Chin. Ann. of Math.
19B: 3(1998),311-320.

H-SEPARABLE RINGS AND THEIR HOPF-GALOIS EXTENSIONS

Jiang Xiaolong* Xu Yonghua**

Abstract

First, some properties of H-separable rings are discussed, and it is shown that the H-separable ring A can be represented as the tensor product of its subrings under certain conditions. Secondly, a necessary and sufficient condition is obtained for a Hopf Galois extension A/B to be H-separable. Finally, some equivalent conditions are got for an H-separable ring A to be a Hopf-Galois extension over a certain subring B.

Keywords H-separable ring, Hopf-Galois extension, Subring
1991 MR Subject Classification 16W30
Chinese Library Classification O153.3

§1. Introduction

Let A be a ring and B a subring of A. A is called an extensiuon of B denoted by A/B if B and A admit the same identity. For an extension A/B, we always denote by $C(A)$ the center of A, and by $V_A(B)$ the centralizer of B in A, i.e., $C(A) = \{a \in A | aa' = a'a, \ \forall a' \in A\}$, $V_A(B) = \{a \in A | ab = ba, \ \forall b \in B\}$. It is clear that both $C(A)$ and $V_A(B)$ are subrings of A.

Kreimer and Takeuchi[1] introduced the notion of Hopy-Galois extension of a noncommutative ring A over its subring B, which generalized the former notions of both the Galois exiension with Galois group G acting on a ring and the commutative Hopf-Galois extension defined by Chase and Sweedler[2]. Since the concept of H-separable extension was introduced by K. Hirata, many studies on the property and structure of H-separable rings in Galois extensions of skew polynormal rings[3−7] have revealed closed structure relations between H-separable extensions and Hopf-Galois extensions.

In Section 2 of this paper, we discuss some properties of H-separable extensions and show that if A/B is H-separable, the centers of A and B are equal, and B is a direct summand of A as (B, B)-bimodule, then $V_A(B)$ is C-Azumaya, and $A \cong B \otimes_C V_A(B)$. Since a central separable extension is H-separable, this result extends the commutor theorem[8,§4], which says that if A/C is a central separable extension, then for any central separable subalgebra $B, A \cong B \otimes V_A(B)$.

It is known that a Galois extension A/B with finite Galois group G is always separable, but this property does not exist in Hopf-Galois extensions. In the last part of Section 2 we discuss the relations between Hopf-Galois extensions and H-separable extensions, a

Manuscript received November 6, 1995.
*Department of Mathematics, Zhongshan University, Guangzhou 510275, China.
**Institute of Mathematics, Fudan University, Shanghai 200433, China.

necessary and sufficient condition is given for A/B to be H-separable when it is a Hopf-Galois extension.

In Section 3, we apply the results in Section 2 to obtain some equivalent conditions for an H-separable extension A/B to be Hopf-Galois.

§2. Properties of H-Separable Extensions

Let A, A' be any rings with identities ${}_AM_{A'}, {}_AN_{A'}$ be (A, A')-bimodules. If there are a bimodule ${}_AL_{A'}$ and an integral $n > 0$ with $M \oplus L = \bigoplus\limits_{i=1}^{n} N_i$, where $N_i = N,\ i = 1, \cdots, n$, then we denote it by ${}_AM_{A'}|{}_AN_{A'}$. In particular, for $n = 1$, it is denoted by ${}_AM_{A'} < \oplus_A N_{A'}$. So ${}_AM_{A'}|{}_AN_{A'}$ means ${}_AM_{A'} < {}_A\Big(\bigoplus\limits_{i=1}^{n} N_i\Big)_{A'} N_i = N,\ i = 1, \cdots, n$, for some integral $n > 0$.

A ring extension A/B is said to be H-separable, if ${}_AA \otimes_B A_A|{}_AA_A$. Here the (A, A)-module action on $A \otimes_B A$ is $a\big(\sum\limits_i a_i \otimes a_i'\big)a' = \sum\limits_i aa_i \otimes a_i'a'$. If we set $(A \otimes_B A)^A = \{x \in A\otimes_B A | ax = xa,\ \forall a \in A\}$, then it can be proved that A/B is H-separable iff there exist some $v_i \in V (i = 1, \cdots, n)$ and $\sum\limits_j x_{ij}\otimes y_{ij} \in (A\otimes_B A)^A$ such that $\sum\limits_{i,j} v_i x_{ij}\otimes y_{ij} = 1\otimes 1\{\sum\limits_{i,j} x_{ij}\otimes y_{ij} \in (A \otimes_B A)^A,\ v_i \in V_A(B)\}$ is called an H-separable system of A/B. Separable extension has been studied in [8]. It is known that a ring extension A/B is separable iff there is an element $\sum\limits_i x_i \otimes y_i \in (A \otimes_B A)^A$ with $\sum\limits_i x_i y_i = 1$, while $\{x_i, y_i\}_{i=1}^n$ is called a separable system. It is proved in [9] that if A/B is H-separable then it is also separable and $V_A(B)$ is a finite generated projective $C(A)$-module. Denote by p the projection $V_A(B) \to C(A)$. Then we have

Lemma 2.1. *If A/B is H-separable with H-separable system $\{x_{ij}\otimes y_{ij} \in (A\otimes_B A)^A,\ v_i \in V_A(B)\}$, the $\{p(v_i)x_{ij}, y_{ij}\}_{ij}$ is separable system of A over B.*

Proof. By hypothesis, $p(v_i) \in C(A)$, and

$$\sum_j x_{ij} \bigotimes y_{ij} \in (A \otimes_B A)^A \Rightarrow \begin{cases} \sum\limits_j x_{ij} y_{ij} \in C(A), \\ \sum\limits_{ij} p(v_i) x_{ij} \otimes y_{ij} \in (A \otimes_B A)^A. \end{cases}$$

Then

$$\sum_{ij} p(v_i) x_{ij} y_{ij} = \sum_i p(v_i)\Big(\sum_j x_{ij} y_{ij}\Big) = \sum_i p\Big(\sum_j v_i x_{ij} y_{ij}\Big) = p\Big(\sum_{ij} v_i x_{ij} y_{ij}\Big) = p(1) = 1,$$

which completes the proof.

For a separable extension A/B, if $B \subset C(A)$, A is called a separable algebra. When $B = C(A)$, A becomes a central separable algebra, or a B-Azumaya algebra. It is proved in [8, Theorem II. 3.4 and Lemma II. 3.1] that if A is C-Azumaya, then (i) C is a direct summand of A as C-submodule, (ii) A is a C-progenerator, (iii) $A \otimes_C A^{\mathrm{op}} \cong \mathrm{Hom}_C(A, A)$. By them we have the following lemma.

Lemma 2.2. *If $C = C(A)$ for a ring A and D is C-Azumaya, then $D' = A \otimes_C D$ is H-separable over A and ${}_AD'_A|{}_AA_A$.*

Proof. Recall that if D is C-Azumaya, then D is a C-progenerator[8, Theorem 3.4]. So ${}_CD_C|{}_CC_C$, and then ${}_AD'_A|{}_AA \otimes_C D_A|A \otimes_C C_A$. But $A \otimes_C C \cong A$, we have ${}_AD'_A|{}_AA_A$.

Still, as a C-Azumaya algebra D has the property $D\otimes D^{\rm op}\cong \mathrm{Hom}_C(D,D)$. The isomorphism is $d\otimes d'\mapsto(\psi: x\mapsto dxd')$, which is also a (D,D)-map. The (D,D)-bimodule action on $D\otimes_C D$ and $\mathrm{Hom}_C(D,D)$ are respectively: $\forall x,y,d\in D, \forall \sum\limits_i d_i\otimes d_i'\in D\otimes_C D,\ x\big(\sum\limits_i d_i\otimes d_i'\big)y=\sum\limits_i xd_i\otimes d_i'y, (xfy)(d)=xf(d)y$. So the D-bimodule structure of $\mathrm{Hom}_C(D,D)$ is induced by the latter D-bimodule D (the domain). We write the former isomorphism as: ${}_DD\otimes_C D_D\cong\mathrm{Hom}_C(D,{}_DD_D)$. So

$${}_DD\otimes_C D_D\cong\mathrm{Hom}_C(D,{}_DD_D)|\mathrm{Hom}_C(C,{}_DD_D)\cong{}_DD_D,$$

that is, D/C is H-separable. As C is a direct summand of D, A is a subring of $A\otimes_C D$ and

$$(A\otimes_C D)\otimes_A(A\otimes_C D)\cong(A\otimes_A A)\otimes_C(D\otimes_C D)|(A\otimes_A A)\otimes_C D\cong A\otimes_C D.$$

Checking the morphism we get ${}_{D'}D'\otimes_A D'_{D'}|{}_{D'}D'_{D'}$, that is, D'/A is also H-separable.

Proposition 2.1. *Set A/B to be a ring extension, D is one of its intermediate rings. Then the folloing are equivalent:*

(1) *The (D,A)-epimorphism $\pi: D\otimes_B A\to A$ is splitting (i.e., there exists a (D,A)-module morphism $f: A\to D\otimes_B A$ with $\pi f=I_A$), where $\pi(d\otimes a)=da,\ \forall d\in D,\ a\in A$.*

(2) *There exists an element $\sum\limits_i d_i\otimes x_i\in(D\otimes_B A)^D$ with $\sum\limits_i d_ix_i=1$.*

(3) *A is a direct summand of ${}_DD\otimes_B A_A$ as (D,A)-module.*

(4) *${}_DA_A|{}_DD\otimes_B A_A$.*

Proof. (1) $\Rightarrow$ (2). Set $f(1)=\sum\limits_i b_i\otimes x_i,\ \forall b\in D$. Then

$$bf(1)=f(b)=f(1)b.$$

Here

$$\sum_i b_i\otimes x_i\in(D\otimes_B A)^D.$$

By $\pi f=I_A$, we get $\sum\limits_i b_ix_i=1$.

(2) $\Rightarrow$ (1). Define $f(a)=\sum_i b_i\otimes x_ia,\ \forall a\in A$. It is easy to see that f is a (D,A)-module map and $\pi f(a)=\big(\sum\limits_i b_ix_i\big)a=a,\ \forall a\in A$, that is, $\pi f=I_A$.

(3) $\Rightarrow$ (4). Recalling the notion of ${}_DA_A|{}_DD\otimes_B A_A$, we can see that (3) is a spesial case of (4).

(4) $\Rightarrow$ (2). By the assumption, there exists a natural number n with A a direct summand of $\bigoplus\limits_1^n(D\otimes_B A)$ as (D,A)-bimodule. So we have (D,A)-bimodule maps f_i,g_i :

$${}_DA_A \underset{g_i}{\overset{f_i}{\rightleftarrows}} {}_D D\otimes_B A_B$$

with

$$\sum_{i=1}^n g_if_i=I_A.$$

Onviously, $f_i(1)\in(D\otimes_B A)^D,\ g_i(1\otimes 1)\in V_A(B)$. Denote $f_i(1)=\sum\limits_j b_{ij}\otimes x_{ij}$. Then

$$\sum_{i,j}b_{ij}\otimes g_i(1\otimes 1)x_{ij}\in(D\otimes_B A)^D.$$

Here

$$\sum_{i,j} b_{ij} \otimes g_i(1 \otimes 1)x_{ij} = \sum_{i,j} g_i(b_{ij} \otimes x_{ij}) = \sum_i g_i f_i(1) = 1.$$

So we get $\sum\limits_k b_k \otimes x_k = \sum\limits_{i,j} b_{ij} \otimes g_i(1 \otimes 1)x_{ij}$ as desired.

(1) $\Leftrightarrow$ (3). It is easy to see, so we omit the proof.

Note. When D satisfies one of the above conditions in Proposition 2.1, it is called a left relative separable extension of B in A. From the condition (2) we know that a separable extension D/B is also a left relative separable extension.

Lemma 2.3. *If a ring extension A/B is H-separable and its intermediate subring D is left relative separable over B, then A/D is also H-separable.*

Proof. By the hypothesis D is left relative separable over B, so ${}_DA_A|_DD \otimes_B A_A$ by Proposition 2.1(4). Thus

$${}_AA \otimes_D A_A|_AA \otimes_D D \otimes_B A_A \cong_A A \otimes_D A_A,$$

that is, A/D is H-separable.

Lemma 2.4. *If A/B is H-separable, A'/B is another extension with a ring epimorphism $f : A \to A'$, and f fixes B pointwise, then A'/B is also H-separable.*

Proof. Denote by $\{\sum\limits_j x_{ij} \otimes y_{ij} \in (A \otimes_B A)^A,\ v_i \in V_A(B)\}$ the H-separable system of A over B. Then $f(v_i) \in V_{A'}(B)$. Also $\forall a' \in A'$, there exists $a \in A$ with $f(a) = a'$. Then we have

$$\begin{aligned}\sum_j a' f(x_{ij}) \otimes f(y_{ij}) &= f \otimes f\Big(\sum_j a x_{ij} \otimes y_{ij}\Big)\\ &= \sum_j f(x_{ij}) \otimes f(y_{ij}a) = \sum_j f(x_{ij}) \otimes f(y_{ij})a',\end{aligned}$$

$$\begin{aligned}\sum_j f(v_i) f(x_{ij}) \otimes f(y_{ij}) &= f \otimes f\Big(\sum_j v_i x_{ij} \otimes y_{ij}\Big)\\ &= f \otimes f(1 \otimes 1) = 1 \otimes 1.\end{aligned}$$

So $\big\{\sum\limits_j f(x_{ij}) \otimes f(y_{ij}) \in (A' \otimes_B A')^{A'},\ f(v_i) \in V_{A'}(B)\big\}_i$ is the desired H-separable system.

Lemma 2.5. *Suppose A/B is H-separable, $C(A) = C$. For brevity denote $V_A(B)$ by V. $\mathfrak{B}_l, \mathfrak{B}, \mathfrak{V}, \mathfrak{V}_l$ are respectively the sets.*

$\mathfrak{B}_l = \{B' \supset B|_{B'}B'_{B'} < \oplus_{B'}A_{B'},\ _{B'}B' \otimes_B A_A \xrightarrow{\mu}_{B'} A_A$ *splits, i.e., there is a (B', A)-module map f with $\mu f = I_A$, here $\mu(b' \otimes a) = b'a\}$;*

$\mathfrak{B} = \{A \supset B' \supset B|B'/B$ *is separable,* $_{B'}B'_{B'} < \oplus_{B'}A_{B'}\}$;

$\mathfrak{V}_i = \{V' \supset C|_{V'}V' < \oplus_{V'}V,\ _{V'}V' \otimes_C V_V \xrightarrow{\pi}_{V'} V_V$ *splits, i.e., there is a $(V'V)$-module map g with $\pi g = I_V,\ \pi(v' \otimes v) = v'v\}$;*

$\mathfrak{V} = \{V \supset V' \supset C|V'/C$ *is separable*$\}$.

Then $B' \mapsto V_A(B')$ and $V \mapsto V_A(V')$ are mutually conversible 1-1 *correspondence between $\mathfrak{B}_l$ (resp.$\mathfrak{B}$) and $\mathfrak{V}_l$ (resp. $\mathfrak{V}$).*

For a ring extension A/B, $B \cdot V_A(B)$ is its intermdiate subring. In fact, it is obvious that $A \supset B \cdot V_A(B) \supset B$, and $\forall b_1, b_2 \in B, v_1, v_2 \in V_A(B), (b_1v_1)(b_2v_2) = (b_1b_2) \cdot (v_1v_2) \in$

$B \cdot V_A(B)$. That is, the product is closed in $B \cdot V_A(B)$ as desired.

Theorem 2.1. *Let A/B be a ring extension, $C(A) = C(B)$. Then A/B is H-separable, B is a direct summand of A as (B, B)-bimodule iff $V_A(B)$ is C-Azumaya, and $A \cong B \otimes_C V_A(B)$.*

Proof. ($\Rightarrow$) A/B is H-separable ${}_B B_B < \oplus_B A_B$, so $V_A(V_A(B)) = B$ (see [9]). Therefore

$$V_{V_A(B)}(V_A(B)) = V_A(B) \cap V_A(V_A(B)) = V_A(B) \cap B = V_B(B) = C,$$

that is,

$$C(V_A(B)) = C.$$

By the correspondence between $\mathfrak{B} \to \mathfrak{V}, \mathfrak{B} \ni B \mapsto V_A(B), V_A(B)/C$ is separable, so $V_A(B)$ is C-Azumaya. As a notational convenience we set $V = V_A(B)$ afterwords. From [8, Theorem II.3.4 and Lemma II.3], we see that C is a direct summand of V as C-module, $V \otimes_C V^{\mathrm{op}} \cong \mathrm{Hom}_C(V, V)$, the map is $\varphi(v \otimes v')(x) = vxv'$, and also V is a finitely generated C-projection. Define the $(V \otimes_C V^{\mathrm{op}})$-module action on A as: $(v \otimes v')a = vav',\ \forall v, v' \in V,\ a \in A$. Now we prove

$$\mathrm{Hom}_{V \otimes_C V^{\mathrm{op}}}(V, A) \cong B.$$

First, $\forall f \in \mathrm{Hom}_{V \otimes_C V^{\mathrm{op}}}(V, A)$, f is determined by $f(1)$, but $vf(1) = f(v) = f(1)v,\ \forall v \in V$. So $f(1) \in V_A(V) = B$. Conversely, $\forall b \in B$, define a map $f_b : f_b(v) = bv,\ \forall v \in V$. Obviously, $f_b \in \mathrm{Hom}_{V \otimes_C V^{\mathrm{op}}}(V, A)$. So we get that $\psi : f \mapsto f(1)$ is an isomorphism from B to $\mathrm{Hom}_{V \otimes_C V^{\mathrm{op}}}(V, A)$. Next simce V is a C-generator,

$$I_C(V) = \Big\{ \sum_i f_i(v_i) | f_i \in \mathrm{Hom}_C(V, C),\ v_i \in V \Big\} = C.$$

So by [10, Proposition A.6] we have

$$\begin{aligned} \rho : \mathrm{Hom}_{\mathrm{Hom}_C(V,V)}(V, A) \otimes_C V &\to A, \\ f \otimes v &\mapsto f(v), \end{aligned}$$

is an isomorphism. But $\varphi : \mathrm{Hom}_C(V, V) \cong V \otimes_C V^{\mathrm{op}}$ is an algebra isomorphism, we get the following isomorphism:

$$\rho' : \mathrm{Hom}_{V \otimes_C V^{\mathrm{op}}}(V, A) \otimes_C V \to A.$$

Hence $\rho'' : B \otimes_C V \cong A$, by $b \otimes v \mapsto bv$, which is induced by ρ'. Checking it directly we can see that the map is an algebra morphism.

($\Leftarrow$) By Lemma 2.2, $A \cong B \otimes_C V_A(B)/B$ is H-separable, and $V_A(B)/C$ is C-Azumaya. So C is a direct summand of $V_A(B)$ as a C-module. Thus B is a direct summand of A as a left B-module. But B commutates with $V_A(B)$, so B is a direct summand of A as a B-bimodule.

Before presenting the following Theorem 2.2 we need some preparation. We assume the reader to be familiar with the basic notions of Hopf algebra theory. Let R be a commutative ring with identity, J be a finite Hopy algebra over R (that is, J is a finitely generated projective R-module) with structure maps μ, m, Δ, ϵ. Throughout we adopt Sweedler's "sigma notation". Denote by J^* the dual algebra of J. As J is finitely generated projective, the Hopf algebra structure of J induces that of J^*.

Let A be an R-algebra. A is called a right J-comodule algebra if there is an R-algebra map $\rho_A : A \to A \otimes J$ satisfying (i) $(I_A \otimes \Delta_J)\rho_A = (\rho_A \otimes I_J)\rho_A$, (ii) $(1 \otimes e)\rho_A = I_A$. If A is an R-algebra, J a Hopf algerbra, then $\mathrm{Hom}_R(J,A)$ becomes an algebra with the convolution product

$$\phi_1 * \phi_2(j) = \sum_{(j)} \phi_1(j_{(1)})\phi_2(j_{(2)}), \quad \forall j \in J, \quad \phi_1, \phi_2 \in \mathrm{Hom}_R(J,A).$$

If A is also a right J-comodule algebra with the structure map $\rho_A : A \to A \otimes J$ as before, $\psi \in \mathrm{Hom}_R(J,A)$ is called an integral if ψ is a right J-comodule map, that is, $\rho_A\psi = (\psi \otimes 1)\Delta_J$, Morefore, if $\psi(1_J) = 1_\Lambda$, ψ is called a total integral. If there is a total integral $\psi \in \mathrm{Hom}_R(J,A)$, which is invertible according to the convolution product given above, A is called left.

Let J be a finite Hopf R-algebra, A an R-algebra with B its subalgebra. Then A/B is called a J-Galois extension if the following conditions are satisfied:

(1) A is a right J-comodule algebra with its structure map:

$$\alpha : \quad A \to A \otimes J.$$

(2) $B = A^{\mathrm{co}J} = \{a \in A | \alpha(a) = a \otimes 1\}$.

(3) The left A-module map β induced by α is an isomorphism:

$$\beta : \quad A \otimes_B A \to A \otimes J, \quad \beta(a \otimes a') = \sum_{(a')} aa'_{(0)} \otimes a'_{(1)}, \quad \forall a, a' \in A.$$

Remark. The condition (3) can be replaced by:

(3') The α-induced right A-module map $\beta' : A \otimes_B A \to A \otimes J$ is an isomorphism, where $\beta'(a \otimes a') = \sum\limits_{(a)} a_{(0)}a' \otimes a_{(1)}, \quad \forall a, a' \in A$.

From [11] we know that when A/B is a J-Galois extension, then besides the right J-comodule algebra structure inheriting from A's, $V_A(B)$ can also be given a left J^*-comodule algebra structure. In the following we will show the structure. First we say that a left J^*-comodule algebra structure is equivalent to a right J-module algebra structure, then we give the left J^*-comodule structure by showing the right J-module action.

If the Hopf algebra J is a finitely generated projective R-module with its dual basis $\{f_k \in \mathrm{Hom}_R(J,R),\ j_k \in J\}_k$, then an R-module M is a J-comodule algebra iff it is a left J^*-module algebra. Set $\rho_M : M \to M \otimes J$ to be the comodule algebra map, denote

$$\rho_M(m) = \sum_{(m)} m_{(0)} \otimes m_{(1)}, \ \forall m \in M.$$

Then its left J^*-module algebra action is defined by

$$j^* \cdot m = \sum_{(m)} m_{(0)} j^*(m_{(1)}), \forall m \in M, \ j^* \in J^*, \ m \in M.$$

Conversely, for a left J^*-module algebra M, the map $\rho_M M \to M \otimes J$, $\rho_M(m) = \sum_{(k)} f_k \cdot m \otimes j_k$, $\forall m \in M$, defines a right J-comodule algebra structure of M.

If A/B is J-Galois, then the left J^*-comodue algebra structure of $V_A(B)$ is induced by the following J-module action: $v \cdot j = \sum\limits_i b_i v b'_i$, where $\beta^{-1}(1 \otimes j) = \sum\limits_i b_i \otimes b'_i$, $\forall j \in J$, $v \in V_A(B)$.

From now on we denote the right J-module action on $V_A(B)$ by v^j, $\forall v \in V_A(B)$, $j \in J$.

Lemma 2.6.[11, Theorem 3.4 (1)] *The proceeding right J-module action is characterized by*

$$v \cdot a = \sum_{(a)} a_{(0)} v^{a_{(1)}}, \quad \forall a \in A, \ v \in V_A(B),$$

$$\lambda(a)=\sum_{(a)} a_{(0)}\otimes a_{(1)}. \tag{2.1}$$

Theorem 2.2. *Let A/B be a J-Galois extension. Then A/B is H-separable iff there exist integrals $\phi_i\in \mathrm{Hom}_R(J^*,V_A(B))$ and $v_i\in V_A(B)$ with $\sum\limits_i \phi_i v_i = 1_{\mathrm{Hom}_R(J^*,V_A(B))}$, $i=1,\cdots,n$. (Recall that $Hom_R(J^*,V_A(B))$ is an algebra).*

Proof. Necessity. Let A's H-separable system be $\big\{\sum\limits_j x_{ij}\otimes y_{ij}\in(A\otimes_B A)^A,\ v_i\in V\big\}_{i=1}^n$. Set $\phi_i=\beta'\big(\sum\limits_j x_{ij}\otimes y_{ij}\big)$. Recall that

$$\beta':\quad A\otimes_B A\to A\otimes J,\ \beta'(a\otimes a')=\sum_{(a)} a_{(0}a'\otimes a_{(1)},$$

β' is an isomorphism. Then

$$\begin{aligned}\phi_i(a\otimes 1)&=\beta'\Big(\sum_j x_{ij}\otimes y_{ij}a\Big)=\beta'\Big(\sum_j ax_{ij}\otimes y_{ij}\Big)\\&=\alpha(a)\beta'\Big(\sum_j x_{ij}\otimes y_{ij}\Big)=\alpha(a)\phi_i,\quad \forall a\in A.\end{aligned} \tag{2.2}$$

$$\sum_{j,(a)} a_{(0)}z_{ij}^{a_{(1)}}\otimes a_{ij}=\sum_{j,(a)} a_{(0)}z_{ij}\otimes a_{(1)}a_{ij}. \tag{2.3}$$

J is a finitely generated projective R-module, so we have

$$V_A(B)\otimes J\cong \mathrm{Hom}_R(J^*,V_A(B)); \tag{2.4}$$

the isomorphism is

$$(v\otimes h)(h^*)=v\cdot h^*(h),\quad \forall v\in V,\quad h\in J,\quad h^*\in J^*.$$

Now we prove that (2.3) is equivalent to that $\phi_i\in V_A(B)\otimes J\cong \mathrm{Hom}_R(J^*,V_A(B))$ are integrals.

$\forall h\in J,\ \beta^{-1}(1\otimes h)=\sum\limits_k b'_k\otimes b_k$. Then from (2.2) and (2.1) we have

$$\begin{aligned}\sum_j z_{ij}^h\otimes a_{ij}&=\sum_j\sum_k b'_k z_{ij}b_k\otimes a_{ij}=\sum_k b'_k\sum_{j,(b_k)} b_{k_{(0)}}z_{ij}^{b_{k_{(1)}}}\otimes a_{ij}\\&=\sum_k b'{}_k\sum_{j,(b_k)} b_{k_{(0)}}z_{ij}\otimes b_{k_{(1)}}a_{ij}=\Big(\sum_{k,(b_k)} b'_k b_{k_{(0)}}\otimes b_{k_{(1)}}\Big)\Big(\sum_j z_{ij}\otimes a_{ij}\Big)\\&=\beta\Big(\sum_k b'_k\otimes b_k\Big)\Big(\sum_j z_{ij}\otimes a_{ij}\Big)=(1\otimes h)\sum_j z_{ij}\otimes a_{ij}=\sum_j z_{ij}\otimes ha_{ij}.\end{aligned}$$

So $\forall h^*\in J^*$, $h\in J$, we have

$$\phi_i(h^*\cdot h)=\sum_j z_{ij}h^*(h\cdot a_{ij})=\sum_j z_{ij}^h h^*(a_{ij})=(\phi_i(h^*))\cdot h, \tag{2.5}$$

that is, ϕ_i are integrals.

Conversely, when ϕ_i are integrals, $\phi_i=\sum\limits_j z_{ij}\otimes a_{ij}$. Then by (2.5) we have $\phi_i(h^*\cdot h)=(\phi_i(h^*))\cdot h,\quad \forall h\in J,\ h^*\in J^*$, so

$$\sum_j z_{ij}^h\otimes a_{ij}=\sum_j z_{ij}\otimes h\cdot a_{ij}.$$

For an element $a \in A$, $\alpha(a) = \sum_{(a)} a_{(0)} \otimes a_{(1)}$,

$$\sum_j z_{ij}^{a_{(1)}} \otimes a_{ij} = \sum_j z_{ij} \otimes a_{(1)} a_{ij}.$$

So we get

$$\sum_{(a),j} a_{(0)} z_{ij}^{a_{(1)}} \otimes a_{ij} = \sum_{(a),j} a_{(0)} z_{ij} \otimes a_{(1)} a_{ij},$$

that is (2.3), the desired equivalence is obtained.

Similarly, by $V_A(B) \otimes J \cong \mathrm{Hom}_R(J^*, V_A(B))$, $1 \otimes 1 \leftrightarrow 1_{\mathrm{Hom}_R(J^*, V_A(B))}$, we have

$$\sum_i \phi_i v_i = 1_{\mathrm{Hom}_R(J^*, V_A(B))} = \beta'(1 \otimes 1) = 1 \otimes 1 \in V_A(B) \otimes J \cong \mathrm{Hom}_R(J^*, V_A(B)).$$

(Note that $\sum_i \phi_i v_i = \sum_i \beta'\big(\sum_j x_{ij} \otimes y_{ij} v_i\big)$.)

Sufficiency. Regarding ϕ_i as elements in $V_A(B) \otimes J$, we denote ${\beta'}^{-1}(\phi_i) = \sum_j x_{ij} \otimes y_{ij}$. ϕ_i are inegrals, so (2.2) and then (2.1) is satisfied. Reversing the sufficiency's proof we get $\sum_j x_{ij} \otimes y_{ij} \in (A \otimes_B A)^A$. Since $V_A(B) \otimes J \cong \mathrm{Hom}(J^*, V_A(B))$ and $1 \otimes 1 \leftrightarrow 1_{\mathrm{Hom}(J^*, V_A(B))}$, we have

$$\begin{aligned} \sum_i \phi_i v_i = 1_{\mathrm{Hom}(J^*, V_A(B))} &\Leftrightarrow \sum_i \phi_i v_i = 1 \otimes 1 \in V_A(B) \otimes J \\ &\Leftrightarrow \sum_{i,j} \sum_{(x_{ij})} x_{ij(0)} y_{ij} v_i \otimes x_{ij(1)} = 1 \otimes 1 = \beta'\Big(\sum_{i,j} x_{ij} \otimes y_{ij} v_i\Big) \\ &\Leftrightarrow \sum_{i,j} v_i x_{ij} \otimes y_{ij} = \sum_{i,j} x_{ij} \otimes y_{ij} v_i = 1 \otimes 1. \end{aligned}$$

This shows that $\big\{\sum_j x_{ij} \otimes y_{ij} \in (A \otimes_B A)^A,\ v_i \in V_A(B)\big\}_i$ is an H-separable system of A/B, the sufficiency is proved.

Corollary 2.1. *Let J be a finite Hopf algebra, A/B a J-Galois extension. If A/B is also H-separable, then there is a total integral $\phi \in \mathrm{Hom}(J^*, V_A(B))$.*

Proof. From Lemma 2.2 we know that if A/B is H-separable with its H-separable system $\big\{\sum_j x_{ij} \otimes y_{ij} \in (A \otimes_B A)^A,\ v_i \in V_A(B)\big\}_i$, p is the projection $V_A(B) \to C$, then $\{p(v_i)x_{ij}, y_{ij}\}_{i,j}$ is a separable system. Here C is $C(A)$, the center of A. Then Theorem 2.2 shows that there exist integrals $\phi_i \in \mathrm{Hom}(J^*, V_A(B))$, so

$$\sum_i p(v_i)\phi_i \in \mathrm{Hom}(J^*, V_A(B)), \quad \forall j^* \in J^*.$$

$$\sum_i p(v_i)\phi_i(j^*) = \sum_i p(v_i) z_{ij} j^*(a_{ij}) = \sum_{i,j,(x_{ij})} p(v_i) x_{ij(0)} y_{ij} j^*(x_{ij(1)}).$$

When $j^* = 1_{J^*} = \epsilon$ (the counit of J), we have

$$\sum_i p(v_i) x_{ij(0)} y_{ij} \epsilon(x_{ij(1)}) = \sum_i p(v_i) x_{ij} y_{ij} = 1 \in V_A(B).$$

Also ϕ_i are integrals, and so is $\sum_i p(v_i)\phi_i$; that is, therte exists a total integral $\phi = \sum_i p(v_i)\phi_i$ in $\mathrm{Hom}(J^*, V_A(B))$.

§3. H-Separable Ring's Hopf-Galois Extension

In this section, we discuss the Hopf-Galois extension of H-separable rings. First we need the following lemma.

Lemma 3.1.[12, Lemma 2.8] *Let A/B be a J-Galois extension. Then $V_A(B)$ is a J-Galois extension over $V_B(B)$ iff $V_A(B)$ is finiely generated $V_B(B)$-projective, and A is isomorphic to $B \otimes_C V_A(B)$ as a $V_B(B)$-algebra.*

Applying Theorem 2.1 we obtain the main theorem in the section.

Theorem 3.1. *Let A/B be H-separable, $C(A) = C(B)$, ${}_BB_B < \oplus_B A_B$, and B be C-flat. Then the following are equivalent:*

(1) *A/B is J-Galois.*

(2) *$V_A(B)/C$ is J-Galois with a total integral $\phi \in \mathrm{Hom}(J^*, V_A(B))$.*

(3) *$V_A(B)/C$ is J-Galois and C-Azumaya.*

Proof. (2) $\Leftrightarrow$ (3) By [11, Theorem 3.14], $V_A(B)/C$ is J-Galois. Then $V_A(B)/C$ is separable iff there exists a total integral $\phi \in \mathrm{Hom}(J^*, V_A(B))$. But by ${}_BB_B < \oplus_B A_B$, we know that the center of $V_A(B)$ is C. Then the equivalence is easy to see.

(1) $\Rightarrow$ (2) Since the condition in Theorem 2.1 is satisfied, we have $A \cong B \otimes_C V_A(B)$, $V_A(B)$ is C-Azumaya and of ocurse finitely generated projective as C-module. So by Lemma 3.1, $V_A(B)/C$ is J-Galois and there is a total integral $\phi \in \mathrm{Hom}(J^*, V_A(B))$ (see Corollary 2.1).

(2) $\Rightarrow$ (1) By Theorem 2.1 we have $A = B \otimes_C V_A(B)$. It is easy to see the J-comodule algebra structure map of $V_A(B)\rho_{V_A(B)} : V_A(B) \to V_A(B) \otimes J$ induces that of A:

$$\rho_A = 1 \otimes \rho_{V_A(B)} : B \otimes_C V_A(B) \to B \otimes_C V_A(B) \otimes J,$$

i.e., ρ satisfies

(i) $(I_A \otimes \Delta_J)\rho_A = (\rho_A \otimes I_J)\rho_A$,

(ii) $(1 \otimes \epsilon)\rho_A = I_A$.

Now we prove the structure defined this way makes A a J-Galois extension of B. First recall that $V_A(B)/C$ is J-Galois means the following conditions are satisfied:

$$0 \to C \to V_A(B) \xrightarrow{\rho_{V_A(B)} - i_{V_A(B)}} V_A(B) \otimes J \tag{3.1}$$

is exact, where $i_{V_A(B)}(v) = v \otimes 1, \quad \forall v \in V_A(B)$.

$$\beta_{V_A(B)} : \ V_A(B) \otimes_C V_A(B) \to V_A(B) \otimes J \tag{3.2}$$

is an isomorphism, where

$$\beta_{V_A(B)}(v \otimes v') = \sum_{(v')} vv'_{(0)} \otimes v'_{(1)}, \ \forall v, v' \in V,$$

$$\rho_{V_A(B)}(V') = \sum_{(v')} v'_{(0)} \otimes v'_{(1)}.$$

By the hypothesis, B is C-flat. So we get an exact sequence

(i')

$$0 \to B \otimes_C \to B \otimes_C V_A(B) \xrightarrow{I_B \otimes \rho_{V_A(B)} - I_B \otimes i_{V_A(B)}} B \otimes_C V_A(B) \otimes J \to 0,$$

that is,

$$0 \to B \to A \overset{\rho_A - i_A}{\longrightarrow} A \otimes J$$

is exaxt, where $i_A(a) = a \otimes 1, \quad \forall a \in A$.

So $B = A^{\mathrm{co}J} = \{a \in A | \rho_A(a) = a \otimes 1\}$, and by (3.2) we have

(ii') the following diagram is commutative:

$$\begin{tikzcd} A \otimes_B A \arrow[r, equal] & B \otimes_C V_A(B) \otimes_B B \otimes_C V_A(B) \arrow[r, "\beta_A"] \arrow[d, "t"] & B \otimes_C V_A(B) \otimes J \arrow[d, "1\otimes\beta_{V_A(B)}"] \\ & B \otimes_C V_A(B) \otimes_C V_A(B) \arrow[r, equal] & B \otimes_C V_A(B) \otimes_C V_A(B) \end{tikzcd}$$

where

$$\beta_A(a \otimes a') = \sum_{(a')} aa'_{(0)} \otimes a'_{(1)}, \ \forall a, a' \in A = B \otimes_C V_A(B),$$

$$t[(b \otimes_C v) \otimes_B (b' \otimes_C v')] = bb' \otimes_C v \otimes_C v',$$

which is an isomorphism.

By the assumption $\beta_{A(B)}$ is an isomorphism, and so is $1 \otimes \beta_{V_A(B)}$. Hence, β_A is also an isomorphism. With (i') and (ii') we have shown that $A = B \otimes_C V_A(B)$ is a J-Galois extension over B. This completes the proof.

Let R be a commutative ring, A an R-algebra. Suppose A is a right J-comodule algebra with its structure map ρ_A and $B = A^{\mathrm{co}J} = \{a \in A | \rho_A(a) = a \otimes 1\}$. We say A has the normal basis property, if there exists a left B-module, right J-comodule isomorphism from $B \otimes J$ to A. It is easy to see from Theorem 3.1 that

Corollary 3.1. *If the equivalent condition in Theorem* 3.1 *is satisfied, then A has the normal basis property if and only if $V_A(B)$ has the property too.*

Proof. ($\Leftarrow$) $V_A(B) \cong C \otimes J$, so $A \cong B \otimes J$ as left B-module, right J-comodule.

($\Rightarrow$) $A \cong B \otimes J$, so $V_A(B) \cong (B \otimes J)^B = C \otimes J$, which is C-module isomorphic, and $B = A^{\mathrm{co}J}$. So $(A)^B \cong (B \otimes J)^B$ is still a J-comodule isomorphism, that is, $V_A(B) \cong C \otimes J$ as C-module, right J-comodule.

References

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

[2] Chase, S. U. & Sweedler, M. E., Hopf algebras and Galois theory, Lecture Notes in Mathematics, Vol. 97, Springer-Verlag, Berlin, 1969.

[3] Ikehata, S., Note on Azumaya algebra and H-separable extensions, *Math. J. Okayama Univ.,* **23** (1981), 17–18.

[4] Ikehata, S., Azumaya algebras and skew polynomial rings, *Math. J. Okayama Univ.,* **23** (1981), 19–32.

[5] Nakamoto, T., On QF-extensions in an H-separable extensions, *Proc. Japan Acad.,* **50** (1974), 440–443.

[6] Okamoto, H., On projective H-separable extensions of Azumaya algebras, *Results in Math.,* **141** (1988), 330–332.

[7] Nakajima, A., On Hopf-Galois extensions, Azumaya algebras and skew polynomial rings, *Math. J. Okayama Univ.,* **29** (1987), 109–117.

[8] DeMeyer, F. R. & Ingraham, E., Separable algebars over commutative rings, Lecture Notes Math., Vol. 181, Springer-Verlag, Berlin, 1971.

[9] Nakamoto, T. & Sugano, K., Notes on H-separable extensions, *Hokkaido Math. J.,* **4:**2(1975), 295–299.

[10] Auslander, M. & Goldman, O., Maximal orders, *Trans. Amer. Math. Soc.,* **97** (1960), 1–24.

[11] Doi, Y. & Takeuchi, M., Hopf-Galois extensions of algebras, the Miyashita-Ulbrich action and Azumaya algebras, *J. Alg.,* **2** (1989), 488–516.

[12] Kreimer, H. F. & Takeuchi, M., Hopf algebars and Galois extensions of an algebra, *Indiana Univ. Math. J.,* **30:** 5(1981), 675–692.