Indag. Mathem., N.S., 5 (2), 221–226 June 20, 1994

A class of free rotation groups

by S. Świerczkowski

Department of Mathematics and Computing, Sultan Qaboos University, P.O. Box 36, Al-Khod, P.C. 123, Muscat, Sultanate of Oman

Communicated by Prof. W.T. van Est at the meeting of June 21, 1993

ABSTRACT

The following theorem is proved: If $\cos\phi \in \mathbb{Q}$ then the subgroup of $SO_3(\mathbb{R})$ generated by two rotations about the angle ϕ, with rotation axes perpendicular to each other is free iff $\cos\phi \neq 0, \pm\frac{1}{2}, \pm 1$. This is used to exhibit free subgroups of $SO_3(\mathbb{Q})$, also to find all rational values of $\cos\phi$ when ϕ is a rational multiple of π. A similar result about the values of $\tan\phi$, due to P. Walker, is also presented.

1. THE RESULT

Consider two rotations of the 3-dimensional Euclidean space, about axes which are perpendicular to each other and with the same rotation angle ϕ. Assume that $\cos\phi$ is rational, say $\cos\phi = a/b$, where a, b are integers. Putting $c = b^2 - a^2$, we may represent those rotations by the matrices

$$(1.1) \qquad A = \begin{bmatrix} \frac{a}{b} & \frac{-\sqrt{c}}{b} & 0 \\ \frac{\sqrt{c}}{b} & \frac{a}{b} & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{a}{b} & \frac{-\sqrt{c}}{b} \\ 0 & \frac{\sqrt{c}}{b} & \frac{a}{b} \end{bmatrix}$$

In 1958 the following result was announced in [2]:

Theorem 1.1. *The subgroup of $SO_3(\mathbb{R})$ generated by A and B is free, with the free generators A, B iff $a/b \notin \{0, \pm\frac{1}{2}, \pm 1\}$.*

In [2] this theorem was proved for $a/b = \frac{1}{3}$; this case was of interest because it served to solve a problem posed in [1] by H. Steinhaus (concerning tetrahedra, the solution is in [3]). Since that time, a powerful result was obtained which yields free subgroups of $SO_3(\mathbb{R})$: J. Tits proved in [4] that a linear group over a field of characteristic zero either has a free (nonabelian) subgroup or it possesses a solvable subgroup of finite index. However this theorem does not seem to imply that the subgroup of $SO_3(\mathbb{Q})$ generated by the matrices

$$\begin{bmatrix} \frac{3}{5} & \frac{-4}{5} & 0 \\ \frac{4}{5} & \frac{3}{5} & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{3}{5} & \frac{-4}{5} \\ 0 & \frac{4}{5} & \frac{3}{5} \end{bmatrix}$$

is free. Such group is of interest, as it can be employed to construct paradoxical decompositions of the rational sphere $S^2 \cap \mathbb{Q}^3$, without assuming the Axiom of Choice ([5], Thm. 4.5). So it appears that our theorem creates some useful groups, and this, we hope, justifies publishing belatedly its proof.

2. PROOF OF THEOREM 1.1.

The necessity of $\cos\phi \neq 0, \pm\frac{1}{2}, \pm 1$ is obvious. To prove sufficiency, assume that $\cos\phi = a/b$ where a, b are integers satisfying

$$b > 0, \quad |a| \leq b \quad \text{and} \quad a/b \neq 0, \pm\tfrac{1}{2} \pm 1.$$

Clearly, we then may also assume that

(2.1) $\quad a \neq 0$, a and b are co-prime and $b > 2$.

We ought to prove that for any $n \geq 1$ and matrices $C_1, \ldots, C_n$, where

$$C_j = A^{\varepsilon} \text{ or } B^{\varepsilon};\ \varepsilon = \pm 1, \quad \text{and} \quad C_j \cdot C_{j+1} \neq I;\ 1 \leq j < n,$$

(I = the unit matrix), we have

(2.2) $\quad C_1 \cdot C_2 \cdot \cdots \cdot C_n \neq I.$

Since (2.2) is equivalent to $A^{\varepsilon} \cdot C_1 \cdot \cdots \cdot C_n \cdot A^{-\varepsilon} \neq I$, we may assume that $C_1 = A^{\pm 1}$.

Let us define, for $j = 1, \ldots, n$ the numbers $d_k^{(j)}$; $k = 1, 2, 3$ by

$$(2.3) \qquad C_1 \cdot C_2 \cdot \cdots \cdot C_j = \begin{bmatrix} \frac{d_1^{(j)}}{b^j} & \frac{d_2^{(j)}\sqrt{c}}{b^j} & \frac{d_3^{(j)}}{b^j} \\ * & * & * \\ * & * & * \end{bmatrix}$$

We shall show that $d_2^{(n)} \neq 0$, and evidently this will do. We begin by establishing some recursive relations for the $d_k^{(j)}$. Obviously (1.1) and (2.3) imply that

$d_1^{(1)} = a$, $d_2^{(1)} = -\varepsilon$ and $d_3^{(1)} = 0$. Let us define $d_1^{(0)} = 1$, $d_2^{(0)} = d_3^{(0)} = 0$; we claim that then

(A) If $C_{j+1} = A^{\varepsilon}$; $j \geq 0$, then:

$$d_1^{(j+1)} = ad_1^{(j)} + \varepsilon c d_2^{(j)}, \quad d_2^{(j+1)} = -\varepsilon d_1^{(j)} + ad_2^{(j)}, \quad d_3^{(j+1)} = bd_3^{(j)}.$$

This is easily checked if $j = 0$ (we substitute the above values of $d_k^{(0)}, d_k^{(1)}$) and for $j \geq 1$, we multiply on the right both sides of (2.3) by A^{ε}.

(B) If $C_{j+1} = B^{\varepsilon}$; $j \geq 1$, then:

$$d_1^{(j+1)} = bd_1^{(j)}, \quad d_2^{(j+1)} = ad_2^{(j)} + \varepsilon d_3^{(j)}, \quad d_3^{(j+1)} = -\varepsilon c d_2^{(j)} + ad_3^{(j)}.$$

This is verified similarly as (A). The first conclusion from these equalities is that all $d_k^{(j)}$ are integers. The next conclusion: if $C_j = C_{j+1}$ then $d_k^{(j+1)}$ can be expressed by $d_k^{(j)}$ and $d_k^{(j-1)}$ for $k = 1, 2, 3$. We have seen this in (A) for $k = 3$ and in (B) for $k = 1$. The other cases are dealt with in (AA) and (BB).

(AA) If $C_j = C_{j+1} = A^{\pm 1}$; $j \geq 1$, then:

$$d_k^{(j+1)} = 2ad_k^{(j)} - b^2 d_k^{(j-1)} \quad \text{for } k = 1, 2.$$

We check this as follows (using (A) twice):

$$\begin{aligned} d_1^{(j+1)} &= ad_1^{(j)} + \varepsilon c d_2^{(j)} = ad_1^{(j)} + \varepsilon c(-\varepsilon d_1^{(j-1)} + ad_2^{(j-1)}) \\ &= ad_1^{(j)} + a\varepsilon c d_2^{(j-1)} + a^2 d_1^{(j-1)} - (a^2 + c)d_1^{(j-1)} \\ &= 2ad_1^{(j)} - b^2 d_1^{(j-1)}, \end{aligned}$$

by the definition of c.

$$\begin{aligned} d_2^{(j+1)} &= -\varepsilon d_1^{(j)} + ad_2^{(j)} = -\varepsilon(ad_1^{(j-1)} + \varepsilon c d_2^{(j-1)}) + ad_2^{(j)} \\ &= ad_2^{(j)} - a\varepsilon d_1^{(j-1)} + a^2 d_2^{(j-1)} - (a^2 + c)d_2^{(j-1)} \\ &= 2ad_2^{(j)} - b^2 d_2^{(j-1)}. \end{aligned}$$

(BB) If $C_j = C_{j+1} = B^{\pm 1}$; $j > 1$, then:

$$d_k^{(j+1)} = 2ad_k^{(j)} - b^2 d_k^{(j-1)} \quad \text{for } k = 2, 3.$$

This is proved similarly as (AA), now applying (B) twice. Alternately, we may note that the identities in (A) turn into the identities of (B) after the simultaneous replacements $d_1 \mapsto d_3$, $\varepsilon \mapsto -\varepsilon$, $d_3 \mapsto d_1$, moreover the same replacements turn (AA) into (BB).

For $C_j \neq C_{j+1}$, we conclude from (A), (B) that:

(AB) If $C_j = A^{\pm 1}$, $C_{j+1} = B^{\varepsilon}$; $j \geq 1$, then:

$$\begin{aligned} d_2^{(j+1)} &= ad_2^{(j)} + \varepsilon d_3^{(j)} = ad_2^{(j)} + \varepsilon b d_3^{(j-1)}, \\ d_3^{(j+1)} &= -\varepsilon c d_2^{(j)} + ad_3^{(j)} = -\varepsilon c d_2^{(j)} + abd_3^{(j-1)}. \end{aligned}$$

(BA) If $C_j = B^{\pm 1}$, $C_{j+1} = A^{\varepsilon}$ $j \geq 1$, then:

$$d_1^{(j+1)} = \varepsilon c d_2^{(j)} + a d_1^{(j)} = \varepsilon c d_2^{(j)} + ab d_1^{(j-1)},$$

$$d_2^{(j+1)} = a d_2^{(j)} - \varepsilon d_1^{(j)} = a d_2^{(j)} - \varepsilon b d_1^{(j-1)}.$$

Proof of (2.2) when b is not a power of 2. Let $b = 2^m s$, where s is an odd number and $s > 1$. Obviously s and $2a$ are co-prime. We shall deduce from this, by induction on j, that $d_2^{(j)}$ is not divisible by s for $j = 1, \ldots, n$, so that $d_2^{(n)} \neq 0$, as required. Since $d_2^{(1)} = -\varepsilon$, we have non $s \mid d_2^{(1)}$. For the inductive step, note that for $j \geq 1$, by (AA), (BB),

$$d_2^{(j+1)} = 2a d_2^{(j)} - b^2 d_2^{(j-1)}$$

when $C_j = C_{j+1}$, and by (AB), (BA),

$$d_2^{(j+1)} = a d_2^{(j)} \pm 2^m s \varepsilon d_k^{(j-1)}; \quad (k = 1 \text{ or } 3)$$

when $C_j \neq C_{j+1}$. Thus the inductive assumption that non $s \mid d_2^{(j)}$ implies non $s \mid d_2^{(j+1)}$. □

Proof of (2.2) when b is a power of 2. This is slightly more complicated. Suppose that $b = 2^m$. Then $m \geq 2$ (see (2.1)) and both a and c are odd. It will be enough to prove the following lemma:

Lemma 2.1. There is a function $f : \{1, \ldots, n\} \to \{0, 1, \ldots, n\}$ such that for all $j \geq 1$, we have $f(j+1) \leq f(j) + 1$ and

[A] If $C_j = A^{\pm 1}$ then

$$d_1^{(j)} = 2^{f(j)} r_1^{(j)}; \qquad d_2^{(j)} = 2^{f(j)} r_2^{(j)}; \qquad 2^{f(j)} \mid d_3^{(j)},$$

where $r_1^{(j)}, r_2^{(j)}$ are some *odd* numbers, and

[B] If $C_j = B^{\pm 1}$ then

$$2^{f(j)} \mid d_1^{(j)}; \qquad d_2^{(j)} = 2^{f(j)} r_2^{(j)}; \qquad d_3^{(j)} = 2^{f(j)} r_3^{(j)},$$

where $r_2^{(j)}, r_3^{(j)}$ are some *odd* numbers.

Obviously this lemma implies $d_2^{(n)} \neq 0$, so (2.2) follows.

The proof is by induction. We have $C_1 = A^{\pm 1}$ and $d_1^{(1)} = a$, $d_2^{(1)} = -\varepsilon$, $d_3^{(1)} = 0$, thus [A], [B] hold for $j = 1$ with $f(1) = 0$. We make now the assumption that [A], [B] hold for $C_1, \ldots, C_j$ and consider, for the inductive step, various possibilities for the pair C_j, C_{j+1}.

[AA] $C_j = C_{j+1} = A^{\pm 1}$.

We have to show that then [A] holds for $j+1$, and we claim that this will be so when $f(j+1) = f(j) + 1$. Indeed, then by (A), $d_3^{(j+1)} = 2^m d_3^{(j)}$, so $2^{f(j)} \mid d_3^{(j)}$ implies $2^{f(j+1)} \mid d_3^{(j+1)}$.

By (AA), for $j \geq 1$ and $k = 1, 2$

$$d_k^{(j+1)} = 2a d_k^{(j)} - 2^{2m} d_k^{(j-1)}. \tag{2.4}$$

If $j = 1$, then this means, since $f(1) = 0$, that

$$d_k^{(2)} = 2ad_k^{(1)} - 2^{2m}d_k^{(0)} = 2ar_k^{(1)} - 2^{2m}d_k^{(0)}$$
$$= 2(ar_k^{(1)} - 2^{2m-1}d_k^{(0)}) = 2^{f(2)}r_k^{(2)},$$

where $r_k^{(2)}$ is an odd number because $2m \geq 4$.

If $j \geq 2$, (2.4) becomes

$$d_k^{(j+1)} = 2^{f(j)+1}ar_k^{(j)} - 2^{2m+f(j-1)}r_k^{(j-1)}$$
$$= 2^{f(j)+1}(ar_k^{(j)} - 2^{2m+f(j)-f(j)-1}r_k^{(j-1)}) = 2^{f(j+1)}r_k^{(j+1)}$$

where $r_k^{(j+1)}$ is odd, because $2m \geq 4 > f(j) - f(j-1) + 1$.

[BB] $C_j = C_{j+1} = B^{\pm 1}$.

We have to show that [B] holds for $j+1$, and we claim that this will be so for $f(j+1) = f(j) + 1$. The argument, starting from (BB) is analogous to the second part of the proof of [AA] (the case $j = 1$ need not be considered now, as $C_1 = A^{\pm 1}$).

[AB] $C_j = A^{\pm 1}$, $C_{j+1} = B^{\varepsilon}$.

Let us check that [B] holds for $j+1$, with $f(j+1) = f(j)$. From the first equality in (B) we then have $2^{f(j+1)} \mid d_1^{(j+1)}$. The first equality in (AB) gives

$$d_2^{(j+1)} = ad_2^{(j)} + \varepsilon 2^m d_3^{(j-1)} = a2^{f(j)}r_2^{(j)} + \varepsilon 2^m d_3^{(j-1)}.$$

By inductive assumption, $f(j) \leq f(j-1) + 1$, so it follows from $2^{f(j-1)} \mid d_3^{(j-1)}$ that $2^{f(j)} \mid 2d_3^{(j-1)}$, and we obtain

$$d_2^{(j+1)} = 2^{f(j)}(ar_2^{(j)} + 2^{m-1}\varepsilon(2d_3^{(j-1)}/2^{f(j)})) = 2^{f(j+1)}r_2^{(j+1)},$$

where $r_2^{(j+1)}$ is odd, by $m \geq 2$.

The existence of $r_3^{(j+1)}$ is proved similarly, starting from the last equality in (AB).

[BA] $C_j = B^{\pm 1}$, $C_{j+1} = A^{\varepsilon}$.

Using (A) and (BA), we show that [A] holds for $j+1$, with $f(j+1) = f(j)$, proceeding similarly as in the case [AB].

This completes the proof of Lemma 2.1, which, as we pointed out, implies Theorem 1.1. □

3. APPENDIX

Theorem 1.1 implies a curious property ((1) below) of the functions $\cos x$ and $\sin x$. It led Peter Walker to prove a similar property for $\tan x$ ((2) below). His result (private communication to the author) is presented here, with some modifications, as Lemma 3.1.

Theorem 3.1. *Let* $\cos(\pi\mathbb{Q}) = \{\cos(\pi x) : x \in \mathbb{Q}\}$ *and let* $\sin(\pi\mathbb{Q})$ *and* $\tan(\pi\mathbb{Q})$ *be defined similarly. Then*

1. $\mathbb{Q} \cap \cos(\pi\mathbb{Q}) = \mathbb{Q} \cap \sin(\pi\mathbb{Q}) = \{0, \frac{1}{2}, \pm 1\}$,
2. $\mathbb{Q} \cap \tan(\pi\mathbb{Q}) = \{0, \pm 1\}$.

Part (1) is an immediate consequence of Theorem 1.1. Indeed, if $\cos\phi = a/b$ (a, b integers, $b \neq 0$) then $\phi \in \pi\mathbb{Q}$ iff the matrix A satisfies $A^n = I$ for

some natural $n \geq 1$. By the Theorem 1.1, this will happen precisely when $\cos\phi \in \{0, \pm\frac{1}{2}, \pm 1\}$.

To prove part (2), let us first state (2) as a property of the ring $\mathbb{Z}(i)$ of Gaussian integers. We have $\tan\phi = a/b$ (with a, b as above) iff $\phi = \arg(z)$ for $z = a + ib$. Thus $\phi \in \pi\mathbb{Q}$ iff $z^n \in \mathbb{R}$ for some $n \geq 1$. Hence (2) is a consequence of

Lemma 3.1. *If $z \in \mathbb{Z}(i)$ satisfies $z^n \in \mathbb{R}$ for some natural $n \geq 1$, then*

$$z = u(1+i)^\eta a,$$

where $u \in \{\pm 1, \pm i\}$, $\eta \in \{0, 1\}$ and $a \in \mathbb{Z}$.

Proof. Let $\mathbb{U} = \{\pm 1, \pm i\}$ be the set of units of $\mathbb{Z}(i)$ and let $\equiv$ be the equivalence relation on $\mathbb{Z}(i)$, where $z_1 \equiv z_2$ iff z_1, z_2 are associates, i.e., $z_1 = uz_2$ for some $u \in \mathbb{U}$. We denote by $[z]$ the $(\equiv)$-equivalence class of z and by $\mathcal{F}$ the set of equivalence classes. The multiplication in $\mathbb{Z}(i)$ induces an abelian semigroup structure on $\mathcal{F}$. Each $z \in \mathbb{Z}(i)$ can be written as a product of prime elements of $\mathbb{Z}(i)$, moreover such representation is unique, up a permutation of these primes and up to the presence of some multipliers belonging to $\mathbb{U}$. Thus $\mathcal{F}$ is a *free* abelian semigroup (whose free generators are the equivalence classes $[p]$, where p are primes in $\mathbb{Z}(i)$). Let us denote by $h : \mathcal{F} \to \mathcal{F}$ the semigroup endomorphism induced by the complex conjugation, i.e., given by $h([z]) = [\bar{z}]$. Then it is easy to check that z is of the form asserted by the lemma (i.e., $z = u(1+i)^\eta a$; $u \in \mathbb{U}$, $\eta \in \{0, 1\}$ and $a \in \mathbb{Z}$) iff $h([z]) = [z]$, that is, $[z] = [\bar{z}]$.

Assume now that $z^n \in \mathbb{R}$ for some $n \geq 1$. Then $h([z^n]) = [z^n]$, whence $(h([z]))^n = [z]^n$. But if in a free semigroup the n-th powers of two elements are equal, for $n \geq 1$, then these elements are equal. So we get $h([z]) = [z]$, hence z is of the form asserted by the lemma. □

REFERENCES

1. Steinhaus, H. – P 175. Coll. Math. **4**, 243 (1957).
2. Świerczkowski, S. – On a free group of rotations of the Euclidean space. Indag. Math. **20**, 376–378 (1958).
3. Świerczkowski, S. – On chains of regular tetrahedra. Coll. Math. **7**, 9–10 (1959).
4. Tits, J. – Free subgroups in linear groups. J. of Algebra **20**, 250–270 (1972).
5. Wagon, S. – The Banach–Tarski Paradox. Cambridge University Press, London 1985.