Nova Série
BOLETIM
DA SOCIEDADE BRASILEIRA DE MATEMÁTICA

Bol. Soc. Bras. Mat., Vol. 20, No. 2, 87-93

On the generators of subgroups of unit groups of group rings

Ashwani K. Bhandari

Abstract. In this paper we find the generators of a subgroup of finite index in the unit group of the integral group ring of the metacyclic group of order pq given by

$$G = \langle a, x : a^p = 1 = x^q, xax^{-1} = a^f \rangle,$$

where p is an odd prime, $q \geq 2$ a divisor of $p-1$, and f belongs to the exponent q modulo p.

Results

Let $U = U_1(\mathbb{Z}G)$ be the group of units, having augmentation one, of the integral group ring $\mathbb{Z}G$ of a finite group G. It is a difficult problem to find generators of U. It might be easier to do the same for a subgroup of finite index. This note is a contribution towards the latter problem when G is the metacyclic group of order pq given by

$$G = \langle a, x : a^p = 1 = x^q,\ xax^{-1} = a^f \rangle,$$

where p is an odd prime, $q \geq 2$ a divisor of $p-1$ and where f belongs to the exponent q mod p.

Let $k = \mathbf{Q}(\varsigma)$ with $\varsigma = e^{2\pi i/p}$, and let k_0 be the fixed field of the automorphism $\phi : \varsigma \mapsto \varsigma^f$ of k. We denote by $\mathfrak{o}$ and $\mathfrak{o}_0$ the rings of integers of k and k_0 respectively. Let $\Pi = \varsigma - 1$ be the prime in $\mathfrak{o}$ above the rational prime p. The prime in $\mathfrak{o}_0$ above p is $\Pi_0 = (\varsigma - 1)(\varsigma^f - 1)\ldots(\varsigma^{f^{q-1}} - 1)$. We recall that $\mathfrak{o}/\Pi\ \mathfrak{o} = \mathbb{Z}/p\mathbb{Z} = \mathfrak{o}_0/\Pi_0\mathfrak{o}_0$.

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

$$m = m(a,x) = m_1(a) + m_2(a)x + \cdots + m_q(a)x^{q-1}$$

Received 15 May 1988.

where $m_i(T)$ are polynomials with rational integral coefficients. It is clear that the numbers $m_i(1)$ and $m_i(\varsigma)$ depend only on m and that two elements m and n of $\mathbb{Z}G$ are equal if and only if $m_i(1) = n_i(1)$ and $m_i(\varsigma) = n_i(\varsigma)$ for $1 \le i \le q$.

Let C denote the cyclic group generated by x and let N be the kernel of the homomorphism $U_1(\mathbb{Z}G) \to U_1(\mathbb{Z}C)$ which maps the unit $m(a,x)$ to $m(1,x)$; an element m of $U_1(\mathbb{Z}G)$ is in N if and only if

$$m_1(1) = 1,\ m_2(1) = 0,\ \dots,\ m_q(1) = 0.$$

It is clear that $U_1(\mathbb{Z}G)$ is the semidirect product of N and $U_1(\mathbb{Z}C)$.

We put

$$P = \begin{pmatrix} 1 & \Pi & \dots & \Pi^{q-1} \\ 1 & \phi(\Pi) & \dots & \phi(\Pi^{q-1}) \\ & & \dots & \\ 1 & \phi^{q-1}(\Pi) & \dots & \phi^{q-1}(\Pi^{q-1}) \end{pmatrix}$$

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

$$X \equiv \begin{pmatrix} 1 & 0 \\ & \\ * & 1 \end{pmatrix} \quad \bmod \Pi_0$$

If $\alpha_1, \alpha_2, \dots \alpha_q$ are elements of k, we put

$$\operatorname{circ}_\phi(\alpha_1, \alpha_2, \dots, \alpha_q) = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_q \\ \phi(\alpha_q) & \phi(\alpha_1) & \dots & \phi(\alpha_{q-1}) \\ & & \dots & \\ \phi^{q-1}(\alpha_2) & \phi^{q-1}(\alpha_3) & \dots & \phi^{q-1}(\alpha_1) \end{pmatrix}$$

As shown in [3], Lemma 1.4, the mapping

$$\psi : m \mapsto P^{-1} \operatorname{circ}_\phi(m_1(\varsigma),\ m_2(\varsigma), \dots, m_q(\varsigma))P$$

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

For $1 \le i \le q-1$, we shall denote by $S_i(t_1, t_2, \dots, t_{q-1})$ the ith symmetric

function in $t_1, t_2, \dots, t_{q-1}$, and we put $S_0(t_1, t_2, \dots, t_{q-1}) = 1$. We put

$$\delta(T) = \prod_{i=1}^{q-1}(T - \phi^i(\Pi)) = T^{q-1} + \delta_1 T^{q-2} + \dots + \delta_{q-1}$$

with $\delta_i = (-1)^i S_i(\phi(\Pi), \phi^2(\Pi), \dots \phi^{q-1}(\Pi))$, and let $\delta = \prod_{i=1}^{q-1}(\Pi - \phi^i(\Pi))$. One checks easily that the matrix P has the inverse

$$P^{-1} = \begin{pmatrix} \delta_{q-1}/\delta & \phi(\delta_{q-1}/\delta) & \dots & \phi^{q-1}(\delta_{q-1}/\delta) \\ \delta_{q-2}/\delta & \phi(\delta_{q-2}/\delta) & \dots & \phi^{q-1}(\delta_{q-2}/\delta) \\ & & \dots & \\ \delta_0/\delta & \phi(\delta_0/\delta) & \dots & \phi^{q-1}(\delta_0/\delta) \end{pmatrix}$$

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

For an algebraic number field L with ring of integers $\mathfrak{o}_L$, we denote by $SL_n(\mathfrak{o}_L)$ the subgroup of $GL_n(\mathfrak{o}_L)$ consisting of all matrices with determinant 1. For an ideal Q of $\mathfrak{o}_L$ we denote by $E_n(Q)$ the subgroup of $SL_n(\mathfrak{o}_L)$ generated by all Q-elementary matrices $I + \alpha e_{ij}$, $\alpha \in Q$, $i \neq j$, and e_{ij} a matrix unit, and by $\widetilde{E}_n(Q)$ its normal closure in $SL_n(\mathfrak{o}_L)$. We need the following result due to Bass [2] and Vaserstein [7] and [8] (see also [6] and [5]).

Lemma 1.

(i) *If $n \ge 3$, then $\widetilde{E}_n(Q^2) \subset E(Q)$, in particular $[SL_n(\mathfrak{o}_L) : E_n(Q)] < \infty$.*

(ii) *If $n = 2$ and if L is not rational or imaginary quadratic field, then $[SL_2(\mathfrak{o}_L) : E_2(Q)] < \infty$.*

We put

$$\mathcal{W}_1 = \{u_\mu | 2 \le \mu \le \frac{p-1}{2}\},$$

with

$$u_\mu = (1 + a + \dots + a^{\mu-1})^{p-1} + \frac{1-\mu^{p-1}}{p}(1 + a + \dots + a^{p-1}).$$

If $p = 3$, we put $\mathcal{W}_1 = \{1\}$. For any divisor $d > 2$ of q, fix an element $x_d \in \langle x \rangle$ of order d. Let

$$\mathcal{W}_{2,d} = \{v_{d,\mu} | 2 \le \mu < \frac{d}{2}, (\mu, d) = 1\},$$

with

$$v_{d,\mu} = (1 + x_d + \cdots + x_d^{\mu-1})^{\varphi(q)} + \frac{1-\mu^{\varphi(q)}}{d}(1 + x_d + \cdots + x_d^{d-1}),$$

where φ is the Euler φ-function and let $\mathcal{W}_2 = \bigcup_{\substack{d|q \\ d>2}} \mathcal{W}_{2,d}$. If $q \leq 3$, we put $\mathcal{W}_2 = \{1\}$.

Let $\bar{R} = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$ be the reduced residue system modulo p, and let $\bar{R}_f = \{\bar{r}_1, \bar{r}_2, \ldots, \bar{r}_{p-1/q}\}$ be the coset representatives in $\bar{R}$ of the group generated by $\bar{f}$. Let $\mathcal{R} = \{0 = r_0, r_1, r_2, \ldots, r_{p-1/q}\}$.

We denote by σ the automorphism of the cyclic group $\langle a\rangle$ given by $\sigma(a) = a^f$.

For each $r \in \mathcal{R}$ and for $1 \leq i, j \leq q$, $i \neq j$, $1 \leq \omega \leq q$, we define the elements $A_{i,j,r}^{(\omega)}$ of the group ring $\mathbb{Z}\langle a\rangle$ by

$$A_{i,j,r}^{(\omega)} = (-1)^{q-j}\sum_{t=0}^{q-1}\sigma^t(a^r)\cdot\Big(\prod_{\substack{s=0 \\ s\neq\omega-1}}^{q-1}\prod_{\ell=1}^{q-1}(\sigma^s(a) - \sigma^{s+\ell}(a))\Big) \times$$

$$\times\,(a-1)^{i-1}S_{q-j}(\sigma^\omega(a)-1,\ \sigma^{\omega+1}(a)-1, \ldots, \sigma^{\omega+q-2}(a)-1).$$

By $A_{i,j,r}^{(\omega)}(\varsigma)$ we shall mean the complex number obtained on replacing a by ς in the expression (as a polynomial in a) for $A_{i,j,r}^{(\omega)}(a)$.

We have

Theorem 2. *Let $\mathcal{W} = \mathcal{W}_1 \cup \mathcal{W}_2 \cup \mathcal{W}_3$, where $\mathcal{W}_1$ and $\mathcal{W}_2$ are as defined above and where*

$$\mathcal{W}_3 = \{u_{i,j,r} | 1 \leq i,\ j \leq q,\ i \neq j;\ r \in \mathcal{R}\},$$

with

$$u_{i,j,r} = 1 + A_{i,j,r}^{(1)}(a) + \sum_{\omega=2}^{q} A_{i,j,r}^{(\omega)}(a)x^{\omega-1},$$

and where $A_{i,j,r}^{(\omega)}$ are defined as above. Then the group generated by $\mathcal{W}$ is a subgroup of finite index in $U_1(\mathbb{Z}G)$.

Proof. The main observation in the proof of the theorem is that the images (under ψ) of elements of $\mathcal{W}_3$ in $\mathcal{X}$ are elementary matrices, which, in view of Lemma 1, ... a subgroup of finite index in $\mathcal{X}$.

For each $r \in \mathcal{R}$ and for $1 \leq i, j \leq q$, $i \neq j$, let $X_{i,j,r} = I + b_r e_{ij}$ be the elementary matrix with $b_r = Tr_{k|k_0}(\varsigma^r)Nr_{k|k_0}(\delta) \in \mathfrak{o}_0$ and e_{ij} the matrix unit. Then each $X_{i,j,r} \in \mathcal{X}$. Since $\psi : N \to \mathcal{X}$ is an isomorphism, there exist a unit $n_{i,j,r} \in N$ such that $\psi(n_{i,j,r}) = X_{i,j,r}$ and

$$n_{i,j,r} = n_{i,j,r}^{(1)}(a) + n_{i,j,r}^{(2)}(a)x + \cdots + n_{i,j,r}^{(q)}(a)x^{q-1},$$

with $n_{i,j,r}^{(1)}(1) = 1$, $n_{i,j,r}^{(2)}(1) = 0, \ldots, n_{i,j,r}^{(q)}(1) = 0$. Also, by the definition of the map ψ it follows that $n_{i,j,r}^{(\omega)}(\varsigma)$, $1 \leq \omega \leq q$, is the ωth element of the first row of the matrix $PX_{i,j,r}P^{-1}$.

Now, observe that

$$PX_{i,j,r}P^{-1} = \Big(\sum_{\mu=1}^{q}\sum_{\lambda=1}^{q}\phi^{\lambda-1}(\Pi^{\mu-1})e_{\lambda\mu}\Big)(I + b_r e_{ij})\Big(\sum_{\varepsilon}\sum_{\omega}\phi^{\omega-1}(\delta_{q-\varepsilon}/\delta)e_{\varepsilon\omega}\Big)$$

$$= (I + \sum_{\lambda=1}^{q} b_r\phi^{\lambda-1}(\Pi^{i-1})e_{\lambda j})(\sum_{\varepsilon}\sum_{\omega}\phi^{\omega-1}(\delta_{q-\varepsilon}/\delta)e_{\varepsilon\omega})$$

$$= I + \sum_{\lambda=1}^{q}\sum_{\omega=1}^{q} b_r\phi^{\lambda-1}(\Pi^{i-1})\phi^{\omega-1}(\delta_{q-j}/\delta)e_{\lambda\omega}.$$

Thus

$$n_{i,j,r}^{(1)}(\varsigma) = 1 + b_r\Pi^{i-1}\delta_{q-j}/\delta = 1 + Tr_{k|k_0}(\varsigma^r)\cdot Nr_{k|k_0}(\delta)\Pi^{i-1}\delta_{q-j}/\delta$$

and for $2 \leq \omega \leq q$.

$$n_{i,j,r}^{(\omega)}(\varsigma) = b_r\Pi^{i-1}\phi^{\omega-1}(\delta_{q-j}/\delta) = Tr_{k|k_0}(\varsigma^r)Nr_{k|k_0}(\delta)\Pi^{i-1}\phi^{\omega-1}(\delta_{q-j}/\delta).$$

It follows from the above that $1 + A_{i,j,r}^{(1)}(\varsigma) = n_{i,j,r}^{(1)}(\varsigma)$ and for $2 \leq \omega \leq q$, $A_{i,j,r}^{(\omega)}(\varsigma) = n_{i,j,r}^{(\omega)}(\varsigma)$. Moreover, $A_{i,j,r}^{(\omega)}(1) = 0$ for $1 \leq \omega \leq q$ and for each i, j and r. Thus, for each $r \in \mathcal{R}$ and for $1 \leq i, j \leq q, i \neq j$, $u_{i,j,r} = n_{i,j,r}$ are elements of N and $\psi(u_{i,j,r}) = X_{i,j,r} = I + b_r e_{ij}$.

Since the $\mathbb{Z}$-linear combinations of $b_r, r \in \mathcal{R}$ form an ideal Q of $\mathfrak{o}_0$, it follows that the elements of $\mathcal{W}_3$ generate a subgroup of N which is isomorphic to $E_q(Q)$, the subgroup of $SL_q(\mathfrak{o}_0)$ generated by all Q-elementary matrices. We observe that in case $q = 2, k_0$ is the maximal real subfield of $k = \mathbf{Q}(\varsigma)$. Hence, by Lemma 1, $[SL_q(\mathfrak{o}_0) \cap \mathcal{X} : E_q(Q)] < \infty$.

The centre $\mathcal{Z}(\mathcal{X})$ of $\mathcal{X}$ consists of all matrices of the type

$$\begin{pmatrix} u_0 & 0 & \dots & 0 \\ 0 & u_0 & \dots & 0 \\ & & \dots & \\ 0 & 0 & \dots & u_0 \end{pmatrix}$$

where u_0 is a unit of $\mathfrak{o}_0$ and $u_0 \equiv 1 \pmod{\Pi_0}$. Hence $\mathcal{Z}(\mathcal{X})$ is isomorphic to the group $U_1(\mathfrak{o}_0)$ consisting of those units which are congruent to 1 module Π_0. Also, it follows (from the isomorphism ψ) that $\mathcal{Z}(\mathcal{X}) \subset U_1(\mathbb{Z}\langle a\rangle)$. Since by [1], Theorem 4, (or see [4], page 156) the elements of $\mathcal{W}_1$ generate a subgroup of finite index in $U_1(\mathbb{Z}\langle a\rangle)$, the group generated by $\mathcal{W}_1$ contains a subgroup isomorphic under ψ to a subgroup of finite index in $\mathcal{Z}(\mathcal{X})$. Also, $[\mathcal{X} : (SL_q(\mathfrak{o}_0) \cap \mathcal{X})\mathcal{Z}(\mathcal{X})] < \infty$, as the determinant map induces an embedding $\mathcal{X}/(SL_q(\mathfrak{o}_0) \cap \mathcal{X})\mathcal{Z}(\mathcal{X}) \longrightarrow U_1(\mathfrak{o}_0)/(U_1(\mathfrak{o}_0))^q$, we get that $\mathcal{W}_1 \cup \mathcal{W}_3$ generate a subgroup of finite index in N. Finally, since $\mathcal{W}_2$ generate a subgroup of finite index in $U_1(\mathbb{Z}C)$ ([1], Theorem 4), and since N is a normal subgroup of $U_1(\mathbb{Z}C)$, therefore, the group generated by $\mathcal{W} = \mathcal{W}_1 \cup \mathcal{W}_2 \cup \mathcal{W}_3$ is of finite index in $U_1(\mathbb{Z}G)$. □

Example 3. Let G be the group of order 21 given by

$$G = \langle a, x : a^7 = 1 = x^3,\ xax^{-1} = a^2\rangle.$$

Then $\mathcal{W}_3$ consists of 18 elements given for $1 \le i, j \le 3$, $i \ne j$; $r = 0, 1, 3$, by

$$\begin{aligned} u_{i,j,r} = {} & 1+(-1)^{j+1}(a^r+a^{2r}+a^{4r})(a-1)^{i-1}[((a^2-a^4)(a^2-a)(a^4-a)\times \\ & \times (a^4-a^2)S_{3-j}(a^2-1, a^4-1) + (a-a^2)(a-a^4)(a^4-a)(a^4-a^2)\times \\ & \times S_{3-j}(a^4-1, a-1)x + (a-a^2)(a-a^4)(a^2-a^4)(a^2-a)\times \\ & \times S_{3-j}(a-1, a^2-1)x^2]. \end{aligned}$$

$\mathcal{W}_1$ consists of 2 elements

$$\begin{aligned} u_1 &= (1+a)^6 - 9(1+a+\dots+a^6) \\ &= -8 - 3a + 6a^2 + 11a^3 + 6a^4 - 3a^5 - 8a^6 \end{aligned}$$

and

$$\begin{aligned} u_2 &= (1+a+a^2)^6 - 104(1+a+\dots+a^6) \\ &= 23 - 8a - 33a^2 - 33a^3 - 8a^4 + 23a^5 + 37a^6, \end{aligned}$$

and $\mathcal{W}_2$ consists of the element 1. These 21 elements generate a subgroup of finite

index in $U_1(\mathbb{Z}G)$.

Acknowledgments

I am indebted to S.K. Sehgal for suggesting this problem, and for several helpful discussions.

References

1. H. Bass, *The Dirichlet unit theorem, induced characters and Whitehead groups of finite groups*, Topology **4** (1966), 391–410.
2. ———, *K-Theory and stable algebra*, Publ. Math. I.H.E.S. **22** (1964), 5–60.
3. A.K. Bhandari and I.S. Luthar, *Torsion units of integral group rings of metacyclic groups*, J. Number Theory **17** (1983), 270–283.
4. G. Karpilovsky, "Commutative Group Algebras," Marcel Dekker, Inc., 1983.
5. B. Liehl, *On the subgroup SL_2 over orders of arithmetic type*, J. Reine Angew. Math. **323** (1981), 153–171.
6. U. Rehmann, *A survey of the congruence subgroup problem in Algebraic K-Theory*, Springer Lecture notes in Math **966** (1982), 197–207.
7. L.N. Vaserstein, *On the subgroup SL_2 over Dedekind rings of arithmetic type*, Math USSR Sbornik **18** (1972), 321–332.
8. ———, *The structure of classical arithmetic groups of rank greater than one*, Math. USSR Sbornik **20** (1973), 465–492.

Ashwani K. Bhandari
Department of Mathematics
Panjab University
Chandigarh - 160 014
India