NORMAL BASES FOR HOPF-GALOIS ALGEBRAS

H. F. KREIMER

(Communicated by Martin Lorenz)

Abstract. Let $H$ be a Hopf algebra over a commutative ring $R$ such that $H$ is a finitely generated, projective module over $R$, let $A$ be a right $H$-comodule algebra, and let $B$ be the subalgebra of $H$-coinvariant elements of $A$. If $A$ is a Galois extension of $B$ and $B$ is a local subalgebra of the center of $A$, then $A$ is a cleft right $H$-comodule algebra or, equivalently, there is a normal basis for $A$ over $B$.

Let $R$ be a commutative ring, and let $H$ be a Hopf algebra over $R$, which is a finitely generated, projective module over $R$. When there is no notation to indicate otherwise, the bifunctors $\otimes$ and $\text{Hom}$ are applied to the category of $R$-modules. A right $H$-comodule algebra $A$ is an algebra over $R$ and a right $H$-comodule such that the comodule map $\alpha$ of $A$ into $A \otimes H$ is a homomorphism of algebras. Use the sigma notations $\sum_{(h)} h(1) \otimes h(2)$ for the coproduct of an element $h$ of $H$ and $\sum_{(a)} a(0) \otimes a(1)$ for the element $\alpha(a)$ of $A \otimes H$, $a$ in $A$. An element $a$ of $A$ is called $H$-coinvariant if $\sum_{(a)} a(0) \otimes a(1) = a \otimes 1$, and the set $B$ of $H$-coinvariant elements of $A$ is a subalgebra of $A$. If the extension of $\alpha$ to a left $A$-module homomorphism of $A \otimes A$ into $A \otimes H$ is surjective, then $A$ is called an $H$-Galois extension of $B$ [4, Def. 1.4], and an $H$-Galois extension $A$ of $B$ is said to have a normal basis if there is a left $B$-module, right $H$-comodule isomorphism of $B \otimes H$ onto $A$ [4, Def. 2.6]. Y. Doi and M. Takeuchi introduced the notion of a cleft right $H$-comodule algebra and proved that a right $H$-comodule algebra is cleft if, and only if, it is a Galois extension with normal basis [2, Thm. 9].

Now assume that $B$ is contained in the center of $A$. Then $B \otimes H$ is a Hopf algebra and $A$ is a right $B \otimes H$-comodule algebra over the ring $B$. Thus $R$ may be replaced by $B$ so that the subalgebra of $H$-coinvariant elements of $A$ is the ground ring $R$. If $A$ is a Galois extension of $R$, $A$ is called an $H$-Galois algebra. In this case, the extension of $\alpha$ is a left $A$-module isomorphism $\gamma$ of $A \otimes A$ onto $A \otimes H$ by [3, Thm. 1.7]. Henceforth, assume that $A$ is an $H$-Galois algebra. Then $A$ is cleft whenever there is a right $H$-comodule isomorphism of $H$ onto $A$. But a right $H$-comodule is a left module over the dual algebra $H^* = \text{Hom}(H, R)$, and because $H$ is a projective module over $R$, it can be shown that $A$ is cleft exactly when there is a left $H^*$-module isomorphism of $H$ onto $A$. Recently, D. Rumynin [5, §2.4] raised the question of whether $H$-Galois algebras over a local ring $R$ are cleft. In

Received by the editors April 11, 2001 and, in revised form, May 23, 2001.

2000 Mathematics Subject Classification. Primary 16W30.

Key words and phrases. Cleft Hopf algebra, normal basis.
a much earlier paper [3], P.M. Cook and H.F. Kreimer proved that for a local ring \( R \) and commutative or cocommutative Hopf algebra \( H \), every \( H \)-Galois algebra is cleft. The restriction that \( H \) be commutative or cocommutative was used to prove that \( H \) is a finitely generated, projective left \( H^* \)-module, but the restriction is not necessary.

**Proposition 1.** \( H \) is a finitely generated, projective left module over \( H^* \).

**Proof.** \( H \) is a left \( H^* \)-module with respect to the rule \( \varphi \cdot h = \sum_{(h)} \langle \varphi, h(2) \rangle h(1) \) for elements \( \varphi \) of \( H^* \) and \( h \) of \( H \). The antipode \( S \) of \( H \) is an antiautomorphism of the algebra \( H \) by [4] Prop. 1.1, and \( H \) becomes a right \( H \)-module by assigning \( S(g)h \) to the element \( h \otimes g \) of \( H \otimes H \). Because \( H \) is a finitely generated, projective module over \( R \), this right \( H \)-module structure is equivalent to a left \( H^* \)-comodule structure for \( H \). Indeed, let \( \varphi_i \in H^* \) and \( h_i \in H \), \( 1 \leq i \leq n \), be elements such that \( \sum_{i=1}^n \langle \varphi_i, h \rangle h_i = h \) for all elements \( h \) of \( H \). Then \( S(g)h = \sum_{i=1}^n \langle \varphi_i, S(g)h \rangle h_i = \sum_{i=1}^n \langle \varphi_i, (1), S(g) \rangle \langle \varphi_i, (2), h \rangle h_i \) and the left \( H^* \)-comodule structure on \( H \) is given by mapping an element \( h \) of \( H \) to \( \sum_{i=1}^n \langle \varphi_i, (1), h \rangle S^* \langle \varphi_i, (1) \rangle \otimes h_i \), where \( S^* \) denotes the adjoint of \( S \). To show that \( H \) is a left Hopf module over \( H^* \) it is necessary to verify that \( S(g)\varphi(h) \) equals

\[
\sum_{i=1}^n \sum_{(\varphi_i), (\varphi)} \langle \varphi_i, (1), h \rangle \langle \varphi(1), S^* \langle \varphi_i, (1) \rangle, g \rangle \varphi(2) \cdot h_i
\]

\[
= \sum_{i=1}^n \sum_{(\varphi_i), (\varphi)} \langle \varphi_i, (1), h \rangle \langle \varphi(1), g(1) \rangle \langle \varphi_i, (1), S(g(2)) \rangle \varphi(2) \cdot h_i
\]

\[
= \sum_{i=1}^n \sum_{(\varphi), (g)} \langle \varphi_i, S(g(2)) h \rangle \langle \varphi(1), g(1) \rangle \varphi(2) \cdot h_i
\]

\[
= \sum_{(\varphi), (g)} \langle \varphi(1), g(1) \rangle \varphi(2) \cdot (S(g(2)) h).
\]

But

\[
\sum_{(\varphi), (g)} \langle \varphi(1), g(1) \rangle \varphi(2) \cdot (S(g(2)) h)
\]

\[
= \sum_{(\varphi), (g), (h)} \langle \varphi(1), g(1) \rangle \langle \varphi(2), S(g(2)) h(2) \rangle S(g(3)) h(1)
\]

\[
= \sum_{(g), (h)} \langle \varphi, g(1) S(g(2)) h(2) \rangle S(g(3)) h(1)
\]

\[
= \sum_{(h)} \langle \varphi, h(2) \rangle S(g) h(1) = S(g) \langle \varphi, h \rangle.
\]

Letting \( I \) be the set of elements \( h \) of \( H \) such that \( S(g) h = \langle \varepsilon, g \rangle h = \langle \varepsilon, S(g) \rangle h \), \( I \) is the ideal of left integrals in \( H \), and by the theory of Hopf modules, \( I \) is a direct summand of \( H \) and the \( H^* \)-Hopf module \( H \) is isomorphic to \( H^* \otimes I \). In fact the projection of \( H \) onto \( I \) is given by mapping an element \( h \) of \( H \) to
\[ \sum_{i=1}^{n} \sum_{\varphi_i} (\varphi_i(2), h) S^* S^*(\varphi_i(1)) \cdot h_i \text{ and the } H^*-\text{Hopf module isomorphism of } H \text{ onto } \]
\[ H^* \otimes I \text{ is given by mapping } h \text{ to } \sum_{i=1}^{n} \sum_{\varphi_i} (\varphi_i(3), h) S^*(\varphi_i(2)) \otimes S^*(\varphi_i(1)) \cdot h_i. \]
Then
\[ I \text{ is a finitely generated, projective module over } R, \text{ since } I \text{ is a direct summand of } H, \text{ and } H \text{ is a finitely generated, projective left module over } H^*, \text{ since it is isomorphic to } H^* \otimes I. \]

Now the program in \[ \text{[3]} \text{ can be carried out and complete proofs of the following results can be found there.} \]

**Lemma 2.** If \( A \) and \( H \) are free modules over \( R \), then \( A \) and \( H \) have the same rank \( n \) and the direct sum of \( n \) copies of \( A \) is isomorphic as a left module over \( H^* \) to the direct sum of \( n \) copies of \( H \).

Note that an \( H \)-Galois algebra is a finitely generated and projective module over \( R \) \[ \text{[3], Thm. 1.7} \text{]. To prove the lemma, let } n \text{ be the rank of the free module } A \text{ and use the left } A \text{-module isomorphism } \gamma \text{ of } A \otimes A \text{ onto } A \otimes H, \text{ which is induced by the comodule map } \alpha \text{ of } A \text{ into } A \otimes H. \]

**Proposition 3.** If \( R \) is a field, then \( A \) and \( H \) are isomorphic left modules over \( H^* \).

The direct sum of \( n \) copies of \( A \) and the direct sum of \( n \) copies of \( H \) are finite dimensional vector spaces over a field \( R \), and so they satisfy the ascending and descending chain conditions for left \( H^* \)-submodules. Apply the Krull-Schmidt theorem to prove this proposition.

**Lemma 4.** Let \( J \) be an ideal in \( R \), let \( \bar{R} = R/J \), and assume that \( \bar{\omega} : \bar{R} \otimes H \longrightarrow \bar{R} \otimes A \) is a homomorphism of left modules over \( \bar{R} \otimes H^* \). There exists a left \( H^* \)-module homomorphism \( \omega : H \longrightarrow A \) such that \( \bar{\omega} = 1 \otimes \omega \). Moreover, if \( \bar{\omega} \) is an isomorphism and \( J \) is contained in the Jacobson radical of \( R \), then \( \omega \) is an isomorphism.

Since \( H \) is a projective left \( H^* \)-module, the map of \( H \) to \( \bar{R} \otimes A \), obtained by composing \( \bar{\omega} \) with the canonical map of \( H \) onto \( \bar{R} \otimes H \), can be lifted to a left \( H^* \)-module homomorphism \( \omega \) of \( H \) into \( A \). Assume that \( J \) is contained in the Jacobson radical of \( \bar{R} \) and \( \bar{\omega} \) is an isomorphism. Then \( \ker \omega \) is a finitely generated module over \( R \) and \( \bar{R} \otimes \ker \omega = \ker \bar{\omega} = 0 \). By Nakayama’s Lemma, \( \ker \omega = 0 \). Since \( A \) is a projective module over \( R \), the sequence of \( R \)-modules \( \ker \omega \longrightarrow H \longrightarrow \bar{R} \otimes A \) is split, \( \ker \omega \) is a finitely generated module over \( R \), and \( \bar{R} \otimes \ker \omega = \ker \bar{\omega} = 0 \). Again by Nakayama’s Lemma, \( \ker \omega = 0 \).

The fact that every \( H \)-Galois algebra over a local ring is cleft follows easily from Lemma 4 and Proposition 3. Or, one can follow the argument in \[ \text{[3]} \text{ to prove the following theorem.} \]

**Theorem 5.** If there is a basis of sets which are both open and closed for the Zariski topology on the set of maximal ideals of \( R \), then \( A \) and \( H \) are isomorphic left modules over \( H^* \).

The following corollary is the only claim in \[ \text{[3]} \text{ left to be verified.} \]

**Corollary 6.** Any \( H \)-Galois algebra is a finitely generated, projective left module over \( H^* \).
Proof. Let $A$ be an $H$-Galois algebra. First it will be shown that $A$ is a finitely presented left module over $H^*$. Since $A$ is a finitely generated module over $R$, it is a finitely generated left $H^*$-module. Let $K$ be the kernel of an epimorphism of a finitely generated free left $H^*$-module $F$ onto the left $H^*$-module $A$. Since $H^*$ is a finitely generated module over $R$, $F$ is a finitely generated module over $R$, and since $A$ is a projective module over $R$, the $R$-module $K$ is a direct summand of $F$. Therefore $K$ is a finitely generated $R$-module, consequently $K$ is a finitely generated left $H^*$-module, and $A$ is a finitely presented left $H^*$-module. Let $R_p$ denote the local ring at a prime ideal $p$ of $R$, and let $M_p = R_p \otimes M$ for any module $M$ over $R$. Then $\text{Hom}_{H^*}(A, X)_p$ is naturally isomorphic to $\text{Hom}_{H^*}(A, X_p) = \text{Hom}_{H^*_p}(A_p, X_p)$ for any left $H^*$-module $X$ by [1, Chapter I, §2, No. 9, Prop. 10]. $A$ is a finitely generated, projective left module over $H^*$ if, and only if, for every epimorphism of a left $H^*$-module $X$ onto a left $H^*$-module $Y$, the induced map of $\text{Hom}_{H^*}(A, X)$ into $\text{Hom}_{H^*}(A, Y)$ is surjective. But an $R$-module homomorphism of $\text{Hom}_{H^*}(A, X)$ into $\text{Hom}_{H^*}(A, Y)$ is surjective if, and only if, the corresponding map of $\text{Hom}_{H^*_p}(A_p, X_p)$ into $\text{Hom}_{H^*_p}(A_p, Y_p)$ is surjective for every maximal ideal $p$ of $R$ by [1, Chapter II, §3, No. 3, Thm. 1]. Thus it is only necessary to prove Corollary 6 when $R$ is a local ring. But then $A$ and $H$ are isomorphic left modules over $H^*$ by Theorem 5, and $H$ is a finitely generated, projective left module over $H^*$ by Proposition 1.

References


Department of Mathematics, Florida State University, Tallahassee, Florida 32306-4510
E-mail address: kreimer@math.fsu.edu