TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 342, Number 2, April 1994

NOETHER'S THEOREM FOR HOPF ORDERS IN GROUP ALGEBRAS

DAVID M. WEINRAUB

ABSTRACT. Let K be a local field with valuation ring R of residue characteristic p containing a primitive pth root of unity ζ_p. We state an analog to Noether's Theorem for modules over R-Hopf algebras and use induction techniques to deduce a criterion for this analog to hold. We then construct a family of noncommutative Hopf algebras which satisfy the criterion.

1. INTRODUCTION

If L/K is a Galois extension of number fields with group G and rings of integers S/R, then in a natural way, L is a KG-module and S is an RG-module. The Normal Basis Theorem asserts that $L \cong KG$ as KG-modules. The analogous result does not generally hold for S and RG, even after localizing R. In 1931, E. Noether [N] showed that locally (for all primes p of R) $S \cong RG$ as left RG-modules if and only if the extension L/K is tame (that is, for every prime p of R, the ramification index of any prime P of S lying over p is relatively prime to the characteristic of the residue field R/p). In fact, the following are equivalent:

(1) $S \cong RG$, locally, as RG-modules.

(2) L/K is tame.

(3) The trace map $S \to R$ is surjective.

(4) S is a projective RG-module.

In 1986, L. Childs and S. Hurley [C/H] generalized the notions of tameness and local normal basis to H-modules, where H is an R-Hopf algebra. Their definitions specialized to those above when $H = RG$ and they obtained, in particular, the result that when H is commutative, $S \cong H$ locally as H-modules if and only if S is H-tame.

Waterhouse [W] notes that the Childs/Hurley notions of tameness do not imply the existence of local normal basis when H is noncommutative, even for group rings over fields. The counterexample is not entirely satisfactory in that any "natural" number theoretic example would have normal basis over the quotient field, in accordance with a result of Kreimer and Cook [K/C].

Note that the Childs/Hurley results assume commutativity of H, yet Noether's Theorem holds for arbitrary finite groups. Accordingly, there seems reason to believe that analogous results should hold for (at least some) noncommutative H (other than group algebras). We say that Noether's Theorem

Received by the editors June 30, 1991 and, in revised form, February 7, 1992.
1991 *Mathematics Subject Classification*. Primary 16A24, 19A22; Secondary 11S23.
Key words and phrases. Hopf algebras, induction.

holds for a Hopf algebra H (finitely generated and projective) over a discrete valuation ring R with quotient field K if the following are equivalent:

(1) S is a projective H-module and $K \otimes S \cong K \otimes H$ as $K \otimes H$-modules.

(2) $S \cong H$ as H-modules.

The only implication of interest here is $(1) \Rightarrow (2)$, the other being trivial. By the results of Childs and Hurley, if H is commutative, then H satisfies Noether's Theorem.

In this paper we give a general criterion for H to satisfy Noether's Theorem and construct a family of noncommutative Hopf algebras for which this criterion holds. The basic induction techniques used here were first employed by Swan [Swa1], and axiomatized by Lam in the form of Frobenius functors [B, Chapter 9].

This work is adapted from the author's doctoral dissertation at the State University of New York at Albany, completed under the guidance of L. Childs.

2. Conventions

All rings will have unit element 1. Unless explicitly stated otherwise, all module actions are on the left. In any case, we assume 1 acts trivially. All algebras are finitely generated and projective as modules over their base ring and all Hopf algebras are assumed to be cocommutative. Furthermore, unadorned tensoring is over R.

3. Hopf algebraic preliminaries

Let R be a commutative ring and let H be an R-Hopf algebra. Assume that H is finitely generated and projective as an R-module. Denote the structure maps of H by μ (multiplication), η (unit), Δ (comultiplication), ε (counit), and λ (antipode).

We use the Sweedler notation for comultiplication:

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

As an example, if G is a finite group, then the group algebra RG is a Hopf algebra with coalgebra structure given by $\Delta(g) = g \otimes g$, $\varepsilon(g) = 1$, and antipode map given by $\lambda(g) = g^{-1}$, for $g \in G$.

If A is an R-algebra and an H-module, then A is called an H-module algebra if the action satisfies the "measuring property" [see Swe], that is, if

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

for all $h \in H$ and $a, b \in A$. For example, if L/K is a Galois extension of fields with group G, then L is a KG-module algebra.

If A is an H-module algebra, then we may form the smash product $A \# H$. As an R-module, $A \# H = A \otimes H$, though we write a generator of $A \# H$ as $a \# h$. The algebra structure of the smash product is given by

$$(a \# h)(b \# g) = \sum_{(h)} a(h_{(1)} \cdot b) \# (h_{(2)} g).$$

It is easily verified that $A \# H$ is an R-algebra with unit element $1 \# 1$.

Assume now that K is a local field with uniformizing parameter π, ring of integers R, and residue field characteristic p. Also, suppose that R contains ζ, a primitive pth root of unity and that H is an R-Hopf algebra of rank p over R. Then by [T/O], H must be one of the Tate-Oort algebras $H = H_b \cong R[x]/\langle x^p - bx\rangle$, where $b = u\pi^{-(p-1)k}$, u is a unit in R, and $0 \leq k \leq e =$ ramification index of the extension $K/\mathbb{Q}_p(\zeta)$. (In the interests of brevity, we omit the description of the comultiplication on H_b. For such a description, see [T/O].) Furthermore, H_b is an R-order in $KC_p =$ the group algebra of C_p over K, where $C_p = \langle\sigma\rangle$ is the cyclic group of order p. That is, $K \otimes H_b \cong KC_p$ as K-Hopf algebras. In fact, denoting the image of x in H_b by ξ, we can identify the image of ξ in KC_p using the equation

$$\xi = -\pi^{-k} \sum_{m\in\mathbb{F}_p^*} \chi(m)\sigma^m$$

where $\chi\colon \mathbb{F}_p^* \to \mathbb{Z}/p\mathbb{Z} \subseteq R$ is the unique multiplicative section of the residue map $\mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$.

4. K-THEORETIC PRELIMINARIES

In this section, we state some basic results in the K-theory of Hopf algebras. Since most of the results here are simply Hopf algebraic generalizations of analogous group algebra statements, we only sketch the proofs, referring the interested reader to [Swa1] for the details.

Let A be a ring, not necessarily commutative. The Grothendieck group $\mathcal{G}(A)$ is an abelian group defined by generators and relations as follows: $\mathcal{G}(A)$ has one generator $[M]$ for each isomorphism class M of finitely generated A-modules. $\mathcal{G}(A)$ has one relation of the form $[M] = [M'] + [M'']$ for each exact sequence of finitely generated left A-modules

$$0 \to M' \to M \to M'' \to 0.$$

An easy induction argument shows that if

$$0 = X_0 \leq X_1 \leq X_2 \leq \cdots \leq X_n = X$$

is a composition series for an A-module X, then

$$[X] = \sum [X_i] \quad \text{in } \mathcal{G}(A).$$

Accordingly, if A is Artinian, then the Jordan-Hölder Theorem shows that $\mathcal{G}(A)$ is freely generated by the isomorphism classes of simple A-modules. In particular, if A is semisimple, then the rank of $\mathcal{G}(A)$ is simply the number of minimal idempotents in A, by Wedderburn's Theorem. We summarize with

(4.1) **Theorem.** *If A is semisimple, then $\mathcal{G}(A)$ is a free abelian group generated by the isomorphism classes of simple A-modules.*

The group $\mathcal{P}(A)$ is defined similarly, except that one uses finitely generated *projective* left A-modules. It is well known [Swa2, Lemma 4.1, for example] that for two projective A-modules P and Q, $[P] = [Q]$ in $\mathcal{P}(A)$ if and only if P and Q are stably isomorphic, that is, $P \oplus F \cong Q \oplus F$ for some free module F. If R is a complete discrete valuation ring and A is an R-algebra, finitely generated as an R-module, then the Krull-Schmidt Theorem holds for

A [R2, Exercise Chapter 6]. This means that every finitely generated A-module admits a *unique* decomposition into indecomposable direct summands. It then follows that $[P] = [Q]$ in $\mathscr{P}(A)$ if and only if $P \cong Q$. In this case, $\mathscr{P}(A)$ is a free abelian group generated by the isomorphism classes of indecomposable projective modules. In summary,

(4.2) **Theorem.** *If R is a complete discrete valuation ring and A is an R-algebra that is finitely generated as an R-module, then $\mathscr{P}(A)$ is freely generated by the isomorphism classes of indecomposable projective A-modules.*

We henceforth assume that R is at least a Dedekind domain and that H is an R-Hopf algebra, finitely generated and projective as an R-module. Under these hypotheses, we have

(4.3) **Proposition.** *$\mathscr{G}(H)$ is a ring.*

The multiplication is induced by the tensor product, $[M] \cdot [N] = [M \otimes N]$, where the H-module structure on $M \otimes N$ is induced by pulling back the $(H \otimes H)$-module structure via Δ. That is,

$$h \cdot (m \otimes n) = \sum_{(h)} (h_{(1)} \cdot m) \otimes (h_{(2)} \cdot n),$$

for $h \in H$, $m \in M$, and $n \in N$. Of course, the unit element for this multiplication is $[R]$ where R is the trivial H-module via the counit $\varepsilon \colon H \to R$.

The ring structure of $\mathscr{G}(H)$ is compatible with the additive structure of $\mathscr{P}(H)$ in that we have the following.

(4.4) **Proposition.** *$\mathscr{P}(H)$ is a module over $\mathscr{G}(H)$.*

The multiplication is induced by tensor product, as above. The proof basically entails showing that if M is any module and P is projective then $M \otimes P$ is projective. This, in turn, reduces to showing that for a free H-module F, the module $M \otimes F$ is free. For this, it suffices to show that $M \otimes H$ is free. But this essentially the statement of [Theorem 4.1.1 of Swe], which is stated for Hopf algebras over fields, but also holds over arbitrary commutative rings if the Hopf algebra H is finitely generated and projective.

The next theorem forms the basis for much of the work in the next section.

(4.5) **Theorem** (Swan's Triangle). *For any ideal I of R, there is a unique map $\psi_I \colon \mathscr{G}(K \otimes H) \to \mathscr{G}(H/IH)$ such that the following diagram commutes:*

$$\begin{array}{ccc} \mathscr{G}(H) & \xrightarrow{j_*} & G(K \otimes H) \\ {\scriptstyle \phi_{I^*}} \searrow & & \swarrow {\scriptstyle \psi_I} \\ & \mathscr{G}(H/IH) & \end{array}$$

For a proof, see [B, Chapter 10, Proposition 1.1]. Note: the map $j_* \colon \mathscr{G}(H) \to \mathscr{G}(K \otimes H)$ simply sends a generator $[M]$ to $[K \otimes M]$ and the map $\phi_{I^*} \colon \mathscr{G}(H) \to \mathscr{G}(H/IH)$ simply send a generator $[M]$ to $[M/IM]$.

By the uniqueness of ψ_I and the observation that $\phi_{I^*}(1) = 1$, we see that $\psi_I(1) = 1$.

If J is an R-Hopf subalgebra of J, we say that J is *admissible for* H if H is finitely generated and projective as both a left and right J-module. In this case, we obtain maps called, respectively, induction and restriction,

$$\begin{aligned}\mathrm{Ind}_J^H &= \mathrm{Ind} = i_*\colon \mathcal{G}(J) \to \mathcal{G}(H),\\ \mathrm{Ind}_J^H &= \mathrm{Ind} = i_*\colon \mathcal{P}(J) \to \mathcal{P}(H),\\ \mathrm{Res}_J^H &= \mathrm{Res} = i^*\colon \mathcal{G}(H) \to \mathcal{G}(J),\\ \mathrm{Res}_J^H &= \mathrm{Res} = i^*\colon \mathcal{P}(H) \to \mathcal{P}(J),\end{aligned}$$

by defining $\mathrm{Ind}([M]) = [H \otimes_J M]$ and $\mathrm{Res}([M]) = [M]$.

A well-known induction result in group representation theory is Frobenius Reciprocity (sometimes called the tensor identity). In fact, it holds for Hopf algebra representations, in general.

(4.6) **Theorem.** *If J is an admissible sub-Hopf algebra of H, M is a J-module, and N is an H-module, then*

$$(H \otimes_J M) \otimes N \cong H \otimes_J (M \otimes N),$$

as H-modules where

$(H \otimes_J M) \otimes N$ is an H-module via

$$h \cdot ((h' \otimes m) \otimes n) = \sum_{(h)} ((h_{(1)} h' \otimes m) \otimes (h_{(2)} \cdot n)),$$

$H \otimes_J (M \otimes N)$ is an H-module via

$$h \cdot (h' \otimes (m \otimes n)) = hh' \otimes (m \otimes n), \quad \text{and}$$

$M \otimes N$ is a J-module via

$$j \cdot (m \otimes n) = \sum_{(j)} (j_{(1)} \cdot m) \otimes (j_{(2)} \cdot n).$$

In the notation introduced above, we have

$$i_*(x)y = i_*(x i^*(y)) \quad \text{for all } x \in \mathcal{G}(J),\ y \in \mathcal{G}(H).$$

Proof. The following maps are verified to be inverse H-module isomorphisms:

$$\Phi\colon (H \otimes_J M) \otimes N \to H \otimes_J (M \otimes N),$$
$$\Phi((h \otimes m) \otimes n) = \sum_{(h)} h_{(1)} \otimes (m \otimes h^{\lambda}_{(2)} \cdot n)$$

and

$$\Psi\colon H \otimes_J (M \otimes N) \to (H \otimes_J M) \otimes N,$$
$$\Psi(h \otimes (m \otimes n)) = \sum_{(h)} (h_{(1)} \otimes m) \otimes h_{(2)} \cdot n. \quad \square$$

If $\mathcal{C}$ is a collection of admissible sub-Hopf algebras of H, then we obtain an induced map $\mathrm{Ind}\colon \bigoplus \mathcal{G}(J) \to \mathcal{G}(H)$ where the summation runs over all the sub-Hopf algebras J of H in the collection $\mathcal{C}$. Let $\mathcal{G}_{\mathcal{C}}(H)$ denote the image of this map. We say that $\mathcal{C}$ is *cofinite for H* if the quotient group $\mathcal{G}(H)/\mathcal{G}_{\mathcal{C}}(H)$ is finite. In this case, there exists an integer e such that $e\mathcal{G}(H) \subseteq \mathcal{G}_{\mathcal{C}}(H)$. We call such an e an (induction) exponent for the collection $\mathcal{C}$. We do not require that e be minimal. With this notation, Frobenius Reciprocity immediately yields an important corollary.

(4.7) **Corollary.** *$\mathscr{G}_{\mathscr{C}}(H)$ is an ideal in $\mathscr{G}(H)$.*

One consequence of Swan's Triangle and Frobenius Reciprocity is that in searching for cofinite collections for H over R, it suffices to find collections whose base extensions to K are cofinite for $K \otimes H$. Precisely, we have

(4.8) **Theorem.** *Let $\mathscr{C}$ be an admissible collection of sub-Hopf algebras for H and suppose that $K \otimes \mathscr{C} = \{K \otimes J : J \in \mathscr{C}\}$ is cofinite for $K \otimes \mathscr{C}$ with exponent e. Then*

(a) *For any ideal I of R, $\mathscr{C}/I = \{J/IJ : J \in \mathscr{C}\}$ is cofinite for H/IH with exponent e.*

(b) *$\mathscr{C}$ is cofinite for H with exponent e^2.*

Proof. The key observation is that $\mathscr{G}_{\mathscr{C}}$ is an ideal in $\mathscr{G}$. Hence it suffices to show that $e \in \mathscr{G}_{\mathscr{C}/I\mathscr{C}}(H/IH)$ and $e^2 \in \mathscr{G}_{K\otimes\mathscr{C}}(K \otimes H)$.

(a) Let $\phi_I : H \to H/IH$ be the canonical map and $\phi_{I^*} : \mathscr{G}(H) \to \mathscr{G}(H/IH)$ the induced map. The map ψ_I of Swan's Triangle (Theorem 4.5) commutes with induction, hence ψ_I maps $\mathscr{G}_{K\otimes\mathscr{C}}(K \otimes H)$ into $\mathscr{G}_{\mathscr{C}/I\mathscr{C}}(H/IH)$. Clearly, $j_*(1) = 1$. Therefore, $\psi_I(1) = \psi_I(j_*(1)) = \phi_{I^*}(1) = 1$. Hence, $e = \psi_I(e) \in \psi_I(\mathscr{G}_{K\otimes\mathscr{C}}(K \otimes H)) \subseteq \mathscr{G}_{\mathscr{C}/I\mathscr{C}}(H/IH)$. This proves (a).

(b) First note that extension j_* commutes with induction i_* from sub-Hopf algebras, hence j_* maps $\mathscr{G}_{\mathscr{C}}(H)$ into $\mathscr{G}_{K\otimes\mathscr{C}}(K \otimes H)$. Furthermore, this is surjective by the proof of the exactness of the sequence in [Swa2, Lemma 1.1]. Since $e \in \mathscr{G}_{K\otimes\mathscr{C}}(K \otimes H)$, there is an $x \in \mathscr{G}_{\mathscr{C}}(H)$ such that $j_*(x) = e = j_*(e)$. By the exact sequence mentioned above, $x - e = \sum \phi_p^*(x_p)$, where the sum extends over all prime ideals p of R and each $x_p \in \mathscr{G}(H/pH)$. If we let $\phi_p : H \to H/pH$ be the canonical map and $\phi_p^* : \mathscr{G}(H/pH) \to \mathscr{G}(H)$ the restriction map, we have

$$ex - e^2 = \sum e\phi_p^*(x_p) = \sum \phi_p^*(ex_p).$$

Now $ex_p \in \mathscr{G}_{\mathscr{C}/p}(H/pH)$ by part (a), so it follows that $\phi_p^*(ex_p) \in \mathscr{G}_{\mathscr{C}}(H)$ for each p. Thus, $ex - e^2 \in \mathscr{G}_{\mathscr{C}}(H)$. Since $\mathscr{G}_{\mathscr{C}}(H)$ is an ideal in $\mathscr{G}(H)$, $x \in \mathscr{G}_{\mathscr{C}}(H)$ implies that $ex \in \mathscr{G}_{\mathscr{C}}(H)$. Hence, $e^2 \in \mathscr{G}_{\mathscr{C}}(H)$. This proves (b). □

In order to exploit this result, we need some cofinite collections for $K \otimes H$. When $K \otimes H$ is a group algebra KG, this is realized with the following well-known theorem [S, Section 9.2, for example].

(4.9) **Theorem** (Artin induction). *Suppose G is a finite group and K is a field. Let $\mathscr{C}$ be the collection of all subgroup algebras KC, where C is a cyclic subgroup of G. Then $\mathscr{C}$ is cofinite for KG and the order of G serves as an induction exponent for $\mathscr{C}$.*

We finish this section with some general observations about induction in group algebras. Let KG be a group algebra and suppose that $\mathscr{C}$ and $\mathscr{D}$ are collections of subgroup algebras of KG. If every $C \in \mathscr{C}$ is contained in some $D \in \mathscr{D}$, we say that the $\mathscr{C}$ is a refinement of $\mathscr{D}$. If every $C \in \mathscr{C}$ has a conjugate contained in some $D \in \mathscr{D}$, we say that $\mathscr{C}$ is a conjugate refinement of $\mathscr{D}$. We then have two observations.

(4.10) **Proposition.** *If $\mathscr{C}$ is cofinite and a refinement of $\mathscr{D}$, then $\mathscr{D}$ is cofinite.*

Proof. This is simply transitivity of induction. Let e be an induction exponent for $\mathscr{C}$ and let $C \subseteq D$ with $C \in \mathscr{C}$ and $D \in \mathscr{D}$. Then for any KC-module M, we have

$$\mathrm{Ind}_{KC}^{KG}(M) \cong \mathrm{Ind}_{KD}^{KG}(\mathrm{Ind}_{KC}^{KD}(M)).$$

It follows that $\mathscr{G}_{\mathscr{C}}(KG) \subseteq \mathscr{G}_{\mathscr{D}}(KG)$. Therefore, $e\mathscr{G}(KG) \subseteq \mathscr{G}_{\mathscr{C}}(KG) \subseteq \mathscr{G}_{\mathscr{D}}(KG)$. Hence, $\mathscr{D}$ is cofinite. □

(4.11) **Lemma.** *If C and D are conjugate subgroups of G, then*

$$\mathrm{Ind}_{KC}^{KG}\colon \mathscr{G}(KC) \to \mathscr{G}(KG) \quad \text{and} \quad \mathrm{Ind}_{KD}^{KG}\colon \mathscr{G}(KD) \to \mathscr{G}(KG)$$

have the same image.

Proof. In fact, we show that every KG-module induced from a KC is isomorphic to a module induced from KD. Let $C = \tau D \tau^{-1}$, $\tau \in G$, and suppose that M is a KC-module. Define a KD-module structure on M by letting $\delta\colon m = (\tau\delta\tau^{-1}) \cdot m$ for $\delta \in D$ and $m \in M$. We define a map

$$\psi\colon KG \otimes_{KC} M \to KG \otimes_{KD} M,$$
$$\sigma \otimes m \mapsto \sigma\tau \otimes m.$$

This is clearly a KG-linear isomorphism, provided that it is well defined. We need to show that $\psi(\sigma\gamma \otimes m) = \psi(\sigma \otimes \gamma m)$ for all $\sigma \in G$, $\gamma \in C$, and $m \in M$. Computing,

$$\begin{aligned}\psi(\sigma\gamma \otimes m) &= \sigma\gamma\tau \otimes m = \sigma\tau\delta \otimes m, \quad \text{for some } \delta \in D\\ &= \sigma\tau \otimes \delta\colon m = \sigma\tau \otimes (\tau\delta\tau^{-1}) \cdot m\\ &= \sigma\tau \otimes \gamma m = \psi(\sigma \otimes \gamma m), \qquad \text{as required.} \quad \square\end{aligned}$$

(4.12) **Corollary.** *If $\mathscr{C}$ is cofinite and a conjugate refinement of $\mathscr{D}$, then $\mathscr{D}$ is cofinite.*

5. Noether's Theorem

In this section we determine a general criterion for Noether's Theorem to hold for a Hopf algebra. We then construct a family of nontrivial noncommutative Hopf algebras and use the criterion to show that Noether's Theorem holds for this family. In this context, nontrivial means not a group algebra.

Let R be a discrete valuation ring with quotient field K, and let H be an R-Hopf algebra, finitely generated and projective as an R-module. We say that Noether's Theorem holds for H if the following are equivalent:

(1) S is a projective H-module and $K \otimes S \cong K \otimes H$ as $K \otimes H$-modules.

(2) $S \cong H$ as H-modules.

The only implication of interest here is (1) $\Rightarrow$ (2), the other being trivial. By the results of Childs and Hurley [C/H, Theorem 5.2], if H is commutative, then H satisfies Noether's Theorem.

It is a technical simplification to assume that R is complete. This is no loss of generality because two H-modules are isomorphic if and only if their completions are isomorphic [R1, §1, (19)]. Thus, we may assume R complete and then the Krull-Schmidt Theorem holds for H-modules (cf. comment preceding Theorem 4.2).

(5.1) **Proposition.** *The following are equivalent (recall that $j: R \to K$ is the inclusion):*

(a) $j_*: \mathscr{P}(H) \to \mathscr{G}(K \otimes H)$ *is injective.*

(b) *If M, N are projective H-modules and $K \otimes M \cong K \otimes N$ as $K \otimes H$-modules, then $M \cong N$ as H-modules.*

Proof. (a) $\Rightarrow$ (b): Suppose that j_* is injective and M, N are projective H-modules with $K \otimes M \cong K \otimes N$ as $K \otimes H$-modules. Then $j_*([M]) = j_*([N])$. By injectivity, we have $[M] = [N]$. But now Theorem 4.2 implies $M \cong N$.

(b) $\Rightarrow$ (a): If $x = [M] - [N] \in \ker j_*$, then $[K \otimes M] = [K \otimes N]$. Since $K \otimes H$ is semisimple, we have $K \otimes M \cong K \otimes N$. By the assumption (b), we have that $M \cong N$ and therefore $x = [M] - [N] = 0$. Hence, j_* is injective. □

(5.2) **Corollary.** *If $j_*: \mathscr{P}(H) \to \mathscr{G}(K \otimes H)$ is injective, then Noether's Theorem holds for H.*

The map $j_*: \mathscr{P}(H) \to \mathscr{G}(K \otimes H)$ is injective, hence Noether's Theorem holds for H, if H is commutative. For a proof, see [Swa1, Lemma 6.2] or [C/H, Theorem 5.2]. We now show that if H is rich enough in the right kind of admissible sub-Hopf algebras, then Noether's Theorem holds for H.

(5.3) **Theorem.** *Noether's Theorem holds for H if and only if H has a cofinite collection $\mathscr{C}$ of admissible sub-Hopf algebras such that $j_*: \mathscr{P}(J) \to \mathscr{G}(K \otimes J)$ is injective for all $J \in \mathscr{C}$.*

Proof. The necessity is obvious for if Noether's Theorem holds for H then the collection $\mathscr{C} = \{H\}$ does the job. For the sufficiency, it suffices to show that $j_*: \mathscr{P}(H) \to \mathscr{G}(K \otimes H)$ is injective.

Let $x \in \mathscr{P}(H)$ and suppose that $j_*(x) = 0$. Let N be an exponent for the collection $\mathscr{C}$. Then we have

$$N = \sum i_{\nu*}(x_\nu) \quad \text{in } \mathscr{G}(H),$$

where $x_\nu \in \mathscr{G}(J_\nu)$, $J_\nu \in \mathscr{C}$, and $i_\nu: J_\nu \to H$ is the inclusion map and $i_{\nu*}: \mathscr{G}(J_\nu) \to \mathscr{G}(H)$ is the induction map. By admissibility of J_ν, we have $i_\nu^*(x) \in \mathscr{P}(J_\nu)$. (Recall that $i_\nu^*: \mathscr{G}(H) \to \mathscr{G}(J_\nu)$ is the homomorphism induced by restriction.) Since $\mathscr{P}(J_\nu)$ is a module over $\mathscr{G}(J_\nu)$, we have $x_\nu i_\nu^*(x) \in \mathscr{P}(J_\nu)$ and the following equalities in $\mathscr{G}(K \otimes J_\nu)$ for each ν:

$$\begin{aligned} j_*(x_\nu i_\nu^*(x)) &= j_*(x_\nu) j_*(i_\nu^*(x)) = j_*(x_\nu) i_\nu^*(j_*(x)) \\ &= j_*(x_\nu) i_\nu^*(0) = j_*(x_\nu) 0 = 0. \end{aligned}$$

By hypotheses $j_*: \mathscr{P}(J_\nu) \to \mathscr{G}(K \otimes J_\nu)$ is injective. Therefore, $x_\nu i_\nu^*(x) = 0$. Now we have the following in $\mathscr{P}(H)$:

$$\begin{aligned} Nx &= \sum i_{\nu*}(x_\nu) x \\ &= \sum i_{\nu*}(x_\nu i_\nu^*(x)), \quad \text{by Frobenius Reciprocity (4.6)} \\ &= \sum i_{\nu*}(0) = 0. \end{aligned}$$

So $Nx = 0$ in $\mathscr{P}(H)$. But $\mathscr{P}(H)$ is a free abelian group, by Theorem 4.2. Therefore, $x = 0$. This proves that $j_*: \mathscr{P}(H) \to \mathscr{G}(K \otimes H)$ is injective. □

We now construct our family of Hopf algebras for which Noether's Theorem holds. Let $C_p = \langle \sigma \rangle$ be a cyclic group of prime order p, let $C_n = \langle \tau \rangle$ be a cyclic group of order n and suppose that C_n acts faithfully on C_p via $= \tau \cdot \sigma = \sigma^\alpha$, where $\alpha \in \mathbb{F}_p^* = (\mathbb{Z}/p\mathbb{Z})^*$. Let $G = C_pC_n$ denote the semidirect product of C_p and C_n via this action. Let K be a local field with valuation ring R and maximal ideal πR containing p. Also assume that $\zeta = \zeta_p$ is a primitive pth root of unity in R.

Let $\chi\colon \mathbb{F}_p^* \to \mathbb{Z}/p\mathbb{Z} \subseteq R$ be the unique multiplicative section of the residue map $\mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{F}_p$.

Let H_b, $b = u\pi^{k(p-1)}$, be a Tate-Oort Hopf algebra order in KC_p with algebra generator

$$\xi = -\pi^{-k} \sum_{m \in \mathbb{F}_p^*} \chi(m)\sigma^m.$$

The action of C_n on C_p makes KC_p into a KC_n-module algebra and we may form the smash product

$$KC_p \# KC_n \cong K[C_pC_n] \cong K[G].$$

(5.4) **Proposition.** *Under the restricted action, H_b is an RC_n-module algebra.*

Proof. The measuring property follows from the measuring property over K. We merely need to show that H_b is invariant under the action of RC_n. By the measuring property, it suffices to check that the algebra generator ξ of H_b is mapped back into H_b by τ.

$$\begin{aligned} \tau \cdot \xi = \tau \cdot \left(-\pi^{-k} \sum_{x \in \mathbb{F}_p^*} \chi(x)\sigma^x \right) &= -\pi^{-k} \sum_{x \in \mathbb{F}_p^*} \chi(x)\tau \cdot (\sigma^x) \\ = -\pi^{-k} \sum_{x \in \mathbb{F}_p^*} \chi(x)\sigma^{\alpha x} &= -\pi^{-k} \sum_{y \in \mathbb{F}_p^*} \chi(\alpha^{-1}y)\sigma^y \\ = \chi(\alpha^{-1}) \left(-\pi^{-k} \sum_{y \in \mathbb{F}_p^*} \chi(y)\sigma^y \right) &= \chi(\alpha^{-1})\xi. \end{aligned}$$

That is, $\tau \cdot \xi = \chi(\alpha^{-1})\xi \in H_b$, as required. □

Since H_b is RC_n-invariant, we may form the smash product $H = H_b \# RC_n$. Observe that extending the base to K yields

$$\begin{aligned} K \otimes H = K \otimes (H_b \# RC_n) &\cong (K \otimes H_b) \otimes_K (K \otimes RC_n) \\ &\cong KC_p \otimes_K KC_n \cong K[C_pC_n] \cong K[G]. \end{aligned}$$

So H is a nontrivial noncommutative Hopf algebra order in the group algebra KG. Furthermore, H contains the two commutative admissible sub-Hopf algebras H_b and RC_n.

To show that $\{H_b, RC_n\}$ is cofinite for H, it suffices to show that $\{KC_p, KC_n\}$ is cofinite for KG, by Theorem 4.8. That is, we may show that the collection $\mathscr{C} = \{C_p, C_n\}$ is cofinite for the group $G = C_pC_n$ over the field K.

We record the following properties of G as a lemma, whose proof is straightforward.

(5.5) **Lemma.** *Let $G = C_pC_n$, with $\tau\sigma\tau^{-1} = \sigma^\alpha$, $\alpha \in \mathbb{F}_p^*$.*

(a) *Every element $x \in G$ may be expressed in the form $x = \sigma^s\tau^t$, with $s \in \mathbb{Z}/p\mathbb{Z}$, $t \in \mathbb{Z}/n\mathbb{Z}$.*

(b) $\tau^i\sigma^j = \sigma^{\alpha^i}\tau^j$.
(c) $(\sigma^u\tau^v)^{-1} = \sigma^{-u\alpha^{-1}}\tau^{-v}$.
(d) $(\sigma^u\tau^v)(\sigma^s\tau^t)(\sigma^u\tau^v)^{-1} = \sigma^{u+\alpha^v s-\alpha^v u}\tau^v$.

(5.6) **Proposition.** *Every cyclic subgroup C of G (except the normal subgroup C_p itself) is conjugate to a subgroup of $C_n = \langle\tau\rangle$.*

Proof. This is just a computation using the lemma. If $\sigma^s\tau^t$ is a generator for C, we seek u and v such that

$$(\sigma^u\tau^v)(\sigma^s\tau^t)(\sigma^u\tau^v)^{-1} = \tau^t \in \langle\tau\rangle = C_n.$$

But the left side reduces to $\sigma^{u+\alpha^v s-\alpha^t u}\tau^v = \tau^t$. It suffices to take $v = 0$. This leaves us with the task of solving the congruence

$$u + s - \alpha^t u \equiv 0 \pmod p$$

or

$$u(\alpha^t - 1) \equiv s \pmod p.$$

But since $\sigma^s\tau^t \notin C_p$, we have $\tau^t \neq 1$. This implies that τ^t acts nontrivially on σ, by the faithfulness of the action of C_n on C_p. But $\tau^t \cdot \sigma = \sigma^{\alpha^t}$ so $\alpha^t \not\equiv 1 \pmod p$. Therefore, $\alpha^t - 1$ is a unit $\bmod p$ and we may solve for $u = s/(\alpha^t - 1) \in \mathbb{Z}/p\mathbb{Z}$. This completes the proof. □

(5.7) **Proposition.** *$C_p = \langle\sigma\rangle$ is the only abelian subgroup of G whose order is divisible by p.*

Proof. Let A be any such subgroup. Since p divides the order of A, it must have an element of order p, by Sylow's Theorem. But the only elements of order p are in C_p and any one of these generates C_p so $C_p \leq A$. If $\sigma^s\tau^t \in A$, then $\tau^t \in A$. It follows τ^t commutes with every element of C_p. By the faithfulness of the action, we must have $\tau^t = 1$. Therefore, $A \leq C_p$. Hence, $A = C_p$.

We now state the main theorem of this section.

(5.8) **Theorem.** *Noether's Theorem holds for $H = H_b \# RC_n$.*

Proof. By Artin's Theorem, the collection of cyclic subgroups of G is cofinite for G. By Propositions 5.6 and 5.7, we see that the collection $\{C_p, C_n\}$ is a conjugate refinement for the collection of cyclic subgroups of G, hence is also cofinite for G, by Proposition 4.12. By Theorem 4.8, this implies that $\{H_b, RC_n\}$ is cofinite for H. Hence, Noether's Theorem holds for H, by Theorem 5.3. □

Application. If $f(x) \in K[x]$ is a solvable polynomial of prime degree p, then the Galois group of f (that is, the Galois group G of the extension L/K, where L is a splitting field for f) is a subgroup of the holomorph of C_p, $\mathrm{Hol}(C_p) = C_p \mathrm{Aut}(C_P) \cong C_pC_n$, $n = p - 1$. For simplicity, assume that $G = C_pC_n$ and let $H = H_b \# RC_n$ be a Hopf order in KG as before. Let S be the valuation ring of L and following [Ta], set $T = \{t \in S \colon Ht \subseteq S\}$. Then T is clearly an H-module and by the measuring property of the H-action, T is a subring of S. In fact, T is an H-module algebra order in L so we have

$$K \otimes T \cong L \cong KG \cong K \otimes H$$

as H-modules. the isomorphism $L \cong KG$ deriving from the classical normal basis theorem.

To apply Noether's Theorem to the extension T/R, it remains to show that T is H-projective. Let

$$U = T^{H_b} = \{t \in T\colon ht = \varepsilon(h)t \text{ for all } h \in H_b\},$$

the fixed ring of T under H_b. Since H_b is generated as an algebra by ξ and $\varepsilon(\xi) = 0$, it follows that $U = \{t \in T\colon \xi t = 0\}$.

(5.9) **Proposition.** *U is invariant under the action of RC_n on L.*

Proof. Let $u \in U$. We need to show that $\tau u \in U$, that is, we must show that $\xi(\tau u) = 0$. But

$$\begin{aligned}
\xi(\tau u) &= \left(-\pi^{-k} \sum_{x\in\mathbb{F}_p^*} \chi(x)\sigma^x\right) \cdot (\tau u) \\
&= \left(-\pi^{-k} \sum \chi(x)\sigma^x\tau\right) u \\
&= \left(-\pi^{-k} \sum \chi(\alpha y)\sigma^{\alpha y}\tau\right) u \\
&= \chi(\alpha)\left(-\pi^{-k} \sum \chi(y)\tau\sigma^y\right) u \\
&= \chi(\alpha)\tau\xi(u) = 0
\end{aligned}$$

since $u \in U$. That is, $\xi(\tau u) = 0$ so $\tau u \in U$, proving that U is RC_n-invariant.

Now we have an exact sequence of Hopf algebras

$$0 \to H_b \to H \to RC_n \to 0.$$

By [G], the extension T/R is H-tame (i.e., $I_H T = R$, where I_H is the set of integrals in H) if and only if T/U is $(U \otimes H_b)$-tame and U/R is RC_n-tame. The integrals of RC_n are generated by $\sum \tau^i$. Since $n = p - 1$ is a unit in R, the integral $\frac{1}{n}\sum \tau^i$ of RC_n maps $1 \in U$ to $1 \in R$. This shows that $I_{RC} U = R$, so U/R is RC_n-tame. Thus, T/R is H-tame if and only if T/U is $(U \otimes H_b)$-tame.

Let $E = K \otimes U = K \otimes (T^{H_b}) = (K \otimes T)^{K\otimes H_b} = L^{KC_p} = L^{C_p}$. Then L/E is a cyclic extension of degree p and since $\zeta_p \in E$, L/E is a Kummer extension.

Accordingly, let $L = E[z]$, $z^p = w \in U$, where the action of C_p on L is given by $\sigma(z) = \zeta z$. We also assume that $w = 1 + r\pi_1^{kp+1}$ is a unit in R, where π_1 is a uniformizer for U, r is a unit in U and our H_b is the Tate-Oort algebra with $b = u\pi^{-k(p-1)}$. With this assumption, T/U is $(U \otimes H_b)$-Galois [C, Theorem 14.3], hence $(U \otimes H_b)$-tame [C/H, Proposition 2.3]. It follows that T/R is H-tame and hence T is projective as an H-module [C/H, Theorem 5.1].

We may now apply Noether's Theorem to conclude that $T \cong H$ as H-modules. □

References

[B] H. Bass, *Algebraic K-theory*, Benjamin, 1968.

[C1] L. N. Childs, *Taming wild extensions with Hopf algebras*, Trans. Amer. Math. Soc. **304** (1987), 111–140.

[C2] L. N. Childs and S. Hurley, *Tameness and local normal basis for objects of finite Hopf algebras*, Trans. Amer. Math. Soc. **298** (1986), 763–778.

[G] C. Greither, *Hopf Galois structure on extensions of local number rings*, (preprint).

[K/C] H. F. Kreimer and P. M. Cook, *Galois theories and normal basis*, J. Algebra **43** (1976), 115–121.

[N] E. Noether, *Normalbasis bei Korpern ohne hohere Verzweigung*, Crelle, 1931.

[P] B. Pareigis, *When Hopf algebras are Frobenius algebras*, J. Algebra **18** (1971), 588–596.

[R1] I. Reiner, *Integral representations*, Lecture Notes in Math., vol. 744, Springer-Verlag, 1979.

[R2] ——, *Maximal orders*, Academic Press, 1975.

[S] J.-P. Serre, *Integral representations of finite groups*, Graduate Texts in Math., no. 42, Springer, 1977.

[Swa1] R. Swan, *Induced representations and projective modules*, Ann. of Math. (2) **71** (1960), 552–578.

[Swa2] ——, *The Grothendieck ring of a finite group*, Topology **2** (1963), 85–110.

[Swe] M. E. Sweedler, *Hopf algebras*, Benjamin, 1972.

[T/O] J. Tate and F. Ort, *Group schemes of prime order*, Ann. Sci. Ecole Norm. Sup. (4) **3** (1970).

[Ta] M. Taylor, *Hopf structure and the Kummer theory of formal groups*, J. Reine Angew. Math. **375/376** (1987), 1–11.

[W] W. Waterhouse, *Tame objects for finite commutative Hopf algebras*, Proc. Amer. Math. Soc. **103** (1988), 354–356.

Department of Mathematics and Computer Science, Russell Sage College, Troy, New York 12180