^{p-1})\}.$$

Then $a_0, \cdots, a_{p-1}$ are contained in $R[x]$ and $\phi(\sum_{i=0}^{p-1} a_i\# \delta^i)=\rho_k$. Since

$\mathrm{Hom}(R[x], R[x])$ is generated by $\rho_1, \cdots, \rho_{p-1}$ as an $R[x]$-algebra and ϕ is an $R[x]$-algebra homorphism, ϕ is an epimorphism, completing the proof.

Corollary 1.7. *Let $R[X_1, \cdots, X_m]$ be a polynomial ring, and $f_i(X_i) = X_i^p - r_iX_i - s_i \in R[X_i]$. If there exist $v_1, \cdots, v_m$ in R such that $v_i^{p-1} = r_i$, then $B = R[X_1, \cdots, X_m]/(f_1(X_1), \cdots, f_m(X_m))$ is an $H(v_1,p) \otimes \cdots \otimes H(v_m,p)$-Hopf Galois extension of R.*

Proof. Let $x_i = X_i + (f_i(X_i)) \in R[X_i]/(f_i(X_i))$. Then B is isomorphic to $R[X_1]/(f_1(X_1)) \otimes \cdots \otimes R[X_m]/(f_m(X_m))$ as R-algebras. Thus the assertion is clear by Cor.1.6 and [1, Prop.3.2.].

Theorem 1.8. *Let $H = H(u_1,p) \otimes \cdots \otimes H(u_m,p)$, $\{1, \delta_i, \cdots, \delta_i^{p-1}\}$ a free basis of $H(u_i,p)$, and A an H-module algebra. Then A is an H-Hopf Galois extension of R if and only if there exist $x_1, \cdots, x_m$ in A such that $\delta_i(x_i) = 1$, $\delta_i(x_j) = 0$ $(i \neq j)$ and A is generated by $x_1, \cdots, x_m$ as an R-algebra. When this is the case, if we set $f_i(X_i) = X_i^p - u_i^{p-1}X_i - s_i (s_i \in R)$, then $A \cong R[X_1]/(f_1(X_1)) \otimes \cdots \otimes R[X_m]/(f_m(X_m))$ as H-module algebras.*

Proof. Let A be an H-Hopf Galois extension of R. Since $H^H = R(\delta_1^{p-1} \otimes \cdots \otimes \delta_m^{p-1})$, we have by [8, Prop.1.2] and the proof of Lemma 1.1, there exists $a \in A$ such that $(\delta_1^{p-1} \otimes \cdots \otimes \delta_m^{p-1})(a) = 1$. We set $x_i = (\delta_1^{p-1} \otimes \cdots \otimes \delta_{i-1}^{p-1} \otimes \delta_i^{p-2} \otimes \delta_{i+1}^{p-1} \otimes \cdots \otimes \delta_m^{p-1})(a)$. Then $\delta_i(x_i) = 1$, $\delta_j(x_i) = 0$, $\delta_i(x_i^p - u_i^{p-1}x_i) = 0$ and $\delta_j(x_i^p - u_i^{p-1}x^i) = 0$ $(i \neq j)$. Moreover by Cor.1.6, $R[x_i]$ is an $H(u_i,p)$-Hopf Galois extension of R. Since $R[x_1] \otimes \cdots \otimes R[x_m]$ is an H-Hopf Galois extension of R and $R[x_1] \otimes \cdots \otimes R[x_m]$ is contained in A, then by [1, Th.1.12], $A = R[x_1] \otimes \cdots \otimes R[x_m]$. The converse part is clear by Cor.1.7.

Let A be a commutative R-algebra, and $\mu: A \otimes A \to A$ a map defined by $\mu(a \otimes b) = ab$. A is called a *purely inseparable algebra* over R if $\mathrm{Ker}(\mu)$ is contained in the Jacobson radical $J(A \otimes A)$ of $A \otimes A$ (cf. [6, Def.1 and Lemma 1 (a)]). A is called a *strongly radicial* over R if A is a finitely generated projective R-module and $\mathrm{Ker}(\mu)$ is a nil ideal (cf. [7]).

Theorem 1.9. *Let A be an $H(u,p^m)$-Hopf Galois extension of R.*

(1) *If u is contained in the Jacobson radical $J(R)$ of R, then A is a purely inseparable algebra.*

(2) *A is strongly radicial if and only if u is nilpotent.*

Proof. Let $x_1, \cdots, x_m$ be an R-algebra generator which is obtained in

Th.1.3. Note that $\mathrm{Ker}(\mu)$ is generated by

$$x_1^{j_1}\cdots x_m^{j_m}\otimes 1-1\otimes x_1^{j_1}\cdots x_m^{j_m}$$
$$=a_m(x_m\otimes 1-1\otimes x_m)+\cdots+a_1(x_1\otimes 1-1\otimes x_1)\ (a_i\in A\otimes A)$$

$(0\leqq j_1,\cdots,j_m\leqq p-1)$ as an $A\otimes A$-module, and $J(R)\subset J(A\otimes A)$ because $A\otimes A$ is integral over R. First, we prove (1). If $u\in J(R)$, then

$$(*)\qquad (x_1\otimes 1-1\otimes x_1)^p=u^{p-1}(x_1\otimes 1-1\otimes x_1)$$

is contained in $J(A\otimes A)$ and so $x_1\otimes 1-1\otimes x_1\in J(A\otimes A)$. Assume that $x_1^{j_1}\cdots x_{m-1}^{j_{m-1}}\otimes 1-1\otimes x_1^{j_1}\cdots x_{m-1}^{j_{m-1}}\in J(A\otimes A)$ $(0\leqq j_1,\cdots,j_{m-1}\leqq p-1)$. By Th. 1.3 (4),

$$(**)\qquad (x_m\otimes 1-1\otimes x_m)^p=(u^{p^{m-1}})^{p-1}(x_m\otimes 1-1\otimes x_m)$$
$$+\sum r_{i_1\cdots i_{m-1}}(x_1^{i_1}\cdots x_{m-1}^{i_{m-1}}\otimes 1-1\otimes x_1^{i_1}\cdots x_{m-1}^{i_{m-1}})$$

is contained in $J(A\otimes A)$ and so $x_m\otimes 1-1\otimes x_m\in J(A\otimes A)$. This proves (1). Next we prove (2). If A is strongly radicial, then $x_1\otimes 1-1\otimes x_1$ is nilpotent and so u is nilpotent by (*). Conversely if u is nilpotent, then $x_1\otimes 1-1\otimes x_1$ is nilpotent by (*). If $x_1^{i_1}\cdots x_{m-1}^{i_{m-1}}\otimes 1-1\otimes x_1^{i_1}\cdots x_{m-1}^{i_{m-1}}$ are nilpotent, then $x_m\otimes 1-1\otimes x_m$ is nilpotent by (**). This proves (2).

Remark 1.10. Let u be an idempotent, $H=H(u,p^m)$, and A an H-Hopf Galois extension of R. Then it is easy to see that Au is a cyclic p^m-extension of Ru (cf. Prop.1.5). On the other hand $A(1-u)$ is an $H(0,p^m)$-extension of $R(1-u)$ (cf. Cor.1.4).

2. Isomorphisms of $H(u,p^2)$-Hopf Galois extensions. In this section, for $H(u,p^2)$-Hopf Galois extensions A and B, we determine $H(u,p^2)$-module algebra isomorphisms from A to B.

Let A be an $H(u,p^2)$-Hopf Galois extension of R. Then by Th.1.3, there exist $x,y\in A$ such that the following conditions hold:

(2.1) $\delta(x)=1$ and $\delta^{p-1}(y)=x$.

(2.2) $\{x^jy^k\}_{0\leq j,k\leq p-1}$ is a free basis of A.

(2.3) $x^p=u^{p-1}x+r$ and $y^p=(u^p)^{p-1}y+f(x)$, where $f(x)=\sum_{i=0}^{p-1}s_ix^i$ $(r,s_i\in R)$.

Under the above notations, we have the following lemma which is easily obtained by Lemma 0.4.

Lemma 2.1. *For any* $n(1\leqq n\leqq p-1)$, *there exists a polynomial* $f_n(X)\in GF(p)[u][X]$ *with* deg $f_n(X)=n$ *such that*

$$\delta(f_n(x))=x^{n-1} \text{ and } \delta^p(f_n(y))=y^{n-1}.$$

Lemma 2.2. *Under the above notations, for any* n $(0 \leqq n \leqq p-1)$, *there exists a polynomial* $g_n(X) \in R[X]$ *with* deg $g_n(X) = n$ *such that* $\delta^{p-n}(y)=g_n(x)$.

Proof. For $n=0$, the result is clear. Assume that there exists a polynomials $g_k(X) \in R[X]$ with deg $g_k(X)=k$ such that $\delta^{p-k}(y)=g_k(x)$ $(1 \leqq k \leqq n)$. By Cor.0.5, there exists a polynomial $h(X) \in R[X]$ with deg $h(X)=n+1$ such that $\delta(h(x))=g_n(x)=\delta^{p-n}(y)$, and thus $\delta(\delta^{p-(n+1)}(y)-h(x))=0$. Since $R=\{a \in A | \delta(a)=0\}$, $\delta^{p-(n+1)}(y)=h(x)+s$ for some $s \in R$, completing the proof.

Theorem 2.3. *Let* $R[x_i]$ *be* $H(u,p)$*-Hopf Galois extensions of* R, *where* $\delta(x_i)=1$, $\{1, x_i, \cdots, x_i^{p-1}\}$ *is a free basis of* $R[x_i]$, *and* $x_i^p=u^{p-1}x_i+r_i$ $(i=1, 2)$. *Then there exists an* $H(u,p)$*-module algebra homomorphism* $\psi: R[x_1] \to R[x_2]$ (*such map is necessarily an isomorphism by* [1, Th.1.12]) *if and only if there exists* $r \in R$ *such that*

$$r^p=u^{p-1}r+(r_1-r_2).$$

When this is the case, ψ *is given by* $\psi(x_1)=x_2+r$.

Proof. Let $\psi: R[x_1] \to R[x_2]$ be an $H(u,p)$-module algebra homomorphism. We set $\psi(x_1)=\sum_{i=0}^{p-1} t_i x_2^i$ $(t_i \in R)$. Since ψ is an $H(u,p)$-module algebra homomorphism, and by Lemma 0.1,

$$\delta^{p-1}(\psi(x_1))=\delta^{p-1}(\textstyle\sum_{i=0}^{p-1} t_i x_2^i)=t_{p-1}(p-1)!=\psi(\delta^{p-1}(x_1))=0.$$

Thus $t_{p-1}=0$. Repeating the above computations, we have $\psi(x_1)=t_1x_2+t_0$, and $\delta(\psi(x_1))=t_1=\psi(\delta(x_1))=1$. Moreover, by $\psi(x_1)^p=\psi(x_1^p)$, we have $t_0^p=u^{p-1}t_0+r_1-r_2$.

Conversely, assume that there exists $r \in R$ such that $r^p=u^{p-1}r+(r_1-r_2)$. We define an R-linear map $\psi: R[x_1] \to R[x_2]$ by $\psi(x_1^i)=(x_2+r)^i$ $(0 \leqq i \leqq p-1)$. Then it is easy to see that ψ is an $H(u,p)$-module algebra homomorphism. This proves the theorem.

Theorem 2.4. *Let* $A_i=R[x_i, y_i]$ *be* $H(u,p^2)$*-Hopf Galois extensions of* R, *where* $\{x_i, y_i\}$ *satisfies the conditions* (2.1)-(2.3) $(i=1, 2)$. *Then there exisis an* $H(u,p^2)$*-module algebra homomorphism* $\psi: A_1 \to A_2$ *if and only if there exist* $r \in R$ *and* $g(X) \in R[X]$ *with* deg $g(X) \leqq p-1$ *such that the following conditions hold* :

(1) $r^p=u^{p-1}r+(r_1-r_2)$.

(2) $g(x_2)^p=(u^p)^{p-1}g(x_2)+f_1(x_2+r)-f_2(x_2)$, *where* $f_i(x_i)=y_i^p-(u^p)^{p-1}y_i$ (*cf.* (2.3)).

(3) $\delta(g(x_2))=g_{p-1}(x_2+r)-g_{p-1}(x_2)$, *where* $g_{p-1}(x_i)=\delta(y_i)$ (*cf.* Lemma 2.2).

When this is the case, ψ *is given by*

$$\psi(x_1)=x_2+r \text{ and } \psi(y_1)=y_2+g(x_2).$$

Moreover the coefficients of $g(X)$ *is determined by Lemmas* 0.1 *and* 0.2, *explicitly.*

Proof. Assume that there exists an $H(u,p^2)$-module algebra homomorphism $\psi: A_1\rightarrow A_2$.

(1) We set $\psi(x_1)=\sum_{j=0}^{p-1}(\sum_{i=0}^{p-1}r_{ij}x_2^i)y_2^j$. By Lemma 0.1,

$$(\delta^p)^{p-1}(\psi(x_1))=(\sum_{i=0}^{p-1}r_{i,p-1}x_2^i)(p-1)!=\psi((\delta^p)^{p-1}x_1)=0,$$

and so $r_{i,p-1}=0$ for any $0\leqq i\leqq p-1$. Repeating the above computations, we obtain $\psi(x_1)=\sum_{i=0}^{p-1}r_ix_2^i$ and so (1) is easily seen by Th.2.3.

(2) We set $\psi(y_1)=\sum_{j=0}^{p-1}(\sum_{i=0}^{p-1}s_{ij}x_2^i)y_2^j$. Since $\delta^p(y_2)=1$, $(\delta^p)^k(y_2)=0$, and $(\delta^p)^k(\sum_{i=0}^{p-1}s_{ij}x_2^i)=0$ $(2\leqq k\leqq p-1)$, we have $\psi(y_1)=y_2+g(x_2)$, where $g(X)\in R[X]$ with deg $g(X)\leqq p-1$. Moreover by (2.3) and $\psi(x_1)=x_2+r$, we have

$$\psi(y_1^p)=(u^p)^{p-1}(y_2+g(x_2))+f_1(x_2+r)=\psi(y_1)^p=y_2^p+g(x_2)^p.$$

(3) Since ψ is an $H(u,p^2)$-module algebra homomorphism, we have

$$\begin{aligned}\delta(\psi(y_1))&=\delta(y_2+g(x_2))=g_{p-1}(x_2)+\delta(g(x_2))\\&=\psi(\delta(y_1))=\psi(g_{p-1}(x_1))=g_{p-1}(x_2+r).\end{aligned}$$

Conversely we assume that there exist $r\in R$ and $g(X)\in R[X]$ which satisfy the conditions (1)–(3). Define a map $\psi: A_1\rightarrow A_2$ by

$$\psi(\sum_{i=0}^{p-1}\sum_{j=0}^{p-1}r_{ij}x_1^iy_1^j)=\sum_{i=0}^{p-1}\sum_{j=0}^{p-1}r_{ij}(x_2+r)^i(y_2+g(x_2))^j.$$

Then by (1) and (2), ψ is an R-algebra homomorphism. Since $\delta(y_i)=g_{p-1}(x_i)$ and $\delta(x_i)=\delta(x_i+r)=1$ $(i=1, 2)$, we have

$$\begin{aligned}&\psi(\delta(x_1^ly_1^n))\\&=\psi\{\sum_{i=1}^{l}\binom{l}{i}u^{i-1}x_1^{l-i}y_1^n+\sum_{i=1}^{n}\binom{n}{i}u^{i-1}x_1y_1^{n-i}\delta(y_1)^i\\&\quad+\sum_{i=1}^{l}\sum_{j=1}^{n}\binom{l}{i}\binom{n}{j}u^{i+j-2}x_1^{l-i}y_1^{n-j}\delta(y_1)^j\}\\&=\sum_{i=1}^{l}\binom{l}{i}u^{i-1}(x_2+r)^{l-i}(y_2+g(x_2))^n\\&\quad+\sum_{i=1}^{n}\binom{n}{i}u^{i-l}(x_2+r)^l(y_2+g(x_2))^{n-i}g_{p-1}(x_2+r)^i\end{aligned}$$

$$+\sum_{i=1}^{l}\sum_{j=1}^{n}\binom{l}{i}\binom{n}{j}u^{i+j-2}(x_2+r)^{l-i}(y_2+r)^{n-j}g_{p-1}(x_2+r)^j$$
$$=\sum_{i=1}^{l}\binom{l}{i}u^{i-1}(x_2+r)^{l-i}(y_2+g(x_2))^n$$
$$+\sum_{i=1}^{n}\binom{n}{i}u^{i-1}(x_2+r)^l(y_2+g(x_2))^{n-i}\delta(y_2+g(x_2))^i$$
$$+\sum_{i=1}^{l}\sum_{j=1}^{n}\binom{l}{i}\binom{n}{j}u^{i+j-2}(x_2+r)^{l-i}(y_2+g(x_2))^{n-j}\delta(y_2+g(x_2))^j$$
$$=\delta(\psi(x_1^l y_1^n)),$$

because $g_{p-1}(x_2+r)=\delta(g(x_2))+g_{p-1}(x_2)=\delta(y_2+g(x_2))$. Thus ψ is an $H(u,p^2)$-module homomorphism. Finally let $g(X)=\sum_{i=0}^{p-1}t_iX^i \in R[X]$. By Lemmas 0.1 and 0.2,

$$\delta^{p-1}(\psi(y_1))=\delta^{p-1}(\textstyle\sum_{i=0}^{p-1}t_ix_2^i+y_2)=(p-1)!\,t_{p-1}+x_2$$
$$=\psi(\delta^{p-1}(y_1))=x_2+r,$$

and so $t_{p-1}=((p-1)!)^{-1}r$. Moreover by Lemma 2.2, there exists $f_k(X)=\sum_{i=0}^{k}r_{ki}X^i \in R[X]$ such that $\delta^{p-k}(y_j)=f_k(x_j)$ $(j=1, 2)$. Then

$$\delta^{p-k}(\psi(y_1))=\textstyle\sum_{i=0}^{p-1}t_i\delta^{p-k}(x_2^i)+f_k(x_2)=\psi(\delta^{p-k}(y_1))=f_k(x_2+r).$$

Since $\delta^{p-k}(x_2^i)=0$ for $i<p-k$, $\delta^{p-k}(x_2^{p-k})=(p-k)!$ and $\delta^{p-k}(x_2^i)=\sum_{j=0}^{i+k-p}s_jx_2^j \in R[x_2]$ for $p-k<i<p-1$, the constant term of the above equation is

$$(p-k)!\,t_{p-k}+\text{constant term of } \textstyle\sum_{i=p-k+1}^{p-1}t_i\delta^{p-k}(x_2^i)+r_{k0}$$
$$=r_{k0}+r_{k1}r+\cdots+r_{kk}r^k.$$

Therefore by induction, $t_{p-2},\cdots, t_0$ are determined, completing the proof.

Let $A_i=R[x_i, y_i]$ be $H(u,p^2)$-Hopf Galois extensions of R, where $\{x_i, y_i\}$ satisfies the conditions (2.1)—(2.3) $(i=1, 2)$. Then the *product* of $H(u,p^2)$-Hopf Galois extensions of R is defined by

(2.5) $\quad A_1\cdot A_2=\{\sum a_{1i}\otimes a_{2i} \in A_1\otimes A_2 \mid \sum\delta(a_{1i})\otimes a_{2i}=\sum a_{1i}\otimes\delta(a_{2i})\}$,

where δ acts on $A_1\cdot A_2$ by $\delta(a\otimes b)=\delta(a)\otimes b$ $(=a\otimes\delta(b))$. We set

$x=x_1\otimes 1+1\otimes x_2$ and
$y=y_1\otimes\delta^p(y_2)+\delta(y_1)\otimes\delta^{p-1}(y_2)+\cdots+\delta^{p-1}(y_1)\otimes\delta(y_2)+\delta^p(y_1)\otimes y_2.$

Then by the proof of Th.1.3, we have the following

Theorem 2.5. *Under the above notations, we have*

(1) $\delta(x)=1$ *and* $\delta^{p-1}(y)=x$.

(2) $\{x^jy^k\}_{0\le j,k\le p-1}$ *is a free basis of* $A_1\cdot A_2$.

3. The group of $H(u,p^m)$-Hopf Galois extensions. Let Gal($H(u,p^m)$) be the group of $H(u,p^m)$-isomorphism classes of commutative $H(u,p^m)$-Hopf Galois extensions of R with product defined by (2.5). In this section, using results of §2, we compute Gal($H(u,p^m)$) in case of

(1) p is an arbitrary prime and $m=1$,

(2) $p=2$ and $m=2$.

Let H be a finite cocommutative Hopf algebra over R. Then $H^*=\mathrm{Hom}(H, R)$ has an H-module structure defined by

(3.0.1) $\quad h(h^*)=\sum_{(h^*)}\langle h^*_{(1)}, h\rangle h^*_{(2)}$, where $\Delta_{H^*}(h^*)=\sum_{(h^*)}h^*_{(1)}\otimes h^*_{(2)}$

and $\langle,\rangle : H^*\otimes H \to R$ is evaluation.
We say that an H-Hopf Galois extension A of R has a *normal basis*, or a *dual normal basis* according as A is isomorphic to H, or H^* as H-modules. We show that an $H(u,p)$-Hopf Galois extension has a normal basis, or equivalently, a dual normal basis.

Lemma 3.0.1. *$H(u,p^m)^* \cong H(u,p^m)$ as $H(u,p^m)$-modules.*

Proof. Let $\{\delta_0=\varepsilon, \delta, \cdots, \delta_{q-1}\}$ be the dual basis of $\{1, \delta, \cdots, \delta^{q-1}\}$, where $q=p^m$. By (3.0.1),

$$\delta^k(\delta_{q-1})=\sum_{i=0}^{q-1}\langle\delta_i, \delta^k\rangle\delta_{q-1-i}=\delta_{q-k-1},$$

and so $H(u,p^m)^*$ is generated by δ_{q-1} as an $H(u,p^m)$-module, and by $(\sum_{i=0}^{q-1} r_i\delta^i)(\delta_{q-1})=\sum_{i=0}^{q-1} r_i\delta_{q-1-i}$, $\{\delta_{q-1}\}$ is a free basis of $H(u,p^m)^*$ as an $H(u,p^m)$-module, completing the proof.

Theorem 3.0.2. *An $H(u,p)$-Hopf Galois extension A of R has a normal basis, or equivalently, a dual normal basis.*

Proof. By Cor.1.6, there exists $x \in A$ such that $A=R[x]$ and $\delta(x)=1$. Then

$$\delta(x^{p-1})=\binom{p-1}{1}x^{p-2}+rx^{p-3}+\cdots,$$
$$\delta^2(x^{p-1})=\binom{p-1}{1}\binom{p-2}{1}x^{p-3}+sx^{p-4}+\cdots,$$
$$\cdots\cdots$$
$$\delta^{p-2}(x^{p-1})=(p-1)!\,x+t$$
$$\delta^{p-1}(x^{p-1})=(p-1)!.$$

Thus it is easy to see that $\{\delta(x^{p-1}), \cdots, \delta^{p-1}(x^{p-1})\}$ is an R-free basis of A. This proves the theorem.

3.1. Gal($H(u,p)$). Let $H=H(u,p)$, and A an H-Hopf Galois extension of R. By Th.1.3, there exists $x\in A$ such that the following conditions hold:

(3.1.1) $\delta(x)=1$.
(3.1.2) $\{1, x, \cdots, x^{p-1}\}$ is a free basis of A.
(3.1.3) $x^p=u^{p-1}x+r$ for some $r\in R$.

Thus we may write $A=R[x\,;r]$. Let $B=R[y\,;s]$ be another H-Hopf Galois extension of R, and $z=x\otimes 1+1\otimes y$. By Th.2.5, $A\cdot B$ has a free basis $\{1, z, \cdots, z^{p-1}\}$, $\delta(z)=1$ and $z^p=u^{p-1}z+(r+s)$. Therefore $A\cdot B=R[z\,;r+s]$. Let R^+ be the additive group of R. Define a map $\psi: R^+\rightarrow \mathrm{Gal}(H)$ by $\psi(r)=(R[x\,;r])$, where $(R[x\,;r])$ is the isomorphism classes of $R[x\,;r]$. Then by Cor.1.6, ψ is a group epimorphism.

We shall determine the kernel of ψ. To this purpose we have to determine the structure of H^*. Let $\{\delta_0=\varepsilon, \delta_1, \cdots, \delta_{p-1}\}$ be the dual basis of H^*. Then we easily see that $\delta(\delta_1)=1_{H^*}$, and by the proof of Th.1.3, $\{\varepsilon, \delta_1, \cdots, \delta_1^{p-1}\}$ is a free basis of H^* and

$$\delta_1^p=u^{p-1}\delta_1+t \text{ for some } t\in R.$$

But by $\langle\delta_1^p, 1\rangle=\langle u^{p-1}\delta_1+t, 1\rangle=0$, we have $t=0$. Thus we have the following

Theorem 3.1.1. *Under the above notations, H^* has the following structure*:

(1) $\{\varepsilon, \delta_1, \cdots, \delta_1^{p-1}\}$ *is a free basis of* H^*.
(2) $\delta_1^p=u^{p-1}\delta_1$.

Now we have the following theorem which is a generalization of [1, Cor.17.14 or 3, Th. 2.4].

Theorem 3.1.2. *There exists a group isomorphism*

$$\bar{\psi}: R^+/\{t^p-u^{p-1}t\,|\,t\in R\}\longrightarrow \mathrm{Gal}(H(u,p))$$

defined by $\bar{\psi}(\bar{r})=(R[x\,;r])$.

Proof. By Cor.1.6, it suffices to show that $\mathrm{Ker}\,(\bar{\psi})=\{t^p-u^{p-1}t\,|\,r\in R\}$. By Th.3.1.1, the identity element of Gal($H(u,p)$) is $(R[\delta_1\,;0])$. Let r be in R such that $(R[x\,;r])=(R[\delta\,;0])$. Since $R[x\,;0]$ is isomorphic to $R[\delta_1\,;0]$ as $H(u,p)$-module algebras, there exists $t\in T$ such that $t^p=u^{p-1}t+r$ by Th.2.3, completing the proof.

3.2. Gal($H(u,2^2)$). Let $H=H(u,2^2)$), and A an H-Hopf Galois extension of R. By Th.1.3, there exist x, $y\in A$ and $f(X)\in R[X]$ with deg $f(X)=1$ such that the following conditions hold:

(3.2.1) $\delta(x)=1$ and $\delta(y)=x$.
(3.2.2) $\{1, x, y, xy\}$ is a free basis of A.
(3.2.3) $x^2=ux+r$ for some $r\in R$ some $r\in R$ and $y^2=u^2y+f(x)$.

Under the above notations, the following lemma is easily seen.

Lemma 3.2.1. *$f(X)=urX+s$ for some $s\in R$.*

By Lemma 3.2.1, we may write $A=R[x, y; r, s]$. Then by (3.2.1)-(3.2.3), we have the following

Theorem 3.2.2. *Let $A_i=R[x_i, y_i; r_i, s_i]$ be H-Hopf Galois extensions of R ($i=1, 2$). If we set*

$$x=x_1\otimes 1+1\otimes x_2 \quad and \quad y=y_1\otimes 1+x_1\otimes x_2+1\otimes y_2,$$

then the product $A_1\cdot A_2$ has the following structure:
(1) $\delta(x)=1$ *and* $\delta(y)=x$.
(2) $\{1, x, y, xy\}$ *is a free basis of* $A_1\cdot A_2$.
(3) $x^2=ux+r_1+r_2$ *and* $y^2=u^2y+u(r_1+r_2)x+r_1r_2+s_1+s_2$.

Thus by Th.3.2.2, we have $A_1\cdot A_2=R[x, y; r_1+r_2, r_1r_2+s_1+s_2]$.

Let $\{\delta_0=\varepsilon, \delta_1, \delta_2, \delta_3\}$ be the dual basis of H^* with respect to $\{1, \delta, \delta^2, \delta^3\}$. By (3.0.1) we have

$$H^*=R[\delta_1, \delta_2; 0, 0].$$

Proposition 3.2.3. *Let r, s be elements in R. Then*

$$R[X, Y]/(X^2+uX+r, Y^2+u^2Y+urX+s)$$

is an H-Hopf Galois extension of R with a suitable action of δ.

Proof. We define an H-action on $R[X, Y]$ by $\delta(r)=0$ ($r\in R$), $\delta(X)=1$, $\delta(Y)=X$ and $\delta(fg)=f\delta(g)+\delta(f)g+u\delta(f)\delta(g)$ ($f, g\in R[X, Y]$). Let I be the ideal generated by X^2+uX+r and $Y^2+u^2Y+urX+s$. Then one can easily check that $R[X, Y]/I$ is an H-module algebra with $\delta(x)=1$ and $\delta(y)=x$, where $x=X+I$ and $y=Y+I$. Moreover $R[X, Y]/I=R[x, y]$ is a free R-module with basis $\{1, x, y, xy\}$ and $\{x, y\}$ satisfies the condition (3.2.3). Since $\delta^3(xy)=1$, $R[x, y]$ is an H-Hopf Galois extension of R.

Now we set $R_2^+ = R \times R$. Define an addition on R_2^+ by

$$(r_1, s_1)+(r_2, s_2)=(r_1+r_2, r_1r_2+s_1+s_2).$$

Then R_2^+ is an abelian group with zero element (0, 0). Under the above notations, we have the following

Theorem 3.2.4. *There exists a group isomorphism*

$$\bar{\psi}: R_2^+/M \longrightarrow \mathrm{Gal}(H(u,2^2))$$

defined by $\bar{\psi}(\overline{(r, s)})=(R[x, y; r, s])$, *where* $\psi: R_2^+ \longrightarrow \mathrm{Gal}(H(u,2^2))$ *is defined by* $\psi((r, s))=(R[x, y; r, s])$, $M=\{(r_0^2+ur_0, ur_0(r_0^2+ur_0)+s_0(u^2+s_0))|r_0, s_0 \in R\}$ *and* $\overline{(r, s)}=(r, s)+M$.

Proof. By Prop.3.2.3, it is easy to see that ψ is a group epimorphism. Let $A=R[x, y; r, s]$ be an $H(u,2^2)$-Hopf Galois extension of R, and let $\alpha: A \rightarrow H(u,2^2)^*$ be an isomorphism of $H(u,2^2)$-Hopf Galois extensions of R. By Th.2.4, we may set

$$\alpha(x)=\delta_1+r_0 \text{ and } \alpha(y)=\delta_2+s_1\delta_1+s_0 \ (r_0, s_i \in R),$$

where $r_0^2=ur_0+r$. Since α is an $H(u,2^2)$-module algebra homomorphism, we have $s_1=r_0$ and $s=ur_0^3+u^2r_0^2+s_0^2+u^2s$. Thus $(r, s)\in M$. Conversely, let $(r_1, s_1)=(r_0^2+ur_0, ur_0^3+u^2r_0^2+s_0^2+u^2s_0)\in M$, and $\bar{\psi}(\overline{(r, s_1)})=(R[x_1, y_1; r_1, s_1])$. Define a map $\alpha_1: R[x_1, y_1; r_1, s_1] \rightarrow R[\delta_1, \delta_2; 0, 0]$ by

$$\alpha_1(1)=\varepsilon, \quad \alpha_1(x_1)=\delta_1+r_0 \text{ and } \alpha_1(y_1)=\delta_2+r_0\delta_1+s_0.$$

Then it is easy to see that α_1 is an $H(u,2^2)$-module algebra isomorphism. Therefore $\mathrm{Ker}(\psi)=M$, completing the proof.

In general, to calculate the group $\mathrm{Gal}(H(u,p^m))$ is a complicated work. For example, $\mathrm{Gal}(H(u,3^2))$ has a following isomorphism.

Theorem 3.2.5. *Let* $R_2^+=R\times R$ *be an abelian gronp with addition*

$$(r_1, s_1)+(r_2, s_2)=(r_1+r_2, s_1+s_2+2r_1r_2(r_1+r_2+u^3)).$$

Then there exists a group isomorphism

$$\psi: R_2^+/N \longrightarrow \mathrm{Gal}(H(u,3^2))$$

defined by $\psi(\overline{(r, s)})=(R[x, y; r, s])$, *where* $N=\{(r_0^3-u^2r_0, s_0^3-u^6s_0-2u^4(r_0^3-u^2r_0)r_0^2-2u^2(r_0^3-u^2r_0)((r_0^3-u^2r_0)+u^3)r_0|r_0, s_0\in R\}$ *and* $\overline{(r, s)}=(r, s)+N$.

REFERENCES

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

[2] T. NAGAHARA and A. NAKAJIMA: On cyclic extensions of commutative rings, Math. J. Okayama Univ. **15** (1971), 81—90.

[3] A. NAKAJIMA: On a group of cyclic extensions over commutative rings, Math. J. Okayama Univ. **15** (1972), 163—172.

[4] A. NAKAJIMA: Free algebras and Galois objects of rank 2, Math. J. Okayama Univ. **23** (1981), 181—187.

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

[6] M.E. SWEEDLER: Purely inseparable algebras, J. Alg. **35** (1975), 342—355.

[7] Y. TAKEUCHI: On strongly radicial extensions, Pacific J. Math. **55** (1974), 619—627.

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

[9] K. YOKOGAWA: The cohomological aspects of Hopf Galois extensions over commutative rings, Osaka J. Math. **18** (1981), 75—93.

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY

(Received May 8, 1982)