Can. J. Math. Vol. **45** (2), 1993 pp. 369–379

BIRELATIVE K_2 OF GROUPS OF SQUARE-FREE ORDER

BRUCE A. MAGURN

ABSTRACT Birelative K_2-groups are computed for the fiber squares needed to study K_2 and K_3 of $\mathbb{Z}G$ when G is a group of square-free order

0. **Introduction.** Suppose R is a ring with ideals I and J, with $I \cap J = 0$. The birelative K_2-group $K_2(R; I, J)$ is an abelian group B_2 which fits in a K-theory exact sequence (see [3]):

$$K_3(R, I) \longrightarrow K_3\big(R/J, (I+J)/J\big) \longrightarrow B_2 \longrightarrow K_2(R, I) \longrightarrow K_2\big(R/J, (I+J)/J\big) \longrightarrow 0.$$

Here $I \cong (I+J)/J$; so B_2 measures the failure of excision for K_2 of an ideal.

Since $I \cap J = 0$, R embeds as a subring of $(R/I) \times (R/J)$. The relation between $K_n(R)$ and K_n of this bigger ring is displayed in a long exact Mayer-Vietoris sequence:

$$\cdots \longrightarrow K_{n+1}(R/I \times R/J) \longrightarrow K_{n+1}\big(R/(I+J)\big) \oplus B_n \longrightarrow K_n(R) \longrightarrow K_n(R/I \times R/J) \longrightarrow \cdots$$

under certain conditions on R, I and J (see [4], Theorem 2.1). Here B_n is the birelative $K_n(R; I, J)$.

This paper is a sequel to the paper [5], in which R. C. Laubenbacher and this author applied such Mayer-Vietoris sequences to obtain partial computations of $K_2(\mathbb{Z}G)$ and $K_3(\mathbb{Z}G)$ for dihedral groups G of square-free order. Here the birelative K_2 computations of [5] are extended to include those needed when G is any finite group of square-free order. These are the groups with presentation:

$$(a, b : a^m = 1, b^s = 1, bab^{-1} = a^q),$$

where $|G| = ms$ is square-free (see [2], Section 9.4).

1. **Specification of the B_2s.** For a group G with the above presentation,

$$\mathbb{Q}G = \mathbb{Q}[a] \oplus \mathbb{Q}[a]b \oplus \cdots \oplus \mathbb{Q}[a]b^{s-1},$$

with multiplication determined by

$$ba = a^q b, \quad b^s = 1.$$

If d is a positive divisor of m, and ζ_d is a primitive d-th root of unity, replacing a by ζ_d defines a surjective ring homomorphism

$$\psi_d \colon \mathbb{Q}G \longrightarrow \Sigma(d),$$

Received by the editors May 4, 1992
AMS subject classification 19C40, 19D99

where $\Sigma(d)$ is a $\mathbb{Q}$-algebra with the same description as $\mathbb{Q}G$ (above), but with ζ_d in place of a. As in [6], Section 7, there is a $\mathbb{Q}$-algebra isomorphism:

$$\mathbb{Q}G \cong \bigoplus_{d|m} \Sigma(d),$$

which is ψ_d in each d-component.

If $\mathcal{D}$ is a set of positive divisors of m, let $O(\mathcal{D})$ denote the image of the projection:

$$\mathbb{Z}G \longrightarrow \bigoplus_{d\in\mathcal{D}} \Sigma(d)$$

to $\mathcal{D}$-components. Then $O(\mathcal{D})$ is the twisted group ring

$$\mathbb{Z}[\alpha_{\mathcal{D}}] \circ \langle b \rangle = \mathbb{Z}[\alpha_{\mathcal{D}}] \oplus \mathbb{Z}[\alpha_{\mathcal{D}}]b \oplus \cdots \oplus \mathbb{Z}[\alpha_{\mathcal{D}}]b^{s-1}$$

where the minimal polynomial of $\alpha_{\mathcal{D}}$ over $\mathbb{Q}$ is

$$\prod_{d\in\mathcal{D}} \Phi_d(x)$$

($\Phi_d(x)$ being the minimal polynomial of ζ_d over $\mathbb{Q}$), and where

$$b\alpha_{\mathcal{D}} = \alpha_{\mathcal{D}}^q b \text{ and } b^s = 1.$$

The Mayer-Vietoris sequences needed to study $K_n(\mathbb{Z}G)$ are based on the fiber squares:

(1.1)
$$\begin{array}{ccc} O(\mathcal{D}\cup p\mathcal{D}) & \xrightarrow{\pi_{p\mathcal{D}}} & O(p\mathcal{D}) \\ {\scriptstyle \pi_{\mathcal{D}}}\downarrow & & \downarrow \\ O(\mathcal{D}) & \underset{\text{mod} p}{\longrightarrow} & O(\mathcal{D})/pO(\mathcal{D}) \end{array}$$

in which p is a prime factor of m, $\mathcal{D}$ is a non-empty set of positive factors of m/p, $\pi_{\mathcal{D}}$ and $\pi_{p\mathcal{D}}$ are projections, and the right vertical map can be defined by commutativity of the square. In this paper the birelative groups $B_2(\mathcal{D}, p\mathcal{D}) := K_2(R; I, J)$ are computed, where $R = O(\mathcal{D} \cup p\mathcal{D})$, $I = \ker \pi_{\mathcal{D}}$ and $J = \ker \pi_{p\mathcal{D}}$.

2. **Reduction to single divisors.** In [1] and [3] the birelative $K_2(R; I, J)$ was determined to be

$$I/I^2 \otimes_{R^e} J/J^2$$

where R^e is additively the same as $R \otimes_{\mathbb{Z}} R$, and its multiplication is extended $\mathbb{Z}$-bilinearly from

$$(x_1 \otimes y_1)(x_2 \otimes y_2) = (x_1x_2 \otimes y_2y_1)$$

for all $x_i, y_i \in R$. The R^e-module actions on J and I are

$$(x \otimes y) \cdot m = xmy, \quad m \cdot (x \otimes y) = ymx,$$

respectively. In [5] it is proved that:

THEOREM 2.1. *In the notation used in the square (1.1), the projections $O(\mathcal{D}\cup p\mathcal{D}) \longrightarrow O(d,pd)$ applied to I and J induce an isomorphism:*

$$B_2(\mathcal{D},p\mathcal{D}) \cong \bigoplus_{d\in\mathcal{D}} B_2(d,pd). \qquad \blacksquare$$

3. **Generators and relations for $B_2(d,pd)$.** It only remains to compute

$$B_2(d,pd) = I/I^2 \otimes_{R^e} J/J^2,$$

where I and J are the kernels indicated in the diagram with short exact rows and columns:

$$\begin{array}{ccccc} & & I & & I' \\ & & \downarrow & & \downarrow \\ J & \longrightarrow & \mathbb{Z}[\alpha]\circ\langle b\rangle & \longrightarrow & \mathbb{Z}[\zeta_{pd}]\circ\langle b\rangle \\ & & \downarrow & & \downarrow \\ J' & \longrightarrow & \mathbb{Z}[\zeta_d]\circ\langle b\rangle & \longrightarrow & \mathbb{F}_p[\zeta_d]\circ\langle b\rangle, \end{array}$$

where $d\in\mathcal{D}$, the minimal polynomial of α over $\mathbb{Q}$ is $\Phi_d(x)\Phi_{pd}(x)$, and $R = \mathbb{Z}[\alpha]\circ\langle b\rangle$.

The following facts were established in [5]: In $\mathbb{Z}[\alpha]\circ\langle b\rangle$, I (resp. J) is both a principal left and principal right ideal generated by $\Phi_d(\alpha)$ (resp. $\Phi_{pd}(\alpha)$). Then both $\Phi_d(\alpha)$ and p annihilate both I/I^2 and J/J^2; so the multiplication actions of $\mathbb{Z}[\alpha]\circ\langle b\rangle$ on these quotients factor through $\mathbb{F}_p[\zeta_d]\circ\langle b\rangle$. Further, with the notation

$$(x,y) := \big(x\cdot\overline{\Phi_d(\alpha)}\otimes y\cdot\overline{\Phi_{pd}(\alpha)}\big),$$

for $x,y\in\mathbb{F}_p[\zeta_d]\circ\langle b\rangle$, the $\mathbb{F}_p$-vector space $I/I^2\otimes_{\mathbb{Z}} J/J^2$ has $\mathbb{F}_p$-basis:

$$\{(\zeta^i b^k, \zeta^j b^\ell) : 0\le i,j<\varphi(d), 0\le k,\ell<s\}$$

where $\zeta = \zeta_d$. The left and right actions of $\mathbb{F}_p[\zeta]\circ\langle b\rangle$ on I/I^2 and J/J^2 may differ due to noncommutativity of G:

$$ba = a^q b \text{ and } ab = ba^r$$

for positive integers q and r with $qr\equiv 1 \pmod m$. In detail, the quotients

$$\sigma(x) = \frac{\Phi_d(x^r)}{\Phi_d(x)} \text{ and } \tau(x) = \frac{\Phi_{pd}(x^r)}{\Phi_{pd}(x)}$$

are in $\mathbb{Z}[x]$, and the action of b satisfies:

$$\Phi_d(\alpha)\cdot b = b\cdot\Phi_d(\alpha^r) = b\sigma(\zeta)\cdot\Phi_d(\alpha),$$
$$\Phi_{pd}(\alpha)\cdot b = b\cdot\Phi_{pd}(\alpha^r) = b\tau(\zeta)\cdot\Phi_{pd}(\alpha).$$

Therefore, to pass from $I/I^2\otimes_{\mathbb{Z}} J/J^2$ to $I/I^2\otimes_{R^e} J/J^2$, mod out the additional relators:

1. $(\zeta x,y) - (x,y\zeta)$
2. $(x\zeta,y) - (x,\zeta y)$
3. $(bx,y) - \big(x, yb\tau(\zeta)\big)$
4. $\big(xb\sigma(\zeta),y\big) - (x,by)$.

With these it is easy to see that the $\mathbb{F}_p$-vector space $B_2(d,pd)$ is spanned by the elements: $(1,\zeta^j b^\ell)$ with $0 \le j < \varphi(d)$, and $0 \le \ell < s$.

4. **A modulo p cyclotomic unit.** In order to compute $B_2(d,pd)$ from its presentation, it is helpful to produce a certain unit in $\mathbb{F}_p[\zeta_d]$ related to the polynomials $\sigma(x)$ and $\tau(x)$ by a formula resembling Hilbert's Theorem 90. For this section, suppose d is any square-free integer with $d > 1$ and p is a prime not dividing d. Then $d = q_1 q_2 \cdots q_n$ for n distinct primes q_i. For each j with $0 \le j \le n$, let $D(j)$ denote the set of all products $x_1 \cdots x_j$ where $x_1, \ldots, x_j$ are distinct primes chosen from $\{q_1, \ldots, q_n\}$. Here $D(0) = \{1\}$. Define the polynomials:

$$v_j(x) = \prod_{e \in D(j)} (x^{pd/e} - 1)$$

in $\mathbb{Z}[x]$.

LEMMA 4.1. *In $\mathbb{Z}[x]$,*

$$\Phi_{pd}(x)\Phi_d(x) = \frac{\prod_{j \text{ even}} v_j(x)}{\prod_{j \text{ odd}} v_j(x)}.$$

PROOF. Suppose $f \in D(n-k)$ where $0 \le k \le n$; so d/f is a product of k primes. Then $\Phi_f(x)$ divides $x^{pd/e} - 1$ if and only if $\Phi_{pf}(x)$ divides $x^{pd/e} - 1$, and these are true if and only if e divides d/f. So the number of $e \in D(j)$ where these equivalent conditions hold is the binomial coefficient $\binom{k}{j}$. Thus there are $\binom{k}{j}$ occurrences of both $\Phi_f(x)$ and $\Phi_{pf}(x)$ in the factorization of $v_j(x)$ into irreducibles. Since

$$(1-1)^k = \sum_{j \text{ even}} \binom{k}{j} - \sum_{j \text{ odd}} \binom{k}{j}.$$

both $\Phi_f(x)$ and $\Phi_{pf}(x)$ cancel out completely for $k \ge 1$, leaving only the product $\Phi_{pd}(x)\Phi_d(x)$ for $k = 0$. ∎

Now $v_j(\zeta_d)$ is a product of factors

$$\zeta_d^{pd/e} - 1 = \zeta_e^p - 1,$$

where $e \in D(j)$. So if $j > 1$, then e (= the order of ζ_e^p) is composite, and hence $v_j(\zeta_d)$ is a unit in $\mathbb{Z}[\zeta_d]$. On the other hand, if $j = 1$, then $e = q_i$ for some i, and $\zeta_e^p - 1$ divides q_i in $\mathbb{Z}[\zeta_d]$; so, since p does not divide d, $v_1(\zeta_d)$ is a unit in $\mathbb{F}_p[\zeta_d]$. Define:

$$u = \Big[\prod_{\substack{j \text{ odd} \\ j \ge 1}} v_j(\zeta_d)\Big]^{-1} \Big[\prod_{\substack{j \text{ even} \\ j \ge 1}} v_j(\zeta_d)\Big]$$

in $\mathbb{F}_p[\zeta_d]^*$.

PROPOSITION 4.2. *Suppose q and r are positive integers with $qr \equiv 1 \pmod{pd}$, θ is the ring automorphism of $\mathbb{F}_p[\zeta_d]$ with $\theta(\zeta_d) = \zeta_d^r$, and*

$$\sigma(x) = \frac{\Phi_d(x^r)}{\Phi_d(x)}, \quad \tau(x) = \frac{\Phi_{pd}(x^r)}{\Phi_{pd}(x)}$$

are expressed as polynomials in $\mathbb{Z}[x]$. Then in $\mathbb{F}_p[\zeta_d]$,

$$\sigma(\zeta_d)\tau(\zeta_d) = r\theta(u)u^{-1}.$$

PROOF.

$$\prod_{j \text{ odd}} v_j(x^r) \prod_{\substack{j \text{ even} \\ j>0}} v_j(x)\sigma(x)\tau(x) = \frac{x^{rpd}-1}{x^{pd}-1} \prod_{j \text{ odd}} v_j(x) \prod_{\substack{j \text{ even} \\ j>0}} v_j(x^r),$$

and

$$\frac{x^{rpd}-1}{x^{pd}-1} = 1 + x^{pd} + \cdots + x^{(r-1)pd}.$$

Evaluate at ζ_d and reduce mod p to get the desired equation. ∎

5. **Computations.** Define m, s and q as in Section 1, d, p, r $\sigma(x), \tau(x)$ and the pairing (x, y) as in Section 3, and u and θ as in Section 4. So ms is square-free, p is a prime factor of m, d divides m/p, and in the group G, $bab^{-1} = a^q$ and $b^s = 1$; so $q^s \equiv 1 \pmod m$. Similarly $b^{-1}ab = a^r$; so $r^s \equiv 1 \pmod m$, and $qr \equiv 1 \pmod m$.

In $(\mathbb{Z}/d\mathbb{Z})^*$, q and r represent inverse elements of order t dividing s.

THEOREM 5.1. *The birelative K_2-group $B_2(d, pd)$ is an $\mathbb{F}_p$-vector space.*

a) If p does not divide $r^t - 1$, then $B_2(d, pd) = 0$.

b) If p divides $r^t - 1$, then $B_2(d, pd)$ has an $\mathbb{F}_p$-basis:

$$\{(1, u^{-1}\zeta^j b^\ell) : j \in J, \ell \in t\mathbb{Z}, 0 \leq \ell < s\}$$

where J is any set consisting of one integer from each coset of $\langle r \rangle$ in $(\mathbb{Z}/d\mathbb{Z})^*$. The rank of $B_2(d, pd)$ in this case is $\varphi(d)s/t^2$.

PROOF. If $f(x) \in \mathbb{Z}[x]$ and $n \geq 0$, define $f_n(x)$ by:

$$f_n(x) = \begin{cases} f(x)f(x^r)\cdots f(x^{r^{n-1}}), & \text{if } k \geq 1 \\ 1, & \text{if } k = 0 \end{cases}.$$

Then iterating relations 3 and 4 of Section 3, in $B_2(d, pd)$:

$$(b^n a^i b^k, a^j b^\ell) = \big(a^i b^k, a^j b^{\ell+n}\tau_n(\zeta)\big),$$
$$(a^i b^k, b^n a^j b^\ell) = \big(a^i b^{k+n}\sigma_n(\zeta), a^j b^\ell\big).$$

Note that since $r^t \equiv 1 \pmod{d}$, b^t commutes with $\zeta\ (= \zeta_d)$ in $\mathbb{Z}[\zeta] \circ \langle b \rangle$. Also note that from Proposition 4.2,

$$\sigma_t(\zeta)\tau_t(\zeta) = r^t.$$

So in $B_2(d, pd)$,

$$\begin{aligned}(1, \zeta^j b^\ell) &= (b^t b^{-t}, \zeta^j b^\ell) \\ &= \big(b^{-t}, \zeta^j b^{\ell+t}\tau_t(\zeta)\big) \\ &= \big(b^{-t} b^t \sigma_t(\zeta), \zeta^j b^\ell \tau_t(\zeta)\big) \\ &= \big(\tau_t(\zeta)\sigma_t(\zeta), \zeta^j b^\ell\big) \\ &= (r^t, \zeta^j b^\ell) \\ &= r^t(1, \zeta^j b^\ell).\end{aligned}$$

So $(1 - r^t)(1, \zeta^j b^\ell) = 0$ for all $j, \ell \in \mathbb{Z}$. Thus if p does not divide $r^t - 1$, then every generator $(1, \zeta^j b^\ell)$ of $B_2(d, pd)$ vanishes, proving part (a).

By relations 1 and 2 of Section 3, in $B_2(d, pd)$, for any integers j and ℓ,

$$\begin{aligned}(1, \zeta^j b^\ell) &= (\zeta, \zeta^{j-1} b^\ell) \\ &= (1, \zeta^{j+q^\ell-1} b^\ell).\end{aligned}$$

So one can add to j any element of

$$d\mathbb{Z} + (q^\ell - 1)\mathbb{Z}$$

with no effect. In particular, if v is the greatest common divisor of d and $q^\ell - 1$, then

$$\begin{aligned}(\zeta^v - 1, \zeta^j b^\ell) &= (1, \zeta^{j+v} b^\ell) - (1, \zeta^j b^\ell) \\ &= 0.\end{aligned}$$

If $\ell \notin t\mathbb{Z}$, then d does not divide $q^\ell - 1$, and $v < d$. If d/v is composite, $\zeta^v - 1$ is a unit in $\mathbb{Z}[\zeta]$. If d/v is prime, $\zeta^v - 1$ divides that prime in $\mathbb{Z}[\zeta]$ and so becomes a unit in $\mathbb{F}_p[\zeta]$. Either way there exist $x, y \in \mathbb{Z}[\zeta]$ with

$$(\zeta^v - 1)x = 1 + py.$$

So in $B_2(d, pd)$,

$$\begin{aligned}(1, \zeta^j b^\ell) &= \big((\zeta^v - 1)x - py, \zeta^j b^\ell\big) \\ &= (\zeta^v - 1, x\zeta^j b^\ell) \\ &= 0.\end{aligned}$$

Thus $B_2(d, pd)$ is spanned by the elements $(1, \zeta^j b^\ell)$ with $0 \le j < \varphi(d)$, $0 \le \ell < s$ and $\ell \in t\mathbb{Z}$. In detail,

$$(\zeta^i b^k, \zeta^j b^\ell) = \begin{cases} (1, \zeta^{j+iq^\ell}\tau_k(\zeta) b^{k+\ell}, & \text{if } k + \ell \in t\mathbb{Z} \\ 0, & \text{if } k + \ell \notin t\mathbb{Z}, \end{cases}$$

by the relations 1 and 3, and the fact that $b^{k+\ell}$ commutes with ζ if $k+\ell \in t\mathbb{Z}$.

Now if $\ell \in t\mathbb{Z}$ and $j \in \mathbb{Z}$, in $B_2(d,pd)$:

$$\begin{aligned}(1,\zeta^j b^\ell) &= (b^s,\zeta^j b^\ell)\\ &= \big(b^{s-1},\zeta^j b^{\ell+1}\tau(\zeta)\big)\\ &= \big(b^s\sigma(\zeta),\zeta^{jr}b^\ell\tau(\zeta)\big)\\ &= \big(1,\sigma(\zeta)\tau(\zeta)\zeta^{jr}b^\ell\big).\end{aligned}$$

If $C = \langle b^t\rangle$, which is the subgroup of $\langle b\rangle$ consisting of those elements commuting with ζ, the group ring $\mathbb{F}_p[\zeta]C$ is the center of $\mathbb{F}_p[\zeta]\circ\langle b\rangle$. Then there is an $\mathbb{F}_p$-linear surjective map

$$f\colon \mathbb{F}_p[\zeta]C \longrightarrow B_2(d,pd),$$

with $f(\zeta^j b^\ell) = (1,\zeta^j b^\ell)$, and the kernel of f contains the $\mathbb{F}_p$-linear span R_1 of the elements:

$$\big(\zeta^j - \sigma(\zeta)\tau(\zeta)\zeta^{jr}\big)b^\ell$$

with $j \in \mathbb{Z}$, $\ell \in t\mathbb{Z}$.

CLAIM. *The induced $\mathbb{F}_p$-linear map*

$$\bar f\colon \mathbb{F}_p[\zeta]C/R_1 \longrightarrow B_2(d,pd)$$

is an isomorphism.

To construct an inverse to $\bar f$, begin by considering the $\mathbb{F}_p$-subspace V of $I/I^2\otimes_{\mathbb{Z}} J/J^2$ spanned by the elements $(1,\zeta^j b^\ell)$ for $0 \le j < \varphi(d)$, $0 \le \ell < s$ and $\ell \in t\mathbb{Z}$. This V contains the elements $(1,\zeta^j b^\ell)$ for all $j \in \mathbb{Z}$ and $\ell \in t\mathbb{Z}$, but those elements restricted as above are $\mathbb{F}_p$-linearly independent. Define

$$F_1\colon I/I^2\otimes_{\mathbb{Z}} J/J^2 \longrightarrow V$$

to be the $\mathbb{F}_p$-linear map with

$$F_1\big((\zeta^i b^k,\zeta^j b^\ell)\big) = \begin{cases}(1,\zeta^{j+iq^\ell}\tau_k(\zeta)b^{k+\ell}, & \text{if } k+\ell \in t\mathbb{Z}\\ 0 & \text{if } k+\ell \notin t\mathbb{Z},\end{cases}$$

for $0 \le i,j < \varphi(d)$ and $0 \le k,\ \ell < s$.

This description of the effect of F_1 on $(\zeta^i b^k,\zeta^j b^\ell)$ holds even if we do not restrict the integers i, j, k and ℓ, except to require $k \ge 0$, so that $\tau_k(x)$ is defined. To see that i and j need not be restricted, note that the pairing (x,y) is bilinear and there is a ring automorphism of $\mathbb{Z}[\zeta]$ taking

$$\zeta \longmapsto \zeta^{q^\ell}.$$

To lift the restriction on k, note that the list

$$\tau(\zeta),\tau(\zeta^r),\tau(\zeta^{r^2}),\ldots$$

is periodic with a period of length s. So the product of any s consecutive terms is

$$\tau_s(\zeta) = \frac{\Phi_{pd}(\zeta^{r^s})}{\Phi_{pd}(\zeta)} = 1,$$

since $r^s \equiv 1 \pmod{d}$. So $\tau_v(\zeta) = \tau_w(\zeta)$ whenever $v \equiv w \pmod{s}$.

The map F_1 kills the relators of type 1, 2 and 3 from Section 3; but F_1 of the fourth type of relator is an $\mathbb{F}_p$-linear combination of elements:

$$(1, \zeta^j b^\ell) - \big(1, \sigma(\zeta)\tau(\zeta)\zeta^{jr} b^\ell\big)$$

where $j \in \mathbb{Z}$ and $\ell \in t\mathbb{Z}$. Define

$$F_2 \colon V \longrightarrow \mathbb{F}_p[\zeta]C$$

to be the $\mathbb{F}_p$-linear map with

$$F_2\big((1, \zeta^j b^\ell)\big) = \zeta^j b^\ell$$

for $0 \leq j < \varphi(d)$, $0 \leq \ell < s$ and $\ell \in t\mathbb{Z}$; then the same formula holds for all $j \in \mathbb{Z}$ and $\ell \in t\mathbb{Z}$. Then define

$$F_3 \colon \mathbb{F}_p[\zeta]C \longrightarrow \mathbb{F}_p[\zeta]C/R_1$$

to be the canonical map. The composite $F_3F_2F_1$ kills all the relators for $B_2(d, pd)$; so it induces an $\mathbb{F}_p$-linear map

$$g \colon B_2(d, pd) \longrightarrow \mathbb{F}_p[\zeta]C/R_1$$

taking $(1, \zeta^j b^\ell)$ to the coset of $\zeta^j b^\ell$ for all $j \in \mathbb{Z}$ and $\ell \in t\mathbb{Z}$. Thus the composite $g\bar{f}$ is the identity on $\mathbb{F}_p[\zeta]C/R_1$. Since $\bar{f}$ is surjective, $\bar{f}g$ is also the identity on $B_2(d, pd)$, proving the claim.

It only remains to compute $\mathbb{F}_p[\zeta]C/R_1$. Recall that R_1 is spanned by the elements:

$$[\zeta^j - \sigma(\zeta)\tau(\zeta)\theta(\zeta^j)]b^\ell$$

with $j \in \mathbb{Z}$ and $\ell \in t\mathbb{Z}$. Define R_2 to be the $\mathbb{F}_p$-linear span of the elements:

$$[\zeta^j - r\theta(\zeta^j)]b^\ell$$

for $j \in \mathbb{Z}$ and $\ell \in t\mathbb{Z}$. That is, if we extend θ to an automorphism of $\mathbb{F}_p[\zeta]C$ fixing the elements of C, R_2 is the image of of the linear operator $1 - r\theta$. The unit u of Section 4 was chosen so that, by Proposition 4.2,

$$\sigma(\zeta)\tau(\zeta) = r\theta(u)u^{-1}.$$

Hence $uR_1 \subseteq R_2$ and $u^{-1}R_2 \subseteq R_1$. So left multiplication by u defines an $\mathbb{F}_p$-linear isomorphism:

$$\mathbb{F}_p[\zeta]C/R_1 \cong \mathbb{F}_p[\zeta]C/R_2.$$

LEMMA 5.2. *If n is a square-free positive integer, the primitive n-th roots of unity form a $\mathbb{Z}$-basis of $\mathbb{Z}[\zeta_n]$.*

PROOF. The multiplicativity of the Euler function φ has the following generalization: If U_n denotes the multiplicative group of primitive n-th roots of unity in $\mathbb{C}$, then for relatively prime positive integers c and d, $U_{cd} = U_c U_d$.

For a prime p,

$$U_p = \zeta_p\{1, \zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-2}\}$$

is a $\mathbb{Z}$-basis of $\mathbb{Z}[\zeta_p]$. Now the fact that U_n spans $\mathbb{Z}[\zeta_n]$ over $\mathbb{Z}$ (for square-free n) follows by induction on n. ∎

Define J to be a full set of representatives of the cosets of $\langle r \rangle$ in $(\mathbb{Z}/d\mathbb{Z})^*$. Then J has $\varphi(d)/t$ elements. The proof of Theorem 5.1, part (b), is completed if it is shown that

$$\{\overline{\zeta^j b^\ell} : j \in J, \ell \in t\mathbb{Z}, 0 \leq \ell < s\}$$

is an $\mathbb{F}_p$-basis of $\mathbb{F}_p[\zeta]C/R_2$.

Modulo R_2,

$$\zeta^j b^\ell \equiv r\zeta^{rj} b^\ell \equiv rr\zeta^{rrj} b^\ell \equiv \cdots \equiv r^t \zeta^{r^{t-1}} b^\ell.$$

Since each power of r is nonzero mod p, each element

$$\overline{\zeta^{r^t j} b^\ell}$$

is a scalar multiple of $\overline{\zeta^j b^\ell}$ in $\mathbb{F}_p[\zeta]C/R_2$. So the proposed basis spans $\mathbb{F}_p[\zeta]C/R_2$.

To simplify notation, let K denote $(\mathbb{Z}/d\mathbb{Z})^*$, and let L denote the set of $\ell \in t\mathbb{Z}$ with $0 \leq \ell < s$. Suppose

$$\sum_{\substack{j \in J \\ \ell \in L}} c(j, \ell)\overline{\zeta^j b^\ell} = 0$$

for some coefficients $c(j, \ell) \in \mathbb{F}_p$. By Lemma 5.2,

$$\{\zeta^k b^\ell : k \in K, \ell \in L\}$$

is an $\mathbb{F}_p$-basis of $\mathbb{F}_p[\zeta]C$. So $1 - r\theta$ of this basis is a spanning set for R_2. Thus there are $d(k, \ell) \in \mathbb{F}_p$ with

$$\begin{aligned}\sum_{\substack{j \in J \\ \ell \in L}} c(j, \ell)\zeta^j b^\ell &= \sum_{\substack{k \in K \\ \ell \in L}} d(k, \ell)(1 - r\theta)\zeta^k b^\ell \\ &= \sum_{\substack{k \in K \\ \ell \in L}} \big(d(k, \ell) - rd(qk, \ell)\big)\zeta^k b^\ell.\end{aligned}$$

Comparing coefficients, if $k \notin J$,

$$d(k, \ell) = rd(qk, \ell),$$

so for each $j \in J$,

$$d(qj,\ell) = rd(q^2 j,\ell) = r^2 d(q^3 j,\ell) = \cdots = r^{t-1} d(j,\ell),$$

since $q^t \equiv 1 \pmod d$. And again comparing coefficients, for each $j \in J$,

$$\begin{aligned} c(j,\ell) &= d(j,\ell) - rd(qj,\ell) \\ &= d(j,\ell) - rr^{t-1} d(j,\ell) \\ &= 0, \end{aligned}$$

since in this part (b), we have assumed $r^t \equiv 1 \pmod p$. ∎

NOTE. When pd divides $r-1$, so that $t=1$, θ has no effect, and $\sigma(\zeta), \tau(\zeta) = 1$, then $R_1 = R_2 = 0$ and there is no need for u. In this case $B_2(d,pd) \cong \mathbb{F}_p[\zeta] \circ \langle b \rangle$, with $\mathbb{F}_p$-basis:

$$\{(1, \zeta^j b^\ell) : 0 \leq j < \varphi(d), 0 \leq \ell < s\}.$$

6. **Comments on computation of $K_n(\mathbb{Z}G)$.** For those groups G of square-free order with presentations

$$(a, b : a^m = 1, b^s = 1, bab^{-1} = a^q)$$

and those d dividing m where the order of q in $(\mathbb{Z}/d\mathbb{Z})^*$ is s, the K_3 of the rings $O(d)$ and $O(d)/p$ (where pd divides m) have been determined in [5]. In the special case of dihedral groups of square-free order ($s = 2$, $q = m-1$) those computations, and birelative K_2 computations led to estimates on $K_3(\mathbb{Z}G)$ and $SK_2(\mathbb{Z}G)$ (see [5], Section 9). Now that the birelative K_2 computations have been extended to all groups of square-free order, Mayer-Vietoris sequences should lead to information on $K_3(\mathbb{Z}G)$ and $SK_2(\mathbb{Z}G)$ for a wider class of square-free order groups G.

Unfortunately, when the center of $O(d)$ is totally imaginary, $K_3\big(O(d)\big)$ has just enough copies of $\mathbb{Z}$ to map onto the next terms

$$K_3\big(O(d)/p\big) \oplus B_2(d,pd)$$

in the Mayer-Vietoris sequence. So such information must await a closer analysis of the maps in the sequence. The determination of a basis for $B_2(d,pd)$ helps set the stage for this next step.

REFERENCES

1. D Guin-Waléry and J -L Loday, *Obstruction a l'excision en K-theorie algebrique* In Algebraic K-Theory, Lect Notes Math **854**, Springer-Verlag, 1981, 179–216
2. M Hall, *The Theory of Groups*, Macmillan, New York, 1959
3. F Keune, *Double relative K-theory and the relative K_3*, J Pure Appl Algebra **20**(1981), 39–53

4. R C Laubenbacher, *Generalized Mayer-Vietoris sequences in algebraic K-theory*, J Pure Appl Algebra **51**(1988), 175–192

5. R C Laubenbacher and B A Magurn, *SK_2 and K_3 of dihedral groups*, Canad J Math (3) **44**(1992), 591–623

6. B A Magurn, *SK_1 of dihedral groups*, J Algebra (2) **51**(1978), 399–415

Department of Mathematics and Statistics
Miami University
Oxford Ohio 45056
U S A