Canad. Math. Bull. Vol. **30** (2), 1987

UNITS IN INTEGRAL GROUP RINGS OF SOME METACYCLIC GROUPS

BY

P. J. ALLEN AND C. HOBBY

ABSTRACT. Let p be odd prime and suppose that $G = \langle a, b\rangle$ where $a^{p-1} = b^p = 1$, $a^{-1}ba = b^r$, and r is a generator of the multiplicative group of integers mod p. An explicit characterization of the group of normalized units V of the group ring ZG is given in terms of a subgroup of $GL(p - 1, Z)$. This characterization is used to exhibit a normal complement for G in V.

Let $U = U(ZG)$ be the group of units in the integral group ring ZG. A number of authors have characterized U for special groups (see [1], [2], [5], [6], [7], [8]). In particular, characterizations of U as a group of integer matrices were obtained by Hughes and Pearson [5] for $G = S_3$, by Polcino Milies [7] for $G = D_4$, and by the authors [1] for $G = A_4$. These presentations as integer matrices relied on a technique introduced by Hughes and Pearson which, while theoretically adaptable to larger groups, is very difficult to use since it depends on solving a system of n linear congruences where n is the order of the group G.

In this article, we use a variation on the Hughes and Pearson technique to represent $V = V(ZG) = \{\alpha \in U \mid \alpha \text{ has augmentation } 1\}$ as integer matrices for some metacyclic groups G of order $(p - 1)p$. The procedure is straight-forward, with necessary and sufficient constraints on the matrices emerging as consequences of the nature of certain representations of G rather than as solutions of huge systems of congruences. A complete characterization of V is obtained when $p = 3$, 5, or 7; for larger primes, our representation characterizes $V/\mathfrak{z}$ where $\mathfrak{z} \neq 1$ is the center of V. As an application of this representation, we show that for every $p > 2$, G has a normal complement in V.

Let p be an odd prime and let G be the group defined by

$$a^{p-1} = b^p = 1,\ a^{-1}ba = b^r$$

where r is a generator of the multiplicative group of integers mod p. Each non-identity coset of $\langle b\rangle$ is a conjugate class, and the other conjugate classes consist of $\{1\}$ and of $\{b^i \mid i \neq 0\}$. Thus the number of 1-dimensional representations of G is $p - 1$ and there is a single representation of degree $p - 1$. Any faithful representation is nonabelian and thus must be an absolutely irreducible representation of degree $p - 1$. We shall be

Received by the editors October 31, 1985.

AMS Subject Classification (1980): Primary 20D15; Secondary 16A26, 20C05.

concerned with the faithful representation σ of degree $p - 1$ obtained by letting $\sigma(b) = B$ be the matrix which has a subdiagonal of 1's, a last column consisting of -1's, and 0 elsewhere, while $\sigma(a) = A$ is constructed by performing the permutation $i \to ri \pmod p$ on the columns of the identity matrix.

Let τ be the homomorphism of ZG onto $Z\langle a\rangle$ obtained by setting $b = 1$, and let $S = \{s \mid \tau(s) = 1\}$. Then τ is the identity map on $V_a = V(Z\langle a\rangle)$, and V splits as V_aD where $D = V \cap S$. Clearly, $D \lhd V$ and $D \cap V_a = \langle 1\rangle$. We shall see that the representation σ, when extended to ZG, is an isomorphism if restricted to V_a or to D. Theorem 1 gives an explicit characterization of $\sigma(V_a)$ and $\sigma(D)$. Consequently, $\sigma(V)$ is known. If the center of V is trivial (as it must be when $p = 3$, 5, or 7), $\sigma(V)$ is isomorphic to V.

THEOREM 1. *Let H be the set of all $X \in GL(p - 1, Z)$ such that for each $k = 1, 2, \ldots, p - 2$*

(i) $\operatorname{tr} X \equiv -1(p)$ *and* $\operatorname{tr} XA^k \equiv 0(p)$
(ii) $w(B - I)^kX(B - I)^{p-1-k} \equiv 0(p)$ *where* $w = (0, 0 \ldots 0, -1, 1)$.

Then σ is an isomorphism from D to $\sigma(D) = H$. Moreover, σ is an isomorphism from V_a to $\sigma(V_a) = V_A$, where V_A consists of the doubly stochastic matrices X in $GL(p - 1, Z)$ which have the property that, for each i, all entries on the main diagonal of XA^i are equal. Finally, σ is a homomorphism of V onto V_AH which has $\mathfrak{z}$ as its kernel, where $H \lhd \sigma(V)$.

We begin by verifying that σ is a faithful representation of G.

LEMMA 1. *The subgroup $\langle A, B\rangle$ of $GL(p - 1, Z)$ is isomorphic to $G = \langle a, b\rangle$.*

PROOF. One can check that B^k has a column of -1's as its $(p - k)^{\text{th}}$ column, 1's in the $(k + 1, 1), \ldots (p - 1, p - 1 - k)$ and $(1, p - k + 1), \ldots, (k - 1, p - 1)$ entries, and has 0 elsewhere. Note for future reference that the k^{th} row of B^k has -1 as its only nonzero entry, while each other row contains exactly one 1 and one -1. It is clear that $B^p = I$. Also, since the matrix A arises from a permutation of order $p - 1$, $A^{p-1} = I$. Conjugation by A sends the (i, j) entry of B to the (ri, rj) entry (where ri, rj are computed mod p), thus $A^{-1}BA$ has 1's in the $(2r, r)$, $(3r, 2r), \ldots, ((p - 1)r, (p - 2)r)$ entries; these are precisely the entries where B^r has 1's since, mod p, $\{(ir, (i - 1)r) \mid i \neq 1\} = \{(j, j - r) \mid j \neq r\}$. Multiplying B on the right by A sends the $(p - 1)^{\text{th}}$ column to the $(p - r)^{\text{th}}$ column, so $A^{-1}BA$ has -1's in the same locations as B^r. Consequently, $A^{-1}BA = B^r$.

LEMMA 2. $\sigma(V_a) = V_A$ *and σ is an isomorphism on V_a.*

PROOF. Elements of V_a are of the form $\alpha = \Sigma c_ja^j$ where $\Sigma c_j = 1$. It is easy to check that each c_i appears once in each row and column of $\sigma(\alpha)$, thus $\sigma(\alpha)$ is doubly stochastic. The main diagonal of $\sigma(\alpha)$ comes from c_0I, so each entry is c_0. The main diagonal of $\sigma(\alpha)A^{-i}$ comes from the entries c_i in $c_i\sigma(A^i)$, so each entry is c_i. Clearly, $\sigma(\alpha) = I$ implies $c_0 = 1$, $c_j = 0$ for $j > 0$. Thus σ is an isomorphism.

LEMMA 3. *Each element of $\sigma(S)$ satisfies conditions (i) and (iii).*

PROOF. If $s = \Sigma c_{ij}a^ib^j \in S$, then $\tau(s) = 1$ so if $\bar{c}_k = \Sigma_j c_{kj}$, then $\bar{c}_0 = 1$ and $c_k = 0$ for $k > 0$. Each non-trivial coset $a^i\langle b\rangle$ of $\langle b\rangle$ is a set of conjugates, so for each $i > 0$, $\sigma(a^ib^j)$ has the same trace as $\sigma(a^i)$, namely 0. Each non-trivial power of B has trace -1, thus the trace of $\sigma(s)$ is $pc_{00} - \bar{c}_0$. Similarly, the trace of $\sigma(s)A^{-k}$ is $pc_{k0} - \bar{c}_k$. Thus condition (i) holds.

Condition (ii) is almost equally obvious. If we think of B as a matrix over the integers mod p, the eigenvalues of B must be p^{th} roots of 1 and thus must be 1. The rank of $B - I$ is clearly at least $p - 2$, so its must be exactly $p - 2$. It follows that the Jordan form of $B(\text{mod } p)$ consists of a single block, so $(B - I)^{p-1} \equiv 0(\text{mod } p)$ while $(B - I)^{p-2} \not\equiv 0(\text{mod } p)$. Now $(B - I)A = A(B^r - I)$, where $B^r - I$ is a multiple of $B - I$. Consequently, if

$$X = \sigma(s) = \sum c_{ij}A^iB^j.$$

Then $(B - I)^kX(B - I)^{p-1-k}$ can be rearranged to have a factor of $(B - I)^{p-1}$ on the right and therefore is 0 mod p. Thus condition (ii) holds for all matrices in $\sigma(S)$.

It follows from Lemmas 2 and 3 that the conditions given in the theorem are necessary. Moreover, the calculation of traces in the proof of Lemma 3 plays an important role in showing that the conditions are sufficient. We found that if $X = \Sigma c_{ij}A^iB^j \in \sigma(S)$, then

$$\operatorname{tr}\left(\left[\sum c_{ij}A^iB^j\right]A^{-i}\right) = pc_{i0} - \bar{c}_i$$

where $\bar{c}_0$ is 1 and $\bar{c}_i = 0$ if $i > 0$. Thus the coefficients c_{i0} of X can be written as

$$c_{i0} = \frac{\operatorname{tr}(XA^{-i}) + \bar{c}_i}{p}.$$

Similar relations can be obtained for c_{ij} by considering the trace of $XB^{-j}A^{-i}$. It follows that if $X = \sigma(s)$ where $s = \Sigma c_{ij}a^ib^j$, then

$$(1) \quad c_{ij} = \frac{\operatorname{tr} X(B^{-j}A^{-i}) + \bar{c}_i}{p}, \quad \text{where} \quad \bar{c}_0 = 1 \quad \text{and } \bar{c}_i = 0 \quad \text{for} \quad i > 0.$$

Let K denote the set of $(p - 1) \times (p - 1)$ matrices over Z which satisfy conditions (i) and (ii). Then $\sigma(S) \subseteq K$.

LEMMA 4. *If $X \in K$. then the c_{ij} determined by (1) are coefficients of an element $\Sigma c_{ij}a^ib^j \in S$.*

PROOF. We first show that the numbers c_{ij} given by (1) are integers. It is clear that condition (i) ensures that the numbers c_{ij} given by (1) are integers when $j = 0$. The only way (1) can fail to produce an integer is for there to be a j such that

$$\operatorname{tr}(XB^{-j}A^{-i}) \not\equiv \operatorname{tr}(XA^{-i})(\text{mod } p).$$

https://doi.org/10.4153/CMB-1987-033-5 Published online by Cambridge University Press

We shall use condition (ii) to show that this cannot happen. Note first that $XA^{-i}B^n$ satisfies condition (ii) whenever X does since

$$XA^{-i}B^n(B - I)^{p-1-k}$$

can be written in the form

$$X(B - I)^{p-1-k}A^{-i}f(B)$$

where $f(B)$ is a polynomial in B. Next, rewrite

$$XB^{-j}A^{-i} \quad \text{as} \quad XA^{-i}B^t$$

for some t. Since each of X, XA^{-i}, $XA^{-i}B^n$ satisfy condition (ii), it will suffice to show that if Y satisfies condition (ii), then

$$\operatorname{tr}(Y) \equiv \operatorname{tr}(YB)(\operatorname{mod} p).$$

In what follows, all calculations are made mod p. Since 1 is an eigenvalue of B of multiplicity $p - 1$, there is a matrix M such that $M^{-1}BM = J$ where J is the Jordan form with a superdiagonal of 1's.

It is easy to find both M and M^{-1}. As noted in the proof of Lemma 1, if $k < p$ then the k^{th} row of B^k contains -1 and zeroes while every other row contains -1, 1, and zeroes. Consequently, if u is the vector of all 1's, then the last two entries in B^iu are zero for $i < p - 2$ while $B^{p-2}u$ ends with -1 and 0. Therefore $(B - I)^{p-2}u$ ends with -2 and -1, so u is a generalized eigenvector (mod p) of degree $p - 1$. We may take M to be the matrix whose j^{th} column is $(B - I)^{p-1-j}u$. From what has been said, $w = (0, 0, \ldots, 0, -1, 1)$ is clearly the first row of M^{-1}. Also, since $(B - I)^{p-1} \equiv 0$, successive rows of M^{-1} are $w(B - I)^i$ for $i = 1, 2, \ldots, p - 2$.

Clearly,

$$\operatorname{tr}(YB) = \operatorname{tr}(M^{-1}YM)J$$

where $\operatorname{tr}(M^{-1}YM)J$ differs from $\operatorname{tr}(M^{-1}YM) = \operatorname{tr} Y$ only by the sum of the entries in the (2, 1), (3, 2), $\ldots$, $(p - 1, p - 2)$ locations of $M^{-1}YM$. These entries are all of the form

$$w(B - I)^kY(B - I)^{p-1-k}u$$

and hence are 0 mod p because of condition (ii).

So far, we have shown that any element of K, that is any $(p - 1) \times (p - 1)$ matrix which satisfies conditions (i) and (ii), is associated by (1) with an element of ZG. One consequence of (1) is that the c_{ij} defined by it satisfy $\Sigma_j c_{ij} = \bar{c}_i$ since $I + B + \cdots + B^{p-1} = 0$, therefore the choice of the $\bar{c}_i$ ensures that the $\Sigma c_{ij}a^ib^j$ is in the set S. Note that S must be closed under multiplication and that S contains D.

LEMMA 5. $\sigma(S) = K$.

PROOF. We must show that if X satisfies (i) and (ii), and if $\alpha = \Sigma c_{ij}a^ib^j$ has coefficients given by (1), then $\sigma(\alpha) = X$. We can write α in the form

$$\alpha = \frac{1}{p} \sum_{g \in G} tr(X\sigma(g^{-1}))g + \frac{1}{p}(1 + b + \cdots + b^{p-1})$$

where the second term, which comes from $\bar{c}_0 = 1$, can be disregarded since the sum of powers of B is 0. If σ_{rs} denotes the r, s entry, then

$$\begin{aligned}\sigma_{rs}(\alpha) &= \frac{1}{p} \sum_{g} \operatorname{tr}(X\sigma(g^{-1}))\sigma_{rs}(g) \\ &= \frac{1}{p} \operatorname{tr}\left\{X\left(\sum_{g} \sigma(g^{-1})\sigma_{rs}(g)\right)\right\}.\end{aligned}$$

Since σ is absolutely irreducible, it follows from the Schur relations (see Hall [4], Theorem 16.6.4) that the u, v entry of the inner sum is

$$\sum_{g} \sigma_{uv}(g^{-1})\sigma_{rs}(g) = \begin{cases} |G|/(p-1), & \text{if} \quad u = s \quad \text{and} \quad v = r \\ 0, & \text{otherwise.} \end{cases}$$

Therefore the inner sum is pE_{sr}, where E_{sr} is the matrix with 1 in the s, r entry and 0 elsewhere. Consequently, $\sigma_{rs}(\alpha) = x_{rs}$ and $\sigma(S) = K$.

LEMMA 6. *σ is a one-to-one map of S onto K.*

PROOF. If $\sigma(\alpha) = I$ for some $\alpha \in S$, then the trace of $\sigma(\alpha)$ is $p - 1$, and the traces of $\sigma(\alpha)A^{-i}$ are 0 for $i > 0$. Thus

$$pc_{00} - \bar{c}_0 = p - 1$$

and

$$pc_{i0} - \bar{c}_i = 0 \quad \text{for} \quad i > 0$$

where $\bar{c}_0 = 1$ and $\bar{c}_i = 0$ for $i > 0$. Thus c_{00} must be 1 and $c_{i0} = 0$ for $i > 0$. Next, note that $\sigma(\alpha b) = B$ has trace -1 while $\sigma(\alpha b)A^{-i}$ has trace 0 for $i > 0$. Thus

$$pc_{0,p-1} - \bar{c}_0 = -1$$

and

$$pc_{i,p-1} - \bar{c}_i = 0 \quad \text{for } i > 0$$

so $c_{i,p-1} = 0$ for all i. Repeating this argument with higher powers of b shows that $\alpha = 1$.

LEMMA 7. *σ is a one-to-one map of $D = V \cap S$ onto $H = K \cap GL(p - 1, Z)$.*

PROOF. Since S is closed, it follows from Lemma 6 that K, and thus also H, is closed. The congruence subgroup H_1, consisting of invertible matrices which are I mod p, is contained in H and is of finite index in $GL(p - 1, Z)$. Thus it follows from the closure of H that H is a group. We know that σ is homomorphism on D and it is clear the $\sigma(D) \subseteq H$. If $h \in H$, then $h^{-1} \in H$ and Lemma 6 implies that h and h^{-1} have preimages in S; the product of these preimages is mapped to I by σ, so $h = \sigma(d)$ for some $d \in D$.

LEMMA 8. *If $v \in V$, then $\sigma(v) = I$ iff v is in the center of V.*

PROOF. Any central element of V can be written as $v = 1 + v_1(1 + b + \cdots + b^{p-1})$ so $\sigma(v) = I$ since $\Sigma B^i = 0$. On the other hand, if v is not central then there is an x such that the commutator $(v, x) \neq 1$. We know that V/D is abelian, so $(v, x) \in D$. But σ is an isomorphism on D, therefore $\sigma(v, x) \neq I$. In particular, $\sigma(v)$ cannot be I.

PROOF OF THEOREM 1. Observe that H is normal since D is normal in V, and the remaining assertions are consequences of Lemmas 2, 7, 8.

REMARKS. We shall show in Lemma 9 that $\mathfrak{z}$ is isomorphic to a group of non-trivial units of $V(Z\langle A\rangle)$. There are no non-trivial units in $Z\langle A\rangle$ when $p = 3$, 5, or 7, consequently σ is an isomorphism on $V(ZG)$ and V_A is just $\langle A\rangle$.

When $p = 3$, condition (ii) says merely that the column sums of X must be 1 mod 3; given condition (ii), condition (i) holds automatically for any X which is non-singular mod 3. Thus the characterization of $V(ZS_3)$ obtained here is the same as the one given by Hughes and Pearson. The characterizations obtained for $p = 5$ and $p = 7$ seem to be new.

LEMMA 9. *The center $\mathfrak{z}$ of $V(ZG)$ is isomorphic to the subgroup of V_a consisting of*

$$R = \{\alpha \in V(Z\langle a\rangle) \,|\, \alpha \equiv 1 \bmod p\},$$

In particular, $\mathfrak{z}$ is a torsion free abelian group of rank

$$r = \frac{p+1}{2} - \ell$$

where ℓ is the number of divisors of $p - 1$.

PROOF. Central units in V are of the form $1 + u\lambda$ where $\lambda = \Sigma b^i$ and $u \in Z\langle a\rangle$; their images under τ are units of the form $1 + pu$. Thus $\tau(\mathfrak{z}) \subseteq R$. Note that τ is one-to-one on $\mathfrak{z}$ since $\tau(1 + u\lambda) = 1$ implies $pu = 0$ so $u = 0$. On the other hand, if $1 + pu \in R$ then $(1 + pu)^{-1}$ is some $1 + pv$ such that $p(u + v + puv) = 0$, so

$$u + v + puv = 0.$$

But then

$$\begin{aligned}(1 + u\lambda)(1 + v\lambda) &= 1 + (u + v + puv)\lambda \\ &= 1\end{aligned}$$

so $1 + u\lambda \in \mathfrak{z}$ and we see that $\tau(\mathfrak{z}) = R$.

Next, if $\alpha \in V_a$, then

$$\alpha^p \equiv \alpha \bmod p$$

since $a^p = a$, therefore $\alpha^{p-1} \in R$. By a theorem of Higman (see [9], Theorem 3.1) the group V_a is the direct product of $\langle a\rangle$ and a free abelian group F of rank $(p + 1)/2$

$- \ell$. The only torsion elements in V_a lie in $\langle a \rangle$, and $\langle a \rangle$ has trivial intersection with R, thus R is torsion free. Since R has finite index in V_a, R must have the same rank as F.

In view of Lemma 9, the characterization of V given by Theorem 1 is fairly complete even when $p > 7$ since both $\mathfrak{z}$ and $V/\mathfrak{z}$ are known.

As an application of Theorem 1, we show that G has a normal complement in V. A theorem of Cliff, Sehgal, and Weiss [3] guarantees that G has a torsion free normal complement if $p = 3$, 5, or 7. For these primes, the complement N which appears natural in $\sigma(V)$ turns out to be the same as the one produced from the ideal I_0 in [3]. However, their description of N requires one to decide whether an element of $1 + I_0$ is a unit, while the corresponding question in our description is whether a matrix belongs to $GL(p - 1, Z)$. The matrix question may be easier to answer in a specific case.

THEOREM 2. *Let $u = (1, 1, \ldots, 1)$, $v = (1, 2, \ldots, p - 1)$, and let N be the subset of $H = \sigma(D)$ consisting of matrices X which satisfy*

$$uXv' \equiv p(p-1)/2 \bmod p^2.$$

Let C be the subset of V_A consisting of matrices $\Sigma\, c_i A^i$ such that $\Sigma\, c_i r^i \equiv 1(p)$, where r is the number for which $a^{-1}ba = b^r$. Then C is a subgroup and N a normal subgroup of $\sigma(V)$, and CN is a normal complement of $\sigma(G)$ in $\sigma(V)$.

Note that in the special cases where $p = 3$, 5, or 7, we have $\sigma(V)$ isomorphic to V, $V_A = \langle A \rangle$, and C turns out to be trivial, consequently N can be thought of as a normal complement of G.

The conditions used to define N arise in a natural way. The vector u is an eigenvector of A for the eigenvalue 1 and, mod p, is also an eigenvector for B for the eigenvalue 1; this property is what underlies the conditions on column sums found in [5] and in the second representation of ZA_4 given in [1]. The vector v' is, mod p, an eigenvector of B for the eigenvalue 1, and is at least an eigenvector for A. Clearly, u and v' are still eigenvectors (mod p) for each X in $\sigma(V)$. The requirement

$$uXv' \equiv p(p-1)/2 \bmod p^2$$

is satisfied by I but by no other power of B; imposing the additional condition that $N \subseteq \sigma(D)$ excludes the remaining elements of $\sigma(G)$ from N.

LEMMA 10. *N is a normal subgroup of $\sigma(V)$, $H = \langle B \rangle N$, and $N \cap \sigma(G) = \{I\}$.*

PROOF. As noted above, it is easy to check that

$$uA = u$$

$$uB \equiv u$$

$$Bv' \equiv v'$$

$$Av' \equiv rv',$$

where $a^{-1}ba = b^r$ and all congruences are mod p. Thus if $X = \Sigma\, c_{ij} A^i B^j$, then there are integer vectors u_x and v_x such that

$$uX = u + pu_x$$

$$Xv' = \lambda v' + pv_x$$

where $\lambda = \Sigma_i \Sigma_j c_{ij} r^i$. When $X \in H = \sigma(D)$, λ is 1 since $\Sigma\, c_{0j} = 1$ and $\Sigma_j c_{ij}$ is 0 for $i > 0$. Therefore, if $X \in H$

$$\begin{aligned} uXv' &= uv' + pu_X v' \\ &= uv' + puv_X. \end{aligned}$$

Thus each of the conditions $u_X v' \equiv 0(p)$ and $uv_X \equiv 0(p)$ is a necessary and sufficient condition for $X \in H$ to imply $X \in N$.

When X and Y belong to H,

$$\begin{aligned} uXYv' &= (u + pu_X)(v' + pv_Y) \\ &\equiv uv' + pu_X v' + puv_Y \bmod p^2 \end{aligned}$$

If X and Y are both in N, then the last two terms are 0 mod p^2, so it follows that N is closed. Also, if X is in N, we let $Y = X^{-1}$ and see that uv_Y is 0 mod p, thus X^{-1} is in N. (H is a group, so there is no need to check that products and inverses of elements in N are also in H.)

Observe that $Bv' = v' - pu'$, thus

$$uXBv' = uXv' - p(p - 1).$$

It follows that if $X \in H$, then XB^j is in N for some j, so the powers of B are a complete set of coset representatives of N in H. Next, note that $uB^{-1} = u - (p, 0, 0, \ldots, 0)$, so

$$uB^{-1}XBv' = (uX - (p, 0, \ldots)X)(v' - pu')$$

A straightforward calculation using $uX = u + pu_X$ and $Xv' = v' + pv_X$ shows that B normalizes N. If $Y \in V_A$, then $uY^{-1} = u$ and $Yv' = \lambda v' + pv_Y$. Therefore, if $X \in N$.

$$\begin{aligned} uY^{-1}XYv' &= (u + pu_X)(\lambda v' + pv_Y) \\ &\equiv u(\lambda v' + pv_Y) \bmod p^2 \end{aligned}$$

since $u_X v' \equiv 0(p)$. Thus the right hand side is $uYv' = uv'$, so Y normalizes N. (N is contained in the normal subgroup H so its is clear that $Y^{-1}XY \in H$.)

Finally, $\sigma(G) \cap N = \{I\}$ since $\sigma(G) \cap H = \langle B \rangle$ and B is not in N.

LEMMA 11. *If C is the subset of V_A consisting of elements which centralize B* modulo *N, then C is a subgroup and CN is a normal complement to $\sigma(G)$ in $\sigma(V)$.*

PROOF. It is clear that C is a subgroup. Modulo N, $\langle B \rangle$ is a normal subgroup of order p, and conjugation by A is an automorphism of order $p - 1$. Thus $V_A = \langle A \rangle C$ where $\langle A \rangle \cap C = \{I\}$. The group C is central modulo N, so CN is normal. Moreover, $V =$

$\sigma(G)CN$ and $\sigma(G) \cap CN = \{I\}$.

PROOF OF THEOREM 2. The theorem will follow from Lemmas 10 and 11 as soon as we show that the C of Lemma 11 is the set of all $\alpha = \Sigma\, c_i A^i$ in V_A such that $\Sigma\, c_i r^i \equiv 1 \bmod p$. We use the fact that

$$B^{-1}A^iB = A^iB^{1-r^i}$$

to write the commutator $\alpha^{-1}B^{-1}\alpha B$ in the form

$$\gamma = 1 + \alpha^{-1} \sum c_i A^i(B^{1-r^i} - I).$$

This commutator is known to be in H so it will be in N iff $u\gamma v' \equiv uv' \bmod p^2$. Since $uB^k = u - (0, 0, \ldots, p, \ldots 0)$, where the p appears in the $(p-k)^{\text{th}}$ column, we see that $uB^kv' = uv' - p(p-k)$. Moreover, $uA = u$, so

$$u\gamma v' = uv' + \sum c_i\{uv' - p[p - (1 - r^i)] - uv'\}.$$

Thus γ is in N iff $\Sigma\, c_i(1 - r^i) \equiv 0(p)$. This completes the proof.

The following result in an immediate consequence of Theorems 1 and 2.

COROLLARY 1. *G has a normal complement in V consisting of all units α such that $\sigma(\alpha) \in CN$.*

There does not seem to be a tidy description of the normal complement in V when $p > 7$; the difficulty is that one must take into account the nontrivial units in V_a and in $\mathfrak{z}$. This difficulty vanishes when p is 3, 5, or 7 since $V_a = \langle a \rangle$ and $\mathfrak{z} = \{1\}$.

COROLLARY 2. *When p is 3, 5, or 7, G has a normal complement in V consisting of all $\alpha = \Sigma\, c_{ij}a^ib^j$ in V such that*

$$\sum_j \left(\sum_i c_{ij}\right) j \equiv 0(p)$$

and

$$\sum_j c_{ij} = \begin{cases} 1 & \text{when } \quad i = 0 \\ 0 & \text{otherwise.} \end{cases}$$

PROOF. For the primes in question, the normal complement in V consists of α such that $\sigma(\alpha) \in N$. The second condition holds iff $\sigma(\alpha) \in H$. The first condition is necessary and sufficient for $u\sigma(\alpha)v' \equiv uv' \bmod p^2$. To see this, we perform a calculation similar to the one in the proof of Theorem 2.

$$\begin{aligned} u\sigma(\alpha)v' &= \sum_j \left(\sum_i c_{ij}uB^jv'\right) \\ &= \sum_j \left(\sum_i c_{ij}(uv' - p[p - j])\right) \end{aligned}$$

https://doi.org/10.4153/CMB-1987-033-5 Published online by Cambridge University Press

$$\equiv uv' + \sum_j \left(\sum_i c_{ij}\right) jp \pmod{p^2}.$$

The reader can check that the conditions given in Corollary 2 are equivalent to the conditions which hold for units in the complement $1 + I_0$ found by Cliff, Sehgal, and Weiss [3]. They proved that their complements were torsion free when $p = 3$, 5, or 7. We have been unable to determine whether our normal complement is torsion free when $p > 7$.

References

1. P. J. Allen and C. Hobby, *A Characterization of Units in $Z[A_4]$*, J. Algebra **66**(1980), 534–543.
2. A. K. Bhandari and I. S. Luthar, *Torsion Units of Integral Group Rings of Metacyclic Groups*, J. Number Theory **17**(1983), 270–283.
3. G. H. Cliff, S. K. Sehgal and A. R. Weiss, *Units of Integral Group Rings ZS_3*, Canad. Math. Bull. **15**(1972), 529–534.
4. M. Hall, *The Theory of Groups*, Chelsea, New York, 1976.
5. I. Hughes and K. R. Pearson, *The Group of Units of the Integral Group Ring ZS_3*, Canad. Math. Bull. **15**(1972), 529–534.
6. E. Kleinert, *Einheiten in $Z[D_{2m}]$*, J. Number Theory **13**(1981), 541–561.
7. C. Polcino Milies, *The Units of the Integral Group Ring ZD_4*, Bol. Soc. Mat. Brasil **4**(1972), 85–92.
8. J. Ritter and S. K. Sehgal, *Integral Group Rings of Some p-Groups*, Can. J. Math. **34**(1982), 233–246.
9. S. K. Sehgal, *Topics in Group Rings*, Dekker, New York, 1978.

Department of Mathematics
University of Alabama
University, AL 35486