Hopf Bigalois Extensions

Peter Schauenburg *
Department of Mathematics, University of Southern California

1 Introduction

Let k be a commutative base ring and H a Hopf algebra. An H-Galois extension A of k is an H-comodule algebra such that $A^{\mathrm{co}\,H} = k$ and a certain map $A \otimes A \to A \otimes H$ is bijective. The notion of a Hopf-Galois extension generalizes that of a Galois extension of rings.

The group G in a G-Galois extension A/k is uniquely determined by the ring extension A/k. By contrast, the Hopf algebra H in an H-Galois extension A/k is not unique. Examples for the case when A is a field can be found in [7].

In [22], the ambiguity of the Hopf algebra H in an H-Galois extension is exhibited in the form of an interesting systematic construction: Given a right H-Galois extension A/k of commutative rings (in particular H is also commutative) the authors construct another Hopf algebra $\mathcal{L}$ such that A is also an $\mathcal{L}$-Galois extension of k. Greither [6] discusses some aspects of the construction, in particular the link to the results of [7]. He also proves that the construction of [22] is involutive: applying it to the $\mathcal{L}$-Galois extension A/k we get the original Hopf algebra H back.

In this paper we will generalize the construction of [22] to the case of noncommutative H-Galois extensions A/k with noncommutative H (note we restrict ourselves to the case when the subring of coinvariants is the base ring; our

*Current address: Mathematisches Institut der Universität München, Theresienstraße 39, 80333 München, Germany

construction still generalizes that of [22] since in the commutative case we can extend the base ring to be the fixed ring). Given a right H-Galois extension A/k we construct a Hopf algebra $L = L(A, H)$ such that A is an L-H-bicomodule algebra and a left L-Galois extension of k (we say that A is an L-H-bigalois extension of k). The switching of sides from a right to a left Hopf-Galois extension is natural but can be made to disappear if H has bijective antipode; in the case of commutative rings $L(A, H) = \mathcal{L}$ coincides with the construction from [22].

If H is a finite projective cocommutative Hopf algebra, then the isomorphism classes of H-Galois extensions of k form a group [5]. If H is the dual of the group algebra of a finite commutative group G, the classically G-Galois extensions of commutative rings form a subgroup of this group, known as the Harrison group. In Section 4 we show that bigalois extensions form a groupoid: Morphisms in this groupoid between k-flat Hopf algebras L and H are the isomorphism classes of L-H-bigalois extensions. Composition is given by cotensor product, which generalizes the composition in the Harrison group. As a special case, the set of isomorphism classes of H-H-bigalois extensions is a group; after the present paper had been accepted for publication, the author has received a copy of [21], where this group is considered. We prove that if H is cocommutative, then the group of H-H-bigalois extensions is a semidirect product of the group of Hopf algebra automorphisms of H with the group of H-Galois extensions.

In Section 5 we discuss the relations of Hopf bigalois extensions to the theory of Morita equivalences of the monoidal categories of comodules over Hopf algebras. We find that equivalences of monoidal categories ${}^B\mathcal{M} \cong {}^H\mathcal{M}$ are classified by B-H-bigalois extensions of k; the composition of such equivalences corresponds to the composition of bigalois extensions considered in Section 4.

In the case that k is a field, we can combine reconstruction theorems well known in quantum group theory [20] and a bijection between H-Galois extensions and fiber functors on the category of H-comodules [18] to give another explanation for the construction of $L(A, H)$.

One of the motivations for the construction of $\mathcal{L}$ in [22] was the study of analogues of the Galois correspondence for classical Galois extensions. By [22, Thm. 4.4] there is a bijective correspondence between H-costable intermediate fields in an H-Galois field extension K/k and Hopf ideals of $\mathcal{L} = L(K, H)$.

(Taking into account the result from [6] that applying the construction that led to $\mathcal{L}$ to $\mathcal{L}$ gives H back, this theorem can be used to characterize those subfields of L that correspond to Hopf ideals of H in a generalized Galois correspondence). In the last section we present two variations of this idea. One is a generalization of [22, Thm. 4.4] to the noncommutative case, covering Hopf-Galois skew field extensions of a base field. This uses our generalization of $\mathcal{L}$, but the same technique of proof as [22], based on the main theorem of [16]. The other version of a Galois correspondence covers commutative Hopf-Galois extensions of rings in case the Hopf algebra is finitely generated projective. Here we are dealing with the original commutative version of $L(A, H)$, but need a different proof, since the main correspondence theorem in [16] only holds in the field case.

2 Preliminaries

Throughout the paper, k denotes a fixed commutative base ring. All algebras, coalgebras, etc. are k-algebras, k-coalgebras etc. We denote the multiplication map of an algebra by ∇, the comultiplication of a coalgebra by Δ, comodule structures by δ etc. We make free use of Sweedler's notation for comultiplcations and comodule structures, omitting the summation symbol: $\Delta(c) = c_{(1)} \otimes c_{(2)}$, and $\delta(v) = v_{(0)} \otimes v_{(1)}$ for a right, $\delta(v) = v_{(-1)} \otimes v_{(0)}$ for a left comodule structure, respectively.

A right H-Galois extension A/k is a right H-comodule algebra A such that $A^{\mathrm{co}\,H} = k$, and the Galois map $\kappa_r : A \otimes A \to A \otimes H$ defined by $\kappa_r(x \otimes y) = xy_{(0)} \otimes y_{(1)}$ is a bijection. If A is faithfully flat over k, then bijectivity of κ_r implies $k = A^{\mathrm{co}\,H}$ by [19, Lem. 1.1], and H is faithfully flat over k since $A \otimes H \cong A \otimes A$ is faithfully flat over A.

A left H-Galois extension A/k is a left H-comodule algebra A such that ${}^{\mathrm{co}\,H}A = k$ and the Galois map $\kappa_\ell : A \otimes A \to H \otimes A$ defined by $\kappa_\ell(x \otimes y) = x_{(-1)} \otimes x_{(0)}y$ is a bijection. Note that with this definition A is a left H-Galois extension of k if and only if A^{op} is a right H^{opcop}-Galois extension of k.

For calculations with the inverse of κ_r we adopt a notation similar to that in [15]. We define a map $\gamma : H \to A \otimes A$ by $\gamma(h) = \kappa^{-1}(1 \otimes h)$ and write $\gamma(h) =: \sum \ell_i(h) \otimes r_i(h)$. From [15, (3.4)], we take the following identities for

γ, where $g, h \in H$, $x \in A$ and $b \in B$:

$$\nabla\gamma(h) = \sum \ell_i(h) r_i(h) = \varepsilon(h) \tag{2.1}$$

$$\sum \ell_i(h) \otimes r_i(h)_{(0)} \otimes r_i(h)_{(1)} = \sum \ell_i(h_{(1)}) \otimes r_i(h_{(1)}) \otimes h_{(2)} \tag{2.2}$$

$$\sum \ell_i(h)_{(0)} \otimes r_i(h) \otimes \ell_i(h)_{(1)} = \sum \ell_i(h_{(2)}) \otimes r_i(h_{(2)}) \otimes S(h_{(1)}) \tag{2.3}$$

$$\gamma(gh) = \sum \ell_i(h)\ell_j(g) \otimes r_j(g) r_i(h) \tag{2.4}$$

$$\sum x_{(0)}\ell_i(x_{(1)}) \otimes r_i(x_{(1)}) = 1 \otimes x \tag{2.5}$$

Let A be a right H-comodule algebra. A Hopf module $M \in \mathcal{M}_A^H$ is a right A-module and H-comodule such that $\delta(ma) = m_{(0)}a_{(0)} \otimes m_{(1)}a_{(1)}$ holds for all $a \in A$, $m \in M$.

If A is faithfully flat over k, then there is a structure theorem for Hopf modules in the form of inverse category equivalences

$$\begin{aligned} \mathcal{M}_k &\to \mathcal{M}_A^H \qquad & \mathcal{M}_A^H &\to \mathcal{M}_k \\ N &\mapsto N \otimes A & M &\mapsto M^{\mathrm{co}\, H} \end{aligned}$$

Specifically, multiplication induces an isomorphism $M^{\mathrm{co}\, H} \otimes A \to M$, whose inverse is given by $M \ni m \mapsto \sum m_{(0)}\ell_i(m_{(1)}) \otimes r_i(m_{(1)}) \in M^{\mathrm{co}\, H} \otimes A$.

We will need to consider the Hopf module $A \otimes A \in \mathcal{M}_A^H$ as a special case, where the right A-module structure is that induced by the right tensorand, and the comodule structure is the codiagonal one. In this case,

$$\begin{aligned} A \otimes A &\cong (A \otimes A)^{\mathrm{co}\, H} \otimes A \\ x \otimes y &\mapsto \sum x_{(0)} \otimes \ell_i(x_{(1)}) \otimes r_i(x_{(1)}) y \end{aligned} \tag{2.6}$$

The cotensor product of a right C-comodule V and a left C-comodule W is defined to be the equalizer

$$V \underset{C}{\square} W \to V \otimes W \rightrightarrows V \otimes C \otimes W$$

where the two parallel arrows are given by the right comodule structure of V and the left comodule structure of W, respectively. We have a (canonical) isomorphism $M \otimes (V \underset{C}{\square} W) \cong (M \otimes V) \underset{C}{\square} W$ if M is a flat k-module or if C is k-flat and W is C-coflat. For a right C-comodule U, a C-D-bicomodule V and a left D-comodule W, there is a right D-comodule structure on $U \underset{C}{\square} V$ provided D is k-flat, and a left C-comodule structure on $V \underset{D}{\square} W$ provided C is k-flat. However, $(U \underset{C}{\square} V) \underset{D}{\square} W \cong U \underset{C}{\square} (V \underset{D}{\square} W)$ does not necessarily hold. We note for later use that if H is a Hopf algebra, A is a faithfully flat right H-Galois extension of k, V is an H-D-bicomodule and W is a left D-comodule, then we do have a canonical isomorphism $(A \underset{H}{\square} V) \underset{D}{\square} W \to A \underset{H}{\square} (V \underset{D}{\square} W)$. In fact, by flatness of A there is a map

$$(A \underset{H}{\square} V) \underset{D}{\square} W \to (A \otimes V) \underset{D}{\square} W \cong A \otimes (V \underset{D}{\square} W)$$

To see that this maps isomorphically onto $A \underset{H}{\square} (V \underset{D}{\square} W)$ we have to show that

$$(A \underset{H}{\square} V) \underset{D}{\square} W \to A \otimes (V \underset{D}{\square} W) \rightrightarrows A \otimes H \otimes (V \underset{D}{\square} W)$$

is an equalizer. This in turn needs only to be verified after tensoring with the faithfully flat module A, that is, we want to show $A \otimes \left((A \underset{H}{\square} V) \underset{D}{\square} W\right) \cong A \otimes \left(A \underset{H}{\square} (V \underset{D}{\square} W)\right)$. Using flatess of A and the fact that $A \otimes A \cong A \otimes H$ as right H-comodules with the structures induced by those of the respective right tensorands, we compute:

$$\begin{aligned}
A \otimes \left((A \underset{H}{\square} V) \underset{D}{\square} W\right) &\cong \left(A \otimes (A \underset{H}{\square} V)\right) \underset{D}{\square} W \\
&\cong \left((A \otimes A) \underset{H}{\square} V\right) \underset{D}{\square} W \\
&\cong \left((A \otimes H) \underset{H}{\square} V\right) \underset{D}{\square} W \\
&\cong (A \otimes V) \underset{D}{\square} W \\
&\cong A \otimes (V \underset{D}{\square} W) \\
&\cong (A \otimes H) \underset{H}{\square} (V \underset{D}{\square} W) \\
&\cong (A \otimes A) \underset{H}{\square} (V \underset{D}{\square} W) \\
&\cong A \otimes \left(A \underset{H}{\square} (V \underset{D}{\square} W)\right)
\end{aligned}$$

3 The main construction

Given a faithfully flat right H-Galois extension A of k, we construct a second Hopf algebra L such that A is also a left L-Galois extension of k. The construction generalizes [22, Sec.3].

3.1. Definition: *Let H be a Hopf algebra and A/k a faithfully flat right H-Galois extension. We define $L(A,H) := (A \otimes A)^{\mathrm{co}\,H}$, where the H-comodule structure on A is the codiagonal one.*

Similarly to [14, Lem. 3.1] one can see that for any right H-comodules V and W the space $(V \otimes W)^{\mathrm{co}\,H}$ consists of those $\sum v_i \otimes w_i \in V \otimes W$ satisfying $\sum v_i \otimes w_{i(0)} \otimes w_{i(1)} = \sum v_{i(0)} \otimes w_i \otimes S(v_{i(1)})$.

3.2. Lemma: *Let H be a Hopf algebra and A a faithfully flat right H-Galois extension of k. Set $L := L(A,H)$. There is a right H-colinear map $\delta' : A \to L \otimes A$ given by $\delta'(a) = \sum a_{(0)} \otimes \ell_i(a_{(1)}) \otimes r_i(a_{(1)})$, which has the following universal property: Given a k-module V and an H-colinear map $\phi : A \to V \otimes A$, there is a unique map $f : L \to V$ with $\phi = (f \otimes A)\delta'$. We have $f(\sum x_i \otimes y_i) \otimes 1_A = \sum \phi(x_i) y_i$.*

Proof: We have natural bijections

$$T : \mathrm{Hom}^H(A, V \otimes A) \cong \mathrm{Hom}^H_{-A}(A \otimes A, V \otimes A)$$

given by $T(\phi)(x \otimes y) = \phi(x)y$ and $T^{-1}(g)(a) = \phi(a \otimes 1)$, and

$$B : \mathrm{Hom}^H_{-A}(A \otimes A, V \otimes A) \cong \mathrm{Hom}_k((A \otimes A)^{\mathrm{co}\,H}, V)$$

from the structure theorem for Hopf modules. Composing them yields the desired universal property for the map $\delta' := T^{-1}B^{-1}(\mathrm{id}_L)$. The map $B^{-1}(\mathrm{id}_L)$ is the isomorphism (2.6), so that $\delta'(a) = B^{-1}(\mathrm{id}_L)(a \otimes 1) = \sum a_{(0)} \otimes \ell_i(a_{(1)}) \otimes r_i(a_{(1)})$ as claimed. For ϕ and f corresponding to each other as in the statement of the Lemma, we have $f(\sum x_i \otimes y_i) \otimes 1_A = B^{-1}(f)(\sum x_i \otimes y_i) = T(\phi)(\sum x_i \otimes y_i) = \sum \phi(x_i) y_i$. $\square$

3.3. Lemma: *Let H be a Hopf algebra and A a faithfully flat right H-Galois extension of k. Put $L := L(A,H)$.*

(1) L is a subalgebra of $A \otimes A^{\mathrm{op}}$, and $\delta' : A \to L \otimes A$ is an algebra map.

(2) If V is an algebra and $\phi : A \to V \otimes A$ is an algebra map, then so is the induced map $f : L \to V$.

PROOF:

(1) For $\sum w_i \otimes x_i, \sum y_j \otimes z_j \in (A \otimes A)^{\mathrm{co}\,H}$ we have $\delta(\sum w_i y_j \otimes z_j x_i) = \sum w_{i(0)} y_{j(0)} \otimes z_{j(0)} x_{i(0)} \otimes w_{i(1)} y_{j(1)} z_{j(1)} x_{i(1)} = \sum w_{i(0)} y_j \otimes z_j x_{i(0)} \otimes w_{i(1)} x_{i(1)} = \sum w_i y_j \otimes z_j x_i \otimes 1$, so that L is a subalgebra of $A \otimes A^{\mathrm{op}}$. That δ' is an algebra map is a direct consequence of equation (2.4).

(2) Let $\sum w_i \otimes x_i, \sum y_j \otimes z_j \in (A \otimes A)^{\mathrm{co}\,H}$. Writing $\phi(a) = a_V \otimes a_A$ for $a \in A$, we have $f\left((\sum w_i \otimes x_i)(\sum y_j \otimes z_j)\right) \otimes 1 = f(\sum w_i y_j \otimes z_j x_i) \otimes 1 = \sum \phi(w_i y_j) z_j x_i = \sum \phi(w_i)\phi(y_j) z_j x_i = \sum w_{iV} y_{jV} \otimes w_{iA} y_{jA} z_j x_i = \sum w_{iV} f(\sum y_j \otimes z_j) \otimes w_{iA} x_i = f(\sum w_i \otimes x_i) f(\sum y_j \otimes z_j) \otimes 1$.

□

3.4. Definition: *Let L and H be Hopf algebras. We say that an algebra A is an L-H-bigalois extension of k, if A is both a left L-Galois extension of k and a right H-Galois extension of k such that the two comodule structures make it an L-H-bicomodule.*

3.5. Theorem: *Let H be a Hopf algebra and A a faithfully flat right H-Galois extension of k. Then $L := L(A, H)$ is a Hopf algebra. The comultiplication, counit and antipode of L are given by*

$$\begin{aligned}
\Delta(\sum x_i \otimes y_i) &= \sum x_{i(0)} \otimes \ell_j(x_{i(1)}) \otimes r(x_{i(1)}) \otimes y_i \\
\varepsilon(\sum x_i \otimes y_i) &= \sum x_i y_i \in A^{\mathrm{co}\,H} = k \\
S(\sum x_i \otimes y_i) &= \sum y_{i(0)} \otimes \ell_j(y_{i(1)}) x_i r(y_{i(1)}),
\end{aligned}$$

respectively.

A is a L-H-bigalois extension of k. For any bialgebra B and left B-comodule structure ϕ on A making A a B-H-bigalois extension of k, there is a unique isomorphism $f : L \to B$ of bialgebras such that $\phi = (f \otimes A)\delta'$.

PROOF: The algebra map $(L\otimes\delta')\delta' : A\to L\otimes L\otimes A$ corresponds to an algebra map $\Delta : L\to L\otimes L$ given by

$$\begin{aligned}\Delta(\sum x_i\otimes y_i)\otimes 1 &= \sum(L\otimes\delta')\delta'(x_i)y_i\\ &= \sum x_{i(0)}\otimes \ell_j(x_{i(1)})\otimes\delta'(r_j(x_{i(1)}))y_i\\ &= \sum x_{i(0)}\otimes\ell_j(x_{i(1)})\otimes r_j(x_{i(1)})\otimes y_i\otimes 1\end{aligned}$$

By the same reasoning as in [17], Δ is coassociative and L has a counit. By construction, δ' makes A a left L-comodule algebra. δ' being H-colinear means that A is thus a bicomodule algebra.

The Galois map $\kappa_\ell : A\otimes A\to L\otimes A$ is given by $\kappa_\ell(x\otimes y)=\sum x_{(0)}\otimes \ell_i(x_{(1)})\otimes r_i(x_{(1)})y$ and thus coincides with the isomorphism (2.6). Given any bialgebra B and left B-comodule algebra structure ϕ on A making A a B-H-bigalois extension of k, there is, by 3.3, a unique algebra map $f : L\to B$ with $\phi=(f\otimes A)\delta'$. It is easy to prove using the universal property of L that f is a coalgebra map (see [17] for a similar proof). Let $\kappa'_\ell : A\otimes A\to B\otimes A$ be the canonical map associated with the B-comodule algebra structure ϕ. We have $\kappa'_\ell=(f\otimes A)\kappa_\ell$, and since κ_ℓ and κ'_ℓ are isomorphisms, so is f.

By [13] we know that that L is a Hopf algebra; it remains to show that the antipode of L has the claimed form. Since L has an antipode S_L, the algebra inclusion $i : L\to A\otimes A^{\mathrm{op}}$ is convolution invertible with inverse iS_L. It is therefore sufficient to check that

$$\hat{S}(\sum x_i\otimes y_i)=\sum y_{i(0)}\otimes\ell_j(y_{i(1)})x_ir(y_{i(1)})$$

defines a left convolution inverse $\hat{S} : L\to A\otimes A^{\mathrm{op}}$ for i.

$$\begin{aligned}&\nabla_{A\otimes A^{\mathrm{op}}}(\hat{S}\otimes i)\Delta\left(\sum x_i\otimes y_i\right)=\nabla(\hat{S}\otimes i)\left(\sum x_{i(0)}\otimes\ell_j(x_{i(1)})\otimes r_j(x_{i(1)})\otimes y_i\right)\\ &=\nabla\left(\sum \ell_j(x_{i(1)})_{(0)}\otimes\ell_k(\ell_j(x_{i(1)})_{(1)})x_{i(0)}r_k(\ell_j(x_{i(1)})_{(1)})\otimes r_j(x_{i(1)})\otimes y_i\right)\\ &=\sum\ell_j(x_{i(2)})r_j(x_{i(2)})\otimes y_i\ell_k(S(x_{i(1)}))x_{i(0)}r_k(S(x_{i(1)}))\\ &=1\otimes\sum y_i\ell_k(S(x_{i(1)}))x_{i(0)}r_k(S(x_{i(1)}))=1\otimes\sum y_{i(0)}\ell_k(y_{i(1)})x_ir_k(y_{i(1)})\\ &=1\otimes\sum x_iy_i=1\otimes\varepsilon(\sum x_i\otimes y_i)\end{aligned}$$

□

The point in which our construction of $L(A,H)$ deviates the most from that in [22] is the form of the antipode. The antipode for the commutative case treated in [22] is simply induced by switching tensorands in $A\otimes A$, which is a colinear map if H is commutative. In fact the antipode given in Theorem 3.5 is a natural generalization of the commutative case. Recall that a Yetter-Drinfel'd module $V\in\mathcal{YD}^H_H$ is a right H-module and H-comodule satisfying the compatibility condition

$$v_{(0)}\leftharpoonup h_{(1)}\otimes v_{(1)}h_{(2)}=(v\leftharpoonup h_{(2)})_{(0)}\otimes h_{(1)}(v\leftharpoonup h_{(2)})_{(1)}$$

for all $v\in V$ and $h\in H$, where $\leftharpoonup$ denotes the H-module structure. Yetter-Drinfel'd modules were introduced in [23]. Their most important property is that the category $\mathcal{YD}^H_H$ is prebraided with prebraiding defined by

$$\sigma: V\otimes W\ni v\otimes w\mapsto w_{(0)}\otimes v\leftharpoonup w_{(1)}\in W\otimes V$$

for $V,W\in\mathcal{YD}^H_H$. We will not need the axioms of a prebraiding, all we need is the fact that σ is colinear, and an isomorphism with $\sigma^{-1}(w\otimes v)=v\leftharpoonup S^{-1}(w_{(1)})\otimes w_{(0)}$ in case H has bijective antipode. Before the axioms of a Yetter-Drinfel'd module had ben formulated, it was proved in [4] that every H-Galois extension A of k is in a natural way a Yetter-Drinfel'd module, the module structure being the Miyashita-Ulbrich action $a\leftharpoonup h=\sum \ell_i(h)ar_i(h)$ (this is in fact only a special case of [4, (3.4)], see also [1, Prop.2.3.2] and [12, Sec.3]).

3.6. Corollary: *Let H be a Hopf algebra and A a faithfully flat H-Galois extension of k. Put $L=L(A,H)$. Then we have*

$$S_L=(\sigma_{AA})^{\mathrm{co}\,H}$$

where σ is the prebraiding of $\mathcal{YD}^H_H$, and $A\in\mathcal{YD}^H_H$ via the Miyashita-Ulbrich action. In particular the antipode of L is bijective if the antipode of H is.

3.7. Definition and Remark: *Let A be a faithfully flat left H-Galois extension of k. Recall that this means that A^{op} is a right H^{opcop}-Galois extension of k. We define $R(A,H)=L(A^{\mathrm{op}},H^{\mathrm{opcop}})^{\mathrm{opcop}}$. Thus $R(A,H)$ is the unique up to isomorphism Hopf algebra making A an H-$R(A,H)$-bigalois extension. As a k-module we have $R(A,H)={}^{\mathrm{co}\,H}(A\otimes A)$, which is a subalgebra of $A^{\mathrm{op}}\otimes A$.*

The two constructions $R(-,-)$ and $L(-,-)$ are inverse to each other in the sense that

$$R(A, L(A, R)) \cong R \qquad L(A, R(A, L)) \cong L$$

hold for a faithfulla flat right R-Galois extension A/k and a faithfully flat left L-Galois extension A/k, respectively.

3.8. Remark: *If H is cocommutative and A is a faithfully flat right H-Galois extension of k, then $L(A, H) \cong H$.*

Indeed, H being cocommutative, A is also a left H-Galois extension by $\delta_\ell(a) = a_{(1)} \otimes a_{(0)}$ (bijectivity of κ_ℓ follows from bijectivity of the antipode, see [10, (1.2)]), and in this way clearly H-H-bigalois.

Let H be a k-flat Hopf algebra. A 2-cocycle $\sigma : H \otimes H \to k$ is a map satisfying

$$\sigma(f_{(1)}, g_{(1)})\sigma(f_{(2)}g_{(2)}, h) = \sigma(g_{(1)}, h_{(1)})\sigma(f, g_{(2)}h_{(2)})$$

and $\sigma(1, h) = \sigma(h, 1) = \varepsilon(h)$ for all $f, g, h \in H$.

Given a (convolution) invertible 2-cocycle σ, Doi [3] constructs a twisted Hopf algebra H^σ which is isomorphic to H as a coalgebra with multiplication defined by

$$g \cdot h = \sigma(g_{(1)}, h_{(1)})g_{(2)}h_{(2)}\sigma^{-1}(g_{(3)}, h_{(3)}).$$

On the other hand, using a 2-cocycle σ on H one can construct the crossed product algebra $k\#_\sigma H$ (with the trivial H-action on k), which is an H-comodule algebra isomorphic to H as a right H-comodule, with multiplication

$$(1\#g)(1\#h) = \sigma(g_{(1)}, h_{(1)})\#g_{(2)}h_{(2)}$$

For a right H-comodule algebra A with $A^{\mathrm{co}\,H} = k$, the following are equivalent: H is H-Galois with a normal basis, that is $A \cong H$ as H-comodules; A is cleft, that is, there is a right H-colinear and convolution invertible map $H \to A$; $A \cong k\#_\sigma H$ for a convolution invertible 2-cocycle $\sigma : H \otimes H \to k$. We refer to sections 7 and 8 of [11] for the results just compiled.

3.9. Theorem: *Let H be a k-flat Hopf algebra and A a cleft right H-Galois extension of k. Then A is a cleft left $L(A, H)$-extension of k. If $A \cong k\#_\sigma H$, then $L(A, H) \cong H^\sigma$, and $A \cong H^\sigma\#_\sigma k$ as a left H^σ-comodule algebra.*

PROOF: We can make $k\#_\sigma H$ a left H-comodule via $\delta_\ell(1\#h) = h_{(1)}\otimes 1\#h_{(2)}$. It is in this way a left H^σ-comodule algebra because

$$\begin{aligned}\delta_\ell((1\#g)(1\#h)) &= \delta_\ell(\sigma(g_{(1)}, h_{(1)})\#g_{(2)}h_{(2)}) \\ &= \sigma(g_{(1)}, h_{(1)})g_{(2)}h_{(2)} \otimes 1\#g_{(3)}h_{(3)} = g_{(1)} \cdot h_{(1)} \otimes \sigma(g_{(2)}, h_{(2)})\#g_{(3)}h_{(3)} \\ &= g_{(1)} \cdot h_{(1)} \otimes (1\#g_{(2)})(1\#h_{(2)})\end{aligned}$$

The obvious left H^σ-colinear isomorphism $\psi : H^\sigma\#_\sigma k \to k\#_\sigma H$ is also an isomorphism of algebras:

$$\begin{aligned}\psi(g\#1)\psi(h\#1) = (1\#g)(1\#h) &= \sigma(g_{(1)}, h_{(1)})\#g_{(2)}h_{(2)} \\ &= \psi(\sigma(g_{(1)}, h_{(1)})g_{(2)}h_{(2)}\#1) = g_{(1)} \cdot h_{(1)}\#\sigma(g_{(2)}, h_{(2)})\end{aligned}$$

Now since the crossed product $H^\sigma\#_\sigma k$ is left H^σ-Galois, we are done. $\square$

The referee pointed out that one can describe the resulting isomorphism $f : (A \otimes A)^{\mathrm{co}\, H} = L(A, H) \to H^\sigma$ explicitly as follows: We have

$$f(\sum 1\#g_i \otimes 1\#h_i) = \sum g_{i(1)}\sigma(g_{i(2)}, h_i)$$

for $\sum 1\#g_i \otimes 1\#h_i \in (A \otimes A)^{\mathrm{co}\, H}$ and

$$f^{-1}(h) = 1\#h_{(1)} \otimes 1\#S(h_{(2)})\sigma^{-1}(S(h_{(3)}), h_{(4)}).$$

for $h \in H^\sigma$. In fact, the form of f can be deduced directly from Lemma 3.2:

$$\begin{aligned}f(\sum 1\#g_i \otimes 1\#h_i) \otimes 1_A &= \sum (\delta_\ell(1\#g_i))\,(1\#h_i) \\ &= \sum g_{i(1)} \otimes (1\#g_{i(2)})(1\#h_i) \\ &= \sum g_{i(1)} \otimes \sigma(g_{i(2)}, h_{i(1)})\#g_{i(3)}h_{i(2)} \\ &= \sum g_{i(1)}\sigma(g_{i(2)}, h_i) \otimes 1_A\end{aligned}$$

To check the form of the inverse of f, we use the formula $\sigma(h_{(1)}, S(h_{(2)}))\sigma^{-1}(S(h_{(3)}), h_{(4)}) = \varepsilon(h)$ for $h \in H$, which occurs in the proof of [11, Prop.7.2.7]. It is straightforward to check that $1\#h_{(1)} \otimes 1\#S(h_{(2)})\sigma^{-1}(S(h_{(3)}), h_{(4)}) \in (A \otimes A)^{\mathrm{co}\, H}$, and

$$\begin{aligned}&f(1\#h_{(1)} \otimes 1\#S(h_{(2)})\sigma^{-1}(S(h_{(3)}), h_{(4)})) \\ &\qquad = h_{(1)}\sigma(h_{(2)}, S(h_{(3)}))\sigma^{-1}(S(h_{(4)}), h_{(5)}) = h\end{aligned}$$

3.10. Remark: *Let A be a faithfully flat H-Galois extension of k. Assume H is a Hopf algebra with bijective antipode. Then so is $L := L(A,H)$, and we can define $T = T(A,H) = L^{\mathrm{cop}}$, which is again a Hopf algebra. A is a right T-Galois extension of k, and the right H and T-comodule structures make it an $H \otimes T$-comodule. Observe that T is the unique up to isomorphism Hopf algebra making A a right T-Galois extension and an $H \otimes T$-comodule algebra. We conclude that the "operation" T is involutive in the sense that $T(A, T(A,H)) \cong H$.*

If all algebras considered are commutative, then $T(A,H) \cong L(A,H) \cong \mathcal{L}$ via the antipode, so we recover the fact from [6] that the construction $\mathcal{L}$ from [22] is involutive.

Let H be a Hopf algebra. We define $\mathrm{Gal}(H)$ to be the set of isomorphism classes of faithfully flat right H-Galois extensions of k. For another Hopf algebra L we define $\mathrm{BiGal}(L,H)$ to be the set of isomorphism classes of faithfully flat L-H-bigalois extensions of k. Note that although the Hopf algebra L in an L-H-bigalois extension A is determined uniquely up to isomorphism by the class of A in $\mathrm{Gal}(H)$, this does not necessarily determine the class of A in $\mathrm{BiGal}(L,H)$, as we shall see in the next Lemma. We define

$$\mathrm{CoInn}(L) := \{f \in \mathrm{Aut}(L) | \exists \phi \in \mathrm{Alg}(L,k) : f(\ell) = \phi(\ell_{(1)})\ell_{(2)}\phi^{-1}(\ell_{(3)})\}$$

to be the set of coinner automorphisms of the Hopf algebra L. (Note that an algebra map $\phi : L \to k$ is necessarily convolution invertible with $\phi^{-1} = \phi S_L$.) It is easy to check that $\mathrm{CoInn}(L)$ is a normal subgroup of the group $\mathrm{Aut}_{\mathrm{Hopf}}(L)$ of Hopf algebra automorphisms of L. Further, we denote by

$$\mathrm{CoOut}(L) := \mathrm{Aut}_{\mathrm{Hopf}}(L)/\mathrm{CoInn}(L)$$

the group of co-outer automorphisms of L.

Let $f : C \to D$ be a coalgebra homomorphism and V a left C-comodule. We denote by ${}^fV$ the left D-comodule V with the structure defined by $V \ni v \mapsto f(v_{(-1)}) \otimes v_{(0)} \in D \otimes V$; the symbol V^f for a right C-comodule V is defined similarly.

3.11. Lemma: *Let L and H be Hopf algebras such that* $\mathrm{BiGal}(L,H)$ *is nonempty. The group* $\mathrm{CoOut}(L)$ *acts freely on* $\mathrm{BiGal}(L,H)$*. The orbit of* *the class of a bigalois extension A in* $\mathrm{BiGal}(L,H)$ *consists of the classes in* $\mathrm{BiGal}(L,H)$ *of those bigalois extensions B such that $A \cong B$ as right H-Galois extensions of k.*

PROOF: Clearly $\mathrm{Aut}_{\mathrm{Hopf}}(L)$ acts on $\mathrm{BiGal}(L,H)$ via $f \rightharpoonup A = {}^fA$. Assume we have $f(\ell) = \phi(\ell_{(1)})\ell_{(2)}\phi^{-1}(\ell_{(3)})$ for $\phi \in \mathrm{Alg}(L,k)$. To establish that we have an action of $\mathrm{CoOut}(L)$ on $\mathrm{BiGal}(L,H)$, we have to show that f acts as the identity on $\mathrm{BiGal}(L,H)$. Let A be a faithfully flat L-H-bigalois extension of k. Define $g : {}^fA \to A$ by $g(a) = \phi(a_{(-1)})a_{(0)}$. Clearly g is an algebra automorphism of A and right H-colinear. Let δ_ℓ denote the original left L-coaction on A, and put $\delta_f = (f \otimes A)\delta_\ell$. We have

$$\begin{aligned}\delta_\ell g(a) = \phi(a_{(-2)})a_{(-1)} \otimes a_{(0)} &= \phi(a_{(-4)})a_{(-3)}\phi^{-1}(a_{(-2)}) \otimes \phi(a_{(-1)})a_{(0)} \\ &= f(a_{(-1)}) \otimes g(a_{(0)}) = (L \otimes g)\delta_f(a)\end{aligned}$$

showing that g is left L-colinear, and thus ${}^fA \cong A$ as bigalois extensions.

To prove freeness of the action, assume that we have $f \in \mathrm{Aut}_{\mathrm{Hopf}}(L)$, a faithfully flat L-H-bigalois extension A of k and an isomorphism $g : {}^fA \to A$ of bigalois extensions. By the universal property of L (which is isomorphic to $L(A,H)$), we find a unique algebra map $\phi : L \to k$ with $g(a) = \phi(a_{(-1)})a_{(0)}$ for all $a \in A$. To verify $f(\ell) = \phi(\ell_{(1)})\ell_{(2)}\phi^{-1}(\ell_{(3)})$ for all $\ell \in L$, it is, by bijectivity of the left Galois map κ_ℓ, bijectivity of g and faithful flatness of A, sufficient to do the following calculation for $x, y \in A$:

$$\begin{aligned} f(x_{(-1)}) \otimes g(x_{(0)}y) &= f(x_{(-1)}) \otimes g(x_{(0)})g(y) \\ &= g(x)_{(-1)} \otimes g(x)_{(0)}g(y) \\ &= \phi(x_{(-2)})x_{(-1)} \otimes x_{(0)}g(y) \\ &= \phi(x_{(-4)})x_{(-3)}\phi^{-1}(x_{(-2)}) \otimes \phi(x_{(-1)})x_{(0)}g(y) \\ &= \phi(x_{(-3)})x_{(-2)}\phi^{-1}(x_{(-1)}) \otimes g(x_{(0)})g(y) \\ &= \phi(x_{(-3)})x_{(-2)}\phi^{-1}(x_{(-1)}) \otimes g(x_{(0)}y) \end{aligned}$$

The statement about orbits is clear by the uniqueness statement in Theorem 3.5. □

4 A Harrison Groupoid

The cotensor product defines a composition of bigalois extensions making them the morphisms of a groupoid. Before we work out the details of this statement, let us indicate how this composition generalizes the multiplication in the Harrison group of a finite abelian group [8].

Let $\pi : F \to G$ be a homomorphism of finite groups and E a commutative F-Galois extension of k. The G-Galois extension π^*E of k is defined by

$$\pi^*E = \mathrm{Map}_\pi(G, E) = \{\alpha : G \to E | \forall f \in F, g \in G : \ x(\pi(f)g) = fx(g)\}.$$

If G and G' are finite groups, A is a G-Galois extension and B is a G'-Galois extension of k, then $A \otimes B$ is a $G \times G'$-Galois extension of k. If G is finite abelian then multiplication is a homomorphism $\mu : G \times G \to G$ and we can form

$$A \cdot B = \mu^*(A \otimes B)$$

for two commutative G-Galois extensions A and B of k. This defines a group structure on the set of all isomorphism classes of commutative G-Galois extensions of k, which is called the Harrison group; we denote it by $\mathrm{Har}(G, k)$.

Let G be a finite abelian group. Then a G-Galois extension of commutative rings $k \subset A$ is the same as an H-Galois extension of k for the dual Hopf algebra $H = (kG)^*$ of the group algebra of G. Let B be another G-Galois extension of k. Then the cotensor product is

$$\begin{aligned} A \underset{H}{\square} B &= \{\sum x_i \otimes y_i \in A \otimes B | \forall g \in G : \ \sum gx_i \otimes y_i = \sum x_i \otimes gy_i\} \\ &= \{\xi \in A \otimes B | \forall g \in G : (g, 1)\xi = (1, g)\xi\} \end{aligned}$$

where the last line uses the action of $G \times G$ on $A \otimes B$. It follows that

$$\begin{aligned} \alpha : A \cdot B &\to A \underset{H}{\square} B \\ \phi &\mapsto \phi(1) \end{aligned}$$

is an isomorphism with inverse defined by $\alpha^{-1}(\xi)(g) = (g, 1)\xi = (1, g)\xi$ for $\xi \in A \underset{H}{\square} B$ and $g \in G$.

A generalization of the Harrison group to a group $\mathcal{H}(H,k)$ of all H-Galois extensions of k where H is a cocommutative Hopf algebra finitely generated projective over k has appeared in [5]. We omit the details of showing that the group law agrees with the one discussed below.

4.1. ***Proposition:*** *Let L, H and R be Hopf algebras, let A be a faithfully flat L-H-bigalois extension of k, and let B be a faithfully flat H-R-bigalois extension of k. Then $A \underset{H}{\square} B$ is a faithfully flat L-R-bigalois extension of k.*

PROOF: A is a faithfully flat k-algebra, and the left A-module

$$A \otimes (A \underset{H}{\square} B) \cong (A \otimes A) \underset{H}{\square} B \cong (A \otimes H) \underset{H}{\square} B \cong A \otimes B$$

is faithfully flat, hence $A \underset{H}{\square} B$ is k-faithfully flat. Clearly, $A \underset{H}{\square} B$ is an L-R-bicomodule subalgebra of $A \otimes B$. The canonical map $\kappa_r : (A \underset{H}{\square} B) \otimes (A \underset{H}{\square} B) \to (A \underset{H}{\square} B) \otimes R$ can be written as the composition

$$(A \underset{H}{\square} B) \otimes (A \underset{H}{\square} B) \xrightarrow{\xi} A \underset{H}{\square} (B \otimes B) \cong A \underset{H}{\square} (B \otimes R) \cong (A \underset{H}{\square} B) \otimes R$$

in which

$$\xi : (A \underset{H}{\square} B) \otimes (A \underset{H}{\square} B) \to A \underset{H}{\square} (B \otimes B)$$
$$\left(\sum w_i \otimes x_i\right) \otimes \left(\sum y_j \otimes z_j\right) \mapsto \sum w_i y_j \otimes (x_i \otimes z_j)$$

is an isomorphism as in [18, (1.4)]. Consequently κ_r is an isomorphism. The proof that $A \underset{H}{\square} B$ is left L-Galois is analogous. $\square$

4.2. ***Definition:*** *The category $\mathcal{H}$ has objects all faithfully flat k-Hopf algebras. The morphisms in $\mathcal{H}$ are isomorphism classes of faithfully flat bigalois extensions of k, $\mathrm{Mor}_{\mathcal{H}}(L,R) := \mathrm{BiGal}(L,R)$, with the composition given by cotensor product as in the preceding proposition.*

The fact that composition is associative follows from faithful flatness of the bigalois extensions in consideration, and the remark concluding Section 2. The identity in $\mathrm{Mor}_{\mathcal{H}}(H,H)$ is of course H.

4.3. ***Theorem:*** *The category $\mathcal{H}$ is a groupoid.*

PROOF: Observe that $\mathcal{H}$ has an involutive self-duality that assigns to an object H the Hopf algebra H^{opcop}, and to an L-R-bigalois extension of k the R^{opcop}-L^{opcop}-bigalois extension A^{op}. It is therefore sufficient to show that each morphism in $\mathcal{H}$ has a one-sided inverse.

Let A be a faithfully flat L-H-bigalois extension of k.

Put $A^{-1} := (H \otimes A)^{\mathrm{co}\,H}$, where the right comodule structure on $H \otimes A$ is the codiagonal one. Being the coinvariant subcomodule of a right A-faithfully flat Hopf module in $\mathcal{M}_A^H$, the k-module A^{-1} is faithfully flat. It is easy to see that A^{-1} is a left H-subcomodule algebra of $H \otimes A^{\mathrm{op}}$ (the left H-comodule structure of A^{-1} is given by $\delta_\ell\left(\sum h_i \otimes a_i\right) = \sum h_{i(1)} \otimes h_{i(2)} \otimes a_i$). The Galois map for the left H-comodule algebra A^{-1} is given by

$$\kappa_\ell\left(\sum g_i \otimes x_i \otimes \sum h_j \otimes y_j\right) = \sum g_{i(1)} \otimes g_{i(2)} h_j \otimes y_j x_i.$$

We claim that κ_ℓ is an isomorphism with inverse defined by

$$\overline{\kappa}_\ell(g \otimes \sum h_i \otimes a_i) = \sum g_{(1)} \otimes r_j(Sg_{(2)}) \otimes S(g_{(3)}) h_i \otimes a_i \ell_j(Sg_{(2)})$$

We have to check first that $\overline{\kappa}_\ell$ is well defined, that is that it has its image in $A^{-1} \otimes A^{-1} \subset (H \otimes A) \otimes (H \otimes A)$. We have

$$\begin{aligned}\sum \delta_r(g_{(1)} \otimes r_j(Sg_{(2)})) &\otimes S(g_{(3)}) h_i \otimes a_i \ell_j(Sg_{(2)}) \\ &= g_{(1)} \otimes r_j(Sg_{(4)}) \otimes g_{(2)} S(g_{(3)}) \otimes S(g_{(5)}) h_i \otimes a_i \ell_j(Sg_{(4)}) \\ &= g_{(1)} \otimes r_j(Sg_{(2)}) \otimes 1 \otimes S(g_{(3)}) h_i \otimes a_i \ell_j(Sg_{(2)})\end{aligned}$$

and

$$\begin{aligned}&\sum g_{(1)} \otimes r_j(Sg_{(2)}) \otimes \delta_r(S(g_{(3)}) h_i \otimes a_i \ell_j(Sg_{(2)})) \\ &= g_{(1)} \otimes r_j(Sg_{(2)}) \otimes S(g_{(5)}) h_{i(1)} \otimes a_{i(0)} \ell_j(Sg_{(2)}) \otimes S(g_{(4)}) h_{i(2)} a_{i(1)} S^2(g_{(3)}) \\ &= g_{(1)} \otimes r_j(Sg_{(2)}) \otimes S(g_{(5)}) h_i \otimes a_i \ell_j(Sg_{(2)}) \otimes S(g_{(4)}) S^2(g_{(3)}) \\ &= g_{(1)} \otimes r_j(Sg_{(2)}) \otimes S(g_{(3)}) h_i \otimes a_i \ell_j(Sg_{(2)}) \otimes 1\end{aligned}$$

Next, κ_ℓ and $\overline{\kappa}_\ell$ are inverse to each other, since

$$\begin{aligned}\kappa_\ell \overline{\kappa}_\ell\left(g \otimes \sum h_i \otimes a_i\right) &= \kappa_\ell\left(\sum g_{(1)} \otimes r_j(Sg_{(2)}) \otimes S(g_{(3)}) h_i \otimes a_i \ell_j(Sg_{(2)})\right) \\ &= \sum g_{(1)} \otimes g_{(2)} S(g_{(4)}) h_i \otimes a_i \ell_j(Sg_{(2)}) r_j(Sg_{(2)}) \\ &= \sum g_{(1)} \otimes g_{(2)} S(g_{(3)}) h_i \otimes a_i \\ &= \sum g \otimes h_i \otimes a_i\end{aligned}$$

and

$$
\begin{aligned}
\overline{\kappa}_\ell \kappa_\ell \left(\sum g_i \otimes x_i \otimes \sum h_j \otimes y_j\right)
&= \overline{\kappa}_\ell \left(\sum g_{i(1)} \otimes g_{i(2)} h_j \otimes y_j x_i\right)\\
&= \sum g_{i(1)} \otimes r_k(S g_{i(2)}) \otimes S(g_{i(3)}) g_{i(4)} h_j \otimes y_j x_i \ell_k(S g_{i(2)})\\
&= \sum g_{i(2)} \otimes r_k(S g_{i(2)}) \otimes h_j \otimes y_j x_i \ell_k(S g_{i(2)})\\
&\stackrel{*}{=} \sum g_{i(1)} \otimes x_i \ell_k(S g_{i(2)}) r_k(S g_{i(2)}) \otimes h_j \otimes y_j\\
&= \sum g_i \otimes x_i \otimes h_j \otimes y_j
\end{aligned}
$$

where the starred equality uses the fact that for $\sum g_i \otimes x_i \in A^{-1}$ we have

$$\sum g_{i(1)} \otimes r_k(S g_{i(2)}) \otimes x_i \ell_k(S g_{i(2)}) \in H \otimes A \otimes A^{\mathrm{co}\, H} = H \otimes A \otimes k$$

since

$$
\begin{aligned}
\sum g_{i(1)} \otimes r_k(S g_{i(2)}) \otimes \delta_r(x_i \ell_k(S g_{i(2)}))
&= \sum g_{i(1)} \otimes r_k(S g_{i(2)}) \otimes x_{i(0)} \ell_k(S g_{i(2)}) \otimes x_{i(1)} S^2(g_{i(3)})\\
&= \sum g_{i(1)} \otimes r_k(S g_{i(2)}) \otimes x_{i(0)} \ell_k(S g_{i(2)}) \otimes x_{i(1)} S(x_{i(2)})\\
&= \sum g_{i(1)} \otimes r_k(S g_{i(2)}) \otimes x_i \ell_k(S g_{i(2)}) \otimes 1
\end{aligned}
$$

(we have used that $\sum g_i \otimes x_{i(0)} \otimes x_{i(1)} = \sum g_{i(1)} \otimes x_i \otimes S(g_{i(2)})$ similarly to [14, Lem.3.1]).

Clearly A^{-1} represents a morphism in $\mathrm{Mor}_{\mathcal{H}}(H, R)$ for $R = R(A, H)$, and $A \underset{H}{\square} A^{-1}$ is an L-R-bigalois extension of k. We can assume that $L = L(A, H)$. We have an isomorphism

$$
\begin{aligned}
\phi : A \underset{H}{\square} (H \otimes A)^{\mathrm{co}\, H} &\to (A \otimes A)^{\mathrm{co}\, H}\\
\sum x_i \otimes \sum h_{ij} \otimes y_{ij} &\mapsto \sum x_i \varepsilon(h_{ij}) \otimes y_{ij}
\end{aligned}
$$

with inverse $\phi^{-1}\left(\sum x_i \otimes y_i\right) = \sum x_{i(0)} \otimes x_{i(1)} \otimes y_i$, which we claim to be an isomorphism of left L-comodule algebras $A \underset{H}{\square} A^{-1} \cong L$. It is easy to see that

ϕ is an algebra homomorphism, and

$$\begin{aligned}\delta_\ell\phi^{-1}\left(\sum x_i\otimes y_i\right) &= \delta_\ell\left(\sum x_{i(0)}\otimes x_{i(1)}\otimes y_i\right)\\ &= \sum x_{i(0)}\otimes \ell_j(x_{i(1)})\otimes r_j(x_{i(1)}\otimes x_{i(2)}\otimes y_i)\\ &= \sum x_{i(0)}\otimes \ell_j(x_{i(1)})\otimes \phi^{-1}(r_j(x_{i(1)})\otimes y_i)\\ &= (L\otimes\phi^{-1})\Delta_L\left(\sum x_i\otimes y_i\right).\end{aligned}$$

It follows that $A \mathop{\square}\limits_H A^{-1}$ is an L-L-bigalois extension isomorphic to the L-L-bigalois extension L, in particular $R\cong L$ and we can endow A^{-1} with a right L-comodule structure making it an H-L-bigalois extension with $A \mathop{\square}\limits_H A^{-1}\cong L$ as L-L-bigalois extensions. We have found a one-sided inverse for the morphism A in $\mathcal{H}$, and the proof is complete. $\square$

4.4. ***Remark:*** *If we make the additional assumption that H has bijective antipode, then $A^{-1}\cong A^{\mathrm{op}}$ with left H-comodule structure*

$$A^{\mathrm{op}}\ni a\mapsto S^{-1}(a_{(1)})\otimes a_{(0)}\in H\otimes A$$

4.5. ***Corollary:*** *The faithfully flat bigalois extensions of k having a normal basis (as left or right Hopf-Galois extensions, see 3.9) form a subgroupoid $\mathcal{N}$ of $\mathcal{H}$.*

Proof: If A is a cleft L-H-bigalois extension of k and B is a cleft H-R-bigalois extension of k, then $A\cong H$ as a right H-comodule, and $B\cong R$ as a right R-comodule, so that

$$A \mathop{\square}\limits_H B\cong H \mathop{\square}\limits_H B\cong B\cong R$$

as right R-comodules. Moreover

$$A^{-1}=(H\otimes A)^{\mathrm{co}\,H}\cong(H\otimes H)^{\mathrm{co}\,H}\cong H$$

The last isomorphism maps $\sum g_i\otimes h_i\in(H\otimes H)^{\mathrm{co}\,H}$ to $\sum g_i\varepsilon(h_i)$, and its inverse maps $h\in H$ to $h_{(1)}\otimes S(h_{(2)})$, which is coinvariant under the diagonal coaction. The resulting isomorphism $A^{-1}\cong H$ is clearly left H-colinear, so that A^{-1} has a normal basis. $\square$

4.6. ***Corollary:*** *The commutative faithfully flat bigalois extensions of k form a subgroupoid $\mathcal{H}_c \subset \mathcal{H}$.*

The proof is obvious. All objects of $\mathcal{H}_c$ are clearly commutative.

In the case that H is cocommutative, for example $H = (kG)^*$ is the dual Hopf algebra of the group algebra of a finite commutative group, $\mathrm{BiGal}(H,H)$ is a group, and we can regard $\mathrm{Gal}(H)$ as the subgroup of $\mathrm{BiGal}(H,H)$ consisting of the isomorphism classes of all bigalois extensions A satisfying $a_{(0)} \otimes a_{(1)} = a_{(0)} \otimes a_{(-1)}$ for all $a \in A$ (which makes sense since H is cocommutative). We denote composition in $\mathrm{Gal}(H)$ by a dot. The following lemma makes the relation between the groups $\mathrm{Gal}(H)$ and $\mathrm{BiGal}(H,H)$ more precise.

4.7. ***Lemma:*** *Assume that H is a cocommutative Hopf algebra. Then $\mathrm{Aut}_{\mathrm{Hopf}}(H)$ acts on $\mathrm{Gal}(H)$ on the right by $A \leftharpoonup f := A^{f^{-1}}$ and we have an isomorphism of $\mathrm{BiGal}(H,H)$ with a semidirect product of groups*

$$\begin{aligned}\Phi : \mathrm{Aut}_{\mathrm{Hopf}}(H) \ltimes \mathrm{Gal}(H) &\longrightarrow \mathrm{BiGal}(H,H)\\ (f,A) &\longmapsto {}^{f}A\end{aligned}$$

Proof: The fact that Φ is a bijection follows from Lemma 3.11. The computation

$$\begin{aligned}\Phi(f,A)\Phi(g,B) &= {}^{f}A \mathop{\square}_{H} {}^{g}B\\ &\cong {}^{f}A^{gg^{-1}} \mathop{\square}_{H} {}^{g}B\\ &\cong ({}^{f}A^{g^{-1}})^{g} \mathop{\square}_{H} {}^{g}B\\ &\cong {}^{f}A^{g^{-1}} \mathop{\square}_{H} B\\ &\cong {}^{fg}({}^{g^{-1}}A^{g^{-1}} \mathop{\square}_{H} B)\\ &\cong \Phi(fg, (A \leftharpoonup g) \cdot B))\end{aligned}$$

shows Φ to be an isomorphism of groups. $\square$

5 Relations to Morita Theory

In this section we will show that the Hopf algebra $L(A,H)$ constructed from an H-Galois extension A of k in section 3 has an interpretation in terms of representation theory of Hopf algebras and monoidal categories.

Let $\mathcal{C}$ and $\mathcal{D}$ be two monoidal categories. For simplicity assume that the tensor products are strictly associative, $X \otimes (Y \otimes Z) = (X \otimes Y) \otimes Z$. Recall that a monoidal functor $\mathcal{F} = (\mathcal{F}, \xi)$ from $\mathcal{C}$ to $\mathcal{D}$ consistst of an ordinary functor $\mathcal{F} : \mathcal{C} \to \mathcal{D}$, and, as an additional structure, a functorial isomorphism $\xi : \mathcal{F}(X) \otimes \mathcal{F}(Y) \to \mathcal{F}(X \otimes Y)$ making

$$\begin{tikzcd} \mathcal{F}(X) \otimes \mathcal{F}(Y) \otimes \mathcal{F}(Z) \arrow[r, "\xi\otimes 1"] \arrow[d, "1\otimes\xi"'] & \mathcal{F}(X \otimes Y) \otimes \mathcal{F}(Z) \arrow[d, "\xi"'] \\ \mathcal{F}(X) \otimes \mathcal{F}(Y \otimes Z) \arrow[r, "\xi"] & \mathcal{F}(X \otimes Y \otimes Z) \end{tikzcd}$$

commute. A natural transformation $\phi : \mathcal{F} \to \mathcal{F}'$ between monoidal functors $(\mathcal{F}, \xi)$ and $(\mathcal{F}', \xi')$ is monoidal if the diagrams

$$\begin{tikzcd} \mathcal{F}(X) \otimes \mathcal{F}(Y) \arrow[r, "\xi"] \arrow[d, "\phi\otimes\phi"'] & \mathcal{F}(X \otimes Y) \arrow[d, "\phi"'] \\ \mathcal{F}'(X) \otimes \mathcal{F}'(Y) \arrow[r, "\xi"] & \mathcal{F}'(X \otimes Y) \end{tikzcd}$$

commute. It should be clear what we mean by a monoidal equivalence, and by a monoidal isomorphism of functors.

5.1. Definition ([19, p. 41–42]): *Let H be a k-flat Hopf algebra. Let ${}^H\mathcal{M}$ denote the category of left H-comodules.*

A fiber functor $\omega : {}^H\mathcal{M} \to \mathcal{M}_k$ is a faithful, monoidal, k-linear exact functor that preserves colimits.

Assume k is a field. Denote by ${}^H\mathcal{M}_f$ the category of finite dimensional left H-comodules. A fiber functor $\omega : {}^H\mathcal{M}_f \to \mathcal{M}_k$ is a k-linear exact monoidal functor.

It can be shown that all fiber functors on ${}^H\mathcal{M}_f$ take values in the category of finite dimensional vector spaces.

By [19, Prop. 2.2] restriction induces a category equivalence between the category of fiber functors on ${}^H\mathcal{M}$ and fiber functors on ${}^H\mathcal{M}_f$ (if k is a field), due to the finiteness theorems for comodules.

5.2. Theorem ([19, Thm. 1.2.]): *Let H be a Hopf algebra. There is a bijection between isomorphism classes of fiber functors $\omega : {}^H\mathcal{M} \to \mathcal{M}_k$ and isomorphism classes of faithfully flat right H-Galois extensions A/k. The functor $\omega_A : {}^H\mathcal{M} \to \mathcal{M}_k$ corresponding to a right H-Galois extension A is given by $\omega_A(V) = A \underset{H}{\square} V$. The H-Galois extension A_ω corresponding to a fiber functor $\omega : {}^H\mathcal{M} \to \mathcal{M}_k$ is given by $A = \omega(H)$.*

Of course, two fiber functors are considered isomorphic if they are isomorphic as *monoidal* functors.

The monoidal structure of the functor ω_A is given by the isomorphisms

$$\begin{aligned} \xi : (A \underset{H}{\square} V) \otimes (A \underset{H}{\square} W) &\to A \underset{H}{\square} (V \otimes W) \\ (\sum x_i \otimes v_i) \otimes (\sum y_j \otimes w_j) &\mapsto \sum x_i y_j \otimes v_i \otimes w_j \end{aligned}$$

Let $\mathcal{U} : {}^H\mathcal{M} \to \mathcal{M}_k$ denote the underlying functor. Then A_ω has the following universal property: There is a natural transformation $\rho : \omega \to A_\omega \otimes \mathcal{U}$ such that for all k-modules M and natural transformations $\phi : \omega \to M \otimes \mathcal{U}$ there is a unique map $f : A_\omega \to M$ such that $\phi = (f \otimes \mathcal{U})\rho$. In the case of $\omega = \omega_A$, the map $\rho_V : A \underset{H}{\square} V \to A \otimes V$ is the inclusion.

5.3. Definition: *Let $\mathcal{C}$ be a category and $\omega : \mathcal{C} \to \mathcal{M}_k$ a functor. A (left) coendomorphism object of ω is a k-module $\operatorname{coend}(\omega)$ together with a natural transformation $\delta^\omega : \omega \to \operatorname{coend}(\omega) \otimes \omega$ such that for any k-module and natural transformation $\phi : \omega \to M \otimes \omega$ there is a unique homomorphism $f : \operatorname{coend}(\omega) \to M$ such that $\phi = (f \otimes \omega)\delta^\omega$.*

A coendomorphism object does not necessarily exist, but if it does, it is a coalgebra, and the natural transformation δ^ω induces a functor $\mathcal{F} : \mathcal{C} \to$

${}^{\mathrm{coend}(\omega)}\mathcal{M}$. The coalgebra $\mathrm{coend}(\omega)$ is the universal one such that ω factors through a functor into ${}^{\mathrm{coend}(\omega)}\mathcal{M}$.

If H is a coalgebra and $\mathcal{U} : {}^H\mathcal{M} \to \mathcal{M}_k$ is the underlying functor, then $\mathrm{coend}(\mathcal{U}) \cong H$ (in particular, a coendomorphism object exists). If k is a field and $\mathcal{U} : {}^H\mathcal{M}_f \to \mathcal{M}_k$ is the underlying functor, then also $\mathrm{coend}(\mathcal{U}) \cong H$.

5.4. Theorem (The main results of [20]): *Assume k is a field. Let $\mathcal{C}$ be a k-linear abelian monoidal category and let $\omega : \mathcal{C} \to \mathcal{M}_k$ be a faithful exact k-linear monoidal functor with values in the category of finite dimensional vector spaces. Then $B = \mathrm{coend}(\omega)$ exists, and it has a unique bialgebra structure such that the functor $\mathcal{F} : \mathcal{C} \to {}^{\mathrm{coend}(\omega)}\mathcal{M}$ satisfying $\mathcal{U}\mathcal{F} = \omega$ is monoidal. The functor $\mathcal{F}$ is an equivalence.*

Assume that k is a field, H is a k-Hopf algebra and A is a right H-Galois extension of k. The results just cited assert that there is a fiber functor $\omega_A : {}^H\mathcal{M}_f \ni V \mapsto A \underset{H}{\Box} V \in \mathcal{M}_k$, which has values in the category of finite dimensional vector spaces, and this fiber functor induces an equivalence $\mathcal{F}_A : {}^H\mathcal{M}_f \to {}^{\mathrm{coend}(\omega_A)}\mathcal{M}_f$ for a certain bialgebra $\mathrm{coend}(\omega_A)$. We will show that $\mathrm{coend}(\omega_A) \cong L(A, H)$, which amounts to saying that the construction from Section 3 can be obtained by combining results from [19, 20] in the case that k is a field, and we will generalize the result to the case of general k in a suitable way.

5.5. Theorem: *Let A be an L-H-bigalois extension of k. Then*

$$\mathcal{F}_A : {}^H\mathcal{M} \ni V \mapsto A \underset{H}{\Box} V \in {}^L\mathcal{M}$$

is an equivalence of monoidal categories, and we have

$$\mathrm{coend}(\omega_A) \cong L(A, H).$$

In particular, every fiber functor $\omega : {}^H\mathcal{M} \to \mathcal{M}_k$ factors as $\omega \cong \mathcal{U}\mathcal{F}$ where $\mathcal{U} : {}^L\mathcal{M} \to \mathcal{M}_k$ is the underlying functor, with L a Hopf algebra, and $\mathcal{F}$ is an equivalence.

Proof: The natural isomorphism

$$\xi : (A \underset{H}{\square} V) \otimes (A \underset{H}{\square} W) \cong A \underset{H}{\square} (V \otimes W)$$

from [18, Prop. 1.4] is clearly left L-colinear, and thus makes $\mathcal{F}_A$ a monoidal functor. A quasiinverse for $\mathcal{F}_A$ is given by $\mathcal{F}_{A^{-1}}$. In fact, since A^{-1} is a faithfully flat Hopf-Galois extension of k, the remark concluding section 2 gives

$$A^{-1} \underset{L}{\square} (A \underset{H}{\square} V) \cong (A^{-1} \underset{L}{\square} A) \underset{H}{\square} V \cong H \underset{H}{\square} V \cong V$$

for each $V \in {}^H\mathcal{M}$ and

$$A \underset{H}{\square} (A^{-1} \underset{L}{\square} W) \cong (A \underset{H}{\square} A^{-1}) \underset{L}{\square} W \cong L \underset{L}{\square} W \cong W$$

for each $W \in {}^L\mathcal{M}$.

If $\mathcal{U} : {}^L\mathcal{M} \to \mathcal{M}_k$ denotes the underlying functor, then $\omega_A = \mathcal{U}\mathcal{F}_A$. We conclude

$$\operatorname{coend}(\omega_A) = \operatorname{coend}(\mathcal{U}\mathcal{F}_A) \cong \operatorname{coend}(\mathcal{U}) \cong L,$$

since $\mathcal{F}_A$ is an equivalence. The remaining statement is clear. $\square$

As a byproduct of the preceding theorem, we can extend [19, Prop.3.2] to the situation when the antipode of H is not necessarily bijective: Every fiber functor $\omega : {}^H\mathcal{M} \to \mathcal{M}_k$ is left adjoint. In fact we can assume $\omega = \omega_A$ for a right H-Galois extension A of k, we then have $\omega_A = \mathcal{U}\mathcal{F}_A$, the underlying functor $\mathcal{F} : {}^L\mathcal{M} \to \mathcal{M}_k$ is left adjoint with right adjoint $M \mapsto L \otimes M$, and $\mathcal{F}_A$ is an equivalence, so that

$$\mathcal{M}_k \ni M \mapsto A^{-1} \underset{L}{\square} (L \otimes M) \cong A^{-1} \otimes M \in {}^H\mathcal{M}$$

defines a right adjoint for ω_A.

5.6. Definition: *Let H and F be two bialgebras. We say that H and F are monoidally co-Morita equivalent if the monoidal categories ${}^H\mathcal{M}$ and ${}^F\mathcal{M}$ are equivalent as monoidal k-linear categories.*

5.7. Corollary: *Let H and F be k-flat Hopf algebras. The following are equivalent:*

(1) H and F are monoidally co-Morita equivalent.

(2) There is a faithfully flat F-H-bigalois extension of k.

More precisely, there is a bijection between monoidal isomorphism classes of k-linear monoidal equivalences ${}^H\mathcal{M} \cong {}^F\mathcal{M}$ and isomorphism classes of F-H-bigalois extensions of k; the bijection maps the bigalois extension A to the functor $\mathcal{F}_A$ from Theorem 5.5.

The bijection is compatible with multiplication in $\mathcal{H}$ and composition of functors, respectively: For an L-H-bigalois extension A and an H-R-bigalois extension B of k we have

$$\mathcal{F}_{A \underset{H}{\Box} B} \cong \mathcal{F}_A \mathcal{F}_B.$$

5.8. Corollary: *Assume H is cocommutative. Then the group $\mathcal{H}(H,k)$ is isomorphic to the group of monoidal isomorphism classes of monoidal self-equivalences of the category ${}^H\mathcal{M}$.*

If H is also commutative then the subgroup $\mathcal{H}_c(H,k)$ is isomorphic to the group of monoidal isomorphism classes of symmetric monoidal self-equivalences of ${}^H\mathcal{M}$.

5.9. Corollary: *Assume k is a field and H is a finite dimensional k-Hopf algebra. Then every Hopf algebra monoidally co-Morita equivalent to H is obtained from H by twisting with a 2-cocycle.*

In fact all H-Galois extensions of k are cleft in this case by [9, Prop.2].

6 Galois correspondences

Let H be a Hopf algebra and A a right H-Galois extension of k. There is a map

$$\begin{aligned} \{\text{Hopf ideals in } H\} &\to \{\text{subalgebras in } A\} \\ I &\mapsto A^{\mathrm{co}\, H/I} \end{aligned}$$

that preserves inclusions (in view of the fact that subgroups of a finite group G correspond bijectively to quotient Hopf algebras and thus Hopf ideals of the dual of the group algebra kG if k is a field this generalizes well known properties of the classical Galois correspondence) and is at least injective in favorable cases, see [2, Thm. 7.6] and [22, Sec. 2]. It is not clear which subalgebras of A actually occur in this correspondence. The approach taken in [22] is to study the correspondence for $L(A,H)$ instead of H, and for A a field extension of a base field k [22, Thm. 4.4] characterizes those intermediate fields coming from a Hopf ideal of $L(A,H)$ as being those intermediate fields that are H-subcomodules of A.

We extend this idea in two directions: Once by dropping commutativity of A and studying Hopf Galois skew field extensions of a base field, and once dealing with commutative Hopf Galois ring extensions of a base ring, assuming the Hopf algebra is finite.

Apart from these two cases in which we will find exact Galois-type correspondences, we can describe a Galois-type connection in the general cases. In the noncommutative version we have to either allow coideals in $L(A,H)$ that are only one-sided ideals, or restrict the subcomodule algebras of A to those that are also submodule algebras with the Miyashita-Ulbrich action and thus Yetter-Drinfel'd submodule algebras.

The following definition of a coring is [16, Def. 1.1] Let A be a ring. An A-coring is an A-A-bimodule M together with maps $\Delta : M \to M \underset{A}{\otimes} M$ and $\varepsilon : M \to A$ of A-A-bimodules such that $(\Delta \underset{A}{\otimes} M)\Delta = (M \underset{A}{\otimes} \Delta)\Delta$ (coassociativity) and $(\varepsilon \underset{A}{\otimes} M)\Delta = \mathrm{id}_M = (M \underset{A}{\otimes} \varepsilon)\Delta$. A coideal in an A-coring M is an A-A-subbimodule $J \subset \mathrm{Ker}(\varepsilon)$ satisfying $\Delta(J) \subset \mathrm{Im}(J \underset{A}{\otimes} M) + \mathrm{Im}(M \underset{A}{\otimes} J) \subset M \underset{A}{\otimes} M$. This condition is equivalent to the requirement that there be a (unique) coring structure on M/J making the canonical surjection $M \to M/J$ a coring map (in the obvious sense). The most important example of an A-coring is the following: Let R be any subring of A. Then $A \underset{R}{\otimes} A$ is an A-A-coring with $\Delta(x \otimes y) = x \otimes 1 \otimes 1 \otimes y$ and $\varepsilon(x \otimes y) = xy$.

The maps in the following proposition are obvious generalizations of the ones that occur in the main theorem of [16].

6.1. Proposition: *Let A be a ring and $R \subset A$ a subring. There are maps*

$$\{\textit{Coideals in } A \underset{R}{\otimes} A\} \underset{\hat{\mathcal{I}}}{\overset{\hat{\mathcal{F}}}{\rightleftarrows}} \{\textit{Intermediate rings } R \subset B \subset A\}$$

defined by

$$\begin{aligned}\hat{\mathcal{F}}(J) &= \{b \in A | b \otimes 1 - 1 \otimes b \in J\} \\ \hat{\mathcal{I}}(B) &= \operatorname{Ker}(A \underset{R}{\otimes} A \to A \underset{B}{\otimes} A)\end{aligned}$$

These maps have the following properties:

$$\begin{aligned}&\hat{\mathcal{I}}\hat{\mathcal{F}}(J) \subset J \\ &\hat{\mathcal{F}}\hat{\mathcal{I}}(B) \supset B \\ &B \subset B' \Rightarrow \hat{\mathcal{I}}(B) \subset \hat{\mathcal{I}}(B') \\ &J \subset J' \Rightarrow \hat{\mathcal{F}}(J) \subset \hat{\mathcal{F}}(J')\end{aligned}$$

PROOF: It is straightforward to check that $\hat{\mathcal{F}}(J)$ is an intermediate ring if J is a coideal in $A \underset{R}{\otimes} A$ (we only need that J is an A-A-sub-bimodule), and that $\hat{\mathcal{I}}(B)$ is a coideal if B is an intermediate ring (in fact $A \underset{B}{\otimes} A$ is a quotient coring of $A \underset{R}{\otimes} A$). The least obvious of the inclusions stated is $\hat{\mathcal{I}}\hat{\mathcal{F}}(J) \subset J$ for a coideal J. We have

$$\begin{aligned}\hat{\mathcal{I}}\hat{\mathcal{F}}(J) &= \operatorname{Ker}(A \underset{R}{\otimes} A \to A \underset{\hat{\mathcal{F}}(J)}{\otimes} A) \\ &= \{\sum x_i f_i \otimes y_i - \sum x_i \otimes f_i y_i | f_i \in \hat{\mathcal{F}}(J), x_i, y_i \in A\} \\ &= \{\sum x_i (f_i \otimes 1 - 1 \otimes f_i) y_i | f_i \in \hat{\mathcal{F}}(J), x_i, y_i \in A\} \\ &\subset AJA = J\end{aligned}$$

□

6.2. Remark: *Let H be a Hopf algebra and A a right H-comodule algebra. The maps from Proposition 6.1 for $R = k$ restrict to maps between the set of those coideals of $A \otimes A$ that are H-subcomodules and the set of subcomodule algebras of A.*

Before applying the results just stated to the constructions from section 3 we give another characterization of the comultiplication of $L(A,H)$ (namely by the description used to define it in [22] in the commutative case.)

6.3. Remark: *We have isomorphisms*

$$\phi : L \otimes A \cong A \otimes A$$
$$\psi : L \otimes L \otimes A \cong (L \otimes A) \underset{A}{\otimes} (L \otimes A) \cong A \otimes A \underset{A}{\otimes} A \otimes A$$

with $\phi(\sum x_i \otimes y_i \otimes a) = \sum x_i \otimes y_i a$ *and* $\psi(\sum w_i \otimes x_i \otimes \sum y_j \otimes z_j \otimes a) = \sum w_i \otimes x_i \otimes y_j \otimes z_j a$. *The following diagram commutes*

$$\begin{tikzcd} L \otimes A \arrow[r, "\Delta_L \otimes A"] \arrow[d, "\phi"'] & L \otimes L \otimes A \arrow[d, "\psi"] \\ A \otimes A \arrow[r, "\Delta_{A \otimes A}"] & A \otimes A \underset{A}{\otimes} A \otimes A \end{tikzcd}$$

so that $\Delta_{A\otimes A} = \psi(\Delta_L \otimes A)\phi^{-1}$ *and* $\Delta_L = (\psi^{-1}\Delta_{A\otimes A}\phi)^{\mathrm{co}\, H}$.

In fact

$$\begin{aligned} \Delta\phi(\sum x_i \otimes y_i \otimes a) &= \Delta(\sum x_i \otimes y_i a) \\ &= \sum x_i \otimes 1 \underset{A}{\otimes} 1 \otimes y_i a \\ &= \sum x_{i(0)} \otimes \ell_j(x_{i(1)}) \otimes r_j(x_{i(1)}) \otimes y_i a \\ &= \psi(\sum x_{i(0)} \otimes \ell_j(x_{i(1)}) \otimes r_j(x_{i(1)}) \otimes y_i \otimes a) \\ &= \psi(\Delta(\sum x_i \otimes y_i) \otimes a) \end{aligned}$$

6.4. Theorem: *Let A be a faithfully flat right H-Galois extension of k and put $L = L(A,H)$. There are maps*

$$\{\textit{Coideal left ideals of } L\} \underset{\mathcal{I}}{\overset{\mathcal{F}}{\rightleftarrows}} \{H\textit{-subcomodule algebras of } A\}$$

given by

$$\mathcal{I}(B) = \hat{\mathcal{I}}(B)^{\mathrm{co}\, H} = \mathrm{Ker}(A \otimes A \to A \underset{B}{\otimes} A)^{\mathrm{co}\, H}$$
$$\mathcal{F}(I) = {}^{\mathrm{co}\, L/I}A$$

These maps satisfy

$$\begin{aligned}
\mathcal{I}\mathcal{F}(I) &\subset I \\
\mathcal{F}\mathcal{I}(B) &\supset B \\
B \subset B' &\Rightarrow \mathcal{I}(B) \subset \mathcal{I}(B') \\
I \subset I' &\Rightarrow \mathcal{F}(I) \subset \mathcal{F}(I')
\end{aligned}$$

PROOF: We have a bijection

$$\{H\text{-subcomodule coideals of } A \otimes A\} \xrightarrow{\mathcal{G}} \{\text{Coideal left ideals of } L\}$$

given by $\mathcal{G}(J) = J^{\mathrm{co}\,H}$ and $\mathcal{G}^{-1}(I) = IA \cong I \otimes A$.

In fact, $\mathcal{G}$ and $\mathcal{G}^{-1}$ clearly define inverse bijections between sub-Hopf modules of $A \otimes A$ in $\mathcal{M}_A^H$ and k-submodules of L. Now if I is a left ideal of L, then IA is a sub A-bimodule of $A \otimes A$ because for $\xi \in I$, $y, a \in A$ we have

$$a\xi y = \sum a_{(0)}\xi\ell_j(a_{(1)})r_j(a_{(1)})y = \sum \left((a_{(0)} \otimes \ell_j(a_{(1)}))\xi\right) r_j(a_{(1)})y \in IA.$$

Conversely, if J is a sub-bimodule of $A \otimes A$, then $J^{\mathrm{co}\,H}$ is a left L-submodule of L, because for $\sum w_i \otimes x_i \in L$ and $\sum y_j \otimes z_j \in J$ the product $(\sum w_i \otimes x_i)(\sum y_j \otimes z_j) = \sum w_i y_j \otimes z_j x_i$ is in J.

Now let I be a left ideal of L. Then the isomorphisms from Remark 6.3 induce isomorphisms

$$\begin{aligned}
\overline{\phi} &: L/I \otimes A \cong A \otimes A/IA \\
\overline{\psi} &: L/I \otimes L/I \otimes A \cong (L/I \otimes A) \underset{A}{\otimes} (L/I \otimes A) \cong (A \otimes A/IA) \underset{A}{\otimes} (A \otimes A/IA)
\end{aligned}$$

Thus, if I is a coideal in L, then so is IA in $A \otimes A$, since

$$\Delta_{A\otimes A/IA} = \overline{\psi}(\Delta_{L/I} \otimes A)\overline{\phi}^{-1}$$

is a well defined comultiplication on $A \otimes A/IA$, and if IA is a coideal in $A \otimes A$, then so is $I = IA^{\mathrm{co}\,H}$ in L, since

$$\Delta_L = \left(\overline{\psi}^{-1}\Delta_{A\otimes A/IA}\overline{\phi}\right)^{\mathrm{co}\,H}$$

is a well defined comultiplication on L/I.

Given the bijection $\mathcal{G}$ and the results of Proposition 6.1, we can define maps between the two sets in the statement of the Theorem by setting $\mathcal{F} = \hat{\mathcal{F}}\mathcal{G}^{-1}$ and $\mathcal{I} = \mathcal{G}\hat{\mathcal{I}}$; the inclusion statements are obvious, we only have to check that the maps $\mathcal{F}$ and $\mathcal{I}$ have the stated form.

$$\begin{aligned}
\hat{\mathcal{F}}\mathcal{G}^{-1}(I) = \hat{\mathcal{F}}(IA) & \\
&= \{a \in A | a \otimes 1 - 1 \otimes a \in IA\} \\
&= \{a \in A | \sum a_{(0)} \otimes \ell_i(a_{(1)}) r_i(a_{(1)}) - 1 \otimes a \in IA\} \\
&= \{a \in A | \sum a_{(0)} \otimes \ell_i(a_{(1)}) \otimes r_i(a_{(1)}) - 1 \otimes 1 \otimes a \in I \otimes A\} \\
&= \{a \in A | \delta_\ell(a) - 1 \otimes a \in I \otimes A\} \\
&= {}^{\mathrm{co}\, L/I}A
\end{aligned}$$

while $\mathcal{I}$ obviously has the form stated. □

The behavior of the maps $\mathcal{F}$ and $\mathcal{I}$ with respect to inclusions mean that we are dealing with a Galois connection between the ordered set of subcomodule algebras of A and the set of left ideal coideals of $L(A, H)$, provided we take the order of the latter to be the reverse of that by inclusion. This ordering makes sense for the analogy with classical Galois correspondences, because a classical G-Galois extension is a $(kG)^*$-Galois extension for the dual of the group algebra.

The next proposition studies further properties of the Galois connection. Parts (1) and (4) begin to address the question in which cases the Galois connection comes close to being a precise correspondence. Parts (2) and (3) show that restricting to only Hopf ideals of $L(A, H)$ instead of left ideal coideals corresponds to restricting from subcomodule algebras to Yetter-Drinfel'd submodule algebras. We have already mentioned preceding Corollary 3.6 that A is a Yetter-Drinfel'd module over H if it is an H-Galois extension. Now we will also have to use that the H-module structure makes it an H-module algebra, so it is an algebra in the category of Yetter-Drinfel'd modules, and that A is a commutative Yetter-Drinfel'd module algebra, that is, $xy = y_{(0)}(x \leftharpoonup y_{(1)})$ holds for all $x, y \in A$. These facts can be found in [4], see also [1, 12].

6.5. Proposition: *Let H be a Hopf algebra and A a faithfully flat right H-Galois extension of k, and put $L = L(A, H)$.*

(1) If $B \subset A$ is an H-subcomodule algebra with A_B faithfully flat, then $\mathcal{F}\mathcal{I}(B) = B$.

(2) If $B \subset A$ is a Yetter-Drinfel'd submodule algebra of A, then $\mathcal{I}(B) \subset L$ is a Hopf ideal.

(3) If $I \subset L$ is a Hopf ideal, then $\mathcal{F}(I) \subset A$ is an H-submodule (hence a Yetter-Drinfel'd submodule algebra).

(4) Assume that H is finitely generated projective. If $I \subset L$ is a Hopf ideal and a k-direct summand, then $A_{\mathcal{F}(I)}$ is finitely generated projective and $\mathcal{I}\mathcal{F}(I) = I$.

PROOF:

(1) $\mathcal{F}\mathcal{I}(B) = \hat{\mathcal{F}}\hat{\mathcal{I}}(B) = \{x \in A | x \otimes 1 = 1 \otimes x \text{ in } A \underset{B}{\otimes} A\} = B$ if A_B is faithfully flat.

(2) We have to show that $\mathcal{I}(B)$ is a right ideal and stable under the antipode. For the first assertion we show that $L/\mathcal{I}(B) \cong (A \underset{B}{\otimes} A)^{\mathrm{co}\, H}$ is a quotient right L-module of L. For this in turn we show that $(w \otimes x)(\sum y_i \otimes z_i) = \sum w x_i \otimes z_i y$ gives $A \underset{B}{\otimes} A$ the structure of a right L-module, of which $(A \underset{B}{\otimes} A)^{\mathrm{co}\, H}$ is then just a submodule. For $w, x \in A$, $b \in B$ and $\sum y_i \otimes z_i \in L$ we have, in $A \underset{B}{\otimes} A$,

$$\begin{aligned}
\sum w b y_i \otimes z_i x &= \sum w y_{i(0)}(b \leftharpoonup y_{i(1)}) \otimes z_i x \\
&= \sum w y_{i(0)} \otimes (b \leftharpoonup y_{i(1)}) z_i x \\
&= \sum w y_{i(0)} \otimes z_{i(0)}(b \leftharpoonup y_{i(1)} z_{i(1)}) x \\
&= \sum x y_i \otimes z_i b x
\end{aligned}$$

To show that $\mathcal{I}(B)$ is stable under the antipode of L, it is sufficient to show that the map

$$A \underset{B}{\otimes} A \ni x \otimes y \mapsto y_{(0)} \otimes x \leftharpoonup y_{(1)} \in A \underset{B}{\otimes} A$$

is well defined. Now for $b \in B$, $x, y \in A$ we have, in $A \underset{B}{\otimes} A$,

$$\begin{aligned} y_{(0)} \otimes (xb) \leftharpoondown y_{(1)} &= y_{(0)} \otimes (x \leftharpoondown y_{(1)})(b \leftharpoondown y_{(2)}) \\ &= y_{(0)} \otimes (b \leftharpoondown y_{(2)})_{(0)}(x \leftharpoondown y_{(1)}(b \leftharpoondown y_{(2)})_{(1)}) \\ &= y_{(0)} \otimes (b_{(0)} \leftharpoondown y_{(1)})(x \leftharpoondown b_{(1)}y_{(2)}) \\ &= y_{(0)}(b_{(0)} \leftharpoondown y_{(1)}) \otimes x \leftharpoondown b_{(1)}y_{(2)} \\ &= b_{(0)}y_{(0)} \otimes x \leftharpoondown b_{(1)}y_{(1)} \end{aligned}$$

(3) Let $b \in \mathcal{F}(I)$ and $h \in H$. We have to show that $\delta_\ell(b \leftharpoondown h) \equiv 1 \otimes b \leftharpoondown h$ holds modulo $I \otimes A$ in $L \otimes A$. We have

$$\begin{aligned} \delta_\ell(b \leftharpoondown h) &= \delta_\ell(\textstyle\sum \ell_i(h) b r_i(h)) \\ &= \textstyle\sum \ell_i(h)_{(-1)} b_{(-1)} r_i(h)_{(-1)} \otimes \ell_i(h)_{(0)} b_{(0)} r_i(h)_{(0)} \\ &\equiv \textstyle\sum \ell_i(h)_{(-1)} r_i(h)_{(-1)} \otimes \ell_i(h)_{(0)} b r_i(h)_{(0)} \\ &= \textstyle\sum (\ell_i(h)_{(0)} \otimes \ell_j(\ell_i(h)_{(1)}))(r_i(h)_{(0)} \otimes \ell_k(r_i(h)_{(1)})) \\ &\qquad \otimes r_j(\ell_i(h)_{(1)}) b r_k(r_i(h)_{(1)}) \\ &= \textstyle\sum \ell_i(h_{(2)}) r_i(h_{(2)}) \otimes \ell_k(h_{(3)}) \ell_j(Sh_{(1)}) \otimes r_j(Sh_{(1)}) b r_k(h_{(3)}) \\ &= \textstyle\sum 1 \otimes \ell_k(h_{(2)}) \ell_j(Sh_{(1)}) \otimes r_j(Sh_{(1)}) b r_k(h_{(2)}) \\ &\overset{*}{=} 1 \otimes 1 \otimes \ell_k(h_{(2)}) \ell_j(Sh_{(1)}) r_j(Sh_{(1)}) b r_k(h_{(2)}) \\ &= 1 \otimes 1 \otimes \ell_k(h) b r_k(h) \\ &= 1_L \otimes b \leftharpoondown h \end{aligned}$$

where in the equality marked $*$ we could pull the term "$\ell_k(h_{(2)})\ell_j(Sh_{(1)})$" across the tensor product because it is coinvariant, hence in k: the expression preceding the equality is in $(A \otimes A)^{\operatorname{co} H} \otimes A \cap k \otimes A \otimes A = k \otimes A^{\operatorname{co} H} \otimes A$.

(4) Note that $\mathcal{F}(I) = {}^{\operatorname{co} L/I}A$. Since A is a left L-Galois extension of k, the Galois map $\beta : A \underset{\mathcal{F}(I)}{\otimes} A \to L/I \otimes A$ is onto. By Theorem 1.7 of [10], it follows that β is a bijection, in particular $\beta^{\operatorname{co} H}$ is an isomorphism $L/\mathcal{I}\mathcal{F}(I) \cong (A \underset{\mathcal{F}(I)}{\otimes} A)^{\operatorname{co} H} \cong (L/I \otimes A)^{\operatorname{co} H} \cong L/I$, whence $\mathcal{I}\mathcal{F}(I) = I$, and $A_{\mathcal{F}(I)}$ is finitely generated projective.

□

6.6. Theorem: *Let H be a finitely generated projective (commutative) Hopf algebra and A a commutative right H-Galois extension of k. Then the maps $\mathcal{F}$ and $\mathcal{I}$ from Theorem 6.4 induce inverse bijections between*

- *The set of subcomodule algebras $B \subset A$ such that A_B is faithfully projective, and*
- *The set of Hopf ideals $I \subset L$ that are k-direct summands.*

Proof: After the preceding proposition it only remains to remark that by [10, Cor.(1.10)] the L/I-Galois extension $\mathcal{F}(I) \subset A$ for a k-direct summand Hopf ideal of L is faithfully flat. □

6.7. Theorem: *Let k be a field, H a Hopf algebra, and A a right H-Galois extension of k that is a skew field. Then we have a bijective correspondence between*

- *Coideal left ideals of $L(A, H)$.*
- *H-subcomodule skew subfields of A.*

induced by the maps from Theorem 6.4. It induces a bijective correspondence between the subsets of

- *Hopf ideals of $L(A, H)$.*
- *Yetter-Drinfel'd submodule subfields of A.*

Proof: By [16, Thm. 2.1] the maps $\hat{\mathcal{F}}$ and $\hat{\mathcal{I}}$ from 6.1 induce bijections between intermediate skew fields between k and A and coideals of $A \otimes A$, hence between H-subcomodule skew subfields of A and H-subcomodule coideals of $A \otimes A$; at the beginning of the proof of 6.4 we have shown that the latter correspond to coideal left ideals of $L(A, H)$. The rest of the statement follows from parts (2) and (3) of Proposition 6.5 □

References

[1] Caenepeel, S., van Oystaeyen, F., and Zhang, Y. H. Quantum Yang-Baxter module algebras. *K-Theory 8* (1994), 231–255.

[2] Chase, S., and Sweedler, M. *Hopf algebras and Galois theory*, vol. 97 of *Lecture Notes in Math.* Springer, Berlin, Heidelberg, New York, 1969.

[3] Doi, Y. Braided bialgebras and quadratic bialgebras. *Comm. in Alg. 21* (1993), 1731–1749.

[4] Doi, Y., and Takeuchi, M. Hopf-Galois extensions of algebras, the Miyashita-Ulbrich action, and Azumaya algebras. *J. Algebra 121* (1989), 488–516.

[5] Early, T. E., and Kreimer, H. F. Galois algebras and Harrison cohomology. *J. Algebra 58* (1979), 136–147.

[6] Greither, C. On the transformation of the Hopf algebra in a Hopf Galois extension. *Comm. in Alg. 24* (1996), 737–747.

[7] Greither, C., and Pareigis, B. Hopf Galois theory for separable field extensions. *J. Algebra 106* (1987), 239–258.

[8] Harrison, D. K. Abelian extensions of commutative rings. *Mem. AMS 52* (1965).

[9] Kreimer, H. F., and Cook II, P. M. Galois theories and normal bases. *J. Algebra 43* (1976), 115–121.

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

[11] Montgomery, S. *Hopf algebras and their actions on rings*, vol. 82 of *CBMS Regional Conference Series in Mathematics*. AMS, Providence, Rhode Island, 1993.

[12] Schauenburg, P. Hopf bimodules over Hopf-Galois-extensions, Miyashita-Ulbrich actions, and the monoidal center construction. *Comm. in Alg. 24* (1996), 143–163.

[13] SCHAUENBURG, P. A bialgebra that admits a Hopf-Galois extension is a Hopf algebra. *Proc. Amer. Math. Soc.* (to appear).

[14] SCHNEIDER, H.-J. Principal homogeneous spaces for arbitrary Hopf algebras. *Israel J. of Math. 72* (1990), 167–195.

[15] SCHNEIDER, H.-J. Representation theory of Hopf-Galois extensions. *Israel J. of Math. 72* (1990), 196–231.

[16] SWEEDLER, M. The predual theorem to the Jacobson-Bourbaki theorem. *Trans. Amer. Math. Soc. 213* (1975), 391–406.

[17] TAMBARA, D. The bialgebra of coendomorphisms of an algebra. *J. Fac. Sci. Univ. Tokyo, Sect.IA, Math. 37* (1990), 425–456.

[18] ULBRICH, K.-H. Galois extensions as functors of comodules. *manuscripta math. 59* (1987), 391–397.

[19] ULBRICH, K.-H. Fiber functors of finite dimensional comodules. *manuscripta math. 65* (1989), 39–46.

[20] ULBRICH, K.-H. On Hopf algebras and rigid monoidal categories. *Israel J. Math. 72* (1990), 252–256.

[21] VAN OYSTAEYEN, F., AND ZHANG, Y. Bi-Galois objects form a group. *Preprint* (1993).

[22] VAN OYSTAEYEN, F., AND ZHANG, Y. Galois-type correspondences for Hopf Galois extensions. *K-Theory 8* (1994), 257–269.

[23] YETTER, D. N. Quantum groups and representations of monoidal categories. *Math. Proc. Camb. Phil. Soc. 108* (1990), 261–290.