Counterexamples to the Isomorphism Problem in Finite Group Algebras

Fergal Gallagher and Leo Creedon
Institute of Technology Sligo, Ireland

Abstract

Techniques by Perlis and Walker [4] and more recently by Broche and Del Rio [1] are used to find the Wedderburn decomposition of semisimple finite abelian group algebras. These methods are here used and adapted to give new results. In doing so, we get a further insight into the isomorphism problem for group algebras, which asks, given two groups \( G \) and \( H \) and a field \( F \), is it true that if \( FG \) and \( FH \) are isomorphic, then \( G \) and \( H \) are isomorphic? The answer to this question is no. For example, the minimum counterexample to this problem is given by Creedon in [2]. The non-isomorphic groups \( C_4 \) and \( C_2 \times C_2 \) have isomorphic group algebras over \( F_2 \). Here we show that this is a special case of a general class of counterexamples. We also construct a more general class of isomorphic group algebras and give examples.

Broche and del Rio's Theorem [1]:
Let \( F \) be a field of order \( q \) and let \( \zeta \) be a primitive \( d \)-th root of unity in an extension of \( F \). Let \( s \) be the multiplicative order of \( q \mod d \). Then \( F(\zeta) \) has size \( q^s \).

We use the notation \( F(\zeta) \) for the field generated by \( F \) and \( \zeta \).

Perlis-Walker Theorem [4]:
Let \( G \) be a finite abelian group of order \( n \) and let \( K \) be a field such that \( \text{char}(K) \) does not divide \( n \). Then

\[
KG \cong \bigoplus_{d | n} \bigoplus_{j=1}^{d(n/d)} K(\zeta_d^j)
\]

where \( \zeta_d \) denotes a primitive root of unity of order \( d \), \( n(d) \) denotes the number of elements of order \( d \) in \( G \) and \( (d, n(d)) = (d, |K(\zeta_d)|) \).

For each divisor \( d \) of \( |G| \), we have \( d(n/d) \) summands of copies of the extension field \( K(\zeta_d) \) in the decomposition.

Corollary 1: Let \( G \) be a finite abelian group of order \( n \) and exponent \( e \). Let \( K \) be a field such that \( \text{char}(K) \) does not divide \( e \). Then

\[
KG \cong \bigoplus_{d | e} \bigoplus_{j=1}^{d(n/d)} K(\zeta_d^j)
\]

Proof: The exponent \( e \) is a factor of \( n = |G| \). \( \text{char}(K) \) is prime and so if \( \text{char}(K) \) does not divide \( e \), then \( \text{char}(K) \) does not divide \( n \) and so the Perlis-Walker theorem applies. Thus

\[
KG \cong \bigoplus_{d | e} \bigoplus_{j=1}^{d(n/d)} K(\zeta_d^j)
\]

Now if \( d \) is a divisor of \( n \) such that \( d \) does not divide \( e \), then \( n(d) \) (the number of elements of order \( d \)) = 0, so \( (d, n(d)) = 0 \). Thus there will be no summands in the decomposition resulting from divisors of \( |G| \) that do not divide \( e \) and the result follows.

Corollary 2: Let \( G \) be an abelian group of order \( n \) and exponent \( e \). Let \( K \) be a field such that \( \text{char}(K) \) does not divide \( e \). If \( K \) contains a primitive root of order \( e \) then

\[
KG \cong \bigoplus_{d | e} \bigoplus_{j=1}^{d(n/d)} K(\zeta_d^j)
\]

Proof: If \( K \) contains a primitive root of unity of order \( e \), then \( K(\zeta_d) = K \), for all \( d | e \). There will be \( n(d) \) copies of \( K \) for each divisor \( d \), and all of the elements of \( G \) have exponent dividing \( e \), and so there are \( n(d) \) copies of \( K \) in the decomposition.

Note that Corollary 2 is Higman’s Theorem from 1940 [3].

Isomorphic Group Algebras

Theorem: Given two non-isomorphic abelian groups \( G \) and \( H \) each with order \( n \) and exponents \( e_1 \) and \( e_2 \) respectively, and a field \( F \) of order \( q \), then:

1. If \( q \equiv 1 \mod e_1 \) and \( q \equiv 2 \mod e_2 \), we have

\[
FG \approx FH \approx \bigoplus_{l=1}^{n} F_l
\]

2. If \( q^2 \equiv 1 \mod e_1 \) and \( q^2 \equiv 1 \mod e_2 \), and \( G \) and \( H \) both contain exactly \( m \) non-identity elements of order dividing \( q \) (that is with order \( d \) such that \( q \equiv 1 \mod d \)) we have

\[
FG \approx FH \approx \bigoplus_{l=1}^{n} F_l \bigoplus \bigoplus_{d=1}^{2} F_{q^2}
\]

Proof:
1. \( F \) contains a primitive root of order \( e_1 \) and \( e_2 \) and so Corollary 2 applies in each case.
2. \( q^2 \equiv 1 \mod e_1 \) and \( q^2 \equiv 1 \mod e_2 \) and Corollary 1 applies. By Broche and Del Rio’s theorem the degree of the field extensions for both decompositions will be at most 2. The only elements of the groups giving rise to field extensions of degree 1 are the identity and the elements of order \( d \) such that \( q \equiv 1 \mod d \), and both groups have \( m \) of these. The remaining \( n-m \) elements of each group must all give rise to field extensions of degree 2, hence we get \( (n-m)/2 \) fields of size \( q^2 \) in the decomposition.

Example 1. [2] \( F_2 C_4 \cong F_2 (C_2 \times C_2) \cong \bigoplus_{l=1}^{4} F_2 \) since \( 5 \equiv 1 \mod 4 \) and \( 5 \equiv 1 \mod 2 \).

Example 2. \( F_2 (C_2 \times C_2 \times C_2) \cong F_2 (C_2^3) \cong \bigoplus_{l=1}^{8} F_2 \bigoplus \bigoplus_{l=1}^{28} F_2 \)

Example 3. \( F_2 C_{12} \cong F_2 (C_2 \times C_6) \cong \bigoplus_{l=1}^{4} F_2 \bigoplus \bigoplus_{l=1}^{8} F_2 \bigoplus \bigoplus_{l=1}^{28} F_2 \)

Conjecture.
Given two non-isomorphic abelian groups \( G \) and \( H \) each with order \( n \) and with exponents \( e_1 \) and \( e_2 \) respectively, and a field \( F \) of order \( q \), where \( q^2 \equiv 1 \mod e_1 \) and \( q^2 \equiv 1 \mod e_2 \) for some \( w \), then if \( G \) and \( H \) contain exactly the same number of elements with order \( d \) such that \( q^2 \equiv 1 \mod d \) for each \( v \) less than \( w \), then \( FG \approx FH \).

References


Acknowledgements

The research has received funding from the IT Sligo President’s Bursary Award.

Contact details: gallagher.fergal@itsligo.ie