RT-MAT 2004-10

FREE GROUPS AND INVOLUTIONS IN THE UNIT GROUP OF A GROUP ALGEBRA

A. Giambruno and
C. Polcino Milies

Abril 2004

FREE GROUPS AND INVOLUTIONS IN THE UNIT GROUP OF A GROUP ALGEBRA

A. GIAMBRUNO AND C. POLCINO MILIES

ABSTRACT. We study the existence of free groups of rank 2 in the group generated by the involutions of a group algebra over a non-absolute field.

1. Introduction

Let $U(RG)$ denote the group of units of the group ring of a group G over a commutative ring with unity R. The study of the structure of $U(RG)$ is an interesting problem and it turns out that, in most cases, this group is quite large. For instance, Hartley and Pickel [9] showed that, for a finite group G, the group $U(\mathbb{Z}G)$ where $\mathbb{Z}$ denotes the ring of rational integers, always contains a free group of rank two, except when G is either abelian or a Hamiltonian 2-group. Then, Marciniak and Sehgal [11] gave a method of explicitly constructing units that generate such a free group, provided that $\mathbb{Z}G$ contains a nontrivial bicyclic unit.

In case the ring of coefficients is a field F or a ring of algebraic integers, the existence of free subgroups of rank 2 was studied by Gonçalves in [2], [3] and [4]. Related results were given by Bovdi in [1]. A construction of free subgroups of units when F is a non-absolute field with char $F = p > 0$ and G is a torsion p'-group was given by Gonçalvez and Passman [6] and yet another construction appeared in [7].

At the light of these results, it is natural to ask which significant subgroups of the unit group are large in the sense that they still contain a free subgroup of rank 2 or, in other words, if one can built generators of the free group out of some special kind of units. In this vein, Gonçalvez and Passman [8] investigated the existence of free groups in the subgroup of unitary units with respect to the natural involution of FG induced by the map $g \mapsto g^{-1}$, for all $g \in G$.

In this paper we discuss the existence of free groups in another significant subgroup of $U(FG)$: the subgroup $U_2(FG)$ generated by all units of order 2.

2. Main results

Throughout this note F will be a field and, in case R is an algebra over F, $U_2(R) = \langle u \in R \mid u^2 = 1\rangle$ will denote the multiplicative group generated by all units of order 2 in R.

We start by observing that there is a $1-1$ correspondence between units of order 2 and semi-idempotents $0 \neq e \in R$ such that $e^2 = 2e$. In fact, if $u \in R$ is such that $u^2 = 1$, then $(1-u)^2 = 2(1-u)$. Whereas if $e^2 = 2e$, then $1-e$ is a unit of order 2.

2000 *Mathematics Subject Classification.* Primary 16U60; Secondary 20C07, 20E05.

Key words and phrases. free group, group algebra, unit group, involution.

Research partially supported by MIUR (Italy) and FAPESP and CNPq (Brazil).

In case $\frac{1}{2} \in R$, the above correspondence can be set between units of order 2 and nonzero idempotents of R. In fact, if $e^2 = e$, then $1 - 2e$ is a unit of order 2 and, if $u^2 = 1$, then $\frac{1}{2}(1 - u)$ is an idempotent.

We start our investigation of $U_2(R)$ by exploiting the above correspondence in matrices.

Proposition 1. *Let R be a semisimple artinian algebra over a non-absolute field F, $\operatorname{char} F \neq 2$. Then $U_2(R)$ does not contain a free group of rank two if and only if R is a finite direct sum of division algebras.*

Proof. Let $R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_k}(D_k)$ be the Wedderburn decomposition of R where $D_1, \ldots, D_k$ are division rings and suppose that $n_i > 1$, for some i.

Assume first that $\operatorname{char} F = p > 2$. Let P be the prime subfield of F and let $t \in F$ be transcendental over P. We next prove that $M_{n_i}(P(t)) \subseteq M_{n_i}(D_i)$ contains a free group of rank two.

Let e_{hk} denote the usual matrix units of $M_{n_i}(D_i)$ and consider the following elements of R:

$$u_1 = 1 - 2e_{11},\ u_2 = 1 - 2e_{22},$$

$$v = 1 - 2(e_{11} + te_{12}),\ w = 1 - 2(e_{22} + te_{21}).$$

Clearly $u_1, u_2, v, w \in U_2(R)$. Moreover $u_1v = 1 + 2te_{12}$ and $u_2w = 1 + 2te_{21}$ are units of order p and it is well known that they generate a free product $\mathbb{Z}_p * \mathbb{Z}_p$, where $\mathbb{Z}_p$ is the cyclic group of order p. Since $\mathbb{Z}_p * \mathbb{Z}_p$ contains a free group of rank two (see for instance [10, pag. 195]) and $u_1v, u_2w \in U_2(R)$, it follows that the same conclusion holds for $U_2(R)$.

If $\operatorname{char} F = 0$, we construct units $u_1, u_2, v, w \in U_2(R)$ by specializing $t = 1$ in the above, and we obtain that u_1v and u_2w are of infinite order in this case. Since it is well known that u_1v and u_2w generate a free group of rank two in $M_{n_i}(\mathbb{Q})$ (see [14, Theorem 10.1.3]), this completes the proof of the only if part of the proposition.

Conversely, suppose that $R = D_1 \oplus \cdots \oplus D_k$ is a direct sum of division algebras. In this case $U_2(R)$ is an elementary abelian 2-group of order 2^k and, so, it cannot contain a free group of rank two. In fact, if $e_1, \ldots, e_k$ are the minimal central idempotents of R, the elements $\sum_{i=1}^{k} \epsilon_i e_i$ with $\epsilon_i \in \{1, -1\}$, account for all units of R of order at most 2. It is clear that they are 2^k in number and they form an elementary abelian 2-group. □

We next point out two consequences of the previous result in the setting of group algebras. Let FG denote the group algebra of a group G over a field F.

Corollary 2. *Let G be a finite group and let F be a non-absolute field, $\operatorname{char} F \neq 2$, such that either $\operatorname{char} F = 0$ or $\operatorname{char} F = p > 0$ and $p \nmid |G|$. Then, $U_2(FG)$ does not contain a free group of rank two if and only if one of the following conditions holds:*

(i) *G is abelian.*
(ii) *$\operatorname{char} F = 0$, G is a Hamiltonian group of order $2^n m$, where m is odd, the multipliative order of 2 in $\mathbb{Z}_m$ is odd and the equation $x^2 + y^2 = -1$ has no non-trivial solution in every extension field of the form $F(\zeta_d)$ for every primitive d-th root of unity ζ_d with $d \nmid m$.*

Proof. Since FG is semisimple artinian, by the previous proposition if $U_2(FG)$ contains a free group of rank two, then FG is a direct sum of division rings. In this last case all idempotents of G are central and thus G is either abelian or a Hamiltonian group (see [14, p. 227]).

In case G is Hamiltonian it is of the form $G = K_8 \times E \times A$ where K_8 is the quaternion group of order 8, E is an elementary abelian 2-group and A is an abelian group of odd order m. As $FG \cong F(E \times A)K_8$ and $F(E \times A)$ is a direct sum of fields of the form $F(\zeta_d)$ where $d|m$, it follows that FG is a direct sum of rings of the form $F(\zeta_d)K_8$.

It is well known that, when $\operatorname{char} F > 2$, FK_8 contains a copy of the algebra of 2×2 matrices over F and this in turn contains a free group of rank two, so it follows that when G is nonabelian, we must have $\operatorname{char} F = 0$.

Also notice that

$$F(\zeta_d)K_8 \cong F(\zeta_d) \oplus F(\zeta_d) \oplus F(\zeta_d) \oplus F(\zeta_d) \oplus \mathbb{H}_{F(\zeta_d)},$$

where $\mathbb{H}_{F(\zeta_d)}$ denotes the ring of quaternions over $F(\zeta_d)$. It is well-known that this is a division rings if and only if the equation $x^2 + y^2 = -1$ has no solution in $F(\zeta_d)$.

Since this implies that the equation above has no solution also in $\mathbb{Q}(\zeta_d)$ for all d dividing m, it follows that the multiplicative order of 2 in $\mathbb{Z}_m$ is odd (see [12]). □

Notice that an equivalent formulation of Proposition 1 is that $U_2(R)$ does not contain a free group of rank two if and only if R has no nonzero nilpotent elements. Hence, using standard reductions to the finite case, we have the following.

Corollary 3. *Let F be a non-absolute field with $\operatorname{char} F \neq 2$ and let G be a locally finite group such that, when $\operatorname{char} F = p > 0$, G contains no p-elements. Then, $U_2(R)$ does not contain a free group of rank two if and only if FG contains no non-zero nilpotent elements.*

The next result is a simplified version of the lemma in [5, p.4212]

Lemma 4. *Let R be an F-algebra, $\operatorname{char} F = p > 2$ and let $a, b \in R$ be such that $a^2 = b^2 = 0$ and ab is not nilpotent. If $R[t]$ denotes the polynomial ring in an indeterminate t, then $1 + ta$ and $1 + tb$ are units of order p of $R[t]$ and $\langle 1 + ta, 1 + tb\rangle \cong \mathbb{Z}_p * \mathbb{Z}_p$.*

Proof. For any integer k and for any $x \in R$, we have that $(1 + tx)^k = 1 + ktx$. Hence it is clear that $1 + ta$ and $1 + tb$ are units of order p. Suppose, by way of contradiction, that there exists a nontrivial relation of the type

$$(1 + ta)^{k_1}(1 + tb)^{l_1} \cdots (1 + ta)^{k_r}(1 + tb)^{l_r} = 1, \tag{1}$$

for some integers $k_1, l_1, \ldots, k_r, l_r$. By eventually exchanging the role of a and b if necessary, we may clearly assume that $1 \leq k_1, l_1, \ldots, k_r \leq p - 1$. Moreover, by eventually multiplying by $(1+ta)^{i_1}$ on the left and by $(1+ta)^{p-i_1}$ on the right, we may also assume that $1 \leq l_r \leq p - 1$.

By expanding the left hand side of (1) we obtain a relation of the form

$$f_1 t + f_2 t^2 + \cdots + f_{2r} t^{2r} = 0$$

where $f_1, \ldots, f_{2r}$ are elements of the subalgebra generated by a and b and $f_{2r} = k_1 l_1 \cdots k_r l_k (ab)^r$. Since t is an indeterminate, it follows that $f_1 = \cdots = f_{2r} = 0$ and, so, $k_1 l_1 \cdots k_r l_k (ab)^r = 0$. Since $1 \leq k_1, l_1, \ldots k_r, l_r \leq p - 1$, we obtain that $(ab)^r = 0$, contrary to the assumption. □

We also recall the following result of Salwa.

Lemma 5 ([15]). *Let R be an F-algebra, $\operatorname{char} F = 0$. If $a, b \in R$ are such that $a^2 = b^2 = 0$ and ab is not nilpotent, then there exists a positive integer n such that $1 + na$ and $1 + nb$ generate a free group of rank two.*

The following result is an immediate consequence of [13, Theorem 2.3.4].

Lemma 6. *Let G be a group such that G has no p-elements in case $\operatorname{char} F = p > 0$. Then FG has no non-zero nil one-sided ideals.*

Proof. Let $tr : FG \to F$ be the trace function defined by

$$tr(\sum_{g \in G} \alpha_g g) = \alpha_1.$$

Let ρ be a nil right ideal of FG and let $a = \sum_{g \in G} \alpha_g g \in \rho$. For $h \in G$, we have $\sum_{g \in G} \alpha_g g h^{-1} = ah^{-1} \in \rho$ and $tr(ah^{-1}) = \alpha_h$. Since ρ is nil, ah^{-1} is nilpotent. Hence, by [13, Lemma 2.3.3] and by our hypothesis, $\alpha_h = tr(ah^{-1}) = 0$. Thus $a = 0$. □

We are now in a position to prove the main result of this note. For a group G let $T(G)$ denote the set of its torsion elements.

Theorem 7. *Let F be a non-absolute field of characteristic different from two and let G be a group. In case $\operatorname{char} F = p > 2$, suppose that G has no p-elements. If $U_2(FG)$ does not contain a free group of rank two, then $T(G)$ is an abelian or a Hamiltonian group and every subgroup of $T(G)$ is normal in G. The Hamiltonian case can occur only if $\operatorname{char} F = 0$.*

Proof. Suppose that $\operatorname{char} F = p > 2$, let P be the prime subfield of F and let $t \in F$ be transcendental over P. For $g \in T(G)$ of order $o(g)$, let $\hat{g} = 1 + g + \cdots + g^{o(g)-1}$ and set $\tilde{g} = \frac{1}{o(g)}\hat{g}$. The element $\tilde{g}$ is an idempotent and, for every $x, y \in FG$, also the elements

$$\tilde{g} + t(1 - \tilde{g})x\tilde{g} \quad \text{and} \quad \tilde{g} + t\tilde{g}y(1 - \tilde{g})$$

are idempotents of FG. Thus, by the correspondence between units of order two and idempotents, the elements

$$u = 1 - 2\tilde{g}, \quad v = 1 - 2(\tilde{g} + t(1 - \tilde{g})x\tilde{g}) \quad \text{and} \quad w = 1 - 2(\tilde{g} + t\tilde{g}y(1 - \tilde{g}))$$

are units of order two of FG. Notice that in case $\operatorname{char} F = 0$, by specializing t to any integer, we still obtain that the above u, v and w are units of order two.

Now, $uv = 1 - 2t(1 - \tilde{g})x\tilde{g}$ and $uw = 1 + 2t\tilde{g}y(1 - \tilde{g})$ lie in $U_2 = U_2(FG)$. Since $a = -2(1 - \tilde{g})x\tilde{g}$ and $b = 2\tilde{g}y(1 - \tilde{g})$ are square-zero elements, by Lemma 4, either uv and uw generate the free product $\mathbb{Z}_p * \mathbb{Z}_p$ or ab is nilpotent. Since by hypothesis U_2 does not contain a free group of rank two, ab must be nilpotent.

Notice that in case $\operatorname{char} F = 0$, we can invoke Lemma 5 by specializing t to the integer n in that lemma and uv and uw will generate a free group of rank two unless ab is nilpotent. Thus we conclude that in any case, ab must be nilpotent.

Since $\operatorname{char} F \neq 2$, this is the same as to say that

$$(1 - \tilde{g})x\tilde{g}\tilde{g}y(1 - \tilde{g}) = (1 - \tilde{g})x\tilde{g}y(1 - \tilde{g})$$

is nilpotent. Thus $((1-\tilde{g})x\tilde{g}y(1-\tilde{g}))^k = 0$ for some k, and recalling that $1-\tilde{g}$ is also an idempotent, by multiplying by $x\tilde{g}y$ on the left, we obtain that $(x\tilde{g}y(1-\tilde{g}))^{k+1} = 0$, for all $x, y \in FG$. This says that $FG\tilde{g}y(1 - \tilde{g})$ is a nil left ideal of FG.

In view of our hypothesis on G, Lemma 6 implies that

$$FG\tilde{g}y(1-\tilde{g}) = 0.$$

Hence $\tilde{g}y(1-\tilde{g}) = 0$, for all $y \in FG$. We have proved that $\tilde{g}y = \tilde{g}y\tilde{g}$ and, by exchanging the role of $\tilde{g}$ and $1-\tilde{g}$, we obtain that also $y\tilde{g} = \tilde{g}y\tilde{g}$ holds, for all $y \in FG$. Thus $\tilde{g}$ is central in FG. This says that $\langle g \rangle$, the cyclic subgroup generated by g, is normal in G. In particular $T(G)$ is a subgroup and all subgroups of $T(G)$ are normal in G. Also $T(G)$, being torsion, must be abelian or a Hamiltonian group. As we have seen in the proof of Lemma 2, the Hamiltonian case can occur only in case char $F = 0$. □

REFERENCES

[1] A.A. Bovdi, *Free subgroups of the group of units in group algebras*, Publ. Math. Debrecen, **49** (1996), 157-165.

[2] J.Z. Gonçalves, *Free subgroups of units in group rings*, Canad. Math. Bull., **27** (1984), 309-312.

[3] J.Z. Gonçalves, *Free subgroups in subnormal subgroups and the residual nilpotence of the group of units of group rings*, Canad. Math. Bull., **27** (1984), 365-370.

[4] J.Z. Gonçalves, *Free subroups and the residual nipotence of the group of units of modular and p-adic group rings*, Canad. Math. Bull., **29** (1986), 321-328.

[5] J.Z. Gonçalves and D.S. Passman, *Construction of free groups in the group of units of modular group algebras*, Comm. Algebra **24** (1996), 4211-4215.

[6] J.Z. Gonçalves and D.S. Passman, *Free unit groups in group algebras*, J. Algebra, **246** (2001), 226-252.

[7] J.Z. Gonçalves and D.S. Passman, *Unitary units in group algebras*, Israel J. Math., **125**, (2001), 131-155.

[8] J.Z. Gonçalves and D.S. Passman, *Free units in group algebras*, Comm. Algebra, **31**, 5 (2003), 2219-2227.

[9] B. Hartley and P. F. Pickel, *Free subgroups in the unit group of integral group rings*, Canad. J. Math. **32** (1980), 1342-1352.

[10] W. Magnus, A. Karrass and D. Solitar, *Combinatorial Group Theory*, Dover, New York, 1976.

[11] Z. Marciniak and S.K. Sehgal, *Constructing free subgroups of integral group ring units*, Proc. Amer. Math. Soc., **125** (1997), 1005-1009.

[12] C. Moser, *Representation de -1 comme somme de carres dans un corps cyclotomique quelconque*, J. Number Theory, **5** (1973), 139-141.

[13] D. S. Passman, *The Algebraic Structure of Group Rings*, Wiley-Interscience, New York, 1977.

[14] C. Polcino Milies and S. K. Sehgal, *An Introduction to Group Rings*, Kluwer Acad. Publishers, Dordrecht, 2002.

[15] A. Salwa, *On free subgroups of units of rings*, Proc. Amer. Math. Soc. **127** (1999), 2569-2572.

DIPARTIMENTO DI MATEMATICA E APPLICAZIONI, VIA ARCHIRAFI 34, 90123 PALERMO, ITALY
E-mail address: agiambr@unipa.it

INSTITUTO DE MATEMÁTICA E ESTATÍSTICA, UNIVERSIDADE DE SÃO PAULO, 05315-970 - SÃO PAULO - BRAZIL
E-mail address: polcino@ime.usp.br

TRABALHOS DO DEPARTAMENTO DE MATEMÁTICA

TÍTULOS PUBLICADOS

2003-01 COELHO, F.U. and LANZILOTTA, M.A. Weakly shod algebras. 28p.

2003-02 GREEN, E.L., MARCOS, E. and ZHANG, P. Koszul modules and modules with linear presentations. 26p.

2003-03 KOSZMIDER, P. Banach spaces of continuous functions with few operators. 31p.

2003-04 GORODSKI, C. Polar actions on compact symmetric spaces which admit a totally geodesic principal orbit. 11p.

2003-05 PEREIRA, A.L. Generic Hyperbolicity for the equilibria of the one-dimensional parabolic equation $u_t = (a(x)u_x)_x + f(u)$. 19p.

2003-06 COELHO, F.U. and PLATZECK, M.I. On the representation dimension of some classes of algebras. 16p.

2003-07 CHERNOUSOVA, Zh. T., DOKUCHAEV, M.A., KHIBINA, M.A., KIRICHENKO, V.V., MIROSHNICHENKO, S.G., ZHURAVLEV, V.N. Tiled orders over discrete valuation rings, finite Markov chains and partially ordered sets. II. 43p.

2003-08 ARAGONA, J., FERNANDEZ, R. and JURIAANS, S.O. A Discontinuous Colombeau Differential Calculus. 20p.

2003-09 OLIVEIRA, L.A.F., PEREIRA, A.L. and PEREIRA, M.C. Continuity of attractors for a reaction-diffusion problem with respect to variation of the domain. 22p.

2003-10 CHALOM, G., MARCOS, E., OLIVEIRA, P. Gröbner basis in algebras extended by loops. 10p.

2003-11 ASSEM, I., CASTONGUAY, D., MARCOS, E.N. and TREPODE, S. Quotients of incidence algebras and the Euler characteristic. 19p.

2003-12 KOSZMIDER, P. A space C(K) where all non-trivial complemented subspaces have big densities. 17p.

2003-13 ZAVARNITSINE, A.V. Weights of the irreducible $SL_3(q)$-modules in defining characteristic. 12p.

2003-14 MARCOS, E. N. and MARTÍNEZ-VILLA, R. The odd part of a N-Koszul algebra. 7p.

2003-15 FERREIRA, V.O., MURAKAMI, L.S.I. and PAQUES, A. A Hopf-Galois correspondence for free algebras. 12p.

2003-16 KOSZMIDER, P. On decompositions of Banach spaces of continuous functions on Mrówka's spaces. 10p.

2003-17 GREEN, E.L., MARCOS, E.N., MARTÍNEZ-VILLA, R. and ZHANG, P. D-Koszul Algebras. 26p.

2003-18 TAPIA, G. A. and BARBANTI, L. Um esquema de aproximação para equações de evolução. 20p.

2003-19 ASPERTI, A. C. and VILHENA, J. A. Björling problem for maximal surfaces in the Lorentz-Minkowski 4-dimensional space. 18p.

2003-20 GOODAIRE, E. G. and MILIES, C. P. Symmetric units in alternative loop rings. 9p.

2003-21 ALVARES, E. R. and COELHO, F. U. On translation quivers with weak sections. 10p.

2003-22 ALVARES, E.R. and COELHO, F.U. Embeddings of non-semiregular translation quivers in quivers of type $Z\Delta$. 23p.

2003-23 BALCERZAK, M., BARTOSZEWICZ, A. and KOSZMIDER, P. On Marczewski-Burstin representable algebras. 6p.

2003-24 DOKUCHAEV, M. and ZHUKAVETS, N. On finite degree partial representations of groups. 24p.

2003-25 GORODSKI, C. and PODESTÀ, F. Homogeneity rank of real representations of compact Lie groups. 13p.

2003-26 CASTONGUAY, D. Derived-tame blowing-up of tree algebras. 20p.

2003-27 GOODAIRE, E.G. and MILIES, C. P. When is a unit loop *f*-unitary? 18p.

2003-28 MARCOS, E.N., MARTÍNEZ-VILLA, R. and MARTINS, M.I.R. Hochschild Cohomology of skew group rings and invariants. 16p.

2003-29 CIBILS, C. and MARCOS, E.N. Skew category, Galois covering and smash product of a category over a ring. 21p.

2004-01 ASSEM, I., COELHO. F.U., LANZILOTTA, M., SMITH, D.and TREPODE, SONIA Algebras determined by their left and right parts. 34p.

2004-02 FUTORNY, V., MOLEV, A. and OVSIENKO, S. Harish-Chandra Modules for Yangians. 29p.

2004-03 COX, B. L. and FUTORNY, V. Intermediate Wakimoto modules for affine $sl(n+1, C)$. 35p.

2004-04 GRISHKOV, A. N. and ZAVARNITSINE, A. V. Maximal subloops of simple Moufang loops. 43p.

2004-05 GREEN, E.L. and MARCOS, E. δ-Koszul Algebras. 15p.

2004-06 GORODSKI, C. Taut Representantions of compact simple lie groups. 16p.

2004-07 ASPERTI, A.C. and VALÉRIO, B.C. Ruled helicoidal surfaces in a 3-dimensional space form. 9p.

2004-08 ASSEM, I., CASTONGUAY, D., MARCOS, E.N. and TREPODE, S. Strongly simply connected schurian algebras and multiplicative bases. 26p.

2004-09 RODRIGUES, A.A.M., MIRANDA FILHO, R.C. and SOUZA, E.G. Definability and Invariance in First Order Structures. 15p.

2004-10 GIAMBRUNO, A. and MILIES, C. P. Free groups and involutions in the unit group of a group algebra. 5p

Nota: Os títulos publicados nos Relatórios Técnicos dos anos de 1980 a 2002 estão à disposição no Departamento de Matemática do IME-USP.
Cidade Universitária "Armando de Salles Oliveira"
Rua do Matão, 1010 - Cidade Universitária
Caixa Postal 66281 - CEP 05315-970