JOURNAL OF ALGEBRA **188,** 476–505 (1997)
ARTICLE NO. JA966827

Representations of Finite-Dimensional Hopf Algebras

Martin Lorenz*

Department of Mathematics, Temple University, Philadelphia, Pennsylvania 19122-6094

Communicated by Susan Montgomery

Received April 3, 1995

Let H denote a finite-dimensional Hopf algebra with antipode S over a field $\Bbbk$. We give a new proof of the fact, due to Oberst and Schneider [*Manuscripta Math*. **8** (1973), 217–241], that H is a symmetric algebra if and only if H is unimodular and S^2 is inner. If H is involutory and not semisimple, then the dimensions of all projective H-modules are shown to be divisible by char $\Bbbk$. In the case where $\Bbbk$ is a splitting field for H, we give a formula for the rank of the Cartan matrix of H, reduced mod char $\Bbbk$, in terms of an integral for H. Explicit computations of the Cartan matrix, the ring structure of $G_0(H)$, and the structure of the principal indecomposable modules are carried out for certain specific Hopf algebras, in particular for the restricted enveloping algebras of completely solvable p-Lie algebras and of $sl(2, \Bbbk)$. © 1997 Academic Press

INTRODUCTION

This article is a study of representations of finite-dimensional Hopf algebras H in the spirit of Larson's "Characters of Hopf Algebras" [L], but with the emphasis on the non-semisimple case. Thus particular attention is given to the properties of projective modules. To a large extent, we work inside the Grothendieck groups $G_0(H)$ and $K_0(H)$ of the categories of finitely generated H-modules and finitely generated projective H-modules, respectively, and the various connections between $G_0(H)$ and $K_0(H)$ are among our main focal points: The comultiplication of H causes $G_0(H)$ to be a ring and $K_0(H)$ to be a module over $G_0(H)$; there is a canonical duality between $K_0(H)$ and $G_0(H)$ which has a very natural interpretation in terms of Hattori–Stallings ranks (for $K_0(H)$) and ordinary characters (for $G_0(H)$); and, of course, there is the Cartan map $c : K_0(H) \to G_0(H)$.

*The author was supported in part by NSF Grant DMS-9400643. E-mail address: lorenz@math.temple.edu.

0021-8693/97 $25.00

Here are the main results of the article. Throughout, H denotes a finite-dimensional Hopf algebra over a field $\Bbbk$ of characteristic $p \geq 0$, and S is the antipode of H.

THEOREM 1. *If H is involutory* (that is, $S^2 = \mathrm{Id}$) *and not semisimple, then p divides the dimension of every projective H-module.*

The next result determines the rank of the map $\tilde{c} = \mathrm{Id}_{\Bbbk} \otimes c : \Bbbk \otimes_{\mathbb{Z}} K_0(H) \to \Bbbk \otimes_{\mathbb{Z}} G_0(H)$. This is a lower bound for the rank of c, and the two ranks are identical for $p = 0$. We let C denote the Cartan matrix, that is, the matrix of the Cartan map with respect to the canonical $\mathbb{Z}$-bases of $G_0(H)$ and $K_0(H)$ that are afforded by the irreducible H-modules and their projective covers, respectively.

THEOREM 2. *Suppose that k is a splitting field for H. Then*

$$\operatorname{rank} \tilde{c} = \dim_{\Bbbk} (H \triangleleft t).$$

Here t is any non-zero left integral of H and $\triangleleft$ denotes the right adjoint action of H on itself. Moreover, if S^2 is inner, then H is semisimple iff $C = \mathrm{Id}$ iff p does not divide $\det C$.

The article also contains explicit computations of the Cartan matrix C and of the ring structure of $G_0(H)$ for a number of specific Hopf algebras H that are of interest, in particular for the restricted enveloping algebras of completely solvable p-Lie algebras and of $sl(2, \Bbbk)$. These algebras display features that contrast sharply with the classical case of finite group algebras: C is always singular, and the ring $G_0(H)$ is not semiprime for the restricted enveloping algebra of $sl(2, \Bbbk)$.

A brief summary of the contents of the individual sections is as follows.

Section 1 reviews the basic pertinent material on Grothendieck groups in the more general setting of finite-dimensional associative algebras. This section is, to a large degree, a summary of parts of [Ba2], specialized to finite-dimensional algebras.

Section 2, on symmetry and dimensions, is independent of Grothendieck groups and is entirely based on a few simple observations about duality and traces. Theorem 1 is proved in Section 2.3 and, in Section 2.5, unimodularity of H is shown to be equivalent with self-duality of the projective cover of the "trivial" H-module. As a consequence, one obtains that H is a symmetric algebra if and only if H is unimodular and S^2 is inner.

Section 3 takes up the material of Section 1 in the context of Hopf algebras and contains the proof of Theorem 2 (in Sect. 3.4). The main emphasis is on the ring and module structures that are now carried by the various objects of Section 1. This section also contains an analysis of the special case where the Jacobson radical of H is a Hopf ideal.

Section 4 is devoted to a detailed discussion of some explicit examples: the Sweedler algebra H_4, a class of algebras that were constructed by Radford [R3] (based on earlier examples due to Taft [T]), and the restricted enveloping algebras of completely solvable p-Lie algebras and of $sl(2, \Bbbk)$. In each case, the ring $G_0(H)$, its module $K_0(H)$, the principal indecomposable modules, and the Cartan matrix are determined.

The author would like to thank Susan Montgomery for her thorough reading of the first version of this article which lead to a number of improvements, clarifications, and proper accreditations. In particular, she pointed out to us that the aforementioned characterization of symmetry was first observed by Oberst and Schneider [OS]. The present proof is a simplification of our original argument which incorporates a suggestion of hers and H.-J. Schneider. After the first version of the article was circulated, the author learned from Jim Humphreys that many of the features of the $sl(2, \Bbbk)$-example exhibited in Section 4.4 have previously been discovered by Pollack [Po] and have been rederived by Humphreys in [H]. There is also previous work of Humphreys on symmetry [H2]. Related material on representations of finite-dimensional cocommutative Hopf algebras, phrased in the language of (finite) algebraic groups, can be found in [V].

Notations and Conventions. All algebras, Hopf and otherwise, considered in this article are finite dimensional over a commutative base field $\Bbbk$ of characteristic $p \geq 0$, and all modules are left modules and are assumed to be finite dimensional over $\Bbbk$. Finally, $\otimes$ stands for $\otimes_{\Bbbk}$ and $(\cdot)^* = \mathrm{Hom}_{\Bbbk}(\cdot, \Bbbk)$ denotes the linear dual. Further assumptions will be explicitly stated at the beginning of each section.

1. BACKGROUND FROM THE THEORY OF FINITE-DIMENSIONAL ALGEBRAS

Throughout this section, A will denote a (finite-dimensional) algebra over $\Bbbk$ and $J = \operatorname{rad} A$ is the Jacobson radical of A. We fix a full set of non-isomorphic irreducible A-modules $V_1, \ldots, V_t$ and we let $P_i = P(V_i)$ denote their projective covers, the principal indecomposable A-modules (cf. [CR, p. 131]).

1.1. *Grothendieck groups*

Let $G_0(A)$ denote the Grothendieck group of the category of (finite-dimensional left) A-modules. This is the abelian group that is generated by the isomorphism classes $[V]$ of A-modules V modulo the relations $[V] = [U] + [W]$ for each short exact sequence of A-modules $0 \to U \to V \to W$

$\to 0$. It is a classical fact (cf. [Ba1, p. 404]) that $G_0(A)$ is a free abelian group with basis given by the classes $[V_i]$ $(i = 1, \ldots, t)$.

Similarly, $K_0(A)$ denotes the Grothendieck group of the category of *projective* (finite-dimensional left) A-modules, that is, the abelian group that is generated by the isomorphism classes $[P]$ of projective A-modules P modulo the relations $[P \oplus Q] = [P] + [Q]$. Again, $K_0(A)$ is free abelian, with basis $\{[P_i] | i = 1, \ldots, t\}$.

The two Grothendieck groups are related via the *Cartan map*

$$c = c_A : K_0(A) \to G_0(A), \qquad [P] \mapsto [P].$$

The matrix $C \in M_t(\mathbb{Z})$ which represents c with respect to the above bases is called the *Cartan matrix*:

$$C = (c_{i,j})_{t \times t} \qquad \text{with } c_{i,j} = \text{multiplicity of } V_j \text{ as composition factor of } P_i.$$

1.2. *Orthogonality*

Putting

$$\langle \cdot , \cdot \rangle : K_0(A) \times G_0(A) \to \mathbb{Z}, \qquad \langle P, V \rangle = \dim_{\Bbbk} \operatorname{Hom}_A(P, V),$$

one obtains a well-defined bilinear map (cf. [Ba2, Sect. 4.3]; for simplicity, the parentheses $[\cdot]$ are omitted). Since $P_i/JP_i \cong V_i$, we have $\operatorname{Hom}_A(P_i, V_j) \cong \operatorname{Hom}_A(V_i, V_j)$ which yields the *orthogonality relations*

$$\langle P_i, V_j \rangle = \begin{cases} 0 & \text{if } i \neq j, \\ d_i & \text{if } i = j, \end{cases} \quad \text{where } d_i = \dim_{\Bbbk} \operatorname{End}_A(V_i).$$

If $\Bbbk$ is a splitting field for A then all $d_i = 1$. Defining

$$\{\cdot, \cdot\} : K_0(A) \times K_0(A) \to \mathbb{Z}, \qquad \{a, b\} = \langle a, c(b) \rangle$$

one obtains a bilinear form on $K_0(A)$ whose matrix with respect to the given basis of $K_0(A)$ is

$$C' = (c'_{i,j})_{t \times t}, \qquad \text{where } c'_{i,j} = d_i c_{j,i}.$$

Indeed, $c([P_j]) = \sum_l c_{j,l}[V_l]$ implies $\{P_i, P_j\} = \sum_l c_{j,l} \langle P_i, V_l \rangle = c'_{i,j}$, by the orthogonality relations.

1.3. *Trace Spaces*

Following [Ba2], we write

$$T = T_A : A \to T(A) = A/[A, A]$$

for the natural projection to the quotient of A by the $\Bbbk$-linear span $[A, A]$ of the Lie commutators $[a, b] = ab - ba$ in A. We let

$$[\cdot]: A \to T(A)_{\text{reg}} = A/([A, A] + J) \cong T(A/J)$$

denote the canonical map. The space of *$\Bbbk$-valued trace functions* on A is the $\Bbbk$-subspace of $A^* = \operatorname{Hom}_{\Bbbk}(A, \Bbbk)$ that is defined by

$$C(A) = \{f \in A^* : f(ab) = f(ba) \text{ for all } a, b \in A\} \cong T(A)^*.$$

We define the space of *regular $\Bbbk$-valued trace functions* by

$$C(A)_{\text{reg}} = \{f \in C(A) : f \text{ vanishes on } J\} \cong C(A/J) \cong T(A)^*_{\text{reg}}.$$

If $\Bbbk$ is a splitting field for A and $p = \operatorname{char} \Bbbk > 0$, then $[A, A] + J = \{a \in A : a^{p^n} \in [A, A]$ for some $n \geq 0\}$ (e.g., [P, p. 56]), and hence

$$C(A)_{\text{reg}} = \left\{f \in A^* : f(a) = 0 \text{ for all } a \in A \text{ with } a^{p^n} \in [A, A] \text{ for some } n \geq 0\right\}.$$

1.4. *Hattori–Stallings Ranks*

Let P be a projective A-module. The *trace map* is defined by

$$\operatorname{tr}_P = \operatorname{tr}_{P/A} : \operatorname{End}_A(P) \xrightarrow{\cong} \operatorname{Hom}_A(P, A) \otimes_A P \xrightarrow{\tau_P} T(A),$$

$$\tau_P(f \otimes v) = T(f(v))$$

(cf. [Ba2]). If $\{(f_i, v_i)\}_1^n \subseteq \operatorname{Hom}_A(P, A) \times P$ is a dual basis for P, that is, $v = \sum_i f_i(v) v_i$ holds for all $v \in P$, then

$$\operatorname{tr}_P(\phi) = \sum_i f_i(\phi(v_i)) + [A, A] \qquad (\phi \in \operatorname{End}_A(P)).$$

The *Hattori–Stallings rank map* is defined by (cf. [Ba2, Sect. 2.4])

$$r : K_0(A) \to T(A), \qquad [P] \mapsto r_P = \operatorname{tr}_P(\operatorname{Id}_P).$$

Explicitly, writing $P = A^n \cdot e$ for some idempotent matrix $e = (e_{i,j}) \in M_n(A)$, we have $r_P = \sum T(e_{i,i})$. In particular, if P is free of rank n over A then $r_P = T(n)$. Since each P_i has the form $P_i = Ae_i$ for some primitive idempotent $e_i \in A$, the image of the Hattori–Stallings rank map is exactly the additive subgroup of $A/[A, A]$ that is generated by the (primitive) idempotents of A. Finally, we define

$$\rho : K_0(A) \xrightarrow{r} T(A) \twoheadrightarrow T(A)_{\text{reg}},$$

where the last map is the canonical epimorphism $A/[A, A] \twoheadrightarrow A/([A, A]$

$+ J$), and we put

$$\rho_i = \rho([P_i]) = [e_i] \in T(A)_{\mathrm{reg}} \qquad (i = 1, \ldots, t).$$

1.5. *Characters*

Let V be an A-module and denote its structure map $A \to \mathrm{End}_{\Bbbk}(V)$ by $a \mapsto a_V$ ($a \in A$). Then the *character* χ_V of V is defined by

$$\chi_V(a) = \mathrm{tr}_{V/\Bbbk}(a_V) \in \Bbbk \qquad (a \in A).$$

The characters $\chi_i = \chi_{V_i}$ are called the *irreducible characters* of A. Each character χ_V is an element of $C(A)$ and if $0 \to U \to V \to W \to 0$ is a short exact sequence of A-modules then $\chi_V = \chi_U + \chi_W$. In particular, since the irreducible characters clearly belong to $C(A)_{\mathrm{reg}}$, so do all characters χ_V, and the *character map*

$$\chi : G_0(A) \to C(A)_{\mathrm{reg}}, \qquad [V] \mapsto \chi_V$$

is a well-defined group homomorphism which satisfies $\chi_V(1) = \dim_{\Bbbk}(V)$.

1.6. THEOREM. (a) *The following diagrams commute*:

$$\begin{array}{ccc} K_0(A) \times G_0(A) & \xrightarrow{\langle \cdot, \cdot \rangle} & \mathbb{Z} \\ {\scriptstyle \rho \times \chi} \downarrow & & \downarrow {\scriptstyle \text{can.}} \\ T(A)_{\mathrm{reg}} \times C(A)_{\mathrm{reg}} & \xrightarrow[\text{evaluation}]{} & \Bbbk \end{array} \quad \text{and} \quad \begin{array}{ccc} K_0(A) & \xrightarrow{c_A} & G_0(A) \\ {\scriptstyle \rho} \downarrow & & \downarrow {\scriptstyle \chi} \\ T(A)_{\mathrm{reg}} & \xrightarrow[(\cdot)^t]{} & C(A)_{\mathrm{reg}}. \end{array}$$

Here, the map ρ is as in Section 1.4 *and* $(\cdot)^t : T(A)_{\mathrm{reg}} \to C(A)_{\mathrm{reg}} = T(A)^*_{\mathrm{reg}}$ *is defined by*

$$([a])^t([b]) = \mathrm{tr}_{A/\Bbbk}(L_b \circ R_a) \qquad (a, b \in A),$$

where $L_b, R_a \in \mathrm{End}_{\Bbbk}(A)$ are left multiplication with b and right multiplication with a, respectively.

(b) *The non-zero irreducible characters $\chi_i \in C(A)_{\mathrm{reg}}$ are linearly independent over $\Bbbk$. If $\Bbbk$ is a splitting field for A then the χ_i $(i = 1, \ldots, t)$ form a $\Bbbk$-basis of $C(A)_{\mathrm{reg}}$ and χ induces an isomorphism of $\Bbbk$-vector spaces*

$$\tilde{\chi} = \mathrm{Id}_{\Bbbk} \otimes \chi : \widetilde{G_0(A)} = \Bbbk \otimes_{\mathbb{Z}} G_0(A) \xrightarrow{\cong} C(A)_{\mathrm{reg}}.$$

(c) *If $\Bbbk$ is a splitting field for A then the ρ_i $(i = 1, \ldots, t)$ form a $\Bbbk$-basis of $T(A)_{\mathrm{reg}}$ and ρ induces an isomorphism of $\Bbbk$-vector spaces*

$$\tilde{\rho} = \mathrm{Id}_{\Bbbk} \otimes \rho : \widetilde{K_0(A)} = \Bbbk \otimes_{\mathbb{Z}} K_0(A) \xrightarrow{\cong} T(A)_{\mathrm{reg}}.$$

Proof. The diagrams in (a) are minor modifications of [Ba2, 4.3 and 4.7, respectively]. To see that $(\cdot)^t$ is a well-defined map, note that $\mathrm{tr}_{A/\Bbbk}(L_b \circ R_a) = 0$ if $a \in J$ or $a \in [A, A]$, because $L_b \circ R_a = R_a \circ L_b$ is a nilpotent endomorphism in the former case and a commutator of endomorphisms in the latter. Similarly for b in place of a.

(b) Assume first that $\Bbbk$ is a splitting field for A. Then all $d_i = 1$ in the orthogonality relations in Section 1.2, and the first diagram in (a) yields $\chi_i(\rho_j) = \delta_{i,j}1_{\Bbbk}$. Thus, if $\sum k_i \chi_i = 0$ for $k_i \in \Bbbk$ then $0 = \sum k_i \chi_i(\rho_j) = k_j$ for all j, thereby proving linear independence of the χ_i's. Furthermore, the number, t, of non-isomorphic irreducible A-modules, equals the number of matrix components of A/J which in turn is equal to the dimension of $T(A/J) \cong C(A)^*_{\mathrm{reg}}$. Hence $t = \dim_{\Bbbk} C(A)_{\mathrm{reg}}$, and so the χ_i span $C(A)_{\mathrm{reg}}$.

For independence of the non-zero irreducible characters χ_i in the general case, choose a field extension $\mathbb{K}/\Bbbk$ so that $\mathbb{K}$ is a splitting field for $\tilde{A} = \mathbb{K} \otimes A$ and let $\tilde{\chi}_i \in C(\tilde{A}) = \mathbb{K} \otimes C(A)$ denote the character of the $\tilde{A}$-module $\tilde{V}_i = \mathbb{K} \otimes V_i$. So $\tilde{\chi}_i = 1 \otimes \chi_i$. For $i \neq j$, the $\tilde{A}$-modules $\tilde{V}_i$ and $\tilde{V}_j$ have no common composition factor [CR, p. 170, Exercise 7.9]. Therefore, writing each $\tilde{\chi}_i$ in terms of irreducible characters of $\tilde{A}$, there is no overlap between the various i's. In view of the foregoing, this implies that the non-zero $\tilde{\chi}_i$'s are independent over $\Bbbk$, and hence the non-zero χ_i's are independent over $\mathbb{K}$.

(c) The proof of (c) is dual to the first part of the proof of (b). ∎

1.7. *Symmetric Algebras*

The $\Bbbk$-algebra A is called *symmetric* if there exists a non-degenerate $\Bbbk$-bilinear form

$$\beta : A \times A \to \Bbbk$$

which is associative and symmetric, that is, $\beta(ab, c) = \beta(a, bc)$ and $\beta(a, b) = \beta(b, a)$ holds for all $a, b, c \in A$. We recall some well-known facts about symmetric algebras:

(1) Group algebras of finite groups and all finite-dimensional semisimple algebras are symmetric.

(2) If A is symmetric then, for any irreducible A-module V, the socle of $P(V)$ is isomorphic to V. In particular, it follows that $P(V^*) \cong P(V)^*$ as (right) A-modules. (In case A is a Hopf algebra, the switch from left to right modules is unnecessary, because the side of the action is preserved for duals by means of the antipode. See Section 2.1 below.)

(3) If A is symmetric then the matrix $C' = (c'_{i,j})$ of Section 1.2 is symmetric and, consequently, the form $\{\cdot, \cdot\}$ is symmetric.

Facts (1) and (2) can be found in [CR, pp. 198 ff.] and (3) is [La, Theorem 9.8] (at least for $\Bbbk$ large enough; the general case follows along the same lines). Part (b) of the following lemma, apparently a well-known fact, has been pointed out to us by S. Montgomery and H.-J. Schneider who also provided the proof given below. It is included here for lack of a suitable reference.

LEMMA. *Let A be a symmetric algebra with form β. Then*:

(a) $\beta([a,b],c) = \beta(a,[b,c])$ *holds for all $a, b, c \in A$. In particular, $C(A) \cong Z(A)$, the center of A, and $C(A)_{\mathrm{reg}} \cong \mathrm{ann}_{Z(A)}(J)$ as $\Bbbk$-vector spaces.*

(b) *If $\gamma : A \times A \to \Bbbk$ is any non-degenerate bilinear form which is associative then there exists a unit $u \in A$ such that $\gamma(a,b) = \gamma(u^{-1}bu, a)$ holds for all $a, b \in A$.*

Proof. (a) First, $\beta(ba, c) = \beta(c, ba) = \beta(cb, a) = \beta(a, cb)$ and so $\beta([a, b], c) = \beta(ab, c) - \beta(ba, c) = \beta(a, bc) - \beta(a, cb) = \beta(a, [b, c])$. Thus, $a \in Z(A)$ if and only if $\beta(a, \cdot\,)$ vanishes on $[A, A]$, whence the first isomorphism follows. For the second isomorphism, observe that $\beta(a, J) = 0$ is equivalent with $\beta(aJ, A) = 0$, and hence with $aJ = 0$.

(b) Viewing A^* as left A-module via $(af)(b) = f(ba)$ for $f \in A^*$ and $a, b \in A$, the form γ determines a left A-isomorphism $G : A \to A^*$, $G(a) = \gamma(\cdot, a)$. Letting $B : A \to A^*$ denote the analogous isomorphism corresponding to β, we obtain a left A-isomorphism $\phi = B^{-1} \circ G : A \to A$. Thus $\phi(a) = au$, where $u = \phi(1)$ is a unit of A, and so $G(1) = B(u)$. Now, for $a, b \in A$,

$$\gamma(a,b) = \gamma(ab,1) = G(1)(ab) = B(u)(ab) = \beta(ab,u)$$

and, consequently, $\gamma(u^{-1}bu, a) = \beta(u^{-1}bua, u)$. Finally, using associativity and symmetry of β, one computes $\beta(u^{-1}bua, u) = \beta(u, u^{-1}bua) = \beta(bu, a) = \beta(a, bu) = \beta(ab, u)$ which entails the claimed identity $\gamma(a,b) = \gamma(u^{-1}bu, a)$. ∎

2. DIMENSIONS AND SYMMETRY

Throughout this section, H denotes a finite-dimensional Hopf algebra over $\Bbbk$, with counit ε, antipode S, and comultiplication Δ. The latter will be written $\Delta(h) = \sum h_1 \otimes h_2$ for $h \in H$. Recall that all H-modules are left modules and are assumed to be finite dimensional over $\Bbbk$.

2.1. *Homomorphisms*

Let V and W be H-modules. Then $\operatorname{Hom}_{\Bbbk}(V,W)$ can be made into an H-module by defining

$$(hf)(v) = \sum h_1 f(S(h_2)v) \qquad \big(h \in H,\ v \in V,\ f \in \operatorname{Hom}_{\Bbbk}(V,W)\big).$$

In the special case where $W = \Bbbk = \Bbbk_\varepsilon$ is the trivial H-module, so H acts on $\Bbbk$ via the counit ε, this simplifies to the following formula describing the H-action on $V^* = \operatorname{Hom}_{\Bbbk}(V,\Bbbk)$:

$$(hf)(v) = f(S(h)v) \qquad (h \in H, v \in V, f \in V^*).$$

Viewing tensor products of H-modules as H-modules by means of the diagonal map Δ, the canonical isomorphisms (cf. [Bou, p. II.77 and II.80])

$$W \otimes V^* \xrightarrow{\cong} \operatorname{Hom}_{\Bbbk}(V,W), \qquad w \otimes f \mapsto (v \mapsto f(v)w)$$
$$V^* \otimes W^* \xrightarrow{\cong} (W \otimes V)^*, \qquad f \otimes g \mapsto (w \otimes v \mapsto g(w)f(v))$$

are in fact H-module isomorphisms. Finally, the space of H-invariants $\operatorname{Hom}_{\Bbbk}(V,W)^H = \{f \in \operatorname{Hom}_{\Bbbk}(V,W) : hf = \varepsilon(h)f \text{ for all } h \in H\}$ coincides with the space of H-module maps $\operatorname{Hom}_H(V,W)$ ([L, Proposition 2.3] or [Zhu, Lemma 1]).

2.2. *Duality*

Let V be an H-module. Viewing V^{**} as H-module as in Section 2.1, the canonical isomorphism $\psi : V \to V^{**}$, $\psi(v)(f) = f(v)$ satisfies $\psi(hv) = S^{-2}(h)\psi(v)$. Therefore, as H-modules,

$$V^{**} \cong V^{(S^{-2})},$$

the S^{-2} twist of V. Since twists by inner automorphisms do not affect the isomorphism type, we see in particular:

If S^2 is inner then $V^{**} \cong V$ holds for all H-modules V.

Using $(\cdot)^*$ to denote transpose maps, we have an isomorphism of $\Bbbk$-vector spaces

$$(\cdot)^* : \operatorname{Hom}_H(V,W) \xrightarrow{\cong} \operatorname{Hom}_H(W^*,V^*).$$

Thus $(\cdot)^*$ becomes an exact contravariant automorphism of the category of finite-dimensional H-modules. Clearly, $(\cdot)^*$ respects direct sums, and some power of $(\cdot)^*$ is equivalent to the identity, because S has finite order [R3]. In particular, V^* is irreducible (resp., indecomposable) if and only if V is.

The H-module V is called *self-dual* if $V^* \cong V$. The trivial H-module $\Bbbk = \Bbbk_\varepsilon$ and the regular left H-module H are self-dual, the former as a consequence of the identity $\varepsilon \circ S = \varepsilon$, the latter by [Sw, Theorem 5.1.3]. Consequently, projectivity also transfers between V and V^*.

2.3. THEOREM. *Assume that H is involutory* (*that is*, $S^2 = \mathrm{Id}$).

(a) [*L, Theorem* 2.8] *If H is semisimple then p does not divide the dimensions of any absolutely irreducible H-module*.

(b) *If H is not semisimple, then p divides the dimension of every projective H-module*.

Recall that an H-module V is *absolutely irreducible* if for every field extension $\mathbb{K}/\Bbbk$, $\mathbb{K} \otimes V$ is an irreducible $\mathbb{K} \otimes H$-module or, equivalently, if $\mathrm{End}_\Bbbk(V) = \Bbbk$ (cf. [CR, Theorem 3.43]).

Proof. Both parts follow from the observation that, for any H-module V, the trace map $\mathrm{tr}_{V/\Bbbk} : \mathrm{End}_\Bbbk(V) \to \Bbbk = \Bbbk_\varepsilon$ of Section 1.4 is an H-module map. Indeed, identifying $\mathrm{End}_\Bbbk(V)$ with $V \otimes V^*$ as in Section 2.1, it suffices to check H-linearity of the map $\tau : V \otimes V^* \to \Bbbk$, $v \otimes f \mapsto f(v)$. Using the identity $\sum S(h_2)h_1 = \varepsilon(h)1_H$ for $h \in H$ (from $S^2 = \mathrm{Id}$) we compute

$$\begin{aligned}\tau(h \cdot v \otimes f) &= \tau\Big(\sum h_1 v \otimes h_2 f\Big) = \sum (h_2 f)(h_1 v) \\ &= \sum f(S(h_2)h_1 v) = \varepsilon(h) f(v) = h \cdot \tau(v \otimes f),\end{aligned}$$

as required.

(a) Since H is semisimple, there is a left integral t in H with $\varepsilon(t) \neq 0$ in $\Bbbk$. Note that $t \cdot \mathrm{End}_\Bbbk(V)$ consists of H-invariants and hence is contained in $\mathrm{End}_H(V)$, by Section 2.1. Thus, if $f \in \mathrm{End}_\Bbbk(V)$ and V is absolutely irreducible, then $tf = c_f \mathrm{Id}_V$ for some $c_f \in \Bbbk$, and hence

$$c_f \dim_\Bbbk V = \mathrm{tr}_{V/\Bbbk}(tf) = t\, \mathrm{tr}_{V/\Bbbk}(f) = \varepsilon(t)\mathrm{tr}_{V/\Bbbk}(f).$$

Choosing $f \in \mathrm{End}_{\Bbbk(V) \text{ with } \mathrm{tr} V/\Bbbk}(f) = 1$, we deduce that $\dim_\Bbbk V \neq 0$ in $\Bbbk$.

(b) Now let P be a projective H-module and assume, by way of contradiction, that p does not divide $\dim_\Bbbk P$. Then the trace map $\mathrm{tr}_{P/\Bbbk}$ splits via $\sigma : \Bbbk_\varepsilon \to \mathrm{End}_\Bbbk(P)$, $k \mapsto (\dim_\Bbbk P)^{-1} k \cdot \mathrm{Id}_P$. Therefore, $\Bbbk_\varepsilon$ is isomorphic to a direct summand of $\mathrm{End}_\Bbbk(P)$. Inasmuch as $\mathrm{End}_\Bbbk(P) \cong P \otimes P^*$ is projective, by the Fundamental Theorem of Hopf Modules [Mo, Theorem 1.9.4], we conclude that $\Bbbk_\varepsilon$ is projective as well. This forces H to be semisimple, contrary to our assumption. ∎

Remarks. The semisimplicity hypothesis in (a) is definitely necessary. Indeed, the restricted enveloping algebra $H = u(\mathfrak{g})$ of the restricted p-Lie algebra $\mathfrak{g} = sl(2, \Bbbk)$ over a field $\Bbbk$ of characteristic $p > 2$ has an irreducible module of dimension p. See Section 4.4 below for a detailed discussion of this example. Part (b) implies in particular the known result [L, Theorem 4.3] that any involutory Hopf algebra H with $\dim_{\Bbbk} H$ not divisible by p is semisimple. Since this is false in general if H is not involutory (cf. Section 4.1), this hypothesis is necessary for (b) to hold. In (a), semisimplicity of H may very well entail that H is involutory (Kaplansky's conjecture [K]; known to be true in characteristic 0 [LR2]. For an alternative proof, see [PQ2]).

2.4. *Local Hopf Subalgebras*

Stronger estimates than the one provided by Theorem 2.3(b) are sometimes possible by using local Hopf subalgebras. These are exactly those Hopf subalgebras L of H such that the augmentation ideal $L^{+} = \operatorname{Ker} \varepsilon_L$ is nilpotent.

LEMMA. *Let L be a local Hopf subalgebra of H. Then* $\dim_{\Bbbk} L$ *divides the dimension of every projective H-module*.

Proof. Since H is free as (left and right) L-module, by the Nichols–Zoeller Theorem [Mo, Theorem 3.1.5], every projective H-module is projective, and hence free, over L. ∎

Remarks and Examples. If $H = \Bbbk G$ is the group algebra of a finite group G then the local Hopf subalgebras of H are the group subalgebras $\Bbbk P$, where P is a p-subgroup of G (0-subgroup means $\langle 1 \rangle$). The local Hopf subalgebras of the restricted enveloping algebra $H = u(\mathfrak{g})$ of a finite-dimensional restricted p-Lie algebra $(\mathfrak{g}, [p])$ over a field $\Bbbk$ of characteristic $p > 0$ are the enveloping subalgebras $u(\mathfrak{p})$, where $\mathfrak{p}$ is a p-nilpotent p-Lie subalgebra of $\mathfrak{g}$. Here, $\mathfrak{p}$ is p-nilpotent if some power of the p-map $[p]$ is 0 on $\mathfrak{p}$. If H is a semisimple Hopf algebra then all Hopf subalgebras are semisimple as well [Mo, Corollary 3.2.3]. Therefore, $\Bbbk$ is the only local Hopf subalgebra in this case. Even if H is not semisimple, local Hopf subalgebras $\neq \Bbbk$ need not exist; the Hopf algebra H_4 in characteristic $p \neq 2$ is an example. (Note, however, that H_4 is free over the local non-Hopf subalgebra $L = \Bbbk[x]$, in the notation of Section 4.1, and so the conclusion of the lemma applies to L as well.)

2.5. *Projective Covers*, *Unimodularity*, *and Symmetry*

Recall that if V is an irreducible H-module then the *projective cover* $P(V)$ is the unique (up to isomorphism) indecomposable projective H-

module which maps onto V (cf. [CR, p. 131]). In the following lemma, we let $\alpha \in H^*$ denote the "distinguished" group-like element of H^* such that

$$th = \alpha(h)t$$

holds for every left integral t in H and every $h \in H$ (cf. [Mo, p. 22]). The Hopf algebra H is *unimodular* if every left integral is a right integral for H or, equivalently, if $\alpha = \varepsilon$.

LEMMA. *$P(\Bbbk_\varepsilon)^* \cong P(\Bbbk_\alpha)$. In particular, $P(\Bbbk_\varepsilon)$ is self-dual if and only if H is unimodular.*

Proof. Put $Q = P(\Bbbk_\varepsilon)^*$, an indecomposable projective H-module, by Section 2.2. It suffices to show that Q maps onto $\Bbbk_\alpha$. But $Q \cong He$ for some primitive idempotent $e \in H$, and He contains a non-zero left integral t of H, because $\Bbbk_\varepsilon \cong \Bbbk_\varepsilon^*$ embeds into Q. Thus $t = te = \alpha(e)t$, and so $\alpha(e) = 1$ and $Q \overset{\cong}{\to} He \overset{\alpha}{\to} \Bbbk_\alpha$ is epi. ∎

PROPOSITION [OS]. *H is a symmetric algebra precisely if H is unimodular and S^2 is inner.*

Proof. The conditions are sufficient. For, if $\lambda \in H^*$ is a non-zero right integral then, putting $(h,k) = \lambda(hk)$ for $h, k \in H$, one obtains an associative bilinear form $(\cdot,\cdot)\colon H \times H \to \Bbbk$ which is well known to be non-degenerate ([LS, Theorem] or [R, Cor. 2(b)]). Moreover, since H is unimodular, the form also satisfies $(h,k) = (S^2(k), h)$ for $h, k \in H$ ([LS, Proposition 8] or [R, Theorem 3(a)]). Thus, choosing a unit $u \in H$ so that $S^2(h) = uhu^{-1}$ holds for all $h \in H$, we can define $\beta\colon H \times H \to \Bbbk$ by $\beta(h,k) = (uh,k)$ to obtain the required symmetric form.

Conversely, assume that H is symmetric. Then $P(V^*) \cong P(V)^*$ holds for all irreducible H-modules V, by Section 1.7(2). In particular, the above lemma implies that H is unimodular. (For a more elementary proof of this implication, see [H2, Theorem 2].) Thus the associative non-degenerate form $(h,k) = \lambda(hk)$ used in the first paragraph of the proof satisfies $(h,k) = (S^2(k), h)$. On the other hand, by Lemma 1.7(b), $(h,k) = (u^{-1}ku, h)$ for some unit $u \in H$. Consequently, $S^2(k) = u^{-1}ku$ which shows that S^2 is inner. ∎

Remarks and Examples. (1) Finite-dimensional commutative Hopf algebras are symmetric, since they are unimodular and involutory. Cocommutative Hopf algebras are symmetric precisely if they are unimodular which is not generally the case (cf. (4) below). Thus symmetry does not pass from a Hopf algebra to its dual. (See also (3) below.)

(2) The fact that S^2 is inner for symmetric Hopf algebras H entails in particular that $V^{**} \cong V$ holds for all H-modules V (Sect. 2.2). Further-

more, in view of Section 1.7(1), the proposition implies that

$$S^2 \textit{ is inner if } H \textit{ is semisimple}.$$

For $\Bbbk$ algebraically closed, this fact has been noted by Larson [L, Prop. 3.5]; see also [R, Theorem 5]); the general case is due to Oberst and Schneider [OS]. We also remark that Drinfeld has shown that S^2 is inner for any *almost cocommutative* Hopf algebra ([Dr], cf. also [Mo, Proposition 10.1.4]).

(3) The Drinfeld double $D(H)$ of any Hopf algebra H is always symmetric, because the conditions of the proposition are satisfied by [R2, Theorem 4 and Cor. 2]. (For the fact that S^2 is inner, one could also quote Drinfeld's more general theorem about almost commutative Hopf algebras mentioned in (2) above.) Therefore, any H embeds in a symmetric Hopf algebra, and symmetry is not in general inherited by Hopf subalgebras. Moreover, the dual $D(H)^*$ is unimodular precisely if both H and H^* are, and similarly for the property of the square of the antipode being inner [R2, Cor. 4 and Prop. 8]. Consequently, $D(H)^*$ is symmetric if and only if both H and H^* are.

(4) Let $H = u(\mathfrak{g})$ denote the restricted enveloping algebra of the finite-dimensional restricted p-Lie algebra $(\mathfrak{g}, [p])$ over a field $\Bbbk$ of characteristic $p > 0$, and let $\mathrm{ad}_{\mathfrak{g}}(x) \in \mathrm{End}_{\Bbbk}(\mathfrak{g})$ be defined as usual by $\mathrm{ad}_{\mathfrak{g}}(x)(y) = [x, y]$ for $x, y \in \mathfrak{g}$. By [LS, Cor. on p. 91] (cf. also [Sch]), symmetry (or unimodularity) of H is equivalent to

$$\mathrm{tr}\big(\mathrm{ad}_{\mathfrak{g}}(x)\big) = 0 \qquad \text{for all } x \in \mathfrak{g}.$$

This condition is certainly satisfied if $\mathfrak{g}$ is nilpotent or if $\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$ and so, in particular, if $\mathfrak{g}$ is simple. The condition is also satisfied for the diamond algebra, for example, but not for the 2-dimensional solvable p-Lie algebra (cf. Sect. 4.3).

3. THE GROTHENDIECK RING

The notations introduced at the beginning of Section 2 *remain in effect. Furthermore, as in Section* 1, $V_1, \ldots, V_t$ *denotes a full set of nonisomorphic irreducible H-modules,* $P_i = P(V_i)$ *are their projective covers, and* $J = \mathrm{rad}\, H$ *is the Jacobson radical of* H.

3.1. *The Grothendieck Ring*

As is well known (e.g., [Ser]), the Grothendieck group $G_0(H)$ is endowed with the structure of an augmented $\mathbb{Z}$-algebra with identity element

$1 = [\Bbbk_\varepsilon]$: The augmentation is $\dim_{\Bbbk} : G_0(H) \to \mathbb{Z}$ and multiplication is given by $[V] \cdot [W] = [V \otimes W]$. We will refer to $G_0(H)$ as the *Grothendieck ring* of H. Putting $[V]^* = [V^*]$ we obtain an anti-automorphism $*$ of the ring $G_0(H)$ which permutes the basis $\{[V_i]\}$ of $G_0(H)$, and $*$ is an involution of $G_0(H)$ if S^2 is inner (Sects. 2.1, 2.2).

Similarly, $[P]^* = [P^*]$ yields an automorphism of the group $K_0(H)$ which permutes the basis $\{[P_i]\}$ and has order 2 if S^2 is inner. Putting $[P] \cdot [V] = [P \otimes V]$ we obtain a right $G_0(H)$-module structure on $K_0(H)$. The fact that $P \otimes V$ is projective if P is can be seen as follows. Clearly, it suffices to prove that $H \otimes V$ is projective for any V. Now $H \otimes V$ is a (left) H-Hopf module (cf. [Mo, Example 1.9.3]), and so $H \otimes V$ is in fact free as left H-module, by the Fundamental Theorem of Hopf Modules [Mo, Theorem 1.9.4]—The Cartan map $c : K_0(H) \to G_0(H)$ is a $*$-equivariant map of $G_0(H)$-modules.

With respect to the $G_0(H)$-module structures and duality maps $*$ on $K_0(H)$ and $G_0(H)$, the bilinear maps $\langle \cdot , \cdot \rangle : K_0(A) \times G_0(A) \to \mathbb{Z}$ and $\{\cdot , \cdot\} : K_0(H) \times K_0(H) \to \mathbb{Z}$ of Section 1.2 satisfy the identities

$$\langle ax, y \rangle = \langle a, yx^* \rangle, \qquad \{a, b\} = \{b^*, a^*\}$$

for $x, y \in G_0(H)$ and $a, b \in K_0(H)$. The first follows from the $\Bbbk$-linear isomorphisms $\mathrm{Hom}_H(P \otimes V, W) \cong (W \otimes V^* \otimes P^*)^H \cong \mathrm{Hom}_H(P, W \otimes V^*)$, and the second from the isomorphism $\mathrm{Hom}_H(V, W) \cong \mathrm{Hom}_H(W^*, V^*)$ (cf. Sects. 2.1, 2.2). We point out two consequences of these formulas.

- *The $G_0(H)$-module $K_0(H)$ is faithful*: Indeed, if $x \in G_0(H)$ satisfies $K_0(H)x = 0$ then $0 = \langle K_0(H)x, 1 \rangle = \langle K_0(H), x^* \rangle$. In view of the orthogonality relations, the latter condition is equivalent with $x^* = 0$, and hence with $x = 0$.

- *The left and right radical of the form $\{\cdot , \cdot\}$ are both equal to the kernel of the Cartan map c*: Since $\mathrm{Ker}(c)$ is $*$-invariant and $\{a, b\} = \{b^*, a^*\}$ holds for all $a, b \in K_0(H)$, it suffices to show that the right radical of $\{\cdot , \cdot\}$ equals $\mathrm{Ker}(c)$. But, as above, $\{K_0(H), a\} = \langle K_0(H), c(a) \rangle = 0$ is equivalent to $c(a) = 0$.

Recall also that the form $\{\cdot , \cdot\}$ has matrix C', and it is symmetric if H is symmetric.

Remarks and Examples. (1) If I is an ideal of H that is contained in $J = \mathrm{rad}\, H$, then inflation of modules along the canonical map π: $H \to H/I$ gives a group isomorphism $G_0(H/I) \xrightarrow{\cong} G_0(H)$ (cf. [Ba1, p. 455]). In case I is a Hopf ideal of H, this is an isomorphism of rings. This applies in particular if J is a Hopf ideal of H. See Section 3.3 below for a detailed discussion of this case.

(2) If H is *semisimple* then all H-modules are projective. Thus $K_0(H) = G_0(H)$ and the Cartan map c is the identity map in this case. For example, let $H = (\Bbbk G)^*$ denote the dual of the group algebra $\Bbbk G$ of the finite group G, so $H \cong \Bbbk^{|G|}$ as $\Bbbk$-algebras. Here, $G_0(H) \cong \mathbb{Z}G$, the integral group ring of G. Up to a finite separable field extension, this example covers all semisimple commutative Hopf algebras (cf. [Mo, Theorem 2.3.1).

(3) Let H be *almost cocommutative* in the sense of Drinfeld [Dr]. Then S^2 is inner and $V \otimes W \cong W \otimes V$ holds for all H-modules V and W ([Dr]; cf. also [Mo, Lemma 10.1.2 and Proposition 10.1.4]). Hence $G_0(H)$ is a *commutative* ring and $*$ is an involution in this case.

3.2. *Semiprimeness*

Recall a subgroup X of $K_0(H)$ is said to be *isotropic* with respect to form $\{\cdot,\cdot\}$ if $\{X, X\} = 0$. In case $\{\cdot,\cdot\}$ is symmetric, this condition is equivalent with $\{x, x\} = 0$ for all $x \in X$.

PROPOSITION. *$K_0(H)$ contains no non-zero $*$-invariant isotropic $G_0(H)$-submodules if and only if $G_0(H)$ is a semiprime ring and the Cartan map c is injective.*

Proof. First assume that $K_0(H)$ contains no non-zero $*$-invariant isotropic $G_0(H)$-submodules. Then, in particular, $\operatorname{Ker}(c) = 0$ and so c is injective. Let N denote the nilpotent radical of the (Noetherian) ring $G_0(H)$ and suppose, by way of contradiction, that $N \neq 0$. Choose n so that $I = N^n \neq 0$, but $I^2 = 0$, and note that I is $*$-invariant, because N certainly is. Also, since c is injective, $c \otimes_{\mathbb{Z}} \mathbb{Q}$ is bijective, and so $I \cap \operatorname{Im}(c) \neq 0$. Consequently, letting X denote the preimage of I in $K_0(H)$ under c, we have $I \supseteq c(X)$ and X is a non-zero $*$-invariant $G_0(H)$-submodule of $K_0(H)$. Since $I^2 \supseteq c(XI)$, we deduce that $c(XI) = 0$, and hence $XI = 0$. On the other hand, $\langle XI, 1\rangle = \langle X, I\rangle \supseteq \{X, X\} \neq 0$, by assumption on the form $\{\cdot,\cdot\}$. This contradiction shows that we must have $N = 0$, and so $G_0(H)$ is semiprime.

Conversely, assume that $G_0(H)$ is a semiprime ring and the Cartan map c is injective. If X is a non-zero $*$-invariant isotropic $G_0(H)$-submodule of $K_0(H)$, then $I = c(X)$ is a non-zero $*$-invariant right ideal of $G_0(H)$ (and so I is actually a two-sided ideal of $G_0(H)$). Moreover, $0 = \{X, X\} = \langle X, I\rangle = \langle XI, 1\rangle = \langle XIG_0(H), 1\rangle = \langle XI, G_0(H)\rangle$, and hence the orthogonality relations imply that $XI = 0$. Therefore, $I^2 = c(XI) = 0$, contradicting semiprimeness of $G_0(H)$. ∎

EXAMPLES. (1) *Semisimple Hopf algebras H*: In this case, C is the identity matrix and C' is a diagonal matrix with positive entries. Therefore the quadratic form $Q(x) = \{x, x\}$ is positive definite and no non-zero isotropic submodules of $K_0(H)$ can exist. Thus, $G_0(H)$ is semiprime if H is semisimple. More generally, this shows that $G_0(H)$ is a semiprime ring if J is a *Hopf ideal* of H, because $G_0(H) \cong G_0(H/J)$ holds in this case.

(2) *Group algebras over sufficiently large fields*: For group algebras $\Bbbk G$ of finite groups G, the Grothendieck ring $G_0(\Bbbk G)$ can be explicitly described in terms of (Brauer or ordinary) characters, and semiprimeness is evident from this description. However, it also follows from the proposition, in view of the fact that the Cartan matrix C ($= C'$, because $\Bbbk$ is assumed large) is known to be invertible and to have the form $C = D^T D$, where D is an integer matrix, the so-called *decomposition matrix* (cf. [CR, Cor. 18.10 and Theorem 18.25]). Consequently, C is positive definite, and semiprimeness of $G_0(\Bbbk G)$ follows as in (1).

(3) The restricted enveloping algebra $H = u(sl(2, \Bbbk))$ provides an example of a Grothendieck ring $G_0(H)$ which is not semiprime. See Section 4.4.

3.3. *The Case When* $J = \operatorname{rad} H$ *Is a Hopf Ideal*

We discuss the case where $J = \operatorname{rad} H$ is a Hopf ideal of H in some detail. Some properties of this case have already been noted in Section 3.1, Remarks and Examples (1), and in Section 3.2, Examples (1).

Since $\varepsilon(J) = 0$ and $S(J) \subseteq J$ are automatic, $J = \operatorname{rad} H$ is a Hopf ideal if and only if

$$\Delta(J) \subseteq H \otimes J + J \otimes H.$$

Several further equivalent conditions are given in the following lemma. In this regard, see also [PQ] and the remarks in [Mo, pp. 62–63].

LEMMA. *The following conditions are equivalent.*

(1) *J is a Hopf ideal of H.*

(2) *Tensor products of semisimple H-modules are semisimple.*

(3) *If V, W are H-modules, then $J \cdot (W \otimes V) \subseteq JW \otimes V + W \otimes JV$.*

(4) *If V, W are H-modules, with V semisimple, then $J \cdot (W \otimes V) = JW \otimes V$.*

(5) *Same as* (4), *but with V semisimple and W projective.*

(6) *If V, W are H-modules, with V semisimple, then $P(W \otimes V) \cong P(W) \otimes V$.*

(7) *Same as* (6), *but with V and W both semisimple.*

Proof. (1) $\Leftrightarrow$ (2): (2) is equivalent to the equation $J \cdot (H/J \otimes H/J) = 0$ which in turn is equivalent to $\Delta(J) \subseteq H \otimes J + J \otimes H$.

(1) $\Rightarrow$ (3) is clear, and (3) $\Rightarrow$ (1) follows by taking $V = W = H$.

(3) ⇒ (5): Write $W \oplus Q \cong H^r$ for suitable Q and r. Then we have H-module isomorphisms

$$(W \otimes V) \oplus (Q \otimes V) \cong H^r \otimes V \cong H^{r \dim_{\Bbbk} V},$$

the last isomorphism being a consequence of the Fundamental Theorem of Hopf Modules (cf. Sect. 3.1). Hence, as $\Bbbk$-vector spaces,

$$\begin{aligned} J \cdot (W \otimes V) \oplus J \cdot (Q \otimes V) &\cong J^{r \dim_{\Bbbk} V} \cong J^r \otimes V \\ &\cong (JW \oplus JQ) \otimes V \cong (JW \otimes V) \oplus (JQ \otimes V). \end{aligned}$$

But (3) implies that $J \cdot (W \otimes V) \subseteq JW \otimes V$, and similarly for Q, because V is semisimple. Thus, comparing dimensions, we obtain (5).

(5) ⇒ (4) and (6): We write head $X = X/JX$ for all H-modules X. Now let V, W be H-modules, with V semisimple. Then head $P(W) \cong$ head W, a general property of projective covers, and (5) implies that head$(P(W) \otimes V) \cong (\text{head}(P(W)) \otimes V$. Thus $(\text{head}\, W) \otimes V \cong \text{head}(P(W) \otimes V)$ is semisimple, and so head$(W \otimes V)$ canonically maps onto $(\text{head}\, W) \otimes V$. On the other hand, the canonical epimorphism $P(W) \otimes V \twoheadrightarrow W \otimes V$ entails an epimorphism $(\text{head}\, W) \otimes V \cong \text{head}(P(W) \otimes V) \twoheadrightarrow \text{head}(W \otimes V)$. So $(\text{head}\, W) \otimes V$ and head$(W \otimes V)$ are in fact isomorphic which proves (4). For (6), consider the composite epimorphism

$$\begin{aligned} P(W \otimes V) \twoheadrightarrow W \otimes V \twoheadrightarrow \text{head}(W \otimes V) \\ \cong (\text{head}\, W) \otimes V \cong \text{head}(P(W) \otimes V), \end{aligned}$$

where the first two epimorphisms are the canonical ones and the last isomorphism was established above. Using the Nakayama Lemma we deduce that $P(W \otimes V)$ maps onto $P(W) \otimes V$. Similarly, the canonical epimorphism $P(W) \otimes V \twoheadrightarrow W \otimes V$ implies that $P(W) \otimes V$ maps onto $P(W \otimes V)$. Inasmuch as $P(W) \otimes V$ and $P(W \otimes V)$ are both finite dimensional, the latter two epimorphisms are in fact isomorphisms, thereby proving (6).

(6) ⇒ (7) is trivial.

(7) ⇒ (2): Let V and W be semisimple H-modules and put $X = W \otimes V$. By two applications of (7),

$$P(X) \cong P(W) \otimes V \cong P(\Bbbk_{\varepsilon}) \otimes X.$$

On the other hand, by general properties of projective covers, $P(X) \cong P(\text{head}\, X)$, and (7) applied to head X further implies that $P(X) \cong P(\Bbbk_{\varepsilon}) \otimes \text{head}\, X$. Therefore, $P(\Bbbk_{\varepsilon}) \otimes X \cong P(\Bbbk_{\varepsilon}) \otimes \text{head}\, X$. Comparing dimensions, we conclude that the canonical map $X \twoheadrightarrow \text{head}\, X$ is an isomorphism and so X is semisimple.

Since (4) clearly implies (5), the proof is complete. ∎

COROLLARY. *Assume that* $J = \mathrm{rad}\, H$ *is a Hopf ideal of* H. *Then, for any* H*-module* V, *the projective cover* $P(V)$ *is given by* $P(V) \cong P(\Bbbk_\varepsilon) \otimes (V/JV)$. *Consequently,* $K_0(H)$ *is a free* $G_0(H)$*-module of rank* 1 *with generator* $[P(\Bbbk_\varepsilon)]$. *Furthermore,* $\dim_\Bbbk P(\Bbbk_\varepsilon)$ *is an eigenvalue of the Cartan matrix* C, *and hence a divisor of* $\det C$ *in* $\mathbb{Z}$.

Proof. In view of the general isomorphism $P(V) \cong P(V/JV)$, the isomorphism $P(V) \cong P(\Bbbk_\varepsilon) \otimes (V/JV)$ follows from (7) in the lemma applied to V/JV.

In particular, we have $P_i \cong P(\Bbbk_\varepsilon) \otimes V_i$ for $i = 1, \ldots, t$ which can be written as a matrix equation over $G_0(H)$ as follows:

$$[P(\Bbbk_\varepsilon)] \cdot \begin{pmatrix} [V_1] \\ \vdots \\ [V_t] \end{pmatrix} = C \cdot \begin{pmatrix} [V_1] \\ \vdots \\ [V_t] \end{pmatrix}.$$

The assertion concerning $\dim_\Bbbk P(\Bbbk_\varepsilon)$ now follows by applying the augmentation $\dim_\Bbbk : G_0(H) \to \mathbb{Z}$ to this equation. ∎

Remarks and Examples. (1) If all simple H-modules are 1-dimensional (equivalently, $H/J \cong \Bbbk^r$ as $\Bbbk$-algebras for some r) then all tensor products of simple H-modules are 1-dimensional as well, and hence condition (2) of the lemma is clearly satisfied. Thus J is a Hopf ideal in this case. By Section 3.1, Remarks and Examples (1) and (2), we conclude that

$$G_0(H) \cong \mathbb{Z}G,$$

where G is the group of group-like elements of H^*. For explicit examples of this kind, see Sections 4.1–4.3 below.

(2) If $H = \Bbbk G$ is a finite group algebra then J is a Hopf ideal precisely if G has a normal Sylow p-subgroup [M]. Furthermore, Brockhaus [Br] has shown that if $P(V) \cong P(\Bbbk_\varepsilon) \otimes V$ holds for all semisimple $\Bbbk G$-modules V then J is a Hopf ideal of $\Bbbk G$. This is a substantial strengthening of the implication (6) ⇒ (1) in the lemma for group algebras. I do not know to what extent this fact generalizes to Hopf algebras. The present proof of Brockhaus' theorem depends on the classification of finite simple groups.

(3) The example $H = u(sl(2, \Bbbk))$ shows that all assertions of the corollary are false in general: $K_0(H)$ is no longer generated by $[P(\Bbbk_\varepsilon)]$ in this case, and $\dim_\Bbbk P(\Bbbk_\varepsilon) = 2p$ is not an eigenvalue of the Cartan matrix C. See Section 4.4.

3.4. *The Cartan Matrix*

In this subsection, we determine the rank of the $\Bbbk$-linear map

$$\widetilde{c_H} = \mathrm{Id}_\Bbbk \otimes c_H : \widetilde{K_0(H)} = \Bbbk \otimes_\mathbb{Z} K_0(H) \to \widetilde{G_0(H)} = \Bbbk \otimes_\mathbb{Z} G_0(H).$$

Note that $\operatorname{rank}\widetilde{c_H}$ equals the rank of the Cartan matrix C of H in case $p = 0$, and the rank of the reduction of $C \bmod p$ when $p > 0$. We will need the *right adjoint action* $\triangleleft$ of H on H which is defined by

$$h \triangleleft k = \sum S(k_2) h k_1 \qquad (h, k \in H).$$

THEOREM. *Suppose that* $\Bbbk$ *is a splitting field for* H. *Then*

$$\operatorname{rank}\widetilde{c_H} = \dim_{\Bbbk}(H \triangleleft t),$$

where t *is any non-zero left integral of* H. *Moreover, if* S^2 *is inner then the following are equivalent.*

(1) *H is semisimple*;

(2) $C = \mathrm{Id}$;

(3) *p does not divide* $\det C$.

Note that, for $p = 0$, *condition* (3) *just says that* $\det C \neq 0$.

Proof. By Theorem 1.6, we have a commutative diagram

$$\begin{array}{ccc}
\widetilde{\mathrm{K}_0(\mathrm{H})} & \xrightarrow{\ \widetilde{\mathrm{c}_{\mathrm{H}}}\ } & \widetilde{\mathrm{G}_0(\mathrm{H})} \\
\cong \big\downarrow \tilde{\rho} & & \tilde{\chi} \big\downarrow \cong \\
\mathrm{T(H)}_{\mathrm{reg}} & \xrightarrow[(\cdot)^{\mathrm{t}}]{} & \mathrm{C(H)}_{\mathrm{reg}}.
\end{array}$$

So $\operatorname{rank}\widetilde{c_H} = \operatorname{rank}(\cdot)^t$. By [R, Proposition 7], the map $(\cdot)^t$ has the following description: Let t be a left integral for H and λ a right integral for H^* such that $\lambda(t) = 1$. Then, for any $h \in H$,

$$([h])^t = (h \triangleleft t) \rightharpoonup \lambda,$$

where $\rightharpoonup$ is defined by $(h \rightharpoonup f)(k) = f(kh)$ for $h, k \in H$ and $f \in H^*$. Furthermore, λ is a free H-basis of $(H^*, \rightharpoonup)$ ([LS, p. 83] or [R, Corollary 2]). Therefore, $\operatorname{rank}(\cdot)^t = \dim_{\Bbbk}(H \triangleleft t)$, as claimed.

The implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) are trivial. For (3) $\Rightarrow$ (1), note that (3) says that $\widetilde{c_H}$ is injective, and hence so is the map $(\cdot)^t$ in the above diagram. Now suppose that S^2 is inner, say $S^2(h) = uhu^{-1}$ for some unit $u \in H$. Since $\varepsilon(u) \neq 0$, we have $[u] \neq 0$ in $T(H)_{\mathrm{reg}}$, and so $([u])^t \neq 0$. Therefore, by the above formula for $(\cdot)^t$, $u \triangleleft t \neq 0$. The computation

$$u \triangleleft t = \sum S(t_2) u t_1 = \sum S(t_2) S^2(t_1) u = S\Big(\sum S(t_1) t_2\Big) u = \varepsilon(t) u$$

now shows that $\varepsilon(t) \neq 0$, and so H is semisimple. ∎

Remarks and Examples. (1) *Finite group algebras* $H = \Bbbk G$: Taking $t = \sum_{g \in G} g$ we have $g \triangleleft t = |\mathbb{C}_G(g)| \mathfrak{c}_g$ for $g \in G$, where $\mathbb{C}_G(g)$ denotes the centralizer of g in G and $\mathfrak{c}_g \in \Bbbk G$ is the class sum of g, that is, the sum of the elements in the conjugacy class of g. Therefore, $\Bbbk G \triangleleft t$ is the $\Bbbk$-linear span of all class sums $\mathfrak{c}_g$ such that p does not divide $|\mathbb{C}_G(g)|$. (These classes are in particular *p-regular*, that is, they consist of elements having order not divisible by p.) Consequently,

$$\operatorname{rank} \widetilde{c_{\Bbbk G}} = \#\{\text{conj. classes } \mathfrak{C} \text{ of } G \text{ such that } |\mathfrak{C}|_p = |G|_p\},$$

where $|\cdot|_p$ denotes the p-part of the size ($|\cdot|_0 = 1$).

(2) If H is involutory then the implication (3) $\Rightarrow$ (1) above follows more simply from Theorem 2.3(b) which asserts that, for H not semisimple, the map $G_0(H) \to^{\dim_\Bbbk} \mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$ factors through the cokernel of the Cartan map c. Now just use the fact that if $\det C \neq 0$ then $\det C$ is the size of this cokernel.

(3) If K is a local Hopf subalgebra of H (or, more generally, a local subalgebra so that H is free over K) then $\dim_\Bbbk K$ divides $\det C$. Indeed, since $G_0(K) = \langle [\Bbbk_{\varepsilon_K}] \rangle$ and projective H-modules are projective, and hence free, over K, the restriction map induces an epimorphism

$$G_0(H)/cK_0(H) \overset{\text{Res}}{\twoheadrightarrow} G_0(K)/cK_0(K) \cong \mathbb{Z}/\dim_\Bbbk K \cdot \mathbb{Z}.$$

3.5. *Trace Spaces for Hopf Algebras*

Reference [R, Lemma 1] gives two alternative descriptions of the space of $\Bbbk$-valued traces $C(H)$. Namely, $C(H)$ is the set of invariants with respect to the *left coadjoint action* of H on H^* that is given by

$$(h \triangleright f)(k) = \sum f(S(h_2)kh_1) \qquad \text{for } h, k \in H,\ f \in H^*.$$

(This is the transpose of the action $\triangleleft$ that was used in Section 3.4.) Alternatively, one can characterize $C(H)$ as the set $\operatorname{Cocom} H^*$ of cocommutative elements of H^*. To summarize,

$$C(H) = \operatorname{Cocom} H^* = (H^*)^H.$$

Note that $\{f \in H^* : f \text{ vanishes on } J\}$ is the *coradical* $(H^*)_0$ of H^* (cf. [Mo, Proposition 5.2.9]). Therefore, $C(H)_{\text{reg}}$ can be viewed as the set $\operatorname{Cocom}(H^*)_0$ of cocommutative elements of the coradical of H^*. Since the coradical $(H^*)_0$ is clearly mapped to itself under $\triangleright$, we have

$$C(H)_{\text{reg}} = \operatorname{Cocom}(H^*)_0 = (H^*)_0^H.$$

From the foregoing, we see in particular that $C(H)$ is a $\Bbbk$-subalgebra of H^*, because Cocom H^* clearly is. In Corollary 3.7 we will show that if H/J is separable then $C(H)_{\text{reg}}$ is also a $\Bbbk$-subalgebra of H^* or, equivalently, $[H, H] + J$ is a coideal of H. Note further that $C(H)$ and $C(H)_{\text{reg}}$ are both stable under the antipode S^* of H^*, since $[H, H]$ and $J = \text{rad } H$ are stable under S.

EXAMPLES. (1) $H = (\Bbbk G)^*$ for G a finite group: Here $C(H)_{\text{reg}} = C(H) = H^* = \Bbbk G$. Since $\Bbbk G$ need not be commutative, this example shows in particular that the isomorphism $Z(H) \cong C(H)$ of Lemma 1.7 is not in general an isomorphism of $\Bbbk$-algebras.

(2) $H = \Bbbk G$ for G a finite group: Here, $(h \triangleright f)(g) = f(g^h)$ for $g, h \in G$ and $f \in H^*$, where $g^h = h^{-1}gh$ is conjugation in G. Thus $C(H)$ is canonically isomorphic with the $\Bbbk$-algebra of all $\Bbbk$-valued functions on the set of conjugacy classes of G, with "pointwise" multiplication of functions. Furthermore, $[H, H] + J$ is the $\Bbbk$-linear span of the elements $g - g_{p'}^h$ for $g, h \in G$, where $g_{p'}$ denotes the p'-part of g ($= g$ if $p = 0$). Therefore, $T(H)_{\text{reg}}$ can be identified with the $\Bbbk$-vector space with basis the set of p-regular conjugacy classes of G. Under this identification, the image $[g] \in T(H)_{\text{reg}}$ of $g \in G$ becomes the conjugacy class of p'-part of g. Furthermore, $C(H)_{\text{reg}}$ can be viewed as the algebra of $\Bbbk$-valued functions on the set of p-regular conjugacy classes of G: A trace $f \in C(H)$ belongs to $C(H)_{\text{reg}}$ precisely if it satisfies $f(g) = f(g_{p'})$ for all $g \in G$. See [P, p. 56–58] for all this.

3.6. PROPOSITION. *The character map $\chi : G_0(H) \to C(H)$ is a ring homomorphism which satisfies $\chi_{V^*} = S^*(\chi_V)$ and $\chi_V(1) = \dim_{\Bbbk}(V)$. If $\Bbbk$ is a splitting field for H then $C(H)_{\text{reg}}$ is a $\Bbbk$-subalgebra of H^* and χ induces an isomorphism of $\Bbbk$-algebras*

$$\tilde{\chi} = \text{Id}_{\Bbbk} \otimes \chi : \widetilde{G_0(H)} = \Bbbk \otimes_{\mathbb{Z}} G_0(H) \xrightarrow{\cong} C(H)_{\text{reg}}.$$

Proof. First, $\chi_{\Bbbk_\varepsilon} = \varepsilon$, and so χ respects the identity elements of $G_0(H)$ and $C(H)$. Let V and W be H-modules. Then, by Section 2.1, there are $\Bbbk$-isomorphisms $\text{End}_{\Bbbk}(V \otimes W) \cong V \otimes W \otimes W^* \otimes V^* \cong \text{End}_{\Bbbk}(V) \otimes \text{End}_{\Bbbk}(W)$. Under this identification, $\text{tr}_{V \otimes W}$ becomes

$$\text{tr}_{V\otimes W} : \text{End}_{\Bbbk}(V \otimes W) \cong \text{End}_{\Bbbk}(V) \otimes \text{End}_{\Bbbk}(W) \xrightarrow{\text{tr}_V \otimes \text{tr}_W} \Bbbk \otimes \Bbbk \cong \Bbbk,$$

and

$$h_{V\otimes W} = \sum (h_1)_V \otimes (h_2)_W \qquad (h \in H),$$

where $h \mapsto h_V$ denotes the structure map $H \to \text{End}_{\Bbbk}(V)$, etc. Therefore, the fact that χ is a ring homomorphism follows from the computation $\chi_{V\otimes W}(h) = \sum \mathrm{tr}_V(h_1)_V\, \mathrm{tr}_W(h_2)_W = \sum \chi_V(h_1)\chi_W(h_2) = (\chi_V\chi_W)(h)$. The formula $\chi_{V^*} = S^*(\chi_V)$ follows similarly, since the obvious $\Bbbk$-linear isomorphism $\mathrm{End}_{\Bbbk}(V^*) \cong \mathrm{End}_{\Bbbk}(V)$ sends $h_{V^*} \mapsto S(h)_V$. The formula $\chi_V(1) = \dim_{\Bbbk}(V)$ is trivial. The remaining assertions now follow from the fact that, for $\Bbbk$ a splitting field, the map $\tilde{\chi}$ is an isomorphism between $\widetilde{G_0(H)}$ and $C(H)_{\mathrm{reg}}$, by Theorem 1.6(b). ∎

3.7. COROLLARY. *If H/J is separable over $\Bbbk$ then $C(H)_{\mathrm{reg}}$ is a $\Bbbk$-subalgebra of H^*.*

Proof. Choose a field extension $\mathbb{K}/\Bbbk$ so that $\mathbb{K}$ is a splitting field for $\tilde{H} = \mathbb{K} \otimes H$. By Proposition 3.6, $C(\tilde{H})_{\mathrm{reg}}$ is a $\mathbb{K}$-subalgebra of $\tilde{H}^* = \mathbb{K} \otimes H^*$. By separability, rad $\tilde{H} = \mathbb{K} \otimes J$ and so $C(\tilde{H})_{\mathrm{reg}} = \mathbb{K} \otimes C(H)_{\mathrm{reg}}$. Therefore, $C(H)_{\mathrm{reg}} = C(\tilde{H})_{\mathrm{reg}} \cap H^*$ is closed under multiplication, since both H^* and $C(\tilde{H})_{\mathrm{reg}}$ are. ∎

Remark. Of course, H/J is separable in case the base field $\Bbbk$ is perfect. In addition, H/J is known to be separable if either $J = 0$ (cf. [Mo, Cor. 2.2.2(1)], or if $H = \Bbbk G$ is the group algebra of a finite group G [CR, Theorem 7.10], or if $H = u(\mathfrak{g})$ is the restricted enveloping algebra of a "classical" p-Lie algebra $\mathfrak{g}$ [Se, p. 101]. I am not aware of an example where H/J is not separable.

4. EXAMPLES

4.1. *The Sweedler Algebra*

Let $H = H_4 = \Bbbk\langle 1, g, x, gx \mid g^2 = 1,\ x^2 = 0,\ xg = -gx\rangle$ and assume that $\Bbbk$ has characteristic $p \neq 2$. This algebra is quasitriangular but not unimodular (cf. [Mo, 1.5.6, 2.1.2, 10.1.17]). Here, $J = xH$ and $H/J \cong \Bbbk\langle g\rangle \cong (\Bbbk\langle g\rangle)^*$. Thus J is a Hopf ideal, and so we obtain ring isomorphisms $G_0(H) \cong \mathbb{Z}\langle g\rangle$. The two irreducible H-modules are $\Bbbk_\varepsilon$ and $\Bbbk_\alpha$, where $\alpha : g \mapsto -1,\ x \mapsto 0$ is the distinguished group-like element of H^*. Their projective covers, $P(\Bbbk_\varepsilon)$ and $P(\Bbbk_\alpha)$, are dual to each other, by Lemma 2.5. Therefore, $P(\Bbbk_\varepsilon)$ has socle isomorphic to $\Bbbk_\alpha$, and the socle of $P(\Bbbk_\alpha)$ is isomorphic to $\Bbbk_\varepsilon$. Thus, in $G_0(H)$, we have $c([P(\Bbbk_\varepsilon)] = c([P(\Bbbk_\alpha)]) = [\Bbbk_\varepsilon] + [\Bbbk_\alpha]$, and so the Cartan matrix is

$$C = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Note that the foregoing applies verbatim whenever H has only two irreducible modules, $\Bbbk_\varepsilon$ and $\Bbbk_\alpha$, where α is the distinguished group-like element. A cocommutative example of this form is the restricted enveloping algebra $H = u(\mathfrak{g})$ of the restricted 2-dimensional solvable 2-Lie algebra $\mathfrak{g}$ in characteristic $p = 2$ (cf. Sect. 4.3 below).

4.2. *Radford's Algebra*

The following Hopf algebra H is taken from [R3, Example 1] which in turn is based on an earlier construction due to Taft [T]. Fix $n > 1$ and assume that $\Bbbk$ contains a root of unity ω of order n. Then H is generated by elements x, y, g subject to the relations

$$g^n = 1,\ x^n = y^n = 0,\ xg = \omega gx,\ gy = \omega yg,\ xy = \omega yx.$$

Furthermore, g is group-like, and x and y are $(g, 1)$-primitive. The Hopf algebra has $\Bbbk$-basis $\{g^l x^r y^s : 0 \le l, r, s < n\}$, H is unimodular, and $S^2(h) = ghg^{-1}$ holds for all $h \in H$ (see [R3]). Thus H is symmetric. The radical of H is $J = xH + yH$, a Hopf ideal of H, and $H/J \cong \Bbbk\langle g\rangle$. The simple H-modules are: $\Bbbk_{\phi^i}$ $(i = 0, \ldots, n-1)$, where $\phi \in G(H^*)$ is given by $\phi(g) = \omega$, $\phi(x) = \phi(y) = 0$, and the map $[\Bbbk_{\phi^i}] \mapsto g^i$ gives a ring isomorphism $G_0(H) \to \mathbb{Z}\langle g\rangle$. Putting $e = (1/n)\sum g^i \in H$ we have $e = e^2$ and $P(\Bbbk_\varepsilon) = He = \bigoplus_{0 \le r,\, s < n} \Bbbk x^r y^s e$. The Loewy factors of $P(\Bbbk_\varepsilon)$ are given by

$$J^l P(\Bbbk_\varepsilon)/J^{l+1}P(\Bbbk_\varepsilon) = \sum_{r+s=l} \Bbbk x^r y^s e \bmod J^{l+1}P(\Bbbk_\varepsilon) \cong \bigoplus_{r+s=l} \Bbbk_{\phi^{s-r}}.$$

Therefore, in $G_0(H) = \mathbb{Z}\langle g\rangle$, we have

$$\begin{aligned} c([P(\Bbbk_\varepsilon)]) &= \sum_{l=0}^{2n-2} \sum_{r+s=l} [\Bbbk_{\phi^{s-r}}] \\ &= \left(1 + g^{-1} + \cdots + g^{-(n-1)}\right) \cdot \left(1 + g + \cdots + g^{n-1}\right) \\ &= n\left(1 + g + \cdots + g^{n-1}\right). \end{aligned}$$

Corollary 3.3 now implies that $c([P(\Bbbk_{\phi^i})]) = n(1 + g + \cdots + g^{n-1})g^i = n(1 + g + \cdots + g^{n-1})$ holds for all i. Hence the Cartan matrix is

$$C = n \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \cdots & \cdots & \cdots & \cdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}.$$

4.3. *Restricted Enveloping Algebras of Completely Solvable p-Lie Algebras*

Let $H = u(\mathfrak{g})$ be the restricted enveloping algebra of the finite-dimensional completely solvable restricted p-Lie algebra $(\mathfrak{g}, [p])$ over an algebraically closed field $\Bbbk$ of characteristic $p > 2$. If the p-map $[p]$ is normalized so as to be trivial on the center of $\mathfrak{g}$, then $\mathfrak{g} = \mathfrak{t} \oplus \mathfrak{r}$, where $\mathfrak{r} = \mathrm{rad}_p(\mathfrak{g})$ is the p-radical of $\mathfrak{g}$ and $\mathfrak{t}$ is a maximal torus. Furthermore, $J = \mathfrak{r}H$ and $H/J \cong u(\mathfrak{t})$ is commutative. (See [SF, pp. 240 ff. and Theorem 5.3, p. 221] for all this.) In particular, by Section 3.1, Remarks and Examples (3), there is an isomorphism

$$G_0(H) \cong \mathbb{Z}G, \qquad [\Bbbk_\alpha] \mapsto \alpha \ (\alpha \in G),$$

where G is the group of group-like elements of H^*, written multiplicatively. Note that G is canonically isomorphic to $\{\alpha \in \mathfrak{g}^* | \alpha([\mathfrak{g}, \mathfrak{g}]) = 0,\ \alpha(x^{[p]}) = \alpha(x)^p\ \forall x \in \mathfrak{g}\}$, and hence G is an elementary abelian p-group of rank $\dim_\Bbbk \mathfrak{t}$ (cf. [SF, Proposition 8.8 and Exercise 4, p. 243]). So

$$|G| = p^g \qquad \text{with } g = \dim_\Bbbk \mathfrak{t}.$$

Putting $T = u(\mathfrak{t})$ and $R = u(\mathfrak{r})$, we have $H \cong R \otimes T$ as $\Bbbk$-vector spaces, by the restricted Poincaré–Birkhoff–Witt Theorem [SF, Theorem 5.1]. Choose an integral $e \in T$ with $\varepsilon(e) = 1$. Then e is idempotent, and

$$P(\Bbbk_\varepsilon) = He = Re \cong R$$

as H-modules, viewing R as H-module by means of the left adjoint representation ad_l that is given by $(\mathrm{ad}_l h)(r) = \sum h_1 r S(h_2)$. (The isomorphism follows from the calculation $hre = \sum h_1 r \varepsilon(h_2) e = \sum h_1 r \varepsilon(Sh_2) e = \sum h_1 r S(h_2) e$.) In particular,

$$\dim_\Bbbk P(\Bbbk_\varepsilon) = p^r \qquad \text{with } r = \dim_\Bbbk \mathfrak{r}.$$

In order to determine $c([P(\Bbbk_\varepsilon)]) \in G_0(H)$, it suffices to analyze R as a T-module. To this end, decompose $\mathfrak{r}$ as a T-module. This amounts to choosing a basis $\{x_1, \ldots, x_r\}$ of $\mathfrak{r}$ such that $(\mathrm{ad}_l y)(x_i) = \alpha_i(y) x_i$ holds for all $y \in \mathfrak{t}$, where $\alpha_i \in \mathfrak{t}^*$ are suitable linear forms. We will view the α_i as elements of G by inflation and call them the *Jordan–Hölder values* of $\mathfrak{g}$ in $\mathfrak{r}$ (following [BGR]). By the PBW Theorem, we have T-module isomorphisms

$$R \cong \Bbbk[x_1] \otimes \Bbbk[x_2] \otimes \cdots \otimes \Bbbk[x_r],$$

$$\Bbbk[x_i] = \bigoplus_{j=0}^{p-1} \Bbbk x_i^j \cong \bigoplus_{j=0}^{p-1} \Bbbk_{j\alpha_i}.$$

Thus, as T-modules,

$$R \cong \bigoplus_{j_1, \ldots, j_r = 0}^{p-1} \Bbbk_{j_1\alpha_1 + \cdots + j_r\alpha_r}.$$

Viewing the α_i as elements of G as above, this isomorphism yields the following equation for $[P(\Bbbk_\varepsilon)] = [R]$ in $G_0(H) = \mathbb{Z}G$:

$$[P(\Bbbk_\varepsilon)] = \sum_{j_1,\dots,j_r=0}^{p-1} \alpha_1^{j_1} \cdots \alpha_r^{j_r}.$$

Let $A \subseteq G$ denote the subgroup that is generated by the Jordan–Hölder values $\{\alpha_i\}$ and let a ($\leq r$) denote the rank of A. Then the above expression for $[P(\Bbbk_\varepsilon)]$ can be written as

$$[P(\Bbbk_\varepsilon)] = p^{r-a}\hat{A}, \qquad \text{where } \hat{A} = \sum_{\alpha \in A} \alpha \in \mathbb{Z}G.$$

By Corollary 3.3, the projective covers of the remaining simple H-modules $\Bbbk_\alpha$ ($\alpha \in G$) are given by $[P(\Bbbk_\alpha)] = [P(\Bbbk_\varepsilon)]\alpha$. Consequently, the Cartan matrix C has the form

$$C = p^{r-a} \cdot \begin{pmatrix} B & & \\ & \ddots & \\ & & B \end{pmatrix}_{p^{g-a} \times p^{g-a}} \qquad \text{with } B = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}_{p^a \times p^a}.$$

We briefly discuss some explicit examples.

(1) *The* 2*-Dimensional Solvable p-Lie Algebra*. This Lie algebra is defined by $\mathfrak{g} = \Bbbk t \oplus \Bbbk x$ with $[t, x] = x$, $t^{[p]} = t$, $x^{[p]} = 0$. Here, $\mathfrak{t} = \Bbbk t$, $\mathfrak{r} = \Bbbk x$, and $G = A = \langle \alpha \rangle$ with $\alpha(t) = 1$, $\alpha(x) = 0$. This is also the only Jordan–Hölder value of $\mathfrak{g}$ in $\mathfrak{r}$. So $g = r = a = 1$ and we obtain

$$[P(\Bbbk_\varepsilon)] = \hat{G} \in \mathbb{Z}G \qquad \text{and} \qquad C = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}_{p \times p}.$$

(2) *The Diamond Algebra*. Here, $\mathfrak{g} = \Bbbk t \oplus \Bbbk x \oplus \Bbbk y \oplus \Bbbk z$ with $[t, x] = x$, $[t, y] = -y$, $[x, y] = z$, $[\mathfrak{g}, z] = 0$, and $t^{[p]} = t$, $x^{[p]} = y^{[p]} = z^{[p]} = 0$. Again, $\mathfrak{t} = \Bbbk t$, $\mathfrak{r} = \Bbbk x \oplus \Bbbk y \oplus \Bbbk z$, and $G = A = \langle \alpha \rangle$ with $\alpha(t) = 1$, $\alpha(x) = \alpha(y) = \alpha(z) = 0$. The Jordan–Hölder values in $\mathfrak{r}$ are α, $-\alpha$, and 0. Thus $g = a = 1$, $r = 3$, and so

$$[P(\Bbbk_\varepsilon)] = p^2\hat{G} \in \mathbb{Z}G \qquad \text{and} \qquad C = p^2 \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}_{p \times p}.$$

4.4. *The Restricted Enveloping Algebra of* $sl(2, \Bbbk)$ (*cf*. [Po])

We now consider the restricted enveloping algebra $H = u(\mathfrak{g})$ of the p-Lie algebra $\mathfrak{g} = sl(2, \Bbbk)$ over a field $\Bbbk$ of characteristic $p > 2$. Thus $\mathfrak{g} = \Bbbk f \oplus \Bbbk h \oplus \Bbbk e$, with $[h, f] = -2f$, $[h, e] = 2e$, $[e, f] = h$, and the p-map is given by $e^{[p]} = f^{[p]} = 0$, $h^{[p]} = h$. Let $V = \Bbbk a \oplus \Bbbk b$ denote the canonical $\mathfrak{g}$-module that is given by the matrices

$$h_V = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad e_V = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad f_V = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

The symmetric group $\mathscr{S}_m$ acts on the m-fold tensor product $V^{\otimes m}$ by permuting positions, and this action commutes with the H-action on $V^{\otimes m}$, since H is cocommutative. Thus the $\mathscr{S}_m$-fixed points form an H-submodule of $V^{\otimes m}$ which we denote by $V(m)$:

$$V(m) = (V^{\otimes m})^{\mathscr{S}_m}.$$

By [Bou, Proposition 4 on p. IV.44],

$$\dim_{\Bbbk} V(m) = m + 1.$$

The modules $V(m)$ $(0 \leq m < p)$ form a complete set of irreducible H-modules, and they are in fact absolutely irreducible (cf. [C] or [SF, p. 207 ff.]). Furthermore, all $V(m)$ $(0 \leq m < p)$ are self-dual, by uniqueness of dimension. Note that $V(0) = \Bbbk_\varepsilon$ and $V(1) = V$. In the following, we will write $v_m = [V(m)] \in G_0(H)$ and $v = [V] \in G_0(H)$. Thus $v_0 = 1$ and

$$G_0(H) = \bigoplus_{m=0}^{p-1} \mathbb{Z} v_m \cong \mathbb{Z}^p.$$

The Ring Structure of $G_0(H)$. Identifying $\mathscr{S}_{m-1}$ with the subgroup $\mathrm{Stab}_{\mathscr{S}_m}(m) \subseteq \mathscr{S}_m$ we have $(V^{\otimes m})^{\mathscr{S}_{m-1}} = V(m-1) \otimes V$ which shows that $V(m)$ is a submodule of $V(m-1) \otimes V$ for all m. Furthermore, if $m \geq 2$ then $V(m-1) \otimes V$ contains the element $x = (m-1)! a^{\otimes m-1} \otimes b - \sum_{\sigma \in \mathscr{S}_{m-1}} (b \otimes a^{\otimes m-1})^\sigma$ which satisfies $hx = (m-2)x$, $ex = 0$, and $f^{m-1}x = 0$. It follows that, for $2 \leq m < p + 2$, Hx is the simple module $V(m-2)$. For $m < p$, the submodules $V(m-2)$ and $V(m)$ of $V(m-1) \otimes V$ intersect trivially, and so $V(m-1) \otimes V = V(m) \oplus V(m-2)$ if $2 \leq m < p$, by counting dimensions. For $m = p$, the element $y = a^{\otimes p} \in V(p)$ satisfies $hy = py = 0 = ey$, and the element x belongs to $V(p)$, since $(p-1)! = -1$ mod p. Therefore, $V(p)$ has $V(p-2)$ and $V(0)$ as composition factors, and there must be another copy of $V(0)$, for dimension reasons. Since

$V(p) \subseteq V(p-1) \otimes V$, we conclude that $V(p-1) \otimes V$ has two copies of each of $V(0)$ and at least one copy of $V(p-2)$ as composition factors. There actually is a second copy of $V(p-2)$. For,

$$\begin{aligned} &\operatorname{Hom}_H(V(p-1) \otimes V, V(p-2)) \\ &\quad \cong \operatorname{Hom}_H(V(p-1), V(p-2) \otimes V) \\ &\quad = \operatorname{Hom}_H(V(p-1), V(p-1) \oplus V(p-3)) \end{aligned}$$

shows that there is an epimorphism $\pi \colon V(p-1) \otimes V \twoheadrightarrow V(p-2)$, and π does not split, because $V(p-1) \otimes V$ is projective while $V(p-2)$ is not (see below).

Summarizing, we have shown that the following equations hold in $G_0(H)$:

$$\begin{aligned} v_0 \cdot v &= v_1, \\ v_{m-1} \cdot v &= v_m + v_{m-2} \qquad (2 \le m < p), \\ v_{p-1} \cdot v &= 2v_{p-2} + 2v_0. \end{aligned}$$

It follows easily by induction that $\sum_{i=0}^{m} \mathbb{Z} v_i = \sum_{i=0}^{m} \mathbb{Z} v^i$ holds for all $m = 0, \dots, p-1$. In particular,

$$G_0(H) = \mathbb{Z}[v] \cong \mathbb{Z}[X]/(g(X)),$$

where $g(X)$ is the characteristic polynomial of the $p \times p$-matrix of the endomorphism of $G_0(H) = \mathbb{Z}^p$ that is given by multiplication with v. One can show that

$$g(X) = (2 - X) f_p(X)^2,$$

where

$$f_p(X) = \sum_{k=0}^{(p-1)/2} (-1)^{a_{p,k}} \binom{k + a_{p,k}}{a_{p,k}} X^k, \qquad a_{p,k} = \left\lfloor \frac{1}{4}(p - 1 - 2k) \right\rfloor.$$

Consequently, $G_0(H)$ is not a semiprime ring. We also remark that $f_p(X)$ is irreducible and satisfies $f_p(X) = (X-2)^{(p-1)/2} \bmod p$. In particular:

$$C(H)_{\text{reg}} \cong k[X]/\big((X-2)^p\big) \cong kC_p,$$

where C_p is the cyclic group of order p.

The Principal Indecomposable Modules. We now discuss the projective covers

$$P(m) = P(V(m)) \qquad (0 \le m < p).$$

By Theorem 2.3(b), we know that $\dim_{\Bbbk} P(m) = pl_m$ for some $l_m \in \mathbb{N}$. In particular, if $m < p-1$ then $V(m)$ is not projective, and consequently $P(m)$ has at least two constituents $V(m)$, one in the head and another one in the socle. (Recall that H is a symmetric algebra.) This forces $\dim_{\Bbbk} P(m) \geq 2(m+1)$. Thus, if $(p-1)/2 \leq m < p-1$ then we must have $l_m \geq 2$. Furthermore, using the isomorphism $V(m) \otimes V \cong V(m+1) \oplus V(m-1)$ for $1 \leq m < p-1$, we see that the projective module $P(m) \otimes V$ maps onto $V(M+1) \oplus V(m-1)$, and hence $P(m+1) \oplus P(m-1)$ is a direct summand of $P(m) \otimes V$. This implies $l_{m+1} + 1 \leq 2l_m$, and it follows by induction that $l_m \geq 2$ holds for all $m < p-1$. On the other hand, since $\Bbbk$ is a splitting field for H, we have an isomorphism

$$H \cong \bigoplus_{m=0}^{p-1} P(m)^{m+1}.$$

Counting dimensions, we conclude that $l_m = 2$ for $m < p-1$ and $l_{p-1} = 1$. Thus

$$\dim_{\Bbbk} P(m) = 2p \quad (0 \leq m < p-1) \quad \text{and} \quad P(p-1) \cong V(p-1).$$

In particular, $V(p-1)$ is the only projective module of dimension p. Since the projective module $V(p-1) \otimes V$ maps onto $V(p-2)$, we have

$$P(p-2) \cong V(p-1) \otimes V.$$

Using the fact that $P(m+1) \oplus P(m-1)$ is a direct summand of $P(m) \otimes V$ for $1 \leq m < p-1$, we obtain the following isomorphisms

$$P(m) \otimes V \cong P(m+1) \oplus P(m-1) \qquad (1 \leq m < p-2)$$

$$P(p-2) \otimes V \cong P(p-3) \oplus V(p-1)^2.$$

Put $a_m = [P(m)] \in K_0(H)$, so $a_0, a_1, \ldots, a_{p-1}$ is the canonical $\mathbb{Z}$-basis of $K_0(H)$. An easy induction shows that $a_{p-1} = [V(p-1)]$ generates $K_0(H)$ as $G_0(H)$-module, and so $K_0(H)$ is free over $G_0(H)$.

The Cartan Map. We claim that the Cartan map $c\colon K_0(H) \to G_0(H)$ is given by

$$c(a_{p-1}) = v_{p-1}$$

$$c(a_m) = 2v_m + 2v_{p-2-m} \qquad (0 \leq m < p-1).$$

Indeed, the first formula is clear from $P(p-1) \cong V(p-1)$, and the second formula for $m = p-2$ follows from $P(p-2) \cong V(p-1) \otimes V$ which implies $c(a_{p-2}) = v_{p-1}v = 2v_{p-2} + 2v_0$. For $m = p-3$, we use the isomorphism $P(p-2) \otimes V \cong P(p-3) \oplus V(p-1)^2$ to obtain

$c(a_{p-3}) = c(a_{p-2})v - 2v_{p-1} = (2v_{p-2} + 2v_0)v - 2v_{p-1} = 2(v_{p-1} + v_{p-3}) + 2v - 2v_{p-1} = 2v_{p-3} + 2v_1$, as required. The assertion for the remaining $0 \leq m < p - 3$ now follows by induction, based on the isomorphism $P(m + 1) \otimes V \cong P(m + 2) \oplus P(m)$, or $c(a_m) = c(a_{m+1})v - c(a_{m+2})$. Therefore, the Cartan matrix has the form

$$C = \begin{pmatrix} 2 & 0 & \cdots & 0 & 2 & 0 \\ 0 & 2 & \cdots & 2 & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 2 & \cdots & 2 & 0 & 0 \\ 2 & 0 & \cdots & 0 & 2 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}_{p \times p} .$$

Loewy Series. The Loewy series of the principal indecomposable modules $P(m)$ $(0 \leq m < p - 1)$ follows easily. Indeed, the head $P(m)/JP(m)$ and the socle $\operatorname{ann}_{P(m)}(J)$ are both isomorphic to $V(m)$, and the core $JP(m)/\text{socle } P(m)$ consists of two copies of $V(p - 2 - m)$. It follows that $\operatorname{Ext}_H(V(m), V(m)) = 0$ for $0 \leq m < p - 1$ (and of course also for the projective module $V(p - 1)$), and hence the core of $P(m)$ must actually be isomorphic with $V(p - 2 - m) \oplus V(p - 2 - m)$. Thus, for $0 \leq m < p - 1$, we have

$$P(m) = \begin{array}{c} V(m) \\ V(p - 2 - m) \quad \bigoplus \quad V(p - 2 - m) \\ V(m) \end{array}.$$

Consequently, the radical $J = \operatorname{rad} H$ has nilpotence index 3. This could of course also be checked using the explicit generators $e^{p-1}(h + 1)$ and $(h + 1)f^{p-1}$ for J that are given in [Se, p. 99].

REFERENCES

[Ba1] H. Bass, "Algebraic *K*-Theory," Benjamin, New York, 1968.

[Ba2] H. Bass, Euler characteristics and characters of discrete groups, *Invent. Math.* **35** (1976), 155–196.

[BGR] W. Borho, P. Gabriel, and R. Rentschler, Primideale in Einhüllenden auflösbarer Lie Algebren, Lecture Notes in Math., Vol. 357, Springer-Verlag, Berlin/Heidelberg/New York, 1973.

[Bou] N. Bourbaki, "Algèbre," Chaps. 1–3 and 4–7, Hermann and Masson, Paris, 1970, 1981.

[Br] P. Brockhaus, "Das Radikal einer Gruppenalgebra," Ph.D. thesis, University of Essen, 1982.

[C] C. W. Curtis, Representations of Lie algebras of classical type with applications to linear groups, *J. Math. Mech.* **9** (1960), 307–326.

[CR] C. W. Curtis and I. Reiner, "Methods of Representation Theory," Vol. 1, Wiley–Interscience, New York, 1981.

[Dr] V. G. Drinfeld, On almost commutative Hopf algebras, *Leningrad Math. J.* **1** (1990), 321–342.

[H] J. E. Humphreys, Projective modules for SL$(2, q)$, *J. Algebra* **25** (1973), 513–518.

[H2] J. E. Humphreys, Symmetry for finite dimensional Hopf algebras, *Proc. Amer. Math. Soc.* **68** (1978), 143–146.

[K] I. Kaplansky, "Bialgebras," Univ. of Chicago Press, Chicago, 1975.

[La] P. Landrock, "Finite Group Algebras and Their Modules," LMS Lect. Notes Series, Vol. 84, Cambridge Univ. Press, Cambridge, UK, 1983.

[L] R. G. Larson, Characters of Hopf algebras, *J. Algebra* **17** (1971), 352–368.

[LR] R. G. Larson and D. E. Radford, Finite dimensional cosemisimple Hopf algebras in characteristic 0 are semisimple, *J. Algebra* **117** (1988), 267–289.

[LR2] R. G. Larson and D. E. Radford, Semisimple cosemisimple Hopf algebras, *Amer. J. Math.* **109** (1987), 187–195.

[LS] R. G. Larson and M. E. Sweedler, An associative orthogonal bilinear form for Hopf algebras, *Amer. J. Math.* **91** (1969), 75–93.

[M] R. K. Molner, Tensor products and semisimple modular representations of finite groups and restricted Lie algebras, *Rocky Mountain J. Math.* **11** (1981), 581–591.

[Mo] S. Montgomery, "Hopf Algebras and Their Actions on Rings," CBMS Regional Conf. Series in Math. No. 82, Amer. Math. Soc., Providence, RI, 1993.

[OS] U. Oberst and H.-J. Schneider, Über Untergruppen endlicher algebraischer Gruppen, *Manuscripta Math.* **8** (1973), 217–241.

[P] D. S. Passman, "The Algebraic Structure of Group Rings," Wiley, New York, 1977.

[PQ] D. S. Passman and D. Quinn, Burnside's theorem for Hopf algebras, *Proc. Amer. Math. Soc.* **123** (1995), 327–333.

[PQ2] D. S. Passman and D. Quinn, Involutory Hopf algebras, *Trans. Amer. Math. Soc.* **347** (1995), 2657–2668.

[Po] R. D. Pollack, Restricted Lie algebras of bounded type, *Bull. Amer. Math. Soc. (N.S.)* **74** (1968), 326–331.

[R] D. E. Radford, The trace function and Hopf algebras, *J. Algebra* **163** (1994), 583–622.

[R2] D. E. Radford, Minimal quasitriangular Hopf algebras, *J. Algebra* **157** (1993), 285–315.

[R3] D. E. Radford, The order of the antipode of a finite dimensional Hopf algebra is finite, *Amer. J. Math.* **98** (1976), 333–355.

[Sch] J. R. Schue, Symmetry for the enveloping algebra of a restricted Lie algebra, *Proc. Amer. Math. Soc.* **16** (1965), 1123–1124.

[Se] G. B. Seligman, "Modular Lie Algebras," Springer-Verlag, New York, 1967.

[Ser] J.-P. Serre, Groupes de Grothendieck des schémas en groupes réductifs déployés, *Publ. IHES* **34** (1968), 37–52.

[SF] H. Strade and R. Farnsteiner, Modular Lie Algebras and Their Representations, Dekker, New York/Basel, 1988.

[Sw] M. Sweedler, "Hopf Algebras," Benjamin, New York, 1969.

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

[V] D. Voigt, Induzierte Darstellungen in der Theorie der endlichen algebraischen Gruppen, Lecture Notes in Math., Vol. 592, Springer-Verlag, Berlin/Heidelberg/New York, 1977.

[Zhu] Yongchang Zhu, Hopf algebras of prime dimension, *Internat. Math. Res. Notices* **1** (1994), 53–59.