ON THE MODULAR GROUP RING OF A p-GROUP

DONALD B. COLEMAN

Let G be a finite p-group, p a prime, and let F be a field of characteristic p. $F(G)$ will denote the group ring of G over F. In the first section of this note, two elementary results are given that concern G as a subgroup of the group of units of $F(G)$. In the second section the center of $F(G)$ is considered.

1. Let $G=\{g_1, g_2, \cdots, g_n\}$, and let $\mathfrak{G}$ denote the group of units of $F(G)$. $\mathfrak{G}$ consists of those elements $x=\sum_1^n \alpha_i g_i$ in $F(G)$ such that $c(x)=\sum_1^n \alpha_i \neq 0$. Moreover, $\mathfrak{G}=\mathfrak{G}^* \times F^*$, where $\mathfrak{G}^*=\{x: x\in F(G), c(x)=1\}$ and F^* is the multiplicative group of nonzero members of F. Note that $\mathfrak{G}^*=\mathfrak{N}+1$, where $\mathfrak{N}$ is the radical of $F(G)$. (See [4, p. 175].) $\mathfrak{Z}$ will denote the center of $\mathfrak{G}$.

THEOREM 1. *Let N be the normalizer of G in $\mathfrak{G}$. Then $N=G\mathfrak{Z}$.*

PROOF. Clearly $G\mathfrak{Z}\subset N$.

Let $x=\sum \alpha_i g_i \in N$. For each $g_j\in G$, let g_k $(k=k(j))$ be such that $xg_k=g_jx$. For each $j=1, 2, \cdots, n$, let γ_j be the permutation of G defined by

$$g^{\gamma_j} = g_j g g_k^{-1}.$$

$\gamma_j=\tau_j\beta_j=\beta_j\tau_j$, where $\tau_j: g\to g_jg$ and $\beta_j: g\to gg_k^{-1}$. The orders of τ_j and β_j are powers of p. Hence γ_j has order a power of p. Each member of the group S generated by $\gamma_1, \gamma_2, \cdots, \gamma_n$ has a similar form, so that S is a p-group of permutations of G. Moreover $xg_k=g_sx$ if and only if $\alpha_r=\alpha_s$ whenever $g_s^{\gamma_j}=g_r$. Thus the coefficients of x must agree on the transitivity classes of S. Since S is a p-group, these classes consist of either 1 or a power of p elements each. Since F has characteristic p, and since $c(x)\neq 0$, it follows that some transitivity class of S must consist of a single element. Hence S has a fixed point, say g.

Then $g=g_jgg_k^{-1}$ for each $j=1, 2, \cdots, n$, so that $g^{-1}g_jg=g_k=x^{-1}g_jx$ $(j=1, 2, \cdots, n)$. Hence $x\equiv g \pmod{C(G)}$, where $C(G)$ denotes the centralizer of G in $\mathfrak{G}$; and since $C(G)=\mathfrak{Z}$, it follows that $x\in G\mathfrak{Z}$. This completes the proof.

Let $(x, y)=x^{-1}y^{-1}xy$ $(x, y\in\mathfrak{G})$.

COROLLARY. *Let $x\in\mathfrak{G}$, $g_j\in G$. If $(g_j, x)\in G$, then $(g_j, x)=(g_j, g)$ for some $g\in G$.*

Received by the editors February 27, 1963.

PROOF. The proof follows that of Theorem 1, except here we only need to use the fact that γ_j has a fixed point.

COROLLARY. *If C is the conjugate class in $\mathfrak{G}$ containing the element $g \in G$, then $C \cap G$ is the conjugate class in G that contains g.*

For a group H, let H' denote the commutator subgroup of H.

THEOREM 2. $G \cap \mathfrak{G}' = G'$.

PROOF. Let $I(G')$ denote the ideal in $F(G)$ generated by elements of the form $g-1$, $g \in G'$. Let $X = \{x+1 : x \in I(G')\}$. It is easily verified that X is a normal subgroup of $\mathfrak{G}$ (in fact, of $\mathfrak{G}^*$). According to [2, p. 36], $X \cap G = G'$. The quotient algebra $F(G)/I(G')$ is commutative [1, p. 2]. Thus for each x, $y \in \mathfrak{G}$, $(x, y)-1 \in I(G')$, so that $(x, y) \in X$; i.e., $\mathfrak{G}' \subset X$. Hence $\mathfrak{G}' \cap G \subset G'$. Obviously $G' \subset \mathfrak{G}' \cap G$. This completes the proof.

2. Let $C_1, C_2, \cdots, C_t$ denote the noncentral conjugate classes of G; for each $i = 1, 2, \cdots, t$, let $K_i = \sum_{x \in C_i} x$. It is well known that if $Z = \{z_1, z_2, \cdots, z_m\}$ is the center of G, then the elements $z_1, \cdots, z_m$, $K_1, \cdots, K_t$ form a basis for the center $ZF(G)$ of $F(G)$.

THEOREM 3. (1) $K_i K_j = \sum_k c_{ijk} K_k$, *with* $c_{ijk} \in GF(p)$; $i, j = 1, 2, \cdots, t$. *Thus the sub-(vector) space of $F(G)$ with basis $K_1, \cdots, K_t$ is an ideal in $ZF(G)$.*

(2) *Suppose that G satisfies the condition that $(a^p, b) = 1$ if and only if $(a, b^p) = 1$; $a, b \in G$. Then $K_i^p = 0$; $i = 1, 2, \cdots, t$.*

PROOF. (1) Suppose that $K_i K_j = \sum_1^m \alpha_r z_r + \sum_1^t \beta_s K_s$; α_r, β_s non-negative integers.

Let g_i and g_j be members of C_i and C_j, respectively. Then for g_i^x and g_j^y in C_i and C_j, it follows that

$$(*) \qquad g_i^x g_j^y = z_r \in Z$$

if and only if $g_i^{xy^{-1}} = g_j^{-1} z_r$. (Here $a^b = b^{-1}ab$.)

If for fixed x and r, there is some $y \in G$ such that (*) holds, then

$$g_i^x = (g_j^{-1})^y \cdot z_r = (g_j^{-1} z_r)^y,$$

so that (*) holds for exactly one y modulo $C(g_j^{-1} z_r) = C(g_j)$.

Thus if $C_i = \{g_i^{x_q} : q = 1, 2, \cdots, u\}$ and if $C_j = \{g_j^{y_s} : s = 1, 2, \cdots, v\}$, and if g_i and $g_j^{-1} z_r$ are conjugate, then for each x_q, there is a unique y_s $(1 \leqq s \leqq v)$ such that

$$g_i^{x_q} g_j^{y_s} = z_r.$$

Hence $\alpha_r = u \equiv 0 \pmod{p}$. If g_i and $g_j^{-1}z_r$ are not conjugate, then z_r does not occur in the group product C_iC_j, so that $\alpha_r = 0$.

(2) Let $K = K_i$, with $C = C_i$ a class containing an element g.

Case 1. Assume that C is a commutative set. Choose a subgroup H of G containing $C(g)$ such that $|H: C(g)| = p$. Then let $D = \{g, g^x, \cdots, g^{x^{p-1}}\}$ be the conjugate class in H that contains g, with $g^{x^p} = g$; i.e., $(g, x^p) = 1$. Then by hypothesis, $(g^p, x) = 1$, so that for $L = \sum_{y \in D} y$, we have

$$L^p = g^p + x^{-1}g^p x + \cdots + x^{-(p-1)}g^p x^{p-1} = pg^p = 0.$$

Let $C = D_1 \cup D_2 \cup \cdots \cup D_q$, with $D_i \cap D_j = \varnothing$ for $i \neq j$, and with each D_i conjugate to D. Then for $L_i = \sum_{y \in D_i} y$, we have

$$K = L_1 + L_2 + \cdots + L_q,$$

so that

$$K^p = L_1^p + L_2^p + \cdots + L_q^p = 0.$$

Case 2. Assume that g fails to commute with one of its conjugates. The proof is by induction on $n = |G|$, the order of G.

Since $C \subset gG' \subset g\Phi$, where Φ is the Frattini subgroup of G, and since G is not cyclic, we see that the subgroup W of G generated by C is proper. Let C decompose into conjugate classes $D_1, D_2, \cdots, D_w$ in W. As before, let L_i denote the sum of elements in D_i. If D_i is commutative, then $L_i^p = 0$ by Case 1. If not, since D_i is a conjugate class in a p-group of order less than n (which satisfies the standing hypothesis of (2)), then $L_i^p = 0$ by induction. Hence $K^p = L_1^p + L_2^p + \cdots + L_w^p = 0$. This completes the proof.

Note that a regular p-group satisfies the condition of (2) [**3**, p. 185]. If C is a commutative class, then $K^p \neq 0$ if and only if $C(g) = C(g^p)$; in this case $K^p = L$, where L is the sum of the elements in the class containing g^p.

The following theorem is due to Deskins [**2**, p. 39]. An alternate proof will be given here and it will be followed by a slightly more general theorem.

THEOREM 4 (DESKINS). *If G and H are finite Abelian p-groups, and if $F(G) \cong F(H)$ for some field F of characteristic p, then $G \cong H$.*

PROOF. For any set A of group ring elements, let $A^p = \{a^p : a \in A\}$. This proof of the theorem is by induction on $n = |G| = |H|$.

Under any isomorphism of $A = F(G)$ onto $B = F(H)$, it is clear that A^p maps onto B^p. But $A^p = F^p(G^p)$ and $B^p = F^p(H^p)$ where F^p is the field of pth powers of members of F. Hence by induction, since $|G^p| = |H^p| < n$, we have that $G^p \cong H^p$. For finite Abelian p-groups G and H, the two conditions (i) $G^p \cong H^p$ and (ii) $|G| = |H|$ are enough to ensure that G and H are isomorphic.

THEOREM 5. *Let G and H be finite p-groups satisfying the condition of Theorem* 3(2). *If $ZF(G) \cong ZF(H)$, then $Z_1^p \cong Z_2^p$, where Z_1 and Z_2 denote the centers of G and H, respectively. Thus in this case, if Z_1 and Z_2 have the same order, then $Z_1 \cong Z_2$.*

PROOF. By Theorem 3(2),

$$[ZF(G)]^p = [F(Z_1)]^p = F^p(Z_1^p)$$

and

$$[ZF(H)]^p = [F(Z_2)]^p = F^p(Z_2^p).$$

Thus if $ZF(G) \cong ZF(H)$, it follows that $F^p(Z_1^p) \cong F^p(Z_2^p)$. Hence by Theorem 4, $Z_1^p \cong Z_2^p$.

In [2, p. 39] it is stated that Theorem 4 fails for arbitrary p-groups, and the quaternion group and the dihedral group of order 8 are said to have isomorphic group rings over $GF(2)$. This is not, however, the case. For in the group ring of the quaternion group all units of order 2 are central. This is not true, of course, for the dihedral group.

BIBLIOGRAPHY

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

2. W. E. Deskins, *Finite Abelian groups with isomorphic group algebras*, Duke Math. J. **23** (1956), 35–40.

3. M. Hall, *The theory of groups*, Macmillan, New York, 1959.

4. S. A. Jennings, *The structure of the group ring of a p-group over a modular field*, Trans. Amer. Math. Soc. **50** (1941), 175–185.

VANDERBILT UNIVERSITY