ISRAEL JOURNAL OF MATHEMATICS, Vol. 72, Nos. 1-2, 1990

PRINCIPAL HOMOGENEOUS SPACES FOR ARBITRARY HOPF ALGEBRAS

BY

HANS-JÜRGEN SCHNEIDER

Mathematisches Institut, Universität München, Theresienstr. 39, D-8000 München 2, FRG

ABSTRACT

Let H be a Hopf algebra over a field with bijective antipode, A a right H-comodule algebra, B the subalgebra of H-coinvariant elements and can : $A \otimes_B A \to A \otimes H$ the canonical map. Then A is a faithfully flat (as left or right B-module) Hopf Galois extension iff A is coflat as H-comodule and can is surjective (Theorem I). This generalizes results on affine quotients of affine schemes by Oberst and Cline, Parshall and Scott to the case of non-commutative algebras. The dual of Theorem I holds and generalizes results of Gabriel on quotients of formal schemes to the case of non-cocommutative coalgebras (Theorem II). Furthermore, in the dual situation, a normal basis theorem is proved (Theorem III) generalizing results of Oberst–Schneider, Radford and Takeuchi.

Introduction

This paper tries to provide evidence for the following assertion:

There is a non-trivial quotient theory of arbitrary Hopf algebras coacting on arbitrary algebras or acting on arbitrary coalgebras.

Such a theory should generalize well-known results in the quotient theory of algebraic or formal groups. One should hope that there are applications of such a general theory, since nowadays arbitrary Hopf algebras occur in the guise of quantum groups.

For simplicity, assume in this introduction that k is a field. Algebras and coalgebras will be defined over k, and $\otimes = \otimes_k$.

Received July 4, 1989

Let X be an affine algebraic group scheme over k, $G \subset X$ a closed subgroup, and X/G the quotient scheme. Then it was shown by Oberst [19] and independently by Cline, Parshall and Scott [2] (for smooth groups over an algebraically closed field) that X/G is affine if and only if induction of G-modules to X-modules is exact.

More generally, let X be an affine scheme, G an affine algebraic group scheme and $\mu : X \times G \to X$ a *free action* of G on X, i.e. an action such that the canonical map can: $X \times G \to X \times X$, defined on rational points by $\mathrm{can}(x, g) := (x, x \cdot g)$, is a closed embedding. For example, if X is an affine group scheme and $G \subset X$ a closed subgroup, then G acts freely on X by translation (multiplication in X). Let Y be the quotient in the category of affine schemes. Thus

$$X \times G \underset{\mathrm{pr}}{\overset{\mu}{\rightrightarrows}} X \xrightarrow{p} Y$$

is an exact sequence of affine schemes.

The quotient map $X \to Y$ satisfies "all that one might hope for" [16], p. 16, if can: $X \times G \to X \times_Y X$ is an isomorphism, and $X \to Y$ is faithfully flat. In this case, $X \to Y$ is called a *G-torsor* [3] (in the faithfully flat topology), or a *principal homogeneous G-space* or a *principal fibre bundle with group G* [16], p. 16, and

$$X \times G \rightrightarrows X \to Y$$

is exact in the category of all schemes, hence the quotient exists in the category of schemes, and it is affine.

Oberst [19] gave a criterion in terms of representation theory of the free action for X to be a principal fibre bundle over Y with group G. This criterion generalizes the one described before in case of the quotient of a group modulo a subgroup.

These results on affine quotients are proved in [19] and [2] using the theory of affine groups. For example, in [2] the theorem of Haboush (a reductive group is geometrically reductive) was applied. Then Doi [6] gave a purely Hopf algebraic proof.

It is shown in this paper that the above results on affine quotients are particular cases of a theorem on arbitrary Hopf algebras (with bijective antipode) coacting on arbitrary algebras.

Let H be a Hopf algebra, and $\Delta_A : A \to A \otimes H$ a right *H-comodule algebra* (cf. [15], 4.5), i.e. A is an algebra, Δ_A a right H-comodule structure and an algebra map. Define $B := A^{\mathrm{co}\,H} := \{a \in A \mid \Delta_A(a) = a \otimes 1\}$, the algebra of coinvariant elements. Thus

$$B \subset A \underset{\text{in}}{\overset{\Delta_A}{\rightrightarrows}} A \otimes H$$

is exact. The canonical map can: $A \otimes_B A \to A \otimes H$ is defined by $\mathrm{can}(x \otimes y) := x \cdot \Delta_A(y)$.

Denote by $\mathcal{M}_B$ the category of right B-modules. If M is a right B-module, then the induced module $M \otimes_B A$ is an A-module and a right H-comodule in the natural way. Thus $M \otimes_B A$ is an object of $\mathcal{M}_A^H$, the category of (A, H)-*Hopf modules* (see Section 3). This defines a functor $\mathcal{M}_B \to \mathcal{M}_A^H$. Similarly, ${}_B\mathcal{M} \to {}_A\mathcal{M}^H$, $M \mapsto A \otimes_B M$, is defined.

THEOREM I. *Assume the antipode of H is bijective. Then the following are equivalent*:

(1) (a) *A is injective as right H-comodule.*
    (b) can: $A \otimes_B A \to A \otimes H$ *is surjective.*

(2) $\mathcal{M}_B \to \mathcal{M}_A^H$, $M \mapsto M \otimes_B A$, *is an equivalence.*

(3) ${}_B\mathcal{M} \to {}_A\mathcal{M}^H$, $M \mapsto A \otimes_B M$, *is an equivalence.*

(4) (a) *A is faithfully flat as left B-module.*
    (b) can *is an isomorphism.*

(5) (a) *A is faithfully flat as right B-module.*
    (b) can *is an isomorphism.*

By definition, $B \subset A$ is called an *H-Galois extension*, if can is an isomorphism. Hence Theorem I characterizes faithfully flat H-Galois extensions.

Takeuchi [29], 4.1, calls H-Galois extensions satisfying (4) or (5) in Theorem I *torsor-like*. However, in [29], (4) and (5) (for H cocommutative) are treated as different cases.

In Theorem I, the implication (4)$\Rightarrow$(2) is a general imprimitivity statement, and (1)$\Rightarrow$(4) (the main part of Theorem I) is a non-commutative version of the above-mentioned criterion for affineness.

By 3.7, (4)$\Rightarrow$(2) holds under very general assumptions over arbitrary commutative rings k. This implication was shown by Voigt in [33], 5.2, in case A and H are commutative, and by Ulbrich [32], p. 662, for H finitely generated and projective over k. 3.7 implies the imprimitivity theorem of Koppinen and Neuvonen [11] which contains the analogue of Blattner's imprimitivity theorem [1] for restricted Lie algebras (see 3.9). The oldest version of (4)$\Rightarrow$(2) (in case $A = H$) seems to be the theorem on Hopf modules in Sweedler's book

[26]. In the case of H-Galois extensions, related sufficient conditions implying (2) have been given recently by Doi and Takeuchi [7], (2.11).

If H is finitely generated and projective over the ring k, then (1)$\Rightarrow$(4) follows from results of Kreimer and Takeuchi [13], (1.7) and (1.9), and Doi [6], (2.4). If H is the group algebra of an abstract group, then (1)(b) is the definition of strongly group-graded algebras, and (1)$\Leftrightarrow$(2) is Theorem 2.8 of Dade [3].

Finally, assume A and H are commutative. Then condition (1)(b) means that the group scheme $G = \mathrm{Spec}(H)$ acts freely on $X = \mathrm{Spec}(A)$. In this case, (1)$\Rightarrow$(4) is the criterion on affine quotients by Oberst [19] and Cline, Parshall and Scott [2], and Theorem I is Theorem 3.2 of Doi [6].

Once there is a general theorem like Theorem I, one can formally dualize it, i.e. turn all the arrows around. In fact, the dual of Theorem I holds, although its proof cannot be dualized completely.

Let H be a Hopf algebra and C a right *H-module coalgebra* (cf. [15], 4.2), i.e. C is a coalgebra, $C \otimes H \to C$ a right H-module structure and a coalgebra map. Define $\bar{C} := C/CH^+$, where H^+ is the augmentation ideal of H.

If V is a right $\bar{C}$-comodule, and W a left $\bar{C}$-comodule, then $V \square_{\bar{C}} W$ denotes the *cotensor product*, already introduced in [15] (see Section 1). Now the dual of Theorem I can be stated.

Theorem II. *Assume the antipode of H is bijective. Then the following are equivalent*:

(1) (a) *C is a projective right H-module.*
 (b) can: $C \otimes H \to C \square_{\bar{C}} C$ *is injective.*

(2) $\mathcal{M}^{\bar{C}} \to \mathcal{M}^{C}_{H}$, $M \mapsto M \square_{\bar{C}} C$, *is an equivalence.*

(3) ${}^{\bar{C}}\mathcal{M} \to {}^{C}\mathcal{M}_{H}$, $M \mapsto C \square_{\bar{C}} M$, *is an equivalence.*

(4) (a) *C is faithfully coflat as left $\bar{C}$-comodule.*
 (b) can *is an isomorphism.*

(5) (a) *C is faithfully coflat as right $\bar{C}$-comodule.*
 (b) can *is an isomorphism.*

For unexplained notions in this theorem, see Sections 1 and 4. Again, (1)(b) means that H operates "freely" on C. Take, for example, a Hopf algebra C and a Hopf subalgebra $H \subset C$. Then C is a right H-module coalgebra by multiplication in C. Clearly, condition (1)(b) is satisfied in this case.

It turns out that Theorem II can be viewed as a non-cocommutative version of the main theorem on quotients of formal schemes under free actions of formal group schemes (cf. Gabriel [8]). Formal schemes are (covariantly) equivalent to cocommutative coalgebras. In the cocommutative case, (1)(a) is a consequence of (1)(b). More generally, assume the coradical of C is cocommutative (for example, C is pointed or cocommutative). Then it is shown in 4.11 that (1)(a) follows from (1)(b). Hence, if C has cocommutative coradical, there is always a good quotient for free actions.

In the situation of Theorem II, the following *normal basis theorem* is proved in 4.13.

THEOREM III. *Assume that* can: $C \otimes H \to C \square_{\bar{C}} C$ *is injective, and that one of the following holds*:

(1) *The coradical of C is contained in $G(C)H$, for example, C is pointed ($G(C)$ denotes the group-like elements).*
(2) *The coradical of C is cocommutative, and H is finite dimensional.*
(3) *The coradical of C is cocommutative, and any simple subcoalgebra of $\bar{C}$ is liftable along $C \to \bar{C}$.*

Then $C \cong \bar{C} \otimes H$ as left $\bar{C}$-comodules and right H-modules.

In case C and H are cocommutative, Theorem III was proved in [18] using the theory of formal groups.

Consider the special case of a Hopf algebra C and a Hopf subalgebra $H \subset C$, H acting on C by multiplication in C. Then can is always injective, and by Theorem III, C is free as a right H-module in each of the cases (1), (2) and (3). In this situation, the freeness of C over H was proved by Radford [21], [22], and Takeuchi [31] in cases (1) and (2). But this does not imply the normal basis theorem.

Finally, in 4.15, an easy proof is given of the following fundamental result on quotients of a cocommutative Hopf algebra H:

$H' \mapsto HH'^{+}$ is a bijection between Hopf subalgebras and coideals which are also left ideals (cf. [8], [17], [31]).

Most of the results in this paper were obtained after the stimulating Hopf algebra conference in Beer-Sheva and Sde Boker, January 1989.

1. Preliminaries

Let k be a commutative ring. Algebras and coalgebras are always defined over k, and $\otimes = \otimes_k$. If (C, Δ, ε) is a coalgebra with comultiplication $\Delta : C \to C \otimes C$ and augmentation $\varepsilon : C \to k$, then the following version of Sweedler's sigma notation [26] will be used: $\Delta(c) = \Sigma\, c_1 \otimes c_2$, for $c \in C$. Similarly, if (V, Δ_V) is a right (resp. left) C-comodule, then its structure map will be denoted by $\Delta_V(v) = \Sigma\, v_0 \otimes v_1$ (resp. $\Sigma\, v_{-1} \otimes v_0$), for $v \in V$. The category of left resp. right C-comodules will be denoted by ${}^C\mathcal{M}$ resp. $\mathcal{M}^C$. If R is a ring, then ${}_R\mathcal{M}$ resp. $\mathcal{M}_R$ will denote the category of left resp. right R-modules. The module structure map of an R-module M will be denoted by μ_M. Let $V \in \mathcal{M}^C$ and $W \in {}^C\mathcal{M}$. Then the *cotensor product* $V \square_C W$ is defined by the exact sequence in $\mathcal{M}_k$ (equalizer of k-modules)

$$V \square_C W \subset V \otimes W \rightrightarrows V \otimes C \otimes W,$$

where the arrows on the right are $\Delta_V \otimes W$ and $V \otimes \Delta_W$ (cf. [15], 2, [28], §1, and [23], p. 130).

Let R be an algebra, and $X \in \mathcal{M}_R$, $Y \in {}_R\mathcal{M}$. Then

$$X \otimes R \otimes Y \rightrightarrows X \otimes Y \rightarrow X \otimes_R Y,$$

where the arrows on the left are $\mu_X \otimes Y$ and $X \otimes \mu_Y$, is exact. Thus cotensor product and tensor product are dual notions in the sense of duality of $\otimes$-categories $(\mathcal{M}_k, \otimes)$ and $(\mathcal{M}_k, \otimes)^{\mathrm{op}}$ (cf. [23], p. 12).

Let C be flat over k. Then $\mathcal{M}^C$ and ${}^C\mathcal{M}$ are abelian categories, and a sequence of C-comodules is exact, if and only if it is exact as a sequence of k-modules.

$Y \in {}^C\mathcal{M}$ is called *coflat* resp. *faithfully coflat*, if the functor $-\square_C Y : \mathcal{M}^C \rightarrow \mathcal{M}_k$ is exact resp. is exact and reflects exact sequences. If k is a field, then Y is coflat if and only if Y is an injective object in ${}^C\mathcal{M}$ ([30], A. 2.1).

Let R be an algebra, and C a coalgebra. ${}_R\mathcal{M}\mathrm{od}^C$ will denote the category of (R, C)-bimodules. Its objects are k-modules V which are left R-modules and right C-comodules such that Δ_V is left R-linear, i.e. $\Delta_V(rv) = \Sigma\, rv_0 \otimes v_1$ for all $r \in R$ and $v \in V$, or equivalently, μ_V is right C-collinear. Morphisms in ${}_R\mathcal{M}\mathrm{od}^C$ are R-linear and C-collinear maps.

Now assume the situation $U \in \mathcal{M}_R$, $V \in {}_R\mathcal{M}\mathrm{od}^C$ and $W \in {}^C\mathcal{M}$. Then $V \square_C W$ is a left R-submodule of $V \otimes W$, and $U \otimes \Delta_V : U \otimes_R V \rightarrow U \otimes_R V \otimes C$ is a right C-comodule structure. Let $i : V \square_C W \rightarrow V \otimes W$ be the inclusion. Then the image of $U \otimes_R i$ lies in $(U \otimes_R V) \square_C W$. Hence, $U \otimes i$ induces a canonical map

$$\mathrm{can}: U \otimes_R (V \square_C W) \rightarrow (U \otimes_R V) \square_C W.$$

This map is bijective, if U is R-flat, or dually, if C is k-flat, and W is C-coflat (cf. [28], §1).

Let C and D be coalgebras, and $p : C \rightarrow D$ a coalgebra map. Then C is a left resp. right D-comodule with structure map $(p \otimes C)\Delta$ resp. $(C \otimes p)\Delta$.

1.1. Proposition (*faithfully coflat descent*). *Let C and D be k-flat coalgebras and $p: C \to D$ a coalgebra map. Assume C is faithfully coflat as right D-comodule. Then for any left D-comodule V, the canonical sequence*

$$C \square_D (C \square_D V) \underset{p_2}{\overset{p_1}{\rightrightarrows}} C \square_D V \xrightarrow{p} V,$$

where p_1, p_2 and p are induced by $\varepsilon \otimes 1 \otimes 1$, $1 \otimes \varepsilon \otimes 1$ and $\varepsilon \otimes 1$, is exact.

Proof. By the flatness of D, $C \square_D V$ is a left D-comodule with structure map $C \square_D V \to (D \otimes C) \square_D V \cong D \otimes (C \square_D V)$, defined by $(p \otimes 1)\Delta \otimes 1$. By the flatness of C, $C \square_D (C \square_D V)$ can be handled as a submodule of $C \otimes C \otimes V$.

Since C is faithfully coflat, it is enough to show that the sequence is exact after cotensoring with C. The exactness of the latter sequence is easily proved in a way dual to the case of a faithfully flat ring extension (note that $\Delta \otimes 1_X: C \square_D X \to C \square_D (C \square_D X)$ is well-defined for any left D-comodule X, and use this map for $X = V$ and $X = C \square_D V$).

Assume for the rest of this section that k is a field. If C is a coalgebra, then C_0 will denote its *coradical*, C_0 = sum of all simple subcoalgebras of C. Then for any right C-comodule V, the *socle* of V (= the sum of all simple subcomodules) is $\Delta_V^{-1}(V \otimes C_0) \cong V \square_C C_0$. Note that for any subcoalgebra $C' \subset C$ the comultiplication of V defines an isomorphism $\Delta_V^{-1}(V \otimes C') \cong V \square_C C'$.

1.2. Lemma. *Let $X, Y \in \mathcal{M}^C$ and $f: X \to Y$ C-collinear.*

(1) *Assume X is an injective (= coflat) comodule, and $f \square_C C_0 : X \square_C C_0 \to Y \square_C C_0$ is bijective. Then f is bijective.*

(2) *Assume X and Y are injective comodules, and $f \square_C C_0$ is surjective. Then f is a split surjection of comodules.*

Proof. (1) This follows easily from the fact that $X \square_C C_0$ is isomorphic to the socle of X: f is injective, since its restriction to the socle is injective. Hence f is a split injection of comodules by the injectivity of X. The retraction of f is injective, hence an isomorphism, since its restriction on the socle is the inverse map of $f \square_C C_0$.

(2) This is proved in the same way as [30], 6.7: Since C_0 is cosemisimple, there is a C_0-collinear map $g_0: Y \square_C C_0 \to X \square_C C_0$ such that $f_0 g_0 = \mathrm{id}$, $f_0 := f \square_C C_0$. Let

$$i_X: X \square_C C_0 \cong \Delta_X^{-1}(X \otimes C_0) \subset X \quad \text{and} \quad i_Y: Y \square_C C_0 \to Y$$

be the canonical injections. By the injectivity of X there is a C-collinear map $g: Y \to X$ such that $gi_Y = i_X g_0$. Then fg is bijective by (1) using the injectivity of Y.

1.3. Proposition. *Let C, D be coalgebras over the field k, and $p: C \to D$ a coalgebra map. Then the following are equivalent:*

(1) *C is right faithfully D-coflat.*

(2) (a) *C is right D-coflat.*

(b) *For all left D-comodules, $\varepsilon \otimes 1: C \square_D X \to X$ is surjective.*

(3) (a) *C is right D-coflat.*

(b) *$\varepsilon \otimes 1: C \square_D D_0 \to D_0$ is surjective.*

(4) (a) *C is right D-coflat.*

(b) *p is a split surjection of right D-comodules.*

Proof. (1)$\Rightarrow$(2). By 1.1.

(2)$\Rightarrow$(3). Take $X = D_0$.

(3)$\Rightarrow$(4). This follows from 1.2(2), since C and D are injective D-comodules.

(4)$\Rightarrow$(1). This is obvious, since any right D-comodule M is faithfully coflat if and only if M is coflat, and for all $0 \neq X \in {}^D\mathcal{M}$: $M \square_D X \neq 0$.

2. Normal basis for (R, D)-bimodules

In this section, k is a field.

Let R be an algebra, and D a coalgebra. Then $R \otimes D$ will always be considered as (R, D)-bimodule in ${}_R\mathcal{M}\mathrm{od}^D$ in the obvious way with module structure $a(r \otimes d) := ar \otimes d$, and comodule structure $r \otimes d \mapsto \Sigma\, r \otimes d_1 \otimes d_2$, for $a, r \in R$ and $d \in D$.

If X is an (R, D)-bimodule, then X has a *normal basis* (by definition), if

$$R \otimes D \cong X \quad \text{as } (R, D)\text{-bimodules.}$$

The following criterion for the existence of normal bases will yield normal basis theorems for module coalgebras later on.

2.1. Theorem. *Let R be an algebra, C and D coalgebras, and $f: C \to D$ a coalgebra map. Assume that the coradical of D can be lifted along f, i.e. there is a coalgebra map $g: D_0 \to C$ such that fg is the inclusion map $D_0 \subset D$.*

Let $X \in {}_R\mathcal{M}\mathrm{od}^D$, and assume X is injective as D-comodule. Then the following are equivalent:

(1) *$R \otimes D \cong X$ as (R, D)-bimodules.*

(2) *$R \otimes C \cong X \square_D C$ as (R, C)-bimodules (where C is a D-comodule via f).*

PROOF. (1)$\Rightarrow$(2). This is obvious by cotensoring with C.

(2)$\Rightarrow$(1). Consider D_0 as left C-comodule via g. By (2), $R\otimes C\square_C D_0\cong X\square_D C\square_C D_0$ in ${}_R\mathcal{M}\mathrm{od}^{D_0}$. But $R\otimes C\square_C D_0\cong R\otimes D_0$, and $X\square_D C\square_C D_0\cong X\square_D D_0$, where $D_0\subset D$ defines the D-comodule structure of D_0, since fg is the inclusion $D_0\subset D$.

Hence there is an isomorphism $\Phi_0: R\otimes D_0\to X\square_D D_0$ of (R, D_0)-bimodules.

Since Φ_0 is R-linear and D_0-collinear, it has the form $\Phi_0(r\otimes d)=r\cdot j(d)$, where $j: D_0\to X\square_D D_0$ is a right D_0-, hence D-collinear map.

The comodule structure of X induces an isomorphism $X_0:=\Delta_X^{-1}(X\otimes D_0)\cong X\square_D D_0$. Since X is an injective D-comodule by assumption, the D-collinear map

$$D_0\xrightarrow{j} X\square_D D_0\cong X_0\subset X$$

can be lifted to a D-collinear map $J: D\to X$ such that $J(d)=(1\otimes\varepsilon)j(d)$ for all $d\in D$. Then J defines a map $\Phi: R\otimes D\to X$, $\Phi(r\otimes d):=r\cdot J(d)$, in ${}_R\mathcal{M}\mathrm{od}^D$. Since $R\otimes D$ is clearly D-injective, by 1.2(1), Φ is bijective if and only if $\Phi\square_D D_0$ is bijective. But the composition

$$R\otimes D_0\cong R\otimes D\square_D D_0\xrightarrow{\Phi\square D_0} X\square_D D_0$$

is Φ_0, hence bijective, since $(\Phi\square D_0)(\sum r\otimes d_1\otimes d_2)=\sum r\cdot J(d_1)\otimes d_2=\sum r(1\otimes\varepsilon)j(d_1)\otimes d_2=r\cdot j(d)$ for all $r\in R$ and $d\in D_0$ by the collinearity of j.

2.2. COROLLARY. *Let $X\in{}_R\mathcal{M}\mathrm{od}^D$, and assume X is injective as D-comodule. Then the following are equivalent*:

(1) *$R\otimes D\cong X$ as (R, D)-bimodules.*

(2) *For all simple subcoalgebras $D'\subset D$: $R\otimes D'\cong X\square_D D'$ as (R, D')-bimodules, or equivalently, $X\square_D D'$ is free of rank 1 as left $R\otimes D'^*$-module.*

PROOF. (1)$\Rightarrow$(2). Cotensor with D'. Note that $R\otimes D'\cong R\otimes D'^*$ as left modules over $R\otimes D'^*$ ($D'^*:=\mathrm{Hom}(D', k)$ is the dual algebra), since D' is a simple coalgebra, hence D'^* is a Frobenius algebra, and $D'\cong D'^*$ as left D'^*-modules.

(2)$\Rightarrow$(1). Write $D_0=\bigoplus_i D_i$, D_i simple subcoalgebras of D. By assumption, there are isomorphisms $R\otimes D_i\cong X\square_D D_i$ in ${}_R\mathcal{M}\mathrm{od}^{D_i}$ for all i. Their direct sum defines an isomorphism $R\otimes D_0\cong\bigoplus_i R\otimes D_i\cong\bigoplus_i X\square_D D_i\cong X\square_D D_0$ in ${}_R\mathcal{M}\mathrm{od}^{D_0}$.

By 2.1, where C is D_0 and f is the inclusion map $D_0 \subset D$, $R \otimes D \cong X$ in ${}_R\mathcal{M}\mathrm{od}^D$.

2.3. Corollary. *Assume in the situation of 2.2 that R is finite dimensional. Let $k \subset k'$ be any field extension. Then the following are equivalent*:

(1) $R \otimes D \cong X$ *as* (R, D)*-bimodules*.

(2) $(R \otimes k') \otimes_{k'} (D \otimes k') \cong X \otimes k'$ *as* $(R \otimes k', D \otimes k')$*-bimodules*.

Proof. (1)$\Rightarrow$(2) is trivial.

(2)$\Rightarrow$(1). $X \otimes k'$ is an injective ($=$coflat) $D \otimes k'$-comodule, since the cotensor product commutes with field extensions. Take any simple subcoalgebra $D' \subset D$. Then the given isomorphism induces an isomorphism $R \otimes D' \otimes k' \cong X \square_D D' \otimes k'$ of left $R \otimes D'^* \otimes k'$-modules. Now $R \otimes D'^*$ is a finite dimensional algebra, hence $R \otimes D' \cong X \square_D D'$ as left $R \otimes D'^*$-modules by Deuring–Noether. Therefore, $R \otimes D \cong X$ in ${}_R\mathcal{M}\mathrm{od}^D$ by 2.2.

2.4. Remark. Let $f: C \to D$ be a coalgebra map. Then clearly the coradical of D is liftable along f if and only if any simple subcoalgebra of D is liftable along f.

Now assume C and D are cocommutative. Let $\varphi: G_1 \to G_2$ be the map of formal schemes represented by f. Recall that for any cocommutative coalgebra T, the formal scheme represented by T is the functor $R \mapsto \mathrm{Coalg}(R^*, T)$, R a commutative finite dimensional algebra (cf. [8]). Hence, any simple subcoalgebra of D is liftable along f if and only if for all finite field extensions $k \subset k'$ the induced map on the k'-rational points $\varphi(k'): G_1(k') \to G_2(k')$ is surjective.

This latter condition appears in the normal basis theorem for cocommutative Hopf algebras in [18], Satz A, and 2.1 can be viewed as a generalization of this theorem.

Finally, the dual of Theorem 2.1 also holds.

2.5. Theorem. *Let C be a coalgebra, R and S algebras, and $f: R \to S$ an algebra map. Assume that there is an algebra map $g: S \to R/\mathrm{Ra}(R)$* ($\mathrm{Ra}$ = *Jacobson radical*) *such that gf is the canonical map $R \to R/\mathrm{Ra}(R)$.*

Let $X \in {}_R\mathcal{M}\mathrm{od}^C$, and assume X is projective as R-module. Then the following are equivalent:

(1) $R \otimes C \cong X$ *as* (R, C)*-bimodules*.

(2) $S \otimes C \cong S \otimes_R X$ *as* (S, C)*-bimodules* (*where S is an R-module via f*).

PROOF. (1)$\Rightarrow$(2). This is obvious by tensoring with S.

(2)$\Rightarrow$(1). Consider $\overline{R} := R/\mathrm{Ra}(R)$ as right module over S via g. Then the isomorphism in (2) induces an isomorphism $\overline{\Phi}: \overline{R} \otimes_R X \cong \overline{R} \otimes_S S \otimes_R X \cong \overline{R} \otimes_S S \otimes C \cong \overline{R} \otimes C$ of $(\overline{R}, C)$-bimodules. This map has the form $\overline{\Phi}(\bar{r} \otimes x) = \Sigma\, q(\bar{r} \otimes x_0) \otimes x_1$, where $q: \overline{R} \otimes_R X \to \overline{R}$ is left $\overline{R}$-linear. Since X is R-projective, there is a left R-linear map $Q: X \to R$ such that the diagram

$$\begin{array}{ccc} X & \xrightarrow{\quad Q \quad} & R \\ \downarrow & & \downarrow \\ \overline{R} \otimes_R X & \xrightarrow{\quad q \quad} & \overline{R} \end{array}$$

with canonical vertical maps commutes. Define $\Phi: X \to R \otimes C$, $\Phi(x) := \Sigma\, Q(x_0) \otimes x_1$. Then Φ is a morphism of (R, C)-bimodules, and the diagram

$$\begin{array}{ccc} X & \xrightarrow{\quad \Phi \quad} & R \otimes C \\ \downarrow & & \downarrow \\ \overline{R} \otimes_R X & \xrightarrow{\quad \overline{\Phi} \quad} & \overline{R} \otimes C \end{array}$$

with canonical vertical maps commutes.

Take any finite dimensional subcoalgebra $C' \subset C$. Then $\Phi \,\square_C\, C': X \,\square_C\, C' \to R \otimes C'$ is surjective by Nakayama, since it induces an isomorphism modulo $\mathrm{Ra}(R)$. Therefore, Φ is surjective, hence R-split. But this implies that Φ is bijective, since $\mathrm{Ke}(\Phi)$ is R-projective by the projectivity of X, and $\overline{R} \otimes_R \mathrm{Ke}(\Phi) = 0$, hence $\mathrm{Ke}(\Phi) = 0$ (cf. [24], p. 325).

3. Faithfully flat Hopf Galois extensions

Let k again be an arbitrary commutative ring.

Let H be a Hopf algebra, and A a right H-comodule algebra (see introduction). The category of right (A, H)-Hopf modules will be denoted by $\mathcal{M}_A^H$. Its objects are k-modules N which are right H-comodules and right A-modules such that the comodule structure map is A-linear, i.e. $\Delta_N(na) = \Sigma\, n_0 a_0 \otimes n_1 a_1$ for all $n \in N$ and $a \in A$. Morphisms in $\mathcal{M}_A^H$ are A-linear and H-collinear maps. The category ${}_A\mathcal{M}^H$ is defined similarly. If the antipode of H is bijective, then the dual algebra H^{op} is a Hopf algebra with the same coalgebra structure as H. Note that ${}_A\mathcal{M}^H = \mathcal{M}_{A^{\mathrm{op}}}^{H^{\mathrm{op}}}$. $A \otimes H$ will always be considered as Hopf module in ${}_A\mathcal{M}^H$ and in $\mathcal{M}_A^H$ in the obvious way, where the comodule structure is $1 \otimes \Delta$ and

$a(x\otimes h)=\Sigma\, a_0x\otimes a_1h$ resp. $(x\otimes h)a=\Sigma\, xa_0\otimes ha_1$, $a, x\in A$ and $h\in H$, define the A-module structures. Define

$$B:=\{a\in A \mid \Sigma\, a_0\otimes a_1=a\otimes 1\}.$$

If N is a Hopf module, then $N^{\mathrm{co}\,H}:=\{n\in N \mid \Sigma\, n_0\otimes n_1=n\otimes 1\}$ is a left B-submodule of N. Clearly, $N\,\square_H\, k\cong N^{\mathrm{co}\,H}$, where k is the trivial H-comodule $k\to H\otimes k$, $1\mapsto 1\otimes 1$.

For any right B-module M, the induced module $M\otimes_B A$ is a right (A, H)-Hopf module with comodule structure $M\otimes\Delta_A$ and A-module structure $(m\otimes x)a=m\otimes xa$, $m\in M$ and $x, a\in A$.

The induction functor $\mathcal{M}_B\to\mathcal{M}_A^H$, $M\mapsto M\otimes_B A$, is left adjoint to the functor of coinvariants. The adjunction maps are

$$M\to(M\otimes_B A)^{\mathrm{co}\,H},\qquad m\mapsto m\otimes 1,$$

$$N^{\mathrm{co}\,H}\otimes_B A\to N,\qquad n\otimes a\mapsto na,$$

where $M\in\mathcal{M}_B$, $N\in\mathcal{M}_A^H$, and $m\in M$, $n\in N$ and $a\in A$ (cf. [6], [31]).

In the same way, the induction functor ${}_B\mathcal{M}\to{}_A\mathcal{M}^H$, $M\mapsto A\otimes_B M$, is left adjoint to $N\mapsto N^{\mathrm{co}\,H}$.

There is a close relationship between the functor of coinvariants and $A\,\square_H$- (cf. [19], 5, in the context of affine group schemes):

3.1. LEMMA. *Let H be a Hopf algebra with antipode S, and A a right H-comodule algebra.*

(1) *If $V\in{}^H\mathcal{M}$, then $A\otimes V\in{}_A\mathcal{M}^H$ and $(A\otimes V)^{\mathrm{co}\,H}=A\,\square_H\, V$, where $A\otimes V$ is a left A-module by multiplication on the first factor, and where $a\otimes v\mapsto\Sigma\, a_0\otimes v_0\otimes a_1S(v_{-1})$, $a\in A$ and $v\in V$, is the H-comodule structure.*

(2) *If $N\in\mathcal{M}_A^H$, then $i: N^{\mathrm{co}\,H}\to A\,\square_H\, N$, $i(n):=1\otimes n$, and $p: A\,\square_H\, N\to N^{\mathrm{co}\,H}$, $p(\Sigma\, a_i\otimes n_i):=\Sigma\, n_ia_i$, are well-defined k-linear maps, and $pi=\mathrm{id}$. Here, $n\mapsto\Sigma\, S(n_1)\otimes n_0$ is the left H-comodule structure of N.*

PROOF. (1) $A\otimes V$ as a comodule is the usual tensor product of right H-comodules, where V is a right H-comodule via S. To prove $(A\otimes V)^{\mathrm{co}\,H}=A\,\square_H\, V$, take $t=\Sigma\, a_i\otimes v_i$ in $A\otimes V$. If $t\in(A\otimes V)^{\mathrm{co}\,H}$, then

$$\Sigma\, a_{i0}\otimes v_{i0}\otimes a_{i1}S(v_{i,-1})=\Sigma\, a_i\otimes v_i\otimes 1,$$

hence

$$\Sigma\, a_{i0}\otimes v_{i0}\otimes a_{i1}S(v_{i,-2})v_{i,-1}=\Sigma\, a_i\otimes v_{i0}\otimes v_{i,-1}$$

and

$$\Sigma\, a_{i0} \otimes a_{i1} \otimes v_i = \Sigma\, a_i \otimes v_{i,-1} \otimes v_{i0}.$$

Similarly, if $t \in A \,\square_H\, V$, then $t \in (A \otimes V)^{\mathrm{co}\, H}$.

(2) Take $\Sigma\, a_i \otimes n_i \in A \,\square_H\, N$. Then $\Sigma\, a_{i0} \otimes a_{i1} \otimes n_i = \Sigma\, a_i \otimes S(n_{i1}) \otimes n_{i0}$, hence

$$\Delta_N(\Sigma\, n_i\, a_i) = \Sigma\, n_{i0} a_{i0} \otimes n_{i1} a_{i1} = \Sigma\, n_{i0} a_i \otimes n_{i1} S(n_{i2}) = \Sigma\, n_i a_i \otimes 1.$$

This shows that p is well-defined. Trivially, i is well-defined, and $pi = \mathrm{id}$.

3.2. Corollary. *Let H be a Hopf algebra with bijective antipode, and A a right H-comodule algebra, $B := A^{\mathrm{co}\, H}$. Assume H and A are flat over k. Then the following are equivalent:*

(1) *A is coflat as right H-comodule.*

(2) *${}_A\mathcal{M}^H \to {}_B\mathcal{M}$, $N \mapsto N^{\mathrm{co}\, H}$, is exact.*

(3) *$\mathcal{M}_A^H \to \mathcal{M}_B$, $N \mapsto N^{\mathrm{co}\, H}$, is exact.*

Proof. (1)$\Rightarrow$(3). The functor $N \mapsto N^{\mathrm{co}\, H}$ is clearly left exact, and the functorial epimorphism in 3.1(2) shows that it preserves surjective morphisms, since $N \mapsto A \,\square_H\, N$ does.

(2)$\Rightarrow$(1). The functor $V \mapsto (A \otimes V)^{\mathrm{co}\, H}$ in 3.1(1) is exact by (2), and since A is flat over k.

(1)$\Rightarrow$(2). Since the antipode of H is bijective, (1)$\Rightarrow$(3) can be applied to A^{op} as H^{op}-comodule algebra. Therefore, $N \mapsto N^{\mathrm{co}\, H}$, $N \in {}_A\mathcal{M}^H = \mathcal{M}_{A^{\mathrm{op}}}^{H^{\mathrm{op}}}$, is exact.

(3)$\Rightarrow$(1) Follows similarly from (2)$\Rightarrow$(1) applied to A^{op}.

A right H-comodule Z is *relative injective*, if Δ_Z has an H-collinear retraction, or equivalently, if for all k-split monomorphisms $i: X \to Y$ of right H-comodules and for all H-collinear maps $f: X \to Z$ there is an H-collinear map $g: Y \to Z$ such that $f = gi$.

The following characterization of relative injective comodule algebras by Doi will be used in the sequel.

3.3. Remark ([6], (1.6)). Let A be a right H-comodule algebra. Then the following are equivalent:

(1) A is relative injective as right H-comodule.

(2) There is a right H-collinear and unitary map $H \to A$.

(3) Any Hopf module in $\mathcal{M}_A^H$ is relative injective as right H-comodule.

(4) There is a morphism $\varphi: A \otimes H \to A$ in ${}_A\mathcal{M}^H$ such that $\varphi\Delta_A = \mathrm{id}_A$.

If the antipode of H is bijective, then each of the above is equivalent to:

(5) Any Hopf module in ${}_A\mathcal{M}^H$ is relative injective as right H-comodule.

(6) There is a morphism $\varphi' : A \otimes H \to A$ in $\mathcal{M}_A^H$ such that $\varphi'\Delta_A = \mathrm{id}_A$.

3.4. LEMMA. *Let H be a Hopf algebra, A a right H-comodule algebra which is relative injective as right H-comodule, and $B := A^{\mathrm{co}\,H}$. Then the adjunction map $M \to (M \otimes_B A)^{\mathrm{co}\,H}$ is an isomorphism for any right B-module M.*

PROOF. More generally, the canonical map

$$M \otimes_B (A \,\square_H\, W) \to (M \otimes_B A) \,\square_H\, W$$

is bijective for all left H-comodules (since the defining sequence of the cotensor product $A \,\square_H\, W$ can be seen to be a split equalizer by 3.3(4)). In case $W = k$, this map is identified with the adjunction map $M \to (M \otimes_B A)^{\mathrm{co}\,H}$.

The referee suggested the following more direct proof: By assumption there is a left H-collinear and unitary map $j : H \to A$. Let $t : A \to B$, $t(a) := \Sigma\, a_0 j(S(a_1))$, by the associated trace map. Then one sees as in [7], p. 497, that $(M \otimes_B A)^{\mathrm{co}\,H} \to M$, $\Sigma\, m_i \otimes a_i \mapsto \Sigma\, m_i t(a_i)$, is an inverse for the adjunction map. (Still another proof was given by Doi [6], 3.1, in case k is a field.)

If A is a right H-comodule algebra, $B := A^{\mathrm{co}\,H}$, there are canonical maps

$$\mathrm{can} : A \otimes_B A \to A \otimes H, \quad x \otimes y \mapsto \Sigma\, x y_0 \otimes y_1,$$

$$\mathrm{can}' : A \otimes_B A \to A \otimes H, \quad x \otimes y \mapsto \Sigma\, x_0 y \otimes x_1.$$

If the antipode of H is bijective, then $\Phi : A \otimes H \to A \otimes H$, $\Phi(a \otimes h) := \Sigma\, a_0 \otimes a_1 S(h)$, is an isomorphism, and $\mathrm{can}' = \Phi\, \mathrm{can}$. Hence can is surjective resp. bijective if and only if can′ is so ([13], (1.2), [29], p. 1464).

3.5. THEOREM. *Let H be a Hopf algebra. Assume H is projective over k, and the antipode of H is bijective. Let A be a right H-comodule algebra, and $B := A^{\mathrm{co}\,H}$. Assume*

(a) *A is relative injective as right H-comodule.*

(b) can: $A \otimes_B A \to A \otimes H$ *is surjective.*

Then both induction functors $\mathcal{M}_B \to \mathcal{M}_A^H$ and ${}_B\mathcal{M} \to {}_A\mathcal{M}^H$ are equivalences.

PROOF. Since the antipode of H is bijective, it is enough to consider only right modules (then take the dual algebras). The induction functor $\mathcal{M}_B \to \mathcal{M}_A^H$ is an equivalence if and only if for any $M \in \mathcal{M}_B$ and $N \in \mathcal{M}_A^H$ the adjunction maps $M \to (M \otimes_B A)^{\mathrm{co}\,H}$ and $N^{\mathrm{co}\,H} \otimes_B A \to N$ are bijective.

By 3.4 and hypothesis (a), the adjunction map is bijective for any right B-module M. Now take any $N \in \mathcal{M}_A^H$. By 3.3 and hypothesis (a) (and the bijectivity of the antipode), there is a map $\varphi' : A \otimes H \to A$ in $\mathcal{M}_A^H$ such that $\varphi'\Delta_A = \mathrm{id}_A$.

Define $f\colon N\otimes A\otimes H\to N$ by $f(n\otimes a\otimes h):=\Sigma\, n_0\varphi'(a\otimes S(n_1)h)$.

$N\otimes A\otimes H$ lies in $\mathcal{M}_A^H$ with A-module structure $(n\otimes a\otimes h)\cdot x=\Sigma\, n\otimes ax_0\otimes hx_1$ for all $n\in N$ and $a,x\in A$ and $h\in H$, and with comodule structure $1\otimes 1\otimes\Delta$.

Then f is obviously right A-linear, since φ' is so. The following calculation shows that f is also H-collinear:

$$\Delta_A f(n\otimes a\otimes h)=\Sigma\, n_0\varphi'(a\otimes S(n_3)h_1)\otimes n_1S(n_2)h_2$$

(since N is a Hopf module, and φ' is collinear)

$$=\Sigma\, n_0\varphi'(a\otimes S(n_1)h_1)\otimes h_2$$

$$=\Sigma\, f(n\otimes a\otimes h_1)\otimes h_2.$$

Furthermore, for all $n\in N$: $f(\Sigma\, n_0\otimes 1\otimes n_1)=\Sigma\, n_0\varphi'(1\otimes S(n_1)n_2)=n\varphi'(1\otimes 1)=n$ ($\varphi'(1\otimes 1)=1$, since $\varphi'\Delta_A=\mathrm{id}_A$).

Hence $f\colon N\otimes A\otimes H\to N$ is a map in $\mathcal{M}_A^H$, and a k-split surjection.

By assumption (b), the canonical map can: $A\otimes A\to A\otimes H$, $x\otimes y\mapsto\Sigma\, xy_0\otimes y_1$, is surjective. Since H is projective over k, $A\otimes H$ is a projective left A-module. Obviously can is left A-linear (A operates on the first factor from the left). Therefore, can is a k-split (even A-split) epimorphism.

Now consider $N\otimes A\otimes A$ as Hopf module in $\mathcal{M}_A^H$ with comodule structure $1\otimes 1\otimes\Delta_A$ and module structure $(n\otimes x\otimes y)\cdot a=n\otimes x\otimes ya$ for all $n\in N$ and $x,y,a\in A$. Then $1\otimes\mathrm{can}\colon N\otimes A\otimes A\to N\otimes A\otimes H$ is a morphism of Hopf modules in $\mathcal{M}_A^H$, and a k-split surjection.

Hence $g=f(1\otimes\mathrm{can})\colon N\otimes A\otimes A\to N$ is a k-split epimorphism in $\mathcal{M}_A^H$. Since any Hopf module, in particular $\mathrm{Ke}(g)$, is relative injective by (a) and 3.3(3), $\mathrm{Ke}(g)$ is a direct summand of $N\otimes A\otimes A$ as H-comodule.

Now $N\otimes A\otimes A$ is a Hopf module of the form $V\otimes A$, V a k-module, with H-comodule structure $V\otimes\Delta_A$ and A-module structure $(v\otimes a)\cdot x=v\otimes ax$, for all $v\in V$ and $a,x\in A$. By hypothesis (a) and 3.4 again,

$$(V\otimes A)^{\mathrm{co}\,H}\cong V\otimes B.$$

Hence the adjunction map for $V\otimes A$ is bijective as composition of the canonical isomorphisms $(V\otimes A)^{\mathrm{co}\,H}\otimes_B A\cong(V\otimes B)\otimes_B A\cong V\otimes A$.

Therefore, continuing the resolution with $\mathrm{Ke}(g)$ instead of N, one obtains an exact sequence in $\mathcal{M}_A^H$

$$N_2\to N_1\to N\to 0$$

which splits as sequence of H-comodules and such that the adjunction maps for N_2 and N_1 are bijective. Hence

$$N_2^{\mathrm{co}\,H} \to N_1^{\mathrm{co}\,H} \to N^{\mathrm{co}\,H} \to 0,$$

and finally

$$N_2^{\mathrm{co}\,H} \otimes_B A \to N_1^{\mathrm{co}\,H} \otimes_B A \to N^{\mathrm{co}\,H} \otimes_B A \to 0$$

are exact, and the adjunction map for N is an isomorphism, since both adjunction maps for N_2 and N_1 are bijective.

3.6. Example. Let $p : H \to \overline{H}$ be a surjective map of Hopf algebras. Then $(1 \otimes p)\Delta : H \to H \otimes \overline{H}$ defines an $\overline{H}$-comodule algebra structure on H, and condition (b) in 3.5 is satisfied.

Proof. The canonical map can: $H \otimes H \to H \otimes \overline{H}$ is surjective, since $H \otimes H \to H \otimes H, x \otimes y \mapsto \Sigma\, xy_1 \otimes y_2$, is an isomorphism with inverse $x \otimes y \mapsto \Sigma\, xS(y_1) \otimes y_2$.

The following imprimitivity theorem proves the equivalence of (2) and (4) in Theorem I in a more general situation. Let $\overline{H} = H/I$ be a quotient coalgebra and a quotient right H-module of the Hopf algebra H, and A a right H-comodule algebra. Then the canonical map $p : H \to \overline{H}$, $p(h) := \overline{h}$, is collinear and right H-linear, and A is a right $\overline{H}$-comodule via p. Define

$$A' := A^{\mathrm{co}\,\overline{H}} := \{a \in A \mid \Sigma\, a_0 \otimes \overline{a}_1 = a \otimes \overline{1}\}.$$

Then A' is a subalgebra of A, and the canonical map

$$\mathrm{can}: A \otimes_{A'} A \to A \otimes \overline{H}, \quad x \otimes y \mapsto \Sigma\, xy_0 \otimes \overline{y}_1,$$

is well-defined (if $x, y \in A$ and $z \in A'$, then

$$\mathrm{can}(x \otimes zy) = \Sigma\, xz_0 y_0 \otimes \overline{z_1 y_1} = \Sigma\, xz_0 y_0 \otimes \overline{z}_1 y_1 = \Sigma\, xzy_0 \otimes \overline{1} y_1 = \mathrm{can}(xz \otimes y)).$$

The adjoint functors $\mathcal{M}_{A'} \to \mathcal{M}_A^{\overline{H}}$, $M \mapsto M \otimes_{A'} A$, and

$$\mathcal{M}_A^{\overline{H}} \to \mathcal{M}_{A'}, \; N \mapsto N^{\mathrm{co}\,\overline{H}} := \{n \in N \mid \Sigma\, n_0 \otimes n_1 = n \otimes \overline{1}\},$$

are defined as before. Here, the category $\mathcal{M}_A^{\overline{H}}$ of right $(A, \overline{H})$-*Hopf modules* is defined in the obvious way: A right $(A, \overline{H})$-Hopf module N is a k-module which has a right A-module and a right $\overline{H}$-comodule structure such that the comodule structure map is A-linear, i.e. $\Delta_N(na) = \Sigma\, n_0 a_0 \otimes n_1 a_1$ for all $n \in N$ and $a \in A$. This notion generalizes $\mathcal{M}_H^{\overline{H}}$ of [31] and $\mathcal{M}_A^H$ of [5]. Note that ${}_A\mathcal{M}^{\overline{H}}$ is not well-defined, since H does not operate on the left of $\overline{H}$. Also,

$$\mathrm{can}': A \otimes_{A'} A \to A \otimes \overline{H},\ x \otimes y \mapsto \Sigma\, x_0 y \otimes \overline{x}_1,$$

does not exist. If X is a right A-module, in particular if $X = A$, then $X \otimes \overline{H}$ will be considered as right $(A, \overline{H})$-Hopf module with comodule structure $1 \otimes \overline{\Delta}$ and module structure $(x \otimes \overline{h})a := \Sigma\, xa_0 \otimes \overline{h}a_1$ for all $x \in X$, $\overline{h} \in \overline{H}$ and $a \in A$.

3.7. THEOREM. *Let H be a Hopf algebra, $\overline{H} = H/I$ a quotient coalgebra and a quotient right H-module of H, and $p: H \to \overline{H}$ the canonical map. Let A be a right H-comodule algebra and $A' := A^{\mathrm{co}\,\overline{H}}$, where $(1 \otimes p)\Delta_A$ is the $\overline{H}$-comodule structure on A. Assume $\overline{H}$ is flat over k. Then the following are equivalent:*

(1) (a) *A is faithfully flat as left A'-module.*

(b) $\mathrm{can}: A \otimes_{A'} A \to A \otimes \overline{H}$ *is an isomorphism.*

(2) *The induction functor $\mathcal{M}_{A'} \to \mathcal{M}_A^{\overline{H}}$, $M \mapsto M \otimes_{A'} A$, is an equivalence.*

(The implication (1)$\Rightarrow$(2) holds without the assumption that $\overline{H}$ is flat over k.)

PROOF. (2)$\Rightarrow$(1). Clearly, A is left faithfully flat over A', since (by the flatness of $\overline{H}$) exact sequences of $(A, \overline{H})$-Hopf modules are exact as sequences of k-modules. The adjunction map of $N := A \otimes \overline{H}$ can be identified with the canonical map $\mathrm{can}: A \otimes_{A'} A \to A \otimes \overline{H}$. Hence can is bijective.

(1)$\Rightarrow$(2). (i) Let N be a right $(A, \overline{H})$-Hopf module. Then the adjunction map μ_N of N is bijective.

PROOF. This was shown in [7], 2.11, in case $H = \overline{H}$ using the assumption that $\overline{H}$ is a Hopf algebra. A slight modification of this proof also works in the general case: For any right A-module X, the canonical map $\mathrm{can}_X: X \otimes_{A'} A \to X \otimes \overline{H}, x \otimes a \mapsto \Sigma\, xa_0 \otimes \overline{a}_1$, is bijective, since $\mathrm{can}_X \cong X \otimes_A \mathrm{can}$. The following diagram commutes:

$$\begin{array}{ccccc}
N^{\mathrm{co}\,\overline{H}} \otimes_{A'} A & \to & N \otimes_{A'} A & \rightrightarrows & (N \otimes \overline{H}) \otimes_{A'} A \\
\downarrow{\scriptstyle \mu_N} & & \downarrow{\scriptstyle \mathrm{can}_N} & & \downarrow{\scriptstyle \mathrm{can}_{N \otimes \overline{H}}} \\
N & \underset{\Delta_N}{\to} & N \otimes \overline{H} & \rightrightarrows & N \otimes \overline{H} \otimes \overline{H}.
\end{array}$$

Here, $N \otimes \overline{H}$ is a right A-module by diagonal action as above. The row on top is the defining sequence of $N^{\mathrm{co}\,\overline{H}}$ tensored with $- \otimes_{A'} A$, hence exact. The unlabelled maps on the bottom are $\Delta_N \otimes \overline{H}$ and $N \otimes \Delta_{\overline{H}}$. Since $N \cong N \square_{\overline{H}} \overline{H}$, the sequence on the bottom is exact. Now can_N and $\mathrm{can}_{N \otimes \overline{H}}$ are isomorphisms, so μ_N is an isomorphism.

(ii) Let M be a right A'-module. Then the adjunction map ι_M of M is bijective.

PROOF. The following diagram commutes:

$$\begin{array}{ccccc} M & \xrightarrow{i} & M \otimes_{A'} A & \rightrightarrows & M \otimes_{A'} A \otimes_{A'} A \\ \downarrow{\scriptstyle \iota_M} & & \downarrow{\scriptstyle =} & & \downarrow{\scriptstyle M \otimes \mathrm{can}} \\ (M \otimes_{A'} A)^{\mathrm{co}\,\overline{H}} & \subset & M \otimes_{A'} A & \rightrightarrows & M \otimes_{A'} A \otimes \overline{H}. \end{array}$$

In the sequence on the top, $i(m) := m \otimes 1$, and the unlabelled maps are $M \otimes i_1$ and $M \otimes i_2$, where $i_1(a) := a \otimes 1$ and $i_2(a) := 1 \otimes a$. By faithfully flat descent, the sequence is exact. The lower sequence is the defining sequence of the covariant elements. By assumption, can is an isomorphism. Hence ι_M is bijective.

3.8. PROOF OF THEOREM I (INTRODUCTION). (1)$\Rightarrow$(2). By 3.5.

(2)$\Rightarrow$(4). By (2)$\Rightarrow$(1) of 3.7, where $\overline{H} = H$.

(4)$\Rightarrow$(1) is proved similarly to [28], 1.5: Since k is a field, it is enough to show that A is coflat as right comodule. By (b) and the bijectivity of the antipode, $\mathrm{can}': A \otimes_B A \to A \otimes H$, $x \otimes y \mapsto \Sigma\, x_0 y \otimes x_1$, is bijective. As explained above, can′ is a morphism in ${}_A\mathcal{M}^H$, hence in ${}_B\mathcal{M}\mathrm{od}^H$. For any left H-comodule V

$$(A \,\square_H\, V) \otimes_B A \cong (A \otimes_B A) \,\square_H\, V \cong (A \otimes H) \,\square_H\, V \cong A \otimes V,$$

where the first map is an isomorphism, since A is flat as left B-module by (a), and the second one is $\mathrm{can}' \,\square\, V$. Hence, the functor $V \mapsto A \,\square_H\, V$ is exact, since A is faithfully flat as left B-module by (a).

(1)$\Leftrightarrow$(3)$\Leftrightarrow$(5). Apply (1)$\Leftrightarrow$(2)$\Leftrightarrow$(4) to A^{op} as right H^{op}-comodule algebra.

3.9. REMARK. (1) Note that in the situation of Theorem I, another proof of 3.7, (1)$\Rightarrow$(2), is given in 3.8.

(2) In Theorem I, conditions (1)–(5) are equivalent to

(6) (a) B is a direct summand in A as left B-module.
(b) can is bijective.

(7) (a) B is a direct summand in A as right B-module.
(b) can is bijective.

PROOF. If can is bijective, then (1)(a), (6)(a) and (7)(a) are equivalent by [6], (2.4).

(3) Assume in Theorem I the equivalent conditions (1)–(5). Then A is faithfully coflat as right H-comodule by 3.8 or 3.1(1).

(4) The imprimitivity theorem of Koppinen and Neuvonen [11] is a special

case of 3.7. Let $H' \subset H$ be a Hopf subalgebra (or just a subalgebra such that $\Delta(H')$ lies in the image of $H \otimes H'$) such that H is a finitely generated projective generator as a left H'-module. Then $\bar{H} := H/H'^{+}H \cong k \otimes_{H'} H$ is finitely generated and projective over k. H is faithfully flat as a left H'-module, since it is a progenerator (cf. [12], 1.5 and 1.6). The canonical map can: $H \otimes_{H'} H \to H \otimes \bar{H}$ is bijective (with inverse as in 3.6). Now it follows from the proof of 3.7 (1)⇒(2)(ii), applied to $M = H'$, that $H' = H^{\mathrm{co}\bar{H}}$. The canonical map induces an isomorphism of algebras $\bar{H}^* := \mathrm{Hom}(\bar{H}, k) \cong F := \mathrm{Hom}_{H'}({}_{H'}H, {}_{H'}k)$ with convolution as algebra structure. Hopf modules in $\mathcal{M}_H^{\bar{H}}$ are the same as right H-modules satisfying the rule $f(na) = \Sigma\, ((a_2 f)n)a_1$ for all $f \in \bar{H}^*$, $n \in N$ and $a \in H$. Here, $\bar{H}^*$ is a left H-module in the usual way by $(af)(\bar{x}) = f(\bar{x}\bar{a})$ for all $a, x \in H$ and $f \in \bar{H}^*$. Hence 3.7, with $A = H$ and $A' = H'$, contains the (right version of the) theorem in [11].

3.10. Corollary. *Let k be a field. Let H and $\bar{H}$ be Hopf algebras with bijective antipodes, and $p: H \to \bar{H}$ a surjective Hopf algebra map. Assume H is an injective right $\bar{H}$-comodule via p. Let $B \subset A$ be a right H-Galois extension such that A is faithfully flat as left B-module. Consider the induced $\bar{H}$-comodule algebra $(1 \otimes p)\Delta_A : A \to A \otimes \bar{H}$, and define $A' := A^{\mathrm{co}\bar{H}}$. Then $A' \subset A$ is an $\bar{H}$-Galois extension, and A is faithfully flat as left A'-module.*

Proof. This follows immediately from Theorem I, since
(a) A is $\bar{H}$-coflat, since A is H-coflat by Theorem I, and H is $\bar{H}$-coflat.
(b) The canonical map $A \otimes A \to A \otimes H \xrightarrow{A \otimes p} A \otimes \bar{H}$ is surjective.

3.11. Remark. The above results show that there is a rich theory of faithfully flat Hopf Galois extensions.

Furthermore, some of the basic properties of principal homogeneous spaces or torseurs in algebraic geometry (cf. [4], III, §4) still hold over arbitrary rings k for H-Galois extensions $B \subset A$ such that A is faithfully flat as right B-module (with more or less the same proofs), for example:

(1) Let $i: B \to A$ and $\hat{\imath}: B \to \hat{A}$ be H-Galois extensions, and assume $\hat{A}$ is faithfully flat as right B-module (via $\hat{\imath}$). Then any H-collinear algebra map $f: A \to \hat{A}$ satisfying $fi = \hat{\imath}$ is an isomorphism (cf. [4], III, §4, 1.4).

Proof. The composition

$$\hat{A} \otimes_B A \xrightarrow{\hat{A} \otimes f} \hat{A} \otimes_B \hat{A} \xrightarrow{\widehat{\mathrm{can}}} \hat{A} \otimes H$$

can be identified with $\hat{A} \otimes_A$ can, where $\hat{A}$ is an A-module via f. Hence $\hat{A} \otimes_B f$ is bijective, and so is f, since $\hat{A}$ is a faithfully flat right B-module.

(2) Let $B \subset A$ be an H-Galois extension, and assume A is faithfully flat as right B-module. Let $H' \subset H$ be a k-direct Hopf subalgebra which is flat over k. Define $A' := \Delta_A^{-1}(A \otimes H') \cong A \,\Box_H\, H'$. Then $B \subset A'$ is an H'-Galois extension, and A' is faithfully flat as right B-module.

Proof. The canonical isomorphism can: $A \otimes_B A \to A \otimes H$ induces an isomorphism

$$f: A \otimes_B A' \cong A \otimes_B (A \,\Box_H\, H') \cong (A \otimes_B A) \,\Box_H\, H' \cong (A \otimes H) \,\Box_H\, H' \cong A \otimes H',$$

where the second map is bijective, since A is flat as right B-module. Explicitly, $f(a \otimes x) = \Sigma\, a x_0 \otimes x_1$ for all $a \in A$ and $x \in A'$. Note that f is right and left B-linear. Hence A' is faithfully flat as right B-module, since A_B and H'_k are faithfully flat.

To show the bijectivity of the canonical map can: $A' \otimes_B A' \to A' \otimes H'$, it is enough to show that $A \otimes_B$ can is bijetive, since A_B is faithfully flat. But applying f on the right and twice on the left, $A \otimes_B$ can is identified with the bijection $A \otimes H' \otimes H' \to A \otimes H' \otimes H'$, $a \otimes x \otimes y \mapsto \Sigma\, a \otimes y x_1 \otimes x_2$.

(3) In fact, the above proof in (2) shows that $B \to A \,\Box_H\, H'$, $b \mapsto b \otimes 1$, is an H'-Galois extension, and $A \,\Box_H\, H'$ is right faithfully flat over B for any Hopf algebra map $H' \to H$, where H' is flat over k, as was remarked by C. Wenninger. In the geometric case, this is the usual functorial behaviour of torsors for variable groups (cf. [4], III, §4, 3.2).

If A is a commutative algebra over a field, and $B \subset A$ a faithfully flat H-Galois extension, then it follows from a general descent theorem [10], Th. 3.13, Cor., that A is projective over B (since $A \otimes_B A \cong A \otimes H$ is projective over A, and A is faithfully flat over B). Hence the criterion 2.5 for the existence of a normal basis can be applied to A as left B-module and right H-comodule.

On the other hand, A is H-injective by Theorem I and from 2.2 one obtains the following

3.12. Theorem. *Let H be a commutative Hopf algebra over a field, and $B \subset A$ a commutative H-Galois extension such that A is faithfully flat over B. If B is semilocal (for example, finite dimensional), then*

$A \cong B \otimes H$ as left B-modules and right H-comodules.

Proof. By Theorem I, A is an injective H-comodule. Therefore, it is enough, by 2.2, to show $A \square_H H' \cong B \otimes H'$ in ${}_B\mathcal{M}\mathrm{od}^{H'}$ for any simple subcoalgebra H' in H. But if $H' \subset H$ is a simple subcoalgebra, then the canonical isomorphism $A \otimes_B A \cong A \otimes H$ induces an isomorphism $(A \otimes_B A) \square_H H' \cong (A \otimes H) \square_H H' \cong A \otimes H'$ in ${}_B\mathcal{M}\mathrm{od}^{H'}$. Since A_B is flat, $(A \otimes_B A) \square_H H' \cong A \otimes_B (A \square_H H')$. Hence $A \otimes_B (A \square_H H') \cong A \otimes_B (B \otimes H')$ as left $A \otimes H'^*$- modules.

Define $W := A \square_H H'$, $V := B \otimes H'$ as left modules over $S := B \otimes H'^*$. Then ${}_SV \cong {}_SS$, and $A \otimes_B W \cong A \otimes_B V$ as $A \otimes S$-modules.

By assumption, the commutative ring A is faithfully flat over the semilocal ring B. Therefore, the general form of the Deuring–Noether theorem in [9], 2.5.8 (ii) implies that $A \square_H H \cong B \otimes H'$ in ${}_B\mathcal{M}\mathrm{od}^{H'}$.

3.13. Remark. As a special case of 3.12, take any finite dimensional Hopf subalgebra B of H. Then $H \cong B \otimes \bar{H}$ as left B'-modules and right $\bar{H}$-comodules, where $\bar{H} := H/HB^+$. This contains [22], Th. 1, where it is shown that H is free over B. But the methods in [22] or [31] do not prove the normal basis property.

In general, if B is not finite dimensional, A need not be free over B. For positive and negative results in this direction, see [25].

4. The dual case

Let H be a Hopf algebra over the commutative ring k, and let C be a right *H-module coalgebra*, i.e. C is a coalgebra with a right H-module structure $\mu_C : C \otimes H \to C$ such that μ_C is a coalgebra map, in other words,

$$\Delta(ch) = \Sigma\, c_1 h_1 \otimes c_2 h_2 \quad \text{and} \quad \varepsilon(ch) = \varepsilon(c)\varepsilon(h) \qquad \text{for all } c \in C \text{ and } h \in H.$$

$\mathcal{M}_H^C$ is the category of right C-comodules and right H-modules N such that $\Delta_N : N \to N \otimes C$ is H-linear, i.e. $\Delta_N(nh) = \Sigma\, n_0 h_1 \otimes n_1 h_2$ for all $n \in N$, $h \in H$. Morphisms in $\mathcal{M}_H^C$ are H-linear and C-collinear maps. The category of Hopf modules ${}^C\mathcal{M}_H$ is defined similarly. If the antipode of H is bijective, then the dual coalgebra H^{cop} is a Hopf algebra with the same mutliplication as H. Again, ${}^C\mathcal{M}_H = \mathcal{M}_{H^{\mathrm{cop}}}^{C^{\mathrm{cop}}}$. $C \otimes H$ is a Hopf module in $\mathcal{M}_H^C$ and ${}^C\mathcal{M}_H$ in the obvious way, where the comodule structure is defined by $c \otimes h \mapsto \Sigma\, c_1 \otimes h_1 \otimes c_2 h_2$ and $c \otimes h \mapsto \Sigma\, c_1 h_1 \otimes c_2 \otimes h_2$, and where $C \otimes H$ is a right H-module by multiplication on H.

Define $\bar{C} := C/CH^+$. Then the canonical map $p : C \to \bar{C}$, $c \mapsto \bar{c}$, is a coalgebra surjection. For any $N \in \mathcal{M}_H^C$, $\bar{N} := N/NH^+ \cong N \otimes_H k$ is a $\bar{C}$-comodule.

Let C be flat over k. Then for any right $\bar{C}$-comodule M, $M \square_{\bar{C}} C \in \mathcal{M}_H^C$, where the Hopf module structure is defined by the structure maps of C. Note that the comodule structure $M \otimes \Delta$ on $M \square_{\bar{C}} C$ is well-defined, since C is flat over k. Dually to Section 3, the functor $\mathcal{M}^{\bar{C}} \to \mathcal{M}^C_H$, $M \mapsto M \square_{\bar{C}} C$, is right adjoint to $\mathcal{M}^C_H \to \mathcal{M}^{\bar{C}}$, $N \mapsto \bar{N}$. The adjunction maps are

$$\overline{M \square_{\bar{C}} C} \to M, \quad \overline{\Sigma\, m_i \otimes c_i} \mapsto \Sigma\, m_i \varepsilon(c_i),$$

$$N \to \bar{N} \square_{\bar{C}} C, \quad n \mapsto \Sigma\, \bar{n}_0 \otimes n_1,$$

where M is a right $\bar{C}$-comodule and N a Hopf module.

In the same way, ${}^{\bar{C}}\mathcal{M} \to {}^C\mathcal{M}_H$, $M \mapsto C \square_{\bar{C}} M$, is right adjoint to $N \mapsto \bar{N}$.

4.1. Lemma. *Let H be a Hopf algebra with antipode S, and C a right H-module coalgebra.*

(1) *If $V \in {}_H\mathcal{M}$, then $C \otimes V \in {}^C\mathcal{M}_H$ and $\overline{C \otimes V} \cong C \otimes_H V$, $\overline{c \otimes v} \mapsto c \otimes v$, where $C \otimes V$ is a left C-comodule by $\Delta \otimes V$, and where $(c \otimes v) \cdot h := \Sigma\, ch_1 \otimes S(h_2)v$ is the H-module structure.*

(2) *If $N \in \mathcal{M}^C_H$, then $i : \bar{N} \to C \otimes_H N$, $i(\bar{n}) := \Sigma\, n_1 \otimes n_0$, and $p : C \otimes_H N \to \bar{N}$, $p(c \otimes n) := \varepsilon(c)\bar{n}$, are well-defined, and $pi = \mathrm{id}$. Here, N is considered as a left H-module by $hn := nS(h)$.*

Proof. Dual to 3.1.

4.2. Corollary. *Let H be a Hopf algebra with bijective antipode, C a right H-module coalgebra, and $\bar{C} = C/CH^+$. Assume C and $\bar{C}$ are flat over k. Then the following are equivalent:*

(1) *C is flat as H-right module.*

(2) *${}^C\mathcal{M}_H \to {}^{\bar{C}}\mathcal{M}$, $N \mapsto \bar{N}$, is exact.*

(3) *$\mathcal{M}^C_H \to \mathcal{M}^{\bar{C}}$, $N \mapsto \bar{N}$, is exact.*

Proof. Dual to 3.2.

A right H-module Z will be called *relative projective*, if $\mu_Z : Z \otimes H \to Z$ has an H-linear section, or equivalently, if Z is projective relative to all k-split H-epimorphisms.

4.3. Remark. Let H be a Hopf algebra, and C a right H-module coalgebra. Then the following are equivalent:

(1) C is relative projective as right H-module.

(2) There is a right H-linear and augmented map $C \to H$.

(3) Any Hopf module in $\mathcal{M}^C_H$ is relative projective as right H-module.

(4) There is a morphism $\psi : C \to C \otimes H$ in ${}^C\mathcal{M}_H$ such that $\mu_C \psi = \mathrm{id}_C$.

If the antipode of H is bijective, then each of the above is equivalent to:

(5) Any Hopf module in ${}^C\mathcal{M}_H$ is relative projective as right H-module.

(6) There is a morphism $\psi' : C \to C \otimes H$ in $\mathcal{M}_H^C$ such that $\mu_C \mu' = \mathrm{id}_C$.

PROOF. Dual to 3.3 (cf. [5]).

4.4. LEMMA. *Let H be a Hopf algebra, C a right H-module coalgebra, and $\bar{C} = C/CH^+$. Assume C is relative projective as right H-module. Then the adjunction map $\overline{M \square_{\bar{C}} C} \to M$ is an isomorphism for any right $\bar{C}$-comodule M.*

PROOF. Dual to 3.4.

If C is a right H-module coalgebra, $\bar{C} = C/CH^+$, there are canonical maps

$$\mathrm{can}\colon C \otimes H \to C \square_{\bar{C}} C, \quad c \otimes h \mapsto \Sigma\, c_1 \otimes c_2 h,$$

$$\mathrm{can}'\colon C \otimes H \to C \square_{\bar{C}} C, \quad c \otimes h \mapsto \Sigma\, c_1 h \otimes c_2.$$

If the antipode S of H is bijective, then $\Phi : C \otimes H \to C \otimes H$, $\Phi(c \otimes h) := \Sigma\, ch_1 \otimes S(h_2)$, is bijective, and $\mathrm{can}' = \mathrm{can}\, \Phi$.

4.5. THEOREM. *Let H be a Hopf algebra with bijective antipode, which is flat and injective as k-module. Let C be a k-flat right H-module coalgebra, and $\bar{C} := C/CH^+$. Assume*

(a) *C is relative projective as right H-module.*

(b) can: *$C \otimes H \to C \square_{\bar{C}} C$ is injective.*

Then both (co-)induction functors $\mathcal{M}^{\bar{C}} \to \mathcal{M}_H^C$ and ${}^{\bar{C}}\mathcal{M} \to {}^C\mathcal{M}_H$ are equivalences.

PROOF. Dual to the proof of 3.5. If N is a Hopf module in $\mathcal{M}_H^C$, then the dual map to f in the proof of 3.5 is

$$N \xrightarrow{\Delta_N} N \otimes C \xrightarrow{N \otimes \Psi'} N \otimes C \otimes H \to N \otimes C \otimes H,$$

where Ψ' is the map in 4.3(6), and where the last map is the isomorphism $n \otimes c \otimes h \mapsto \Sigma\, nS(h_1) \otimes c \otimes h_2$.

Note that the injective map can: $C \otimes H \to C \otimes C$ is left C-collinear, hence is a split H-collinear map, since H is injective over k (collinear maps into $C \otimes H$ are given by linear maps into H).

4.6. EXAMPLE. Let H be a Hopf algebra, and $H' \subset H$ a Hopf subalgebra. Then H is a right H'-module coalgebra in the natural way by multiplication in H. Define $\bar{H} := H/HH'^+$. Then condition (b) in 4.5 is satisfied.

PROOF. The canonical map $H \otimes H \to H \otimes H$, $x \otimes y \mapsto \Sigma\, x_1 \otimes x_2 y$, is an isomorphism with inverse $x \otimes y \mapsto \Sigma\, x_1 \otimes S(x_2) y$.

From now on, assume k is a field.

If $H' \subset H$ is a *right coideal subalgebra* of the Hopf algebra H, i.e. a subalgebra such that $\Delta(H') \subset H' \otimes H$, and C is a right H-module coalgebra, then $\overline{C} := C/CH'^{+}$ is a coalgebra, and the category of Hopf modules $\mathcal{M}_{H'}^{C}$ is defined in the same way as $\mathcal{M}_{H}^{C}$ (dually to Section 3).

4.7. THEOREM. *Let H be a Hopf algebra and $H' \subset H$ a right coideal subalgebra. Let C be a right H-module coalgebra, and $\overline{C} := C/CH'^{+}$. Then the following are equivalent*:

(1) (a) *C is faithfully coflat as left $\overline{C}$-comodule.*

(b) can: $C \otimes H' \to C \square_{\overline{C}} C$ *is an isomorphism.*

(2) *The coinduction functor $\mathcal{M}^{\overline{C}} \to \mathcal{M}_{H'}^{C}$, $M \mapsto M \square_{\overline{C}} C$, is an equivalence.*

PROOF. Dual to 3.7.

4.8. PROOF OF THEOREM II (INTRODUCTION). (1)$\Rightarrow$(2). By 4.5.

(2)$\Rightarrow$(4). See 4.7, (2)$\Rightarrow$(1).

(4)$\Rightarrow$(1). By (a), it follows from 1.3 that there is a left $\overline{C}$-collinear map $s: \overline{C} \to C$ such that $ps = \mathrm{id}_{\overline{C}}$. Now apply the functor ${}^{\overline{C}}\mathcal{M} \to {}^{C}\mathcal{M}_{H}$. Then $c \square_{\overline{C}} s: C \square_{\overline{C}} \overline{C} \to C \square_{\overline{C}} C$ is an H-split monomorphism. But the canonical maps $C \square_{\overline{C}} \overline{C} \cong C$, and can′: $C \otimes H \to C \square_{\overline{C}} C$ are right H-linear. By (b), can′ is bijective (since the antipode is bijective). Hence C is projective as right H-module.

(1)$\Leftrightarrow$(3)$\Leftrightarrow$(5). Apply (1)$\Leftrightarrow$(2)$\Leftrightarrow$(4) to C^{cop} as right H^{cop}-module coalgebra.

4.9. REMARK. (1) In Theorem II, conditions (1)–(5) are equivalent to:

(6) (a) $C \to \overline{C}$ has a left $\overline{C}$-collinear section.

(b) can is bijective.

(7) (a) $C \to \overline{C}$ has a right $\overline{C}$-collinear section.

(b) can is bijective.

PROOF. Dual to 3.9(2).

(2) Assume in Theorem II the equivalent conditions (1)–(5). Then C is faithfully flat as right H-module by 4.1(1).

4.10. REMARK. A right action of a formal group scheme on a formal group (cf. [8]) corresponds (covariantly) to a right H-module coalgebra, where the coalgebra C and the Hopf algebra H are cocommutative. The action is called free, if the canonical map $C \otimes H \to C \otimes C$ is injective, i.e. if (1)(b) in Theorem II is satisfied. In this situation, C is automatically projective as right H-module, hence (1)(a) follows from (1)(b). This is shown in the next theorem under less restrictive assumptions than cocommutativity by a modification of results of

Takeuchi and Radford. The main theorem on quotients of formal schemes under free actions of formal groups ([8], 1.4 and 2.4) is the implication (1)(b)$\Rightarrow$(4) in Theorem II for cocommutative C and H. Thus Theorem II together with 4.11 generalizes the full quotient theorem for formal groups (cf. 4.12).

4.11. THEOREM. *Let H be a Hopf algebra, and C a right H-module coalgebra, $\bar{C} := C/CH^+$. Let $G(—)$ denote the group-like elements of $(—)$. Assume*

(a) *There is a field extension $k \subset k'$ such that the coradical of $C \otimes k'$ is contained in $G(C \otimes k') \cdot (H \otimes k')$.*

(b) can: $C \otimes H \to C \square_{\bar{C}} C$ *is injective.*

Then all Hopf modules in $\mathcal{M}_H^C$ are projective as right H-modules. In particular, C is a projective right H-module.

PROOF. It is enough to consider the case $k' = k$ in (a), since a module over a k-algebra is projective if it is projective after some field extension.

Assume condition (a) with $k' = k$. Then it will be shown that all Hopf modules are even free over H.

(1) Let $0 \neq N \in \mathcal{M}_H^C$ such that N is finitely generated as H-module. Then N is free as H-module. This is shown by the following modification of [27], Th. 3.2. Choose a finite dimensional subcomodule V of N such that $N = V \cdot H$. Then there is a simple subcoalgebra C' of C and a subspace $0 \neq W$ of V such that $\Delta_V(W) \subset W \otimes C'$, since $V \square_C C_0 \neq 0$. By assumption (a), C' is contained in $G(C) \cdot H$. Hence there is a group-like element $g \in C$ such that $C' \subset g \cdot H$, since $G(C) \cdot H$ is the sum of the subcoalgebras $g \cdot H$, $g \in G(C)$. Then $\Delta_N(W \cdot H) \subset W \cdot H \otimes g \cdot H$. But the surjective coalgebra map $H \to g \cdot H$, $h \mapsto g \cdot h$, is injective, since $g \otimes H \to C \otimes C$, $g \otimes h \mapsto g \otimes g \cdot h$, is injective by assumption (b). Hence $H \to g \cdot H$ is a right H-linear coalgebra isomorphism, and $\mathcal{M}_H^H \cong \mathcal{M}_H^{g \cdot H}$. By [26], 4.1.1, any Hopf module in $\mathcal{M}_H^H$ is free as right H-module. Hence $W \cdot H$ is free as right H-module.

Now consider the exact sequence in $\mathcal{M}_H^C$

$$0 \to W \cdot H \subset N \to N/W \cdot H \to 0.$$

$N/W \cdot H$ is generated over H by the image of the C-comodule V/W and $\dim(V/W) < \dim(V)$. Therefore, by induction on $\dim(V)$, one can assume that $N/W \cdot H$ is H-free. Then the sequence splits, and N is free as module over H.

(2) Let N be any non-zero Hopf module in $\mathcal{M}_H^C$. As in [22], Prop. 1, it follows from (1) that N is a free H-module.

4.12. COROLLARY. *Let H be a Hopf algebra with bijective antipode, and C a right H-module coalgebra, $\overline{C} := C/CH^+$. Assume the coradical of C is cocommutative. If the canonical map* can: $C \otimes H \to C \square_{\overline{C}} C$ *is injective, then it is bijective, and C is faithfully coflat as left and right $\overline{C}$-comodule.*

PROOF. Condition (a) in 4.11 is satisfied for $k' = \overline{k}$ an algebraic closure of k, since $C \otimes \overline{k}$ is pointed. Hence 4.12 follows from Theorem II and 4.11.

The normal basis Theorem III in the introduction is a corollary of the above results together with Theorem 2.1 for bimodules in ${}^{D}\mathcal{M}od_R$ instead of ${}_R\mathcal{M}od^D$.

4.13. PROOF OF THEOREM III (INTRODUCTION). In all three cases, the equivalent conditions in Theorem II are satisfied by 4.11. Assume (1). Denote by G the set of group-like elements of C and let $(\text{—})_0$ be the coradical. By [26], 11.1.1, $\overline{C}_0 \subset p(C_0)$. By assumption, $p(C_0) \subset p(G \cdot H) = p(k[G])$. But $p(k[G])$ lies in the coradical, since it is spanned by group-like elements. Hence $\overline{C}_0 = p[k[G])$ is pointed, and p induces a surjective map $G(p): G(C) \to G(\overline{C})$ between the group-like elements. Any set-section of $G(p)$ defines a coalgebra map $i: \overline{C}_0 \to C$ such that pi is the inclusion map $\overline{C}_0 \subset \overline{C}$. Furthermore, by Theorem II, C is injective as left $\overline{C}$-comodule, and can: $C \otimes H \to C \square_{\overline{C}} C$ is an isomorphism in ${}^{C}\mathcal{M}od_H$. Hence, by 2.1, $C \cong \bar{C} \otimes H$ in ${}^{\overline{C}}\mathcal{M}od_H$.

In case (2), by 2.3, one can again assume that k is algebraically closed. Then C is pointed, and (2) is a special case of (1).

Finally, in case (3), 2.1 can be applied directly.

4.14. REMARK. (1) In the situation of Theorem III, all Hopf modules in $\mathcal{M}_H^C$ are free as right H-modules. This follows from Theorems II and III, since any Hopf module is isomorphic to $M \square_{\overline{C}} C$, M a right $\overline{C}$-comodule, and $M \square_{\overline{C}} C \cong M \square_{\overline{C}} \overline{C} \otimes H \cong M \otimes H$ as right H-modules.

(2) Let H be a Hopf algebra, and $H' \subset H$ a Hopf subalgebra with bijective antipode.

Then H is a right H'-module coalgebra as in 4.6, and all the above results can be applied. In particular, assume one of the following conditions:

(a) $H_0 \subset G(H) \cdot H'$ (for example, H is pointed).

(b) H_0 is cocommutative, and H' is finite dimensional.

(c) H_0 is cocommutative, and any simple subcoalgebra of $\overline{H} = H/HH'^+$ is liftable along $p: H \to \overline{H}$ (for example, H is irreducible).

Then $H \cong \overline{H} \otimes H'$ as left $\overline{H}$-comodules and right H'-modules.

In cases (a) and (b), the freeness of H over H' was proved by Radford in

[22], Prop. 3, [21], Cor. 6. More generally, in these cases it was shown in [22], Prop. 3, and [31], Prop. 4, that all Hopf modules in $\mathcal{M}_{H'}^H$ are free over H'.

Finally, for completeness, an easy proof of the following basic result on quotients of cocommutative Hopf algebras will be given in the context of this paper.

4.15. THEOREM. *Let H be a cocommutative Hopf algebra. Then*

$$\{H' \subset H \mid H' \text{ Hopf subalgebra}\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{I \subset H \mid I \text{ coideal and left ideal}\},$$

where $\Phi(H') := HH'^+$ and $\Psi(I) := \{x \in H \mid \Sigma\, \overline{x_1} \otimes x_2 = \overline{1} \otimes x \text{ in } H/I \otimes H\} \cong k \square_{H/I} H$ are inverse bijections.

PROOF. (1) Let $H' \subset H$ be a Hopf subalgebra. Define $I := HH'^+$. By 4.11 and Theorem II, $\mathcal{M}_{H'}^H \rightleftarrows \mathcal{M}^{H/I}$ are equivalences. But $H' \in \mathcal{M}_{H'}^H$, and $H' \otimes_{H'} k \cong k$. Hence $H' \cong k \square_{H/I} H$. This also follows by the method in 3.9(4). (Note that this part of the proof holds, if only the coradical is cocommutative.)

(2) Let $I \subset H$ be a coideal and a left ideal. Define

$$\overline{H} := H/I \quad \text{and} \quad H' := \{x \in H \mid \Sigma\, \overline{x_1} \otimes x_2 = \overline{1} \otimes x\}.$$

Then H' is a Hopf subalgebra, and $H'^+ \subset I$, as is easily seen (cf. [31], Th. 4). Here, the cocommutativity of H is essential. To show that the coalgebra surjection $\hat{H} := H/HH'^+ \to H/I = \overline{H}$ is bijective, or equivalently, that $HH'^+ = I$, it is enough to show that $1 \otimes \varepsilon : \overline{H_0} \square_{\overline{H}} \hat{H} \to \overline{H_0}$ is injective, since the kernel of $\hat{H} \to \overline{H}$ is a left $\overline{H}$-subcomodule (and cotensoring with the coradical gives the socle). Clearly one can assume that k is algebraically closed. Then $H_0 = k[G]$, $\overline{H_0} = k[\overline{G}]$, where G and $\overline{G}$ are the group-like elements of H and $\overline{H}$. Note that $G \to \overline{G}$ is surjective. The above map $\overline{H_0} \square_{\overline{H}} \hat{H} \to \overline{H_0}$ is the direct sum of all $k\overline{g} \square_{\overline{H}} \hat{H} \to k\overline{g}$, $\overline{g} \in \overline{G}$.

Take any group-like element g of H. It remains to prove that $1 \otimes \varepsilon : k\overline{g} \square_{\overline{H}} \hat{H} \to k\overline{g}$ is injective, i.e. that $k\overline{g} \square_{\overline{H}} \hat{H}$ is 1-dimensional.

By 4.12 (or [31], Th. 1, since H is a faithfully flat left H'-module by [27], Th. 3.2), H is faithfully coflat as left $\hat{H}$-comodule. Hence, by 1.3, $1 \otimes \varepsilon : (k\overline{g} \square_{\overline{H}} \hat{H}) \square_{\hat{H}} H \to (k\overline{g} \square_{\overline{H}} \hat{H})$ is surjective. Since $k\overline{g} \square_{\overline{H}} \hat{H} \square_{\hat{H}} H \cong k\overline{g} \square_{\overline{H}} H$, it follows that the canonical map

$$k\overline{g} \square_{\overline{H}} H \to k\overline{g} \square_{\overline{H}} \hat{H}$$

is surjective. In other words, any $y \in \hat{H}$ such that $\Sigma\, \overline{y_1} \otimes y_2 = \overline{g} \otimes y$ in $\overline{H} \otimes \hat{H}$ is the canonical image of an element $x \in H$ such that $\Sigma \overline{x_1} \otimes x_2 = \overline{g} \otimes x$ in $\overline{H} \otimes H$. But then $\Sigma g^{-1}\overline{x_1} \otimes g^{-1}x_2 = g^{-1}\overline{g} \otimes g^{-1}x = \overline{1} \otimes g^{-1}x$, and hence $g^{-1}x \in H'$, which means that $x \in gH'$ and $y \in k\hat{g}$. Therefore, $k\overline{g} \square_{\overline{H}} \hat{H}$ is 1-dimensional.

4.16. REMARK. In a note added in proof, however without proof, Theorem 4.15 was stated by Takeuchi in [31]. 4.15 was already stated and proved by Newman as the main result of [17]. For irreducible cocommutative Hopf algebras H, i.e. in the crucial case when the corresponding formal group is infinitesimal, 4.15 was proved by Gabriel in the Séminaire Schémas en Groupes 1962/64 [8], 5.1. The above proof of 4.15 seems to be much easier than the proofs in [17] and [8]. It was inspired from Oberst's proof of a variant of [8], 5.1, in [20], 13(5).

Added in revision. Meanwhile, Masuoka [14] has shown the following generalization of 4.15. Assume only that the coradical H_0 of H is cocommutative. Then the mappings in 4.15 are bijections between all right coideal subalgebras $H' \subset H$ such that the group-like elements in $H' \otimes \overline{k}$ form a group and all coideals and left ideals I of H. A crucial point in Masuoka's proof is to use the H-coring structure on $H \otimes_{H'} H$. However, the above direct proof of 4.15 also works in the more general case. The only missing information is the following ([14], 1.6, applying the method of [31], Prop. 4): If H' is a right coideal subalgebra of H such that the group-like elements in $H' \otimes \overline{k}$ form a group, then H is a faithfully flat left H'-module.

REFERENCES

1. R. J. Blattner, *Induced and produced representations of Lie algebras*, Trans. Am. Math. Soc. **144** (1969), 457–474.

2. E. Cline, B. Parshall and L. Scott, *Induced modules and affine quotients*, Math. Ann. **230** (1977), 1–14.

3. E. C. Dade, *Group-graded rings and modules*, Math. Z. **174** (1980), 241–262.

4. M. Demazure and P. Gabriel, *Groupes algébriques*, North-Holland, Amsterdam, 1970.

5. Y. Doi, *On the structure of relative Hopf modules*, Commun. Algebra **11** (1983), 243–255.

6. Y. Doi, *Algebras with total integrals*, Commun. Algebra **13** (1985), 2137–2159.

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

8. P. Gabriel, *Etude infinitésimale des schémas en groupes — groupes formels*, Exp. VII$_B$, *Schémas en groupes I*, Lecture Notes in Mathematics, No. 151, Springer, Berlin, Heidelberg, New York, 1970.

9. A. Grothendieck and J. Dieudonné, *Eléments de géométrie algébrique*, *IV*, Publ. Math. **24** (1965).

10. L. Gruson and M. Raynaud, *Critères de platitude et de projectivite*, Invent. Math. **13** (1971), 1–81.

11. M. Koppinen and T. Neuvonen, *An imprimitivity theorem for Hopf algebras*, Math. Scand. **41** (1977), 193–198.

12. H. F. Kreimer, *A note on the outer Galois theory of rings*, Pacific J. Math. **31** (1969), 417–432.

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

14. A Masuoka, *On Hopf algebras with cocommutative coradicals*, preprint, 1989.

15. J. W. Milnor and J. C. Moore, *On the structure of Hopf algebras*, Ann. of Math. **81** (1965), 211–264.

16. D. Mumford and J. Fogarty, *Geometric Invariant Theory*, Springer, Berlin, Heidelberg, New York, 1982.

17. K. Newman, *A correspondence between bi-ideals and sub-Hopf algebras in cocommutative Hopf algebras*, J. Algebra **36** (1975), 1–15.

18. U. Oberst and H.-J. Schneider, *Untergruppen formeller Gruppen von endlichem Index*, J. Algebra **31** (1974), 10–44.

19. U. Oberst, *Affine Quotientenschemata nach affinen, algebraischen Gruppen und induzierte Darstellungen*, J. Algebra **44** (1977), 503–538.

20. U. Oberst, *Actions of formal groups on formal schemes. Applications to control theory and combinatorics*, in *Seminaire d'Algebre* (P. Dubreil and M.-P. Malliavin, eds.), Lecture Notes in Mathematics, No. 1146, Springer, Berlin, Heidelberg, New York, 1985.

21. D. Radford, *Pointed Hopf algebras are free over Hopf subalgebras*, J. Algebra **45** (1977), 266–273.

22. D. Radford, *Freeness (projectivity) criteria for Hopf algebras over Hopf subalgebras*, J. Pure Appl. Algebra **11** (1977), 15–28.

23. N. S. Rivano, *Catégories tannakiennes*, Lecture Notes in Mathematics, No. 265, Springer, Berlin, Heidelberg, New York, 1972.

24. L. Rowen, *Ring Theory*, Volume I, Academic Press, Boston, 1988.

25. H.-J. Schneider, *Zerlegbare Untergruppen affiner Gruppen*, Math. Ann. **255** (1981), 139–158.

26. M. Sweedler, *Hopf Algebras*, Benjamin, New York, 1969.

27. M. Takeuchi, *A correspondence between Hopf ideals and sub-Hopf algebras*, Manuscr. Math. **7** (1972), 251–270.

28. M. Takeuchi, *A note on geometrically reductive groups*, J. Fac. Sci., Univ. Tokyo, Sect. 1, **20**, No. 3 (1973), 387–396.

29. M. Takeuchi, *On extensions of formal groups by* μ^A, Commun. Algebra **13** (1977), 1439–1481.

30. M. Takeuchi, *Formal schemes over fields*, Commun. Algebra **14** (1977), 1483–1528.

31. M. Takeuchi, *Relative Hopf modules — Equivalences and freeness criteria*, J. Algebra **60** (1979), 452–471.

32. K.-H. Ulbrich, *Galoiserweiterungen von nicht-kommutativen Ringen*, Commun. Algebra **10** (1982), 655–672.

33. D. Voigt, *Induzierte Darstellungen in der Theorie der endlichen, algebraischen Gruppen*, Lecture Notes in Mathematics, No. 92, Springer, Berlin, New York, Heidelberg, 1977.