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 $H_F$ (nota-
tionally: $G_F \cong H_F$). 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 char-
acteristic does not divide n, the group algebra $G_F$ has the structure

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

where $\zeta_d$ 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 $F_S \cong F$ and
maps the elements of G on nth roots of unity. The image of G is a subgroup of
the group of all nth roots of unity, thus is a cyclic group of some order divid-
ing $n$. It follows that $F_S = F(\zeta_d)$ where $\zeta_d$ is a primitive $d$th root of unity.
Formula (1) expresses the fact that a complete set of irreducible representa-
tions 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

$$G_K = \sum_{d|n} n_d K_d$$

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
representations $T = T_{\gamma}$. The formulae (3) for this correspondence make it evident that $g$ has order $d$ if and only if $T_{\gamma}$ 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 $G_{\mathbb{F}}$ over $F$ may be extended to a representation of $G_K$ over $K$, the extension not altering the map of $G$. If $S$ maps $G_{\mathbb{F}}$ onto $F(\xi_d)$ where the degree of $F(\xi_d)/F$ is

\begin{equation}
\text{deg } F(\xi_d)/F = v_d,
\end{equation}

then $S$ maps $G_K$ on the direct sum (4)

\begin{equation}
F(\xi_d)_K = K^{(1)} \oplus \cdots \oplus K^{(v_d)} = v_dK,
\end{equation}

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 $K^{(g)}$, and the corresponding irreducible representations over $K$ are $T_i$: $g^S_i \equiv g_i$. It may be seen (4) that the $g_i$ are obtainable from one another by automorphisms of $F(\xi_d)_K$ 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 $T_i$, 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 the degree $F(\xi_d)/F$.

Now let $G$ and $H$ be abelian of common order $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ 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 $n_i = p_i^{\alpha_i}$. Then:

**Corollary 1.** $G_{\mathbb{F}} \cong H_{\mathbb{F}}$ if and only if $G_i \mathbb{F} \cong H_i \mathbb{F}$ for $i = 1, \cdots, k$.

By hypothesis and Theorem 1

---

(3) Ibid.
(4) The authors are indebted to the referees for the simple approach to Theorem 1 which has been presented here.
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 $d 
mid n_i$, the elements of $G$ having order $d$ lie in $G_i$, so $m_d = g_{id}$ and likewise $h_d = h_{id}$, whence $G_{id} \cong H_{id}$. The converse is trivial.

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

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

$$G_P = \sum_{d \mid n} m_d/v_dF(\xi_d) \cong H_P,$$

$$G_{i_P} = \sum_{d \mid n_i} g_{id}/v_dF(\xi_d), \quad H_{i_P} = \sum_{d \mid n_i} h_{id}/v_dF(\xi_d)$$

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 $d \nmid n_i$, the elements of $G$ having order $d$ lie in $G_i$, so $m_d = g_{id}$ and likewise $h_d = h_{id}$, whence $G_{i_P} \cong H_{i_P}$. The converse is trivial.

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

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

$$G_P = \sum_{i=0}^a a_iF(\xi_i)$$

where $\xi_i$ and $a_i$ are new symbols for $\xi_d$ and $a_d$, $d = p^i$. This section explores conditions under which $F(\xi_d) \cong F(\xi_j)$. Taking $i \leq j$ we may and shall assume that $F(\xi_i) \subseteq F(\xi_j)$, 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 $F(\xi_i) = F(\xi_j)$ if and only if $F$ has a subfield $F_0 \subseteq P(\xi_j)$ such that $F_0(\xi_i) = F_0(\xi_j)$.

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

$$\deg F_0(\xi_j)/F_0 = s \geq \deg F_0(\xi_i)/F_0 = r \geq \deg F(\xi_i)/F = s,$$

whence $r = s$, $F_0(\xi_i) = F_0(\xi_j)$.

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

$$P \leq P(\xi_1) = \cdots = P(\xi_e) \leq P(\xi_{e+1}) \quad (e \geq 1)$$

if $p$ is odd, and

$$P \leq P(\xi_2) = \cdots = P(\xi_e) \leq P(\xi_{e+1}) \quad (e \geq 2)$$

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 $\pi$, $n$ be an integer not
divisible by \( \pi \), and \( P(\xi) \) be the root field over \( P \) of \( x^n - 1 \). Then \( \deg P(\xi)/P = e \) where \( e \) is defined as the exponent to which \( \pi \) belongs modulo \( n \).

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

Now let \( n = p^i \), where \( p \) is a prime not equal to \( \pi \), and denote the corresponding integer \( e \) of Lemma 4 by \( e_i \). Then the cyclotomic \( p \)-number of \( P \) is the integer \( e \) determined by the conditions \( e_1 = e_2 = \cdots = e_e < e_{e+1} \ (p \ odd) \), \( e_2 = e_3 = \cdots = e_e < e_{e+1} \ (p = 2) \). Hence:

**Lemma 5.** The cyclotomic \( p \)-number of \( P \) is the maximum integer \( e \) such that \( p^e \) divides \( n^e - 1 \) where \( e \) is the exponent to which \( \pi \) belongs modulo \( p \) if \( p \) is odd, or modulo 4 if \( p = 2 \).

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

**Lemma 6.** The extension \( P(\xi_{i+1})/P(\xi_i) \) has degree \( \delta_i = p^i \ (i = 1, 2, \cdots) \).

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

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

for \( i = 0, 1, 2, \cdots \). This proves that \( e_{e+1} = p^e \epsilon \).

**Lemma 7.** If \( p \) is an odd prime and \( P \) is any prime field of characteristic not \( p \), \( P(\xi_p) \) has the structure

\[
P(\xi_p) = P(\xi_1) \times L_q, \quad \deg L_q/P = \text{power of } p,
\]

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) \( F(\xi_q) = F(\xi_i), \ 1 \leq i < q \).

(ii) \( F(\xi_q) = F(\xi_{q-1}) = \cdots = F(\xi_1) \).

(iii) \( F \) contains the field \( L_q \) defined by Lemma 7.

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


License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
The condition (iii) implies that $F(\zeta_i)$ contains $L_q(\zeta_i) = P(\zeta_q)$, $F(\zeta_i) = F(\zeta_q)$, so (ii) follows. That (ii) implies (i) is obvious. Now we assume (i) and use Lemma 3 to reduce considerations to the case $F \leq P(\zeta_q) = F(\zeta_i)$. 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 $F \cap P(\zeta_i)$. Denoting the intersection $F \cap P(\zeta_i)$ by $F_i$, we have

$$\text{deg } F/F_i = \text{deg } F(\zeta_i)/P(\zeta_i) = \text{deg } P(\zeta_i)/P(\zeta_i).$$

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

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

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

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

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

and $\text{deg } L_q/P = 2^{v-2}$. 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) $F(\zeta_q) = F(\zeta_{q-1}) = \cdots = F(\zeta_2)$.

(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 $p^a$ 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

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

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 (\( \alpha \)) holds when \( p \) is odd, and (\( \beta \)) or (\( \gamma \)) holds when \( p = 2 \):

(\( \alpha \)) \( F \cong L_q \) defined by Lemma 7.

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

(\( \gamma \)) \( G \) and \( H \) have unequal numbers, \( \gamma \) and \( \eta \), of invariants and \( F \) contains \( P(\xi_q) \) 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

\[
A = \sum_{i=0}^{q} a_i F(\xi_i), \quad B = \sum_{i=0}^{q} b_i F(\xi_i).
\]

Suppose (\( \alpha \)) holds. Then (Lemma 8) both \( A \) and \( B \) becomes \( F \oplus m F(\xi_i) \) for a suitable integer \( m \), so \( A \cong B \). If \( p = 2 \), \( F(\xi_i) = F \), \( a_i = 2^{-1} \) so

\[
A = 2^q F \oplus \sum_{i=2}^{q} a_i F(\xi_i), \quad B = 2^q F \oplus \sum_{i=2}^{q} b_i F(\xi_i)
\]

whence (\( \beta \)) implies that \( A = 2^q F \oplus m F(\xi_i) \cong B \). If (\( \gamma \)) 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 \( F(\xi_i) \) is not isomorphic to \( F(\xi_j) \) for \( i < q \) implies that \( A \) has precisely \( a_q \) components \( F(\xi_i) \) 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 \( F(\xi_i) = F(\xi_j) \) for \( i < q \) so \( F \cong L_q \). 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 \( p^n \). 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 \( \pi \equiv 1 \) (mod 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 \( p^n \), \( G \) and \( H \) have the same number of elements of order \( k \). This number is \( N_k(G)\phi(k) \) where \( \phi \) denotes the Euler \( \phi \)-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 \( N_k \)

---

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 \(p^i_i (i = 1, \ldots, \gamma)\) and \(p^j_i (i = 1, \ldots, \eta)\), respectively, numbered in descending order of magnitude.

**Theorem 4.** Define \(\lambda\) 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 \(p^\iota\), \(i = 1, \ldots, \lambda - 1\), 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 \(p^\iota\) 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.**