PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 125, Number 4, April 1997, Pages 1005–1009
S 0002-9939(97)03812-4

# CONSTRUCTING FREE SUBGROUPS OF INTEGRAL GROUP RING UNITS

ZBIGNIEW S. MARCINIAK AND SUDARSHAN K. SEHGAL

(Communicated by Ronald M. Solomon)

ABSTRACT. Let $G$ be an arbitrary group. It is proved that if $\mathbb{Z}G$ contains a bicyclic unit $u \neq 1$, then $\langle u, u^* \rangle$ is a nonabelian free subgroup of invertible elements.

## INTRODUCTION

Let $\mathbb{Z}G$ be the integral group ring of a group $G$. Let $\mathcal{U}_1\mathbb{Z}G$ be the group of invertible elements in this ring which are of augmentation one.

Properties of this group have been investigated for many years. We now know that $\mathcal{U}_1\mathbb{Z}G$ only rarely belongs to well studied manifolds of groups like solvable, nilpotent, etc. It is caused by the existence of nonabelian free subgroups. The following theorem was proved by Sehgal [7, p. 200] and also by Hartley-Pickel [1] (see also [6, page 19]).

**1. Theorem.** *Let $G$ be a solvable group which has a nonnormal finite subgroup. Then $\mathcal{U}_1\mathbb{Z}G$ contains a nonabelian free subgroup.*

*Also, all nonabelian finite groups $G$, except Hamiltonian 2-groups, have a free subgroup inside $\mathcal{U}_1\mathbb{Z}G$.*

These are really existence results. The main idea for finite groups is as follows (see [6]). Since $\mathbb{Z}G$ contains a nonzero nilpotent element the Wedderburn decomposition of $\mathbb{Q}G$ contains a matrix ring $M_d(D)$ over a division ring $D$ with $d \geq 2$. There we can easily find a free subgroup:

**2. Theorem** (Sanov, see [4, page 92])**.** *For a complex number $z$ satisfying $|z| \geq 2$ the matrices $\left(\begin{smallmatrix} 1 & z \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ z & 1 \end{smallmatrix}\right)$ generate a nonabelian free subgroup in $GL_2(\mathbb{C})$.*

We just take $z = m$, an integer. For $m$ large enough both Sanov's matrices will lie in the image of $\mathcal{U}_1\mathbb{Z}G$ and thus they will be images of two units generating a nonabelian free subgroup of $\mathcal{U}_1\mathbb{Z}G$. However, it is hard to write them down explicitly.

The study of free subgroups in $\mathcal{U}_1\mathbb{Z}G$ was continued by Jespers who characterised in [2] all finite groups $G$ which have a free complement in $\mathcal{U}_1\mathbb{Z}G$. Recently Jespers,

Received by the editors October 25, 1995.
1991 *Mathematics Subject Classification.* Primary 16S34, 16U60.
The authors were supported by Canadian NSERC Grant A-5300 and Polish Scientific Grant 2P30101007.

Leal and del Rio [3] classified finite nilpotent groups $G$ such that $\mathcal{U}_1\mathbb{Z}G$ has a subgroup of finite index which is a direct product of noncyclic free groups.

In this paper we offer an easy way of constructing nonabelian free subgroups of $\mathcal{U}_1\mathbb{Z}G$, also for infinite groups $G$. For this purpose we use *bicyclic units*. They are constructed as follows: take any $x, y \in G$ with $o(x) = n < \infty$. For $\nu = (1-x)y\hat{x}$, $\hat{x} = 1 + x + \cdots + x^{n-1}$, we have $\nu^2 = 0$. Then $u = 1 + \nu$ is the unit in question.

**Main Theorem.** *Let $G$ be any group. If $u \in \mathcal{U}_1\mathbb{Z}G$ is a bicyclic unit and $u \neq 1$, then the pair $\{u, u^*\}$ generates a nonabelian free subgroup of $\mathcal{U}_1\mathbb{Z}G$.*

As usual, $*$ denotes here the anti-involution on $\mathbb{Z}G$ given by $(\sum a_g g)^* = \sum a_g g^{-1}$.

## Proof of the Main Theorem

Consider the monoid defined by the presentation $\Sigma = \langle s, t | s^2 = 0, t^2 = 0\rangle$. For any pair of elements $a, b \in \mathbb{Z}G$ satisfying $a^2 = b^2 = 0$ we have a monoid homomorphism $\phi : \Sigma \to (\mathbb{Z}G, \cdot)$ given by $\phi(s) = a, \phi(t) = b$.

When $\phi$ is an embedding, we say that $\{a, b\}$ is a pair of independent nilpotents. It is easy to characterise all such pairs.

**3. Lemma.** *Let $a, b \in \mathbb{Z}G$ satisfy $a^2 = b^2 = 0$. The pair $\{a, b\}$ is independent if and only if the element $ab$ is not nilpotent.*

*Proof.* Suppose first that $\phi$ is injective. Because the elements 0 and $(st)^k$, $k \geq 1$, are all different in $\Sigma$, so are the elements 0 and $(ab)^k$, $k \geq 1$, in $\mathbb{Z}G$. Therefore no power of $ab$ is equal to 0.

Suppose now that $ab$ is not nilpotent but $\phi(x) = \phi(y)$ for some $x \neq y \in \Sigma$. We can decompose $\Sigma$ into disjoint subsets $\Sigma = \{0\} \cup \mathcal{T} \cup t\mathcal{T} \cup \mathcal{T}s \cup t\mathcal{T}s$, where $\mathcal{T} = \{(st)^k | k \geq 0\}$.

If $x, y$ belong to different parts of $\Sigma$, then we can multiply them simultaneously by $t$ and/or $s$ on the proper side to achieve a pair $x' = 0, y' = (st)^k$ for some $k$. Then we have $0 = \phi(x') = \phi(y') = (ab)^k$, i.e. $ab$ is nilpotent—a contradiction.

If both $x, y$ belong to the same part of $\Sigma$, then by a similar multiplication we can achieve a pair $x' = (st)^k, y' = (st)^l \in \mathcal{T}$ with $k > l$. Thus $(ab)^k = \phi(x') = \phi(y') = (ab)^l$.

It easily follows that $(ab)^l = (ab)^k = (ab)^{k+r(k-l)}$ for all $r \geq 0$. Hence we can change $k$ to a larger number, if necessary, to assure that $k > 2l$. When we multiply both sides of $(ab)^l = (ab)^k$ by $(ab)^{k-2l}$, we get $(ab)^{k-l} = (ab)^{2(k-l)}$, i.e. $(ab)^{k-l}$ is an idempotent.

From Kaplansky's Theorem [5, Theorem 2.1.8] it follows that the only idempotents in $\mathbb{Z}G$ are 0 and 1. But $(ab)^{k-l} = 1$ is impossible as $a$ is nilpotent. Thus we are left with $(ab)^{k-l} = 0$, i.e. $ab$ is nilpotent—again a contradiction. □

The next lemma shows that pairs of independent nilpotents are abundant.

**4. Lemma.** *If $a \in \mathbb{Z}G$ is such that $a^2 = 0$ and $a \neq 0$, then the pair $\{a^*, a\}$ is independent.*

*Proof.* Recall from [5, Lemma 2.3.3] that the group ring trace of any nilpotent element is equal to zero. On the other hand, if $a = \sum a_g g \neq 0$, then $\mathrm{tr}(a^*a) = \sum a_g^2 > 0$, i.e. $a^*a$ is not nilpotent. □

We are now ready to produce the first free subgroups in $\mathcal{U}_1\mathbb{Z}G$.

**5. Lemma.** *Let $S$ be the monoid generated by a pair $\{a, b\}$ of independent nilpotents in $\mathbb{Z}G$. If the set $S\setminus\{0\} \subset \mathbb{C}G$ is linearly independent, then the pair $1+a, 1+b$ of units generates a nonabelian free subgroup in $\mathcal{U}_1\mathbb{Z}G$.*

*Proof.* As the nilpotents $a, b$ are independent, so $S$ is isomorphic to $\Sigma$. From the linear independence of $S\setminus\{0\}$ it follows that its $\mathbb{Z}$-linear span $R \subset \mathbb{Z}G$ is isomorphic to the semigroup ring $\mathbb{Z}\Sigma$. Clearly $1 + a, 1 + b \in R$.

Consider the representation $\rho : \Sigma \to M_2(\mathbb{Z})$ given by $\rho(s) = \left(\begin{smallmatrix} 0 & 2 \\ 0 & 0 \end{smallmatrix}\right), \rho(t) = \left(\begin{smallmatrix} 0 & 0 \\ 2 & 0 \end{smallmatrix}\right)$. It extends by linearity to a ring homomorphism $\overline{\rho} : R \approx \mathbb{Z}\Sigma \to M_2(\mathbb{Z})$. Then

$$\overline{\rho}(1 + a) = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \qquad \overline{\rho}(1 + b) = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

and hence $1 + a, 1 + b$ generate together a nonabelian free subgroup, by Theorem 2. □

Obviously, when $G$ is finite, the infinite set $S \setminus \{0\}$ has no chance to be independent. Now we describe its linear dependence in simpler terms.

**6. Lemma.** *Let $S \subset \mathbb{Z}G$ be the monoid generated by a pair of independent nilpotents $\{a, b\}$. Let $T = \{(ab)^k | k = 0, 1, 2, \dots\} \subset S$. Then the following conditions are equivalent.*

(i) *The set $S \setminus \{0\}$ is linearly independent in $\mathbb{C}G$.*

(ii) *The set $T$ is linearly independent in $\mathbb{C}G$.*

*Proof.* We only need to prove that (ii) $\Rightarrow$ (i). Suppose that $T$ is independent and consider any linear combination of elements from $S \setminus \{0\}$. We can write it in the form $\alpha + \beta + \gamma + \delta = 0$ where the four summands have disjoint supports: $\operatorname{supp}(\alpha) \subset T, \operatorname{supp}(\beta) \subset bT, \operatorname{supp}(\gamma) \subset Ta, \operatorname{supp}(\delta) \subset bTa$.

If $\alpha \not\equiv 0$, then we multiply our combination on both sides by $ab$. We obtain a nonzero combination $(ab)\alpha(ab) = 0$ of elements of $T$, a contradiction. Hence $\alpha \equiv 0$ and so $\beta + \gamma + \delta = 0$.

If $\beta \not\equiv 0$, then we multiply our combination on the left by $a$ and on the right by $ab$. We obtain a nonzero combination $a\beta(ab) = 0$ of $T$, again a contradiction. Thus $\beta \equiv 0$ and $\gamma + \delta = 0$.

If $\gamma \not\equiv 0$, then we multiply on the left by $ab$ and on the right by $b$. We then get $(ab)\gamma b = 0$, a contradiction as before. It must then be $\gamma \equiv 0$ and we are thus left with $\delta = 0$. When we multiply this equation by $a$ on the left and by $b$ on the right we get a $T$-combination $a\delta b = 0$. It follows that also $\delta \equiv 0$. Therefore $\alpha \equiv \beta \equiv \gamma \equiv \delta \equiv 0$, i.e. our combination is trivial. □

Now we restrict our attention to independent pairs of the form $\{\nu^*, \nu\}$ where $\nu = (1-x)y\hat{x}$ is a nonzero bicyclic nilpotent and $o(x) = n$. Consider $c = \nu^*\nu \in \mathbb{Z}G$. Then we have $c = \hat{x}y^{-1}(1 - x^{-1}) \cdot (1 - x)y\hat{x} = \hat{x}(2 - z - z^{-1})\hat{x}$ where $z = y^{-1}xy$.

**7. Lemma.** *If the set $T = \{c^k | k = 0, 1, 2, \dots\} \subset \mathbb{C}G$ is linearly dependent, then the subgroup $H = \langle x, z\rangle < G$ is finite.*

*Proof.* We first show that for each $h \in H$ there exists $m \geq 1$ such that $h \in \operatorname{supp}(c^m)$. To this end define a function $\|\cdot\| : H \to \mathbb{N}$ by

$$\|h\| = \inf\{|j_1| + \cdots + |j_s| : h = x^{i_1}z^{j_1} \cdots x^{i_s}z^{j_s}x^{i_{s+1}}\}.$$

If $\|h\| = 0$, then $h = x^i \in \operatorname{supp}(c)$. Otherwise write $h$ as a product $x^{i_1}z^{j_1} \cdots x^{i_s}z^{j_s}x^{i_{s+1}}$ with $|j_1| + \cdots + |j_s| = \|h\|$. If there are many such presentations, just pick one.

Now we take $m = \|h\|$. Then $c^m = n^{m-1} \cdot \hat{x}(2 - z - z^{-1})\hat{x} \cdots \hat{x}(2 - z - z^{-1})\hat{x}$ with precisely $m$ factors of the form $(2 - z - z^{-1})$. It is clear that when we expand this product, the chosen expression of $h$ will appear. Moreover, any product equal to $h$ must use either $-z$ or $-z^{-1}$ from each factor $(2 - z - z^{-1})$—otherwise we would get a presentation of $h$ with $|j_1| + \cdots + |j_s| < \|h\|$. Thus all products equal to $h$ will have the same coefficient equal to $(-1)^m n^{m-1}$. Hence $h$ will appear in $c^m$ with a nonzero coefficient $(-1)^m n^{m-1} \cdot k$ for some positive integer $k$.

From the linear dependence of $T$ it follows that $c^d = \sum_{i=0}^{d-1} q_i c^i$ for some $d > 1$ and $q_i \in \mathbb{Q}$. Recursively, we can express each $c^m$ as a linear combination of $1, c, c^2, \ldots, c^{d-1}$. Hence $\operatorname{supp}(c^m) \subset B = \bigcup_{i=1}^{d-1} \operatorname{supp}(c^i)$. Therefore each $h \in H$ belongs to the finite set $B$ and so $H$ is a finite group. □

**8. Lemma.** *Let $H$ be a finite group. Suppose that $x, z \in H$ are such that $o(x) = o(z) = n$ and $c = \hat{x}(2 - z - z^{-1})\hat{x} \neq 0$. Then all eigenvalues of $L_c : \mathbb{C}H \to \mathbb{C}H, L_c(\alpha) = c \cdot \alpha$, are real and at least one of them is bigger than or equal to 4.*

*Proof.* Consider the left regular representation $\mathbb{C}H \to \operatorname{End}_{\mathbb{C}}(\mathbb{C}H), \alpha \mapsto L_\alpha$. After fixing the basis $H \subset \mathbb{C}H$ we obtain a matrix representation $\rho : \mathbb{C}H \to M_r(\mathbb{C})$ where $r = |H|$.

Notice that for $h \in H$ the map $\rho(h)$ permutes the basis and thus it is an orthogonal transformation. Therefore for any $h \in H$ we have $\rho(h^{-1}) = \rho(h)^{-1} = \rho(h)^T$. Hence $\rho(\alpha^*) = \rho(\alpha)^T$ for all $\alpha \in \mathbb{Z}H$.

Let $C$ be the matrix of $L_c$. We have $C = \rho(c) = \rho(c^*) = C^T$, i.e. $C$ is a symmetric matrix. In particular, all its eigenvalues are real numbers.

To estimate the eigenvalues let us change the basis in $\mathbb{C}$ to obtain a new representation $\rho' : \mathbb{C}H \to M_r(\mathbb{C})$ such that $\rho'(x)$ is diagonal: $\rho'(x) = \operatorname{diag}(\lambda_1, \ldots, \lambda_r)$, $\lambda_i^n = 1$. Then, after a suitable permutation of the basis, we will have $\rho'(\hat{x}) = \operatorname{diag}(n, \ldots, n, 0, \ldots, 0) = E$.

We have

$$\begin{aligned}\operatorname{rank}(E) = \#\{i|\lambda_i = 1\} = &\text{ dimension of the subspace of } \mathbb{C}^r \text{ fixed by } \rho'(x)\\ &= \text{dimension of the subspace of } \mathbb{C}H \text{ fixed by } (x\cdot) = \dim_{\mathbb{C}}(\hat{x}\mathbb{C}H).\end{aligned}$$

Consider the idempotent $e = (1/n)\hat{x} \in \mathbb{C}H$. Clearly $\hat{x}\mathbb{C}H = e\mathbb{C}H$. Moreover, we have $\dim_{\mathbb{C}}(e\mathbb{C}H) = |H| \cdot \operatorname{tr}(e) = r/n$. Therefore $E$ has rank $r/n$.

Let $C' = \rho'(c)$ and $Z = \rho'(z)$. Then

$$C' = E \cdot (2I - Z - Z^T) \cdot E = \begin{pmatrix} A & 0 \\ 0 & 0 \end{pmatrix}$$

where $A$ is a square matrix of degree $r/n$. Hence the matrix $C'$, and hence $C$, has at most $r/n$ nonzero eigenvalues.

Suppose that all eigenvalues $\mu_i$ of $C$ satisfy $\mu_i < 4$. Then the trace of $C$ can be estimated by $4r/n$. On the other hand, $\operatorname{Tr}(C) = |H| \cdot \operatorname{tr}(c) = r \cdot 2n$. The previous estimate gives us an inequality

$$\begin{aligned}2rn = \operatorname{Tr}(C) &< 4r/n,\\ n^2 &< 2,\end{aligned}$$

and hence $n = 1$ which contradicts the assumption that $c \neq 0$. Therefore at least one of the eigenvalues of $C$ satisfies $\mu \geq 4$. □

## Conclusion of the proof

Let $u = 1 + \nu \in \mathbb{Z}G$ be a bicyclic unit with $\nu = (1-x)y\hat{x} \neq 0$ and $o(x) = n$.

Let us write $a = \nu^*, b = \nu$. From Lemma 4 we know that $\{a, b\}$ is a pair of independent nilpotents. Let $S$ be the multiplicative monoid generated by this pair in $\mathbb{Z}G$. If the set $S \setminus \{0\}$ is linearly independent, then $u^* = 1 + a, u = 1 + b$ generate a nonabelian free group of units, by Lemma 5.

In the remaining case the set $S \setminus \{0\}$ is linearly dependent. Let $c = ab$. By Lemma 6, the subset $T = \{1, c, c^2, \dots\}$ is also linearly dependent. From Lemma 7 it follows that the subgroup $H = \langle \mathrm{supp}(c) \rangle < G$ is finite. From Lemma 8 we conclude that the map $L_c : \mathbb{C}H \to \mathbb{C}H$ has a real eigenvalue $\mu \geq 4$.

Let $v \in \mathbb{C}H$ be an eigenvector of $L_c$ corresponding to $\mu$. Then the extended map $L_c : \mathbb{C}G \to \mathbb{C}G, L_c(\alpha) = c \cdot \alpha$, still satisfies $L_c(v) = \mu \cdot v$. Consider also the vector $w = (1/\sqrt{\mu})L_b(v)$.

Then the subspace $V = \mathrm{span}(v, w) \subset \mathbb{C}G$ is invariant under the transformations $L_a$ and $L_b$. In fact,

$$L_a(v) = (1/\mu)L_aL_c(v) = (1/\mu)L_{a^2}L_b(v) = 0,\ L_b(v) = \sqrt{\mu} \cdot w,$$
$$L_a(w) = (1/\sqrt{\mu})L_{ab}(v) = 1/\sqrt{\mu}L_c(v) = \sqrt{\mu} \cdot v,\ L_b(w) = (1/\sqrt{\mu})L_{b^2}(v) = 0.$$

From the above equalities it follows that the vectors $v, w$ are linearly independent and hence they form a basis of $V$.

Obviously the transformations $L_{1+a}, L_{1+b}$ also preserve the subspace $V$. With respect to the basis $\{v, w\}$ they are represented by the matrices

$$L_{u^*} = \begin{pmatrix} 1 & \sqrt{\mu} \\ 0 & 1 \end{pmatrix}, \quad L_u = \begin{pmatrix} 1 & 0 \\ \sqrt{\mu} & 1 \end{pmatrix}.$$

However, we have $\mu \geq 4$ and hence $\sqrt{\mu} \geq 2$. Under this assumption, the above pair of matrices generates a nonabelian free group, by Theorem 2. Hence the units $u, u^* \in \mathcal{U}_1\mathbb{Z}G$ do the same. □

## References


1. B. Hartley and P. F. Pickel, *Free subgroups in the unit groups of integral group rings*, Canadian Journal of Math. **32** (1980), 1342–1352. MR **82i:**20008
2. E. Jespers, *Free normal complements and the unit group of integral group rings*, Proceedings of AMS **122** (1994), 59–66. MR **94k:**16058
3. E. Jespers, G. Leal, and A. del Rio, *Products of free groups in the unit group of integral group rings*, J. Algebra **180** (1996), 22–40. CMP 96:08
4. M. Kargapolov and Yu. Mierzljakov, *Fundamentals of the theory of groups*, Springer-Verlag, 1979. MR **80k:**20002
5. D. S. Passman, Algebraic structure of group rings, Interscience, New York, 1977. MR **81d:**16001
6. S. K. Sehgal, *Units in integral group rings*, Longman's, Essex, 1993. MR **94m:**16039
7. S. K. Sehgal, *Topics in group rings*, Marcel Dekker, 1978. MR **80j:**16001



Institute of Mathematics, Warsaw University, ul. Banacha 2, 02-097 Warszawa, Poland

*E-mail address*: zbimar@mimuw.edu.pl

Department of Mathematical Sciences, University of Alberta, Edmonton, Alberta, Canada T6G 2G1

*E-mail address*: s.sehgal@ualberta.ca