

TWISTED GROUP RINGS OF METACYCLIC GROUPS

RACHEL QUINLAN

ABSTRACT. Given a finite metacyclic group G , a central extension F having the projective lifting property over all fields is constructed. This extension and its group rings are used to investigate the faithful irreducible projective representations of G and the fields over which they can be realized. A full description of the finite metacyclic groups having central simple twisted group rings over fields is given.

1. INTRODUCTION

Let G be a finite group and let k be a field. A function $\alpha : G \times G \longrightarrow k^\times$ is called a *2-cocycle* if

1. $\alpha(x, 1) = \alpha(1, x) = 1, \forall x \in G$, and
2. $\alpha(x, y)\alpha(xy, z) = \alpha(x, yz)\alpha(y, z)$ for $x, y, z \in G$.

We will use the notation $Z^2(G, k^\times)$ for the set of such cocycles. A 2-cocycle α in $Z^2(G, k^\times)$ can be combined with the group operation on G to define an associative multiplication on a k -vector space of dimension $|G|$ as follows:

Definition 1.1. The *twisted group algebra* $k^\alpha G$ is a k -vector space with basis $\{u_x, x \in G\}$, on which multiplication is defined on basis elements by $u_x u_y = \alpha(x, y)u_{xy}$ and extended by k -bilinearity.

The twisted group algebra $k^\alpha G$ is a ring with identity element u_1 , which we identify with the multiplicative identity of k and denote by 1. An example of a twisted group algebra is the ordinary group algebra kG , determined by the *trivial* cocycle, which sends every element of $G \times G$ to 1.

Many standard results concerning group algebras extend without difficulty to the more general setting of twisted group algebras. For example, we have

Theorem 1.2 (Maschke). *Let G be a finite group and let k be a field whose characteristic if positive does not divide $|G|$. Then twisted group algebras of G over k are completely reducible.*

We will assume throughout that the hypotheses of Maschke's theorem are satisfied, so the twisted group algebra $k^\alpha G$ is a direct sum of simple k -algebras.

Definition 1.3. If V is a left $k^\alpha G$ -module, the function

$$T : G \longrightarrow GL(V)$$

Received by the editors July 15, 2002 and, in revised form, December 12, 2002.
2000 *Mathematics Subject Classification.* Primary 20C25.
Research supported in part by the Higher Education Authority, Ireland.

defined for $x \in G$ by

$$T(x)(v) = u_x.v \quad \forall v \in V$$

is called a *projective representation* of G over k , associated to the cocycle α . This projective representation is called *irreducible* if V is simple as a $k^\alpha G$ -module, and *absolutely irreducible* if it remains irreducible under field extensions of k .

If $\dim_k V = n$, the choice of a k -basis for V associates to T a *projective matrix representation*

$$T : G \longrightarrow GL(n, k)$$

satisfying

$$\begin{aligned} T(1_G) &= 1_{GL(n, k)}, \text{ and} \\ T(x)T(y) &= \alpha(x, y)T(xy) \text{ for } x, y \in G. \end{aligned}$$

The *kernel* of T is $\{g \in G : T(g) \in \mathcal{Z}(GL(n, k)) \cong k^\times\}$, which is a normal subgroup of G . The projective representation T is said to be *faithful* if its kernel is trivial.

Definition 1.4. Projective matrix k -representations T_1 and T_2 of degree n of G are called *projectively equivalent* over k if for some $A \in GL(n, k)$ and for some function $\mu : G \longrightarrow k^\times$ satisfying $\mu(1_G) = 1$,

$$T_2(x) = \mu(x)A^{-1}T_1(x)A, \quad \forall x \in G.$$

For $\alpha \in Z^2(G, k^\times)$, the number of mutually inequivalent irreducible projective α -representations of G is at most equal to the number of simple components of the twisted group algebra $k^\alpha G$, which in turn is at most equal to the number of conjugacy classes of G but generally less. We remark that (provided G has at least two elements) the ordinary group ring kG always has at least two components since it has the direct sum decomposition

$$kG = A_1 \oplus A_2,$$

where A_2 is the augmentation ideal of kG and A_1 , which is isomorphic to k , is generated as a two-sided ideal of kG by the central idempotent

$$e_1 = \frac{1}{|G|} \sum_{x \in G} x.$$

Projection on A_1 maps every element of kG to its augmentation and every element of G to 1. The irreducible component A_1 of G corresponds to the trivial representation of G .

Twisted group algebras generally do not come equipped with an augmentation homomorphism, nor with an automatic decomposition into direct summands as above. It is not difficult to exhibit examples of twisted group algebras which are simple. For instance every quadratic extension of the field of rational numbers may be realized as a twisted group algebra of C_2 over \mathbb{Q} . Of course, such algebras do not remain simple under extensions of scalars; better examples are provided by the rational quaternion division algebra and the matrix ring $M_2(\mathbb{Q})$, each of which is a central simple \mathbb{Q} -algebra arising as a twisted group ring of $C_2 \times C_2$ over \mathbb{Q} . Indeed, these are instances of the following fact, of which a proof can be found in [6].

Theorem 1.5. *Let A be a finite abelian group. Then there exist fields over which A has central simple twisted group algebras if and only if A is of symmetric type, i.e., A is a direct product of two isomorphic abelian groups.*

In this paper we consider the question of which finite metacyclic groups possess central simple twisted group algebras over fields of characteristic zero. The methods used involve the investigation of *generic central extensions* of metacyclic groups and irreducible representations of their group algebras. Before specializing to the case of metacyclic groups, some relevant background information is given in Section 2.

2. GENERIC CENTRAL EXTENSIONS

Suppose $T : G \rightarrow GL(n, k)$ is a projective representation of a finite group G . It is easily observed that the subgroup of $GL(n, k)$ generated by $\{T(g), g \in G\}$ is an extension of some (not necessarily finite) subgroup of k^\times ($\cong \mathcal{Z}(GL(n, k))$) by a homomorphic image of G . Thus associated to T is an ordinary representation \tilde{T} of some (not necessarily finite) group \tilde{G} whose quotient modulo a central subgroup is a homomorphic image of G . In this situation \tilde{T} is called a *lift* of T to \tilde{G} .

Suppose H is a group having a central subgroup A for which $H/A \cong G$. Then (A, H) is called a *central extension* of G , and this central extension is said to have the *projective lifting property* for G over k if every irreducible projective k -representation of G is projectively equivalent over k to one which is defined by restricting an ordinary k -representation of H to some transversal for A in H . Examples of central extensions having the projective lifting property over all fields arise from the following construction, which is due to Schur.

Let \tilde{F} be a free group mapping onto G with kernel \tilde{R} . Define

$$F := \tilde{F}/[\tilde{F}, \tilde{R}], \quad R := \tilde{R}/[\tilde{F}, \tilde{R}].$$

Then $R \subseteq \mathcal{Z}(F)$ and $F/R \cong G$. It follows easily from the freeness of \tilde{F} that if $\theta : G \rightarrow G_1$ is a surjective group homomorphism and (A_1, H_1) is any central extension of G_1 , then there exists a homomorphism $\beta : F \rightarrow H$ mapping R into A and inducing θ on G . It then follows from the comments at the beginning of this section that the central extension (R, F) has the projective lifting property for G over all fields.

Later it will be useful to consider an alternative formulation of this statement: every simple component of a twisted group algebra of G over the field k is isomorphic as a k -algebra to a simple image of the group algebra kF under a k -algebra homomorphism sending R into k^\times . We will refer to extensions such as (R, F) as *generic central extensions* for G . We now list some relevant properties of generic central extensions and their group rings. Details can be found in [5].

In the following, (R, F) is a generic central extension for the finite group G . The first two properties are due to Schur (see [1], for example).

1. The set of torsion elements of F is equal to its commutator subgroup F' . This group is finite and is determined by G up to isomorphism.
2. $R = S \times (F' \cap R)$, where the torsion subgroup $F' \cap R$ of R is isomorphic to $M(G)$, the Schur multiplier of G , and S is a free abelian group of rank equal to the free rank of \tilde{F} .
3. Every central idempotent of kF belongs to the completely reducible ring kF' (see [4], Chapter 4, Theorem 3.8). If \mathcal{I} is the set of primitive central idempotents of kF' , then F acts on \mathcal{I} by conjugation, and every primitive central idempotent of kF is the sum of the elements of one orbit of this action. These primitive central idempotents give a description of kF as a direct sum of indecomposable components.

4. Suppose $T : G \rightarrow GL(n, k)$ is an irreducible projective representation of G , and let $\tilde{T} : F \rightarrow GL(n, k)$ be a lift of T to F . Then the linear extension of \tilde{T} to kF annihilates all but one of the components of kF . The component which survives does not depend on the choice of lift; so T belongs to a particular component (or a particular primitive central idempotent) of kF . Projectively equivalent irreducible projective representations of G belong to the same component of kF . Moreover, if k is algebraically closed, then irreducible projective representations of G belonging to the same component of kF are projectively equivalent over k . So in this case the components of kF precisely distinguish the equivalence classes of irreducible projective k -representations of G . (This is Theorem 3.2 of [5]).

3. METACYCLIC GROUPS

Let G be the metacyclic group given by

$$(3.1) \quad G = \langle x, y \mid x^m = 1, y^s = x^t, y^{-1}xy = x^r \rangle,$$

where $\gcd(r, m) = 1$, $m \mid t(r - 1)$, $m \mid r^s - 1$, and we can assume (by replacing x if necessary with another generator of $\langle x \rangle$) that $t \mid m$.

Let (R, F) be a generic central extension for G . Then F is generated by elements X and Y with $X \rightarrow x$, $Y \rightarrow y$. Let c denote the element $Y^{-1}XYX^{-1}$ of F' . Then $c \in RX^{r-1}$, so c commutes with X . Also,

$$Y^{-1}cY = c^r \implies \langle c \rangle \trianglelefteq F.$$

It is easily checked that every simple commutator in F belongs to $\langle c \rangle$, and so $\langle c \rangle = F'$. We observe that both X^t and Y^s belong to $\mathcal{Z}(F)$; it follows that

$$c^t = Y^{-1}X^tYX^{-t} = 1 \quad \text{and} \quad Y^{-s}XY^sX^{-1} = c^{1+r+r^2+\dots+r^{s-1}} = 1,$$

For a positive integer $i \geq 2$ we define

$$\alpha(i) = 1 + r + r^2 + \dots + r^{i-1} = \frac{r^i - 1}{r - 1}.$$

Then $|F'|$ divides $\gcd(t, \alpha(s))$. In fact, this is exactly the order of F' since

$$[F' : F' \cap R] = |G'| = m / \gcd(m, r - 1)$$

and

$$|F' \cap R| = |M(G)| = \frac{\gcd(m, r - 1) \gcd(t, \alpha(s))}{m}$$

(for a proof of this see, for example, [3]). For convenience we define $n = \gcd(t, \alpha(s)) = |F'|$. Note that $n \mid m$ since $t \mid m$.

Study of the structure of components of group algebras of F and their simple images is greatly facilitated by the cyclicity of F' . We begin by considering the group ring of F over the field \mathbb{C} of complex numbers.

Let ξ be a root of unity of order n in \mathbb{C} . The group ring $\mathbb{C}F'$ is a direct sum of n copies of \mathbb{C} , and its primitive idempotents f_0, f_1, \dots, f_{n-1} are given by

$$f_i = \frac{1}{n} \sum_{j=1}^n (\xi^i c)^j.$$

The group F acts on $\{f_0, f_1, \dots, f_{n-1}\}$ by conjugation, with kernel $C_F(c) = \langle X, Y^b, c \rangle$, where $b = \text{ord}_n(r)$. We have

$$f_i^Y = Y^{-1} f_i Y = \frac{1}{n} \sum_{j=1}^n (\xi^i c^r)^j = \frac{1}{n} \sum_{j=1}^n (\xi^{ir'} c)^j$$

where r' denotes the inverse of r modulo n .

We note that $f_i \in \mathbb{Q}(\xi)F'$ for $i = 0, 1, \dots, n-1$, and we have an action of $\text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ on $\mathbb{Q}(\xi)F'$ defined for $\tau \in \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ and $a_0, \dots, a_{n-1} \in \mathbb{Q}(\xi)$ by

$$\left(\sum_{i=0}^{n-1} a_i c^i \right)^\tau = \sum_{i=0}^{n-1} a_i^\tau c^i.$$

If $\sigma \in \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ is defined by $\sigma(\xi) = \xi^r$, then

$$f_i^{\sigma^{-1}} = f_i^Y \text{ for } i = 0, \dots, n-1.$$

The primitive central idempotents of $\mathbb{C}F$ are sums of orbits of $\{f_0, \dots, f_{n-1}\}$ under the action of $\langle Y \rangle$, or equivalently, of $\langle \sigma \rangle$. Hence each has coefficients in the fixed field of $\mathbb{Q}(\xi)$ under σ . We let k denote this field. Its degree as an extension of \mathbb{Q} is $\phi(n)/b$.

The group algebras kF , $\mathbb{C}F$ and kF' all have the same set of primitive central idempotents. The field k is an example of a *projective splitting field* for G ; i.e., every complex projective representation of G is projectively equivalent (over \mathbb{C}) to a projective k -representation of G . Furthermore, any subfield E of \mathbb{C} which is a projective splitting field for G must contain k ; otherwise, EF will have primitive central idempotents not remaining primitive in $\mathbb{C}F$, and complex irreducible representations of G belonging to the corresponding components will not be realizable over E .

Let e be a primitive central idempotent of kF and let $A = kFe$. We are interested in central simple k -algebras which arise as images of A under k -algebra homomorphisms sending the centre of A into k . With this in mind, we begin with a description of $\mathcal{Z}(Fe)$.

Let d be the order of the group $F'e$, so $c^d e = e$, and $d|n$. Then

$$Y^{-1} X^i Y = X^i c^i \implies \langle X \rangle e \cap \mathcal{Z}(A) = \langle X^d \rangle e.$$

Also,

$$Y^{-i} X Y^i = X c^{\alpha(i)} \implies Y^i e \in \mathcal{Z}(A) \iff d|\alpha(i) \implies \langle Y \rangle e \cap \mathcal{Z}(A) = \langle Y^{b'} \rangle e$$

where $d|\alpha(b')$ and $d \nmid \alpha(i)$ for $i < b'$. Let b_d denote the order of r modulo d . Then

$$d|\alpha(b') \implies d|(r^{b'} - 1) \text{ and } b_d|b'.$$

Say $b' = b_d i$. Then

$$\begin{aligned} \alpha(b') &= \alpha(b_d)(1 + r^b + \dots + r^{(i-1)b_d}) \\ \implies g|(1 + r^b + \dots + r^{(i-1)b_d}), \text{ where } g &= \frac{d}{\text{gcd}(d, \alpha(b_d))}. \end{aligned}$$

Now $g|r-1$ since $d|r^{b_d} - 1$, hence $r \equiv 1 \pmod{g}$, and g can divide $1 + r^b + \dots + r^{(i-1)b}$ only if g divides i . We conclude $i = g$ and $b' = b_d g$.

Suppose for some finite group H , field \mathcal{F} and $\alpha \in \mathcal{Z}^2(H, \mathcal{F}^\times)$ that $\mathcal{F}^\alpha H$ is a central simple \mathcal{F} -algebra. If \mathcal{F} is an algebraically closed field containing \mathcal{F} , then α can be regarded as a 2-cocycle in $\mathcal{Z}^2(H, \mathcal{F}^\times)$, and $\mathcal{F}^\alpha H$ is a central simple

$\bar{\mathcal{F}}$ -algebra. Then H has, up to projective equivalence, a unique irreducible α -representation over $\bar{\mathcal{F}}$, and this projective representation is faithful. Thus any finite group having a central simple twisted group ring over a field has a faithful absolutely irreducible projective representation. In the metacyclic case, the above observations on the centre of a component of kF lead to the following result.

Theorem 3.1. *The metacyclic group G of (3.1) possesses a faithful irreducible projective representation over \mathbb{C} if and only if*

1. $n = m$, and
2. m does not divide $\alpha(i)$ for any $i < s$.

Proof. Suppose T is an irreducible complex projective representation of G , and let e be the primitive central idempotent of kF to which T belongs. Let $d = |F'e|$, and let \tilde{T} be a lift of T to F . Then $X^d \in \mathcal{Z}(kFe)$ and $\tilde{T}(X^d)$ is a scalar matrix, so $x^d \in \ker T$. Thus T can be faithful only if $m|d$, which means $m = d = n$ since $d|n$, and $n|m$. It follows also that $t = m$ (since $t|m$ and $n|t$), so $y^s = 1$ and $G = \langle x \rangle \rtimes \langle y \rangle$.

Assume now that $n = m$. Then $m|\alpha(s)$ since $n|\alpha(s)$. If $m|\alpha(s')$ for some $s' < s$, then $Y^{s'} \in \mathcal{Z}(kFe)$ and $y^{s'} \in \ker T$. Hence T can be faithful only if m does not divide $\alpha(s')$ whenever $s' < s$. This establishes the necessity of conditions 1 and 2 for the existence of faithful absolutely irreducible projective representations of G .

For the sufficiency, assume 1 and 2 are satisfied and let e be a primitive central idempotent of $\mathbb{C}F$ with $|F'e| = m$. If $T : G \rightarrow GL(l, \mathbb{C})$ is an irreducible projective representation of G belonging to e , let \tilde{T} be a lift of T to F . Then \tilde{T} restricts faithfully to $F'e \cong C_m$. Let $x^i y^j \in G$, with $0 \leq i < m$, $0 \leq j < s$. If $j \neq 0$, then

$$(X^i Y^j)^{-1} X (X^i Y^j) X^{-1} = c^{\alpha(j)} X \neq X;$$

so $\tilde{T}(X^i Y^j) \notin k^\times$ and $x^i y^j \notin \ker T$.

If $j = 0$ and $i \neq 0$, then

$$Y^{-1} X^i Y X^{-i} = c^i;$$

so $\tilde{T}(X^i) \notin k^\times$ and $x^i \notin \ker T$. Hence faithfulness of T follows from faithfulness of $\tilde{T}|_{F'}$. □

Theorem 3.1 is originally due to Ng (see [3]). We will further show that if E is a subfield of \mathbb{C} and G is a metacyclic group satisfying the conditions of the theorem, then G has faithful absolutely irreducible projective representations over E if and only if E contains k . Certainly EF must have a primitive central idempotent e for which $F'e$ has order m . The coefficient of c^i in e is a rational multiple of $\gamma_i = \text{Tr}_{\mathbb{Q}(\xi)/k}(\xi^i)$ where ξ is some primitive m th root of unity in \mathbb{C} . Then $\gamma_i \in E$ for each i and $k \subseteq E$ since k is generated over \mathbb{Q} by $\{\gamma_i\}$.

We now return to the group algebra kF to investigate the degree and Schur index of the representations described in Theorem 3.1. From now on we will assume that the hypotheses of the theorem are satisfied by the metacyclic group G and its generic central extension (R, F) . Let e be a primitive central idempotent of kF for which $F'e$ has order m and let $A = kFe$. Then $kF'e \cong k(\xi_m)$.

Consider the k -subalgebra A_0 of A generated over $kF'e$ by Y . Since k is the subfield of $kF'e$ fixed by the automorphism defined by conjugation by Y , $\mathcal{Z}(A_0) \cap kF'e = ke$. Since $\langle Y \rangle$ is right independent over $kF'e$ and $\langle Y \rangle \cap C_F(ce) = \langle Y^b \rangle$, the centre of A_0 is generated as a k -algebra by Y^b and is isomorphic to the ring of Laurent polynomials in one variable over k . From A_0 we can form the

ring of quotients $A_1 = (\mathcal{Z}(A_0))^{-1}A_0$, in which every nonzero element of $k\langle Y^b \rangle e$ is invertible. The centre of A_1 is K , the field of quotients of $k\langle Y^b \rangle e$.

Lemma 3.2. A_1 is a cyclic K -algebra of degree b .

Proof. The subfield $KF'e \cong K(\xi_m)$ is a cyclic extension of degree b of K on which $\langle Y \rangle / \langle Y^b \rangle$ acts as the full Galois group. Moreover, A_1 is generated as a left module over $KF'e$ by $\{1, Y, \dots, Y^{b-1}\}$. \square

In particular, A_1 is a central simple K -algebra. We now use this fact to produce a pair of algebraically independent generators for $\mathcal{Z}(A)$ over k . We define

$$g = \frac{m}{\gcd(m, \alpha(b))}.$$

Then by the comments preceding Theorem 3.1, we have $m|\alpha(gb)$ and $m \nmid \alpha(i)$ for $i < gb$, so $s = gb$ and $g = b/s$. Moreover,

$$\langle X \rangle \cap C_F(Y^b) = \langle X^g \rangle,$$

since $Y^{-b}X^iY^b = X^{i\alpha(b)}$ and m divides $i\alpha(b)$ if and only if g divides i .

Lemma 3.3. There exists an element c' of $kF'e$ with $X^g c' \in \mathcal{Z}(A)$.

Proof. By the above comments X^g acts by conjugation as a central automorphism of A_1 . This automorphism is inner by the Noether-Skolem theorem, so there exists an invertible element c'' of A_1 for which $X^g c''$ centralizes Ye and hence all of A . After multiplying if necessary by an element of $k\langle Y^b \rangle e$, we may assume $c'' \in A_0$. Then

$$c'' = \sum_{i=0}^l a_i Y^i,$$

where $a_i \in kF'e$ for $i = 0, \dots, l$. Thus $X^g c'' = \sum_{i=0}^l X^g a_i Y^i$, and since X centralizes $X^g c''$ and each a_i , this means X centralizes $Y^i e$ whenever $a_i \neq 0$, i.e., $s|i$ whenever $a_i \neq 0$. It follows that Y centralizes $X^g a_i$ for each i , and we may take $c' = a_i$ for any nonzero a_i . Of course, different nonzero a_i differ only by multiplication by elements of $(kF'e)^\times \cap \mathcal{Z}(A) = k^\times$. \square

From now on we will assume $c' \in kF'e$ has been fixed.

Lemma 3.4. $Z = \mathcal{Z}(A)$ is generated as a k -algebra by $X^g c'$ and Y^s .

Proof. Let $z \in Z$. Then, since z is centralized by X , and $\langle Y \rangle$ is right independent over $k\langle X, c \rangle$, $z = \sum_{i=0}^l a_i Y^{is}$ where each $a_i \in k\langle X, c \rangle$. Since z is centralized by Y , each a_i is centralized by Y and belongs to Z . Now suppose $a \in k\langle X, c \rangle \cap Z$, and

$$a = \sum_{i=0}^{l'} d_i X^i, \quad d_i \in kF'e.$$

Each d_i is centralized by Y^b , hence d_i can be nonzero only if X^i is centralized by Y^b , i.e., only if $g|i$. Suppose $d_{jg} \neq 0$ for some j . Then

$$d_{jg} X^{jg} \in Z \implies (c')^{-j} d_{jg} \in \mathcal{Z}(A_1) \cap k\langle X, F' \rangle = ke.$$

Thus $a \in k\langle X^g c' \rangle e$, and $z \in k\langle X^g c', Y^s \rangle e$. \square

It is clear that Y^s and $X^g c'$ are algebraically independent over k ; Z is isomorphic to a ring of Laurent polynomials in two commuting variables over k .

Let χ be the character of F' associated to the primitive central idempotent e of kF' . Then χ has degree b ; it need not be absolutely irreducible, but its absolutely irreducible constituents are all conjugate under F . Let \tilde{T}' be a k -representation of F' affording χ , whose linear extension to kF' we also call \tilde{T}' . Let $F_0 = \langle X^g, Y^s, c \rangle \subseteq F$. Then F_0 is a subgroup of F isomorphic to $\mathbb{Z} \times \mathbb{Z} \times C_m$, and we can extend \tilde{T}' to an irreducible representation \tilde{T}_0 of kF_0 by choosing elements P and Q of k^\times and defining

$$\tilde{T}_0(X^g c'^{-1}) = PI, \quad \tilde{T}_0(Y^s) = QI,$$

where I denotes the identity matrix in $GL(b, k)$. Then the image of kF_0 under \tilde{T}_0 is isomorphic to $k(\xi_m)$, and \tilde{T}_0 has degree b and maps R into k^\times by Lemma 3.4.

The induced representation $\text{Ind}_{F_0}^F \tilde{T}_0$ is completely reducible over k : let \tilde{T} be one of its irreducible constituents. We let B denote the image of kF under \tilde{T} ; so B is a finite-dimensional simple k -subalgebra of $M_b(k)$.

The field $kF'e \cong k(\xi_m)$ is embedded by \tilde{T} in B ; we identify c and c' with their images under \tilde{T} , and we let X_T and Y_T denote respectively the images of X and Y .

Lemma 3.5. *The commutative subalgebra B_0 of B generated by c and X_T has dimension g over $k(c)$.*

Proof. If $g = 1$, then $X_T \in k(c)$ and there is nothing to prove.

If $g > 1$, then certainly B_0 is spanned over $k(c)$ by $\{1, X_T, \dots, X_T^{g-1}\}$, since $X_T^g = c'P \in k(c)^\times$. Let h be minimal with $\{1, X_T, \dots, X_T^h\}$ linearly dependent over $k(c)$, so $h \leq g$.

Assume $h < g$, and suppose

$$a_0 + a_1 X_T + \dots + a_h X_T^h = 0,$$

where $a_i \in k(c)$ for $i = 0, \dots, h$ and $a_0 \neq 0$, $a_h \neq 0$. Conjugating by Y_T^b (which centralizes c and hence each a_i) gives

$$\begin{aligned} a_0 + a_1 c^{\alpha(b)} X_T + \dots + a_h c^{h\alpha(b)} X_T^h &= 0 \\ \implies a_1(1 - c^{\alpha(b)}) X_T + \dots + a_h(1 - c^{h\alpha(b)}) X_T^h &= 0 \\ \implies a_1(1 - c^{\alpha(b)}) + \dots + a_h(1 - c^{h\alpha(b)}) X_T^{h-1} &= 0. \end{aligned}$$

All of the coefficients in this expression must be zero; otherwise, we have a contradiction to the choice of h . In particular, then $1 - c^{h\alpha(b)} = 0$, so $m|h\alpha(b)$ and $g|h$. Thus $h = g$, and $a_i = 0$ for $i = 1, \dots, h - 1$. \square

By Clifford's theorem \tilde{T} restricts to a completely reducible representation of $\langle X, c \rangle$ whose irreducible constituents are all conjugate under F . Thus, since B_0 is commutative, it is a direct sum of fields, each isomorphic to an extension of $kF'e$ obtained by adjoining a g th root of the element Pc'^{-1} . (Of course, $kF'e$ contains primitive g th roots of unity.) If this extension has degree g'' over $kF'e$, then $g''|g$ and the number of simple components of B_0 is $g' := g/g''$. We let $e_1, \dots, e_{g'}$ denote the primitive central idempotents of B_0 , and define $B_1 = e_1 B e_1$.

Then

$$B \cong M_{g''}(B_1),$$

by Lemma 1.6 in Chapter 6 of [4].

Lemma 3.6. $B_1 = k\langle c, X_T, Y^{g''} \rangle e_1$.

Proof. Every element of B can be written in the form

$$\sum_{i=m_1}^{m_2} a_i Y_T^i,$$

where m_1 and m_2 are integers and for $i = m_1, \dots, m_2$ a_i belongs to $k\langle c, X_T \rangle$ and commutes with e_1 . Since $\langle Y_T \rangle$ acts transitively on $\{e_1, \dots, e_{g''}\}$, the kernel of this action is $\langle Y_T^{g''} \rangle$. Thus $e_1 Y_T^i = Y_T^i e_1$ if and only if g'' divides i ; otherwise, $e_1 Y_T^i = Y_T^i e_j$ where $e_j e_1 = 0$. Hence $e_1 B e_1 \subseteq k\langle c, X_T, Y_T^{g''} \rangle e_1$.

The reverse inclusion is obvious since $Y^{g''} e_1 = e_1 Y^{g''} e_1 \in B_1$. □

Now $k\langle c, X_T \rangle e_1$ is a cyclic field extension of k of degree $g'b$, on which $\langle Y_T^{g''} \rangle$ acts by conjugation as the full Galois group. If σ denotes the automorphism of $k\langle c, X_T \rangle e_1$ defined as conjugation by $Y_T^{g''}$, then B_1 is isomorphic to the cyclic k -algebra

$$\left(kF'e(\sqrt[g]{Pc^{g'-1}}/k, \sigma, Q) \right)$$

which has degree bg' over k . Here $Q = (Y_T g'')^{bg'} = Y_T^s$. Since $B = M_{g''}(B_1)$, the degree of B over k is $g''bg' = bg = s$.

Lemma 3.7. *The Schur index of B divides bg' .*

Proof. Since $B \cong M_{g''}(B_1)$, the Schur index of B is the same as that of B_1 . This index is the order of Q modulo the norm group $N_{E/k}(E^\times)$ (see [2], for example). This order certainly divides $[E : k] = bg'$. □

Lemma 3.8. *G possesses a faithful absolutely irreducible projective representation of degree s over k .*

Proof. We are free to choose P and Q arbitrarily in k^\times ; by choosing $Q \in (k^\times)^{bg'}$, for example, we guarantee that $Q \in N_{E/k}(E^\times)$ and $B_1 \cong M_{g'b}(k)$.

In this case $B \cong M_s(k)$ and the restriction of \tilde{T} to any transversal for R in F is a faithful absolutely irreducible projective representation of G of degree s . □

By counting dimensions over k it is apparent that B is isomorphic to a twisted group ring of G over k if and only if $s^2 = |G|$, i.e., if and only if $m = s$. We summarize these results as follows.

Theorem 3.9. *Let G be the finite metacyclic group of (3.1) and let E be a subfield of \mathbb{C} . Then G possesses central simple twisted group rings over E if and only if $E \supseteq k$ and*

1. $G = \langle x \rangle \rtimes \langle y \rangle$;
2. $|\langle x \rangle| = |\langle y \rangle| = m$;
3. $m \mid \alpha(m)$ and $m \nmid \alpha(i)$ for $i < m$.

4. METACYCLIC GROUPS HAVING CENTRAL SIMPLE TWISTED GROUP RINGS

The remainder of this paper is devoted to a description and enumeration of the finite metacyclic groups described in Theorem 3.9. Of course, these include all groups of the form $C_m \times C_m$, but there are also nonabelian examples.

Let G be a metacyclic group of order m^2 with presentation

$$(4.1) \quad G = \langle x, y \mid x^m = 1, y^m = 1, y^{-1}xy = x^r \rangle.$$

For a particular value of m we will determine those values of r for which G has central simple twisted group rings. In general, for a positive integer r , we define the function $\alpha_r : \mathbb{N} \rightarrow \mathbb{N}$ by

$$\alpha_r(i) = 1 + r + r^2 + \dots + r^{i-1}.$$

We begin with some observations about α_r . First we remark that $\alpha_r(n_1)$ divides $\alpha_r(n_2)$ if n_1 divides n_2 .

Lemma 4.1. *Let p be an odd prime dividing $r - 1$. Then for positive integers i and j we have*

$$p^i | \alpha_r(j) \iff p^i | j.$$

Proof. Since $r \equiv 1 \pmod p$, $\alpha_r(j) \equiv j \pmod p$ and $p | \alpha_r(j)$ if and only if $p | j$.

Thus $p | \alpha_r(p)$ and $p \nmid \alpha_r(l)$ for $l < p$. Suppose $r = ap + 1$, $a \in \mathbb{Z}$. Then

$$\begin{aligned} \alpha_r(p) &= 1 + r + \dots + r^{p-1} \\ &= 1 + (ap + 1) + \dots + (ap + 1)^{p-1} \\ \implies \alpha_r(p) &\equiv p + ap \frac{p(p-1)}{2} \pmod{p^2} \\ \implies \alpha_r(p) &\equiv p \pmod{p^2} \text{ since } 2 | p - 1. \end{aligned}$$

Thus $p | \alpha_r(p)$ but $p^2 \nmid \alpha_r(p)$.

The result now follows easily by induction, since, in general,

$$\alpha_r(p^i j') = \alpha_r(p^i) \left(1 + r^{p^i} + r^{2p^i} + \dots + r^{(j'-1)p^i} \right)$$

and $1 + r^{p^i} + r^{2p^i} + \dots + r^{(j'-1)p^i}$ is divisible by p only if $p | j'$ and by p^2 only if $p^2 | j'$. \square

Lemma 4.2. *Suppose r is odd. Then:*

- (i) *If $r \equiv 1 \pmod 4$, then $2^i | \alpha_r(j) \iff 2^i | j$.*
- (ii) *If $r \equiv 3 \pmod 4$ and $i \geq 2$, then $2^i | \alpha_r(j) \iff 2^{i-1} | j$.*

Lemma 4.2 can be proved in exactly the same way as Lemma 4.1. \square

Now suppose that m and r are relatively prime positive integers for which $r < m$ and $m | \alpha_r(m)$ but $m \nmid \alpha_r(i)$ for any $i < m$. This leads to the following conclusions.

Lemma 4.3. *Every prime divisor of m divides $r - 1$.*

Proof. Suppose not, and let $m = p_1^{a_1} \dots p_t^{a_t} q$, where p_1, \dots, p_t are the distinct prime divisors of m which do not divide $r - 1$, and q is relatively prime to $p_1 p_2 \dots p_t$. For $i = 1, \dots, t$, let s_i denote the order of r modulo $p_i^{a_i}$. Then

$$p_i^{a_i} | r^{s_i} - 1 \implies p_i^{a_i} | \alpha_r(s_i),$$

since $p_i \nmid r - 1$. It now follows from Lemmas 4.1 and 4.2 that $q | \alpha_r(q)$, hence $m | \alpha_r(s_1 \dots s_t q)$. This is a contradiction since $s_1 \dots s_t q < m$. \square

Lemma 4.4. *Let $b = \text{ord}_m(r)$. Then $b|m$ and $b = \text{gcd}(m, \alpha_r(b))$.*

Proof. That $b|m$ is obvious since $m|\alpha(m) \implies m|r^m - 1$. Also, $b|\alpha_r(b)$ since every prime divisor of b divides m and hence $r - 1$. Let $b' = \text{gcd}(m, \alpha_r(b))$ and let $d = m/b'$. Then $b|b'$ and $d|r - 1$ since $m|\alpha_r(b)(r - 1)$. Now

$$\alpha_r(bd) = \alpha_r(b)(1 + r^b + \cdots + r^{(d-1)b}),$$

and $m|\alpha_r(bd)$ since $b'|\alpha_r(b)$ and $d|1 + r^b + \cdots + r^{(d-1)b}$ as $r \equiv 1 \pmod{d}$. Thus $bd = m$, so $b' = b$ and $d = m/b$. \square

Lemma 4.5. $d = \text{gcd}(m, r - 1)$.

Proof. Let $d' = \text{gcd}(m, r - 1)$ and let $b'' = m/d'$. Then $d|d'$, $b''|b$ and

$$b''|\alpha_r(b'') \implies b''d'|r^{b''} - 1 \implies m|r^{b''} - 1.$$

So $b|b''$ and $b = b''$, $d' = d$. \square

It follows from Lemmas 4.3 and 4.5 that every prime divisor of m must divide d .

We now show that the necessary conditions established in Lemmas 4.3 and 4.5 for the metacyclic group of (4.1) to have central simple twisted group rings are generally sufficient, except when $4|m$ in which case an additional stipulation is needed.

Lemma 4.6. *Suppose $d|m$ and that every prime divisor of m divides d . Let $b = m/d$ and let $r = ad + 1$, where $1 \leq a \leq b$ and $\text{gcd}(a, b) = 1$. Then $m|\alpha_r(m)$ and, provided that $4|d$ if $4|m$, $m|\alpha_r(i)$ for $i \leq m$.*

Proof. That $m|\alpha_r(m)$ is immediate from Lemmas 4.2 and 4.1. Let $m = 2^{m_1}m_2$, where m_2 is odd, and suppose that $m|\alpha_r(i)$. If p is an odd prime with $p^j|m$, then $p^j|i$ by Lemma 4.1, hence $m_2|i$. Also, if $m_1 = 0$ or $m_1 = 1$, then $2^{m_1}|i$ by Lemma 4.2, and $m|i$.

Suppose $m_1 \geq 2$. Then by Lemma 4.2, $2^{m_1}|\alpha_r(i)$ implies $2^{m_1}|i$ only if $r \equiv 1 \pmod{4}$, i.e., only if $4|d$. If $4|m$ and $r \equiv 3 \pmod{4}$, then $2^{m_1}|\alpha_r(2^{m_1-1})$ and $m|\alpha_r(m/2)$. \square

Lemma 4.6 shows that given m , we may construct a finite metacyclic group of order m^2 having central simple twisted group rings. We first choose a divisor d of m which is divisible by every prime dividing m , and by 4 if $4|m$, then choose $a \in \{1, \dots, m/d\}$ with $\text{gcd}(a, m/d) = 1$ and set $r = ad + 1$ in (4.1). In the resulting metacyclic group G we have $|\mathcal{Z}(G)| = d^2$, so that different choices of d certainly determine nonisomorphic groups.

We now show that having chosen d as described above, there is no loss of generality in setting $r = d + 1$. For a given d , different choices of r correspond to different choices of the generator of $\langle y \rangle$ in (4.1).

Lemma 4.7. *Given m , the metacyclic group of (4.1) is fully determined by the choice of $d = \text{gcd}(m, r - 1)$.*

Proof. Having chosen d , and defined $b = m/d$, we may set $r = ad + 1$ where $1 \leq a \leq b$ and $\text{gcd}(a, b) = 1$. So the number of possible choices for r is $\phi(b)$.

On the other hand, suppose G has been determined by choosing $a = 1$ and setting $r = d + 1$. Changing the presentation of G in (4.1) by substituting for y another generator y^l of $\langle y \rangle$ amounts to replacing r in (4.1) by the residue modulo

m of r^l , where $\gcd(l, m) = 1$. For any such l , $\gcd(r^l - 1, m) = d$; so r^l is congruent modulo m to one of the $ad + 1$ described above.

The number of generators of $\langle y \rangle$ is $\phi(m)$. We now show that amongst the $\phi(m)$ possible r^l are $\phi(b)$ having distinct residues modulo m .

Let $a_1, \dots, a_{\phi(b)}$ be the elements of $\{1, \dots, b\}$ which are relatively prime to b . For $i = 1, \dots, \phi(b)$ define d_i as follows:

- $d_i = 0$ if $\gcd(a_i, m) = 1$.
- If $\gcd(a_i, m) \neq 1$, d_i is defined as the greatest divisor of d which is relatively prime to a_i . So d_i is divisible by any prime which divides m but not a_i .

Now define

$$a'_i = a_i + bd_i, \quad i = 1, \dots, \phi(b).$$

Then $\gcd(m, a'_i) = 1$ for $i = 1, \dots, \phi(b)$, since for each i every prime dividing m divides either a_i or bd_i , but not both. Now suppose for some $1 \leq j_1 \leq j_2 \leq \phi(b)$ that

$$r^{a'_{j_1}} \equiv r^{a'_{j_2}} \pmod{m}.$$

Then

$$r^{a'_{j_1} - a'_{j_2}} \equiv 1 \pmod{m} \implies b|a'_{j_1} - a'_{j_2}.$$

This is impossible since $a'_1, a'_2, \dots, a'_{\phi(b)}$ all have different residues modulo b .

We conclude that every admissible choice of $r = ad + 1$ is congruent modulo m to some $(d + 1)^i$ with $1 \leq i \leq m$ and $\gcd(i, m) = 1$, proving the lemma. \square

It follows from Lemma 4.7 and the comments preceding it that the number of isomorphism types of metacyclic groups of order m^2 having central simple twisted group rings is the number of factors d of m having the properties described in Lemma 4.6: every prime dividing m divides d and $4|d$ if $4|m$. We have proved the following result.

Theorem 4.8. *Let m be a positive integer with*

$$m = 2^a p_1^{a_1} \dots p_t^{a_t},$$

where p_1, \dots, p_t are distinct odd primes, $a \geq 0$ and $a_i \geq 1$ for $i = 1, \dots, t$. Then the number of isomorphism types of metacyclic groups of order m^2 having central simple twisted group rings is

$$\prod_{i=1}^t a_i \quad \text{if } a \leq 1,$$

$$(a - 1) \prod_{i=1}^t a_i \quad \text{if } a \geq 2.$$

\square

In particular, if m is a product of distinct primes, or if m is even and $m/2$ is a product of distinct primes, then the only metacyclic group of order m^2 having central simple twisted group rings over fields is the abelian group $C_m \times C_m$.

REFERENCES

1. B. Huppert, *Endliche gruppen I*, Springer-Verlag, Berlin-Heidelberg-New York, 1967. MR **37**:302
2. N. Jacobson, *Basic algebra II*, W.H. Freeman, San Francisco, 1980. MR **81g**:00001
3. H.N. Ng, *Faithful irreducible projective representations of metabelian groups*, J. Algebra **38** (1976), 8–28. MR **55**:5732
4. D.S. Passman, *The algebraic structure of group rings*, Wiley, New York, 1977. MR **81d**:16001
5. R. Quinlan, *Generic central extensions and projective representations of finite groups*, Represent. Theory **5** (2001), 129–146. MR **2002e**:20021
6. K. Yamazaki, *On projective representations and ring extensions of finite groups*, J. Fac. Sci. Univ. Tokyo Sect. 1 **10** (1964), 147–195. MR **31**:4842

DEPARTMENT OF MATHEMATICS, UNIVERSITY COLLEGE, DUBLIN, IRELAND
E-mail address: `rachel.quinlan@ucd.ie`