JOURNAL OF ALGEBRA 85, 410–423 (1983)

Nilpotent Elements in Integral Representation Rings of Hopf-Algebra Orders in Group Algebras of Prime Order

A. L. JENSEN

Department of Mathematics, Mundelein College, Chicago, Illinois 60660

Communicated by I. N. Herstein

Received December 11, 1981; revised July 5, 1982

In this paper we shall find necessary and sufficient conditions for integral representation rings of Hopf-algebra orders to have non-zero nilpotent elements, when the order is a module over a discrete valuation ring, and an order in a group of prime order.

1. INTRODUCTION

Let R be a discrete valuation ring of characteristic 0 with field of quotients K. Let $A(\mu, \eta, \Delta, \varepsilon)$ be a Hopf-algebra over R. A is called a Hopf-algebra order in a Hopf-algebra H over K if $K \otimes_R A \simeq H$. An element Λ of A is called a left integral if $a\Lambda = \varepsilon(A)\Lambda$ for all $a \in A$. Let L_A be the ideal of all left integrals in A. The ideal $\varepsilon(L_A)$ gives much information on the structure of H and A. It plays a role similar to that played by the order of the group in the representation theory of a finite group. In fact, it is always a divisor of $\dim H$. R. G. Larson [6] has used properties of $\varepsilon(L_A)$ to apply the theory of Hopf-algebra orders to the representation theory of finite groups and has obtained a new bound on the degrees of the absolutely irreducible representations of a finite group.

Integral representation theory developed from matrix representation of associative algebras and number theory, especially from ideal theory. Methods of homological algebra have played an increasingly important role in recent years.

By definition all integral representation rings are free Z-modules. Let M denote a finitely generated A-module which is R-torsion free. Let $[M]$ denote the isomorphim class of the A-module M. The integral representation ring ${}_A\mathcal{J}$ is the free Abelian group with generators $[M]$, addition defined by $[M] + [N] = [M \oplus N]$ and multiplication defined by $[M][N] = [M \otimes N]$. The action of A on $M \otimes N$ is given by $a(m \otimes n) = \sum a_{(1)}m \otimes a_{(2)}n$.

0021-8693/83 $3.00

I. Reiner [7–9] has shown that when G is a cyclic group of order n, R has maximal ideal P and the Krull–Schmidt theorem holds for RG-modules, then ${}_{RG}\mathscr{J}$ contains at least one non-zero nilpotent element if $n \in P^2$. If $n \notin P^2$ then ${}_{RG}\mathscr{J}$ contains no non-zero nilpotent element.

Let p be a fixed rational prime and A a Hopf-algebra order in KZ_p. We show in this paper that if p is odd then ${}_A\mathscr{J}$ contains a non-zero nilpotent element if $\varepsilon(L_A) \subseteq P^2$, and ${}_A\mathscr{J}$ contains no non-zero nilpotent elements if $\varepsilon(L_A) \not\subseteq P^2$. This is a generalization of Reiner's result for $n = p$, since for the group ring RG, $\varepsilon(L_{RG}) = pR$, the ideal generated by the order of the group.

Tate and Oort [13] have shown that when A is a Hopf-algebra order in KZ_p and $P = (\Pi)$, then A has a basis $\{1, X, X^2, \ldots, X^{p-1}\}$, where $X^p = \omega_p \Pi^\alpha X$ for some $\alpha \geqslant 0$ and some ω_p, a unit in R. We shall refer to this basis as the "Tate Oort basis." It will be used throughout this paper. The ideal of integrals in A is a rank 1 free R-module with basis $\Lambda_A = X^{p-1} - \omega_p \Pi^\alpha$ and $\varepsilon(\Lambda_A) = -\omega_p \Pi^\alpha$.

R is assumed to be a discrete valuation ring of characteristic 0 with maximal ideal P, field of quotients K and residue class field k.

All A-modules are assumed to be finitely generated torsion-free R-modules. K is assumed to be a splitting field for G, and so the Krull–Schmidt theorem holds for A-modules [1].

2. The Case Where p Is Odd and $\varepsilon(L_A) \subseteq P^2$

In this section we prove that ${}_A\mathscr{J}$ contains a non-zero nilpotent element if $\varepsilon(L_A) \subseteq P^2$. We shall use the following test due to I. Reiner [7] when a non-zero element is nilpotent.

Lemma 2.1. *If X and Y are a pair of nonisomorphic A-modules satisfying $PA \subseteq X \subseteq A$, $PA \subseteq Y \subseteq A$ and $X/PX \simeq Y/PY$ as A/PA-modules, then $[X] - [Y]$ is a non-zero nilpotent element of ${}_A\mathscr{J}$.*

Theorem 2.2. *Let p be an odd prime and let A be a Hopf-algebra order in KZ_p. ${}_A\mathscr{J}$ contains a non-zero nilpotent element if $\varepsilon(L_A) \subseteq P^2$.*

Proof. We shall construct an element that satisfies the conditions of Lemma 2.1. Let X be the Tate–Oort generator for A. Since $\varepsilon(L_A) \subseteq P^2$ we have that $X^p = \omega_p \Pi^\alpha X$, where $\alpha \geqslant 2$. Let $M = A^+ + \Pi A$, where A^+ is the augmentation ideal of A. M has an R-basis $m_1 = X$, $m_2 = X^2, \ldots, m_{p-1} = X^{p-1}$, $m_p = \Pi$. Let $N = R\Lambda + \Pi A$, where Λ is the integral of A. N has an R-basis $n_1 = \Pi$, $n_2 = \Pi X, \ldots, n_{p-1} = \Pi X^{p-2}$, $m_p = \Lambda$.

Observe that $PA \subseteq M \subseteq A$ and $PA \subseteq N \subseteq A$. Let $\bar{M}$ denote M/PM and $\bar{N}$ denote N/PN. By Lemma 2.1, to show $[M] - [N]$ is a non-zero nilpotent element of ${}_A\mathscr{J}$ we have to show that (a) $\bar{M} \simeq \bar{N}$ and (b) $M \not\simeq N$. To prove

this consider the action of X on M. With respect to the given basis this is given by

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & \omega_p \Pi^{\alpha} & \Pi \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}_{p \times p}.$$

This shows that $\bar{M} = \bar{U} \oplus \bar{R}\bar{m}_p$, where $\bar{X}\bar{m}_p = 0$ and $\bar{U} = \sum_{i=1}^{p-1} \bar{R}\bar{m}_i$; moreover, $\bar{X}\bar{m}_i = \bar{m}_{i+1}$ for $1 \leqslant i \leqslant p-2$ and $\bar{X}\bar{m}_{p-1} = 0$, since $\alpha \geqslant 2$.

The action of X on N with respect to the given basis is given by

$$\begin{pmatrix} 0 & 0 & \cdots & \omega_p \Pi^{\alpha+1} & 0 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & \Pi & 0 \end{pmatrix}_{p \times p}.$$

Hence $\bar{N} = \bar{W} \oplus \bar{R}\bar{n}_p$, where $\bar{X}\bar{n}_p = 0$, $\bar{W} = \sum_{i=1}^{p-1} \bar{R}\bar{n}_i$, $\bar{X}\bar{n}_i = \bar{n}_{i+1}$ for $1 \leqslant i \leqslant p-2$ and $\bar{X}\bar{n}_{p-1} = 0$. So $\bar{M} \simeq \bar{N}$ and (a) has been proved. We must show that M and N are not isomorphic as A-modules.

Now $U = \sum_{i=1}^{p-1} Rm_i$ is an R direct summand of M and M/U is isomorphic to the trivial A-module. Suppose we have constructed a submodule V of N such that V is an R-direct summand of N, $N/V \simeq R$ and $K \otimes_R V \simeq K \otimes_R U$.

U is the augmentation ideal of A, hence $\mathrm{Hom}_A(U, R) = 0$. Let φ be any A-module homomorphism from M to N and consider the following diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U & \xrightarrow{i} & M & \longrightarrow & R & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle \varphi} & & & & \\ 0 & \longrightarrow & V & \longrightarrow & N & \xrightarrow{\Pi} & R & \longrightarrow & 0 \end{array}$$

Here $\pi\varphi i = 0$ since $\mathrm{Hom}_A(U, R) = 0$. Therefore φ induces $\varphi' : U \to V$ and $\varphi'' : R \to R$ such that the following diagram commutes:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U & \xrightarrow{i} & M & \longrightarrow & R & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi'} & & \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi''} & & \\ 0 & \longrightarrow & V & \longrightarrow & N & \longrightarrow & R & \longrightarrow & 0 \end{array}$$

By the 5-lemma, φ is an isomorphism if and only if φ' and φ'' are isomorphisms. In particular, if $M \simeq N$ as A-modules then $U \simeq V$ as A-modules and $\bar{U} \simeq \bar{V}$ as $\bar{A}$-modules. We shall now show that $\bar{U}$ is not isomorphic to $\bar{V}$ by showing that the trivial $\bar{A}$-module $\bar{R}$ is not an $\bar{A}$-direct sum of $\bar{U}$, but we shall construct $\bar{V}$ such that $\bar{R}$ is an $\bar{A}$-direct summand of $\bar{V}$.

Looking at the representation of $\bar{U}$ it is obvious that $\bar{U}$ has no proper direct summands by the uniqueness of the Jordan canonical form.

Now let V be the R-module with basis

$$v_1 = \Pi X, \qquad v_2 = \Pi X^2, \ldots, \qquad v_{p-2} = \Pi X^{p-2},$$
$$v_{p-1} = A + \omega_p \Pi^\alpha = X^{p-1}.$$

V is R-pure and R is a principal ideal domain, hence V is an R-direct summand of N. $K \otimes_R V$ is the augmentation ideal of KG, so $K \otimes_R V \simeq K \otimes_R U$ and $N/V \simeq R$ since $K \otimes N/V \simeq K \otimes N/K \otimes V \simeq KG/K \otimes U \simeq K$. We see that

$$Xv_i = v_{i+1} \qquad \text{for} \quad 1 \leqslant i \leqslant p-3,$$
$$Xv_{p-2} = \Pi X^{p-1} = \Pi v_{p-1},$$
$$Xv_{p-1} = X^p = \omega_p \Pi^\alpha X = \omega_p \Pi^{\alpha-1} v_1.$$

Therefore, since $\alpha > 2$ $\overline{Xv}_{p-1} = 0$ and $\bar{V} = \sum_{i=1}^{p-2} \bar{R}v_i \oplus \bar{R}v_{p-1}$, i.e., the trivial $\bar{A}$-module $\bar{R}$ is a direct summand of $\bar{V}$, so $\bar{V} \not\simeq \bar{U}$, i.e., $N \not\simeq M$. This concludes the proof of (b). Hence N and M satisfy the conditions for Lemma 2.1 and we may conclude that $[M] - [N]$ is a non-zero nilpotent element of ${}_A\mathscr{S}$.

3. The Case Where p Is Odd and $\varepsilon(L_A) \supseteq P$

We show that if p is an odd prime, and A is a Hopf-algebra order in KZ_p, then ${}_A\mathscr{S}$ contains no non-zero nilpotent elements when $\varepsilon(L_A) \supset P$. In the case where $\varepsilon(L_A) = P$ we shall first find all indecomposable A-modules. If $\varepsilon(L_A) = P = \Pi R$, and X is the Tate–Oort generator for A, then $X^p = \omega_p \Pi X$ and $A \simeq R[X]/(X^p - \omega_p \Pi X)$. Let S denote the ring $R[X]/(X^{p-1} - \rho)$, where $\rho = \omega_p \Pi$.

LEMMA 3.1. *Let $S = R[X]/(X^{p-1} - \rho)$ and let M be a R-free S-module. If m is a non-zero element of M then $m, mX, \ldots, mX^{p-2}$ are R-linearly independent.*

Proof. Suppose $0 = \sum_{i=0}^{p-2} a_o m X^i = m \sum_{i=0}^{p-2} a_i X^i$ for some $a_i \in R$. View $\sum_{i=0}^{p-2} a_i X^i$ as an element of $K \otimes_R S$. $K \otimes_R S$ is a field since $X^{p-1} - \rho$ is

irreducible by Eisenstein's criterion. Hence $m \cdot \sum_{i=2}^{p-2} a_i X^i = 0$ and $m \neq 0$ implies $a_i = 0$ for all $i = 0,..., p-2$, so $m, mX,..., mX^{p-2}$ are R-linearly independent.

Notation. Let M be a R-free S-module. For $\tilde{m} \in M$, let N_m denote a maximal S-submodule of M subject to the conditions that $\tilde{m} \in N_m$ and N_m has a R-basis of the form $m, mX,..., mX^{p-2}$ for some $m \in N$. Note that $\tilde{m}$ is not necessarily equal to m, for example, if $\tilde{m} = rm$, $r \in R$, $m \in N$, then in order to get the maximal submodule we must choose the basis $m, mX,..., mX^{p-2}$ instead of $\tilde{m}, \tilde{m}X,..., \tilde{m}X^{p-2}$.

LEMMA 3.2. *Let N_m be as above. N_m is an R-direct summand of M.*

Proof. Since R is a principal ideal domain we must show that N_m is R-pure. It suffices to show that for any $m' \in M$, $\Pi m' \in N_m$ implies that $m' \in N_m$. So choose $m' \in M$ such that $\Pi m' \in N_m$. Since $\Pi m' \in N_m$ there are elements α_i of K for $0 \leqslant i \leqslant p-2$ such that

$$m' = \sum_{i=0}^{p-2} \alpha_i m X^i. \qquad (*)$$

Since R is a discrete valuation ring we may assume that each α_i is of the form $\alpha_i = u_i/\Pi$ or $\alpha_i = r_i$, where u_i is a unit in R and $r_i \in R$. If $\alpha_i = r_i$ for all i then $m' \in N_m$ and the lemma is proved.

We shall prove this by contradiction. Suppose α_i is not in R for some i, and let i_0 be the smallest i with $\alpha_i \notin R$, i.e., $\alpha_0,..., \alpha_{i-1}$ are in R and $\alpha_i = u_i/\Pi$. Using $(*)$ we get

$$X^{p-2-i}m' = \alpha_{i+1} m\rho + \alpha_{i+2} m\rho X + \cdots + \alpha_{p-2} m\rho X^{p-3-i} + \alpha_0 m X^{p-2-i} + \cdots + \alpha_i m X^{p-2}$$

and we let

$$v = X^{p-2-i}m' - \alpha_{i+1} m\rho - \alpha_{i+2} mX\rho - \cdots - \alpha_{i-1} mX^{p-3} = \alpha_i m X^{p-2}.$$

$v \in M$ since $\Pi\alpha_j \in R$ and $\alpha_0 \cdots \alpha_{i-1}$ are elements of R. $Xv = X\alpha_i mX^{p-2} = \alpha_i m\rho = \omega_p u_i m$. Hence m is an element of the S-submodule V of M generated by v. But $v = (u_i/\Pi) mX^{p-2} \notin N_m$, therefore $N_m \not\subseteq V$. This contradicts the maximality of N_m, so we conclude that $\alpha_i \in R$. This proves Lemma 3.2.

PROPOSITION 3.3. *Let M be an R-free S-module. Then M is a free S-module.*

Proof. The proof is by induction on the R-rank of M. Assume that the R-rank of M is less than or equal to $p-1$. Take $0 \neq \tilde{m} \in M$. Then $\tilde{m}, \tilde{m}X,...,$

$\tilde{m}X^{p-2}$ are R-linearly independent, so the R-rank of M is $p-1$: Using Lemma 3.2 we see that for some $m \in M$ and some R-submodule U of M, $M = N_m \oplus U$ as R-direct sum, but the R-rank of N_m is $p-1$. Therefore the R-rank of U is zero. Hence $M = N_m$, but $N_m \simeq S$, so M is a free S-module.

Now let the R-rank of M be t, and assume that every R-free S-module with R-rank less than t is S-free. Choose N_m as before, i.e., N_m is a pure R-submodule of M with R-basis $m, mX, \ldots, mX^{p-2}$ for some $m \in M$, and N_m is a S-submodule of M. Hence we have a short exact sequence of S-modules

$$0 \to N_m \to M \to M/N_m \to 0.$$

Let $B = M/N_m$. B is a free R-module since N_m is R-pure. Hence $M \simeq N_m \oplus B$ as R-modules and the R-rank of B is less than the R-rank of M, so by induction $B \simeq \bigoplus^l S$, i.e., B is a free S-module, hence $0 \to N_m \to M \to B \to 0$ splits as S-modules, i.e., $M \simeq N_m \oplus B$ as S-modules, and $M \simeq \bigoplus^{l+1} S$. This proves that M is a free S-module.

PROPOSITION 3.4. *If $\varepsilon(L_A) = \Pi R$ then up to isomorphism the only indecomposable R-free A-modules are the trivial A-module R, the augmentation ideal A^+ and A itself.*

Proof. Since $\varepsilon(L_A) = \Pi R$, $A \simeq R[X]/(X^p - \rho X)$ and $A^+ \simeq R[X]/(X^{p-1} - \rho) = S$, as A-modules.

Let M be an R-free A-module. Set $M' = \{m \in M \mid Xm = 0\}$. M' is a free R-module.

We have a short exact sequence of A-modules $0 \to M' \to M \to M/M' \to 0$. M/M' is a free S-module by Proposition 3.3.

Hence M is an extension of a free R-module by a free S-module. Let us calculate $\mathrm{Ext}^1_A(S, R)$. We have a short exact sequence of A-modules

$$0 \to (X^{p-1} - \rho)A \to A \to A/(X^{p-1} - \rho)A \to 0.$$

So since A is a projective A-module and $A/(X^{p-1} - \rho)A \simeq S$, we have

$$0 \to \mathrm{Hom}_A(S, R) \to \mathrm{Hom}_A(A, R) \to \mathrm{Hom}_A((X^{p-1} - \rho)A, R)$$
$$\to \mathrm{Ext}^1_A(S, R) \to 0$$

is exact. Hence

$$\mathrm{Ext}^1_A(S, R) \simeq \mathrm{Hom}_A((X^{p-1} - \rho)A, R)/\mathscr{J}m(\mathrm{Hom}_A(A, R))$$
$$\simeq R/\rho R \simeq k.$$

Let s be the S-rank of M/M' and r the R-rank of M'. Now [14] $\mathrm{Ext}(M/M', M') \simeq \mathrm{Ext}(\bigoplus^s S, \bigoplus^r R)) \simeq (\mathrm{Ext}(S, R))^{r \times s} = (k)^{r \times s}$, where $(k)^{r \times s}$

denotes r by s matrices with entries in k. Thus M corresponds to an $r \times s$ matrix with entries in k. Also $\mathrm{Hom}_A(R, S) = 0$, since S is isomorphic to the augmentation ideal of A. Hence the isomorphism classes of M's correspond bijectively to isomorphism classes of $r \times s$ matrices with entries in k under the actions of $GL(r, R)$ and $GL(s, \mathrm{Aut}_A(S)) \simeq GL(s, R)$ [10]. Now k is a field so every matrix in $(k)^{r \times s}$ can be diagonalized by elementary row and column operations. Since R is a principal ideal domain each such operation comes from one in $GL(r, R)$ or $GL(s, R)$, so each isomorphism class contains a diagonal matrix. Thus the indecomposable A-modules are R, S and non-split extensions, $M : R \to M \to S$, corresponding to a non-zero $k_0 \in k$. The isomorphism class of M is determined by the isomorphism class of k_0 under the action of the units in R. But k is the residue class field of R, hence there is only one isomorphism class. This isomorphism class corresponds to the non-split extension $A : R \to A \to S$.

In order to find the multiplication table for ${}_A\mathcal{J}$ we need the following lemma and proposition.

LEMMA 3.5. *Let M be an A-module. Assume M has an R-basis of cardinality s. Then $A \otimes_R M \simeq \bigoplus^s A$.*

Note. Lemma 3.5 is valid for any Hopf-algebra order A.

Proof. Let $N_1 = A \otimes_R M$ with A-module action given by

$$b(a \otimes m) = ba \otimes m. \qquad N_1 \simeq \overset{s}{\oplus} A.$$

Let $N_2 = A \otimes_R M$. The A-module action on N_2 is given by $b(a \otimes m) = \sum b_{(1)} a \otimes b_{(2)} m$.

Define $f : N_1 \to N_2$ by $b \otimes m \to \sum b_{(1)} \otimes b_{(2)} m$. The inverse of f, $f^{-1} : N_2 \to N_1$ is given by $b \otimes m \to \sum b_{(1)} \otimes S(b_{(2)})\, m$. Hence $N_1 \simeq N_2$ and $A \otimes_R M \simeq \bigoplus^s A$.

PROPOSITION 3.6. $S \otimes S \simeq \bigoplus^{p-2} A \oplus R$.

Proof. $\bar{A} \simeq k[Y]/(Y^p)$, where k is the residue class field and $\Delta Y = Y \otimes 1 + 1 \otimes Y$. We will compute $S \otimes S$ by computing $\bar{S} \otimes \bar{S}$. We can do this since $S \otimes S$ is a direct sum of indecomposable A-modules, and $\bar{S}$, $\bar{A}$ and k are not isomorphic. Hence

$$S \otimes S = \left(\overset{n}{\oplus} S\right) \oplus \left(\overset{m}{\oplus} R\right) \oplus \left(\overset{t}{\oplus} A\right)$$

if and only if

$$\bar{S} \otimes \bar{S} = \left(\overset{n}{\oplus} \bar{S}\right) \oplus \left(\overset{m}{\oplus} k\right) \oplus \left(\overset{t}{\oplus} \bar{A}\right).$$

Now $\bar{S}$ is the augmentation ideal of $\bar{A}$. Thereore $\bar{S} \otimes \bar{S}$ has a k-basis $Y^s \otimes Y^t$, $1 \leqslant s \leqslant p-1$ and $1 \leqslant t \leqslant p-1$. Let $v_i = Y^i \otimes Y$ for $1 \leqslant i \leqslant p-2$.

Claim:

$$\{Y^j v_i, w \mid 0 \leqslant j \leqslant p-1, 1 \leqslant i \leqslant p-2\},$$

where $w = \sum_{l=1}^{p-1} (-1)^{l+1} Y^l \otimes Y^{p-l}$ is also a k-basis for $\bar{S} \otimes \bar{S}$.

Since $Y \cdot w = 0$ this will prove that $\bar{S} \otimes \bar{S} \simeq \oplus^{p-2} \bar{A} \oplus k$ and hence $S \oplus S \simeq \oplus^{p-2} A \oplus R$.

To prove the claim we must prove that $Y^j v_i$ for $0 \leqslant j \leqslant p-1$, $1 \leqslant i \leqslant p-2$ and $w = \sum_{l=1}^{p-1} (-1)^{l+1} Y^l \otimes Y^{p-l}$ are linearly independent.

$Y^j v_i$ can be expressed in terms of $Y^s \otimes Y^t$, where $s+t = i+j+1$, so it suffices to prove that for fixed c,

(a) $Y^j v_i$ for $j+i+1 = c$ and $2 \leqslant c \leqslant p-1$ are linearly independent,

(b) $Y^j v_i$ for $j+i+1 = p$ and $w = \sum_{l=1}^{p-1} (-1^{l+1} Y^l \otimes Y^{p-l}$ are linearly independent,

(c) $Y^j v_i$ for $j+i+1 = c$ and $p+1 \leqslant c \leqslant 2(p-1)$ are linearly independent.

For (a) the representation of the $Y^{c-i-1} v_i$ for $1 \leqslant i \leqslant c-1$, $2 \leqslant c \leqslant p-1$ in terms of the $Y^k \otimes Y^{c-k}$ for $1 \leqslant k \leqslant c-1$ is given by

$$Y^{c-i-1} v_i = \sum_{k=1}^{c-1} a_{ki} Y^k \otimes Y^{c-k},$$

where

$$a_{ki} = \binom{c-i-1}{c-k-1}, \qquad k \geqslant i,$$

$$= 0, \qquad k < i.$$

Hence the $Y^{c-i-1} v_i$ are linearly independent in case (a).

For (b) the representation of the $Y^{p-i-1} v_i$ for $1 \leqslant i \leqslant p-2$ in terms of $Y^k \otimes Y^{p-k}$ for $1 \leqslant k \leqslant p-1$ is given by

$$Y^{p-i-1} v_i = \sum_{k=1}^{p-1} a_{ik} Y^k \otimes Y^{p-k},$$

where

$$a_{ki} = \binom{p-i-1}{k-i}, \qquad k \geqslant i,$$
$$= 0, \qquad k < i.$$

Obviously $Y^{p-2}v_1$, $Y^{p-3}v_2,\ldots, Yv_{p-2}$ are linearly independent. Hence if w, $Y^{p-2}v_1,\ldots, Yv_{p-2}$ are dependent, then there exists $\alpha_1,\ldots,\alpha_{p-2}$ in k such that $\sum_{i=1}^{p-2}\alpha_i Y^{p-i-1}v_i = w$. Looking at the coefficients of $Y^{p-1}\otimes Y$, this implies that (1) $\sum_{i=1}^{p-2}\alpha_i = p-1$. We shall show by induction that $\alpha_i = 1$ for all i. Hence (1) yields $p-2 = p-1$, which is a contradiction, and we can conclude that w, $Y^{p-2}v_1,\ldots, Yv_{p-2}$ are linearly independent. Clearly $\alpha_1 = 1$. Assume that $\alpha_1 = \alpha_2 = \cdots = \alpha_{i-1} = 1$ and consider

$$\alpha_i + \binom{p-2}{i-1} + \binom{p-3}{i-2} + \cdots + \binom{p-(i-1)}{2} + \binom{p-i}{1}.$$

We will show that

$$\sum_{s=2}^{i}\binom{p-s}{i-s+1} \underset{p}{\equiv} 0 \qquad \text{if } i \text{ is odd},$$
$$\underset{p}{\equiv} -2 \qquad \text{if } i \text{ is even}.$$

Now

$$\binom{p-s}{i-s+1} = \frac{(p-s)!}{(i-s+1)!\,(p-i-1)!}$$
$$= \frac{(p-i)\cdots(p-s)}{(i-s+1)!}$$
$$\underset{p}{\equiv} (-1)^{i-s+1}\frac{i!}{(i-s+1)!\,(s-1)!}$$
$$= (-1)^{i-s+1}\binom{i}{s-1}.$$

Hence

$$\sum_{s=2}^{i}\binom{p-s}{i-s+1} \underset{p}{\equiv} \sum_{s=2}^{i}(-1)^{i-s+1}\binom{i}{s-1}$$
$$= \sum_{t=1}^{i-1}(-1)^{i-t}\binom{i}{t}$$

$$= (-1)^i \sum_{t=0}^{i} (-1)^t \binom{i}{t} - (-1)^i - (-1)^i (-1)^i$$
$$= -(-1)^i - 1$$
$$= -2 \qquad \text{if} \quad i \text{ is even},$$
$$= 0 \qquad \text{if} \quad i \text{ is odd}.$$

Hence if i is even $\alpha_i - 2 \equiv_p p-1$, that is, $\alpha_i \equiv_p 1$, and if i is odd $\alpha_i \equiv_p 1$.

For (c) the representation of the $Y^{c-i-1}v_i$ for $c-p \leqslant i \leqslant p-2$ in terms of $Y^k \otimes Y^{c-k}$ for $c-(p-1) \leqslant k \leqslant p-1$ is given by

$$Y^{c-i-1}v_i = \sum_{k=c-(p-1)}^{p-1} a_{ki} Y^k \otimes Y^{c-k},$$

where

$$a_{ki} = \binom{c-i-1}{k-i}, \qquad k \geqslant i,$$
$$= 0, \qquad k < i.$$

A direct computation shows that

$$\det(a_{ki}) = \frac{(p-1)(p-2)\cdots(p-(2p-c-1))}{(2p-c-1)!},$$

which is clearly different from zero for $c = p+1, p+2, \ldots, 2p-2$. Since the $Y^k \otimes Y^{c-k}$ are linearly independent, this implies that the $Y^{c-i-1}v_i$ are linearly independent. This concludes the proof of Proposition 3.6.

THEOREM 3.7. *Let p be an odd prime and let A be a Hopf-algebra order in KZ_p. ${}_A\mathscr{S}$ contains no non-zero nilpotent elements if $\varepsilon(L_A) \supseteq P$.*

Proof. If $\varepsilon(L_A) = R$, then A is separable [5] and so ${}_A\mathscr{S} = {}_{KG}\mathscr{S}$, which has no nilpotent elements [2].

If $\varepsilon(L_A) = P$, then using Proposition 3.6 and Lemma 3.5 we have the multiplication table for ${}_A\mathscr{S}$ with respect to the Z-basis $[R]$, $[S]$, $[A]$:

	$[R]$	$[S]$	$[A]$
$[R]$	$[R]$	$[S]$	$[A]$
$[S]$	$[S]$	$(p-2)[A]+[R]$	$(p-1)[A]$
$[A]$	$[A]$	$(p-1)[A]$	$p[A]$

$Q \otimes_{Z\,A} \mathcal{J}$ has a basis of orthogonal idempotents $E_1 = 1/p\,[A]$, $E_2 = \frac{1}{2}([R] + [S] - [A])$ and $E_3 = \frac{1}{2}([R] - [S] + (p-2)/p\,[A])$. Therefore $Q \otimes_{Z\,A} \mathcal{J}$ is a commutative semisimple ring. Hence ${}_A\mathcal{J} \subseteq Q \otimes_{Z\,A} \mathcal{J}$ has no non-zero nilpotent elements and the proof of Theorem 3.7 is complete.

4. The Case Where $p = 2$

Let G be the group of order 2 and as before let A be a Hopf-algebra order in KG containing RG, where $\varepsilon(L_A) = \rho R$, $\rho = \omega_2 \Pi^\alpha$. Also let S denote $R[X]/(X - \rho)$. First we classify the indecomposable A-modules. Then we compute the multiplication table for the integral representation ring and, finally, we prove that the integral representation ring has no non-zero nilpotent elements if $p = 2$.

Proposition 4.1. *The R-free indecomposable A-modules are R, S and for each i, $i = 0, 1, \ldots, \alpha - 1$, a module M_i. Note $A = M_0$.*

Proof. Let M be an R-free A-module. Set $M' = \{m \in M \mid Xm = 0\}$. M' is a free R-module. We have a short exact sequence of A-modules $0 \to M' \to M \to M/M' \to 0$.

M/M' is a free S-module, since it is a finitely generated torsion-free R-module and S is isomorphic to R. Hence M is an extension of a free R-module by a free S-module. To calculate $\operatorname{Ext}^1_A(S, R)$ consider the short exact sequence of A-modules

$$0 \to (X - \rho)A \to A \to A/(X - \rho)A \to 0.$$

Now $A/(X - \rho)A \simeq S$ and A is a projective A-module. Hence

$$0 \to \operatorname{Hom}_A(S, R) \to \operatorname{Hom}_A(A, R) \to \operatorname{Hom}_A((X - \rho A, R) \to \operatorname{Ext}^1_A(S, R) \to 0$$

is exact, and

$$\operatorname{Ext}^1_A(S, R) \simeq \operatorname{Hom}_A((X - \rho A, R)/\mathcal{J}m \operatorname{Hom}_A(A, R) \simeq R/\rho R).$$

Let s be the S-rank of M/M' and r the R-rank of M'. Now [14] $\operatorname{Ext}^1_A(M/M', M') \simeq \operatorname{Ext}^1_A(\oplus^s S, \oplus^r R) \simeq (\operatorname{Ext}^1_A(S, R))^{r \times s} = (R/\rho R)^{r \times s}$. $(R/\rho R)^{r \times s}$ denotes r by s matrices with entries in $R/\rho R$. Thus M corresponds to an $r \times s$ matrix with entries is $R/\rho R$. The same argument as the one used in Proposition 3.4 shows that there is a one-to-one correspondence between isomorphism classes of non-split extensions $M : R \to M \to S$ and isomorphism classes of non-zero elements $r \in R/\rho R$ under the action of the group of units in R. Recall $\rho = \omega_2 \Pi^\alpha$. Thus for each $i = 0, 1, \ldots, \alpha - 1$ we get an isomorphism class represented by a non-split extension M_i: $R \to M_i \to S$,

and up to isomorphism the R-free indecomposable A-modules are R, S and the M_i's for $i=0, 1,..., \alpha-1$. M_i has an R-basis v_{i1} and v_{i2} such that $Xv_{i1}=0$ and $Xv_{i2}=-\Pi^{\alpha}v_{i2}+u\Pi^{i}v_{i1}$, where u is a unit in R. A has an R-basis 1 and X. To see that $M_0 \simeq A$ change this to $v_1=X+\Pi^{\alpha}$ and $v_2=1+X$, then $Xv_1=0$ and $Xv_2=-\Pi^{\alpha}v_2+v_1$.

PROPOSITION 4.2. *With the above notation the multiplication table for* ${}_A\mathscr{S}$ *is*

	$[R]$	$[S]$	$[M_{\alpha-1}]$	$\cdots$	$[M_1]$	$[M_0]$
$[R]$	$[R]$	$[S]$	$[M_{\alpha-1}]$	$\cdots$	$[M_1]$	$[M_0]$
$[S]$	$[S]$	$[R]$	$[M_{\alpha-1}]$	$\cdots$	$[M_1]$	$[M_0]$
$[M_{\alpha-1}]$	$[M_{\alpha-1}]$	$[M_{\alpha-1}]$	$2[M_{\alpha-1}]$	$\cdots$	$2[M_1]$	$2[M_0]$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
$[M_1]$	$[M_1]$	$[M_1]$	$2[M_1]$	$\cdots$	$2[M_1]$	$2[M_0]$
$[M_0]$	$[M_0]$	$[M_0]$	$2[M_0]$	$\cdots$	$2[M_0]$	$2[M_0]$

Proof. The Tate–Oort basis for A is 1, X, where $X^2=aX$ and $\Delta X = 1\otimes X + X\otimes 1 + bX\otimes X$ and $a\cdot b=2$.

${}_A\mathscr{S}$ is commutative and $[R]$ is the identity, so it suffices to show that

(a) $[S][S]=[R]$,

(b) $[S][M_i]=[M_i]$, and

(c) $[M_j][M_i]=2[M_{\min(j,i)}]$.

(a) Let s be an R-generator for S, then $S\otimes S$ is generated by $s\otimes s$ and

$$\begin{aligned}\Delta X(s\otimes s) &= -a(s\otimes s)-a(s\otimes s)+a^2b(s\otimes s)\\ &= 0, \qquad \text{since} \quad ab=2.\end{aligned}$$

(b) $S\otimes M_i$ has R-generators $s\otimes v_{i1}$ and $s\otimes v_{i2}$,

$$\begin{aligned}X(s\otimes v_{i1}) &= -a(s\otimes v_{i1}),\\ X(s\otimes v_{i2}) &= -a(s\otimes v_{i2})+s\otimes(-av_{i2}+u\Pi^{i}v_{i1})\\ &\quad + b(-as\otimes(-av_{i2}+u\Pi^{i}v_{i1}))\\ &= (-a-a+a^2b)(s\otimes v_{i2})\\ &\quad + (u\Pi^{i}-ab\Pi^{i}u)(s\otimes v_{i1})\\ &= -u\Pi^{i}(s\otimes v_{i1}), \qquad \text{since} \quad ab=2.\end{aligned}$$

Choose j and u_1 such that $u_1\Pi^{i+j} = a$ and an R-basis

$$X_1 = s \otimes v_{i1} - uu_1\Pi^j(s \otimes v_{i1}),$$
$$X_2 = s \otimes v_{i2}, \qquad \text{for} \quad S \otimes M_i.$$

Now $XX_1 = 0$ and $XX_2 = -aX_2 - u\Pi^i X_1$. Hence $[S][M_i] = [M_i]$.

(c) $M_i \otimes M_j$ has R-generators $v_{i1} \otimes v_{j1}$, $v_{i1} \otimes v_{j2}$, $v_{i2} \otimes v_{j1}$, $v_{i2} \otimes v_{j2}$.

$$\begin{aligned}
\Delta X(v_{i1} \otimes v_{j1}) &= 0,\\
\Delta X(v_{i1} \otimes v_{j2}) &= -av_{i1} \otimes v_{j2} + u_j\Pi^j v_{i1} \otimes v_{j1},\\
\Delta X(v_{i2} \otimes v_{j1}) &= -av_{i2} \otimes v_{j1} + u_i\Pi^i v_{i1} \otimes v_{j1},\\
\Delta X(v_{i2} \otimes v_{j2}) &= (-av_{i2} + u_i\Pi^i v_{i1}) \otimes v_{j2}\\
&\quad + v_{i2} \otimes (-av_{j2} + u_j\Pi^j v_{j1})\\
&\quad + b(-av_{i2} + u_i\Pi^i v_{i1}) \otimes (-av_{j2} + u_j\Pi^j v_{j1})\\
&= b\Pi^{i+j}u_iu_j(v_{i1} \otimes v_{j1})\\
&\quad + (u_i\Pi^i - u_i\Pi^i ab)(v_{i1} \otimes v_{j2})\\
&\quad + (u_j\Pi^j - u_j\Pi^j ab)(v_{i2} \otimes v_{j1})\\
&\quad + (-a - a + a^2 b)(v_{i2} \otimes v_{j2})\\
&= a\Pi^{j+i}u_iu_jv_{i1} \otimes v_{i2} - u_i\Pi^i v_{i1} \otimes v_{j2}\\
&\quad - u_j\Pi^j v_{i2} \otimes v_{j1}.
\end{aligned}$$

Assume $j \leqslant i$ and choose $v_{i1} \otimes v_{j1}$, $v_{i1} \otimes v_{j2}$, $u_i b\Pi^i v_{i1} \otimes v_{j1} - (u_i/u_j)\,\Pi^{i-j}v_{i1} \otimes v_{j2} - v_{i2} \otimes v_{j1}$, $v_{i2} \otimes v_{j2}$ as an R-basis for $M_i \otimes M_j$. To see that $[M_i][M_j] = 2[M_j]$, note

$$\begin{aligned}
&\Delta X(u_i b\Pi^i v_{i1} \otimes v_{j1} - (u_i/u_j)\,\Pi^{i-j}v_{i1} \otimes v_{j2} - v_{i2} \otimes v_{j1})\\
&\quad = -(u_i/u_j)\,\Pi^{i-j}(-av_{i1} \otimes v_{j2} + u_j\Pi^j v_{i1} \otimes v_{j1})\\
&\quad = -(-av_{i2} \otimes v_{j1} + u_i\Pi^i v_{i1} \otimes v_{j1})\\
&\quad = -a(-(u_i/u_j)\,\Pi^{i-j}v_{i1} \otimes v_{j2} - v_{i2} \otimes v_{j1} + u_i b\Pi^i v_{i1} \otimes v_{j1}).
\end{aligned}$$

We can now prove the following:

THEOREM 4.3. *Let $p = 2$, let G be the cyclic group of order 2 and let A be a Hopf-algebra order in KG containing RG. The integral representation ring ${}_A\mathcal{Y}$ does not contain any non-zero nilpotent elements.*

Proof. $Q \otimes_{Z} {}_{A}\mathcal{I}$ has a basis of orthogonal idempotents.

$$
\begin{aligned}
e_1 &= \tfrac{1}{2}[M_0], \\
e_2 &= \tfrac{1}{2}([M_1] - [M_0]), \\
e_3 &= \tfrac{1}{2}([M_2] - [M_1]) \\
&\vdots \\
e_\alpha &= \tfrac{1}{2}([M_{\alpha-1}] - [M_{\alpha-2}]), \\
e_{\alpha+1} &= \tfrac{1}{2}([R] + [S] - [M_{\alpha-1}]), \\
e_{\alpha+2} &= \tfrac{1}{2}([R] - [S]).
\end{aligned}
$$

Hence ${}_{A}\mathcal{I}$ has no nilpotent elements.

Acknowledgments

Part of this work was done in my thesis, prepared under the supervision of Professor R. Larson, and submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Mathematics at the University of Illinois.

References

1. C. W. Curtis and I. Reiner, "Representation Theory of Finite Groups and Associative Algebras," Interscience, New York, 1962.
2. J. A. Green, The modular representation algebra of a finite group, *Illinois J. Math.* 6 (1962), 607–619.
3. A. L. Jensen, "Grothendieck Rings and Integral Representation Rings of Hopf-Algebra Orders," Ph.D. thesis, University of Illinois at Chicago Circle, 1981.
4. R. G. Larson, Characters of Hopf-algebra, *J. Algebra* **17** (1971), 352–368.
5. R. G. Larson, Orders in Hopf-algebras, *J. Algebra* **22** (1972), 201–210.
6. R. G. Larson, Orders from valuations, *J. Algebra* **38** (1976), 414–452.
7. I. Reiner, The integral representation ring of a finite group, *Michigan Math. J.* 12 (1965), 11–22.
8. I. Reiner, Nilpotent elements in rings of integral representations, *Proc. Amer. Math. Soc.* **17** (1966), 270–274.
9. I. Reiner, Integral representation algebras, *Trans. Amer. Math. Soc.* **124** (1966), 111–121.
10. I. Reiner, Invariants of integral representation, *Pacific J. Math.*, in press.
11. I. Reiner, A survey of integral representation theory, *Bull. Amer. Math. Soc.* **76** (1970), 159–227.
12. M. Sweedler, "Hopf-Algebras," Benjamin, New York, 1969.
13. J. Tate and F. Oort, Group schemas of prime order, *Ann. Ecole Norm. Sup.* 2 (1970), 1–21.
14. G. C. Wraith, Homological algebra notes, mimeographed lecture notes, Aarhus, 1969.