# ON THE STRUCTURE OF GROUP ALGEBRAS, I

JAMES A. COHN AND DONALD LIVINGSTONE

**1. Introduction.** With this paper we begin a study of the structure of the group algebra $RG$ of a finite group $G$ over the ring of algebraic integers $R$ in an algebraic number field $k$. The basic question is whether non-isomorphic groups can have isomorphic algebras over $R$. We shall show that this is impossible if $G$ is

(a) abelian,

(b) Hamiltonian,

(c) one of a special class of $p$-groups.

When $R = Z$, the ring of rational integers, (a) and (b) have been shown by Higman **(4)** and Berman **(1)**.

Our basic line of attack is a study of $U(RG)$, the group of units in $RG$. More precisely, let $\mu$ be the identity representation, let

$$V(RG) = \{u \in U(RG) | \mu(u) = 1\},$$

and let $H$ be a finite subgroup of $V(RG)$. We shall show that

(d) $(H : 1) \leqslant (G : 1)$;

(e) the exponent of $H$ divides the exponent of $G$;

(f) if $(H : 1) = (G : 1)$, then the elements of $H$ generate $RG$;

(g) if $G$ is nilpotent of class c, and $K$ is a finite group such that $RG \cong RK$, then $K$ is nilpotent of class c and the factor groups of the (ascending) descending central series for $G$ and $K$ are isomorphic.

In addition we shall give a complete description of $U(RG)$ when $G$ is an abelian group, obtaining a result of Higman **(4**, p. 238**)** as a consequence.

When $R = Z$, Coleman **(3)** has obtained part of (g), and Theorems 2.1 and 3.1 below are results of Berman **(1)**. However, all these results were obtained independently.

Finally, we wish to express our gratitude to the referee for several helpful suggestions.

**2.** If $u$ lies in the centre of $RG$, then $u = \sum u_\alpha C_\alpha$, where $u_\alpha \in R$ and $C_\alpha$ is the sum of the elements in the $\alpha$th conjugate class of $G$. Let $\Gamma_\lambda$ be an absolutely irreducible representation of $G$, let $f_\lambda$ be its degree, and let $\chi^\lambda$ be its character. Then $\Gamma_\lambda(u)$ is a diagonal matrix with $\omega_\lambda$ on the diagonal; thus we have

$$\sum u_\alpha n_\alpha \chi_\alpha{}^\lambda = f_\lambda \omega_\lambda, \qquad \lambda = 1, 2, \ldots, h, \tag{2.1}$$

Received September 20, 1963. The work of both authors was supported in part by NSFG-24333.

where $n_\alpha$ is the number of elements in the $\alpha$th conjugate class, and $\chi_\alpha^\lambda$ is the character of an element in the $\alpha$th class.

Viewing the $u_\alpha n_\alpha$ as unknowns in (2.1), we see that the coefficient matrix is just the character table of $G$. The orthogonality relations then yield

$$gu_\alpha = \sum \bar{\chi}_\alpha^\lambda f_\lambda \omega_\lambda, \qquad \alpha = 1, 2, \ldots, h. \tag{2.2}$$

Assume that for some $\alpha$ we have $0 < |u_\alpha| < 1$. Then $u_\alpha$ has a conjugate $v_\alpha$ such that $|v_\alpha| > 1$. Let $k'$ be a finite normal extension of the field of rational numbers, $Q$, which contains both $k$ and a splitting field for $G$. $k'$ has an automorphism $\sigma$ such that $\sigma(u_\alpha) = v_\alpha$. Applying $\sigma$ to (2.2), we obtain

$$gv_\alpha = \sum \sigma(\bar{\chi}_\alpha^\lambda) f_\lambda \sigma(\omega_\lambda).$$

It follows that

$$g < \sum f_\lambda |\sigma(\bar{\chi}_\alpha^\lambda)\sigma(\omega_\lambda)|.$$

Now $\bar{\chi}_\alpha^\lambda$ is a sum of $f_\lambda$ roots of unity, and hence so is $\sigma(\bar{\chi}_\alpha^\lambda)$. This yields

$$g < \sum f_\lambda^2 |\sigma(\omega_\lambda)|. \tag{2.3}$$

Assume now that $u$ is a unit of finite order, and therefore $\omega_\lambda$ is a root of unity. Applying this to (2.3) yields $g < \sum f_\lambda^2$, which is impossible. A similar argument shows $|u_\alpha| > 1$ is also impossible if $u$ is a unit of finite order. Thus assuming that $u$ is a unit of finite order and $u_\alpha \neq 0$ we have (from (2.2))

$$g = |\sum f_\lambda \bar{\chi}_\alpha^\lambda \omega_\lambda| = \sum f_\lambda |\bar{\chi}_\alpha^\lambda|.$$

It follows that $\bar{\chi}_\alpha^\lambda = f_\lambda \omega$ where $\omega$ is a root of unity. The orthogonality relations now show that $u_\alpha \neq 0$ for exactly one $\alpha$ and $C_\alpha$ is in the centre of $G$. Thus we have shown

THEOREM 2.1. *If $u$ is a unit of finite order in the centre of $RG$, then $u = \omega x$ where $\omega$ is a root of unity and $x$ is in the centre of $G$.*

Before stating the next result, we introduce the following notation. Let $\omega_n$ be a primitive $n$th root of unity, and let $R_n$ be the ring of algebraic integers in $k(\omega_n)$. We define $v_n$ to be $[k(\omega_n) : k]$, and $d_n$ to be the rank of the group of units in $R_n$.

THEOREM 2.2. *Let $G$ be an abelian group of order $g$, and let $U$ be the group of units in $RG$. If $n|g$, let $c_n$ be the number of elements in $G$ of order $n$ and define $a_n = c_n v_n^{-1}$. Then*

$$U = G \times H \times Z^t$$

*where $H$ is the (cyclic) group of units of finite order in $R$ and $t = \sum a_n d_n$, the sum being taken over all divisors $n$ of $g$.*

*Proof.* By (**6**, Theorem 1) we have

$$kG = \sum_{n|g} a_n k(\omega_n),$$

https://doi.org/10.4153/CJM-1965-058-2 Published online by Cambridge University Press

where by $a_n\, k(\omega_n)$ we mean, of course, the direct sum of $a_n$ copies of $k(\omega_n)$. Let $S = \sum a_n R_n$, which, of course, we view as a subring of $\sum a_n\, k(\omega_n)$; then the isomorphism identifying $kG$ with the direct sum **(6)** clearly carries $RG$ into $S$. Viewing $RG$ and $S$ as $Z$-modules, we claim they have the same rank. First note that

$$\mathrm{rk}_Z\, R_n = [k(\omega_n) : Q] = [k(\omega_n) : k][k : Q] = v_n[k : Q].$$

Hence

$$\mathrm{rk}_Z\, S = \sum_{n|g} a_n\, \mathrm{rk}_Z\, R_n = \sum_{n|g} a_n\, v_n[k : Q] = [k : Q] \sum_{n|g} c_n = g[k : Q].$$

Clearly, $\mathrm{rk}_Z\, RG = g[k : Q]$, and so $\mathrm{rk}_Z\, RG = \mathrm{rk}_Z\, S$.

LEMMA 2.1. *Let $A$ be a ring with* 1, *and let $B$ be a subring containing* 1. *Let $A'(B')$ be the group of units of $A(B)$. Finally assume that $B$ contains an ideal $C$ of $A$. If $\bar{A} = A/C$, then $[A' : B'] = [\bar{A}' : \bar{B}']$. In particular if $\bar{A}$ is finite, then so is $[A' : B']$.*

*Proof.* Let $D$ be the group of units in $A$ which are congruent to 1 (mod $C$). Since $C \subset B$, we have $D \subset B'$. The lemma is now obvious because $\bar{A}' = A'/D$ and $\bar{B}' = B'/D$.

We return now to the proof of the theorem. Since $S$ and $RG$ have the same $Z$-rank, $S/RG$ is a finite $Z$-module. Hence there exists an integer $m$ such that $mS \subset RG$. We now apply the lemma with $S = A$, $RG = B$, and $C = mS$. It follows that $U$ has finite index in the group of units $W$ of $S$, and therefore $U$ and $W$ have the same rank.

We must now show that the rank of $W$ is $t$. But this is obvious since the rank of the group of units in $R_n$ is $d_n$.

All that remains is to show that $G \times H$ is the torsion subgroup of $U$. Since this is an immediate consequence of Theorem 2.1, our proof is complete.

We say that a unit of $RG$ is *trivial* if it is of the form $\alpha x$ where $x \in G$ and $\alpha$ is a unit of $R$. We shall now determine under what conditions (on $R$ and $G$) $RG$ has only trivial units.

Since every unit of finite order in $RG$ is trivial, we must see when $t = d$, where $d$ is the rank of the group of units of $R$. By definition $t = a_1 d_1 + \sum a_n d_n$, where the sum, which we denote by $w$, is taken over all $n$ such that $n|g$ and $n \geqslant 2$. Since $a_1 = 1$ and $d_1 = d$, we have $t = d + w$. Clearly then we wish to know when $w = 0$.

Now $a_n \geqslant 1$ if, and only if, $G$ has elements of order $n$. Thus for $w = 0$, we must have $d_n = 0$ whenever $a_n \geqslant 1$. Since $R \subset R_n$, $d \leqslant d_n$; and since $a_n \geqslant 1$ for some $n > 1$, it follows that $d = 0$. Let $r = [k : Q]$; then we have $r = r_1 + 2r_2$, where $r_1$ $(2r_2)$ is the number of real (complex) embeddings of $k$. By the Dirichlet Unit Theorem **(5**, p. 128**)**, we have $d = r_1 + r_2 - 1$. Thus $d = 0$ if, and only if, $k = Q$ or $k = Q(\sqrt{D})$, where $D$ is a negative square-free integer. Dirichlet's theorem also shows that $d_n = 0$ if, and only if, $n = 2$, 3, 4, or 6.

We have thus shown that if $w = 0$, then

(1) $x \in G$, $x \neq 1$, implies that the order of $x$ is 2, 3, 4, or 6; and

(2) $R = Z$, or $R$ is the ring of integers in an imaginary quadratic number field.

Assume that $k$ is an imaginary quadratic field distinct from $Q(\omega_3) = Q(\omega_6)$, $Q(\omega_4)$. Let $K = k(\omega_n)$ where $n = 3, 4$, or 6; then $[K : Q] = 4$, $r_1 = 0$, and $r_2 = 2$. It follows that if $G$ has an element of order 3, 4, or 6, then $w > 0$; hence $G$ must be an elementary abelian 2-group.

If $K = Q(\omega_3) = Q(\omega_6)$ and $G$ has an element of order 4, or if $k = Q(\omega_4)$ and $G$ has an element of order 3, we also find that $w > 0$.

Thus we have shown most of

THEOREM 2.3. *If $G$ is a finite abelian group, then every unit of $RG$ is trivial if, and only if, one of the following conditions holds:*

(a) *$R = Z$ and every non-trivial element of $G$ has order 2, 3, 4, or 6;*

(b) *$R = Z[\omega_3]$ and every non-trivial element of $G$ has order 2, 3, or 6;*

(c) *$R = Z[\omega_4]$ and every non-trivial element of $G$ has order 2 or 4;*

(d) *$R$ is the ring of integers in an imaginary quadratic number field, and $G$ is an elementary abelian 2-group.*

*Proof.* We have already shown that these are the only possible cases. On the other hand in each of these four cases $d_n = 0$ for $n > 1$, and hence $t = d$.

We note that (a) is a result of Higman (**4**, p. 238).

It is possible to give an elementary constructive proof of part of Theorem 2.3: If $G$ is a group of order $g$, and $p|g$, $p > 3$, then $RG$ has non-trivial units. It clearly suffices to show this when $R = Z$, and $G$ is a cyclic group of order $p$ generated by $x$. Then $(x - 1)^p = p(x - 1)u$, where $u \in ZG$. We shall show that $u$ is a unit.

We have $(x - 1)(pu - (x - 1)^{p-1}) = 0$, and so $pu - (x - 1)^{p-1} = rN$ where $r \in Z$ and $N = \sum x^i$. However, if $u = \sum u_i x^i$, $u_i \in Z$, we see that $u_{p-1} = 0$; hence $r = -1$. If $v = \sum v_i x^i \in ZG$, we define $\mu(v) = \sum v_i$. Then $\ker \mu = I$, the ideal generated by $x - 1$. From $pu - (x - 1)^{p-1} = -N$, it follows that $\mu(u) = -1$. Now let $A$ be any maximal ideal of $ZG$. Since $N(x - 1) = 0$, either $N \in A$ or $x - 1 \in A$. Thus if $u \in A$, we must have $x - 1 \in A$, and so $I \subset A$. It follows that $ZG/A \cong Z/(q)$ for some prime $q$. But then $\mu(u) \equiv 0 \pmod{q}$, and this is a contradiction. Therefore $u$ is in no maximal ideal and is a unit. Provided $p > 3$, it is clear that at least two distinct powers of $x$ occur with non-zero coefficients in $u$, and so $u$ is non-trivial.

**3.** Let $u = \sum u_x x$ be in $RG$, and let $\chi$ be the trace of the regular representation $\Gamma$ of $G$; then $\chi(u) = u_1 g$. If $u$ is a unit of finite order, then

https://doi.org/10.4153/CJM-1965-058-2 Published online by Cambridge University Press

$\chi(u) = \omega_1 + \omega_2 + \ldots + \omega_g$ where the $\omega_i$ are roots of unity. By an argument analogous to that used to prove Theorem 2.1, we find that $|u_1| = 1$ or 0. If $u_1 \neq 0$, then it follows that $\Gamma(u)$ is similar to $\operatorname{diag}(\omega, \ldots, \omega)$, and hence $\Gamma(u) = \operatorname{diag}(\omega, \ldots, \omega)$. Thus $u = u_1 1$ and we have shown

THEOREM 3.1. *If $u = \sum u_x x$ is a unit of finite order in $RG$, and if $u_y \neq 0$ for some $y$ in the centre of $G$, then $u = u_y y$ and $u_y$ is a root of unity.*

Again let $u = \sum u_x x$ be a unit of finite order in $RG$. Let $\mathfrak{a}$ be an ideal of $R$, and let $f$ be the natural homomorphism of $RG$ onto $R/\mathfrak{a}(G)$. If $f(u) = a \in R/a$, then $u_1 \neq 0$; hence $u = u_1$. This proves

COROLLARY 3.1. *If $\mathfrak{a}$ is an ideal of $R$, $f : RG \to R/\mathfrak{a}(G)$, and $u$ is a unit of finite order in $RG$, then $f(u) = 1$ if and only if $u = 1 + a$ where $a \in \mathfrak{a}$.*

We recall the definition of $V(RG)$ given in the Introduction. If $\mu : RG \to R$ is the identity representation, then

$$V(RG) = \{u \in U(RG) | \mu(u) = 1\}.$$

COROLLARY 3.2. *Let $\mathfrak{a}$ and $f$ be as above. If $H$ is any finite subgroup of $V(RG)$, then $f(H) \cong H$.*

LEMMA 3.1. *If $H$ is a finite subgroup of $V(RG)$ and $\mathfrak{a}$ is any ideal of $R$ distinct from $R$ ($\mathfrak{a}$ may be (0)), then the elements of $H$ are linearly independent over $R/\mathfrak{a}$ in $R/\mathfrak{a}(G)$.*

*Proof.* Let $u_1, \ldots, u_n$ be the distinct elements of $H$. If $\alpha \in RG$, let $\bar{\alpha}$ be its image in $R/\mathfrak{a}(G)$. Assume that $\sum \bar{c}_i \bar{u}_i = 0$, where the $c_i$ are in $R$ and $\bar{c}_i \neq 0$ for some $i$. For definiteness suppose $\bar{c}_1 \neq 0$. Then

$$\bar{c}_1 = -\sum_{i=2}^{n} \bar{c}_i \bar{u}_i \bar{u}_1^{-1}.$$

If we express the elements $\bar{u}_i \bar{u}_1^{-1}$ in terms of the elements of $G$, it follows that for some $i \neq 1$ the coefficient of the identity in $\bar{u}_i \bar{u}_1^{-1}$ is not zero. *A fortiori*, the coefficient of the identity in $u_i u_1^{-1}$ is not zero. Since $H \subseteq V(RG)$, Theorem 3.1 implies that $u_i u_1^{-1} = 1$, which is a contradiction.

LEMMA 3.2. *If $H$ is a finite subgroup of $V(RG)$ and $S$ is the $R$-submodule of $RG$ generated by $H$, then $RG/S$ is $R$-torsion free.*

*Proof.* If $RG/S$ is not torsion free, then there exists $v \in RG$, $v \notin S$, and $a \in R$ such that $av \in S$. If $u_1, \ldots, u_n$ are the elements of $H$, then $av = \sum c_i u_i$. Letting $\mathfrak{a} = Ra$ in Lemma 3.1, we see that $a$ divides $c_i$ for all $i$, and so $v \in S$, which is a contradiction.

The following lemma is obvious, and we omit its proof.

LEMMA 3.3. *Let $H$ be a finite subgroup of $U(RG)$. If $u \in H$, let $f(u) = \mu(u)^{-1}u$. Then $f$ is a homomorphism of $H$ onto a subgroup $\bar{H}$ of $V(RG)$ such that*

https://doi.org/10.4153/CJM-1965-058-2 Published online by Cambridge University Press

$\ker f = H \cap R$, *hence* $H \cong \bar{H}$ *if, and only if,* $H \cap R = \{1\}$. *Furthermore,* $H$ *and* $\bar{H}$ *generate the same* $R$*-submodule of* $RG$.

THEOREM 3.2. *If* $H$ *is a finite subgroup of* $U(RG)$ *such that* $H \cap R = \{1\}$, *then* $(H:1) \leqslant (G:1)$. *Furthermore, if* $(H:1) = (G:1)$, *then the* $R$*-submodule generated by the elements of* $H$ *is all of* $RG$ *and so* $RH \cong RG$.

*Proof.* By Lemma 3.3. we can assume that $H \subseteq V(RG)$. Then the first statement follows from Lemma 3.1. Assume $(H:1) = (G:1)$, and let $S$ be the $R$-submodule generated by the elements of $H$. Since the elements of $H$ are linearly independent over $R$, $kS = kG$. It follows that the $k$-dimension of $RG/S$ is zero; but $RG/S$ is $R$-torsion free by Lemma 3.2, and therefore $RG = S$. Finally if $K$ is an abstract group isomorphic to $H$, the independence of the elements of $H$ over $R$ implies that $RK \cong S = RG$.

COROLLARY 3.3. *If* $G$ *and* $K$ *are finite groups, then* $RG \cong RK$ *if, and only if,* $(G:1) = (K:1)$ *and there is a subgroup of* $V(RG)$ *which is isomorphic to* $K$.

An immediate consequence of this is

COROLLARY 3.4. *If* $G$ *is abelian, then* $RG \cong RK$ *if, and only if,* $G \cong K$.

*Remark.* Let $G$ and $K$ be finite groups such that $RG \cong RK$. Corollary 3.3 then asserts the existence of a subgroup $H$ of $V(RG)$ such that $H \cong K$. Let $\lambda$ be an isomorphism of $K$ onto $H$; then $\lambda$ can be extended to an $R$-linear isomorphism of the algebra $RK$ onto the $R$-subalgebra of $RG$ generated by $H$, which we have shown is $RG$. In this fashion we can identify $RK$ with $RG$ by identifying $K$ with $\lambda K = H$. In the future we shall often assume implicitly that this identification has been made.

Let $N \lhd G$, and let $\psi$ be the natural homomorphism of $RG$ onto $R(G/N)$. If $H$ is a periodic subgroup of $U(RG)$, we define

$$\phi_H N = \{u \in H \mid \psi(u) = 1\}.$$

Using Theorem 3.1 we can also characterize $\phi_H N$ as

$$\phi_H N = \left\{u \in H \,\middle|\, \sum_{x \in N} u_x = 1, \text{ where } u = \sum u_x x\right\}.$$

THEOREM 3.3. (a) $\phi_H N \lhd H$.

*Assume that* $H \subseteq V(RG)$ *and* $(H:1) = (G:1)$; *then*

(b) $\phi_H$ *is an isomorphism of the lattice of normal subgroups of* $G$ *onto the lattice of normal subgroups of* $H$, *and* $(N:1) = (\phi_H N:1)$;

(c) *the centres of* $G$ *and* $H$ *coincide, and* $\phi_H$ *restricted to the centre of* $G$ *is the identity.*

*Proof.* (a) is obvious.

Assume that $(H:1) = (G:1)$; then by Theorem 3.2 we have $RG = RH$.

Clearly $H/\phi N$ generates $R(G/N)$, and so the orders of $H/\phi N$ and $G/N$ are the same since $H/\phi N \subseteq V(R(G/N))$. This in turn implies that $(N:1) = (\phi N:1)$.

Let $N$ and $K$ be normal subgroups of $G$. We see immediately that if $N \subseteq K$, then $\phi N \subseteq \phi K$. Now let $N$ and $K$ be arbitrary normal subgroups. Clearly $\phi(N \cap K) \subseteq \phi N \cap \phi K$. On the other hand, if $u \in \phi N \cap \phi K$, then $u$ goes to 1 when we divide out $G$ by either $N$ or $K$. Hence $u \in \phi(N \cap K)$. This shows that $\phi$ preserves intersections.

The lattice join of $N$ and $K$ is, of course, $NK$. Since both $\phi N$ and $\phi K$ are contained in $\phi(NK)$, it follows that $\phi N \phi K \subseteq \phi(NK)$. An easy argument on orders now shows us that $\phi N \phi K = \phi(NK)$. This proves (b).

Since $H \subseteq V(RG)$ and $RG = RH$, it follows from Theorem 2.1 and Lemma 3.4 that $u$ is in the centre of $G(H)$ if, and only if, $u$ is in the centre of $H(G)$. The rest of (c) is now obvious.

COROLLARY 3.5. *If $G$ is a Hamiltonian group, then $RG \cong RH$ if, and only if, $G \cong H$.*

*Proof.* $G = A \times B$ where $A$ is a quaternion group and $B$ is in the centre of $G$. Identifying $H$ with its image in $RG$, we have $\phi H = \phi(A) \times B$. Thus $R(G/B) = RA = R(\phi A)$ where $A$ and $\phi A$ are non-abelian groups of order eight. We shall show later that $A \cong \phi A$ (Theorem 4.2). Assuming this result, we see that $G \cong H$.

THEOREM 3.4. *Let $G$ be a nilpotent group and let $H$ be a finite subgroup of $V(RG)$. If*

$$1 = N_0 \subset N_1 \subset \ldots \subset N_r = G$$

*is a central series of $G$, then*

$$1 = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r = H, \qquad K_i = \phi N_i,$$

*is a central series of $H$. If $(H:1) = (G:1)$, then $K_i \neq K_{i+1}$, $i = 0, 1, \ldots, r-1$, and $N_{i+1}/N_i \cong K_{i+1}/K_i$.*

*Proof.* Let $(G:1) = \prod p_i^{a_i}$ and let $a = \sum a_i$. We shall prove the first assertion by induction on $a$. If $a = 1$, then the statement is obvious since $G$ is abelian. Since $N_1$ is in the centre of $G$ and $H \subseteq V(RG)$, we see by Theorem 3.1 that $K_1 \subseteq N_1$. Hence $K_1$ is certainly contained in the centre of $H$. If we divide out $G$ by $N_1$, passing to $R(G/N_1)$, then $H$ goes to $H/K_1$. Applying the induction hypothesis, we see that the groups $K_i/K_1$, $i = 1, \ldots, r$, form a central series for $H/K_1$. This proves the first assertion.

Assume that $G$ and $H$ have the same order. Since the $N_i$ are distinct, it follows that the $K_i$ are distinct. The last assertion is proved in the same way as the first.

COROLLARY 3.6. *If $G$ is nilpotent of class $c$ and $H$ is a finite subgroup of $U(RG)$, then $H$ is nilpotent of class $d$ where $d \leqslant c$.*

*Proof.* Let $f$ and $\bar{H}$ be as in Lemma 3.3; then $\bar{H}$ is nilpotent by Theorem 3.4. Since the kernel of $f$ is contained in the centre of $R$, it is certainly contained in the centre of $H$. It follows immediately that $H$ is nilpotent and has the same class as $\bar{H}$. Since the class of $\bar{H}$ is at most that of $G$, our proof is complete.

COROLLARY 3.7. *Let $G$ be nilpotent of class $c$, let $H \subseteq V(RG)$, and assume that $(G:1) = (H:1)$. Then $H$ is nilpotent of class $c$, and $\phi$ carries the ascending (descending) central series of $G$ to the ascending (descending) central series of $H$.*

*Proof.* Since the centres of $G$ and $H$ coincide, we see immediately by induction that $H$ is nilpotent of class $c$.

Let $G_c$ and $H_c$ be the last non-trivial terms in the descending central series for $G$ and $H$ respectively. Since $G/G_c$ has class $c-1$, and since $H/G_c \subseteq V(R(G/G_c))$, it follows that $H/G_c$ has class $c-1$ (since $G_c$ is contained in the centre of $G$, it is a subgroup of $H$). Thus $G_c \supseteq H_c$. If $H_c \neq G_c$, then $G/H_c$ has class $c$, while $H/H_c$ has class $c-1$, which is impossible by the first part of the corollary. Thus $G_c = H_c$, and proceeding by induction we see that $\phi$ carries the descending central series of $G$ to the descending central series of $H$. A similar proof holds for the ascending central series.

This last result clearly implies

COROLLARY 3.8. *Let $G$ and $K$ be finite groups such that $RG \cong RK$. If $G$ is nilpotent of class $c$, then so is $K$, and if $\{G_i\}$ and $\{K_i\}$ are the ascending (descending) central series of $G$ and $K$ respectively, then $G_i/G_{i-1} \cong K_i/K_{i-1}$ for all $i$.*

When $R = Z$, Coleman (**3**, pp. 6–7) has obtained part of Theorem 3.4. and the corollaries following it.

**4.** Let $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ be elements of $G$. We define

$$x_1 x_2 \ldots x_n \sim y_1 y_2 \ldots y_n$$

if some power of the cycle $(12 \ldots n)$ carries $x_1 \ldots x_n$ to $y_1 \ldots y_n$, i.e., if one product is a cyclical permutation of the other. Clearly $\sim$ is an equivalence relation; and if two products are $\sim$-equivalent, then they are conjugate in $G$. Furthermore, if the subgroup of $\langle(12 \ldots n)\rangle$ fixing a product $x_1 \ldots x_n$ has order $m$, then the order of its $\sim$-class is $nm^{-1}$ and this order is 1 if, and only if, all the $x_i$ are equal.

If $n = p^a$, $p$ a prime, it follows that the order of an $\sim$-class is either 1 (in which case the element of the class is $x^n$) or $p^b$ where $0 < b \leqslant a$. Let $u = \sum u_x x$; then

$$u^n = \sum u_x{}^n x^n + w, \tag{$*$}$$

where $w$ is a sum of products of $n$ elements which are formally not $n$th powers.

https://doi.org/10.4153/CJM-1965-058-2 Published online by Cambridge University Press

It follows that if we sum the coefficients of $w$ over the elements of one $\sim$-class, the result is divisible by $p$. Thus if we write $w = \sum w_y\, y$ and take the coefficient sum of $w$ over a conjugate class of $G$, this will also be divisible by $p$.

Let $\mathfrak{p}$ be a prime ideal of $R$ dividing $(p)$, and let $N(c)$ be the set of elements in $G$ of order $p^c$. Assume there exists some integer $c$ such that

$$\sum_{x \in N(c)} u_x \not\equiv 0 \pmod{\mathfrak{p}}.$$

Let $a$ be the smallest such integer, and let

$$\alpha_a = \sum_{x \in N(a)} u_x.$$

Then $\alpha_a{}^r \not\equiv 0 \pmod{\mathfrak{p}}$ and

$$\alpha_a{}^{p^b} \equiv \sum_{x \in N(a)} u_x{}^{p^b} \pmod{\mathfrak{p}}.$$

Now we consider (*). From the previous paragraph we know that $\beta$, the coefficient of 1 in $w$, must be congruent to zero (mod $\mathfrak{p}$). Defining $\alpha_c$ analogously to $\alpha_a$, the minimality of $a$ implies $\alpha_c \equiv 0 \pmod{\mathfrak{p}}$ for $c < a$. Clearly then $\alpha_c^n \equiv 0 \pmod{\mathfrak{p}}$ for $c < a$. On the other hand, $\alpha_a \not\equiv 0 \pmod{\mathfrak{p}}$. Since the coefficient of 1 in $u^n$ is

$$\alpha = \alpha_a + \beta + \sum_{c<a} \alpha_c,$$

it follows that $\alpha \not\equiv 0 \pmod{\mathfrak{p}}$, and so 1 occurs in $u^n$ with a non-zero coefficient. Thus if $u$ is a unit of finite order, we see that $u^n = \alpha \in R$. Finally if we require $\mu(u) = 1$, we obtain $u^n = 1$ and the order of $u$ divides $p^a$. However, if the order of $u$ is $p^c$, $c < a$, then setting $n = p^c$ in (*), we easily see that $\alpha_c \not\equiv 0 \pmod{\mathfrak{p}}$; this contradicts the minimality of $a$. Therefore the order of $u$ is exactly $p^a$. Finally we note that clearly $\alpha_c \equiv 0 \pmod{\mathfrak{p}}$ for $c > a$.

On the other hand if $\alpha_c \equiv 0 \pmod{\mathfrak{p}}$ for all $c$, it is immediate that $u$ cannot be a unit of $p$-power order. Thus we have shown

THEOREM 4.1. *Let $u = \sum u_x\, x$ be a unit of finite order in $V(RG)$, let $N(a)$ be the set of all elements in $G$ of order $p^a$, and let*

$$\alpha_a = \sum_{x \in N(a)} u_x.$$

*Then $u$ has order $p^b$ if, and only if, $\alpha_b \not\equiv 0 \pmod{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$ dividing $(p)$. Furthermore, if $u$ has order $p^b$, then $\alpha_a \equiv 0 \pmod{\mathfrak{p}}$ for all $a \neq b$ and all $\mathfrak{p}$ dividing $(p)$.*

COROLLARY 4.1. *If $p^a$ is the exponent of a $p$-Sylow subgroup of $G$ and $u$ is a unit of $p$-power order in $V(RG)$, then the order of $u$ is at most $p^a$. In particular, if $G$ is a $p$-group and $RG \cong RH$, then $G$ and $H$ have the same exponent.*

From this we see

COROLLARY 4.2. *Let $|G| = g$. If $u$ is a unit of order $n$ in $V(RG)$, then $n|g$. If $u$ is any unit of order $n$ in $ZG$, then $g$ even (odd) implies $n|g$ $(n|2g)$.*

LEMMA 4.1. *Let $G$, $H$, and $\phi$ be as in Theorem 3.4. If $N$ is a normal cyclic subgroup of $G$, then $\phi(N)$ is a normal cyclic subgroup of $H$ and $|N| = |\phi(N)|$.*

*Proof.* All we need show is that $\phi(N)$ is cyclic. Since the $p$-Sylow subgroups of $N$ are characteristic, they are normal in $G$. Thus $\phi(N)$ is the direct product of its $p$-Sylow subgroups and so we need only show that they are cyclic. We can therefore assume that $N$ is a $p$-group and we proceed by induction on $|N|$. If $|N| = p$, the result is obvious. Let $|N| = p^n$ and assume the result for any cyclic normal subgroup of smaller order in any finite group. Let $L$ be the Frattini subgroup of $\phi(N)$. Since $L \lhd H$, there is a subgroup $K \subseteq N$, $K \lhd G$ such that $\phi(K) = L$. If $\psi$ is the lattice isomorphism between $G/K$ and $H/L$, then $\psi(N/K) = \phi(N)/L$. But $N/K$ is cyclic and so by induction $\phi(N)/L$ is cyclic. However, $\phi(N)/L$ is also an elementary abelian $p$-group and therefore $|\phi(N)/L| = p$. It follows that $\phi(N)$ is cyclic.

THEOREM 4.2. *If $G$ is a $p$-group with a cyclic normal subgroup of index at most $p^2$ if $p$ is odd or of index 2 if $p = 2$, then $RG \cong RH$ if and only if $G \cong H$.*

*Proof.* We first treat the case where $p$ is odd. Let $N$ be the cyclic normal subgroup. If $(G : N) = p$, then $(H : \phi(N)) = p$ and $\phi(N)$ is cyclic. Since there is only one such group of order $p^n$, our proof is complete.

Now assume that $(G : N) = p^2$. Let $|G| = p^n$. There are in general four such groups. One of these is of the type $K \times C$, where $K, C \lhd G$, $K$ has a cyclic subgroup of index $p$, and $|C| = p$. Then $H = \phi(G) = \phi(K) \times \phi(C)$ and so $H \cong G$.

The other three are defined as follows:

$$\text{(I)}\quad x^{p^{n-2}} = y^p = z^p = 1,\quad xy = yx,\quad xz = zx,\quad zxz^{-1} = yx^{p^{n-3}};$$

$$\text{(II)}\quad x^{p^{n-2}} = y^{p^2} = 1,\quad yxy^{-1} = x^{1+p^{n-3}};$$

$$\text{(III)}\quad x^{p^{n-2}} = y^{p^2} = 1,\quad yxy^{-1} = x^{1+p^{n-4}}.$$

The centre of $G$ is $\langle x\rangle$, $\langle x^p\rangle$, and $\langle x^{p^2}\rangle$ respectively in the three groups. Since the centre of $H$ is the centre of $G$, this part of the proof is complete.

Now assume that $p = 2$. There are four groups of order $2^n$ with a cyclic subgroup of index 2:

$$\text{(I)}\quad x^{2^{n-1}} = 1,\quad y^2 = x^{2^{n-2}},\quad y^{-1}xy = x^{-1};$$

$$\text{(II)}\quad x^{2^{n-1}} = y^2 = 1,\quad yxy = x^{1+2^{n-2}};$$

$$\text{(III)}\quad x^{2^{n-1}} = y^2 = 1,\quad yxy = x^{-1+2^{n-2}};$$

$$\text{(IV)}\quad x^{2^{n-1}} = y^2 = 1,\quad yxy = x^{-1}.$$

Let $RG \cong RH$; then we can identify $H$ with a subgroup of $V(RG)$.

Group (I) is of course the generalized quaternion group and hence has exactly one cyclic subgroup of order two which is a normal subgroup. It follows immediately from Theorem 4.1 that $H$ has the same property. Hence $G \cong H$.

Group (II) is distinguished from the other groups by the size of its centre.

Group (IV) has only one cyclic subgroup of order four and it is a normal subgroup. Thus again Theorem 4.1 shows that $G \cong H$.

**5.** Let $G$ be a $p$-group. If $H$ is a subgroup of $V(RG)$ and $|H| = |G|$, then we know that $H$ has the same class and exponent as $G$. Let $\Omega(\alpha)$ denote the class of all $p$-groups such that the subset

$$\Omega_\alpha(G) = \{x \in G | x^{p^\alpha} = 1\}$$

is in fact a subgroup; e.g., if $G$ is regular, then $G \in \Omega(\alpha)$ for all $\alpha$. As before $\phi$ denotes the lattice isomorphism between $G$ and $H$.

LEMMA 5.1. *If $G \in \Omega(\alpha)$, then $H \in \Omega(\alpha)$ and $\phi(\Omega_\alpha(G)) = \Omega_\alpha(H)$.*

*Proof.* This follows immediately from Theorems 4.1 and 3.1.

We say that $G \in \Omega$ if $G \in \Omega(\alpha)$ for all $\alpha$.

PROPOSITION 5.1. *If $G \in \Omega$ and $N \lhd G$, then $N$ and $\phi(N)$ have the same exponent.*

*Proof.* If $\alpha$ is the smallest integer such that $N \subseteq \Omega_\alpha(G)$, then $\alpha$ is also the smallest integer such that $\phi(N) \subseteq \Omega_\alpha(H)$. Thus the exponent of both $N$ and $\phi(N)$ is $p^\alpha$.

While we have not been able to show that $H$ is regular if $G$ is regular, we do have

COROLLARY 5.1. *If $G$ and $H$ are regular and $RG \cong RH$, then $G$ and $H$ have the same type invariants.*

Finally if $G$ and $H$ have order 16, one can show (using Proposition 5.1) that $RG \cong RH$ only if $G \cong H$.

## REFERENCES


1. S. D. Berman, *On certain properties of integral group rings*, Dokl. Akad. Nauk SSSR (n.s.), *91* (1953), 7–9.
2. J. A. Cohn and D. Livingstone, *On groups of order $p^3$*, Can. J. Math., *15* (1963), 622–624.
3. D. B. Coleman, *Finite groups with isomorphic group algebras*, Trans. Amer. Math. Soc., *105* (1962), 1–8.
4. G. Higman, *The units of group rings*, Proc. London Math. Soc., *46* (1940), 231–248.
5. H. B. Mann, *Introduction to algebraic number theory* (Columbus, 1955).
6. S. Perlis and G. Walker, *Abelian group algebras of finite order*, Trans. Amer. Math. Soc., *68* (1950), 420–426.


*University of Michigan*