Canad. Math. Bull. Vol. **37** (2), 1994 pp. 228–237

UNITS OF INTEGRAL GROUP RINGS OF SOME METACYCLIC GROUPS

ERIC JESPERS, GUILHERME LEAL AND C. POLCINO MILIES

ABSTRACT. In this paper, we consider all metacyclic groups of the type $\langle a, b \mid a^n = 1, b^2 = 1, ba = a^i b\rangle$ and give a concrete description of their rational group algebras. As a consequence we obtain, in a natural way, units which generate a subgroup of finite index in the full unit group, for almost all such groups.

1. **Introduction.** Let $U = U(\mathbf{Z}G)$ denote the group of units of the integral group ring of a finite group G, and set $V = V(\mathbf{Z}G) = \{u \in U \mid \epsilon(u) = 1\}$, where $\epsilon: \mathbf{Z}G \longrightarrow \mathbf{Z}$ denotes the augmentation mapping. A natural question is to describe this group constructively, by giving a set of generators. Since this is a difficult problem, it has been a general trend to look for sets of generators of subgroups of finite index in V. This was first done in a paper by H. Bass [1]. Given an element $a \in G$ of order d, if we set $\phi(|G|) = m$, where ϕ denotes the Euler function, the element

$$u = (1 + a + \cdots + a^{i-1})^m + \frac{1 - i^m}{d}(1 + a + \cdots + a^{d-1})$$

is integral when $i^m \equiv 1 \pmod d$ and belongs to V. Moreover, all these elements, called the *Bass cyclic units* of $\mathbf{Z}G$, generate a subgroup which is of finite index in V in the case where G is abelian.

When G is not abelian more units are needed to generate a subgroup of finite index. J. Ritter and S. K. Sehgal [13] introduced the units

$$\mu_{a,b} = 1 + (a - 1)b(1 + a + \cdots + a^{o(a)-1}),$$

$a, b \in G$, and called these elements the *bicyclic units* of $\mathbf{Z}G$. They have shown that the Bass cyclic units together with all the bicyclics generate a subgroup of finite index in $V(\mathbf{Z}G)$ when G is either a dihedral group of order $2n$ (denoted D_{2n}) or a nilpotent group—except for a few cases, which concern groups G having certain types of Wedderburn components in $\mathbf{Q}G$. In [14] Ritter and Sehgal showed that the same result holds for some metacyclic groups, including those of the type $\langle a, b \mid a^p = 1, b^2 = 1, ba = a^i b\rangle$, p an odd prime. For a survey of these and related results, the reader may consult the surveys by J. Ritter [11] or S. K. Sehgal [15].

The first author was supported in part by NSERC-grant OGP0036631.
The last two authors were partially supported by a research grant from CNPq.
Received by the editors September 30, 1992; revised April 14, 1993 and June 25, 1993.
AMS subject classification: 20C05, 16S34, 16U60.

In this paper, we shall consider all metacyclic groups of the type:

$$G = \langle a, b \mid a^n = 1, b^2 = 1, ba = a^i b\rangle.$$

First, we shall give a description of the rational group algebra $\mathbf{Q}G$. In the case of the dihedral group, this was done by E. Kleinert in [8], however even in this case our description contains more information in the sense that we completely determine the Wedderburn decomposition by giving the elements that are mapped to the matrix units. Also our methods are more elementary since we need no representation theory.

As a consequence we obtain, in a natural way, units which generate a subgroup of finite index in the full unit group, for almost all groups G in this family.

2. **Rational group algebras.** Throughout the paper G is a metacyclic group with presentation

$$G = \langle a, b \mid a^n = 1, b^2 = 1, ba = a^i b\rangle.$$

Note, it follows that $i^2 \equiv 1 \pmod{n}$. Examples of such groups are dihedral groups.

For a subgroup H of G we denote $\hat{H} = \frac{1}{|H|}\sum_{h\in H} h$, and for an element $g \in G$ we set $\hat{g} = \widehat{\langle g\rangle}$.

Clearly

$$\begin{aligned} \mathbf{Q}G &= \mathbf{Q}G\widehat{G'} \oplus \mathbf{Q}G(1-\widehat{G'}) \\ &\cong \mathbf{Q}(G/G') \oplus \Delta(G:G'). \end{aligned}$$

where $\Delta(G : G')$ denotes the kernel of the natural homomorphism $\mathbf{Q}G \longrightarrow \mathbf{Q}(G/G')$. As shown in [2, Lemma 1.2], $\Delta(G : G')$ contains no commutative simple component. Also, it is easy to see that $\Delta(G : G') = \mathbf{Q}G(1 - \widehat{G'})$.

Set $d = \gcd(n, i-1)$. We have that $Z(G) = \langle a^{\frac{n}{d}}\rangle$, $G' = \langle a^{i-1}\rangle$, and the non-central conjugacy classes are either of the form $a^j bG'$, $0 \leq j \leq d-1$, or of the form $\{a^r, a^{ri}\}$ with $a^r \notin Z(G)$. So the number of conjugacy classes of G is $[Z(\mathbf{Q}G) : \mathbf{Q}] = 2d + \frac{n-d}{2}$.

Write:

$$\mathbf{Q}G \cong \mathbf{Q}(G/G') \oplus A_1 \oplus \cdots \oplus A_t$$

where A_i is simple and $[A_i : Z(A_i)] \geq 4$, $1 \leq i \leq t$.

It follows from [3, §47] that all these simple components are four dimensional over their respective centers. We give an elementary proof of this fact.

As

$$Z(\mathbf{Q}G) \cong \mathbf{Q}(G/G') \oplus Z(A_1) \oplus \cdots \oplus Z(A_t)$$

we obtain $2n - 2d = [\Delta(G : G') : \mathbf{Q}] = \sum_{i=1}^{t}[A_i : \mathbf{Q}] \geq 4\sum_{i=1}^{t}[Z(A_i) : \mathbf{Q}] = 4\left[\left(2d + \frac{n-d}{2}\right) - 2d\right]$. Hence, all simple components of $\Delta(G : G')$ are four-dimensional over their centers.

We recall, from the proof of [5, Theorem (2.4)], that if we write $n = p_1^{n_1}\cdots p_t^{n_t}$, where p_j is a rational prime and $n_j \geq 1$, $1 \leq j \leq t$, then the primitive idempotents of $\mathbf{Q}\langle a\rangle$ are all products of the form

$$E_1E_2\cdots E_t, \quad E_j = \widehat{K_j} - \widehat{H_j} \quad \text{or} \quad E_j = \widehat{\langle a^{np_j^{-n_j}}\rangle}$$

https://doi.org/10.4153/CMB-1994-034-0 Published online by Cambridge University Press

where K_j, H_j denote p_j-subgroups of $\langle a\rangle$ such that $K_j \subseteq H_j$ and $|H_j/K_j| = p_j$, $1 \leq j \leq t$.

Let $L_j = \widehat{K_j}$ if $E_j = \widehat{K_j} - \widehat{H_j}$ and $L_j = E_j$ otherwise. Then, each idempotent is uniquely determined by

$$\operatorname{supp}(L_1)\cdot\operatorname{supp}(L_2)\cdots\operatorname{supp}(L_t) = \langle a^m\rangle,$$

and hence, is completely determined by a divisor m of n. So we will denote an arbitrary primitive central idempotent by e_m, $m \mid n$. Also it is easy to verify that $Ge_m \cong G/\langle a^m\rangle$. Hence $|Ge_m| = 2m$, and if $\mathbf{Q}Ge_m$ is non-commutative then $m > 2$.

Since all the subgroups of $\langle a\rangle$ are normal in G, it follows that every idempotent of $\mathbf{Q}\langle a\rangle$ is central in $\mathbf{Q}G$. Therefore, the primitive central idempotents of $\Delta(G : G')$ are those idempotents $e_m \in \mathbf{Q}\langle a\rangle$ such that $e_m\widehat{G'} = 0$. Using the above notation, one can easily verify that this happens if and only if e_m has a factor of the form $\widehat{K_j} - \widehat{H_j}$, with $H_j \subseteq G'$.

Let $e_m \in \Delta(G : G')$. As $e_m \in \mathbf{Q}\langle a\rangle$, it follows that $e_m(1+b) \neq 0$, $e_m(1-b) \neq 0$ but $\big(e_m(1+b)\big)\big(e_m(1-b)\big) = 0$. Therefore any simple component $\mathbf{Q}Ge_m = A_j$ has zero divisors and thus is a two-by-two matrix ring over a field.

Now, we shall give a constructive description of $\mathbf{Q}Ge_m$, by exhibiting a basis of matrix units.

PROPOSITION 2.1. *Let e_m be a primitive central idempotent in $\Delta(G : G')$. Then the following elements form a basis of matrix units of $\mathbf{Q}Ge_m$:*

$$e_{11} = \Big(\frac{1+b}{2}\Big)e_m \quad e_{12} = \Big(\frac{1+b}{2}\Big)a\Big(\frac{1-b}{2}\Big)e_m$$
$$e_{21} = 4\big((a-a^i)e_m\big)^{-2}\Big(\frac{1-b}{2}\Big)a\Big(\frac{1+b}{2}\Big)e_m \quad e_{22} = \Big(\frac{1-b}{2}\Big)e_m.$$

PROOF. Let $R = \mathbf{Q}Ge_m$. Write

$$R = \Big(\frac{1+b}{2}\Big)R\Big(\frac{1+b}{2}\Big) + \Big(\frac{1+b}{2}\Big)R\Big(\frac{1-b}{2}\Big) + \Big(\frac{1-b}{2}\Big)R\Big(\frac{1+b}{2}\Big) + \Big(\frac{1-b}{2}\Big)R\Big(\frac{1-b}{2}\Big).$$

Since $\mathbf{Q}Ge_m$ is non-commutative it follows that $be_m \neq -e_m$. Hence $\big(\frac{1+b}{2}\big)e_m \neq 0$. Because R is prime we therefore obtain $\big(\frac{1+b}{2}\big)R\big(\frac{1+b}{2}\big) \neq \{0\}$. Similarly, $\big(\frac{1-b}{2}\big)R\big(\frac{1-b}{2}\big) \neq \{0\}$. Because $[R : Z(R)] = 4$, we obtain $1 \leq \big[\big(\frac{1+b}{2}\big)R\big(\frac{1+b}{2}\big) : Z(R)\big] < 4$. As $\big(\frac{1+b}{2}\big)R\big(\frac{1+b}{2}\big)$ is a central simple algebra, this yields $\big[\big(\frac{1+b}{2}\big)R\big(\frac{1+b}{2}\big) : Z(R)\big] = 1$. Similarly $\big[\big(\frac{1-b}{2}\big)R\big(\frac{1-b}{2}\big) : Z(R)\big] = 1$. As $\big(\frac{1+b}{2}\big)R\big(\frac{1-b}{2}\big)$ and $\big(\frac{1-b}{2}\big)R\big(\frac{1+b}{2}\big)$ are isomorphic as additive groups, it also follows that $\big(\frac{1+b}{2}\big)R\big(\frac{1-b}{2}\big)$ and $\big(\frac{1-b}{2}\big)R\big(\frac{1+b}{2}\big)$ have dimension 1 over $Z(R)$.

We now claim that $\big(\frac{1+b}{2}\big)a\big(\frac{1-b}{2}\big)e_m \neq 0$. For if not, then

$$ae_m = \Big[\Big(\frac{1+b}{2}\Big)a\Big(\frac{1+b}{2}\Big) + \Big(\frac{1-b}{2}\Big)a\Big(\frac{1+b}{2}\Big) + \Big(\frac{1-b}{2}\Big)a\Big(\frac{1-b}{2}\Big)\Big]e_m.$$

Hence, for any $r \geq 1$, $\big(\frac{1+b}{2}\big)a^r\big(\frac{1-b}{2}\big)e_m = 0$. Consequently $\big(\frac{1+b}{2}\big)R\big(\frac{1-b}{2}\big) = \{0\}$, a contradiction. Similarly, $\big(\frac{1-b}{2}\big)a\big(\frac{1+b}{2}\big)e_m \neq 0$.

Next we claim

$$\frac{(a-a^i)^2}{4}\Big(\frac{1-b}{2}\Big)e_m = \Big[\Big(\frac{1-b}{2}\Big)a\Big(\frac{1+b}{2}\Big)\Big]\Big[\Big(\frac{1+b}{2}\Big)a\Big(\frac{1-b}{2}\Big)\Big]e_m \neq 0.$$

For if not, then, because $\left(\frac{1+b}{2}\right)R\left(\frac{1-b}{2}\right)$ and $\left(\frac{1-b}{2}\right)R\left(\frac{1+b}{2}\right)$ are one dimensional over $Z(R)$ and because of the previous claim,

$$\alpha\Big[\Big(\Big(\frac{1+b}{2}\Big)R\Big(\frac{1-b}{2}\Big)\Big)+\Big(\Big(\frac{1-b}{2}\Big)R\Big(\frac{1-b}{2}\Big)\Big)\Big] = \{0\},$$

where $\alpha = \left(\frac{1-b}{2}\right)a\left(\frac{1+b}{2}\right)$. So $\alpha R\left(\frac{1-b}{2}\right) = \{0\}$, a contradiction as R is a simple ring and $\alpha \neq 0$.

Since $(a-a^i)^2 e_m$ is central, the second claim yields that $(a-a^i)^2 e_m$ has an inverse in $Z(\mathbf{Q}Ge_m)$. The result now follows by verifying the identities $e_{11}+e_{22} = e_m$ and $e_{uv}e_{kl} = \delta_{vk}e_{ul}$. ∎

Now, we wish to compute the centers of the simple components of $\Delta(G : G')$. Let $e_m \in \Delta(G : G')$ be a primitive central idempotent. Note that $Z(\mathbf{Q}Ge_m)$ is generated as a vector space over $\mathbf{Q}$ by the elements of $\{(a^r + a^{ri})e_m \mid 0 \leq r \leq n\}$. By [10], write $\mathbf{Q}\langle a\rangle = \oplus_{m|n}\mathbf{Q}\langle a\rangle e_m \cong \oplus_{m|n}\mathbf{Q}(\xi_m)$, where ξ_m denotes a primitive root of unity of order m. Since a corresponds with $(\xi_m)_{m|n}$ under this isomorphism, we see that

$$Z(\mathbf{Q}Ge_m) \cong \mathbf{Q}(\xi_m + \xi_m^i, \xi_m^2 + \xi_m^{2i}, \ldots).$$

We shall denote this field by $\mathbf{Q}_m$. Further, since

$$\begin{aligned}\mathbf{Q}\langle a\rangle &= \mathbf{Q}\langle a\rangle\widehat{G'} \oplus \mathbf{Q}(1-\widehat{G'})\\ &\cong \mathbf{Q}(\langle a\rangle/\langle a^{i-1}\rangle) \oplus \big(\mathbf{Q}\langle a\rangle \cap \Delta(G : G')\big)\end{aligned}$$

and $|\langle a\rangle/\langle a^{i-1}\rangle| = d$, we have that

$$\mathbf{Q}(\langle a\rangle/\langle a^{i-1}\rangle) \cong \bigoplus_{m|d}\mathbf{Q}(\xi_m),$$

and thus

$$\mathbf{Q}\langle a\rangle \cap \Delta(G : G') \cong \bigoplus_{\substack{m|n\\ m\nmid d}}\mathbf{Q}(\xi_m).$$

So we have shown:

THEOREM 2.2. *Let G be a group as above, and $d = \gcd(n, i-1)$. Then*

$$\mathbf{Q}G \cong \mathbf{Q}(G/G') \oplus \Big(\bigoplus_{\substack{m|n\\ m\nmid d}} M_2(\mathbf{Q}_m)\Big).$$

3. **Subgroups of finite index.** The concrete description of the rational group algebra by means of matrix units allows one to compute explicitly the unit group of integral group rings of some dihedral group rings. This was done by E. Jespers and M. M. Parmenter in [6] for D_6, and by E. Jespers and G. Leal in [4] for D_8. In both cases it was shown that the bicyclic units generate a free normal complement of rank 3.

In this section we show that the explicit description of the rational group algebra also allows us to determine generators of a subgroup of finite index in $V(\mathbf{Z}G)$, for almost all groups in this family. We need the following result of L. N. Vaserstein [17] which we quote from [12].

LEMMA 3.1. *Let K be a number field which is not rational or imaginary quadratic, and let O be the ring of integers. Then*

$$[\mathrm{SL}(2, O) : E(I)] < \infty,$$

where I is a non-zero ideal of O and $E(I)$ is the group generated by the matrices $\begin{bmatrix} 1 & 0 \\ x & 1 \end{bmatrix}, \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}, x \in I$.

Our next lemma shows precisely when the exceptions above occur.

LEMMA 3.2. *Let $e_m \in \Delta(G : G')$ be a primitive central idempotent, i.e. $m \mid n$ but $m \not| d$.*

1. $\mathbf{Q}Ge_m \cong M_2(\mathbf{Q})$ if and only if $m = 3$, $m = 4$ or $m = 6$. Furthermore, if $m = 3$ (respevtively 4), then $Ge_m \cong D_6$ (respectively D_8).

2. $\mathbf{Q}Ge_m$ is a simple component which is a two-by-two matrix ring over a quadratic imaginary extension of $\mathbf{Q}$ if and only if one of the following conditions hold:

(a) $m = 8$ and $i \equiv 3$ or $5 \pmod 8$;

(b) $m = 12$ and $i \equiv 5$ or $7 \pmod{12}$.

PROOF. By Theorem 2.2, $\mathbf{Q}Ge_m = M_2(\mathbf{Q}_m)$, $\mathbf{Q}_m = \mathbf{Q}(\xi_m + \xi_m^i, \xi_m^2 + \xi_m^{2i}, \ldots)$. Because of the non-commutativity of $\mathbf{Q}Ge_m$, $babe_m = \xi_m^i e_m \neq \xi_m e_m = ae_m$.

PROOF OF (1). Clearly $\mathbf{Q}_m = \mathbf{Q}$ implies $\xi_m^i = \xi_m^{-1}$ or $\xi_m^i = -\xi_m$. We consider these two cases separately.

If $\xi_m^i = \xi_m^{-1}$, since $[\mathbf{Q}(\xi_m) : \mathbf{Q}(\xi_m + \xi_m^{-1})] = 2$, we obtain that $[\mathbf{Q}(\xi_m + \xi_m^{-1}) : \mathbf{Q}] = \frac{\varphi(m)}{2} \geq \frac{p^{\alpha-1}(p-1)}{2}$, where $p^\alpha \mid m$, p a prime. Hence $m = 3$, $m = 4$ or $m = 6$ and it is clear that Ge_3 (respectively Ge_4) is isomorphic with D_6 (respectively D_8).

Clearly the converse also holds, *i.e.* $\mathbf{Q}_3 = \mathbf{Q}_4 = \mathbf{Q}$ as $(i, m) = 1$.

On the other hand, if $\xi_m^i = -\xi_m$ then $\xi_m^2 + \xi_m^{2i} = 2\xi_m^2 \in \mathbf{Q}$. So $m = 4$, and as $(m, i) = 1$, we obtain that $i \equiv -1 \pmod 4$. Consequently $Ge_m \cong D_8$, and (1) follows.

PROOF OF (2). Assume $\mathbf{Q}_m$ is quadratic imaginary. Let p be a prime divisor of m. Clearly $\mathbf{Q}_m$ contains the field

$$F = \mathbf{Q}(\xi_p + \xi_p^i),$$

where ξ_p is a primitive p-th root of unity.

We now first show that $p \leq 5$. If not, then F has the Frobenius automorphism defined by $\xi_p \longmapsto \xi_p^2$. As $[F : \mathbf{Q}] \leq 2$, the square of this automorphism is the identity mapping. Hence

$$\xi_p + \xi_p^i = \xi_p^4 + \xi_p^{4i}.$$

However this is impossible since $\{1, \xi_p, \ldots, \xi_p^{p-1}\}$ are linearly independent, and because, by assumption $p > 5$.

If $p = 5$, then one can see that $i \equiv -1 \pmod 5$. So, $\mathbf{Q}_m$ contains a real field of degree 2, and therefore is not quadratic imaginary; a contradiction.

If $p = 3$ and $9 \mid m$, then $\mathbf{Q}_m$ contains the subfield $F = \mathbf{Q}(\xi_9 + \xi_9^i)$, ξ_9 a 9-th root of unity. Since $i^2 \equiv 1 \pmod n$ it follows that $i \equiv -1 \pmod 9$. So F is a real field and by (1) is different from $\mathbf{Q}$. Hence in this case $\mathbf{Q}_m$ is not quadratic imaginary; again a contradiction.

So far we have shown that $m = 2^k$ or $m = 2^k 3$ for some $k \geq 1$. We now claim that $k \geq 2$. For if not, then, because of (1), $m = 6$. Therefore $i^2 \equiv 1 \pmod 6$, and thus $\xi_m^i = \xi_m^{-1}$. In particular, $\mathbf{Q}_m$ is real, a contradicition. This proves the claim.

Let us now deal with the remaining cases, *i.e.* $m = 2^k$ or $m = 2^k 3$, $k \geq 2$. Assume $m = 2^k$. Let $H = \langle c, d \mid c^{2^k} = 1, d^2 = 1, dc = c^i d\rangle$. Then it is easily seen that $\mathbf{Q}Ge_m$ is a homomorphic image of

$$\mathbf{Q}H \cong \mathbf{Q}(H/\langle c^{2^{k-1}}\rangle) \oplus \mathbf{Q}H\Big(\frac{1 - c^{2^{k-1}}}{2}\Big).$$

Since $\big(\frac{1-c^{2^{k-1}}}{2}\big)$ is a primitive central idempotent of $\mathbf{Q}H$, and because $|H/\langle c^{2^{k-1}}\rangle| = 2^k$, it follows that $\mathbf{Q}H\big(\frac{1-c^{2^{k-1}}}{2}\big)$ is isomorphic with a two-by-two matrix ring over a field of degree $\frac{2^{k+1}-2^k}{4} = 2^{k-2}$. Since $2^{k-2} > 2$ if $k \geq 4$, we obtain, by induction, that $\mathbf{Q}Ge_m$ is a homomorphic image of the rational group algebra $\mathbf{Q}C$ where $C = \langle c, d \mid c^8 = 1, d^2 = 1, dc = c^i d\rangle$. Since $i^2 \equiv 1 \pmod 8$ it follows that $i \equiv 3, 5$ or $7 \pmod 8$. If $i \equiv 7 \pmod 8$, then $C = D_{16}$, and it is well-known that $\mathbf{Q}D_{16}$ has no simple component which is a two-by-two matrix ring over a quadratic imaginary extension of $\mathbf{Q}$. On the other hand if $i \equiv 3 \pmod 8$ (respectively $5 \pmod 8$), then C is isomorphic with group D_{16}^- (respectively D_{16}^+, *cf.* [12]). It is well-known (see for example [4, 7]) that in both cases $\mathbf{Q}C$ has a simple component which is a two-by-two matrix ring over a quadratic imaginary extension of $\mathbf{Q}$.

Finally we deal with $m = 2^k 3$. Let $J = \langle c, d \mid c^{2^k 3} = 1, d^2 = 1, dc = c^i d\rangle$. Again it is easily seen that $\mathbf{Q}Ge_m$ is a homomorphic image of

$$\begin{aligned}
\mathbf{Q}J &\cong \mathbf{Q}J\Big(\frac{1 + c^{2^{k-1}3}}{2}\Big) \oplus \mathbf{Q}J\Big(\frac{1 - c^{2^{k-1}3}}{2}\Big) \\
&\cong \mathbf{Q}J\Big(\frac{1 + c^{2^{k-1}3}}{2}\Big) \oplus \mathbf{Q}J\widehat{c^{2^k}}\Big(\frac{1 - c^{2^{k-1}3}}{2}\Big) \\
&\quad \oplus \mathbf{Q}J(1 - \widehat{c^{2^k}})\Big(\frac{1 - c^{2^{k-1}3}}{2}\Big)
\end{aligned}$$

https://doi.org/10.4153/CMB-1994-034-0 Published online by Cambridge University Press

$$\cong \mathbf{Q}(J/\langle c^{2^{k-1}3}\rangle) \oplus \mathbf{Q}(J/\langle c^{2^k}\rangle)\Big(\frac{1-(c^3)^{2^{k-1}}}{2}\Big)$$
$$\oplus\, \mathbf{Q}J\Big(\frac{1-c^{2^{k-1}3}}{2}\Big)(1-\widehat{c^{2^k}}).$$

Either $\mathbf{Q}J\big(\frac{1-c^{2^{k-1}3}}{2}\big)(1-\widehat{c^{2^k}})$ is a field, or otherwise it is a two-by-two matrix ring over a field extension of $\mathbf{Q}$ which, by calculating dimensions of the above terms, is of degree

$$\frac{2^{k+1}3 - 2^k 3 - (2^{k+1} - 2^k)}{4} = 2^{k-1}.$$

If $k \geq 3$ then this degree is larger than 2, and hence $\mathbf{Q}Ge_m$ is not this simple component. Also, as $|J/\langle c^{2^k}\rangle|$ is not divisible by three, it follows that $\mathbf{Q}Ge_m$ is not a simple component of $\mathbf{Q}(J/\langle c^{2^k}\rangle)\big(\frac{1-(c^3)^{2^{k-1}}}{2}\big)$. So, by induction, we obtain that $k = 2$, and thus $m = 12$.

So assume now that $m = 12$ and $J = \langle c, d \mid c^{12} = 1, d^2 = 1, dc = c^i d\rangle$, and $\mathbf{Q}Ge_m$ is a simple component of $\mathbf{Q}J$. Now $i^2 \equiv 1 \pmod{12}$ yields $i = 5$, 7 or 11 modulo 12. The case $i \equiv 11 \pmod{12}$ gives that $Z(\mathbf{Q}Ge_m)$ is a real field, a contradiction. If $i \equiv 7 \pmod{12}$ then

$$J = \langle c^3, d\rangle \times \langle c^4\rangle \cong D_8 \times C_3,$$

where C_3 denotes the cyclic group of order 3. Since $\mathbf{Q}D_8$ has a simple component $M_2(\mathbf{Q})$ and because $\mathbf{Q}C_3$ has simple component $\mathbf{Q}(\sqrt{-3})$ it follows that $\mathbf{Q}J$ has simple component $M_2\big(\mathbf{Q}(\sqrt{-3})\big)$. Actually this is the only simple component of $\mathbf{Q}J$ which is a two-by-two matrix ring over a quadratic imaginary extension. Finally if $i \equiv 5 \pmod{12}$ then

$$J = \langle c^3\rangle \times \langle c^4, d\rangle \cong C_4 \times D_6.$$

So, $\mathbf{Q}J$ has exactly one simple component which is a two-by-two matrix ring over a quadratic imaginary field. The result follows. ∎

The next lemma, due to Ritter and Sehgal [14, Lemma 2.4 and Lemma 2.5] will be needed in the proof of Theorem 3.4.

For every $m \mid n$ with $m \nmid d$, we have that $\mathbf{Q}Ge_m = M_2(\mathbf{Q}_m)$. Let O_m denote the ring of integers of the field $\mathbf{Q}_m$ defined earlier. Further let $\pi_m\colon \mathbf{Q}G \longrightarrow \mathbf{Q}Ge_m \cong M_2(\mathbf{Q}_m)$ denote the natural projection.

LEMMA 3.3. *Let S be a subgroup of $\mathcal{U}(\mathbf{Z}G)$ containing the subgroup generated by the Bass cyclic units. If for every $m \mid n$, with $m \nmid d$, the projection $\pi_m(S)$ contains a subgroup of finite index in* $\mathrm{SL}(2, O_m)$, *then S is of finite index in $\mathcal{U}(\mathbf{Z}G)$.*

We now give generators of a subgroup of finite index of $\mathcal{U}(\mathbf{Z}G)$ for many of the metacyclic groups of our class. Because of Lemma 3.1, the groups which cause problems are those which have a two-by-two matrix ring over the rationals or an imaginary quadratic extension of the rationals as a simple component in $\mathbf{Q}G$. Lemma 3.2 tells us that the former case occurs when D_6 or D_8 is a homomorphic image of G. It turns out that the D_6 case poses no difficulty, nor does the case where all elements of order 2 in D_8 have a preimage of order 2 in G.

THEOREM 3.4. *Let* $G = \langle a, b \mid a^n = 1, b^2 = 1, ba = a^i b\rangle$ *and suppose that the following conditions are satisfied:*

1. if $8 \mid n$ *and* $8 \nmid d$ *then* $i \equiv 7 \pmod 8$*;*

2. if $12 \mid n$ *and* $12 \nmid d$ *then* $i \equiv 11 \pmod{12}$.

Let S_1 *be the subgroup of* $\mathcal{U}(\mathbf{Z}G)$ *generated by the Bass cyclic units and the units of the form*

$$1 + (1+b)a^v(1-b) \quad \text{and} \quad 1 + (1-b)a^v(1+b),$$

and let S_2 *be the subgroup generated by the Bass cyclic units and the units of the form*

$$1 + (1+a^u b)a^v(1-a^u b) \quad \text{and} \quad 1 + (1-a^u b)a^v(1+a^u b),$$

where $0 \le u, v \le n$*, and* $n \mid (i+1)u$*. If* $6 \mid d$ *whenever* $6 \mid n$*, then the following statements hold:*

1. If $4 \nmid n$ *or* $4 \mid d$*, then*

(a) if $3 \nmid n$ *or* $3 \mid d$*, then* S_1 *is of finite index in* $\mathcal{U}(\mathbf{Z}G)$*;*

(b) if $3 \mid n$ *and* $3 \nmid d$*, then* S_2 *is of finite index in* $\mathcal{U}(\mathbf{Z}G)$.

2. If $4 \mid n$ *and* $4 \nmid d$*, then if there exists* $u \ge 1$ *with* $4 \mid (u-1)$ *and* $n \mid u(i+1)$*, then* S_2 *is of finite index in* $\mathcal{U}(\mathbf{Z}G)$.

PROOF. Since $[(1+b)a^v(1-b)]^w = 0$, for any $v, w \ge 1$, it follows that S_1 contains the elements of the form $1 + (1+b)\alpha(1-b)$, with $\alpha \in \mathbf{Z}G$. Let e_m be a central primitive idempotent in $\Delta(G : G')$ and let n_m be a non-zero integer such that $n_m e_m \in \mathbf{Z}G$. Further let $R = \mathbf{Z}[\xi_m + \xi_m^i, \xi_m^2 + \xi_m^{2i}, \ldots] = Z(\mathbf{Z}G) \cap \mathbf{Q}Ge_m$ and let d_m be a non-zero integer such that $d_m O_m \subseteq R$. Clearly $I_m = 4(a - a^i)^2 d_m n_m e_m O_m$ is a non-zero ideal of O_m contained in R. Consequently, with notations as in Proposition 2.1, S_1 contains the subgroup generated by $1 + \alpha e_{12}$, $\alpha \in I_m$. Similarly S_1 also contains the subgroup generated by the elements $1 + \alpha e_{21}$, $\alpha \in I_m$.

It therefore follows from Lemma 3.1, Lemma 3.2 and the assumptions that $\pi_m(S_1)$ contains a subgroup of finite index in $\mathrm{SL}(2, O_m)$ if m is different from 3 and 4. On the other hand if $m = 3$ (respectively 4) then by Lemma 3.2, $\mathbf{Q}Ge_m \cong M_2(\mathbf{Q})$ is the non-commutative simple component of $\mathbf{Q}D_6$ (respectively $\mathbf{Q}D_8$). It was shown in [4, 6] that in each case the projection of the group generated by the bicyclic units of $\mathbf{Z}D_6$ (respectively $\mathbf{Z}D_8$) is isomorphic with a free rank 3 subgroup of finite index in $\mathrm{SL}(2, \mathbf{Z})$. Note also that the bicyclic units for the groups D_6 and D_8 are of the type mentioned in S_2. Now if the bicyclic units of the integral group ring $\mathbf{Z}(Ge_m)$ are images of bicyclic units of $\mathbf{Z}G$ (these are units of type S_2), it follows that $\pi_m(S_2)$ contains a subgroup of finite index in $\mathrm{SL}(2, O_m)$ for each $m \mid n$ with $m \nmid d$. The result then follows from Lemma 3.3.

Let us now show that we can lift the bicyclics. First assume that $m = 3$ with $3 \nmid d$. In this case, $D_6 \cong \langle a^{\frac{n}{3}}, b\rangle$ and $\mathbf{Q}Ge_3 \cong M_2(\mathbf{Q})$ is a simple component of $\mathbf{Q}D_6$. Note that it follows that $i \equiv 2 \pmod 3$. So, we consider the map $a \longmapsto a^{\frac{n}{3}}$, $b \longmapsto b$; then the bicyclics (up to inverses) of $\mathbf{Z}D_6$ are $1 + (1-b)a^{\frac{n}{3}}(1+b)$, $1 + (1 - a^{\frac{n}{3}}b)a^{\frac{n}{3}}(1 + a^{\frac{n}{3}}b)$ and $1 + (1 - a^{2\frac{n}{3}}b)a^{\frac{n}{3}}(1 + a^{2\frac{n}{3}}b)$. So to lift these it is sufficient to show that the elements $a^{\frac{n}{3}}b$ and $a^{2\frac{n}{3}}b$ can be lifted to elements $a^u b$ of order 2. Clearly $a^u b$ is of order 2 if and only if

$n \mid u(i+1)$, and $a^{\frac{n}{3}u}b = a^{\frac{n}{3}}b$ (respectively $a^{\frac{n}{3}2u}b = a^{2\frac{n}{3}}b$) if and only if $3 \mid (i-1)$. Since $i \equiv 2 \pmod 3$ we can therefore take $u = i-1$.

Finally the case $m = 4$ is proved similarly under the assumption that $4 \mid (i-1)$ and that there exists $u \geq 1$ with $n \mid u(i+1)$. This finishes the proof. ∎

Let $G = \langle a, b \mid a^{16} = 1, b^2 = 1, ba = a^7 b\rangle$, that is $n = 16$ and $i = 7$. Then $D_8 = \langle a^4, b\rangle$ is a homomorphic image of G. The only elements of D_8 of order 2 which have a preimage in G of order 2 are b and a^8b. Since G is a 2-group, it follows from Theorem 2 in [7] that the Bass cyclic units together with the bicyclic units do not generate a subgroup of finite index in $\mathcal{U}(\mathbf{Z}G)$. For this group G it is easily verified that the image of S_2 in $\mathbf{Z}D_8$ conincides with the group generated by the bicyclic units. Hence it follows that S_2 is not of finite index in $\mathcal{U}(\mathbf{Z}G)$. This example shows that without the assumptions in part two of the theorem the conclusion does not hold.

REFERENCES

1. H. Bass, *The Dirichlet Unit Theorem, Induced Characters and Whitehead Groups of Finite Groups*, Topology **4**(1966), 391–410.

2. D. B. Coleman, *Finite Groups with Isomorphic Group Algebras*, Trans. Amer. Math. Soc. **105**(1962), 1–8.

3. C. W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, Wiley, New York, 1962.

4. E. Jespers and G. Leal, *Describing Units in Integral Group Rings of some p-Groups*, Comm. Algebra (6) **19**(1991), 1809–1827.

5. E. Jespers, G. Leal and C. Polcino Milies, *Idempotents in Rational Abelian Group Algebras*, preprint.

6. E. Jespers and M. M. Parmenter, *Bicyclic Units in* $\mathbf{Z}S_3$, Bull. Belgian Math. Soc. (2) **44**(1992), 141–145.

7. ———, *Units of Group Rings of Groups of Order* 16, Glasgow Math. J., to appear.

8. E. Kleinert, *Einheiten in* $\mathbf{Z}D_{2m}$, J. Number Theory **13**(1981), 541–561.

9. G. Leal and C. Polcino Milies, *Isomorphic Group (and Loop) Algebras*, J. Algebra **155**(1993), 195–210.

10. S. Perlis, G. L. Walker, *Abelian Group Algebras of Finite Order*, Trans. Amer. Math. Soc. **68**(1950), 420–426.

11. J. Ritter, *Large Subgroups in the Unit Group of Group Rings (a Survey)*, Bayreuth. Math. Schr. **33**(1990), 153–171.

12. J. Ritter and S. K. Sehgal, *Construction of Units in Integral Group Rings of Finite Nilpotent Groups*, Trans. Amer. Math. Soc. (2) **324**(1991), 603–621.

13. ———, *Generators of Subgroups of* $U(\mathbf{Z}G)$, Contemporary Math. **93**(1989), 331–347.

14. ———, *Construction of units in group rings of monomial and symmetric groups*, J. Algebra, to appear.

15. S. K. Sehgal, *Units of Integral Group Rings; a Survey*, to appear.

16. ———, *Topics in Group Rings*, Marcel Dekker, New York, 1978.

17. L. N. Vaserstein, *The Structure of Classic Arithmetic Groups of Rank greater than One*, Math. USSR-Sb. **20**(1973), 465–492.

Department of Mathematics and Statistics
Memorial University of Newfoundland
St. John's, Newfoundland
A1C 5S7

Instituto de Matemática
Universidade Federal do Rio de Janeiro
Caixa Postal 68530
21910 Rio de Janeiro
Brasil

Instituto de Matemática e Estatística
Universidade de São Paulo
Caixa Postal 20570—Ag. Iguatemi
01498–São Paulo
Brasil