COLLOQUIUM MATHEMATICUM

VOL. 88 2001 NO. 1

ON FREE SUBGROUPS OF UNITS IN QUATERNION ALGEBRAS

BY

JAN KREMPA (Warszawa)

Abstract. It is well known that for the ring $\mathrm{H}(\mathbb{Z})$ of integral quaternions the unit group $\mathrm{U}(\mathrm{H}(\mathbb{Z}))$ is finite. On the other hand, for the rational quaternion algebra $\mathrm{H}(\mathbb{Q})$, its unit group is infinite and even contains a nontrivial free subgroup. In this note (see Theorem 1.5 and Corollary 2.6) we find all intermediate rings $\mathbb{Z} \subset A \subseteq \mathbb{Q}$ such that the group of units $\mathrm{U}(\mathrm{H}(A))$ of quaternions over A contains a nontrivial free subgroup. In each case we indicate such a subgroup explicitly. We do our best to keep the arguments as simple as possible.

1. Motivation and main result. In this paper $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ have standard meaning as subsets of the field $\mathbb{C}$ of complex numbers, $\mathrm{U}(R)$ denotes the group of units of any associative ring R with $1 \neq 0$, $\mathcal{F}$ stands for a free nonabelian group with two generators, and $\mathrm{SO}_n(R) \subset \mathrm{GL}_n(R)$ for the well known linear groups over a given ring R. We also apply some other standard notation and terminology (see for example [10, 13, 17]).

In [4, 8, 9, 11], and some other papers, for various rings R explicit copies of $\mathcal{F} \subset \mathrm{U}(R)$ were found. We consider the same problem for orders, but not only $\mathbb{Z}$-orders, in finite-dimensional, semisimple $\mathbb{Q}$-algebras. An old and simple, but very useful and effective result in this direction, due to Sanov and Brenner (see [17]), is:

LEMMA 1.1. *For any $c \in \mathbb{C}$ put*

$$u_c = \begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad u_c^* = \begin{bmatrix} 1 & 0 \\ c & 1 \end{bmatrix}.$$

If either $|c| \geq 2$ or c is transcendental over $\mathbb{Q}$ then the subgroup $\langle u_c, u_c^* \rangle \subset \mathrm{GL}_2(\mathbb{C})$ is free.

As a consequence of this result we have

THEOREM 1.2. *Let R be any order in a finite-dimensional semisimple $\mathbb{Q}$-algebra. If R has a nonzero nilpotent element then there exists an effective way to construct a copy of $\mathcal{F} \subseteq \mathrm{U}(R)$.*

2000 *Mathematics Subject Classification*: Primary 16U60; Secondary 16H05, 11A99.
Supported by Polish KBN Research Grant.

Sketch of proof. By the assumption there exists a semisimple, finite-dimensional $\mathbb{Q}$-algebra A with nontrivial nilpotent element such that $R \subseteq A$ and $A = \mathbb{Q}R$. In particular, for any $a \in A$ there exists $n \in \mathbb{N}$ such that $na \in R$. Hence, if $B \subseteq A$ is any finitely generated subring, then $mB \subseteq R$ for some $m \in \mathbb{N}$. Combining these observations with the existence of a nontrivial nilpotent in A, and with the arguments from [6, 7, 8], one can reduce the consideration to matrices of degree greater than one, and complete the proof with the help of Lemma 1.1.

The situation is more complicated when considering rings with no non-zero nilpotent elements, in particular integral domains. For this case (see [3, 6]) the standard argument for the existence of a copy of $\mathcal{F}$ in groups of units is via a result from [16], known as Tits' Alternative. This result is very strong and fairly nontrivial, but not effective.

Tits' Alternative seems to be indispensable in the proof of the following (again noneffective) result from [3]:

THEOREM 1.3 (Gonçalves). *Let D be a division algebra which is finite-dimensional over its center. If D is not a field then $\mathcal{F} \subset \mathrm{U}(D)$.*

We have been unable to find in the literature an example of $\mathcal{F} \subset \mathrm{U}(D)$, even if D is the algebra of rational quaternions. So we decided to fill this gap. Our first example was based on [12] but now, using a result from [14, 15], we are able to exhibit infinitely many different copies of $\mathcal{F}$ in the group of units of rational quaternions. Our approach is restricted to rational quaternions, but it is based only on elementary number theory and on the result of S. Świerczkowski, mentioned above. This result is also elementary.

Lately, in [4], a more general, but more complicated approach to effective construction of free subgroups of units in quaternion algebras was found. This approach is different from that presented here and, for example, has the result of Świerczkowski from [15] only as a consequence of the main theorems.

Now let us fix the necessary notation. $\mathbb{H}$ will denote the algebra of real quaternions with standard base $1, i, j, k$. For any $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}$ let, as usual,

$$\overline{\alpha} = a_0 - a_1 i - a_2 j - a_3 k \quad \text{and} \quad \|\alpha\| = \alpha\overline{\alpha} = a_0^2 + a_1^2 + a_2^2 + a_3^2 \tag{1}$$

be the conjugate and the norm of α. Then for any $\alpha, \beta \in \mathbb{H}$ we have

$$\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}, \quad \overline{\alpha\beta} = \overline{\beta}\,\overline{\alpha}, \quad \text{and} \quad \|\alpha\beta\| = \|\alpha\| \cdot \|\beta\|. \tag{2}$$

If $A \subseteq \mathbb{R}$ is any subring then we denote by $\mathrm{H}(A)$ the algebra of quaternions over A. Clearly $\mathrm{H}(A)$ is freely generated as an A-module by the elements $1, i, j, k$ and is a subring of $\mathbb{H}$ invariant under conjugation. For $n \in \mathbb{N}$,

we also set $A_n = \mathbb{Z}[1/n]$ and $H_n = \mathrm{H}(A_n)$. Instead of $H_1 = \mathrm{H}(\mathbb{Z})$ we write simply H.

It is well known that the group $\mathrm{U}(H)$ is of order 8 and is characterized as the set of elements $\alpha \in H$ with $\|\alpha\| = 1$. More generally, by (1) and (2), if $\alpha \neq 0$ then $\|\alpha\| \neq 0$ and $\alpha^{-1} = (1/\|\alpha\|)\overline{\alpha}$. Hence, for any subring $A \subseteq \mathbb{R}$ we have

$$\mathrm{U}(\mathrm{H}(A)) = \{\alpha \in \mathrm{H}(A) : \|\alpha\| \in \mathrm{U}(A)\}. \tag{3}$$

From Theorem 1.3 we know that $\mathcal{F} \subset \mathrm{U}(\mathrm{H}(\mathbb{Q}))$. In particular we have the following, again noneffective result:

PROPOSITION 1.4. *There exists $n \in \mathbb{N}$ such that $\mathcal{F} \subset \mathrm{U}(H_n)$.*

In this paper we determine which numbers $n \in \mathbb{N}$ can be taken in the above proposition. More precisely, our main result is:

THEOREM 1.5. *Let $n \in \mathbb{N}$. Then $\mathcal{F} \subseteq \mathrm{U}(H_n)$ if and only if n is not a power of two. For any such n we can indicate a concrete copy of $\mathcal{F} \subseteq \mathrm{U}(H_n)$.*

2. The proof. For the proof of Theorem 1.5 we apply the following result of S. Świerczkowski [15] about subgroups of orthogonal matrices:

LEMMA 2.1. *Let*

$$A = \begin{bmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & \sin\theta \\ 0 & -\sin\theta & \cos\theta \end{bmatrix}$$

be matrices of two linear rotations of 3-dimensional Euclidean space over $\mathbb{R}$. If $\cos\theta \notin \{0, \pm 1/2, \pm 1\}$ but is a rational number, then the group $\langle A, B\rangle$ is a free subgroup of $\mathrm{SO}_3(\mathbb{R})$.

The proof of the lemma is straightforward and not very complicated. We use this lemma only in the easiest case, when the denominator of $\cos\theta$ is an odd rational integer. Hence, in fact, we only apply a result from [14].

To make use of the above lemma let us recall some elementary connections of quaternions with geometry (see [10]). As a vector space, $\mathbb{H} = \mathbb{R} \oplus \mathbb{P}$ where $\mathbb{P}$, the subspace of pure quaternions, is spanned over $\mathbb{R}$ by its standard base i, j, k. From (1) we also have

$$\pi \in \mathbb{P} \quad \text{if and only if} \quad \overline{\pi} = -\pi. \tag{4}$$

We will consider $\mathbb{P}$ as a 3-dimensional Euclidean space in which the base i, j, k is orthonormal.

With any $\xi \in \mathrm{U}(\mathbb{H})$ we can associate a map $\varphi_\xi : \mathbb{P} \to \mathbb{P}$ given by the formula

$$\varphi_\xi(\pi) = \xi\pi\xi^{-1} \quad \text{for any } \pi \in \mathbb{P}.$$

From this definition and formulas (2) and (4) it is clear that φ_ξ is an $\mathbb{R}$-linear map, preserves the norm of quaternions, and the space $\mathbb{P}$ is φ_ξ-invariant. Hence φ_ξ, being always a linear isometry, is either a rotation of $\mathbb{P}$ with axis parallel to the pure part of ξ if $\xi \notin \mathbb{R}$, or is the identity if $\xi \in \mathbb{R}$. More precisely, if $\xi = x_0 + x_1 i + x_2 j + x_3 k$ then in the standard base of $\mathbb{P}$ the matrix of φ_ξ, denoted by M_ξ, is

$$M_\xi = \frac{1}{\|\xi\|} \begin{bmatrix} x_0^2 + x_1^2 - x_2^2 - x_3^2 & 2(x_1x_2 - x_0x_3) & 2(x_0x_2 + x_1x_3) \\ 2(x_0x_3 + x_1x_2) & x_0^2 - x_1^2 + x_2^2 - x_3^2 & 2(x_2x_3 - x_0x_1) \\ 2(x_1x_3 - x_0x_2) & 2(x_0x_1 + x_2x_3) & x_0^2 - x_1^2 - x_2^2 + x_3^2 \end{bmatrix}. \tag{5}$$

Counting the trace of M_ξ in the standard base of $\mathbb{P}$ and in an orthonormal base containing a vector parallel to the axis of the rotation φ_ξ we obtain

$$\begin{aligned} \operatorname{tr}(M_\xi) &= \frac{1}{\|\xi\|}(3x_0^2 - x_1^2 - x_2^2 - x_3^2) \\ &= 1 + 2\frac{x_0^2 - x_1^2 - x_2^2 - x_3^2}{x_0^2 + x_1^2 + x_2^2 + x_3^2} = 1 + 2\cos\theta, \end{aligned}$$

where θ is the angle of the rotation φ_ξ. Hence

$$\cos\theta = \frac{x_0^2 - x_1^2 - x_2^2 - x_3^2}{x_0^2 + x_1^2 + x_2^2 + x_3^2}. \tag{6}$$

It is well known that the map f given by $f(\xi) = \varphi_\xi$ is a homomorphism of the group $\mathrm{U}(\mathbb{H})$ into the group of proper linear rotations of the Euclidean space $\mathbb{P}$. In fact f maps onto this group of isometries, which is isomorphic to $\mathrm{SO}_3(\mathbb{R})$ (see [10]), but we will not use the surjectivity of f here.

EXAMPLE 2.2. *Let $a, b, c \in \mathbb{N}$ form a Pythagorean triple ($a^2 + b^2 = c^2$), where c is odd. Then the elements $u = a + bi$ and $v = a + bk$ generate a copy of $\mathcal{F} \subset \mathrm{U}(H_c)$.*

Indeed, from the choice of u and v we have $\|u\| = \|v\| = c^2$. Hence, by (3), $u, v \in \mathrm{U}(H_c)$. From (5), $\varphi_u = f(u)$ and $\varphi_v = f(v)$ have the following matrices in the standard base of $\mathbb{P}$:

$$M_u = \frac{1}{c^2} \begin{bmatrix} c^2 & 0 & 0 \\ 0 & a^2 - b^2 & -2ab \\ 0 & 2ab & a^2 - b^2 \end{bmatrix},$$

$$M_v = \frac{1}{c^2} \begin{bmatrix} a^2 - b^2 & -2ab & 0 \\ 2ab & a^2 - b^2 & 0 \\ 0 & 0 & c^2 \end{bmatrix}.$$

In both cases, by (6) we have

$$\cos\theta = \frac{a^2 - b^2}{a^2 + b^2} = \frac{a^2 - b^2}{c^2}.$$

Because the numbers a, b, c form a nontrivial Pythagorean triple, it follows that $\cos\theta \notin \{0, \pm 1\}$. If $\cos\theta = \varepsilon/2$, where $\varepsilon = \pm 1$, then we would obtain $\varepsilon c^2 = 2a^2 - 2b^2$, which is impossible, because c is odd.

Now, Lemma 2.1 shows that the group $\langle f(u), f(v)\rangle$ is free, hence the group $\langle u, v\rangle$ is free as well.

EXAMPLE 2.3. *Let $a, b, c \in \mathbb{N}$ be such that $a^2 + b^2 + c^2 = d^2$ for some odd $d \in \mathbb{N}$. Then the elements $u = a + bi + cj$ and $v = a + ci - bj$ generate a copy of $\mathcal{F} \subset \mathrm{U}(H_d)$.*

Indeed, from (1) we have $\|u\| = \|v\| = d^2$. Hence $u, v \in \mathrm{U}(H_d)$. Further, by the definition, it is clear that the axis of the rotation φ_u is parallel to the vector $(b, c, 0)$ while the axis of φ_v is parallel to $(c, -b, 0)$. Hence, these axes are orthogonal. From (6) one can easily calculate that for both rotations the number $\cos\theta$ is the same, equal to

$$\frac{a^2 - b^2 - c^2}{a^2 + b^2 + c^2} = \frac{a^2 - b^2 - c^2}{d^2},$$

and does not belong to the set $\{0, \pm 1/2, \pm 1\}$, because d is odd. Hence, by Lemma 2.1 applied to the matrices of φ_u and φ_v in the base $\left\{\frac{1}{d}(c, -b, 0), \beta, \frac{1}{d}(b, c, 0)\right\}$, where $\beta \in \mathbb{P}$ is a vector orthogonal to both the others and $\|\beta\| = 1$, we conclude that the subgroup $\langle f(u), f(v)\rangle \subset \mathrm{SO}_3(\mathbb{R})$ is free, and so is $\langle u, v\rangle \subset \mathrm{U}(H_d)$.

EXAMPLE 2.4. *The group $\mathrm{U}(H_2)$ is abelian-by-finite, hence does not contain any copy of $\mathcal{F}$.*

Indeed, by (3), $\alpha \in \mathrm{U}(H_2)$ if and only if $\|\alpha\| = 2^n$ for some $n \in \mathbb{Z}$. On the other hand,

$$\alpha = 2^m\beta, \quad \text{where} \quad m \in \mathbb{Z} \text{ and } \beta = b_0 + b_1 i + b_2 j + b_3 k \in H.$$

Without loss of generality we can assume that at least one b_i is odd. We use the elementary fact that if a sum of four squares of rational integers is divisible by 8, then all these numbers are even.

Consider the subgroup $\langle 2\rangle \subset \mathrm{U}(H_2)$. This subgroup is central and, according to the observations mentioned above, it is of finite index. As representatives of cosets it is enough to use, for example, some $\beta \in H$ with $\|\beta\| \in \{1, 2, 4\}$.

LEMMA 2.5. *Let p be an odd natural prime.*

- *If $p \equiv 1 \pmod 4$ then p^2 is a nontrivial sum of two squares.*
- *If $p \equiv 3 \pmod 4$ then p^2 is a nontrivial sum of three squares.*

Proof. If $p = 4m + 1$ then it is well known, for example from [13], that $p = a^2 + b^2$ for some $a, b \in \mathbb{N}$. Then $p^2 = (a^2 - b^2)^2 + (2ab)^2$.

Now let $p = 4m + 3$. By the theorem of Legendre $p = a^2 + b^2 + c^2 + d^2$ where at least three summands are nonzero (see [13]). As in [2] we can apply the Lebesgue identity. In this way we obtain

$$p^2 = (a^2+b^2+c^2+d^2)^2 = (a^2+b^2-c^2-d^2)^2 + (2ac+2bd)^2 + (2ad-2bc)^2$$

and we can verify that the summands are nontrivial.

Proof of Theorem 1.5. Let $A_n \subseteq \mathbb{Q}$ for some $n \in \mathbb{N}$. If n is not a power of 2 then let p be an odd prime divisor of n. Then certainly $A_p \subseteq A_n$. By Lemma 2.5, p can be either the c of Example 2.2 or the d of Example 2.3. Hence, in any case $\mathcal{F} \subseteq \mathrm{U}(H_p) \subseteq \mathrm{U}(H_n)$ and its explicit copy is indicated.

If $A_n \subseteq A_2$ then either $A_n = \mathbb{Z}$ or $A_n = A_2$ and, by Example 2.4, $\mathcal{F} \not\subseteq \mathrm{U}(H_n)$.

COROLLARY 2.6. *Let $A \subseteq \mathbb{Q}$ be any subring. Then $\mathcal{F} \subseteq \mathrm{U}(\mathrm{H}(A))$ if and only if $A \not\subseteq A_2$.*

Proof. Let $A \subseteq \mathbb{Q}$ be a subring such that $A \not\subseteq A_2$. Then there exists an irreducible fraction $a/b \in A$ such that $a, b \in \mathbb{N}$ and b is not a power of 2. We also know that $1 = b/b \in A$, hence $1/b \in A$ because a and b are coprime. This means that $H_b \subseteq A$ and, by Theorem 1.5, $\mathcal{F} \subseteq \mathrm{U}(H_b) \subseteq \mathrm{U}(\mathrm{H}(A))$.

The converse implication is evident by Example 2.4.

In several papers (see [1] and references there) groups of units containing a free noncommutative semigroup with two generators (denote it by $\mathcal{S}$) are investigated. From our earlier results we obtain:

PROPOSITION 2.7. *Let $A \subseteq \mathbb{Q}$ be any subring. Then $\mathcal{S} \subseteq \mathrm{U}(\mathrm{H}(A))$ if and only if $A \not\subseteq A_2$.*

Proof. From Example 2.4 we deduce that the group $\mathrm{U}(H_2)$ satisfies a semigroup identity of the form $x^m y^m \equiv y^m x^m$ for some $m > 1$. Hence $\mathcal{S} \not\subseteq \mathrm{U}(H_2)$.

On the other hand, if $A \not\subseteq A_2$ then, by Corollary 2.6, $\mathrm{U}(\mathrm{H}(A))$ contains even $\mathcal{F}$. From these facts the result follows immediately.

Let us finish with a question inspired by Theorem 1.5. To formulate it, for any $n \in \mathbb{N}$ denote by C_n the algebra of Cayley numbers over the ring A_n. This nonassociative ring with unity can be represented as an H_n-module as follows:

$$C_n = H_n \oplus H_n e,$$

where

$$(\alpha + \beta e)(\gamma + \delta e) = \alpha\gamma - \beta\overline{\delta} + (\alpha\delta + \beta\overline{\gamma})e \quad \text{for all } \alpha, \beta, \gamma, \delta \in H_n.$$

For any $n \in \mathbb{N}$ it is well known (see [5]) that the set $\mathrm{U}(C_n)$ of units of C_n is a Moufang loop. Hence any subloop of $\mathrm{U}(C_n)$ generated by two elements is a group. Moreover, $H_n \subset C_n$ as a subring. By Theorem 1.5, this gives

$\mathcal{F} \subseteq \mathrm{U}(C_n)$ for n not being a power of two. On the other hand the loop $\mathrm{U}(C_1)$ is finite. Thus the following question is well posed and interesting:

Does the loop $\mathrm{U}(C_2)$ *contain a copy of* $\mathcal{F}$ (*or at least* $\mathcal{S}$)*? If the answer is yes, then exhibit such a subgroup* (*subsemigroup*).

REFERENCES

[1] M. Boffa, *Elimination of inverses in groups*, in: Model Theory of Groups and Automorphism Groups, D. M. Evans (ed.), Cambridge Univ. Press, Cambridge, 1997, 134–143.

[2] O. Fraser and B. Gordon, *On representing a square as the sum of three squares*, Amer. Math. Monthly 76 (1969), 922–923.

[3] J. Z. Gonçalves, *Free subgroups of units in group rings*, Canad. Math. Bull. 27 (1984), 309–312.

[4] J. Z. Gonçalves, A. Mandel and M. Shirvani, *Free products of units in algebras. I. Quaternion algebras*, J. Algebra 214 (1999), 301–316.

[5] E. G. Goodaire, E. Jespers and C. Polcino Milies, *Alternative Loop Rings*, Elsevier, Amsterdam, 1996.

[6] G. Karpilovsky, *Unit Groups of Classical Rings*, Clarendon Press, Oxford, 1988.

[7] J. Krempa, *Rings with periodic unit groups*, in: Abelian Groups and Modules, A. Facchini and C. Menini (eds.), Kluwer, Dordrecht, 1995, 313–321.

[8] —, *Rings with periodic groups of units II*, in: Groups St Andrews 1997 in Bath II, C. M. Campbell *et al.* (eds.), Cambridge Univ. Press, Cambridge, 1999, 503–511.

[9] Z. S. Marciniak and S. K. Sehgal, *Units in group rings and geometry*, in: Methods in Ring Theory, V. Drensky *et al.* (eds.), Dekker, New York, 1998, 185–198.

[10] I. R. Porteous, *Topological Geometry*, van Nostrand Reinhold, London, 1969.

[11] A. Salwa, *On free subgroups of units of rings*, Proc. Amer. Math. Soc. 127 (1999), 2569–2572.

[12] K. Satô, *A free group acting without fixed points on the rational unit sphere*, Fund. Math. 148 (1995), 63–69.

[13] W. Sierpiński, *Elementary Theory of Numbers*, 2nd ed., revised by A. Schinzel, PWN–Polish Sci. Publ., Warszawa, 1987.

[14] S. Świerczkowski, *On a free group of rotations of the Euclidean space*, Indag. Math. 20 (1958), 376–378.

[15] —, *A class of free rotation groups*, Indag. Math. (NS) 5 (1994), 221–226.

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

[17] B. A. F. Wehrfritz, *Infinite Linear Groups*, Springer, Berlin, 1973.

Institute of Mathematics
Warsaw University
Banacha 2
02-097 Warszawa, Poland
E-mail: jkrempa@mimuw.edu.pl

Received 7 February 2000;
revised 11 May 2000 (3884)