TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 298, Number 2, December 1986

# TAMENESS AND LOCAL NORMAL BASES FOR OBJECTS OF FINITE HOPF ALGEBRAS

LINDSAY N. CHILDS AND SUSAN HURLEY

ABSTRACT. Let $R$ be a commutative ring, $S$ an $R$-algebra, $H$ a Hopf $R$-algebra, both finitely generated and projective as $R$-modules, and suppose $S$ is an $H$-object, so that $H^* = \mathrm{Hom}_R(H, R)$ acts on $S$ via a measuring. Let $I$ be the space of left integrals of $H^*$. We say $S$ has normal basis if $S \cong H$ as $H^*$-modules, and $S$ has local normal bases if $S_p \cong H_p$ as $H_p^*$-modules for all prime ideals $p$ of $R$. When $R$ is a perfect field, $H$ is commutative and cocommutative, and certain obvious necessary conditions on $S$ hold, then $S$ has normal basis if and only if $IS = R = S^{H^*}$. If $R$ is a domain with quotient field $K$, $H$ is cocommutative, and $L = S \otimes_R K$ has normal basis as $(H^* \otimes K)$-module, then $S$ has local normal bases if and only if $IS = R = S^{H^*}$.

Suppose $K$ is a number field with ring of integers $R$, $L$ is a finite Galois extension of $K$ with Galois group $G$, and $S$ is the integral closure of $R$ in $L$. Then $G$ acts as a group of automorphisms of $S$. Relative Galois module theory seeks to understand $S$ as an $RG$-module via this action. The most basic question is to inquire whether $S$ is locally isomorphic to $RG$, that is, for all primes $p$ of $R$, $S_p$ has a local normal basis as a free $R_p$-module. This question was answered by Emmy Noether, who showed that $S$ has a local normal basis at every prime $p$ of $R$ if and only if $L/K$ is tamely ramified. Here, tamely ramified means that at each prime ideal $p$ of $R$, the ramification index of any prime $P$ of $S$ lying over $p$ is relatively prime to the residue field characteristic. It is well known that this latter condition is equivalent to the surjectivity of the trace map $\mathrm{tr}\colon S \to R$, $\mathrm{tr}(s) = \sum_{\sigma \in G} \sigma(s)$.

The purpose of this paper is to formulate and prove an extension of Noether's theorem to objects of finite cocommutative Hopf algebras.

Assume now only that $R$ is a commutative ring, $H$ is a Hopf $R$-algebra which is a finitely generated projective $R$-module, and $H^* = \mathrm{Hom}_R(H, R)$, the dual Hopf algebra. A commutative $R$-algebra $S$ is an $H$-object if $S$ is a right $H$-comodule via a map $\alpha\colon S \to S \otimes H$ which is an $R$-algebra homomorphism. If $S$ is an $H$-object, then $\alpha$ induces a measuring $\alpha^*\colon H^* \otimes S \to S$ in the sense of Sweedler [**21**].

Galois module theory in this setting is the study of $S$ as an $H^*$-module via the measuring $\alpha^*$. The "trivial" example is $S = H$ itself, with $\alpha = \Delta$, the comultiplication on $H$. So we say that the $H$-object $S$ has normal basis if $S \cong H$ as $H^*$-modules, and $S$ has local normal bases if for all primes $p$ of $R$, $S_p \cong H_p$ as $H_p^*$-modules.

Since $RG \cong (RG)^*$ as $RG$-modules for $G$ any finite group, this notion of normal basis, when specialized to $H^* = RG$, is equivalent to the classical notion.

Received by the editors May 7, 1985 and, in revised form, January 7, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 13B05; Secondary 16A24.

Noether's result in the classical situation says that $S/R$ has local normal bases if and only if the trace map is onto. The trace map is the result of acting by $\sum \sigma$, a generator of the space of integrals of the Hopf algebra $RG$. Thus in seeking an extension of Noether's theorem to an $H$-object $S$, a natural condition to consider is that if $I$ is the space of integrals of $H^*$, then $IS = R$. We call an $H$-object $S$ *tame* if the induced $H^*$-module action on $S$ is faithful, $\operatorname{rank}_R S = \operatorname{rank}_R H$, and $IS = R$.

Our main results are that if the Hopf algebra $H$ is commutative and cocommutative and $S$ is an $H$-object with $S^{H^*} = R$, then tameness of $S$ is necessary and sufficient for $S$ to have a normal basis when $R$ is a perfect field, and is necessary and sufficient for $S$ to have local normal bases when $R$ is an integral domain with perfect quotient field $K$. These results are valid without the commutativity assumption on $H$ if $K$ has characteristic zero.

For $H$-objects where $H$ is cocommutative, these results generalize both Noether's theorem and Kreimer and Cook's result [**15**] that Galois $H$-objects have local normal bases.

The paper is organized as follows.

The first two sections of the paper are devoted to basic properties of tame $H$-objects. We show that if $S$ is an $H$-object which is Galois or which has local normal bases, then $S$ is a tame $H$-object.

The next two sections contain the characterization of $H$-objects with normal basis over a perfect field, when $H$ is commutative and cocommutative. The proof is very "abelian" in the sense that it uses the etale-connected decomposition of finite abelian group schemes over perfect fields.

The final section extends the characterization of $H$-objects with normal basis over fields to a similar characterization of $H$-objects with local normal bases over integral domains.

The basic references for this work are Sweedler [**21**] for the theory and notation of Hopf algebras, and Chase and Sweedler [**7**] for the theory of $H$-objects and, in particular, Galois $H$-objects.

Unadorned tensor products are over $R$.

Much of this work is contained in the second author's doctoral dissertation [**13**]. We wish to thank the referee for numerous insightful suggestions.

**1. Preliminaries.** We begin by collecting the definitions and results on Hopf algebras which we will need.

Throughout, $R$ is a commutative ring with unity.

(1.1) A Hopf $R$-algebra, in this paper, will be a finitely generated projective $R$-module together with maps

$\mu\colon H \otimes H \to H$ (multiplication),

$i\colon R \to H$ (unit),

$\varepsilon\colon H \to R$ (counit),

$\Delta\colon H \to H \otimes H$ (comultiplication), and

$s\colon H \to H$ (antipode)

making $H$ into a Hopf $R$-algebra. As is customary, we write

$$\mu(h_1 \otimes h_2) = h_1 h_2$$

and we adopt the Sweedler notation

$$\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$$

for comultiplication.

(1.2) The linear dual $H^* = \mathrm{Hom}_R(H, R)$ is a Hopf $R$-algebra with operations induced by duality; for example, for $f, g$ in $H^*$,

$$\Delta^*(f) = f \cdot \mu, \qquad \mu^*(f \otimes g) = (f \otimes g) \circ \Delta.$$

The $^*$ in $\Delta^*$ will often be suppressed when there is no danger of confusion.

(1.3) The augmentation ideal of $H$ is $\ker\{\varepsilon\colon H \to R\}$.

(1.4) The space of integrals $I$ of $H$ is defined by

$$I = \{f \in H^* | gf = \varepsilon(g)f \text{ for all } g \text{ in } H^*\}.$$

Since $H$ is finitely generated and projective as $R$-module, $I$ is nonzero, and, in fact, as $R$-modules, $H^* \cong H \otimes I$ [**21**, p. 98], so that $I$ is a rank one projective $R$-module.

(1.5) EXAMPLES. (a) If $G$ is a finite group, the group ring $RG$ is a Hopf algebra with $\varepsilon, \Delta, s$ defined by $\varepsilon(\sigma) = 1$, $\Delta(\sigma) = \sigma \otimes \sigma$, $s(\sigma) = \sigma^{-1}$, and $I = R(\sum_{\sigma \in G} \sigma)$.

(b) $(RG)^*$ is a Hopf algebra. If $\{v_\sigma\} \subseteq (RG)^*$ is the dual basis to $\{\sigma | \sigma \in G\}$, then the $v_\sigma$ are pairwise orthogonal idempotents summing to 1, and

$$\Delta(v_\sigma) = \sum_\tau v_\tau \otimes v_{\tau^{-1}\sigma},$$

$$\varepsilon(v_\sigma) = \delta_{1,\sigma} \quad \text{(Kronecker's delta)},$$

$$s(v_\sigma) = v_{\sigma^{-1}}.$$

Here $I = Rv_1$.

(c) Over rings of integers of algebraic number fields, group schemes of order $p$ have been classified by J. Tate and F. Oort [**22**]; locally, and in some cases globally these group schemes are represented by Hopf algebras which are free of rank $p$. When $p = 2$ see also [**17**].

(1.6) Let $R$ be a perfect field of characteristic $p$, and $H$ be a Hopf $R$-algebra which is commutative and cocommutative. Then

$$H^* \cong H_1^* \otimes_R H_2^*,$$

where $H_1^*$ is a separable $R$-algebra (cf. [**23**, p. 47]) and $H_2^*$ is connected, that is, as algebra has the form

$$H_2^* = R[h_1, \ldots, h_n]/\langle h_1^{p^{e_1}}, \ldots, h_n^{p^{e_n}} \rangle$$

(where if $p = 0$, $H^* = H_1^*$). For a proof, see Waterhouse [**23**, pp. 52, 112].

(1.7) DEFINITION. A commutative $R$-algebra $S$ is an $H$-object if $S$ is a finitely generated projective $R$-module and a right $H$-comodule via a map $\alpha\colon S \to S \otimes H$ which is an $R$-algebra homomorphism. (Notation: $\alpha(s) = \sum_{(s)} s_{(0)} \otimes s_{(1)}$.)

(1.8) $S$ is an $H$-object if and only if $S$ is a left $H^*$-module via a module structure map $\cdot\colon H^* \otimes S \to S$ which is a measuring, in the sense that

$$f \cdot (st) = \sum_{(f)} (f_{(1)} \cdot s)(f_{(2)} \cdot t), \qquad f \text{ in } H;\ s, t \text{ in } S.$$

The correspondence between $\alpha$ and $\cdot$ is as follows:

$$f \cdot s = \sum_{(s)} \langle f, s_{(1)} \rangle s_{(0)},$$

where $\langle\ ,\ \rangle$ is the duality pairing $H^* \otimes H \to R$; if $\{h_i, f_i\}_{i \in I}$ is a projective coordinate system for $H$ and $H^*$ so that

$$h = \sum_{i \in I} f_i(h) h_i,$$

for all $h$ in $H$, then

$$\alpha(s) = \sum_i f_i s \otimes h_i \quad \text{(cf. [\textbf{21}, p. 36]).}$$

(1.9) If $S$ is an $H$-object, the fixed ring under the action of $H^*$ is

$$S^{H^*} = \{s \in s | f \cdot s = \varepsilon(f) s \quad \text{for all } f \text{ in } H^*\}.$$

When $H^* = RG$, an $H$-object $S$ is an $R$-algebra on which $G$ acts as a group of $R$-algebra automorphisms and $S^{H^*} = S^G$, the fixed ring under the action of $G$.

(1.10) The trivial $H$-object is $H$ itself, with $\alpha = \Delta$. Then $H^*$ acts on $H$ by

$$f \cdot h = \sum_{(h)} \langle f, h_{(1)} \rangle h_{(0)}.$$

(1.11) Suppose $S$ is an $H$-object via $\alpha$. Then $S$ is a Galois $H$-object if the map $\gamma\colon S \otimes S \to S \otimes H$ defined by $\gamma(s \otimes t) = \sum_{(t)} st_{(0)} \otimes t_{(1)}$ is surjective. (By [**16**, 1.7] this is equivalent to $\gamma$ being an isomorphism.)

(1.12) EXAMPLES. (a) $S$ is a Galois $(RG)^*$-object if and only if $S$ is a Galois extension with group $G$ in the sense of [**6**].

(b) $S$ is a Galois $RG$-object if and only if $S = \sum_{\sigma \in G} S_\sigma$, where $S_\sigma$ are rank one projective $R$-modules, with

$$S_\sigma S_\tau = S_{\sigma\tau} \quad \text{for all } \sigma, \tau \text{ in } G.$$

In particular, $S$ is fully graded in the sense of Dade [**10**].

(c) $H$ is a Galois $H$-object: the map $\gamma\colon H \otimes H \to H \otimes H$ defined by $\gamma(g \otimes h) = (g \otimes 1)\Delta(h) = \sum g h_{(1)} \otimes h_{(2)}$ has an inverse $\theta$ ([**7**, Proposition 9.1]),

$$\theta(g \otimes h) = \sum g s(h_{(1)}) \otimes h_{(2)} \qquad (s = \text{antipode}).$$

(d) Sources of examples of Galois $H$-objects, $H \neq RG, (RG)^*$, include Chase and Sweedler [**7**, p. 35, Example 4.11], Chase [**5**, Proposition 5.2], Kreimer [**17**], Hurley [**13**], and Childs [**8, 9**].

(1.13) Suppose $S$ is a Galois $H$-object. The smash product of $S$ and $H^*$, $D = S \# H^*$, is defined to be $S \otimes H^*$ as $R$-module, with multiplication defined by

$$(s \# h)(\bar{s} \# \bar{h}) = \sum_{(h)} s(h_{(1)} \cdot \bar{s}) \# h_{(2)} \bar{h}.$$

Then $D \cong \operatorname{End}_R(S)$. If $M$ is any left $D$ module, then $M$ is also an $H^*$-module and $M \cong S \otimes (IM)$ as $D$-module where $I$ is the space of integrals of $H^*$, via the map $s \otimes f \cdot m = s(f \cdot m)$ [**7**, p. 69].

From (1.13) we have immediately

(1.14) $H$ is a faithful $H^*$-module,

and the useful

(1.15) PROPOSITION. *Suppose $S, T$ are $H$-objects and $\phi\colon S \to T$ is an $R$-algebra, $H^*$-module homomorphism. If $S$ is a Galois $H$-object and $IT = R$ where $I$ is the space of integrals of $H^*$, then $\phi$ is an isomorphism.*

PROOF OF (1.15). View $T$ as a $(D = S \# H^*)$-module via $(s \# f)t = \phi(s)ft$: that is, $S$ acts on $T$ via $\phi$. Then $T \cong S \otimes IT$ via $s \otimes ft \to \phi(s)ft$. If $IT = R$, then $S \cong S \otimes IT$ by $s \to s \otimes 1$, and the composite isomorphism $S \to S \otimes IT \to T$ is $\phi$.

**2. Tame objects.** Let $G$ be a finite group, $R$ the ring of integers of an algebraic number field $K$, $L$ a Galois extension field of $K$ with group $G$, and $S$ the ring of integers of $L$. Then $S \supset R$ is tame if for each prime ideal $p$ of $R$, the ramification index of $p$ in $S$ is relatively prime to the characteristic of $R/p$. This condition is equivalent to the condition that the trace map tr: $S \to R$, $\mathrm{tr}(s) = \sum \sigma(s)$, is onto [**4**, p. 33].

When $R$ and $S$ are not necessarily rings of integers, and $G$ is a group of $R$-algebra automorphisms of $S$ with $S^G = R$, notions of tameness have been developed by Auslander and Rim [**1**] and A. D. Barnard [**2**]. Auslander and Rim assume $R$ is an integrally closed, local, Noetherian domain, and develop (without assuming a group $G$ of automorphisms) a generalization of the ramification index using multiplicity theory. Tameness is defined as in the classical case to be the condition that for all primes of $S$, the ramification index is prime to the residue field characteristic. Barnard works with general commutative rings and develops a theory of decomposition group, inertia group, and ramification group analogous to the classical theory for number fields [**4**, p. 33]. Tameness is defined as triviality of the ramification group at every prime, which again conforms to the classical definition.

Both Auslander/Rim and Barnard show that in their respective situations, $S \supset R$ is tame if and only if the trace map tr: $S \to R$ is surjective.

If we translate these situations into Hopf algebra terms, we are considering $S$ to be an $H$-object for $H = (RG)^*$. Then $S^G = S^{RG} = S^{H^*}$.

It is easy to verify that the image of the trace map is $(\sum \sigma)S$ and $\sum \sigma$ generates the space of integrals for $H = RG$. Thus the statement that tr: $S \to S^{RG} = R$ is surjective translates to $IS = S^{RG} = R$.

Note that for any $s$, $\mathrm{tr}(s)$ is in $R$, so $IS \subseteq S^{RG}$. More generally, the reader may easily verify (or see [**21**, p. 203]):

(2.1) If $H$ is a Hopf algebra and $S$ an $H$-object, then $IS \subseteq S^{H^*}$.

The above observations motivate (c) of the next definition. Recall that in this paper both Hopf algebras and their objects are assumed to be finitely generated projective $R$-modules.

(2.2) DEFINITION. Suppose $H$ is a Hopf $R$-algebra and $S$ is an $H$-object. Then $S$ is a tame $H$-object if

(a) $\mathrm{rank}_R(S) = \mathrm{rank}_R(H)$ as projective $R$-modules (this means locally at each prime ideal of $R$ if $S$ and $H$ do not have constant rank);

(b) $S$ is a faithful $H^*$-module; and

(c) $IS = S^{H^*} = R$.

In view of the preceding discussion it is clear that if $O_L \supset O_K$ is a tame extension of number rings, $O_L$ is a tame $O_K G^*$-object in our sense, and vice versa, conditions (a) and (b) being known to hold for number ring extensions.

When $H^* = RG$ and $R \subset S$ are rings of integers, $S$ is a Galois extension of $R$ if no prime ideal of $R$ ramifies in $S$, and so Galois implies tame. That implication holds generally:

(2.3) PROPOSITION. *Let $H$ be a Hopf algebra and $S$ a Galois $H$-object. Then $S$ is tame.*

PROOF. That $S^{H^*} = R$ is [**7**, Theorem 7.6]. If $S$ is a Galois $H$-object, then for all primes $p$ of $R$, $S \otimes S \otimes R_p \cong S \otimes H \otimes R_p$ as $R_p$-modules; it is then clear that the local ranks agree. The faithfulness of $S$ follows from the isomorphism $S \# H^* \cong \mathrm{End}_R(S)$.

For condition (c), we view $S$ as a module over the smash product $D = S \# H^*$, $(s \# u) \cdot x = s(u \cdot x)$. Then by (1.13), $S = (IS)S$. But $S$ is finitely generated and projective so a routine Cramer's rule argument yields that $IS = R$ (or see the proof of (1.9) and (1.10) of [**16**]). It follows that $S$ is a tame $H$-object.

(2.4) COROLLARY. $H^{H^*} = R = IH$.

For $H$ is a Galois $H$-object (1.12)(c).

We wish to show that $H$-objects with local normal bases are tame. Using Kreimer and Cook's result [**15**] that Galois $H$-objects have local normal bases, this will give a second proof of (2.3). We first need a "base change" lemma.

(2.5) LEMMA. (i) *If $\tilde{R}$ is a flat extension of $R$ and $S$ is a tame $H$-object, then $S \otimes_R \tilde{R}$ is a tame $(H \otimes_R \tilde{R})$-object.*

(ii) *If $\tilde{R}$ is faithfully flat and $S$ is an $H$-object such that $S \otimes \tilde{R}$ is a tame $(H \otimes \tilde{R})$-object, then $S$ is a tame $H$-object.*

PROOF. Set $\tilde{S} = S \otimes_R \tilde{R}$, $\tilde{H} = H \otimes_R R$, and $\tilde{H}^* = H^* \otimes_R \tilde{R}$ (unambiguous since $H$ is finitely generated projective over $R$).

(a) If $S$, $H$ are finitely generated and projective, then so are $\tilde{S}$ and $\tilde{H}$, and conversely if $\tilde{R}$ is faithfully flat [**3**, I, §3, no. 6, Proposition 12].

If $\mathrm{rank}_R S = \mathrm{rank}_R H$ locally, then $\mathrm{rank}_{\tilde{R}} \tilde{S} = \mathrm{rank}_{\tilde{R}} \tilde{H}$ locally by the proof of [**3**, II, §5, no. 4, Proposition 4]; for $\tilde{R}$ faithfully flat, the converse follows from the fact that every prime ideal of $R$ is the contraction of a prime ideal of $\tilde{R}$ [**3**, II, §2, no. 5, Corollary 4 to Proposition 11].

(b) and (c) $S$ is a faithful $H^*$-module if and only if $\ker\{\beta^* \colon H^* \to \mathrm{End}_R(S)\}$ is zero. Also, $S^{H^*} = \ker\{\beta \colon S \to S \otimes H\}$ where $\beta = \alpha - \varepsilon_1$, $\varepsilon_1(s) = s \otimes 1$ [**7**, Proposition 10.1]. Thus the faithfulness property and the property $S^{H^*} = R$ are preserved under flat extension and reflected under faithfully flat extension. Finally $I_{H^* \otimes \tilde{R}} = I_{H^*} \otimes \tilde{R}$ if $\tilde{R}$ is $R$-flat since $I_{H^*} = (H^*)^{H^*}$; it follows that $I_{\tilde{H}^*} \tilde{S}^* = I_{H^*} S \otimes \tilde{R}$, and the property $I_{H^*} S = R$ is also preserved under flat extension and reflected under faithfully flat extension.

(2.6) COROLLARY. *The $H$-object $S$ is tame if and only if $S \otimes R_p$ is a tame $(H \otimes R_p)$-object for all primes $p$ of $R$.*

PROOF. If $S$ is a tame $H$-object, then, since $R_p$ is $R$-flat, $S \otimes R_p$ is a tame $(H \otimes R_p)$-object for any prime $p$. The converse follows from the easily seen fact that if $S \otimes R_p$ is a tame $(H \otimes R_p)$-object for all $p$, then $S \otimes \prod_p R_p$ is a tame $(H \otimes \prod_p R_p)$-object, and $\prod_p R_p$ is $R$-faithfully flat.

(2.7) THEOREM. *Suppose $S$ is an $H$-object such that $S^{H^*} = R$ and $S \otimes R_p \simeq H \otimes R_p$ as $(H^* \otimes R_p)$-module for all primes $p$ of $R$. Then $S$ is tame.*

PROOF. In view of Corollary (2.6) we may without loss of generality assume $R$ is local and $S \simeq H$ as $H^*$-module.

Suppose $\phi\colon S \to H$ is the $H^*$-isomorphism. Then since $H$ satisfies conditions (a) and (b) and $\phi^{-1}$ must preserve these properties, $S$ satisfies (a) and (b). Since $\phi$ is an $H^*$-module homomorphism, $\phi(IS) \subseteq IH$; also, $\phi(S^{H^*}) \subseteq H^{H^*}$ since

$$S^{H^*} = \{s \text{ in } S | (f - \varepsilon(f))s = 0 \text{ for all } f \text{ in } H^*\}.$$

Since $\phi$ is an isomorphism, the inclusions are equalities.

(2.8) *Note.* If $R$ is integrally closed, then the assumption in (2.7) that $S^{H^*} = R$ may be dropped. Since $H$ is the trivial $H$-Galois object, $H^{H^*} = R$; by the measuring property, $S^{H^*} \supseteq R$. If $\phi\colon H \to S$ is an $H^*$-module isomorphism, then $\phi(S^{H^*}) = H^{H^*} = R$ so $\phi(1_S) = t$ for some $t$ in $R$. But then, since $\phi^{-1}$ is $R$-linear,

$$1_S = \phi^{-1}(t) = t\phi^{-1}(1)$$

in $S^{H^*}$. So $t$ is invertible in $S$. If $R$ is integrally closed, since $S$ is integral over $R$, then $t^{-1} = \phi^{-1}(1)$ is in $R$. But as $R$-module, $S^{H^*} = R\phi^{-1}(1)$, and so $S^{H^*} \subseteq R$.

(2.9) REMARK. Theorem 2.7 shows that the following three conditions making up the definition of tame $H$-object are necessary for the existence of local normal basis:

(a) equal ranks of $H$ and $S$,
(b) faithful $H$-action on $S$, and
(c) the space of integrals maps $S$ onto $R$, the fixed ring of $S$ under $H^*$.

The following two examples show that conditions (a) and (b) are independent of condition (c).

(2.10) The first example is due to A. D. Barnard [**2**, p. 283] and shows that it is possible to construct an $H$-object with $S^{H^*} = IS = R$ but which is not finitely generated as an $R$-module.

Let $R$ be a field (char $\neq 2$). As a set let

$$S = \{a + p(x) | a \in R,\ p(x) \in R[x] \text{ with only odd powers of } x\}.$$

$S$ is a ring with the usual addition and multiplication given by $x^{\text{odd}} \cdot x^{\text{odd}} = 0$, that is

$$(a + p(x))(b + q(x)) = ab + aq(x) + bp(x).$$

$S$ is an $R$-algebra via $a \mapsto a + 0$. The group ring $RG$, $G$ of order 2, acts on $S$: if $\sigma$ generates $G$, then

$$\sigma(a + p(x)) = a - p(x).$$

It is easy to check that

$$\sigma((a + p(x))(b + q(x))) = \sigma(a + p(x))\sigma(b + q(x))$$

so that the $RG$-action measures and $S$ is an $(RG)^*$-object. It is clear that $S^G = R$ and $\operatorname{trace}(\frac{1}{2}) = 1$ so $IS = S^G = R$. Hence condition (c) holds. It is also clear that $S$ is not finitely generated over $R$. So (a) fails, and we cannot have $S \cong H$ as $H^*$-module.

(2.11) For the second example, let $G$ be a finite group and $H$ the group ring $RG$. Then $H^* = RG^* = \bigoplus_{\sigma \in G} Rv_\sigma$ as $R$-algebra with $\{v_\sigma\}_{\sigma \in G}$ mutually orthogonal idempotents. Let $S$ be an $H$-object such that $S^{H^*} = R$. We shall show condition (c) always holds but not condition (b).

Since $H^* = \bigoplus_{\sigma\in G} Rv_\sigma$ as $R$-algebra, the action of $H^*$ on $S$ yields $S = \bigoplus_{\sigma\in G} v_\sigma \cdot S$ as $H^*$-module, where $v_\sigma \cdot s = s$ for $s \in v_\sigma \cdot S$, and $v_\tau \cdot s = 0$ for $\tau \neq \sigma$. Since $\varepsilon(v_\sigma) = \delta_{1,\sigma}$, it is straightforward to show that $I = Rv_1$, and that $v_1 \cdot S = S^{H^*} = IS$. In fact:

(2.12) PROPOSITION. *For $H = RG$, an $H$-object $S$ is tame if and only if $S^{H^*} = R$ and $S$ satisfies conditions* (a) *and* (b) *of* (2.2).

To show that an $H$-object may not be a faithful $H^*$-module for $H = RG$, consider the following example.

Let $R$ be a field and $H = R(\mathbf{Z}/3\mathbf{Z})$. Let $S$ be the $R$-algebra

$$S = \frac{R[x,y]}{\langle x^2, y^2, xy\rangle}.$$

$S$ is an $H$-object via the map $\alpha\colon S \to S \otimes H$ given by

$$\alpha(r) = r \otimes 1 \quad \text{for all } r \in R,$$
$$\alpha(x) = x \otimes \sigma, \qquad \alpha(y) = y \otimes \sigma,$$

extended to $S$ by the requirement that $\alpha$ be an $R$-algebra map. This is well defined since

$$\alpha(x^2) = x^2 \otimes \sigma^2 = 0, \quad \alpha(y^2) = y^2 \otimes \sigma^2 = 0, \quad \alpha(xy) = xy \otimes \sigma^2 = 0,$$

so $S$ is an $H$-object. But, recalling that $f \cdot s = \sum_{(s)} \langle f, s_{(1)}\rangle s_{(0)}$, for $f \in H^*$ and $s \in S$, we see that $S$ is not a faithful $H^*$-module since

$$v_{\sigma^2} \cdot r = \langle v_{\sigma^2}, 1\rangle r = 0, \qquad v_{\sigma^2} \cdot x = \langle v_2, \sigma\rangle x = 0,$$

and

$$v_{\sigma^2} \cdot y = \langle v_{\sigma^2}, \sigma\rangle y = 0$$

so $v_{\sigma^2} \cdot S = 0$.

**3. Two special cases.** In Theorem (2.7) we showed that $H$-objects with local normal basis are tame. This section establishes the converse for cocommutative Hopf algebras whose duals are separable or connected. We consider the separable case first.

(3.1) THEOREM. *Let $H$ be a cocommutative Hopf $R$-algebra such that $H^*$ is separable. If $S$ is a tame $H$-object, then $S$ has local normal bases, i.e. $S \otimes R_p \cong R_p$ as $(H^* \otimes R_p)$-module for all primes $p$ of $R$.*

This theorem applies, for example, if $\dim H$ is a unit of $R$, for then $H$ and $H^*$ are separable [**22**, Lemma 5]. Thus tame implies normal basis over fields of characteristic 0.

The proof of this theorem makes use of the following lemma.

(3.2) LEMMA. *Suppose $H$ is a cocommutative Hopf algebra over a local ring $R$ and $S$ is an $H$-object. Suppose $\tilde{R}$ is a faithfully flat extension of $R$. Then $S \simeq H$ as $H^*$-module if and only if $S \otimes \tilde{R} \cong H \otimes \tilde{R}$ as $(H^* \otimes \tilde{R})$-module.*

PROOF. If $S \cong H$ as $H^*$-modules, then $S \otimes \tilde{R} \cong H \otimes \tilde{R}$ as $(H \otimes \tilde{R})$-modules. Conversely, suppose $S \otimes \tilde{R} \cong H \otimes \tilde{R}$ as $(H^* \otimes \tilde{R})$-modules. Now $H \otimes \tilde{R}$ is a Galois

$(H \otimes \tilde{R})$-object, hence is a rank one projective $(H^* \otimes \tilde{R})$-module by [**15**], as is, therefore, $S \otimes \tilde{R}$. If $\tilde{R}$ is faithfully flat over $R$, then $H^* \otimes \tilde{R}$ is faithfully flat over $H^*$. Thus $S$ and $H$ are rank one projective $H^*$-modules. Since $H^*$ is semilocal, the lemma follows.

PROOF OF THEOREM (3.1). We can assume $R$ is local by (2.6). Then both tameness and $S \simeq H$ are preserved and reflected by faithfully flat extensions (Lemmas (2.5) and (3.2)). Using [**11**, Lemma 2.8, p. 97], we may therefore assume in the proof of the theorem that since $H^*$ is separable, $H^* = Re_1 \oplus Re_2 \oplus \cdots \oplus Re_n$ as $R$-algebra with the $\{e_i\}$ mutually orthogonal idempotents.

Since $S$ is an $H$-object, the action of $H^*$ on $S$ yields $S \simeq \bigoplus_{i=1}^n S_i$ as $H^*$-module, where $S_i = e_i \cdot S$. Now $S$ is free so each $S_i$ is a projective $R$-module which is free since $R$ is local. Since $S$ is tame, $\dim_R S = n$ and each $S_i$ is nonempty by faithfulness. Hence for each $i$, $S_i \simeq R$ as $R$-module. Let $s_i$ generate $S_i$ over $R$. Then $S \simeq \bigoplus_{i=1}^n Rs_i$ as $H^*$-module with $e_i \cdot s_j = \delta_{i,j} s_j$. In particular, since $H$ is a tame $H$-object $H \simeq \bigoplus_{i=1}^n Rx_i$ as $H^*$-module with $e_i x_j = \delta_{i,j} x_j$.

It is then apparent that the map $\phi\colon S \to H$ given by $\phi(s_i) = x_i$ is an $H^*$-module isomorphism. This establishes Theorem (3.1).

Now we consider $H$-objects when $H^*$ is connected (cf. (1.6)).

(3.3) THEOREM. *Suppose $R$ is a commutative ring and $H$ is a cocommutative Hopf algebra such that, as $R$-algebra,*

$$H^* = \frac{R[f_1, f_2, \ldots, f_n]}{\langle f_1^{p^{e_1}}, f_2^{p^{e_2}}, \ldots, f_n^{p^{e_n}} \rangle}$$

*for some prime $p$, where $\varepsilon(f_i) = 0$ for all $i = 1, \ldots, n$. Suppose $S$ is an $H$-object, not necessarily finitely generated and projective as $R$-module, such that $IS = S^{H^*} = R$. Then $S$ is a Galois $H$-object.*

The hypothesis on $S$ is (c) of the definition of tameness. Thus this theorem implies that when $H^*$ is connected, an $H$-object $S$ is tame if and only if $S$ is Galois if and only if $IS = S^{H^*} = R$.

PROOF. Kreimer and Takeuchi [**16**] proved that an $H$-object $S$, not a priori finitely generated and projective as $R$-module, is a Galois $H$-object (and hence is finitely generated and projective as $R$-module) if the left $S$-module map $\gamma\colon S \otimes S \to S \otimes H$ given by

$$\gamma(s \otimes t) = \sum_{(t)} st_{(0)} \otimes t_{(1)}$$

is surjective.

If $\{x_i, f_i\}_{i \in H}$ is a dual basis sytem for $H$, $H^*$, then $\alpha$ can be recovered from the $H^*$-module action on $S$ by

$$\alpha(s) = \sum_i f_i \cdot s \otimes x_i \quad \text{(see (1.8))}$$

so

$$\gamma(s \otimes t) = \sum_i sf_i \cdot t \otimes x_i.$$

Thus the set $\{1 \otimes x_i\}$ is an $S$-basis for $S \otimes H$, and to show $S$ is Galois we find, for each $i$, a set $\{(a_K, b_K)\} \subseteq S \times S$ such that

$$\gamma\left(\sum_K a_K \otimes b_K\right) = 1 \otimes x_i.$$

Now $H^*$ has $R$-basis $\{f_1^{j_1} f_2^{j_2} \cdots f_n^{j_n} | 0 \leq j_i < p^{e_i} \text{ for } i = 1, \ldots, n\}$, and we have

(3.4) The space of integrals $I$ of $H^*$ is generated by the element

$$\phi = f_1^{p^{e_1}-1} f_2^{p^{e_2}-1} \cdots f_n^{p^{e_n}-1}.$$

To see (3.4), note that for any integral $\psi$ of $I$ and any $i$, $f_i\psi = \varepsilon(f_i)\psi = 0$. Thus $\psi$ must be a multiple of $\phi$.

Since $IS = R$, there exists some $z \in S$ such that $\phi z = 1$.

(3.5) We adopt the following multinomial notation.

If

$$F = (f_1, f_2, \ldots, f_n), \qquad J = (j_1, j_2, \ldots, j_n),$$

then

$$F^J = f_1^{j_1} f_2^{j_2} \cdots f_n^{j_n}, \qquad |J| = \sum_{i=1}^n j_i,$$

and

$$F^{\overline{J}} = f_1^{p^{e_1}-j_1-1} f_2^{p^{e_2}-j_2-1} \cdots f_n^{p^{e_n}-j_n-1}.$$

In this notation, our basis for $H^*$ becomes

$$\{F^J | 0 \leq j_i < p^{e_i},\ i = 1, \ldots, n\}.$$

Let $\{X^J | 0 \leq j_i < p^{e_i}, i = 1, \ldots, n\}$ denote the basis of $H$ dual to that for $H^*$.

To show that $S$ is a Galois $H$-object, we shall find for every $J$ a set $\{(a_K, b_K)\} \subseteq S \times S$ such that

$$\gamma\left(\sum_K a_K \otimes b_K\right) = \sum_L \left(\sum_K a_K(F^L \cdot b_K)\right) \otimes X^L = 1 \otimes X^J,$$

where the sum over $L$ is over all elements of the basis of $H^*$; that is:

(3.6) Given any $J$ such that $0 \leq j_i < p^{e_i}$ for all $i$, there exists $\{(a_K, b_K)\} \subseteq S \times S$ such that

$$\sum_K a_K(F^J \cdot b_K) = 1, \qquad \sum_K a_K(F^H \cdot b_K) = 0 \quad \text{for all } H \neq J.$$

We define $a_K, b_K$ as follows: for all $K = (k_1, \ldots, k_n)$, $0 < k_i \leq p^{e_i}$, let $b_K = F^{\overline{K}} \cdot z$ ($F^{\overline{K}}$ as defined above). We define $a_K$ as follows:

$$\begin{aligned} a_K &= 0 && \text{if } |K| \geq |J|, K \neq J, \\ a_J &= 1, && \\ a_K &= -\sum_{|L|>|K|} a_L(F^K b) && \text{if } |K| < |J|. \end{aligned}$$

Observe that:

(3.7) For all $K$ such that $|K| \geq |J|$, $K \neq J$, and all $H$,

$$a_K(F^H \cdot b_K) = 0 \quad \text{since } a_K = 0.$$

(3.8) For all $H, K$ such that $|H| \geq |K|$, $H \neq K$,

$$F^H \cdot b_K = (F^H F^{\overline{K}}) \cdot z = 0$$

since for some $i$, $f^{p^{e_i}} = 0$ is a factor of $F^H F^{\overline{K}}$.

(3.9) $F^K \cdot b_K = (f_1^{p^{e_1}-1} \cdots f_n^{p^{e_n}-1}) \cdot z = 1$ for all $K$.

To show that

$$\sum_K a_K(F^H \cdot b_K) = \begin{cases} 1 & \text{if } H = J, \\ 0 & \text{otherwise,} \end{cases}$$

we have from (3.7) that

$$\sum_K a_K(F^H \cdot b_K) = a_J(F^H \cdot b_J) + \sum_{|K|<|J|} a_K(F^H \cdot b_K). \tag{3.10}$$

*Case* 1. When $|H| \geq |J|$ but $H \neq J$, (3.8) and (3.10) imply that

$$\sum_K a_K(F^H \cdot b_K) = 0.$$

*Case* 2. When $H = J$, (3.8) and (3.10) imply that

$$\sum_{|K|<|J|} a_K(F^J \cdot b_K) = 0,$$

so $\sum_K a_K(F^J \cdot b_K) = a_J(F^J \cdot b_J) = 1$ by (3.9) and the definition of $a_J$.

*Case* 3. When $|H| < |J|$,

$$\sum_K a_K(F^H \cdot b_K) = \sum_{\substack{|H|\geq|K| \\ H\neq K}} a_K(F^H \cdot b_K) + a_H(F^H \cdot b_H) + \sum_{|H|<|K|} a_K(F^H \cdot b_K).$$

The first summand $= 0$ by (3.8). The second summand $= a_H$ by (3.9) but

$$a_H = -\sum_{|K|>|H|} a_K(F^H \cdot b_K),$$

so $\sum_K a_K(F^H \cdot b_K) = 0$.

This establishes (3.6). It follows that $\gamma$ is surjective and $S$ is a Galois $H$-object, completing the proof of Theorem (3.3).

It follows that $S$ is finitely generated and projective over $R$ by [**16**, (1.7)]. In fact, the reader may verify that if $z \in S$ satisfies $\phi z = 1$, then $\{F^J \cdot z\}$ is an $R$-basis of $S$. Thus the map $1 \mapsto z$ yields an $H^*$-isomorphism $H^* \to S$, and $S$ has a normal basis (cf. also [**16**, Proposition 2.7]).

**4. Normal bases over perfect fields.** In this section we put together the results from §§2 and 3 to characterize, over a perfect field, those $H$-objects with normal basis when $H$ is commutative and cocommutative.

(4.1) THEOREM. *Suppose $H$ is a Hopf $R$-algebra, $R$ a commutative ring, such that $H^* = H_1^* \otimes H_2^*$, where $H_1^*$ is commutative and separable* (*as in* (3.1)) *and $H_2^*$ is connected* (*as in* (3.3)). *Then an $H$-object $S$ is tame if and only if $S$ has local normal bases.*

PROOF. The "if" part is Theorem 2.7.

For the converse, let $S$ be a tame $H$-object. Let $H_1^*$ act by restriction on $S^{H_2^*}$, and $H_2^*$ on $S^{H_1^*}$. Then the measuring property is inherited so that $S^{H_2^*}$ is an $H_1$-object, and $S^{H_1^*}$ an $H_2$-object (except that we must check finite generation and projectivity over $R$). We shall show that $S \cong S^{H_2^*} \otimes S^{H_1^*}$, $S^{H_1^*} \cong H_2$, and $S^{H_2^*} \cong H_1$ locally, as $H^*$-, $H_2^*$-, and $H_1^*$-modules, respectively, from which it will follow that as $H^*$-modules, locally $S \cong H_1 \otimes H_2 = H$.

One verifies easily that $R = S^{H^*} = S^{H_1^* \otimes H_2^*} = (S^{H_1^*})^{H_2^*} = (S^{H_2^*})^{H_1^*}$, and that $I_{H^*} = I_{H_1^*} \otimes I_{H_2^*}$.

We have

$$R = I_{H^*}S = I_{H_2^*}(I_{H_1^*}S) \subseteq I_{H_2^*}(S^{H_1^*}) \subseteq (S^{H_2^*})^{H_1^*} = R.$$

Since $H_2^*$ is connected, by (3.3) $S^{H_1^*}$ is a Galois $H_2$-object and $S^{H_1^*} \cong H_2$ as $H_2^*$-objects. In particular, $S^{H_1^*}$ is finitely generated and projective over $R$.

Now $S$ is a left $D$-module, $D = S^{H_1^*} \# H_2^* \cong \mathrm{End}_R(S^{H_1^*})$. By (1.15) $S \cong S^{H_1^*} \otimes I_{H_2^*}S$ as left $D$-modules. Then $S^{H_2^*} \cong (S^{H_1^*})^{H_2^*} \otimes I_{H_2^*}S$ (since the action of $D$ on $S$ is via its action on $S^{H_1^*}$), so $S^{H_2^*} = I_{H_2^*}S$. Thus $S \cong S^{H_1^*} \otimes S^{H_2^*}$. The isomorphism is given by the multiplication in $S$, and this is easily seen to be an $H^*$-module map. We must show that $S^{H_2^*}$ is a tame $H_1^*$-object.

First, since $S^{H_1^*}$ is $R$-projective, $R$ is an $R$-module direct summand of $S^{H_1^*}$, so $S^{H_2^*} \cong R \otimes S^{H_2^*}$ is an $R$-direct summand of $S$. Since $S$ is $R$-projective, so is $S^{H_2^*}$.

Then $\mathrm{rank}_R\, S^{H_2^*} = \mathrm{rank}_R\, H_1$ since $\mathrm{rank}\, S = \mathrm{rank}\, H$ and $\mathrm{rank}\, S^{H_1^*} = \mathrm{rank}\, H_2$. Also $S^{H_2^*}$ is a faithful $H_1^*$-module since $S$ is a faithful $H$-module; and

$$R = I_{H^*}S = I_{H_1^*}(I_{H_2^*}S) \subseteq I_{H_1^*}(S^{H_2^*}) \subseteq (S^{H_2^*})^{H_1^*} = R.$$

Thus $S^{H_2^*}$ is a tame $H_1$-object. By (3.1) $S^{H_2^*}$ has local normal basis. This completes the proof.

(4.2) COROLLARY. *Suppose $R$ is a perfect field and $H$ a commutative, cocommutative Hopf algebra over $R$. Then an $H$-object $S$ is tame if and only if $S \simeq H$ as $H^*$-module.*

PROOF. This follows immediately from (4.1) and the decomposition of (1.6).

**5. Local normal bases over integral domains.** Corollary (4.2) established a criterion for the existence of a normal basis for an $H$-object $S$, $H$ commutative and cocommutative, over a perfect field. In case the field has characteristic 0, Theorem (3.1) applies whenever $H$ is cocommutative.

In this section we consider the situation where $R$ is an integral domain with quotient field $K$, $H$ is a Hopf $R$-algebra, and $S$ is an $H$-object (both finitely generated and projective as $R$-modules). We suppose that $S \otimes K$ is an $(H \otimes K)$-object with normal basis, and seek criteria for $S$ to be an $H$-object with local normal bases.

Since $H$ is locally isomorphic to $H^*$ as $H^*$-module, an obvious necessary condition is that $S$ be $H^*$-projective. In the classical situation, $H^* = RG$, surjectivity of the trace map $S \to R$ implies projectivity (cf. [**20**, Lemma 20]). So also here.

(5.1) THEOREM. *Let $R$ be a commutative ring, $H$ be an $R$-Hopf algebra which is a finitely generated projective $R$-module, and $S$ an $R$-algebra which is an $H$-object and a finitely generated projective $R$-module. Let $I$ be the space of integrals of $H^*$. If $IS = R$, then $S$ is $H^*$-projective.*

PROOF. Since $S$ is $H^*$-projective if and only if $S_p$ is $H_p^*$-projective for every prime ideal $p$ of $R$, we can assume $R$ is local. In that case, $I$ is free of rank one over $R$, $I = R\phi$ for some integral $\phi$, and the condition $IS = R$ becomes the condition that there exists $z$ in $S$ so that $\phi(z) = 1$.

Since $S$ is $R$-projective, $H^* \otimes S$, with $H^*$-action on $H^*$, is $H^*$-projective.

Let $\mu\colon H^* \otimes S \to S$ be the $H^*$-action on $S$. With $H^*$-action on $H^* \otimes S$ via that on $H^*$, $\mu$ is an $H^*$-module map.

Let $\lambda\colon S \to H^* \otimes S$ be defined by

$$\lambda(x) = \sum_{(\phi)} \phi_{(1)} \otimes z(\phi^s_{(2)} x).$$

Then

$$\begin{aligned}\mu\lambda(x) &= \sum_{(\phi)} \phi_{(1)}(z \cdot \phi^s_{(2)} x) = \sum_{(\phi)} (\phi_{(1)} \cdot z)(\phi_{(2)} \phi^s_{(3)} x) \\ &= \sum_{(\phi)} (\phi_{(1)} \cdot z)\varepsilon(\phi_{(2)})x = \sum_{(\phi)} (\phi_{(1)}\varepsilon(\phi_{(2)})z)x \\ &= \phi(z)x = x.\end{aligned}$$

So $\lambda$ is injective and splits $\mu$.

To show that $S$ is $H^*$-projective, it suffices to show that $\lambda$ is an $H^*$-module map, that is, $f \cdot \lambda(x) = \lambda(f \cdot x)$.

We thank the referee for pointing out the following direct argument of Sweedler [**2**, p. 104]:

For $f \in H^*$ we have $f = (1 \otimes \varepsilon)\Delta f = \sum_{(f)} \varepsilon(f_{(2)}) f_{(1)}$. Hence

$$\begin{aligned}\sum f\phi_{(1)} \otimes \phi^s_{(2)} &= \sum_{(\phi)(f)} \varepsilon(f_{(2)}) f_{(1)}\phi_{(1)} \otimes (\phi^s_{(2)}) \\ &= \sum_{(\phi)(f)} f_{(1)}\phi_{(1)} \otimes \varepsilon(f_{(2)})\phi^s_{(2)} \\ &= \sum f_{(1)}\phi_{(1)} \otimes \phi^s_{(2)} f^s_{(2)} f_{(3)} \\ &= \sum f_{(1)}\phi_{(1)} \otimes (f_{(2)}\phi_{(2)})^s f_{(3)} \\ &= \sum_{(f)} ((1 \otimes s)\Delta)(f_{(1)}\phi)(1 \otimes f_{(2)}) \\ &= \sum_{(f)} ((1 \otimes s)\Delta)(\varepsilon(f_{(1)})\phi)(1 \otimes f_{(2)}) \\ &\qquad\qquad \text{(since } \phi \text{ is an integral)} \\ &= (1 \otimes s)\Delta(\phi) \sum_{(f)} (1 \otimes \varepsilon(f_{(1)}) f_{(2)}) \\ &= (1 \otimes s)\Delta(\phi)(1 \otimes f) = \sum_{(\phi)} \phi_{(1)} \otimes \phi^s_{(2)} f.\end{aligned}$$

Hence

$$\begin{aligned} f(\lambda(x)) &= \sum_{(\phi)} f\phi_{(1)} \otimes z(\phi^s_{(2)}x) \\ &= (1\otimes z)\left(\left(\sum f\phi_{(1)}\otimes\phi^s_{(2)}\right)(1\otimes x)\right) \qquad (1\in H^*) \\ &= (1\otimes z)\left(\left(\sum \phi_{(1)}\otimes\phi^s_{(2)}f\right)(1\otimes x)\right) \\ &= \sum_{(\phi)} \phi_{(1)}\otimes z(\phi^s_{(2)}(f(x)) = \lambda(f(x)). \end{aligned}$$

Thus $\lambda$ is an $H^*$-module map, as was to be shown. Hence $S$ is $H^*$-projective, since it is an $H^*$-direct summand of the $H^*$-projective module $H^*\otimes S$.

(5.2) THEOREM. *Suppose $R$ is a domain with quotient field $K$, $H^*$ is a commutative Hopf $R$-algebra, and $S$ is an $H$-object. Let $L = S\otimes K$. If $S$ is a projective $H^*$-module and $L$ has a normal basis as an $H\otimes K$-object, then $S$ has local normal bases as an $H$-object.*

PROOF. We may clearly assume that $R$ is a local ring. Write $H^* = \sum_i H^*e_i$, where $1 = \sum_i e_i$, and the $e_i$ are indecomposable pairwise mutually orthogonal idempotents. Set $H^*e_i = I_i$, indecomposable $H^*$-modules. Let $S = J_1\oplus J_2\oplus\cdots\oplus J_r$ and $H = Y_1\oplus Y_2\oplus\cdots\oplus Y_x$ be direct sums of indecomposable $H^*$-modules.

We show $S\cong H$ as $H^*$-modules by showing, by induction on $r$:

(5.3) If $J = J_1\oplus\cdots\oplus J_r$ and $Y = Y_1\oplus\cdots\oplus Y_s$ are two projective $H^*$-modules, direct sums of indecomposable $H^*$-modules, and $J\otimes K\cong Y\otimes K$ as $(H^*\otimes K)$-modules, then $J\cong Y$.

The proof is obvious for $r=1$.

For $r>1$, since $J$ is a projective $H^*$-module, $J_r\cong I_i = e_iH^*$ for some $i$. Then $e_iJ\neq 0$, so $e_i(J\otimes K)\neq 0$. Since $J\otimes K\cong Y\otimes K$, $e_i(Y\otimes K)\neq 0$, so $e_i(Y)\neq 0$. But $e_i(Y)=0$ if $Y_j\not\cong I_i$ for all $j$. So some $Y_j\cong I_i\cong J_r$.

Suppose $Y_s\cong J_r$. Write $J = J'\oplus J_r$, $Y = Y'\oplus Y_s$. Then

$$J\otimes K\cong (J'\otimes K)\oplus(J_r\otimes K)$$

and

$$Y\otimes K\cong (Y'\otimes K)\oplus(Y_s\otimes K).$$

By the Krull-Schmidt Theorem [**19**, p. 88]

$$J'\otimes K\cong Y'\otimes K.$$

By induction, $J'\cong Y'$. Since $J_r\cong Y_s$, we obtain $J\cong Y$, completing the proof of (5.3) and Theorem (5.2).

(5.4) THEOREM. *Let $R$ be an integral domain with quotient field $K$, $H$ a cocommutative Hopf $R$-algebra which is a finitely generated projective $R$-module, and $S$ an $R$-algebra, finitely generated and projective as $R$-module, and an $H$-object such that $S^{H^*} = R$.*

*If $S$ has local normal bases, then $S$ is a tame $H$-object. Conversely, if $S$ is a tame $H$-object, then $S$ has local normal bases whenever*

(a) *$K$ is perfect and $H$ is commutative, or*

(b) $H \otimes K$ *is separable.*
*Condition* (b) *holds if* $\operatorname{char} K = 0$ *or* $\operatorname{char} K$ *is relatively prime to* $\dim_K(H \otimes K)$.

PROOF. That local normal bases implies tame is Theorem (2.7).

For the converse, since $K$ is $R$-flat, if $S$ is a tame $H$-object, then $S \otimes K$ is a tame $(H \otimes K)$-object, and $S$ is a tame $H$-object for all prime ideals $p$ of $R$, both by Lemma (2.5)(i). So we may assume $R$ is a local domain. If $K$ is perfect, and $H$ is commutative, or if $H \otimes K$ is separable, we have $S \otimes K \cong H \otimes K$ as $(H^* \otimes K)$-modules, by Theorem (4.2), resp. (3.1). Since $S$ is tame, $S$ is $H^*$-projective by Theorem (5.1), and so by Theorem (5.2), $S$ has a normal basis. That completes the proof.

(5.5) REMARK. If $R$ is the ring of integers of a number field $K$, there are many examples of extensions $L \supset K$ whose ring of integers $S$ is a tame $H$-object for some Hopf algebra $H$. For example, if $K = Q$, $L = Q(\sqrt{m})$, $G = \mathrm{Gal}(L/K)$, $R = \mathbf{Z}$, and $m \equiv 2$ or $3 \pmod 4$, then $S$ is a tame $RG$-object, but is Galois only when $m = -1$. A characterization of those Kummer extensions $L \supset K$ of prime degree with Galois group $G$ such that the order $A$ over $R$ in $KG$, $A = \{\alpha \in KG | \alpha S \subseteq S\}$ (cf. [**18** or **12**, p. 251]) is a Hopf algebra (of the kind studied in [**22**]) and $S$ is a tame $A^*$-object, is given in [**9**]. For those extensions, Theorem (5.4) guarantees a reasonable local description of $S$, with the aid of the characterizations of [**14**].

## REFERENCES


1. M. Auslander and D. Rim, *Ramification index and multiplicity*, Illinois J. Math. **7** (1963), 566–581.
2. A. D. Barnard, *Commutative rings with operators* (*Galois theory and ramification*), Proc. London Math. Soc. (3) **28** (1974), 274–290.
3. N. Bourbaki, *Algèbre commutative*, Chapitres I and II, Hermann, Paris, 1961.
4. J. Cassels and A. Frohlich (eds.), *Algebraic number theory*, Thompson, Washington, D. C., 1967.
5. S. Chase, *Infinitesimal group scheme actions on finite field extensions*, Amer. J. Math. **98** (1976), 441–480.
6. S. Chase, D. Harrison and A. Rosenberg, *Galois theory and Galois cohomology over a commutative ring*, Mem. Amer. Math. Soc. No. 52 (1965), 15–33.
7. S. Chase and M. Sweedler, *Hopf algebra and Galois theory*, Lecture Notes in Math., vol. 97, Springer-Verlag, Berlin and New York, 1969.
8. L. Childs, *Azumaya algebras over number rings as smash products* (preprint).
9. ——, *Taming wild extensions with Hopf algebras* (preprint).
10. E. Dade, *The equivalence of various generalizations of group rings and modules*, Math. Z. **181** (1982), 335–344.
11. F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings*, Lecture Notes in Math., vol. 181, Springer-Verlag, Berlin and New York, 1971.
12. A. Frohlich, *Galois module structure of algebraic integers*, Springer-Verlag, Berlin and New York, 1983.
13. S. Hurley, *Tame and Galois Hopf objects with normal bases*, Thesis, SUNY at Albany, 1984.
14. ——, *Galois objects with normal bases for free Hopf algebras or prime degree*, J. Algebra (to appear).
15. H. F. Kreimer and P. Cook, *Galois theories and normal bases*, J. Algebra **43** (1976), 115–121.
16. H. Kreimer and M. Takeuchi, *Hopf algebras and Galois extensions of an algebra*, Indiana Univ. Math. J. **30** (1981), 675–692.

17. H. F. Kreimer, *Quadratic Hopf algebras and Galois extensions*, Contemp. Math. **13** (1981), 353–361.
18. H. W. Leopoldt, *Uber die Hauptordnung der ganzen Elemente eines abelschen Zahlkorpers*, J. Reine Angew. Math. **201** (1959), 119–149.
19. I. Reiner, *Maximal orders*, Academic Press, London, 1975.
20. J.-P. Serre, *Representations linears des groupes fini*, Hermann, Paris, 1971.
21. M. Sweedler, *Hopf algebras*, Benjamin, New York, 1969.
22. J. Tate and F. Oort, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3** (1970), 1–21.
23. W. Waterhouse, *Introduction to affine group schemes*, Springer-Verlag, Berlin and New York, 1979.

DEPARTMENT OF MATHEMATICS, STATE UNIVERSITY OF NEW YORK AT ALBANY, ALBANY, NEW YORK 12222

DEPARTMENT OF MATHEMATICS, SIENA COLLEGE, LOUDONVILLE, NEW YORK 12211