COLLOQUIUM MATHEMATICUM

VOL. 97 2003 NO. 1

ON FREE SUBGROUPS OF UNITS IN QUATERNION ALGEBRAS II

BY

JAN KREMPA (Warszawa)

Abstract. Let $A \subseteq \mathbb{Q}$ be any subring. We extend our earlier results on unit groups of the standard quaternion algebra $\mathrm{H}(A)$ to units of certain rings of generalized quaternions $\mathrm{H}(A,a,b) = \left(\frac{-a,-b}{A}\right)$, where $a, b \in A$. Next we show that there is an algebra embedding of the ring $\mathrm{H}(A,a,b)$ into the algebra of standard Cayley numbers over A. Using this embedding we answer a question asked in the first part of this paper.

1. Generalized quaternions. We apply the notation of [2]. In particular, $\mathcal{F}$ stands for a free group of rank two and $A_n = \mathbb{Z}[1/n]$ for any $n \in \mathbb{N}$.

For any subring $A \subseteq \mathbb{Q}$ we consider not only the standard quaternion A-algebra $\mathrm{H}(A)$, but also a generalized quaternion algebra $\mathrm{H}(A,a,b)$, where $a, b \in A$ are positive numbers. By definition $\mathrm{H}(A,a,b) = \left(\frac{-a,-b}{A}\right)$ is an associative A-algebra free as an A-module, with base $1, i_a, j_b, k_{ab}$, and with multiplication given by

$$i_a^2 = -a, \quad j_b^2 = -b, \quad k_{ab}^2 = -ab, \quad i_a j_b = -j_b i_a = k_{ab}. \tag{1}$$

Under this notation $\mathrm{H}(A) = \mathrm{H}(A,1,1)$, $i = i_1$, $j = j_1$ and $k = k_1$. Using (1) we have a natural embedding ε of $\mathrm{H}(A,a,b)$ into the algebra $\mathbb{H}$ of real quaternions induced by

$$\varepsilon(i_a) = \sqrt{a}\, i, \quad \varepsilon(j_b) = \sqrt{b}\, j. \tag{2}$$

Using this embedding we can apply the standard quaternion notation. In particular, for $\alpha = a_0 + a_1 i_a + a_2 j_b + a_3 k_{ab} \in \mathrm{H}(A,a,b)$ we can write

$$\overline{\alpha} = a_0 - a_1 i_a - a_2 j_b - a_3 k_{ab},$$
$$\mathrm{n}(\alpha) = \alpha\overline{\alpha} = a_0^2 + a a_1^2 + b a_2^2 + ab a_3^2. \tag{3}$$

The unit group of an arbitrary ring R is denoted by $\mathrm{U}(R)$. For any $\alpha \in \mathrm{H}(A,a,b)$, by (3), we know that $\alpha \in \mathrm{U}(\mathrm{H}(A,a,b))$ if and only if $\mathrm{n}(\alpha) \in \mathrm{U}(A)$, because in $\mathbb{H}$ we have $\alpha^{-1} = \overline{\alpha}/\mathrm{n}(\alpha)$.

2000 *Mathematics Subject Classification*: Primary 16U60, 17D05; Secondary 16H05, 11D57.

Work supported in part by Onderzoeksraad of Vrije Universiteit Brussel, Fonds voor Wetenschappelijk Onderzoek (Belgium), Flemish-Polish bilateral agreement BIL 01/31.

In [2] the following result was proved:

THEOREM 1.1. *Let $\mathbb{Z} \subset A \subseteq \mathbb{Q}$ be a subring. If $A = A_2$ then the group* $\mathrm{U}(\mathrm{H}(A))$ *is cyclic-by-finite. In any other case $\mathcal{F} \subseteq \mathrm{U}(\mathrm{H}(A))$.*

We are going to extend this result. Because any subring of $\mathbb{Q}$ is a localization of $\mathbb{Z}$ at a subset of $\mathbb{N}$, we have

PROPOSITION 1.2. *Let $A \subseteq \mathbb{Q}$ and let $a, b, c, d \in A$ be positive numbers. Then* $\mathrm{H}(A, ac^2, bd^2) \subseteq \mathrm{H}(A, a, b)$. *In particular*, $\mathrm{H}(A, a, b) \subseteq \mathrm{H}(A, a', b')$, *where $a', b' \in \mathbb{N}$ and are square free.*

If in generalized quaternions one of parameters is equal to 1 then a further reduction is possible.

PROPOSITION 1.3. *Let $A \subseteq \mathbb{Q}$ be a subring and $b \in \mathbb{N}$ be square free. If in $\mathbb{N}$ we have $b = cd$, where d is a sum of two squares, then there exists an embedding of* $\mathrm{H}(A, 1, b)$ *into* $\mathrm{H}(A, 1, c)$.

Proof. Let $d = x^2 + y^2$ where $x, y \in \mathbb{N}$. Then the A-algebra homomorphism ϕ induced by $\phi(i) = i$ and $\phi(j_b) = xj_c + yk_c$ is the required embedding. ∎

COROLLARY 1.4. *Let $\mathbb{Z} \subset A \subseteq \mathbb{Q}$ be a subring and let $b \in A$ be a positive element which is a sum of two squares in A. If $A = A_2$ then* $\mathrm{U}(\mathrm{H}(A, 1, b))$ *is cyclic-by-finite. In any other case $\mathcal{F} \subseteq \mathrm{U}(\mathrm{H}(A, 1, b))$.*

Proof. By previous propositions we have an embedding $\eta : \mathrm{H}(A, 1, b) \to \mathrm{H}(A, 1, 1) = \mathrm{H}(A)$, as an A-algebra. Now it is not hard to check that the image of η has finite additive index in $\mathrm{H}(A)$. From Lemma 4.2 in [3] it then follows that the group $\mathrm{U}(\mathrm{H}(A, 1, b))$ has a finite index in the group $\mathrm{U}(\mathrm{H}(A))$. Hence the claim becomes a consequence of Theorem 1.1. ∎

Now we show that this corollary cannot be extended to all $b \in \mathbb{N}$.

PROPOSITION 1.5. *Let $b \in \mathbb{N}$ be square free and let $p \in \mathbb{N}$ be a prime of the form $4k + 3$, where $k \geq 0$. If $p \mid b$ then the group* $\mathrm{U}(\mathrm{H}(A_p, 1, b))$ *is cyclic-by-finite.*

Proof. Let $S = \mathrm{H}(A_p, 1, b)$. Then the group $\langle p \rangle$ is a central subgroup of $\mathrm{U}(S)$. Moreover, any $u \in \mathrm{U}(S)$ can be written in the form $u = p^k \alpha$, where $k \in \mathbb{Z}$ and $\alpha = a_0 + a_1 + a_2 j_b + a_3 k_b \in \mathrm{H}(\mathbb{Z}, 1, b)$. We can assume that not all a_i's are divisible by p and of course $\mathrm{n}(\alpha) = p^r$ for some $r \geq 0$.

Assume $r \geq 2$. This implies that $p \mid (a_0^2 + a_1^2)$, hence $p \mid a_0$ and $p \mid a_1$ because p is not a sum of two squares in $\mathbb{N}$ (see [5, §13.5]). From (3) we then deduce that $p \mid (a_2^2 + a_3^2)$. Hence, as above, $p \mid a_2$ and $p \mid a_3$, a contradiction to the choice of α.

In this way we proved that $r < 2$. Hence we have only a finite number of elements α, and the group $\langle p \rangle$ has finite index in $\mathrm{U}(S)$. ∎

On the other hand we have

EXAMPLE 1.6. Consider the ring $R = \mathrm{H}(A_2, 1, 3)$ and elements $\alpha = 1 + j_3 + 2k_3$, $\beta = 1 - 2j_3 + k_3$. Then, from (3), $\mathrm{n}(\alpha) = \mathrm{n}(\beta) = 16$. Hence $\alpha, \beta \in \mathrm{U}(R)$. Let $G = \langle \alpha, \beta \rangle$. Using the embedding $\varepsilon : R \to \mathbb{H}$ defined by (2) we obtain an embedding of G into $\mathrm{U}(\mathbb{H})$. Now, as in §2 of [2], we can apply a result of Świerczkowski to show that the group $\varepsilon(G)$ is free nonabelian with free generators $\varepsilon\alpha$ and $\varepsilon\beta$. Hence $G \simeq \mathcal{F}$.

2. Cayley numbers. In this section $\mathrm{C}(A)$ denotes the ring of classical Cayley numbers over a ring A. Hence $\mathrm{C}(A) = \mathrm{H}(A) \oplus \mathrm{H}(A)e$, where

$$(a + be)(c + de) = ac - b\overline{d} + (ad + b\overline{c})e \tag{4}$$

for all $a, b, c, d \in \mathrm{H}(A)$. Under this multiplication $\mathrm{C}(A)$ is an alternative ring, in which the set $\mathrm{U}(\mathrm{C}(A))$ of invertible elements is a Moufang loop (for details see [1]). Hence, any two-generated subloop of $\mathrm{U}(\mathrm{C}(A))$ is a subgroup.

We need the following classical result of Gauss in number theory (see [4, p. 45]):

LEMMA 2.1. *Let $n \in \mathbb{N}$. Then n can be represented as a sum of three squares of nonnegative integers if and only if n is not of the form $2^k(8l+7)$, where $k, l \geq 0$, $k, l \in \mathbb{Z}$.*

THEOREM 2.2. *Let $A \subseteq \mathbb{Q}$ be a subring and let $a, b \in A$ be positive numbers. Then there exists an A-algebra embedding of $\mathrm{H}(A, a, b)$ into $\mathrm{C}(A)$.*

Proof. By Proposition 1.2 we can assume that $a, b \in \mathbb{N}$ and are square free.

First let $a = a_1^2 + a_2^2 + a_3^2$ and $b = b_0^2 + b_1^2 + b_2^2 + b_3^2$, where all a_r, b_s are nonnegative integers. Consider the A-module mapping φ of $\mathrm{H}(A, a, b)$ into $\mathrm{C}(A)$ such that $\varphi(1) = 1$ and

$$\varphi(i_a) = a_1 i + a_2 j + a_3 k, \qquad \varphi(j_b) = (b_0 + b_1 i + b_2 j + b_3 k)e,$$
$$\varphi(k_{ab}) = \varphi(i_a)\varphi(j_b).$$

With the help of (4) and (1) it can be checked that φ is an embedding of A-algebras.

If b is a sum of three squares in $\mathbb{Z}$, then it is enough to observe first that $\mathrm{H}(A, a, b) \simeq \mathrm{H}(A, b, a)$ and then to apply the previous case.

Finally, suppose neither a nor b is a sum of three squares of nonnegative integers. We can also assume that $a \leq b$. Because a and b are square free, by Lemma 2.1 we have $a \equiv 7 \bmod 8$ and $b \equiv 7 \bmod 8$. By the Legendre Four Square Theorem (see [5, 4]) and our assumption we know that a is a sum of four squares in $\mathbb{N}$. Write

$$a = a_1^2 + a_2^2 + a_3^2 + a_4^2.$$

It is easy to check that two a_i's, say a_3 and a_4, are odd. Set $c = b - (a_3^2 + a_4^2)$. Then $c \in \mathbb{N}$ and it is congruent to 5 modulo 8. Hence, by Lemma 2.1 we can write $c = c_1^2 + c_2^2 + c_3^2$ and consequently

$$b = a_3^2 + a_4^2 + c_1^2 + c_2^2 + c_3^2.$$

Now we can define an A-module mapping φ of $\mathrm{H}(A, a, b)$ into $\mathrm{C}(A)$ by

$$\varphi(1) = 1, \quad \varphi(i_a) = a_1 i + a_2 j + a_3 k + a_4 e,$$
$$\varphi(j_b) = -a_4 k + (a_3 + c_1 i + c_2 j + c_3 k)e, \quad \varphi(k_{ab}) = \varphi(i_a)\varphi(j_b).$$

Using (4) and (1) it can be checked that φ is an embedding of A-algebras. ∎

As a consequence of the above theorem, Theorem 1.1 and Example 1.6 we obtain the following result, answering in particular a question from [2, p. 27].

Corollary 2.3. *Let $\mathbb{Z} \subset A \subseteq \mathbb{Q}$ be a subring. Then $\mathcal{F} \subseteq \mathrm{U}(\mathrm{C}(A))$.*

Remark. From Theorem 1.1, Example 1.6 and [2] it is visible that there is an effective construction of $\mathcal{F} \subseteq \mathrm{C}(A)$ for any $\mathbb{Z} \subset A \subseteq \mathbb{Q}$.

REFERENCES

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

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

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

[4] J.-P. Serre, *Cours d'arithmétique*, Presses Univ. de France, Paris, 1970.

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

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

Received 14 March 2003 (4329)