Free products of units in algebras
Part I: quaternion algebras

Jairo Z. Gonçalves*
Departamento de Matemática, Universidade de São Paulo, São Paulo, SP, Brazil 05508-970
jzg@ime.usp.br

Arnaldo Mandel†
Departamento de Ciência da Computação, Universidade de São Paulo, São Paulo, SP, Brazil 05508-970
am@ime.usp.br

Mazi Shirvani‡
Department of Mathematical Sciences, University of Alberta, Edmonton, Alberta, Canada T6G 2G1
mazi@schur.math.ualberta.ca

August 31, 1998

Abstract

Let A be a quaternion algebra over a commutative unital ring. We find sufficient conditions for pairs of units of A to generate a free group. Using the well-known isomorphism between $SO(3, \mathbb{R})$ and the group of real quaternions of norm 1, we obtain free groups of rotations of the Euclidean 3-space. Specialization techniques allow us to find similar free subgroups in skew polynomial rings. A consequence is the following: let kG be the group algebra of a residually (torsion-free nilpotent) group G over a field k whose characteristic is not 2. If x and y are any pair of non-commuting elements of G, and $c, d \in k^*$ then $1 + cx$ and $1 + dy$ generate a free subgroup of the Malcev-Neumann field of fractions of kG.

*Research partially supported by CNPq.

†Research partially supported by CNPq, by FAPESP Proc. 96/4505–2 and MCT/FINEP, Projeto PRONEX 107/97.

‡Research partially supported by NSERC.

1 Introduction

The existence of free noncyclic subgroups of the multiplicative group of a division ring was conjectured by Lichtman[13], and has been widely investigated [8], [9], [14], [15], [19], [21]. The conjecture was proved [6], [19] in the case where the ring is finite-dimensional over its centre. Either proof makes use of the Tits' Alternatives Theorem [24], and consequently, does not exhibit the free groups explicitly.

We address the question of explicitly finding pairs of elements such that the subgroup they generate is the free product of the respective cyclic subgroups. Given groups $H \lhd G$ we say that a pair $\{g_1, g_2\}$ of elements of G is *semifree modulo* H provided that the images $\bar{g}_1, \bar{g}_2$ in G/H satisfy:

a. The group $\langle \bar{g}_1, \bar{g}_2 \rangle$ is the free product $\langle \bar{g}_1 \rangle * \langle \bar{g}_2 \rangle$.

b. $\bar{g}_1$ has order at least 3 and $\bar{g}_2$ has order 2 (the condition on $\bar{g}_2$ is convenient, that on $\bar{g}_1$ is to avoid $\mathbb{Z}_2 * \mathbb{Z}_2$).

If H is the centre of G, we say that the pair is *semifree modulo centre*, and if $H = \{1\}$, then the pair is *semifree*. We also say that the pair is *free* if it freely generates a free group. Notice that from a semifree pair one can easily obtain free pairs.

All rings are assumed to be unital, and $\mathcal{U}X$ denotes the group of units of the ring X. For a commutative ring R of characteristic different from 2, and elements a, b of R^*, the quaternion algebra $\left(\frac{a,b}{R}\right)$is defined as follows: as an R-module, $\left(\frac{a,b}{R}\right) = R \oplus P$, where P (the *pure quaternions*) is a rank-3 free R-module with basis $\{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$, with $\mathbf{i}^2 = a, \mathbf{j}^2 = b, \mathbf{ij} = -\mathbf{ji} = \mathbf{k}$. Our main results on these algebras are as follows:

Theorem 1 *Let R be an integral domain of characteristic $\neq 2$ with quotient field Q, and let $a, b, \alpha, \beta \in R^*$. Suppose that there exists a non-archimedean valuation ν on $R[\mathbf{i}]$ such that $\nu(a) = \nu(b) = \nu(\beta) = 0$ and $\nu(1 + \alpha\mathbf{i}) \neq \nu(1 - \alpha\mathbf{i})$. Then $\{1 + \alpha\mathbf{i}, \mathbf{i} + \beta\mathbf{j}\}$ is semifree modulo centre in $\mathcal{U}\left(\frac{a,b}{Q}\right)$.*

Theorem 2 *Let R be an integral domain of characteristic $\neq 2$ with quotient field Q, and let $a, b, \alpha, \beta \in R$. Suppose that there exists a non-archimedean valuation ν on the field $Q(\sqrt{a}, \sqrt{b})$, such that $\nu(a) = \nu(b) = \nu(\alpha) = \nu(\beta) = 0$, $\nu(1+\alpha\sqrt{a}) \neq \nu(1-\alpha\sqrt{a})$, and $\nu(1+\beta\sqrt{b}) \neq \nu(1-\beta\sqrt{b})$. Then $\{1+\alpha\mathbf{i}, 1+\beta\mathbf{j}\}$ is a free pair in $\mathcal{U}\left(\frac{a,b}{Q}\right)$.*

Given the well known isomorphism of $SO(3,\mathbb{R})$ and the group of real quaternions of norm 1, the above apply in several different forms to exhibit free groups of rotations in Euclidean 3-space. Results by de Groot [10], Dekker [3], Świerczkowski [23] will follow, as well as a generalization of one by Hausdorff [12].

In characteristic 2, quaternion algebras have to be defined differently ([2], [4]): if F is a field of characteristic 2 and $a, b \in F^*$, let $\left(\frac{a,b}{F}\right] = F + F\mathbf{i} + F\mathbf{j} + F\mathbf{ij}$, with the defining relations $\mathbf{i}^2 = \mathbf{i} + a$, $\mathbf{j}^2 = b$, $\mathbf{ji} = (\mathbf{i}+1)\mathbf{j}$. Our main result on these algebras is the following:

Theorem 3 *Let F be a field of characteristic 2, and consider the quaternion algebra $\left(\frac{a,b}{F}\right]$. Let $\alpha \in F^*$. Assume that $b \neq 1$, and that there is a valuation ν on $\mathbb{F}_2(a, b, \alpha, \mathbf{i}) \subseteq F(\mathbf{i})$ such that $\nu(b) = 0$ and $\nu(a + \alpha^{-1} + \alpha^{-2}) > 0$. Then $\{1 + \alpha\mathbf{i}, 1 + \mathbf{j}\}$ is semifree modulo centre in $\mathcal{U}\left(\frac{a,b}{F}\right]$.*

In a sequel to this paper we will prove analogous results about more general cyclic algebras.

Even though quaternions are a very restricted class of rings, the above results enable us to find free pairs in larger classes of rings. We will show examples of free pairs in fields of fractions of some skew polynomial rings and group algebras. These are obtained by suitable specializations to quaternion algebras. In particular, here are two applications:

Consider the first Weyl algebra $A_1(\mathbb{Q}) = \mathbb{Q}<s,t>/<ts - st - 1>$, an Ore domain with a classical field of fractions.

Theorem 4 *$\{1 + st, 1 + s\}$ is semifree modulo some subgroup in the field of fractions of $A_1(\mathbb{Q})$.*

To appreciate this fully, note the following (unpublished) example of A. Lichtman: in $A_1(\mathbb{Q})$, the pair $\{1+s, 1+t\}$ is *not* free, since it does not even generate a free semigroup. Just notice that, if $S = 1+s, T = 1+t$, then $TS - ST = 1$, so TS and ST commute.

As another application, let L be a Lie algebra over a field K of characteristic 0, such that its enveloping algebra $U(L)$ is Ore. Lichtman [17] showed that if x, y are noncommuting elements of L, there exists a specialization of $U(L)$ onto $A_1(K)$ such that $(yx^{-1} - x^{-1}y)^{-1} \mapsto s$ and $\frac{x^{-1}y}{2} \mapsto t$. This can be combined with Theorem 4 to produce explicit free pairs in $U(L)$.

Eizenbud and Lichtman [5] have constructed a Malcev-Neumann field of fractions for the group rings of residually (torsion-free nilpotent) groups (it is not known whether this is the universal field of fractions of the group ring.) We close the paper with the following consequence of the previous results which, in the nilpotent case, answers a question of J. Lewin:

Theorem 5 *Let k be a field of characteristic not 2, and let G be a residually (torsion-free nilpotent) group. If x, y are any pair of non-commuting elements of G, and $c, d \in k^*$ then the group $\langle 1 + cx, 1 + dy \rangle$ is free in the Malcev-Neumann field of fractions of kG.*

We are thankful to A. I. Lichtman for bringing this application to our attention, and for making very useful comments on the earlier versions of this paper.

2 Proofs of the Main Theorems

The basic tool for proving Theorems 1, 2, and 3, is the Table-Tennis Lemma, which has long been used for the recognition of free products (see [18]). Here is a version specially tailored for semifree pairs:

Table-Tennis Lemma: *Let G be a group acting on a set X, and let $g_1, g_2 \in G$, where g_1 has order at least 3 and g_2 has order 2. Suppose that there exist distinct nonempty subsets X_1 and X_2 of X such that $(X_1)g_2 \subseteq X_2$ and, for all integers n such that $g_1^n \neq 1$, $(X_2)\, g_1^n \subseteq X_1$. Then the pair $\{g_1, g_2\}$ is semifree.*

The following elementary result will be used without further reference.

Proposition 6 (1) *If a group morphism maps a pair of elements to a free pair, then the original pair is also free.*

(2) *Suppose that $\{g_1, g_2\}$ is semifree in G modulo H. Then, the following pairs are free in G:*

a. $\{g_1^n g_2, g_1^m g_2\}$, *with n, m distinct nonzero integers;*

b. $\{g_1, g_2 g_1 g_2\}$, *provided $\bar{g}_1$ has infinite order in G/H.*

Proof: (a) Any identity satisfied by the original pair would be satisfied by the images.

(b) The image of each pair is clearly free in G/H, hence lifts to a free pair in G. $\square$

Proof of Theorem 1: Let $F = Q(\mathbf{i})$, so $T = \left(\frac{a,b}{Q}\right) = F \oplus F\mathbf{j}$. Let

$$X_1 = \{x + y\,\mathbf{j} \in T : \nu(x) = \nu(y)\}$$

$$X_2 = \{x + y\,\mathbf{j} \in T : \nu(x) \neq \nu(y)\}.$$

If $n \neq 0$, then $(x + y\,\mathbf{j})(1 + \alpha\mathbf{i})^n = x(1 + \alpha\mathbf{i})^n + y(1 - \alpha\mathbf{i})^n\mathbf{j}$, which is in X_2 if $x + y\mathbf{j} \in X_1$. In other words, $X_1(1 + \alpha\mathbf{i})^n \subseteq X_2$. Similarly, $(x + y\mathbf{j})(\mathbf{i} + \beta\mathbf{j}) = (\mathbf{i}x + b\beta y) + (\beta x - \mathbf{i}y)\mathbf{j} \in X_1$ provided that $x + y\mathbf{j} \in X_2$, since the coefficients $\mathbf{i}$, b, and β, all have valuation zero. The result follows from the Table-Tennis Lemma. $\square$

Proof of Theorem 2: The proof uses the same apparatus as in the previous case. However, since $1 + \beta\mathbf{j}$ no longer has order 2, we need a formula for its powers. Since $Q(\mathbf{j})$ is a quadratic extension of Q, for all integers n we have:

$$(1 + \beta\,\mathbf{j})^n = d_n(1 + r_n\,\mathbf{j})$$

for some $d_n, r_n \in F$, and standard techniques show that

$$r_n = \frac{1}{\sqrt{b}}\left(\frac{\theta^n - 1}{\theta^n + 1}\right)$$

where

$$\theta = \frac{1 + \beta\sqrt{b}}{1 - \beta\sqrt{b}}.$$

As in the previous proof, $X_1(1 + \alpha\mathbf{i})^m \subseteq X_2$ for every non-zero integer m. Next, $\nu(\theta) \neq 0$ by assumption, whence, for $n \neq 0$, we also have $\nu(r_n) = 0$. Now, if n is a non-zero integer, then $(1 + \beta\mathbf{j})^n$ maps the element $x + y\,\mathbf{j}$ to a scalar multiple of $u = (x + r_n by) + (r_n x + y)\,\mathbf{j}$. If $x + y\,\mathbf{j} \in X_2$ (so $\nu(x) \neq \nu(y)$), then since the coefficients have valuation zero, the coefficients of u have equal valuation $\min(\nu(x), \nu(y))$. In other words, $X_2(1 + \beta\mathbf{j})^n \subseteq X_1$ for every non-zero integer n. The result follows from the usual form of the Table-Tennis Lemma (as in [18]). $\square$

Proof of Theorem 3: We use the same sets X_1 and X_2 introduced in the proof of Theorem 1. The conditon $b \neq 1$ ensures that $(1+\mathbf{j})^2 = b+1 \in F^*$, so $1+\mathbf{j}$ has order 2 modulo the centre. Since $(x + y\,\mathbf{j})(1 + \alpha\,\mathbf{i}) = x(1 + \alpha\,\mathbf{i}) + y(1 + \alpha + \alpha\,\mathbf{i})\mathbf{j}$, the proof may be concluded exactly as before, once we have proven that $\nu(1+\alpha\mathbf{i}) \neq \nu(1+\alpha+\alpha\mathbf{i})$. To begin with, write $f = a\alpha^2 + \alpha + 1 = (1 + \alpha\mathbf{i})(1+\alpha+\alpha\mathbf{i})$. Then $\nu(f) = 2\nu(\alpha) + \nu(a + \alpha^{-1} + \alpha^{-2}) \neq -\infty$, so $f \neq 0$, and $1+\alpha\mathbf{i}, 1+\alpha+\alpha\mathbf{i}$ are units. Let $x = \frac{1+\alpha+\alpha\mathbf{i}}{1+\alpha\mathbf{i}}$, so we need to show that $\nu(x) \neq 0$. Since $x + x^{-1} = \frac{\alpha^2}{f}$, it follows that $\nu(x + x^{-1}) = -\nu(a + \alpha^{-1} + \alpha^{-2}) < 0$, hence $\nu(x) \neq 0$. $\square$

3 Rotations

Throughout this section, the rings have characteristic different from 2. The pure quaternions P are invariant under ring automorphisms, so there is a homomorphism $\rho : \mathcal{U}\left(\frac{a,b}{R}\right) \to GL(3, R)$, given by $v(x\rho) = x^{-1}vx$ for all $v \in P$. Indeed, as this factors over the centre, we may consider its domain to be $\mathcal{U}\left(\frac{a,b}{R}\right)/\mathcal{Z}\left(\mathcal{U}\left(\frac{a,b}{R}\right)\right)$. In particular, for the Hamilton quaternions $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$, the domain can be thought of (by choice of representatives) as the quaternions of norm 1, and the image is $SO(3, \mathbb{R})$.

It will be useful to write ρ explicitly in rings of symmetric quaternions, using the ordered basis $\{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$ for the pure quaternions:

Lemma 7 *Identify R^3 with the set P of pure quaternions, and let $\rho : \mathcal{U}\left(\frac{a,a}{R}\right) \to GL(3, R)$ be the group homomorphism defined by $v(x\rho) = x^{-1}vx$ for all $v \in P$. One has:*

$$\begin{aligned}
(\mathbf{i}+\mathbf{j})\rho &= \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \\
(\alpha + \beta\,\mathbf{i})\rho &= (\alpha^2 - \beta^2 a)^{-1} \begin{pmatrix} \alpha^2 - \beta^2 a & 0 & 0 \\ 0 & \alpha^2 + \beta^2 a & -2\alpha\beta \\ 0 & -2\alpha\beta a & \alpha^2 + \beta^2 a \end{pmatrix}
\end{aligned}$$

provided that $\alpha^2 - \beta^2 a$ is a unit in R. In particular, this gives an explicit embedding of $\mathcal{U}\left(\frac{a,a}{R}\right)/\mathcal{U}(R)$ into $GL(3, R)$.

Proof: Straightforward computation of the action on the basis $\{\mathbf{i},\mathbf{j},\mathbf{k}\}$ gives the formula. For the embedding, just notice that the centre of $\mathcal{U}\left(\frac{a,a}{R}\right)$ is $\mathcal{U}(R)$. $\square$

Corollary 8 *If t is an indeterminate over R, then for any $a \in R^*$, the pair $\{1+t\mathbf{i}, 1+t\mathbf{j}\}$ is free in the ring $\left(\frac{a,a}{R[t]}\right)$.*

Proof: Consider the valuation ν of $R[t][\mathbf{i}])$ given by the principal ideal generated by $1-t\mathbf{i}$. Then, $\nu(1+t\mathbf{i}) = 0$, $\nu(1-t\mathbf{i}) = 1$, and the result follows from Theorem 2. $\square$

In the real case, it is useful to have a dictionary between the languages of rotations and quaternions. A rotation of angle θ about the $\mathbf{i}$-axis is usually represented by $(\cos\frac{\theta}{2} + \sin\frac{\theta}{2}\mathbf{i})\rho = (1+\tan\frac{\theta}{2}\mathbf{i})\rho = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{pmatrix}$, to which any other rotation of angle θ is conjugate. In particular, a rotation about an axis in the $\mathbf{i}-\mathbf{j}$-plane, at an angle ϕ with $\mathbf{i}$ will be, as a quaternion, the conjugate of the above by $\cos\frac{\phi}{2}\mathbf{i} + \sin\frac{\phi}{2}\mathbf{j}$, or more conveniently, by $1+\tan\frac{\phi}{2}\mathbf{i}$. Indeed, we will favour the "tangent" form of quaternions over the traditional norm 1 format, as it makes the computations easier, with no loss of generality.

Corollary 9 *[de Groot [10]] If $\theta \in \mathbb{R}$ is such that $\cos\theta$ is transcendental, then any pair of rotations of angle θ on perpendicular axes form a free pair.*

Proof: If $\cos\theta$ is transcendental, then so is $\alpha = \tan\frac{\theta}{2}$. Hence, the statement amounts to saying that $\{1+\alpha\mathbf{i}, 1+\alpha\mathbf{j}\}$ is free; this follows from the preceding result. $\square$

Corollary 10 *If $\theta \in \mathbb{R}$ is such that the complex number $z = \cos\theta + \sin\theta\mathbf{i}$ is algebraic, but not an algebraic integer, then any pair of rotations of angle θ on perpendicular axes, is free.*

Proof: The number field $\mathbb{Q}[z,\mathbf{i}]$ affords a valuation ν such that $\nu(z) < 0$. If $\alpha = \tan\frac{\theta}{2}$, then one quickly verifies that $z = \frac{(1+\alpha\mathbf{i})^2}{1+\alpha^2} = \frac{1+\alpha\mathbf{i}}{1-\alpha\mathbf{i}}$, whence $\nu(1+\alpha\mathbf{i}) = \nu(z) + \nu(1-\alpha\mathbf{i})$. Now apply Theorem 2. $\square$

The following result was proved after a considerable *tour de force* by Świerczkowski [23]:

Corollary 11 *If* $\cos\theta$ *is rational, then a pair of rotations by angle* θ*, on perpendicular axes, is free if and only if* $\cos\theta \neq 0, \pm\frac{1}{2}, \pm 1$.

Proof: It is easy to see that the excluded cases are exactly those in which $\cos\theta + \sin\theta\mathbf{i}$ is an algebraic integer, so one gets a free group in all the other cases (by the previous corollary). The excluded cases are not free, since then $\cos\theta + \sin\theta\mathbf{i}$ is a root of 1. $\square$

At this point, the only cases that remain are those in which $\zeta = \cos\theta + \sin\theta\mathbf{i}$ is an algebraic integer. We do not know what happens when ζ has infinite order, but for finite order one can settle the matter completely.

Proposition 12 *Suppose that* $\zeta = \cos\theta + \sin\theta\mathbf{i}$ *is a primitive* n*-th root of 1. Then, the pair* $\{\cos\theta + \sin\theta\mathbf{i}, \mathbf{i}+\mathbf{j}\}$ *is not semifree modulo centre if either* $n = 2$ *or* $4|n$*, and is semifree modulo centre otherwise.*

Proof: The case $n = 2$ is trivial, and when $4|n$, the $\dfrac{n}{4}$-th power of the first term is $\pm\mathbf{i}$, and $(\mathbf{i}(\mathbf{i}+\mathbf{j}))^4$ is central. Next, consider the case where n is odd.

First notice that if $0 < k < n$, then $\zeta^k + 1$ is a unit in $\mathbb{Z}[\zeta]$; indeed, as $1 - X^n = \prod_{k=0}^{n-1}(\zeta^k - X)$, evaluation at $X = -1$ leads to the identity $\prod_{k=1}^{n-1}(\zeta^k + 1) = 1$. Next, as n is odd, ζ^4 is also a primitive n-th root, so $\zeta^{4k}+1$ is also a unit. It follows that $2\cos 2k\theta = \zeta^{-2k}(\zeta^{4k}+1)$ is also a unit. Hence, if ν is the valuation of $\mathbb{Q}[\zeta]$ induced by the prime 2, then $\nu(\cos 2k\theta) = -1$, and since $\nu(\cos^2 2k\theta + \sin^2 2k\theta) = 0$, it follows that $\nu(\sin 2k\theta) = \nu(\cos 2k\theta)$. Now, Lemma 7 gives an embedding of $\mathbb{H}^*/\mathbb{R}^*$ into $GL(3,\mathbb{R})$, so it is enough to show that $\{\zeta\rho, (\mathbf{i}+\mathbf{j})\rho\}$ is semifree, thus generating a group isomorphic to $\mathbb{Z}_n * \mathbb{Z}_2$. Using Lemma 7 we have, for $0 < k < n$:

$$2(\zeta^k\rho) = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2\cos(2k\theta) & -2\sin(2k\theta) \\ 0 & 2\sin(2k\theta) & 2\cos(2k\theta) \end{pmatrix}$$

In other words, $2(\zeta^k\rho)$ has the form $\left(\begin{smallmatrix} + & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{smallmatrix}\right)$, where the $+$ entry has positive valuation, and the $*$ entries have zero valuation.

If $\{\zeta\rho, (\mathbf{i}+\mathbf{j})\rho\}$ were not semifree, then there would exist a sequence $n_1, n_2, \ldots, n_k$ of integers, each between 1 and $n-1$, such that

$$(\zeta\rho)^{n_1}(\mathbf{i}+\mathbf{j})\rho(\zeta\rho)^{n_2}(\mathbf{i}+\mathbf{j})\rho \cdot \ldots \cdot (\zeta\rho)^{n_k}(\mathbf{i}+\mathbf{j})\rho = \mathrm{I}.$$

Defining $A_s = 2^{n_s}(\zeta\rho)^{n_s}(\mathbf{i}+\mathbf{j})\rho$, it follows that $A_1 A_2 \cdot \ldots \cdot A_k = 2^m \mathrm{I}$, where $m = \sum_{s=1}^{k} n_s > 0$. As each A_s has all its entries in the valuation ring of ν, we may pass to the corresponding residue field, where each A_s becomes of form $\begin{pmatrix} 0 & 0 & 0 \\ * & 0 & * \\ * & 0 & * \end{pmatrix}$, with $*$ representing nonzero elements, so the product of $A_s's$ has the same form. On the other hand, $2^m\mathrm{I} = 0$ over the residue field since $m > 0$, a contradiction.

Finally, consider the case $n = 2m$, where m is odd. Then $\zeta^m = -1$ is central, and ζ has order m modulo centre. Therefore, $\langle\zeta\rangle = \langle\zeta^2\rangle$ modulo centre, so it is sufficient to prove that $\{\zeta^2, \mathbf{i}+\mathbf{j}\}$ is semifree. As ζ^2 is a primitive m-th root of unity, this case follows from the previous one. □

The case $n = 6$, which yields a free product $\mathbb{Z}_3 * \mathbb{Z}_2$, is due to Hausdorff [12]. It is worth pointing out that the technique used in this last proof can be also adapted to prove a special case of Theorem 1, where $a = b, \beta = 1$.

It is worthwhile to review Corollary 9 from another viewpoint. A pair of quaternions is semifree modulo centre if, for every nontrivial word in the abstract free product of the corresponding (mod centre) cyclics, the actual value has nonzero pure part. Now, replace one member of the pair by its conjugate by $x + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}$. Each word now results in a quaternion whose entries are rational functions of x, y, z, w. The requirement that the pure part be nonzero is equivalent to the statement that a specific polynomial is nonzero. It follows that if one replaces x, y, z, w by algebraically independent transcendentals over the field generated by $\mathbb{Q}$ and the coefficients of the original pair, then the new pair will still be semifree modulo centre.

To be more specific, suppose that in the cases examined above instead of perpendicular rotation axes we consider rotations at an arbitrary angle ϕ. Then, the role of $\mathbf{i}+\mathbf{j}$ is taken by $\mathbf{i}+\beta\mathbf{j}$, where $\beta = \tan\frac{\phi}{2}$. Applying the same argument as before, we are led to considering polynomials in β. The propositions above show, upon substituting $\beta = 1$, that these polynomials are all nonzero; hence, there are countably many values of β for which the rotated pair fail to generate a free product (a slightly more cumbersome variation of this argument appears in [1]). In particular, if β is transcendental over the field generated by the original two matrices, we have semifree pairs also.

Corollary 13 *Two rotations through the same angle θ, on axes at an angle ϕ, form a free pair provided $\cos\theta$ is transcendental over $\mathbb{Q}(\cos\phi)$.*

Proof: As remarked before, we may assume that one rotation has axis $\mathbf{i}$, and the other has its axis in the $\mathbf{i}$-$\mathbf{j}$-plane. Let $\alpha = \tan\frac{\theta}{2}, \beta = \tan\frac{\phi}{2}$; the hypothesis implies that α is transcendental over $\mathbb{Q}(\beta)$, and so over $\mathbb{Q}(\beta)[\mathbf{i}]$. Hence, the valuation defined by the principal ideal generated by $1-\alpha\mathbf{i}$ clearly satisfies the requirements of Theorem 1. Then $\langle 1+\alpha\mathbf{i}, \mathbf{i}+\beta\mathbf{j}\rangle$ is semifree modulo centre, and so the required rotations, being the ρ-images of $1+\alpha\mathbf{i}$ and $(\mathbf{i}+\beta\mathbf{j})^{-1}(1+\alpha\mathbf{i})(\mathbf{i}+\beta\mathbf{j})$, form a free pair. $\square$

De Groot, on proving Corollary 9, asked whether the same result was true with arbitrary distinct rotation axes. That was proved by Dekker[3], but there is a mistake in the proof, and indeed the result as suggested by De Groot is not true. To see this, choose any transcendental $\alpha > 1$ and let $\beta = \sqrt{\frac{\alpha^2-1}{\alpha^2+1}}$. If $w = (1+\alpha\mathbf{i})(\mathbf{i}+\beta\mathbf{j}) \in \mathbb{H}$, then w^2 is a pure quaternion, hence w^4 is central. It follows that $\langle 1+\alpha\mathbf{i}, \mathbf{i}+\beta\mathbf{j}\rangle$ is not semifree modulo centre, hence the rotations by angle $\theta = 2\arctan\alpha$, with axes inclined at an angle $\phi = 2\arctan\beta$ do not form a free pair, even though $\cos\theta$ is transcendental. From this idea one can get many more examples to show that the hypothesis of Corollary 13 cannot be easily weakened. Dekker's proof, while wrong for the intended result, is correct for Corollary 13.

4 A Special Case

Consider the direct product of a cyclic group of odd prime order p and the quaternion group of order 8, and the corresponding integral group ring. In the Wedderburn decomposition of the rational group algebra, one of the components contains the quaternion ring $\left(\frac{-1,-1}{\mathbb{Z}[\theta]}\right)$, where θ is a primitive p-th root of 1; in [11] it is shown how to obtain a free group in the units of the group ring from a free group of quaternions. The latter appears on applying Tits' Criterion to show that $\langle (1+\theta\mathbf{i})^m, (1+\theta\mathbf{j})^m\rangle$ is a free group for some integer $m > 0$.

That proof gives no explicit m, and we do not know of a case where $m = 1$ can be proved not to work - we present below an $O(p)$ bound for m. It would have been fortunate if Theorem 1 could be applied here, but this is not possible: there is no nonarchimedean valuation separating these two, since $1 \pm \theta\mathbf{i}$ are units in $\mathbb{Z}[\theta, \mathbf{i}]$ (see the proof of Proposition 12.)

In order to handle this case, one has to resort to the archimedean absolute value in $\mathbb{C}$; still some ideas from the proof of Theorem 1 can be used, and by following through with the computations we will give an idea of how much harder this case is. As before, we seek conditions for $\{(1+\theta\mathbf{i})^m, \mathbf{i}+\mathbf{j}\}$ to be semifree modulo centre. Regard the algebra as a $\mathbb{Q}[\theta, \mathbf{i}]$-vector space with basis $\{1, \mathbf{j}\}$. The right regular action then yields the matrices

$$1+\theta\mathbf{i} \mapsto \begin{pmatrix} 1+\theta\mathbf{i} & 0 \\ 0 & 1-\theta\mathbf{i} \end{pmatrix}, \qquad \mathbf{i}+\mathbf{j} \mapsto \begin{pmatrix} \mathbf{i} & 1 \\ -1 & -\mathbf{i} \end{pmatrix}.$$

Here it is convenient to identify $PGL(2,\mathbb{C})$ with the group of Möbius transformations of $\mathbb{C}\cup\{\infty\}$ in the usual way; thus, $1+\theta\mathbf{i}$ maps to $g_1(x) = \dfrac{1+\theta i}{1-\theta i}\, x$, and $\mathbf{i}+\mathbf{j}$ maps to $g_2(x) = \dfrac{ix+1}{-x-i} = \dfrac{x-i}{ix-1}$.

Proposition 14 *The Möbius transformations $g_1(x) = \lambda x, g_2(x) = \frac{x-i}{ix-1}$ form a semifree pair if $0 < |\lambda| < 3-2\sqrt{2}$.*

Proof: Denote $\sigma = \sqrt{2}-1$; the stated bound is $0 < |\lambda| < \sigma^2$. We will use the Table-Tennis Lemma, choosing subsets of $\mathbb{C}\cup\{\infty\}$. Let

$$\begin{aligned} X_1 &= N_< \cup N_>, \quad N_< = \{x : |x| < \sigma\}, \quad N_> = \{x : |x| > \sigma^{-1}\}, \\ X_2 &= \{x : \sigma < |x| < \sigma^{-1}\}. \end{aligned}$$

1. $g_2(X_1) \subset X_2$.

   First we show that $g_2(N_<) \subset X_2$. Let $x = a+bi \in N_<$, $\mu = |x|$. Then $|g_2(x)|^2 = \left|\frac{a+(b-1)i}{-b-1+ai}\right|^2 = \frac{a^2+(b-1)^2}{a^2+(b+1)^2} = \frac{\mu^2-2b+1}{\mu^+2b+1}$. With μ fixed b ranges from $-\mu$ to μ and this expression monotonically decreases with b, therefore

   $$\left(\frac{1-\mu}{1+\mu}\right)^2 \le |g_2(x)|^2 \le \left(\frac{1+\mu}{1-\mu}\right)^2.$$

   As $0 \le \mu < \sigma < 1$, this yields the bounds

   $$\frac{1-\sigma}{1+\sigma} < |g_2(x)| < \frac{1+\sigma}{1-\sigma}.$$

   The trivial fact that $\frac{1-\sigma}{1+\sigma} = \sigma$ implies that $g_2(x) \in X_2$.

   If $x \in N_>$, then $x^{-1} \in N_<$, hence $g_2(x^{-1}) \in X_2$. It follows that $g_2(x) = (g_2(x^{-1}))^{-1} \in X_2$, whence $g_2(N_>) \subset X_2$.

2. $g_1^n(X_2) \subset X_1$ for every $n \neq 0$.

   As $g_1(N_<) \subset N_<$ and $g_1^{-1}(N_>) \subset N_>$, it is enough to show that $g_1(X_2) \subset N_<$ and $g_1^{-1}(X_2) \subset N_>$. Recalling that $|\lambda| < \sigma^2$, note that if $x \in X_2$, $|g_1(x)| = |\lambda x| < \sigma^2\sigma^{-1} = \sigma$, and similarly $|g_1^{-1}(x)| > \sigma^{-1}$, so the result follows.

$\square$

The usefulness of the above lies in the fact that $\left|\dfrac{1+\theta i}{1-\theta i}\right| \neq 1$, when θ is not real, in sharp contrast with the rotations in Section 3.

Proposition 15 *If $\theta = e^{2\pi i/p}, p \geq 3$, then the pair $\{(1+\theta\mathbf{i})^m, \mathbf{i}+\mathbf{j}\}$ is semifree provided that one of the following holds:*

1. *$p = 3$, and $m \geq 2$.*
2. *$p = 5$, and $m \geq 1$.*
3. *$p \geq 6$, and $m \geq \lceil \frac{L}{2\pi} p \rceil$, where $L = \log(3+2\sqrt{2})$* ($\lceil x \rceil$ denotes x rounded up to the next integer).

Proof: In view of the previous result, we seek the smallest m such that $\left|\dfrac{1+\theta\mathbf{i}}{1-\theta\mathbf{i}}\right|^m < 3-2\sqrt{2}$. Elementary manipulations shows that $\left|\frac{1+\theta\mathbf{i}}{1-\theta\mathbf{i}}\right| = \frac{1-t}{1+t}$, where $t = \tan(\pi/p)$. Hence, $m(p) = \lceil f(p) \rceil$, where $f(p) = \frac{L}{\log\frac{1+t}{1-t}}$. Here are some computed values — for each i, the first $p \geq 6$ such that $m(p) = i$:

i	2	3	4	5	6	7	8	9
p	6	9	12	15	19	22	26	29

To get the estimate, notice that for $0 < t < 1$,

$$\log\frac{1+t}{1-t} = \log(1+t) - \log(1-t) = 2(t + \frac{t^3}{3} + \frac{t^5}{5} + \cdots) > 2(t + \frac{t^3}{3}),$$

hence

$$\begin{aligned} f(p) &< \frac{L}{2t}(1 - \frac{t^2}{3} + \frac{t^4}{9} - \cdots) \\ &< \frac{L}{2t}(1 - \frac{t^2}{3} + \frac{t^4}{9}) \\ &= \frac{L}{2t} - \frac{Lt}{6}(1 - \frac{t^2}{3}). \end{aligned}$$

Since $t = \tan\frac{\pi}{p} > \frac{\pi}{p}$ and the right-hand side decreases as $t \to 0$, we finally obtain:

$$\begin{aligned} f(p) &< \frac{L}{2\pi}p - \frac{L\pi}{6p}(1 - \frac{\pi^2}{3p^2}) \\ &< \frac{L}{2\pi}p, \quad \text{for } p > 2. \end{aligned}$$

The result follows. A similar technique shows that $f(p) > \frac{L}{2\pi}p - 1$, so that $\lfloor \frac{L}{2\pi}p \rfloor \leq m(p) \leq \lceil \frac{L}{2\pi}p \rceil$ (and computations suggest that $m(p)$ rarely meets the lower bound); we do not present the details, as this does not shed light on the main issue.

□

The authors are indebted to Y. Kohayakawa for the last part of the estimate.

5 Weyl Algebras and Skew Polynomial Rings

Fields of fractions of skew polynomial rings are a common way of describing division rings. Sometimes the description hides a quaternion algebra or a specialization to one. By recovering the appropriate morphisms, we can exhibit free pairs in some of these algebras. We begin with the following result.

Proposition 16 *Let X, Y be commuting indeterminates over a field k. Then $\{1+\mathbf{i}, 1+\mathbf{j}\}$ is free (resp. semifree) in the quaternion algebra $\left(\frac{X,Y}{k(X,Y)}\right)$ (resp. $\left(\frac{X,Y}{k(X,Y)}\right]$, when char $k = 2$).*

Proof: Use the appropriate result (Theorem 2 or Theorem 3), with $\alpha = \beta = 1$. The fields one needs to look at are purely transcendental extensions of k, so the existence of the required valuations is trivial. □

Proposition 17 *Let Q be the field of fractions of the skew polynomial ring $R = k(X)[Y; \theta]$, where k is a field of characteristic 2, X is an indeterminate, and θ is the automorphism of $k(X)$ given by $X^\theta = X + 1$. Then, the pair $\{1 + X, 1 + Y\}$ is semifree in Q.*

Proof: Direct computation shows that $\alpha = X^2 + X$ and $\beta = Y^2$ are central in Q. It follows that $Q = \left(\frac{\alpha,\beta}{k(\alpha,\beta)}\right]$. Since α, β are algebraically independent over k, the result follow from Proposition 16. $\square$

Proposition 18 *Let Q be the field of fractions of the skew polynomial ring $R = k(X)[Y;\theta]$, where k is a field of characteristic distinct from 2, X is an indeterminate over k, and θ is the automorphism of $k(X)$ given by $X^\theta = \lambda X$, where λ is a primitive $2n$-th root of unity in k. Then, $\{1 + X^n, 1 + Y^n\}$ is a free pair in Q.*

Proof: As in the previous proof, $\alpha = X^{2n}$ and $\beta = Y^{2n}$ are central in Q. Also, as $\lambda^n = -1$, it follows that the subfield of Q generated by $\{X^n, Y^n\}$ is isomorphic to $\left(\frac{\alpha,\beta}{k(\alpha,\beta)}\right)$ via $X^n \mapsto \mathbf{i}, Y^n \mapsto \mathbf{j}$. As α, β are algebraically independent over k, the result follows from Proposition 16. $\square$

Proposition 19 *Let R be an integral domain with quotient field F, and let A be a prime ideal of R. Assume that there exists a discrete valuation ν of F such that $A = \{x \in R : \nu(x) > 0\}$. Let $a, b \in R$, $\nu(a) = 0$, and let θ be the R-automorphism of the polynomial ring $R[X]$ given by $X^\theta = aX + b$. Finally, let $Q = R[X][Y;\theta]$. Then, the complement M of the ideal AQ is a right denominator set in Q. Further, in the right quotient ring Q_M of Q with respect to M, the set B of non-units is an ideal, and $B \cap Q = AQ$. In particular, if R is a Dedekind domain, then the conclusion holds for every prime ideal of R.*

Proof: The second part of the proof of [14, Thm. 1] applies, by using the valuation ν. The rings in [14, Thm. 1] look like the case $b = 0$, but the proof works in general. $\square$

Identifying a quaternion algebra within a skew field may seem like contrived luck. In more general settings one can still get free pairs via specializations, by following the methods of [14]. There is no need to delve seriously into specializations, the general idea being as follows: to study a pair of elements in the multiplicative group of a division ring, find a subring T whose units contain the subgroup generated by the pair; apply a morphism from T to a division ring where the pair maps to a free or semifree pair. Lift the information back to the original ring. Thus we have:

Proof of Theorem 4: First we show a skew polynomial ring embedded in $A_1(\mathbb{Q})$. Consider the ring morphism $\psi : \mathbb{Q}<s,t>\to \mathbb{Q}(X)(Y; X\mapsto X+1)$ given by $\psi(s) = Y, \psi(t) = Y^{-1}X$. Then, $\psi(ts-st-1) = Y^{-1}XY-X-1 = 0$, hence the map induces a morphism $A_1(\mathbb{Q}) \to \mathbb{Q}(X)(Y; X \mapsto X+1)$. Since the Weyl algebra is simple, this morphism is one to one and induces an isomorphism of the fields of fractions.

We can now apply Proposition 19 to $Q = \mathbb{Z}[X][Y; X \mapsto X+1]$, with $A = 2\mathbb{Z}$, obtaining a local subring Q_M of $\mathbb{Q}(X)(Y; X\mapsto X+1)$, with maximal ideal B, such that $B \cap \mathbb{Z} = 2\mathbb{Z}$. The division algebra Q_M/B is just $\mathbb{F}_2(X)(Y; X \mapsto X+1)$. By Proposition 17, $\{1+X, 1+Y\}$ is semifree modulo centre in Q_M/B; since $1+X, 1+Y \in \mathcal{U}Q_M$, this pair is semifree modulo a subgroup of $\mathcal{U}Q_M$. The result follows by applying ψ^{-1}. $\square$

It is reasonable to expect that the above pair is in fact free.

Note that Proposition 6 can be used to produce free pairs from Theorem 4. It is also interesting to compare this with [9], where a free group algebra is found in the field of fractions of $A_1(\mathbb{Q})$; there, the whole free group consists of proper fractions, while the present result provides free monoids inside $A_1(\mathbb{Q})$ generating free groups in the field of fractions.

As a sort of complement for Proposition 18 we have:

Proposition 20 *Let k be a field of characteristic distinct from 2, let θ be the automorphism of $k[X]$ given by $X^\theta = \lambda X$, with $\lambda \in k^*$. Then $\langle 1+X, 1+Y\rangle$ is a free subgroup of the field of fractions $k(X)(Y;\theta)$ provided that either*

(i) λ is transcendental over the prime field of k; or

(ii) char $k = 0$ *and λ is an algebraic number such that $2 \notin (1+\lambda)\mathbb{Z}[\lambda]$.*

Proof: Let P be the prime field of k. In each case we construct appropriate specializations from $k(X)(Y;\theta)$ to $F(X)(Y; X\mapsto -X)$, for some field F.
Case(i): Let $R = P[\lambda]$, and $Q = R[X][Y;\theta]$. Applying Proposition 19 with $A = (1+\lambda)R$ we obtain M and B such that both $1+X, 1+Y$ are invertible in Q_M, and, as $1+\lambda \in B$, the relation $Y^{-1}XY = -X$ holds in Q_M/B. It follows that $Q_M/B \simeq P(X)(Y; X\mapsto -X)$.
Case(ii): Let $R = \mathbb{Z}[\lambda]$, and $Q = R[X][Y;\theta]$. Extend $(1+\lambda)\mathbb{Z}[\lambda]$ to a maximal ideal A of R not containing 2 and apply Proposition 19. We obtain M and B such that both $1+X, 1+Y$ are invertible in Q_M, and, as before, the relation $Y^{-1}XY = -X$ holds in Q_M/B. As $B\cap\mathbb{Z} = p\mathbb{Z}$ for some prime $p \neq 2$, $Q_M/B \simeq \mathbb{F}_p(X)(Y; X\mapsto -X)$.

The result now follows from observing for any field F the obvious isomorphism $F(X)(Y;X\mapsto -X)\simeq \left(\frac{X^2,Y^2}{F(X^2,Y^2)}\right)$, and using Proposition 16. $\square$

6 Proof of Theorem 5

To begin with, we prove the result when G is nilpotent. Suppose the result is false, and choose a (non-abelian) counterexample $M=\langle x,y\rangle$ of minimal Hirsh number. By Proposition 20, M is not nilpotent of class 2. Let $R=kM$. The centre of M is torsion-free abelian of finite rank; choose a non-trivial central element $a\in M$, and set $t=a-1\in R\setminus 0$ and $\bar{M}=M/<a>$. One easily verifies that $\bigcap_{i=0}^{\infty}(tR)^i=(0)$ (see, e. g. [22, section 3.4]), and $R/tR\simeq k\bar{M}$ is an Ore domain. By [16, Theorem 1], the ring of fractions $Q(kM)$ has a specialization onto the ring of fractions $Q(k\bar{M})$. Since M is not of class 2 and a is central, $\bar{M}$ is not abelian, hence $\bar{x}$ and $\bar{y}$ do not commute. Since $\bar{M}$ has smaller Hirsch number than M, the minimal choice of M implies that $\langle 1+\bar{x},1+\bar{y}\rangle$ is free. Since $1+x$ and $1+y$ map onto the free generators, they also form a free pair, a contradiction.

Now consider the general case. Let $G=N_0\supseteq N_1\supseteq\dots$ be a chain of normal subgroups of G such that each $G_i=G/N_i$ is torsion-free nilpotent, and $\bigcap_i N_i=\{1\}$. Further, let D and D_i denote the division subrings of the Malcev-Neumann series rings $k\langle G\rangle$ and $k\langle G_i\rangle$, generated by kG and kG_i respectively.

Let x,y be non-commuting elements of G, and choose an index i such that $xyx^{-1}y^{-1}\notin N_i$. By [5, Corollary 2 of Proposition 3.1], there exists a specialization of D to D_i extending the canonical group morphism $G\to G_i$; from the proof of that result one sees that both $(1+cx)^{-1}$ and $(1+dy)^{-1}$ are in the domain of the specialization. Since the images of cx,dy do not commute in D_i, the first paragraph of the proof implies that the images of the pair $\{1+cx,1+dy\}$ form a free pair, whence the result.

Remark. The same argument shows the existence of free group algebras in the ring of fractions of the group ring of a residually (torsion-free nilpotent) group G. The result is known in the nilpotent case (e.g., [7], Corollary 2.2). These free group algebras can then be lifted back via specializations.

References

[1] S. Balcezyk and J. Mycielsky, On faithful representations of free products of groups, *Fund. Math.* **50** (1961), 63–71.

[2] A. Blanchard, "Les corps non commutatifs," Presses Universitaires de France, 1972.

[3] Th. J. Dekker, On free products of cyclic rotation groups, *Canadian J. of Math.* **11** (1959), 446-448.

[4] P. K. Draxl, "Skew Fields," Cambridge Univ. Press, 1983.

[5] A. Eizenbud and A. I. Lichtman, On embedding of group rings of residually torsion free nilpotent groups into skew fields, *Trans. Amer. Math. Soc.* **299** (1987), 373–386.

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

[7] J. Z. Gonçalves, L. M. V. Figueiredo and M. Shirvani, Free group algebras in certain division rings, *J. of Algebra* **185** (1996), 298–313.

[8] J. Z. Gonçalves and A. Mandel, Are there free groups in division rings?, *Israel J. of Math.* **53** (1986), 69–80.

[9] J. Z. Gonçalves and M. Shirvani, Free group algebras in the field of fractions of differential polynomial rings and enveloping algebras, to appear in J. Algebra.

[10] J. de Groot, Orthogonal isomorphic representations of free groups, *Canadian J. of Math.* **8** (1956), 256–262.

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

[12] F. Hausdorff, "Grundzüge der Mengehnlehre," Veit, 1914.

[13] A. I. Lichtman, On the subgroups of the multiplicative group of skew-fields, *Proc. Amer. Math. Soc.* **63** (1977), 15–16.

[14] A. I. Lichtman, Free subgroups of normal subgroups of the multiplicative group of skew fields, *Proc. Amer. Math. Soc.* **71** (1978), 174–178.

[15] A. I. Lichtman, On normal subgroups of multiplicative groups of skew-fields generated by polycyclic-by-finite groups, *J. of Algebra* **78** (1982), 548–577.

[16] A. I. Lichtman, Valuation methods in division rings, *J. of Algebra* **177** (1995), 870–898.

[17] A. I. Lichtman, Free Subalgebras in Division Rings Generated by Universal Enveloping Algebras, preprint, 1998.

[18] R. C. Lyndon and P. E. Schupp, “Combinatorial group theory,” Springer, 1977.

[19] L. Makar-Limanov, On Free Subobjects of Skew Fields, *in* “Methods in Ring Theory,” Proceedings NATO ASI, Antwerp 1983 (F. van Oystaeyen ed.), NATO ASI series (C) vol. 129, pp. 281–286.

[20] L. Makar-Limanov, On group rings of nilpotent groups, *Israel. J. of Math.* **48** (1984), 245–248.

[21] Makar-Limanov, L. , On subnormal subroups of skew fields, *J. of Algebra* **114** (1988), 261–267.

[22] D. S. Passman, “Algebraic structure of group rings,” Wiley, New York, 1977.

[23] S. Świerczkowski, A class of free rotation groups, *Indag. Math.* **5** (1994), 221–226.

[24] Tits, J. , Free groups in linear groups, *J. of Algebra* **20** (1972), 250–270.