SCIENTIA
Series A: *Mathematical Sciences*, Vol. 16 (2008), 109–117
Universidad Técnica Federico Santa María
Valparaíso, Chile
ISSN 0716-8446

Free groups of rotations acting without fixed points on the rational unit sphere

Sebastian Agata

Abstract. The purpose of this paper is to generalize an example of Sato of a free group of rotations of the Euclidean 3-space whose action on the rational unit sphere is fixed point free. Such groups are of interest, as they can be employed to construct paradoxical decompositions of spheres without assuming the Axiom of Choice.

1. Introduction

The study of free subgroups in $\mathrm{SO}(3,\mathbb{R})$ can be tracked to Hausdorff who first proved in 1914 that there is a free subgroup of rank 2 in the group of rotations in $\mathbb{R}^3$. He showed that if ϕ and ρ are rotations through $180°, 120°$, respectively, about axes containing the origin, and if $\cos(2\theta)$ is a transcendental number where θ is the angle between the axes, then ϕ and ρ are free generators of the free product $\mathbb{Z}_2 * \mathbb{Z}_3$. Since $\mathbb{Z}_2 * \mathbb{Z}_3$ has a free subgroup of rank 2, the group $\mathrm{SO}(3,\mathbb{R})$ contains a rank 2 free subgroup.

Since that time, a powerful result was obtained which yields free subgroups of $\mathrm{SO}(3,\mathbb{R})$. J. Tits proved in [**6**] 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. Tits's result however does not seem to be helpful to prove that some given group is free.

Now, consider two rotations of the 3-dimensional Euclidean space with respect to 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 these rotations by the matrices

$$A = \begin{bmatrix} a/b & -\sqrt{c}/b & 0 \\ \sqrt{c}/b & a/b & 0 \\ 0 & 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & a/b & -\sqrt{c}/b \\ 0 & \sqrt{c}/b & a/b \end{bmatrix}.$$

In paper [**5**] Świerczkowski proved the following theorem.

Theorem 1.1. *The subgroup of $SO(3,\mathbb{R})$ generated by A and B is free, with the free generators A and B if and only if $a/b \notin \{0, \pm 1/2, \pm 1\}$.*

1991 *Mathematics Subject Classification.* Primary 20E05, 20H20; Secondary 51F20, 51F25.
Key words and phrases. free groups, orthogonal groups, Axiom of Choice.
Supported by BW 5100-5-0205-6.

Świerczkowski developed an approach that avoids the use of transcendental numbers. Especially interesting amongst groups obtained from Theorem 1.1 are those that belong to $\mathrm{SO}(3,\mathbb{Q})$. Such groups are of interest, as they can be employed to construct paradoxical decompositions of the rational sphere $S^2 \cap \mathbb{Q}^3$, without assuming the Axiom of Choice (see [**7**]). To obtain some special paradoxical decompositions, a free subgroup of $\mathrm{SO}(3,\mathbb{Q})$ should act without fixed points on the rational unit sphere. In paper [**4**] Sato gave such an example. We show how to generalize this example.

2. Preliminaries

We will remind some elementary connections of quaternions with geometry (see [**2**]). As a vector space quaternions $\mathbb{H} = \mathbb{R} \oplus \mathbb{P}$, where $\mathbb{P}$ the subspace of pure quaternions, is spanned over $\mathbb{R}$ by its standard base $\{i, j, k\}$. One consider $\mathbb{P}$ as the $3-$dimensional Euclidean space in which the base i, j, k is orthonormal. With any unit $\xi \in \mathbb{H}$ we can associate a map $\psi_\xi : \mathbb{P} \to \mathbb{P}$ given by the formula:

$$\psi_\xi(x) = \xi x \xi^{-1} \text{ for any } x \in \mathbb{P}.$$

One can prove that ψ_ξ is an $\mathbb{R}-$linear map, it preserves the norm of quaternions, and the space $\mathbb{P}$ is ψ_ξ -invariant. Hence ψ_ξ, being always an isometry, is either a rotation of $\mathbb{P}$ with its axis parallel to the pure part of ξ if $\xi \notin \mathbb{R}$ or is the identity if $\xi \in \mathbb{R}$.

In this article we use the following model of quaternions $\mathbb{H} = \mathbb{R} \times \mathbb{R}^3$ with $*$, where

$$(c', s') * (c, s) = (c'c - s' \cdot s, cs' + c's + s' \times s),$$

where $\cdot$ and $\times$ denote scalar and vector products in the Euclidean 3-space. We denote by $s(A)$ the vector part of the quaternion A.

By $\mathbb{H}^1$ we denote the set of quaternions of norm 1. Therefore

$$\mathbb{H}^1 = \{(c, s) : c^2 + |s|^2 = 1)\},$$

where $|\cdot|$ denotes the length of a vector in the Euclidean 3-space. One can prove that the following short sequence is exact

$$1 \longrightarrow \{-1, 1\} \longrightarrow \mathbb{H}^1 \xrightarrow{\psi} \mathrm{SO}(3,\mathbb{R}) \longrightarrow 1 \ .$$

If A belongs to $\mathrm{SO}(3,\mathbb{R})$ then let $\widetilde{A}$ denotes one of the two elements of $\psi^{-1}(A)$. Every rotation A is represented by the set $\{\widetilde{A}, -\widetilde{A}\}$. The map ψ induces an isomorphism $\bar{\psi}$ from $\mathbb{H}^1/\{1, -1\}$ onto $SO(3,\mathbb{R})$. For given positive integer x we create two matrices

$$A_x = \frac{1}{n+1} \begin{bmatrix} n & x & x+1 \\ x & x+1 & -n \\ -x-1 & n & x \end{bmatrix},$$

$$B_x = \frac{1}{n+1} \begin{bmatrix} x & -n & x+1 \\ n & x+1 & x \\ -x-1 & x & n \end{bmatrix},$$

where $n = x \cdot (x+1)$. A straightforward computation shows that A_x and B_x belong to $\mathrm{SO}(3,\mathbb{Q})$ for arbitrary positive integers x. We denote by Γ_x the subgroup of $\mathrm{SO}(3,\mathbb{Q})$ generated by A_x and B_x.

LEMMA 2.1. *Rotations $A_x, B_x, A_x^{-1}, B_x^{-1}$ are represented by quaternions as follows*

$$\begin{aligned}
\widetilde{A}_x &= \pm\tfrac{1}{\sqrt{2(1+x+x^2)}}([(x+1),[x,1,0]]),\\
\widetilde{B}_x &= \pm\tfrac{1}{\sqrt{2(1+x+x^2)}}([(x+1),[0,1,x]]),\\
\widetilde{A_x^{-1}} &= \pm\tfrac{1}{\sqrt{2(1+x+x^2)}}([(x+1),[-x,-1,0]]),\\
\widetilde{B_x^{-1}} &= \pm\tfrac{1}{\sqrt{2(1+x+x^2)}}([(x+1),[0,-1,-x]]).
\end{aligned}$$

Proof. The axis of rotation is determined by an eigenvector. □

Moreover we consider the quaternions which are obtained by multiplying by the factor $\sqrt{2(1+x+x^2)}$ each of the four quaternions above. We denote them by $\widehat{A_x}, \widehat{B_x}, \widehat{A_x^{-1}}, \widehat{B_x^{-1}}$ respectively. All of them belong to $\mathbb{Z}\times\mathbb{Z}^3$. The mapping ψ can be extended to epimorphism $\widetilde{\psi} : \mathbb{H}\setminus\{0\} \to \mathrm{SO}(3,\mathbb{R})$ with $ker(\widetilde{\psi}) = \mathbb{R}\setminus\{0\}$. It is well known (see [**3**] for example) that already the restriction of $\widetilde{\psi}$ to non-zero integer quaternions is an epimorphism onto the group $\mathrm{SO}(3,\mathbb{Q})$. Such integer quaternions are called quaternion covers. For given rotation $q \in \mathrm{SO}(3,\mathbb{Q})$ we denote by $\widehat{q}$ its quaternion cover. It is obvious that for $q \in \mathrm{SO}(3,\mathbb{Q})$ the following equality holds

$$\{\frac{1}{\sqrt{n(\widehat{q})}}\widehat{q}, -\frac{1}{\sqrt{n(\widehat{q})}}\widehat{q}\} = \psi^{-1}(q), \tag{2.1}$$

where $n(\cdot)$ denotes norm of a quaternion. Now consider the word $w = w(A_x, B_x) \in \Gamma_x$. We have $\bar{\psi}^{-1}(w(A_x,B_x)) = w([\widetilde{A_x}],[\widetilde{B_x}])$. Using 2.1 we obtain that $w(\widehat{A_x},\widehat{B_x})$ is the quaternion cover of the rotation w.

PROPOSITION 2.2. *If $x \neq y$ then Γ_x and Γ_y are not conjugated in $SO(3,\mathbb{Q})$.*

Proof. Let $x < y$. Conversely, assume that there exists an element $g \in \mathrm{SO}(3,\mathbb{Q})$ that $g\Gamma_y g^{-1} = \Gamma_x$. Hence, there exists the word $w = w(A_x, B_x)$ such that $gA_yg^{-1} = w$. So $\widetilde{g} * \widetilde{A}_y * \widetilde{g^{-1}} = \pm\widetilde{w}$. We compute

$$[(\frac{1}{\sqrt{n(\widehat{g})}})^2 \cdot \frac{1}{\sqrt{2(y^2+y+1)}}] \cdot \widehat{g} * [y+1,[y,1,0]] * \widehat{g^{-1}} = \pm\frac{1}{\sqrt{n(\widehat{w})}}\widehat{w}. \tag{2.2}$$

If $\widehat{g} = [a,[b,c,d]]$ then $\widehat{g^{-1}} = [a,[-b,-c,-d]]$. Comparing the $c-$part of both sides of the equation 2.2 we have

$$\sqrt{n(\widehat{w})}\cdot(y+1)\cdot n(\widehat{g}) = \pm n(\widehat{g})\cdot\sqrt{2(y^2+y+1)}\cdot c_{\widehat{w}}.$$

By the multiplication property of norm we have $n(\widehat{w}) = (2(x^2+x+1))^k$, where k is a length of the word w. Finally, we have

$$\sqrt{(2(x^2+x+1))^k}\cdot(y+1) = \pm\sqrt{2(y^2+y+1)}\cdot c_{\widehat{w}}$$

If k is an even integer then we have contradiction, because $\sqrt{2(y^2+y+1)}$ is an irrational number. Assume now that k is odd. Then

$$(2(x^2+x+1))^{\frac{k-1}{2}}\sqrt{2(x^2+x+1)}\cdot(y+1) = \pm\sqrt{2(y^2+y+1)}\cdot c_{\widehat{w}}$$

Therefore the number $\frac{\sqrt{2(x^2+x+1)}}{\sqrt{2(y^2+y+1)}}$ is a rational integer. We know that $x < y$, hence $0 < \frac{2(x^2+x+1)}{2(y^2+y+1)} < 1$ so the number $\frac{2(x^2+x+1)}{2(y^2+y+1)}$ cannot be a square of an integer. □

In [**4**] Sato showed that the group Γ_2 is free and acts without fixed points on the rational unit sphere. His proof works in fact for all positive integers $x \equiv 2 \mod 7$. We present first some tools for settling whether the given group is free. The general idea is that if we want to show that some relations do not hold in some structure then it is sufficient to show that they do not hold in some factor-structure which is yielded from a given one.

Definition 1. Let m be a positive integer. For integer quaternions $q^{(1)} = [c^{(1)}, [s_1^{(1)}, s_2^{(1)}, s_3^{(1)}]]$ and $q^{(2)} = [c^{(2)}, [s_1^{(2)}, s_2^{(2)}, s_3^{(2)}]]$ we put
$q^{(1)} \equiv_m q^{(2)}$ if and only if $c^{(1)} \equiv c^{(2)} \mod m$ and $s_i^{(1)} \equiv s_i^{(2)} \mod m$ for $i = 1, 2, 3$.

LEMMA 2.3. *The relation $\equiv_m$ is an equivalence congruence relation.*

Proof. It is evident that the relation $\equiv_m$ is an equivalence relation. For congruence, let us consider integer quaternions $q^{(1)}, q^{(2)}, q^{(3)}, q^{(4)}$ such that $q^{(1)} \equiv_m q^{(2)}$ and $q^{(3)} \equiv_m q^{(4)}$. We have to show that $q^{(1)} * q^{(3)} \equiv_m q^{(2)} * q^{(4)}$. Using the definition of quaternion multiplication and applying assumptions we obtain straightforwardly

$$\begin{aligned}
c^{(1)}c^{(3)} - s_1^{(1)}s_1^{(3)} - s_2^{(1)}s_2^{(3)} - s_3^{(1)}s_3^{(3)} &\equiv c^{(2)}c^{(4)} - s_1^{(2)}s_1^{(4)} - s_2^{(2)}s_2^{(4)} - s_3^{(2)}s_3^{(4)},\\
c^{(3)}s_1^{(1)} + c^{(1)}s_1^{(3)} + s_2^{(1)}s_3^{(3)} - s_2^{(3)}s_3^{(1)} &\equiv c^{(4)}s_1^{(2)} + c^{(2)}s_1^{(4)} + s_2^{(2)}s_3^{(4)} - s_2^{(4)}s_3^{(2)},\\
c^{(4)}s_2^{(2)} + c^{(2)}s_2^{(4)} + s_3^{(2)}s_1^{(4)} - s_3^{(4)}s_1^{(2)} &\equiv c^{(3)}s_2^{(1)} + c^{(1)}s_2^{(3)} + s_3^{(1)}s_1^{(3)} - s_3^{(3)}s_1^{(1)},\\
c^{(3)}s_3^{(1)} + c^{(1)}s_3^{(3)} + s_1^{(1)}s_2^{(3)} - s_1^{(3)}s_2^{(1)} &\equiv c^{(4)}s_3^{(2)} + c^{(2)}s_3^{(4)} + s_1^{(2)}s_2^{(4)} - s_1^{(4)}s_2^{(2)}.
\end{aligned}$$

□

Now, we define a weaker relation.

Definition 2. Let m be a positive integer. For integer quaternions $q^{(1)}, q^{(2)}$ we put $q^{(1)} \asymp_m q^{(2)}$ if $q^{(1)} \equiv_m t \cdot q^{(2)}$ for some $t \in Z_m^*$. We abuse the language a little here making the identification of t and its class modulo m.

LEMMA 2.4. *The relation $\asymp_m$ is an equivalence congruence relation.*

Proof. The reflexivity is obvious. For the symmetry, if $a \asymp_m b$ then there exists $t \in Z_m^*$ such that $a \equiv_m tb$, so $b \equiv_m t^{-1}a$. Now let $a \asymp_m b$ and $b \asymp_m c$. Then there exist $t_1, t_2 \in Z_m^*$ such that $a \equiv_m t_1 b$ and $b \equiv_m t_2 c$. Therefore in virtue of Lemma 2.3 and fact that representatives of t_1 and t_2 are central elements in the ring of quaternions we have $a \equiv (t_1 t_2)c$ and $a \asymp_m c$. Finally, to prove that the relation $\asymp_m$ is a congruence with respect to the operation $*$ suppose that $a \asymp_m b$ and $c \asymp_m d$. Then there exist $t_1, t_2 \in Z_m^*$ such that $a \equiv_m t_1 b$ and $c \equiv_m t_1 d$. Using the congruence property of the relation $\equiv_m$ we obtain $a * c \equiv_m (t_1 t_2)(b * d)$. □

When considering vector parts of quaternions we will need relations confined to these parts. So we shall abuse introduced notations for these new relations.

Assume now that a word $w = w(A, B)$ is a non-trivial relation in a subgroup Γ of $\mathrm{SO}(3, \mathbb{Q})$. So $\bar{\psi}^{-1}(w(A, B)) = \bar{\psi}^{-1}(I_3) = [1] = \{-1, 1\}$. On the other hand $\bar{\psi}^{-1}(w(A, B)) = w([\widetilde{A}], [\widetilde{B}]) =$

$[w(\widetilde{A},\widetilde{B})]$. Therefore $s(w(\widetilde{A},\widetilde{B}))=[0,0,0]$ and $s(w(\widehat{A},\widehat{B}))=[0,0,0]$. To show that the group is free it is sufficient to show that $s(w(\widehat{A},\widehat{B}))\neq[0,0,0]$ for every non-trivial word w. For brevity we replace $w(\widehat{A},\widehat{B})$ by $\widehat{w}$. Observe that $s(\widehat{w})=[0,0,0]$ imply $s(\widehat{w})\asymp_m[0,0,0]$ for all propositioner moduli m. Hence it is sufficient to show that for some modulus m and for every non-trivial word w it is false that $s(\widehat{w})\asymp_m[0,0,0]$.

3. Main theorem

Let x be a positive integer greater than 1 and let p be a prime divisor of x^2+x+1.

LEMMA 3.1. *A number p can be chosen so that $p>3$.*

Proof. Observe first that the number $x(x+1)+1$ is odd and it suffices to show that the equation

$$x^2+x+1=3^\alpha$$

has no solution with $x>1,\alpha\in\mathbb{N}$. Let us assume that x,α satisfy this equation. Now if α is even then 3^α is a square of a positive integer. But this is impossible because

$$x^2<3^\alpha<x^2+2x+1=(x+1)^2$$

So let α be odd. Reduction modulo 3 gives $x\equiv 1 \mod 3$. Then one can write $x=3k+1$ and finds $9k^2+9k+3=3^\alpha$. Since $\alpha>1$ then the reduction modulo 9 gives a contradiction again. □

Let us write our property for p in the form

$$x(x+1)\equiv -1 \mod p. \tag{3.1}$$

The following lemma is crucial.

LEMMA 3.2. *For every $\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4,\delta,\varepsilon\in\{-1,1\}$*

$$(\widehat{A_x^{\varepsilon_1}}*\widehat{B_x^{\varepsilon_2}})*(\widehat{A_x^{\varepsilon_3}}*\widehat{B_x^{\varepsilon_4}})\asymp_p(\widehat{A_x^{\varepsilon_1}}*\widehat{B_x^{\varepsilon_4}}). \tag{3.2}$$

$$\widehat{A_x^{\varepsilon}}*\widehat{A_x^{\varepsilon}}\asymp_p\widehat{A_x^{\varepsilon}},\widehat{B_x^{\delta}}*\widehat{B_x^{\delta}}\asymp_p\widehat{B_x^{\delta}}, \tag{3.3}$$

Proof. One has to find t from the definition of the relation $\asymp_p$ for every combination of indices. The Tables 1,2 and 3 below present the results of our computations. Consider for example the first row of the Table 1. Let

$$(\widehat{A_x}*\widehat{B_x})*(\widehat{A_x}*\widehat{B_x^{-1}})-t*(\widehat{A_x}*\widehat{B_x^{-1}})=[c,[s_1,s_2,s_3]].$$

We will show that $[c,[s_1,s_2,s_3]]\equiv_p[0,[0,0,0]]$. We compute

$$\begin{aligned}
c_1 &= 2x^4+4x^3+8x^2+4x-tx^2-2tx-2t,\\
s_1 &= 2x^4+4x^3-tx^2,\\
s_2 &= 8x^2+2x^4+8x+4+8x^3-tx^2,\\
s_3 &= 2x^4+4x+tx^2+2tx.
\end{aligned}$$

In virtue of (3.1) we have

$$\begin{aligned}
c_1 &\equiv -2x-tx-t-4 \mod p,\\
s_1 &\equiv 2x+tx+4+t \mod p,\\
s_2 &\equiv 2x+tx+4+t \mod p,\\
s_3 &\equiv 6x+tx-t \mod p.
\end{aligned}$$

Now we search out t in $\mathbb{Z}_p^*$ for which c_1 and $s_i, i = 1, 2, 3$ are equal to 0 in $\mathbb{Z}_p$. So let

$$\begin{aligned} 2x + tx + t + 4 &\equiv 0 && \mod p \\ t(x+1) &\equiv -2x - 4 && \mod p \end{aligned}$$

Multiplying both sides of the last congruence by x and using (3.1) we have

$$\begin{aligned} -t &\equiv -2(x+2)x && \mod p, \\ t &\equiv 2x(x+1) + 2x && \mod p, \\ t &\equiv 2x - 2 && \mod p. \end{aligned}$$

Putting result into s_3 we obtain

$$\begin{aligned} 6x + tx - t &\equiv 6x + (2x-2)x - (2x-2) && \mod p \\ &= 6x + 2x^2 - 2x - 2x + 2 \\ &= 2x(x+1) + 2 \\ &\equiv 0 && \mod p \end{aligned}$$

We checked remaining cases in a similar way.

$(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4)$	$(\widehat{A_x^{\varepsilon_1}} * \widehat{B_x^{\varepsilon_2}}) * (\widehat{A_x^{\varepsilon_3}} * \widehat{B_x^{\varepsilon_4}}) - t * (\widehat{A_x^{\varepsilon_1}} * \widehat{B_x^{\varepsilon_4}})$	t
$(1,1,1,-1)$	$[-2\,x - t\,x - t - 4,\ [2\,x + t\,x + 4 + t,\ 2\,x + t\,x + 4 + t,\ 6\,x + t\,x - t]]$	$2x-2$
$(1,1,-1,1)$	$[-2\,x - t\,x - 4 + t,\ [-2\,x - t\,x - 4 + t,\ 6\,x - 3\,t\,x - 3\,t,\ -2\,x - t\,x - 4 + t]]$	$2x+2$
$(1,1,-1,-1)$	$[2\,x - t\,x + 4 - t,\ [-2\,x + t\,x - 4 + t,\ -2\,x + t\,x - 4 + t,\ -6\,x + t\,x - t]]$	$-2x+2$
$(1,-1,1,1)$	$[-2\,x - t\,x - 4 + t,\ [-2\,x - t\,x - 4 + t,\ 6\,x - 3\,t\,x - 3\,t,\ -2\,x - t\,x - 4 + t]]$	$2x+2$
$(1,-1,-1,1)$	$[2\,x - t\,x + 4 + t,\ [2\,x - t\,x + 4 + t,\ -6\,x - 3\,t\,x - 3\,t,\ 2\,x - t\,x + 4 + t]]$	$-2x-2$
$(1,-1,-1,-1)$	$[-2\,x - t\,x - t - 4,\ [2\,x + t\,x + 4 + t,\ 2\,x + t\,x + 4 + t,\ 6\,x + t\,x - t]]$	$2x-2$
$(-1,1,1,1)$	$[-2\,x - t\,x - t - 4,\ [6\,x + t\,x - t,\ 2\,x + t\,x + 4 + t,\ 2\,x + t\,x + 4 + t]]$	$2x-2$
$(-1,1,1,-1)$	$[2\,x - t\,x + 4 + t,\ [-2\,x - t\,x - t,\ 2\,x + t\,x + t,\ -2\,x - t\,x - t]]$	$-2x-2$
$(-1,1,-1,-1)$	$[-2\,x - t\,x - 4 + t,\ [2\,x - t\,x - t,\ -2\,x + t\,x + t,\ 2\,x - t\,x - t]]$	$2x+2$
$(-1,-1,1,1)$	$[2\,x - t\,x + 4 - t,\ [-6\,x + t\,x - t,\ -2\,x + t\,x - 4 + t,\ -2\,x + t\,x - 4 + t]]$	$-2x+2$
$(-1,-1,1,-1)$	$[-2\,x - t\,x - 4 + t,\ [2\,x - t\,x - t,\ -2\,x + t\,x + t,\ 2\,x - t\,x - t]]$	$2x+2$
$(-1,-1,-1,1)$	$[-2\,x - t\,x - t - 4,\ [6\,x + t\,x - t,\ 2\,x + t\,x + 4 + t,\ 2\,x + t\,x + 4 + t]]]$	$2x-2$
$(1,1,1,1)$	$[-6\,x - t\,x + t,\ [-6\,x - t\,x + t,\ -6\,x - 3\,t\,x - 3\,t - 12,\ -6\,x - t\,x + t]]$	$2x-2$
$(1,-1,1,-1)$	$[2\,x - t\,x - t,\ [-2\,x + t\,x + t,\ -2\,x + t\,x + t,\ 2\,x + t\,x + 4 - t]]$	$2x+2$
$(-1,1,-1,1)$	$[2\,x - t\,x - t,\ [2\,x + t\,x + 4 - t,\ -2\,x + t\,x + t,\ -2\,x + t\,x + t]]$	$2x+2$
$(-1,-1,-1,-1)$	$[-6\,x - t\,x + t,\ [-2\,x - t\,x - t - 4,\ 2\,x + t\,x + 4 + t,\ -2\,x - t\,x - t - 4]]$	$2x-2$

Table 1

To finish the proof of the lemma we have to show that $\pm 2x \pm 2$ is never zero modulo p. In contrary, let us assume that $\pm 2x \pm 2 \equiv 0 \mod p$. Then $x \equiv \pm 1 \mod p$. If $x \equiv 1 \mod p$ then in virtue of (3.1) we have $1 \cdot 2 \equiv -1 \mod p$. This means that p divides 3 which is not our case by Lemma 3.1. If $x \equiv -1 \mod p$ then we have $1 \cdot 0 \equiv -1 \mod p$ which is an absurd.

□

ε	$\widehat{A_x^{\varepsilon}} * \widehat{A_x^{\varepsilon}} - t * \widehat{A_x^{\varepsilon}}$	t
-1	$[2\,x - t\,x - t,\ [t\,x + 2,\ -2\,x - 2 + t,\ 0]]$	$2x + 2$
1	$[2\,x - t\,x - t,\ [-t\,x - 2,\ 2\,x + 2 - t,\ 0]]$	$2x + 2$

Table 2

δ	$\widehat{B_x^{\delta}} * \widehat{B_x^{\delta}} - t * \widehat{B_x^{\delta}}$	t
1	$[2\,x - t\,x - t,\ [0,\ -2\,x - 2 + t,\ t\,x + 2]]$	$2x + 2$
-1	$[2\,x - t\,x - t,\ [0,\ 2\,x + 2 - t,\ -t\,x - 2]]$	$2x + 2$

Table 3

THEOREM 3.3. *If $x > 1$ then the group Γ_x is free on free generators A_x and B_x.*

Proof. We need to consider only reduced words. So let w be an alternating product of non-zero powers of A_x and B_x. It is evident that w is conjugated either to a non-zero power of A_x or B_x or to a word of a form

$$w(A_x, B_x) = A_x^{j_1} B_x^{k_1} \dots A_x^{j_n} B_x^{k_n}, \text{ where } j_i, k_i \neq 0. \tag{3.4}$$

First, let us consider the latter case. Using (3.3) of the Lemma 3.2 and the congruence property of the relation $\asymp_p$ we reduce

$$w(\widehat{A_x}, \widehat{B_x}) \asymp_p \widehat{A_x^{j_1'}}\widehat{B_x^{k_1'}} \dots \widehat{A_x^{j_n'}}\widehat{B_x^{k_n'}} \text{ for some } j_i', k_i' \in \{-1, 1\}. \tag{3.5}$$

Next using (3.2) of the Lemma 3.2 and again the congruence property of $\asymp_p$ we reduce the word (3.5)

$$w(\widehat{A_x}, \widehat{B_x}) \asymp_p \widehat{A_x^{j}}\widehat{B_x^{k}} \text{ for some } j, k \in \{-1, 1\}.$$

Similarly we can consider the case when w is conjugated to a non-zero power of A_x or B_x. Therefore the word $w(\widehat{A_x}, \widehat{B_x})$ is related with respect to $\asymp_p$ with one of the quaternions of the set

$$R_x = \{\widehat{A_x^{j_1}} * \widehat{B_x^{k_1}}, \widehat{A_x^{\pm 1}}, \widehat{B_x^{\pm 1}}\} \text{ where } j_1, k_1 \in \{-1, 1\}.$$

We will show that for every $w \in R_x$ it is false that $s(w) \asymp_p [0, 0, 0]$. So Theorem 3.3 will directly follow from the transitivity of the relation $\asymp_p$. In contrary let us assume that $s(w) \asymp_p [0, 0, 0]$. If $w = \widehat{A_x}\widehat{B_x}$ then $s(w) \equiv_p [x - 1, 3x + 3, x - 1]$. We have $3x \equiv -3 \mod p$. But $(3, p) = 1$, hence $x \equiv -1 \mod p$. But this is a contradiction with the property of p. Now let $w \in \{\widehat{A_x}\widehat{B_x^{-1}}, \widehat{A_x^{-1}}\widehat{B_x}, \widehat{A_x^{-1}}\widehat{B_x^{-1}}\}$. Then $s(w)$ is related, with respect to $\equiv_p$, to one of the vectors from the set $\{[-x-1, -x-1, -x+1], [-x+1, -x-1, -x-1], [x+1, -x-1, x+1]\}$. So in each case we have $x \equiv -1 \mod p$. If $w = \widehat{A_x^{\pm 1}}$ then $s(w) \equiv_p [\pm x, \pm 1, 0]$. Hence the relation

$s(w) \asymp_p [0,0,0]$ does not hold. In a similar way we show this fact for $w = \widehat{B_x^{\pm 1}}$. □

4. Fixed points

In this section we focus our attention on those integers x for which Γ_x acts without fixed points on the rational unit sphere. For a given integer x assume that there exists a vector $q \in \mathbb{Q}^3$ and some nontrivial element w from Γ_x for which $w(q) = q$. Without loss of generality we can assume that w is of a form (3.4) or w is a non-zero power of A_x or B_x. Let $s(\widehat{w}) = (x_1, x_2, x_3)$. So we have

$$q = \frac{s(\widehat{w})}{\sqrt{x_1^2 + x_2^2 + x_3^2}}.$$

Therefore $\sqrt{x_1^2 + x_2^2 + x_3^2} \in \mathbb{Q}$ and $x_1^2 + x_2^2 + x_3^2$ must be a square of an integer. From the previous section we know that $\widehat{w} \asymp_p w'$, where $w' \in R_x$ which implies the following relation

$$t^2(x_1^{'2} + x_2^{'2} + x_3^{'2}) \equiv x_1^2 + x_2^2 + x_3^2 \mod p \text{ for some } t \in \mathbb{Z}_p^*.$$

Hence the expression on the left is a square in $\mathbb{Z}_p$. Now we define two subsets of $\mathbb{Z}_p$, namely

$$\begin{aligned} Z_1 &= \{y^2 \mid y \in \mathbb{Z}_p\}, \\ Z_2 &= \bigcup_{w' \in R_x} \{t^2(x_1^{'2} + x_2^{'2} + x_3^{'2}) \mid t \in \mathbb{Z}_p^*\}. \end{aligned}$$

So to show that the action of the group Γ_x is fixed point free on $S^2 \cap \mathbb{Q}^3$ it is sufficient to show that $Z_1 \cap Z_2 = \emptyset$. If $w' \in R_x$ the expression $x_1^{'2} + x_2^{'2} + x_3^{'2}$ is congruent modulo p with one of the element of the set $\{4x+4, 3x, -x\}$. So we seek for pairs (x, p) such that

$$(\frac{4x+4}{p}) = -1, (\frac{3x}{p}) = -1 \text{ and } (\frac{-x}{p}) = -1, \tag{4.1}$$

where $(\frac{a}{b})$ denotes Legendre symbol. We have $(\frac{4x+4}{p}) = (\frac{2^2}{p})(\frac{x+1}{p})$ so we only consider the value of $(\frac{x+1}{p})$. Using the relation 3.1 we observe the sequence of powers of $(x+1)$ modulo p has periodicity 6.

k	0	1	2	3	4	5
$(x+1)^k$	1	$x+1$	x	-1	$-x-1$	$-x$

Neither $x, x+1, -x$ nor $-x-1$ is congruent to 1 or -1 modulo p. This can be checked by proceeding similar considerations from the end of the last section. So we have that $(x+1)^q \equiv -1 \mod p$ if and only if $q = 6k+3, k \in \mathbb{Z}$ and $(x+1)^q \equiv 1 \mod p$ if and only if $q = 6k, k \in \mathbb{Z}$. Observe that $(\frac{x+1}{p}) = \pm 1$ and $(\frac{x+1}{p}) \equiv (x+1)^{\frac{p-1}{2}} \mod p$. Thus $p \equiv 1 \mod 12$ or $p \equiv 7 \mod 12$. Let us denote by P_1 and P_7 sets of primes which satisfy appropriate condition. Moreover we denote for every x the set

$$D_x = \{p \mid p \text{ is prime and } p > 3 \text{ and } p \text{ divides } x^2 + x + 1\}.$$

Now let assume that $D_x \cap P_7 \neq \emptyset$. Let $p \in D_x \cap P_7$. We compute

$$(\tfrac{x+1}{p}) \equiv (x+1)^{\frac{p-1}{2}} = (x+1)^{6k+3} \equiv -1 \mod p.$$

Taking both sides of the congruence 3.1 to the $\frac{p-1}{2}$-th power we obtain

$$(\tfrac{x+1}{p})(\tfrac{x}{p}) \equiv (-1)^{\frac{p-1}{2}} = (-1)^{6k+3} = -1 \mod p.$$

Therefore

$$(\tfrac{-x}{p}) \quad = \quad (\tfrac{x}{p})(\tfrac{-1}{p}) \quad \equiv \quad 1 \cdot -1 \quad = \quad -1 \mod p.$$

Finally, from [**1**] chapter 2.3 exercise 4 we deduce that $(\frac{3}{p}) = -1$ and relations 4.1 are satisfied. To obtain such pairs (x, p) we can start from $p \in P_7$ and solve the equation 3.1. For $p = 7$ we have $x = 2$ and $x = 4$. Thus we obtain the pair that Sato has found in paper [**4**]. However, there are many x for which the set $D_x \cap P_7$ is empty and we don't know how to settle this case.

Acknowledgments

Supported by BW 5100-5-0205-6.

References

[1] G. Davidoff, P. Sarnak, A. Valette *Elementary number theory, group theory and Ramanujan Graphs*, London Mathematical Society, Student Texts **55** (2003).

[2] J. Krempa, On free subgroups of units in quaternion algebras. *Colloq. Math.*, **88** (2001), 21-27.

[3] G. Liu, L. C. Robertson, Free subgroups of $\mathrm{SO}(3, \mathbb{Q})$. *Communications in Algebra*, **27(**4) (1999), 1555-1570.

[4] K. Sato, A free group acting without fixed points on the rational unit sphere. *Fundamenta Mathematicae*, **148** (1995), 63-69.

[5] S. Świerczkowski, A class of free rotations groups. *Indag. Mathem., N.S.* , **5(**2) (1994), 221-226.

[6] J. Tits, Free subgroups in linear groups. *J. Algebra* **20** (1972), 250-270.

[7] S. Wagon, *The Banach-Tarski Paradox*. Corrected reprint of the 1985 original, Cambridge Univ. Press, Cambridge, 1993.

Received 01 08 2007, revised 09 04 2008

Institute of Mathematics,
University of Gdańsk,
Wita Stwosza 57, 80-952 Gdańsk,
Poland
E-mail address: sagata@math.univ.gda.pl