Hopf Galois theory: A survey

SUSAN MONTGOMERY

We consider a Hopf Galois extension $B \subset A$, for A a comodule algebra over the Hopf algebra H with coinvariant algebra B. After giving a number of examples, we discuss Galois extensions with additional properties, such as having a normal basis. We then consider when there is a category equivalence between the category of modules over B and the category of "relative Hopf modules" for A and H. Finally we discuss more recent work of van Oystaeyen and Zhang and of Schauenburg on obtaining correspondence theorems between suitable subalgebras of A and Hopf ideals of H.

16W30; 16S40, 16S34

The definition of Hopf Galois extension has its roots in the approach of Chase, Harrison and Rosenberg who wanted to generalize the classical Galois theory of automorphism groups of fields to groups acting on commutative rings [4]. In 1969 Chase and Sweedler extended these ideas to coactions of Hopf algebras acting on a commutative $\mathbf{k}$–algebra, for $\mathbf{k}$ a commutative ring [5]; the general definition is due to Kreimer and Takeuchi in 1980 [13].

The outline of the paper is as follows: In Section 1, we review our terminology for Hopf algebras, their actions and coactions and give a basic "zoo" of examples of Hopf algebras which we will look at again later. In Section 2 we define Hopf Galois extensions and then give a number of examples of Galois extensions, using our Hopf algebras from Section 1. Next in Section 3 we characterize Galois extensions which have normal bases and see that they are crossed products. We also give examples of how crossed products arise "in nature". In Section 4 we study Galois extensions for actions of a finite-dimensional Hopf algebra H and study when the invariant algebra is Morita equivalent to the smash product algebra. In Section 5 we return to coactions. We consider faithfully flat Galois extensions and show that in this situation there are natural category equivalences between the module category of the coinvariant algebra and the category of relative Hopf modules. In Section 6 we consider some recent work on finding a Galois correspondence theory; this necessitates looking at algebras which are Hopf bi-Galois in the sense that they are both left and right Galois, with possibly different Hopf algebras. Finally in Section 7 we consider a different approach to the Galois correspondence via actions.

Published: 4 July 2009 DOI: 10.2140/gtm.2009.16.367

Some basic references on Hopf algebras are Sweedler [34] or Abe [1]. Chapter 8 of Montgomery [20] is all on Hopf Galois extensions. Recent surveys are Schauenburg [29] and Schauenburg and Schneider [30].

Acknowledgements The author was supported by NSF grant DMS 07-01291. She would also like to thank Andrew Baker and Birgit Richter for organizing a very interesting conference.

1 Hopf algebras: Definitions and examples

Let H be a Hopf algebra over the field $\mathbf{k}$. As an algebra, H has multiplication $m\colon H\otimes_{\mathbf{k}} H\to H$, $a\otimes b\mapsto ab$, and unit $u\colon \mathbf{k}\to H$, $\alpha\mapsto \alpha 1_H$. The coalgebra structure is given by comultiplication $\triangle\colon H\to H\otimes_{\mathbf{k}} H$, written $\triangle(h)=\sum_h h_1\otimes h_2$, and counit $\varepsilon\colon H\to \mathbf{k}$. In addition H has an antipode $S: H\to H$. The ideal $H^+ := \mathrm{Ker}(\varepsilon)$ is sometimes called the *augmentation ideal* of H.

If $H=(H,m,u,\triangle,\varepsilon,S)$ is finite-dimensional, then its linear dual H^* is also a Hopf algebra, with structure maps dual to those in H, that is, $H^*=(H^*,\triangle^*,\varepsilon^*,m^*,u^*,S^*)$. When H is infinite-dimensional, its dual H^* is an algebra but not a coalgebra; to construct a dual, one may consider a suitable subset of functions in H^*, usually involving some topology.

Let A be an algebra with 1 over $\mathbf{k}$.

Definition 1.1 (1) A is a left H*–module algebra* if A is a unital left H–module, via $h\otimes a\mapsto h\cdot a\in A$, such that

$$h\cdot(ab)=\sum_h h_1\cdot a\otimes h_2\cdot b \text{ and } h\cdot 1=\varepsilon(h)1$$

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

(2) A is a right H*–comodule algebra* if A is a counital right H–comodule, via $\delta_A(a)\mapsto\sum_a a_0\otimes a_1\in A\otimes_{\mathbf{k}} H$, such that δ is an algebra map.

If A is an H–module algebra, we usually just say that H *acts* on A, and if A is an H- comodule algebra, we say H *coacts* on A. The *invariants* of an H–action are

$$A^H=\{a\in A\mid h\cdot a=\varepsilon(h)a, \text{ for all } h\in H\}.$$

The *coinvariants* of a coaction are

$$A^{\mathrm{co}\,H}=\{a\in A\mid \delta(a)=a\otimes 1_H\}.$$

In the case of an H–action on A, we say a subspace $V \subseteq A$ is H–*stable* if $H \cdot V \subseteq V$. Dually, if H coacts on A, a subspace $V \subseteq A$ is H–*costable* if V is an H–subcomodule of A.

Assume that H is finite-dimensional. If A is a right comodule algebra, then it is also a left H^*–module algebra, via

$$f \cdot a := \sum_a f(a_1)a_0$$

for all $f \in H^*$ and $a \in A$. Dually, any left H–module algebra is also a right H^*–comodule algebra, and the two notions are equivalent: that is, H^* acts on A if and only if H coacts on A, and under this equivalence, $A^{H^*} = A^{\mathrm{co}\,H}$.

In particular, consider $A = H$ itself. H is a right H–comodule algebra using $\delta_A = \triangle$. This action dualizes to a left action $\rightharpoonup$ of H^* on H, that is,

$$f \rightharpoonup h = \sum_h f(h_2)h_1,$$

for $f \in H^*$ and $h \in H$. The (co)invariants are given by $H^{H^*} = H^{\mathrm{co}\,H} = \mathbf{k} \cdot 1$.

We review some standard examples of Hopf algebras, to fix our notation.

Example 1.2 Let G be any group. The *group algebra* $H = \mathbf{k}G$ is a $\mathbf{k}$–space with basis the set of group elements $\{g \in G\}$. The algebra structure on $\mathbf{k}G$ is given by multiplying the basis elements using the group operation. $\mathbf{k}G$ becomes a coalgebra by defining, for each $g \in G$,

$$\triangle(g) = g \otimes g \quad \text{and} \quad \varepsilon(g) = 1,$$

and then extending linearly. The antipode is given by $S(g) = g^{-1}$ for all $g \in G$. In any Hopf algebra H, an element $g \in H$ satisfying $\triangle(g) = g \otimes g$, $\varepsilon(g) = 1$, and $S(g) = g^{-1}$ is called a *group-like element*.

A is a $\mathbf{k}G$–module algebra if and only if G acts as automorphisms of A. The subalgebra of $\mathbf{k}G$–invariants is simply A^G, the usual subalgebra of fixed points for G.

Dually A is a $\mathbf{k}G$–comodule algebra if and only if A is a G–*graded algebra*, that is, $A = \bigoplus_{g \in G} A_g$, where the A_g are $\mathbf{k}$–subspaces of A and $A_g A_h \subseteq A_{gh}$, for all $g, h \in G$. To see this, note that the $\mathbf{k}G$–comodule algebra structure is given by

$$\rho\colon A \to A \otimes_{\mathbf{k}} \mathbf{k}G \quad \text{via} \quad a \mapsto a \otimes g,$$

for each homogeneous element $a \in A_g$. Moreover the subalgebra of coinvariants is $A^{\mathrm{co}\,H} = A_1$, the identity component.

Example 1.3 Let G be a finite group and let $H = \mathbf{k}^G = (\mathbf{k}G)^*$, the algebra of functions from G to $\mathbf{k}$. The Hopf structure of $\mathbf{k}^G$ is the formal dual of that of $\mathbf{k}G$. Thus for $f, h \in \mathbf{k}^G$, $x, y \in G$, $(f*h)(x) := m(f\otimes h)(\triangle(x)) \in \mathbf{k}$ and $\triangle(f)(x\otimes y) := f(xy) \in \mathbf{k}$. The antipode S of H is given by $S(f)(x) := f(Sx)$.

Since G is finite, $\mathbf{k}^G$ has as a basis the coordinate functions $\{p_x \mid x \in G\}$ dual to the group elements, that is, $p_x(y) = \delta_{x,y}$. For these elements, we have

$$p_x * p_y = \delta_{x,y} p_x \text{ and } \triangle(p_x) = \sum_{y\in G} p_y \otimes p_{y^{-1}x}.$$

$H = \mathbf{k}^G$ is commutative, but not cocommutative unless G is abelian. When G is abelian and $\mathbf{k}$ contains a primitive n–th root of 1 for $n = |G|$, then in fact $\mathbf{k}^G \cong \mathbf{k}G$ as Hopf algebras.

Actions of $\mathbf{k}^G$ correspond to coactions of $\mathbf{k}G$, that is gradings by G, and coactions of $\mathbf{k}^G$ give actions of G.

If G is not finite, we may consider a restricted set of functions on G, given some suitable topological conditions. Thus for example if G is an algebraic group over $\mathbf{k}$, then we may let H be the regular functions $f\colon G \to \mathbf{k}$. More generally:

Example 1.4 Let G be an affine algebraic group scheme, that is, $G = \operatorname{Spec} H$ for H a commutative affine $\mathbf{k}$–Hopf algebra. What is meant by an "action" of G? To define this, let X be an affine scheme, so that $X = \operatorname{Spec} A$ for A a commutative affine $\mathbf{k}$–algebra. Then an action $\mu\colon X \times G \to X$ is determined by a coaction

$$\rho = \mu^*\colon A \to A \otimes_{\mathbf{k}} H.$$

Example 1.5 Let $\mathfrak{g}$ be a Lie algebra over $\mathbf{k}$ and let $H = U(\mathfrak{g})$ be the universal enveloping algebra of $\mathfrak{g}$. Recall that by the PBW-theorem, the ordered monomials in a fixed basis of $\mathfrak{g}$ form a basis of H. H becomes a Hopf algebra by defining $\triangle(x) = x \otimes 1 + 1 \otimes x$, $\varepsilon(x) = 0$, and $S(x) = -x$ for all $x \in \mathfrak{g}$ and extending multiplicatively to all of H. In any Hopf algebra H, such an element x is called a *primitive element*.

If A is an H–module algebra, then every element $x \in \mathfrak{g}$ acts as a derivation, that is, $x\cdot(ab) = x\cdot(a)b + a(x\cdot b)$ and $x\cdot 1 = 0$. It follows that

$$A^H = A^{\mathfrak{g}} = \{a \in A \mid x\cdot a = 0, \text{ for all } x \in \mathfrak{g}\}.$$

As a related example, let $\mathbf{k}$ be a field of characteristic $p > 0$ and let $\mathfrak{g}$ be a restricted Lie algebra over $\mathbf{k}$; restricted means that $\mathfrak{g}$ has a "p–map" $\mathfrak{g} \to \mathfrak{g}$, $x \mapsto x^{[p]}$, such that in the restricted enveloping algebra $H = u(\mathfrak{g})$, $x^{[p]} = x^p$, the usual p–th power. If $\mathfrak{g}$ has dimension n, $u(\mathfrak{g})$ will have dimension p^n.

Example 1.6 Assume that $\mathbf{k}$ contains a primitive n–th root of unity ω, where $n > 1$. The n^2–dimensional *Taft Hopf algebra* $H = T_{n^2}(\omega)$ is given as an algebra by

$$T_{n^2}(\omega) = \mathbf{k}\langle g, x \mid g^n = 1, x^n = 0, xg = \omega g x\rangle.$$

As a coalgebra, $\triangle(g) = g \otimes g$, $\varepsilon(g) = 1$, $S(g) = g^{-1}$, and $\Delta(x) = x \otimes 1 + g \otimes x$, $\varepsilon(x) = 0$, $S(x) = -g^{-1}x$. That is, g is a group-like element and x is a $(1, g)$–*skew-primitive element*.

If H acts on A, we must have g acting as an automorphism of A and x as a *skew-derivation*, that is, $x \cdot (ab) = (x \cdot a)b + (g \cdot a)(x \cdot b)$, for all $a, b, \in A$.

The construction depends on the choice of ω, and thus there are in fact $\Phi(n)$ nonisomorphic Taft Hopf algebras for each dimension n^2.

These Hopf algebras were constructed by Taft in 1971 [35], to show that the antipode could have arbitrarily high order: in $H = T_{n^2}(\omega)$, S has order $2n$. They are among the first examples of Hopf algebras which are neither commutative nor cocommutative. It has recently been shown by Ng [23] that for p a prime, the *only* Hopf algebras over $\mathbb{C}$ of dimension p^2 are the two group algebras and the Taft algebras.

Example 1.7 Let $\mathbf{k} = \mathbb{C}$ and let $\mathfrak{g}$ be the Lie algebra $\mathfrak{sl}_2$. Recall that $\mathfrak{g}$ may be identified with the 2×2 matrices of trace 0, with basis

$$e = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad f = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad h = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

and Lie operation the usual additive commutator of matrices. The "quantum group" $U_q(\mathfrak{sl}_2)$ defined by Drinfel′d and Jimbo may be considered as a deformation of the ordinary universal enveloping algebra $U(\mathfrak{sl}_2)$. For the parameter q, it is given by

$$U_q(\mathfrak{sl}_2) := \mathbb{C}\langle E, F, K\rangle$$

where E, F, K satisfy the relations

$$KE = q^2 EK, \quad KF = q^{-2} FK, \quad EF - FE = \frac{K - K^{-1}}{q - q^{-1}}.$$

The coalgebra structure is given by $\Delta E = E \otimes K + 1 \otimes E$, $\Delta F = F \otimes 1 + K^{-1} \otimes F$, and $\Delta K = K \otimes K$. Notice that e and f are deformed to skew-primitive elements E and F, whereas h is replaced by the group-like element K (a kind of exponentiation).

Here we consider the *Frobenius–Lusztig kernel* (or *small quantum group*) associated to $U_q(\mathfrak{sl}_2)$, when q is a primitive $2n$–th root of 1, for $n > 2$; it is a finite-dimensional

quotient of $U_q(\mathfrak{sl}_2)$. See Kassel [12, IV.5.6]. This Hopf algebra is also called the *restricted quantum enveloping algebra* of $\mathfrak{sl}_2$. Specifically,

$$u_q(\mathfrak{sl}_2) := \frac{U_q(\mathfrak{sl}_2)}{(E^n, F^n, K^n - 1)}.$$

That is, we assume that E, F, K also satisfy the relations $E^n = 0,\ F^n = 0,\ K^n = 1$. Note that u_q is generated by two different copies of the Taft algebra Example 1.6, although with two different choices for ω. Namely, use $H_1 := \mathbb{C}\langle K^{-1}, F\rangle \cong T_{n^2}(q^{-2})$ and use $H_2 := \mathbb{C}\langle K^{-1}, EK^{-1}\rangle \cong T_{n^2}(q^2)$. One can think of H_1 as $\mathfrak{n}^-$, a Borel subalgebra of u_q, and similarly of H_2 as $\mathfrak{n}^+$.

2 Hopf Galois extensions: Definition and examples

Hopf Galois extensions are defined in terms of coactions, since this is more useful for arbitrary H.

Definition 2.1 Let $B \subset A$ be a $\mathbf{k}$–algebra, and let H be a Hopf algebra. Then $B \subset A$ is a *(right) H–extension* if A is a right H–comodule algebra with $A^{\mathrm{co}\,H} = B$.

Definition 2.2 Let A be a right H–comodule algebra with structure map $\rho\colon A \to A \otimes_{\mathbf{k}} H$. Then the extension $A^{\mathrm{co}\,H} \subset A$ is *right H–Galois* if the map

$$\beta\colon A \otimes_{A^{\mathrm{co}\,H}} A \to A \otimes_{\mathbf{k}} H, \text{ given by } r \otimes s \mapsto (r \otimes 1)\rho(s),$$

is bijective.

Some remarks are in order about the definition:

(1) In the case considered by Chase and Sweedler, $\mathbf{k}$ was assumed to be a commutative ring, A a (commutative) faithfully flat $\mathbf{k}$–algebra, H a finitely generated projective $\mathbf{k}$–algebra, and β was an isomorphism between $A \otimes_{\mathbf{k}} A$ and $A \otimes_{\mathbf{k}} H$. Among other things, this had the effect of forcing $A^{\mathrm{co}\,H} = \mathbf{k}$.

(2) Kreimer and Takeuchi [13] only required β to be surjective. However, they were also assuming H was finite over $\mathbf{k}$, in which case it follows that β is also injective. For infinite-dimensional Hopf algebras, problems can arise if β is not injective, and so we require that β be bijective as part of the definition.

(3) There seems to be an asymmetry in the definition of β; why not use $\beta'(r \otimes s) = \rho(r)(s \otimes 1)$? In fact if the antipode S is bijective, then β is surjective, injective or bijective, respectively, if and only if β' is surjective, injective, or bijective [13, 1.2]. Thus either β or β' may be used when S is bijective.
We give some elementary examples to illustrate the definition. First, surely any definition of Galois should include the classical case of automorphisms of fields.

Example 2.3 *Field extensions* Let G be a finite group acting as $\mathbf{k}$–automorphisms on a field $E \supset \mathbf{k}$, and let $F = E^G$. As in Example 1.2, the group algebra $\mathbf{k}G$ acts on E, and so its dual $H = \mathbf{k}^G$ coacts, which is what we shall need for our new definition.

We know that E/F is classically Galois with Galois group G if and only if G acts faithfully on E if and only if $[E : F] = |G|$. To see that this is equivalent to Definition 2.2, first assume E/F is classically Galois. Set $n = |G|$, write $G = \{x_1, \dots, x_n\}$ and let $\{b_1, \dots, b_n\}$ be a basis of E/F. Let $\{p_1, \dots, p_n\} \subset \mathbf{k}^G$ be the dual basis to the $\{x_i\} \subset \mathbf{k}G$. The action of G on E determines the corresponding coaction $\rho\colon E \to E \otimes_{\mathbf{k}} \mathbf{k}^G$ via $\rho(a) = \sum_{i=1}^n (x_i \cdot a) \otimes p_i$, and thus the Galois map $\beta\colon E \otimes_F E \to E \otimes_{\mathbf{k}} \mathbf{k}^G$ is given by $\beta(a \otimes b) = \sum_i a(x_i \cdot b) \otimes p_i$. Thus if $w = \sum_j a_j \otimes b_j \in \operatorname{Ker} \beta$, then $\sum_j a_j (x_j \cdot b_j) = 0$ for all i, by the independence of the $\{p_i\}$. Since G acts faithfully, Dedekind's lemma on independence of automorphisms gives that the $n \times n$ matrix $C = [x_i \cdot b_j]$ is invertible. Thus $a_j = 0$ for all j, and so $w = 0$. Thus β is injective, and so bijective since both tensor products are finite-dimensional F–algebras.

The converse is easier: assume that Definition 2.2 holds, that is, $F \subset E$ is a right $\mathbf{k}^G$–comodule algebra via $\rho(a) = \sum_{h \in G} a_h \otimes p_h$ such that $F = E^{\operatorname{co} \mathbf{k}^G}$, and the Galois map $\beta\colon E \otimes_F E \to E \otimes_{\mathbf{k}} \mathbf{k}^G$ in Definition 2.2 is bijective. The dual action of G is then given by $g \cdot a = \sum_h \langle g, p_h \rangle a_h = a_g$. Thus $g \cdot a = a$ for all $g \in G$ if and only if $a_g = a$, for all g if and only if $\rho(a) = a \otimes (\sum_{h \in G} p_h) = a \otimes 1$. That is, $E^{\operatorname{co} \mathbf{k}^G} = F = E^G$. The bijectivity of β implies that the F–ranks of $E \otimes_F E$ and $E \otimes_{\mathbf{k}} \mathbf{k}^G$ are equal, and thus $[E : F] = |G|$. Thus E/F is G–Galois in the usual sense.

Recall that any finite Galois field extension $F \subset E$ has a *normal basis*, that is, there exists some $u \in E$ such that the set $\{g \cdot u \mid g \in G\}$ is a basis of E over F (this is a classical result of Kummer). Equivalently, E is a cyclic FG–module. We will consider a Hopf version of this property in Definition 3.4.

Surprisingly, it is possible for a finite separable field extension $F \subset E$ to be H–Galois for some H although it is not Galois in the classical sense. The following example is due to Greither and Pareigis [10]; an exposition also appears in Pareigis [24].

Example 2.4 *Separable Galois field extensions without groups* For any $\mathbf{k}$, let $H_{\mathbf{k}}$ denote the Hopf algebra with algebra structure given by $H_{\mathbf{k}} = \mathbf{k}[c, s]/(c^2 + s^2 - 1, cs)$ and with coalgebra structure given by $\triangle c = c \otimes c - s \otimes s$, $\triangle s = c \otimes s + s \otimes c$, $\varepsilon(c) = 1$, $\varepsilon(s) = 0$, $S(c) = c$, and $S(s) = -s$; $H_{\mathbf{k}}$ is called the *circle Hopf algebra*.

Now let $F = \mathbb{Q} = \mathbf{k}$ and $E = F(\omega)$, where ω is the real 4–th root of 2; $F \subset E$ is not Galois for any group G. However, it is $(H_{\mathbb{Q}})^*$–Galois. In this case $H_{\mathbb{Q}}$ acts on E in

the following way:

$\cdot$	1	ω	ω^2	ω^3
c	1	0	$-\omega^2$	0
s	0	$-\omega$	0	ω^3

It is shown in [10] that $\mathbb{Q} \subset E$ is $H_{\mathbb{Q}}^*$–Galois. Note that this extension has a normal basis in the more general sense, that is, it is a cyclic $H_{\mathbb{Q}}$–module with generator $u = 1 + \omega + \omega^2 + \omega^3$.

Note also that when $\mathbf{k} = \mathbb{Q}(i)$, $H_{\mathbf{k}} \cong \mathbf{k}\mathbb{Z}_4$, the group algebra, that is, $\mathbb{Q}\mathbb{Z}_4$ and $H_{\mathbb{Q}}$ are $\mathbb{Q}(i)$–forms of each other.

In fact $\mathbb{Q} \subset E$ is also H^*–Galois for a second Hopf algebra H; this second Hopf algebra is a $\mathbb{Q}(\sqrt{-2})$–form of $\mathbb{Q}[\mathbb{Z}_2 \times \mathbb{Z}_2]$. Thus an extension can be Hopf Galois with two different Hopf algebras. On the other hand, there exist separable field extensions which are not Hopf Galois at all. Conditions for exactly when an extension is Hopf Galois are given in [24].

Example 2.5 *Graded rings* Let G be any group and let A be a G–graded algebra as in Example 1.2, with $H = \mathbf{k}G$ and $A^{\mathrm{co}\,H} = A_1$. A result of Ulbrich describes when the extension $A_1 \subset A$ is H–Galois:

Theorem 2.6 [37; 20, 8.1.7] *$A_1 \subset A$ is $\mathbf{k}G$–Galois if and only if A is strongly graded, that is, $A_x A_y = A_{xy}$, for all $x, y \in G$.*

Strongly graded algebras are known to have many nice properties; in particular their module theory is very well behaved. We give several examples.

Example 2.7 *Crossed products over groups* Let G be a group acting as (twisted) automorphisms of the $\mathbf{k}$–algebra R, that is, there exists a 2–cocycle $\sigma\colon G \times G \to R$ such that σ and the action $\cdot$ of G on A satisfy the following:

(1) (Cocycle condition) For all $g, h, k \in G$,

$$[g \cdot \sigma(h,k)]\sigma(g,hk) = \sigma(g,h)\sigma(gh,k) \text{ and } \sigma(g,1) = \sigma(1,g) = 1.$$

(2) (Twisted module condition) For all $g, h \in G$ and $r \in R$,

$$g \cdot (h \cdot r) = \sigma(g,h)(gh \cdot r)\sigma(g,h)^{-1}.$$

The crossed product $A = R * G$ is then defined to be $A = R \otimes_{\mathbf{k}} \mathbf{k}G$ as a $\mathbf{k}$–space, with multiplication given by

$$(r * g)(s * h) = r(g \cdot s)\sigma(g, h) * gh,$$

for $r, s \in R$, $g, h \in G$.

Notice that σ has values in the ring R, which may be noncommutative.

Any crossed product $A = R * G$ is a G–graded algebra, with $A_g = R \otimes g$ and $A_1 = R \otimes 1_g \cong R$. Clearly A is strongly G–graded, and so $R \subset A$ is $\mathbf{k}^G$–Galois.

Example 2.8 Group crossed products arise naturally from any group extension. That is, let G be any group with normal subgroup N and quotient $L = G/N$. We claim that $A = \mathbf{k}G = \mathbf{k}N * \mathbf{k}L$.

Fix a set of coset representatives $T = \{g_i\}$ for N in G, so that if $l_i \in L$, then $l_i = g_i N$. If $l_i l_j = l_k$, then $l_i l_j = g_i N g_j N = g_i g_j N = g_k N = N g_k$; however $g_i g_j = \sigma(l_i, l_j) g_k$ for some $\sigma(l_i, l_j) \in N$. It is then easy to see that the function $\sigma\colon L \times L \to N$ satisfies the conditions in Example 2.7. If the extension does not split, then the cocycle will be nontrivial.

Crossed products are "transitive" in the sense that if $R * G$ is a crossed product over G and $L = G/N$, then we may find a new cocycle $\tau\colon L \times L \to R * N$ such that $R * G \cong (R * N) * L$.

Note that if $A = R * G$, then A is free over $R = A_1$ of rank $|G|$. Using this fact it is easy to see that not all strongly graded algebras are crossed products.

Example 2.9 Let $A = M_3(\mathbf{k})$ and let $G = \{1, g\} \cong \mathbb{Z}_2$. A is G–graded by setting

$$A_1 = \begin{bmatrix} \mathbf{k} & \mathbf{k} & 0 \\ \mathbf{k} & \mathbf{k} & 0 \\ 0 & 0 & \mathbf{k} \end{bmatrix} \quad \text{and} \quad A_g = \begin{bmatrix} 0 & 0 & \mathbf{k} \\ 0 & 0 & \mathbf{k} \\ \mathbf{k} & \mathbf{k} & 0 \end{bmatrix}.$$

A is strongly graded, and so $A_1 \subset A$ is Galois by Theorem 2.6. However A is not free over A_1 since $5 \nmid 9$, and so A is not a crossed product over A_1.

Example 2.10 A similar example works for any finite group G. Let $|G| = n$ and let $A = M_n(B)$, the $n \times n$ matrices over another algebra B. Fix an ordering $\{x_1, \ldots, x_n\}$ of G, and index the rows and columns of A by G. Let $\{e_{xy} \mid x, y \in G\}$ denote the usual matrix units. For each $x \in G$, define $A_x := \sum_{yz^{-1}=x} B e_{yz}$. Then $A = \bigoplus_x A_x$ is a G–graded algebra. Note that $A_1 = \bigoplus_x B e_{xx}$.

In fact A is strongly graded. This follows since for any $y \in G$, $e_{yy} = e_{y,x^{-1}y}e_{x^{-1}y,y} \in A_x A_{x^{-1}}$. Thus $1 = \sum_y e_{yy} \in A_x A_{x^{-1}}$ and so $A_1 = A_x A_{x^{-1}}$. It follows that A is strongly graded, and so $A_1 \subset A$ is Galois.

When $G = \mathbb{Z}_n$, it is easy to see what the graded components of A look like. Symbolically:

$$A = \begin{bmatrix} A_{\bar{0}} & A_{\bar{1}} & \cdots & A_{\overline{n-1}} \\ A_{\overline{n-1}} & A_{\bar{0}} & \cdots & A_{\overline{n-2}} \\ \cdots & \cdots & \cdots & \cdots \\ A_{\bar{1}} & A_{\bar{2}} & \cdots & A_{\bar{0}} \end{bmatrix}$$

Thus $A_1 = A_{\bar{0}}$ consists of all diagonal matrices.

We investigate in Section 3 just when a Galois extension is a crossed product.

Example 2.11 *Groups acting on sets* The Galois map β can be viewed as the dual of a natural map arising whenever a group G acts on a set X. For, write the action $\mu\colon X \times G \to X$ by $(x, g) \mapsto x \cdot g$, and consider the natural map

$$\alpha\colon X \times G \to X \times X$$

given by $(x, g) \mapsto (x, x \cdot g)$. The image of α is $X \times_Y X$, the fiber product of X with itself over Y, where $Y = X/G$ is the set of G–orbits on X. Moreover α is injective if and only if the action is free, that is, no $g \neq 1$ in G has any fixed point. For example, if $G \subset X$ are groups, G acts freely on X by translation.

We now dualize this set-up; for simplicity assume that X and G are finite. Let $H = \mathbf{k}^G$ and let $A = \mathbf{k}^X$, the algebra of functions from X to $\mathbf{k}$ under pointwise addition and multiplication. The G–action on X induces a left G–action on A, given by $(g \cdot a)(x) = a(x \cdot g)$, and thus a right H–coaction $\mu^*\colon A \to A \otimes_{\mathbf{k}} H$. If we let $B = \mathbf{k}^Y$, the functions from X to $\mathbf{k}$ which are constant on G–orbits, then it follows that $B = A^G = A^{\mathrm{co}\,H}$. Since for any sets T and U, $\mathbf{k}^{T \times U} \cong \mathbf{k}^T \otimes_{\mathbf{k}} \mathbf{k}^U$, we see that the map α dualizes to

$$\alpha^*\colon A \otimes_B A \to A \otimes_{\mathbf{k}} H.$$

It is now straightforward, using the definition of the transpose of a map, to verify that $\alpha^*(a \otimes b) = (a \otimes 1)\mu^*(b)$. Thus $\alpha^* = \beta$, our Galois map, and by the remarks in the previous paragraph, β is bijective if and only if $\alpha\colon X \times G \to X \times_Y X$ is bijective if and only if the G–action is free.

Example 2.12 *Algebraic group schemes* Now consider Example 1.4. Let X be an affine scheme and G an affine algebraic group scheme, that is, $X = \operatorname{Spec} A$ and $G = \operatorname{Spec} H$ for A a commutative affine $\mathbf{k}$–algebra and H a commutative affine $\mathbf{k}$–Hopf algebra. An action $\mu\colon X \times G \to X$ is determined by a coaction

$$\rho = \mu^*\colon A \to A \otimes_{\mathbf{k}} H.$$

The coaction ρ is *free* if

$$\alpha^*\colon A \otimes_{\mathbf{k}} A \to A \otimes_{\mathbf{k}} H,\ a \otimes b \mapsto (a \otimes 1)\rho(b)$$

is surjective, since dually this means that

$$\alpha\colon X \times G \to X \times X,\ (x, g) \mapsto (x, x \cdot g)$$

is a closed embedding, and so free as in the previous example.

However, we cannot use $\beta = \alpha^*$ as we did in Example 2.11 since the domain of α is not $A \otimes_B A$, for $B = A^{\operatorname{co} H}$. The *affine quotient* of X by G is defined to be $Y := \operatorname{Spec} B$, that is, the sequence

$$B \hookrightarrow A \underset{\otimes 1}{\overset{\rho}{\rightrightarrows}} A \otimes_B A$$

is exact. This corresponds to an exact sequence of affine schemes

$$X \times G \underset{\pi}{\overset{\mu}{\rightrightarrows}} X \to Y$$

where $\pi(x, g) = x$. How is this affine quotient Y related to the true quotient X/G? In general, Y may be much smaller than X/G (for example if $X = \mathrm{GL}_2(\mathbf{k})$ and G consists of the upper triangular matrices in X, then Y is just a point but $X/G \approx \mathbb{P}^1$). Given a free action as above, it will happen that $Y = X/G$ provided the map $X \times G \to X \times_Y X$ is an isomorphism and $X \to Y$ is faithfully flat; in this case one says that X is a *principal fibre bundle* over Y with group G. The algebraic version of these conditions says that

(a) $\beta\colon A \otimes_B A \to A \otimes_{\mathbf{k}} H$ is bijective (and so $B \subset A$ is Galois), and

(b) A is a faithfully flat B–module.

Faithfully-flat Galois extensions are very important and are considered in more detail in Section 5.

Example 2.13 *Differential Galois theory* Let $E \supset \mathbf{k}$ be a field of characteristic $p > 0$, and let $\mathfrak{g} \subset Der_{\mathbf{k}} E$ be a restricted Lie algebra of $\mathbf{k}$–derivations of E which is finite-dimensional over $\mathbf{k}$. The restricted enveloping algebra $u(\mathfrak{g})$ acts on E via $\mathfrak{g}$ acting as derivations, and so we consider its dual $H = u(\mathfrak{g})^*$. The H–coinvariants are

$$E^{\mathfrak{g}} = \{a \in E \mid x \cdot a = 0, \text{ all } x \in \mathfrak{g}\}.$$

Note that we are already assuming that $\mathfrak{g}$ acts faithfully on E; however unlike the situation for groups, this does not suffice for $E^{\mathfrak{g}} \subset E$ to be an H–Galois extension, as the following example shows:

Let $E = \mathbb{Z}_2(z)$, rational functions over $\mathbf{k} = \mathbb{Z}_2$, and let $\mathfrak{g}$ be the $\mathbf{k}$–span of $d_1 = \frac{d}{dz}$ and $d_2 = z\frac{d}{dz}$. Over $\mathbb{Z}_2$, $\mathfrak{g}$ is the 2–dim solvable Lie algebra with relation $[d_1, d_2] = d_1$; it is restricted since $d_1^2 = 0$ and $d_2^2 = d_2$. Now $E^{\mathfrak{g}} = \mathbb{Z}_2(z^2)$, and $E^{\mathfrak{g}} \subset E$ is not H–Galois. For, $E \otimes_{\mathbf{k}} u(\mathfrak{g})^* \cong E \otimes_{E^{\mathfrak{g}}} (E^{\mathfrak{g}} \otimes_{\mathbf{k}} u(\mathfrak{g})^*)$ is 8–dim over $E^{\mathfrak{g}}$ but $E \otimes_{E^{\mathfrak{g}}} E$ is 4–dim over $E^{\mathfrak{g}}$, so β is not a bijection.

The difficulty with this example is that d_1 and d_2 are dependent over E; when $\mathbf{k}$–independent derivations remain independent over E, the extension will be Galois. The next result follows from [20, 8.3.5 and 8.3.7]:

Theorem 2.14 *$E^{\mathfrak{g}} \subset E$ is $u(\mathfrak{g})^*$–Galois if and only if $E \otimes_{\mathbf{k}} \mathfrak{g} \to \operatorname{Der} E$ is injective.*

This result differs from Jacobson's classical result on Galois theory for inseparable field extensions (see Abe [1, Chapter 5]); for he assumes that $\mathfrak{g}$ is an E–space, and then obtains a Galois correspondence theorem between intermediate fields and restricted Lie subalgebras.

Example 2.15 Galois extensions for the Taft Hopf algebras (Example 1.6) were studied by Masuoka [16] and for the quantum enveloping algebra $u_q(\mathfrak{sl}_2)$ (Example 1.7) by Günther [11]. Schauenburg [27] extended their results to the Drinfel′d double of the Taft algebra.

3 Normal bases, integrals and Hopf crossed products

A classical theorem in Galois theory says that if $F \subset E$ is a finite Galois extension of fields with Galois group G, then E/F has a normal basis: that is, there exists $a \in E$ such that the set $\{x \cdot a \mid x \in G\}$ is a basis for E over F. In this section we consider this property for H–extensions.

We first review some basic facts about finite-dimensional Hopf algebras, going back to Larson and Sweedler [14].

Definition 3.1 The space of *left integrals* in H is

$$\int_H^l = \{\lambda \in H \mid h\lambda = \varepsilon(h)\lambda, \text{ for all } h \in H\};$$

similarly the space of *right integrals* in H is

$$\int_H^r = \{\rho \in H \mid \rho h = \varepsilon(h)\rho, \text{ for all } h \in H\}.$$

When H is finite-dimensional, both $\int_H^l$ and $\int_H^r$ are always 1–dimensional, and if $0 \neq \lambda \in \int_H^l$, then H is a cyclic left H^*–module with generator λ for the standard action $\rightharpoonup$ of H^* on H, that is, $H = H^* \rightharpoonup \lambda$. Another result of [14] is that H is a semisimple algebra if and only if $\varepsilon(\int_H^l) \neq 0$; this fact generalizes the classical theorem of Maschke for finite groups. In this case also $\int_H^l = \int_H^r$, and we may choose λ with $\varepsilon(\lambda) = 1$.

(If H is infinite-dimensional, then it cannot contain a nonzero integral. However one may still define a (left) integral *on* H; this is a functional $f \in H^*$ such that $f * g = f(1)g$, for all $g \in H^*$. If there exists an integral on H, H is called *co-Frobenius*.)

Example 3.2 Let G be a finite group. If $H = \mathbf{k}G$, we may use $\lambda = \rho = \sum_g g$; if also $\operatorname{char}(\mathbf{k}) \nmid |G|$, then we may use $\lambda = (1/|G|)\sum_g g$, so that $\varepsilon(\lambda) = 1$. If $H = \mathbf{k}^G$, then we may use $\lambda = p_1$.

Example 3.3 Recall the Taft Hopf algebras from Example 1.6. The Taft algebras are not semisimple (since x generates a nilpotent ideal) and in fact $\int_H^l \neq \int_H^r$; one may check that

$$\lambda = \Big(\sum_{i=0}^{n-1} g^i\Big)x^{n-1} \in \int_H^l, \quad \rho = x^{n-1}\Big(\sum_{i=0}^{n-1} g^i\Big) \in \int_H^r, \quad \text{but } \lambda \notin \mathbf{k}\rho.$$

One possible definition of normal basis for a right H–extension $B \subset A$ is to simply extend the classical definition for groups. That is, assume that H is finite-dimensional and dualize to an action of H^* on A with $A^{H^*} = B$. Then A has a *classical* normal basis over B if, for some $u \in A$ and basis $\{f_i\}$ of H^*, $\{f_1 \cdot u, \ldots, f_n \cdot u\}$ is a basis for the free left B–module A.

However, it is more useful to replace this definition by a coaction version.

Definition 3.4 [13] Let $B \subset A$ be a right H–extension. We say that the extension has the (right) *normal basis property* if $A \cong B \otimes_{\mathbf{k}} H$ as left B–modules and right H–comodules.

The two definitions of normal basis are equivalent when H is finite-dimensional.

Lemma 3.5 *Let* $\dim H = n < \infty$ *and let* $B \subset A$ *be an* H*–extension. Consider* H^* *acting on* A *with* $A^{H^*} = B$*. Then* A *has a normal basis over* B *in the classical sense if and only if* A *has a normal basis over* B *in the sense of Definition 3.4.*

We sketch the proof: assume that A has a normal basis over B in the classical sense, and let $u \in A$ and basis $\{f_i\}$ of H^* be such that $\{f_1 \cdot u, \dots, f_n \cdot u\}$ is a basis for the free left B–module A. We may then define

$$\phi\colon B \otimes_{\mathbf{k}} H \to A \quad \text{by} \quad b \otimes (f \rightharpoonup \lambda) \mapsto b(f \cdot u).$$

$B \otimes_{\mathbf{k}} H$ is a left H^*–module via $f \cdot (b \otimes h) = b \otimes (f \rightharpoonup h)$; this is the dual of the right comodule structure given by $\mathrm{id} \otimes \triangle$. Thus since ϕ is a left H^*–module map, it is a right H–comodule map. It is clearly a left B–module isomorphism, and thus $B \subset A$ has the normal basis property in Definition 3.4. The converse is similar.

We next consider crossed products for arbitrary Hopf algebras, generalizing the construction for group actions in Example 2.7.

Example 3.6 *Hopf crossed products* Let H be a Hopf algebra and R an algebra which is an H–module via $\cdot$. Assume that there exists a map $\sigma\colon H \otimes_{\mathbf{k}} H \to R$ such that σ and the action $\cdot$ satisfy the following:

(1) (Hopf 2–cocycle condition) For all $g, h, k \in H$,

$$\sum_{g,h,k} [g_1 \cdot \sigma(h_1, k_1)]\sigma(g_2, h_2 k_2) = \sum_{g,h,k} \sigma(g_1, h_1)\sigma(g_2 h_2, k)$$

and $\sigma(g, 1) = \sigma(1, g) = \varepsilon(g)1$.

(2) (Hopf twisted module condition) For all $g, h \in H$ and $a \in R$,

$$g \cdot (h \cdot r) = \sum_{g,h} \sigma(g_1, h_1)(g_2 h_2 \cdot r)\sigma(g_3, h_3)^{-1}.$$

The *crossed product* $A = R \#_\sigma H$ is then defined to be $A = R \otimes_{\mathbf{k}} H$ as a $\mathbf{k}$–space, with multiplication given by

$$(r \# g)(s \# h) = \sum_{g,h} r(g_1 \cdot s)\sigma(g_2, h_2) \# g_3 h_2,$$

for $r, s \in R$, $g, h \in H$.

We note that Hopf cocycles were first introduced by Sweedler [33] for the case when H was cocommutative and R was commutative.

Now $R \subset A$ is a right H–extension, via $\delta\colon A \to A \otimes_{\mathbf{k}} H$ given by

$$r \# h \mapsto \sum (r \# h_1) \otimes h_2,$$

and clearly it has a normal basis as in Definition 3.4. For more details see Montgomery [20, Chapter 7].

Example 3.7 Two important special cases of crossed products are *smash products* $R \# H$ and *twisted products* $R_\sigma H$. In a smash product, the cocycle σ is trivial, that is, $\sigma(g,h) = \varepsilon(g)\varepsilon(h)$. In this case, R is an H–module as usual, that is, $g\cdot(h\cdot r) = (gh)\cdot r$. In addition the multiplication is simply

$$(r \# g)(s \# h) = \sum_{g,h} r(g_1 \cdot s) \# g_2 h.$$

Smash products are considered in more detail in Section 4.

In a twisted product, the action is trivial but the cocycle is not. Thus multiplication is given by

$$(r \otimes g)(s \otimes h) = \sum_{g,h} rs\ \sigma(g_1, h_1) \otimes g_2 h_2.$$

If $R = \mathbf{k}$, the resulting algebra is sometimes called a *twisted Hopf algebra* H_σ; it is not in general a Hopf algebra. However in Definition 6.9 we will see that one may always obtain a new Hopf algebra by "double-twisting" the multiplication with a 2–cocycle $\sigma\colon H \otimes_{\mathbf{k}} H \to \mathbf{k}$.

The next theorem, which characterizes Galois extensions with the normal basis property, combines work of Doi and Takeuchi [7] and of Blattner and Montgomery [3].

Theorem 3.8 *Let $B \subset A$ be an H–extension. Then the following are equivalent:*

(1) *$B \subset A$ is H–Galois and has the normal basis property.*

(2) *$A \cong B \#_\sigma H$, a crossed product of A with H.*

(3) *The extension $A \subset B$ is H–cleft, that is, there exists an H–comodule map $\gamma\colon H \to B$ which is convolution invertible.*

Any crossed product is "cleft" using the convolution invertible map $\gamma\colon H \to A$ given by $\gamma(h) = 1\#h$. The proof that crossed products are Galois uses the map $\gamma(h) = \phi(1\otimes h)$, where ϕ is the map in the proof of Lemma 3.5. See Montgomery [20, Section 8.2] for details.

The theorem gives a new view of classical Galois field extensions:

Example 3.9 Let $F \subset E$ be a classical Galois field extension, with (finite) Galois group G. By Example 2.3 we know E/F is H–Galois for $H = \mathbf{k}^G$, and by Lemma 3.5 we know E/F has the normal basis property in the sense of Definition 3.4. Thus E is a crossed product of F with H. Since E is commutative, the action of H is trivial. Thus in fact $E \cong F_\sigma[H]$, a twisted product with H.

The crossed product multiplication and the cocycle for $F \subset E$ may be constructed explicitly as in [8; 20], using the "cleft" map $\gamma(h) = \phi(1 \otimes h) \in E$ as above. Choose $u \in E$ such that the set $\{x \cdot u \mid x \in G\}$ is a normal basis of E over F. Since $p_1 \in \int_H$ and $p_x = x^{-1} \rightharpoonup p_1$, it follows that

$$\gamma(p_x) = \phi(1 \otimes (x^{-1} \rightharpoonup p_1)) = x^{-1} \cdot u.$$

The cocycle σ may then be determined from the crossed-product multiplication above:

$$(x^{-1} \cdot u)(y^{-1} \cdot u) = \gamma(p_x)\gamma(p_y) = \sum_{z \in G} \sigma(p_{xz^{-1}}, p_{yz^{-1}})(z^{-1} \cdot u).$$

These equations are solvable. For, the structure constants $a^z_{x,y} \in F$ of E/F with respect to the normal basis $\{x \cdot u\}$, that is, the solutions of $(x \cdot u)(y \cdot u) = \sum_{z \in G} a^z_{x,y}(z \cdot u)$, satisfy the condition $a^z_{x,y} = a^1_{z^{-1}x, z^{-1}y}$ since the elements of G are automorphisms of E over F. Thus we can set $\sigma(p_x, p_y) = a^1_{x^{-1}, y^{-1}}$.

Example 3.10 Crossed products arise from any exact sequence of finite-dimensional Hopf algebras. Let $K \subset H$ be a Hopf subalgebra of H which is *normal*, that is, K is stable under the Hopf adjoint action $ad_h(k) = \sum h_1 k S(h_2)$, for all $h \in H$, $k \in K$. Then $I = HK^+ = K^+H$ is a Hopf ideal of H, and we let $\bar{H} := H/I$ denote the quotient. The exact sequence is then

$$K \hookrightarrow H \twoheadrightarrow \bar{H}.$$

By work of Schneider [32], there exists a cocycle $\sigma\colon \bar{H} \otimes_{\mathbf{k}} \bar{H} \to K$ such that $H \cong K \#_\sigma \bar{H}$. Unlike the case of crossed products over groups, this is a highly nontrivial fact and is false if H is not finite-dimensional. In fact there are old examples which show that a Hopf algebra need not be free over a Hopf subalgebra.

We remark at this point that not all quotient Hopf algebras H/I arise from normal Hopf subalgebras K. To see this, consider $H = \mathbf{k}^G$ for G a finite group. A Hopf surjection $\pi\colon H \to H/I$ arises from an injection $(H/I)^* \hookrightarrow H^* \cong \mathbf{k}G$, that is from a subgroup $M \subset G$. Simply choose G with a nonnormal subgroup M. Then for $\pi\colon \mathbf{k}^G \to \mathbf{k}^M$ given by restriction, $I = \ker(\pi)$ does not come from a Hopf subalgebra of H.

Remark 3.11 Hopf crossed products do not have the "transitivity" property of group crossed products noted at the end of Example 2.8. That is, there exist crossed products $R \#_\sigma H$, with H in an exact sequence as in Example 3.10, such that there does not exist a cocycle τ from $\bar{H}$ to $R \#_\sigma K$ such that $R \#_\sigma H \cong (R \#_\sigma K) \#_\tau \bar{H}$. See Schneider [32]. This is a problem since, for example, one would like to use inductive arguments on $\dim H$. One way around this difficulty is to use Hopf Galois extensions instead; see Section 5.

4 Actions of H and Morita equivalence

In this section we assume that H is finite-dimensional and that A is an H–module algebra (and thus an H^*–comodule; a purely coaction approach to some of the results in this section is given in Section 5). In the situation of actions, there are two other algebras which arise naturally: one is the algebra of invariants A^H, and the other is the smash product $A\#H$ as in Example 3.7. We will see that for a Hopf Galois extension, there is a close connection between these two algebras, in terms of their categories of modules.

We first discuss several other conditions which are equivalent to $A^H \subset A$ being H^*–Galois; most of these conditions are the Hopf versions of ones considered by Chase, Harrison and Rosenberg [4] in their Galois theory of groups acting on commutative rings.

We may view $A \in {}_{A\#H}\mathcal{M}$, the category of left $A\#H$–modules, by defining the action of $A\#H$ on A by

$$(a\#h)\cdot b = a(h\cdot b) \tag{4.1}$$

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

A is a right A^H–module via right multiplication, and thus we may consider $A \in {}_{A\#H}\mathcal{M}_{A^H}$, the category of $(A\#H, A^H)$–bimodules. The action of $A\#H$ determines an algebra map

$$\pi\colon A\#H \to \mathrm{End}({}_{A^H}A)$$

Lemma 4.2 *Let H be finite-dimensional and A an H–module algebra. Then $A^H \cong \mathrm{End}({}_{A\#H}A)^{\mathrm{op}}$ as algebras.*

We also need a generalization of the *trace* function for a group action. Recall that if a finite group G acts on an algebra A,

$$\mathrm{tr}\colon A \to A^G \quad \text{is given by} \quad a \mapsto \sum_{g\in G} g\cdot a.$$

We may rephrase this by writing $\mathrm{tr}(a) = \lambda\cdot a$, where $\lambda = \sum g$ is an integral in $\mathbf{k}G$, as in Definition 3.1. This formulation generalizes:

Definition 4.3 Let $\lambda \neq 0$ be a left integral in H. A map $\widehat{\lambda}\colon A \to A^H$ given by $\widehat{\lambda}(a) = \lambda\cdot a$ is called a (left) *trace function* for H on A.

It is easy to see that the map $\widehat{\lambda}\colon A \to A$ is an A^H–bimodule map with values in A^H.

Our next lemma comes from [6]; it generalizes a well-known fact for group actions. Note that in a smash product $A\#H$, we frequently write a for $a\#1$ and h as $1\#h$. Thus ahb means $(a\#h)(b\#1)$.

Lemma 4.4 [6] *Let H be finite-dimensional acting on A and assume that $\widehat{\lambda}\colon A \to A^H$ is surjective. Then there exists a nonzero idempotent e in $A\#H$ such that $e(A\#H)e = A^H e \cong A^H$ as algebras.*

One case in which the trace is always surjective is if H is a semisimple algebra. In that case we may assume that $\varepsilon(\lambda) = 1$, as noted in Section 1, and thus for any $a \in A^H$, $\lambda\cdot a = \varepsilon(\lambda)a = a$. The idempotent in this situation is $e = 1\#\lambda$.

We come to our first theorem giving other characterizations of Galois. We note that (1) $\Rightarrow$ (2) and (1) $\Leftrightarrow$ (4) are in [13], (2) $\Rightarrow$ (1) is in [37], and (5) appears in [7] in dual form.

Theorem 4.5 *Let H be a finite-dimensional Hopf algebra and A a left H–module algebra. Then the following are equivalent:*

(1) *$A^H \subset A$ is right H^*–Galois.*

(2) (a) *The map $\pi\colon A\#H \to \mathrm{End}({}_{A^H}A)$ is an algebra isomorphism.*
(b) *A is a finitely generated projective right A^H–module.*

(3) *A is a generator for ${}_{A\#H}\mathcal{M}$.*

(4) *If $0 \neq \lambda \in \int_H^l$, then the map*

$$[\,,\,]\colon A \otimes_{A^H} A \to A\#H,\quad a\otimes b \mapsto a\lambda b$$

is surjective.

(5) *For any $M \in {}_{A\#H}\mathcal{M}$, consider $A\otimes_{A^H} M^H$ as a left $A\#H$–module as above. Then the map*

$$\Phi\colon A\otimes_{A^H} M^H \to M,\quad a\otimes m \mapsto a\cdot m$$

is a left $A\#H$–module isomorphism.

Example 2.13 already shows that the conditions in Theorem 4.5 do not always hold when $H = u(\mathfrak{g})^*$. The next example shows that they do not always hold, even for group actions.

Example 4.6 [6] Let D be a division algebra of characteristic 2, of dimension 4 over its center Z, with an element $x \notin Z, x^2 \in Z$. Let g and h be inner automorphisms of D given by conjugation by x and $x+1$, respectively. Let $G = \langle g, h\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$; then the Hopf algebra $H = ZG$ acts on D. Now $D^H = \mathrm{Cent}_D(x) = Z[x]$, so $[D : D^H] = 2$ although $\dim H = 4$. Thus by Theorem 4.5 we know that $D^H \subset D$ is not Galois.

In order to study more carefully the relationship between the module categories of A^H and $A\#H$, we will find conditions for when these two algebras are Morita equivalent. We will then see that Theorem 4.5 shows that $A^H \subset A$ being H^*–Galois gives "half" of the Morita equivalence.

Recall that two rings R, S are *Morita equivalent* if their module categories are equivalent via tensoring with a (suitable) fixed pair of bimodules. That is, there exists an (R,S)–bimodule ${}_RV_S$ and an (S,R)–bimodule ${}_SW_R$ such that the functors

$$-\otimes_R V\colon \mathcal{M}_R \to \mathcal{M}_S, \qquad -\otimes_S W\colon \mathcal{M}_S \to \mathcal{M}_R,$$
$$W\otimes_R -\colon {}_R\mathcal{M} \to {}_S\mathcal{M}, \qquad V\otimes_S -\colon {}_S\mathcal{M} \to {}_R\mathcal{M}$$

are equivalences of categories. More generally, one may consider a *Morita context*; see McConnell and Robson [18, Sections 1.1, 3.6]. The basic idea is to find a relationship between two rings via their modules which is weaker than Morita equivalence, but is still strong enough to enable the rings to share some properties.

To say that two rings R and S are connected by a Morita context means the following: we need bimodules ${}_R V_S$ and ${}_S W_R$ as above, although now we only need two bimodule maps

$$[\,,\,]\colon W \otimes_R V \to S \quad \text{and} \quad (\,,\,)\colon V \otimes_S W \to R,$$

such that for all $v, v' \in V$ and $w, w' \in W$, "associativity" holds, that is

$$v' \cdot [w, v] = (v', w) \cdot v \in V \quad \text{and} \quad [w, v] \cdot w' = w \cdot (v, w') \in W.$$

Alternatively, the existence of a Morita context is equivalent to saying that the array

$$T = \begin{bmatrix} R & V \\ W & S \end{bmatrix}$$

becomes an associative ring, by using the given module actions of R and S on V and W in the usual matrix multiplication.

A Morita context will give a Morita equivalence if and only if the two maps $[\,,\,]$ and $(\,,\,)$ are surjective.

We will see that such a set-up exists with $R = A^H$ and $S = A\#H$, for any finite-dimensional H, using $V = W = A$. Now A is a left (or right) A^H–module simply by left (or right) multiplication, and A is a left $A\#H$ module as before. To define a right $A\#H$ action which will work is a trickier matter, if λ is only a left integral and not a right integral (as in Example 3.3). Let $\alpha \in H^*$ be such that $\lambda h = \alpha(h)\lambda$. Using the left action $\rightharpoonup$ as in Section 1, we may define

$$h^\alpha := \alpha \rightharpoonup h.$$

Since α is a group-like element (check!), the map $h \mapsto h^\alpha$ is an automorphism of H. It is known that $\lambda^\alpha = S\lambda$ for $0 \neq \lambda \in \int_H^l$. We define our new right action of $A\#H$ on A by

$$a \leftarrow (b\#h) = S^{-1}h^\alpha \cdot (ab) \tag{4.7}$$

for all $a, b \in A$ and $h \in H$. This is the usual right action but with h "twisted" by α. In this notation, $\lambda a h = \lambda(a \leftarrow h)$. We now have:

Theorem 4.8 [6] *Consider A as a left (respectively right) A^H–module via left (resp. right) multiplication, as a left $A\#H$–module via* (4.1) *and as a right $A\#H$–module via* (4.7)*. Then $V = {}_{A^H}A_{A\#H}$ and $W = {}_{A\#H}A_{A^H}$, together with the maps*

$$[\,,\,]\colon A \otimes_{A^H} A \to A\#H \quad \text{given by} \quad [a,b] = a\lambda b$$

$$(\,,\,)\colon A \otimes_{A\#H} A \to A^H \qquad \text{given by} \quad (a,b) = \widehat{\lambda}(ab)$$

give a Morita context for A^H and $A\#H$.

Note that the trace function $\widehat{\lambda}$ and the ideal $A\lambda A$ of $A\#H$ play an important role here: for, $\widehat{\lambda}(A) = (A,A)$, and $A\lambda A = [A,A]$. This observation gives us a criterion for Morita equivalence (and thus for an equivalence of module categories):

Corollary 4.9 *Let A be an H–module algebra, where H is finite-dimensional, and choose $0 \neq \lambda \in \int_H^l$. If both $\widehat{\lambda}\colon A \to A^H$ is surjective and $A\lambda A = A\#H$, then $A\#H$ is Morita-equivalent to A^H.*

Corollary 4.10 *Assume that H is semisimple and that $A\#H$ is a simple algebra. Then $A^H \subset A$ is H^*–Galois and A^H is Morita equivalent to $A\#H$.*

This follows since simplicity of $A\#H$ implies that $A\lambda A = A\#H$, and semisimplicity of H implies that the trace is surjective.

We close this section by noting that Takeuchi [36] has given a version of Morita theory for comodules over coalgebras.

5 Faithfully flat Hopf Galois extensions

So far we have studied Galois extensions which have various additional properties, such as normal bases or a surjective trace. In this section, we return to our basic situation of an H–extension $B \subset A$, with comodule map $\delta\colon A \to A \otimes_{\mathbf{k}} H$ and $B = A^{\mathrm{co}\,H}$. We will study the very useful property of the extension being faithfully flat.

We first need the notion of "relative Hopf modules" .

Definition 5.1 (Y Doi) Let A be a right H–comodule algebra, with structure map $\rho\colon A \to A \otimes_{\mathbf{k}} H$. Then M is a *right (H, A)–Hopf module* if:

(1) M is a right H–comodule, via $\tau\colon M \to M \otimes_{\mathbf{k}} H$.

(2) M is a right A–module.

(3) $\tau(m \cdot a) = \tau(m) \cdot \rho(a)$, that is, τ is a right A–module map via ρ.

Let $\mathcal{M}_A^H$ denote the category of right (H, A)–Hopf modules. Analogously we may define ${}_A\mathcal{M}^H$, ${}^H\mathcal{M}_A$, and ${}_A^H\mathcal{M}$.

Example 5.2 Let N be a right B–module. Then $M = N \otimes_B A$ becomes an (A, H)–Hopf module as follows:

(1) M is a right H–comodule via $\tau = \mathrm{id} \otimes \delta$.

(2) M is a right A–module via right multiplication on A.

Note that $M^{\mathrm{co}\,H} = N$. In general an (A, H)–Hopf module is called *trivial* if $M \cong M^{\mathrm{co}\,H} \otimes_B A$.

Example 5.3 When H is finite-dimensional, it is straightforward to see that ${}_A\mathcal{M}^H = {}_{A\#H^*}\mathcal{M}$, using the usual duality as in Section 1 between right H–comodules and left H^*–modules. We may also identify $\mathcal{M}_A^H$ with $\mathcal{M}_{A\#H^*}$, although in this case one of the actions is twisted, as in the previous section.

Example 5.4 Let $H = \mathbf{k}G$ be a group algebra. Then we know that $A = \bigoplus_{g\in G} A_g$ is a G–graded algebra. The category $\mathcal{M}_A^H$ is precisely the category of G–graded right A–modules.

Example 5.5 Let G be an affine algebraic group over an algebraically closed field $\mathbf{k}$; then $G = \mathrm{Spec}(H)$ for H a commutative affine $\mathbf{k}$–Hopf algebra. The category $\mathcal{M}_A^H$ consists of those right A–modules M with a left G–action such that

$$g \cdot (m \cdot a) = (g \cdot m)(g \cdot a),$$

for all $g \in G, m \in M, a \in A$. This category is usually written as ${}_G\mathcal{M}_A$, the category of (G, A)–*modules*.

There is great interest in when the categories $\mathcal{M}_B$ and $\mathcal{M}_A^H$ are equivalent. We define the two functors

$$\Phi\colon \mathcal{M}_B \to \mathcal{M}_A^H, \quad N \mapsto A \otimes_B N$$
$$\Psi\colon \mathcal{M}_A^H \to \mathcal{M}_B, \quad M \mapsto M^{\mathrm{co}\,H}.$$

We have already seen (the dual of) a partial result on equivalence. Example 5.3 and the coaction version of Theorem 4.5, (1) $\Leftrightarrow$ (5) imply the following:

Theorem 5.6 [8] *Let H be finite-dimensional. Then $B \subset A$ is H–Galois if and only if $\Phi \circ \Psi = \mathrm{id}$.*

To get a complete equivalence, we consider the coaction version of the trace function in Definition 4.3; it is a less restrictive version of the cleft map in Theorem 3.8.

Definition 5.7 (Doi) Let A be a right H–comodule algebra. Then a (right) *total integral* for A is a right H–comodule map $\phi\colon H \to A$ such that $\phi(1) = 1$.

Lemma 5.8 *Let H be finite-dimensional with a left integral $\lambda \neq 0$. Let A be a left H–module algebra and consider A as a right H^*–comodule algebra. Then the trace $\widehat{\lambda}\colon A \to A^H$ is surjective if and only if there exists a (right) total integral $\phi\colon H^* \to A$.*

The next result, giving an equivalence of the categories $\mathcal{M}_{A^{\mathrm{co}\,H}}$ and $\mathcal{M}_A^H$, is due to Doi and Takeuchi [8].

Theorem 5.9 *Let $B \subset A$ be a right H–extension. Then the following are equivalent:*

(1) *$B \subset A$ is H–Galois and A has a total integral.*

(2) *The maps Φ and Ψ are inverse category equivalences.*

This result is similar to Corollary 4.9, although there are no longer two algebras involved, and the map Ψ is described differently.

The next theorem in its final form is due to Schneider, although Doi and Takeuchi [8] also considered when $B \subset A$ is faithfully-flat.

Theorem 5.10 [31] *Let H be a Hopf algebra with bijective antipode and A a right H–comodule algebra with $B = A^{\mathrm{co}\,H}$. Then the following are equivalent:*

(1) *$B \subset A$ is right H–Galois and A is a faithfully flat left (or right) B–module.*

(2) *The Galois map β is surjective and A is an injective H–comodule.*

(3) *The functor $\Phi\colon \mathcal{M}_B \to \mathcal{M}_A^H$ given by $N \mapsto N \otimes_B A$ is an equivalence.*

(4) *The functor $\Phi'\colon {}_B\mathcal{M} \to {}_A\mathcal{M}^H$ given by $N \mapsto A \otimes_B N$ is an equivalence.*

The most difficult part of Schneider's theorem is the equivalence of (1) and (2). This part has as a special case the following theorem on algebraic groups, due independently to Cline, Parshall and Scott and to Oberst in 1977.

Theorem 5.11 *Let* $\mathbf{k}$ *be algebraically closed, and let* $G \subset X$ *be affine algebraic groups with* G *closed in* X*. Then the quotient* X/G *is affine if and only if induction of* G*–modules to* X*–modules is exact.*

We give some idea as to why Theorem 5.11 is in fact a special case of Theorem 5.10. Oberst's version of Theorem 5.11 says that for a free action, X is a principal fibre bundle over Y with group G if and only if the functor

$$^G(-)\colon {}_{G,A}\mathcal{M} \to {}_B\mathcal{M} \quad \text{given by} \quad M \mapsto M^G$$

is exact. Here ${}_{G,A}\mathcal{M}$ is the category of left (G, A)–modules as in Example 5.5, although here the compatibility condition is $g \cdot (a \cdot m) = (g \cdot a)(g \cdot m)$. But this is the same as the category ${}_A\mathcal{M}^H$, the right H, left A–Hopf modules, for $G = \text{Spec } H$.

We consider the map β as in Example 2.12; we saw there that the condition of being faithfully-flat Hopf Galois arises naturally in considering when the quotient X/G is affine. Now in Theorem 5.10 (2), β being surjective means that the action is free, and A an injective H–comodule says that induction of modules is exact. Thus when A and H are commutative, Theorem 5.11 follows from Theorem 5.10.

There are many things that can be said about the relationship between the ideal structure of the algebra A and that of $B = A^{\text{co}\,H}$ in a faithfully-flat Hopf Galois extension. We give a few such results from [22].

If M is an H–comodule, a subspace $N \subset M$ which is also a right H–subcomodule will be called H*–costable*. If I is an ideal of B, we say that I is H*–stable* if $IA = AI$.

In the special case that $A = B \#_\sigma H$, a crossed product in which H actually acts on B, then I being H–stable in the usual way, that is $H \cdot I \subseteq I$, is equivalent to $IA = AI$. Thus the new definition generalizes the usual one.

Lemma 5.12 [22] *Let* H *be finite-dimensional and let* $B \subset A$ *be any faithfully-flat* H*–Galois extension. Then there is a bijection of sets*

$$\{H\text{–stable ideals of } B\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{H\text{–costable ideals of } A\}$$

given by $\Phi\colon I \mapsto IA = AI$*, for* I *an* H*–stable ideal of* B*, and* $\Psi\colon J \mapsto J \cap B$*, for* J *an* H*–costable ideal of* A*. These bijections preserve sums, intersections, and products.*

Another result is that transitivity of Galois extensions is true in the faithfully-flat case, unlike the situation for Hopf crossed products, as discussed in Remark 3.11. That is,

let $B \subset A$ be an H–extension, with comodule map $\delta_A\colon A \to A \otimes_{\mathbf{k}} H$, and let K be a normal Hopf subalgebra of H. Let

$$K \hookrightarrow H \twoheadrightarrow \bar{H}$$

be an exact sequence of Hopf algebras with quotient map $\pi\colon H \to \bar{H}$. Let

$$C =: \delta_A^{-1}(A \otimes_{\mathbf{k}} K).$$

Then C is a right K–comodule by restricting δ_A to C, and A becomes a right $\bar{H}$–comodule algebra using $\delta_A \circ (\mathrm{id} \otimes \pi)$.

Proposition 5.13 (Transitivity [22]) *Let $B \subset A$ be a faithfully-flat H–Galois extension and consider $B \subset C \subset A$ as above.*

(1) *$B \subset C$ is faithfully-flat K–Galois.*

(2) *$C \subset A$ is faithfully-flat $\bar{H}$–Galois.*

The above results are only a small sample of the large literature on faithfully-flat Galois extensions.

6 Hopf bi-Galois extensions and the Galois correspondence

This section discusses some recent attempts to extend the classical Galois correspondence for field extensions. We review this correspondence, for a classical Galois field extension $A/\mathbf{k}$ with Galois group G. Classically,

$$\{\text{subgroups } M \text{ of } G\} \underset{\mathcal{G}}{\overset{\mathcal{F}}{\rightleftarrows}} \{\text{intermediate fields } F \text{ with } \mathbf{k} \subseteq F \subseteq A\}\ ,$$

given by $\mathcal{F}\colon M \mapsto A^M$ and $\mathcal{G}\colon F \mapsto M = \{g \in G \mid a^g = a,\ \forall a \in F\}$. Under this correspondence, normal subgroups N of G go to "normal" extensions E of $\mathbf{k}$, that is, the extension $\mathbf{k} \subset E$ is also Galois (with group G/N).

There are a number of difficulties in extending this correspondence to the Hopf situation. The first is that we are dealing with coactions of $H = \mathbf{k}^G$ instead of actions of G, and so our intuition is not always correct. Subgroups of G determine Hopf subalgebras of $H^* = \mathbf{k}G$, and thus quotient Hopf algebras H/I of H.

Moreover, normal subgroups of G correspond to normal Hopf subalgebras of H^*, which come from *normal ideals* of H. A Hopf ideal of H is called normal if it is also a left and right coideal of H, that is, both $\triangle(I) \subset H \otimes_{\mathbf{k}} I$ and $\triangle(I) \subset I \otimes_{\mathbf{k}} H$. In this situation we also say that H/I is a *conormal quotient*.

Using this dualization, the usual Galois correspondence determines the map

$$I \mapsto A^{\mathrm{co}(H/I)} \tag{6.1}$$

which gives a bijective correspondence between quotient Hopf algebras H/I, where I is a Hopf ideal of H, and the $\mathbf{k}$–subalgebras of A (all of which are necessarily fields). Under this correspondence, conormal quotients H/I correspond to normal extensions of $\mathbf{k}$.

A second difficulty is that when H is not cocommutative, there are not "enough" Hopf subalgebras (or quotients). In the Galois correspondence this difficulty arises already for a field extension $A/\mathbf{k}$ which is H–Galois for a Hopf algebra H. At least if H is finite-dimensional, the map in Equation (6.1) is injective and inclusion-preserving. However it is not clear which intermediate fields can be obtained in this way, since in general there are not enough Hopf subalgebras to hit all the subfields. One positive result is that of [10], which states that any normal (Galois) separable field extension $A/\mathbf{k}$ is H–Galois with a Hopf algebra for which the subfields of A of the form $A^{\mathrm{co}(H/I)}$ are precisely the *normal* intermediate fields between $\mathbf{k}$ and A.

This lack of Hopf subalgebras arises in many places. One solution is to consider the right (or left) coideal subalgebras of H.

Definition 6.2 A *right coideal subalgebra* of H is a subalgebra K which is also a right coideal, that is $\triangle(K) \subseteq K \otimes_{\mathbf{k}} H$. Left coideal subalgebras are defined similarly.

Example 6.3 Recall the Taft Hopf algebras from Section 1. As an algebra

$$H = T_{n^2}(\omega) = k\langle g, x \mid g^n = 1, x^n = 0, xg = \omega g x\rangle.$$

Let $K = k\langle x\rangle \cong k[x]/(x^n)$. Certainly K is a subalgebra, and since $\Delta(x) = x \otimes 1 + g \otimes x \in H \otimes_{\mathbf{k}} K$, K is also a left coideal. Similarly, $g^{-1}x$ generates a right coideal subalgebra. However neither is a Hopf subalgebra.

Example 6.4 A similar problem arises in quantized enveloping algebras. Consider a Lie subalgebra $\mathfrak{t}$ of the Lie algebra $\mathfrak{g}$; then the enveloping algebra $U(\mathfrak{t})$ is a Hopf subalgebra of $U(\mathfrak{g})$. However in passing to the quantum case, $U_q(\mathfrak{t})$, even when it is defined, is often not isomorphic to a subalgebra of $U_q(\mathfrak{g})$. In many cases there are coideal subalgebras of $U_q(\mathfrak{g})$ which are not Hopf subalgebras but are still good quantum analogs of $U_q(\mathfrak{t})$. In particular, let $\mathfrak{g}$ be a semisimple Lie algebra with a Borel subalgebra $\mathfrak{n}^+$. Then there is a natural coideal subalgebra U^+ of $U_q(\mathfrak{g})$ which is an analog of the Hopf subalgebra $U(\mathfrak{n}^+)$ of $U(\mathfrak{g})$.

In Example 1.7, note that $\mathfrak{n} = \mathbf{k}e$ is a Borel (Lie) subalgebra of $\mathfrak{sl}_2$, and so $U(\mathfrak{n})$ is a Hopf subalgebra of $U(\mathfrak{sl}_2)$. However in $U_q(\mathfrak{sl}_2)$, the subalgebra generated by E (or F) is a coideal subalgebra which is not a Hopf subalgebra.

For a survey of the use of coideal subalgebras in quantum groups, see Letzter [15].

What is the dual notion to a (right) coideal subalgebra? Using the standard bilinear pairing between H and H^*, a right coideal subalgebra of H^* corresponds to a subcoalgebra of H which is also a left H–module. A quotient H/I of H is a left H–module subcoalgebra if and only if I is a coideal and a left ideal. Thus left ideal coideals will be objects of interest.

The third major difficulty is a "left-right" problem. To see this, let H be any Hopf algebra, let $A = H$, and consider H as a left H–Galois extension of $\mathbf{k}$. Then there are always maps

$$\{\text{Coideal left ideals } I \text{ of } H\} \underset{\mathcal{G}}{\overset{\mathcal{F}}{\rightleftarrows}} \{\text{Right coideal subalgebras } B \text{ of } H\},$$

given by $\mathcal{F}\colon I \mapsto {}^{\mathrm{co}(H/I)}H$ and $\mathcal{G}\colon B \mapsto HB^+$. The map from left to right is the analog of the Galois correspondence. In many cases, the two maps are known to be inverse bijections, at least on certain classes of coideal left ideals and right coideal subalgebras. However the map from right to left only makes sense if we know the *right* H–comodule structure of H, although we began with considering H as a *left* H–Galois extension. Thus the correspondence above does not generalize very well to the case of a general Hopf Galois extension.

The first real progress on this left-right problem was made by van Oystaeyen and Zhang [38] in the case when A was commutative and $\mathbf{k}$ a field, by constructing a second Hopf algebra $L = L(A, H)$ for which the extension is Galois on the other side. This was extended by Schauenburg [25] to the case when A was noncommutative, still assuming $B = \mathbf{k}$, a field. We begin with this case.

Definition 6.5 Let L and H be Hopf algebras over $\mathbf{k}$. An *L–H bi-Galois extension* $A/\mathbf{k}$ is an L–H bicomodule algebra such that $A/\mathbf{k}$ is both a left L–Galois and a right H–Galois extension of $\mathbf{k}$.

Theorem 6.6 [25] *For a right H–Galois extension $A/\mathbf{k}$, there exists a unique Hopf algebra $L = L(A, H)$ such that $A/\mathbf{k}$ is L–H bi-Galois.*

To construct the Hopf algebra L, first note that $A \otimes_{\mathbf{k}} A$ is an H–comodule, using the codiagonal coaction (this is the formal dual of the usual diagonal action of H on $A \otimes_{\mathbf{k}} A$). Then

$$L := (A \otimes_{\mathbf{k}} A)^{\mathrm{co}\, H}.$$

The uniqueness of L follows from the Hopf module structure theorem: using the new Galois map $\beta_L\colon A \otimes_{\mathbf{k}} A \to L \otimes_{\mathbf{k}} A$ and the isomorphism β_L, we have $L \cong (L \otimes_{\mathbf{k}} A)^{\mathrm{co}\, H}$. Then one proves that L is in fact a Hopf algebra over $\mathbf{k}$. See Schauenburg [25, 3.7].

We first give the correspondence theorem of van Oystaeyen and Zhang.

Theorem 6.7 [38] *If $\mathbf{k} \subset A$ are fields such that $A/\mathbf{k}$ is L–H bi-Galois, then there is a one-to-one correspondence*

$$\{\textit{Hopf ideals } I \textit{ of } L\} \underset{\mathcal{G}}{\overset{\mathcal{F}}{\rightleftarrows}} \{H\textit{–costable intermediate fields } F \subset A\},$$

via $\mathcal{F}(I) := {}^{\mathrm{co}(L/I)}A$ and $\mathcal{G}(F) = I$ such that $L/I = (A \otimes_F A)^{\mathrm{co}\, H}$, under the identification $L \cong (A \otimes_{\mathbf{k}} A)^{\mathrm{co}\, H}$.

Question 6.8 How close is the new Hopf algebra L to the original Hopf algebra H?

It is not difficult to see that if H is cocommutative, then $L \cong H$. Although this is not true in general, we will see below that at least when H is finite-dimensional,

$$L \cong H^{\sigma},$$

a twisted version of H. We define this twisting as follows:

Definition 6.9 Let H be a Hopf algebra and σ a Hopf cocycle $\sigma\colon H \otimes_{\mathbf{k}} H \to \mathbf{k}$, that is, σ satisfies

$$\sum_{h,k} \sigma(h_1, k_1)\sigma(g, h_2k_2) = \sum_{g,h} \sigma(g_1, h_1)\sigma(g_2h_2, k)$$

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

Then we may construct a new Hopf algebra H^{σ} from H by "double-twisting" the multiplication by σ. That is, H^{σ} has the same comultiplication $\triangle$ as H, but new multiplication, given by

$$h \star k := \sum_{h,k} \sigma(h_1, k_1)h_2k_2\sigma(h_3, k_3).$$

This construction should be contrasted with the twisted Hopf algebra H_{σ} in Example 3.7, in which H was only twisted on one side. In that case H_{σ} is not a Hopf algebra.

Remark 6.10 The construction of H^σ is due to Doi. It is the formal dual of the "twist" H^Ω, for $\Omega \in H \otimes_{\mathbf{k}} H$, introduced by Drinfel′d [9]; see Kassel [12, XV.3]. In Drinfel′d's construction, H^Ω has the same multiplication as H, but new comultiplication $\triangle^\Omega(h) = \Omega\triangle(h)\Omega^{-1}$. Viewing Ω dually as a map from $H^* \otimes_{\mathbf{k}} H^*$ to $\mathbf{k}$, it is a 2–cocycle on H^*.

It is known that for the Taft Hopf algebras in Example 1.6, $H^\sigma \cong H$ for any σ, and also that $L \cong H$. However for $H = u_q(\mathfrak{sl}_2)$ as in Example 1.7, there exists a cocycle σ such that H^σ is *not* isomorphic to H. Hopf bi-Galois theory for these two examples has been considered in [28].

Following [25, Section 5], we say that two $\mathbf{k}$–Hopf algebras H and L are *monoidally co-Morita equivalent* if their monoidal categories of comodules ${}^H\mathcal{M}$ and ${}^L\mathcal{M}$ are equivalent as monoidal $\mathbf{k}$–linear categories.

Theorem 6.11 [25] *Let H and L be $\mathbf{k}$–Hopf algebras. The following are equivalent:*

(1) *H and L are monoidally co-Morita $\mathbf{k}$–equivalent.*

(2) *There exists an L–H bi-Galois extension of $\mathbf{k}$.*

In fact Schauenburg proves that there is a bijection between monoidal isomorphism classes of $\mathbf{k}$–linear monoidal equivalences ${}^H\mathcal{M} \cong {}^L\mathcal{M}$ and isomorphism classes of L–H–bi-Galois extensions of $\mathbf{k}$.

Corollary 6.12 [25] *Assume that H is a finite-dimensional $\mathbf{k}$–Hopf algebra. Then every Hopf algebra L such that there exists an L–H bi-Galois extension of $\mathbf{k}$ is obtained from H by twisting with a 2–cocycle.*

If H is not finite-dimensional, then it is possible to have an L–H bi-Galois extension of $\mathbf{k}$ in which L is *not* a twist of H [2].

Schauenburg then extends the correspondence theorem of [38] to general L–H bi-Galois algebras $A/\mathbf{k}$. First, for the Hopf algebra L, we may identify $\mathrm{Quot}(L)$ with the set of coideals I of L. Then there are well-defined maps

$$\{\mathrm{Quot}(L)\} \underset{\mathcal{G}}{\overset{\mathcal{F}}{\rightleftarrows}} \{\mathrm{Sub}(A)\}\ ,$$

given by $\mathcal{F}(I) = {}^{\mathrm{co}(L/I)}A$ for a coideal I of C and $L/\mathcal{G}(B) := (A \otimes_B A)^{\mathrm{co}\,H}$ for B a subalgebra of A.

However in order to obtain a one-to-one correspondence, we need to restrict to suitable subsets of $\mathrm{Quot}(L)$ and of $\mathrm{Sub}(A)$. For a coalgebra C and a quotient coalgebra $C \to \overline{C}$, we say $\overline{C}$ is left (right) *admissible* if C is right (left) faithfully coflat over $\overline{C}$, where recall that a comodule being coflat is defined in terms of the cotensor product. Then a coideal $I \subset C$ is right (left) admissible if C/I is admissible.

Theorem 6.13 [26, 3.6] *Let H and L be Hopf algebras with bijective antipodes and let A be an L–H bi-Galois extension of $\mathbf{k}$. Then the maps $\mathcal{F}$ and $\mathcal{G}$ give a one-to-one correspondence between the (left, right) admissible coideal left ideals $I \subset L$, and those H–subcomodule algebras $B \subset A$ such that A is (left, right) faithfully flat over B.*

In fact Schauenburg only assumes in [26] that $\mathbf{k}$ is a commutative ring, although of course some additional assumptions are then needed.

For further reading, there are several longer survey papers with many proofs, such as Schauenburg [29] and Schauenburg and Schneider [30].

7 Another approach to the Galois correspondence

We note that there is an alternate approach to Galois theory for Hopf algebras. Inspired by work of Noether in the 1930's, Cartan and Jacobson looked at the Galois correspondence for automorphism groups of division algebras in the 1940's. This was extended to simple Artinian rings in the 1950's. A major difficulty was how to handle inner automorphisms of an algebra A (that is, for some unit $u \in A$, $\sigma(a) = uau^{-1}$ for all $a \in A$); such automorphisms do not arise in the commutative case. If the automorphism group is outer (that is, no nontrivial inner automorphisms), they obtained a one-to-one correspondence between subgroups and intermediate rings.

The Jacobson–Cartan Galois theory was extended in the 1960's to automorphisms of more general rings, and in fact this was the motivation of the work in [4]. Now additional trouble can arise from automorphisms which, although not inner on the algebra A itself, can become inner on some natural ring of fractions $Q(A)$ of A. We give a classical example of Rosenberg and Zelinsky:

Example 7.1 Let $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$; note that $\mathcal{O}$ is the ring of integers in the field $F = \mathbb{Q}[\sqrt{-5}]$. Let $A := M_2(\mathcal{O})$, and consider the matrix

$$u = \begin{bmatrix} 2 & -1+\sqrt{-5} \\ 1+\sqrt{-5} & -2 \end{bmatrix} \in A.$$

Then $\sigma(a) = uau^{-1}$ is an automorphism of A (of order 2) but it is not inner on A itself since $u^{-1} \notin A$. However σ becomes inner when considered as an automorphism of the quotient ring $Q(A) = M_2(F)$.

In the above example, $I = (2, -1+\sqrt{-5})$ is a nonprincipal ideal of $\mathcal{O}$. More generally, such examples can be constructed for $A = M_n(\mathcal{O})$ whenever the ring of integers $\mathcal{O}$ in a number field F contains a nonprincipal ideal with n generators. One can still obtain a nice Galois correspondence by assuming that $G \subset \mathrm{Aut}(A)$ contains no "generalized inner" automorphisms of this type. Note that in these example the quotient ring $Q(A)$ is obtained by simply inverting the nonzero scalar matrices in A.

In the 1970's and 1980's, Kharchenko extended this Galois theory to *prime rings*, that is, noncommutative rings in which the product of two nonzero ideals is always nonzero. Any prime ring R has a Martindale quotient ring $Q(R)$, generalizing the matrix example above, by inverting certain maps. An automorphism of R is then called X–*inner* if it becomes inner when extended to $Q(R)$, and an automorphism group of R is called X–*outer* if its subgroup of X–inner automorphisms is trivial. Kharchenko proved a Galois correspondence using finite groups of X–outer automorphisms; a simpler proof of his result may be found in [21]. Kharchenko also looked at derivations, although the situation there is more complicated; we already see this in Example 2.13.

Recently there have been several papers trying to extend Kharchenko's work to the Hopf case, in particular to the case when H is *pointed*. This means that all the minimal (nonzero) subcoalgebras are 1–dimensional (equivalently, any simple subcoalgebra is the $\mathbf{k}$–span of a group-like element). Examples of pointed Hopf algebras are group algebras, enveloping algebras of Lie algebras, the Taft algebras (Example 1.6) and the quantum enveloping algebras (Example 1.7). In all known examples of pointed Hopf algebras, they are generated by their group-like and skew-primitive elements, and thus the Galois theory for pointed Hopf algebras should be a natural extension of what we know for automorphisms and (skew) derivations.

In this case yet more difficulties arise, and it is no longer sufficient to consider X–outer actions. Milinski [19] proposed a more restrictive definition, now called M–*outer*. With this more restrictive notion, in fact the Galois correspondence works when H is a finite-dimensional pointed Hopf algebra. See work of Masuoka, Westreich and Yanai [17; 39; 40; 41].

References

[1] **E Abe**, *Hopf algebras*, Cambridge Tracts in Math. 74, Cambridge Univ. Press (1980) MR594432 Translated from the Japanese by H Kinoshita and H Tanaka

[2] **J Bichon**, *The representation category of the quantum group of a nondegenerate bilinear form*, Comm. Algebra 31 (2003) 4831–4851 MR1998031

[3] **R J Blattner**, **S Montgomery**, *Crossed products and Galois extensions of Hopf algebras*, Pacific J. Math. 137 (1989) 37–54 MR983327

[4] **S U Chase**, **D K Harrison**, **A Rosenberg**, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. No. 52 (1965) 15–33 MR0195922

[5] **S U Chase**, **M E Sweedler**, *Hopf algebras and Galois theory*, Lecture Notes in Math. 97, Springer, Berlin (1969) MR0260724

[6] **M Cohen**, **D Fischman**, **S Montgomery**, *Hopf Galois extensions, smash products, and Morita equivalence*, J. Algebra 133 (1990) 351–372 MR1067411

[7] **Y Doi**, **M Takeuchi**, *Cleft comodule algebras for a bialgebra*, Comm. Algebra 14 (1986) 801–817 MR834465

[8] **Y Doi**, **M Takeuchi**, *Hopf–Galois extensions of algebras, the Miyashita–Ulbrich action, and Azumaya algebras*, J. Algebra 121 (1989) 488–516 MR992778

[9] **V G Drinfel′d**, *Almost cocommutative Hopf algebras*, Algebra i Analiz 1 (1989) 30–46 MR1025154

[10] **C Greither**, **B Pareigis**, *Hopf Galois theory for separable field extensions*, J. Algebra 106 (1987) 239–258 MR878476

[11] **R Günther**, *Crossed products for pointed Hopf algebras*, Comm. Algebra 27 (1999) 4389–4410 MR1705876

[12] **C Kassel**, *Quantum groups*, Graduate Texts in Math. 155, Springer, New York (1995) MR1321145

[13] **H F Kreimer**, **M Takeuchi**, *Hopf algebras and Galois extensions of an algebra*, Indiana Univ. Math. J. 30 (1981) 675–692 MR625597

[14] **R G Larson**, **M E Sweedler**, *An associative orthogonal bilinear form for Hopf algebras*, Amer. J. Math. 91 (1969) 75–94 MR0240169

[15] **G Letzter**, *Coideal subalgebras and quantum symmetric pairs*, from: "New directions in Hopf algebras", (S Montgomery, H-J Schneider, editors), Math. Sci. Res. Inst. Publ. 43, Cambridge Univ. Press (2002) 117–165 MR1913438

[16] **A Masuoka**, *Cleft extensions for a Hopf algebra generated by a nearly primitive element*, Comm. Algebra 22 (1994) 4537–4559 MR1284344

[17] **A Masuoka**, **T Yanai**, *Hopf module duality applied to X–outer Galois theory*, J. Algebra 265 (2003) 229–246 MR1984909

[18] **J C McConnell**, **J C Robson**, *Noncommutative Noetherian rings*, revised edition, Graduate Studies in Math. 30, Amer. Math. Soc. (2001) MR1811901 With the cooperation of L W Small

[19] **A Milinski**, *Actions of pointed Hopf algebras on prime algebras*, Comm. Algebra 23 (1995) 313–333 MR1311791

[20] **S Montgomery**, *Hopf algebras and their actions on rings*, CBMS Regional Conference Series in Math. 82, Conference Board of the Math. Sciences, Washington, DC (1993) MR1243637

[21] **S Montgomery**, **D S Passman**, *Outer Galois theory of prime rings*, Rocky Mountain J. Math. 14 (1984) 305–318 MR747279

[22] **S Montgomery**, **H-J Schneider**, *Prime ideals in Hopf Galois extensions*, Israel J. Math. 112 (1999) 187–235 MR1715517

[23] **S-H Ng**, *Nonsemisimple Hopf algebras of dimension p^2*, J. Algebra 255 (2002) 182–197 MR1935042

[24] **B Pareigis**, *Forms of Hopf algebras and Galois theory*, from: "Topics in algebra, Part 1 (Warsaw, 1988)", (S Balcerzyk, T Józefiak, J Krempa, D Simson, W Vogel, editors), Banach Center Publ. 26, PWN, Warsaw (1990) 75–93 MR1171227

[25] **P Schauenburg**, *Hopf bi-Galois extensions*, Comm. Algebra 24 (1996) 3797–3825 MR1408508

[26] **P Schauenburg**, *Galois correspondences for Hopf bi-Galois extensions*, J. Algebra 201 (1998) 53–70 MR1608691

[27] **P Schauenburg**, *Galois objects over generalized Drinfeld doubles, with an application to $u_q(\mathfrak{sl}_2)$*, J. Algebra 217 (1999) 584–598 MR1700516

[28] **P Schauenburg**, *Bi-Galois objects over the Taft algebras*, Israel J. Math. 115 (2000) 101–123 MR1749674

[29] **P Schauenburg**, *Hopf–Galois and bi-Galois extensions*, from: "Galois theory, Hopf algebras, and semiabelian categories", (G Janelidze, B Pareigis, W Tholen, editors), Fields Inst. Commun. 43, Amer. Math. Soc. (2004) 469–515 MR2075600

[30] **P Schauenburg**, **H-J Schneider**, *Galois type extensions and Hopf algebras*, to appear in the Proceedings of the 2001 Warsaw Conference

[31] **H-J Schneider**, *Principal homogeneous spaces for arbitrary Hopf algebras*, Israel J. Math. 72 (1990) 167–195 MR1098988

[32] **H-J Schneider**, *Normal basis and transitivity of crossed products for Hopf algebras*, J. Algebra 152 (1992) 289–312 MR1194305

[33] **M E Sweedler**, *Cohomology of algebras over Hopf algebras*, Trans. Amer. Math. Soc. 133 (1968) 205–239 MR0224684

[34] **M E Sweedler**, *Hopf algebras*, Math. Lecture Note Ser., W. A. Benjamin, New York (1969) MR0252485

[35] **E J Taft**, *The order of the antipode of finite-dimensional Hopf algebra*, Proc. Nat. Acad. Sci. U.S.A. 68 (1971) 2631–2633 MR0286868

[36] **M Takeuchi**, *Morita theorems for categories of comodules*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 24 (1977) 629–644 MR0472967

[37] **K-H Ulbrich**, *Galoiserweiterungen von nichtkommutativen Ringen*, Comm. Algebra 10 (1982) 655–672 MR647213

[38] **F Van Oystaeyen**, **Y Zhang**, *Galois-type correspondences for Hopf-Galois extensions*, from: "Proceedings of Conference on Algebraic Geometry and Ring Theory in honor of Michael Artin, Part III (Antwerp, 1992)", K–Theory 8 (1994) 257–269 MR1291021

[39] **S Westreich**, *A Galois-type correspondence theory for actions of finite-dimensional pointed Hopf algebras on prime algebras*, J. Algebra 219 (1999) 606–624 MR1706837

[40] **S Westreich**, **T Yanai**, *More about a Galois-type correspondence theory*, J. Algebra 246 (2001) 629–640 MR1872117

[41] **T Yanai**, *Correspondence theory of Kharchenko and X–outer actions of pointed Hopf algebras*, Comm. Algebra 25 (1997) 1713–1740 MR1446125

Mathematics Department, University of Southern California
Los Angeles, CA 90089-1113, USA

smontgom@math.usc.edu

Received: 23 November 2009 Revised: 7 May 2009