PACIFIC JOURNAL OF MATHEMATICS
Vol. 15, No. 2, 1965

ISOMORPHIC GROUPS AND GROUP RINGS

D. S. PASSMAN

Let $\mathfrak{G}$ be a finite group, S a commutative ring with one and $S[\mathfrak{G}]$ the group ring of $\mathfrak{G}$ over S. If $\mathfrak{H}$ is a group with $\mathfrak{G} \cong \mathfrak{H}$ then clearly $S[\mathfrak{G}] \cong S[\mathfrak{H}]$ where the latter is an S-isomorphism. We study here the converse question: For which groups $\mathfrak{G}$ and rings S does $S[\mathfrak{G}] \cong S[\mathfrak{H}]$ imply that $\mathfrak{G}$ is isomorphic to $\mathfrak{H}$?

We consider first the case where $S = K$ is a field. It is known that if $\mathfrak{G}$ is abelian then $Q[\mathfrak{G}] \cong Q[\mathfrak{H}]$ implies that $\mathfrak{G} \cong \mathfrak{H}$ where Q is the field of rational numbers. We show here that this result does not extend to all groups $\mathfrak{G}$. In fact by a simple counting argument we exhibit a large set of nonisomorphic p-groups with isomorphic group algebras over all noncharacteristic p fields. Thus for groups in general the only fields if interest are those whose characteristic divides the order of the group.

We now let $S = R$ be the ring of integers in some finite algebraic extension of the rationals. We show here that the group ring $R[\mathfrak{G}]$ determines the set of normal subgroups of $\mathfrak{G}$ along with many of the natural operations defined on this set. For example, under the assumption that $\mathfrak{G}$ is nilpotent, we show that given normal subgroups $\mathfrak{M}$ and $\mathfrak{N}$, the group ring determines the commutator subgroup $(\mathfrak{M}, \mathfrak{N})$. Finally we consider several special cases. In particular we show that if $\mathfrak{G}$ is nilpotent of class 2 then $R[\mathfrak{G}] \cong R[\mathfrak{H}]$ implies $\mathfrak{G} \cong \mathfrak{H}$.

1. Remarks on group algebras.

Recently examples have been given of pairs of groups $\{\mathfrak{G}, \mathfrak{H}\}$ for which $K[\mathfrak{G}]$ is K-isomorphic to $K[\mathfrak{H}]$ for all fields K whose characteristic does not divide the order of the groups. We show here by a simple counting argument that this is not particularly surprising. This approach was suggested by Professor R. Brauer.

We prove

THEOREM A. *Suppose $\boldsymbol{Q}[\mathfrak{G}] \simeq \boldsymbol{Q}[\mathfrak{H}]$ where $\boldsymbol{Q}$ is the field of rational numbers. Then for all fields K whose characteristic does not divide $|\mathfrak{G}| = |\mathfrak{H}|$, the order of the groups, we have $K[\mathfrak{G}[\simeq K[\mathfrak{H}]$.*

THEOREM B. *There exists a set of $p^{B(n)}$ nonisomorphic groups of order p^n where $B(n) = 2/27\,(n^3 - 17\,n^2)$ which have isomorphic group algebras over all noncharacteristic p fields.*

Received January 28, 1964.

Let χ be the character of an absolutely irreducible representation of group algebra $K[\mathfrak{G}]$ in some extension field of K. We set $K(\chi)$ equal to the field obtained by adjoining to K all $\chi(g)$ for $g \in \mathfrak{G}$. If ε is a primitive $|\mathfrak{G}|$th root of unity then of course $K(\chi) \subseteq K(\varepsilon)$. If $K = \boldsymbol{Q}$ then $\boldsymbol{Z}(\chi)$ denotes the ring extension of the rational integers $\boldsymbol{Z}$ by the $\chi(g)$. Clearly

$$\boldsymbol{Z}(\chi) \subseteq \text{int } \boldsymbol{Q}(\chi)$$

where the latter is the ring of algebraic integers in $\boldsymbol{Q}(\chi)$. We need a partial converse.

LEMMA 1. *$\boldsymbol{Z}(\chi) \supseteq |\mathfrak{G}|^r$ int $\boldsymbol{Q}(\chi)$ where $|\mathfrak{G}|^r$ is a suitably high power of the order of $\mathfrak{G}$.*

Proof. $\boldsymbol{Q}(\chi) \subseteq \boldsymbol{Q}(\varepsilon)$ and the latter is a normal abelian extension of $\boldsymbol{Q}$. Hence $\boldsymbol{Q}(\chi)$ is also normal over $\boldsymbol{Q}$. Let $\mathscr{H}$ be the Galois group of order $h = \dim \boldsymbol{Q}(\chi)$. Then the h characters χ^σ with $\sigma \in \mathscr{H}$ are all distinct. Let us assume that the characters of $\mathfrak{G}$ are so numbered that these constitute the first h. Let $g_i \in \mathfrak{G}$ be a representative of the ith class of $\mathfrak{G}$ and let $n_i = |\mathfrak{G}: \mathfrak{C}(g_i)|$ be the number of conjugates of g_i. Set $\boldsymbol{X} = [\chi_i(g_j)]$ and $\boldsymbol{N} = [n_i \delta_{ij}]$. These are $k \times k$ matrices where k is the number of classes of $\mathfrak{G}$. They have row index i, column index j and δ_{ij} is the Kronecker delta. Then by the orthogonality relations for the characters we have $\boldsymbol{X}\boldsymbol{N}\boldsymbol{X}^* = |\mathfrak{G}| I$ where * denotes the conjugate transpose and $\boldsymbol{I}$ is the $k \times k$ identity matrix.

Let p be a prime not dividing $|\mathfrak{G}|$ and let (p) denote the principal ideal $p\boldsymbol{Z}(\varepsilon)$ in $\boldsymbol{Z}(\varepsilon)$. By the above matrix equation we see that $\det \boldsymbol{X} \neq 0 \bmod (p)$. We expand this determinant by the Laplace expansion with respect to the first h rows so that

$$\det \boldsymbol{X} = \Sigma_\lambda^{\pm} \det \boldsymbol{M}_\lambda \det \boldsymbol{N}_\lambda \not\equiv 0 \bmod (p) ,$$

where $\boldsymbol{M}_\lambda$ is an $h \times h$ minor in the first h rows and $\boldsymbol{N}_\lambda$ is its complementary minor. Thus for some λ, $\det \boldsymbol{M}_\lambda \not\equiv 0 (p)$. We can of course assume this is the principal minor.

Set $m_p = \det [\chi_i(g_j)]^2 \quad i, j = 1, 2, \cdots, h$. Then m_p is a rational integer not divisible by p since it is integral and invariant under $\mathscr{H}$. In particular $m_p \neq 0$ so that $\chi(g_1), \cdots, \chi(g_h)$ are linearly independent over $\boldsymbol{Q}$. Hence they span $\boldsymbol{Q}(\chi)$ over $\boldsymbol{Q}$. Let $\alpha \in$ int $\boldsymbol{Q}(\chi)$. Then

$$\alpha = \Sigma_j q_j \chi(g_j) \qquad q_j \in \boldsymbol{Q} .$$

We apply each element of $\mathscr{H}$ in turn to this equation and obtain upon multiplying the system of equations by $[\chi_i(g_j)]$ the matrix equation

$$[\chi_i(g_j)]^2 \begin{bmatrix} q_1 \\ q_2 \\ \vdots \\ q_h \end{bmatrix} = [\chi_i(g_i)] \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_h \end{bmatrix}$$

where $\alpha_i = \sigma_i(\alpha)$. Hence $q_i = \beta_i/m_p$ where β_i is an algebraic and hence rational integer. Thus

$$\boldsymbol{Z}(\chi) \supseteq m_p \operatorname{int} \boldsymbol{Q}(\chi) .$$

Let J be the ideal in $\boldsymbol{Z}$ spanned by the m_p for all primes p prime to $|\boldsymbol{G}|$. Since $(p, m_p) = 1$ we see that $|\boldsymbol{G}|^r$ belongs to J for some suitable integer r. But clearly for any element $m \in J$ we have $\boldsymbol{Z}(\chi) \supseteq m \operatorname{int} \boldsymbol{Q}(\chi)$ so the result follows.

We now consider some well known results on group algebras. Let K be a perfect field with $K[\mathfrak{G}]$ semi-simple. Then $K[\mathfrak{G}]$ is a direct sum of simple rings A_i and each A_i is a full matrix ring over a division algebra D_i. Let $A = [D]_n$ be such a component and let $\mathscr{F}$ be any absolutely irreducible representation of A over some extension field. Suppose $\mathscr{F}$ has degree f and character χ. Then the center of D is isomorphic to $K(\chi)$ (see for example [8] whose proof generalizes to the case of perfect fields.)

If K is a finite field then since all finite division rings are commutative we see that $D = K(\chi)$. Moreover $f = n$ and A has exactly $\dim_K K(\chi)$ distinct absolutely irreducible representations. Thus in this case $K[\mathfrak{G}]$ is determined by the set of ordered pairs $\{f_i, F_i\}$ where $f_i = \deg \chi_i$ and $F_i = K(\chi_i)$ for all absolutely irreducible characters χ_i. This follows since the number of direct summands of $K[\mathfrak{G}]$ isomorphic to $[F]_n$ is equal to the number of pairs $\{f_i, F_i\}$ with $F_i = F$, $f_i = n$ all divided by $\dim_K F$.

Proof of Theorem A. Clearly it suffices to assume that K is a prime field. Since $K = \boldsymbol{Q}$ is given we assume that $K = GF(p)$ with p prime to $|\mathfrak{G}| = |\mathfrak{H}|$. Since $\boldsymbol{Q}$ is perfect we see that $\boldsymbol{Q}[\mathfrak{G}]$ determines the ordered pairs $\{f_i, \boldsymbol{Q}(\chi_i)\}$ where $f_i = \deg \chi_i$. Let ε be a primitive $|\mathfrak{G}|$th root of unity over $\boldsymbol{Q}$. Then $\boldsymbol{Q}(\chi) \subseteq \boldsymbol{Q}(\varepsilon)$. Moreover since $\boldsymbol{Q}(\chi)$ is normal over $\boldsymbol{Q}$ as we mentioned above this inclusion is essentially unique.

Now $\chi: \mathfrak{G} \to \boldsymbol{Z}(\varepsilon)$. Let $\mathfrak{p}$ be a prime divisor of p in $\boldsymbol{Z}(\varepsilon)$. Then as is well known (see for example [1], 6E) the maps $\bar{\chi}: \mathfrak{G} \to K(\bar{\varepsilon})$ defined by composing χ with the quotient map $\boldsymbol{Z}(\varepsilon) \to \boldsymbol{Z}(\varepsilon)/\mathfrak{p} = K(\bar{\varepsilon})$ are the absolutely irreducible characters of $K[\mathfrak{G}]$.

Thus $K(\bar{\chi}) = \boldsymbol{Z}(\chi)/\mathfrak{p}$ and $\deg \bar{\chi} = \deg \chi$. Now $\boldsymbol{Q}(\chi) \subseteq \boldsymbol{Q}(\varepsilon)$ and

$\boldsymbol{Z}(\varepsilon) \cap \boldsymbol{Q}(\chi) = \text{int } \boldsymbol{Q}(\chi)$ the latter being determined by $\boldsymbol{Q}[\mathfrak{G}]$. Since p is prime to $|\mathfrak{G}|$ we see by Lemma 1 that $\boldsymbol{Z}(\chi)\mathfrak{p}/\mathfrak{p} = \text{int } \boldsymbol{Q}(\chi)\mathfrak{p}/\mathfrak{p}$ and the latter is determined by $\boldsymbol{Q}[\mathfrak{G}]$. Thus $\boldsymbol{Q}[\mathfrak{G}]$ yields the pairs $\{f_i, F_i\}$ and hence by our previous remarks $K[\mathfrak{G}]$ is determined up to isomorphism.

Proof of Theorem B. Let $\mathfrak{G}$ be a p-group and let $A = [D]_m$ be a direct summand of $Q[\mathfrak{G}]$. Let $\mathscr{T}$ be an absolutely irreducible representation of A of degree f and character χ. If $p > 2$ then ([9] Satz 1 and pg. 249) $D = \boldsymbol{Q}(\chi)$ and $f = m$. If $p = 2$ then either $D = \boldsymbol{Q}(\chi)$ and $f = m$ or $\boldsymbol{Q}(\chi)$ is a real field, D is the quaternion division algebra over $\boldsymbol{Q}(\chi)$ and $f = 2m$.

We note by Theorem A that it suffices to show that such a set of groups exists with isomorphic group algebras over $\boldsymbol{Q}$.

Let us assume that $\mathfrak{G}$ has period p^2. Then if χ is any nonprincipal character of G we have

$$\boldsymbol{Q}(\varepsilon_1) \subseteqq \boldsymbol{Q}(\chi) \subseteqq \boldsymbol{Q}(\varepsilon_2) ,$$

where ε_1 is a primitive pth root of unity and ε_2 is a primitive p^2th root. The second inclusion is clear. The first follows by considering the restriction of χ to an element of order p in the center of the representation. Now there are no intermediate fields so either

$$\boldsymbol{Q}(\chi) = \boldsymbol{Q}(\varepsilon_1) \qquad \dim = p - 1$$

or

$$\boldsymbol{Q}(\chi) = \boldsymbol{Q}(\varepsilon_1) \qquad \dim = p(p-1) .$$

For p-groups in general $f = p^i$.

Suppose $p > 2$. Let $\boldsymbol{Q}[\mathfrak{G}]$ have a_i direct summands isomorphic to $[\boldsymbol{Q}(\varepsilon_1)]_{p^i}$ and b_i direct summands isomorphic to $[\boldsymbol{Q}(\varepsilon_2)]_{p^i}$. Then by computing dimensions we have assuming that the order of $\mathfrak{G}$ is p^n

$$p^n = \dim \boldsymbol{Q}[\mathfrak{G}] = 1 + \Sigma_i (p-1)(a_i + pb_i) p^{2i} .$$

Moreover the values of a_i and b_i completely determine the group algebra.

We have clearly

$$0 \leqq a_i \leqq (p^n - 1)/\{(p-1)p^{2i}\} \leqq p^{n-2i} - 1$$
$$0 \leqq b_i \leqq (p^n - 1)/\{(p-1)p^{2i+1}\} \leqq p^{n-2i-1} - 1 .$$

Hence the number of possible group algebras is less than or equal to

$$\prod_{i=0} p^{n-2i} p^{n-2i-1} = \prod_{i=0}^{n} p^j = p^{n(n+1)/2} .$$

Now let $p = 2$. The direct summands of $\boldsymbol{Q}[\mathfrak{G}]$ are then $[\boldsymbol{Q}]_{2^i}$ with

multiplicity a_i, $[\boldsymbol{Q}(\sqrt{-1})]_{2^i}$ with multiplicity b_i and $[D]_{2^i}$ with multiplicity c_i where D is the usual quaternion division ring over the rationals. Thus taking dimensions as before we have

$$2^n = \sum_i a_i 2^{2i} + \sum_i b^i 2^{2i+1} + \sum_i c_i 2^{2i+2}.$$

Since $a_0 > 0$ this yields

$$1 \leqq a_0 \leqq 2^n \qquad 0 \leqq a_i \leqq 2^{n-2i} - 1 \quad i > 0$$
$$0 \leqq b_i \leqq 2^{n-2i-1} - 1 \qquad 0 \leqq c_i \leqq 2^{n-2i-2} - 1.$$

Hence there are at most

$$\{\prod_i 2^{n-2i}\}\{\prod_i 2^{n-2i-1}\}\{\prod_i 2^{n-2i-2}\} \leqq 2^{3n^2/4}$$

possible group algebras. Since $3n^2/4 \geqq n(n+1)/2$ we see that for all primes p there are at most $p^{e(n)}$ group algebras over $\boldsymbol{Q}$ for groups of order p^n and period p^2 where $e(n) = 3n^2/4$.

Finally ([5] Theorem 2.3) there are at least $p^{f(n)}$ groups of order p^n and period p^2 where $f(n) = 2(n^3 - 6n^2)/27$. Thus there is a set of at least

$$p^{f(n)-e(n)} \geqq p^{2(n^3-17n^2)/27}$$

nonisomorphic groups of order p^n with isomorphic group algebras over $\boldsymbol{Q}$ and hence over all noncharacteristic p fields. This completes the proof.

Of course the above result is trivial for $n < 18$. However for small n we can compute specific examples.

For $p > 2$, the two non-abelian groups of order p^3 have $p^2 - 1$ nonprincipal linear characters and $p - 1$ characters of degree p. Moreover in all of these cases $\boldsymbol{Q}(\chi) = \boldsymbol{Q}(\varepsilon_1)$. Hence their group algebras are isomorphic over all K with p prime to the characteristic of K.

For $p = 2$, the group algebras over $\boldsymbol{Q}$ for all groups of order less than or equal to 8 are not isomorphic. On the other hand, as can be easily checked, the following groups of order 16 ([2] pg. 146) have isomorphic $\boldsymbol{Q}$ group algebras.

1. $\alpha^4 = 1, \quad \beta^4 = 1, \quad \alpha^{-1}\beta\alpha = \beta^{-1}$

and

2. $\alpha^4 = 1, \quad \beta^2 = 1, \quad \gamma^2 = 1, \quad \beta^{-1}\alpha\beta = \alpha\gamma, \quad \alpha^{-1}\gamma\alpha = \gamma, \quad \beta^{-1}\gamma\beta = \gamma.$

As a consequence of the above theorems we see that the only pertinent fields to study are the prime fields $GF(p)$ with p dividing $|\mathfrak{G}|$. An example of the techniques used there can be found in [7] where the following result is proved: Let $\mathfrak{G}$ be a p-group of order

$\leqq p^4$. Then $\mathfrak{G} \cong \mathfrak{H}$ if and only if $F[\mathfrak{G}] \cong F[\mathfrak{H}]$ where F is the field $GF(p)$.

In the remainder of this paper we discuss group rings $R[\mathfrak{G}]$ where R is the ring of integers in some algebraic number field.

2. **Class sums and normal subgroups.** Let F be a finite algebraic extension of $\boldsymbol{Q}$ and let R be a subring of the ring of algebraic integers in F. We assume $1 \in R$. Whenever we write $R[\mathfrak{G}]$ we assume that its structure as an R-module as well as a ring is known. In particular $R[\mathfrak{G}] \cong R[\mathfrak{H}]$ means that the two group rings are R-isomorphic.

Elements of particular interest in $R[\mathfrak{G}]$ are the class sums. These are the sum of all the group elements in any given class of $\mathfrak{G}$. We will generally denote these by K_x, corresponding to the class containing $x \in \mathfrak{G}$, or by K_i, corresponding to the ith conjugacy class of $\mathfrak{G}$. It is well known that these K_i form an R-basis for $\mathscr{Z}$ the center of $R[\mathfrak{G}]$. We need the following result of G. Glauberman which states that these are essentially characteristic elements of the group ring.

THEOREM C. *The class sums in $R[\mathfrak{G}]$ can be obtained canonically from the group ring up to factors of roots of unity in R. Moreover a consistent set of such class sums can be chosen.*

Proof. Define an inner product on $\mathscr{Z}$ by

$$(a, b)_0 = \sum_i \chi_i(a)\,\overline{\chi_i(b)}$$

where the χ_i are the characters of all irreducible representations of $\boldsymbol{C}[\mathfrak{G}] = \boldsymbol{C} \otimes_R R[\mathfrak{G}]$ and $\boldsymbol{C}$ is the field of complex numbers. This is clearly definable in the ring.

Write $a = \sum_i a_i K_i$ and $b = \sum_i b_i K_i$ where the K_i are the class sums and let n_i be the number of conjugate elements in the ith class. Then

$$(a, b)_0 = \sum_{ijk} a_j \bar{b}_k\, \chi_i(K_j)\,\overline{\chi_i(K_k)}\ .$$

But by the orthognality relations for the group characters we have $\sum_i \chi_i(K_j)\,\overline{\chi_i(K_k)} = n_j \delta_{jk} \mid \mathfrak{G} \mid$ so $(a, b)_0 = \mid \mathfrak{G} \mid \sum_j a_j \bar{b}_j n_j$.

Embed F in a normal extension of $\boldsymbol{Q}$ with Galois group $\mathscr{H}$. Set

$$(a, b) = 1/\mid \mathfrak{G} \mid \sum_{\sigma \in \mathscr{H}} (a, b)_0^\sigma = \sum_{j\sigma} a_j^\sigma \bar{b}_j^\sigma n_j\ .$$

Let $\mathfrak{B} = \{\beta_1, \cdots, \beta_r\}$ be an R-basis of $\mathscr{Z}$. We define the weight of $\mathfrak{B}$ to be

$$w(\mathfrak{B}) = \sum_i (\beta_i, \beta_i) .$$

In particular if $\mathfrak{B}_0$ is the basis $\{K_1, \cdots, K_r\}$ then

$$w(\mathfrak{B}_0) = |\mathscr{H}| \sum_j n_j = |\mathscr{H}| \, |\mathfrak{G}| .$$

On the other hand if $\mathfrak{B}$ is any other basis set with

$$\beta_i = \sum_j b_{ij} K_j$$

then

$$w(\mathfrak{B}) = \sum_{ij\sigma} |b_{ij}^{\sigma}|^2 n_j .$$

We can assume the subscripts so chosen that $b_{ii} \neq 0$. Then

$$w(\mathfrak{B}) \geqq \sum_{j\sigma} |b_{jj}^{\sigma}|^2 n_j \geqq |\mathscr{H}| \sum_j n_j = w(\mathfrak{B}_0) ,$$

with strict inequality unless $b_{ij} = 0$ for $i \neq j$ and $|b_{jj}^{\sigma}| = 1$ for all j, σ.

Now if an element and all its conjugates has absolute value one then it must be a root of unity. Hence the basis sets $\mathfrak{B}$ of minimal weight are those of the form $\{\varepsilon_i K_i\}$ where ε_i is a root of unity in R. This proves the first part of the result.

Choosing a consistent set of class sums is equivalent to choosing a principal character. Let λ: $R[\mathfrak{G}] \to R$ be any R-linear homomorphism of $R[\mathfrak{G}]$ onto R. There is at least one such, namely the principal character of $\mathfrak{G}$. Then there is a unique basis set $\mathfrak{B}$ of minimal weight with $\lambda(\beta_i) \in Z^+$ the positive integers. In fact if g_i is a representative of the ith class then

$$\lambda(\varepsilon_i K_i) = \varepsilon_i \lambda(g_i) \, n_i \in Z^+ ,$$

if and only if $\varepsilon_i = \bar{\lambda}(g_i)$ since $\lambda(g_i)$ is a root of unity. Moreover these classes form a consistent system since the R-automorphism of $R[\mathfrak{G}]$ defined by $g \to \bar{\lambda}(g)g$ maps $K_i \to \varepsilon_i K_i$. This completes the proof.

We assume for the remainder of this paper that a fixed consistent system of class sums has been chosen.

We will see below that $R[\mathfrak{G}]$ determines the set $\mathscr{N}$ of normal subgroups of $\mathfrak{G}$. On this set we of course have certain operations defined, for example the lattice operations and the function $|\ |$ which associates to each normal subgroup $\mathfrak{N}$ its order $|\mathfrak{N}|$. In this and the following section we will discuss these operations. In the case of nilpotent groups we will be able to give the complete result.

To each normal subgroup $\mathfrak{N}$ of $\mathfrak{G}$ we have associated the set of

class sums of elements in $\mathfrak{N}$. If we add these class sums in $R[\mathfrak{G}]$ we obtain

$$\hat{\mathfrak{N}} = \sum_{g \in \mathfrak{N}} g \in R[\mathfrak{G}] \ .$$

Clearly $(\hat{\mathfrak{N}})^2 = |\mathfrak{N}|\hat{\mathfrak{N}}$. Conversely let $A \in R[\mathfrak{G}]$ be a sum with positive integer coefficients of class sums such that $A^2 = nA$ for some integer n. Let $\{K_\alpha\}$ be the set of class sums which add to A. If say $K_{\alpha 1}K_{\alpha 2} = \sum_i a_i K_i$ and $a_i \neq 0$ then clearly K_i occurs in A^2 and so $K_i \in \{K_\alpha\}$. Now if we assume that all the coefficients are equal to one we see that there is a normal subgroup $\mathfrak{M}$ of $\mathfrak{G}$ with $A = \hat{\mathfrak{M}}$ since the set of all elements of $\mathfrak{G}$ belonging to the classes corresponding to the K_α form a normal multiplicatively closed subset of $\mathfrak{G}$. Thus the set $\mathscr{N}$ of all normal subgroups of $\mathfrak{G}$ is determined by $R[\mathfrak{G}]$.

Given $\hat{\mathfrak{N}}$ and $\hat{\mathfrak{M}}$ we see that $\widehat{\mathfrak{N} \cap \mathfrak{M}}$ is the sum of those class sums which occur in both $\hat{\mathfrak{N}}$ and $\hat{\mathfrak{M}}$ and $\widehat{\mathfrak{N}\mathfrak{M}} = 1/|\mathfrak{N} \cap \mathfrak{M}|\ \hat{\mathfrak{N}}\hat{\mathfrak{M}}$. The order of any normal subgroup is of course obtainable. For example $\hat{\mathfrak{N}}\hat{\mathfrak{G}} = |\mathfrak{N}|\hat{\mathfrak{G}}$. More generally given any $\gamma = \Sigma a_g\, g \in R[\mathfrak{G}]$ then

$$\gamma\hat{\mathfrak{G}} = (\Sigma a_g g)\,\hat{\mathfrak{G}} = (\Sigma a_g)\,\hat{\mathfrak{G}} \ .$$

Thus Σa_g is determined. This is of course the value of γ under the principal character of $\mathfrak{G}$.

Think of $R[\mathfrak{G}]$ as being embedded in $F[\mathfrak{G}]$. For any normal subgroup $\mathfrak{N}$ of $\mathfrak{G}$ define an R-linear map $\theta_{\mathfrak{N}}$ by

$$\theta_{\mathfrak{N}}(\gamma) = \gamma\hat{\mathfrak{N}}/|\mathfrak{N}| \ ,$$

for every $\gamma \in R[\mathfrak{G}]$. If $g,h \in \mathfrak{G}$ we have

$$\theta_{\mathfrak{N}}(g)\,\theta_{\mathfrak{N}}(h) = (g\hat{\mathfrak{N}}/|\mathfrak{N}|)\,(h\hat{\mathfrak{N}}/|\mathfrak{N}|) = gh\hat{\mathfrak{N}}/|\mathfrak{N}| = \theta_{\mathfrak{N}}(gh) \ .$$

Thus $\theta_{\mathfrak{N}}$ is a homomorphism. In fact it is not hard to see that $\theta_{\mathfrak{N}}$ is the natural homomorphism $R[\mathfrak{G}] \to R[\mathfrak{G}/\mathfrak{N}]$.

Since we can pick out the central subgroups of $\mathfrak{G}$ we can determine the terms of the upper central series $1 = \mathfrak{Z}_0 \subseteq \mathfrak{Z}_1 \subseteq \cdots$ where $\mathfrak{Z}_{i+1}/\mathfrak{Z}_i$ is the center of $\mathfrak{G}/\mathfrak{Z}_i$. Moreover for any normal subgroup $\mathfrak{N}$ of $\mathfrak{G}$ the group $(\mathfrak{N}, \mathfrak{G})$ is the smallest normal subgroup $\mathfrak{M} \subseteq \mathfrak{N}$ such that $\mathfrak{N}/\mathfrak{M}$ is central in $\mathfrak{G}/\mathfrak{M}$. In particular the terms of the lower central series are determined. This is the series $\mathfrak{G} = \Gamma^1 \supseteq \Gamma^2 \supseteq \cdots$ where $\Gamma^{i+1} = (\Gamma^i, \mathfrak{G})$. The last term of the upper central series which we might call $\mathfrak{Z}_\infty$ will be of importance later. $\mathfrak{G}$ is nilpotent if and only if $\mathfrak{G} = \mathfrak{Z}_\infty$.

Finally we point out that for each $\mathfrak{N}$ we can determine $\Phi(\mathfrak{N})$ the Frattini subgroup of $\mathfrak{N}$. Since $\Phi(\mathfrak{N})$ is characteristic in $\mathfrak{N}$ it is normal in $\mathfrak{G}$. Then $\Phi(\mathfrak{N})$ is the largest normal subgroup $\mathfrak{M}$ of $\mathfrak{G}$ contained in $\mathfrak{N}$ such that if $\mathfrak{M}$ and any set $\{K_\alpha\}$ of class sums generate $\mathfrak{N}$ then the $\{K_\alpha\}$ alone generates $\mathfrak{N}$. Note a set of classes generates a normal subgroup $\mathfrak{N}$ if $\mathfrak{N}$ is the smallest normal subgroup with $\hat{\mathfrak{N}}$ containing the class sums K_α.

This completes some of the more elementary remarks about $\mathscr{N}$. In the next section we discuss some additional results.

3. **Powers and commutators.** In $R[\mathfrak{G}]$ let Δ denote the R-linear subspace spanned by all Lie products $ab - ba$ with $a, b \in R[\mathfrak{G}]$. For any prime p let $\Delta_p = \Delta + pR[\mathfrak{G}]$. We have the following well known results (see [1] pg 411). For $g, h \in \mathfrak{G}$ let $g \sim h$ mean that g and h are conjugate then

1. $\Sigma a_g g \in \Delta$ if and only if for all $g \in \mathfrak{G}$ we have

$$\sum_{h \sim g} a_h = 0 .$$

2. $\Sigma a_g g \in \Delta_p$ if and only if for all $g \in \mathfrak{G}$

$$\sum_{h \sim g} a_h \in pR .$$

3. If $\gamma_1 \equiv \gamma_2 \bmod \Delta_p$ then $\gamma_1^p \equiv \gamma_2^p \bmod \Delta_p$.

As a consequence of (1) we have if $r \neq 0$ is an element of R and $r\gamma \in \Delta$ then $\gamma \in \Delta$.

PROPOSITION 2. With every class sum K_x in $R[\mathfrak{G}]$ and every integer n we can find the class sum K_{x^n} corresponding to the class of the nth powers of the elements of K_x.

Proof. It clearly suffices to assume $n = p$ is a prime. For every class K_x we have

$$K_x \equiv n_x x \bmod \Delta ,$$

where n_x is the number of terms in K_x and x is one such term. This follows from (1). Note $K_x \hat{\mathfrak{G}} = n_x \hat{\mathfrak{G}}$ so that n_x is determined by the class sum. Hence we can find $\gamma_x \in R[\mathfrak{G}]$ with $K_x \equiv n_x \gamma_x \bmod \Delta$. Choose one such γ_x for each class sum. We have $n_x(\gamma_x - x) \in \Delta$ so by our previous remarks $\gamma_x \equiv x \bmod \Delta$.

Thus by (3)

$$\gamma_x^p \equiv x^p \bmod \Delta_p \text{ and } \gamma_{x^p} \equiv x^p \bmod \Delta .$$

Hence there is a γ_y with

$$\gamma_x^p \equiv \gamma_y \mod \Delta_p .$$

But for this y we have $x^p \equiv y \mod \Delta_p$. Since $x^p, y \in \mathfrak{G}$ we see by (2) that y is conjugate to x^p. Hence $K_y = K_{x^p}$ and so the latter is determined.

This has many obvious consequences in terms of normal subgroups. For example the period of every normal subgroup is determined by $R[\mathfrak{G}]$. Clearly this settles most of the problems related to the class sum of powers of elements. More interesting is the problem of commutators.

We state first several commutator identities which will be of use ([4] pg 150).

4. $(x, y) = x^{-1}y^1xy$
5. $(y, x) = (x, y)^{-1}$
6. $(xy, z) = (x, z)\,(x, z, y)\,(y, z)$
7. $(x, yz) = (x, z)\,(x, y)\,(x, y, z)$
8. $(x, y^{-1}, z)^y\,(y, z^{-1}, x)^z\,(z, x^{-1}, y)^x = 1$

where $(x, y, z) = ((x, y), z)$ and $a^x = x^{-1}ax$. The last identity (8) has the following consequence known as the "Three Subgroups Lemma."

9. If $\mathfrak{L}, \mathfrak{M}, \mathfrak{N}$ are three normal subgroups of $\mathfrak{G}$ then

$$(\mathfrak{L}, \mathfrak{M}, \mathfrak{N}) \subseteq (\mathfrak{M}, \mathfrak{N}, \mathfrak{L})\,(\mathfrak{N}, \mathfrak{L}, \mathfrak{M}) .$$

Here $(\mathfrak{M}, \mathfrak{N})$ is the normal subgroup generated by all commutators (x, y) with $x \in \mathfrak{M}$ and $y \in \mathfrak{N}$ and $(\mathfrak{M}, \mathfrak{N}, \mathfrak{L}) = ((\mathfrak{M}, \mathfrak{N}), \mathfrak{L})$.

We will have need for the lemma given below. It is most likely true more generally, that is without the $\mathfrak{Z}_\infty$ assumption. However this is all that is needed.

For any normal subgroup $\mathfrak{N}$ of $\mathfrak{G}$ let $(\mathfrak{N})$ denote the ideal in $R[\mathfrak{G}]$ given by all γ with $\gamma\hat{\mathfrak{N}} = 0$. This is of course the kernel of $\theta_{\mathfrak{N}}$. Let $\gamma \in (\mathfrak{N})$ with $\gamma = \Sigma r_g g$. Let $\bar{g}$ denote a fixed coset representative of $g\mathfrak{N}$. Since $\theta_{\mathfrak{N}}(\gamma) = 0$ we see that $\Sigma r_g \bar{g} = 0$. Hence

$$\gamma = \Sigma r_g(g - \bar{g}) = \Sigma r_g(1 - \bar{g}g^{-1})g .$$

But $\bar{g}g^{-1} \in \mathfrak{N}$. Thus we see that $(\mathfrak{N})$ is spanned as an R-linear space by terms of the form $(1 - a)b$ with $a \in \mathfrak{N}$ and $b \in \mathfrak{G}$. Note that $(1 - a)b = b(1 - a^b)$ so this result is actually symmetric.

LEMMA 3. *Let $\mathfrak{L}, \mathfrak{M}, \mathfrak{N}$ be three normal subgroups of $\mathfrak{G}$ with $\mathfrak{L} \subseteq \mathfrak{M} \subseteq \mathfrak{N}$ and $\mathfrak{M} \subseteq \mathfrak{Z}_\infty$. Then*

$$(\mathfrak{L}) \cap (\mathfrak{M})\,(\mathfrak{N}) \subseteq (\mathfrak{L})\,(\mathfrak{N}) .$$

Proof. First suppose we know the result to be true if $\mathfrak{M}/\mathfrak{L}$ is

cyclic of prime order. Since $\mathfrak{M} \subseteqq \mathfrak{Z}_\infty$ we can find a principal series of $\mathfrak{G}$ joining $\mathfrak{L}$ to $\mathfrak{M}$ with cyclic quotients of prime order. Say

$$\mathfrak{L} = \mathfrak{L}_0 < \mathfrak{L}_1 < \cdots < \mathfrak{L}_n = \mathfrak{M} \subseteqq \mathfrak{N} .$$

Then

$$(\mathfrak{L}_i)(\mathfrak{N}) \supseteqq (\mathfrak{L}_i) \cap (\mathfrak{L}_{i+1})(\mathfrak{N})$$

and so

$$(\mathfrak{L})(\mathfrak{N}) \supseteqq (\mathfrak{L}_0) \cap (\mathfrak{L}_1) \cap \cdots \cap (\mathfrak{L}_{n-1}) \cap (\mathfrak{M})(\mathfrak{N}) .$$

But $\mathfrak{L}_i \supseteqq \mathfrak{L}$ implies that $(\mathfrak{L}_i) \supseteqq (\mathfrak{L})$ so $(\mathfrak{L})(\mathfrak{N}) \supseteqq (\mathfrak{L}) \cap (\mathfrak{M})(\mathfrak{N})$.

Hence we need only consider the case where $\mathfrak{M}/\mathfrak{L}$ is cyclic of prime order p. Let $\mathfrak{M} = \langle \mathfrak{L}, x \rangle$ with of course $x^p \in \mathfrak{L}$. Let $\{\varepsilon_j\}$ be a fixed set of coset representatives of $\mathfrak{N}/\mathfrak{M}$ and let $\{\delta_k\}$ be a set for $\mathfrak{G}/\mathfrak{N}$. Then $\{x^i \varepsilon_j \delta_k\}$ is a set of representatives of $\mathfrak{G}/\mathfrak{L}$.

Let $\gamma \in (\mathfrak{L}) \cap (\mathfrak{M})(\mathfrak{N})$. Since $\gamma \in (\mathfrak{M})(\mathfrak{N})$ we have

$$\gamma = \Sigma \rho_{abc} (1 - a)(1 - b)c$$

with $a \in \mathfrak{M}$, $b \in \mathfrak{N}$ and $c \in \mathfrak{G}$. Now $a = e\,x^i$ with $e \in \mathfrak{L}$ and

$$(1 - a) = (1 - e\,x^i) = (1 - e)x^i + (1 - x^i) .$$

But $(1 - e)x^i (1 - b)c \in (\mathfrak{L})(\mathfrak{N})$. Moreover

$$(1 - x^i) = (1 - x)(1 + x + \cdots + x^{i-1})$$

so we see that

$$\gamma \equiv (1 - x)\eta \mod (\mathfrak{L})(\mathfrak{N})$$

with $\eta \in (\mathfrak{N})$. We can clearly assume $\gamma = (1 - x)\eta$.

Write $\eta = \Sigma A_{ijk} x^i \varepsilon_j \delta_k$ with $A_{ijk} \in R[\mathfrak{L}]$ naturally embedded in $R[\mathfrak{G}]$. Let r_{ijk} be the sum of the coefficients of A_{ijk} that is $r_{ijk}\hat{\mathfrak{L}} = A_{ijk}\hat{\mathfrak{L}}$. Now $\gamma \in (\mathfrak{L})$ so $\hat{\mathfrak{L}}\gamma = 0$ and hence $x\hat{\mathfrak{L}}\eta = \hat{\mathfrak{L}}\eta$. Since

$$\hat{\mathfrak{L}}\eta = \Sigma r_{ijk}\, \hat{\mathfrak{L}} x^i \varepsilon_j \delta_k$$

we see from the above that r_{ijk} is in fact independent of i and we set $r_{ijk} = s_{jk}$. Thus

$$\hat{\mathfrak{L}}\eta = \Sigma s_{jk}\, \hat{\mathfrak{L}} x^i \varepsilon_j \delta_k .$$

Since $\hat{\mathfrak{N}}\eta = 0$ we have $\hat{\mathfrak{N}}\hat{\mathfrak{L}}\eta = 0$ and so for each k we have $\Sigma_j s_{jk} = 0$.

Now

$$\eta \equiv \Sigma r_{ijk}\, x^i \delta_j \varepsilon_k \mod (\mathfrak{L}) = (1 + x + \cdots + x^{p-1})\xi ,$$

where $\xi = \Sigma s_{jk} \varepsilon_j \delta_k$. But $\Sigma_j s_{jk} = 0$ so we see that $\xi \in (\mathfrak{N})$. Hence since $1 - x \in (\mathfrak{N})$ we have

$$\begin{aligned}\gamma = (1 - x)\eta &\equiv (1 - x)(1 + x + \cdots + x^{p-1})\xi \bmod (\mathfrak{N})(\mathfrak{L}) \\ &= (1 - x^p)\xi .\end{aligned}$$

But $1 - x^p \in (\mathfrak{L})$ so $\gamma \equiv 0 \bmod (\mathfrak{N})(\mathfrak{L})$ and the result follows.

For any $x \in \mathfrak{G}$ and $\mathfrak{N}$ normal in $\mathfrak{G}$ we set $(x, \mathfrak{N}) = (\mathfrak{N}, x)$ equal to the normal subgroup generated by all commutators of the form (x, y) with $y \in \mathfrak{N}$. This is easily seen to be the same as $(\langle x \rangle_n, \mathfrak{N})$ where $\langle x \rangle_n$ is the smallest normal subgroup containing x. If K_x is the class sum containing x then $(x, \mathfrak{G})$ is the smallest normal subgroup $\mathfrak{M}$ such that x is central in $R[\mathfrak{G}/\mathfrak{M}]$. Hence $\widehat{(x, \mathfrak{G})}$ is determined in $R[\mathfrak{G}]$.

We identify $\mathfrak{Z} = \mathfrak{Z}_1$ the center of $\mathfrak{G}$ with the set of those class sums K_i in $R[\mathfrak{G}]$ with $n_i = 1$. This is of course consistent with the natural embedding of $\mathfrak{G}$ in $R[\mathfrak{G}]$.

PROPOSITION 4. Let K_x and K_y be two class sums in $R[\mathfrak{G}]$. Suppose that $(x, \mathfrak{G}, y) = (y, \mathfrak{G}, x) = 1$. Moreover we assume that $(x, \mathfrak{G}) \cap (y, \mathfrak{G}) \subseteqq \mathfrak{Z}_\infty$. Then we can find $(x, y) \in \mathfrak{Z}$ in $R[\mathfrak{G}]$.

Proof. By (9) we see that $(y, x, \mathfrak{G}) = 1$ so that (x, y) is central. Now if x^g is conjugate to x and y^h to y then with $k = hg^{-1}$ and $u = (k, y^{-1})$ we have

$$(x^g, y^h) = (x, y^k)^g = (x, uy)^g .$$

Now $(x, uy) = (x, y)(x, u)(x, u, y)$ and since $u \in (y, \mathfrak{G})$ we have $(x, uy) = (x, y)$. But this is central so we have finally $(x^g, y^h) = (x, uy)^g = (x, y)^g = (x, y)$.

Let $\mathfrak{N} = (x, \mathfrak{G}) \cap (y, \mathfrak{G})$. As we mentioned above this is determined by $R[\mathfrak{G}]$ and K_x and K_y. Clearly $(x, y) \in \mathfrak{N} \cap \mathfrak{Z}$. Under the map $\theta_{\mathfrak{N}}$: $R[\mathfrak{G}] \to R[\mathfrak{G}/\mathfrak{N}]$, K_x maps onto a central element of the group ring. Since all the group elements in the image are conjugate, K_x must map onto some multiple say m_x of a class sum. Similarly for K_y. Hence if $x_1, \cdots, x_r$ and $y_1, \cdots, y_s$ are conjugates of x and y respectively which are a full set of coset representatives for each of the classes modulo $\mathfrak{N}$ we have

$$\begin{aligned}K_x \hat{\mathfrak{N}} &= m_x (x_1 + \cdots + x_r) \hat{\mathfrak{N}} \\ K_y \hat{\mathfrak{N}} &= m_y (y_1 + \cdots + y_s) \hat{\mathfrak{N}}\end{aligned}$$

Note that $\hat{\mathfrak{N}}$, m_x and m_y are determined in $R[\mathfrak{G}]$. Now choose $\gamma_x, \gamma_y \in R[\mathfrak{G}]$ and $z \in \mathfrak{N} \cap \mathfrak{Z}$ with

10. $m_x \gamma_x \hat{\mathfrak{N}} = K_x \mathfrak{M} \qquad m_y \gamma_y \hat{\mathfrak{N}} = K_y \hat{\mathfrak{N}}$

11. $\gamma_x \gamma_y = z \gamma_y \gamma_x$.

This system does have a solution. For example set $z = (x, y)$, $\gamma_x = (x_1 + \cdots + x_r)$ and $\gamma_y = (y_1 + \cdots + y_s)$. We show now that for any solution we must have $z = (x, y)$. This will show that (x, y) is determined in $R[\mathfrak{G}]$.

Write

$$\gamma_x = x_1 + \cdots + x_r + A \qquad \gamma_y = y_1 + \cdots + y_s + B$$

with $A, B \in R[\mathfrak{G}]$. Then by (10) and the above we see that $A \hat{\mathfrak{N}} = B \hat{\mathfrak{N}} = 0$.

By (11) we have

$$\begin{aligned} 0 = \gamma_x \gamma_y - z \gamma_y \gamma_x = &\sum_{ij} \{x_i y_j - z y_j x_i\} \\ &+ \sum_i \{A y_i - z y_i A\} + \sum_i \{x_i B - z B x_i\} \\ &+ \{AB - zBA\} . \end{aligned}$$

We study each of these four terms.

Clearly $\{AB - zBA\} \in (\mathfrak{N})\,(\mathfrak{N})$. Write $A = \Sigma A_\lambda \lambda$ where the $A_\lambda \in R[\mathfrak{N}]$ and the λ are coset representatives of $\mathfrak{G}/\mathfrak{N}$. Since $\hat{\mathfrak{N}} A = 0$ we see that $\hat{\mathfrak{N}} A_\lambda = 0$. Now y_i and z commute with $(x, \mathfrak{G})$ and hence with $\mathfrak{N}$. Thus

$$\begin{aligned} \sum_i \{A y_i - z y_i A\} &= \sum_{i\lambda} \{A_\lambda \lambda y_i - z y_i A_\lambda \lambda\} \\ &= \sum_\lambda A_\lambda \sum_i \{\lambda y_i - z y_i \lambda\} . \end{aligned}$$

Now $(\Sigma y_i) \hat{\mathfrak{N}}$ is central and $z \in \mathfrak{N}$ so we have $\hat{\mathfrak{N}} \sum_i \{\lambda y_i - z y_i \lambda\} = 0$. Thus

$$\sum_i \{A y_i - z y_i A\} \in (\mathfrak{N})\,(\mathfrak{N}) .$$

Similarly for the term $\sum_i \{x_i B - z B x_i\}$. Thus

12. $0 = \sum_{ij} \{x_i y_j - z y_j x_i\} + C$

where $C \in (\mathfrak{N})\,(\mathfrak{N})$.

Now $y_j x_i = x_i y_j (y_j, x_i) = x_i y_j (y, x)$. Let $w = z(y, x)$ and let $\mathfrak{Z}$ be the cyclic central subgroup generated by w. Since $z \in \mathfrak{N} \cap \mathfrak{Z}$, $(y, x) \in \mathfrak{N} \cap \mathfrak{Z}$ we have of course $\mathfrak{Z} \subseteqq \mathfrak{N} \cap \mathfrak{Z}$. Thus (12) becomes

13. $(1 - w) \sum_{ij} x_i y_j + C = 0$

and since $(1 - w) \hat{\mathfrak{Z}} = 0$ we have $C \hat{\mathfrak{Z}} = 0$.

Hence $C \in (\mathfrak{Z}) \cap (\mathfrak{N})\,(\mathfrak{N})$ and since $\mathfrak{N} \subseteqq \mathfrak{Z}_\infty$ we have by Lemma 3, $C \in (\mathfrak{Z})\,(\mathfrak{N})$. Now $(\mathfrak{Z})$ is clearly the principal ideal generated by $(1 - w)$ so $C = (1 - w)D$ with $D \in (\mathfrak{N})$. Set

$$E = \sum_{ij} x_i y_j + D .$$

By (13) and the above $(1 - w)E = 0$. Hence $E = wE = w^2E = \cdots$. Thus $\hat{\mathfrak{F}}E = |\mathfrak{F}| E$. Write $\hat{\mathfrak{N}} = (\Sigma\nu_i)\hat{\mathfrak{F}}$ where the ν_i are coset representatives of $\mathfrak{N}/\mathfrak{F}$. Then

$$\hat{\mathfrak{N}}E = (\Sigma\nu_i)\,\hat{\mathfrak{F}}E = |\mathfrak{F}|\,(\Sigma\nu_i)E .$$

On the other hand since $\hat{\mathfrak{N}}D = 0$ we have

$$\hat{\mathfrak{N}}E = \sum_{ij} x_i y_j \hat{\mathfrak{N}} .$$

Hence

14. $|\mathfrak{F}|\,\Sigma\nu_i E = \sum_{ij} x_i y_j \hat{\mathfrak{N}}$.

Let ρ be the coefficient of x_1y_1 in $\Sigma\nu_i E$. Then the coefficient of x_1y_1 on the left hand side of (14) is $|\mathfrak{F}|\rho$. Now if $x_iy_j \equiv x_1y_1 \bmod \mathfrak{N}$ then $x_1^{-1}x_i \equiv y_1y_j^{-1}$. But $x_1^{-1}x_i \in (x, \mathfrak{G})$, $y_1y_j^{-1} \in (y, \mathfrak{G})$ and $\mathfrak{N} = (x, \mathfrak{G}) \cap (y, \mathfrak{G})$ so both terms are in $\mathfrak{N}$. By our choice of the sets $\{x_i\}$ and $\{y_j\}$ this implies that $i = 1$, $j = 1$. Hence the coefficient of x_1y_1 on the right hand side of (14) is 1. Thus $\rho|\mathfrak{F}| = 1$. Then $1/|\mathfrak{F}| \in R \cap \boldsymbol{Q} = \boldsymbol{Z}$ and so $|\mathfrak{F}| = 1$. This means that $w = 1$ and therefore $z = (x, y)$.

By our previous remarks this completes the proof.

For convenience we introduce the following notation. We say class sum K_x "belongs to" subgroup $\mathfrak{H}$ or "$K_x \in \mathfrak{H}$" if all the elements of the conjugacy class associated with K_x belong to $\mathfrak{H}$. In particular if $\mathfrak{H}$ is normal in $\mathfrak{G}$ then $K_x \in \mathfrak{H}$ if and only if $x \in \mathfrak{H}$. With this we have the following numerous set of corollaries for the previous proposition.

COROLLARY 5. *Let $K_x \in \Gamma^i$ and $K_y \in \Gamma^j$. Then $R[\mathfrak{G}]$ determines (x, y) modulo Γ^{i+j+1}.*

Proof. It clearly suffices to assume $\Gamma^{i+j+1} = 1$. Then $\mathfrak{G}$ is nilpotent so $\mathfrak{G} = \mathfrak{Z}_\infty$. Now $(x, \mathfrak{G}, y) \subseteq \Gamma^{i+j+1} = 1$ and $(y, \mathfrak{G}, x) = 1$. Hence by the above (x, y) is determined by K_x, K_y and $R[\mathfrak{G}]$.

COROLLARY 6. *Let $K_x \in \mathfrak{Z}_2$. Then for any class sum K_y the commutator $(x, y) \in \mathfrak{Z}$ is determined by $R[\mathfrak{G}]$.*

Proof. Since $x \in \mathfrak{Z}_2$, $(x, \mathfrak{G}) \subseteq \mathfrak{Z} \subseteq \mathfrak{Z}_\infty$. Thus we have $(x, \mathfrak{G}, y) = 1$, $(y, x, \mathfrak{G}) = 1$ and by the three subgroups lemma $(y, \mathfrak{G}, x) = 1$. Hence by Proposition 4 the result follows.

COROLLARY 7. *Let $K_x \in \mathfrak{Z}_{n+1}$. Let $K_{y_1}, \cdots, Ky_n$ be any n class*

sums of $\mathfrak{G}$ *not necessarily distinct. Then* $(x, y_1, \cdots, y_n) \in \mathfrak{Z}$ *is determined by* $R[\mathfrak{G}]$.

Proof. By induction on n, $n = 0$ being trivial. Under the map $R[\mathfrak{G}] \to R[\mathfrak{G}/\mathfrak{Z}]$, x maps to $\bar{x} \in \mathfrak{Z}_n(\mathfrak{G}/\mathfrak{Z})$. Hence $(\bar{x}, \bar{y}_1, \cdots, \bar{y}_{n-1}) = (x, y_1, \cdots, y_{n-1})$ mod $\mathfrak{Z}$ is determined. Since $(x, y_1, \cdots, y_{n-1}) \in \mathfrak{Z}_2$ we see by Corollary 6 that $((x, y_1, \cdots, y_{n-1}), y_n) = (x, y_1, \cdots, y_n)$ is determined.

COROLLARY 8. *Let* K_x *and* K_y *belong to* $\mathfrak{Z}_\infty$. *Then* $R[\mathfrak{G}]$ *determines* $\langle (x, y) \rangle_n$ *the normal subgroup generated by all commutators* (x^g, y^h).

Proof. We say that class sums K_x and K_y "commute" if the elements of $\mathfrak{G}$ belonging to the class corresponding to K_x commute with all those elements corresponding to K_y. Since $\langle (x, y) \rangle_n$ is the smallest normal subgroup $\mathfrak{M}$ such that K_x and K_y commute modulo $\mathfrak{M}$ it suffices to show that we can decide in $R[\mathfrak{G}]$ whether two class sums commute.

If $K_x \in \mathfrak{Z}_i$ and $K_y \in \mathfrak{Z}_j$ we prove this by induction on $i + j$. For $i + j \leqq 2$ the result is trivial. If K_x and K_y commute then every x^g commutes with $y^h y^{-1}$. Hence K_x commutes with every class sum in $(y, \mathfrak{G})$. Since $(y, \mathfrak{G}) \subseteqq \mathfrak{Z}_{j-1}$ we can check to see whether this occurs by induction. The result is determined provided $(y, \mathfrak{G}, x) \neq 1$. So we assume $(y, \mathfrak{G}, x) = 1$. Similarly we can assume $(x, \mathfrak{G}, y) = 1$. Since $(x, \mathfrak{G}) \subseteqq \mathfrak{Z}_\infty$ the result follows from Proposition 4.

This in turn yields the result that if $\mathfrak{N}$ and $\mathfrak{M}$ are normal subgroups of $\mathfrak{G}$ contained in $\mathfrak{Z}_\infty$ then $(\mathfrak{N}, \mathfrak{M})$ is determined. We now group together our results on operations on the set of normal subgroups of $\mathfrak{G}$. Since the results are complete for nilpotent $\mathfrak{G}$ we state this as a separate theorem.

THEOREM D. *Suppose* $R[\mathfrak{G}] \cong R[\mathfrak{H}]$. *Then there is a one-to-one correspondence between the set,* $\mathscr{N}(\mathfrak{G})$, *of normal subgroups of* $\mathfrak{G}$ *and* $\mathscr{N}(\mathfrak{H})$ *which preserves the following*:

1. *the upper and lower central series and in particular the group* $\mathfrak{Z}_\infty$
2. *the lattice operations* $\mathfrak{N} \cap \mathfrak{M}$ *and* $\mathfrak{N}\mathfrak{M}$
3. *the order and period of every normal subgroup. In fact the number of elements of* $\mathfrak{N}$ *having any given order is determined.*
4. *The groups* $(\mathfrak{G}, \mathfrak{N})$, $\Phi(\mathfrak{N})$, $C^n(\mathfrak{N})$ *and* $C_n(\mathfrak{N})$ *where the latter two are the subgroups of* $\mathfrak{N}$ *generated by all* n*th powers of elements*

of $\mathfrak{N}$ *and the subgroup generated by all elements of* $\mathfrak{N}$ *whose order divides* n

5. *the group* $(\mathfrak{M}, \mathfrak{N})$ *if both* $\mathfrak{M}, \mathfrak{N} \subseteq \mathfrak{Z}_\infty$.

THEOREM E. *Suppose* $R[\mathfrak{G}] \cong R[\mathfrak{H}]$ *and* $\mathfrak{G}$ *is nilpotent. Then there is a one-to-one correspondence between* $\mathcal{N}(\mathfrak{G})$ *and* $\mathcal{N}(\mathfrak{H})$ *preserving*

1. *the lattice operations* $\mathfrak{N} \cap \mathfrak{M}$ *and* $\mathfrak{N}\mathfrak{M}$

2. *the order and period of every normal subgroup. In fact the number of elements of* $\mathfrak{N}$ *having any given order is determined.*

3. *the group* $(\mathfrak{M}, \mathfrak{N})$ *and in particular* $\mathfrak{N}'$. *Thus the terms of the derived series of* $\mathfrak{G}$ *are determined.*

4. *the groups* $\Phi(\mathfrak{N})$, $C^n(\mathfrak{N})$ *and* $C_n(\mathfrak{N})$.

In the next section we study some specific examples.

4. Two special cases. In terms of its structure and its representations the abelian groups are of course the simplest. Perhaps the next simplest in structure are the nilpotent groups of class 2. On the other hand in terms of its representations the next simplest are the p-groups of type (p), that is p-groups with irreducible representations of degree 1 and p only. We study both cases here.

As a consequence of Theorem C we see that we can find the elements of $\mathfrak{Z}(\mathfrak{G})$ in $R[\mathfrak{G}]$ and hence $R[\mathfrak{G}]$ determines the center of $\mathfrak{G}$. We show now that the structure of the second center is also determined.

THEOREM F. *Let* $R[\mathfrak{G}] \cong R[\mathfrak{H}]$. *Then* $\mathfrak{Z}_2(\mathfrak{G}) \cong \mathfrak{Z}_2(\mathfrak{H})$. *In particular if* $\mathfrak{G}$ *is nilpotent of class* 2 *then* $R[\mathfrak{G}] \cong R[\mathfrak{H}]$ *implies* $\mathfrak{G} \cong \mathfrak{H}$.

It is interesting to point out that the groups studied in Theorem B are all class 2. This shows the marked difference between considering the group algebra $\boldsymbol{Q}[\mathfrak{G}]$ and the group ring $R[\mathfrak{G}]$.

Proof. We identify $R[\mathfrak{G}]$ and $R[\mathfrak{H}]$. Let $\mathfrak{Z}$ be the common center of $\mathfrak{G}$ and $\mathfrak{H}$. Choose class sums $K_{x_1}, \cdots, K_{x_n}$ in $\mathfrak{Z}_2$ so that their images under the natural map $R[\mathfrak{G}] \to R[\mathfrak{G}/\mathfrak{Z}]$ are multiples of a basis for the abelian group $\mathfrak{Z}(\mathfrak{G}/\mathfrak{Z}) = \mathfrak{Z}(\mathfrak{H}/\mathfrak{Z})$.

Then $\mathfrak{Z}_2(\mathfrak{G})$ and $\mathfrak{Z}_2(\mathfrak{H})$ are generated by $x_1, \cdots, x_n$ and $\mathfrak{Z}$. By Corollary 6, the commutators $(x_i, x_j) \in \mathfrak{Z}$ are uniquely determined in $R[\mathfrak{G}]$. Also by Proposition 2 we can find the order α_i of x_i mod $\mathfrak{Z}$ and in fact find $x_i^{\alpha_i} \in \mathfrak{Z}$. Thus clearly $\mathfrak{Z}_2(\mathfrak{G}) \cong \mathfrak{Z}_2(\mathfrak{H})$.

We digress for a moment to mention a few obvious additional results.

PROPOSITION 9. Let $\mathfrak{G}$ be nilpotent. Suppose $R[\mathfrak{G}] \cong R[\mathfrak{H}]$. Then there is a one-to-one correspondence between the set of normal abelian subgroups $\mathscr{A}(\mathfrak{G})$ of $\mathfrak{G}$ and $\mathscr{A}(\mathfrak{H})$ such that corresponding groups are isomorphic and inclusions are preserved.

Proof. In the correspondence given in Theorem E, we see by (3) that the abelian normal subgroups correspond. Moreover by (2) the number of elements of any given order in the subgroup is determined so in fact the isomorphism class of that subgroup is also determined.

PROPOSITION 10. Let $R[\mathfrak{G}] \cong R[\mathfrak{H}]$. Suppose that $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2$. Then $\mathfrak{H} = \mathfrak{H}_1 \times \mathfrak{H}_2$ with $R[\mathfrak{G}_1] \cong R[\mathfrak{H}_1]$ and $R[\mathfrak{G}_1] \cong R[\mathfrak{H}_2]$.

Proof. Under the correspondence of Theorem D, let $\mathfrak{H}_i$ correspond to $\mathfrak{G}_i$. Then $\mathfrak{H}_1\mathfrak{H}_2 = \mathfrak{H}$ and $\mathfrak{H}_1 \cap \mathfrak{H}_2 = 1$ clearly. Finally $R[\mathfrak{H}_1] \cong R[\mathfrak{H}/\mathfrak{H}_2] \cong R[\mathfrak{G}/\mathfrak{G}_2] \cong R[\mathfrak{G}_1]$ so the result follows.

As a consequence of the above we see that it suffices to assume that $\mathfrak{G}$ is indecomposable. In particular in studying nilpotent groups we can really restrict our attention to p-groups.

In the characterization of groups of type (p) one possibility which can occur is $|\mathfrak{G}/\mathfrak{Z}| = p^3$. We consider this case first.

PROPOSITION 11. Let $\mathfrak{G}/\mathfrak{Z}$ be a p-group with $|\mathfrak{G}/\mathfrak{Z}| \leqq p^3$. If $R[\mathfrak{G}] \cong R[\mathfrak{H}]$ then $\mathfrak{G} \cong \mathfrak{H}$. In particular if $\mathfrak{G}$ is a p-group of order $\leqq p^4$ then $R[\mathfrak{G}] \cong R[\mathfrak{H}]$ implies $\mathfrak{G} \cong \mathfrak{H}$.

Proof. We first note that all such groups are nilpotent. Also $R[\mathfrak{G}] \cong R[\mathfrak{H}]$ implies that $R[\mathfrak{G}/\mathfrak{Z}] \cong R[\mathfrak{H}/\mathfrak{Z}]$. But the latter groups are abelian or class 2 so $\mathfrak{G}/\mathfrak{Z} \cong \mathfrak{H}/\mathfrak{Z}$. We consider the possibilities for $\bar{\mathfrak{G}} = \mathfrak{G}/\mathfrak{Z}$.

If $|\bar{\mathfrak{G}}| = p^2$ then $\bar{\mathfrak{G}}$ is abelian and $\mathfrak{G}$ is class 2. So the result follows in this case by Theorem F. We assume $|\bar{\mathfrak{G}}| = p^3$. Suppose $\bar{\mathfrak{G}}$ is generated by cyclic subgroups $\mathfrak{F}_\alpha$ with $\bigcap \mathfrak{F}_\alpha > 1$. Then each $\mathfrak{Z}\mathfrak{F}_\alpha$ is abelian and together they generate $\mathfrak{G}$. Hence $\bigcap \mathfrak{Z}\mathfrak{F}_\alpha$ is central. But $\bigcap \mathfrak{Z}\mathfrak{F}_\alpha > \mathfrak{Z}$ so this is a contradiction. Hence $\bar{\mathfrak{G}}$ cannot have this property.

For $|\bar{\mathfrak{G}}| = p^3$ we see easily that the only possibilities are:

(i) elementary abelian

(ii) dihedral $(p = 2)$

(iii) non-abelian of period p $(p > 2)$.

The first case is again class 2. We consider case (ii).

Choose class sums K_a and K_b such that K_a corresponds to an

element of order 4 in $\mathfrak{G}/\mathfrak{Z}$ and K_b to an element not in the cyclic group generated by a. In $\mathfrak{G}$ and $\mathfrak{H}$ we have

$$a^4 = z_1 \qquad b^2 = z_2 \qquad b^{-1}ab = a^{-1}z_3 ,$$

with z_1, z_2, and z_3 in $\mathfrak{Z}$. By Proposition 2, z_1 and z_2 are determined. Finally $K_a = a + a^{-1}z_3$ so we have

$$(K_a)^2 = a^2 + a^{-2}z_3^2 + 2z_3 = K_{a^2} + 2z_3 .$$

Hence z_3 is determined and clearly $\mathfrak{G} \cong \mathfrak{H}$.

We need only consider case (iii). Choose class sums K_a and K_b which modulo $\mathfrak{Z}_2$ form a basis for $\mathfrak{G}/\mathfrak{Z}_2$. Then $\mathfrak{G}$ is generated by a, b, c and $\mathfrak{Z}$ with

$$\begin{aligned} a^p = z_1 \qquad & b^p = z_2 \qquad & c^p = z_3 \\ (c,\ a) = z_4 \qquad & (c,\ b) = z_5 \qquad & (a,\ b) = c , \end{aligned}$$

and z_1, z_2, z_3, z_4 and z_5 are elements of $\mathfrak{Z}$.

By Proposition 2, z_1 and z_2 are determined. Since $a,\ b \in \mathfrak{Z}_3$ we have by Corollary 7

$$z_4 = (c,\ a) = (a,\ b,\ a) \qquad z_5 = (c,\ b) = (a,\ b,\ a) ,$$

are determined. This leaves only z_3. However we show below that z_3 must be 1. This will clearly yield the result.

We use the commutator identity

$$(u,\ vw) = (u,\ w)\ (u,\ v)\ (u,\ v,\ w)$$

to conclude

$$(a,\ b^{i+1}) = (a,\ b^i)\ (a,\ b)\ (a,\ b,\ b^i) = (a,\ b^i)\ c\,(c,\ b^i) .$$

Since $(c,\ b^i)$ is central we obtain

$$(a,\ b^p) = c^p(c,\ b)\ (c,\ b^2)\cdots(c,\ b^{p-1}) .$$

But $b^p \in \mathfrak{Z}$ so $(a,\ b^p) = 1$. Now $c \in \mathfrak{Z}_2$ so using again the above identity we have

$$(c,\ uv) = (c,\ v)\ (c,\ u)\ (c,\ u,\ v) = (c,\ u)\ (c,\ v)$$

since $(c,\ u)$ and $(c,\ v)$ are central. Hence

$$(c,\ b)\ (c,\ b^2)\cdots(c,\ b^{p-1}) = (c,\ b^n)$$

where $n = 1 + 2 + \cdots + (p-1) = p(p-1)/2$ is divisible by p since $p > 2$. Then $b^n \in \mathfrak{Z}$ and $(c,\ b^n) = 1$. Therefore $c^p = 1$ and the result follows.

We will have need for the following

LEMMA 12. *Let $\mathfrak{A}$ be a normal abelian subgroup of $\mathfrak{G}$ with $\mathfrak{G}/\mathfrak{A}$ cyclic. Suppose $x \in \mathfrak{G}$ generates the quotient. Then the map $a \to (a, x)$ is a homomorphism of $\mathfrak{A}$ onto $\mathfrak{G}'$ with kernel $\mathfrak{Z} \cap \mathfrak{A}$.*

Proof. First $(a, x) = a^{-1}a^x$ is the product of two endomorphisms of abelian group $\mathfrak{A}$. Hence $a \to (a, x)$ is also an endomorphism of $\mathfrak{A}$. Let $\mathfrak{B} \subseteq \mathfrak{A}$ be its image.

Clearly $\mathfrak{B} \subseteq \mathfrak{G}'$. Now $N(\mathfrak{B}) \supseteq \mathfrak{A}$ and $(a, x)^x = (a^x, x)$ and this is contained in $\mathfrak{B}$ so $N(\mathfrak{B}) \supseteq \langle \mathfrak{A}, x \rangle = \mathfrak{G}$. Hence $\mathfrak{B}$ is normal in $\mathfrak{G}$. Since $\mathfrak{G}/\mathfrak{B} = \langle \mathfrak{A}/\mathfrak{B}, \bar{x} \rangle$ and $\bar{x}$ commutes with $\mathfrak{A}/\mathfrak{B}$ we see that $\mathfrak{G}/\mathfrak{B}$ is abelian. Thus $\mathfrak{B} \supseteq \mathfrak{G}'$ and so $\mathfrak{B} = \mathfrak{G}'$.

If $a \in \mathfrak{Z} \cap \mathfrak{A}$ then $(a, x) = 1$. Conversely if $(a, x) = 1$ then $C(a) \supseteq \langle \mathfrak{A}, x \rangle = \mathfrak{G}$ so a is central. This completes the proof.

Suppose $|\mathfrak{G}/\mathfrak{A}| = p$. If $x \notin \mathfrak{A}$ then $x^p \in \mathfrak{A}$ and $C(x^p) \supseteq \langle \mathfrak{A}, x \rangle = \mathfrak{G}$ so $x^p \in \mathfrak{Z}$. We make the simplifying assumption that $\mathfrak{G}/\mathfrak{Z}$ has period p.

PROPOSITION 13. Let $\mathfrak{G}$ be a non-abelian p-group with an abelian subgroup of index p. Suppose also that $\mathfrak{G}/\mathfrak{Z}$ has period p. Then $R[\mathfrak{G}] \cong R[\mathfrak{H}]$ implies $\mathfrak{G} \cong \mathfrak{H}$.

Proof. By Proposition 2, $\mathfrak{H}/\mathfrak{Z}$ has period p. Also by Proposition 9, $\mathfrak{H}$ has an abelian subgroup of index p. Hence it suffices to show that under these assumptions $R[\mathfrak{G}]$ determines $\mathfrak{G}$. By Lemma 12, $\mathfrak{G}' \cong \mathfrak{A}/\mathfrak{Z}$ so $\mathfrak{G}'$ has period p.

Choose $\hat{\mathfrak{A}}$ in $R[\mathfrak{G}]$ with $\mathfrak{A}$ normal and abelian of index p and let K_x be a class sum not in $\mathfrak{A}$. Choose normal subgroups $\mathfrak{N}_1, \mathfrak{N}_2, \cdots, \mathfrak{N}_r$ such that (i) $\mathfrak{A} \supseteq \mathfrak{N}_i > \mathfrak{Z}$, (ii) the $\bar{\mathfrak{N}}_i = \mathfrak{N}_i/\mathfrak{Z}$ direct sum to $\bar{\mathfrak{A}} = \mathfrak{A}/\mathfrak{Z}$ and (iii) the $\bar{\mathfrak{N}}_i$ are indecomposable, that is we cannot find normal $\bar{\mathfrak{M}}$ and $\bar{\mathfrak{N}}$ both > 1 with $\bar{\mathfrak{N}}_i = \bar{\mathfrak{M}} \times \bar{\mathfrak{N}}$. Of course such a choice can be made in $R[\mathfrak{G}]$.

We have $\bar{\mathfrak{A}} = \bar{\mathfrak{N}}_1 \times \bar{\mathfrak{A}}_2 \times \cdots \times \bar{\mathfrak{N}}_r$. $\bar{\mathfrak{A}}$ can be viewed additively as a vector space over $GF(p)$. If $\bar{x}$ is x mod $\mathfrak{Z}$ then $\bar{x}$ acts on $\bar{\mathfrak{A}}$ as a linear transformation of order p. Moreover $\bar{x}$ acts on each $\bar{\mathfrak{N}}_i$ a b_i-dimensional subspace. Since $\bar{\mathfrak{N}}_i$ is indecomposable, by an appropriate choice of basis, $\bar{x}$ on $\bar{\mathfrak{N}}_i$ has the Jordan form

$$\bar{x} = \begin{pmatrix} 1 & 1 & & & 0 \\ & 1 & 1 & & \\ & & 1 & \cdot & \\ & & & \cdot & 1 \\ 0 & & & & 1 \end{pmatrix}.$$

In fact let $v \in \bar{\mathfrak{N}}_i$ be any element such that $\bar{\mathfrak{N}}_i$ is the smallest normal subgroup containing v, then we can assume that the first vector in the above basis is v.

Now choose K_{g_i} in $\mathfrak{N}_i$ so that $\mathfrak{N}_i$ is the smallest normal subgroup containing K_{g_i} and $\mathfrak{Z}$. Such a class sum clearly exists in view of the above form for $\bar{x}$. Then we see that $\mathfrak{G}$ is generated by x, g_{ij} and $\mathfrak{Z}$ with $j = 1, 2, \cdots, b_i$ subject to the relations

$$(g_{ij}, x) = g_{i,j+1} \quad \text{for} \quad j \leqq b_i - 1, \ (g_{i,b_i}, x) = z_i$$
$$g_{i1}^p = w_i, \ g_{ij}^p = 1 \quad \text{for} \quad j \geqq 2, \ x^p = w_0$$

and $$(g_{ij}, g_{st}) = 1$$

with the w_i and z_i in $\mathfrak{Z}$.

Here we have set

$$g_{i1} = g_i \quad \text{and} \quad g_{ij} = (g_i \underbrace{x, x, \cdots, x}_{j-1}).$$

That $g_{ij}^p = 1$ for $j \geqq 2$ follows from the fact that $\mathfrak{G}'$ has period p. By Proposition 2, the w_i are determined. Also we have clearly $g_i \in \mathfrak{Z}_{b_i+1}$ so by Corollary 7

$$z_i = (g_i, \underbrace{x, x, \cdots, x}_{b_i}),$$

is determined by K_{g_i} and K_x. Hence the result follows.

THEOREM G. *Let $\mathfrak{G}$ be a p-group of type (p). Suppose that $\mathfrak{G}/\mathfrak{Z}$ has period p. Then $R[\mathfrak{G}] \cong R[\mathfrak{H}]$ implies $\mathfrak{G} \cong \mathfrak{H}$.*

Proof. In the characterization of p-groups of type (p) ([6] Theorem 2.3) the following possibilities can occur. Either $\mathfrak{G}$ has a center $\mathfrak{Z}$ with $|\mathfrak{G}/\mathfrak{Z}| = p^3$ or $\mathfrak{G}$ has a normal abelian subgroup of index p. The first case has been handled in Proposition 11 and the second in Proposition 13. Thus the result follows.

COROLLARY 14. *Let $\mathfrak{G}$ be a p-group of type (p). Suppose that*

$\mathfrak{G}/\mathfrak{Z}$ *is regular. Then* $R[\mathfrak{G}] \cong R[\mathfrak{H}]$ *implies* $\mathfrak{G} \cong \mathfrak{H}$. *In particular if* $\mathfrak{G}$ *has class at most* p *then the result follows.*

Proof. The assumption of $\mathfrak{G}/\mathfrak{Z}$ is only used in the case where $\mathfrak{G}$ has an abelian subgroup of index p. In this case clearly $\mathfrak{G}/\mathfrak{Z}$ is generated by all elements not in $\mathfrak{A}/\mathfrak{Z}$. But these all have period p. Hence by ([4] Theorem 12.4.3) $\mathfrak{G}/\mathfrak{Z}$ has period p. The second result follows from the well known sufficient condition for regularity ([4] pg 183).

We should mention here a simple result ([3] Theorem 2.1) on group algebras of p-groups of type (p).

PROPOSITION 15. Let $\mathfrak{G}$ and $\mathfrak{H}$ be p-groups of type (p) with $p > 2$. Then for any field K whose characteristic is prime to p we have $K[\mathfrak{G}] \cong K[\mathfrak{H}]$ if any only if $\mathfrak{G}/\mathfrak{G}' \cong \mathfrak{H}/\mathfrak{H}'$ and the centers of $K[\mathfrak{G}]$ and $K[\mathfrak{H}]$ are isomorphic.

This again shows the great difference between group rings and algebras.

We can now discuss the groups of order p^5. For simplicity we assume $p \geqq 5$ so that all groups considered will be regular.

PROPOSITION 16. Let $\mathfrak{G}$ be a group of order p^5 with $p \geqq 5$. If $R[\mathfrak{G}] \cong R[\mathfrak{H}]$ then $\mathfrak{G} \cong \mathfrak{H}$.

Proof. If $|\mathfrak{G}/\mathfrak{Z}| \leqq p^3$ then the result follows by Proposition 11. So we assume $|\mathfrak{G}/\mathfrak{Z}| = p^4$. As in the proof of that proposition, $\bar{\mathfrak{G}} = \mathfrak{G}/\mathfrak{Z}$ cannot be generated by cyclic groups $\mathfrak{F}_\alpha$ with $\bigcap \mathfrak{F}_\alpha > 1$. With this we conclude from the table of groups of order p^4 ([2] pg. 145) that the only possibilities are:

(i) abelian of type (p^2, p^2)

(ii) abelian of type (p, p, p, p)

(iii) the group generated by a and b subject to $a^{p^2} = b^{p^2} = 1$ and $(a, b) = a^p$

(iv) direct product of a cyclic group of order p with the non-abelian group of order p^3 and period p

(v) the group generated by a, b, c, d subject to $a^p = b^p = c^p = d^p = 1$, $b = (c, d)$, $a = (b, d)$ and $(a, d) = (b, c) = (a, c) = (a, b) = 1$.

Using regularity the computation to conclude the above is quite easy. For example consider the group $\bar{\mathfrak{G}}$ generated by a, b, c subject to

$$a^{p^2} = b^p = c^p = 1,\ (a, b) = a^p,\ (a, c) = b \text{ and } (b, c) = 1\ .$$

Its commutator subgroup is clearly generated by a^p and b both of order p. Hence by regularity $\mathfrak{G}'$ has period p. Thus for any $x, y \in \bar{\mathfrak{G}}$ we have $(xy)^p = x^p y^p$. In particular $(ab)^p = a^p$ and $(ac)^p = a^p$. Hence $\bar{\mathfrak{G}}$ is generated by a, ab and ac all having the same pth power.

If $R[\mathfrak{G}] \cong R[\mathfrak{H}]$ then $R[\mathfrak{G}/\mathfrak{Z}] \cong R[\mathfrak{H}/\mathfrak{Z}]$. But $|\mathfrak{G}/\mathfrak{Z}| = p^4$ so by Proposition 11, $\mathfrak{G}/\mathfrak{Z} \cong \mathfrak{H}/\mathfrak{Z}$. Hence we can consider each of the above cases separately.

Now cases (i) and (ii) yield groups $\mathfrak{G}$ of class 2. Hence by Theorem F the result follows here. We consider case (iii) and in fact show that there is only one such group. This will of course yield the result.

In $\mathfrak{G}$ we have elements a and b with $\mathfrak{G} = \langle a, b, \mathfrak{Z} \rangle$ and

$$a^{p^2} = z_1 \quad b^{p^2} = z_2 \quad b^{-1}ab = a^{1+p}z_3$$

where z_1, z_2 and z_3 are elements of $\mathfrak{Z}$. Then

$$b^{-1}a^p b = (b^{-1}ab)^p = a^{(1+p)p}\, z_3^p = a^p z_1 .$$

Since a^p is not central we see that $z_1 \neq 1$. Hence a generates a cyclic normal subgroup of order p^3. Now b^p is not central so b acts as an element of order p^2 on $\langle a \rangle$. Since for p odd the automorphism group of a cyclic p-group is cyclic, by replacing b by a suitable power if necessary, we can assume that $b^{-1}ab = a^{1+p}$. Finally if $b^{p^2} = a^{p^2 j}$ then $(ba^{-j})^{p^2} = 1$ since $\mathfrak{G}$ is regular and $\mathfrak{G}'$ has period p^2. Moreover ba^{-j} acts in the same manner as b on $\langle a \rangle$. Hence we see that there is only one such group.

In the last two cases $\mathfrak{G}/\mathfrak{Z}$ has period p. Hence by regularity $\mathfrak{G}'$ has period p. Case (iv) follows in a manner similar to (iii) of Proposition 11. $\mathfrak{G}$ is a direct product so we can find $\hat{\mathfrak{F}}$ and $\hat{\mathfrak{N}}$ in $R[\mathfrak{G}]$ with $|\mathfrak{F}| = p$, $|\mathfrak{N}| = p^3$ and $\mathfrak{F} \cap \mathfrak{N} = 1$. Choose class sum K_d in $R[\mathfrak{G}]$ which maps to a generator of $\mathfrak{F}$ in $R[\mathfrak{G}] \to R[\mathfrak{G}/\mathfrak{Z}]$ and choose class sums K_a and K_b which yield generators of $\mathfrak{N}$ modulo its center. Then $\mathfrak{G}$ is generated by $\mathfrak{Z}$, a, b, c and d subject to

$$a^p = z_1 \quad b^p = z_2 \quad c^p = z_3 \quad d^p = z_4 \quad (a, b) = c$$
$$(a, c) = z_5 \quad (b, c) = z_6 \quad (d, a) = z_7 \quad (d, b) = z_8 \quad (d, c) = z_9 ,$$

with $z_i \in \mathfrak{Z}$. By Proposition 2, z_1, z_2 and z_4 are determined. Since $c \in \mathfrak{G}'$ we have $c^p = 1$. By Corollaries 6 and 7, z_5, z_6, z_7, and z_8 are determined. Finally $d \in \mathfrak{Z}_2$ and $c \in \mathfrak{G}'$ implies that $(c, d) = 1$. Hence the result follows here.

We need only consider case (v). Let a, b, c, d be elements of $\mathfrak{G}$ corresponding to the terms with the same name in $\bar{\mathfrak{G}}$. Then $\mathfrak{G}$ is generated by these and $\mathfrak{Z}$ subject to

$$a^p = z_1 \quad b^p = z_2 \quad c^p = z_3 \quad d^p = z_4 \quad (c, d) = b$$
$$(b, d) = a \quad (a, d) = z_5 \quad (b, c) = z_6 \quad (a, c) = z_7 \quad (a, b) = z_8$$

with $z_i \in \mathfrak{Z}$.

Now $b \in \mathfrak{G}'$ implies that b commutes with $\mathfrak{Z}_2$, Hence b centralizes $\langle b, a, \mathfrak{Z} \rangle = \mathfrak{G}'$, and so $(c, \mathfrak{G}, b) = 1$. Since (b, c) and (a, c) are central we see that $(b, c, \mathfrak{G}) = 1$. Therefore by the three subgroups lemma $(\mathfrak{G}, b, c) = 1$. Hence c centralizes $\mathfrak{Z}_2$.

Now choose class sums K_c and K_d in $R[\mathfrak{G}]$ which generate $\mathfrak{G}/\mathfrak{Z}_3$ such that c centralizes $\mathfrak{Z}_2$. We can of course do this by Corollary 8 and the above. Set $b = (c, d)$ and $a = (b, d)$. Again $(c, \mathfrak{G}, b) = 1$ since we know that $\mathfrak{G}'$ is abelian. By assumption $(\mathfrak{G}, b, c) = 1$ since $(\mathfrak{G}, b) \subseteq \mathfrak{Z}_2$. So by the three subgroups lemma $(b, c, \mathfrak{G}) = 1$ and so (b, c) is central. With this it is easy to see that $\mathfrak{G}$ is generated by a, b, c, d and $\mathfrak{Z}$ with the above relations.

By Proposition 2, z_3 and z_4 are determined by K_c and K_d. Also $a, b \in \mathfrak{G}'$ so $a^p = b^p = 1$. Now $c, d \in \mathfrak{Z}_4$ so by Corollary 7

$$z_5 = (a, d) = (c, d, d, d)$$

is determined. Of course $(a, c) = 1$. Also $b \in \mathfrak{G}'$ and $a \in \mathfrak{Z}_2$ implies that $(a, b) = 1$. This leaves only $(b, c) = z_6$ to be determined.

Now by Corollary 5, b is determined modulo $\Gamma^3 \subseteq \mathfrak{Z}_2$. So we can find a $K_{\tilde{b}}$ where $\tilde{b} = ub$ with $u \in \mathfrak{Z}_2$. Since c centralizes $\mathfrak{Z}_2$ we have

$$(c, b) = (c, ub) = (c, b)\,(c, u)\,(c, u, b) = (c, b)\,.$$

Hence it suffices to find $(c, \tilde{b})$. But again $(c, \mathfrak{G}, \tilde{b}) = 1$ and $(\tilde{b}, \mathfrak{G}, c) = 1$ so by Proposition 4, $(c, \tilde{b})$ is determined in $R[\mathfrak{G}]$. This completes the proof.

REFERENCES

1. R. Brauer, *Zur Darstellungstheorie der Gruppen endlicher Ordnung*, Math. Zeitschr. **63** (1956), 406-444.

2. W. Burnside, *Theory of groups of Finite order*, 2nd ed., Dover Publications, New York, 1955.

3. D. B. Coleman, *Finite groups with isomorphic group algebras*, Trans. Amer. Math. Soc. **105** (1962), 1-8.

4. M. Hall, *Theory of groups*, Macmillan Co., New York, 1959.

5. G. Higman, *Enumerating p-groups I: inequalities*, Proc. London Math. Soc. (3) **37** (1960), 24-30.

6. I. M. Isaacs and D. S. Passman, *Groups whose irreducible representations have degrees dividing p^e*, Illinois J. Math. **8** (1964), 446-457.

7. D. S. Passman, *The group algebras of groups order p^4 over a modular field*, Michisan Math. J. (to appear).

8. I. Reiner, *The Schur index in the theory of group representations*, Michigan Math. J. **8** (1961), 39-47.

9. P. Roquette, *Realisierung von Darstellungen endlicher nilpotenter Gruppen*, Archiv. der Math. **9** (1958), 241-250.

HARVARD UNIVERSITY