Yokogawa, K.
Osaka J. Math.
18 (1981), 63–73

NON-COMMUTATIVE HOPF GALOIS EXTENSIONS

KENJI YOKOGAWA

(Received October 12, 1979)

Introduction. S. Chase and M. Sweedler [1] defined commutative Hopf Galois extensions as a generalization of separable Galois extensions, and then established a Galois theory to such extensions. On the other hand, T. Kanzaki [3], Y. Takeuchi [7] and others studied non-commutative separable Galois extensions and a Galois theory.

In this paper we consider the case where the rings are not necessarily commutative. In § 1, we shall give the definitions of Hopf Galois extensions, which is divided into three definitions—Hopf Galois extensions, strong Hopf Galois extensions and very strong Hopf Galois extensions— since in non-commutative case, finitely generated faithful projective modules are not necessarily pro-generators. Besides non-commutative separable Galois extensions, we can view certain types of p-algebras as Hopf Galois extensions. Also we shall prove some elementary properties of Hopf Galois extensions in §1. In §2 we examine the integral. Finally in §3, we shall establish a usual Galois theory of very strong Hopf Galois extensions.

In a subsequent paper [8], we shall deal with Hopf Galois extensions over a commutative ring and shall show that the above definition is natural from cohomological view-points.

Throughout this paper, R denotes a commutative ring with identity, H denotes a finite co-commutative Hopf algebra over R. A denotes an R-algebra which is a finitely generated faithful projective R-module. H measures A to A and makes A an H-module algebra, that is there exists an R-homomorphism $\rho: H\otimes_R A\rightarrow A$ with the properties $\rho(h\otimes xy)=\sum_{(h)}\rho(h_{(1)}\otimes x)\rho(h_{(2)}\otimes y)$, $\rho(h\otimes 1)=\varepsilon(h)$, ε is an augumentation, $\rho(gh\otimes x)=\rho(g\otimes\rho(h\otimes x))$, $g, h\in H$, $x, y\in A$. $\rho(h\otimes x)$ is denoted by $h\cdot x$. B denotes the fixed subalgebra $A^H=\{x\in A\,|\,h\cdot x=\varepsilon(h)x \textit{ for any } h\in H\}$. An unspecified $\otimes$ is taken over R. For a left (*resp.* right) B-module M, $\mathrm{End}_B^l(M)$ (*resp.* $\mathrm{End}_B^r(M)$) denotes the left (*resp.* right) B-endomorphism ring of M. This is also denoted as $\mathrm{End}_B({}_BM)$ (*resp.* $\mathrm{End}_B(M_B)$). For other notations and terminologies we shall refer to [1].

1. Hopf Galois extensions

As the commutative case, we make a smash product algebra $A\#H$ as follows;

$A\#H=A\otimes H$ as R-modules, we write $a\#h$ rather than $a\otimes h$. Then multiplication is given by the formula;

$$(a\#g)(b\#h)=\sum_{(g)} ag_{(1)}\cdot b\#g_{(2)}h,\ a,b\in A,\ g,h\in H\,.$$

This is a well-defined R-algebra, since A and H are R-algebras. Well, we have a homomorphism $\alpha\colon A\#H\to \mathrm{End}^r_B(A)$ defined by $(\alpha(a\#h))(x)=ah\cdot x$, $x\in A$. α is an R-algebra homomorphism and A is a left $A\#H$-module. Also we have a left A-homomorphism $\beta\colon {}_A(A\otimes_B A)\to \mathrm{Hom}_R(H, {}_AA)$ and a right A-homomorphism $\beta'\colon (A\otimes_B A)_A\to \mathrm{Hom}_R(H, A_A)$ defined by

$$(\beta(a\otimes b))(h)=ah\cdot b,\ (\beta'(a\otimes b))=(h\cdot a)b\,.$$

Theorem 1.1 *The following conditions are equivalent (the assumption of R-projectivity of A is unnecessary).*

(i) *A is a finitely generated projective right B-module and α is an isomorphism.*

(ii) *A is a left $A\#H$-generator.*

(iii) *A is a finitely generated projective right B-module and β is an isomorphism.*

(iv) *A is a finitely generated projective right B-module and β' is an isomorphism.*

Proof. (i)$\Rightarrow$(ii). From Morita theory, that A is a finitely generated projective right B-module means that A is a left $\mathrm{End}^r_B(A)$-generator. Hence A is a left $A\#H$-generator.
(ii)$\Rightarrow$(i). Since A is a left $A\#H$-generator, A is a finitely generated projective left $\mathrm{End}^l_{A\#H}(A)$-module. $\mathrm{End}^l_{A\#H}(A)$ is anti-isomorphic to $A^H=B$ by $f\mapsto f(1)$, $f\in \mathrm{End}^l_{A\#H}(A)$. Hence A is a finitely generated projective right B-module. As easily checked, this right B-module structure of A coincides with the original one. Again from Morita theory, $\mathrm{End}^r_B(A)=\mathrm{End}^l_{\mathrm{End}^l_{A\#H}(A)}(A)\cong A\#H$, and this isomorphism coincides with α.
(i)$\Leftrightarrow$(iv). Let γ be the composite of the isomorphisms;

$$A\#H=A\otimes H\cong \mathrm{Hom}_R(H^*, A)\cong \mathrm{Hom}^r_A(A\otimes H^*, A)\cong \mathrm{Hom}^r_A(\mathrm{Hom}_R(H, A), A),$$
where $H^*=\mathrm{Hom}_R(H, R)$.

The explicit form of γ is given by

$$(\gamma(a\#h))(f)=af(h),\ a\in A,\ h\in H,\ f\in H^*\,.$$

Next let δ be the composite of the isomorphisms;

$\mathrm{End}^r_B(A)\cong \mathrm{Hom}^r_B(A_B, \mathrm{Hom}^r_A({}_BA, A))\cong \mathrm{Hom}_A(A\otimes_B A_A, A_A)$, where the latter isomorphism is the adjoint isomorphism.

The explicit form of δ is given by

$$\delta(f)(a\otimes b)=f(a)b,\ f\in \mathrm{End}_B^r(A),\ a, b\in A\,.$$

Now, we have the following commutative diagram;

$$\begin{array}{ccc} A\sharp H & \xrightarrow{\quad\alpha\quad} & \mathrm{End}_B^r(A) \\ \wr\| \gamma & & \wr\| \delta \\ \mathrm{Hom}_A^r(\mathrm{Hom}_R(H, A), A) & \xrightarrow{\beta'^*} & \mathrm{Hom}_A^r(A\otimes_B A, A) \end{array}$$

Thus if α is an isomorphism, then β'^* is an isomorphism. Taking the dual again, we get that β' is an isomorphism since $\mathrm{Hom}_R(H, A)$ and $A\otimes_B A$ are finitely generated projective right A-modules.

If β' is an isomorphism, then β'^* is an isomorphism. So α is an isomorphism.

To prove (iii)$\Leftrightarrow$(iv), we use the antipode S of H. Let Φ: $\mathrm{Hom}_R(H, A)\rightarrow \mathrm{Hom}_R(H, A)$ be the homomorphism defined by

$$(\Phi(f))(h)=\sum_{(h)} S(h_{(1)})\cdot f(h_{(2)}),\ f\in \mathrm{Hom}_R(H, A),\ h\in H\,.$$

Φ is an isomorphism, the inverse Φ^{-1} of Φ is given by

$$\Phi^{-1}((f))(h)=\sum_{(h)} h_{(1)}\cdot f(h_{(2)})\,.$$

Now, we have the following diagram, which is commutative as easily checked.

$$\begin{array}{ccc} A\otimes_B A & \xrightarrow{\quad\beta'\quad} & \mathrm{Hom}_R(H, A) \\ \downarrow \beta & & \wr\| \Phi \\ \mathrm{Hom}_R(H, A) & \overset{S^*}{=\!=\!=} & \mathrm{Hom}_R(H, A) \end{array}$$

Thus that β is an isomorphism is equivalent to that β' is an isomorphism.
This completes the proof.

Proposition 1.2. *Let B be merely a subalgebra of A such that α: $A\sharp H\cong \mathrm{End}_B^r(A)$, and A be not only a finitely generated projective right B-module, but also a right B-generator. Then the coherent condition $B=A^H$ follows automatically.*

Proof. Since A is a right B-generator, $B\cong \mathrm{End}^l_{\mathrm{End}_B^r(A)}(A)\cong \mathrm{End}^l_{A\sharp H}A\cong A^H\subset A$. As easily checked, this isomorphism is given by $B\ni b\mapsto b\in A^H\subset A$. Hence $B=A^H$.

DEFINITION. We call an extension A/B *an H-Hopf Galois extension* if an R-algebra A is a finitely generated faithful projective R-module and satisfies the equivalent conditions of Theorem 1.1.

We call an H-Hopf Galois extension A/B *a strong H-Hopf Galois extension* if A is a right B-generator, or equivalently if A is a left $A\sharp H$-pro-generator.

We call a strong H-Hopf Galois extension A/B is *a very strong H-Hopf Galois extension* if A is a left B-pro-generator, or equivalently (as the following Proposition asserts) if A is a left $B\sharp H$-pro-generator.

REMARK. If A/B is a strong H-Hopf Galois extension, then B is a finitely generated faithful projective R-module as is easily proved.

Proposition 1.3. *Let A/B be a strong H-Hopf Galois extension, then the following conditions are equivalent.*

(i) *A is a left B-pro-generator, i.e. A/B is a very strong H-Hopf Galois extension.*

(ii) *A is a left $B\sharp H$-pro-generator.*

(iii) *$A\sharp H$ is a left $B\sharp H$-pro-generator.*

Proof. (i)$\Rightarrow$(ii). We consider the following isomorphism induced from β; ${}_{B\sharp H}(A\otimes_B A)_A \overset{\beta}{\cong} \mathrm{Hom}_R(H, A) = {}_{B\sharp H}(\mathrm{Hom}_B^l(B\sharp H, A))_A$. This isomorphism is a $(B\sharp H, A)$-isomorphism. The right side is isomorphic to ${}_{B\sharp H}\mathrm{Hom}_B^l(B\sharp H, B)\otimes_B A \cong {}_{B\sharp H}(\mathrm{Hom}_R(H_H, R)\otimes_B B)\otimes_B A$ since A is a finitely generated projective left B-module by hypothesis. We know that $\mathrm{Hom}_R(H_H, R)$ is a left H-pro-generator (c.f. [4] Proposition 1). Thus the right side is a finitely generated projective left $B\sharp H$-module. B is a left B-direct summand of A by hypothesis, hence A is a left $B\sharp H$-direct summand of a finitely generated projective left $B\sharp H$-module $A\otimes_B A$. Thus A is a finitely generated projective left $B\sharp H$-module. Also ${}_{B\sharp H}(\mathrm{Hom}_R(H, R)\otimes B)$ is a left $B\sharp H$-generator, so ${}_{B\sharp H}(A\otimes_B A)$ is a left $B\sharp H$-generator. Since A is a finitely generated projective left B-module, a left $B\sharp H$-generator $A\otimes_B A$ is a direct summand of a direct sum of a finite number of copies of A as a left $B\sharp H$-module. Thus A is a left $B\sharp H$-generator.

(ii)$\Rightarrow$(iii). Since A is a $B\sharp H$-generator, $B\sharp H$ is a left $B\sharp H$-direct summand of a direct sum of a finite number of copies of A. And A/B is a strong H-Hopf Galois extension, so A is a finitely generated projective left $A\sharp H$-module. A is a direct summand of a direct sum of finite copies of $A\sharp H$ as a left $A\sharp H$-module, hence as a left $B\sharp H$-module. Thus $B\sharp H$ is a direct summand of a direct sum of finite copies of $A\sharp H$ as a left $B\sharp H$-module, so $A\sharp H$ is a left $B\sharp H$-generator. Similarly using the fact that A is a left $A\sharp H$-generator and that A is a finitely generated projective left $B\sharp H$-module, we get that

$A\sharp H$ is a finitely generated projective left $B\sharp H$-module.

(iii)$\Rightarrow$(i). First we shall show that A is a finitely generated projective left B-module. Since A is a finitely generated projective left $A\sharp H$-module, A is a direct summand of a direct sum of finite copies of $A\sharp H$ as a left $A\sharp H$-module. Since $A\sharp H$ is a finitely generated projective left $B\sharp H$-module, $A\sharp H$ is a direct summand of a direct sum of finite copies of $B\sharp H$ which is a finitely generated projective left B-module. Thus A is a finitely generated projective left B-module. That A is a left B-generator follows easily from that $B\sharp H$ is a left B-generator, that $A\sharp H$ is a left $B\sharp H$-generator and that A is a left $A\sharp H$-generator. This completes the proof.

REMARK. In (iii)$\Rightarrow$(i), in order to prove the finitely generated projectivity of a left B-module A, we used only the projectivity of a left $B\sharp H$-module $A\sharp H$. In Corollary 2.4, we shall show that a strong H-Hopf Galois extension A/B is a very strong Hopf Galois extension if $A\sharp H$ is a finitely generated projective left $B\sharp H$-module.

Here we shall list up some properties in a case $B=R$, which are necessary in a subsequent paper [8].

Corollary 1.4. *If A/R is an H-Hopf Galois extension, then A is an H-progenerator.*

Proof. The assertion follows immediately from Proposition 1.3.

Also we have the following well-known

Proposition 1.5 ([1] Prop. 9.1). *The extension H^*/R is an H-Hopf Galois extension.*

Next we shall consider the fixed subalgebra $A^{H'}$ of A by an admissible (definition below) Hopf subalgebra H' of H.

DEFINITION. We call a Hopf subalgebra H' of H *admissible* if H' is a direct summand of H as R-modules.

We shall list up some properties of an admissible Hopf subalgebra H' of H, which will be found in [1].

(*) *H' is a direct summand of H as a left H'-module* ([1] Theorem 9.9).

(**) *H is a finitely generated projective left* (*resp. right*) *H'-module* ([1] Corollary 10.2).

From now on, H' denotes an admissible Hopf subalgebra of H.

Proposition 1.6. *If A/B is an H-Hopf Galois extension* (*resp. a strong H-Hopf Galois extension*), *then $A/A^{H'}$ is an H'-Hopf Galois extension* (*resp. a* *strong H'-Hopf Galois extension*).

Proof. First we shall show that A is a left $A\# H'$-generator. But this follows easily since A is a left $A\# H$-generator and H' satisfies the condition (*). If A is a finitely generated projective left $A\# H$-module then A is a finitely generated projective left $A\# H'$-module by (**). This verifies the assertion.

Proposition 1.7. *Let A/B be an H-Hopf Galois extension and H' and H'' be admissible Hopf subalgebras of H. Then $A^{H'}\subset A^{H''}$ if and only if $H'\supset H''$. Especially, $A^{H'}=A^{H''}$ if and only if $H'=H''$.*

Proof. "*if part*" is trivial, we shall prove "*only if part*". We have the isomorphism $\alpha\colon A\# H\cong \mathrm{End}_B^r(A)$ and by the restrictions of α, we have $A\# H'\cong \mathrm{End}_{A^{H'}}^r(A)$ and $A\# H''\cong \mathrm{End}_{A^{H''}}^r(A)$. Thus $A^{H'}\subset A^{H''}$ means $A\# H'\supset A'\# H''$. Since A is a finitely generated faithful projective R-module, we get $H'\supset H''$. This completes the proof.

EXAMPLES. (i) Commutative Hopf Galois extensions ([1]) are Hopf Galois extensions in our sense.

(ii) Commutative or non-commutative separable Galois extensions can be regarded as Hopf Galois extensions in our sense. A typical model is the following; Let R be the field of real numbers and Q be a quaternion algebra over R with basis $1, i, j, ij, i^2=j^2=-1, ij=-ji$. σ, τ be the R-automorphism of Q defined by $\sigma(x)=jxj^{-1}$, $\tau(x)=ixi^{-1}$, $x\in Q$. G_1 and G_2 be the group generated by σ and τ respectively. Then Q/R is an $RG_1\otimes RG_2$-Hopf Galois extension with the obvious measuring. If we put $C_1=Q^{RG_1}=R(j)$ then C/C_1 is an $RG_1/$-Hopf Galois extension by Proposition 1.6.

(iii) Let K be a field of characteristic $p\neq 0$ and A be a cyclic algebra (with a cyclic subfield C) of dimension p^2over K. Then $C=K(\theta)$, $\theta^p-\theta+1=0$, $\theta\in A$. The generating automorphism σ of C is given by $\sigma(\theta)=\theta+1$, and σ is extended innerly (say by ξ) to the automorphism of A. Next we consider the K-derivation d of $K(\xi)$ given by $d(\xi)=\xi$. Then we can extend d to the inner derivation (given by θ) of A. We put $D=K[X]/(X^p-X)$ and we shall denote the canonical image of X by the same letter d. D is a Hopf algebra with the diagonalization $\Delta(d)=1\otimes d+d\otimes 1$, the augumentation $\varepsilon(d)=0$, and the antipode $S(d)=-d$. Let G be the group generated by σ, and H be $KG\otimes_K D$. Then H measures A to A naturally and A/K is an H-Hopf Galois extension. So $A/K(\xi)$ is a KG-Hopf Galois extension and $A/K(\theta)$ is a D-Hopf Galois extension.

2. The integral H^H

We shall call $H^H=\{h\in H\mid gh=\varepsilon(g)h \textit{ for any } g\in H\}$ the *integral*. As is well-known, if H is a group ring RG then RG^{RG} is generated by the trace map $\sum_{g\in G} g$.

Proposition 2.1. *Let A/B be an H-Hopf Galois extension and $A\#H$ be a finitely generated projective left $B\#H$-module, then we have*

$\mathrm{Hom}_B^r(A, B)=(1\#H^H)\cdot(A\#H)=H^H\cdot(A\#H)=H^H\cdot(A\#1)$ *where we identify $A\#H$ with $\mathrm{End}_B^r(A)$ by α.*

Proof. $f=\sum_i a_i\#h_i\in A\#H=\mathrm{End}_B^r(A)$ is contained in $\mathrm{Hom}_B^r(A, B)$, if and only if, $f(a)\in B=A^H$ for any $a\in A$. This means

$(1\#g)(\sum_i a_i\#h_i))(a)=\sum_{i,(g)}(g_{(1)}\cdot a_i)(g_{(2)}h_i\cdot a)=g\cdot f(a)=\varepsilon(g)\cdot f(a)=\sum_i \varepsilon(g)a_ih_i\cdot a$ $=((1\#\varepsilon(g))(\sum_i a_i\#h_i))(a)$, for any $a\in A$, $g\in G$. Thus $(1\#g)(\sum_i a_i\#h_i)=\varepsilon(g)(\sum_i a_i\#h_i)$. Hence we have

$$\mathrm{Hom}_B^r(A, B)=(A\#H)^H=\{x\in A\#H\,|\,(1\#g)x=\varepsilon(g)x \text{ for any } g\in H\}\ .$$

The inclusion $(A\#H)^H\supset H^H\cdot(A\#H)$ is clear, and to show the converse we may assume that R is a local ring. Further since $A\#H$ is a finitely generated projective left $B\#H$-module and $(A\#H)^H$ depends only on the left H-module structure of $A\#H$, we first assume that $A\#H=B\#H$ as a left $B\#H$-module. Let $\{b_i\}$, $\{h_i\}$ be an R-basis of B, H respectively. Then for $x=\sum_i b_i\#r_ih_i\in B\#H$, $r_i\in R$,

$$x\in(B\#H)^H, \text{ if and only if, } hx=\sum_i b_i\#r_ihh_i=\varepsilon(h)x=\sum_i b_i\#r_i\varepsilon(h)h_i, \text{ for any } h\in H.$$

Thus $r_ihh_i=r_i\varepsilon(h)h_i$. Hence $x=\sum_i(1\#r_ih_i)(b_i\#1)\in(1\#H^H)\cdot(A\#H)$. By usual direct sum arguments, we get $\mathrm{Hom}_B^r(A, B)=(1\#H^H)\cdot(A\#H)=H^H\cdot(A\#H)$. Since $(1\#g)(a\#h)=\sum_{(h)}(1\#gh_{(1)})(S(h_{(2)})\cdot a\#1)$, we get $(1\#H^H)\cdot(A\#H)=(1\#H^H)\cdot(A\#1)$. This completes the proof.

Corollary 2.2. *Further if we assume that A/B is a strong H-Hopf Galois extension, then*

$$H^H(A)=A^H(=B)$$

where H^H is regarded as a subalgebra of $\mathrm{End}_B^r(A)$ via α.

Proof. We shall consider the homomorphism τ: $\mathrm{Hom}_B^r(A, B)\otimes_{\mathrm{End}_B^r(A)}A\to B$ defined by $\tau(f\otimes a)=f(a)$, $f\in\mathrm{Hom}_B^r(A, B)$, $a\in A$. By the isomorphism $\mathrm{Hom}_B^r(A, B)\cong(1\#H^H)\cdot(A\#1)$, τ is converted to τ': $((1\#H^H)\cdot(A\#1))\otimes_{\mathrm{End}_B^r(A)}A\to B$, defined by $\tau'((1\#h)(a\#1)\otimes b)=h\cdot(ab)$, $h\in H^H$, $a, b\in A$. $(A\#1)(A)=A$, hence the image of τ' equals to $H^H(A)=H^H\cdot A$, which is $B=A^H$ since A is a right B-generator.

REMARK. The assumption of Corollary 2.2 is equivalent to the A/B is a very strong H-Hopf Galois extension as Corollary 2.4 asserts.

Proposition 2.3. *Under the same assumption as Corollary 2.2, B is a direct summand of A as a B-B-bimodule. Especially A is a left B-generator.*

Proof. Since $H^H \cdot A = B$, there exists $a_i \in A$, $h_i \in H^H$ such that $1_B = \sum_i h_i \cdot a_i$. Let ϕ_i be the homomorphism $A \to B$ defined by $\phi_i(a) = h_i \cdot a$, $a \in A$. Then ϕ_i is not only a right B-homomorphism but also a left B-homomorphism. Thus B is a direct summund of A as a B-B-bimodule. This verifies the assertion.

Corollary 2.4. *A strong H-Hopf Galois extension A/B is a very strong H-Hopf Galois extension if $A \# H$ is a finitely generated projective left $B \# H$-module.*

Proof. From the Remark following Proposition 1.3, we may only prove that A is a left B-generator. But this follows readily from Proposition 2.1 and 2.3.

Proposition 2.5. *Let A/B be a very strong H-Hopf Galois extension, then* $\mathrm{End}_B^r(A) = A \# H$ *is separable over B in the sense of Hirata* [2] *(H-separable in* [5]).

Proof. We get it easily by Sugano [6] Theorem 7, since B is a direct summand of A as a B-B-bimodule.

3. Hopf Galois theory

In this section, we shall investigate the fixed subalgebra $A^{H'}$ of A by an admissible Hopf subalgebra H' of H. From now on, we always assume that A/B is a very strong H-Hopf Galois extension.

First we shall show that $A^{H'} = (H'^{H'} \cdot (A \# H))(A)$. For this purpose, we shall define $\mu: A \otimes_B \mathrm{Hom}_B^r(A, B) \to \mathrm{End}_B^r(A)$, $\tau: \mathrm{Hom}_B^r(A, B) \otimes_{\mathrm{End}_B^r(A)} A \to B$ by the formulas;

$$(\mu(a \otimes f))(b) = af(b)\,, \quad \tau(f \otimes a) = f(a)\,, \quad a, b \in A\,, \quad f \in \mathrm{Hom}_B^r(A, B)\,.$$

Then from Morita theory, there exists a one-to-one correspondence between right ideals of $A \# H = \mathrm{End}_B^r(A)$ and right B-submodules of A. Let I be a right ideal of $A \# H$, then the corresponding right B-submodule of A is the image $I(A)$. Furthermore, there exists a one-to-one correspondence between left B-submodules of $\mathrm{Hom}_B^r(A, B)$ and left ideals of $A \# H$, for a left B-submodule J of $\mathrm{Hom}_B^r(A, B)$ the corresponding left ideal is $(A \# H) \cdot J$ (the product is taken as subalgebras of $\mathrm{End}_B^r(A)$). If we denote the right annihilator of $(A \# H) \cdot J$ by $((A \# H) \cdot J)^r$, which is a right ideal of $A \# H$. Then by the former correspondence, the corresponding right B-sumbodule of A is $J^r=\{a\in A\mid \tau(J\otimes a)=0\}$ the right annihilator of J relative to τ. Simultaneously if we denote a left annihilator of a right ideal I by I^l, then by the later correspondence, the corresponding left B-submodule of $\mathrm{Hom}_B^r(A,B)$ is $(I(A))^l=\{f\in \mathrm{Hom}_B^r(A,B)\mid \tau(f\otimes I(A))=0\}$, the left annihilator of $I(A)$ relative to τ.

Lemma 3.1 (c.f. [1] Lemma 11.1). *A is a pro-generator as a left $B\#H'$-module. Further let τ' be the canonical pairing τ': $\mathrm{Hom}_B^r(A,B)\otimes_{B\#H'}A\to B$, $\tau'(f\otimes a)=f(a)$, $f\in\mathrm{Hom}_B^r(A,B)$, $a\in A$. Then $(H'^{H'}\cdot A)^l=\{f\in\mathrm{Hom}_B^r(A,B)\mid \tau'(f\otimes H'^{H'}\cdot A)=0\}$ equals to $\mathrm{Hom}_H^r(A,B)I_{H'}$, where $I_{H'}=\{h\in H'\mid \varepsilon(h)=0\}$, and $(\mathrm{Hom}_B^r(A,B)I_{H'})^r=\{a\in A\mid \tau'(\mathrm{Hom}_B^r(A,B)I_{H'}\otimes a)=0\}$ equals to $H'^{H'}\cdot A$.*

Proof. A is a left $B\#H$-pro-generator and H is a left H'-pro-generator by (*), (**). Hence A is a left $B\#H'$-pro-generator.

Next the inclusions $(H'^{H'}\cdot A)^l\supset\mathrm{Hom}_B^r(A,B)I_{H'}$ and $(\mathrm{Hom}_B^r(A,B)I_{H'})^r\supset H'^{H'}\cdot A$ are clear. To show the inverse inclusions, we may assume that R is a local ring. First we assume that $A=B\#H'$ as a left $B\#H'$-module. If a is an element of $\mathrm{Hom}_B^r(A,B)=B\otimes\mathrm{Hom}_R(H',R)$, then $\tau'(a\otimes H'^{H'}\cdot A)=\tau'(a\otimes H'^{H'}\cdot B\# H')=\tau'(aH'^{H'}\otimes B\# H')$. So $\tau'(a\otimes H'^{H'}\cdot A)=0$ if and only if $aH'^{H'}=0$. But by [4] Proposition 1, $\mathrm{Hom}_R(H',R)\cong M\otimes H'$ as right H'-modules, with M an invertible R-module. Since we have assumed that R is a local ring, $M\cong R$, thus $B\otimes\mathrm{Hom}_R(H',R)\overset{\phi}{\cong}B\otimes H'$ as right $B\#H'$-modules. Hence we have $\phi(a)H'^{H'}=0$. An easy computation shows that $\phi(a)\in(B\otimes H')I_{H'}$. So we get $a\in(B\otimes\mathrm{Hom}_R(H',R))I_{H'}$. Next if u is an element of $B\#H'$, then $\tau'(\mathrm{Hom}_B^r(A,B)I_{H'}\otimes u)=\tau'(\mathrm{Hom}_B^r(A,B)\otimes I_{H'}u)$, hence $\tau'(\mathrm{Hom}_B^r(A,B)I_{H'}\otimes u)=0$ if and only if $I_{H'}u=0$. As is easily proved, this is true if and only if $u\in B\#H'^{H'}=H'^{H'}(B\#H)$. The general case follows from a routine direct sum argument. This verifies the assertion.

Corollary 3.2. $(A\#H\cdot I_{H'})^r=H'^{H'}\cdot(A\#H)$, $(H'^{H'}\cdot(A\#H))^l=(A\#H)\cdot I_{H'}$ *and* $\mu(A^H\otimes_B\mathrm{Hom}_B^r(A,B))\subset H'^{H'}\cdot(A\#H)$.

Proof. By the former Morita correspondence of this section, $((A\#H)\cdot I_{H'})^r$ corresponds to $(\mathrm{Hom}_B^r(A,B)I_{H'})^r$ and $H'^{H'}\cdot(A\#H)$ corresponds to $H'^{H'}\cdot A$, and by the later correspondence, $(H'^{H'}\cdot(A\#H))^l$ corresponds to $((H'^{H'}\cdot(A\#H))^l=(H'^{H'}\cdot A)^l$, and $(A\#H)\cdot I_{H'}$ corresponds to $\mathrm{Hom}_B^r(A,B)I_{H'}$. So we get the former two relations by Lemma 3.1.

Next as can be easily proved, $\mu(A^{H'}\otimes\mathrm{Hom}_B^r(A,B))$ is contained in $((A\#H)\cdot I_{H'})^r$, which is equal to $H'^{H'}\cdot(A\#H)$ by Lemma 3.1. This verifies the assertion.

Now we shall prove

Proposition 3.3. $A^{H'}=(H'^{H'}\cdot(A\#H))(A)(=H'^{H'}\cdot A)$ *and* $A^{H'}$ *is a direct* *summand of A as an $A^{H'}$-$A^{H'}$-bimodule.*

Proof. By the Morita correspondence, $H'^{H'}\cdot(A\# H) \rightsquigarrow (H'^{H'}\cdot(A\# H))(A) \rightsquigarrow \mu((H'^{H'}\cdot(A\# H))(A)\otimes_B \mathrm{Hom}_B^r(A, B))$ is identity, so $H'^{H'}\cdot(A\# H)=\mu((H'^{H'}\cdot(A\# H))(A)\otimes_B \mathrm{Hom}_B^r(A, B))$, which is clearly contained in $\mu(A^{H'}\otimes_B \mathrm{Hom}_B^r(A, B))$, and by Corollary 3.2, $\mu(A^{H'}\otimes_B \mathrm{Hom}_B^r(A, B))$ is contained in $H'^{H'}\cdot(A\# H)$. Thus $\mu(A^{H'}\otimes_B \mathrm{Hom}_B^r(A, B))=H'^{H'}\cdot(A\# H)$. Again by the Morita correspondence, $A^{H'} \rightsquigarrow \mu(A^{H'}\otimes_B \mathrm{Hom}_B^r(A, B))=H'^{H'}\cdot(A\# H) \rightsquigarrow (H'^{H'}\cdot(A\# H)(A)=H'^{H'}\cdot A$ is identity, we get $A^{H'}=H'^{H'}\cdot A$. Similarly to the proof of Proposition 2.3, we get that $A^{H'}$ is a direct summand of A as an $A^{H'}-A^{H'}$-bimodule. This completes the proof.

Definition. Let T be an intermediate ring of A and B. We shall write $T\Rightarrow H'$ to mean that the following condition holds: Given w in $A\# H$, $w(T)=0$ if and only if $w\in(A\# H)I_{H'}$.

Theorem 3.4. *Let H be a finite co-commutative Hopf algebra over a commutative ring R, and A/B be a very strong H-Hopf Galois extension. Then*

(i) *If H' is an admissible Hopf subalgebra of H and T is an intermediate ring of A and B, which is a direct summaud of A as a B-B-bimodule, then $T\Rightarrow H'$ if and only if $T=A^{H'}$. If these conditions hold, then A/T is a strong H'-Hopf Galois extension.*

(ii) *If $T'\Rightarrow H'$ and $T''\Rightarrow H''$ with T', T'', H', H'' as in* (i), *then $T'\subset T''$ if and only if $H'\supset H''$. In particular, $T'=T''$ if and only if $H'=H''$.*

(iii) *Let H', H'' be an admissible Hopf subalgebra of H, then $H'\subset H''$ if and only if $A^{H'}\supset A^{H''}$. In particular, $H'=H''$ if and only if $A^{H'}=A^{H''}$.*

Proof. (iii) is proved in Proposition 1.5 and in view of (i), (ii) is simply a restatement of (iii). We shall prove (i). Let $T=A^{H'}$, then by Proposition 3.3, T is a direct summand of A as a T-T-bimodule, hence as a B-B-bimodule. For $w\in A\# H$, $w(T)=w(A^{H'})=0$ means $w\cdot(H'^{H'}\cdot(A\# H))=0$ since $A^{H'}=(H'^{H'}\cdot(A\# H))(A)$. Thus w is contained in $(H'^{H'}\cdot(A\# H))^l$, which is $(A\# H)\cdot I_{H'}$ by Corollary 3.2.

Conversely, let T be an intermediate ring of A and B which is a direct summand of A as a B-B-bimodule, and assume that $T\Rightarrow H'$ for some admissible Hopf subalgebra H' of H. If $w\in A\# H$, then since $\mu(T\otimes_B \mathrm{Hom}_B^r(A, B))(A)=T$, it is clear that $w\cdot\mu(T\otimes_B \mathrm{Hom}_B^r(A, B))=0$ if and only if $w(T)=0$. But by definition, this is true if and only if $w\in(A\# H)\cdot I_{H'}$. Hence $(\mu(T\otimes_B \mathrm{Hom}_B^r(A, B))^l=(A\# H)\cdot I_{H'}$. Since T is a diect summand of A as a B-B-bimodule, $\mu(T\otimes_B \mathrm{Hom}_B^r(A, B))$ is generated by a projection homomorphism $A\rightarrow T$ in $\mathrm{End}_B^r(A)=A\# H$, which is an idempotent. Hence $\mu(T\otimes_B \mathrm{Hom}_B^r(A, B))=(\mu(T\otimes_B \mathrm{Hom}_B^r(A, B)))^{lr}=((A\# H)\cdot I_{H'})^r=H'^{H'}\cdot(A\# H)$ by Corollary 3.2. Thus

$T=(\mu(T\otimes_B \mathrm{Hom}_B^r(A, B))(A)=(H'^{H'}\cdot(A\# H))(A)=A^{H'}$ by Proposition 3.3. This completes the proof.

References

[1] S. Chase and M. Sweedler: *Hopf algebras and Galois theory,* Lect. Note in Math. **97**, Springer, 1969.

[2] K. Hirata: *Some types of separable extensions of rings,* Nagova Math. J. **33** (1968), 107–115.

[3] T. Kanzaki: *On commutor rings and Galois theory of separable algebras,* Osaka J. Math. **2** (1965), 137–145.

[4] R. Larson and M. Sweedler: *An associative orthogonal bilinear form for Hopf algebras,* Amer. J. Math. **91** (1967), 75–94.

[5] K. Sugano: *Note on semisimple extensions and separable extensions,* Osaka J. Math. **4** (1967), 265–270.

[6] K. Sugano: *Note on separability of endomorphism rings,* J. Fac. Sci. Hokkaido Univ. **21** (1971), 196–208.

[7] Y. Takeuchi: *On Galois extensions over commutative rings,* Osaka J. Math. **2** (1965), 137–145.

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

Department of Mathematics
Faculty of Science
Nara Women's University
Nara 630, Japan