PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 127, Number 9, Pages 2569–2572
S 0002-9939(99)05309-5
Article electronically published on May 17, 1999

ON FREE SUBGROUPS OF UNITS OF RINGS

A. SALWA

(Communicated by Ronald M. Solomon)

ABSTRACT. We prove that if $a^2 = b^2 = 0$ for elements a, b of a ring R of characteristic zero and ab is not nilpotent, then there exists $m \in \mathbf{N}$ such that the group generated by $1 + ma$ and $1 + mb$ is free nonabelian. This is used to prove that a noncommutative positive-definite algebra with involution over an uncountable field contains a free nonabelian subsemigroup.

Consider the following general problem: when does a ring R (of characteristic zero) contain a free nonabelian subgroup, or subsemigroup, and how does one construct such free objects? In [2] Klein proved that if R is a noncommutative domain and the center of R is uncountable, then R contains free nonabelian subsemigroups. It is still an open problem whether every noncommutative division ring R contains a free nonabelian subgroup. In this paper we are interested in the case when R contains nilpotent elements. In [3] Marciniak and Sehgal proved that the group generated by a nontrivial bicyclic unit of an integral group ring $\mathbf{Z}[G]$ and by its conjugate (under the natural involution of $\mathbf{Z}[G]$) must be free. Unexpectedly, this has led to a new insight into the structure of unit groups and in particular to new simple proofs of several results. Bicyclic units have the form $1 + a$, where $a^2 = 0$. This result was generalized to algebras over $\mathbf{C}$ with involution $*$ and endowed with a Hermitian inner product which is compatible with $*$, and to subgroups generated by $1 + a$ and $1 + a^*$, where $a^2 = 0$ [4]. In this paper we investigate the general case of subgroups generated by elements $1 + a$ and $1 + b$, $a^2 = b^2 = 0$, in unit groups of rings.

Throughout the paper $\mathbf{C}$, $\mathbf{R}_+$, $\mathbf{Z}$ and $\mathbf{N}$ denote the sets of complex, positive real, integer and natural numbers, respectively. By $|a|$ we mean the absolute value of $a \in \mathbf{C}$.

We will investigate torsion free rings with unity. $\mathcal{J}(R)$ denotes the Jacobson radical of a ring R. We say that an algebra A over $\mathbf{C}$ admits a trace function if there exists a $\mathbf{C}$-linear map $Tr : A \longrightarrow \mathbf{C}$ such that $Tr(ab) = Tr(ba)$ for $a, b \in A$, $Tr(e) \in \mathbf{R}_+$ for all idempotents $e \in A \setminus \{0\}$ and $Tr(n) = 0$ for every nilpotent element $n \in A$.

Let $\langle x, y\rangle$ denote the subgroup of the ring R generated by two units $x, y \in R$. F_2 stands for the free group on two generators.

Theorem 1. *Let R be a torsion free ring. Assume that $a, b \in R, a^2 = b^2 = 0$ and ab is not nilpotent. Then there exists $m \in \mathbf{N}$ such that $\langle 1 + ma, 1 + mb\rangle \cong F_2$. If*

Received by the editors October 15, 1997.
1991 *Mathematics Subject Classification.* Primary 16U60.
The author was supported by KBN reasearch grant 2P03A 003 12.

moreover $\mathbf{C}\otimes_{\mathbf{Z}} R$ *admits a trace function* Tr*, then* $\langle 1+a, 1+b\rangle \cong F_2$*, provided that* $|Tr(ab)| > 2Tr(1)$.

Proof. Let $\mathbf{Z}\langle a,b\rangle$ be the subring of R generated by a and b. Denote $A = \mathbf{C}\otimes_{\mathbf{Z}} \mathbf{Z}\langle a,b\rangle$. If there are no relations in A other than those coming from $a^2 = b^2 = 0$, then A is isomorphic to $\mathbf{C}\langle a,b : a^2 = b^2 = 0\rangle$. Hence we can define a homomorphism $\phi : A \longrightarrow M_2(\mathbf{C})$ by the rule $\phi(a) = \begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$, $\phi(b) = \begin{pmatrix} 0 & 0 \\ 2 & 0 \end{pmatrix}$ since matrices in the definition of ϕ are nilpotent of degree 2. Because $\langle 1+\phi(a), 1+\phi(b)\rangle \cong F_2$ by [6], we have also $\langle 1+a, 1+b\rangle \cong F_2$. So assume that there exists a nontrivial relation between elements of the set S of nonzero words in a,b. Elements of S are of the form $x(ab)^n y$ where $n \geq 0, x \in \{1,b\}, y \in \{1,a\}$. S can be ordered by lexicographic order assuming that $a > b$. So there is a relation of the form $w = \sum_i \alpha_i w_i$, where $\alpha_i \in \mathbf{C}, w, w_i \in S$ and $w > w_i$ for all i. Note that any word $z \in S$ of length greater than the length of w has to contain w as a subword. Hence substituting $\sum_i \alpha_i w_i$ in place of w we can express z as a linear combination of words which are smaller than z. Repeating this argument we can prove that $A = Lin_{\mathbf{C}}\{z \in S : \text{length of } z \leq \text{length of } w\}$. In particular $dim_{\mathbf{C}} A < \infty$. Let

$$A/\mathcal{J}(A) \cong M_{n_1}(\mathbf{C}) \times M_{n_2}(\mathbf{C}) \times \cdots \times M_{n_k}(\mathbf{C}).$$

First we will prove that $n_i \leq 2$ for each i. Clearly there exists a homomorphism $\phi_i : A \longrightarrow M_{n_i}(\mathbf{C})$ which is onto. Since $\phi_i(a)^2 = 0$, one obtains $ker\phi_i(a) \supseteq Im\phi_i(a)$. It follows that $n_i - dimIm\phi_i(a) \geq dimIm\phi_i(a)$ and therefore $rank\phi_i(a) \leq n_i/2$. Define $X = Lin\{(\phi_i(a)\phi_i(b))^t : t = 0,1,\dots\}$. Since $rank[\phi_i(a)\phi_i(b)] \leq [n_i/2]$ we get $dimX \leq [n_i/2]+1$ by the Cayley-Hamilton theorem. It is easy to see that

$$M_{n_i}(\mathbf{C}) = X + \phi_i(b)X + X\phi_i(a) + \phi_i(b)X\phi_i(a).$$

This implies $n_i^2 \leq 4([n_i/2]+1)$. Hence $n_i \leq 2$, as desired. Suppose that $n_i = 1$ for all i. This means that $A/\mathcal{J}(A)$ is commutative. Hence $ab - ba \in \mathcal{J}(A)$ which is nilpotent, say of index m. This implies $[(ab-ba)a(ab-ba)b]^m = 0$ and leading to $(-ababab)^m = 0$, a contradiction, as ab is assumed not to be nilpotent. Hence there exists i such that $n_i = 2$ and an onto homomorphism $\phi : A \longrightarrow M_2(\mathbf{C})$. Clearly $M_2(\mathbf{C}) = \mathbf{C}\langle\phi(a),\phi(b)\rangle$. Now $\phi(a)^2 = 0$ and $\phi(a) \neq 0$, hence $rank\phi(a) = 1$. Similarly $rank\phi(b) = 1$. If $\phi(a)\phi(b) = 0$, then $Im\phi(b)$ is $\phi(a)$- and $\phi(b)$-invariant. This gives $M_2(\mathbf{C})Im\phi(b) \subseteq Im\phi(b)$, a contradiction. Hence $\phi(a)\phi(b) \neq 0$ and similarly $\phi(b)\phi(a) \neq 0$. Since $rank[\phi(a)\phi(b)] \leq 1$ and $\phi(a)\phi(b) \neq 0$, we get $rank[\phi(a)\phi(b)] = 1$. This implies

$$Im[\phi(a)\phi(b)] = Im\phi(a), \qquad ker[\phi(a)\phi(b)] = ker\phi(b). \tag{1}$$

Assume that $\phi(a)\phi(b)$ is nilpotent. Then $Im[\phi(a)\phi(b)] = ker[\phi(a)\phi(b)]$ implies $Im\phi(a) = ker\phi(b)$ and we get $\phi(b)\phi(a) = 0$, a contradiction. Hence $\phi(a)\phi(b)$ is not nilpotent and we can find a basis $\{v_1, v_2\}$ of $\mathbf{C}^2$ such that $\phi(a)\phi(b) = \begin{pmatrix} \lambda & 0 \\ 0 & 0 \end{pmatrix}, \lambda \in \mathbf{C}\setminus\{0\}$. From (1) it follows that $\phi(a) = \begin{pmatrix} p & q \\ 0 & 0 \end{pmatrix}$ and $\phi(b) = \begin{pmatrix} r & 0 \\ s & 0 \end{pmatrix}$ for some $p,q,r,s \in \mathbf{C}$. Because $\phi(a)$ and $\phi(b)$ are nilpotent we have $p = r = 0$. Now we can find $m \in \mathbf{N}$ such that $|mq|, |ms| \geq 2$. In this case $\langle 1+m\phi(a), 1+m\phi(b)\rangle \cong F_2$, whence $\langle 1+ma, 1+mb\rangle \cong F_2$. This completes the proof of the first assertion of the theorem.

Now assume that A admits a trace function Tr and $|Tr(ab)| > 2Tr(1)$. By the first part of the proof we can assume that $dim A < \infty$. Hence $\mathcal{J}(A)$ is nilpotent. Define $tr : A/\mathcal{J}(A) \longrightarrow \mathbf{C}$ by the rule $tr(a + \mathcal{J}(A)) = Tr(a)$ for $a \in A$. Then tr is well defined because if $a \in A$ is nilpotent, then $Tr(a) = 0$. It follows also that $tr(c) = 0$ for all nilpotent elements $c \in A/\mathcal{J}(A)$. Of course tr is $\mathbf{C}$-linear and $tr(\overline{a}\overline{b}) = tr(\overline{b}\overline{a})$ for $\overline{a}, \overline{b} \in A/\mathcal{J}(A)$. Moreover if $\overline{e} \in A/\mathcal{J}(A)$ is a nonzero idempotent, then there exists a nonzero idempotent $e \in A$ such that $\overline{e} = e + \mathcal{J}(A)$. This implies $tr(\overline{e}) = Tr(e) \in \mathbf{R}_+$. It follows that tr is a trace function. By the proof of the first part of the theorem we know that

$$A/\mathcal{J}(A) = \underbrace{\mathbf{C} \times \cdots \times \mathbf{C}}_{k} \times \underbrace{M_2(\mathbf{C}) \times \cdots \times M_2(\mathbf{C})}_{l}.$$

Let ϕ_i denote the composition of the quotient map $A \longrightarrow A/\mathcal{J}(A)$ with the projection on the $i-$th factor of $A/\mathcal{J}(A)$. Then $\phi_i(a) = 0$ for $i \leq k$ because $a^2 = 0$ and $\phi_i(a) = \begin{pmatrix} 0 & q_i \\ 0 & 0 \end{pmatrix}$ for $i > k$. Similarly $\phi_i(b) = 0$ for $i \leq k$ and $\phi_i(b) = \begin{pmatrix} 0 & 0 \\ s_i & 0 \end{pmatrix}$ for $i > k$. The trace function tr has the form $tr = \sum_i \lambda_i tr_i, \lambda_i \in \mathbf{R}_+$, where tr_i denotes the usual trace function. In fact, it is easy to verify that the trace function on matrices has to be a scalar multiple of the usual trace function. The condition $|Tr(ab)| > 2Tr(1)$ implies $|\sum_{i>k} \lambda_i q_i s_i| > 2(\sum_{i \leq k} \lambda_i + \sum_{i>k} 2\lambda_i)$. Assume that $|q_i s_i| \leq 4$ for all $i > k$. This implies

$$4\sum_{i>k} \lambda_i \leq 2\sum_{i \leq k} \lambda_i + 4\sum_{i>k} \lambda_i < |\sum_{i>k} \lambda_i q_i s_i| \leq \sum_{i>k} \lambda_i |q_i s_i| \leq 4\sum_{i>k} \lambda_i,$$

a contradiction. Hence we can find i_0 such that $|q_{i_0} s_{i_0}| > 4$. It is clear that $\phi_{i_0}(1+a) = \begin{pmatrix} 1 & q_{i_0} \\ 0 & 1 \end{pmatrix}$, $\phi_{i_0}(1+b) = \begin{pmatrix} 1 & 0 \\ s_{i_0} & 1 \end{pmatrix}$, or changing the basis $\phi_{i_0}(1+a) = \begin{pmatrix} 1 & \sqrt{q_{i_0} s_{i_0}} \\ 0 & 1 \end{pmatrix}$, $\phi_{i_0}(1+b) = \begin{pmatrix} 1 & 0 \\ \sqrt{q_{i_0} s_{i_0}} & 1 \end{pmatrix}$ where $|\sqrt{q_{i_0} s_{i_0}}| > 2$. Therefore $\langle 1+a, 1+b \rangle \cong F_2$. □

Next we will prove a few corollaries concerning rings R with involution $*$ satisfying the condition: $aa^* = 0 \Longrightarrow a = 0$ for $a \in R$. This is the positive-definite condition explored in [1, 2.2]. There exist many examples of rings of this type: $M_n(\mathbf{C})$ with Hermitian conjugation, group rings $\mathbf{C}[G]$ or more generally $\mathbf{C}[S]$ where S is an inverse semigroup and $(\sum \alpha_s s)^* = \sum \overline{\alpha}_s s^{-1}$; cf. [5, the proof of Lemma 2.3]. Also it is known that many examples of rings of operators on a Hilbert space are of this kind.

By $U(R)$ and $Z(R)$ we denote the group of units and the center of a ring R, respectively.

Corollary 2. *Let R be a positive-definite ring. Then $F_2 \subseteq U(R)$ if either of the following holds*:

(1) *R contains nonzero nilpotent elements,*
(2) *R contains noncentral idempotents.*

Proof. (1) There exists $a \in R \setminus \{0\}, a^2 = 0$. Because aa^* is not nilpotent, Theorem 1 implies that we can find $m \in \mathbf{N}$ such that $\langle 1 + ma, 1 + ma^* \rangle \cong F_2$. This implies $F_2 \subseteq U(R)$.

(2) If $eR(1-e) = 0$ and $(1-e)Re = 0$, then $er = ere$ and $re = ere$ for $r \in R$. Hence $er = re$ and $e \in Z(R)$, a contradiction. Therefore $eR(1-e) \neq 0$ or $(1-e)Re \neq 0$. Let for example $eR(1-e) \neq 0$. Then we can find $r \in R$ such that $er(1-e) \neq 0$. Since $[er(1-e)]^2 = 0$, case (1) applies. □

Corollary 3. *Let R be a positive-definite prime ring. If R has zero divisors, then $F_2 \subseteq U(R)$.*

Proof. Assume that $ab = 0, a, b \in R \setminus \{0\}$. By primeness of R we can find $r \in R$ such that $bra \neq 0$. Because $(bra)^2 = 0$, we have $F_2 \subseteq U(R)$ by Corollary 2. □

Corollary 4. *Let R be a positive-definite noncommutative algebra over an uncountable field. Then the multiplicative semigroup R° of R contains a free noncommutative subsemigroup.*

Proof. If R contains nilpotent elements, then $F_2 \subseteq U(R)$ by Corollary 2. If R does not contain nilpotent elements, R can be represented as a subdirect product of domains $D_i, i \in I$; cf. [1, Theorem 1.1.1]. Because R is noncommutative, we can find $i \in I$ such that D_i is noncommutative. By [2] D_i° contains a noncommutative free semigroup and hence R° also. □

References

[1] Herstein, I.N. "*Rings with involution*", Chicago Lect. in Math., The Univ. of Chicago Press, 1976. MR **56:**406

[2] Klein, A.A. "*Free subsemigroups of domains*", Proc. AMS 116(1992), 339-341. MR **92m:**16045

[3] Marciniak, Z.S. and Sehgal, S.K. "*Constructing free subgroups of integral group ring units*", Proc. AMS 125(1997), 1005–1009. MR **97f:**16057

[4] Marciniak, Z.S. and Sehgal, S.K. "*Subnormal subgroups of group ring units*", Proc. AMS 126(1998), 343–348. MR **98d:**16046

[5] Munn, W.D. "*Semiprimitivity of inverse semigroup algebras*", Proc. Royal Soc. Edinb. 93A(1982), 83-98. MR **84e:**20077a

[6] Sanow. I.N. "*The property of certain representation of free group*", Dokl. AN SSSR 57(1947), 657-659, in Russian.

Institute of Mathematics, University of Warsaw, Banacha 2, 02-097 Warsaw, Poland
E-mail address: `asalwa@mimuw.edu.pl`