

ABELIAN GROUP ALGEBRAS OF FINITE ORDER

BY

SAM PERLIS AND GORDON L. WALKER

Introduction. A group G of finite order n and a field F determine in well known fashion an algebra G_F of order n over F called the group algebra of G over F . One fundamental problem⁽¹⁾ is that of determining all groups H such that H_F is isomorphic to G_F .

It is convenient to recast this problem somewhat: If groups G and H of order n are given, find all fields F such that G_F is isomorphic to H_F (notationally: $G_F \cong H_F$). We present a complete solution of this problem for the case in which G (and thus necessarily H) is abelian and F has characteristic infinity or a prime not dividing n . The result, briefly, is that F shall contain a certain subfield which is determined by the invariants of G and H and the characteristic of F .

1. Multiplicities. If G is abelian of order n and F is a field whose characteristic does not divide n , the group algebra G_F has the structure

$$(1) \quad G_F = \sum_{d|n} a_d F(\zeta_d)$$

where ζ_d is a primitive d th root of unity, a_d is a non-negative integer, and $a_d F(\zeta_d)$ denotes the direct sum of a_d isomorphic copies of $F(\zeta_d)$. In fact, each irreducible representation S of G_F maps G_F onto a field $F_S \supseteq F$ and maps the elements of G on n th roots of unity. The image of G is a subgroup of the group of all n th roots of unity, thus is a cyclic group of some order dividing n . It follows that $F_S = F(\zeta_d)$ where ζ_d is a primitive d th root of unity. Formula (1) expresses the fact that a complete set of irreducible representations of G_F over F include precisely a_d which map G onto a cyclic group of order d . Now if K is the root field over F of $x^n - 1 = 0$ we have

$$(2) \quad G_K = \sum_{d|n} n_d K_d$$

where every $K_d = K(\zeta_d)$ is isomorphic to K , $\sum n_d = n$, and each n_d is the number of irreducible representations T of G_K mapping G on a cyclic group of order d .

LEMMA 1. *The integer n_d in (2) is the number of elements of order d in G .*

There is a one-to-one correspondence between the elements g of G and the

Presented to the Society, April 16, 1948, and October 30, 1948, under the titles *Finite abelian group algebras*, I and II; received by the editors September 22, 1948 and, in revised form, April 29, 1949.

⁽¹⁾ Proposed by R. M. Thrall at the Michigan Algebra Conference in the summer of 1947.

representations $T = T_g$. The formulae⁽²⁾ for this correspondence make it evident that g has order d if and only if T_g maps a basis of G onto a set of elements, the l.c.m. of whose orders is d . Then some element of G is mapped on an element of order d , all others on elements of order not greater than d . The map of G is thus a cyclic group of order d , and this proves the lemma.

Each irreducible representation S of G_F over F may be extended to a representation of G_K over K , the extension not altering the map of G . If S maps G_F onto $F(\zeta_d)$ where the degree of $F(\zeta_d)/F$ is

$$(3) \quad \deg F(\zeta_d)/F = v_d,$$

then S maps G_K on the direct sum⁽³⁾

$$(4) \quad F(\zeta_d)_K = K^{(1)} \oplus \cdots \oplus K^{(v_d)} = v_d K,$$

thus giving rise to v_d irreducible representations T of G_K over K .

LEMMA 2. *If S maps G onto a cyclic group of order d , so does each representation T defined above.*

Each element g in G is mapped by S on $g^S = \sum g_i$, g_i in $K^{(i)}$, and the corresponding irreducible representations over K are T_i : $g^{T_i} = g_i$. It may be seen⁽⁴⁾ that the g_i are obtainable from one another by automorphisms of $F(\zeta_d)_K$ leaving the elements of K invariant. Hence all the g_i have the same minimum function over K , and all of them are primitive d th roots of unity if g^S is one. Lemma 2 follows immediately, and it follows that the T_i into which the representations S split are the only irreducible representations of G_K mapping G on a cyclic group of order d . The a_d choices of S give rise to $a_d v_d$ representations T , whence $n_d = a_d v_d$.

THEOREM 1. *The multiplicity a_d in (1) is given⁽⁵⁾ by $a_d = n_d/v_d$ where n_d is the number of elements of order d in G and v_d is $\deg F(\zeta_d)/F$.*

Now let G and H be abelian of common order $n = p_1^{a_1} \cdots p_k^{a_k}$ for distinct primes p_i , so there are unique expressions $G = G_1 \times \cdots \times G_k$ and $H = H_1 \times \cdots \times H_k$ for G and H as direct products of groups G_i and H_i of order $n_i = p_i^{a_i}$. Then:

COROLLARY 1. $G_F \cong H_F$ if and only if $G_{iF} \cong H_{iF}$ for $i = 1, \dots, k$.

By hypothesis and Theorem 1

⁽²⁾ A. Speiser, *Die Theorie der Gruppen von endlicher Ordnung*, New York, 1945, p. 179.

⁽³⁾ A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloquium Publications, vol. 24, New York, 1939, p. 31.

⁽⁴⁾ Ibid.

⁽⁵⁾ The authors are indebted to the referees for the simple approach to Theorem 1 which has been presented here.

$$G_F = \sum_{d|n} m_d/v_d F(\zeta_d) \cong H_F,$$

$$G_{iF} = \sum_{d|n_i} g_{id}/v_d F(\zeta_d), \quad H_{iF} = \sum_{d|n_i} h_{id}/v_d F(\zeta_d)$$

where the number of elements of order d in G_i is g_{id} , in H_i is h_{id} , and in G or H is m_d . But if $d|n_i$, the elements of G having order d lie in G_i , so $m_d = g_{id}$ and likewise $m_d = h_{id}$ so $g_{id} = h_{id}$, whence $G_{iF} \cong H_{iF}$. The converse is trivial.

In the remaining sections only the prime-power case is considered.

2. Cyclotomic fields. When $n = p^a$ for a prime p the notation in (1) will be changed to

$$(5) \quad G_F = \sum_{i=0}^a a_i F(\zeta_i)$$

where ζ_i and a_i are new symbols for ζ_d and a_d , $d = p^i$. This section explores conditions under which $F(\zeta_i) \cong F(\zeta_j)$. Taking $i \leq j$ we may and shall assume that $F(\zeta_i) \leq F(\zeta_j)$, so the question now is concerned with the equality of these fields. Let P always denote the prime subfield of F .

LEMMA 3. *Let i and j be positive integers such that $i < j$. Then $F(\zeta_i) = F(\zeta_j)$ if and only if F has a subfield $F_0 \leq P(\zeta_j)$ such that $F_0(\zeta_i) = F_0(\zeta_j)$.*

Proof. If $F_0(\zeta_i) = F_0(\zeta_j)$, the field $F(\zeta_i)$ must contain ζ_j . Conversely, suppose $F(\zeta_i) = F(\zeta_j)$. The minimum function $f(x)$ of ζ_j over F has degree s equal to that of ζ_i , and is a factor of the minimum function $m(x)$ of ζ_j over P . The coefficients of $f(x)$ then must lie in the root field $P(\zeta_j)$ of $m(x)$ over P , and hence generate a subfield F_0 of $P(\zeta_j)$ such that $F_0 \leq F$. Then $F_0(\zeta_j) \geq F_0(\zeta_i)$, and

$$\deg F_0(\zeta_j)/F_0 = s \geq \deg F_0(\zeta_i)/F_0 = r \geq \deg F(\zeta_i)/F = s,$$

whence $r = s$, $F_0(\zeta_i) = F_0(\zeta_j)$.

It is necessary now to make a brief detour because of some peculiarities arising if P is finite. Suppose that

$$(6) \quad P \leq P(\zeta_1) = \cdots = P(\zeta_e) < P(\zeta_{e+1}) \quad (e \geq 1)$$

if p is odd, and

$$(7) \quad P \leq P(\zeta_2) = \cdots = P(\zeta_e) < P(\zeta_{e+1}) \quad (e \geq 2)$$

if $p = 2$. These equalities never occur if $P = R$ but do occur if P is a finite prime field whose characteristic is appropriately related to p (see Lemma 5).

DEFINITION. Let p be a prime and let P be a prime field of characteristic not equal to p . Then the integer e defined by (6) and (7) is called the cyclotomic number of P relative to p (or cyclotomic p -number of P).

LEMMA 4. *Let P be a finite prime field of characteristic π , n be an integer not*

divisible by π , and $P(\zeta)$ be the root field over P of $x^n - 1$. Then $\deg P(\zeta)/P = \epsilon$ where ϵ is defined as the exponent to which π belongs modulo n .

Let P_f be a field of degree f over P so its nonzero quantities are roots of $x^f - 1 = 0$, $\nu = \pi^f - 1$. Then P_f contains the n th roots of unity if n divides ν . Conversely, if P_f contains a primitive n th root of unity, ζ , the equation $\nu = qn + r$ ($0 \leq r < n$) leads to $\zeta^\nu = 1 = \zeta^r$ so $r = 0$, and n divides ν . The smallest value of $\nu = \pi^f - 1$ obeying this condition is given by $f = \epsilon$. On the other hand the smallest value surely belongs to $P_f = P(\zeta)$.

Now let $n = p^i$, where p is a prime not equal to π , and denote the corresponding integer ϵ of Lemma 4 by ϵ_i . Then the cyclotomic p -number of P is the integer e determined by the conditions $\epsilon_1 = \epsilon_2 = \dots = \epsilon_e < \epsilon_{e+1}$ (p odd), $\epsilon_2 = \epsilon_3 = \dots = \epsilon_e < \epsilon_{e+1}$ ($p = 2$). Hence:

LEMMA 5. The cyclotomic p -number of P is the maximum integer e such that p^e divides $\pi^e - 1$ where ϵ is the exponent to which π belongs modulo p if p is odd, or modulo 4 if $p = 2$.

The fact that $P(\zeta_i) < P(\zeta_{i+1})$ for every $i \geq e$ is a consequence of the following result.

LEMMA 6. The extension $P(\zeta_{e+i})/P(\zeta_e)$ has degree $\delta_i = p^i$ ($i = 1, 2, \dots$).

Writing $\epsilon_e = \epsilon$ we have $\delta_i = \epsilon_{e+i}/\epsilon$ and know⁽⁶⁾ that $\delta_i = p^i$, $j \leq i$, $\epsilon_{e+i} = p^i \epsilon$. By Lemma 5, $\pi^e = 1 + ap^e$ where a is not divisible by p . A trivial induction shows that

$$\pi^{p^i \epsilon} = 1 + a_i p^{e+i}, \quad (a_i, p) = 1,$$

for $i = 0, 1, 2, \dots$. This proves that $\epsilon_{e+i} = p^i \epsilon$.

LEMMA 7. If p is an odd prime and P is any prime field of characteristic not p , $P(\zeta_q)$ has the structure

$$(8) \quad P(\zeta_q) = P(\zeta_1) \times L_q, \quad \deg L_q/P = \text{power of } p,$$

where L_q is unique. Moreover, $L_q = P$ if q does not exceed the cyclotomic p -number of P .

The proof of this result is similar to the known⁽⁷⁾ proof for the case $P = R$.

LEMMA 8. Let p be odd and $q > 1$. Then the following conditions are equivalent:

- (i) $F(\zeta_q) = F(\zeta_i)$, $1 \leq i < q$.
- (ii) $F(\zeta_q) = F(\zeta_{q-1}) = \dots = F(\zeta_1)$.
- (iii) F contains the field L_q defined by Lemma 7.

⁽⁶⁾ A. A. Albert, *Modern higher algebra*, Chicago, 1937, p. 188, Theorem 21. The desired result is obtained by repeated application of this reference theorem.

⁽⁷⁾ Robert Fricke, *Lehrbuch der Algebra*, vol. 3, Braunschweig, 1928, p. 205.

The condition (iii) implies that $F(\zeta_1)$ contains $L_q(\zeta_1) = P(\zeta_q)$, $F(\zeta_1) = F(\zeta_q)$, so (ii) follows. That (ii) implies (i) is obvious. Now we assume (i) and use Lemma 3 to reduce considerations to the case $F \leq P(\zeta_q) = F(\zeta_q)$. If $q \leq e$ where e is the cyclotomic p -number of P , $L_q = P \leq F$ so (iii) is valid. Now let q be greater than e .

The field $F(\zeta_i)$ is the composite $F \cup P(\zeta_i)$. Denoting the intersection $F \cap P(\zeta_i)$ by F_i , we have

$$(9) \quad \deg F/F_i = \deg F(\zeta_i)/P(\zeta_i) = \deg P(\zeta_q)/P(\zeta_i).$$

Also, $\deg P(\zeta_k)/P = p^{\epsilon_k u}$, $\deg F/P = p^{av}$ for suitable integers ϵ_k , a , u = $\deg (P(\zeta_1)/P$, and v a divisor of u . To complete preparations for substituting in (9) note that $P(\zeta_q)/P$ is cyclic, hence possesses a unique subfield of any given degree dividing $p^{\epsilon_q u}$. Thus: $\deg F_i/P = \gcd[p^{av}, p^{\epsilon_i u}] = p^{\mu v}$ where $\mu = \min [a, \epsilon_i]$. From (9), $p^{a-\mu} = p^c$ where $c = \epsilon_q - \epsilon_i = a - \mu$. Since $q > e$, we have $\epsilon_q - \epsilon_i > 0$, $\mu < a$, $\mu = \epsilon_i$, so $a = \epsilon_q$, $\deg F/P = p^{\epsilon_q v}$. Every such subfield F of $P(\zeta_q)$ must contain the subfield L_q of degree p^{ϵ_q} .

For the case $p=2$ similar results are obtainable. The extension $P(\zeta_q)/P$ is cyclic of degree a power of 2 if P is finite, and for this case we define

$$(10) \quad L_q = P \quad \text{if } q \leq e, \quad L_q = P(\zeta_q) \quad \text{if } q > e,$$

where e is the cyclotomic number of P relative to $p=2$. For $P=R$ we have $P(\zeta_q) = P(\zeta_2) \times L_q$ where L_q is arbitrarily one of the fields

$$(11) \quad L_q = P(\zeta_q + \zeta_q^{-1}), \quad L_q = P(\zeta_q - \zeta_q^{-1})$$

and $\deg L_q/P = 2^{q-2}$. We then state without proof:

LEMMA 9. Let $p=2$ and $q>2$. Then the following conditions are equivalent:

- (i) $F(\zeta_q) = F(\zeta_i)$, $2 \leq i < q$.
- (ii) $F(\zeta_q) = F(\zeta_{q-1}) = \dots = F(\zeta_2)$.
- (iii) F contains one of the fields L_q above.

3. Determination of the fields. Let G and H be abelian groups of common prime-power order p^α and let F be any field of characteristic not p . In this section all fields F are determined such that $G_F \cong H_F$.

As in (5) we have

$$(12) \quad G_F = \sum_{i=0}^{\alpha} a_i F(\zeta_i), \quad H_F = \sum_{i=0}^{\alpha} b_i F(\zeta_i),$$

so there is a unique integer $q = q(G, H)$ defined as the maximum integer i such that $a_i \neq b_i$. From Theorem 1 this integer is the maximum i such that $m_i \neq n_i$ where m_i and n_i are the numbers of elements of order p^i in G and H , respectively. Thus q is independent of F . Since $m_0 = n_0 = 1$, q is never less than 2, but it may happen that q does not exist, that is, every $m_i = n_i$. In

this case we define $q=0$.

THEOREM 2. *The group algebras G_F and H_F are isomorphic if and only if (α) holds when p is odd, and (β) or (γ) holds when $p=2$:*

(α) $F \geq L_q$ defined by Lemma 7.

(β) G and H have the same number of invariants and F contains one of the fields L_q defined by Lemma 9.

(γ) G and H have unequal numbers, γ and η , of invariants and F contains $P(\zeta_q)$ where P is the prime subfield of F .

If $q=0$ the theorem is trivial, so we assume $q>0$, hence $q \geq 2$. Note that $G_F \cong H_F$ if and only if $A \cong B$ where

$$(13) \quad A = \sum_{i=0}^q a_i F(\zeta_i), \quad B = \sum_{i=0}^q b_i F(\zeta_i).$$

Suppose (α) holds. Then (Lemma 8) both A and B becomes $F \oplus mF(\zeta_1)$ for a suitable integer m , so $A \cong B$. If $p=2$, $F(\zeta_1) = F$, $a_1 = 2^\gamma - 1$ so

$$(14) \quad A = 2^\gamma F \oplus \sum_{i=2}^q a_i F(\zeta_i), \quad B = 2^\eta F \oplus \sum_{i=2}^q b_i F(\zeta_i)$$

whence (β) implies that $A = 2^\gamma F \oplus mF(\zeta_2) \cong B$. If (γ) holds, A and B are diagonal over F and of the same order, hence isomorphic. Conversely, suppose $A \cong B$ and first let p be odd. The assumption that $F(\zeta_q)$ is not isomorphic to $F(\zeta_i)$ for $i < q$ implies that A has precisely a_q components $F(\zeta_q)$ and B has precisely b_q such components. But then the fact that $a_q \neq b_q$ conflicts with the isomorphism of A and B . Hence $F(\zeta_q) = F(\zeta_i)$ for $i < q$ so $F \geq L_q$. The proofs for $p=2$ are obtained in similar fashion.

The case in which F is a prime field is interesting.

THEOREM 3. *Let G and H be abelian groups of order p^α . If R is the rational number field, $G_R \cong H_R$ if and only if $G \cong H$. If P is a finite prime field of characteristic $\pi \neq p$, $G_P \cong H_P$ if and only if $q \leq e$ (where e is the cyclotomic p -number of P) unless $p=2$ and G and H have different numbers of invariants. In the latter case $G_P \cong H_P$ if and only if $q \leq e$ and $\pi \equiv 1 \pmod{4}$.*

For $F=R$ the decompositions (12) are unique. Hence the condition $G_R \cong H_R$ implies that $q=0$, and for each integer $k=p^h$ dividing p^α , G and H have the same number of elements of order k . This number is $N_k(G)\phi(k)$ where ϕ denotes the Euler ϕ -function and $N_k(G) = N_k$ the number of cyclic subgroups of order k in G . The numbers N_k have been determined⁽⁸⁾ by formulae which show that the group invariants are determined when the N_k

⁽⁸⁾ G. A. Miller, *Number of the sub-groups of any abelian group*, Proc. Nat. Acad. Sci. U. S. A. vol. 25 (1939) pp. 256-262; see also Yenchien Yeh, *On prime power abelian groups*, Bull. Amer. Math. Soc. vol. 54 (1948) pp. 323-327.

are specified. Thus $G \cong H$. The remaining parts of the theorem follow from Theorem 2 and our lemmas.

To compute the "q-number" directly from the invariants of G and H , denote the latter by p^e_i ($i=1, \dots, \gamma$) and p^f_i ($i=1, \dots, \eta$), respectively, numbered in descending order of magnitude.

THEOREM 4. *Define λ as the minimum integer i such that $e_i \neq f_i$. Then $q = \max [e_\lambda, f_\lambda]$.*

For proof, note that $G = K \times \bar{G}$, $H = K \times \bar{H}$ where K has invariants p^e_i , $i=1, \dots, \lambda-1$, and those of $\bar{G}$ and $\bar{H}$ are evident. Let the common order of $\bar{G}$ and $\bar{H}$ be $\bar{n}$ and let the numbers of elements of order p^i in G , H , and K , respectively, be m_i , n_i , and k_i . Then $i > e_\lambda$ implies $m_i = \bar{n}k_i$ and $i > f_\lambda$ implies $n_i = \bar{n}k_i$. For definiteness take $e_\lambda > f_\lambda$, so $i > e_\lambda$ implies $m_i = n_i$, $q \leq e_\lambda$. For $i = e_\lambda > f_\lambda$, however, $n_i = \bar{n}k_i$, $m_i > n_i$. This proves that $q = e_\lambda$.

PURDUE UNIVERSITY,
LAFAYETTE, IND.