Math. J. Okayama Univ. 25 (1983), 49—55

HOPF GALOIS EXTENSIONS WITH HOPF ALGEBRAS OF DERIVATION TYPE

ATSUSHI NAKAJIMA and KENJI YOKOGAWA

Throughout the present paper, R will denote a commutative ring with identity of prime characteristic p. Let H be a Hopf algebra over R. A commutative ring extension A of R is called an *H-Hopf Galois extension* of R (or A/R is an *H-Hopf Galois extension*) if A is a finitely generated faithful projective R-module and an H-module algebra and the natural homomorphism (arising from the H-module structure of A) from the smash product algebra $A \# H$ to the endomorphism algebra $\mathrm{End}_R(A)$ is an isomorphism. For details, we refer to [2], [6], [7] and [8]. Unadorned $\otimes$ and Hom etc. are taken over R and every map is R-linear. All the modules and R-algebra homomorphisms considered are unitary.

By the *Hopf algebra of derivation type of degree* p^m (cited below as $H(p^m)$) we mean a Hopf algebra over R 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

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

where Δ, ε and λ are the diagonalization, augmentation and antipode, respectively. (Hereafter, the letter "d" will always mean the above generator.) In [4, Corollary 1.4], the first named author shows that any $H(p^m)$-Hopf Galois extension of R is of the form

$$R[X_1]/(X_1^p - \alpha_1) \otimes \cdots \otimes R[X_m]/(X_m^p - \alpha_m) \quad (\alpha_i \in R).$$

As is easily checked, such an extension is an $H(p)^m$-Hopf Galois extension of R, where $H(p)^m = H(p) \otimes \cdots \otimes H(p)$. Conversely, in case $A_m = R[X_1]/(X_1^p - \alpha_1) \otimes \cdots \otimes R[X_m]/(X_m^p - \alpha_m)$ is a field, the existence of a non-integrable element in A_{m-1} enabled R.Baer [1] to show inductively that any derivation of A_{m-1} over R can be extended to that of A_m satisfying the same conditions as for d (especially its p^m-th power equals zero and the invariant subfield is R). This fact may be interpreted as A_m to be an $H(p^m)$-Hopf Galois extension of R. But unfortunately the explicit form of the non-integrable element was not given.

In this paper we shall consider a typical non-integrable element and construct a derivation (compatible with the above characterization) on an $H(p)^m$-Hopf Galois extension of R. Furthermore, we shall show that a commutative R-algebra A is an $H(p^m)$-Hopf Galois extension of R if and only if it is an $H(p)^m$-Hopf Galois extension.

Now, we begin our study with stating two propositions quoted from [4].

Proposition 1 ([4, Corollary 1.6]). *Let A be a commutative R-algebra. Then A is an $H(p)$-Hopf Galois extension of R if and only if A is isomorphic to $R[X]/(X^p-\alpha)$ $(\alpha\in R)$ as H-module algebra, where the action of $d\in H(p)$ on $R[X]/(X^p-\alpha)$ is defined by $d(x)=1$, x the residue class of X.*

Proposition 2 ([4, Lemma 1.2 and Corollary 1.4]). *Let A/R be an $H(p^m)$-Hopf Galois extension. Then A is isomorphic to $R[X_1]/(X_1^p-\alpha_1)\otimes\cdots\otimes R[X_m]/(X_m^p-\alpha_m)$ $(\alpha_i\in R)$. When this is the case, $d(x_1)=1$, $x_i=d^{p^{m-1}-p^{i-1}}(x_m)$ and $d(x_i)\in R[x_1,\cdots,x_{i-1}]$ $(2\leqq i)$, where x_i is the residue class of X_i.*

Proposition 3. *Let H_1, H_2 be finite cocommutative Hopf algebras over R. If A/R is an $H_1\otimes H_2$-Hopf Galois extension, then there exist subalgebras A_1, A_2 of A such that A_i/R is an H_i-Hopf Galois extension $(i=1, 2)$ and $A=A_1\otimes A_2$ as $H_1\otimes H_2$-module algebra. Conversely, if A_i/R is an H_i-Hopf Galois extension, then $A_1\otimes A_2$ is an $H_1\otimes H_2$-Hopf Galois extension of R.*

Proof. The converse part has been proved in [2, Proposition 3.2] and [8, Lemma 4.2]. Let $\varepsilon_i: H_i\rightarrow R$ be an augmentation, $p_1=1\otimes\varepsilon_2: H_1\otimes H_2\rightarrow H_1$ and $p_2=\varepsilon_1\otimes 1: H_1\otimes H_2\rightarrow H_2$. Then, by [8, Lemma 4.1], $A_i=\mathrm{Hom}_{H_1\otimes H_2}(H_i, A)$ is an H_i-Hopf Galois extension of R, where H_i is regarded as an $H_1\otimes H_2$-module via p_i. Thus $A_1\otimes A_2$ is an $H_1\otimes H_2$-Hopf Galois extension of R. By taking the image of $1\in H_i$, we may identify A_1 with $A^{H_2}=\{a\in A\mid h\cdot a=\varepsilon(h)a \text{ for all } h\in H_2\}$; and A_2 with A^{H_1}. Under these identifications we can define the homomorphism $\phi: A_1\otimes A_2\rightarrow A$ by the product in A. Since A is commutative, ϕ is a well-defined $H_1\otimes H_2$-module algebra homomorphism. Thus ϕ is an isomorphism by [2, Theorem 1.1.12].

By Propositions 1, 2 and 3 we get the following:

Corollary 4. *Let $A=R[X_1]/(X_1^p-\alpha_1)\otimes\cdots\otimes R[X_m]/(X_m^p-\alpha_m)$ be an $H(p^m)$-Hopf Galois extension of R. Then A is an $H(p)^m$-Hopf Galois extension of R, where $\partial_i=\partial/\partial x_i=1\otimes\cdots\otimes 1\otimes d\otimes 1\otimes\cdots\otimes 1\in 1\otimes\cdots\otimes 1\otimes H(p)\otimes 1\otimes\cdots\otimes 1$ (i-th position) acts on A as $\partial_i(x_j)=\delta_{ij}$ (Kronecker's delta).*

Conversely, if A is an $H(p)^m$-Hopf Galois extension of R, then A is isomorphic to $R[X_1]/(X_1^p-a_1')\otimes\cdots\otimes R[X_m]/(X_m^p-a_m')$ as $H(p)^m$-module algebra, ∂_i acts as $\partial_i(x_j)=\delta_{ij}$.

For further investigation, we need the following lemmas.

Lemma 5. $\binom{p^{n-1}-1}{k}\equiv(-1)^k \pmod p$, $n\geqq 2$, $0\leqq k\leqq p^{n-1}-1$.

Proof. Since $(1+X)^{p^{n-1}}\equiv 1+X^{p^{n-1}} \pmod p$, we have

$$\binom{p^{n-1}}{k}\equiv\begin{cases}1 \pmod p & \text{for } k=0,\ p^{n-1}\\ 0 \pmod p & \text{otherwise.}\end{cases}$$

Combining this with $\binom{p^{n-1}-1}{k}+\binom{p^{n-1}-1}{k+1}=\binom{p^{n-1}}{k+1}$, we can easily get the assertion by induction.

Lemma 6. *Let $A=R[X_1]/(X_1^p-a_1)\otimes\cdots\otimes R[X_m]/(X_m^p-a_m)$ be an $H(p)^m$-Hopf Galois extension of R. Then there exists a nilpotent R-derivation $\delta: A\to A$ of index p^m such that $\delta(x_1)=1$ and $\delta^{p^{k-1}-p^{k-2}}(x_k)=x_{k-1}$ $(2\leqq k\leqq m)$.*

Proof. Let $\partial_i: A\to A$ be a derivation defined by $\partial_i(x_j)=\delta_{ij}$. We put $\delta=P_0\partial_1+P_1\partial_2+\cdots+P_{m-1}\partial_m$, where for $p\neq 2$, $P_0=1$, $P_i=(-1)^i x_1^{p-1}\cdots x_i^{p-1}$ $(1\leqq i\leqq m-1)$ and for $p=2$, $P_0=1$, $P_1=x_1$, $P_i=P_{i-1}x_i+\cdots+x_1\cdots x_{i-1}a_{i-1}$ $(2\leqq i\leqq m-1)$. Since the assertion is valid for $m=1, 2$, we proceed by induction on m. Assume that $\delta(x_1)=1$ and $\delta^{p^{k-1}-p^{k-2}}(x_k)=x_{k-1}$ $(2\leqq k\leqq m-1)$. Then, it is easy to see that $\delta^{p^{k-1}}(x_k)=1$ $(1\leqq k\leqq m-1)$, and hence $\delta^{p^{k-1}}(P_{k-1})=0$. First, we consider the case $p\neq 2$. Noting that $\delta^{p^{m-2}}$ is a derivation with $\delta^{p^{m-2}}(P_{m-2})=0$, we have

$$\begin{aligned}\delta^{p^{m-1}-p^{m-2}}(x_m) &= \delta^{p^{m-1}-p^{m-2}-1}((-1)^{m-1}x_1^{p-1}\cdots x_{m-1}^{p-1})\\ &= \delta^{p^{m-2}-1}\delta^{p^{m-2}(p-2)}((-1)^{m-1}x_1^{p-1}\cdots x_{m-1}^{p-1})\\ &= \delta^{p^{m-2}-1}((-1)^{m-1}x_1^{p-1}\cdots x_{m-2}^{p-1}(\delta^{p^{m-2}})^{p-2}(x_{m-1}^{p-1}))\\ &= \delta^{p^{m-2}-1}((-1)^{m-1}x_1^{p-1}\cdots x_{m-2}^{p-1}(p-1)x_{m-1})\\ &= \delta^{p^{m-2}-1}(\delta(x_{m-1})x_{m-1})\\ &= \textstyle\sum_{k=0}^{p^{m-2}-1}\binom{p^{m-2}-1}{k}\delta^{k+1}(x_{m-1})\delta^{p^{m-2}-1-k}(x_{m-1})\\ &= \delta(x_{m-1})\delta^{p^{m-2}-1}(x_{m-1})-\delta^2(x_{m-1})\delta^{p^{m-2}-2}(x_{m-1})+\cdots\\ &\quad+\delta^{p^{m-2}-2}(x_{m-1})\delta^2(x_{m-1})-\delta^{p^{m-2}-1}(x_{m-1})\delta(x_{m-1})\\ &\quad+\delta^{p^{m-2}}(x_{m-1})x_{m-1} \quad \text{(by Lemma 5)}\\ &= x_{m-1}.\end{aligned}$$

Next, we consider the case $p=2$. Noting that $\delta^{2^{k-2}}(x_{k-1})=1$, we have

$$\begin{aligned}\delta^{2^{k-1}-1}(x_1\cdots x_{k-1}) &= \textstyle\sum_{i=0}^{2^{k-1}-1}\binom{2^{k-1}-1}{i}\delta^i(x_1\cdots x_{k-2})\delta^{2^{k-1}-1-i}(x_{k-1})\\ &= \textstyle\sum_{i=0}^{2^{k-1}-1}\delta^i(x_1\cdots x_{k-2})\delta^{2^{k-1}-1-i}(x_{k-1})\\ &= (x_1\cdots x_{k-2})\delta^{2^{k-2}-1}(\delta^{2^{k-2}}(x_{k-1}))\\ &\quad+\delta(x_1\cdots x_{k-2})\delta^{2^{k-2}-2}(\delta^{2^{k-2}}(x_{k-1}))+\cdots\\ &\quad+\delta^{2^{k-2}-1}(x_1\cdots x_{k-2})\delta^{2^{k-2}}(x_{k-1})\\ &\quad+\delta(\delta^{2^{k-2}-1}(x_1\cdots x_{k-2}))\delta^{2^{k-2}-1}(x_{k-1})+\cdots\\ &\quad+\delta^{2^{k-2}}(\delta^{2^{k-2}-1}(x_1\cdots x_{k-2}))x_{k-1}\quad\text{(by Lemma 5)}\\ &= \delta^{2^{k-2}-1}(x_1\cdots x_{k-2})\delta^{2^{k-2}}(x_{k-1})\\ &\quad+\delta(\delta^{2^{k-2}-1}(x_1\cdots x_{k-2}))\delta^{2^{k-2}-1}(x_{k-1})+\cdots\\ &\quad+\delta^{2^{k-2}}(\delta^{2^{k-2}-1}(x_1\cdots x_{k-2}))x_{k-1}.\end{aligned}$$

Hence, by induction method we get $\delta^{2^{k-1}-1}(x_1\cdots x_{k-1})=1$ $(2\leqq k\leqq m-1)$. Now, we see that

$$\begin{aligned}\delta^{2^{m-1}-2^{m-2}}(x_m) &= \delta^{2^{m-2}}(x_m)=\delta^{2^{m-2}-1}(P_{m-1})\\ &= \delta^{m-2-1}(P_{m-2}x_{m-1}+x_1\cdots x_{m-2}a_{m-2})\\ &= \delta^{2^{m-2}-1}(\delta(x_{m-1})x_{m-1}+a_{m-2}\delta^{2^{m-2}-1}(x_1\cdots x_{m-2})\\ &= \textstyle\sum_{i=0}^{2^{m-2}-1}\delta^{1+i}(x_{m-1})\delta^{2^{m-2}-1-i}(x_{m-1})+a_{m-2}\\ &= \delta(x_{m-1})\delta^{2^{m-2}-1}(x_{m-1})+\delta^2(x_{m-1})\delta^{2^{m-2}-2}(x_{m-1})+\cdots\\ &\quad+\delta^{2^{m-3}}(x_{m-1})\delta^{2^{m-3}}(x_{m-1})+\cdots\\ &\quad+\delta^{2^{m-2}-2}(x_{m-1})\delta^2(x_{m-1})+\delta^{2^{m-2}-1}(x_{m-1})\delta(x_{m-1})\\ &\quad+\delta^{2^{m-2}}(x_{m-1})x_{m-1}+a_{m-2}\\ &= (\delta^{2^{m-3}}(x_{m-1}))^2+x_{m-1}+(x_{m-2})^2=x_{m-1}.\end{aligned}$$

It is easy to see that $\delta^{p^m-1}\neq 0$ and $\delta^{p^m}=0$.

We now return back to the investigation of an $H(p)^m$-Hopf Galois extension A/R. Let δ be such a derivation as in Lemma 6. Then δ acts naturally on A and makes A an $H(p^m)$-module algebra. Since $\delta^0=1$, δ^1, $\delta^2,\cdots,\delta^{p^m-1}$ are left A-linearly independent, the usual argument of passing to the residue class fields and counting the ranks shows that A/R is an $H(p^m)$-Hopf Galois extension; especially $A^{\{\delta\}}=\{a\in A\mid\delta(a)=0\}=R$ by [7, Proposition 1.2]. Conversely, by Corollary 4, every $H(p^m)$-Hopf Galois extension is an $H(p)^m$-Hopf Galois extension. Summarizing the above, we get

Theorem 7. *Let A be a commutative R-algebra. Then A is an $H(p^m)$-Hopf Galois extension of R if and only if it is an $H(p)^m$-Hopf Galois extension.*

Remark. It should be noted that if $j < i$ then $H(p^i) \otimes H(p)^{m-i}$ is not isomorphic to $H(p^j) \otimes H(p)^{m-j}$. In fact, $H(p^i) \otimes H(p)^{m-i}$ contains the element $d \otimes (1 \otimes \cdots \otimes 1)$ $(d \in H(p^i))$ with the property $(d \otimes 1 \otimes \cdots \otimes 1)^{p^{i-1}} \notin R$ but $c^{p^{j-1}} \in R$ for any $c \in H(p^j) \otimes H(p)^{m-j}$. It should also be noted that if A/R is an $H(p^m)$-Hopf Galois extension, then it is an $H(p^i) \otimes H(p)^{m-i}$-Hopf Galois extension $(m \neq 1)$, so there exist many non-isomorphic Hopf algebras which make A/R an Hopf Galois extension. Furthermore, A. Hattori [3] has pointed out that $R[X]/(X^p - a)$ $(a \in R)$ is a Hom(RG, R) Hopf Galois extension of R, where G is a cyclic group of order p (cf. also [9]). Therefore there exist much more non-isomorphic Hopf algebras which make A/R an Hopf Galois extension.

Finally, we are going to make a precision of Proposition 2. To this end, we define the (*weighted*) *degree* of a monomial in an $H(p^m)$-Hopf (or $H(p)^m$-Hopf) Galois extension $R[X_1]/(X_1^p - a_1) \otimes \cdots \otimes R[X_m]/(X_m^p - a_m) = R[x_1, \cdots, x_m]$ as follows:

$$\text{degree } (rx_1^{e_1} \cdots x_m^{e_m}) = \begin{cases} \sum_{i=1}^{m} e_i p^{i-1} & \text{if } r \neq 0 \ (\in R),\ 0 \leqq e_i \leqq p-1 \\ -1 & \text{if } r = 0. \end{cases}$$

Since $\{x_1^{e_1} \cdots x_m^{e_m}\}_{0 \leq e_i \leq p-1}$ is an R-free basis of A [4, Theorem 1.3], the above definition is well-defined. Further, considering the p-adic expansion, we see that a monic monomial of given degree is uniquely determined.

Lemma 8. *Let* $A = R[X_1]/(X_1^p - a_1) \otimes \cdots \otimes R[X_m]/(X_m^p - a_m) = R[x_1, \cdots, x_m]$ *be an* $H(p^m)$*-Hopf Galois extension of* R, *and*

$$d(x_1) = 1 \text{ and } d(x_i) = P_{i-1} \quad (i \geqq 2),$$

where P_{i-1} *is given in the proof of* Lemma 6.

(1) *For a monic monomial* f *of degree* ℓ, $d(f)$ *is the sum of a monomial of degree* $\ell - 1$ *with unit coefficient and a sum of monomials of degree less than* $\ell - 1$.

(2) *Every monomial* g *of degree less than* $p^m - 1$ *is integrable, that is there exists an element* G *in* A *such that* $d(G) = g$; *every sum of monomials of degree less than* $p^m - 1$ *is integrable.*

Proof. (1) This can be shown by direct computation.

(2) We shall proceed by induction on degree ℓ. For $\ell = -1$, 0, the assertion is valid. We assume that there holds the assertion for all $k \leqq \ell - 1$ $(< p^m - 2)$. Let G_1 be the monic monomial of degree $\ell + 1$ $(< p^m)$, and $g = rx_1^{e_1} \cdots x_m^{e_m}$ $(0 \leqq e_i \leqq p-1,\ r \in R)$ an arbitrary monomial of degree ℓ. Then by (1), we have

$$d(G_1) = ux_1^{e_1} \cdots x_m^{e_m} + h,$$

where u is a unit of R and h is a sum of monomials of degree less than $\ell-1$. We set $G_2 = ru^{-1}G_1$. Then $d(G_2) = g + ru^{-1}h$, and by induction hypothesis, $ru^{-1}h$ is integrable, say $d(G_3) = ru^{-1}h$. Thus, we get $d(G_2 - G_3) = g$.

Theorem 9. *Let A be a commutative R-algebra. Then A is an $H(p^m)$-Hopf Galois extension of R if and only if A is isomorphic to $R[X_1]/(X_1^p - \alpha_1) \otimes \cdots \otimes R[X_m]/(X_m^p - \alpha_m) = R[x_1, \cdots, x_m]$, $x_i^p \in R$, as H-module algebra, where x_i is the residue class of X_i and the action of $d \in H(p^m)$ on $R[x_1, \cdots, x_m]$ is defined by $d(x_i) = P_{i-1}$* (see the proof of Lemma 6).

Proof. "If" part is already proved in the paragraph preceding Theorem 7. "Only if" part will be proved by induction on m. By Prpoosition 2, we can choose $y_1, \cdots, y_m \in A$ as follows: $A = R[y_1, \cdots, y_m] \cong R[Y_1]/(Y_1^p - \beta_1) \otimes \cdots \otimes R[Y_m]/(Y_m^p - \beta_m)$, $y_i^p = \beta_i \in R$, $d(y_1) = 1$, $y_i = d^{p^{m-1}-p^{i-1}}(y_m)$ and $d(y_i) \in R[y_1, \cdots, y_{i-1}]$. Obviously, the assertion is valid for $m=1$. We assume that there holds the assertion for $m-1$, that is there exist $x_1, \cdots, x_{m-1}$ such that $R[x_1, \cdots, x_{m-1}] = R[y_1, \cdots, y_{m-1}]$ and the restriction of d to $R[x_1, \cdots, x_{m-1}]$ is of the form $P_0\partial_1 + \cdots + P_{m-2}\partial_{m-1}$. Since $d(y_m) \in R[y_1, \cdots, y_{m-1}] = R[x_1, \cdots, x_{m-1}]$ and $d^{p^{m-1}} = 1$, we have

$$d(y_m) = P_{m-1} + g(x_1, \cdots, x_{m-1}),$$

where $g(x_1, \cdots, x_{m-1})$ is a sum of monomials of degree less than $p^{m-1}-1$. By Lemma 8, $g(x_1, \cdots, x_{m-1})$ is integrable, say $dG(x_1, \cdots, x_{m-1}) = g(x_1, \cdots, x_{m-1})$. Setting $x_m = y_m - G(x_1, \cdots, x_{m-1})$, we get $d(x_m) = P_{m-1}$ and $R[x_1, \cdots, x_m] = R[y_1, \cdots, y_m]$. Since d is a derivation and $R = \{a \in A \mid d(a) = 0\}$, it follows that x_m^p is in R. This completes the proof.

Remark. Let $d = P_0'\partial_1 + \cdots + P_{m-1}'\partial_m$ be another derivation on $A = R[X_1]/(X_1^p - \alpha_1) \otimes \cdots \otimes R[X_m]/(X_m^p - \alpha_m)$ satisfying the condition in Lemma 6. Then, for such d, there holds an analogue of Theorem 9.

Corollary 10. *Let A/R be an $H(p^m)$-Hopf Galois extension, and let $x_1, \cdots, x_m$ be elements of A such that $A = R[x_1, \cdots, x_m]$, $x_i^p = \alpha_i \in R$, $d(x_1) = 1$ and $x_i = d^{p^{m-1}-p^{i-1}}(x_m)$. Then, concerning the action of $d \in H(p^m)$ restricted to $A_i = R[x_1, \cdots, x_i]$, A_i/R is an $H(p^i)$-Hopf Galois extension.*

Proof. From the proof of Theorem 9, we may assume that $x_1, \cdots, x_m$ are chosen as in the proof of the only if part of Theorem 9. Then the assertion follows immediately.

REFERENCES

[1] R. BAER: Algebraische Theorie der differentierbaren Funktionenkörper I, Sitzungsber. Heidelb. Akad. Wiss. Math. -Natur. Kl., 1927, 15—32.

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

[3] A. HATTORI: On higher derivations and related topics, (Proc. Seminar on Derivations and Cohomology of Algebras), Sûrikaisekikenkyûsho Kôkyûroku, **94** (1970), 103—117 (in Japanese).

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

[5] S. SUZUKI: Some types of derivations and their applications to field theory, J. Math. Kyoto Univ. **21** (1981), 375—382.

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

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

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

[9] K. YOKOGAWA: A pair of subalgebras in an Azumaya algebra, Osaka J. Math. **20** (1983), 9—20.

OKAYAMA UNIVERSITY
SCIENCE UNIVERSITY OF OKAYAMA

(*Received November 1, 1982*)