

Ring isomorphism of cyclic cyclotomic algebras

Allen Herman (aherman@math.uregina.ca)*

*Department of Mathematics and Statistics,
University of Regina, Regina, Canada, S4S 0A2*

Gabriela Olteanu (olteanu@math.ubbcluj.ro, golteanu@um.es)

*Department of Mathematics and Computer Science,
North University of Baia Mare, Victoriei 76, 430072 Baia Mare, Romania
Current address:*

Department of Mathematics, University of Murcia, 30100 Murcia, Spain

Ángel del Río (adelrio@um.es)

Department of Mathematics, University of Murcia, 30100 Murcia, Spain

Abstract. It is shown that ring isomorphism between cyclic cyclotomic algebras over cyclotomic number fields is essentially determined by the list of local Schur indices at all rational primes. As a consequence, ring isomorphism between simple components of the rational group algebras of finite metacyclic groups is determined by the center, the dimension over \mathbb{Q} , and the list of local Schur indices at rational primes. An example is given to show that this does not hold for finite groups in general.

Keywords: cyclic algebras, cyclotomic algebras, metacyclic groups.

2000 Mathematics Subject Classification: Primary: 16S35; Secondary: 20C15.

To Professor Fred Van Oystaeyen on the occasion of his 60th birthday

Introduction

Let χ be an irreducible complex character of the finite group G , and let S_χ denote the simple component (minimal two-sided ideal) of the rational group algebra $\mathbb{Q}G$ corresponding to χ . If $\chi \in \text{Irr}(G)$ and $\psi \in \text{Irr}(H)$ are irreducible characters of the finite groups G and H , then we would like to be able to decide whether or not the simple components S_χ and S_ψ are ring isomorphic. The main motivation for this problem is that in order to calculate the group of ring automorphisms of $\mathbb{Q}G$ modulo its inner automorphisms, one must be able to decide whether or not distinct simple components of $\mathbb{Q}G$ are ring isomorphic (See [Her] and [ORS2]).

* Research partially supported by the National Science and Engineering Research Council of Canada, M.E.C. of Romania (CEEX-ET 47/2006), D.G.I. of Spain, and Fundación Séneca of Murcia.

If S_χ and S_ψ are ring isomorphic, then it follows that their centers, which are isomorphic to the respective fields of character values $\mathbb{Q}(\chi)$ and $\mathbb{Q}(\psi)$, correspond to the same extension of \mathbb{Q} , that the character degrees $\chi(1)$ and $\psi(1)$ are equal, and that the rational Schur indices $m(\chi)$ and $m(\psi)$ are equal. However, the dicyclic group $G = C_3 \rtimes C_4$ of order 12 and the quaternion group Q_8 of order 8 have rational valued characters of degree 2 for which the simple components are division algebras of index 2 that are not ring isomorphic. This is because the local indices of these characters do not agree at the primes 2 and 3. Ring isomorphism between the simple components of rational group algebras forces all of the local Schur indices $m_p(\chi)$ and $m_p(\psi)$ to be equal for all rational primes p , including the infinite prime. By a result of Benard [Ben], the local index of a simple component of a rational group algebra is the same for all primes of its center that lie over a fixed rational prime. So, by definition, $m_p(\chi)$ is the common Schur index of the \mathfrak{p} -local algebra $\mathbb{Q}(\chi)_{\mathfrak{p}} \otimes_{\mathbb{Q}(\chi)} S_\chi$ for any prime \mathfrak{p} of $\mathbb{Q}(\chi)$ lying over the rational prime p .

The conditions that the centers, dimensions, and local indices of two simple components S_χ and S_ψ of a rational group algebra are all equal are not enough to force the two simple components to be ring isomorphic. We give an example of this situation in the next section. Our goal in this article is to give some conditions on the groups G and H which imply that the above conditions are enough to force the two simple components to be ring isomorphic. We will show in Corollary 7 that this is the case as long as both of the groups are metacyclic. This is an immediate consequence of Theorem 6.

For division algebras whose Brauer classes lie in the Schur subgroup of a cyclotomic number field, a theorem of Spiegel and Trojan provides a necessary and sufficient condition for ring isomorphism, which we will apply several times in this article.

Theorem (Spiegel-Trojan [ST]). *Suppose D and Δ are division algebras of exponent m whose Brauer classes lie in the Schur subgroup of a cyclotomic number field K . Then D and Δ are ring isomorphic if and only if there is an integer s coprime to m for which $[D]^s = [\Delta]$ in $\text{Br}(K)$.*

An Example

We now give an example of two simple components S_χ and S_ψ of a rational group algebra whose centers, dimensions, and local indices of two simple components S_χ and S_ψ of a rational group algebra are all equal, but S_χ and S_ψ are not ring isomorphic.

The nonabelian groups $A = C_{11} \times C_{25}$ and $B = C_{31} \times C_{25}$ both have faithful irreducible characters $\phi \in \text{Irr}(A)$, $\theta \in \text{Irr}(B)$ with degree and Schur index 5. The only nontrivial local indices of these characters are $m_{11}(\phi) = 5$ and $m_{31}(\theta) = 5$. Let $K = \mathbb{Q}(\phi, \theta)$, $D = K \otimes S_\phi$, and $\Delta = K \otimes S_\theta$. Since $[K : \mathbb{Q}(\phi)]$ and $[K : \mathbb{Q}(\theta)]$ are relatively prime to 5, D and Δ are K -central division algebras of index 5.

Example 1. Let $G = A \times A \times B \times B$, where the groups A and B are defined as above. Note that G is metabelian, but not metacyclic. Define $\chi, \psi \in \text{Irr}(G)$ by

$$\chi = \phi \otimes 1_A \otimes \theta \otimes \theta, \text{ and } \psi = \phi \otimes \phi \otimes 1_B \otimes \theta,$$

where ϕ and θ are the characters defined above. Then the simple components S_χ and S_ψ of KG are central simple K -algebras of the same dimension whose local indices are equal to 5 at primes of K lying over 11 and 31, and whose local indices are trivial at all other primes of K . However, the class of S_χ in the Brauer group $Br(K)$ is the class $[D][\Delta]^2$, and the class of S_ψ is $[D]^2[\Delta]$. These classes are not powers of one another in $Br(K)$, so by Spiegel and Trojan's theorem, these two simple components are not ring isomorphic.

Cyclic Cyclotomic Algebras

Let K be a cyclotomic number field; that is, an abelian Galois extension of \mathbb{Q} , which we will consider as a subfield of \mathbb{C} . For any positive integer n , let ζ_n denote a primitive n -th root of unity in \mathbb{C} . A *cyclic cyclotomic algebra over K* is a cyclic algebra that can be presented in the form $(K(\zeta_n)/K, \sigma, \zeta_\ell)$, for some roots of unity $\zeta_n \in \mathbb{C}$ and $\zeta_\ell \in K$.

Since a cyclic cyclotomic algebra over K is automatically a cyclotomic algebra over K , the class in the Brauer group of K generated by a cyclic cyclotomic algebra over K always lies in the Schur subgroup of K by ([Yam], Corollary 3.11). As mentioned earlier, this implies that the \mathfrak{p} -local index of A is the same value $m_p(A)$ for all primes \mathfrak{p} of K lying over the same rational prime p .

Remark 2. There are several additional restrictions on the collection of local indices of central simple algebras that lie in the Schur subgroup of a cyclotomic number field. Two of these that we need in particular are:

- a) if p is an odd prime, then $p \equiv 1 \pmod{m_p(A)}$; and
- b) if $p = 2$ then $m_p(A) \leq 2$.

These facts are consequences of results of Witt ([Wit], Satz 10 and 11). These also hold in the more general setting for central simple algebras over K that have uniformly distributed invariants ([Mol], Theorem 1.1).

Lemma 3. *Let K be a cyclotomic number field. Let $A = (L/K, \sigma, \zeta_\ell)$ and $A' = (L/K, \sigma', \zeta_{\ell'})$ be cyclic algebras defined over the same cyclic extension L/K , with ζ_ℓ and $\zeta_{\ell'}$ roots of unity in K .*

If A and A' have the same exponent in $\text{Br}(K)$ then A is ring isomorphic to A' .

Proof. Since $\text{Gal}(L/K) = \langle \sigma \rangle = \langle \sigma' \rangle$, there exists some integer r , coprime with $[L : K]$, such that $\sigma' = \sigma^r$. If $rs \equiv 1 \pmod{[L : K]}$, then A' is isomorphic to $(L/K, \sigma, \zeta_{\ell'}^s)$ as an algebra over K by ([Rei], Theorem 30.4). Thus one may assume without loss of generality that $\sigma = \sigma'$.

Let α be a root of unity in K such that $\zeta_\ell = \alpha^n$ and $\zeta_{\ell'} = \alpha^{n'}$ for some positive integers n and n' . Let $B = (L/K, \sigma, \alpha)$. Then $[B]^n = [A]$ and $[B]^{n'} = [A']$. Hence $[A]$ and $[A']$ are two elements of the same order in a cyclic group and therefore they generate the same cyclic subgroup in $\text{Br}(K)$. Thus A and A' are isomorphic as rings by Spiegel and Trojan's Theorem. \square

Remark 4. Note that it is not necessary for L/\mathbb{Q} to be an abelian extension in the above lemma.

Lemma 5. *Let K be a cyclotomic number field. Let D and D' be two division algebras with center K whose Brauer classes lie in the Schur subgroup of K . Suppose*

$$[D] = [A_1] \otimes_K \cdots \otimes_K [A_n] \text{ and } [D'] = [A'_1] \otimes_K \cdots \otimes_K [A'_n] \text{ in } \text{Br}(K),$$

with $m(A_i) = m(A'_i) = p_i^{a_i}$ for $i = 1, \dots, n$.

If A_i and A'_i are ring isomorphic for all $i = 1, \dots, n$, then D is ring isomorphic to D' .

Proof. By Spiegel and Trojan's theorem, for each $i = 1, \dots, n$ there is an integer r_i coprime to p_i such that $[A_i]^{r_i} = [A'_i]$. By the Chinese remainder theorem, there is an integer r such that $r \equiv r_i \pmod{p_i^{a_i}}$ for all i . Therefore,

$$[D]^r = \prod_{i=1}^n [A_i]^r = \prod_{i=1}^n [A_i]^{r_i} = \prod_{i=1}^n [A'_i] = [D'].$$

So by Spiegel and Trojan's theorem again, D and D' are ring isomorphic. \square

Theorem 6. *Let A and A' be two cyclic cyclotomic algebras over a cyclotomic number field K . Assume that $[A] = [D]$ and $[A'] = [D']$ in $\text{Br}(K)$, for division algebras D and D' . If A and A' have the same local Schur indices at every rational prime p (including ∞), then D and D' are ring isomorphic.*

Proof. Let $B = (K(\zeta_n)/K, \sigma, \zeta_\ell)$ be a cyclic cyclotomic algebra over K . If $\ell = p_1^{a_1} \cdots p_t^{a_t}$ is the prime factorization of ℓ , then in the Brauer group of K we have

$$[B] = \prod_{i=1}^t [(K(\zeta_n)/K, \sigma, \zeta_{p_i^{a_i}})].$$

It is clear that the index of each cyclic algebra $B_i = (K(\zeta_n)/K, \sigma, \zeta_{p_i^{a_i}})$ divides $p_i^{a_i}$ for each i . Therefore, for each rational prime q , the local index of each B_i at the prime q is a power of p_i , and so it follows that $m_q(B) = m_q(B_1) \cdots m_q(B_t)$ for all rational primes q .

Applying this to A and A' and using Lemma 5, we may assume that $A = (K(\zeta_n)/K, \sigma, \alpha)$ and $A' = (K(\zeta_n)/K, \sigma', \alpha')$ are cyclic cyclotomic algebras such that the common index of A and A' , say m , is a power of a single prime p and α and α' are powers of a p^a -th root of unity $\zeta_{p^a} \in K$, where $m|p^a$. Since the local indices determine elements of the Schur subgroup of K that are of exponent at most 2, we may assume $m > 2$. By Remark 2, the fact that both A and A' lie in the Schur subgroup of K implies that there is an odd prime r for which $m = m_r(A) = m_r(A') > 2$. Since $\zeta_m \in K$, it follows that $[K(\zeta_{p^b}) : K]$ is a power of p , for every positive integer b .

For every subextension E of $K(\zeta_n)/K$, let E_p denote the maximal subextension of E/K of degree a power of p . Let E and E' be two subextensions of $K(\zeta_n)/K$. We claim that $(EE')_p = E_p E'_p$. The inclusion $E_p E'_p \subseteq (EE')_p$ is clear because

$$[E_p E'_p : K] = [E_p E'_p : E_p][E_p : K] = [E_p : E_p \cap E'_p][E_p : K]$$

and $[E_p : E_p \cap E'_p]$ divides $[E_p : K]$. On the other hand, $[E_p E'_p : E_p E'_p]$ divides $[E' : E'_p]$ and so $[E_p E'_p : E_p E'_p]$ is coprime to p . Similarly, $[E_p E'_p : E_p E'_p]$ is coprime to p . Therefore

$$[EE' : E_p E'_p] = [(EE')_p (E_p E'_p) : E_p E'_p]$$

is coprime to p . Thus $(EE')_p \subseteq E_p E'_p$ and the claim follows.

Furthermore, either $E_p \subseteq E'_p$ or $E'_p \subseteq E_p$, since $K(\zeta_n)/K$ is cyclic. In particular, if k and k' are two coprime divisors of n , then $K(\zeta_{kk'})_p$ equals either $K(\zeta_k)_p$ or $K(\zeta_{k'})_p$. Therefore, there exists a prime q and a power $d = q^h$ of q that divides n for which $K(\zeta_n)_p = K(\zeta_d)_p$. Moreover, if $q \neq p$ then $K(\zeta_d)_p = K(\zeta_q)_p$ so in this case one may assume that $d = q$.

It follows from ([Rei], Theorem (30.10)) that there exists an integer w coprime to p such that

$$[A] = [(K(\zeta_n)/K, \sigma, \alpha)] = [(K(\zeta_d)/K, \bar{\sigma}, \alpha^w)].$$

So one may assume that $n = d$. In a similar fashion for the algebra A' one may assume that $n' = d' = q'^{h'}$ for some prime q' and, if $q' \neq p$ then $h' = 1$. If $K(\zeta_d) = K(\zeta_{d'})$ then it is immediate from Lemma 3 that D and D' are ring isomorphic.

Suppose $K(\zeta_d) \neq K(\zeta_{d'})$. Let r be a rational prime for which $m_r(A) = m_r(A') > 2$. The two facts pointed out in Remark 2 imply that r must be an odd prime that is not equal to p . By ([Rei], Theorem (14.1) and Theorem (30.4)), both of the extensions $K(\zeta_d)/K$ and $K(\zeta_{d'})/K$ must ramify at any prime of K lying above r . However, the only finite rational prime that ramifies in the extension $\mathbb{Q}(\zeta_{q^h})/\mathbb{Q}$ is q . By ([Rei], p.67, Exercise 16), it follows that $r = q$. In a similar manner, we can show that $r = q'$. But then $d = d'$, a contradiction. \square

Corollary 7. *Let G and H be finite metacyclic groups. Let $\chi \in \text{Irr}(G)$ and $\psi \in \text{Irr}(H)$, and let S_χ and S_ψ be the simple components of $\mathbb{Q}G$ and $\mathbb{Q}H$ corresponding to χ and ψ , respectively.*

Suppose $\mathbb{Q}(\chi) = \mathbb{Q}(\psi)$, $\chi(1) = \psi(1)$, and $m_p(S_\chi) = m_p(S_\psi)$ for all rational primes p (including ∞).

Then S_χ and S_ψ are ring isomorphic.

Proof. Let $K := \mathbb{Q}(\chi) = \mathbb{Q}(\psi)$. Since $\chi(1) = \psi(1)$, S_χ and S_ψ have the same dimension over K , so it suffices to show that their division algebra parts D_χ and D_ψ are ring isomorphic. Since G is metacyclic, the character χ is induced from a maximal abelian normal subgroup $A/\ker(\chi)$ of $G/\ker(\chi)$, and G/A is cyclic. Suppose that a maximal cyclic subgroup of $A/\ker(\chi)$ has order n and that there is an element $g \in G$ of order ℓ for which $|\langle gA \rangle| = |G/A|$. Then $K \subseteq \mathbb{Q}(\zeta_n)$ and S_χ can be naturally identified with the cyclic cyclotomic algebra $(K(\zeta_n)/K, \sigma, \zeta_\ell)$. (For a more precise explanation, see [ORS1].) In a similar fashion, we can show that S_ψ can also be expressed as a cyclic cyclotomic algebra. The corollary then follows because Theorem 6 can be applied. \square

References

- [Ben] M. Benard, The Schur Subgroup I, *J. Algebra*, **22** (1972), 374–377.
- [BS] M. Benard and M. M. Schacher, The Schur Subgroup II, *J. Algebra*, **22** (1972), 378–385.
- [Her] A. Herman, On the automorphism group of rational group algebras of metacyclic groups, *Comm. Algebra*, **25** (1997), 2085–2097.
- [Jan] G. J. Janusz, Generators for the Schur group of local and global number fields, *Pacific J. Math.*, **56** (1975), 525–546.
- [Mol] R. A. Mollin, Algebras with uniformly distributed invariants, *J. Algebra*, **44** (1977), 271–282.

- [ORS1] A. Olivieri, Á. del Río, and J. J. Simon, On monomial characters and central idempotents of rational group algebras, *Comm. Algebra*, **32** (4), (2004), 1531–1550.
- [ORS2] A. Olivieri, Á. del Río, and J. J. Simon, The group of automorphisms of the rational group algebra fo a finite metacyclic group, *Comm. Algebra*, **34** (10), (2006), 3543–3567.
- [Rei] I. Reiner, Maximal orders, Academic Press 1975, reprinted by LMS 2003.
- [ST] E. Spiegel and A. Trojan, Schur algebras and isomorphic division algebras, *Portugal. Math.*, **46** (1989), 189–192.
- [Wit] E. Witt, Die algebraische Struktur des Gruppenringes einer enlichen Gruppe über einem Zahlenkörper, *J. Reine Angew. Math.*, **190** (1952), 231–245.
- [Yam] T. Yamada, The Schur subgroup of the Brauer group, Lecture Notes in Mathematics **397**, Springer-Verlag, 1974.