ACTA ARITHMETICA
LXXXV.2 (1998)

Free groups acting without fixed points on rational spheres

by

KENZI SATÔ (Yokohama)

For every positive rational number q, we find a free group of rotations of rank 2 acting on $(\sqrt{q}\,\mathbb{S}^2) \cap \mathbb{Q}^3$ whose all elements distinct from the identity have no fixed point.

Introduction. The following conjecture raised by Professor J. Mycielski was proved in [Sa1]:

The subgroup $\langle \mu_1, \nu_1 \rangle$ *of the rational special orthogonal group* $SO_3(\mathbb{Q}) = \{\phi \in \mathrm{Mat}(3,3;\mathbb{Q}) : {}^t\phi \cdot \phi = \mathrm{id}, \det \phi = 1\}$ *is a free group of rank* 2 *whose non-trivial elements have no fixed point on the rational unit sphere* $\mathbb{S}^2 \cap \mathbb{Q}^3 = \{\vec{v} \in \mathbb{Q}^3 : |\vec{v}| = 1\}$, *where* $\langle \mu_1, \nu_1 \rangle$ *is the group generated by*

$$\mu_1 = \frac{1}{7}\begin{pmatrix} 6 & 2 & 3 \\ 2 & 3 & -6 \\ -3 & 6 & 2 \end{pmatrix} \quad \textit{and} \quad \nu_1 = \frac{1}{7}\begin{pmatrix} 2 & -6 & 3 \\ 6 & 3 & 2 \\ -3 & 2 & 6 \end{pmatrix}.$$

In this paper, we consider the same problem about the rational sphere $(\sqrt{q}\,\mathbb{S}^2) \cap \mathbb{Q}^3 = \{\vec{v} \in \mathbb{Q}^3 : |\vec{v}| = \sqrt{q}\}$ for positive $q \in \mathbb{Q}$. Notice that the rational unit sphere $\mathbb{S}^2 \cap \mathbb{Q}^3$ and the rational sphere $(\sqrt{2}\,\mathbb{S}^2) \cap \mathbb{Q}^3$ are not similar. In particular, $\mathbb{S}^2 \cap \mathbb{Q}^3$ has a trio of pairwise orthogonal vectors

$$\vec{e}_0 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad \vec{e}_1 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad \vec{e}_2 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix},$$

but $(\sqrt{2}\,\mathbb{S}^2) \cap \mathbb{Q}^3$ does not have such a trio, because, for two orthogonal vectors $\vec{v}, \vec{v}' \in (\sqrt{2}\,\mathbb{S}^2) \cap \mathbb{Q}^3$, the vector $\frac{1}{\sqrt{2}}\vec{v} \times \vec{v}'$ does not belong to $\mathbb{Q}^3$. The purpose of this paper is to prove:

1991 *Mathematics Subject Classification*: Primary 20E05, 20H05, 20H20; Secondary 15A18, 51F20, 51F25.

For each positive rational q, $SO_3(\mathbb{Q})$ has a free subgroup $\langle \mu_q, \nu_q \rangle$ which acts on $(\sqrt{q}\,\mathbb{S}^2) \cap \mathbb{Q}^3$, the rational sphere with radius $\sqrt{q}$, and whose non-trivial elements have no fixed point on $(\sqrt{q}\,\mathbb{S}^2) \cap \mathbb{Q}^3$.

This implies a paradox: $(\sqrt{q}\,\mathbb{S}^2) \cap \mathbb{Q}^3$ has a Hausdorff decomposition, i.e., $(\sqrt{q}\,\mathbb{S}^2) \cap \mathbb{Q}^3$ can be partitioned into three subsets A, B, and C such that A, B, C, $A \cup B$, $B \cup C$, and $C \cup A$ are all congruent by rotations of $\langle \mu_q, \nu_q \rangle$ (see e.g. [Sa0; W, Cor. 4.12]). We only have to prove the assertion for each positive integer q which is square-free, in other words, q does not have a prime whose square divides q, because the rational spheres $(\sqrt{q}\,\mathbb{S}^2) \cap \mathbb{Q}^3$ and $(\sqrt{q'}\,\mathbb{S}^2) \cap \mathbb{Q}^3$ are similar with similitude ratio $\sqrt{q} : \sqrt{q'}$ if $\sqrt{q}/\sqrt{q'} \in \mathbb{Q}$. Moreover, we can assume $q \neq 1$ from [Sa1].

Remark. It is possible that rational spheres are empty (e.g., with radius $\sqrt{7}$). For given q, it is easy to check whether the rational sphere with radius $\sqrt{q}$ is empty or not (see [M, Ch. 20]):

$$\begin{aligned} &(\sqrt{q}\,\mathbb{S}^2) \cap \mathbb{Q}^3 \neq \emptyset \quad \text{if } q \equiv 1, 2, 3, 5, \text{ or } 6 \pmod 8, \\ &(\sqrt{q}\,\mathbb{S}^2) \cap \mathbb{Q}^3 = \emptyset \quad \text{if } q \equiv 7 \pmod 8. \end{aligned}$$

For higher dimensional spheres, Professor J. Mycielski raised the following problems (see [Sa1]):

Problem A. *For $n \in \mathbb{N}$, n even, $n \geq 4$, does $SO_n(\mathbb{Q})$ have a free non-abelian subgroup F_2 such that no elements of F_2 different from the identity have eigenvectors in $\mathbb{Q}^n$?*

Problem B. *For $n \in \mathbb{N}$, n odd, $n \geq 5$, does $SO_n(\mathbb{Q})$ have a free non-abelian subgroup F_2 which acts without non-trivial fixed points on $\mathbb{S}^{n-1} \cap \mathbb{Q}^n$ and is such that if $f, g \in F_2$ have a common eigenvector in $\mathbb{Q}^n$ then $fg = gf$?*

[Sa2], which gives a free group $\langle \sigma, \tau \rangle$ of $SO_4(\mathbb{Q})$ acting on $\mathbb{S}^3$ without non-trivial fixed points, and [Sa1] answer in the affirmative Problem A for $n \equiv 0 \pmod 4$ and Problem B for $n \equiv -1 \pmod 4$. This paper and [Sa2] also answer in the affirmative the following problem for $n \equiv -1 \pmod 4$:

Problem B′. *For a positive rational q and an odd integer $n \geq 5$, does $SO_n(\mathbb{Q})$ have a free non-abelian subgroup F_2 which acts without non-trivial fixed points on $(\sqrt{q}\,\mathbb{S}^{n-1}) \cap \mathbb{Q}^n$ and is such that if $f, g \in F_2$ have a common eigenvector in $\mathbb{Q}^n$ then $fg = gf$?*

For $n = 3$, similar problems for more general surfaces, which the referee of this paper suggested, can be considered:

PROBLEM C. *Is there a free subgroup of rank* 2 *of the group* $\{\phi \in \mathrm{Mat}(3,3;\mathbb{Q}) : {}^t\phi \cdot \Lambda \cdot \phi = \Lambda,\ \det\phi = 1\}$ *acting on the rational surface*

$$\left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{Q}^3 : \alpha x^2 + \beta y^2 + \gamma z^2 = q \right\}$$

without non-trivial fixed points (*where* $\Lambda = \begin{pmatrix} \alpha & 0 & 0 \\ 0 & \beta & 0 \\ 0 & 0 & \gamma \end{pmatrix}$)*?*

Preliminaries. Let q be a positive and square-free integer distinct from 1. The following two lemmas enable us to find integers p and b such that p is an odd prime divisor of $1+b^2$ but not of q, and q is a quadratic non-residue to the modulus p.

LEMMA 0. *For such an integer* q, *there exists an odd prime* p *such that* q *is not divisible by* p *and*

$$\left(\frac{-1}{p}\right) = 1 \quad \textit{and} \quad \left(\frac{q}{p}\right) = -1,$$

where $\left(\frac{\cdot}{\cdot}\right)$ *is Legendre's symbol.*

Proof. This is a special case of [H, Satz 147]: "Let $a_1, a_2, \ldots, a_r$ be integers such that: a product of powers

$$a_1^{u_1} a_2^{u_2} \ldots a_r^{u_r}$$

is the square of an integer (if and) only if all u_i's are even. Furthermore, let $c_1, c_2, \ldots, c_r$ be arbitrary one of ± 1. Then there exist infinitely many primes p which satisfy the condition

$$\left(\frac{a_i}{p}\right) = c_i \quad \text{for } i = 1, 2, \ldots, r.\text{''} \ \blacksquare$$

LEMMA 1. *For such a prime* p, *there exists an integer* b *such that* $1+b^2 \equiv 0 \pmod{p}$.

Proof. This is obvious from $\left(\frac{-1}{p}\right) = 1$. ■

Using such an integer b, let

$$\mu_q = \frac{1}{1+b^2} \begin{pmatrix} 1+b^2 & 0 & 0 \\ 0 & 1-b^2 & -2b \\ 0 & 2b & 1-b^2 \end{pmatrix}$$

and

$$\nu_q = \frac{1}{1+b^2} \begin{pmatrix} 1-b^2 & -2b & 0 \\ 2b & 1-b^2 & 0 \\ 0 & 0 & 1+b^2 \end{pmatrix}.$$

There are group isomorphisms

$$S(\mathbb{H})/\{\pm 1\} \xrightarrow[\cong]{\sigma} SO(\mathbb{H}_0) \xrightarrow[\cong]{\mathfrak{m}} SO_3(\mathbb{R}),$$

where $S(\mathbb{H})$ is the group of quaternions h whose norm $|h|$ is equal to 1 in the Hamilton quaternion field $\mathbb{H}$ and $SO(\mathbb{H}_0)$ is the group of all linear isometries with determinant 1 of all pure quaternions $\mathbb{H}_0$ onto itself. The left isomorphism σ sends $\pm h$ to the isometry $\mathbb{H}_0 \ni h' \mapsto hh'h^{-1} \in \mathbb{H}_0$. On the other hand, the linear map $\iota : \mathbb{H}_0 \to \mathbb{R}^3$, which takes the basis I, J, and K of $\mathbb{H}_0$ (with $IJ = K$, $JK = I$, $KI = J$, and $I^2 = J^2 = K^2 = -1$) to the standard basis $\vec{e}_0$, $\vec{e}_1$, and $\vec{e}_2$ of $\mathbb{R}^3$ respectively, gives the right isomorphism $\mathfrak{m} : \kappa \mapsto \iota \circ \kappa \circ \iota^{-1}$. So we have $S(\mathbb{H})/\{\pm 1\} \xrightarrow[\cong]{\mathfrak{m}\circ\sigma} SO_3(\mathbb{R})$. See [C, Th. 3.1 of Ch. 10; L, Th. 3.1 of Ch. 3; Sa0; Sa1]. Two matrices above and their inverses are represented by

$$\mu_q^{\varepsilon} = \mathfrak{m} \circ \sigma\left(\pm\frac{1+\varepsilon bI}{\sqrt{1+b^2}}\right) \quad \text{and} \quad \nu_q^{\delta} = \mathfrak{m} \circ \sigma\left(\pm\frac{1+\delta bK}{\sqrt{1+b^2}}\right),$$

where ε and δ are either -1 or 1. For each reduced word w of $\{\mu_q^{-1}, \mu_q, \nu_q^{-1}, \nu_q\}$, we define

$$\pm H_w = \sqrt{1+b^2}^{\sharp w} \sigma^{-1} \circ \mathfrak{m}^{-1}(w) \in Z(\mathbb{H})/\{\pm 1\},$$

where $\sharp w$ is the number of occurrences of μ_q^{-1}, μ_q, ν_q^{-1}, and ν_q in w and $Z(\mathbb{H})$ is the set of quaternions whose components are all integers. The relation $H \asymp H'$ means that H and H' in $Z(\mathbb{H})$ are proportional mod p, i.e., there exists an integer $t \in \{1, \ldots, p-1\}$ such that each component of $H - tH'$ is divisible by p. We consider whether $H \asymp H'$ or not. We can choose H_w from $\sqrt{1+b^2}^{\# w} \sigma^{-1} \circ \mathfrak{m}^{-1}(w)$ whichever you like because $H \asymp -H$.

Main result. The following two lemmas imply the main theorem of this paper which gives a free subgroup of rank 2 of $SO_3(\mathbb{Q})$ whose non-identical elements have no fixed point on the rational sphere with radius $\sqrt{q}$.

Lemma 2. *Let w be a non-empty reduced word of $\{\mu_q^{-1}, \mu_q, \nu_q^{-1}, \nu_q\}$. If $w = \mu_q^{\varepsilon k}$ then*

$$H_w \asymp 1 + \varepsilon bI;$$

if $w = \nu_q^{\delta l}$ then

$$H_w \asymp 1 + \delta bK;$$

if w has the form $\mu_q^{\varepsilon} \ldots \nu_q^{\delta}$ (i.e., w starts with μ_q^{ε} and ends with ν_q^{δ}) then

$$H_w \asymp 1 + \varepsilon bI + \varepsilon\delta J + \delta bK,$$

where ε and δ are either -1 or 1, and k and l are positive integers.

Proof. The following four equations and $1+b^2 \equiv 0 \pmod p$ imply this lemma:

$$\begin{gathered}
(1+\varepsilon bI)(1+\varepsilon bI) = 2(1+\varepsilon bI) - (1+b^2);\\
(1+\delta bK)(1+\delta bK) = 2(1+\delta bK) - (1+b^2);\\
(1+\varepsilon bI)(1+\delta bK) = (1+\varepsilon bI+\varepsilon\delta J+\delta bK) - (1+b^2)\varepsilon\delta J;
\end{gathered}$$

$$\begin{aligned}
(1+\varepsilon' bI+\varepsilon'\delta' J+\delta' bK)&(1+\varepsilon bI+\varepsilon\delta J+\delta bK)\\
&= (1+\varepsilon'\varepsilon+\delta'\delta-\varepsilon'\delta'\varepsilon\delta)(1+\varepsilon' bI+\varepsilon'\delta J+\delta bK)\\
&\qquad - (1+b^2)(\varepsilon'\varepsilon+\delta'\delta+(\varepsilon'\delta-\delta'\varepsilon)J);
\end{aligned}$$

where ε, δ, ε', and δ' are either -1 or 1. ∎

LEMMA 3. *Let w be a word which appeared in Lemma 2, i.e., $w = \mu_q^{\varepsilon k}$, $w = \nu_q^{\delta l}$, or $w = \mu_q^{\varepsilon}\ldots\nu_q^{\delta}$. Then $\sqrt{q}\,|\mathrm{Im}\,H_w|$ is irrational, where $\mathrm{Im}\,H_w$ is the imaginary part of H_w, i.e., $\mathrm{Im}(C+XI+YJ+ZK) = XI+YJ+ZK$.*

Proof. It is enough to show that $q|\mathrm{Im}\,H_w|^2$ is a quadratic non-residue to p, which is a consequence of Lemma 2, the equality $\left(\frac{q}{p}\right) = -1$, and the following three formulae:

$$\begin{gathered}
q((\varepsilon tb)^2+0^2+0^2) = qt^2b^2,\\
q(0^2+0^2+(\delta tb)^2) = qt^2b^2,\\
q((\varepsilon tb)^2+(\varepsilon\delta t)^2+(\delta tb)^2) = qt^2(1+2b^2) \equiv qt^2b^2 \pmod p,
\end{gathered}$$

where $t = 1,\ldots,p-1$. ∎

We attain our objective from the previous lemma:

THEOREM. *The rotations μ_q and ν_q generate a free group whose non-trivial elements have no fixed point on $(\sqrt{q}\,\mathbb{S}^2)\cap\mathbb{Q}^3$.*

Proof. We only have to prove that $\mathrm{Im}\,H_w$ is non-zero and that $\sqrt{q}\cdot\iota(\mathrm{Im}\,H_w)/|\mathrm{Im}\,H_w|$ does not belong to $(\sqrt{q}\,\mathbb{S}^2)\cap\mathbb{Q}^3$ for each reduced word, w, of the form $\mu_q^{\varepsilon}\ldots\nu_q^{\delta}$ (i.e., w starts with μ_q^{-1} or μ_q and ends with ν_q^{-1} or ν_q) or simply a power of μ_q or of ν_q, because

$$w \text{ has a fixed point} \Leftrightarrow w'ww'^{-1} \text{ has a fixed point},$$

for an arbitrary word w' of $\{\mu_q^{-1},\mu_q,\nu_q^{-1},\nu_q\}$. For such a non-empty reduced word w, $\mathrm{Im}\,H_w$ is obviously non-zero and Lemma 3 implies

$$\sqrt{q}\,\frac{\iota(\mathrm{Im}\,H_w)}{|\mathrm{Im}\,H_w|} \notin \mathbb{Q}^3. \ \blacksquare$$

References

[C] J. W. S. Cassels, *Rational Quadratic Forms*, Academic Press, New York, 1978.

[H] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Akademische Verlagsgesellschaft, Leipzig, 1923.
[L] T. Y. Lam, *Algebraic Theory of Quadratic Forms*, W. A. Benjamin Inc., Massachusetts, 1973.
[M] L. J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969.
[Sa0] K. Satô, *A Hausdorff decomposition on a countable subset of* $\mathbb{S}^2$ *without the Axiom of Choice*, Math. Japon. 44 (1996), 307–312.
[Sa1] K. Satô, *A free group acting without fixed points on the rational unit sphere*, Fund. Math. 148 (1995), 63–69.
[Sa2] —, *A free group of rotations with rational entries on the* 3*-dimensional unit sphere*, Nihonkai Math. J. 8 (1997), 91–94.
[W] S. Wagon, *The Banach–Tarski Paradox*, Cambridge Univ. Press, Cambridge, 1985.

Department of Mathematics
Faculty of Engineering
Yokohama National University
Hodogaya, Yokohama 240, Japan
E-mail: kenzi@math.sci.ynu.ac.jp

Current address:
Department of Mathematics
Faculty of Engineering
Tamagawa University
6-1-1, Tamagawa-Gakuen, Machida
Tokyo 194-8610, Japan
E-mail: kenzi@eng.tamagawa.ac.jp

Received on 21.1.1997
and in revised form on 29.1.1998 (3121)