PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 143, Number 2, February 2015, Pages 459–468
S 0002-9939(2014)12230-1
Article electronically published on October 1, 2014

EXPLICIT FREE GROUPS IN DIVISION RINGS

J. Z. GONÇALVES AND D. S. PASSMAN

(Communicated by Lev Borisov)

Abstract. Let D be a division ring of characteristic $\neq 2$ and suppose that the multiplicative group $D^\bullet = D \setminus \{0\}$ has a subgroup G isomorphic to the Heisenberg group. Then we use the generators of G to construct an explicit noncyclic free subgroup of $D^\bullet$. The main difficulty occurs here when D has characteristic 0 and the commutators in G are algebraic over $\mathbb{Q}$.

1. Introduction

Let D be a noncommutative division ring with multiplicative group $D^\bullet = D\setminus\{0\}$. A longstanding conjecture of Lichtman [5] asserts

Conjecture 1.1. *$D^\bullet$ contains a free noncyclic subgroup.*

A great deal of progress has been made on this problem in [1, 2, 6, 7]. See [3] for a more detailed account. Unfortunately, there are some shortcomings to these results. The first is that each one holds only for certain families of division rings due to the fact that we do not know how to generate all of them. The second is that many of the proofs are existential and do not actually exhibit the free subgroup. It is this second problem that we address here.

As a partial answer to a question posed by J. Lewin, reference [1] proved

Theorem 1.2. *Let k be a field of characteristic $\neq 2$, let G be a torsion free nilpotent group of class 2 and let $D = Q(kG)$ be the division ring of fractions of the group algebra kG. If x and y are any pair of noncommuting elements of G, and if $\alpha, \beta \in k^\bullet$, then the subgroup $\langle 1 + \alpha x, 1 + \beta y\rangle$ is free of rank 2.*

With this, it is natural to ask whether a division ring D that is generated over its center by a torsion free nilpotent group $G \subseteq D^*$ has a free subgroup of rank 2 that can be described as above. More precisely, if x and y are suitable noncommuting elements of G, do $1 + x$ and $1 + y$ generate a free subgroup?

Now suppose G is any noncommutative torsion free nilpotent group and choose x in the second center $\mathfrak{Z}_2(G)$ but not in the center $\mathfrak{Z}(G)$. Then there exists $y \in G$ that does not commute with x, so the commutator $[x, y]$ is not 1. Furthermore, since $x \in \mathfrak{Z}_2(G)$, we see that $[x, y] \in \mathfrak{Z}(G)$ commutes with both x and y. Of course,

Received by the editors February 27, 2013.
2010 *Mathematics Subject Classification.* Primary 16K40; Secondary 20C07.
The first author's research was supported in part by Grant CNPq 300.128/2008-8 and by Fapesp-Brazil, Proj. Tematico 2009/52665-0.

since G is torsion free, $[x, y]$ has infinite multiplicative order. In particular, the hypotheses of the following theorem are satisfied if $G \subseteq D^\bullet$. The goal of this paper is to prove

Theorem 1.3. *Let D be a division ring of characteristic different from 2, and assume that $D^\bullet$ contains elements x, y with commutator $[x, y] = \lambda$ of infinite multiplicative order. Suppose also that λ commutes with both x and y.*

(i) If λ is transcendental over the prime subfield of D, then $\langle 1 + x, 1 + y\rangle$ is a free subgroup of $D^\bullet$ of rank 2.

(ii) If $\operatorname{char} D = 0$ and λ is algebraic over the rational field $\mathbb{Q}$, then there exists a nonnegative integer n such that the subgroup $\langle 1 + x^{2^n}, 1 + y\rangle$ of $D^\bullet$ is free of rank 2.

Note that if x and y satisfy the above commutator conditions, then so do αx and βy for all $\alpha, \beta \in \mathfrak{Z}(D)^\bullet$. We will prove the main result in Section 3, and as we will see, part (i) above is actually the group ring case and follows almost immediately from Theorem 1.2. Thus only Theorem 1.3(ii) is really new.

2. Some necessary number theory

We first consider certain absolute value inequalities in the complex numbers $\mathbb{C}$. As usual, in this section, we write i for $\sqrt{-1}$. To begin with, we need

Lemma 2.1. *For any real angle θ and any $n \geq 1$, we have $|\sin 2^n\theta| \leq 2^n\,|\cos\theta|$.*

Proof. Since $\sin 2\theta = 2\sin\theta\cos\theta$, the case $n = 1$ follows from $|\sin\theta| \leq 1$. Furthermore, since $|\cos\theta| \leq 1$, the double angle formula also yields $|\sin 2\theta| \leq 2|\sin\theta|$. Applying the latter iteratively, we obtain $|\sin 2^n\theta| \leq 2^{n-1}|\sin 2\theta| \leq 2^n|\cos\theta|$. □

Next, we observe

Lemma 2.2. *Suppose $\lambda_1, \lambda_2, \ldots, \lambda_s \in \mathbb{C}$ all have absolute value 1 and define*

$$f(n) = \prod_{j=1}^{s} |\lambda_j^{2^n} + 1|$$

for all $n \geq 0$. Then:

(i) There exists $n \leq s + 1$ with $f(n) \geq 2^{-s^2}$.

(ii) There are infinitely many n with $f(n) \geq 2^{-s^2}$.

Proof. (i) Note that this result holds vacuously for $s = 0$ since the value of an empty product is 1. Thus we can assume that $s \geq 1$. Since $|\lambda_j| = 1$, we can write $\lambda_j = e^{i\theta_j}$ for some real angle θ_j. Also note that for any $n \geq 0$, we have

$$\begin{aligned} |\lambda_j^{2^{n+1}} + 1| &= |\lambda_j^{-2^n}|\cdot|\lambda_j^{2^{n+1}} + 1| = |\lambda_j^{2^n} + \lambda_j^{-2^n}| \\ &= |e^{i2^n\theta_j} + e^{-i2^n\theta_j}| = |2\cos 2^n\theta_j|. \end{aligned}$$

Suppose by way of contradiction that $f(n) < 2^{-s^2}$ for all $n = 1, 2, \ldots, s + 1$. Then by the above we have

$$(*) \qquad 2^{-s^2} > f(n+1) = \prod_{j=1}^{s} |2\,\cos 2^{n+1}\theta_j|$$

for all $n = 0, 1, \ldots, s$.

Claim. Suppose that for some integer n with $0 \le n \le s$ we have $|\cos 2^j\theta_j| \le 2^{-s-1}$ for all $j = 1, 2, \ldots, n$, where the hypothesis is vacuous when $n = 0$. Then $n \le s-1$ and by suitably relabeling the remaining θ's, we have $|\cos 2^{n+1}\theta_{n+1}| \le 2^{-s-1}$.

Proof. Now for each $j = 1, 2, \ldots, n$, since $j < n+1$, Lemma 2.1 implies that

$$|\sin 2^{n+1}\theta_j| = |\sin 2^{(n+1-j)}2^j\theta_j| \le 2^{(n+1-j)} \cdot |\cos 2^j\theta_j| \le 2^{(n+1-j)}2^{-s-1},$$

by hypothesis. Furthermore, $(n+1-j)-(s+1) \le (n-s)-1 \le -1$ since $n \le s$. Thus $|\sin 2^{n+1}\theta_j| \le 1/2$ and therefore $|\cos 2^{n+1}\theta_j| \ge \sqrt{3}/2 \ge 1/2$. It follows that $|2\cos 2^{n+1}\theta_j| \ge 1$ for all $j = 1, 2, \ldots, n$, so equation $(*)$ becomes

$$2^{-s^2} \ge \prod_{j=1}^{n} |2\cos 2^{n+1}\theta_j| \cdot \prod_{j=n+1}^{s} |2\cos 2^{n+1}\theta_j| \ge \prod_{j=n+1}^{s} |2\cos 2^{n+1}\theta_j|.$$

We conclude that the final product is nonempty and hence $n \le s-1$. Furthermore, by relabeling, we can assume that the smallest factor in that nonempty right-hand product occurs when $j = n+1$, and of course this factor must be ≤ 1. Thus

$$2^{-s^2} \ge |2\cos 2^{n+1}\theta_{n+1}|^{(s-n)} \ge |2\cos 2^{n+1}\theta_{n+1}|^s$$

since $(s-n) < s$ and $|2\cos 2^{n+1}\theta_{n+1}| \le 1$. Taking sth roots yields

$$2^{-s} \ge |2\cos 2^{n+1}\theta_{n+1}|,$$

so

$$2^{-s-1} \ge |\cos 2^{n+1}\theta_{n+1}|$$

thereby proving the Claim. □

With this, it is now a simple matter to complete the proof of (i). To this end, we show by induction on $n \le s$ that the angles θ_j can be suitably relabeled so that $|\cos 2^j\theta_j| \le 2^{-s-1}$ for all $j = 1, 2, \ldots, n$. Indeed, if $n = 0$, there is nothing to prove. Next, if the inductive statement holds for n, then it holds for $n+1$ by the above Claim. Thus we conclude that the inductive statement holds for all j, that is, for $n = s$. But then, by the Claim again, $n \le s-1$ and this is a contradiction.

(ii) Here we let a be any nonnegative integer and notice that for all j we have $|\lambda_j^{2^a}| = 1$ and $(\lambda_j^{2^a})^{2^b} = \lambda_j^{2^{a+b}}$. Thus, by applying (i) to $\lambda_1^{2^a}, \lambda_2^{2^a}, \ldots, \lambda_s^{2^a}$, we see that there exists $0 \le n' \le s+1$ with $f(a+n') \ge 2^{-s^2}$. By varying a appropriately, we clearly obtain infinitely many integers n with $f(n) \ge 2^{-s^2}$. □

With this, we can easily prove

Lemma 2.3. *Let $\lambda_1, \lambda_2, \ldots, \lambda_m \in \mathbb{C}$ and define*

$$f(n) = \prod_{j=1}^{m} |\lambda_j^{2^n} + 1|$$

for all $n \ge 0$. Then:

- *(i) There exists a positive constant C, depending upon the λ_j's, such $f(n) \ge C$ occurs for infinitely many n.*
- *(ii) If some λ_j has absolute value > 1, then the function $f(n)$ is unbounded.*

Proof. (i) We divide the subscripts j into three sets $\mathcal{R}$, $\mathcal{S}$ and $\mathcal{T}$, corresponding to whether $|\lambda_j| < 1$, $|\lambda_j| = 1$ or $|\lambda_j| > 1$, respectively. If $|\mathcal{S}| = s$, then the preceding lemma implies that the inequality

$$\prod_{j\in\mathcal{S}} |\lambda_j^{2^n} + 1| \geq 2^{-s^2}$$

holds for infinitely many n.

Next, let $|\mathcal{R}| = r$ and let ρ be the maximum of $|\lambda_j|$ with $j \in \mathcal{R}$. Then $\rho < 1$ and $|\lambda_j^{2^n}| \leq \rho$ for all $j \in \mathcal{R}$ and all $n \geq 0$. Thus $|\lambda_j^{2^n} + 1| \geq 1 - |\lambda_j^{2^n}| \geq 1 - \rho$, and hence we have

$$\prod_{j\in\mathcal{R}} |\lambda_j^{2^n} + 1| \geq (1-\rho)^r$$

for all $n \geq 0$. Of course, this is satisfied when $r = 0$ by choosing $1 - \rho = 1$.

Finally, let $|\mathcal{T}| = t$ and let τ be the minimum of $|\lambda_j|$ with $j \in \mathcal{T}$. Then $\tau > 1$ and $|\lambda_j^{2^n}| \geq \tau$ for all $j \in \mathcal{T}$ and all $n \geq 0$. Thus $|\lambda_j^{2^n} + 1| \geq |\lambda_j^{2^n}| - 1 \geq \tau - 1$, and hence we have

$$\prod_{j\in\mathcal{T}} |\lambda_j^{2^n} + 1| \geq (\tau-1)^t$$

for all $n \geq 0$. Again, this is satisfied when $t = 0$ by taking $\tau - 1 = 1$.

Now write $C = (1-\rho)^r \cdot 2^{-s^2} \cdot (\tau-1)^t$ so that $C > 0$. Then, by multiplying the three displayed inequalities above, we conclude that $f(n) \geq C$ occurs infinitely often.

(ii) We can suppose that $|\lambda_m| > 1$ and let $D > 0$ be the constant given by (i) for the product

$$g(n) = \prod_{j=1}^{m-1} |\lambda_j^{2^n} + 1|.$$

Then, for any n with $g(n) \geq D$, we have

$$f(n) = g(n) \cdot |\lambda_m^{2^n} + 1| \geq D \cdot (|\lambda_m|^{2^n} - 1).$$

Since $|\lambda_m| > 1$ and since the above inequality is satisfied for infinitely many n, we conclude that $f(n)$ is unbounded. □

Now let K be a finite Galois extension of the rationals $\mathbb{Q}$. Say $|K : \mathbb{Q}| = m$ and let $G = \mathrm{Gal}(K/\mathbb{Q})$. Then the Galois norm $N\colon k \mapsto \prod_{\sigma\in G} k^\sigma$ is a multiplicative homomorphism from $K^\bullet$ to $\mathbb{Q}^\bullet$. Furthermore, N sends the ring of algebraic integers $\mathcal{O}_K$ to the ring of ordinary integers $\mathbb{Z}$. We fix an embedding of K into the complex numbers $\mathbb{C}$, so we can speak about the absolute values of elements of K. We can now translate the preceding lemma into a norm inequality since the norm is a product of $m = |G|$ factors.

Lemma 2.4. *Let $\alpha \in K$, a finite Galois extension of $\mathbb{Q}$.*

- *(i) There exists a positive constant C depending on α such that the inequality $|N(\alpha^{2^n} + 1)| \geq C$ holds for infinitely many $n \geq 0$.*
- *(ii) If some Galois conjugate of α has absolute value > 1, then $|N(\alpha^{2^n} + 1)|$ is unbounded as a function of n.*

Proof. If $\lambda_1, \lambda_2, \ldots, \lambda_m$ are the m Galois conjugates of α, then $\lambda_1^{2^n}, \lambda_2^{2^n}, \ldots, \lambda_m^{2^n}$ are the Galois conjugates of α^{2^n}. Thus

$$|N(\alpha^{2^n}+1)| = \prod_{j=1}^{m} |\lambda_j^{2^n}+1|$$

and the result follows immediately from Lemma 2.3. □

As a first consequence of the multiplicative nature of the norm map, we have

Lemma 2.5. *Let $\alpha, \beta \in K$. If either $|N(\alpha)| > 1$ or $|N(\beta)| > 1$, then $|N(\alpha^{2^n}+\beta^{2^n})|$ is unbounded as a function of n.*

Proof. By symmetry we can assume that $|N(\beta)| > 1$ and we write $\gamma = \alpha\beta^{-1} \in K$. Then $\alpha^{2^n} + \beta^{2^n} = (\gamma^{2^n}+1)\beta^{2^n}$, so

$$|N(\alpha^{2^n}+\beta^{2^n})| = |N(\gamma^{2^n}+1)| \cdot |N(\beta)|^{2^n}.$$

Now Lemma 2.4(i) implies that there exists a constant $C > 0$ with $|N(\gamma^{2^n}+1)| \geq C$ for infinitely many $n \geq 0$. Thus since $|N(\beta)|^{2^n}$ is strictly increasing and unbounded, the result follows from the above displayed inequality. □

Now we consider algebraic integers and, for convenience, we write $R = \mathcal{O}_K$. Since the expression $|N(\alpha^{2^n}+\beta^{2^n})|$ is easy to understand if either α or β is zero, we can assume that they are both nonzero. Notice also that if α and β are units of $\mathcal{O}_K$ and if $\alpha\beta^{-1} = \varepsilon$ is a root of unity, then $|N(\alpha)| = |N(\beta)| = 1$ and

$$|N(\alpha^{2^n}+\beta^{2^n})| = |N(\varepsilon^{2^n}+1)| \cdot |N(\beta)|^{2^n} = |N(\varepsilon^{2^n}+1)|$$

takes on only finitely many values and hence is bounded as a function of n. As we see below, this is the only situation where boundedness can occur.

Proposition 2.6. *Let $0 \neq \alpha, \beta$ be algebraic integers in the finite Galois extension K of $\mathbb{Q}$. Then $|N(\alpha^{2^n}+\beta^{2^n})|$ is unbounded as a function of n unless α and β are both units in $\mathcal{O}_K$ with $\alpha\beta^{-1}$ a root of unity.*

Proof. Let us assume that $|N(\alpha^{2^n}+\beta^{2^n})|$ is bounded as a function of n. Since $0 \neq \alpha, \beta \in \mathcal{O}_K$, we know that $0 \neq N(\alpha), N(\beta) \in \mathbb{Z}$. If either $|N(\alpha)| > 1$ or $|N(\beta)| > 1$, then the function is unbounded by Lemma 2.5. Thus we must have $|N(\alpha)| = |N(\beta)| = 1$ and hence both α and β are units in $\mathcal{O}_K$. Furthermore, if $\varepsilon = \alpha\beta^{-1} \in \mathcal{O}_K$, then

$$|N(\alpha^{2^n}+\beta^{2^n})| = |N(\varepsilon^{2^n}+1)| \cdot |N(\beta)|^{2^n} = |N(\varepsilon^{2^n}+1)|.$$

In particular, since this is bounded, Lemma 2.4(ii) implies that all of the Galois conjugates of ε have absolute value ≤ 1. But $|N(\varepsilon)| = 1$ so the Galois conjugates of the algebraic integer ε all have absolute value 1. As is well known, this implies that ε is a root of unity. □

For $\alpha, \beta \in R$, let us write

$$\gamma_n = \alpha^{2^n} + \beta^{2^n}$$

for all integers $n \geq 0$. Furthermore, we say that α and β are comaximal if $R = (\alpha, \beta) = R\alpha + R\beta$.

Lemma 2.7. *Let $\alpha, \beta \in R$ and let P be a nonzero prime ideal of the ring R with $\gamma_r, \gamma_s \in P^a$ for some $a \geq 1$ and $r \neq s$. If α and β are comaximal, then $2 \in P^a$.*

Proof. Suppose by way of contradiction that $2 \notin P^a$, so that $1 \not\equiv -1 \bmod P^a$. By comaximality, we have $(\alpha, \beta) \not\subseteq P$, so say $\alpha \notin P$. Now the ring $\overline{R} = R/P^a$ is local with unique maximal ideal $\overline{P} = P/P^a$. Since $\bar{\alpha} \notin \overline{P}$, we see that $\bar{\alpha}$ is invertible in $\overline{R}$ and we can set $\bar{\delta} = \bar{\beta}/\bar{\alpha} \in \overline{R}$.

Now $\gamma_r \in P^a$ implies that $\beta^{2^r} \equiv -\alpha^{2^r} \bmod P^a$ and hence $\bar{\delta}^{2^r} = -1$ in $\overline{R}$. In particular, $\bar{\delta}$ is a unit in $\overline{R}$ whose order divides 2^{r+1}. But $\bar{\delta}^{2^r} = -1 \neq 1$, so the order of $\bar{\delta}$ is precisely 2^{r+1}. Similarly, if $\gamma_s \in P^a$, then $\bar{\delta}$ has order 2^{s+1} in $\overline{R}$. Thus $2^{r+1} = 2^{s+1}$ and $r = s$, a contradiction. □

With this, we can prove

Lemma 2.8. *Let K be a finite Galois extension of $\mathbb{Q}$ and let $0 \neq \alpha, \beta \in \mathcal{O}_K$. Assume that α and β are not both units of $\mathcal{O}_K$ with $\alpha\beta^{-1}$ a root of unity. If α and β are comaximal in $\mathcal{O}_K$, then there exist infinitely many nonzero prime ideals P of $\mathcal{O}_K$ that contain γ_n for some n.*

Proof. As above, we write $R = \mathcal{O}_K$ and let the prime factorization of the principal ideal (2) be given by

$$(2) = P_1^{e_1} P_2^{e_2} \cdots P_k^{e_k}.$$

Of course, in this Galois situation, all e_i are equal. If P is a prime ideal of R and $2 \in P^a$ for some integer $a \geq 1$, then $P^a \mid (2)$, so $P = P_i$ for some i and $a \leq e_i$. Since α and β are comaximal, it therefore follows from the preceding lemma that there is at most one subscript n_i with $\gamma_{n_i} \in P_i^{e_i+1}$.

If I is any proper ideal of R, write $\mathfrak{N}(I) = |R/I|$. As is well known (see [4]), $\mathfrak{N}(IJ) = \mathfrak{N}(I)\cdot\mathfrak{N}(J)$. Furthermore, if $I = (\eta)$ is principal, the $\mathfrak{N}(I) = |N(\eta)|$, where N is the Galois norm.

Now let $n \neq n_1, n_2, \ldots, n_k$. If $\gamma_n \in P_i^{f_i}$ with f_i maximal, then by definition of n_i we have $f_i \leq e_i$. In particular,

$$(\gamma_n) = J_n \cdot \prod_{i=1}^{k} P_i^{f_i}$$

for some ideal J_n not divisible by $P_1, P_2, \ldots,$ or P_k. Thus since $\prod_{i=1}^{k} P_i^{f_i} \mid (2)$, we see that $|N(\gamma_n)| \leq |N(2)|\cdot\mathfrak{N}(J_n) = 2^m \cdot \mathfrak{N}(J_n)$.

By the hypothesis and Proposition 2.6, there are infinitely many n with $|N(\gamma_n)| > 2^m$. For each of these, we see that J_n is a proper ideal of R and hence has a nontrivial prime factor $Q_n \neq P_1, P_2, \ldots, P_k$. Of course, $Q_n \supseteq J_n \supseteq (\gamma_n)$ so $\gamma_n \in Q_n$. Finally, the various Q_n obtained in this way are all distinct since otherwise $\gamma_n, \gamma_t \in Q_n$ and hence $2 \in Q_n$, by Lemma 2.7 again, contradicting the fact that $Q_n \neq P_1, P_2, \ldots, P_k$. □

Finally, we handle arbitrary finite degree field extensions of $\mathbb{Q}$ and almost arbitrary algebraic integers α and β. We do this by extending the field in two different ways.

Theorem 2.9. *Let K be a finite degree field extension of $\mathbb{Q}$ and let $0 \neq \alpha, \beta \in R = \mathcal{O}_K$. Assume that $\alpha/\beta \in K$ is not a root of unity. Then there exist infinitely many nonzero prime ideals P of R that contain $\gamma_n = \alpha^{2^n} + \beta^{2^n}$ for some $n \geq 0$.*

Proof. By [8, Theorem 9.12], there exists a finite degree extension field F of K with $S = \mathcal{O}_F$ such that the ideal $\alpha S + \beta S = \eta S$ is principal. Then $\alpha/\eta, \beta/\eta \in S$ and

$\eta = \alpha x + \beta y$ for some $x, y \in S$. Thus $(\alpha/\eta)x + (\beta/\eta)y = 1$, so α/η and β/η are comaximal in S. Also $(\alpha/\eta)/(\beta/\eta) = \alpha/\beta$ is not a root of unity.

Next, we extend F to its Galois closure E over $\mathbb{Q}$, so $|E : \mathbb{Q}| < \infty$, and we set $T = \mathcal{O}_E \supseteq S$. Then α/η and β/η are comaximal in T and the previous lemma implies that there exists infinitely many nonzero prime ideals Q of T, each containing $(\alpha/\eta)^{2^n} + (\beta/\eta)^{2^n}$ for some n. Multiplying by η^{2^n}, we see that each Q contains $\gamma_n = \alpha^{2^n} + \beta^{2^n}$ for some $n \geq 0$.

But $\gamma_n \in R$, so $\gamma_n \in R \cap Q = P$, a nonzero prime ideal of R. Finally, since the map $Q \mapsto Q \cap R = P$ is finite-to-one by [8, Theorem 5.17], we obtain in this way infinitely many distinct nonzero prime ideals P of R that contain γ_n for some integer n. □

3. Proof of the main result

The proof of Theorem 1.3 is similar to that of Theorem 1.2. Roughly speaking, we first see how x and y are embedded in D. In particular, we find a nice subring S of D that contains x, y, $(1+x)^{-1}$ and $(1+y)^{-1}$. Then we construct a homomorphism $\bar{}$ from S to a division ring $\overline{Q}$ where we know that $1 + \bar{x}$ and $1 + \bar{y}$ generate a free group of rank 2. The division ring $\overline{Q}$ will be a suitable quaternion algebra.

Let F be a field of characteristic different from 2 and let $0 \neq a, b \in F$. Recall that the quaternion algebra $\frac{(a,b)}{F}$ is the 4-dimensional F-algebra with F-basis $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ and with multiplication determined by

$$\mathbf{i}^2 = a, \qquad \mathbf{j}^2 = b, \qquad \mathbf{ij} = -\mathbf{ji} = \mathbf{k}.$$

Of course, the algebra $\frac{(a,b)}{F}$ need not be a division ring in general. The following is [1, Proposition 16].

Theorem 3.1. *Let F_0 be a field of characteristic $\neq 2$ and let $F = F_0(a, b)$ be a function field in the variables a and b. Then $1+\mathbf{i}$ and $1+\mathbf{j}$ generate a free subgroup of rank 2 in the multiplicative group of the quaternion division algebra $\frac{(a,b)}{F}$.*

If S is a ring, then an ideal P of S is said to be completely prime if S/P is a domain. Equivalently, this occurs if $st \in P$ implies that s or t is in P, and again this is equivalent to $M = S \setminus P$ being a multiplicatively closed subset of S. The following argument is from [6]. It is proved by considering the π-adic valuation.

Lemma 3.2. *Let S be a right Ore domain and let $0 \neq \pi$ be a central element of the ring. Assume that $P = \pi S$ is a completely prime ideal of S and that $\bigcap_{n=0}^{\infty} \pi^n S = 0$. Then $M = S \setminus P$ is a multiplicatively closed right divisor set in S.*

Proof. We know that M is multiplicatively closed. If $0 \neq s \in S$, then there exists an integer n with $s \in \pi^n S \setminus \pi^{n+1} S$ and hence $s = \pi^n m$ for some $m \in M$. Since S is a domain, cancellation holds and it is easy to see that this expression for s is unique. In other words, every $0 \neq s \in S$ can be written uniquely as $s = \pi^{\nu(s)}\mu(s)$ with $\mu(s) \in M$. Furthermore, if $0 \neq s, t \in S$, then

$$st = \pi^{\nu(s)}\mu(s) \cdot \pi^{\nu(t)}\mu(t) = \pi^{\nu(s)+\nu(t)}\mu(s)\mu(t).$$

Since $\mu(s)\mu(t) \in M$, uniqueness implies that $\mu(st) = \mu(s)\mu(t)$.

We show now that S satisfies the right divisor condition with respect to M. To this end, let $0 \neq s \in S$ and let $m \in M$. Since S is a right Ore domain, there exist

$0 \neq r, t \in S$ with $sr = mt$. Applying μ yields $\mu(s)\mu(r) = m\mu(t)$ and hence

$$s\mu(r) = \pi^{\nu(s)}\mu(s)\mu(r) = m\pi^{\nu(s)}\mu(t).$$

Thus $sm_1 = ms_1$ with $m_1 = \mu(r) \in M$ and $s_1 = \pi^{\nu(s)}\mu(t) \in S$. □

For the remainder of this paper, let D be a division ring with prime subfield k and let $x, y \in D^\bullet$ have commutator $[x, y] = \lambda$ of infinite multiplicative order. Furthermore, we suppose that λ commutes with both x and y and we let K be the field $K = k(\lambda) \subseteq D$. Recall that the Heisenberg group $\mathcal{H}$ has generators X, Y and Z with relations $[X, Z] = [Y, Z] = 1$ and $[X, Y] = Z$. Part (i) below is not really needed, but it does explain the hypotheses in Theorem 1.3. Part (ii) is a simple special case of work of Zalesskiĭ in [9].

Lemma 3.3. *Let $x, y, \lambda \in D^\bullet$ and let $K \subseteq D$ be as above.*

(i) The subgroup $G = \langle x, y, \lambda \rangle$ of $D^\bullet$ is naturally isomorphic to the Heisenberg group $\mathcal{H}$.

(ii) The monomials $x^r y^s \in D$, for all $r, s \in \mathbb{Z}$, are linearly independent over K.

Proof. (i) The map $\theta\colon \mathcal{H} \to G$ given by $X \mapsto x$, $Y \mapsto y$ and $Z \mapsto \lambda$ is clearly a well-defined group epimorphism. Furthermore, θ is one-to-one when restricted to $\mathfrak{Z}(\mathcal{H}) = \langle Z \rangle$ since λ has infinite multiplicative order. In particular, since any nontrivial normal subgroup of $\mathcal{H}$ meets $\mathfrak{Z}(\mathcal{H})$ nontrivially, we conclude that $\ker\theta = \langle 1 \rangle$ and hence that θ is an isomorphism.

(ii) The commutator relations on x and y imply that $x^y = y^{-1}xy = \lambda x$ and $y^x = x^{-1}yx = \lambda^{-1}y$. Thus since x and y commute with λ we have $(x^i)^y = \lambda^i x^i$ and $(y^j)^x = \lambda^{-j} y^j$. If the monomials $x^r y^s$ are linearly dependent over K, let

$$(**) \qquad \sum_{r,s} a_{r,s} x^r y^s = 0$$

be a dependence relation, with $a_{r,s} \in K$, involving the smallest number of nonzero coefficients $a_{r,s}$. Multiplying by a suitable $x^i y^j$, we can assume that $a_{0,0} \neq 0$.

Conjugating equation $(**)$ by y and subtracting yields

$$\sum_{r,s} (1 - \lambda^r) a_{r,s} x^r y^s = 0,$$

a dependence relation with a smaller number of terms since the $0, 0$-term no longer occurs. Thus $(1 - \lambda^r)a_{r,s} = 0$ and since λ has infinite multiplicative order, we conclude that $a_{r,s} = 0$ if $r \neq 0$.

Similarly, conjugating $(**)$ by x and subtracting yields

$$\sum_{r,s} (1 - \lambda^{-s}) a_{r,s} x^r y^s = 0$$

and hence $a_{r,s} = 0$ if $s \neq 0$. It follows that equation $(**)$ reduces to a single term $a_{0,0}x^0y^0 = 0$, certainly a contradiction. □

With this, we can now prove the main result.

Proof of Theorem 1.3. (i) Suppose that λ is transcendental over k, the prime subfield of D. Then the preceding lemma implies that the elements $x^r y^s \lambda^t$ are linearly independent over k and therefore the group algebra kG is embedded in D. Since kG is a Noetherian domain, it follows that its division ring of quotients $Q(kG)$ also embeds in D. But G is nilpotent of class 2, so Theorem 1.2 yields the result.

(ii) Here we assume that $\operatorname{char} D = 0$, so $k = \mathbb{Q}$ is the field of rational numbers. Also λ is algebraic over $\mathbb{Q}$ so $K = \mathbb{Q}(\lambda)$ is a finite degree extension field of $\mathbb{Q}$, an algebraic number field. If $R = \mathcal{O}_K$, then we can write $\lambda = \alpha/\beta$ for suitable $0 \neq \alpha, \beta \in R$. As in the previous section, for each integer $n \geq 0$, we set $\gamma_n = \alpha^{2^n} + \beta^{2^n} \in R$. Then, by Theorem 2.9, since λ is not a root of unity, there exist infinitely many distinct nonzero prime ideals of R that contain some γ_n. In particular, we can choose a nonzero prime ideal P of R with $2, \alpha, \beta \notin P$ but with $\gamma_n \in P$ for a fixed $n \geq 0$. Say P lies over the rational prime p, so that $p \neq 2$.

Let $\widetilde{R} = R_P$ be the localization of R at P. Then β is a unit in $\widetilde{R}$, so $\lambda = \alpha/\beta \in \widetilde{R}$. Also $\alpha^{2^n} + \beta^{2^n} \in P$, so $\lambda^{2^n} + 1 = (\alpha^{2^n} + \beta^{2^n})/\beta^{2^n} \in \widetilde{P} = P\widetilde{R}$, the unique nonzero prime ideal of $\widetilde{R}$. Since $x^r y^s \cdot x^{r'} y^{s'} \in \widetilde{R} x^{r+r'} y^{s+s'}$, it follows from Lemma 3.3(ii) that

$$\widetilde{S} = \oplus \sum_{r,s \geq 0} \widetilde{R} x^r y^s$$

is a subring of D. Indeed, $\widetilde{S}$ is clearly the skew polynomial ring over $\widetilde{R}$ generated by x and y and subject to the single relation $xy = \lambda yx$.

Set $z = x^{2^n}$ so that $y^{-1} z y = \lambda^{2^n} z$ and let S be the $\widetilde{R}$-subalgebra of $\widetilde{S}$ given by

$$S = \oplus \sum_{r,s \geq 0} \widetilde{R} z^r y^s.$$

Then S is clearly the skew polynomial ring over $\widetilde{R}$ generated by z and y and subject to the single relation $zy = \lambda^{2^n} yz$. Note that S is a Noetherian domain and hence an Ore domain.

Recall that $\widetilde{P} = P\widetilde{R} \lhd \widetilde{R}$ and note that $\widetilde{P}S = \oplus \sum_{r,s \geq 0} \widetilde{P} z^r y^s$ is an ideal of S. If $\bar{}: S \to \overline{S} = S/\widetilde{P}S$ denotes the natural homomorphism, then from the above structure, we see that $\overline{S} = \oplus \sum_{r,s \geq 0} F_0 \bar{z}^r \bar{y}^s$, where F_0 is the field $F_0 = \widetilde{R}/\widetilde{P}$ of characteristic $p > 2$. Furthermore, since $zy = \lambda^{2^n} yz$ and $\lambda^{2^n} + 1 \in \widetilde{P}$, we see that $\bar{z}\bar{y} = -\bar{y}\bar{z}$. Of course, $\overline{S}$ is a skew polynomial ring in the two variables $\bar{z}$ and $\bar{y}$ over a field, so $\overline{S}$ is a domain. In particular, $\widetilde{P}S$ is a completely prime ideal of S.

Since $\bar{z}\bar{y} = -\bar{y}\bar{z}$, we see that $a = \bar{z}^2$ and $b = \bar{y}^2$ are central in $\overline{S}$, and $F_0[a, b]$ is the polynomial ring in the two variables a and b. Thus $F_0[a, b] \subseteq F = F_0(a, b)$, the rational function field in the two variables a and b. It follows that

$$\overline{S} \subseteq F \oplus F\mathbf{i} \oplus F\mathbf{j} \oplus F\mathbf{k} = \overline{Q}$$

where $\mathbf{i} = \bar{z}$, $\mathbf{j} = \bar{y}$ and $\mathbf{k} = \bar{z}\bar{y}$. Furthermore, we have $\mathbf{i}^2 = a$, $\mathbf{j}^2 = b$ and $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$. In other words, by Theorem 3.1, $\overline{S}$ is contained in the quaternion division ring $\overline{Q} = \frac{(a,b)}{F}$ where $F = F_0(a, b)$ and $\operatorname{char} F_0 = p \neq 2$.

Since $\widetilde{P}S$ is a completely prime ideal of S, we know that $M = S \setminus \widetilde{P}S$ is a multiplicatively closed set. Furthermore, since $\widetilde{P}$ is the unique nonzero prime of $\widetilde{R}$, it follows that $\widetilde{R}$ is a valuation ring, $\widetilde{P}$ is the principal ideal $\pi\widetilde{R}$ and $\bigcap_{t=0}^{\infty} \pi^t \widetilde{R} = 0$. With this, and the fact that S is a free $\widetilde{R}$-module, we see that $\widetilde{P}S = \pi S$ and $\bigcap_{t=0}^{\infty} \pi^t S = 0$. In particular, Lemma 3.2 now implies that M is a right divisor set in S. Hence we can localize S at M to obtain the ring SM^{-1}. Of course, this ring is also contained in D. Furthermore, since $1 + z$ and $1 + y$ are contained in M, we see that they are invertible in SM^{-1}, and therefore SM^{-1} contains the multiplicative group $G = \langle 1 + z, 1 + y \rangle$.

Finally, since $\overline{Q}$ is a division ring and since M is disjoint from the kernel of $^-\colon S \to \overline{Q}$, it is easy to see that the map extends uniquely to SM^{-1}. In other words, we now have a ring homomorphism $^-\colon SM^{-1} \to \overline{Q}$. Under this map, $1+z \mapsto 1+\mathbf{i}$ and $1+y \mapsto 1+\mathbf{j}$. But we know from Theorem 3.1 that the group $\overline{G} = \langle 1+\mathbf{i}, 1+\mathbf{j}\rangle$ is free of rank 2 and hence the same must be true of G. This completes the proof. □

References

[1] Jairo Z. Gonçalves, Arnaldo Mandel, and Mazi Shirvani, *Free products of units in algebras. I. Quaternion algebras*, J. Algebra **214** (1999), no. 1, 301–316, DOI 10.1006/jabr.1998.7680. MR1684864 (2000e:16021)

[2] Jairo Z. Gonçalves, Arnaldo Mandel, and Mazi Shirvani, *Free products of units in algebras. II. Crossed products*, J. Algebra **233** (2000), no. 2, 567–593, DOI 10.1006/jabr.2000.8440. MR1793917 (2002c:16044)

[3] J. Z. Gonçalves and M. Shirvani, *A survey on free objects in division rings and in division rings with an involution*, Comm. Algebra **40** (2012), no. 5, 1704–1723, DOI 10.1080/00927872.2011.554934. MR2924478

[4] Gerald J. Janusz, *Algebraic number fields*, 2nd ed., Graduate Studies in Mathematics, vol. 7, American Mathematical Society, Providence, RI, 1996. MR1362545 (96j:11137)

[5] A. Lichtman, *On subgroups of the multiplicative group of skew fields*, Proc. Amer. Math. Soc. **63** (1977), no. 1, 15–16. MR0447432 (56 #5744)

[6] A. I. Lichtman, *Free subgroups of normal subgroups of the multiplicative group of skew fields*, Proc. Amer. Math. Soc. **71** (1978), no. 2, 174–178. MR0480623 (58 #779)

[7] A. I. Lichtman, *On normal subgroups of multiplicative group of skew fields generated by a polycyclic-by-finite group*, J. Algebra **78** (1982), no. 2, 548–577, DOI 10.1016/0021-8693(82)90095-3. MR680374 (84f:16016)

[8] Ian Stewart and David Tall, *Algebraic number theory and Fermat's last theorem*, 3rd ed., A K Peters Ltd., Natick, MA, 2002. MR1876804 (2002k:11001)

[9] A. E. Zalesskiĭ, *The group algebras of solvable groups* (Russian), Vescī Akad. Navuk BSSR Ser. Fīz.-Mat. Navuk **1970** (1970), no. 2, 13–21. MR0289675 (44 #6863)

Department of Mathematics, University of São Paulo, São Paulo, 05508-090, Brazil
E-mail address: jz.goncalves@usp.br

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: passman@math.wisc.edu