FINITE GROUPS WITH ISOMORPHIC GROUP ALGEBRAS(1)

BY
D. B. COLEMAN

Introduction. Let G denote a finite group and F a field. The group algebra (or group ring) $F(G)$ is the algebra over F with a basis multiplicatively isomorphic with G.

Consider the following problem: If G is a group, F a field, find all groups H such that $F(G)$ and $F(H)$ are isomorphic over F. Perlis and Walker [9] solved this problem for Abelian groups over ordinary fields. Deskins [5] solved the problem for Abelian groups over modular fields. In this paper some partial results are obtained in connection with this problem for non-Abelian groups over an ordinary field.

In §1 we see some effects that certain subgroups of G and ideals of $F(G)$ have on $F(G)$. In §2 a certain class of p-groups is studied. The theorem in §2 along with a theorem of S. D. Berman leads to an example of two distinct groups whose group algebras are isomorphic over any ordinary field. Group rings over the complex and real number fields and over the ring of integers are discussed in §3. Some examples, including the one mentioned above, are given in the last section.

PRELIMINARY REMARKS. The following notations will be used.

$A \oplus B$ denotes the direct sum of algebras A and B over F.

$A \otimes_F B = A \otimes B$ denotes the tensor product (direct product) of A and B over F.

If K is an extension field of F, and if A is an algebra over F, then A_K is the set $K \otimes_F A$, considered as an algebra over K.

$G \times H$ denotes the direct product of groups G and H.

$|G|$ denotes the order of the group G.

$|G:S|$ denotes the index of the subgroup S in G.

G' denotes the commutator subgroup of G.

$Z(G)$ denotes the center of G.

The upper central series of G is the series $1 = Z_0 \leqq Z_1 \leqq Z_2 \leqq \ldots$ defined by $Z_i/Z_{i-1} = Z(G/Z_{i-1})$, for $i = 1,2,\ldots$.

Presented to the Society, January 23, 1962 under the title *A theorem on finite group algebras*; received by the editors March 4, 1961.

(1) This paper is taken from the author's doctoral dissertation, presented to Purdue University and written under the direction of Professor J. E. Adney, to whom the author is greatly indebted.

The following facts will prove useful.

Let m be the exponent of G; i.e., m is the least common multiple of the orders of the elements of G. If $n_1, n_2, \ldots, n_t$ are the degrees of the nonequivalent absolutely irreducible representations of G, and if K is a field whose characteristic does not divide the order of G such that the equation $x^m - 1 = 0$ splits over K, then

$$K(G) \cong M_{n_1} \oplus M_{n_2} \oplus \ldots \oplus M_{n_t} \quad , \tag{1}$$

where $M_{n_i} = M_{n_i}(K)$ denotes the algebra of $n_i \times n_i$ matrices over K. (See [4; 6].) The number of conjugate classes in G is equal to t. Precisely $|G:G'|$ of the n_i are equal to 1. Each n_i divides the index of every normal Abelian subgroup of G [8]. $n_1^2 + n_2^2 + \ldots + n_t^2 = |G|$.

1. Let n be the order of G, and let the characteristic of F be 0 or a prime not dividing n. This assumption is made throughout this paper.

LEMMA 1.1. *Let N be a normal subgroup of G, and let $\mathscr{L}(N)$ denote the ideal of $F(G)$ generated by the elements $x - 1$, $x \in N$. Then*

$$F(G) \cong F(G/N) \oplus \mathscr{L}(N).$$

Proof. Let q be the order of N and let $e = 1/q \sum_{x \in N} x$. If $\{1 = y_1, y_2, \ldots, y_k\}$ is a complete set of representatives of G modulo N, then the set $\{e, ey_2, \ldots, ey_k\}$ is a basis for the ideal (e) in $F(G)$ generated by e. This set forms a multiplicative group that is isomorphic with G/N. Hence $(e) \cong F(G/N)$.

$F(G) = (e) \oplus A$, where $A = \{x \in F(G): xe = 0\}$. Clearly $\mathscr{L}(N) \leqq A$. Since A has dimension $n - k = qk - k$, and since the $(q-1)k = qk - k$ elements $(x-1)y_i$, $x \neq 1$, $x \in N$, $i = 1, 2, \ldots, k$, form a linearly independent subset of $\mathscr{L}(N)$, it follows that $A = \mathscr{L}(N)$. This completes the proof.

LEMMA 1.2. *Let I be an ideal of $F(G)$. Then the residue class algebra $F(G)/I$ is commutative if and only if $I \geqq \mathscr{L}(G')$.*

Proof(2). If S is a set of generators of a subgroup N, then it is easily seen that $\mathscr{L}(N)$ is generated by the elements $x - 1$, $x \in S$. Hence $I \geqq \mathscr{L}(G')$ if and only if $ghg^{-1}h^{-1} - 1 \in I$ for all $g, h \in G$; i.e., if and only if $(ghg^{-1}h^{-1} - 1)hg = gh - hg \in I$ for all $g, h \in G$.

THEOREM 1.1. *$F(G) \cong F(H)$ if and only if $F(G/G') \cong F(H/H')$ and $\mathscr{L}(G') \cong \mathscr{L}(H')$.*

Proof. Immediate from the lemmas.

COROLLARY 1.1. *If F is the field of rational numbers, then $F(G) \cong F(H)$ if and only if $\mathscr{L}(G') \cong \mathscr{L}(H')$ and $G/G' \cong H/H'$.*

---

(2) This proof was suggested by Dr. Norman Alling. It is simpler and more general (it holds for modular $F(G)$) than the one originally intended.

Proof. This is immediate from Theorem 1.1 and the fact that two Abelian groups have isomorphic group algebras over the rational numbers if and only if the groups are isomorphic [9].

The following result was proved for Abelian groups in [9].

THEOREM 1.2. *Let* $G = G_1 \times G_2 \times \ldots \times G_r$ *and* $H = H_1 \times H_2 \times \ldots \times H_r$ *be groups such that* $|G_i| = |H_i| = k_i$ *and* $(k_i, k_j) = 1$ *if* $i \neq j$. *Then* $F(G) \cong F(H)$ *if and only if* $F(G_i) \cong F(H_i)$ *for* $i = 1, 2, \ldots, r$.

Proof. The sufficiency of the condition is immediate from the fact that $F(G) \cong F(G_1) \otimes F(G_2) \otimes \ldots \otimes F(G_r)$.

Necessity is proved for $r = 2$, the induction step being clear.

$$
\begin{aligned}
F(G) &\cong [F(G_1/G_1) \oplus \mathscr{L}(G_1')] \otimes [F(G_2/G_2') \oplus \mathscr{L}(G_2')] \\
&\cong [F(G_1/G_1') \otimes F(G_2/G_2')] \oplus [F(G_1/G_1') \otimes \mathscr{L}(G_2')] \\
&\quad \oplus [F(G_2/G_2') \otimes \mathscr{L}(G_1')] \oplus [\mathscr{L}(G_1') \otimes \mathscr{L}(G_2')]. \qquad (2)
\end{aligned}
$$

Have $F(G_1/G_1') \cong F_0 \oplus F_1 \oplus \ldots \oplus F_{r_1}$, with $F_0 = F$.

Have $F(G_2/G_2') \cong K_0 \oplus K_1 \oplus \ldots \oplus K_{r_2}$, with $K_0 = F$.

Each F_i and K_i is a finite field extension of F. (See [9].)

Let $\mathscr{L}(G_1') = A_1 \oplus A_2 \oplus \ldots \oplus A_{s_1}$ and $\mathscr{L}(G_2') = B_1 \oplus B_2 \oplus \ldots \oplus B_{s_2}$, where each A_i and B_i is a simple algebra over F.

(2) now becomes

$$
F(G) \cong \oplus \sum F_i \otimes K_j \oplus \sum F_i \otimes B_j \oplus \sum K_i \otimes A_j \oplus \sum A_i \otimes B_j. \qquad (3)
$$

Similarly, $F(H)$ is decomposable as

$$
F(H) \cong \oplus \sum F_i^* \otimes K_j^* \oplus \sum F_i^* \otimes B_j^* \oplus \sum K_i^* \otimes A_j^* \oplus \sum A_i^* \otimes B_j^*, \qquad (4)
$$

where $F(H_1/H_1') \cong F_0^* + F_1^* + \ldots + F_{r_1}^*$, etc. ... ,

$G/G' \cong (G_1/G_1') \times (G_2/G_2')$ and $H/H' \cong (H_1/H_1') \times (H_2/H_2')$. Since by Theorem 1.1 these two Abelian groups have isomorphic group algebras, it follows that G_i/G_i' and H_i/H_i' have isomorphic algebras, $i = 1, 2$ [9].

Hence $r_1 = r_1^*$ and $r_2 = r_2^*$, and $F_i \cong F_i^*$; $K_i \cong K_i^*$ in some order.

It now suffices to show that $\mathscr{L}(G_i)$ and $\mathscr{L}(H_i)$ are isomorphic for $i = 1, 2$.

Denote the four direct summands of (3) by X_1, X_2, X_3, and X_4, respectively, and those of (4) by X_1^*, X_2^*, X_3^*, and X_4^*, respectively. By the above, $X_1 \cong X_1^*$. Moreover, if β is any isomorphism of $F(G)$ onto $F(H)$, then $X_i^\beta = X_i^*$, $i = 1, 2, 3, 4$. For the orders k_1 and k_2 of G_1 and G_2, H_1 and H_2 are relatively prime; and if E is an appropriate extension of F, then X_{2_E} and $X_{2_E}^*$, X_{3_E} and $X_{3_E}^*$, X_{4_E} and $X_{4_E}^*$ are respectively direct sums of total matric algebras over E of degrees properly dividing k_2, properly dividing k_1, and with factors properly dividing both k_1 and k_2. See (1).

Let $\bar{B}_1$ be of minimal dimension over F among the $F_i \otimes B_j$, $i = 0, 1, \ldots, r_1$; $j = 1, 2, \ldots, s_2$. Since $F_0 = F$, we have that $\bar{B}_1 = B_1$ for some B_1 among the simple direct summands of $\mathscr{L}(G_2')$. Since $X_2 \cong X_2^*$, the dimension of B_1 is also minimal among the components $F_i^* \otimes B_j^*$ of X_2^*. Thus $B_1 \cong \bar{B}_1^*$ for some component $\bar{B}_1^*$ of X_2^* which, being of minimal dimension among the $F_i^* \otimes B_j^*$ is, as before, some simple direct summand of $\mathscr{L}(H_2')$. Put $\bar{B}_1^* = B_1^*$. Then $F_i \otimes B_1 \cong F_i^* \otimes B_1^*$ for each $i = 0, 1, \ldots, r_1$.

Let $\bar{B}_2$ be of minimal dimension among the $F_i \otimes B_j$, $j \neq 1$. As before, $\bar{B}_2 = B_2$ for some component B_2 of $\mathscr{L}(G_2')$; and B_2 is isomorphic with some component B_2^* of $\mathscr{L}(H_2')$.

Repeating this argument, we have that $\mathscr{L}(G_2')$ and $\mathscr{L}(H_2')$ are isomorphic. Similarly $\mathscr{L}(G_1') \cong \mathscr{L}(H_1')$. This completes the proof.

A nilpotent group is the direct product of its Sylow subgroups. Hence we have immediately

COROLLARY 1.2. *Two nilpotent groups have isomorphic group algebras over F if and only if their corresponding Sylow subgroups have isomorphic group algebras over F.*

2. Let p be a prime. A group G is said to satisfy property (p) if every absolutely irreducible representation of G is of degree 1 or p.

Groups of order p, p^2, p^3, and p^4 satisfy property (p); and if G satisfies property (p), and if A is Abelian, then $G \times A$ satisfies property (p). Hence if k is a multiple of p^3, there are at least two distinct groups of order k satisfying property (p). There is a group of order p^5 that does not satisfy property (p).

REMARK. Let t be the number of conjugate classes in the p-group G. Then G satisfies property (p) if and only if the following condition holds: $|G| = |G:G'| + p^2(t - |G:G'|)$.

Proof. Assume that property (p) holds. Then the condition is immediate, since G has precisely $|G:G'|$ absolutely irreducible representations of degree 1, and there are precisely t of them altogether. See (1). Notice that G can be of composite order and the condition is still necessary.

Conversely, suppose that the condition holds. Let $k = t - |G:G'|$ and let $p^{a_1}, p^{a_2} \ldots, p^{a_k}$ be the degrees of the absolutely irreducible representations of G of degree $\neq 1$. Then

$$p^{2a_1} + p^{2a_2} + \ldots + p^{2a_k} = |G| - |G:G'| = p^2(t - |G:G'|) = p^2 k.$$

Hence

$$p^{2a_1 - 2} + \ldots + p^{2a_k - 2} = k.$$

Thus $a_i = 1$ for each $i = 1, 2, \ldots, k$, since each $a_i > 0$. Hence G satisfies property (p).

THEOREM 2.1. *Let G and H be p-groups ($p \neq 2$) satisfying property (p). Then $F(G) \cong F(H)$ if and only if $F(G/G') \cong F(H/H')$ and the centers of $F(G)$ and $F(H)$ are isomorphic over F.*

Proof. The necessity of the conditions is clear.

Sufficiency: $F(G) \cong F(G/G') \oplus \mathscr{L}(G')$. Let

$$\mathscr{L}(G') \cong D_1 \otimes M_{k_1} \oplus D_2 \otimes M_{k_2} \oplus \ldots \oplus D_r \otimes M_{k_r},$$

where D_i is a division algebra over F and $M_{k_i} = M_{k_i}(F)$. Since G satisfies property (p), each k_i divides p. Since p is prime, each k_i is either 1 or p. Suppose $k_i = 1$ for some i. Then D_i is itself a simple direct summand of $F(G)$, so that $D_i \cong \{\sum_{g \in G} \alpha_g \rho(g) : \alpha_g \in F\}$, where ρ is some irreducible representation of G over F. According to Herstein [7] a multiplicative subgroup of order p^n ($p \neq 2$) in a division ring is cyclic. Thus D_i is commutative. This contradicts Lemma 1.2. Hence $k_i = p$ for each $i = 1, 2, \ldots, r$.

Let K be an extension field of F satisfying (1) for G. Since G satisfies property (p), each $(D_i \otimes M_p)_K \cong D_{i_K} \otimes M_p(K)$ is the direct sum of total matric algebras over K of degree p. Thus D_i is a field, and the center Z of $F(G)$ has the structure

$$Z \cong F(G/G') \oplus D_1 \oplus D_2 \oplus \ldots \oplus D_r.$$

Since $k_i = p$ for each i, the algebras appearing in this direct sum completely determine $F(G)$. This completes the proof of the theorem.

Theorem 2.1 fails for $p = 2$. For the quaternion and dihedral groups of order 8 satisfy the two conditions over the real number field, but their group algebras are not isomorphic over the reals. These groups do have isomorphic algebras over the complex number field, however. The theorem is trivially true if F is algebraically closed, even for $p = 2$.

3. Let R denote the real number field and C the complex number field. If $R(G) \cong R(H)$, then $C(G) \cong C(H)$. We have seen above that the converse is false. However, the following does hold.

THEOREM 3.1. *If G and H are odd order groups such that $C(G) \cong C(H)$, then $R(G) \cong R(H)$.*

Proof. Let $|G| = |H| = n$. Since n is odd, we have

$$R(G/G') \cong R \oplus C \oplus C \oplus \ldots \oplus C.$$

(See [9].) C is considered as an algebra over R and occurs $\frac{1}{2}(|G:G'| - 1)$ times as a direct summand.

Let A be a simple component of $\mathscr{L}(G')$ in $R(G)$. Then there is a division algebra D over R and a positive integer m such that $A \cong D \otimes M_m(R)$. D must be R, C, or the algebra R_q of real quaternions. But $D \ncong R$; for an odd order group

cannot possess a nontrivial representation irreducible over R. Neither can D be R_q; for then $R(G)_C \cong C(G)$ would have as a simple component A_C.

$$A_C \cong [D \otimes M_m(R)]_C \cong D_C \otimes M_m(C) \cong M_2(C) \otimes M_m(C) \cong M_{2m}(C).$$

Thus $2m$ divides n, contrary to hypothesis. Hence $D \cong C$.

$\mathscr{L}(G')$ in $C(G)$ therefore completely determines $\mathscr{L}(G')$ in $R(G)$. This completes the proof.

Thus if G is of odd order with absolutely irreducible representations of degrees $1, n_2 = n_3, n_4 = n_5, \ldots, n_{t-1} = n_t$, then

$$R(G) \cong R \otimes \sum_{i=1}^{(t-1)/2} M_{n_{2i}}(C).$$

Let Q denote the rational number field and I the ring of integers. Let $I(G)$ denote the integral group ring of G; i.e., $I(G)$ is the subring $\{\sum a_i g_i : a_i \in I, g_i \in G\}$ of $Q(G)$.

S. D. Berman [3] has given conditions that are necessary if $I(G)$ and $I(H)$ are isomorphic rings, hence I-modules, since these are unitary modules. The following result of his will be used to give other necessary conditions.

LEMMA (BERMAN [1]). *Let* $x = \sum a_i g_i \in I(G)$; *let* $x^* = \sum a_i g_i^{-1}$. *If* $xx^* = x^*x$ *and if* $x^k = \pm 1$ *for some positive integer* k, *then* $x = \pm g$ *for some* $g \in G$.

THEOREM 3.2. *Let* $1 = Z_0 \leqq Z_1 \leqq Z_2 \leqq \ldots$ *and* $1 = Z_0^* \leqq Z_1^* \leqq Z_2^* \leqq \ldots$ *be the upper central series of* G *and* H *respectively. If* $I(G)$ *and* $I(H)$ *are isomorphic, then for each positive integer* i, *the following conditions hold*:

(1) $$Z_i/Z_{i-1} \cong Z_i^*/Z_{i-1}^*.$$

(2) $$I(G/Z_i) \cong I(H/Z_i^*).$$

Proof. Let β be an isomorphism of $I(G)$ onto $I(H)$. If $z \in Z_1$, then z^β satisfies the conditions of the lemma. Hence $z^\beta = \pm h$ for some $h \in H$. But since z and z^β are central (group ring elements), $h \in Z_1$. Z_1^β is a linearly independent set, so that $|Z| = |Z_1^\beta| \leqq |Z_1^*|$. Similarly, we have $|Z_1^*| \leqq |Z_1|$. Hence $|Z_1| = |Z_1^*| = k$.

Let $\{1 = x_1, x_2, \ldots, x_q\}$ be a complete set of representatives of H modulo Z_1^*. Define the mapping α of H into $I(H)$ by letting

$$y^\alpha = \begin{cases} y & \text{if } y = x_i z,\ z \in Z_1^\beta, \\ -y & \text{if } y = x_i z,\ -z \in Z_1^\beta. \end{cases}$$

It is easily verified that α is a multiplicative isomorphism of H into $I(H)$. Thus $Z_1 \cong Z_1^\beta = Z_1^{*\alpha} \cong Z_1^*$, so that G and H have isomorphic centers. Hence condition 1 holds for $i = 1$. Note that if k is odd, then $Z_1^\beta = Z_1^*$ for any isomorphism β of $I(G)$ onto $I(H)$.

Extend α to an automorphism of $I(H)$ and define $\pi = \beta\alpha^{-1}$. Then π is an iso-

morphism of $I(G)$ onto $I(H)$ such that $Z_1^{\pi} = Z_1^*$. Let $e = \sum_{z \in Z_1} z$ and $e^* = \sum_{z \in Z_1^*} z$. Then $e^{\pi} = e^*$, so that $(e) \cong (e^*)$. Thus

$$I(G/Z_1) \cong \{u/k : u \in (e)\} \cong \{v/k : v \in (e^*)\} \cong I(H/Z_1).$$

This proves condition 2 for $i = 1$.

Proceeding inductively, assume $i > 1$ and that (1) and (2) hold. By the above argument,

$$Z_{i+1}/Z_i = Z(G/Z_i) \cong Z(H/Z_i^*) = Z_{i+1}^*/Z_i^*.$$

By the second part of the above argument,

$$G/Z_i/Z(G/Z_i^*),\ H/Z_i/Z(H/Z_i^*)$$

have isomorphic group rings. But these groups are isomorphic with G/Z_{i+1} and H/Z_{i+1}^*, respectively. This completes the proof.

COROLLARY. *If $I(G) \cong I(H)$, and if G is nilpotent of class c, then H is nilpotent of class c.*

The conditions of Theorem 3.2 are not sufficient. The two non-Abelian groups of order p^3, p any prime, satisfy the conditions, but have nonisomorphic integral group rings.

4. Berman [2] gives a necessary and sufficient condition for the ordinary group algebras of two p-groups ($p \neq 2$) to have isomorphic centers. The following well-known groups G_1 and G_2 satisfy this condition for every field of characteristic $\neq 3$.

G_i $(i = 1,2)$ is generated by elements a, b, c with defining relations:

$$a^9 = b^3 = 1, \quad c^3 = a^{3i}, \quad b^{-1}ab = a^4, \quad c^{-1}ac = ab, \quad bc = cb.$$

$|G_1| = |G_2| = 81$. $G_1/G_1' \cong G_2/G_2'$. Hence, by Theorem 2.1, $F(G_1)$ and $F(G_2)$ are isomorphic for any field of characteristic $\neq 3$. The author does not know whether this is the case if F has characteristic 3.

Thus there is no field F such that $F(G)$ completely determines G for all groups G. There are, however, certain classes $\mathscr{C}$ of groups such that for some field F: $G,H \in \mathscr{C}$ and $F(G) \cong F(H)$ imply $G \cong H$. This is the case, for example, if $\mathscr{C}$ is the class of all Abelian groups and F is the rational number field. In the following paragraph this situation is again illustrated.

Let $G(m,n,r)$ be the group of order mn with generators a and b with defining relations:

$$a^m = b^n = 1, \quad b^{-1}ab = a^r, \quad (rn-n,m) = 1, \quad r^n \equiv 1 \pmod{m}.$$

These are precisely those groups whose Sylow subgroups are all cyclic. (See, for example, [6].) Note that the commutator subgroup of $G(m,n,r)$ is the subgroup generated by a, hence it has index n. Thus if $G(m,n,r)$ and $G(m',n',r')$ have

isomorphic group algebras, then $m = m'$ and $n = n'$. Also, it is easily seen that $G(m,n,r)$ and $G(m,n,r')$ are isomorphic groups if and only if there is a positive integer β such that (i) $(n,\beta) = 1$ and (ii) $r^\beta \equiv r' \pmod m$. Using this fact and elementary number theory methods, one can prove the following: Let $G = G(m,n,r)$ and $H = G(m,n,r')$, where $m = p^\alpha$ for some prime p. Let F be an arbitrary field whose characteristic does not divide mn. Then the following statements are equivalent:

(1) $G \cong H$.

(2) $F(G) \cong F(H)$.

(3) $Z(G) \cong Z(H)$.

(4) r and r' belong to the same exponent modulo $m = p^\alpha$.

Let $m = 35$, $n = 12$, $r = 3$, and $r' = 2$. In this case (3) and (4) hold, but (2) fails for any field F (hence (1) fails).

Let $m = 91$, $n = 3$, $r = 9$, and $r' = 16$. In this case (2) holds for some F, and also (3) and (4) hold. However, (1) does not.

For m composite, (3) and (4) are equivalent and (2) implies (3). Trivially (1) implies (2).

BIBLIOGRAPHY

1. S. D. Berman, *On properties of integral group rings*, Dokl. Akad. Nauk SSSR **91** (1953), 7–9.

2. ———, *On the isomorphism of the centers of group rings*, Dokl. Akad. Nauk SSSR **91** (1953), 185–187.

3. ———, *On a necessary condition for the isomorphism of integral group rings*, Dopovidi Akad. Nauk Ukraïn. RSR (1953), 313–316.

4. R. Brauer, *Applications of induced characters*, Amer. J. Math. **69** (1947), 709–716.

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

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

7. I. N. Herstein, *Finite multiplicative subgroups in division rings*, Pacific J. Math. **3** (1951), 5–6.

8. N. Itô, *On the degrees of irreducible representations of a finite group*, Nagoya Math. J. **3** (1951), 5–6.

9. Sam Perlis and G. L. Walker, *Abelian group algebras of finite order*, Trans. Amer. Math. Soc. **68** (1950), 420–426.

VANDERBILT UNIVERSITY,
NASHVILLE, TENNESSEE