Resenhas IME-USP 1993, Vol. 1, No. 1, 116 - 123.

LARGE GROUPS OF UNITS OF INTEGRAL GROUP RINGS OF FINITE NILPOTENT GROUPS

SUDARSHAN K. SEHGAL

Abstract: This paper surveys recent results regarding large subgroups of units in integral group rings of nilpotent groups, exibiting families of generators in several cases.

Key words: Integral Group Ring, Group of Units, Large Subgroups, Congruence Subgroup Theorem.

§1. Introduction

Let G be a finite group and $U(\mathbb{Z}G)$ the group of units of the integral group ring $\mathbb{Z}G$. It is an interesting and difficult question to describe $U(\mathbb{Z}G)$ by giving generators and relations. But this is to be expected as it is not possible even to find fundamental units in rings of algebraic integers. So as in number theory one should be satisfied to find generators upto finite index of $U(\mathbb{Z}G)$. We report in this note on the recent progress on the problem for the case of nilpotent groups G. In the next section we record the various recipes for construction of units and in the third section we state the results.

§2. Examples

(2.1) Trivial units. Of course, the elements $\pm g$, $g \in G$ are invertible in $\mathbb{Z}G$. They are called trivial units.

(2.2) Bass cyclic units. To introduce our second example we recall the notion of "cyclotomic units." These are elements of $\mathbb{Z}[\zeta]$ where ζ is a primitive nth root of unity and are of the form

$$\alpha = 1 - \zeta^i/1 - \zeta = 1 + \zeta + \cdots + \zeta^{i-1} \quad \text{where} \quad (i,n) = 1.$$

The inverse of α is given by

$$1 - \zeta/1 - \zeta^i = 1 - \zeta^{ij}/1 - \zeta^i = 1 + \zeta^i + \zeta^{2i} + \cdots + \zeta^{(j-1)i} \in \mathbb{Z}[\zeta]$$

where $ij \equiv 1 \pmod{n}$.

Now let a be an element of order n in a group G. Then the element of $\mathbb{Z}\langle a\rangle$ analogous to a cyclotomic unit, namely, $\beta = 1 + a + \cdots + a^{i-1}$, $(i,n) = 1$ is not invertible in $\mathbb{Z}\langle a\rangle$ as the augmentation $\varepsilon(\beta) = i > 1$. Remember that the augmentation map $\varepsilon(\Sigma c_i g_i) = \Sigma c_i \in \mathbb{Z}$ is a ring homomorphism and as such ε (unit) is ± 1. We need to be a little more clever.

The rational group algebra $\mathbb{Q}\langle a\rangle$ is a direct sum of fields:

$$\mathbb{Q}\langle a\rangle \cong \sum_{d|n}^{\oplus} \mathbb{Q}(\zeta^d)$$

as can be seen by the isomorphism $a \to \sum^{\oplus}\zeta^d$. Clearly, $\mathbb{Z}\langle a\rangle$ injects into $\sum_{d|n}^{\oplus} \mathbb{Z}[\zeta^d] =$ IM, the unique maximal order. Since $\mathbb{Z}\langle a\rangle \subset$ IM are orders, an element of $\mathbb{Z}\langle a\rangle$ is a unit if and only if it has an inverse in IM (see [11, p. 19]). Thus to check if an element of $\mathbb{Z}\langle a\rangle$ is a unit it suffices to produce its inverse in IM. Let us consider the element β above. Its image under any projection $\mathbb{Z}\langle a\rangle \to \mathbb{Z}[\zeta^d]$ is a cyclotomic unit except when $d = n$. Thus we need to modify β to go around the augmentation obstruction. For technical reasons, let k be a fixed multiple of $|G|$ and $\varphi(|G|)$ with φ denoting Euler's function. Since $(i, n) = 1$, $i^{\varphi(n)} \equiv 1 \pmod{n}$ and so $i^k \equiv 1 \pmod{n}$. Then the element

$$u = (1 + a + \cdots + a^{i-1})^k + (1 - i^k/n)\,\widehat{a}, \quad \widehat{a} = \sum_1^n a^i$$

belongs to $\mathbb{Z}\langle a\rangle$. Moreover, $\varepsilon(u) = 1$, u is invertible in IM and hence $u \in U(\mathbb{Z}\langle a\rangle)$. These units are called *Bass cyclic units* of $\mathbb{Z}G$. We denote by $\mathcal{B}_1 = \mathcal{B}_1(G)$ the group generated by them.

(2.3) Hoechsmann units. Again let $C = \langle a\rangle$ be of order n. We modified the element $\beta = 1 + a + \cdots + a^{i-1}$, $(i, n) = 1$ to obtain the Bass cyclic unit. One could take a quotient of two elements of equal augmentation. In this spirit let

$$v = 1 + a^j + \cdots + a^{j(i-1)}/1 + a + \cdots + a^{(i-1)}, \quad (i, n) = 1,\ (j, n) = 1$$

be an element of $\mathbb{Q}\langle a\rangle$. It is easily seen that $v(\zeta^d)$ is a unit of $\mathbb{Z}[\zeta^d]$ for all $d|n$. Thus v is a unit of IM. In fact,

$$v = (1 + a^j + \cdots + a^{j(i-1)})(1 + a^i + \cdots + a^{(\ell-1)i}) + (1 - i\ell/n)\widehat{a}$$

where $i\ell \equiv 1 \pmod{n}$ is an element of $\mathbb{Z}\langle a\rangle$ (see [11, p. 34]). Hence v is a unit of $\mathbb{Z}\langle a\rangle$. All these units are called *Hoechsmann units* and we denote by $\mathcal{H}(C)$ the group generated by them. It is known that $\mathcal{H}(C)$ contains $\mathcal{B}_1(C)$.

(2.4) Alternating units. If n is odd it is possible to fix the augmentation difficulties in a straight forward manner. Let $(i, 2n) = 1$ then

$$u = 1 - a + a^2 - \cdots + a^{i-1}$$

clearly has augmentation equal to one. Moreover, $u(\zeta) = 1-\zeta+\zeta^2+\cdots+\zeta^{i-1} = 1-\zeta+(-\zeta)^2+\cdots+(-\zeta)^{i+1}$ is a cyclotomic unit. Thus u is a unit of $\mathbb{Z}C$. We call these type of units alternating units and denote the group generated by them by $\mathcal{A}(C)$.

(2.5) The group $\mathcal{C}_1$. Before introducing these units, which have only one non-identity component in the decomposition

$$\mathbb{Q}C = \mathbb{Q}\langle a\rangle = \sum_{d|n}^{\oplus} \mathbb{Q}(\zeta^d), \qquad (*)$$

we recall the formulae for the primitive idempotents of $\mathbb{Q}C$. Let $\langle d\rangle$ be the Sylow p-subgroup of C for a prime dividing n. Then it can be checked directly that the primitive idempotents of $\mathbb{Q}\langle d\rangle$ are given by

$$e_{p0} = \hat{d}, \quad e_{p1} = \hat{d^p} - \hat{d}, \ldots, e_{pn_p} = \hat{d^\ell} - 1$$

with $n = \prod_p p^{n_p}$ and $\ell = p^{n_p-1}$. It follows that the primitive idempotents of $\mathbb{Q}C$ are given by $e = \prod_p e_{pi_p}$, $0 \le i_p \le n_p$.

Let $\alpha \in \mathbb{Z}\langle a\rangle$ and $e = e^2 \in \mathbb{Q}\langle a\rangle$ be a primitive idempotent as described above. Then in the decomposition $(*)$ we have

$$\begin{aligned} \alpha e &= (0,\ldots,0,\overline{\alpha},0,\ldots,0),\\ 1-e &= (1,\ldots,1,0,1,\ldots,1),\\ \alpha e+(1-e) &= 1+(\alpha-1)e = (1,\ldots,1,\overline{\alpha},1,\ldots,1). \end{aligned}$$

Let us specialize α to elements of the form $1+a+\cdots+a^{i-1}$, $(i,n)=1$. Then $1+(\alpha-1)e$ is a unit of the maximal order IM. It follows from [7, p. 379] that $nM \subseteq \mathbb{Z}\langle a\rangle$ and thus there is a fixed number k depending only on n so that $\big(1+(\alpha-1)e\big)^k \in U\mathbb{Z}\langle a\rangle$ (see [11, p. 19]). It is easy to prove that $\mathcal{C}_1 = \langle \big(1+(\alpha-1)e\big)^k : \alpha = 1+a+\cdots+a^{i-1}, (i,n)=1\rangle$ is a subgroup of finite index in $U\mathbb{Z}\langle a\rangle$.

We have given some recipes for writing down explicitly units in some abelian group rings. The next example is a noncommutative one.

(2.6) Bicyclic units. Let $a, b \in G$ then $(a-1)\hat{a} = \hat{a}(a-1) = 0$. Consider the element $\eta = (a-1)b\hat{a}$. It is nilpotent, in fact, $\eta^2 = 0$. Thus $(1+\eta)(1-\eta) = 1$. We have found units

$$u_{a,b} = 1+(a-1)b\hat{a}, \quad a,\ b \in G.$$

Similary, $u'_{a,b} = 1+\hat{a}\,b(a-1)$ is also invertible. We call $\mathcal{B}_2 = \langle u_{a,b} : a,b \in G\rangle$ the group of bicyclic units. We set $\mathcal{B}'_2 = \langle u'_{a,b} : a,b \in G\rangle$. Clearly, $u_{a,b} = 1$ if and

only if b normalizes $\langle a\rangle$. Thus $\mathcal{B}_2 = 1$ if and only if all subgroups of G are normal in G. A nonabelian group with this property is called Hamiltonian. It turns out that a Hamiltonian group can be written as $K_8 \times E \times O$ where $E^2 = 1, O$ is an odd abelian group and K_8 is the quaternion group of order 8. In this situation there are other useful units.

(2.7) **The group $\mathcal{B}_3$.** These units can be constructed whenever G has a homomorphic image $K_8 \times C_p$, with p an odd prime and $\mathbb{Q}(K_8 \times C_p)$ contains nilpotent elements. For simplicity, we shall illustrate only the case $G = K_8 \times C_p$. We have $K_8 = \langle a, b : a^2 = b^2 = z,\ a^b = a^{-1}\rangle$. Let

$$\text{Ш}(\mathbb{Q}) = \mathbb{Q} \dot{+} \mathbb{Q}i \dot{+} \mathbb{Q}j \dot{+} \mathbb{Q}k$$

be the rational Hamiltonian (skew) field. Then

$$\mathbb{Q}K_8 = 4\ \mathbb{Q} \oplus \text{Ш}(\mathbb{Q}).$$

Moreover,

$$\begin{aligned}\mathbb{Q}(K_8 \times C_p) &= (4\ \mathbb{Q} \oplus \text{Ш}(\mathbb{Q})) \otimes (\mathbb{Q} \oplus \mathbb{Q}(\zeta_p)) \\ &= 4\ \mathbb{Q} \oplus 4\ \mathbb{Q}(\zeta_p) \oplus \text{Ш}(\mathbb{Q}) \oplus \text{Ш}(\mathbb{Q}(\zeta_p))\end{aligned}$$

where ζ_p is a primitive pth root of unity. We have assumed that $\text{Ш}(\mathbb{Q}(\zeta_p))$ splits. Therefore, it is possible to find explicitly $x',\ y' \in \mathbb{Z}[\zeta_p]$ so that $x'^2 + y'^2 = -1$. Let x, y be chosen in $\mathbb{Z}(C_p)$ so that $x(\zeta_p) = x',\ y(\zeta_p) = y'$. Let e be the idempotent corresponding to $\text{Ш}(\mathbb{Q}(\zeta_p))$. Then e is given by $e = \frac{1-z}{2} \cdot (1 - \hat{c})$ where $\langle c\rangle = C_p$. Furthermore, $(x^2 + y^2 + 1)e = 0$. Define $\eta = |G|(ya + b + xab)e,\ \eta' = |G|(ya - b + xab)e$. Then

$$\eta^2 = |G|^2(xy(1+z)b + y(1+z)ab + x(1+z)a)e = 0.$$

Similarly, $(\eta')^2 = 0$. Therefore, $(\eta\, \mathbb{Z}G\eta)^2 = 0 = (\eta'\mathbb{Z}G\eta')^2$. We have units $1 + \eta x \eta$ and $1 + \eta' x \eta',\ x \in \mathbb{Z}G$. We define

$$\mathcal{B}_3 = \langle 1 + \eta g \eta,\ 1 + \eta' g \eta',\ g \in G\rangle.$$

These units can be extended to the general situation (see [3]).

§3. Generators of Large Subgroups

We shall say that a subgroup is large if it is of finite index. In many cases it is possible to find very nice explicit generators of large subgroups of $U(\mathbb{Z}G)$. We shall present these results below. We begin with a classical result of Graham Higman [1].

Theorem (3.1). *Let A be a finite abelian group of order n. Then $U(\mathbb{Z}A) = \pm A \times F$ where F is free of rank $\rho = \frac{1}{2}(n + 1 + n_2 - 2\ell)$ with n_2 denoting the number of elements of order 2 in G and ℓ the number of cyclic subgroups of G.*

Proof. See [10, p. 54].

Corollary (3.2). *All units of $\mathbb{Z}A$ are trivial if and only if $A^4 = 1$ or $A^6 = 1$.*

Now let C be cyclic of order n then H. Bass [1] has proved

Theorem (3.3). *The subgroup $\mathcal{B}_1$ of the Bass cyclic units in $\mathbb{Z}C$ is free and of finite index in $U(\mathbb{Z}C)$.*

Proof. See [1] or [11, p. 45].

We shall see now that this solves the problem for the abelian case. Let $\mathcal{M}(A) = \prod_{C \subseteq A} \mathcal{B}_1(C)$ denote the product of the Bass cyclic units where C runs over the cyclic subgroups of the finite abelian group A. We have

Theorem (3.4) (Bass-Milnor). *$\mathcal{M}(A)$ is of finite index in $U(\mathbb{Z}A)$ and the product is direct.*

Proof. See [11, p. 63].

The above result says, in particular, that the units of cyclic subgroups generate a large subgroup of $U\,\mathbb{Z}A$. In fact, more is true.

Theorem (3.5) (Bass-Milnor). *Let G be a finite group. The image of $\langle U(\mathbb{Z}C)\rangle_{C \subseteq G}$ under the natural map $j : U(\mathbb{Z}G) \to K_1(\mathbb{Z}G)$ as C runs over the cyclic subgroups of G is of finite index.*

Proof. See [1].

A straight forward extension of (3.4), namely, $\big(U(\mathbb{Z}G) : \langle U(\mathbb{Z}C)\rangle_{C \subseteq A}\big) < \infty$ is not true as seen by the following example.

Example (3.6). Let $G = \langle a^3 = 1 = b^2 : a^b = a^{-1}\rangle$ be the symmetric group on three letters. Then every cyclic subgroup of G has order $1, 2$ or 3. Thus $U(\mathbb{Z}C) = \pm C$ for all $C \subseteq G$. Thus $\langle U(\mathbb{Z}C)\rangle_{C \subseteq G} = \pm G$ whereas $U(\mathbb{Z}G)$ contains elements of infinite order, for example, $u_{b,a} = 1 + (b-1)a(b+1)$.

However, if one considers the normal subgroup of $U(\mathbb{Z}G)$ generated by all $U(\mathbb{Z}C)$ then we do get a subgroup of finite index as was proved by Kleinert [6].

Theorem (3.7) (Kleinert). *But for a few exceptions, we have that the normal closure of* $\langle U\ \mathbb{Z}C\rangle_{C\subseteq G}$ *in* $U(\mathbb{Z}G)$ *is of finite index in* $U(\mathbb{Z}G)$.

Proof. See [11, p. 116].

The exceptions referred to above arise from the failure of the congruence subgroup theorem. We shall discuss this soon. Let us establish some notation first.

Let

$$\mathbb{Q}G = S_1 \oplus \cdots \oplus S_t$$

be the decomposition of $\mathbb{Q}G$ into its simple Wedderburn components and let π_i be the projections. We identify S_i with $(D_i)_{n_i\times n_i}$, the ring of $n_i \times n_i$ matrices over the division ring D_i. Suppose $n_i \geq 2$. Let $\mathcal{O}_i$ be a maximal order in D_i and $\mathfrak{p}$ an ideal in $\mathcal{O}_i$. Let $E(\mathfrak{p})$ be the $\mathfrak{p}$-elementary matrices and SL_i the matrices of reduced norm one contained in $(\mathcal{O}_i)_{n_i\times n_i}$. We shall assume that in our case, G satisfies the following conditions:

(i) $(SL_i : E(\mathfrak{p})) < \infty$ for all $\mathfrak{p} \lhd \mathcal{O}_i$.

(ii) Any subgroup H of SL_i normalized by a subgroup of finite index in SL_i contains $E(\mathfrak{p})$ for some $0 \neq \mathfrak{p} \lhd \mathcal{O}_i$.

We say that the component $(D_i)_{n_i\times n_i}$ satisfies (C.S.T.). If all the components have this property, we shall say that G satisfies (C.S.T.). In fact, it is a result of Bass-Milnor-Serre-Vaserstein that (i) and (ii) always hold if $n_i \geq 3$ and for $n_i = 2$ they hold provided that $D_i \neq \mathbb{Q}$ or imaginary quadratic or a definite quaternion algebra. We shall further assume that if $n_i = 1$ then D_i is a totally definite quaternion algebra, namely, the group of units of $\mathcal{O}_i$ of reduced norm 1 is finite. If G is nilpotent of odd order then all the D_i's are commutative and also $n_i = 2$. Our first main result for noncommutative groups is

Theorem (3.8) (Ritter-Sehgal). *If* G *is nilpotent of odd order then* $\langle \mathcal{B}_1, \mathcal{B}_2\rangle$ *is of finite index in* $U(\mathbb{Z}G)$.

Remark. In fact, it is proved in [9] that if G is a nilpotent group, satisfying (C.S.T.), for whose Sylow 2-subgroups the D_i's are commutative then $\langle \mathcal{B}_1, \mathcal{B}_2\rangle$ is a large subgroup of $U(\mathbb{Z}G)$. If G has no subhomomorphic image K_8, the quaternian group of order 8, then the second condition holds (see [11, p. 106]).

Now, some words about the strategy of proof of a result as above. By using (3.5) it follows that in order to prove that $\langle \mathcal{B}_1, H\rangle$ is of finite index in $U(\mathbb{Z}G)$ it suffices to show that H contains a subgroup W_i of finite index in SL_i for all i with $n_i \geq 2$ (see [11, p. 123]). To produce W_i we prove

(3.9) $\qquad \pi_i(H)$ contains a subgroup of finite index in SL_i.

Under the assumption of (C.S.T.) it suffices to produce an $E(\mathfrak{p})$ in $\pi_i(H)$. This assumption is used also to obtain the reduction (3.9).

We return to the discussion of the case when G has a homomorphic image K_8. Remember that $\mathbb{Q}\ K_8 = 4\ \mathbb{Q} \oplus \mathrm{III}(\mathbb{Q})$ has no nilpotent elements and moreover,

$U(\mathbb{Z}K_8) = \pm K_8$ (see [10, p. 47]). Further, if ζ is a primitive pth root of unity, $\mathrm{IH}(\mathbb{Q}(\zeta))$ is not always a division ring. The result here is the

Theorem (3.10). *$\mathrm{IH}(\mathbb{Q}(\zeta))$ is not a division ring $\iff$ $o(2)$ mod p is even $\iff$ $x^2 + y^2 = -1$ has a solution in $\mathbb{Q}(\zeta)$.*

Proof. See [10, p. 173].

Remark. If $p \equiv 3 \pmod 8$ then certainly $0(2) \bmod p$ is even as

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \bmod p \equiv (-1)^{(p^2-1)/8} \equiv -1 \pmod p.$$

Here is a list of few orders of 2 mod p.

p	3	5	7	11	13	17	19	23
0(2)	2	4	3	10	12	8	18	11

Recall that $\mathrm{IH}(\mathbb{Q}(\sqrt{-1})) \cong (\mathbb{Q}(i))_{2\times 2}$ by the map

$$i \to \begin{pmatrix} \sqrt{-1} & \\ & \sqrt{-1} \end{pmatrix}, \quad j \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

This can be extended to $\mathrm{IH}(\mathbb{Q}(\zeta)) \cong (\mathbb{Q}(\zeta))_{2\times 2}$ if $\mathbb{Q}(\zeta)$ has elements x, y satisfying $x^2 + y^2 = -1$ by the map

$$i \to \begin{pmatrix} x & y \\ y & -x \end{pmatrix}, \quad j \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Jespers and Leal extended (3.8) to prove

Theorem (3.11). *a) If G is nilpotent satisfying (C.S.T.) and has no homomorphic image $K_8 \times C_p$ where p is an odd prime then $\langle \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_2' \rangle$ is a large subgroup of $U(\mathbb{Z}G)$.*

b) If G is nilpotent satisfying (C.S.T.) and all odd primes dividing $|G|$ are $\equiv 3 \pmod 8$ then there is a finite set $\mathcal{B}_4$ (explicitly defined) so that $\langle \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_2', \mathcal{B}_4 \rangle$ is a large subgroup of $U(\mathbb{Z}G)$.

Proof. See [4] and [5].

This was further extended by Giambruno-Sehgal who proved the following

Theorem (3.12). *Let G be a finite nilpotent group such that for each odd prime p dividing $|G|$, the order of 2 (mod p) is even. If G satisfies (C.S.T.) then $\langle \mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_2', \mathcal{B}_3 \rangle$ is a large subgroup of $U(\mathbb{Z}G)$.*

Proof. See [3].

In order to complete the study for nilpotent groups one needs to know units in cyclotomic quaternions. We suggest the

PROBLEM. Let ζ be a root of unity so that the Hamiltonian quaterions $\mathbb{H}(\mathbb{Q}(\zeta))$ do not split. Find explicit generators of a large subgroup of $U(R)$ where

$$R = \mathbb{Z}[\zeta] \dot{+} \mathbb{Z}[\zeta] i \dot{+} \mathbb{Z}[\zeta] j \dot{+} \mathbb{Z}[\zeta] k.$$

Remark. To prove the sufficiency of (3.9) for exhibiting generators of large subgroups it is possible to allow one simple component of $\mathbb{Q}G$ which doesn't satisfy (C.S.T.). This is used to prove that if G is dihedral then $\langle \mathcal{B}_1, \mathcal{B}_2 \rangle$ is a large subgroup (see [11, p. 125]). The same result is also true for $G = S_n$ (see [11, p. 146]). It is possible to find generators for $U(RG)$ where $R = \mathbb{Z}[\zeta]$ for a suitable root of unity ζ. This was done by Ritter-Sehgal and Jespers-Leal (see [11, p. 154]). We do not know how to descend to $\mathbb{Z}G$.

1 A.V. Babin, M.I. Vishik, *Attractors in Evolutionary Equations* (Russian), Nauka (1989).

REFERENCES

1. H. Bass, *The Dirichlet unit theorem, induced characters, and Whitehead groups of finige groups*, Topology **4** (1966), 391-410.

2. G. Higman, *The units of group rings*, Proc. London Math. Soc. **46** (1940), 231-248.

3. A. Giambruno and S.K. Sehgal, *Generators of large subgroups of units of integral group rings of nilpotent groups*, preprint.

4. E. Jespers and G. Leal, *Generators of large subgroups of the unit group of integral group rings*, Manuscipt Math. **78** (1993), 303-315.

5. E. Jespers and G. Leal, *Units of integral group rings of Hamiltonian groups*, preprint.

6. E. Kleinert, *A theorem of units of integral group rings*, J. Pure Applied Algebra **49** (1987), 161-171.

7. I. Reiner, *Maximal Orders*, Academic Press, New York, 1979.

8. J. Ritter and S.K. Sehgal, *Construction of units in integral group rings of finite nilpotent groups*, Bull. Amer. MAth. Soc. **20** (1989), 165-168.

9. J. Ritter and S.K. Sehgal, *Construction of units in integral group rings of finite nilpotent groups*, Trans. Amer. Math. Soc. **324** (1991), 603-621.

10. S.K. Sehgal, *Topics in Group Rings*, Marcel Dekker, New York and Basel, 1978.

11. S.K. Sehgal, *Units of Integral Group Rings*, Longman's, Essex, 1993.

Department of Mathematics
University of Alberta
Edmonton, Alberta
Canada T6G 2G1