JOURNAL OF NUMBER THEORY 17, 270–283 (1983)

Torsion Units of Integral Group Rings of Metacyclic Groups

I. S. LUTHAR AND A. K. BHANDARI

Department of Mathematics, Panjab University, Chandigarh 160014, India

Communicated by H. Zassenhaus

Received February 6, 1982

Let $V\mathbb{Z}G$ (respectively, $V\mathbb{Q}G$) denote the group of units of augmentation 1 in the integral (respectively, rational) group ring of a finite group G. It has been conjectured [H. Zassenhaus, *in* "Studies in Mathematics," pp. 119–126, Instituto de Alta Cultura, Lisbon, 1974] that each element of finite order of $V\mathbb{Z}G$ is conjugate in $V\mathbb{Q}G$ to an element of G (see also R. K. Dennis ["The Structure of the Unit Group of Group Rings," Lecture Notes in Pure and Applied Mathematics Vol. 26, Sect. 8, Dekker, New York, 1977] and S. K. Sehgal ["Topics in Group Rings," Problem 23, Dekker, New York, 1978]). To the best of our knowledge, the only nonabelian case (other than the Hamiltonian 2-groups) where this conjecture has been verified is $G = S_3$ [I. Hughes and K. R. Pearson, *Canad. Math. Bull.* **15** (1972), 529–534]. In this paper this conjecture is verified for the metacyclic group $G = \langle \sigma, \tau: \sigma^p = 1 = \tau^q,\ \tau\sigma\tau^{-1} = \sigma^j \rangle$ (p, q primes, $p \equiv 1 \bmod q$, $j^q \equiv 1$, $j \not\equiv 1 \bmod p$) by expressing $V\mathbb{Z}G$ and $V\mathbb{Q}G$ as semidirect products of groups of $q \times q$ matrices. Although S. Galovitch, I. Reiner, and S. Ullom [*Mathematika* **19** (1972), 105–111] obtained a description of $V\mathbb{Z}G$, the discussion of torsion units was not attempted by them.

1. DESCRIPTIONS OF $V\mathbb{Z}G$ AND $V\mathbb{Q}G$

Let G be the metacyclic group of order pq given by

$$G = \langle \sigma, \tau: \sigma^p = \tau^q = 1, \tau\sigma\tau^{-1} = \sigma^j \rangle,$$

where p is an odd prime, $q \geqslant 2$ a divisor of $p - 1$, and where j belongs to the exponent q mod p. Let $V\mathbb{Z}G$ (respectively, $V\mathbb{Q}G$) denote the group of units of augmentation 1 in the integral (respectively, rational) group ring of G.

Let $k = \mathbb{Q}(\zeta)$ with $\zeta = e^{2\pi i/p}$, and let k_0 be the fixed field of the automorphism

$$\varphi: \zeta \mapsto \zeta^j$$

of k. We denote by $\mathfrak{o}$ and $\mathfrak{o}_0$ the rings of integers of k and k_0 respectively; one checks easily that $\mathfrak{o}$ is a free $\mathfrak{o}_0$-module with basis $1, \pi, \ldots, \pi^{q-1}$, where

0022-314X/83 $3.00

$\pi = \zeta - 1$ is the prime in $\mathfrak{o}$ above the rational prime p. The prime in $\mathfrak{o}_0$ above p is $\pi_0 = (\zeta - 1)(\zeta^j - 1) \cdots (\zeta^{j^{q-1}} - 1)$. We recall that $\mathfrak{o}/\pi\mathfrak{o} = \mathbb{Z}/p\mathbb{Z} = \mathfrak{o}_0/\pi_0\mathfrak{o}_0$. We put

$$\Pi = \begin{pmatrix} 1 & \pi & \cdots & \pi^{q-1} \\ 1 & \varphi(\pi) & \cdots & \varphi(\pi^{q-1}) \\ & & \cdots & \\ 1 & \varphi^{q-1}(\pi) & \cdots & \varphi^{q-1}(\pi^{q-1}) \end{pmatrix},$$

and for any $q \times q$ matrix T,

$$J_T = \Pi^{-1} T \Pi.$$

Let $\mathscr{X}$ denote the subgroup of $GL_q(\mathfrak{o}_0)$ consisting of matrices X which satisfy the congruence

$$X \equiv \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ * & & & 1 \end{pmatrix} \bmod \pi_0.$$

Finally, let $\mathscr{U}$ (respectively, $\mathscr{W}$) denote the subgroup of $GL_q(\mathbb{Z})$ (respectively, $GL_q(\mathbb{Q})$) consisting of circulants

$$U = \mathrm{Circ}(u_0, u_1, \ldots, u_{q-1}) = \begin{pmatrix} u_0 & u_1 & \cdots & u_{q-1} \\ u_{q-1} & u_0 & \cdots & u_{q-2} \\ & & \cdots & \\ u_1 & u_2 & \cdots & u_0 \end{pmatrix},$$

with

$$u_0 + u_1 + \cdots + u_{q-1} = 1.$$

We shall prove in this section that

(i) The group $V\mathbb{Q}G$ is the semidirect product of $GL_q(k_0)$ and $\mathscr{W}$, the action of $\mathscr{W}$ on $GL_q(k_0)$ being given by

$$X^W = J_W X J_W^{-1}, \qquad W \in \mathscr{W}, X \in GL_q(k_0).$$

(ii) The subgroup $V\mathbb{Z}G$ of $V\mathbb{Q}G$ consists of pairs (X, U) with X in $\mathscr{X}$ and U in $\mathscr{U}$ (see Theorem 1.6).

We shall write elements of $\mathbb{Q}G$ as

$$a = a(\sigma, \tau) = a_0(\sigma) + a_1(\sigma)\tau + \cdots + a_{q-1}(\sigma)\tau^{q-1},$$

where the $a_i(X)$ are polynomials with rational coefficients defined modulo $X^p - 1$ (thus, if $b, c,...$ are elements of $\mathbb{Q}G$ we shall, without mentioning explicitly, consider them written in the above form). It is clear that the numbers $a_i(1)$ and $a_i(\zeta)$ depend only on a, and that two elements a and b of $\mathbb{Q}G$ are equal if and only if $a_i(1) = b_i(1)$ and $a_i(\zeta) = b_i(\zeta)$ for $0 \leqslant i \leqslant q-1$.

Let $\mathscr{A}$ denote the ring of $q \times q$ matrices of the type

$$A = \mathrm{Circ}_\varphi(\alpha_0, \alpha_1, ..., \alpha_{q-1}) = \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{q-1} \\ \varphi\alpha_{q-1} & \varphi\alpha_0 & \cdots & \varphi\alpha_{q-2} \\ & & \cdots & \\ \varphi^{q-1}\alpha_1 & \varphi^{q-1}\alpha_2 & \cdots & \varphi^{q-1}\alpha_0 \end{pmatrix},$$

with α_i in k; it is clear that $\det A$ is invariant under φ and is therefore in k_0. One can check that a matrix A in $\mathscr{A}$ with nonzero determinant has its inverse again in $\mathscr{A}$. Let $\mathscr{N}$ be the subgroup of $GL_q(\mathfrak{o})$ consisting of matrices A in $\mathscr{A}$ which satisfy the congruence

$$A \equiv 1 \bmod \pi,$$

i.e.,

$$\alpha_0 \equiv 1, \alpha_1 \equiv 0, ..., \alpha_{q-1} \equiv 0 \bmod \pi.$$

If a and b are elements of $\mathbb{Q}G$ their product c is given by

$$c_i(\sigma) = \sum_{\mu + \nu \equiv i \bmod q} a_\mu(\sigma)\, b_\nu(\sigma^{j^\mu}), \qquad 0 \leqslant i \leqslant q-1;$$

it follows that the mapping

$$\psi: a \mapsto A = \mathrm{Circ}_\varphi(a_0(\zeta), a_1(\zeta), ..., a_{q-1}(\zeta))$$

is a homomorphism of $\mathbb{Q}G$ onto $\mathscr{A}$.

Let C denote the cyclic group generated by τ, and let N (respectively, L) be the kernel of the homomorphism $V\mathbb{Z}G \to V\mathbb{Z}C$ (respectively, $V\mathbb{Q}G \to V\mathbb{Q}C$) which maps the unit $a(\sigma, \tau)$ to $a(1, \tau)$; an element a of $V\mathbb{Z}G$ (respectively, $V\mathbb{Q}G$) is in N (respectively, L) if and only if

$$a_0(1) = 1, a_1(1) = 0, ..., a_{q-1}(1) = 0.$$

Finally it is clear that $V\mathbb{Z}G$ (respectively, $V\mathbb{Q}G$) is the semidirect product of N and $V\mathbb{Z}C$ (respectively, L and $V\mathbb{Q}C$).

LEMMA 1.1. *The mapping ψ gives isomorphisms of N with $\mathscr{N}$, and of L with the group $\mathscr{A}^{\times}$ of units of $\mathscr{A}$.*

Proof. If $a \in L$ and $\psi(a) = 1$, we have

$$a_0(1) = 1, \qquad a_1(1) = 0, \ldots, \qquad a_{q-1}(1) = 0,$$
$$a_0(\zeta) = 1, \qquad a_1(\zeta) = 0, \ldots, \qquad a_{q-1}(\zeta) = 0,$$

and hence

$$a_0(\sigma) = 1, \qquad a_1(\sigma) = 0, \ldots, \qquad a_{q-1}(\sigma) = 0,$$

so that $a = 1$. Thus ψ is injective on L and hence also on N.

To prove surjectivities, let A be an element of $\mathscr{A}^{\times}$ with first row $(\alpha_0, \alpha_1, \ldots, \alpha_{q-1})$, and let B be its inverse; let $(\beta_0, \beta_1, \ldots, \beta_{q-1})$ be the first row of B.

Write (uniquely)

$$\alpha_0 = a_0(\zeta), \qquad \alpha_1 = a_1(\zeta), \ldots, \qquad \alpha_{q-1} = a_{q-1}(\zeta), \tag{1}$$

where the $a_i(X)$ are polynomials of degree $\leqslant p-1$ with rational coefficients such that

$$a_0(1) = 1, \qquad a_1(1) = 0, \ldots, \qquad a_{q-1}(1) = 0 \tag{2}$$

and form the element

$$a = a(\sigma, \tau) = a_0(\sigma) + a_1(\sigma)\tau + \cdots + a_{q-1}(\sigma)\tau^{q-1}.$$

We similarly form the element

$$b = b(\sigma, \tau) = b_0(\sigma) + b_1(\sigma)\tau + \cdots + b_{q-1}(\sigma)\tau^{q-1}.$$

We notice that in case A is in $\mathscr{N}$ (and hence also B), we have

$$\alpha_0 \equiv 1, \qquad \alpha_1 \equiv 0, \ldots, \qquad \alpha_{q-1} \equiv 0 \bmod \pi,$$
$$\beta_0 \equiv 1, \qquad \beta_1 \equiv 0, \ldots, \qquad \beta_{q-1} \equiv 0 \bmod \pi;$$

in this case the polynomials $a_i(X)$ and $b_i(X)$ have integral coefficients, so that a and b are in $\mathbb{Z}G$.

It is clear that a and b have augmentation 1. Since $AB = 1 = BA$, we have

$$\sum_{\mu + \nu \equiv i \bmod q} a_\mu(\zeta)\, b_\nu(\zeta^{j^\mu}) = \sum_{\mu + \nu \equiv i \bmod q} b_\mu(\zeta)\, a_\nu(\zeta^{j^\mu}) = 1 \text{ or } 0$$

according as $i=0$ or $1 \leqslant i \leqslant q-1$. Moreover by (2) and similar equations for the $b_\nu(1)$ we have

$$\sum_{\mu+\nu \equiv i \bmod q} a_\mu(1)\, b_\nu(1) = 1 \text{ or } 0,$$

according as $i=0$ or $1 \leqslant i \leqslant q-1$. It follows that $ab = ba = 1$, and then by (2) that a is in L; moreover a is in N if A happens to be in $\mathscr{N}$. Clearly, by (1), $\psi(a) = A$, proving the required subjectivities.

We put

$$\delta(X) = \prod_{i=1}^{q-1} (X - \varphi^i \pi) = X^{q-1} + \delta_1 X^{q-2} + \cdots + \delta_{q-1}, \tag{3}$$

and

$$\delta = \delta(\pi) = (\pi - \varphi(\pi))(\pi - \varphi^2(\pi)) \cdots (\pi - \varphi^{q-1}(\pi)). \tag{4}$$

Since $X - \pi \equiv X \bmod \pi$, we have $N_{k/k_0}(X-\pi) \equiv X^q \bmod \pi_0$, and hence on comparing coefficients,

$$\delta_1 \equiv \pi, \qquad \delta_2 \equiv \pi^2, \ldots, \qquad \delta_{q-1} \equiv \pi^{q-1} \bmod \pi_0. \tag{5}$$

One checks easily that the matrix Π has the inverse

$$\Pi^{-1} = \begin{pmatrix} \delta_{q-1}/\delta & \varphi(\delta_{q-1}/\delta) & \cdots & \varphi^{q-1}(\delta_{q-1}/\delta) \\ \delta_{q-2}/\delta & \varphi(\delta_{q-2}/\delta) & \cdots & \varphi^{q-1}(\delta_{q-2}/\delta) \\ & & \cdots & \\ \delta_0/\delta & \varphi(\delta_0/\delta) & \cdots & \varphi^{q-1}(\delta_0/\delta) \end{pmatrix};$$

here, for the sake of symmetry, we have put $\delta_0 = 1$.

LEMMA 1.2. *The conjugation $A \mapsto \Pi^{-1} A \Pi$ is an isomorphism of $\mathscr{A}$ with the ring of all $q \times q$ matrices with entries from k_0.*

Proof. For any matrix M with entries from k, we shall denote by $\varphi(M)$ the matrix obtained from M by applying the automorphism φ to its entries. Let P be the circulant of order q with first row $(0, 1, 0, \ldots, 0)$; then $\varphi(\Pi) = P\Pi$, $\varphi(\Pi^{-1}) = \Pi^{-1}P^{-1}$, and hence for a matrix A with entries in k, $\Pi^{-1}A\Pi$ has entries in k_0 if and only if $\varphi(A) = PAP^{-1}$. One checks easily that this amounts to saying that A is in $\mathscr{A}$.

COROLLARY 1.3. *The mapping*

$$\psi_0 : a \mapsto \Pi^{-1} \psi(a) \Pi$$

is an isomorphism of L with $GL_q(k_0)$.

Proof. Clear from Lemmas 1.1 and 1.2.

LEMMA 1.4. *The mapping*

$$\psi_0 : a \mapsto \Pi^{-1}\psi(a)\Pi$$

is an isomorphism of N with $\mathscr{X}$.

Proof. Let a be an element of N and let $A = \psi(a) = \mathrm{Circ}_\varphi(\alpha_0, \alpha_1, \ldots, \alpha_{q-1})$ be the corresponding element of $\mathscr{N}$; then

$$\alpha_0 \equiv 1, \alpha_1 \equiv 0, \ldots, \alpha_{q-1} \equiv 0 \bmod \pi. \tag{6}$$

One checks easily that the λ-μ entry of $X = \psi_0(a) = \Pi^{-1}A\Pi$ is

$$\begin{aligned} x_{\lambda\mu} &= \sum_{u=0}^{q-1} \sum_{v=0}^{q-1} \varphi^u(\delta_{q-\lambda-1}/\delta)\, \varphi^u(\alpha_v)\, \varphi^{u+v}(\pi^\mu) \\ &= Tr_{k/k_0}\left(\frac{1}{\delta}\,\delta_{q-\lambda-1} \sum_{v=0}^{q-1} \alpha_v \varphi^v(\pi^\mu)\right). \end{aligned}$$

Since δ is the different of the extension k/k_0, the numbers $x_{\lambda\mu}$ are in $\mathfrak{o}_0$. Moreover, in view of the congruences (5) and (6) we have for $\mu \geqslant \lambda$

$$\begin{aligned} x_{\lambda\mu} &\equiv Tr_{k/k_0}\left(\frac{1}{\delta}\,\pi^{q-\lambda-1}\alpha_0\pi^\mu\right) \equiv Tr_{k/k_0}\left(\frac{1}{\delta}\,\pi^{q-1+\mu-\lambda}\right) \\ &\equiv 1 \text{ or } 0 \end{aligned}$$

according as $\mu = \lambda$ or $\mu > \lambda$. It follows that $X = \psi_0(a)$ is in $\mathscr{X}$. Thus ψ_0 maps N into $\mathscr{X}$.

On the other hand suppose that $X = (x_{\lambda\mu})$ is in $\mathscr{X}$. By Lemma 1.2 the matrix $A = \Pi X \Pi^{-1}$ is in $\mathscr{A}$; the entries of the first row of A are

$$\alpha_0 = \frac{1}{\delta}\,[x_0(\pi)\,\delta_{q-1} + x_1(\pi)\,\delta_{q-2} + \cdots + x_{q-1}(\pi)\,\delta_0] = \beta_0/\delta,$$

$$\begin{aligned} \alpha_1 = \frac{1}{\varphi(\delta)}\,&[x_0(\pi)\,\varphi(\delta_{q-1}) + x_1(\pi)\,\varphi(\delta_{q-2}) + \\ &+ \cdots + x_{q-1}(\pi)\,\varphi(\delta_0)] = \beta_1/\varphi(\delta), \end{aligned}$$

$$\cdots$$

$$\begin{aligned} \alpha_{q-1} = \frac{1}{\varphi^{q-1}(\delta)}\,&[x_0(\pi)\,\varphi^{q-1}(\delta_{q-1}) + x_1(\pi)\,\varphi^{q-1}(\delta_{q-2}) + \\ &+ \cdots + x_{q-1}(\pi)\,\varphi^{q-1}(\delta_0)] = \beta_{q-1}/\varphi^{q-1}(\delta), \end{aligned}$$

where

$$x_i(\pi) = x_{0i} + x_{1i}\pi + \cdots + x_{q-1,i}\pi^{q-1} \equiv \pi^i \bmod \pi^{i+1}, \qquad 0 \leqslant i \leqslant q-1,$$

so that, in view of the congruences (5) and the congruences derived from (5) by successive applications of φ, we have, mod π^q

$$\beta_0 \equiv q\pi^{q-1},$$
$$\beta_1 \equiv (\varphi(\pi))^{q-1} + \pi(\varphi(\pi))^{q-2} + \cdots + \pi^{q-2}\varphi(\pi) + \pi^{q-1},$$
$$\cdots$$
$$\beta_{q-1} \equiv (\varphi^{q-1}(\pi))^{q-1} + \pi(\varphi^{q-1}(\pi))^{q-2} + \cdots + \pi^{q-2}\varphi^{q-1}(\pi) + \pi^{q-1}.$$

Since δ and its conjugates are all associates of π^{q-1} we see that α_0, $\alpha_1,\ldots, \alpha_{q-1}$ are elements of $\mathfrak{o}$. Moreover, we have

$$\begin{aligned}\delta/\pi^{q-1} &= (1-\varphi(\pi)/\pi)(1-\varphi^2(\pi)/\pi)\cdots(1-\varphi^{q-1}(\pi)/\pi)\\ &\equiv (-1)^{q-1}(j-1)(j^2-1)\cdots(j^{q-1}-1) \equiv q \bmod \pi,\end{aligned}$$

and hence

$$\alpha_0 = \beta_0/\delta \equiv 1 \bmod \pi.$$

Since

$$(\varphi(\pi)/\pi)^q - 1 = \left(\frac{\zeta^j - 1}{\zeta - 1}\right)^q - 1 \equiv j^q - 1 \equiv 0 \bmod \pi,$$

therefore $(\varphi(\pi))^q - \pi^q \equiv 0 \bmod \pi^{q+1}$ and hence (notice that $\varphi(\pi) - \pi$ is an associate of π)

$$\beta_1 \equiv \frac{(\varphi(\pi))^q - \pi^q}{\varphi(\pi) - \pi} \equiv 0 \bmod \pi^q,$$

so that

$$\alpha_1 = \frac{\beta_1}{\varphi(\delta)} \equiv 0 \bmod \pi.$$

One proves similarly that $\alpha_2,\ldots, \alpha_{q-1}$ are $\equiv 0 \bmod \pi$, and it follows that $A \in \mathcal{N}$. The proof is now complete in view of Lemma 1.1.

LEMMA 1.5. *The mapping*

$$u = u_0 + u_1\tau + \cdots + u_{q-1}\tau^{q-1} \mapsto U = \begin{pmatrix} u_0 & u_1 & \cdots & u_{q-1} \\ u_{q-1} & u_0 & \cdots & u_{q-2} \\ & & \cdots & \\ u_1 & u_2 & & u_0 \end{pmatrix} = \psi(u)$$

is an isomorphism of the group $V\mathbb{Z}C$ (respectively $V\mathbb{Q}C$) with the group $\mathscr{U}$ (respectively $\mathscr{W}$).

Proof. Clear.

THEOREM 1.6. *The mapping*

$$a \cdot w \mapsto (\psi_0(a), W)$$
$$(a \in L,\ w \in V\mathbb{Q}C, \text{ and } W = \psi(w))$$

expresses $V\mathbb{Q}G$ as a semidirect product of groups $GL_q(k_0)$ and $\mathscr{W}$, the action of $\mathscr{W}$ on $GL_q(k_0)$ being

$$X^W = J_W X J_W^{-1} \qquad (X \in GL_q(k_0),\ W \in \mathscr{W}).$$

The subgroup $V\mathbb{Z}G$ of $V\mathbb{Q}G$ consists of pairs (X, U) with X in $\mathscr{X}$ and U in $\mathscr{U}$; in particular $V\mathbb{Z}G$ is the semidirect product of $\mathscr{X}$ and $\mathscr{U}$ with the action as given above.

Proof. In view of Corollary 1.3, Lemma 1.5, and Lemma 1.4, the following suffices. If a, b are in L, and w, v are in $V\mathbb{Q}C$, then $aw \cdot bv = a(wbw^{-1})wv$, and hence the component of $aw \cdot bv$ in $GL_q(k_0)$ is

$$\psi_0(a \cdot wbw^{-1}) = \psi_0(a)\,\psi_0(wbw^{-1});$$

it follows that $(\psi_0(b))^W$ should be defined as $\psi_0(wbw^{-1})$. Putting $B = \psi(b)$, $Y = \psi_0(b) = \Pi^{-1}B\Pi$, we thus have the action

$$\begin{aligned} Y^W &= \psi_0(wbw^{-1}) = \Pi^{-1}\psi(wbw^{-1})\Pi = \Pi^{-1}WBW^{-1}\Pi \\ &= (\Pi^{-1}W\Pi)(\Pi^{-1}B\Pi)(\Pi^{-1}W^{-1}\Pi) = J_W Y J_W^{-1}. \end{aligned}$$

From now on we shall write the pair (X, W) as XW; there is no danger of confusion with the usual product of the two matrices X and W.

2. Torsion Elements of $V\mathbb{Z}G$

For any matrix X with entries in $\mathfrak{o}_0$ we shall denote by $\bar{X}$ the matrix obtained from X on reducing its entries mod π_0; thus $\bar{X}$ has entries in $\mathfrak{o}_0/\pi_0\mathfrak{o}_0 = GF(p)$. If $X \in \mathscr{X}$, then the characteristic polynomial $(T-1)^q$ of $\bar{X}$ divides $T^p - 1 = (T-1)^p$, and hence $\bar{X}^p = 1$.

LEMMA 2.1. *Each torsion element X of $\mathscr{X}$ is of order a power of p.*

Proof. It suffices to prove that the order n of every torsion element $X \neq 1$ of $\mathscr{X}$ is divisible by p. If $\bar{X} \neq 1$, then $\bar{X}$ has order p and hence X has order a multiple of p. Suppose then that $\bar{X} = 1$ and write

$$X = 1 + \pi_0^t B$$

where $t \geqslant 1$, B has entries in $\mathfrak{o}_0$ and $B \not\equiv 0 \bmod \pi_0$, i.e., at least one entry of B is not divisible by π_0. We have

$$1 = X^n = 1 + n\pi_0^t B + \binom{n}{2} \pi_0^{2t} B^2 + \cdots + \pi_0^{nt} B^n,$$

and hence

$$-nB = \binom{n}{2} \pi_0^t B^2 + \cdots + \pi_0^{(n-1)t} B^n;$$

it follows that π_0 and hence p divides n.

LEMMA 2.2. *$X = 1$ is the only element of $\mathscr{X}$ which satisfies*

$$\bar{X} = 1, \qquad X^p = 1.$$

Proof. Suppose that $\bar{X} = 1$, $X^p = 1$, and $X \neq 1$, and write

$$X = 1 + \pi_0^t B,$$

where $t \geqslant 1$, B has entries in $\mathfrak{o}_0$ and $B \not\equiv 0 \bmod \pi_0$; we then have as above

$$pB + \binom{p}{2} \pi_0^t B^2 + \cdots + \pi_0^{(p-1)t} B^p = 0;$$

this is impossible because the first term on the left is divisible exactly by $\pi_0^{(p-1)/q}$ whereas the others are divisible by higher powers of π_0.

THEOREM 2.3. *Each torsion element $X \neq 1$ in $\mathscr{X}$ is of order p.*

Proof. Suppose that X has order p^{μ} with $\mu > 1$; then

$$\bar{X}^{p^{\mu-1}} = 1, \qquad (X^{p^{\mu-1}})^p = 1$$

and hence by Lemma 2.2 $X^{p^{\mu-1}} = 1$, which is obviously not possible.

Let $U \in \mathscr{U}$ and let u be the corresponding element of $V\mathbb{Z}C$; by a result of Higman [4] U is of finite order if and only if $u = \tau^r$, in which case the order of U is $\lambda = q/(q, r)$.

We now consider torsion elements XU, $U \neq 1$, of the semidirect porduct of $\mathscr{X}$ and $\mathscr{U}$; since the components of $(XU)^n$ in $\mathscr{X}$ and $\mathscr{U}$ are, respectively,

$$X^{1+U+\cdots+U^{n-1}} \stackrel{\text{def}}{=} X \cdot X^U \cdots X^{U^{n-1}} \qquad \text{and } U^n,$$

we see that XU, $U \neq 1$, is of finite order if and only if U corresponds to the unit τ^r, $1 \leqslant r \leqslant q-1$, and there exists a multiple n of $\lambda = q/(q, r)$ such that

$$X^{1+U+\cdots+U^{n-1}} = 1,$$

i.e.,

$$(X^{1+U+\cdots+U^{\lambda-1}})^{n/\lambda} = 1.$$

Thus

THEOREM 2.4. *The unit XU, $U \neq 1$, is of finite order if and only if U corresponds to τ^r, $1 \leqslant r \leqslant q-1$ and the unit $X^{1+U+\cdots+U^{\lambda-1}}$ is of finite order, which by Theorem 2.3 is then 1 or p; in that case XU is of order λ or $p\lambda$ according as $X^{1+U+\cdots+U^{\lambda-1}}$ has order 1 or p.*

It is likely that the second case does not arise at all, but we are unable to prove it. We are, however, able to prove:

THEOREM 2.5. *Let U be the circulant corresponding to τ^r with $(q, r) = 1$ (so that $\lambda = q$). Suppose that XU is of finite order. Then*

$$X^{1+U+\cdots+U^{q-1}} = 1,$$

and hence XU is of order q.

COROLLARY 2.6. *In case q is also a prime, all torsion elements $\neq 1$ of $V\mathbb{Z}G$ are of order p or q.*

Proof of Theorem 2.5. In view of Theorem 2.4 and Lemma 2.2 it suffices to prove that

$$X^{1+U+\cdots+U^{q-1}} \equiv 1 \bmod \pi_0,$$

i.e.,

$$(XJ_U)^q \equiv 1 \bmod \pi_0. \tag{7}$$

One checks as in the proof of Lemma 1.4 that the λ-μ entry $x_{\lambda\mu}$ in J_U is

$$x_{\lambda\mu} = \mathrm{Tr}_{k/k_0}\left(\frac{1}{\delta}\,\delta_{q-\lambda-1}\varphi^r(\pi^\mu)\right), \qquad 0 \leqslant \lambda,\ \mu \leqslant q-1. \tag{8}$$

Since δ is the different of the extension k/k_0, the entries of J_U are in $\mathfrak{o}_0$. Thus (7) would follow as soon as we are able to prove that he reduction $\bar{J}_U$ of $J_U \bmod \pi_0$ is lower triangular with diagonal $1, j^r, ..., j^{(q-1)r}$, for then $\overline{XJ_U}$, being of the same type, would have characteristic polynomial

$$(T-1)(T-j^r)\cdots(T-j^{(q-1)r}),$$

which, because of the assumption $(q, r) = 1$, is equal to $T^q - 1$. Therefore it suffices to prove the congruences

$$x_{\lambda\mu} \equiv 0 \bmod \pi_0, \qquad 0 \leqslant \lambda < \mu \leqslant q-1, \tag{9}$$

and

$$x_{\lambda\lambda} \equiv j^{r\lambda} \bmod \pi_0, \qquad 0 \leqslant \lambda \leqslant q-1. \tag{10}$$

By (5), $\delta_{q-\lambda-1}$ is divisible by $\pi^{q-\lambda-1}$; moreover δ is an associate of π^{q-1}; it follows that for $\lambda < \mu$, $(1/\delta)\,\delta_{q-\lambda-1}\varphi^r(\pi^\mu)$ is divisible by π, and hence its trace $x_{\lambda\mu}$ is divisible by π_0. This proves (9).

Thus it only remains to prove (10). By (3) we have

$$N_{k/k_0}(X-\pi) = X^q + \sum_{s=1}^{q-1} (\delta_{q-s} - \pi\delta_{q-s-1})\, X^s - \pi\,\delta_{q-1};$$

multiplying this equation by $\varphi^r(\pi^\lambda)\,\pi^t/\delta$ and taking traces we obtain modulo π_0 (notice that $N_{k/k_0}(X-\pi) \equiv X^q$ and $\pi\,\delta_{q-1} \equiv 0 \bmod \pi_0$)

$$0 \equiv \sum_{s=1}^{q-1} \mathrm{Tr}_{k/k_0}((\delta_{(q-s)}/\delta)\,\varphi^r(\pi^\lambda)\,\pi^t - (\delta_{(q-s-1)}/\delta)\,\varphi^r(\pi^\lambda)\pi^{t+1})\,X^s,$$

and hence

$$\begin{aligned}&\mathrm{Tr}_{k/k_0}((\delta_{(q-s)}/\delta)\,\varphi^r(\pi^\lambda)\,\pi^t)\\ &\quad \equiv \mathrm{Tr}_{k/k_0}((\delta_{(q-s-1)}/\delta)\,\varphi^r(\pi^\lambda)\,\pi^{t+1}) \bmod \pi_0,\\ &\quad (1 \leqslant s \leqslant q-1, 0 \leqslant t, \lambda \leqslant q-1)\end{aligned}$$

Using these relations we obtain for $0 \leqslant \lambda \leqslant q-2$

$$\mathrm{Tr}_{k/k_0}\left(\frac{1}{\delta}\,\delta_{q-\lambda-1}\varphi^r(\pi^\lambda)\right) \equiv \mathrm{Tr}_{k/k_0}\left(\frac{1}{\delta}\,\varphi^r(\pi^\lambda)\,\pi^{q-\lambda-1}\right) \bmod \pi_0.$$

The above relation is also true (trivially) for $\lambda = q-1$. Thus in order to prove (10) we need to prove

$$\mathrm{Tr}_{k/k_0}\left(\frac{1}{\delta}\,\varphi^r(\pi^\lambda)\,\pi^{q-\lambda-1}\right) \equiv j^{r\lambda} \bmod \pi_0, \qquad (11)$$

$$(0 \leqslant \lambda \leqslant q-1)$$

Using the fact that $\mathrm{Tr}_{k/k_0}(\zeta^i/\delta) = 0$ for $0 \leqslant i \leqslant q-2$, and $=1$ for $i = q-1$, we obtain for all nonnegative integers v

$$\mathrm{Tr}_{k/k_0}(\zeta^v/\delta) \equiv \binom{v}{q-1} \bmod \pi_0;$$

hence the left hand-side of (11) is congruent mod π_0 to

$$\sum_{s=0}^{\lambda} (-1)^s \binom{\lambda}{s} \sum_{t=0}^{q-\lambda-1} (-1)^t \times$$

$$\times \binom{q-\lambda-1}{t}\binom{q-\lambda-1+(\lambda-s)\,j^r-t}{q-1}$$

$$= \sum_{s=0}^{\lambda} (-1)^s \binom{\lambda}{s} S(q-\lambda-1, q-\lambda-1+(\lambda-s)\,j^r, q-1),$$

where for any nonnegative integers M, N, R with $N, R \geqslant M$, we have put

$$S(M,N,R) = \sum_{t=0}^{M} (-1)^t \binom{M}{t}\binom{N-t}{R} = \sum_{t=0}^{N} (-1)^t \binom{M}{t}\binom{N-t}{R}.$$

Since, for $M \geqslant 1$,

$$S(M,N,R) = \sum_{t=0}^{M} (-1)^t \binom{M}{t} \sum_{Q=0}^{N-t-1} \binom{Q}{R-1}$$

$$= \sum_{Q=0}^{N-1} \left(\sum_{t=0}^{N-Q-1} (-1)^t \binom{M}{t} \right) \binom{Q}{R-1}$$

$$= \sum_{Q=0}^{N-1} (-1^{N-Q-1} \binom{M-1}{N-Q-1}\binom{Q}{R-1}$$

$$= \sum_{t=0}^{N-1} (-1)^t \binom{M-1}{t}\binom{N-1-t}{R-1} = S(M-1, N-1, R-1),$$

we have

$$S(M, N, R) = S(0, N-M, R-M) = \binom{N-M}{R-M}.$$

It follows that the left-hand side of (11) is congruent mod π_0 to

$$\sum_{s=0}^{\lambda} (-1)^s \binom{\lambda}{s} \binom{(\lambda - s) j^r}{\lambda}.$$

By coupon collector's identity [2, Chap. IV, Problems 12 and 14], this number is $j^{r\lambda}$. We have thus proved (11) and thereby (10), completing the proof of Theorem 2.5.

3. Verification of the Conjecture

We are now able to prove that *in case q is also a prime then for the group G under consideration, every element of finite order of $V\mathbb{Z}G$ is conjugate in $V\mathbb{Q}G$ to an element of G.* In view of Theorem 1.6 it suffices to prove

(1) Each torsion element X in $\mathscr{X}$ is conjugate in $GL_q(k_0)$ to $\psi_0(\sigma^s)$ for some s.

(2) Each torsion element XU, $U \neq 1$, of the semi-direct product of $\mathscr{X}$ and $\mathscr{U}$ is conjugate in the semi-direct product of $GL_q(k_0)$ and $\mathscr{W}$ to an element of the type $\psi(\tau^r)$.

Proof of (1). Let $X \neq 1$ be a torsion element in $\mathscr{X}$. By Theorem 2.3, X is of order p, and hence its eigenvalues are pth roots of 1. If all the eigenvalues of X are 1, then X is conjugate and hence equal to the identity matrix (notice that X is of finite order). Thus X has an eigenvalue $\zeta^s \neq 1$. Since the entries of X are in k_0, its eigenvalues are

$$\zeta^s, \zeta^{js}, \ldots, \zeta^{j^{q-1}s}$$

which are all distinct and in k; it follows that there exists a matrix M in $GL_q(k)$ such that

$$M^{-1}XM = \mathrm{Diag}(\zeta^s, \zeta^{js}, \ldots, \zeta^{j^{q-1}s}) = \psi(\sigma^s),$$

so that

$$(M\Pi)^{-1} X (M\Pi) = \psi_0(\sigma^s).$$

Thus X and $\psi_0(\sigma^s)$ are conjugate in $GL_q(k)$, and hence also in $GL_q(k_0)$.

Proof of (2). By Theorems 2.4 and 2.5, U is a circulant $\psi(\tau^r)$ which corresponds to τ^r, $1 \leqslant r \leqslant q-1$, XU is of order q, and

$$X^{1+U+\cdots+U^{q-1}} = 1. \tag{12}$$

Let

$$Z = 1 + X + X^{1+U} + \cdots + X^{1+U+\cdots+U^{q-2}}.$$

Since

$$Z \equiv \begin{pmatrix} q & & 0 \\ & \ddots & \\ * & & q \end{pmatrix} \bmod \pi_0,$$

therefore $\det Z \neq 0$, and $Z \in GL_q(k_0)$. One checks easily that

$$J_U Z J_U^{-1} = 1 + X^U + X^{U+U^2} + \cdots + X^{U+U^2+\cdots+U^{q-1}},$$

and hence by (12)

$$XJ_U Z J_U^{-1} = Z,$$

so that (in the semidirect product of $GL_q(k_0)$ and $\mathscr{U}$)

$$Z^{-1}(XU)Z = Z^{-1}XZ^U \cdot U = Z^{-1}XJ_U Z J_U^{-1} \cdot U = U = \psi(\tau^r).$$

References

1. R. K. Dennis, "The Structure of the Unit Group of Group Rings," Lecture Notes in Pure and Applied Mathematics Vol. 26, Dekker, New York, 1977.
2. W. Feller, "An Introduction to Probability Theory and Its Applications, Volume 1," Wiley, New York, 1957.
3. S. Galovitch, I. Reiner, and S. Ullom, Class groups for integral representations of metacyclic groups, *Mathematika* **19** (1972), 105–111.
4. G. Higman, The units of group rings, *Proc. London Math. Soc.* (2) **46** (1940), 231–248.
5. I. Hughes and K. R. Pearson, The group of units of the integral group ring $\mathbb{Z}S_3$, *Canad. Math. Bull.* **15** (1972), 529–534.
6. S. K. Sehgal, "Topics in Group Rings," Dekker, New York, 1978.
7. H. Zassenhaus, On the torsion units of finite group rings, *in* "Studies in Mathematics," pp. 119–126. (in honor of A. Almeida Costa), Instituo de Alta Cultura, Lisbon, 1974.

Printed in Belgium