Chin. Ann. Math.
38B(4), 2017, 999–1018
DOI: 10.1007/s11401-017-1108-3

Chinese Annals of Mathematics, Series B

On Hopf Galois Extension of Separable Algebras*

Yu LU[1] Shenglin ZHU[1]

Abstract In this paper, the classical Galois theory to the H^*-Galois case is developed. Let H be a semisimple and cosemisimple Hopf algebra over a field k, A a left H-module algebra, and A/A^H a right H^*-Galois extension. The authors prove that, if A^H is a separable k-algebra, then for any right coideal subalgebra B of H, the B-invariants $A^B = \{a \in A \mid b \cdot a = \varepsilon(b)a, \ \forall b \in B\}$ is a separable k-algebra. They also establish a Galois connection between right coideal subalgebras of H and separable subalgebras of A containing A^H as in the classical case. The results are applied to the case $H = (kG)^*$ for a finite group G to get a Galois 1-1 correspondence.

Keywords Semisimple Hopf algebra, Hopf Galois extension, Separable algebra, Galois connection
2000 MR Subject Classification 17B40, 17B50

1 Introduction

The theory of classical Galois field extension, which establishes a 1-1 correspondence between intermediate fields and subgroups of the Galois group, is one of the most important results in algebraic theory. From the classical Galois field extension theory, we know that a classical Galois field extension must be all the time a separable field extension. A separable k-algebra, which is an associated k-algebra over the base field k, may be seen as a natural generalization for the notion of separable field extension.

Let $B \subset A$ be commutative rings, G a finite group satisfying $B = A^G$. The theory of Galois extension for commutative rings was first introduced by Auslander and Goldman [1] in 1960, then it was generalized to the noncommutative case by Tekuo Kanzaki [11] in 1965. In 1969, Chase and Sweedler [3] presented a generalization of the fundamental theorem of Galois theory for commutative rings to the case of cocommutative Hopf Galois extension. Then in 1980, Kreimer and Takeuchi [10] gave a generalized definition for Hopf Galois extension. In 2010, Wang and Zhu [18] defined the notion $N = \{h \in H \mid \sum h_{(1)} \cdot \lambda \otimes h_{(2)} = \lambda \otimes h\}$ to construct a right coideal subalgebra of H, where $k\lambda$ is a 1-dimensional ideal of an H-module algebra A.

Let H be a semisimple and cosemisimple Hopf algebra over a field k, A a left H-module algebra. Assume that A/A^H is H^*-Galois, Cohen and Fishman proved in [5, Theorem 1.19] that for any Hopf subalgebra $H' \subset H$, $A^{H'}/A^H$ is a separable extension. In particular, A/A^H is a separable extension. Let $H = kG$ and A/A^H be a G-Galois field extension. Then the results imply that a classical Galois field extension must be all the time a separable field

Manuscript received April 6, 2016. Revised August 17, 2016.
[1]School of Mathematical Sciences, Fudan University, Shanghai 200433, China.
E-mail: 10110180004@fudan.edu.cn mazhusl@fudan.edu.cn
*This work was supported by the National Natural Science Foundation of China (No. 11331006).

extension. Notice that in classical G-Galois field extension, there is a 1-1 correspondence between intermediate fields and subgroups of the Galois group G.

Now for the H^*-Galois case, it is natural to ask whether the B-invariants $A^B = \{a \in A \mid ba = \epsilon(b)a,\ \forall b \in B\}$ is separable over A^H, for any right coideal subalgebra B of H, and especially, when A is a field, whether there exists a 1-1 correspondence between intermediate fields and right coideal subalgebras of H. The above two problems have a positive answer in the case of $H = kG$, where G is a finite group (see [11]). But this situation is very special.

In this paper, we prove that, for any right coideal subalgebra B of H, A^B is a separable k-algebra, and thus A^B is separable over A^H. Then we establish a Galois connection between right coideal subalgebras of H and separable subalgebras of A containing A^H as in the classical sense. Moreover, we difine the Galois connection maps ψ and ϕ defined by $\psi(\Omega) = \{h \in H \mid \sum h_{(1)} \cdot \omega \otimes h_{(2)} = \omega \otimes h,\ \forall \omega \in \Omega\}$ and $\phi(B) = A^B = \{a \in A \mid b \cdot a = \varepsilon(b)a,\ \forall b \in B\}$ respectively, and prove that $\psi \circ \phi(B) = B$ for any right coideal subalgebra B of H. In particular, if $H = (kG)^*$ and $C(A)$ is an integral domain, we prove that the Galois connection is just a 1-1 correspondence.

We arrange this paper as follows. In Section 2, we recall the concepts related to Hopf-Galois extension and separable algebras. In Section 3, we first discuss the separability of A^B for an arbitrary right coideal subalgebra B of H. Then we calculate the commutor ring of $C(A)$ in $A\#H$, which will be frequently used in the following calculating of commutor rings. Next, we establish the Galois connection between the coideal subalgebras of H and intermediate separable algebras between A and A^H, and prove the Galois connection theorem (i.e., Theorem 3.2). Finally, the particular case of $H = (kG)^*$ is considered, and we prove that the Galois connection we establish in Theorem 3.2 is just a 1-1 correspondence in this case.

Throughout this paper, k will be a field; all algebras and Hopf algebras are over k, unless otherwise specified; H is a Hopf algebra with multiplication μ, unit u, comultiplication Δ, counit ε, and antipode S.

2 Preliminaries

In this section, we recall definitions of Hopf Galois extension, separable algebras and Galois connection. Let H be a Hopf algebra over k. A left H-module algebra A is an associated algebra with a left H-action, that is,

$$h \cdot 1_A = \varepsilon(h)1_A \quad \text{and} \quad h \cdot (ab) = \sum (h_{(1)} \cdot a)(h_{(2)} \cdot b)$$

for any $h \in H$ and $a, b \in A$.

Dually, a right H-comodule algebra A is an associated algebra with a right H-coaction, that is,

$$\rho(1_A) = 1_A \otimes 1_H \quad \text{and} \quad \rho(ab) = \sum a_{\langle 0\rangle} b_{\langle 0\rangle} \otimes a_{\langle 1\rangle} b_{\langle 1\rangle}$$

for any $a, b \in A$, where $\rho(a) = \sum a_{\langle 0\rangle} \otimes a_{\langle 1\rangle} \in A \otimes H$ is the comodule structure map.

Moreover, we get the H-invariants $A^H = \{a \in A \mid h \cdot a = \varepsilon(h)a,\ \forall h \in H\}$ for a left H-module algebra A. Similarly, we get the H-coinvariants $A^{\mathrm{co}H} = \{a \in A \mid \rho(a) = a \otimes 1_H\}$ for a right H-comodule algebra A.

A subalgebra B of H is called a right coideal subalgebra, if B is also a right coideal of H, i.e., $\Delta(B) \subset B \otimes H$. Similarly, a subalgebra B of H is called a left coideal subalgebra, if B is also a left coideal of H, i.e., $\Delta(B) \subset H \otimes B$.

Assume that H is a finite-dimensional Hopf algebra. By [14] we know that the antipode of H is of finite order. Hence H^{cop} (or H^{op}) is a Hopf algebra with antipode S^{-1}, and H^* is a Hopf algebra with antipode S^*. Furthermore, we have ${}_H\mathcal{M} = \mathcal{M}^{H^*}$, where ${}_H\mathcal{M}$ denotes the category of left H-module, and $\mathcal{M}^{H^*}$ denotes the category of right H^*-comodule.

Now, we recall the definition of Hopf Galois extension in terms of coaction.

Definition 2.1 (see [13, 8.1.1]) *Let H be a Hopf algebra, and A a right H-comodule algebra with structure map $\rho : A \to A \otimes H$. Then the extension $A^{\mathrm{co}H} \subset A$ is right H-Galois if the Galois map*

$$\beta : A \otimes_{A^{\mathrm{co}H}} A \to A \otimes_k H,$$
$$a \otimes b \mapsto \sum ab_{\langle 0 \rangle} \otimes b_{\langle 1 \rangle}$$

is bijective.

Let R be a commutative ring. We recall the definitions of separable R-algebra and central separable R-algebra.

Definition 2.2 (see [7]) *Let A be an algebra over R. A is called a separable R-algebra, if it satisfies any of the following equivalent conditions:*

(1) *A is a projective left $A^{\mathrm{e}} = A \otimes_R A^{\mathrm{op}}$-module.*

(2) *There exists an element $e = \sum e^{(1)} \otimes e^{(2)} \in A \otimes_R A$, such that*

$$\sum e^{(1)} e^{(2)} = 1_A \quad \textit{and} \quad ae = ea \tag{2.1}$$

for any $a \in A$. Such e is called a separable idempotent.

In particular, if $R = k$ is a field, we have another equivalent definition:

(3) *For any field extension $k \subset L$, $A \otimes_k L$ is a semisimple algebra.*

Definition 2.3 (see [7]) *Let A be a separable algebra over a commutative ring R. A is said to be a central separable R-algebra, if R is the center of A, i.e., $R = \{a \in A \mid ab = ba,\ \forall b \in A\}$.*

Next, we recall the definition of separable extension.

Definition 2.4 (see [8, Definition 2]) *Let A be an R-algebra, $B \subset A$ a subring. A is said to be a separable extension over B, if there exists a separable idempotent element $e = \sum e^{(1)} \otimes e^{(2)} \in A \otimes_B A$, such that*

$$\sum e^{(1)} e^{(2)} = 1_A \quad \textit{and} \quad ae = ea \tag{2.2}$$

for any $a \in A$.

Remark 2.1 From Definitions 2.2 and 2.4, we see that the two notions "A is a separable R-algebra" and "A is a separable extension over R" have the same meaning.

Now, we recall an important property of separable extension, which will be used in Section 3.

Lemma 2.1 (see [8, Proposition 2.5]) *Let A be a ring. B and C are subrings of A such that $B \supset C$. If A is a separable extension of C, then A is a separable extension of B.*

Finally, we recall the definition of Galois connection.

Definition 2.5 (see [6]) *Let $(P, \preceq)$ and $(Q, \preceq)$ be two partially ordered sets. Then a pair of antitone morphisms of posets, $\phi : P \to Q$ and $\psi : Q \to P$, is said to establish a Galois connection if*

$$p \preceq \psi \circ \phi(p),\ \forall p \in P \quad \text{and} \quad q \preceq \phi \circ \psi(q),\ \forall q \in Q.$$

3 Main Results

Let H be a semisimple and cosemisimple Hopf algebra, A a left H-module algebra. Assume that A/A^H is a right H^*-Galois extension, and A^H is a separable algebra over k. We prove in Theorem 3.1: For any right coideal subalgebra $B \subset H$, the B-invariants $A^B = \{a \in A \mid b \cdot a = \varepsilon(b)a,\ \forall b \in B\}$ is a separable algebra over k.

Then under the same conditions, we establish a Galois connection between right coideal subalgebras of H and separable subalgebras of A containing A^H as in the classical case (see Theorem 3.2). Moreover, given the Galois connection maps ψ and ϕ defined by $\psi(\Omega) = \{h \in H \mid \sum h_{(1)} \cdot \omega \otimes h_{(2)} = \omega \otimes h,\ \forall \omega \in \Omega\}$ and $\phi(B) = A^B = \{a \in A \mid b \cdot a = \varepsilon(b)a,\ \forall b \in B\}$ respectively, we prove that $\psi \circ \phi(B) = B$ for a right coideal subalgebra B of H. In particular, if $H = (kG)^*$ and $C(A)$ is an integral domain, we prove that the Galois connection is just a 1-1 correspondence.

We recall several lemmas below, which will be needed in the proof of our main results.

Lemma 3.1 (see [10, Theorem 1]) *Let R be a commutative ring, M a faithful A-module, and set $B = \mathrm{End}_A(M)$. If A is a separable R-algebra and M is a finitely generated projective A-module, then we have that B is also a separable R-algebra, M is a finitely generated projective B-module and $\mathrm{End}_B(M) = A$. If A is central over R, then B is also central over R.*

Lemma 3.2 (see [10, Theorem 2]) *Let R be a commutative ring, A a central separable R-algebra. If B is an arbitrary separable R-subalgebra of A, then $C_A(B)$ is a separable k-algebra and we have $C_A(C_A(B)) = B$.*

Lemma 3.3 (see [9, Theorem 1.7]) *Let H be a finite-dimensional Hopf algebra over a field k and A a left H-module algebra. If A/A^H is a right H^*-Galois extension, then*

(1) *the map $\pi : A\#H \to \mathrm{End}(A_{A^H})$, given by $\pi(a\#h)(b) = a(h \cdot b)$, is an algebra isomorphism, and*

(2) *A is a finitely-generated projective right A^H-module.*

We give some propositions below, which play an important role in the proof of our main results.

Proposition 3.1 *Let H be a finite-dimensional Hopf algebra over a field k, A a left H-module algebra. If A/A^H is a right H^*-Galois extension, then for an arbitrary left coideal subalgebra $B \subset H$, the map $\pi : A\#B \to \mathrm{End}(A_{A^B})$, given by $\pi(a\#b)(c) = a(b \cdot c)$, is an algebra isomorphism.*

Proof First, we verify that π is well-defined. For any $a, c \in A$, $d \in A^B$ and $b \in B$, notice that $\Delta(b) = \sum b_{(1)} \otimes b_{(2)} \subset H \otimes B$. Then we have

$$\begin{aligned}\pi(a\#b)(cd) = a(b\cdot(cd)) &= \sum a(b_{(1)}\cdot c)(b_{(2)}\cdot d)\\ &= \sum a(b_{(1)}\cdot c)(\varepsilon(b_{(2)})d) = a(b\cdot c)d\\ &= \pi(a\#b)(c)d.\end{aligned}$$

Next we construct the inverse map for π. Notice that

$$\begin{aligned}\beta' : A \otimes_{A^H} A &\to A \otimes_k H^*,\\ x\otimes y &\mapsto \sum x_{\langle 0\rangle} y \otimes x_{\langle 1\rangle}\end{aligned}$$

is also a bijective map as the Galois map β. This is because we have $\beta' = \phi\circ\beta$, where $\phi \in \mathrm{End}_k(A\otimes_k H^*)$, given by $\phi(a\otimes h^*) = \sum a_{\langle 0\rangle}\otimes a_{\langle 1\rangle} S^* h^*$, is an isomorphism. Then since $B \subset H$ is a left coideal subalgebra, we have that B^* is a left H^*-module quotient coalgebra of H^*, i.e., $B^* = H^*/I$ for some left ideal coideal $I \subset H^*$. Notice that A is a right H^*-comodule algebra, therefore it induces a natural right B^*-comodule structure on A via $(\mathrm{id}\otimes p)\circ\rho$, where $p : H^* \to B^*$ is the natural projection. Now we define

$$\begin{aligned}\beta'_0 : A \otimes_{A^B} A &\to A \otimes_k B^*,\\ x\otimes y &\mapsto \sum x_{\langle 0\rangle} y \otimes \overline{x_{\langle 1\rangle}}\ .\end{aligned}$$

It is straightforward to verify that β'_0 is well-defined. This is because, for any $x, y \in A$ and $z \in A^B = A^{\mathrm{co}B^*}$, we have $\sum z_{\langle 0\rangle}\otimes\overline{z_{\langle 1\rangle}} = z\otimes\overline{1}$. Then noticing that B^* is a left H^*-module quotient coalgebra, we get

$$\begin{aligned}\beta'_0(xz\otimes y) &= \sum x_{\langle 0\rangle} z_{\langle 0\rangle} y \otimes \overline{x_{\langle 1\rangle} z_{\langle 1\rangle}} = \sum x_{\langle 0\rangle} z_{\langle 0\rangle} y \otimes x_{\langle 1\rangle}\overline{z_{\langle 1\rangle}}\\ &= \sum x_{\langle 0\rangle} z y \otimes x_{\langle 1\rangle}\overline{1} = \sum x_{\langle 0\rangle} z y \otimes \overline{x_{\langle 1\rangle}}\\ &= \beta'_0(x\otimes zy).\end{aligned}$$

β'_0 is clearly a surjection as β' and $\mathrm{id}\otimes p$ are surjective. Noticing that $B^{\mathrm{cop}} \subset H^{\mathrm{cop}}$ is a right coideal subalgebra, we have that $(B^*)^{\mathrm{op}} = (B^{\mathrm{cop}})^*$ is a right $(H^*)^{\mathrm{op}}(= (H^{\mathrm{cop}})^*)$-module quotient coalgebra of $(H^*)^{\mathrm{op}}$. Now consider the map

$$\begin{aligned}\beta_0 : A^{\mathrm{op}} \otimes_{A^{\mathrm{op}\,B^{\mathrm{cop}}}} A^{\mathrm{op}} &\to A^{\mathrm{op}} \otimes_k (B^*)^{\mathrm{op}},\\ y\otimes x &\mapsto \sum y\circ x_{\langle 0\rangle}\otimes\overline{x_{\langle 1\rangle}} = \sum x_{\langle 0\rangle} y \otimes \overline{x_{\langle 1\rangle}},\end{aligned}$$

which identifies with β'_0. Hence β_0 is also a surjection as β'_0, then by [15, Corollary 3.3], we have that β_0 is a bijection. It follows that β'_0 is a bijection.

Now we denote

$$\beta_0'^{-1}(1\otimes b^*) = \sum b^{*[1]}\otimes b^{*[2]} \in A\otimes_{A^B} A.$$

Then we define

$$\begin{aligned}\theta : \mathrm{End}(A_{A^B}) &\to A\#B,\\ \psi &\mapsto \sum_{i=1}^{n}\sum \psi(b_i^{*[1]})b_i^{*[2]}\#b_i,\end{aligned}$$

where $n = \dim B$, $\{b_i\}_{i=1}^n$ is a basis of B, and $\{b_i^*\}_{i=1}^n$ is the dual basis for $\{b_i\}_{i=1}^n$ in B^*. Notice that ψ is a right A^B-module map. Then it is obvious to see that θ is well-defined. Now we verify that θ is just the inverse map for π.

(1) We verify that $\theta \circ \pi = \mathrm{id}_{A\#B}$. Noticing that $\beta' \circ \beta'^{-1} = \mathrm{id}_{A\otimes B^*}$, we have

$$\begin{aligned} 1_A \otimes b^* &= (\beta' \circ \beta'^{-1})(1_A \otimes b^*) \\ &= \beta'\Big(\sum b^{*[1]} \otimes b^{*[2]}\Big) \\ &= \sum (b^{*[1]})_{\langle 0\rangle} b^{*[2]} \otimes (b^{*[1]})_{\langle 1\rangle} \end{aligned} \tag{3.1}$$

for any $b^* \in B^*$. So we get

$$\begin{aligned} (\theta \circ \pi)(a\#b) &= \theta(\pi(a\#b)) \\ &= \sum_{i=1}^n \sum \pi(a\#b)(b_i^{*[1]}) b_i^{*[2]} \# h_i \\ &= \sum_{i=1}^n \sum a(b \cdot b_i^{*[1]}) b_i^{*[2]} \# b_i \\ &= \sum_{i=1}^n \sum a\langle b, (b_i^{*[1]})_{\langle 1\rangle}\rangle (b_i^{*[1]})_{\langle 0\rangle} b_i^{*[2]} \# b_i \\ &\overset{\text{by (3.1)}}{=} \sum_{i=1}^n a\langle b, b_i^*\rangle 1_A \# b_i \\ &= \sum_{i=1}^n a\#\langle b, b_i^*\rangle b_i \\ &= a\#b \end{aligned}$$

for any $a \in A$, $b \in B$.

(2) We verify that $\pi \circ \theta = \mathrm{id}_{\mathrm{End}(A_{A^B})}$. Notice that

$$\begin{aligned} \beta'\Big(\sum_{i=1}^n \sum b_i^{*[1]} \otimes b_i^{*[2]}(b_i \cdot x)\Big) &= \sum_{i=1}^n \sum (b_i^{*[1]})_{\langle 0\rangle} b_i^{*[2]}(b_i \cdot x) \otimes (b_i^{*[1]})_{\langle 1\rangle} \\ &\overset{\text{by (3.1)}}{=} \sum_{i=1}^n 1_A(b_i \cdot x) \otimes b_i^* \\ &= \sum_{i=1}^n \sum x_{\langle 0\rangle} \otimes \langle b_i, x_{\langle 1\rangle}\rangle b_i^* \\ &= \sum x_{\langle 0\rangle} \otimes x_{\langle 1\rangle} \\ &= \beta'(x \otimes 1_A) \end{aligned}$$

for any $x \in A$. Noticing that β' is a bijective map, we have

$$\sum_{i=1}^n \sum b_i^{*[1]} \otimes b_i^{*[2]}(b_i \cdot x) = x \otimes 1_A. \tag{3.2}$$

So we get

$$\begin{aligned}(\pi\circ\theta)(\psi)(x) &= \pi(\theta(\psi))(x)\\ &= \pi\Big(\sum_{i=1}^{n}\sum \psi(b_i^{*[1]})b_i^{*[2]}\#b_i\Big)(x)\\ &= \sum_{i=1}^{n}\sum \psi(b_i^{*[1]})b_i^{*[2]}(b_i\cdot x)\\ &\overset{\text{by (3.2)}}{=} \psi(x)1_A\\ &= \psi(x)\end{aligned}$$

for any $x \in A$.

It is straightforward to verify that π is an algebra map, so we have the conclusion.

Remark 3.1 Let $B = H$. Through Proposition 3.1, we give a new proof for the first conclusion of Lemma 3.3.

Proposition 3.2 *Let H be a semisimple and cosemisimple Hopf algebra over a field k, B a left coideal subalgebra of H. Then H has a decomposition: $H = B \oplus C$ in category ${}_B\mathcal{M}_{B\#H^*}$. In particular, B is a direct summand of H both as B-B bimodule and right B-left H relative Hopf module.*

Proof First, notice that a semisimple Hopf algebra (with 1-dimensional integral) is actually a finite-dimensional algebra by Sweedler [17, Corollary 2.7]: If a Hopf algebra contains a non-zero finite-dimensional right ideal, then the Hopf algebra is finite-dimensional. Hence by [16, Theorem 6.1], any left coideal subalgebra $B \subset H$ must be a Frobenius algebra. Then due to [12, Theorem 2.1], we get that B is a separable k-algebra. Since H is a finite-dimensional semisimple and cosemisimple Hopf algebra, we get that H^* is also a semisimple and cosemisimple Hopf algebra. Now we can prove that $B\#H^*$ is a separable k-algebra.

For a field extension $k \subset L$, we set $H' = H \otimes_k L$, $B' = B \otimes_k k$, and ${H'}^* = \mathrm{Hom}_L(H', L)$. Then B' is still a left coideal subalgebra of H'. Noticing

$${H'}^* = \mathrm{Hom}_L(H \otimes_k L, L) \cong \mathrm{Hom}_k(H, \mathrm{Hom}_L(L, L)) \cong \mathrm{Hom}_k(H, L) \cong H^* \otimes_k L,$$

we have that

$$B\#H^* \otimes_k L \cong B \otimes_k k\#H^* \otimes_k L \cong B'\#{H'}^*$$

is a semisimple algebra over L by [2, Theorem 4]. It follows that $B\#H^*$ is a separable k-algebra.

Moreover, $B \otimes_k (B\#H^*)^{\mathrm{op}}$ is a separable k-algebra, as B and $(B\#H^*)^{\mathrm{op}}$ are separable k-algebras. To show this, we denote the separable idempotent elements in $B \otimes_k B$ and $(B\#H^*)^{\mathrm{op}} \otimes_k (B\#H^*)^{\mathrm{op}}$ by $e = \sum e^{(1)} \otimes e^{(2)}$ and $e' = \sum {e'}^{(1)} \otimes {e'}^{(2)}$ respectively. Then we have that

$$e'' = \sum (e^{(1)} \otimes {e'}^{(1)}) \otimes (e^{(2)} \otimes {e'}^{(2)}) \in (B \otimes_k (B\#H^*)^{\mathrm{op}}) \otimes_k (B \otimes_k (B\#H^*)^{\mathrm{op}})$$

is a separable idempotent element for $B \otimes_k (B\#H^*)^{\mathrm{op}}$ over k.

It follows that $B \otimes_k (B\#H^*)^{\text{op}}$ is a semisimple algebra over k, therefore B is a direct summand of H as left $B \otimes_k (B\#H^*)^{\text{op}}$-module, as all modules in ${}_{B\otimes(B\#H^*)^{\text{op}}}\mathcal{M} \cong_B \mathcal{M}_{B\#H^*}$ are projective. Notice that for a finite-dimensional Hopf algebra H, we have $\mathcal{M}_{B\#H^*} = {}^H\mathcal{M}_B$. Consequently, we get that B is a direct summand of H as both B-B bimodule and right B-left H relative Hopf module.

Now, we get to prove our first theorem. From this theorem, we have that $A\#H$ is a separable k-algebra, and A^B is a separable k-algebra for any coideal subalgebra B of H. These two conclusions will be frequently used in our following propositions and theorems.

Theorem 3.1 *Let k be a field, H a semisimple and cosemisimple Hopf algebra over k, A a left H-module algebra, and A/A^H a right H^*-Galois extension. If A^H is a separable algebra over k, then for an arbitrary right coideal subalgebra $B \subset H$, the B-invariants $A^B = \{a \in A \mid ba = \varepsilon(b)a,\ \forall b \in B\}$ is also a separable algebra over k. In particular, $A = A^{k1_H}$ is a separable k-algebra.*

Proof First step, we prove that $A\#H$ is a separable k-algebra. Noticing that A/A^H is a right H^*-Galois extension, from Lemma 3.3, we have that $A\#H \cong \text{End}(A_{A^H})$ and A is a finitely-generated projective right A^H-module. Then using Lemma 3.1, we get that $A\#H \cong \text{End}(A_{A^H})$ is a separable k-algebra.

Second step, we prove that $A\#B$ is a separable k-subalgebra of $A\#H$ for $B \subset H$ a left coideal subalgebra. Notice that the dimension of a semisimple Hopf algebra is actually finite. Then by [16, Theorem 6.1], we have that B is a Frobenius coideal subalgebra of H, and hence H is free over B by [12, Theorem 2.1]. Therefore we have $H = \bigoplus_{i=1}^{s} Br_i$ and $H = \bigoplus_{i=1}^{s} r_i'B$, where $\{r_i\}_{i=1}^s$ and $\{r_i'\}_{i=1}^s$ are left and right B-module basis for H respectively.

On one hand, we have

$$A\#H = \bigoplus_{i=1}^{s}(A\#B)r_i; \tag{3.3}$$

on the other hand, consider

$$\begin{aligned}\varphi : A \otimes H &\to A\#H,\\ a \otimes h &\mapsto ha = \sum h_{(1)} \cdot a\#h_{(2)},\end{aligned}$$

which is a left H-module isomorphism, and its inverse is

$$\begin{aligned}\varphi^{-1} : A\#H &\to A \otimes H,\\ a\#h &\mapsto \sum (S^{-1}h_{(1)}) \cdot a \otimes h_{(2)}.\end{aligned}$$

It is straightforward to verify that $\varphi(A \otimes B) = A\#B$, as for $a \in A$, $b \in B$, we have $\Delta(b) = \sum b_{(1)} \otimes b_{(2)} \in H \otimes B$, and then

$$\begin{aligned}\varphi(a \otimes b) &= \sum b_{(1)} \cdot a\#b_{(2)} \in H \cdot A\#B \subset A\#B,\\ \varphi^{-1}(a\#b) &= \sum (S^{-1}b_{(1)}) \cdot a \otimes b_{(2)} \subset H \cdot A \otimes B \subset A \otimes B.\end{aligned}$$

So we get that

$$\begin{aligned} A\#H &= \varphi(A\otimes H) \\ &= \varphi\Big(A \otimes \Big(\bigoplus_{i=1}^{s} r_i' B\Big)\Big) \\ &= \bigoplus_{i=1}^{s} r_i'\varphi(A\otimes B) \\ &= \bigoplus_{i=1}^{s} r_i'(A\#B). \end{aligned} \tag{3.4}$$

From (3.3)–(3.4), it follows that

$$\begin{aligned} (A\#H)^e &= A\#H \otimes_k (A\#H)^{\text{op}} \\ &= \Big[\bigoplus_{i=1}^{s}(A\#B)r_i\Big] \bigotimes\nolimits_k \Big[\bigoplus_{j=1}^{s}(A\#B)^{\text{op}} \circ r_j'\Big] \\ &= \bigoplus_{i,j=1}^{s} [(A\#B) \otimes_k (A\#B)^{\text{op}}](r_i \otimes r_j') \\ &= \bigoplus_{i,j=1}^{s} (A\#B)^e(r_i \otimes r_j'). \end{aligned} \tag{3.5}$$

Through the first step, we prove that $A\#H$ is a separable k-algebra, so $A\#H$ is a projective $(A\#H)^e$-module. Then by (3.5), $(A\#H)^e$ is free over $(A\#B)^e$, so we get that $A\#H$ is a projective $(A\#B)^e$-module.

Now using Proposition 3.2, we get that $H = B \oplus C$ as both B-B bimodule and right B-left H relative Hopf module, that is, $BCB \subset C$, $\Delta(C) \subset H \otimes C$ and $\Delta(B) \subset H \otimes B$. Hence for any $a, a' \in A$, $b \in B$ and $c \in C$, we have

$$\begin{aligned} (a\#b)(a'\#c) &= \sum a(b_{(1)} \cdot a')\#b_{(2)}c \in A(H \cdot A)\#BC \subset A\#C, \\ (a'\#c)(a\#b) &= \sum a'(c_{(1)} \cdot a)\#c_{(2)}b \in A(H \cdot A)\#CB \subset A\#C. \end{aligned}$$

It follows that $(A\#B)(A\#C)(A\#B) \subset A\#C$. Therefore we get that

$$A\#H = (A\#B) \bigoplus\nolimits_{A\#B} (A\#C)_{A\#B}$$

as $A\#B$-$A\#B$ bimodule.

In other words, $A\#B$ is a direct summand of $A\#H$ as $(A\#B)^e$-module. Notice that $A\#H$ is a projective $(A\#B)^e$-module as proved above, therefore $A\#B$ is a projective $(A\#B)^e$-module. Consequently, $A\#B$ is a separable k-algebra by Definition 2.2.

Third step, we prove that $A^B \cong \text{End}_{A\#B}(A)^{\text{op}}$ is a separable k-algebra for $B \subset H$ a left coideal subalgebra. First, we establish the isomorphism between A^B and $\text{End}_{A\#B}(A)$. Define

$$\begin{aligned} \theta : A^B &\to \text{End}_{A\#B}(A), \\ a &\mapsto a_r, \end{aligned}$$

where a_r is right multiplication by $a \in A^B$. Clearly θ is injective. Now given any $\psi \in \mathrm{End}_{A\#B}(A)$ and $a \in A$, $\psi(a) = a\psi(1)$, and so $\psi = \psi(1)_r$. Moreover $\psi(1) \in A^B$, since that if $b \in B$, we have $b \cdot \psi(1) = \psi(b \cdot 1) = \varepsilon(b)\psi(1)$, and so $\psi(1) \in A^B$. Thus ψ is surjective. It is clearly an anti-morphism.

Notice that A is a finitely generated projective right A^H-module. Then by Lemma 3.1, A is a finitely generated projective left $A\#H(\cong \mathrm{End}(A_{A^H}))$-module. Since $A\#H$ is a free left $A\#B$-module by (3.3), therefore A is a finitely generated projective left $A\#B$-module. Again using Lemma 3.1, we get that $\mathrm{End}_{A\#B}(A)$ is a separable algebra, and consequently $A^B \cong \mathrm{End}_{A\#B}(A)^{\mathrm{op}}$ is a separable k-algebra.

Finally, for $B \subset H$ a right coideal subalgebra, we observe that $B^{\mathrm{cop}} \subset H^{\mathrm{cop}}$ is a left coideal subalgebra, and A^{op} is an H^{cop}-module algebra. Hence $A^B = A^{\mathrm{op}B^{\mathrm{cop}}}$ is a separable k-algebra.

Next, we present a very important proposition, which will be frequently used in the following propositions. In this proposition, we calculate the commutor ring of $C(A)$ in $A\#H$.

Proposition 3.3 *Let k be a field, H a finite-dimensional Hopf algebra over k, and A a left H-module algebra. Let $C(A)$ denote the center of A. Assume that A is a central separable $C(A)$-algebra, $HC(A) \subset C(A)$, and $C(A)$ is an H^*-Galois extension of $C(A)^H$. Then we have*

$$C_{A\#H}(C(A)) = \{\omega \in A\#H \mid \omega c = c\omega,\ \forall c \in C(A)\} = A,$$

where we identify $a \in A$ with $a\#1_H \in A\#H$.

Proof It is obvious to see that $C_{A\#H}(C(A)) \supset A$, so we only need to prove $C_{A\#H}(C(A)) \subset A$. Choose an element $\sum_{i=1}^{n} a_i\#h_i \in C_{A\#H}(C(A))$. Then for any $x \in C(A)$, we have

$$\begin{aligned} x\Big(\sum_{i=1}^{n} a_i\#h_i\Big) &= \Big(\sum_{i=1}^{n} a_i\#h_i\Big)x \\ &= \sum_{i=1}^{n}\sum a_i(h_{i(1)} \cdot x)\#h_{i(2)} \\ &= \sum_{i,j=1}^{n}\sum a_i(h_{i(1)} \cdot x)\#\langle h_{i(2)}, h_j^*\rangle h_j \\ &= \sum_{i,j=1}^{n} a_i((h_j^* \rightharpoonup h_i) \cdot x)\#h_j, \end{aligned} \tag{3.6}$$

where $n = \dim H$, $\{h_i\}_{i=1}^n$ and $\{h_i^*\}_{i=1}^n$ are dual bases for H and H^* respectively. In particular, we can choose the basis $\{h_i\}_{i=1}^n$ for H such that $h_1 = 1_H$, and $\varepsilon(h_i) = 0,\ \forall 2 \le i \le n$.

Now we claim that $h_1^* = \varepsilon$. Since $H = k1_H \oplus \mathrm{Ker}\varepsilon$, notice that for any $h \in H$, we have $h = \sum_{i=1}^{n} h_i^*(h)h_i = h_1^*(h)1_H + \sum_{i=2}^{n} h_i^*(h)h_i$ and $h = \varepsilon(h)1_H + (h - \varepsilon(h)1_H)$. Hence we get $h_1^*(h)1_H = \varepsilon(h)1_H,\ \forall h \in H$, and consequently $h_1^* = \varepsilon$. Then through (3.6), we have

$$\sum_{i=1}^{n} a_i((h_j^* \rightharpoonup h_i) \cdot x) = a_jx, \quad \forall 1 \le j \le n,\ \forall x \in C(A).$$

In particular, when $j = 1$, noticing $h_1^* = \varepsilon$, we have

$$\sum_{i=1}^{n} a_i(h_i \cdot x) = \sum_{i=1}^{n} a_i((\varepsilon \rightharpoonup h_i) \cdot x) = a_1 x, \quad \forall x \in C(A). \tag{3.7}$$

Notice that $h_i \cdot x \in C(A)$, $\forall 1 \le i \le n$. Then for any $f \in \mathrm{Hom}_{C(A)}(A, C(A))$, applying f to both sides of (3.7), we get

$$\sum_{i=1}^{n} f(a_i)(h_i \cdot x) = f(a_1)x, \quad \forall x \in C(A). \tag{3.8}$$

Since $C(A)/C(A)^H$ is a right H^*-Galois extension, by Lemma 3.3, we have that

$$\pi : C(A)\#H \to \mathrm{End}(C(A)_{C(A)^H}),$$
$$c\#h \mapsto \pi(c\#h) :_{d \mapsto c(h \cdot d)}$$

is an algebra isomorphism. Thus from (3.8), we get

$$\pi\Big(\sum_{i=1}^{n} f(a_i)\#h_i - f(a_1)\Big)(x) = 0, \quad \forall f \in \mathrm{Hom}_{C(A)}(A, C(A)),\ \forall x \in C(A). \tag{3.9}$$

Therefore we have

$$\pi\Big(\sum_{i=1}^{n} f(a_i)\#h_i - f(a_1)\Big) = 0, \quad \forall f \in \mathrm{Hom}_{C(A)}(A, C(A)),$$

and then

$$\sum_{i=1}^{n} f(a_i)\#h_i = f(a_1), \quad \forall f \in \mathrm{Hom}_{C(A)}(A, C(A)).$$

It follows that

$$f(a_i) = 0, \quad \forall f \in \mathrm{Hom}_{C(A)}(A, C(A)),\ \forall 2 \le i \le n. \tag{3.10}$$

Since A is separable over its center $C(A)$, through [1, Theorem 2.1], we get that A is finitely generated projective over $C(A)$. Let $\{v_p\}_{i=1}^m$ and $\{v_p^*\}_{i=1}^m$ be dual $C(A)$-bases for A and $\mathrm{Hom}_{C(A)}(A, C(A))$. Then we have

$$a = \sum_{p=1}^{m} v_p v_p^*(a), \quad \forall a \in A. \tag{3.11}$$

Using (3.10)–(3.11), we get

$$a_i = \sum_{p=1}^{m} v_p v_p^*(a_i) = \sum_{p=1}^{m} v_p 0 = 0, \quad \forall 2 \le i \le n.$$

Thus we have

$$\sum_{i=1}^{n} a_i \# h_i = a_1 \in A.$$

It follows that $C_{A\#H}(C(A)) \subset A$, and consequently $C_{A\#H}(C(A)) = A$.

Proposition 3.4 *With conditions as in Proposition* 3.3*, we have*

$$C(A\#H) = C(A^H) = C(A)^H.$$

Proof By [13, Lemma 8.3.2], we have that

$$\theta : A^H \to \mathrm{End}_{A\#H}(A)^{\mathrm{op}},$$
$$a \mapsto a_r \text{ (right multiplication by } a \in A^H)$$

is an algebra isomorphism. Thus we have

$$\theta(C(A^H)) = C(\mathrm{End}_{A\#H}(A)). \tag{3.12}$$

On the other hand, using Lemma 3.3, we have that

$$\pi : A\#H \to \mathrm{End}(A_{A^H}),$$
$$a\#h \mapsto \pi(a\#h) :_{d \mapsto a(h \cdot d)}$$

is an algebra isomorphim. Thus we have

$$\pi(C(A\#H)) = C(\mathrm{End}(A_{A^H})). \tag{3.13}$$

From Proposition 3.3, we have $C(A\#H) \subset C_{A\#H}(C(A)) = A$. Now we get to prove

$$C(A\#H) = C(A^H) = C(A)^H. \tag{3.14}$$

For any $a \in C(A^H)$, we have $\theta(a) = a_r \in C(\mathrm{End}_{A\#H}(A))$ by (3.12). Notice that

$$a_r(bc) = bca = bac = a_r(b)c, \quad \forall b \in A,\ \forall c \in A^H.$$

Hence we have $a_r \in \mathrm{End}(A_{A^H})$. Now we claim that

$$a_r \in C(\mathrm{End}(A_{A^H})).$$

This is because, for any $\varphi \in \mathrm{End}(A_{A^H})$, noticing $a \in C(A^H) \subset A^H$, we have

$$(a_r \circ \varphi)(b) = a_r(\varphi(b)) = \varphi(b)a = \varphi(ba) = \varphi(a_r(b)) = (\varphi \circ a_r)(b), \quad \forall b \in A.$$

It follows that

$$a_r \circ \varphi = \varphi \circ a_r, \quad \forall \varphi \in \mathrm{End}(A_{A^H}).$$

Therefore $a_r \in C(\mathrm{End}(A_{A^H})) = \pi(C(A\#H))$. Since $\pi(\pi^{-1}(a_r))(1_A) = a_r(1_A) = a$, so we have $a = \pi^{-1}(a_r) \in C(A\#H)$. This means

$$C(A^H) \subset C(A\#H). \tag{3.15}$$

On the other hand, since $C(A\#H) \subset C_{A\#H}(C(A)) = A$, we may choose $a \in C(A\#H)$. Then we have

$$a\#h = a(1\#h) = (1\#h)a = \sum h_{(1)} \cdot a\#h_{(2)}, \quad \forall h \in H.$$

Applying $\mathrm{id}\otimes\varepsilon$ to both sides, one gets

$$h\cdot a=\varepsilon(h)a,\quad \forall h\in H.$$

Therefore we have $a\in A^H$. Then since $a\in C(A\#H)$, for any $x\in A^H\subset A$, we have $ax=xa$. It follows that $a\in C(A^H)$, and consequently

$$C(A\#H)\subset C(A^H). \tag{3.16}$$

From (3.15)–(3.16), we have

$$C(A\#H)=C(A^H).$$

Next, we get to prove the last equality of (3.14). It is straightforward to verify that $C(A)^H\subset C(A\#H)$. For any $c\in C(A)^H=A^H\cap C(A)$, $a\in A$ and $h\in H$, we have

$$(a\#h)c=\sum a(h_{(1)}\cdot c)\#h_{(2)}=\sum a(\varepsilon(h_{(1)})c)\#h_{(2)}=ac\#h=ca\#h=c(a\#h).$$

On the other hand, for any $a\in C(A\#H)=C(A^H)\subset A^H$, we have $ab=ba$, $\forall b\in A$. Therefore $a\in C(A)$, and then $a\in C(A)\cap A^H=C(A)^H$, i.e., $C(A\#H)=C(A^H)\subset C(A)^H$. Hence we have

$$C(A)^H\subset C(A\#H)=C(A^H)\subset C(A)^H,$$

which forces

$$C(A\#H)=C(A^H)=C(A)^H.$$

Using Propositions 3.3–3.4, we can calculate the commutor rings for some subrings of $A\#H$.

Proposition 3.5 *Let k be a field, H a semisimple and cosemisimple Hopf algebra over k, and A a finite-dimensional left H-module algebra. Suppose that the following two conditions are satisfied:*

(1) A^H is a separable k-algebra,

(2) $HC(A)\subset C(A)$, and $C(A)$ is a right H^*-Galois extension of $C(A)^H$.

Then we have that A/A^H is a right H^*-Galois extension, therefore $A\#H$ is a central separable $C(A)^H$-algebra, and

$$C_{A\#H}(A)=C(A), \tag{3.17}$$

$$C_{A\#H}(C(A)\#H)=A^H, \tag{3.18}$$

$$C_{A\#H}(A^H)=C(A)\#H. \tag{3.19}$$

Furthermore, $C(A)\#H$ is also a central separable $C(A)^H$-algebra, and

$$C_{C(A)\#H}(C(A))=C(A). \tag{3.20}$$

Proof First step, we prove that A/A^H is a right H^*-Galois extension. Since $C(A)$ is an H^*-Galois extension of $C(A)^H$, by [13, Theorem 8.3.3], we have that

$$\zeta: C(A)\otimes_{C(A)^H}C(A)\to C(A)\#H,$$
$$c\otimes d\mapsto ctd$$

is surjective, where $0 \neq t \in \int_H^l$.

So $C(A)\#H = C(A)tC(A)$, and we get that

$$A\#H = A(C(A)\#H) = AC(A)tC(A) \subset AtA \subset A\#H,$$

which forces $A\#H = AtA$. Again using [13, Theorem 8.3.3], we have that A/A^H is a right H^*-Galois extension.

Second step, we prove that $A\#H$ is a central separable $C(A)^H$-algebra. As proved in the first step of Theorem 3.1, we know that $A\#H \cong \mathrm{End}(A_{A^H})$ is a separable k-algebra by Lemma 3.1. Notice that $A = A^{k1_H}$ is a separable k-algebra as proved in Theorem 3.1. Then using Lemma 2.1, we have that A is a central separable $C(A)$-algebra, therefore Proposition 3.4 holds. Consequently, from Proposition 3.4, we have that $C(A\#H) = C(A)^H$, and $A\#H$ is a central separable $C(A)^H$-algebra.

Finally, we get to calculate the commutor rings. Through [1, Theorem 2.3], we know that: A^H is separable over k, if and only if, A^H is separable over its center $C(A^H)$ and $C(A^H)$ is separable over k. Since A^H is a separable k-algebra, therefore $C(A^H)$ is a separable k-algebra. By Proposition 3.4, we have that $C(A)^H = C(A^H)$ is a separable k-algebra. Then noticing that $C(A)/C(A)^H$ is a right H^*-Galois extension, through Theorem 3.1, we have that $C(A) = C(A)^{k1_H}$ is a separable k-algebra, and therefore a separable $C(A)^H$-algebra by Lemma 2.1. Noticing that $A\#H$ is a central separable $C(A)^H$-algebra, and $C_{A\#H}(C(A)) = A$ by Proposition 3.3, now using Lemma 3.2, we get

$$C_{A\#H}(A) = C_{A\#H}(C_{A\#H}(C(A))) = C(A).$$

Next, we prove

$$C_{A\#H}(C(A)\#H) = A^H \quad \text{and} \quad C_{A\#H}(A^H) = C(A)\#H.$$

Notice that $C_{A\#H}(C(A)\#H) \subset C_{A\#H}(C(A)) = A$. We may choose $a \in C_{A\#H}(C(A)\#H)$, then we have

$$a\#h = a(1\#h) = (1\#h)a = \sum (h_{(1)} \cdot a)\#h_{(2)}, \quad \forall h \in H.$$

Applying $\mathrm{id} \otimes \varepsilon$ to the both sides, we have

$$h \cdot a = \varepsilon(h)a, \quad \forall h \in H.$$

So we get $a \in A^H$, i.e., $C_{A\#H}(C(A)\#H) \subset A^H$. On the other hand, for any $a \in A^H$, $c \in C(A)$ and $h \in H$, we have

$$(c\#h)a = \sum c((h_{(1)} \cdot a))\#h_{(2)} = \sum c(\varepsilon(h_{(1)})a)\#h_{(2)} = ca\#h = a(c\#h).$$

It follows that $a \in C(A)\#H$, i.e., $A^H \subset C(A)\#H$. Thus we get

$$C_{A\#H}(C(A)\#H) = A^H.$$

Replacing A by $C(A)$, in the same way, we get that $C(A)\#H \cong \mathrm{End}(C(A)_{C(A)^H})$ is a separable k-algebra, and so a separable R-algebra by Lemma 2.1. Then by Lemma 3.2, we have

$$C_{A\#H}(A^H) = C_{A\#H}(C_{A\#H}(C(A)\#H)) = C(A)\#H.$$

Moreover, since $C(C(A)\#H) = C(C(A))^H = C(A)^H$, we have that $C(A)\#H$ is a central separable $C(A)^H$-algebra. Similarly, we have

$$C_{C(A)\#H}(C(A)) = C(A).$$

Now, we get to prove the Galois connection theorem.

Theorem 3.2 *Let k be a field, H a semisimple and cosemisimple Hopf algebra over k, and A a finite-dimensional left H-module algebra. If A^H is a separable k-algebra, and A/A^H is a right H^*-Galois extension, then there exists a Galois connection*

$$\mathrm{Sub}_{\mathrm{sep}}(A/A^H) \underset{\phi}{\overset{\psi}{\rightleftarrows}} \mathrm{Sub}_{\mathrm{coi}}(H),$$

where the left hand side is the lattice of all separable subalgebras of A containing A^H, the right hand side denotes the lattice of all the right coideal subalgebras of H, and ψ and ϕ are defined as follows:

$$\psi(\Omega) = \Big\{h \in H \;\Big|\; \sum h_{(1)} \cdot \omega \otimes h_{(2)} = \omega \otimes h,\ \forall \omega \in \Omega\Big\},$$
$$\phi(B) = A^B = \{a \in A \mid ba = \varepsilon(b)a,\ \forall b \in B\}$$

for any intermediate separable k-algebra Ω between A and A^H, and for any right coideal subalgebra $B \subset H$. Moreover, we have

$$\psi \circ \phi(B) = B, \quad \forall B \subset H \textit{ a right coideal subalgebra.}$$

Proof First step, we prove that

$$\mathrm{Sub}_{\mathrm{sep}}(A/A^H) \underset{\phi}{\overset{\psi}{\rightleftarrows}} \mathrm{Sub}_{\mathrm{coi}}(H)$$

is a Galois connection.

First, we verify that ψ and ϕ are both well-defined. Let Ω be an intermediate separable k-algebra between A and A^H, and set $B = \psi(\Omega) = \big\{h \in H \,\big|\, \sum h_{(1)} \cdot \omega \otimes h_{(2)} = \omega \otimes h,\ \forall \omega \in \Omega\big\}$. For any $b \in B$, we have

$$\sum b_{(1)} \cdot \omega \otimes b_{(2)} = \omega \otimes b, \quad \forall \omega \in \Omega.$$

Applying $\mathrm{id} \otimes \Delta$ to both sides:

$$\sum b_{(1)} \cdot \omega \otimes b_{(2)} \otimes b_{(3)} = \sum \omega \otimes b_{(1)} \otimes b_{(2)}, \quad \forall \omega \in \Omega.$$

This means $\Delta(B) \subset B \otimes H$. It is straightforward to verify that B is a subalgebra of H, as for $b, c \in B$ and $\omega \in \Omega$, we have

$$\sum (bc)_{(1)} \cdot \omega \otimes (bc)_{(2)} = \sum b_{(1)}(c_{(1)} \cdot \omega) \otimes b_{(2)}c_{(2)} = \sum b_{(1)} \cdot \omega \otimes b_{(2)}c = \omega \otimes bc.$$

Thus $B \subset H$ is a right coideal subalgebra. On the other hand, let $B \subset H$ be a right coideal subalgebra, from Theorem 3.1, we have that $\phi(B) = A^B$ is an intermediate separable k-algebra between A and A^H. Hence ψ and ϕ are both well-defined.

Then, we verify that ψ and ϕ are antimonotonic morphisms. Let $\Omega_1 \subset \Omega_2$ be intermediate separable k-algebras between A and A^H. By the definition of ψ, for any $b \in \psi(\Omega_2)$, we have

$$\sum b_{(1)} \cdot x \otimes b_{(2)} = x \otimes b, \quad \forall x \in \Omega_2.$$

Noticing that $\Omega_1 \subset \Omega_2$, we get

$$\sum b_{(1)} \cdot \omega \otimes b_{(2)} = \omega \otimes b, \quad \forall \omega \in \Omega_1 \subset \Omega_2.$$

Again, by the definition of ψ, we have $b \in \psi(\Omega_1)$, i.e., $\psi(\Omega_2) \subset \psi(\Omega_1)$. On the other hand, letting $B_1 \subset B_2$ be right coideal subalgebras of H, we have $\phi(B_1) = A^{B_1} \supset A^{B_2} = \phi(B_2)$. This is because, for any $a \in A^{B_2}$, we have $ba = \varepsilon(b)a$, $\forall b \in B_1 \subset B_2$, therefore $a \in A^{B_1}$. Hence ψ and ϕ are both antimonotonic morphisms.

Next, we verify that $\Omega \subset \phi \circ \psi(\Omega)$ and $B \subset \psi \circ \phi(B)$. For any $b \in \psi(\Omega)$, we have

$$\sum b_{(1)} \cdot \omega \otimes b_{(2)} = \omega \otimes b, \quad \forall \omega \in \Omega.$$

Applying $\mathrm{id} \otimes \varepsilon$ to both sides, we get

$$b \cdot \omega = \varepsilon(b)\omega, \quad \forall \omega \in \Omega.$$

By the arbitrariness of b, we have $\omega \in A^{\psi(\Omega)}$, i.e., $\Omega \subset A^{\psi(\Omega)} = \phi \circ \psi(\Omega)$. On the other hand, for any $x \in \phi(B) = A^B$ and $b \in B$, we have $\Delta(b) = \sum b_{(1)} \otimes b_{(2)} \subset B \otimes H$, and then

$$\sum b_{(1)} \cdot x \otimes b_{(2)} = \varepsilon(b_{(1)})x \otimes b_{(2)} = x \otimes b.$$

By the arbitrariness of x, we get $b \in \psi(\phi(B))$, i.e., $B \subset \psi(\phi(B))$.

As proved above, by Definition 2.5, we have that

$$\mathrm{Sub}_{\mathrm{sep}}(A/A^H) \underset{\phi}{\overset{\psi}{\rightleftarrows}} \mathrm{Sub}_{\mathrm{coi}}(H)$$

is a Galois connection between right coideal subalgebras of H and separable subalgebras of A containing A^H.

Second step, we prove that $B = \psi(\phi(B))$ for $B \subset H$ a right coideal subalgebra. Set

$$B' = \psi(\phi(B)) = \psi(A^B) = \Big\{ h \in H \;\Big|\; \sum h_{(1)} \cdot \omega \otimes h_{(2)} = \omega \otimes h, \ \forall \omega \in A^B \Big\}.$$

Then for any $b \in B$, we have

$$\sum b_{(1)} \cdot \omega \otimes b_{(2)} = \sum \varepsilon(b_{(1)})\omega \otimes b_{(2)} = \omega \otimes b, \quad \forall w \in A^B.$$

It follows that $b \in B'$, i.e., $B \subset B'$. Hence we have $A^B \supset A^{B'}$ as proved in the first step. On the other hand, notice that for any intermediate separable algebra Ω between A and A^H, we have $\Omega \subset (\phi \circ \psi)(\Omega)$ as proved in the first step. Therefore we have

$$A^{B'} \subset A^B = \phi(B) \subset (\phi \circ \psi)(\phi(B)) = \phi(\psi(A^B)) = \phi(B') = A^{B'},$$

which forces

$$A^B = A^{B'}.$$

Notice that $A^{\rm op}$ is a left $H^{\rm cop}$-module algebra, and $B^{\rm cop} \subset H^{\rm cop}$ is a left coideal subalgebra, and notice ${A^{\rm op}}^{B^{\rm cop}} = A^B = A^{B'} = {A^{\rm op}}^{{B'}^{\rm cop}}$. Then using Proposition 3.1, we have

$$A^{\rm op}\#B^{\rm cop} = \pi^{-1}(\mathrm{End}({A^{\rm op}}_{{A^{\rm op}}^{B^{\rm cop}}})) = \pi^{-1}(\mathrm{End}({A^{\rm op}}_{{A^{\rm op}}^{{B'}^{\rm cop}}})) = A^{\rm op}\#{B'}^{\rm cop}.$$

It follows that $B^{\rm cop} = {B'}^{\rm cop}$, and consequently we get

$$B = B^{\rm cop} = {B'}^{\rm cop} = B' = \psi(\phi(B)).$$

In particular, if $H = (kG)^*$, we have the following 1-1 correspondence theorem.

Theorem 3.3 *Let k be a field, G a finite group, and A a finite-dimensional G-graded algebra. The characteristic of k does not divide the order of G. Suppose that the following conditions are satisfied:*

(1) *A_1 is a separable k-algebra,*

(2) *$C(A)$ is a strongly G-graded algebra,*

(3) *$C(A)$ is an integral domain.*

Then A is a strongly G-graded algebra, and there is a 1-1 *correspondence between subgroups of G and k-separable subalgebras of A containing A_1.*

Proof Set $H = (kG)^*$. Notice that the characteristic of k does not divide the order of G, therefore $H = (kG)^*$ is a semisimple and cosemisimple Hopf algebra. Then by [13, Theorem 8.17], we know that: $C(A)_1 \subset C(A)$ is kG-Galois, if and only if, $C(A)$ is strongly G-graded. Thus $C(A)$ is a right kG-Galois extension of $C(A)_1 = C(A)^H$. By Proposition 3.5, A is a right kG-Galois extension of $A^H = A_1$, therefore A is a strongly G-graded algebra by [13, Theorem 8.17].

Notice that there is a 1-1 correspondence between subgroups of G and right coideal subalgebras of $(kG)^*$ by [12]. So we only need to prove the 1-1 correspondence between right coideal subalgebras of $(kG)^*$ and k-separable subalgebras of A containing A_1. Notice that by Theorem 3.2, there is a Galois connection between right coideal subalgebras of $(kG)^*$ and k-separable subalgebras of A containing A_1.

Now recall the definition we gave in Theorem 3.2:

$$\psi(\Omega) = \Big\{h \in H \;\Big|\; \sum h_{(1)} \cdot \omega \otimes h_{(2)} = \omega \otimes h, \ \forall \omega \in \Omega\Big\},$$
$$\phi(B) = A^B = \{a \in A \mid ba = \varepsilon(b)a, \ \forall b \in B\}.$$

Again as a conclusion of Theorem 3.2, we have $\psi \circ \phi(B) = B$ for any right coideal subalgebra $B \subset H$. To verify the 1-1 correspondence relation between right coideals of $(kG)^*$ and k-separable subalgebras of A containing A_1, we only need to prove

$$\phi \circ \psi(\Omega) = \Omega \tag{3.21}$$

for any intermediate separable k-algebra Ω between A and A^H.

Since A is a separable k-algebra by Theorem 3.1, we have that

$$A^H \subset \Omega \subset A$$

is a chain of separable k-algebras. It follows that

$$C_{A\#H}(A^H) \supset C_{A\#H}(\Omega) \supset C_{A\#H}(A).$$

Notice that in Proposition 3.5, through (3.17) and (3.19), we have $C_{A\#H}(A) = C(A)$ and $C_{A\#H}(A^H) = C(A)\#H$. Then set

$$T = C_{A\#H}(\Omega).$$

We have

$$C(A)\#H \supset T \supset C(A). \tag{3.22}$$

Since Ω is a separable k-algebra, it is also a separable $C(A)^H$-algebra by Lemma 2.1. Then noticing that $A\#H$ is a central separable $C(A)^H$-algebra by Proposition 3.5, using Lemma 3.2, we have that

$$C_{A\#H}(T) = C_{A\#H}(C_{A\#H}(\Omega)) = \Omega, \tag{3.23}$$

and T is a separable R-algebra.

First, we claim that G must be an abelian group.

Notice that $C(A)$ is a strongly G-graded commutative algebra. Then for any $g, h \in G$, we have $C(A)_{gh} = C(A)_g C(A)_h = C(A)_h C(A)_g = C(A)_{hg}$. It follows that $gh = hg$, $\forall g, h \in G$. Therefore G is an abelian group.

Now by [13, Theorem 2.3.1], there exists a group Q and a separable extension field E of k such that $EG = kG \otimes_k E \cong (EQ)^*$. Therefore $H = (kG)^* = kQ$ is a group algebra.

Set $B = \psi(\Omega) = \{h \in H \mid \sum h_{(1)} \cdot \omega \otimes h_{(2)} = \omega \otimes h,\ \forall \omega \in \Omega\}$. We proved in Theorem 3.2 that B is a right coideal subalgebra of H. Since $H = kQ$ is a group algebra, we have that $B = kW$ for some subgroup $W \subset Q$.

Next, we claim that

$$T = C(A)\#B, \tag{3.24}$$

where $T = C_{A\#H}(\Omega)$ as defined above. On one hand, it is obvious to see $C(A)\#B \subset T$, as for any $c \in C(A)$, $b \in B$, we have

$$(c\#b)\omega = \sum c(b_{(1)} \cdot \omega)\#b_{(2)} = c\omega\#b = \omega(c\#b), \quad \forall \omega \in \Omega.$$

On the other hand, by (3.22), we have $C(A)\#H \supset T \supset C(A)$. Then notice that $H = kQ$ is a group algebra, so we can choose an element $\sum_{q \in Q} c_q\#q \in T$, where $c_q \in C(A)$, $\forall q \in Q$. Since $T = C_{A\#H}(\Omega)$, we have

$$\omega\Big(\sum_{q\in Q} c_q\#q\Big) = \Big(\sum_{q\in Q} c_q\#q\Big)\omega = \sum_{q\in Q} c_q(q \cdot \omega)\#q, \quad \forall \omega \in \Omega.$$

It follows that

$$c_q(q \cdot \omega - \omega) = 0, \quad \forall q \in Q,\ \forall \omega \in \Omega.$$

If $q \notin B$, by the definition of B, we have $q \cdot \omega \neq \omega$ for some $\omega \in \Omega$. Then noticing that $C(A)$ is an integral domain, we have $c_q = 0$. Therefore $\sum\limits_{q \in Q} c_q \# q \in C(A)\#B$, that is, $T \subset C(A)\#B$. Thus (3.24) holds.

Finally, we claim that

$$\Omega = A^B. \tag{3.25}$$

By (3.23)–(3.24), $\Omega = C_{A\#H}(T) = C_{A\#H}(C(A)\#B)$. On one hand, it is obvious to see $A^B \subset \Omega$ as for any $a \in A^B$, $c \in C(A)$, $b \in B$ we have

$$(c\#b)a = \sum c(b_{(1)} \cdot a)\#b_{(2)} = ca\#b = a(c\#b).$$

On the other hand, for any $\omega \in \Omega$, $\sum\limits_{w \in W} c_w \# w \in C(A)\#B$, we have

$$\omega\Big(\sum_{w \in W} c_w \# w\Big) = \Big(\sum_{w \in W} c_w \# w\Big)\omega = \sum_{w \in W} c_w (w \cdot \omega)\# w.$$

It follows that

$$c_w(w \cdot \omega - \omega) = 0, \quad \forall w \in W.$$

Consequently, by the arbitrariness of c_w, we may assume that $c_w \neq 0$, $\forall w \in W$. Noticing that $C(A)$ is an integral domain, therefore we have

$$w \cdot \omega = \omega, \quad \forall w \in W.$$

Thus (3.25) follows. Then noticing $\psi(\phi(B)) = B$ by Theorem 3.2, we have that $\phi(\psi(\Omega)) = \phi(\psi(A^B)) = \phi(\psi(\phi(B))) = \phi(B) = A^B = \Omega$, thus (3.21) holds. Consequently, the Galois connection between right coideal subalgebras of $(kG)^*$ and k-separable subalgebras of A containing A_1 is just a 1-1 correspondence.

Let $A = C(A)$ be a field. Then we have the following corollary.

Corollary 3.1 *Let $E \subset F$ be fields, G a finite group, and the characteristic of E does not divide the order of G. Suppose that F is strongly G-graded, and $F_1 = E$. Then there is a* 1-1 *correspondence between right coideal subalgebras of $(EG)^*$ and separable subfield extensions of F over E in the usual sense of Galois theory.*

At the end of this paper, we present a conjecture: Let H be a semisimple and cosemisimple Hopf algebra over a field k, and let A be a left H-module algebra. Suppose that A is a field, and A/A^H is a right H^*-Galois extension. Then there is a 1-1 correspondence between right coideal subalgebras of H and separable subfield extensions of A over A^H in the usual sense of Galois theory.

References

[1] Auslander, M. and Goldman, O., The brauer group of a commutative ring, *Trans. Amer. Math. Soc.*, **97**, 1960, 367–409.

[2] Chase, S. U., Harrison, D. K. and Rosenberg, A., Galois theory and Galois cohomology of commutative rings, *Mem. Amer. Math. Soc.*, **52**, 1965, 15–33.

[3] Chase, S. U. and Sweedler, M. E., Hopf Algebras and Galois Theory, Lecture Notes in Math., **97**, Springer-Verlag, Berlin, Heidelberg, 1969, 52–83.

[4] Cohen, M. and Fishman, D., Hopf algebra actions, *J. Algebra,* **100**, 1986, 363–379.

[5] Cohen, M. and Fishman, D., Semisimple extensions and elements of trace 1, *J. Algebra,* **149**, 1992, 419–437.

[6] Davey, B. A. and Priestley, H. A., Introduction to Lattices and Order, Cambridge Univ. Press, Cambridge, 2002.

[7] DeMeyer, F. and Ingraham, E., Separable Algebras over Commutative Rings, Lecture Notes in Math., **181**, Springer-Verlag, Berlin, 1971.

[8] Hirata, K. and Sugano, K., On semisimple extensions and separable extensions over non commutative rings, *J. Math. Soc. Japan*, **18**(4), 1966, 360–373.

[9] Kreimer, H. F. and Takeuchi, M., Hopf algebras and Galois extensions of an algebra, *Indiana Univ. Math. J.,* **30**, 1981, 675–692.

[10] Kanzaki, T., On commutor ring and Galois theory of separable algebras, *Osaka J. Math.,* **1**, 1964, 103–115.

[11] Kanzaki, T., On Galois extension of rings, *Nagoya Mathematical Journal,* **27**, Part 1, 1966, 43–49.

[12] Masuoka, A., Freeness of Hopf algebra over coideal subalgebras, *Comm. in Algebra,* **20**, 1992, 1353–1373.

[13] Montgomery, S., Hopf Algebras and Their Actions on Rings, CBMS 82, Amer. Math. Soc., Providence, 1993.

[14] Radford, D. E., The antipode of a finite-dimensional Hopf algebra over a field has finite order, *Bull. Amer. Math. Soc.,* **81**(6), 1975, 1103–1105.

[15] Schauenburg, P. and Schneider, H., On generalized Hopf Galois extensions, *Journal of Pure and Applied Algebra,* **202**, 2005, 168–194.

[16] Skryabin, S., Projectivity and freeness over comodule algebras, *Trans. Amer. Math. Soc.,* **359**, 2007, 2597–2623.

[17] Sweedler, M., Integrals for Hopf algebras, *Ann. of Math., Second Series*, **89**(2), 1969, 323–335.

[18] Wang, C. H. and Zhu, S. L., On smash products of transitive module algebras, *Chin. Ann. Math. Ser. B,* **31**(4), 2010, 541–554.