PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 97, Number 2, June 1986

ON A CONJECTURE OF ZASSENHAUS ON TORSION UNITS IN INTEGRAL GROUP RINGS. II[1]

CÉSAR POLCINO MILIES, JÜRGEN RITTER AND SUDARSHAN K. SEHGAL

ABSTRACT. Suppose that a group G has a normal subgroup C where C and G/C are cyclic of relatively prime orders. Then any torsion unit in ZG is rationally conjugate to a trivial unit.

1. Introduction. Let $U_1\mathbf{Z}G$ be the group of units of augmentation one in the integral group ring $\mathbf{Z}G$ of a finite group G and let $TU_1\mathbf{Z}G$ be the subset of torsion units. For two elements α, β of the rational group algebra $\mathbf{Q}G$ (or of $\mathbf{Z}G$) we write $\alpha \sim \beta$ if there is a unit γ of $\mathbf{Q}G$ such that $\alpha = \gamma^{-1}\beta\gamma$. There is a well-known conjecture of Zassenhaus:

$$\text{(ZC)} \qquad u \in TU_1\mathbf{Z}G \Rightarrow \exists g \in G \quad \text{such that } u \sim g.$$

This conjecture has been confirmed in [**1** and **3**] for groups G which are nilpotent class 2 or are split metacyclic with $G = \langle a \rangle \rtimes \langle x \rangle$, $O(a)$ a prime power and $O(x)$ relatively prime to $O(a)$.

It is the purpose of this paper to extend this to some more metacyclic groups. We prove the following

THEOREM. *Let G be the split metacyclic group, $G = \langle a \rangle \rtimes \langle x \rangle$, with $O(a) = n$, $O(x) = t$ and $(n,t) = 1$. Then for any unit $u \in TU_1\mathbf{Z}G$ there is a $g \in G$ such that $u \sim g$.*

In the proof we need to use the main result of [**3**], namely that (ZC) holds if n is a prime power.

2. Some lemmas. We recall Lemma 2 of [**1**].

LEMMA 2.1. *Let G be a split extension $A \rtimes X$ where A is an abelian normal p-group and X any group. Let $u \in U_1\mathbf{Z}G$ be written as $u = vw$, $v \in U(1+\Delta(G,A))$, $w \in U\mathbf{Z}X$. If u has finite order not divisible by p, then $u \sim w$.*

Here, $\Delta(G,A)$ denotes the kernel of the natural map $\mathbf{Z}G \to \mathbf{Z}(G/A)$.

LEMMA 2.2. *Let $G = \langle a \rangle \rtimes \langle x \rangle$, $O(a) = n$, $O(x) = t$ with $(n,t) = 1$. If $u \in TU_1\mathbf{Z}G$ has prime power order, then $u \sim g$ for some $g \in G$.*

PROOF. Let $O(u) = p^k$. If p divides $O(x)$, then we are done by repeated applications of the last lemma. Therefore, suppose $n = p^m n_1$, $(p, n_1) = 1$, $m > 0$. Then $G = \langle a^{p^m} \rangle \rtimes G_1$, $G_1 = \langle a^{n_1} \rangle \rtimes \langle x \rangle$. It follows by (2.1) that $u \sim v$, $v \in U\mathbf{Z}G_1$. Thus the lemma is a consequence of the main result of [**3**].

The next result is well known.

Received by the editors October 15, 1984 and, in revised form, May 7, 1985.
1980 *Mathematics Subject Classification*. Primary 20C05; Secondary 16A25, 16A26.
[1]This work has been supported by CNPQ of Brazil, DFG of West Germany and NSERC of Canada.

LEMMA 2.3. *Let $G = \langle a \rangle \rtimes \langle x \rangle$ with $a^x = a^j$, $O(a) = n$, $O(x) = t$, $(n,t) = 1$. If an element $a^i x^k$ of G with $x^k \neq 1$ has its order divisible by all primes dividing n then x^k is central.*

PROOF. First let $n = p^m$ with p a prime. Let $a^i = b$, $x^k = y$. Then

$$(by)^t = b^{1+j^k+\cdots+j^{k(t-1)}}.$$

Now, $(1-j^k)(1+j^k+\cdots+j^{k(t-1)}) = (1-j^{kt}) \equiv 0 \pmod{p^m}$. Consequently, either $p|(1-j^k)$ in which case $j^{kp^{m-1}} \equiv 1 \pmod{p^m}$ implying that $j^k \equiv 1 \pmod{p^m}$ (because $(O(j),p) = 1$) and thus y to be central, or $p \nmid (1-j^k)$ and $1 + j^k + \cdots + j^{k(t-1)} \equiv 0 \pmod{p^m}$ which forces $(by)^t = 1$, which is not the case.

Now, let $\langle a \rangle = A_p \times A_{p'}$ where A_p is the p-Sylow subgroup of A. If $A = A_p$ we are done already. We use induction. Write the element $g = a^i x^k$ as $g = a_p z$, $z = a_{p'} x^k$, $a_p \in A_p$, $a_{p'} \in A_{p'}$. By what we have done already z centralizes A_p. Thus x^k centralizes A_p. Similarly x^k centralizes $A_{p'}$ and the proof is complete.

LEMMA 2.4. *Let $G = \langle a \rangle \rtimes \langle x \rangle$, $O(a) = n$, $O(x) = t$, $(t,n) = 1$. Suppose that $u \in TU_1\mathbf{Z}G$ and all primes dividing n divide $O(u)$. Then we can write $u = u_1u_2$, $u_1 \in 1 + \Delta(G, \langle a \rangle)$ and u_2 central.*

PROOF. From $u \equiv a^i x^k \operatorname{mod}(\Delta G \Delta \langle a \rangle)$ for suitable i, k we conclude that $O(u) = O(a^i x^k)$. We have by (2.3) that x^k is central. Then $ux^{-k} \equiv 1 \operatorname{mod} \Delta(G, A)$. We are finished by taking $u_2 = x^k$ and $u_1 = ux^{-k}$.

3. Proof of the theorem—some reductions. We have a group $G = \langle a \rangle \rtimes \langle x \rangle$, $a^x = a^j$, $O(a) = n$, $O(x) = t$ with $(t,n) = 1$ and are given a unit $u \in TU_1\mathbf{Z}G$. We wish to show that there is a $g \in G$ such that $u \sim g$. To that effect we use induction on $|G|$ and thus assume that the result is true for all metacyclic groups G of this type of smaller order. We can restrict ourselves to the case that n is divisible by at least two different primes.

(3.1) *We may assume that all prime divisors of n divide $O(u)$.*

PROOF. Suppose that p is a prime number with $n = p^m n_1, (p, n_1) = 1, m > 0$ and $(O(u), p) = 1$. Write $G = \langle a^{n_1} \rangle \rtimes G_1$, $G = \langle a^{p^m} \rangle \rtimes \langle x \rangle$. Then it follows by (2.1) that $u \sim v$, $v \in U\mathbf{Z}G_1$, and so by induction $v \sim g$, $g \in G$.

(3.2) *We may assume that no Sylow p-subgroup of $\langle a \rangle$ is central in G.*

PROOF. Suppose that $\langle a \rangle$ has a central Sylow p-subgroup $\langle a_1 \rangle$. Write

$$\langle a \rangle = \langle a_1 \rangle \times A_1, \quad G = \langle a_1 \rangle \rtimes G_1, \quad G_1 = A_1 \rtimes \langle x \rangle.$$

Write $u = u_1u_2$, $u_1 \in 1 + \Delta(G, \langle a_1 \rangle)$, where u_1 is a p-element and u_2 is a p'-element. Then since a_1 is central in G it follows by [**4**, p. 34] that $u_1 = a_1^r$, a central element of G. Moreover, $u_2 \sim g$, $g \in G_1$ by induction. Thus $u \sim a_1^r g$ and the assertion follows.

(3.3) *We may assume that $j \not\equiv 1 \pmod p$ for any prime p dividing n and, therefore, $G' = \langle a \rangle$.*

PROOF. $j \equiv 1 \pmod p \Rightarrow j^{p^{m-1}} \equiv 1 \pmod{p^m} \Rightarrow j \equiv 1 \pmod{p^m}$, as the order of $j \operatorname{mod} n$, being a divisor of t, is relatively prime to n. Therefore the Sylow p-subgroup is central and the assertion follows.

We shall prove as in [**1** and **3**] that for every absolutely irreducible representation T of G, $T(u) \sim T(g)$ for some $g \in G$. It is enough to do this for rationally inequivalent representations. This will complete the proof of the Theorem.

From [**5**, p. 62] we see that these representations up to rational equivalence are given by

$$T_{d,\mu}(a) = \begin{bmatrix} \varsigma_d & & & \\ & \varsigma_d^j & & \\ & & \ddots & \\ & & & \varsigma_d^{j^{t_d-1}} \end{bmatrix}_{t_d\times t_d},$$

$$T_{d,\mu}(x) = \begin{bmatrix} 0 & 1 & 0 & . & . & . & . & 0 \\ 0 & 0 & 1 & 0 & . & . & . & 0 \\ 0 & . & . & . & . & 0 & 0 & 1 \\ \eta^\mu & 0 & . & . & . & . & . & 0 \end{bmatrix}_{t_d\times t_d}$$

where d runs over the divisors of n, ς is a fixed primitive nth root of unity, $\varsigma_d = \varsigma^d$, t_d is the order of $j \bmod n/d$, and η is a primitive t/t_dth root of unity; $\mu = 0, 1, 2, \ldots, t/t_d - 1$. It therefore remains to prove the following propositions:

PROPOSITION 3.4. *$u \in T(1 + \Delta(G, \langle a \rangle)) \Rightarrow T_{d,\mu}(u) \sim T_{d,\mu}(a^r)$ for some $r = r(d, \mu)$.*

Notice that for all abelian representations T we have $T(u) = T(a^r) = 1$.

PROPOSITION 3.5. *We can choose an $r = r(d, \mu)$ which is independent of d and μ.*

For proving Proposition 3.4 we may assume that all prime divisors of n divide $O(u)$ by (3.1) and moreover, by (3.3), that we are in the situation $G' = \langle a \rangle$ and $j \not\equiv 1 \bmod p$ for every prime divisor p of n.

4. Completion of the proof of the theorem.

LEMMA 4.1. *$T_{1,\mu}$ is faithful on any cyclic group H of units of order dividing n.*

PROOF. Use induction on $|H|$ and (2.2), remembering that $T_{1,\mu}$ is faithful on $\langle a \rangle$.

LEMMA 4.2. *Let $u \in T(1 + \Delta(G, \langle a \rangle))$. Suppose p is a prime dividing n. Then $T_{1,\mu}(u^p) = 1 \Leftrightarrow T_{p,\mu}(u) = 1$.*

PROOF. By decomposing u into a product of elements of prime power order one sees that it is enough to assume that $O(u)$ is a power of a prime. The result follows by (2.2).

(4.3) *Proof of* (3.4). Write $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, a product of distinct primes. Then

$$O(u) = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \qquad 0 < \beta_i \le m_i.$$

We express $u = u_1 \cdots u_k$, $O(u_i) = p_i^{\beta_i}$. Write $T = T_{1,\mu}$. Then we know by (2.2) that $u_i \sim a^{\lambda_i}$ for some λ_i. Thus

$$T(u_i) \sim T(a^{\lambda_i}) = \begin{bmatrix} \varsigma^{\lambda_i} & & & \\ & \varsigma^{\lambda_i j} & & \\ & & \ddots & \\ & & & \varsigma^{\lambda_i j^{l-1}} \end{bmatrix}, \qquad l = O(j) \bmod n.$$

Now,

$$O(\varsigma^{\lambda_i}) = O(\varsigma^{\lambda_i j}) = O(a^{\lambda_i}) = O(u_i) = p_i^{\beta_i}.$$

This is because $(j,n)=1$ and since T is faithful on $\langle a\rangle$. As the u_i's are powers of u, diagonalizing $T(u)$ gives a diagonal form for $T(u_i)$ as well; the eigenvalues of $T(u)$ are products $\varsigma^{\lambda_i}\cdot\varsigma^{\lambda_j j^{\mu}}\cdots$. Thus all eigenvalues of $T(u)$ have order $O(u)$. Let λ be an eigenvalue of $T(u)$. Then λ^j is also an eigenvalue of $T(u)$ as conjugating $T(u)$ by $T(x)$ means applying the automorphism $\varsigma\to\varsigma^j$ to the entries of $T(u)$. If $\lambda^{j^{\nu}}=\lambda$, then $j^{\nu}\equiv 1(O(u))$ and so $j^{\nu}\equiv 1(p_i^{\beta_i})$ for all i. Because $O(j) \bmod n$ is relatively prime to n we conclude $j^{\nu}\equiv 1(p_i^{\alpha_i})$ for all i and therefore $j^{\nu}\equiv 1 \pmod n$. Thus we have

$$T(u)\sim\begin{bmatrix}\lambda &&&&\\ &\lambda^j&&&\\ &&\lambda^{j^2}&&\\ &&&\ddots&\\ &&&&\lambda^{j^{l-1}}\end{bmatrix}\sim T(a^r)\quad\text{for some } r.$$

We wish to show that $T_{d,\mu}(u)\sim T_{d,\mu}(a^r)$ for a divisor d of n. Clearly, $\langle a^{n/d}\rangle$ is in the kernel of $T_{d,\mu}$. Write $\overline{G}=G/\langle a^{n/d}\rangle$ and $\overline{T}_{d,\mu}$ for the corresponding representations of $\overline{G}$. We see that $\overline{T}_{1,\mu}(\overline{u}) = T_{d,\mu}(u)$. But from what we have already proved, $\overline{T}_{1,\mu}(\overline{u})\sim\overline{T}_{1,\mu}(\overline{a}^r)=T_{d,\mu}(a^r)$. This completes the proof of (3.4).

(4.4) *Proof of* (3.5). (a) We first show that $r=r(d,\mu)$ is independent of d. Write $T_{1,\mu}=T_1$, $T_{p,\mu}=T_p$ for a prime divisor p of n. It is enough to prove

$$T_1(u)\sim T_1(a^r),\quad T_p(u)\sim T_p(a^k)\Rightarrow T_p(a^k)\sim T_p(a^r).$$

We use induction on $O(u)$ and $|G|$. There are two cases: (i) $p^2\nmid n$; (ii) $p^2|n$. In the first case the dimension of T_p may be smaller than that of T_1. In the second case they are the same. We deal with the two cases separately.

Case (i). $p|n$, $p^2\nmid n$. Then we can assume that $p|O(u)$ as otherwise $u\sim$ a unit in a smaller group by the argument in (3.1). Thus

$$T_1(u^p)\sim T_1(a^{rp}),\quad T_p(u^p)\sim T_p(a^{kp})\Rightarrow T_p(a^{rp})\sim T_p(a^{kp}),$$

by induction.

Comparing eigenvalues we get $rp^2\equiv kp^2j^{\nu} \pmod n$ for some ν. Therefore, $rp=kpj^{\nu} \pmod{n/p}$ which implies $r\equiv kj^{\nu}(n/p)$ as $p^2\nmid n$. If follows that $rp = kpj^{\nu} \bmod n$ and thus $T_p(a^r)\sim T_p(a^k)$ as desired.

Case (ii). $p^2|n$, dimension of T_1 = dimension of T_p. Let $u=\sum_{i=0}^{t-1} f_i(a)x^i$ with integral polynomials $f_i(a)$ in a of degree $\le n-1$. Then

$$T_{d,\mu}(u)=\begin{bmatrix}\sum_{\nu=0}^{l-1} f_{\nu s}(\varsigma_d)\eta^{\mu\nu} & \sum_{\nu=0}^{l-1} f_{1+\nu s}(\varsigma_d)\eta^{\mu\nu} & \cdots & \sum_{\nu=0}^{l-1} f_{s-1+\nu s}(\varsigma_d)\eta^{\mu\nu}\\ \cdots & \sum_{\nu=0}^{l-1} f_{\nu s}(\varsigma_d^{j})\eta^{\mu\nu} && \\ &&\ddots& \\ \cdots &&& \sum_{\nu=0}^{l-1} f_{\nu s}(\varsigma_d^{j^{s-1}})\eta^{\mu\nu}\end{bmatrix}$$

where $s=t_d=O(j) \bmod n/d$, $l=t/s$, and η is an lth root of unity. By taking $d=1$ and p, respectively, we obtain $T_1(u)$ and $T_p(u)$. We introduce, as in [**1** and

3], the matrix

$$M(y)=\begin{bmatrix} \sum_{\nu=0}^{l-1} f_{\nu s}(y)\eta^{\mu\nu} & \sum_{\nu=0}^{l-1} f_{1+\nu s}(y)\eta^{\mu\nu} & \cdots & \sum_{\nu=0}^{l-1} f_{s-1+\nu s}(y)\eta^{\mu\nu} \\ & \sum_{\nu=0}^{l-1} f_{\nu s}(y^j)\eta^{\mu\nu} & & \\ \cdots & & & \\ \cdots & & & \sum_{\nu=0}^{l-1} f_{\nu s}(y^{j^{s-1}})\eta^{\mu\nu} \end{bmatrix}$$

where y is an indeterminate. This matrix has coefficients in $\mathbf{Z}[\eta][y]$. Write for the characteristic polynomials

$$Ch_{M(y)}(z)=\sum_{\mu=0}^{s-1}\psi_\mu(y)z^{s-\mu},$$

$$Ch_{T_1(u)}(z)=\prod_{\nu=0}^{s-1}(z-\varsigma^{rj^\nu}),$$

$$Ch_{T_p(u)}(z)=\prod_{\nu=0}^{s-1}(z-\varsigma^{pkj^\nu}).$$

Now we follow pages 263–264 of [**3**] verbatim, only replacing q by s, and conclude that $\varsigma^{pk}=\varsigma^{prj^\nu}$ for some ν. Hence $T_p(a^k)\sim T_p(a^r)$. (Observe that the nth cyclotomic polynomial $\varphi_n(y)$ is also irreducible over the ring $\mathbf{Z}[\eta]$ of coefficients of the $\psi_\mu(y)$.)

(b) We have see that $r(d,\mu)=r(\mu)$ is independent of d. It is enough to show that $T_{1,\mu}(a^{r(\mu)})\sim T_{1,\mu}(a^{r(0)})$.

We are using induction on $|G|$ and $O(u)$. Consequently, we may assume as in (3.1) that all primes dividing n divide $O(u)$. Thus for any proper divisor d of n

$$T_{1,\mu}(u^d)\sim T_{1,\mu}(a^{r(\mu)d}),\quad T_{1,0}(u^d)\sim T_{1,0}(a^{r(0)d})$$

implies that

$$(*)\qquad T_{1,\mu}(a^{r(\mu)d})\sim T_{1,\mu}(a^{r(0)d}).$$

Let us consider the traces of the matrices $T_{1,\mu}(u)$:

$$\chi_{1,\mu}(u)=\operatorname{tr}T_{1,\mu}(u)=\sum_{\nu=0}^{l-1}\operatorname{tr}_j f_{\nu s}(\varsigma)\eta^{\mu\nu}=\operatorname{tr}_j\varsigma^{r(\mu)}=\chi_{1,\mu}(a^{r(\mu)}),$$

where for an element $\alpha\in\mathbf{Q}(\varsigma)$ we have denoted by $\operatorname{tr}_j\alpha$ the trace of α with respect to the automorphism group generated by $\sigma_j:\varsigma\to\varsigma^j$. Adding up the equations over all μ we get

$$\begin{aligned}\sum_{\mu=0}^{l-1}\operatorname{tr}_j\varsigma^{r(\mu)}&=\sum_\mu\sum_\nu\operatorname{tr}_j f_{\nu s}(\varsigma)\eta^{\mu\nu}\\ &=\sum_\nu\left(\operatorname{tr}_j f_{\nu s}(\varsigma)\sum_\mu\eta^{\mu\nu}\right)=l\ \operatorname{tr}_j f_0(\varsigma)\end{aligned}$$

as for $\nu\neq 0$, $\sum_{\nu=0}^{l-1}\eta^{\mu\nu}=0$. Thus we have $\sum_{\mu=0}^{l-1}\operatorname{tr}_j\varsigma^{r(\mu)}\equiv 0\pmod{l}$. Moreover, from $(*)$ we have $\operatorname{tr}_j\varsigma^{r(\mu)d}=\operatorname{tr}_j\varsigma^{r(0)d}$ for all μ and all $d|n$, $d\neq 1$.

Recall that $t_1 = O(j) \bmod n$. Let us write the class sum of $a^{r(\mu)}$ in G: $C_\mu = \sum_{\nu=0}^{t_1-1} a^{r(\mu)j^\nu}$, and $\alpha = \sum_{\mu=0}^{l-1} C_\mu$. Then we have

$$\alpha(\varsigma) = \sum_{\mu=0}^{l-1} C_\mu(\varsigma) = \sum_{\mu=0}^{l-1}\sum_{\nu=0}^{t_1-1} \varsigma^{r(\mu)j^\nu} = \sum_{\mu=0}^{l-1} \mathrm{tr}_j \varsigma^{r(\mu)} \equiv 0 \pmod{l},$$

$$\alpha(\varsigma^d) = \sum_{\mu=0}^{l-1} \mathrm{tr}_j \varsigma^{dr(\mu)} = l\ \mathrm{tr}_j \varsigma^{r(0)d} \equiv 0 \pmod{l},$$

$$\alpha(1) \equiv 0 \pmod{l}.$$

Thus in the embedding $\mathbf{Z}\langle a\rangle \to \sum_{d|n} \mathbf{Z}[\varsigma_d] = R$, the image of α is $\equiv 0 \pmod{l}$. But we know by [**2**, p. 379] that $O(a)R \subseteq \mathbf{Z}\langle a\rangle$. Since we have $(O(a), l) = 1$, it follows that $\alpha \equiv 0 \pmod{l}$. Therefore, $C_\mu = C_0$ for all μ.

We have proved that $\mathrm{tr}_j \varsigma^{r(\mu)} = \mathrm{tr}_j \varsigma^{r(0)}$, $\chi_{1,\mu}(u) = \chi_{1,\mu}(a^{r(0)})$. Thus $\chi_{d,\mu}(u) = \chi_{d,\mu}(a^{r(0)})$ for all d, μ. Repeating this for all powers u^k of u we have

$$\chi_{d,\mu}(u^k) = \chi_{d,\mu}(a^{r(0)k}) \quad \text{for all } d, \mu.$$

Hence $u \sim a^{r(0)}$ and the proof is complete.

REFERENCES

1. C. Polcino Milies and S. K. Sehgal, *Torsion units in integral group rings of metacyclic groups*, J. Number Theory **19** (1984), 103–114.
2. I. Reiner, *Maximal orders*, Academic Press, New York, 1975.
3. J. Ritter and S. K. Sehgal, *On a conjecture of Zassenhaus on torsion units in integral group rings*, Math. Ann. **264** (1983), 257–270.
4. ——, *Isomorphism of group rings*, Arch. Math. **40** (1983), 32–39.
5. J. P. Serre, *Linear representations of finite groups*, Graduate Texts in Math., Vol. 42, Springer-Verlag, New York, 1977.

DEPARTMENT OF MATHEMATICS, UNIVERSIDADE DE SAO PAULO, CAIXA POSTAL 20570, SAO PAULO, BRASIL

DEPARTMENT OF MATHEMATICS, UNIVERSITÄT AUGSBURG, D-8900 AUGSBURG, WEST GERMANY

DEPARTMENT OF MATHEMATICS, 632 CENTRAL ACADEMIC BUILDING, UNIVERSITY OF ALBERTA, EDMONTON, ALBERTA, CANADA T6G 2G1