Indag. Mathem., N.S., 13 (3), 389–405 September 30, 2002

Free isometric actions on the affine space $\mathbb{Q}^n$

by Satô Kenzi

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

Communicated by Prof. M.S. Keane at the meeting of November 26, 2001

ABSTRACT

We will show that for every integer $n \geqq 3$ there exists a free non-abelian group of linear isometries of the vector space $\mathbb{Q}^n$ such that any subgroup fixing any point $\vec{v} \neq \vec{0}$ of $\mathbb{Q}^n$ is cyclic. Recall that two elements of F_2 commute if and only if they belong to a cyclic subgroup of F_2.

0. INTRODUCTION

F_2 will always denote a free (non-abelian) group with 2 free generators. Given a metric space X it is interesting to know if there exists an F_2 of isometries of X acting *without fixed points* (i.e., $\gamma(x) \neq x$ for all $\gamma \in F_2$, $\gamma \neq id$ and all $x \in X$) or at least *locally commutative* (i.e., $\gamma\gamma' = \gamma'\gamma$ for all $\gamma, \gamma' \in F_2$ such that there exists $x \in X$ for which $\gamma(x) = x = \gamma'(x)$).

The existence of such F_2 has several interesting and surprising geometric consequences which were discovered and studied by Klein, Fricke, Hausdorff and later by many authors. Some examples will be given at the end of the introduction. Motivated by those applications we will prove here the existence of such F_2 for some of the spaces $\mathbb{Q}^n$ and $\mathbb{S}^{n-1} \cap \mathbb{Q}^n$ with the usual Euclidean metric.

Here $\mathbb{Q}$ is the field of real rational numbers, $SO_n(\mathbb{Q})$ will denote the special orthogonal group of rotations of $\mathbb{Q}^n$ around the origin $\vec{0}$ and $\|\cdot\|$ the Euclidean norm in $\mathbb{Q}^n$. The main theorem of this paper is the following:

Theorem 0. *If n is odd, $n \geqq 3$, q is a positive rational, and $\sqrt{q}$ is irrational, then the* *group $SO_n(\mathbb{Q})$ has a free subgroup F_2 which acts in a locally commutative way on $\mathbb{Q}^n \setminus \{\vec{0}\}$ and acts without fixed points on $\{\vec{v} \in \mathbb{Q}^n : \|\vec{v}\|/\sqrt{q} \in \mathbb{Q},\ \vec{v} \neq \vec{0}\}$.*

Notice that we can assume without loss of generality that q is a square-free integer. It can happen that the set $\{\vec{v} \in \mathbb{Q}^n : \|\vec{v}\|/\sqrt{q} \in \mathbb{Q},\ \vec{v} \neq \vec{0}\}$ is empty, but for such q this is so if and only if $n = 3$ and $q \equiv 7 (\mathrm{mod}\ 8)$; see Ch. 20 in [8] or [16]. The problem if Theorem 0 is true for $q = 1$ is still open. Also the following problem is still open: Does there exist a free group F_2 of isometries of $\mathbb{Q}^3$ which acts without fixed points? [For $\mathbb{R}^3$ the answer is yes; see [2], [11] or Theorem 5.7 in [18]. For related material (also for the cases of $\mathbb{R}^2$ and $\mathbb{Z}^2$) see [6], [10] and [17].] A similar theorem which was already proved in [15] will be used in the proof of Theorem 0:

Theorem 1. *If n is a positive integer which is divisible by 4, then the group $SO_n(\mathbb{Q})$ has a free subgroup F_2 which acts without fixed points on $\mathbb{Q}^n \setminus \{\vec{0}\}$.*

(As conjectured in [14] and [16], Theorem 1 should be true for all even $n \geqq 4$, and to prove this it would suffice to prove it for $n = 6$. Indeed every even $n \geqq 4$ is of the form $4K$ or $4K + 6$; hence we can construct the required free generators of F_2 for such n by placing along the main diagonal matrices representing the free generators of F_2 for $n = 4$ and $n = 6$. Again in the case of $\mathbb{R}^n$ the answer is positive for all even $n \geqq 4$, see [0] or [3].)

Theorem 0 for $n = 3$ was already proved in [16]. Hence to prove it for all odd $n \geqq 3$ it suffices to prove it for $n = 5$. Indeed every such n is of the form $4K + 3$ or $4K + 5$, hence one can construct the required free generators of F_2 in $SO_n(\mathbb{Q})$ by placing along the main diagonal matrices representing the free generators of F_2 for $n = 4$ and $n = 3$, or $n = 4$ and $n = 5$, where the case $n = 4$ is given by Theorem 1. Thus our proof will discuss only the case $n = 5$.

Corollary 0. *For each $n \geqq 3$ the group $SO_n(\mathbb{Q})$ has a free subgroup F_2 which is locally commutative on $\mathbb{Q}^n \setminus \{\vec{0}\}$.*

Proof. We use in a similar way the fact that each $n \geqq 3$ is of the form $3K_0 + 4K_1 + 5K_2$ applying the cases $n = 3, 4$ and 5 of Theorems 0 and 1. □

Now we give four examples of applications of these theorems. Let G be a group of permutations of a set X, and $A \approx B$ means that A is *G-congruent* to B, i.e., $A, B \subseteq X$ and there exists $\gamma \in G$ such that $\gamma(A) = B$.

Example 0. *If there exists F_2 which acts without fixed points on X then there exists a partition of X into three disjoint sets A, B, C such that*

$$A \approx B \approx C \approx A \cup B \approx B \cup C \approx C \cup A.$$

[This is due essentially to F. Hausdorff; for a stronger theorem of R.M. Robinson; see [12] or Corollary 4.12 in [18].]

Example 1. *The statements* (a) *there exists* F_2 *which is locally commutative on* X, *and* (b) *there exist three partitions of* X *into disjoint sets*

$$X = A_0 \cup A_1 \cup A_2 \cup A_3 = B_0 \cup B_1 = B_2 \cup B_3$$

such that

$$A_h \approx B_h \quad for \quad h = 0,\ 1,\ 2 \text{ and } 3,$$

are equivalent to each other.

[(a)⇒(b) is a special case of a theorem of R.M. Robinson and (b)⇒(a) is due to T.J. Dekker; see [12] and [1], or Theorem 4.5 and Theorem 4.8 in [18].]

Example 2. *If there exists* F_2 *which is locally commutative on a denumerable* X *then there exists a set* $E \subseteqq X$ *such that*

$$E \approx E \triangle F$$

for every finite $F \subseteqq X$ *(*$\triangle$ *denotes the symmetric difference of sets).*

[For more general theorems, see [9].]

Recall that, if X is a metric space, a set $A \subseteqq X$ is called *regular open* iff A is the interior of its closure. Informally speaking A is regular open if it is open without any missing dust. Let $A \vee B$ denote the interior of the closure of $A \cup B$.

Example 3. *For each* $n \geqq 3$ *and each positive rational* q, *the sphere* $(\sqrt{q}\mathbb{S}^{n-1}) \cap \mathbb{Q}^n = \{\vec{v} \in \mathbb{Q}^n : \|\vec{v}\| = \sqrt{q}\}$ *has twelve regular open subsets* $A_0, \ldots, A_5$ *and* $B_0, \ldots, B_5$ *such that* $A_0, \ldots, A_5$ *are pairwise disjoint,* B_0, B_1 *and* B_2 *are pairwise disjoint,* B_3, B_4 *and* B_5 *are pairwise disjoint,*

$$(\sqrt{q}\mathbb{S}^{n-1}) \cap \mathbb{Q}^n = A_0 \vee \cdots \vee A_5 = B_0 \vee B_1 \vee B_2 = B_3 \vee B_4 \vee B_5,$$

and

$$A_h \approx B_h \quad for \quad h = 0, \ldots, 5.$$

[This follows from a more general theorem of R. Dougherty and M. Foreman [4] and our Corollary 0. Indeed a statement similar to Example 3 for the real spheres $\sqrt{q}\mathbb{S}^{n-1} = \{\vec{v} \in \mathbb{R}^n : \|\vec{v}\| = \sqrt{q}\}$, where $n \geqq 3$ and $F_2 \subseteqq SO_n(\mathbb{R})$, follows from the theorem in [4]. So it suffices to pick $F_2 \subseteqq SO_n(\mathbb{Q})$ as in the Corollary 0 and to intersect their sets A_h and B_h with $\mathbb{Q}^n$.]

Unlike for the case of the field $\mathbb{R}$, the Examples 0–3 (which pertain to the field $\mathbb{Q}$) can be proved without using the axiom of choice.

The author is greatful to Jan Mycielski for many remarks which improved this paper.

1. THE GENERATORS OF F_2

As mentioned in the Introduction we can assume without loss of generality that $n = 5$ and that q is a positive integer. We can also assume that q is square-free and $q \neq 1$ (since $\sqrt{q} \notin \mathbb{Q}$). Then there exist an odd prime p and an integer b such that p is a divisor of $1+b^2$ but not of q, and q is a quadratic non-residue to the modulus p; see [16] (this is a special case of Satz 147 in [5]). Let

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

and

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

Thus $\alpha, \beta \in SO_5(\mathbb{Q})$. We will show that the group generated by α and β is a free group of rank 2 which satisfies the conclusion of Theorem 0. From now on, F_2 denotes the group generated by α and β.

2. A LEMMA ABOUT AXES OF ROTATIONS

For each positive integer m, notice that the fixed points of a generic rotation $\phi \in SO_{2m+1}(\mathbb{R})$ constitutes a 1-dimensional line. The purpose of this section is to work out a more explicit representation of this axis. The formula established here will be used in Section 3. A square matrix

$$\phi = \begin{pmatrix} \phi_0^0 & \cdots & \phi_{2m}^0 \\ \vdots & \ddots & \vdots \\ \phi_0^{2m} & \cdots & \phi_{2m}^{2m} \end{pmatrix}$$

which belongs to $SO_{2m+1}(\mathbb{R})$, i.e., ϕ satisfies ${}^t\phi \cdot \phi = id$ and $\det \phi = 1$, can be represented in the form

$$\phi = T \begin{pmatrix} 1 & & & & & & & \mathbf{0} \\ & c & -s & & & & & \\ & s & c & & & & & \\ & & & c' & -s' & & & \\ & & & s' & c' & & & \\ & & & & & \ddots & & \\ & & & & & & c^{(m-1)} & -s^{(m-1)} \\ \mathbf{0} & & & & & & s^{(m-1)} & c^{(m-1)} \end{pmatrix} T^{-1},$$

where

$$T = \begin{pmatrix} t_0^0 & \cdots & t_{2m}^0 \\ \vdots & \ddots & \vdots \\ t_0^{2m} & \cdots & t_{2m}^{2m} \end{pmatrix} \in SO_{2m+1}(\mathbb{R}),$$

and $c^{(r)}, s^{(r)} \in \mathbb{R}$ with $(c^{(r)})^2 + (s^{(r)})^2 = 1$ for $r = 0, 1, \ldots, m-1$ (see for example Chapter IV, §6 in [13] or Theorem 5.4 in [19]). Moreover we have the following lemma, in which we denote the remainder z mod $(2m+1)$ by $[z]$.

Lemma 0. *Let $\phi \in SO_{2m+1}(\mathbb{R})$ be represented as stated above. Then, for $i = 0, 1, \ldots, 2m$, we have*

$$\frac{1}{2^m m!} \sum_{\mathfrak{s} \in \mathfrak{S}_{2m}} \operatorname{sgn} \mathfrak{s} \prod_{r=0}^{m-1} (\phi^{[i+1+\mathfrak{s}(2r+1)]}_{[i+1+\mathfrak{s}(2r)]} - \phi^{[i+1+\mathfrak{s}(2r)]}_{[i+1+\mathfrak{s}(2r+1)]}) = 2^m t^i_0 s s' \cdots s^{(m-1)},$$

where $\mathfrak{S}_{2m}$ is the symmetric group on $\{0, 1, \ldots, 2m-1\}$.

Proof. We observe first

$$(*) \qquad \phi^{j'}_j - \phi^j_{j'} = 2 \sum_{r_*=0}^{m-1} (t^j_{2r_*+1} t^{j'}_{2r_*+2} - t^{j'}_{2r_*+1} t^j_{2r_*+2}) s^{(r_*)},$$

and

$$(\star) \qquad \begin{pmatrix} \tilde{t}^0_0 & \cdots & \tilde{t}^{2m}_0 \\ \vdots & \ddots & \vdots \\ \tilde{t}^0_{2m} & \cdots & \tilde{t}^{2m}_{2m} \end{pmatrix} = \det T \cdot T^{-1} = 1 \cdot {}^tT,$$

where $\tilde{t}^i_j$ is the cofactor of t^i_j in T. We can get this lemma by a direct calculation:

$$\begin{aligned}
&\frac{1}{2^m m!} \sum_{\mathfrak{s} \in \mathfrak{S}_{2m}} \operatorname{sgn} \mathfrak{s} \prod_{r=0}^{m-1} (\phi^{[i+1+\mathfrak{s}(2r+1)]}_{[i+1+\mathfrak{s}(2r)]} - \phi^{[i+1+\mathfrak{s}(2r)]}_{[i+1+\mathfrak{s}(2r+1)]}) = \\
&= \frac{1}{m!} \sum_{\mathfrak{s}} \operatorname{sgn} \mathfrak{s} \prod_{r} \sum_{r_*=0}^{m-1} (t^{[i+1+\mathfrak{s}(2r)]}_{2r_*+1} t^{[i+1+\mathfrak{s}(2r+1)]}_{2r_*+2} - t^{[i+1+\mathfrak{s}(2r+1)]}_{2r_*+1} t^{[i+1+\mathfrak{s}(2r)]}_{2r_*+2}) s^{(r_*)} = \\
&= \frac{1}{m!} \sum_{\mathfrak{s}} \operatorname{sgn} \mathfrak{s} \sum_{r_0=0}^{m-1} \sum_{r_1=0}^{m-1} \cdots \sum_{r_{m-1}=0}^{m-1} (t^{[i+1+\mathfrak{s}(0)]}_{2r_0+1} t^{[i+1+\mathfrak{s}(1)]}_{2r_0+2} - t^{[i+1+\mathfrak{s}(1)]}_{2r_0+1} t^{[i+1+\mathfrak{s}(0)]}_{2r_0+2}) \cdot \\
&\quad \cdot (t^{[i+1+\mathfrak{s}(2)]}_{2r_1+1} t^{[i+1+\mathfrak{s}(3)]}_{2r_1+2} - t^{[i+1+\mathfrak{s}(3)]}_{2r_1+1} t^{[i+1+\mathfrak{s}(2)]}_{2r_1+2}) \cdots \\
&\quad \cdots (t^{[i+1+\mathfrak{s}(2m-2)]}_{2r_{m-1}+1} t^{[i+1+\mathfrak{s}(2m-1)]}_{2r_{m-1}+2} - t^{[i+1+\mathfrak{s}(2m-1)]}_{2r_{m-1}+1} t^{[i+1+\mathfrak{s}(2m-2)]}_{2r_{m-1}+2}) \cdot \\
&\quad \cdot s^{(r_0)} s^{(r_1)} \cdots s^{(r_{m-1})} = \\
&= \frac{1}{m!} \sum_{r_0} \sum_{r_1} \cdots \sum_{r_{m-1}} \Bigl(\sum_{\mathfrak{s}} \operatorname{sgn} \mathfrak{s} (t^{[i+1+\mathfrak{s}(0)]}_{2r_0+1} t^{[i+1+\mathfrak{s}(1)]}_{2r_0+2} - t^{[i+1+\mathfrak{s}(1)]}_{2r_0+1} t^{[i+1+\mathfrak{s}(0)]}_{2r_0+2}) \cdot \\
&\quad \cdot (t^{[i+1+\mathfrak{s}(2)]}_{2r_1+1} t^{[i+1+\mathfrak{s}(3)]}_{2r_1+2} - t^{[i+1+\mathfrak{s}(3)]}_{2r_1+1} t^{[i+1+\mathfrak{s}(2)]}_{2r_1+2}) \cdots \\
&\quad \cdots (t^{[i+1+\mathfrak{s}(2m-2)]}_{2r_{m-1}+1} t^{[i+1+\mathfrak{s}(2m-1)]}_{2r_{m-1}+2} - t^{[i+1+\mathfrak{s}(2m-1)]}_{2r_{m-1}+1} t^{[i+1+\mathfrak{s}(2m-2)]}_{2r_{m-1}+2}) \Bigr) \cdot \\
&\quad \cdot s^{(r_0)} s^{(r_1)} \cdots s^{(r_{m-1})} = \\
&= \frac{1}{m!} \sum_{r_0} \sum_{r_1} \cdots \sum_{r_{m-1}} 2^m \cdot
\end{aligned}$$

$$\cdot \det \begin{pmatrix} t^{[i+1]}_{2r_0+1} & t^{[i+1]}_{2r_0+2} & t^{[i+1]}_{2r_1+1} & t^{[i+1]}_{2r_1+2} & \cdots & t^{[i+1]}_{2r_{m-1}+1} & t^{[i+1]}_{2r_{m-1}+2} \\ t^{[i+2]}_{2r_0+1} & t^{[i+2]}_{2r_0+2} & t^{[i+2]}_{2r_1+1} & t^{[i+2]}_{2r_1+2} & \cdots & t^{[i+2]}_{2r_{m-1}+1} & t^{[i+2]}_{2r_{m-1}+2} \\ t^{[i+3]}_{2r_0+1} & t^{[i+3]}_{2r_0+2} & t^{[i+3]}_{2r_1+1} & t^{[i+3]}_{2r_1+2} & \cdots & t^{[i+3]}_{2r_{m-1}+1} & t^{[i+3]}_{2r_{m-1}+2} \\ t^{[i+4]}_{2r_0+1} & t^{[i+4]}_{2r_0+2} & t^{[i+4]}_{2r_1+1} & t^{[i+4]}_{2r_1+2} & \cdots & t^{[i+4]}_{2r_{m-1}+1} & t^{[i+4]}_{2r_{m-1}+2} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ t^{[i+2m-1]}_{2r_0+1} & t^{[i+2m-1]}_{2r_0+2} & t^{[i+2m-1]}_{2r_1+1} & t^{[i+2m-1]}_{2r_1+2} & \cdots & t^{[i+2m-1]}_{2r_{m-1}+1} & t^{[i+2m-1]}_{2r_{m-1}+2} \\ t^{[i+2m]}_{2r_0+1} & t^{[i+2m]}_{2r_0+2} & t^{[i+2m]}_{2r_1+1} & t^{[i+2m]}_{2r_1+2} & \cdots & t^{[i+2m]}_{2r_{m-1}+1} & t^{[i+2m]}_{2r_{m-1}+2} \end{pmatrix} \cdot$$

$$\cdot s^{(r_0)} s^{(r_1)} \cdots s^{(r_{m-1})} =$$

$$= 2^m \cdot \det \begin{pmatrix} t^{[i+1]}_1 & \cdots & t^{[i+1]}_{2m} \\ \vdots & \ddots & \vdots \\ t^{[i+2m]}_1 & \cdots & t^{[i+2m]}_{2m} \end{pmatrix} \cdot ss' \cdots s^{(m-1)} =$$

$$= 2^m \cdot (-1)^{i(2m-i)} \cdot \det \begin{pmatrix} t^0_1 & \cdots & \cdots & t^0_{2m} \\ \vdots & & & \vdots \\ t^{i-1}_1 & \cdots & \cdots & t^{i-1}_{2m} \\ t^{i+1}_1 & \cdots & \cdots & t^{i+1}_{2m} \\ \vdots & & & \vdots \\ t^{2m}_1 & \cdots & \cdots & t^{2m}_{2m} \end{pmatrix} \cdot ss' \cdots s^{(m-1)} =$$

$$= 2^m \cdot (-1)^i \cdot \det \begin{pmatrix} t^0_1 & \cdots & \cdots & t^0_{2m} \\ \vdots & & & \vdots \\ t^{i-1}_1 & \cdots & \cdots & t^{i-1}_{2m} \\ t^{i+1}_1 & \cdots & \cdots & t^{i+1}_{2m} \\ \vdots & & & \vdots \\ t^{2m}_1 & \cdots & \cdots & t^{2m}_{2m} \end{pmatrix} \cdot ss' \cdots s^{(m-1)} =$$

$$= 2^m \cdot \tilde{t}^i_0 \cdot ss' \cdots s^{(m-1)} =$$

$$= 2^m \cdot t^i_0 \cdot ss' \cdots s^{(m-1)},$$

where the first and last equality were obtained from $(*)$ and $(\star)$, respectively. □

Corollary 1. *Let us denote*

$$\vec{\mathrm{ax}}(\phi) = 2^m \begin{pmatrix} t^0_0 \\ \vdots \\ t^{2m}_0 \end{pmatrix} ss' \cdots s^{(m-1)}.$$

Then $\vec{\mathrm{ax}}(\phi) \neq \vec{0}$ *implies that the set of fixed points of* ϕ *in* $\mathbb{R}^{2m+1}$ *is the line containing the vector* $\vec{\mathrm{ax}}(\phi)$.

Proof. If $\vec{\mathrm{ax}}(\phi) \neq \vec{0}$ then $ss' \cdots s^{(m-1)} \neq 0$. So the set of fixed points of

$$\phi_0 = \begin{pmatrix} 1 & & & & & & & \mathbf{0} \\ & c & -s & & & & & \\ & s & c & & & & & \\ & & & c' & -s' & & & \\ & & & s' & c' & & & \\ & & & & & \ddots & & \\ & & & & & & c^{(m-1)} & -s^{(m-1)} \\ \mathbf{0} & & & & & & s^{(m-1)} & c^{(m-1)} \end{pmatrix}$$

is the 1-dimensional line containing the vector

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Hence the set of fixed points of $\phi = T\phi_0 T^{-1}$ is the line containing the vector

$$T\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} t_0^0 \\ \vdots \\ t_0^{2m} \end{pmatrix}. \quad \square$$

3. SOME LEMMAS

From now on, for any integers z and z', the relation $z \equiv z'$ denotes congruence mod p, where p is the prime chosen in Section 1. Let b be the integer defined in Section 1. For vectors and matrices with integral entries, the relation $\equiv$ means that all respective entries are congruent mod p. Then we can show the following:

Lemma 1. *Let w be a non-empty reduced word in α and β. Then there exist a positive integer M and integers P, Q, R and S such that:*

if w is of the form $\alpha^{\varepsilon'} \cdots \alpha^{\varepsilon}$ then

$$(1+b^2)^{\sharp w} w \equiv \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & P & -\varepsilon Pb & R & -\varepsilon Rb \\ 0 & \varepsilon' Pb & -\varepsilon'\varepsilon Pb^2 & \varepsilon' Rb & -\varepsilon'\varepsilon Rb^2 \\ 0 & Q & -\varepsilon Qb & S & -\varepsilon Sb \\ 0 & \varepsilon' Qb & -\varepsilon'\varepsilon Qb^2 & \varepsilon' Sb & -\varepsilon'\varepsilon Sb^2 \end{pmatrix},$$

$$PS - QR \equiv 4^{M-1},$$

if w is of the form $\alpha^{\varepsilon'} \cdots \beta^{\delta}$ then

$$\begin{aligned}(1+b^2)^{\sharp w}w &\equiv \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ P & -\delta Pb & R & -\delta Rb & 0 \\ \varepsilon' Pb & -\varepsilon'\delta Pb^2 & \varepsilon' Rb & -\varepsilon'\delta Rb^2 & 0 \\ Q & -\delta Qb & S & -\delta Sb & 0 \\ \varepsilon' Qb & -\varepsilon'\delta Qb^2 & \varepsilon' Sb & -\varepsilon'\delta Sb^2 & 0 \end{pmatrix}, \\ PS - QR &\equiv -4^M,\end{aligned}$$

if w is of the form $\beta^{\delta'}\cdots\alpha^{\varepsilon}$ then

$$\begin{aligned}(1+b^2)^{\sharp w}w &\equiv \begin{pmatrix} 0 & P & -\varepsilon Pb & R & -\varepsilon Rb \\ 0 & \delta' Pb & -\delta'\varepsilon Pb^2 & \delta' Rb & -\delta'\varepsilon Rb^2 \\ 0 & Q & -\varepsilon Qb & S & -\varepsilon Sb \\ 0 & \delta' Qb & -\delta'\varepsilon Qb^2 & \delta' Sb & -\delta'\varepsilon Sb^2 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \\ PS - QR &\equiv -4^M,\end{aligned}$$

if w is of the form $\beta^{\delta'}\cdots\beta^{\delta}$ then

$$\begin{aligned}(1+b^2)^{\sharp w}w &\equiv \begin{pmatrix} P & -\delta Pb & R & -\delta Rb & 0 \\ \delta' Pb & -\delta'\delta Pb^2 & \delta' Rb & -\delta'\delta Rb^2 & 0 \\ Q & -\delta Qb & S & -\delta Sb & 0 \\ \delta' Qb & -\delta'\delta Qb^2 & \delta' Sb & -\delta'\delta Sb^2 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \\ PS - QR &\equiv 4^{M-1},\end{aligned}$$

where ε', δ', ε and δ are either -1 or 1 and $\sharp w$ is the length *of w.*

Proof. We can express the conclusion of the lemma in the following way:

if w is of the form $\alpha^{\varepsilon'}\cdots\alpha^{\varepsilon}$ then there exist P, Q, R, S and M as above such that:

$$\begin{aligned}(1+b^2)^{\sharp w}w &\equiv P\vec{u}^{1}_{\varepsilon'}\cdot{}^t\vec{u}^{1}_{-\varepsilon} + Q\vec{u}^{3}_{\varepsilon'}\cdot{}^t\vec{u}^{1}_{-\varepsilon} + R\vec{u}^{1}_{\varepsilon'}\cdot{}^t\vec{u}^{3}_{-\varepsilon} + S\vec{u}^{3}_{\varepsilon'}\cdot{}^t\vec{u}^{3}_{-\varepsilon}, \\ PS - QR &\equiv 4^{M-1},\end{aligned}$$

if w is of the form $\alpha^{\varepsilon'}\cdots\beta^{\delta}$ then there exist P, Q, R, S and M such that:

$$\begin{aligned}(1+b^2)^{\sharp w}w &\equiv P\vec{u}^{1}_{\varepsilon'}\cdot{}^t\vec{u}^{0}_{-\delta} + Q\vec{u}^{3}_{\varepsilon'}\cdot{}^t\vec{u}^{0}_{-\delta} + R\vec{u}^{1}_{\varepsilon'}\cdot{}^t\vec{u}^{2}_{-\delta} + S\vec{u}^{3}_{\varepsilon'}\cdot{}^t\vec{u}^{2}_{-\delta}, \\ PS - QR &\equiv -4^M,\end{aligned}$$

if w is of the form $\beta^{\delta'}\cdots\alpha^{\varepsilon}$ then there exist P, Q, R, S and M such that:

$$\begin{aligned}(1+b^2)^{\sharp w}w &\equiv P\vec{u}^{0}_{\delta'}\cdot{}^t\vec{u}^{1}_{-\varepsilon} + Q\vec{u}^{2}_{\delta'}\cdot{}^t\vec{u}^{1}_{-\varepsilon} + R\vec{u}^{0}_{\delta'}\cdot{}^t\vec{u}^{3}_{-\varepsilon} + S\vec{u}^{2}_{\delta'}\cdot{}^t\vec{u}^{3}_{-\varepsilon}, \\ PS - QR &\equiv -4^M,\end{aligned}$$

if w is of the form $\beta^{\delta'}\cdots\beta^{\delta}$ then there exist P, Q, R, S and M such that:

$$(1+b^2)^{\sharp w} w \equiv P\vec{u}^0_{\delta'}\cdot{}^t\vec{u}^0_{-\delta} + Q\vec{u}^2_{\delta'}\cdot{}^t\vec{u}^0_{-\delta} + R\vec{u}^0_{\delta'}\cdot{}^t\vec{u}^2_{-\delta} + S\vec{u}^2_{\delta'}\cdot{}^t\vec{u}^2_{-\delta},$$

$$PS - QR \equiv 4^{M-1},$$

where

$$\vec{u}^0_\varepsilon = \begin{pmatrix} 1 \\ \varepsilon b \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad \vec{u}^1_\varepsilon = \begin{pmatrix} 0 \\ 1 \\ \varepsilon b \\ 0 \\ 0 \end{pmatrix}, \quad \vec{u}^2_\varepsilon = \begin{pmatrix} 0 \\ 0 \\ 1 \\ \varepsilon b \\ 0 \end{pmatrix} \text{ and } \vec{u}^3_\varepsilon = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ \varepsilon b \end{pmatrix}.$$

Now we will consider four stages of complexity of w: w is α^{-1}, β^{-1}, α or β; w is a power of α or of β; w is a product of a power of α and a power of β; and w is an arbitrary non-trivial reduced word. We will use the following equations which are easy to check

$${}^t\vec{u}^{h'}_{-\varepsilon'}\cdot\vec{u}^h_\varepsilon = \begin{cases} \varepsilon b & \text{if } h-h'=-1, \\ 1-\varepsilon'\varepsilon b^2 & \text{if } h-h'=0, \\ -\varepsilon' b & \text{if } h-h'=1, \\ 0 & \text{if } h-h'=-3,-2,2 \text{ or } 3. \end{cases}$$

First, if $w=\alpha^\varepsilon$, we have

$$(1+b^2)\alpha^\varepsilon = \begin{pmatrix} 1+b^2 & 0 & 0 & 0 & 0 \\ 0 & 1-b^2 & -2\varepsilon b & 0 & 0 \\ 0 & 2\varepsilon b & 1-b^2 & 0 & 0 \\ 0 & 0 & 0 & 1-b^2 & -2\varepsilon b \\ 0 & 0 & 0 & 2\varepsilon b & 1-b^2 \end{pmatrix} \equiv$$

$$\equiv \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & -2\varepsilon b & 0 & 0 \\ 0 & 2\varepsilon b & -2b^2 & 0 & 0 \\ 0 & 0 & 0 & 2 & -2\varepsilon b \\ 0 & 0 & 0 & 2\varepsilon b & -2b^2 \end{pmatrix} = 2(\vec{u}^1_\varepsilon\cdot{}^t\vec{u}^1_{-\varepsilon} + \vec{u}^3_\varepsilon\cdot{}^t\vec{u}^3_{-\varepsilon}).$$

So we can choose $P=S=2$, $Q=R=0$, $M=2$ and we obtain

$$PS-QR = 4 = 4^{M-1},$$

as required. Similarly, if $w=\beta^\delta$, we have

$$(1+b^2)\beta^\delta \equiv 2(\vec{u}^0_\delta\cdot{}^t\vec{u}^0_{-\delta} + \vec{u}^2_\delta\cdot{}^t\vec{u}^2_{-\delta}).$$

So we can choose $P=S=2$, $Q=R=0$, $M=2$ and we obtain

$$PS-QR = 4 = 4^{M-1}.$$

If $w=\alpha^{\varepsilon k}$, we can show that

$$(1+b^2)^k\alpha^{\varepsilon k} \equiv 2^{2k-1}(\vec{u}^1_\varepsilon\cdot{}^t\vec{u}^1_{-\varepsilon} + \vec{u}^3_\varepsilon\cdot{}^t\vec{u}^3_{-\varepsilon}).$$

Indeed, by the induction

$$\begin{aligned}(1+b^2)^k\alpha^{\varepsilon k} &= (1+b^2)^{k-1}\alpha^{\varepsilon(k-1)}\cdot(1+b^2)\alpha^{\varepsilon} \equiv\\ &\equiv 2^{2k-3}(\vec{u}^1_{\varepsilon}\cdot{}^t\vec{u}^1_{-\varepsilon}+\vec{u}^3_{\varepsilon}\cdot{}^t\vec{u}^3_{-\varepsilon})\cdot 2(\vec{u}^1_{\varepsilon}\cdot{}^t\vec{u}^1_{-\varepsilon}+\vec{u}^3_{\varepsilon}\cdot{}^t\vec{u}^3_{-\varepsilon}) =\\ &= 2^{2k-2}((1-b^2)\vec{u}^1_{\varepsilon}\cdot{}^t\vec{u}^1_{-\varepsilon}+0+0+(1-b^2)\vec{u}^3_{\varepsilon}\cdot{}^t\vec{u}^3_{-\varepsilon}) \equiv\\ &\equiv 2^{2k-1}(\vec{u}^1_{\varepsilon}\cdot{}^t\vec{u}^1_{-\varepsilon}+\vec{u}^3_{\varepsilon}\cdot{}^t\vec{u}^3_{-\varepsilon}).\end{aligned}$$

So we can choose $P = S = 2^{2k-1}$, $Q = R = 0$, $M = 2k$ and we obtain

$$PS - QR = 4^{2k-1} = 4^{M-1},$$

as required. Similarly, if $w = \beta^{\delta l}$, we have

$$(1+b^2)^l\beta^{\delta l} \equiv 2^{2l-1}(\vec{u}^0_{\delta}\cdot{}^t\vec{u}^0_{-\delta}+\vec{u}^2_{\delta}\cdot{}^t\vec{u}^2_{-\delta}).$$

So we can choose $P = S = 2^{2l-1}$, $Q = R = 0$, $M = 2l$ and we obtain

$$PS - QR = 4^{2l-1} = 4^{M-1}.$$

If $w = \alpha^{\varepsilon k}\beta^{\delta l}$, we have

$$\begin{aligned}(1+b^2)^{k+l}\alpha^{\varepsilon k}\beta^{\delta l} &= (1+b^2)^k\alpha^{\varepsilon k}\cdot(1+b^2)^l\beta^{\delta l} \equiv\\ &\equiv 2^{2k-1}(\vec{u}^1_{\varepsilon}\cdot{}^t\vec{u}^1_{-\varepsilon}+\vec{u}^3_{\varepsilon}\cdot{}^t\vec{u}^3_{-\varepsilon})\cdot 2^{2l-1}(\vec{u}^0_{\delta}\cdot{}^t\vec{u}^0_{-\delta}+\vec{u}^2_{\delta}\cdot{}^t\vec{u}^2_{-\delta}) =\\ &= 2^{2k+2l-2}(\delta b\vec{u}^1_{\varepsilon}\cdot{}^t\vec{u}^0_{-\delta}+0-\varepsilon b\vec{u}^1_{\varepsilon}\cdot{}^t\vec{u}^2_{-\delta}+\delta b\vec{u}^3_{\varepsilon}\cdot{}^t\vec{u}^2_{-\delta}) =\\ &= 2^{2k+2l-2}b(\delta\vec{u}^1_{\varepsilon}\cdot{}^t\vec{u}^0_{-\delta}-\varepsilon\vec{u}^1_{\varepsilon}\cdot{}^t\vec{u}^2_{-\delta}+\delta\vec{u}^3_{\varepsilon}\cdot{}^t\vec{u}^2_{-\delta}).\end{aligned}$$

So we can choose $P = S = 2^{2k+2l-2}\delta b$, $Q = 0$, $R = -2^{2k+2l-2}\varepsilon b$, $M = 2k + 2l - 2$ and we obtain

$$PS - QR = 4^{2k+2l-2}b^2 \equiv 4^{2k+2l-2}\cdot(-1) \equiv -4^M.$$

Finally, if $w = \alpha^{\varepsilon'}\cdots\beta^{\delta}$, we will show by induction that there are such P, Q, R and S that

$$(1+b^2)^{\sharp w}w \equiv P\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^0_{-\delta}+Q\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^0_{-\delta}+R\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^2_{-\delta}+S\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^2_{-\delta},$$

and there is M such that

$$PS - QR \equiv -4^M.$$

Let $w = \bar{w}\alpha^{\varepsilon k}\beta^{\delta l}$, where $\bar{w} = \alpha^{\varepsilon'}\cdots\beta^{\delta'}$ has shorter length than w. Then, by inductive assumption, we have

$$\begin{aligned}
&(1+b^2)^{\sharp w}w = \\
&= (1+b^2)^{\sharp\bar{w}}\bar{w}\cdot(1+b^2)^{k+l}\alpha^{\varepsilon k}\beta^{\delta l} \equiv \\
&\equiv (\bar{P}\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^0_{-\delta'} + \bar{Q}\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^0_{-\delta'} + \bar{R}\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^2_{-\delta'} + \bar{S}\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^2_{-\delta'})\cdot \\
&\quad\cdot 2^{2k+2l-2}b(\delta\vec{u}^1_{\varepsilon}\cdot{}^t\vec{u}^0_{-\delta} - \varepsilon\vec{u}^1_{\varepsilon}\cdot{}^t\vec{u}^2_{-\delta} + \delta\vec{u}^3_{\varepsilon}\cdot{}^t\vec{u}^2_{-\delta}) = \\
&= 2^{2k+2l-2}b(-\delta'\delta\bar{P}b\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^0_{-\delta} - \delta'\delta\bar{Q}b\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^0_{-\delta} + \varepsilon\delta\bar{R}b\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^0_{-\delta} + \varepsilon\delta\bar{S}b\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^0_{-\delta} + \\
&\qquad\qquad + \delta'\varepsilon\bar{P}b\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^2_{-\delta} + \delta'\varepsilon\bar{Q}b\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^2_{-\delta} - \bar{R}b\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^2_{-\delta} - \bar{S}b\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^2_{-\delta} + \\
&\qquad\qquad + 0 + 0 - \delta'\delta\bar{R}b\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^2_{-\delta} - \delta'\delta\bar{S}b\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^2_{-\delta}) = \\
&= 2^{2k+2l-2}b^2(-\delta(\delta'\bar{P}-\varepsilon\bar{R})\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^0_{-\delta} - \delta(\delta'\bar{Q}-\varepsilon\bar{S})\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^0_{-\delta} + \\
&\qquad\qquad + (\varepsilon(\delta'\bar{P}-\varepsilon\bar{R}) - \delta'\delta\bar{R})\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^2_{-\delta} + (\varepsilon(\delta'\bar{Q}-\varepsilon\bar{S}) - \delta'\delta\bar{S})\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^2_{-\delta}).
\end{aligned}$$

So we put

$$\begin{aligned}
&P = -2^{2k+2l-2}\delta b^2(\delta'\bar{P}-\varepsilon\bar{R}),\;\; R = 2^{2k+2l-2}b^2(\varepsilon(\delta'\bar{P}-\varepsilon\bar{R}) - \delta'\delta\bar{R}), \\
&Q = -2^{2k+2l-2}\delta b^2(\delta'\bar{Q}-\varepsilon\bar{S}),\;\; S = 2^{2k+2l-2}b^2(\varepsilon(\delta'\bar{Q}-\varepsilon\bar{S}) - \delta'\delta\bar{S}), \\
&M = \bar{M} + 2k + 2l - 2,
\end{aligned}$$

and then

$$PS - QR = 4^{2k+2l-2}b^4(\bar{P}\bar{S} - \bar{Q}\bar{R}) \equiv 4^{2k+2l-2}\cdot 1\cdot(-4^{\bar{M}}) = -4^{M}.$$

If $w = \alpha^{\varepsilon'}\cdots\alpha^{\varepsilon}$, let $\bar{w}$ be of the form $\alpha^{\varepsilon'}\cdots\beta^{\delta'}$ such that $w = \bar{w}\alpha^{\varepsilon k}$. Then we have

$$\begin{aligned}
&(1+b^2)^{\sharp w}w = \\
&= (1+b^2)^{\sharp\bar{w}}\bar{w}\cdot(1+b^2)^{k}\alpha^{\varepsilon k} \equiv \\
&\equiv (\bar{P}\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^0_{-\delta'} + \bar{Q}\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^0_{-\delta'} + \bar{R}\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^2_{-\delta'} + \bar{S}\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^2_{-\delta'})\cdot \\
&\quad\cdot 2^{2k-1}(\vec{u}^1_{\varepsilon}\cdot{}^t\vec{u}^1_{-\varepsilon} + \vec{u}^3_{\varepsilon}\cdot{}^t\vec{u}^3_{-\varepsilon}) = \\
&= 2^{2k-1}(-\delta'\bar{P}b\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^1_{-\varepsilon} - \delta'\bar{Q}b\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^1_{-\varepsilon} + \varepsilon\bar{R}b\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^1_{-\varepsilon} + \varepsilon\bar{S}b\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^1_{-\varepsilon} + \\
&\qquad\qquad + 0 + 0 - \delta'\bar{R}b\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^3_{-\varepsilon} - \delta'\bar{S}b\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^3_{-\varepsilon}) = \\
&= 2^{2k-1}b(-(\delta'\bar{P}-\varepsilon\bar{R})\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^1_{-\varepsilon} - (\delta'\bar{Q}-\varepsilon\bar{S})\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^1_{-\varepsilon} - \\
&\qquad\qquad - \delta'\bar{R}\vec{u}^1_{\varepsilon'}\cdot{}^t\vec{u}^3_{-\varepsilon} - \delta'\bar{S}\vec{u}^3_{\varepsilon'}\cdot{}^t\vec{u}^3_{-\varepsilon}),
\end{aligned}$$

and if we choose

$$\begin{aligned}
&P = -2^{2k-1}b(\delta'\bar{P}-\varepsilon\bar{R}),\quad R = -2^{2k-1}\delta' b\bar{R}, \\
&Q = -2^{2k-1}b(\delta'\bar{Q}-\varepsilon\bar{S}),\quad S = -2^{2k-1}\delta' b\bar{S}, \\
&M = \bar{M} + 2k,
\end{aligned}$$

then

$$PS - QR = 4^{2k-1}b^2(\bar{P}\bar{S} - \bar{Q}\bar{R}) \equiv 4^{2k-1}\cdot(-1)\cdot(-4^{\bar{M}}) = 4^{M-1}.$$

If $w = \beta^{\delta'}\cdots\beta^{\delta}$, let $\bar{w}$ be of the form $\alpha^{\varepsilon}\cdots\beta^{\delta}$ such that $w = \beta^{\delta' l}\bar{w}$. Then we have

$$\begin{aligned}(1+b^2)^{\sharp w}w &= (1+b^2)^l\beta^{\delta' l}\cdot(1+b^2)^{\sharp\bar{w}}\bar{w}\equiv\\ &\equiv 2^{2l-1}(\vec{u}^0_{\delta'}\cdot{}^t\vec{u}^0_{-\delta'}+\vec{u}^2_{\delta'}\cdot{}^t\vec{u}^2_{-\delta'})\cdot\\ &\quad\cdot(\bar{P}\vec{u}^1_{\varepsilon}\cdot{}^t\vec{u}^0_{-\delta}+\bar{Q}\vec{u}^3_{\varepsilon}\cdot{}^t\vec{u}^0_{-\delta}+\bar{R}\vec{u}^1_{\varepsilon}\cdot{}^t\vec{u}^2_{-\delta}+\bar{S}\vec{u}^3_{\varepsilon}\cdot{}^t\vec{u}^2_{-\delta})=\\ &= 2^{2l-1}(-\delta'\bar{P}b\vec{u}^0_{\delta'}\cdot{}^t\vec{u}^0_{-\delta}+\varepsilon\bar{P}b\vec{u}^2_{\delta'}\cdot{}^t\vec{u}^0_{-\delta}+\\ &\qquad\quad +0-\delta'\bar{Q}b\vec{u}^2_{\delta'}\cdot{}^t\vec{u}^0_{-\delta}-\\ &\qquad\quad -\delta'\bar{R}b\vec{u}^0_{\delta'}\cdot{}^t\vec{u}^2_{-\delta}+\varepsilon\bar{R}b\vec{u}^2_{\delta'}\cdot{}^t\vec{u}^2_{-\delta}+\\ &\qquad\quad +0-\delta'\bar{S}b\vec{u}^2_{\delta'}\cdot{}^t\vec{u}^2_{-\delta})=\\ &= 2^{2l-1}b(-\delta'\bar{P}\vec{u}^0_{\delta'}\cdot{}^t\vec{u}^0_{-\delta}+(\varepsilon\bar{P}-\delta'\bar{Q})\vec{u}^2_{\delta'}\cdot{}^t\vec{u}^0_{-\delta}-\\ &\qquad\quad -\delta'\bar{R}\vec{u}^0_{\delta'}\cdot{}^t\vec{u}^2_{-\delta}+(\varepsilon\bar{R}-\delta'\bar{S})\vec{u}^2_{\delta'}\cdot{}^t\vec{u}^2_{-\delta}),\end{aligned}$$

and if we choose

$$\begin{aligned}&P=-2^{2l-1}\delta' b\bar{P}, && R=-2^{2l-1}\delta' b\bar{R},\\ &Q=2^{2l-1}b(\varepsilon\bar{P}-\delta'\bar{Q}), && S=2^{2l-1}b(\varepsilon\bar{R}-\delta'\bar{S}),\\ &M=2l+\bar{M},\end{aligned}$$

then

$$PS-QR=4^{2l-1}b^2(\bar{P}\bar{S}-\bar{Q}\bar{R})\equiv 4^{2l-1}\cdot(-1)\cdot(-4^{\bar{M}})=4^{M-1}.$$

If $w=\beta^{\delta'}\cdots\alpha^{\varepsilon}$, let $\bar{w}=w^{-1}$ of the form $\alpha^{-\varepsilon}\cdots\beta^{-\delta'}$. Then we have

$$\begin{aligned}(1+b^2)^{\sharp w}w &= (1+b^2)^{\sharp w}\cdot{}^t\bar{w}\equiv\\ &\equiv {}^t(\bar{P}\vec{u}^1_{-\varepsilon}\cdot\vec{u}^0_{\delta'}+\bar{Q}\vec{u}^3_{-\varepsilon}\cdot\vec{u}^0_{\delta'}+\bar{R}\vec{u}^1_{-\varepsilon}\cdot\vec{u}^2_{\delta'}+\bar{S}\vec{u}^3_{-\varepsilon}\cdot\vec{u}^2_{\delta'})=\\ &= \bar{P}\vec{u}^0_{\delta'}\cdot{}^t\vec{u}^1_{-\varepsilon}+\bar{R}\vec{u}^2_{\delta'}\cdot{}^t\vec{u}^1_{-\varepsilon}+\bar{Q}\vec{u}^0_{\delta'}\cdot{}^t\vec{u}^3_{-\varepsilon}+\bar{S}\vec{u}^2_{\delta'}\cdot{}^t\vec{u}^3_{-\varepsilon},\end{aligned}$$

and if we choose $P=\bar{P}$, $Q=\bar{R}$, $R=\bar{Q}$, $S=\bar{S}$, $M=\bar{M}$, then

$$PS-QR=\bar{P}\bar{S}-\bar{R}\bar{Q}\equiv -4^{\bar{M}}=-4^{M}.\quad\square$$

Lemma 0 and Lemma 1 imply the following:

Lemma 2. *For arbitrary non-empty reduced word w, there exists a positive integer M such that:*

if w is of the form $\alpha^{\varepsilon'}\cdots\alpha^{\varepsilon}$ *then*

$$(1+b^2)^{2\cdot\sharp w}\vec{\mathrm{ax}}(w)\equiv -4^M\begin{pmatrix}(1+\varepsilon'\varepsilon)/2\\ 0\\ 0\\ 0\\ 0\end{pmatrix},$$

if w is of the form $\alpha^{\varepsilon'}\cdots\beta^{\delta}$ *then*

$$(1+b^2)^{2\cdot\sharp w}\vec{\mathrm{ax}}(w) \equiv -4^M \begin{pmatrix} 1 \\ -\delta b \\ \varepsilon'\delta \\ -\varepsilon' b \\ 1 \end{pmatrix},$$

if w is of the form $\beta^{\delta'}\cdots\alpha^{\varepsilon}$ *then*

$$(1+b^2)^{2\cdot\sharp w}\vec{\mathrm{ax}}(w) \equiv -4^M \begin{pmatrix} 1 \\ \delta' b \\ \delta'\varepsilon \\ \varepsilon b \\ 1 \end{pmatrix},$$

if w is of the form $\beta^{\delta'}\cdots\beta^{\delta}$ *then*

$$(1+b^2)^{2\cdot\sharp w}\vec{\mathrm{ax}}(w) \equiv -4^M \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ (1+\delta'\delta)/2 \end{pmatrix}.$$

Proof. By Lemma 0 and Corollary 1, we can calculate $\vec{\mathrm{ax}}(w)$ directly:

$$\vec{\mathrm{ax}}(w) = \begin{pmatrix} (w_1^2-w_2^1)(w_3^4-w_4^3)-(w_1^3-w_3^1)(w_2^4-w_4^2)+(w_1^4-w_4^1)(w_2^3-w_3^2) \\ (w_2^3-w_3^2)(w_4^0-w_0^4)-(w_2^4-w_4^2)(w_3^0-w_0^3)+(w_2^0-w_0^2)(w_3^4-w_4^3) \\ (w_3^4-w_4^3)(w_0^1-w_1^0)-(w_3^0-w_0^3)(w_4^1-w_1^4)+(w_3^1-w_1^3)(w_4^0-w_0^4) \\ (w_4^0-w_0^4)(w_1^2-w_2^1)-(w_4^1-w_1^4)(w_0^2-w_2^0)+(w_4^2-w_2^4)(w_0^1-w_1^0) \\ (w_0^1-w_1^0)(w_2^3-w_3^2)-(w_0^2-w_2^0)(w_1^3-w_3^1)+(w_0^3-w_3^0)(w_1^2-w_2^1) \end{pmatrix}.$$

Hence, if $w = \alpha^{\varepsilon'}\cdots\alpha^{\varepsilon}$, we have

$$(1+b^2)^{2\cdot\sharp w}\vec{\mathrm{ax}}(w) \equiv$$

$$\equiv \begin{pmatrix} (\varepsilon' Pb+\varepsilon Pb)(\varepsilon' Sb+\varepsilon Sb)-(Q-R)(-\varepsilon'\varepsilon Qb^2+\varepsilon'\varepsilon Rb^2)+(\varepsilon' Qb+\varepsilon Rb)(-\varepsilon Qb-\varepsilon' Rb) \\ (-\varepsilon Qb-\varepsilon' Rb)(0-0)-(-\varepsilon'\varepsilon Qb^2+\varepsilon'\varepsilon Rb^2)(0-0)+(0-0)(\varepsilon' Sb+\varepsilon Sb) \\ (\varepsilon' Sb+\varepsilon Sb)(0-0)-(0-0)(-\varepsilon Rb-\varepsilon' Qb)+(R-Q)(0-0) \\ (0-0)(\varepsilon' Pb+\varepsilon Pb)-(-\varepsilon Rb-\varepsilon' Qb)(0-0)+(-\varepsilon'\varepsilon Rb^2+\varepsilon'\varepsilon Qb^2)(0-0) \\ (0-0)(-\varepsilon Qb-\varepsilon' Rb)-(0-0)(Q-R)+(0-0)(\varepsilon' Pb+\varepsilon Pb) \end{pmatrix} =$$

$$= -4(PS-QR)\begin{pmatrix} -(1+\varepsilon'\varepsilon)b^2/2 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \equiv -4^M \begin{pmatrix} (1+\varepsilon'\varepsilon)/2 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Similarly, if $w = \beta^{\delta'}\cdots\beta^{\delta}$, we have

$$(1+b^2)^{2\cdot\sharp w}\vec{\mathrm{ax}}(w) \equiv -4^M \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ (1+\delta'\delta)/2 \end{pmatrix}.$$

If $w = \alpha^{\varepsilon'} \cdots \beta^{\delta}$, we have

$$(1+b^2)^{2\cdot\sharp w}\mathrm{a}\vec{\mathrm{x}}(w) \equiv$$

$$\equiv \begin{pmatrix} (-\varepsilon'\delta Pb^2 - R)(-\varepsilon'\delta Sb^2 - 0) - (-\delta Qb + \delta Rb)(\varepsilon' Sb - 0) + (-\varepsilon'\delta Qb^2 - 0)(S + \varepsilon'\delta Rb^2) \\ (S + \varepsilon'\delta Rb^2)(0 - \varepsilon' Qb) - (\varepsilon' Sb - 0)(0 - Q) + (0 - \varepsilon' Pb)(-\varepsilon'\delta Sb^2 - 0) \\ (-\varepsilon'\delta Sb^2 - 0)(P - 0) - (0 - Q)(0 + \varepsilon'\delta Qb^2) + (-\delta Rb + \delta Qb)(0 - \varepsilon' Qb) \\ (0 - \varepsilon' Qb)(-\varepsilon'\delta Pb^2 - R) - (0 + \varepsilon'\delta Qb^2)(\varepsilon' Pb - 0) + (0 - \varepsilon' Sb)(P - 0) \\ (P - 0)(S + \varepsilon'\delta Rb^2) - (\varepsilon' Pb - 0)(-\delta Qb + \delta Rb) + (Q - 0)(-\varepsilon'\delta Pb^2 - R) \end{pmatrix} =$$

$$= (PS - QR)\begin{pmatrix} b^4 \\ \delta b^3 \\ -\varepsilon'\delta b^2 \\ -\varepsilon' b \\ 1 \end{pmatrix} \equiv -4^M \begin{pmatrix} 1 \\ -\delta b \\ \varepsilon'\delta \\ -\varepsilon' b \\ 1 \end{pmatrix}.$$

If $w = \beta^{\delta'} \cdots \alpha^{\varepsilon}$, we have

$$(1+b^2)^{2\cdot\sharp w}\mathrm{a}\vec{\mathrm{x}}(w) = (1+b^2)^{2\cdot\sharp w}\mathrm{a}\vec{\mathrm{x}}({}^t w) = (1+b^2)^{2\cdot\sharp w}\mathrm{a}\vec{\mathrm{x}}(\bar{w}) \equiv$$

$$\equiv (\bar{P}\bar{S} - \bar{R}\bar{Q})\begin{pmatrix} 1 \\ -(-\delta')b \\ (-\varepsilon)(-\delta') \\ -(-\varepsilon)b \\ 1 \end{pmatrix} \equiv -4^{\bar{M}} \begin{pmatrix} 1 \\ \delta' b \\ \delta'\varepsilon \\ \varepsilon b \\ 1 \end{pmatrix},$$

where $\bar{w} = w^{-1}$ $(= \alpha^{-\varepsilon} \cdots \beta^{-\delta'})$. □

4. PROOF OF THE SECOND PART OF THEOREM 0

Corollary 1 and Lemma 2 imply immediately the following corollary.

Corollary 2. *The set of fixed points of every non-trivial word in α and β is a 1-dimensional line in $\mathbb{R}^5$, and the group F_2 generated by α and β is freely generated by α and β.*

Proof. By Lemma 2, the vector $\mathrm{a}\vec{\mathrm{x}}(w)$ is non-zero (if w is of the form $\lambda \cdots \lambda^{-1}$ we have $\mathrm{a}\vec{\mathrm{x}}(w) \neq \vec{0}$ by using $\mathrm{a}\vec{\mathrm{x}}(\lambda \bar{w} \lambda^{-1}) = \lambda(\mathrm{a}\vec{\mathrm{x}}(\bar{w}))$ inductively). Hence Corollary 2 follows from Corollary 1. Of course the second part of the conclusion about free generation follows from the first part. □

Now we are in position to prove the second part of Theorem 0 (for $n = 5$).

Theorem 2. *F_2 acts without fixed points in the set $\{\vec{v} \in \mathbb{Q}^5 : \|\vec{v}\|/\sqrt{q} \in \mathbb{Q},\ \vec{v} \neq \vec{0}\}$.*

Proof. Let $w \in F_2$, $w \neq id$. We may assume without loss of generality that w is cyclically reduced, i.e., w is not of the form $\lambda \cdots \lambda^{-1}$ (since the non-existence of fixed points of w is equivalent to the non-existence of fixed points of $\lambda w \lambda^{-1}$ in $\{\vec{v} \in \mathbb{Q}^5 : \|\vec{v}\|/\sqrt{g} \in \mathbb{Q},\ \vec{v} \neq \vec{0}\}$; see the equality in parenthesis of the proof of Corollary 2). By Corollaries 1 and 2 all the fixed points of w are of the form $a \cdot \mathrm{a}\vec{\mathrm{x}}(w)$, where $a \in \mathbb{Q}$. Thus it suffices to show that $\|a \cdot \mathrm{a}\vec{\mathrm{x}}(w)\|/\sqrt{q}$ is irrational, i.e., that $\| \vec{\mathrm{ax}}(w) \| / \sqrt{q}$ is irrational. By Section 1, q is a quadratic non-residue to p, and of course $\vec{\mathrm{ax}}(w) \in \mathbb{Q}^5$. By Lemma 2, we have

$$q \cdot (1 + b^2)^{4 \cdot \# w} \cdot \| \vec{\mathrm{ax}}(w) \|^2 \equiv q \cdot 16^M.$$

Hence $\| \vec{\mathrm{ax}}(w) \| / \sqrt{q}$ cannot be rational. □

5. PROOF OF THE FIRST PART OF THEOREM 0.

Let w and w' be non-empty reduced words in F_2. We will use the following relations: $w \sim w'$ which means that w and w' have a common fixed point in $\mathbb{Q}^5 \setminus \{\vec{0}\}$, and $w \simeq w'$ which means that w and w' commute (Thus the first part of Theorem 0 reduces to the implication $w \sim w' \Rightarrow w \simeq w'$).

Remark. Notice that both $\sim$ and $\simeq$ are equivalence relations on $F_2 \setminus \{\mathrm{id}\}$. For $\sim$ this follows from Corollary 2. For $\simeq$ this follows from the fact that in a free group F_2 two elements commute iff they belong to the same maximal cyclic subgroup; see p. 42, 6. in [7].

Proposition 0. *For non-zero integers k and l, we have*

$$w^k \sim w'^l \Leftrightarrow w \sim w' \Leftrightarrow \bar{w} w \bar{w}^{-1} \sim \bar{w} w' \bar{w}^{-1}$$

Furthermore, if $w^{-1} \not\simeq w'$, *we have*

$$w \sim w'w \Leftrightarrow w \sim w' \Leftrightarrow w \sim ww'.$$

And the same facts hold for the relation $\simeq$.

Proof. Notice that $w^k \sim w'^l \Leftrightarrow w \sim w'$ follows from $w^k \sim w$ (by Corollary 2). Likewise for the relation $\simeq$ (since $\{\hat{w} : \hat{w} \simeq w\}$ is a maximal cyclic subgroup of F_2). Now Proposition 0 is visible. □

Proposition 1. *We have the following implication:*

$$w \simeq w' \Rightarrow w \sim w'.$$

Proof. Let $\bar{w}$ be a generator of the maximal cyclic subgroup of F_2 containing w and w' (see Remark above). Since $n = 5$, $\bar{w}$ has a fixed point in $\mathbb{R}^5 \setminus \{\vec{0}\}$ and hence in $\mathbb{Q}^5 \setminus \{\vec{0}\}$. Thus w and w' have the same fixed points and $w \sim w'$ follows. □

The purpose of this section is to prove the converse of the implication of Proposition 1. In the following three lemmas, the relations $\not\sim$ and $\not\simeq$ mean the negation of $\sim$ and $\simeq$ respectively, and we write $w \subseteq w'$ if w is an initial segment of w', i.e., we can represent w' in the form $w\bar{w}$ without cancellation.

It is easy to see that each non-empty reduced word $w \in F_2$ can be inverted, cyclically permuted, and reduced such that it will be of one of the following six types

$$\begin{array}{lll} \alpha\cdots\alpha, & \alpha^{-1}\cdots\beta^{-1}, & \alpha^{-1}\cdots\beta, \\ \beta\cdots\beta, & \alpha\cdots\beta^{-1}, & \alpha\cdots\beta. \end{array}$$

Lemma 3. *If w and w' are reduced words of distinct types of the above kind, then $w \not\sim w'$, i.e., w and w' have no common fixed points in $\mathbb{Q}^5 \setminus \{\vec{0}\}$ (nor in $\mathbb{R}^5 \setminus \{\vec{0}\}$).*

Proof. All fifteen cases follow easily from Lemma 2. □

Lemma 4. *If w and w' are non-empty reduced words of the same type, then $w \sim w'$ implies $w \simeq w'$.*

Proof. Let κ be the first letter of w and w', and λ the last letter. Then $\kappa^{-1} \neq \lambda$. If $w \sim w'$ then $w \subseteq w'$ or $w' \subseteq w$. To prove it, assume not, i.e., assume that we can represent $w = \bar{w}\hat{w}$ and $w' = \bar{w}\hat{w}'$ without cancellation by non-empty reduced words $\bar{w} = \kappa\cdots\sigma$, $\hat{w} = \tau\cdots\lambda$ and $\hat{w}' = \tau'\cdots\lambda$ with $\sigma^{-1} \neq \tau \neq \tau' \neq \sigma^{-1}$. Then, by Lemma 3, two words $\bar{w}^{-1}w\bar{w} = \hat{w}\bar{w} = \tau\cdots\lambda\kappa\cdots\sigma$ and $\bar{w}^{-1}w'\bar{w} = \hat{w}'\bar{w} = \tau'\cdots\lambda\kappa\cdots\sigma$ are not $\sim$-equivalent. This is a contradiction. So we can assume $w \subseteq w'$ without loss of generality. If $w \neq w'$, since w is $\sim$-equivalent to the non-empty reduced word $\tilde{w} = w^{-1}w'$, by Lemma 3, $\tilde{w}$ has the form $\kappa\cdots\lambda$. Then by Proposition 0 it is enough to show that $w \simeq \tilde{w}$ where $\tilde{w}$ is shorter than w'. Hence, arguing by induction, we can assume $w = w'$. Then $w \simeq w'$ is obvious. □

Lemma 5. *Let w be a non-empty reduced word of the form $\alpha^{\varepsilon}\cdots\beta^{\delta}$ and w' a non-empty reduced word of the form $\alpha^{\varepsilon}\cdots\alpha^{-\varepsilon}$ or of the form $\beta^{-\delta}\cdots\beta^{\delta}$. Then $w \not\sim w'$.*

Proof. For $w' = \alpha^{\varepsilon}\cdots\alpha^{-\varepsilon}$, if $w\alpha^{\varepsilon} \subseteq w'$, since the non-empty reduced word $\tilde{w} = w^{-1}w'$ is of the form $\alpha^{\varepsilon}\cdots\alpha^{-\varepsilon}$ which has shorter length than w', we can consider this lemma for w and $\tilde{w}$. So we can assume $w\alpha^{\varepsilon} \not\subseteq w'$. If $w \subseteq w'$, i.e., if $w\alpha^{-\varepsilon} \subseteq w'$ or $w\beta^{\delta} \subseteq w'$, since $(w^{-1}w')^{-1}$ is of the form $\alpha^{\varepsilon}\cdots\alpha^{\varepsilon}$ or $\alpha^{\varepsilon}\cdots\beta^{-\delta}$, by Lemma 3, we have $w \not\sim (w^{-1}w')^{-1}$. If $w \supseteq w'$ (so neither $w \subseteq w'^{-1}$ nor $w \supseteq w'^{-1}$), since $w \not\simeq w'w$ and $w'w$ is of the form $\alpha^{\varepsilon}\cdots\beta^{\delta}$, by Lemma 4, we have $w \not\sim w'w$. Otherwise, i.e., if neither $w \subseteq w'$ nor $w \supseteq w'$, since $w \not\simeq w'^{-1}w$ and $w'^{-1}w$ is of the form $\alpha^{\varepsilon}\cdots\beta^{\delta}$, by Lemma 4, we have $w \not\sim w'^{-1}w$. The proof for $w' = \beta^{-\delta}\cdots\beta^{\delta}$ is similar. □

Finally we are ready to prove the first part of Theorem 0.

Theorem 3. *The action of the group F_2 on $\mathbb{Q}^5 \setminus \{\vec{0}\}$ is locally commutative, in other words, for any non-empty reduced words w and w' we have:*

$$w \sim w' \Rightarrow w \simeq w'.$$

Proof. By the former equivalences of Proposition 0, it is enough to show this for $w = \alpha, \beta, \alpha^{-1}\cdots\beta^{-1}, \alpha^{-1}\cdots\beta, \alpha\cdots\beta^{-1}, \alpha\cdots\beta$. For $w = \alpha$, by the former of Proposition 0 and Lemma 3, we can assume $w' = \alpha^{-1}\cdots\alpha, \alpha\cdots\alpha^{-1}, \alpha\cdots\alpha, \beta^{-1}\cdots\beta$ or $\beta\cdots\beta^{-1}$. If $w' = \beta^{-1}\cdots\beta$ or $w' = \beta\cdots\beta^{-1}$, by Lemma 3, we have

$w \not\sim ww'$. If $w' = \alpha^{-\varepsilon} \cdots \beta^{\delta}\alpha^{\varepsilon k}$ for ε, δ in $\{-1, 1\}$ and a positive integer k, by Lemma 3, we have $w \not\sim w'w^{-\varepsilon k}$. Otherwise, i.e., if $w' = \alpha \cdots \alpha$, by Lemma 4, $w \sim w'$ implies $w \simeq w'$. For $w = \beta$, the proof is similar. For $w = \alpha^{\varepsilon} \cdots \beta^{\delta}$, by the former of Proposition 0 and Lemmas 3 and 5, we can assume $w' = \alpha^{-\varepsilon} \cdots \alpha^{\varepsilon}$, $\beta^{\delta} \cdots \beta^{-\delta}$ or $\alpha^{\varepsilon} \cdots \beta^{\delta}$. If $w' = \alpha^{-\varepsilon} \cdots \alpha^{\varepsilon}$, by Lemma 3, we have $w \not\sim w'w$. If $w' = \beta^{\delta} \cdots \beta^{-\delta}$, by Lemma 3, we have $w \not\sim ww'$. Otherwise, i.e., if $w' = \alpha^{\varepsilon} \cdots \beta^{\delta}$, by Lemma 4, $w \sim w'$ implies $w \simeq w'$. □

REFERENCES

0. Borel, A. – On free subgroups of semi-simple groups. Enseign. Math. **29**, 151–164 (1983).
1. Dekker, T.J. – Decompositions of sets and spaces I. Indag. Mathem. **18**, 581–589 (1956).
2. Dekker, T.J. – On free groups of motions without fixed points. Indag. Mathem. **20**, 348–353 (1958).
3. Deligne, P. and D. Sullivan – Division algebras and the Hausdorff-Banach-Tarski Paradox. Enseign. Math. **29**, 145–150 (1983).
4. Dougherty, R. and M. Foreman – Banach-Tarski decompositions using sets with the property of Baire. J. Amer. Math. Sci. **7**, 75–124 (1994).
5. Hecke, E. – Vorlesungen über die Theorie der algebraischen Zahlen. Akademische Verlagsgesellschaft. Leipzig (1923) .
6. Laczkovich, M. – Paradoxical sets under $SL_2[\mathbb{R}]$. Annales Univ. Sci. Budapest **42**, 141-145 (1999).
7. Magnus, W., A. Karass, and D. Solitar – Combinatorial Group Theory. Interscience. New York (1966).
8. Mordell, L.J. – Diophantine Equations. Academic Press. New York-London (1969).
9. Mycielski, J. – About sets invariant with respect to denumerable changes. Fund. Math. **45**, 296–305 (1958).
10. Mycielski, J. – Non-amenable groups with amenable actions and paradoxical decompositions of the plane. Coll. Math. **75**, 149-157 (1998).
11. Mycielski, J. and S. Świerczkowski – On free groups of motions and decompositions of the Euclidean space. Fund. Math. **45**, 283–291 (1958).
12. Robinson, R.M. – On the decomposition of spheres. Fund. Math. **34**, 246–260 (1947).
13. Satake, I. – Linear algebra. Trans. from Japanese by S. Koh, T. Akiba, and S. Ihara. Marcel Dekker. New York (1975).
14. Satô, K. – A free group acting without fixed points on the rational unit sphere. Fund. Math. **148**, 63–69 (1995).
15. Satô, K. – A free group of rotations with rational entries on the 3-dimensional unit sphere. Nihonkai Math. J. **8**, 91–94 (1997).
16. Satô, K. – Free groups acting without fixed points on rational spheres. Acta Arith. **85**, 135–140 (1998).
17. Satô, K. – A free group acting on $\mathbb{Z}^2$ without fixed points. Enseign. Math. **45**, 189–194 (1999).
18. Wagon, S. – The Banach-Tarski Paradox. Cambridge Univ. Press. Cambridge-New York (1985).
19. Zhang, F. – Matrix Theory. Springer-Verlag. Berlin-Heidelberg (1999).

(Received July 2000)