A NON COMMUTATIVITY STATEMENT FOR ALGEBRAIC QUATERNIONS

FLAVIO D'ALESSANDRO AND ALESSANDRO D'ANDREA

CONTENTS

1. INTRODUCTION

In this paper we provide a constructive version of Tits alternative for a broad class of quaternions with algebraic coefficients. Our result is a generalization of that contained in the paper [1], concerning groups of rational quaternions. Indeed, the tools developed in [1] can be extended to arbitrary number fields by translating them in the corresponding Dedekind domain, as the techniques involved are of a typical "factorization and divisibility" flavour.

Let K be a finite extension of $\mathbb{Q}$. We will say that a quaternion $a+bi+cj+dk$ is *K-rational* if its coefficients a, b, c, d all lie in K. The main result in the paper is then the following.

Theorem 1. *Let G be a group of K-rational quaternions containing at least one element that is* 2-good*. Then either G is solvable or it contains a free non commutative group.*

The 2-goodness assumption will be explained later, and is a technical condition which guarantees, for instance, that coefficients are not algebraic integers. The free non commutative group is explicitly located by choosing appropriate conjugate quaternions p and q. Non triviality of a certain class of words in p and q is insured by measuring *"divisibility"* of their coefficients with respect to an opportune valuation. One can eventually locate a subgroup of $\langle p, q\rangle$ such that all of its elements satisfy the above non triviality assumptions, thus ensuring the group to be a free group.

The explicit construction of free groups by means of quaternions has been thoroughly investigated by several authors. Note that the group $SU(2)$ of unit quaternions is the universal covering of the group $SO(3)$ of rotations of 3-dimensional Euclidean space, so that algebraic properties of quaternions translate in analogue statements for rotations. By a result of De Groot [4], two rotations with orthogonal axes and rotation angle θ generate a free group if $\cos\theta$ is transcendental (see also [3]). Later, Swierczkowski in [7] considered the rational case proving that two rotations with orthogonal axes and rotation angle θ such that θ is rational generate a free group if and only if $\cos\theta \neq 0, \pm 1, \pm 1/2$. More recently, in [5] Gonçalves, Mandel, and Shirvani have considered the case when the cosine of the angle of the two rotations is an algebraic number. In particular, they proved that two rotations with orthogonal axes and rotation angle θ generate a free group when the cosine of θ is algebraic but not an algebraic integer. In this paper, we extend the techniques developed in [7] and [1], thus correcting some details in the proofs of the latter

The first author was partially supported by PRIN "Linguaggi formali e automi: teoria e applicazioni" fundings from Ministero dell'Istruzione, Università e Ricerca Scientifica (MIUR). The second author was partially supported by PRIN "Spazi di Moduli e Teoria di Lie" fundings from MIUR.

paper, and we give an explicit description of free groups generated by pairs of conjugate rotations of arbitrarily oriented axes, whose coefficients belong to a broad class of algebraic numbers.

The plan of the paper is the following: in Section 2 we collect definitions and recall results from [1] that will be of use to us. Furthermore we introduce the concept of 2-goodness for quaternions, and show that any nonsolvable group of algebraic quaternions in which at least one element is 2-good needs to contain a pair p, q of noncommuting conjugate quaternions satisfying some very special properties. In Section 3 we introduce a subset Γ of words in p and q, and show how the above properties for p and q lead to a nontriviality statement for elements of Γ. We locate then a subgroup of $\langle p, q\rangle$ completely contained in the subset Γ. This proves the existence of an explicitly described noncommutative free subgroup of $\langle p, q\rangle$.

In Section 4 we finally give the (lengthy) proof of a technical statement used in Section 3, by exploiting the fact that the evaluation homomorphism maps elements of Γ to algebraic quaternions for which at least one of the coefficient has negative valuation, that are therefore different from the identity.

General introductions to algebraic properties of quaternions can be found in [2] and [6].

2. PRELIMINARIES

In this section, following [1], [2], and [6], we recall some definitions and elementary results. By K we will denote a finite xtension of $\mathbb{Q}$ contained[1] in $\mathbb{R}$. Then D is the ring of algebraic integers of K, and an element $\alpha \in \mathbb{R}$ is said to be K-rational (resp. K-integral) iff $\alpha \in K$ (resp. $\alpha \in D$).

Lemma 1. *Any pair p, q of K-rational conjugate non commuting quaternions can be simultaneously conjugated to the form*

$$zpz^{-1} = \alpha + \beta i, \qquad zqz^{-1} = \alpha + \beta(ai + bj),$$

where z lies in a finite extension of K and $a^2 + b^2 = 1$.

Definition 1. *Let K be a finite extension of $\mathbb{Q}$. An element $\omega \in K$ is* 2-good *if there exists a valuation ν on K such that $\nu(\omega) < 0 = \nu(2)$. A pair (α, β) is 2-good if both α and β are 2-good.*

Remark 1. A rational number is 2-good iff it is not of the form $m/2^n$, $m, n \in \mathbb{Z}$. Similarly, it can be proved that an element of a finite extension K of $\mathbb{Q}$ is 2-good if and only if it cannot be made into an algebraic integer via multiplication by an opportune power of 2. Thus the notion of 2-goodness of an algebraic integer is independent of the particular choice of $K \supset \mathbb{Q}$.

Definition 2. *A K-rational quaternion $p = a + bi + cj + dk$ is 2-good if the pair $(a, (b^2 + c^2 + d^2)^{1/2})$ is 2-good.*

Remark 2. 2-goodness of a unit – i.e. norm 1 – quaternion $p = a + bi + cj + dk$ can be checked on its real part alone. Indeed if $\alpha^2 + \beta^2 = 1$, then 2-goodness of α is equivalent to that of β, as in this case $\nu(\alpha) < 0$ immediately implies $\nu(\alpha) = \nu(\beta)$ where ν is as in Definition 1.

Lemma 2. *No periodic quaternion is 2-good.*

Proof. A periodic quaternion is certainly a unit, i.e. it is of the form $\cos\theta + \sin\theta \cdot I$, where $\theta \in \mathbb{R}$ and I is a purely imaginary unit quaternion. Then, it is 2-good if and only if so is the pair $(\cos\theta, \sin\theta)$. However $2\cos\theta = e^{i\theta} + e^{-i\theta}$ is an algebraic integer if θ is a rational multiple of π, so $\cos\theta$ is not 2-good by Remark 1. □

Remark 3. Let I be a purely imaginary unit quaternion. If $p = \alpha + \beta I$, where $\alpha, \beta \in \mathbb{R}$, then $p^2 = (\alpha^2 - \beta^2) + 2\alpha\beta I$. If p is a 2-good unit quaternion, choose a valuation ν such that $\nu(\alpha) = \nu(\beta) = c < 0, \nu(2) = 0$. Then $\nu(2\alpha\beta) = 2c$. As p cannot be torsion, computing ν on the real part of p^{2^n} we also obtain $2^n c$.

[1] This is unnecessary, but avoids invertibility problems.

Remark 4. Let p and q be non commuting conjugate K-rational 2-good unit quaternions, K a finite extension of $\mathbb{Q}$. Up to conjugating and changing K by a finite extension, we can uniquely write

$$p = \frac{u}{s} + \frac{v}{s}i, \qquad q = \frac{u}{s} + \frac{v}{s} \cdot \left(\frac{x}{y}i + \frac{z}{y}j\right)$$

where u and v are algebraic integers, $s, y \in \mathbb{N}^*$ are minimal among naturals such that sp (resp. yx) is K-integral, and x, z are nonzero numbers such that $x^2 + z^2 = y^2$. As p and q are 2-good, then s is not a power of 2.

Notice also that $-\nu(u/s) = \nu(s) - \nu(u) \leq \nu(s)$. This fact, and the argument of Remark 3, show that up to replacing p and q by suitable common powers, we can make the value of $\nu(s)$ as large as desired, while leaving x, y, z unaffected. In particular we may assume that the following conditions hold:

$$\nu(u) = \nu(v) < \nu(s), \qquad \nu(x \pm y),\ \nu(z),\ \nu(x) < \nu(s) - \nu(u). \tag{1}$$

As we will see later, Condition (1) will be used in the proof of Lemma 3.

3. Main result

We are now ready to state the main result of the paper. Its proof depends on a few technical lemmas, the proof of which is quite involved, and will be postponed to the next section.

We will be concerned with those elements lying in the free group $\mathbb{F}(p, q)$ on the alphabet $\{p, q\}$ whose particolar shape allows us to prove interesting divisibility properties. The words that are relevant to us are reduced ones satisfying the following requirements:

- They begin with a non-trivial power of p;
- the only occurrences of powers of q in the word are with exponent ± 1;
- two occurrences of powers of q in the word are separated by powers p^k with $|k| \geq 2$.
- if $p^a q^b p^c$ occurs as a subword, and $ac > 0$ then the sign of b is the same sign of a and c.

We will denote the set of all such words by $\Gamma \subset \mathbb{F}(p, q)$. It is worthwhile noting that Γ is not a subgroup of $\mathbb{F}(p, q)$. Also every non trivial prefix of a word in Γ also lies in Γ. The following lemma will be proved in the next section.

Lemma 3. *Let p and q be noncommuting conjugate 2-good K-rational quaternions satisfying the conditions defined at the end of the previous section. Then the kernel of the evaluation homomorphism $\mathrm{ev} : \mathbb{F}(p, q) \to \langle p, q\rangle$ does not intesect Γ.*

Injectivity of the evaluation homomorphism on Γ is important because of the following fact, which was proved in [1].

Lemma 4. *All non identical elements of $\langle p^2qp^4, p^4qp^2\rangle < \mathbb{F}(p, q)$ lie in Γ.*

We are now ready to prove the main result.

Theorem 2. *Let p and q be noncommuting conjugate 2-good K-rational quaternions. Then $\langle p, q\rangle$ contains a free non commutative group.*

Proof. By the well known theorem of Nielsen and Schreier, words p^2qp^4 and p^4qp^2 generate a free subgroup of $\mathbb{F}(p, q)$ and, by Lemma 4, all of its elements lie in Γ. By Remark 4, up to replacing p and q with one of its powers, we can suppose that p and q satisfy the conditions defined at the end of the previous section. Then Lemma 3 shows that the subgroup of $\langle p, q\rangle$ generated by p^2qp^4 and p^4qp^2 is an isomorphic image of $\mathbb{F}_2 \simeq \mathbb{F}(p^2qp^4, p^4qp^2)$. □

Remark 5. The above proof is constructive as soon as we are given a valuation measuring 2-goodness of p and q. The valuation is needed in choosing the appropriate powers of p and q so that the condition on $x, z, x \pm y$ is satisfied.

We end this section by showing an interesting consequence of Theorem 2: a Tits alternative for groups of *K-rational* quaternions. For this purpose, let us recall the following fact that is standard (see [1]).

Lemma 5. *Let H be a non solvable subgroup of unit quaternions. Let $q \in H$ such that $q = \alpha + \beta I$ where I is a purely imaginary unit quaternion and α, β are nonzero real numbers. Then there exists a conjugate p of q not commuting with q.*

Corollary 1. *Let G be a subgroup of K-rational quaternions of Q^* containing a 2-good unit element. Then G is solvable or contains a non commutative free groups.*

Proof. Assume G is not solvable. Let U be the group of unit quaternions of Q^*. Then the subgroup $G \cap U$ is not solvable either: indeed the derived subgroup G' of G is a subgroup of $G \cap U$. Choose a 2-good element p of $G \cap U$ and express it (uniquely) as $p = \alpha + \beta I$, where $\alpha, \beta \in \mathbb{R}$ and I is a purely imaginary unit quaternion. Then α and β are nonzero and, by Lemma 5, there exists a conjugate q of p such that p and q do not commute. Then, by Theorem 2, the group generated by p, q contains a free group. □

4. Proof of technical lemmas

This section is devoted to the proof of Lemma 3. For this purpose it is useful to set up some notation. The groups we will be interested in are either subgroups of $\mathbb{F}(p, q)$ or their homomorphic image inside the group of quaternions.

The length of a word $w \in \mathbb{F}(p, q)$ is denoted by $|w|$. The symbol $|w|_q$ denotes the number of occurrences of q or q^{-1} in the reduced expression for w. We will write

$$w \equiv w_1 w_2 ... w_k$$

if the word w is the product of the words $w_1, w_2, ..., w_k$ and $|w| = |w_1| + |w_2| + ... + |w_k|$. This means that the product of the words w_i – that we always assume to be reduced – is a reduced expression for the word w. Moreover we will say that condition (*) holds for $w \in \Gamma$ – see beginning of Section 3 – if $w = p^a$ or

$$w \equiv p^a w' p^b \qquad \text{and} \qquad ab > 0.$$

We will now define functions M^{ab}, M^{cd} that will be needed later in order to give estimates for the discrete valuations of certain elements of interest in a Dedekind domain of algebraic integers over $\mathbb{Q}$.

For any given choice of non-negative integers $h_+ = h_1, h_- = h_{-1}$, k and C such that $k < C$ and $h_\pm < C - k$, we denote by $M^{ab}, M^{cd} : \Gamma \to \mathbb{Q}$ the maps defined as follows on elements of small length:

$$M^{ab}(p^i) = M^{cd}(p^i) = 0,$$

for all $i \in \mathbb{Z} \setminus \{0\}$.

$$\begin{aligned} M^{ab}(p^e q^f) = h_{ef}, \qquad & M^{cd}(p^e q^f) = (h_+ + h_-)/2, \\ M^{ab}(p^e q^e p^e) = h_+, \qquad & M^{cd}(p^e q^e p^e) = (h_+ + h_-)/2, \\ M^{ab}(p^e q^f p^{-e}) = h_{\min} = \min\{h_+, h_-\}, \qquad & M^{cd}(p^e q^f p^{-e}) = (h_+ + h_-)/2, \end{aligned}$$

for all choices of $e, f \in \{\pm 1\}$, and recursively defined on longer words according to the following prescriptions:

- If $w \equiv w' p^e \equiv w'' p^{2e}$, then:

$$M^{ab}(w) = M^{ab}(w'), \qquad M^{cd}(w) = \min\{M^{cd}(w'), M^{cd}(w'')\} \tag{2}$$

if (*) holds for w, and

$$M^{cd}(w) = M^{cd}(w'), \qquad M^{ab}(w) = \min\{M^{ab}(w'), M^{ab}(w'')\} \tag{3}$$

otherwise.

- If $w \equiv w'q^e, e \in \{\pm 1\}$ then

$$M^{ab}(w) = M^{ab}(\overline{w}) + h_{eh}, \qquad M^{cd}(w) = M^{ab}(w') + (h_+ + h_-)/2 \tag{4}$$

if condition (*) holds for w' and

$$M^{cd}(w) = M^{cd}(\overline{w}) + h_{eh}, \qquad M^{ab}(w) = M^{cd}(w') + (h_+ + h_-)/2 \tag{5}$$

otherwise, where $\overline{w}$ and $h \in \{\pm 1\}$ are uniquely chosen so that $w' \equiv \overline{w}p^h$.

- If $w \equiv w'q^f p^e$, with $e, f \in \{\pm 1\}$, and moreover $\overline{w}, h \in \{\pm 1\}$ are chosen so that $w' \equiv \overline{w}p^h$, then:

$$\begin{aligned} M^{ab}(w) &= M^{ab}(w') + h_+, \\ M^{cd}(w) &= \min\left\{M^{ab}(\overline{w}) + \frac{1}{2}(h_+ + h_-), M^{cd}(w') + h_+\right\}, \end{aligned} \tag{6}$$

if (*) holds for both w and w';

$$\begin{aligned} M^{cd}(w) &= M^{ab}(w') + \frac{1}{2}(h_+ + h_-), \\ M^{ab}(w) &= \min\left\{M^{ab}(\overline{w}) + h_{hf}, M^{cd}(w') + \frac{1}{2}(h_+ + h_-)\right\}, \end{aligned} \tag{7}$$

if (*) holds for w' but not for w;

$$\begin{aligned} M^{ab}(w) &= M^{cd}(w') + \frac{1}{2}(h_+ + h_-), \\ M^{cd}(w) &= \min\left\{M^{cd}(\overline{w}) + h_{hf}, M^{ab}(w') + \frac{1}{2}(h_+ + h_-)\right\}, \end{aligned} \tag{8}$$

if (*) holds for w but not for w'; and

$$\begin{aligned} M^{cd}(w) &= M^{cd}(w') + h_+, \\ M^{ab}(w) &= \min\left\{M^{cd}(\overline{w}) + \frac{1}{2}(h_+ + h_-), M^{ab}(w') + h_+\right\}, \end{aligned} \tag{9}$$

if (*) holds for neither w nor w'.

The following results give some useful properties of M^{ab}, M^{cd}.

Lemma 6. *Let $g \equiv g'p^e$, be an element in Γ ending by p^{3e}. Then*

$$M^{ab}(g) = M^{ab}(g'), \qquad M^{cd}(g) = M^{cd}(g').$$

Proof. We prove the claim in case (*) holds for g, the other case being completely analogous. Write $g \equiv g''p^{2e} \equiv g'''p^{3e}$.

Then Equation 2 applied to $w = g$ implies both $M^{ab}(g) = M^{ab}(g')$ and

$$M^{cd}(g) = \min\{M^{cd}(g'), M^{cd}(g'')\}. \tag{10}$$

Using the same equation with $w = g'$ gives

$$M^{cd}(g') = \min\{M^{cd}(g''), M^{cd}(g''')\}. \tag{11}$$

Substituting (11) into (10) one gets

$$M^{cd}(g) = \min\{M^{cd}(g''), \min\{M^{cd}(g''), M^{cd}(g''')\}\} = M^{cd}(g'),$$

whence the second part of the claim. □

Lemma 7. *Let $g \equiv g'p^e, e \in \{\pm 1\}$ be an element in Γ ending by p^{2e}. Then*

$$M^{ab}(g) = M^{ab}(g'), \qquad M^{cd}(g) = M^{cd}(g'). \tag{12}$$

Proof. The case when g ends by p^{3e} has already been treated in the previous lemma, so we can assume g ends exactly by p^{2e}. The claim holds trivially when g is a power of p. Also when $g = p^h q^f p^{2e}$, it can be directly verified using Equations 2 and 3, and the definition of M^{ab}, M^{cd} on words of length ≤ 3. In all other cases, write $g \equiv g'' p^{2e}$, and find $\widetilde{g}, \overline{g} \in \Gamma$ such that $g'' \equiv \widetilde{g} q^f$, and $\widetilde{g} \equiv \overline{g} p^h$.

Suppose that (*) holds for both g and $\widetilde{g}$. Then applying (4) to $w = g'', w' = \widetilde{g}$ yields

$$M^{cd}(g'') = M^{ab}(\widetilde{g}) + \frac{1}{2}(h_+ + h_-).$$

Moreover (6) applied to $w = g', w' = \widetilde{g}, \overline{w} = \overline{g}$ gives

$$M^{cd}(g') = \min\left\{ M^{ab}(\overline{g}) + \frac{1}{2}(h_+ + h_-), M^{cd}(\widetilde{g}) + h_+ \right\}.$$

Notice now that (2) implies $M^{ab}(\overline{g}) = M^{ab}(\widetilde{g})$, when $\widetilde{g} \neq p^{2h}$; however, the same equality holds trivially if $\widetilde{g} = p^{2h}$. Similarly,

$$M^{cd}(g) = \min\{M^{cd}(g'), M^{cd}(g'')\},$$

hence $M^{cd}(g) = M^{cd}(g')$ easily follows. The case when (*) holds for neither g nor $\widetilde{g}$ is handled in the same way, by inverting the role of ab and cd.

Let us now treat the case when (*) holds for $\widetilde{g}$ but not for g. Then using (4) gives

$$M^{ab}(g'') = M^{ab}(\overline{g}) + h_{hf},$$

whereas (7) gives

$$M^{ab}(g') = \min\left\{ M^{ab}(\overline{g}) + h_{hf}, M^{cd}(\widetilde{g}) + \frac{1}{2}(h_+ + h_-) \right\},$$

hence by (3) we conclude that $M^{ab}(g) = M^{ab}(g')$. The case when (*) holds for g but not for $\widetilde{g}$ is then done by exchanging ab with cd. □

Lemma 8. *Let $g \equiv g' p^e, e \in \{\pm 1\}$ be an element in $\Gamma \setminus \{p^e\}$. Then $M^{ab}(g) = M^{ab}(g')$ if (*) holds for g, and $M^{cd}(g) = M^{cd}(g')$ if it does not.*

Proof. We only address the case when (*) holds for g, as the proof in the other case is obtained by exchanging ab and cd. If g ends by p^{2e} then the claim follows by (2). If $g = p^h q^f p^e$ or $p^{2h} q^f p^e, e \in \{\pm 1\}$, then the claim can be checked directly using the definition of M^{ab} and M^{cd} on g and g'.

In all other cases, write $g' \equiv \overline{g} p^h q^f, h, f \in \{\pm 1\}$, for some $\overline{g} \in \Gamma$, and denote by $\widetilde{g}$ the element $\overline{g} p^h$, so that $g' = \widetilde{g} q^f$. Now, if (*) holds for $\widetilde{g}$, then (6) applied to $w = g, w' = \widetilde{g}$ gives

$$M^{ab}(g) = M^{ab}(\widetilde{g}) + h_+,$$

whereas (4) applied to $w = g', w' = \widetilde{g}$ gives

$$M^{ab}(g') = M^{ab}(\overline{g}) + h_{hf}.$$

However, as (*) holds for both g and $\widetilde{g}$, then $e = f = h$, hence

$$M^{ab}(g) - M^{ab}(g') = M^{ab}(\widetilde{g}) - M^{ab}(\overline{g}),$$

which vanishes by Lemma 7. If instead (*) does not hold for $\widetilde{g}$, we proceed as before by using (8) and (5) to obtain

$$M^{ab}(g) = M^{cd}(\widetilde{g}) + \frac{1}{2}(h_+ + h_-) = M^{ab}(g'),$$

hence the claim. □

Lemma 9. *If $g \in \Gamma$ ends with $p^e, e \in \{\pm 1\}$, then*

$$|M^{ab}(g) - M^{cd}(g)| \leq \frac{1}{2}|h_+ - h_-|.$$

Proof. We proceed by induction on the length of g. The basis of induction is proved by directly checking that the statement holds for all words in Γ of length at most three.

Let us prove the inductive step. Suppose first that $g = \overline{g}p^{2e}, e \in \{\pm 1\}$. By Lemma 7, $M^{cd}(g) = M^{cd}(\overline{g}p^e)$ and $M^{ab}(g) = M^{ab}(\overline{g}p^e)$ so that $|M^{ab}(g) - M^{cd}(g)| = |M^{ab}(\overline{g}p^e) - M^{cd}(\overline{g}p^e)|$. Since the length of $\overline{g}p^e$ is less than that of g, the claim follows by inductive assumption.

Suppose now that g ends by $p^e, e \in \{\pm 1\}$ but not by p^{2e}. Then we can write $g \equiv \overline{g}q^f p^e$. Assuming that the length of g is greater or equal than four, we know that $\overline{g}$ ends by $p^{2h}, h \in \{\pm 1\}$. Then using Lemma 7 together with the recursive definition of M^{ab} and M^{cd} on $\overline{g}q^f p^e$, one may easily show that

$$|M^{ab}(g) - M^{cd}(g)| \leq \max\{\frac{1}{2}|h_+ - h_-|,\ |M^{ab}(\overline{g}) - M^{cd}(\overline{g})|\},$$

which equals $|h_+ - h_-|/2$ by inductive assumption. □

Lemma 10. *For each $g \in \Gamma$ one has:*

$$|M^{ab}(g)|,\ |M^{cd}(g)| \leq h_{\max}|g|_q,$$

where $h_{\max} = \max\{h_+, h_-\}$.

Proof. The statement of the lemma is easily proved by induction on the length of g, using the recursive definition of M^{ab}, M^{cd}. □

We now assume to be given a choice of non commuting unit 2-good quaternions p, q that we write as

$$p = \frac{u}{s} + \frac{v}{s}i, \qquad q = \frac{u}{s} + \frac{v}{s}\left(\frac{x}{y}i + \frac{z}{y}j\right),$$

according to the discussion at the end of Section 2. Moreover, we set $h_+ = \nu(x+y)$, $h_- = \nu(x-y)$, $C = \nu(s)$, $k = \nu(u) = \nu(v)$, $k < C$. Also recall that $\nu(z) = \frac{1}{2}(h_+ + h_-)$ and $\nu(x), \nu(y) \geq \min\{h_+, h_-\}$. According to Remark 4, we may suppose that

$$k < C, \qquad h_\pm < C - k.$$

We now establish some recursive relations for the coefficients of the quaternions represented by elements of Γ. Let $g \in \mathbb{F}(p,q)$ and let $\mathrm{ev}(g)$ be the image of g under the evaluation homomorphism $\mathrm{ev} : \mathbb{F}(p,q) \to \langle p, q\rangle$. We agree to write $\mathrm{ev}(g)$ as

$$(1/s)^{|g|}\ (1/y)^{|g|_q}(a(g)\ +\ b(g)i\ +\ c(g)j\ +\ d(g)k).$$

We also adopt the following notation: if $g \in \mathbb{F}(p,q)$, then $a,\ b,\ c$ and d denote $a(g), b(g), c(g), d(g)$ respectively, so that:

$$\mathrm{ev}(g) = (1/s)^{|g|}\ (1/y)^{|g|_q}(a\ +\ bi\ +\ cj\ +\ dk).$$

We do similarly for elements $g', \tilde{g}, \bar{g}, ...$ denoting the coefficients of $\mathrm{ev}(g')$, $\mathrm{ev}(\tilde{g})$, $\mathrm{ev}(\bar{g})$, ... by $a', \tilde{a}, \bar{a}$ and so on.

The coefficients of $\mathrm{ev}(g), g \in \Gamma$ can then be recursively computed according to the following two rules.

First Composition Rule (R1). If g, g' are words on $\{p^{\pm 1}, q^{\pm 1}\}$ such that $g \equiv g'p^e, e \in \{\pm 1\}$, then

$a = ua'\ -\ evb'$
$b = ub'\ +\ eva'$
$c = uc'\ +\ evd'$
$d = ud'\ -\ evc'.$

Second Composition Rule (R2). If g, g' are words on $\{p^{\pm 1}, q^{\pm 1}\}$ such that $g \equiv g'q^e, e \in \{\pm 1\}$, then

$a = (uy)a'\ -\ e(vx)b'\ -\ e(vz)c'$
$b = (uy)b'\ +\ e(vx)a'\ -\ e(vz)d'$

$c = (uy)c' \ + \ e(vx)d' \ + \ e(vz)a'$
$d = (uy)d' \ - \ e(vx)c' \ + \ e(vz)b'.$

The following Lemma follows immediately (see [7]).

Lemma 11. *If g, g', g'' are words on $\{p^{\pm 1}, q^{\pm 1}\}$ such that $g \equiv g''p^{2e}, g' \equiv gp^e$. Then*

$$a = 2ua' \ - \ s^2a'',$$
$$b = 2ub' \ - \ s^2b'',$$
$$c = 2uc' \ - \ s^2c'',$$
$$d = 2ud' \ - \ s^2d''.$$

Proposition 1. *Let $g \in \Gamma$. If g ends by $p^e, \ e \in \{\pm 1\}$, one has*

$$\nu(a) = \nu(b) = k|g| + M^{ab}(g),$$

and

$$\nu(c), \nu(d) \geq k|g| + M^{cd}(g) + 2(C - k),$$

if $(*)$ holds for g and

$$\nu(c) = \nu(d) = k|g| + M^{cd}(g),$$

and

$$\nu(a), \nu(b) \geq k|g| + M^{ab}(g) + 2(C - k),$$

otherwise.

If instead g ends by $q^e, \ e \in \{\pm 1\}$, one has

$$\nu(a) = \nu(b) = k|g| + M^{ab}(g)$$

and

$$\nu(c) = \nu(d) = k|g| + M^{cd}(g).$$

Proof. The statement can be checked directly for words of length ≤ 4.

For all other words, we prove the claim by induction on the length of g, the proof of the inductive step following easily from the following three lemmas. □

Lemma 12. *Let $g \in \Gamma$ be a word of lenght at least three, ending by $p^{2e}, e \in \{\pm 1\}$, and assume Proposition 1 holds for all words of Γ of length $< |g|$. Then*

$$\nu(a) = \nu(b) = k|g| + M^{ab}(g)$$

and

$$\nu(c), \ \nu(d) \geq k|g| + M^{cd}(g) + 2(C - k)$$

if (*) holds for g, and

$$\nu(c) = \nu(d) = k|g| + M^{cd}(g)$$

and

$$\nu(a), \ \nu(b) \geq k|g| + M^{ab}(g) + 2(C - k)$$

otherwise.

Proof. We only address the case when (*) holds for g, as the proof in the other case is obtained by exchanging ab and cd. Let $g' = g''p^e, \ g = g''p^{2e}$. As $|g| \geq 3$, then $g'' \in \Gamma$. First we compute $\nu(a)$. By Lemma 11,

$$a = 2ua' - s^2a''.$$

One has:

$$\nu(a'') = k|g''| + M^{ab}(g''),$$

hence

$$\nu(s^2a'') = k(|g''| + 2) + 2(C - k) + M^{ab}(g'') = k|g| + M^{ab}(g'') + 2(C - k).$$

Moreover, since (*) holds for g', Proposition 1 applied to g' yields

$$\nu(a') = k|g'| + M^{ab}(g')$$

so that

$$\nu(2ua') = k(|g'|+1) + M^{ab}(g') = k|g| + M^{ab}(g').$$

On the other hand, by Lemma 8,

$$M^{ab}(g') = M^{ab}(g'')$$

which yields

$$\nu(2ua') < \nu(s^2a'').$$

Therefore, using (2),

$$\nu(a) = \nu(2ua') = k|g| + M^{ab}(g') = k|g| + M^{ab}(g).$$

One computes $\nu(b)$ using the same argument.

Now we compute $\nu(c)$. By Lemma 11,

$$c = 2uc' - s^2c''.$$

First one has:

$$\nu(c'') \geq k|g''| + M^{cd}(g''),$$

hence

$$\nu(s^2c'') \geq k(|g''|+2) + 2(C-k) + M^{cd}(g'') = k|g| + M^{cd}(g'') + 2(C-k).$$

As (*) holds for g', Proposition 1 applied to g' yields

$$\nu(c') \geq k|g'| + M^{cd}(g') + 2(C-k)$$

so that

$$\nu(2uc') \geq k(|g'|+1) + M^{cd}(g') + 2(C-k) = k|g| + M^{cd}(g') + 2(C-k).$$

Thus, using (2),

$$\nu(c) \geq k|g| + \min\{M^{cd}(g''), M^{cd}(g')\} + 2(C-k) = k|g| + M^{cd}(g) + 2(C-k).$$

Once again, one computes $\nu(d)$ using the same argument. □

Lemma 13. *Let $g \in \Gamma$ be a word of lenght at least four, ending by $q^e,\ e \in \{\pm 1\}$ and assume Proposition 1 holds for all words of of Γ of length $< |g|$. Then*

$$\nu(a) = \nu(b) = k|g| + M^{ab}(g)$$

and

$$\nu(c) = \nu(d) = k|g| + M^{cd}(g).$$

Proof. Since $|g| \geq 4$, we can find elements $\widetilde{g}, \overline{g}, \overline{\overline{g}} \in \Gamma$ such that $g \equiv \widetilde{g}q^e,\ \widetilde{g} \equiv \overline{g}p^h \equiv \overline{\overline{g}}p^{2h}$ with $e, h \in \{\pm 1\}$.

We only address the case when (*) holds for $\widetilde{g}$, as the proof in the other case is similar. Set $h_{\min} = \min\{h_+, h_-\}$ and $h_{\max} = \max\{h_+, h_-\}$. First we compute $\nu(c)$. Applying Rule (R2) to g, we get

$$c = uy\widetilde{c} + evx\widetilde{d} + evz\widetilde{a}.$$

Now, since (*) holds for $\widetilde{g}$, Proposition 1 applied to $\widetilde{g}$ gives

$$\nu(\widetilde{a}) = \nu(\widetilde{b}) = k|\widetilde{g}| + M^{ab}(\widetilde{g}) \quad \text{and} \quad \nu(\widetilde{c}), \nu(\widetilde{d}) \geq k|\widetilde{g}| + M^{cd}(\widetilde{g}) + 2(C-k). \tag{13}$$

Hence we obtain:

$$\nu(evz\widetilde{a}) = k(|\widetilde{g}|+1) + M^{ab}(\widetilde{g}) + (h_+ + h_-)/2$$

and

$$\nu(uy\widetilde{c} + evx\widetilde{d}) \geq k(|\widetilde{g}|+1) + M^{cd}(\widetilde{g}) + 2(C-k) + h_{\min}.$$

By Lemma 9,

$$|M^{ab}(\widetilde{g}) - M^{cd}(\widetilde{g})| \leq \frac{1}{2}|h_+ - h_-| < C - k$$

which yields

$$\nu(evz\widetilde{a}) - \nu(uy\widetilde{c} + evx\widetilde{d}) \leq M^{ab}(\widetilde{g}) - M^{cd}(\widetilde{g}) + |h_+ - h_-|/2 - 2(C-k) \leq |h_+ - h_-| - 2(C-k) < 0.$$

Using (4), one gets:

$$\nu(c) = \nu(evz\widetilde{a}) = k(|\widetilde{g}| + 1) + M^{ab}(\widetilde{g}) + (h_+ + h_-)/2 = k|g| + M^{cd}(g).$$

A similar computation applies to $\nu(d)$.

Let us compute $\nu(a)$. By applying Rule (R2) to g, we get

$$a = uy\widetilde{a} - evx\widetilde{b} - evz\widetilde{c}.$$

Now we show that $\nu(a) = \nu(uy\widetilde{a} - evx\widetilde{b})$ by performing the following steps: first we compute $\nu(evz\widetilde{c})$ and $\nu(uy\widetilde{a} - evx\widetilde{b})$; then, we show that the former quantity is strictly greater than the latter.

- Condition (13) yields:

$$\nu(evz\widetilde{c}) \geq k(|\widetilde{g}|+1) + M^{cd}(\widetilde{g}) + 2(C-k) + (h_+ + h_-)/2 = k|g| + M^{cd}(\widetilde{g}) + (h_+ + h_-)/2 + 2(C-k).$$

- Let us now compute $\nu(uy\widetilde{a} - evx\widetilde{b})$. By Lemma 11, Rule (R1) and the equality $s^2 = u^2 + v^2$, the term $uy\widetilde{a} - evx\widetilde{b}$ may be rewritten as

  $$X + s^2 Y,$$

  with

  $$X = 2u^2(y + ehx)\bar{a}$$

  and

  $$Y = \overline{\overline{b}}evx - u\overline{\overline{a}}(y + 2ehx).$$

  Let us now compute $\nu(X), \nu(Y)$. Since (*) holds for $\overline{g}$,

  $$\nu(\overline{a}) = k|\overline{g}| + M^{ab}(\overline{g})$$

  which gives

  $$\nu(X) = k|g| + M^{ab}(\overline{g}) + h_{eh}.$$

  On the other hand,

  $$\nu(\overline{\overline{a}}) = \nu(\overline{\overline{b}}) = k|\overline{\overline{g}}| + M^{ab}(\overline{\overline{g}})$$

  and

  $$\nu(x),\ \nu(y + 2ehx) \geq h_{\min}$$

  yield

  $$\nu(\overline{\overline{b}}evx),\ \nu(u\overline{\overline{a}}(y + 2ehx)) \geq k|\overline{g}| + M^{ab}(\overline{\overline{g}}) + h_{\min}$$

  whence

  $$\nu(s^2 Y) \geq k|g| + M^{ab}(\overline{\overline{g}}) + h_{\min} + 2(C-k).$$

  By Lemma 8, $M^{ab}(\overline{g}) = M^{ab}(\overline{\overline{g}})$. Moreover, we have

  $$h_{eh} - h_{\min} \leq h_{\max} < C - k$$

  which gives

  $$\nu(X) < \nu(s^2 Y)$$

  and, therefore,

  $$\nu(uy\widetilde{a} - evx\widetilde{b}) = \nu(X + s^2 Y) = \nu(X) = k|g| + M^{ab}(\overline{g}) + h_{eh}.$$

- Finally we compare $\nu(uy\widetilde{a} - evx\widetilde{b})$ and $\nu(evz\widetilde{c})$. By Lemma 7 and Lemma 9,

$$|M^{ab}(\overline{g}) - M^{cd}(\widetilde{g})| = |M^{ab}(\widetilde{g}) - M^{cd}(\widetilde{g})| < \frac{1}{2}|h_+ - h_-| < C - k.$$

Since moreover

$$h_{eh} - \frac{1}{2}(h_+ + h_-) < C - k$$

one has

$$\nu(evz\widetilde{c}) > \nu(uy\widetilde{a} - evx\widetilde{b})$$

and thus

$$\nu(a) = \nu(uy\widetilde{a} - evx\widetilde{b}) = k|g| + M^{ab}(\overline{g}) + h_{eh},$$

hence the claim by the definition of M^{ab}.

One computes $\nu(b)$ using the same argument. □

Lemma 14. *Let $g \in \Gamma$ be a word of length at least five, ending by $q^f p^e, e, f \in \{\pm 1\}$, and assume Proposition 1 holds for all words of Γ of length $< |g|$. Then*

$$\nu(a) = \nu(b) = k|g| + M^{ab}(g),$$
$$\nu(c), \nu(d) \geq k|g| + M^{cd}(g) + 2(C - k)$$

if (*) holds for g and

$$\nu(c) = \nu(d) = k|g| + M^{cd}(g),$$
$$\nu(a), \nu(b) \geq k|g| + M^{cd}(g) + 2(C - k),$$

otherwise.

Proof. As $|g| \geq 5$, we can write $g \equiv \widetilde{g}q^f p^e, \widetilde{g} \equiv \overline{g}p^h \equiv \overline{\overline{g}}p^{2h}$ with $e, f, h \in \{\pm 1\}$, and $\widetilde{g}, \overline{g}, \overline{\overline{g}} \in \Gamma$. We split the proof into the following two cases.

- $e = h$. In this case we have $e = f = h$. Let us first compute $\nu(a)$. By applying Rules (R1) and then (R2) to g, we have

$$a = \widetilde{a}(u^2 y - v^2 x) - \widetilde{b}uvh(x + y) + hvz(hv\widetilde{d} - u\widetilde{c}).$$

Set $X = hvz(hv\widetilde{d} - u\widetilde{c})$ and $Y = \widetilde{a}(u^2 y - v^2 x) - \widetilde{b}uvh(x + y)$. Since $v^2 = s^2 - u^2$, we may rewrite Y as

$$Y = (x + y)(\widetilde{a}u - \widetilde{b}vh)u - xs^2\widetilde{a}.$$

Now we notice that, if $g' \equiv \widetilde{g}p^h$, then $a' = (\widetilde{a}u - \widetilde{b}vh)$. Hence, Lemma 11 gives $a' = 2u\widetilde{a} - s^2\overline{a}$ which yields

$$Y = 2u^2(x + y)\widetilde{a} - s^2 u(x + y)\overline{a} - s^2 x\widetilde{a}.$$

– First we consider the case when $(*)$ holds for g. Since $e = h$, $(*)$ holds for $\widetilde{g}$ as well and thus the inductive assumption applied to $\widetilde{g}$ gives

$$\nu(\widetilde{a}) = \nu(\widetilde{b}) = |\widetilde{g}|k + M^{ab}(\widetilde{g}), \quad \nu(\widetilde{c}), \nu(\widetilde{d}) \geq |\widetilde{g}|k + M^{cd}(\widetilde{g}) + 2(C - k). \tag{14}$$

Now we give estimate for the valuation of X and Y. First condition (14) gives

$$\nu(X) \geq k(|\widetilde{g}| + 2) + M^{cd}(\widetilde{g}) + 2(C - k) + (h_+ + h_-)/2.$$

Now

$$h_+ - \nu(x) < 2(C - k)$$

gives

$$\nu(2u^2(x + y)\widetilde{a}) < \nu(s^2 x\widetilde{a}).$$

On the other hand, since (*) holds for $\widetilde{g}$, Equation (2) applied to $w'' = \widetilde{g}, w' = \overline{g}$ yields $M^{ab}(\widetilde{g}) = M^{ab}(\overline{g})$ which gives

$$\nu(2u^2(x + y)\widetilde{a}) < \nu(s^2 u(x + y)\overline{a}),$$

whence

$$\nu(Y) = \nu(2u^2(x+y)\widetilde{a}) = k(|\widetilde{g}|+2) + M^{ab}(\widetilde{g}) + h_+.$$

Finally, we show $\nu(Y) < \nu(X)$. Since $\widetilde{g} = \overline{g}p^h$,by Lemma 9, we have

$$|M^{ab}(\widetilde{g}) - M^{cd}(\widetilde{g})| \leq |h_+ - h_-|/2 < C - k,$$

from which

$$\nu(Y) < \nu(X).$$

Thus

$$\nu(a) = \nu(Y) = k(|\widetilde{g}|+2) + M^{ab}(\widetilde{g}) + h_+,$$

hence the claim by the definition of M^{ab} and the equality $|g| = |\widetilde{g}| + 2$.

– Now we consider the case when $(*)$ does not hold for g and thus nor for $\widetilde{g}$. The inductive assumption applied to $\widetilde{g}$ gives

$$\nu(\widetilde{a}), \nu(\widetilde{b}) \geq |\widetilde{g}|k + M^{ab}(\widetilde{g}) + 2(C-k), \quad \nu(\widetilde{c}) = \nu(\widetilde{d}) = |\widetilde{g}|k + M^{cd}(\widetilde{g}). \tag{15}$$

Now we give estimate for the valuation of X and Y.
Let us first notice that, if $g' \equiv \widetilde{g}p^h$, then $c' = (\widetilde{c}u + \widetilde{d}vh)$. Hence, Lemma 11 gives $c' = 2u\widetilde{c} - s^2\overline{c}$ which yields

$$X = hvz(2u\widetilde{c} - s^2\overline{c}).$$

By condition (15) and the definition of M^{ab}, one easily proves that

$$\nu(X), \nu(Y) \geq k(|\widetilde{g}|+2) + M^{ab}(\widetilde{g}) + 2(C-k).$$

and thus

$$\nu(a) \geq k(|\widetilde{g}|+2) + M^{ab}(\widetilde{g}) + 2(C-k).$$

The claim now follows from the definition of M^{ab} and the equality $|g| = |\widetilde{g}| + 2$.

- $e \neq h$. Let us now proceed with $\nu(a)$. We recall that

$$a = \widetilde{a}(u^2y - efv^2x) - \widetilde{b}uv(fx+ey) + fvz(ev\widetilde{d} - u\widetilde{c}).$$

As before set $X = fvz(ev\widetilde{d} - u\widetilde{c})$ and $Y = \widetilde{a}(u^2y - efv^2x) - \widetilde{b}uv(fx+ey)$.

– Let us consider the case when $(*)$ holds for g. Since $e \neq h$, $(*)$ does not hold for $\widetilde{g}$. Hence, by the inductive assumption to $\widetilde{g}$, condition (15) holds and therefore

$$\nu(Y) \geq k(|\widetilde{g}|+2) + M^{ab}(\widetilde{g}) + 2(C-k) + h_{ef}.$$

Since $e \neq h$, $X = fvz(hv\widetilde{d} + u\widetilde{c})$. Noticing that, if $g' \equiv \widetilde{g}p^h$, then $c' = u\widetilde{c} + hv\widetilde{d}$, by applying the inductive assumption to g', we have

$$\nu(c') = k(|\widetilde{g}|+1) + M^{cd}(\widetilde{g}),$$

and thus

$$\nu(X) = k(|\widetilde{g}|+2) + M^{cd}(\widetilde{g}) + (h_+ + h_-)/2.$$

Since $\widetilde{g}$ ends by $p^{\pm}$, Lemma 9 gives

$$|M^{ab}(\widetilde{g}) - M^{cd}(\widetilde{g})| \leq |h_+ - h_-|/2 < C - k,$$

from which

$$\nu(X) < \nu(Y).$$

Thus

$$\nu(a) = \nu(X) = k(|\widetilde{g}|+2) + M^{cd}(\widetilde{g}) + (h_+ + h_-)/2,$$

hence the claim by the definition of M^{cd} and the equality $|g| = |\widetilde{g}| + 2$.

– Finally let us consider the case when $(*)$ does not hold for g. Since $e \neq h$, $(*)$ holds for $\widetilde{g}$. Hence, by the inductive assumption applied to $\widetilde{g}$, condition (14) holds and thus

$$\nu(X) \geq k(|\widetilde{g}|+2) + M^{cd}(\widetilde{g}) + 2(C-k) + (h_+ + h_-)/2.$$

Using $v^2 = s^2 - u^2$ and $e \neq h$, Y may be rewritten as

$$Y = u(y+efx)(\widetilde{a}u + hv\widetilde{b}) - s^2efx\widetilde{a}.$$

Now, noticing that $s^2\overline{a} = \widetilde{a}u + hv\widetilde{b}$ yields

$$Y = s^2u(y+efx)\overline{a} - s^2efx\widetilde{a} = s^2(y-efx)u\overline{a} + s^2efx(2u\overline{a} - \widetilde{a}).$$

Lemma 11 gives now $s^2\overline{\overline{a}} = 2u\overline{a} - \widetilde{a}$ so that

$$Y = s^2(y-efx)u\overline{a} + s^4efx\overline{\overline{a}}.$$

Since $(*)$ holds for $\overline{g}$, by applying the inductive assumption to $\overline{g}$, we have

$$\nu(\overline{a}) = k|\overline{g}| + M^{ab}(\overline{g}),$$

so that

$$\nu(s^2(y-efx)u\overline{a}) = k(|\overline{g}|+3) + M^{ab}(\overline{g}) + 2(C-k) + h_{ef}.$$

Moreover we have

$$\nu(s^4efx\overline{\overline{a}}) \geq 4(C-k) + k(|\overline{\overline{g}}|+4) + M^{ab}(\overline{\overline{g}}) + \nu(x).$$

Since, by Lemma 8, $M^{ab}(\overline{g}) = M^{ab}(\overline{\overline{g}})$, and morevover $\nu(x) - h_{ef} < C-k$, we have

$$\nu(s^2(y-efx)u\overline{a}) < \nu(s^4efx\overline{\overline{a}})$$

and thus

$$\nu(Y) = k(|\overline{g}|+3) + M^{ab}(\overline{g}) + 2(C-k) + h_{ef}.$$

Finally, by comparing $\nu(X)$ and $\nu(Y)$ and by the equality $|\widetilde{g}| = |\overline{g}| + 1$, we have

$$\nu(a) \geq k(|\widetilde{g}|+2) + 2(C-k) + \min\{M^{ab}(\overline{g}) + h_{ef}, M^{cd}(\widetilde{g}) + (h_+ + h_-)/2\} + 2(C-k),$$

hence the claim by the definition of M^{ab} and the equality $|g| = |\widetilde{g}| + 2$.

By using the previous argument, one can obtain the computation of $\nu(b)$.

The computation of $\nu(c)$ and $\nu(d)$ can be obtained by exchanging ab with cd. □

We are finally able to give the following

Proof of Lemma 3. By contradiction.

Say we can find $g \neq 1$ in Γ such that $\mathrm{ev}(g) = 1$. Set

$$g = \frac{1}{s^{|g|}}\frac{1}{y^{|g|_q}}(a + bi + cj + dk).$$

We know that $h_{\max} - h_{\min} = |h_+ - h_-| < C-k$. Moreover $|g|_q < |g|$ for all words. Then $(h_{\max} - h_{\min})|g|_q < (C-k)|g|$, hence $k|g| + h_{\max}|g|_q < C|g| + h_{\min}|g|_q$ for all choices of g.

Lemma 10 along with Proposition 1 show that the valuation at least two expressions among a, b, c and d if less or equal than $k|g| + h_{\max}|g|_q$. On the other hand, $\nu(s^{|g|}y^{|g|_q}) = C|g| + \nu(y)|g|_q$.

We know that $\nu(y) \geq h_{\min}$, so that $k|g| + h_{\max}|g|_q < C|g| + \nu(y)|g|_q \leq \nu(s^{|g|}y^{|g|_q})$. This shows that at least two coefficients of $\mathrm{ev}(g)$ have a negative valutation on ν, a contradiction with $\mathrm{ev}(g) = 1$. The lemma is thus proved. □

ACKNOWLEDGEMENTS

We gladly acknowledge Toni Machì for suggesting the subject of this paper and for many helpful discussions, and the patient referee for struggling against an early version of the paper, and for suggesting improvements in the exposition.

REFERENCES

[1] F. D'Alessandro (2004), *'Free groups of quaternions'*, Internat. J. Algebra Comput. **14 (1)**, 69–86.
[2] J. Dauns, *'A Concrete Approach to Division Rings'*, Heldermann Verlag, Berlin, 1982.
[3] Th. J. Dekker (1959), *'On free products of cyclic rotation groups'*, Canad. J. Math. **11**, 67–69.
[4] J. De Groot (1956), *'Orthogonal isomorphic representations of free groups'*, Canad. J. Math. **8**, 256–262.
[5] J. Z. Gonçalves, A. Mandel, and M. Shirvani (1999), *'Free products of units in algebras. I. Quaternion algebras.'*, J. Algebra **214 (1)**, 301–316.
[6] M. Koecher, R. Remmert, *'Hamilton's Quaternions'* in H.-D. Ebbinghaus et al. *'Numbers'*, Springer Verlag, Berlin, 1983.
[7] S. Swierczkowski (1994), *'A class of free rotation groups'*, Indag. Math. **5 (2)**, 221–226.
[8] J. Tits (1972), *'Free subgroups in linear groups'*, J. Algebra **20**, 250–270.

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI ROMA "LA SAPIENZA", PIAZZALE ALDO MORO 2, 00185 ROMA, ITALY.
E-mail address: dalessan@mat.uniroma1.it, dandrea@mat.uniroma1.it