ON MAXIMAL SUBGROUPS OF THE MULTIPLICATIVE GROUP OF A DIVISION ALGEBRA

R. HAZRAT AND A. R. WADSWORTH

Abstract. The question of existence of a maximal subgroup in the multiplicative group D^* of a division algebra D finite dimensional over its center F is investigated. We prove that if D^* has no maximal subgroup, then $\mathrm{ind}(D)$ is not a power of 2, F^{*2} is divisible, and for each odd prime p dividing $\mathrm{ind}(D)$, there exist noncyclic division algebras of degree p over F.

1. Introduction

Let D be a non-commutative division ring with center F. The structure of subgroups of the multiplicative group $D^* = D\backslash\{0\}$, in general, is unknown. Finite subgroups of D^* have been classified by Amistur [5]. Normal and subnormal subgroups of D^* have been studied over the last 70 years. Herstein ([17], 13.26) showed that the number of conjugates of a non-central element of D is infinite. (In fact it has the same cardinal number as D, [25]). This implies that a non-central normal subgroup of a division ring is "big." Confirming this, Stuth [28] proved that if an element commutes with a non-central subnormal subgroup of a division ring, then it is central. In fact he proved that if $[x, G] \subseteq F$ where G is a subnormal subgroup of D^* and $[x, G] = \{xgx^{-1}g^{-1} \mid g \in G\}$ then $x \in F$. He concluded that a subnormal subgroup of a division ring could not be solvable. Another remarkable result has recently been obtained in major work by Rapinchuk, Segev and Seitz [22]. They showed that a normal subgroup of finite dimensional division ring which has a finite quotient in D^* contains one of the groups appearing in the derived series of D^*, i.e., the quotient group itself is solvable.

Now, as with the normal subgroups, one would like to know the structure of maximal subgroups of D^* and how "big" they are in D^*. A maximal subgroup of a nilpotent group is normal. However D^* is not solvable and thus not nilpotent. Indeed, there exist division algebras which contain non-normal maximal subgroups (see Section 2 below). The recent papers [1, 2, 3, 7, 16, 18] study various aspects of maximal subgroups in the multiplicative group of a division ring. But, the question of existence of maximal subgroups in an arbitrary division ring has not been settled. The most extensive previous result in this direction was proved by Keshavarzipour and Mahdavi-Hezavehi. They showed in Cor. 2 of [16] that if D is a division algebra with center F, and with prime power index p^n, and D is not a quaternion algebra, then D^* has a maximal subgroup if $\mathrm{char}(F) = 0$ or $\mathrm{char}(F) = p$ or F contains a primitive p-th root of unity.

Date: 10 May 07.

In this note we investigate the question of existence of a maximal subgroup in the multiplicative group of a division algebra finite dimensional over its center. The general approach is to consider the K-functor $\mathrm{CK}_1(A) = \mathrm{Coker}(\mathrm{K}_1(F) \to \mathrm{K}_1(A))$ for the central simple algebra $A = M_t(D)$ with center F. Whenever F is infinite, we have $\mathrm{CK}_1(A) \cong D^*/F^{*t}D'$, where D' denotes the derived group of D^*. The group $\mathrm{CK}_1(A)$ is abelian of bounded exponent and when it is nontrivial it gives rise to (normal) maximal subgroups in D^* (see Section 2). For quaternion algebras $\mathcal{Q}$ over euclidean fields, separate treatment is required, since we'll see that $\mathrm{CK}_1(M_t(\mathcal{Q}))$ can be trivial for all t.

This paper is organized as follows: In Section 2 we examine the relation between the functor CK_1 and the maximal subgroups of multiplicative group of a division algebra. We prove that for a quaternion division algebra $\mathcal{Q}$, $\mathrm{CK}_1(M_2(\mathcal{Q}))$ is trivial if and only if $\mathcal{Q} = (\frac{-1,-1}{F})$ where F is a euclidean field, if and only if $\mathcal{Q}^*$ has no normal maximal subgroup of index 2. Using valuation theory, we also provide examples of non-normal maximal subgroups of finite index in division algebras. Indeed, for any prime power q we construct a division algebra D with center a local field F such that $D^*/F^*(1+M_D) \cong \mathcal{D}_{q+1}$, the dihedral group of order $2(q+1)$. In Section 3 we consider division algebras with no maximal subgroups. We show that the assumption of not having maximal subgroups in D^* implies very strong conditions on D and on its center (Th. 8). Finally in Section 4 we prove that every quaternion division algebra has a maximal subgroup, by reducing the problem to the existence of a maximal subgroup in a quaternion algebra over a euclidean field; we explicitly construct a (non-normal) maximal subgroup in this case. By combining the results of Sections 3 and 4, we prove:

Theorem. *Let D be a division ring finite-dimensional over its center F, and suppose D^* has no maximal subgroup. Then,*

(i) *If $\deg(D)$ is even, then $D \cong (\frac{-1,-1}{F}) \otimes_F E$, where E is a nontrivial division algebra of odd degree, and F is euclidean (so $\mathrm{char}(F) = 0$) with F^{*2} divisible.*
(ii) *If $\deg(D)$ is odd, then $\mathrm{char}(F) > 0$, $\mathrm{char}(F) \nmid \deg(D)$, and F^* is divisible.*
(iii) *In either case, there is an odd prime p dividing $\deg(D)$; for each such p, we have $[F(\mu_p) : F] \geq 4$ (so $p \geq 5$) and ${}_pBr(F)$ is generated by noncyclic algebras of degree p.*

This result guarantees the existence of a maximal subgroup for a wide range of division algebras. In particular this covers all of the cases of Cor. 2 of [16] mentioned above. It also shows that every division algebra of index $2^n, n \geq 1$ has a maximal subgroup.

Throughout this paper, all division rings are finite dimensional over their centers, hence the use of the terminology division algebras. By a maximal subgroup of a group we mean a proper subgroup which is not contained in any other proper subgroup. A normal maximal subgroup, is a maximal subgroup which is also normal.

2. The functor CK_1 and its relation with maximal subgroups

Since we are interested in the existence of maximal subgroups, we first recall what happens when the group is abelian.

Lemma 1. *Let G be an abelian group. Then,*

(i) *G has no maximal subgroups if and only if G is divisible, if and only if $G = G^p$ (i.e., G is p-divisible) for every prime number p.*
(ii) *If G is nontrivial and has bounded exponent, i.e., $G^n = 1$ for some n, then G is not divisible (so has a maximal subgroup).*

Proof. (i) If G has a maximal subgroup M, then G/M has no nontrivial subgroups, so $|G/M| = p$ for some prime number p. Then, $G^p \subseteq M \subsetneqq G$, so G is not p-divisible. Conversely, if $G \neq G^p$ for some prime p, then G/G^p is a nontrivial vector space over the field $\mathbb{Z}/p\mathbb{Z}$; so, G/G^p has a maximal proper subspace, which pulls back to a maximal subgroup of G. The rest of (i) is clear.

(ii) Suppose G is nontrivial and $G^n = 1$. Then, G has an element of order p for some prime p dividing n. If G were divisible, then G would have an element of order p^m for every positive integer m. This cannot occur, as $G^n = 1$. So, G is not divisible. □

There are several ways to attempt to construct (normal) maximal subgroups for a finite dimensional division algebra D with center F of index n. Consider the central simple algebra $A = M_t(D)$ where t is a non-negative integer. The K-group $\mathrm{CK}_1(A)$ is then defined as

$$\mathrm{CK}_1(A) \;=\; \mathrm{Coker}(\mathrm{K}_1(F) \longrightarrow \mathrm{K}_1(A)).$$

By Th. 4 (iii), p. 138 of [6], if A is different from $M_2(\mathbb{F}_2)$ then $K_1(A) \cong K_1(D)$ via the Dieudonné determinant. Since the Dieudonné determinant is the t-power map on the copy of F^* in A, whenever D is noncommutative we have,

$$\mathrm{CK}_1(A) \;\cong\; D^*/F^{*t}D' \tag{1}$$

where D^* is the multiplicative group of D and D' the derived subgroup of D^*. Thus $\mathrm{CK}_1(D)$ is a factor group of the group $\mathrm{CK}_1(A)$. Now, $x^{-n}\mathrm{Nrd}(x) \in D^{(1)}$ where Nrd is the reduced norm and $D^{(1)} = \{d \in D^* \mid \mathrm{Nrd}(d) = 1\}$. Since, further, the reduced Whitehead group $\mathrm{SK}_1(D) = D^{(1)}/D'$ is n-torsion (by [6], p. 157, Lemma 2), it follows from (1) that $\mathrm{CK}_1(D)$ is an abelian group of bounded exponent n^2. (In fact one can show that the bound can be reduced to n, see the proof of Lemma 4, p. 154 in [6] or pp. 579–580 in [8].) It thus follows from (1) that $\mathrm{CK}_1(M_t(D))$ is an abelian group of bounded exponent tn^2. Therefore, if there is a t such that $\mathrm{CK}_1(M_t(D))$ is nontrivial, then it has a normal maximal subgroup by Lemma 1(ii); thus, D^* has a normal maximal subgroup. In [9] it was conjectured that if $\mathrm{CK}_1(D)$ is trivial then D is a quaternion algebra. In [10], in an attempt to prove this conjecture, it was shown that if D is a tensor product of cyclic algebras then $\mathrm{CK}_1(D)$ is trivial if and only if D is the ordinary quaternion algebra $(\frac{-1,-1}{F})$ over a real pythagorean field F. The non-triviality of the group CK_1 and other factor groups of D^* "close" to CK_1 has been studied in [11, 10, 8, 16].

There are other ways to deduce that D^* has a maximal subgroup. For example, if there exists a surjective homomorphism from F^* to a torsion-free (abelian) group Γ such that Γ has a maximal subgroup, then one can conclude that D^* has a (normal) maximal subgroup. Indeed, let $v\colon F^* \to \Gamma$ be a surjective homomorphism. We only need to consider the case when $\mathrm{CK}_1(D)$ is trivial, i.e., $D^* = F^*D'$. Define $w\colon D^* \to \Gamma$ by $w(d) = v(f)$ where $d = fd'$, $f \in F^*$ and $d' \in D'$. If $a \in D' \cap F^*$, then $1 = \mathrm{Nrd}(a) = a^{\mathrm{ind}(D)}$. Since $D' \cap F^*$ is thus a torsion group while Γ is torsion-free, it follows that $D' \cap F^* \subseteq \ker(v)$ and that w is a well

defined surjective homomorphism. Since Γ has a maximal subgroup, it follows that D^* has a maximal subgroup. From this it follows that if the center of a division algebra D has a valuation with value group $\mathbb{Z}^n$ then D^* has a normal maximal subgroup. (The case of this with a discrete rank 1 valuation is Cor. 8 of [3].)

The approaches just described always produce normal maximal subgroups of D^* (so subgroups containing D'). However, there exist division algebras with non-normal maximal subgroups in their multiplicative groups (see Example 7 and Th. 15 below).

The observations above about CK_1 reduce the question of existence of a maximal subgroup to consideration of the case when $\mathrm{CK}_1(M_t(D))$ is trivial for every positive integer t. In fact we have the following:

Proposition 2. *Let D be a division algebra with center F. Then the following are equivalent:*

(i) *D^* has no normal maximal subgroup.*
(ii) $\mathrm{CK}_1(M_t(D)) = 1$ *for every positive integer t.*
(iii) $\mathrm{CK}_1(M_p(D)) = 1$ *for every prime p.*

Proof. (i) $\Rightarrow$ (ii). If $\mathrm{CK}_1(M_t(D))$ is nontrivial for a positive integer t, then, as pointed out above, D^* has a nontrivial abelian factor group of bounded exponent; so D^* has normal maximal subgroup by Lemma 1(ii).

(ii) $\Rightarrow$ (iii). Clear.

(iii) $\Rightarrow$ (i) (contrapositive). If D^* has a normal maximal subgroup N, then D^*/N is a group with no nontrivial subgroups; thus, $D^*/N \cong \mathbb{Z}/p\mathbb{Z}$ for some prime number p. It then follows that $F^{*p}D' \subseteq N$, so, $\mathrm{CK}_1(M_p(D))$ is nontrivial (see (1)). □

In Section 3 below we will see that the equivalent conditions on a division algebra D given in Prop. 2 yield very strong constraints on D and on its center.

While $\mathrm{CK}_1(D)$ is generally quite difficult to compute, there is a very explicit description of $\mathrm{CK}_1(\mathcal{Q})$ for a quaternion algebra $\mathcal{Q}$, which allows us to determine when $\mathcal{Q}^*$ has a normal maximal subgroup. Recall that if $\mathcal{Q}$ is a quaternion algebra over a field F with $\mathrm{char}(F) \neq 2$, then for some $a, b \in F^*$, $\mathcal{Q} \cong (\frac{a,b}{F})$, where $(\frac{a,b}{F})$ denotes the quaternion algebra over F with F-base $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ satisfying $\mathbf{i}^2 = a$, $\mathbf{j}^2 = b$, and $\mathbf{k} = \mathbf{ij} = -\mathbf{ji}$. For any $x = r + s\mathbf{i} + t\mathbf{j} + u\mathbf{k} \in (\frac{a,b}{F})$ (with $r, s, t, u \in F$), the reduced norm of x is given by

$$\mathrm{Nrd}(x) \;=\; r^2 - as^2 - bt^2 + abu^2\,. \tag{2}$$

Note that if $b \in F^{*2}$, then the quaternion algebra is split. If $\mathrm{char}(F) = 2$, then every quaternion algebra over F has the form $\left[\frac{c,b}{F}\right)$ for $c \in F$, $b \in F^*$; this is the F-algebra with F-base $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ satisfying $\mathbf{i}^2 - \mathbf{i} = c$, $\mathbf{j}^2 = b$, and $\mathbf{k} = \mathbf{ij} = \mathbf{ji} + \mathbf{j}$. Here again, if $b \in F^{*2}$ the quaternion algebra is split.

Lemma 3. *Let $\mathcal{Q}$ be a quaternion division algebra over a field F. Then, $\mathcal{Q}^*/\mathcal{Q}' \cong \mathrm{Nrd}(\mathcal{Q}^*)$ and, for every t,*

$$\mathrm{CK}_1(M_t(\mathcal{Q})) \;\cong\; \mathcal{Q}^*/F^{*t}\mathcal{Q}' \;\cong\; \mathrm{Nrd}(\mathcal{Q}^*)/F^{*2t}\,. \tag{3}$$

Proof. By definition, $\mathrm{SK}_1(\mathcal{Q}) = \mathcal{Q}^{(1)}/\mathcal{Q}'$, where $\mathcal{Q}^{(1)} = \ker(\mathrm{Nrd})$. But, since $\mathcal{Q}$ is a quaternion algebra, it is known that $\mathrm{SK}_1(\mathcal{Q})$ is trivial, see Th. 1, p. 161 in [6]. (In fact, every element of $\mathcal{Q}^{(1)}$ is a commutator.) Consequently, $\mathcal{Q}^*/\mathcal{Q}' \cong \mathrm{Nrd}(\mathcal{Q}^*)$. Since $\mathrm{Nrd}(F^{*t}) = F^{*2t}$, it follows that $\mathcal{Q}^*/F^{*t}\mathcal{Q}' \cong \mathrm{Nrd}(\mathcal{Q}^*)/F^{*2t}$. The rest of (3) is given in (1). □

Recall from the theory of ordered fields that a field F is said to be *formally real* if F admits an ordering, if and only if -1 is not a sum of squares in F. F is said to be *real pythagorean* if every sum of squares is a square in F and $-1 \notin F^{*2}$. F is said to be *euclidean* if F has an ordering with respect to which every positive element of F is a square. Clearly, if F is euclidean then F is real pythagorean and $F^* = F^{*2} \cup -F^{*2}$, so $F^2 = F^4$; furthermore, since $(\frac{a,b}{F})$ is split if $a \in F^{*2}$ or $b \in F^{*2}$ and $(\frac{a,b}{F}) \cong \left(\frac{ac^2,bd^2}{F}\right)$ for any $c, d \in F^*$, the only quaternion division algebra over F is $(\frac{-1,-1}{F})$.

Proposition 4. *Let $\mathcal{Q}$ be a quaternion division algebra with center F. Then the following are equivalent:*

(i) *$\mathcal{Q}^*$ has no subgroup of index 2.*
(ii) *The group $\mathrm{CK}_1(M_2(\mathcal{Q}))$ is trivial.*
(iii) *F is a euclidean field and $\mathcal{Q} \cong (\frac{-1,-1}{F})$.*

Proof. (i) ⇒ (ii) (contrapositive). As noted above (and explicitly clear from Lemma 3), $\mathrm{CK}_1(M_2(\mathcal{Q}))$ is a 4-torsion abelian group. If $\mathrm{CK}_1(M_2(\mathcal{Q}))$ is nontrivial, then by Lemma 1 it has a maximal subgroup N, which is necessarily normal and of prime index, say p. Since $\mathrm{CK}_1(M_2(\mathcal{Q}))/N$ is 4-torsion, we must have $p = 2$. Thus, the inverse image of N in $\mathcal{Q}^*$ has index 2 in $\mathcal{Q}^*$.

(ii) ⇒ (iii). Suppose $\mathrm{CK}_1(M_2(\mathcal{Q}))$ is trivial. Then, $\mathrm{Nrd}(Q^*) = F^{*4}$ by Lemma 3. Since $F^{*2} = \mathrm{Nrd}(F^*) \subseteq \mathrm{Nrd}(\mathcal{Q}^*) = F^{*4}$, we have $F^{*2} = F^{*4}$. If $\mathrm{char}(F) = 2$, then $F = (F^2)^{1/2} = (F^4)^{1/2} = F^2$, i.e., F is perfect. But, since $\mathcal{Q} \cong \left[\frac{c,b}{F}\right)$ and $b \in F^* = F^{*2}$, $\mathcal{Q}$ is split. This cannot occur since $\mathcal{Q}$ is assumed to be a division algebra. Hence, $\mathrm{char}(F) \neq 2$, so $\mathcal{Q} \cong (\frac{a,b}{F})$ for some $a, b \in F^*$. Since $\mathrm{Nrd}(\mathcal{Q}^*) = F^{*2}$, formula (2) shows that $-a, -b \in F^{*2}$ and every sum of squares in F is a square. Also, $-1 \notin F^{*2}$, since otherwise $b = (-1)(-b) \in F^{*2}$ and $\mathcal{Q}$ would be split. Hence, F is real pythagorean. Because $F^{*4} = F^{*2}$, for every $c \in F^*$ there is $d \in F^*$ with $c^2 = d^4$; then $c = \pm d^2$. So, $F^* = F^{*2} \cup -F^{*2}$ (a disjoint union). This shows that every positive element of F with respect to any ordering must be a square. So, F is euclidean. Therefore, as noted above, $\mathcal{Q} \cong (\frac{-1,-1}{F})$.

(iii) ⇒ (ii). Suppose F is euclidean, so $\mathcal{Q} \cong (\frac{-1,-1}{F})$. Then, by the reduced norm formula (2), $\mathrm{Nrd}(\mathcal{Q}^*) = F^{*2} = F^{*4}$, as F is euclidean. Hence, $\mathrm{CK}_1(M_2(\mathcal{Q}))$ is trivial, by Lemma 3.

(ii) ⇒ (i) (contrapositive). Suppose $\mathcal{Q}^*$ has a subgroup H of index 2. Then, H is normal in $\mathcal{Q}^*$ with $\mathcal{Q}^*/H \cong \mathbb{Z}/2\mathbb{Z}$. Hence, $\mathcal{Q}' \subset H$ and $F^{*2} \subseteq H$. Therefore, $F^{*2}\mathcal{Q}' \subseteq H \subsetneqq \mathcal{Q}^*$, so $\mathrm{CK}_1(M_2(\mathcal{Q}))$ is nontrivial. □

In Section 4 we will show that the quaternion division algebra over a euclidean field always has (non-normal) maximal subgroups and thus conclude that every quaternion division algebra over any field has a maximal subgroup. For the moment, we will describe exactly

when a quaternion division algebra has a normal maximal subgroup. This will enable us to give examples of quaternion division algebra over certain euclidean fields whch have normal maximal subgroups (necessarily of odd prime index, by Prop. 4).

Proposition 5. *Let $\mathcal{Q}$ be a quaternion division algebra with center F. For any odd prime p, if $F^* \neq F^{*p}$, then $\mathcal{Q}$ has a normal maximal subgroup of index p or 2. Hence, $\mathcal{Q}^*$ has no normal maximal subgroup if and only if F is euclidean and $F^* = F^{*p}$ for every odd prime p.*

Proof. Suppose $\mathcal{Q}$ has no subgroup of index 2. Prop. 4 shows that this occurs iff F is eucidean. Also by Prop. 4, $\mathrm{CK}_1(M_2(\mathcal{Q}))$ is trivial, so $\mathcal{Q}^* = F^{*2}\mathcal{Q}'$, by (1). Hence,

$$\mathcal{Q}^*/\mathcal{Q}' \;=\; F^{*2}\mathcal{Q}'/\mathcal{Q}' \;\cong\; F^{*2}/(F^* \cap \mathcal{Q}')\,. \tag{4}$$

If $a \in F^* \cap \mathcal{Q}'$, then $a^2 = \mathrm{Nrd}(a) = 1$; so, $F^{*2} \cap \mathcal{Q}' = \{1\}$. As noted previously, a normal maximal subgroup of $\mathcal{Q}^*$ has prime index and contains $\mathcal{Q}'$. Thus, if p is any odd prime, $\mathcal{Q}^*$ has a normal maximal subgroup iff F^{*2} has a maxmial subgroup of index p iff $F^{*2} \neq F^{*2p}$ (see Lemma 1), iff $F^* \neq F^{*p}$. □

Prop. 5 shows that the multiplicative group of Hamilton's quaternion division algebra $(\frac{-1,-1}{\mathbb{R}})$ has no normal maximal subgroup.

The next example shows that the quaternion division algebra $\mathcal{Q} = (\frac{-1,-1}{F})$ over a euclidean field F can have normal maximal subgroups (of odd index, by Prop. 4), i.e., there is a positive integer $t > 2$ such that $\mathrm{CK}_1(M_t(\mathcal{Q}))$ is nontrivial (recall that here $\mathrm{CK}_1(M_2(\mathcal{Q})) = 1$).

Example 6. Let K be any field with an ordering $<$, and let R be a real closure of K with respect to $<$; let $<$ denote also the unique ordering on R. Let F be the Euclidean hull of K in R. That is, $F = \bigcup_{i=0}^{\infty} L_i$, where $L_0 = K$ and for each $i \geq 0$, $L_{i+1} = L_i\big(\{\sqrt{c} \mid c \in L_i,\ c > 0\}\big) \subseteq R$. By construction, the ordering on R restricts to an ordering on F in which each positive element of F is a square; so, F is euclidean. Take any odd prime p. Let D be any quadratic extension of K. The composition of maps $K^*/K^{*p} \to E^*/E^{*p} \xrightarrow{N} K^*/K^{*p}$, where N is induced by the norm $N_{E/F}$, is the squaring map, which is an isomorphism as p is odd. Hence, the map $K^*/K^{*p} \to E^*/E^{*p}$ is injective. Thus, the map $K^*/K^{*p} \to F^*/F^{*p}$ is an injection, as F is the direct limit of iterated quadratic extensions of K. Therefore, whenever $K^{*p} \neq K^*$ the quaternion division algebra $(\frac{-1,-1}{F})$ over the euclidean field F has a normal maximal subgroup of index p. For example, when $K = \mathbb{Q}$, the field F is the field of constructible numbers, in the sense of compass and straightedge constructions, and $(\frac{-1,-1}{F})$ has a normal maximal subgroup of index p for every odd prime p. For another example, let $K = \mathbb{R}((x))$, the Laurent series field in one variable over the real numbers $\mathbb{R}$. Then, with respect to the ordering on K with $x > 0$, the euclidean hull is $F = K(\{\sqrt[2^n]{x} \mid n = 1, 2, \dots\})$; this F has a Henselian (but not complete) valuation induced by the x-adic valuation on F, with value group Γ_F isomorphic to the additive group of the ring $\mathbb{Z}[1/2]$ and $\overline{F} \cong \mathbb{R}$. For every odd prime p, we have $F^*/F^{*p} \cong \Gamma_F/p\Gamma_F \cong \mathbb{Z}/p\mathbb{Z}$. The valuation on F extends uniquely to a valuation v on $\mathcal{Q} = (\frac{-1,-1}{F})$ with $\overline{\mathcal{Q}} \cong \big(\frac{-1,-1}{\mathbb{R}}\big)$ and $\Gamma_{\mathcal{Q}} = \Gamma_F$. For each odd prime p, $\{\, a \in \mathcal{Q}^* \mid v(a) \in p\Gamma_{\mathcal{Q}} \,\}$ is the unique normal subgroup of $\mathcal{Q}$ of index p, and these are all the normal maximal subgroups of $\mathcal{Q}^*$.

In each of these examples, $\mathrm{CK}_1(\mathcal{Q})$ and $\mathrm{CK}_2(\mathcal{Q})$ are trivial by Prop. 4, but $\mathrm{CK}_3(\mathcal{Q})$ is nontrivial as $\mathcal{Q}^*$ has a normal maximal subgroup of index 3, by the proof of Prop. 2.

In the rest of this section we will give some examples of division algebras with non-normal maximal subgroups of finite index.

Example 7. Let q be any prime power. We construct a division algebra D with center a local field F such that

$$D^*/F^*(1+M_D) \;\cong\; \mathcal{D}_{q+1}.$$

Here $\mathcal{D}_{q+1}$ is the dihedral group with $2(q+1)$ elements, and M_D is the maximal ideal of the valuation ring of D. Note that for any $n>2$, the dihedral group $\mathcal{D}_n$ has nonnormal maximal subgroups of index p for each odd prime p dividing n (and these are the only nonnormal maximal subgroups). It thus follows that for each odd prime p dividing $q+1$ there is a maximal subgroup H in D^* of index p such that $F^*(1+M_D)\subseteq H$ but H is not normal in D^*.

For this example we need a finite dimensional valued division algebra D over a field $F=Z(D)$ of index n. That is, there is an epimorphism $v\colon D^*\to\Gamma_D$, where Γ_D is a totally ordered abelian group such that if $v(a)\geq 0$ then $v(a+1)\geq 0$ (this is equivalent to the traditional definition). Let $V_D=\{a\in D^*\mid v(a)\geq 0\}\cup\{0\}$, the valuation ring of D, and let $M_D=\{a\in D^*\mid v(a)>0\}\cup\{0\}$, the unique maximal left and right ideal of V_D. Thus $\overline{D}=V_D/M_D$ is a division ring called the residue division ring, and $U_D=V_D^*=V_D\backslash M_D$ is the group of valuation units. The restriction of v to F induces a valuation on F and gives the corresponding structures $V_F, M_F, U_F, \overline{F}$ and Γ_F. (For a survey of valued division algebras see [29].)

We need an exact sequence relating a homomorphic image of D^* to value group and residue data. For this, note that since $U_D\cap F^*(1+M_D)=U_F(1+M_D)$, we have a short exact sequence,

$$1 \;\longrightarrow\; U_D/U_F(1+M_D) \;\longrightarrow\; D^*/F^*(1+M_D) \;\longrightarrow\; D^*/F^*U_D \;\longrightarrow\; 1 \tag{5}$$

Now, the reduction epimorphism $U_D\to\overline{D}^*$ has kernel $1+M_D$, and likewise $\overline{F}^*\cong U_F/(1+M_F)$. Hence, $U_D/U_F(1+M_D)\cong\overline{D}^*/\overline{F}^*$. Also, the epimorphism $D^*\to\Gamma_D/\Gamma_F$ induced by v has kernel F^*U_D. By plugging this information into (5) we obtain the short exact sequence.

$$1 \;\longrightarrow\; \overline{D}^*/\overline{F}^* \;\longrightarrow\; D^*/F^*(1+M_D) \;\xrightarrow{\;v\;}\; \Gamma_D/\Gamma_F \;\longrightarrow\; 1. \tag{6}$$

Now, suppose v on F is discrete of rank 1, i.e., $\Gamma_F=\mathbb{Z}$, and let L be a cyclic Galois extension of F of degree n, and let $\mathrm{Gal}(L/F)=\langle\sigma\rangle$. Suppose L is unramified over F, i.e., v has a unique extension from F to L with $\overline{L}$ separable of degree n over $\overline{F}$. Take any $\pi\in F^*$ with $v(\pi)=1$, and let D be the cyclic algebra $D=(L/F,\sigma,\pi)$. So, $D=\bigoplus_{i=0}^{n-1}Lx^i$, where $xcx^{-1}=\sigma(c)$ for all $c\in L$, and $x^n=\pi$. It is known, see Cor. 2.9 in [12], and easy to verify that v extends to a valuation on D given by $v\big(\sum_{i=0}^{n-1}c_ix^i\big)=\min_{0\leq i\leq n}\big(v(c_i)+i/n\big)$. Hence, D is a division ring, with $\overline{D}=\overline{L}$ and $\Gamma_D=\frac{1}{n}\mathbb{Z}$. Note that $v(x)=1/n$, so that the image of $v(x)$ generates the cyclic group $\Gamma_D/\Gamma_F\cong\mathbb{Z}/n\mathbb{Z}$. But also, $x^n=\pi\in F^*$, so the image

$\widetilde{x} = xF^*(1+M_D)$ of x in $D^*/F^*(1+M_D)$ has order dividing n. Therefore, there is a well-defined homomorphism $\Gamma_D/\Gamma_F \to D^*/F^*(1+M_D)$ sending $1/n+\Gamma_F$ to $\widetilde{x}$; this is a splitting map for the short exact sequence (6). Hence, the middle group in (6) is a semidirect product,

$$D^*/F^*(1+M_D) \;\cong\; \overline{L}^*/\overline{F}^* \ltimes \mathbb{Z}/n\mathbb{Z}\,, \tag{7}$$

where the conjugation action of the distinguished generator of $\mathbb{Z}/n\mathbb{Z}$ on $\overline{L}^*/\overline{F}^*$ in the semidirect product is induced by the automorphism of $\overline{L}$ induced by σ on L.

To be more specific, let $q = \ell^m$ for any prime ℓ and any positive integer m, and let F be the unramified extension of degree m of the ℓ-adic field $\mathbb{Q}_\ell$. With repect to the (complete, discrete rank 1) valuation v on F extending the ℓ-adic valuation on $\mathbb{Q}_\ell$, we have $\overline{F} \cong \mathbb{F}_q$, the finite field with q elements. Let L be the unramified extension of F of degree n. Then, with respect to the unique extension of v to L, we have $\overline{L} \cong \mathbb{F}_{q^n}$, and L is cyclic Galois over F as the valuation is Henselian and $\overline{L}$ is cyclic Galois over $\overline{F}$. Let σ be the Frobenius automorphism of L, which is the generator of $\mathrm{Gal}(L/F)$ which induces the q-th power map on $\overline{L}$. Since $\overline{L}^*$ is a cyclic group, the isomorphism of (7) becomes

$$D^*/F^*(1+M_D) \;\cong\; \mathbb{Z}/\big((q^n-1)/(q-1)\big)\mathbb{Z} \ltimes \mathbb{Z}/n\mathbb{Z}\,, \tag{8}$$

where the distinguished generator of $\mathbb{Z}/n\mathbb{Z}$ acts on $\mathbb{Z}/\big((q^n-1)/(q-1)\big)\mathbb{Z}$ by multiplication by q. If we specialize to $n=2$, then D is the unique quaternion division algebra over F, and multiplication by q on $\mathbb{Z}/(q+1)\mathbb{Z}$ coincides with the inverse map, so the right group in (8) is the dihedral group $\mathcal{D}_{q+1}$.

Remark. Let D be a *tame* division algebra, i.e., $Z(\overline{D})$ is separable over $\overline{F}$ and $\mathrm{char}(\overline{F}) \nmid \mathrm{ind}(D)$. Then, $1+M_D = (1+M_F)[D^*, 1+M_D]$ (see the proof of Th. 3.1 in [8]). It follows that $F^*(1+M_D) = F^*[D^*, 1+M_D]$. Also if $\mathrm{char}(\overline{F}) \neq 2$, by Th. 21 in [23], $[D^*, 1+M_D] = D''$ where $D'' = [D', D']$. Putting these together, if in the above example $n=2$ and q is not a 2-power, then

$$D^*/F^*D'' \cong \mathcal{D}_{q+1}.$$

3. Maximal subgroups of D^*—reduction to the quaternion case

Let F be a field. For any $m \in \mathbb{N}$, let $\mu_m(F)$ denote the group of all m-th roots of unity in F. Also $\mu_m \subseteq F$ means that F contains a primitive m-th root of unity i.e., $\mu_m(F)$ has order m.

For a prime number p, ${}_p\mathrm{Br}(F)$ denotes the p-torsion subgroup of the Brauer group $\mathrm{Br}(F)$, and $\mathrm{Br}(F)(p)$ denotes the p-primary component of $\mathrm{Br}(F)$.

Throughout this section, D is a non-commutative division algebra finite dimensional over its center F. Recall from Prop. 2 that if D has no (normal) maximal subgroup (of prime finite index) then $\mathrm{CK}_1(M_k(D))$ is trivial for every $k \in \mathbb{N}$. The goal of this section is to prove the following theorem:

Theorem 8. *Let D be a division algebra of index n, with center F, such that the group $\mathrm{CK}_1(M_k(D))$ is trivial for every positive integer k. Then,*

(i) *if n is odd, then* $\mathrm{char}(F) > 0$ *and* $\mathrm{char}(F) \nmid n$ *and for each prime number q, $F^* = F^{*q}$,*
(ii) *if n is even, then $n = 2m$ with m odd,* $\mathrm{char}(F) = 0$*, F is euclidean, $F^* = F^{*q}$ for each odd prime, and* ${}_2\mathrm{Br}(F) = \mathrm{Br}(F)(2) = \{F, (\frac{-1,-1}{F})\}$,
(iii) *in either case, for each odd prime p dividing n, $\mu_p \not\subseteq F$, and ${}_p\mathrm{Br}(F)$ contains (and is generated by) noncyclic algebras of degree p, and $[F(\mu_p) : F] \geq 4$.*

The proof will be given below, after some preliminary steps.

Lemma 9. *Let D be a division algebra with center F, where D has of index $n = p_1^{r_1} \dots p_l^{r_l}$ with the p_i distinct primes. If $\mathrm{CK}_1(M_k(D))$ is trivial for every positive integer k then $F^{*p_i^{r_i}} = F^{*p_i^{r_i+1}}$, $1 \leq i \leq l$ and $F^* = F^{*q}$ for every prime q other than the p_i.*

Proof. Since $\mathrm{CK}_1(M_k(D)) \cong D^*/F^{*k}D'$, if $\mathrm{CK}_1(M_k(D))$ is trivial then, $D^* = F^{*k}D'$ for any $k \in \mathbb{N}$. Applying Nrd to this equation, we get:

$$F^{*n} \subseteq \mathrm{Nrd}(D^*) = \mathrm{Nrd}(F^{*k}D') = F^{*nk} \subseteq F^{*n}.$$

Thus for every $k \in \mathbb{N}$,

$$F^{*n} = F^{*nk}. \tag{9}$$

The Lemma then follows from (9) and Lemma 10 below. □

Lemma 10. *Let A be an abelian group, written additively. Let $n = p_1^{r_1} \dots p_l^{r_l}$ with the p_i distinct primes and $r_i \geq 1$. The following are equivalent:*

(i) *$nA = nkA$ for every $k \in \mathbb{N}$.*
(ii) *$p_i^{r_i}A = p_i^{r_i+1}A$ for each i, and $A = qA$ for every prime q different from the p_i.*

Proof. (ii) ⇒ (i) is clear. (It suffices to check (i) for k a prime number.)

(i) ⇒ (ii). Note that for any $s, t \in \mathbb{N}$ with $\gcd(s,t) = 1$, we have

$$A/stA = \big(sA/stA\big) \bigoplus \big(tA/stA\big). \tag{10}$$

For, as $\gcd(s,t) = 1$, $A = sA + tA$, and $\big(sA/stA\big) \cap \big(tA/stA\big) = (0)$, since sA/stA is t-torsion and tA/stA is s-torsion. Now, take any prime q different from the p_i. Since $\gcd(q,n) = 1$, (10) and (i) yield

$$A/nqA = \big(nA/nqA\big) \bigoplus \big(qA/nqA\big) = (0) \bigoplus \big(qA/nqA\big).$$

So, $A = qA$. Now, for $1 \leq i \leq l$, write $n = p_i^{r_i}u$, so $np_i = p_i^{r_i+1}u$ with $\gcd(p_i^{r_1+1}, u) = 1$. Then (10) shows

$$A/np_iA = \big(p_i^{r_i+1}A/np_iA\big) \bigoplus \big(uA/np_iA\big).$$

Multiplying this by $p_i^{r_i}$:

$$\begin{aligned} p_i^{r_i}A/np_iA &= \big(\big[p_i^{r_i}(p_i^{r_i+1}A) + np_iA\big]/np_iA\big) \bigoplus \big(nA/np_iA\big) \\ &\subseteq \big(p_i^{r_i+1}A/np_iA\big) \bigoplus (0) \subseteq p_i^{r_i}A/np_iA. \end{aligned}$$

So, $p_i^{r_i}A = p_i^{r_i+1}A$. □

Lemma 11. *If p is a prime number and $r \in \mathbb{N}$, then $F^{*p^r} = F^{*p^{r+1}}$ if and only if $F^* = \mu_{p^r}(F)F^{*p}$.*

Proof. Suppose $F^{*p^r} = F^{*p^{r+1}}$. Take any $a \in F^*$. There is a $b \in F^*$ with $a^{p^r} = b^{p^{r+1}}$. Let $\omega = ab^{-p}$. Then $\omega \in \mu_{p^r}(F)$, and $a = \omega b^p \in \mu_{p^r}(F)F^{*p}$. So, $F^* = \mu_{p^r}(F)F^{*p}$. The converse is clear. □

Proposition 12. *Let F be a field with $F^{*p^r} = F^{*p^{r+1}}$ for some prime p and for $r \in \mathbb{N}$, and suppose ${}_p\mathrm{Br}(F) \neq 0$. Then,*

(i) *if p is odd, then* $\mathrm{char}(F) \neq p$, $F^* = F^{*p}$, $\mu_p \nsubseteq F$, *and* ${}_p\mathrm{Br}(F)$ *is generated by noncyclic algebras of degree p.*
(ii) *if $p = 2$, then* $\mathrm{char}(F) = 0$, *F is euclidean and* $\mathrm{Br}(F)(2) = {}_2\mathrm{Br}(F) = \{F, (\frac{-1,-1}{F})\}$.

Proof. Let ω be a generator of the cyclic group $\mu_{p^r}(F)$. By Lemma 11, $F^* = \langle\omega\rangle F^{*p}$.

(i) Assume p is odd. If $\mathrm{char}(F) = p$, then by Albert's theorem (see [4], p. 109, Th. 30 or [14], p. 173, Th. 4.5.7), $\mathrm{Br}(F)(p)$ is generated by cyclic algebras of degree a power of p. But when $\mathrm{char}(F) = p$, we have $\omega = 1$, so $F^* = F^{*p}$, i.e., F is perfect, so F has no cyclic algebra. This contradicts the assumption that ${}_p\mathrm{Br}(F) \neq (0)$. Hence, $\mathrm{char}(F) \neq p$. If $\mu_p \subseteq F$, then the Merkurjev-Suslin theorem (see [27] or [26], Ch. 8) says that ${}_p\mathrm{Br}(F)$ is generated by p-symbol algebras. Since $F^*/F^{*p} = \langle\omega F^{*p}\rangle$, we would then have ${}_p\mathrm{Br}(F)$ is a cyclic group generated by the p-symbol algebra $(\omega, \omega; F)_p$. But $(\omega, \omega; F)_p \cong (\omega, -1; F)_p$, so that $(\omega, \omega; F)_p$ is both p-torsion and 2-torsion in ${}_p\mathrm{Br}(F)$, so it must be split. This cannot occur since ${}_p\mathrm{Br}(F) \neq 0$. Hence $\mu_p \nsubseteq F$. Therefore $\omega = 1$ and $F^* = F^{*p}$. By a theorem of Merkurjev (see [20], Th. 2), since $\mathrm{char}(F) \neq p$, ${}_p\mathrm{Br}(F)$ is generated by algebras of degree p. Since $F^* = F^{*p}$, these generators cannot be cyclic algebras. (Of course, the existence of noncyclic division algebras of prime degree is a major open question).

(ii) Assume now that $p = 2$. As in case (i), if $\mathrm{char}(F) = 2$, then F is perfect, so that ${}_2\mathrm{Br}(F) = 0$ by Albert's theorem, contrary to hypothesis. So, $\mathrm{char}(F) \neq 2$. By Merkurjev's Theorem (see, e.g., [15], Kap. V for a proof), ${}_2\mathrm{Br}(F)$ is generated by quaternion algebras. Since $F^* = \langle\omega\rangle F^{*2}$, ${}_2\mathrm{Br}(F)$ must be a cyclic group generated by the quaternion algebra $(\frac{\omega,\omega}{F})$. But $(\frac{\omega,\omega}{F}) = (\frac{\omega,-1}{F})$. If $\mu_4 \subseteq F$, then $-1 \in F^{*2}$, so that $(\frac{\omega,-1}{F})$ is split; then ${}_2\mathrm{Br}(F) = 0$, a contradiction. Hence $\mu_4 \nsubseteq F$, forcing $\omega = -1$, and $-1 \notin F^{*2}$. Since $F^* = \langle\omega\rangle F^{*2}$, we have $F^* = F^{*2} \cup -F^{*2}$ (a disjoint union). Also, ${}_2\mathrm{Br}(F) = \{[F], [H]\}$ where $H = (\frac{-1,-1}{F})$ which is nonsplit. It follows that $\mathrm{char}(F) = 0$. For, if $\mathrm{char}(F) = q \neq 0$, then H is split, since already over the prime field $\mathbb{F}_q$, $(\frac{-1,-1}{\mathbb{F}_q})$ is split.

Let $\mathbf{i}$ and $\mathbf{j}$ be the standard generators of H. Take any $a, b \in F^*$. Then $a^2 + b^2 = \mathrm{Nrd}(a + b\mathbf{i}) \neq 0$ as H is a division ring. Hence, there is $c \in F^*$ with $a^2 + b^2 = \pm c^2$. If $a^2 + b^2 = -c^2$, then $0 = a^2 + b^2 + c^2 = \mathrm{Nrd}(a + b\mathbf{i} + c\mathbf{j})$, which cannot occur, as H is a division ring. Therefore, $a^2 + b^2 = c^2$. Hence, F is pythagorean. Since $-1 \notin F^{*2}$, -1 is therefore not a sum of squares. Therefore, F is formally real. Since $F^* = F^{*2} \cup -F^{*2}$, F is in fact euclidean. Now, let $L = F(\sqrt{-1})$. By Hilbert's Th. 90, we have the exact sequence

$$F^*/F^{*2} \longrightarrow L^*/L^{*2} \longrightarrow F^*/F^{*2}, \tag{11}$$

where the left map is induced by the inclusion $F^* \hookrightarrow L^*$, and the right map is induced by the norm $N_{L/F}$. For $a, b \in F^*$, we have $N_{L/F}(a + b\sqrt{-1}) = a^2 + b^2 \in F^{*2}$. Thus, the right map in (11) is the 0-map. The left map in (11) is also 0-map, since $-1 \in L^{*2}$. Hence,

$L^* = L^{*2}$. Therefore, Merkurjev's Theorem shows that ${}_2\operatorname{Br}(L) = 0$, so $\operatorname{Br}(L)(2) = 0$. Hence, $\operatorname{Br}(F)(2) \subseteq \operatorname{Br}(L/F)$ $(= \ker(\operatorname{Br}(F) \to \operatorname{Br}(L)))$. But, as $[L:F] = 2$, $\operatorname{Br}(L/F) \subseteq {}_2\operatorname{Br}(F)$. Thus, $\operatorname{Br}(F)(2) = {}_2\operatorname{Br}(F)$ □

Lemma 13. *Suppose* $\operatorname{char}(F) = 0$ *and* $F^* = F^{*q}$ *for each prime* q*. Then* $\mu_q \subseteq F$ *for each prime* q*.*

Proof. This is Lemma 3 of [19]. We include the short proof for the convenience of the reader. The proof is by induction on q. Of course $\mu_2 = \{\pm 1\} \subseteq F$. Now assume $q > 2$ and $\mu_\ell \subseteq F$ for all primes $\ell < q$. We have $F(\mu_q)$ is an abelian Galois extension of F with $[F(\mu_q):F] \mid (q-1)$. If $F(\mu_q) \neq F$, then there is a prime $p \mid (q-1)$ and a sub-extension $F \subseteq K \subseteq F(\mu_q)$ with $[K:F] = p$, so K is cyclic Galois over F. Since $\mu_p \subseteq F$ by induction, K is a p-Kummer extension of F. This cannot occur, as $F^* = F^{*p}$. Hence, $F(\mu_q) = F$, as desired. □

We can now prove Theorem 8.

Proof of Theorem 8. Since $\mathrm{CK}_1(M_k(D))$ is trivial for every $k \in \mathbb{N}$, Lemma 9 shows that $F^* = F^{*q}$ for each prime q with $q \nmid n$. Let p be an odd prime with $p \mid n$. Then ${}_p\operatorname{Br}(F) \neq 0$ since it contains some nonsplit tensor power of D. So, Lemma 9 and Prop. 12(i) show that $F^* = F^{*p}$, $\mu_p \nsubseteq F$, and ${}_p\operatorname{Br}(F)$ is generated by noncyclic algebras of degree p. This last condition implies $[F(\mu_p):F] \geq 4$, by the Corollary to Th. 1 in [20]. Suppose n is odd. Then $F^* = F^{*q}$ for every prime q. Since $\mu_p \nsubseteq F$ for any prime p with $p \mid n$, Lemma 13 shows that $\operatorname{char}(F) \neq 0$. Also Lemma 9 and Prop. 12(i) show that $\operatorname{char}(F) \nmid n$. This completes the proof of (i) and (iii). For (ii) assume now that n is even. Lemma 9 and Prop. 12(ii) show that $\operatorname{char}(F) = 0$, F is euclidean, and ${}_2\operatorname{Br}(F) = \operatorname{Br}(F)(2) = \{F, (\frac{-1,-1}{F})\}$. Since the 2-primary component of D therefore must be $(\frac{-1,-1}{F})$, $n/2$ must be odd. □

Remark. The result of Lemma 13 is definitely not true in prime characteristic, since cyclic Galois extensions of degree $\operatorname{char}(F)$ are Artin-Schreier extensions, not Kummer extensions. For example, let p be a prime number, and let $\mathbb{F}_p$ be the finite field with p elements. In an algebraic closure ${\mathbb{F}_p}^{alg}$ of $\mathbb{F}_p$, let L_i be the field with $[L_i:\mathbb{F}_p] = i$ for all $i \in \mathbb{N}$, and let $F = \bigcup_{p \nmid i} L_i$. Then, $F^* = F^{*q}$ for all primes q, but for all primes q with $p \mid [\mathbb{F}_p(\mu_q):\mathbb{F}_p]$, we have $\mu_q \nsubseteq F$. (E.g., if $p = 3$, then $\mu_7 \nsubseteq F$).)

4. Maximal subgroups of the multiplicative group of a quaternion algebra

In this section we shall prove that the multiplicative group of a quaternion division algebra contains maximal subgroups. We will see that the most difficult case is that of quaternion algebras over euclidean fields. As shown by Prop. 5, such division algebras may not have any normal maximal subgroups.

Theorem 14. *Let* $\mathcal{Q}$ *be a quaternion division algebra with center* F*. Then the multiplicative group of* $\mathcal{Q}$ *has a maximal subgroup.*

Proof. If $\mathcal{Q}$ has no normal maximal subgroup, then by Prop. 4, $\mathcal{Q} = (\frac{-1,-1}{F})$, where F is a euclidean field. We will show in Th. 15 below that such a $\mathcal{Q}$ has a maximal subgroup. That will complete the proof of this theorem. □

The rest of this section is devoted to showing that the quaternion division algebra $(\frac{-1,-1}{F})$ over a euclidean field F contains a (non-normal) maximal subgroup. This will be done by a refinement of the argument given in [18], attributed to C. Ohn, showing that for $F = \mathbb{R}$, $\left(\frac{-1,-1}{\mathbb{R}}\right)$ has a maximal subgroup. Significant added complexity arises here because we need to take into account the possible existence of infinitesimals with respect to the ordering on F. A different proof that $\left(\frac{-1,-1}{\mathbb{R}}\right)$ has maximal subgroups is given in [1].

Let F be a euclidean field. Then F has a valuation ring V which is determined by the ordering:

$$V = \{b \in F \mid |b| \leq n \text{ for some } n \in \mathbb{N}\},$$

whose maximal ideal is

$$M = \{b \in F \mid |b| \leq 1/n \text{ for every } n \in \mathbb{N}\}$$

(see, e.g., [24] p. 135). Note that $F \backslash V$ is the set of elements "infinitely large" relative to the rational numbers $\mathbb{Q} \subseteq F$. M is the set of elements of F "infinitesimal" relative to $\mathbb{Q}$.

We will need some geometric properties for inner product spaces over the euclidean field F, which are familiar when the field is $\mathbb{R}$.

For any $n \in \mathbb{N}$, let $F^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in F\}$. For $\alpha = (a_1, a_2, \ldots, a_n)$ and $\beta = (b_1, b_2, \ldots, b_n)$ in F^n, we have the dot product: $\alpha \cdot \beta = a_1b_1 + a_2b_2 + \ldots + a_nb_n \in F$. The norm $\|\alpha\| = \sqrt{a_1^2 + a_2^2 + \ldots + a_n^2} = \sqrt{\alpha \cdot \alpha} \in F$ (as F is euclidean). Note that the following basic tools carry over to this setting: The Cauchy-Schwarz inequality: $|\alpha \cdot \beta| \leq \|\alpha\|\|\beta\|$, and the triangle inequality: $\|\alpha + \beta\| \leq \|\alpha\| + \|\beta\|$. We write $\alpha \perp \beta$ if $\alpha \cdot \beta = 0$.

Now let

$$\mathrm{O}_n(F) \;=\; \{A \in M_n(F) \mid A^tA = I\}$$

and

$$\mathrm{SO}_n(F) \;=\; \{A \in \mathrm{O}_n(F) \mid \det(A) = 1\}.$$

So, for any $A \in \mathrm{O}_n(F)$ and any $\alpha, \beta \in F^n$, we have $(A\alpha \cdot A\beta) = (\alpha \cdot \beta)$ and $\|A\alpha\| = \|\alpha\|$. Clearly,

$$\mathrm{SO}_2(F) \;=\; \left\{ \begin{pmatrix} c & -s \\ s & c \end{pmatrix} \mid c, s \in F,\ c^2 + s^2 = 1 \right\}$$

is an abelian group, whose elements can be thought of as "rotations". Also,

$$\mathrm{O}_2(F) \backslash \mathrm{SO}_2(F) \;=\; \left\{ \begin{pmatrix} c & s \\ s & -c \end{pmatrix} \mid c, s \in F,\ c^2 + s^2 = 1 \right\}.$$

Each $A \in \mathrm{O}_2(F) \backslash \mathrm{SO}_2(F)$ has eigenvectors 1,-1 with orthogonal eigenspaces. So, A is a reflection.

Note that as F is euclidean, $\mathrm{SO}_2(F)$ is 2-divisible. For, if $A = \left(\begin{smallmatrix} c & -s \\ s & c \end{smallmatrix}\right) \in \mathrm{SO}_2(F)$, with $c^2 + s^2 = 1$, then $|c| \leq 1$, so $c + 1 \geq 0$. Let $B = \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$, where, if $c = -1$ (so $s = 0$), $a = 0$ and $b = \pm 1$, while if $c \neq -1$, $a = \pm\sqrt{(c+1)/2}$ and $b = s/2a$. Then $a^2 + b^2 = 1$ (and $a, b \in F$ as $c + 1 \geq 0$ and F is euclidean), so $B \in \mathrm{SO}_2(F)$, and $B^2 = A$. Basically we are just invoking the half-angle formula from trigonometry. Now, let $A \in \mathrm{SO}_3(F)$. We claim that 1 is an eigenvalue of A. For this, let R be a real closure of F with respect to its unique ordering, and let $\chi_A = \det(x.I - A)$ in $F[x]$ be the characteristic polynomial of A. Since R

is real closed, its irreducible polynomials have degree ≤ 2; so as $\deg(\chi_A) = 3$ which is odd, χ_A has a root $\lambda \in R$; hence A has a λ-eigenvector $\gamma \in R^3$. We have

$$\|\gamma\| \;=\; \|A\gamma\| \;=\; \|\lambda\gamma\| \;=\; |\lambda|\,\|\gamma\|,$$

so $|\lambda| = 1$, so $\lambda = \pm 1$. Since $\lambda \in F$, A has a λ-eigenvector $v \in F^3$. If we enlarge $\{v\}$ to an orthogonal base $\mathcal{B} = \{v, v_1, v_2\}$ of F^3 then the matrix of A (as a linear transformation on F^3) is $B = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & D \end{smallmatrix}\right)$, where $D \in \mathrm{O}_2(F)$, with $\det(D) = \det(A)/\lambda = 1/\lambda = \lambda$. If $\lambda = -1$, then $D \notin \mathrm{SO}_2(F)$, so as noted above, 1 is an eigenvalue of D, hence of A. So, in all cases, 1 is an eigenvalue of A, as claimed.

Note that proof of the claim shows that for $A \in \mathrm{SO}_3(F)$ there is a 1-eigenvector v of A and orthogonal base $\mathcal{B} = \{v, v_1, v_2\}$ so that the matrix of multiplication by A on F^3 relative to $\mathcal{B}$ is $\left(\begin{smallmatrix} 1 & 0 \\ 0 & D \end{smallmatrix}\right)$ where $D \in \mathrm{O}_2(F)$, and $\det(D) = \det(A)/1 = 1$; so $D \in \mathrm{SO}_2(F)$, i.e., D is a "rotation." Thus we can think of A as a rotation about the axis determined by the 1-eigenvector v. Because D is the square of a matrix in $\mathrm{SO}_2(F)$, A is the square of a matrix in $\mathrm{SO}_3(F)$. Thus $\mathrm{SO}_3(F)$ is 2-divisible (though non-abelian).

Let $\mathcal{Q} = (\frac{-1,-1}{F})$ be the ordinary quaternion division algebra over F with its standard base $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ and standard involution given by $\overline{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}} = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$. We identify $\mathcal{Q}$ with F^4 via $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \;\leftrightarrow\; (a, b, c, d)$. Then, for $x \in \mathcal{Q}$, we have $\|x\| = \sqrt{\mathrm{Nrd}(x)}$, where for $x = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$,

$$\mathrm{Nrd}(x) \;=\; x\overline{x} \;=\; a^2 + b^2 + c^2 + d^2\,.$$

Note also that the reduced trace of x is $\mathrm{Trd}(x) = x + \overline{x} = 2a$.

Let

$$S(\mathcal{Q}) \;=\; \{x \in \mathcal{Q} \mid \|x\| = 1\}$$

be the unit sphere in $\mathcal{Q}$. Let $P = \{b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid b, c, d \in F\}$, the "pure part" of $\mathcal{Q}$. Note that

$$P \;=\; \{\alpha \in \mathcal{Q} \mid \mathrm{Trd}(\alpha) = 0\} \;=\; \{\alpha \in \mathcal{Q} \mid \alpha^2 \in F, \alpha \notin F\} \cup \{0\}\,. \tag{12}$$

Let

$$S(P) \;=\; \{\alpha \in P \mid \|\alpha\| = 1\}\,,$$

the unit sphere in P. The geometry in P is nicely tied to the multiplication: A straightforward calculation shows that for $\alpha = a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$ and $\beta = b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k} \in P$, we have

$$\alpha\beta \;=\; -(\alpha \cdot \beta) \;+\; \alpha \times \beta, \tag{13}$$

where the cross product $\alpha \times \beta$ is the formal determinant

$$\alpha \times \beta \;=\; \begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix} \in P\,.$$

Since $\beta \times \alpha = -\alpha \times \beta$, formula (13) shows that $\alpha \cdot \beta = -\frac{1}{2}(\alpha\beta + \beta\alpha)$. Thus, $\alpha \perp \beta$ if and only if α and β anticommute.

Now, $\mathcal{Q}^*$ acts on $\mathcal{Q}$ by conjugation: For $x \in \mathcal{Q}^*, y \in \mathcal{Q}$, set

$$x * y \;=\; xyx^{-1}\,.$$

Note that since conjugation preserves the reduced norm, it also preserves the norm, i.e., $\|x * y\| = \|y\|$, and hence it also preserves the dot product, i.e.,

$$(x * y) \cdot (x * z) \;=\; y \cdot z$$

(as $2(y \cdot z) = \|y + z\|^2 - \|y\|^2 - \|z\|^2$). Note that for $x \in \mathcal{Q}^*$ and $\alpha \in P$, by (12) above we have $x * \alpha \in P$, since $\mathrm{Trd}(x * \alpha) = \mathrm{Trd}(\alpha) = 0$ (or, $x * \alpha \notin F$ as $\alpha \notin F$ (assuming $\alpha \neq 0$), but $(x * \alpha)^2 = x * (\alpha^2) = \alpha^2 \in F$). Thus, the conjugation action of $\mathcal{Q}^*$ on $\mathcal{Q}$ restricts to an action of $\mathcal{Q}^*$ on P, which is norm and dot product preserving. So, $\mathcal{Q}^*$ also acts on the unit sphere $S(P)$. There is a very nice geometric description of this action, as follows:

Take any $x \in \mathcal{Q}^*$. Since conjugation by x coincides with conjugation by $\frac{1}{\|x\|}x$, we may assume that $\|x\| = 1$. Then we can write $x = c + sp$, for some $c, s \in F, p \in P$ with $c^2 + s^2 = 1$ and $\|p\| = 1$. If $s = 0$, then $x \in F$, so $x * \alpha = \alpha$ for all $\alpha \in P$. So, assume $s \neq 0$. Then, s and p are unique up to factor of -1, and $p \neq 0$.

For $\{p\}^\perp = \{y \in \mathcal{Q} \mid y \cdot p = 0\}$, we have $\dim_F(\{p\}^\perp \cap P) = 2$. So, there is $q \in S(P)$ with $q \perp p$. Set $r = pq$. We have $p^2 = -\|p\| = -1, q^2 = -1$, and $r = pq = -qp$; hence, $r^2 = -1, qr = -rq = p$, and $rp = -pr = q$. From this, it is clear that there is an F-automorphism of $\mathcal{Q}$ given by $\mathbf{i} \mapsto p$ and $\mathbf{j} \mapsto q$. In particular, $\{p, q, r\}$ is an orthogonal base of P. Since $\|x\| = 1$ and $x = c + sp$, we have $x^{-1} = \overline{x} = c - sp$. Thus, for any $\alpha = ap + bq + dr$ where $a, b, d \in F$, we have

$$\begin{aligned} x * \alpha \;&=\; (c + sp)\,(ap + bq + dr)\,(c - sp) \\ &=\; ap \;+\; [(c^2 - s^2)b - 2csd]q \;+\; [2csb + (c^2 - s^2)d]r. \end{aligned} \tag{14}$$

That is, the matrix of the F-linear transformation $\alpha \mapsto x * \alpha$ of P relative to the orthogonal base $\{p, q, r\}$ is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & c^2 - s^2 & -2cs \\ 0 & 2cs & c^2 - s^2 \end{pmatrix}.$$

Heuristically, think of $c = \cos(\theta)$ and $s = \sin(\theta)$ for some imagined angle θ, so that $\left(\begin{smallmatrix} c & -s \\ s & c \end{smallmatrix}\right)$ is the matrix for rotation by θ. Then, $x*$ is rotation by an angle 2θ about the p-axis.

Let's imagine the 2-sphere $S(P)$ oriented so that $\mathbf{i}$ is at the north pole and

$$E \;=\; F\text{-span}\{\mathbf{j}, \mathbf{k}\} \cap S(P)$$

as the equator. Take any $\beta = c_1\mathbf{j} + s_1\mathbf{k} \in E$, so $c_1^2 + s_1^2 = 1$, and choose $B = \left(\begin{smallmatrix} c_0 & -s_0 \\ s_0 & c_0 \end{smallmatrix}\right) \in \mathrm{SO}_2(F)$ such that $B^2 = \left(\begin{smallmatrix} c_1 & -s_1 \\ s_1 & c_1 \end{smallmatrix}\right)$ (recall that $\mathrm{SO}_2(F)$ is 2-divisible). Then, for $y = c_0 + s_0\mathbf{i}$, formula (14) shows that $y * \mathbf{j} = \beta$. Thus, the $\mathcal{Q}^*$-orbit of $\mathbf{j}$ contains all of E. Similarly, for any $\gamma \in S(P)$, take a two dimensional subspace W of P containing $\mathbf{j}$ and γ, and choose $p \in S(P)$ with $p \perp W$. Then we can take $q = \mathbf{j}$ and $r = p\mathbf{j}$; $\{q, r\}$ is an orthonormal base of W, so we have $\gamma = c_1 q + s_1 r$ with $c_1^2 + s_1^2 = 1$. From the 2-divisibility of $\mathrm{SO}_2(F)$, as above, there exist $c_0, s_0 \in F$ with $c_0^2 + s_0^2 = 1$, $c_0^2 - s_0^2 = c_1$ and $2c_0s_0 = s_1$; if we set $x = c_0 + s_0 p$, then formula (14) shows that $x * \mathbf{j} = \gamma$. Thus, $\mathcal{Q}^*$ acts transitively on $S(P)$.

Theorem 15. *Let F be a euclidean field, and let $\mathcal{Q} = (\frac{-1,-1}{F})$. Then $\mathcal{Q}^*$ contains a maximal subgroup.*

Proof. Recall that M is the set of $\mathbb{Q}$-infinitesimal elements of F. Let

$$\Delta \;=\; \{\alpha \in S(P) \mid \|\alpha - \mathbf{i}\| \in M\},$$

the set of elements of $S(P)$ "infinitesimally near" $\mathbf{i}$.

Let $C = \{a + b\mathbf{i} \mid a, b \in F\} \cong F(\sqrt{-1})$ which is the centralizer of $\mathbf{i}$ in $\mathcal{Q}$. Let

$$G_0 \;=\; C^* \;=\; \{a + b\mathbf{i} \mid a \neq 0 \text{ or } b \neq 0\} \;\subseteq\; \mathcal{Q}^*,$$

which is the stabilizer of $\mathbf{i}$ in $\mathcal{Q}^*$. For each $a \in F$ with $|a| \leq 1$, let

$$L_a \;=\; \{a\mathbf{i} + b\mathbf{j} + d\mathbf{k} \in P \mid b^2 + d^2 = 1 - a^2\},$$

the "a-latitude" on $S(P)$. We saw above that G_0 acts transitively on $E = L_0$, and an analogous argument shows that G_0 acts transitively on each L_a. Since $\mathbf{j} * (a\mathbf{i} + b\mathbf{j} + d\mathbf{k}) = -a\mathbf{i} + b\mathbf{j} - d\mathbf{k}$, we have $\mathbf{j} * \mathbf{i} = -\mathbf{i}$ and $\mathbf{j} * L_a = L_{-a}$ for each a-latitude.

Let

$$G \;=\; \{x \in \mathcal{Q}^* \mid x * \mathbf{i} \in \Delta \cup -\Delta\}\,.$$

Then, $G_0 \subseteq G$ and $\mathbf{j} \in G$. Note that for $x \in \mathcal{Q}^*$, if $x * \mathbf{i} \in \Delta$, then $x * \Delta \subseteq \Delta$. For, if $\alpha \in \Delta$, then

$$\begin{aligned}\|x * \alpha - \mathbf{i}\| \;&\leq\; \|x * \alpha - x * \mathbf{i}\| \;+\; \|x * \mathbf{i} - \mathbf{i}\| \;=\; \|x * (\alpha - \mathbf{i})\| \;+\; \|x * \mathbf{i} - \mathbf{i}\| \\ &=\; \|\alpha - \mathbf{i}\| \;+\; \|x * \mathbf{i} - \mathbf{i}\| \;\in\; M + M\,,\end{aligned}$$

so $x * \alpha \in \Delta$. Likewise, if $x * \mathbf{i} \in -\Delta$ then $x * \Delta \subseteq -\Delta$ and $x * (-\Delta) \subseteq \Delta$. Therefore, G is closed under multiplication. Furthermore, for $\epsilon = \pm 1$, we have $\|\overline{x} * \mathbf{i} - \epsilon\mathbf{i}\| = \|-\big(\overline{x * \mathbf{i} - \epsilon\mathbf{i}}\big)\| = \|x * \mathbf{i} - \epsilon\mathbf{i}\|$. Hence, if $x \in G$, then $\overline{x} \in G$. Because $x^{-1} = \frac{1}{\|x\|}\overline{x}$ and $F^* \subseteq G$, it follows that G is closed under inverses; hence, G is a subgroup of $\mathcal{Q}^*$. Since $\mathcal{Q}^*$ acts transitively on $S(P)$ but $G * \mathbf{i} \subseteq \Delta \cup -\Delta \subsetneqq S(P)$, G must be a proper subgroup of $\mathcal{Q}^*$.

Claim 1: G is a maximal subgroup of $\mathcal{Q}^*$.

Proof of Claim 1. Take any $y \in \mathcal{Q}^* \backslash G$, and let $K = \langle y, G\rangle$. We show that $K = \mathcal{Q}^*$ by proving that $K * \mathbf{i} = S(P)$. For then, for any $h \in \mathcal{Q}$, there is $z \in K$ with $h * \mathbf{i} = z * \mathbf{i}$. Then $z^{-1}h * \mathbf{i} = \mathbf{i}$, so that $z^{-1}h \in G_0 \subseteq K$; hence $h = z(z^{-1}h) \in K$. Let

$$y \;=\; r + t\mathbf{i} + u\mathbf{j} + v\mathbf{k} \;=\; (r + t\mathbf{i}) + (u + v\mathbf{i})\mathbf{j}\,,$$

with $r, t, u, v \in F$. Replacing y by $y\mathbf{j}$ if necessary (without changing K, as $\mathbf{j} \in G$), we can assume $r + t\mathbf{i} \neq 0$. Then (as $r + t\mathbf{i} \in G_0 \subseteq G$), we can replace y by $(r + t\mathbf{i})^{-1}y$, so we can assume $t = 0$. Furthermore, as $F^* \subseteq G$, we can replace y by $\frac{1}{\|y\|}y$ without changing K; so we can assume that $\|y\| = 1$. Thus, $y = c_0 + s_0 p$, where $c_0, s_0 \in F$ with $c_0^2 + s_0^2 = 1, p \in P, \|p\| = 1$ and $p \perp \mathbf{i}$. Without loss of generality, we may assume that $p = \mathbf{j}$. (For, if $p \neq \mathbf{j}$, just work with the base $\{\mathbf{i}, p, \mathbf{i}p\}$ of P instead of $\{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$, and the same argument as below clearly goes through.) Thus, $y = c_0 + s_0\mathbf{j}$ where $c_0, s_0 \in F$ with $c_0^2 + s_0^2 = 1$. Formula (14) then yields, for any $a, b, d \in F$,

$$\begin{aligned} y * (a\mathbf{i} + b\mathbf{j} + d\mathbf{k}) \;&=\; (c_0 + s_0\mathbf{j})\,(a\mathbf{i} + b\mathbf{j} + d\mathbf{k})\,(c_0 - s_0\mathbf{j}) \\ &=\; [(c_0^2 - s_0^2)a + 2c_0s_0d]\mathbf{i} \;+\; b\mathbf{j} \;+\; [-2c_0s_0a + (c_0^2 - s_0^2)d]\mathbf{k} \qquad (15) \\ &=\; (ca + sd)\mathbf{i} \;+\; b\mathbf{j} \;+\; (-sa + cd)\mathbf{k}, \end{aligned}$$

where

$$c \;=\; c_0^2 - s_0^2 \;\text{ and }\; s \;=\; 2c_0 s_0$$

(so, $c^2 + s^2 = 1$). In particular $y * \mathbf{i} = c\mathbf{i} - s\mathbf{k}$.

We have $c, s \in V$ (the valuation ring) since $c^2 + s^2 = 1$ shows $|c| \le 1$ and $|s| \le 1$. Note further that

$$\|y * \mathbf{i} - \mathbf{i}\|^2 \;=\; (c-1)^2 \,+\, s^2 \;=\; (c-1)^2 \,+\, (1-c^2) \;=\; 2(1-c),$$

and likewise $\|y * \mathbf{i} + \mathbf{i}\|^2 = 2(1+c)$. Since $y * \mathbf{i} \notin \Delta$ and $y * \mathbf{i} \notin -\Delta$ by hypothesis, we must have $1 + c \notin M$, $1 - c \notin M$; hence $s^2 = (1-c)(1+c) \notin M$, so $s \notin M$.

By replacing y by $y\mathbf{j}$ if necessary (which interchanges $|c_0|$ and $|s_0|$), we may assume $c \ge 0$. Also, by replacing y by y^{-1} if necessary (which replaces s_0 by $-s_0$ without changing c_0), we may assume $s \ge 0$.

Claim 2: Finitely many applications of elements of K map $\mathbf{i}$ to any point on any latitude L_b, for any b with $0 \le b \le 1$.

Since $\mathbf{j} * L_b = L_{-b}$, it follows from Claim 2 that $K * \mathbf{i} = \bigcup_{-1 \le b \le 1} L_b = S(P)$, which, as we showed above, proves Claim 1.

Proof of Claim 2. Recall that for $|a| \le 1$,

$$L_a \;=\; \{a\mathbf{i} \pm \sqrt{1 - a^2 - d^2}\,\mathbf{j} + d\mathbf{k} \mid |d| \le \sqrt{1-a^2}\}.$$

Thus, formula (15) shows that for $0 \le a \le 1$,

$$(y * L_a) \cap L_b \ne \varnothing \quad \text{for every } b \in F \text{ with} \quad ca - s\sqrt{1-a^2} \;\le\; b \;\le\; ca + s\sqrt{1-a^2}. \tag{16}$$

If we set $a = c$, so $\sqrt{1-a^2} = s$, condition (16) says that L_c meets L_b for all b with $c^2 - s^2 \le b \le c^2 + s^2 = 1$; in particular, this holds for $c \le b \le 1$, since $c^2 - s^2 \le c^2 \le c \le 1$ (as $0 \le c \le 1$). Now, $y * \mathbf{i} \in L_c$, and G_0 acts transitively on L_c. For any b with $c \le b \le 1$, we have just seen that $y*$ maps some point on L_c to a point on L_b. Also G_0 acts transitively on L_b. So, for any such b, $L_b \subseteq (G_0 y G_0 y) * \mathbf{i} \subseteq K * \mathbf{i}$. Thus, $K * \mathbf{i}$ contains all latitudes above L_c.

To handle the latitudes below L_c, we will need:

$$\text{If } 0 \le a \le c, \text{ then } \; ca - s\sqrt{1-a^2} \;\le\; a - s^2 \;\le\; a \;\le\; ca + s\sqrt{1-a^2}. \tag{17}$$

To see this, note that since $0 \le a \le c \le 1$, we have $\sqrt{1-a^2} \ge \sqrt{1-c^2} = s$. Thus, $ca \le as\sqrt{1-a^2} \ge s^2$, yielding the first inequality in (17). The second inequality in (17) is clear. The third inequality in (17) is equivalent to $2a^2 \le 1 + c$, which holds as $2a^2 \le 2a$ (as $0 \le a \le 1$) and $2a \le 1 + c$ (as $a \le c$ and $a \le 1$).

The inequalities in (17) combined with (16) show that for all $a \in F$ with $0 \le a \le c$,

$$\text{for all } b \in F \text{ with } a - s^2 \le b \le a, \quad (y * L_a) \cap L_b \ne \varnothing, \;\text{ so }\; L_b \subseteq (G_0 y) * L_a. \tag{18}$$

Thus (taking $a = c$ in (18)), for b with for $c - s^2 \le b \le c$, we have

$$L_b \;\subseteq (G_0 y) * L_c \;=\; (G_0 y)^2 * \mathbf{i} \;\subseteq K * \mathbf{i}\,.$$

This gives what we need if $c - s^2 \leq 0$, so we may assume $c > s^2$. For an integer $k \geq 1$, with $c - ks^2 \geq 0$, suppose $L_b \subseteq K * \mathbf{i}$ for $c - ks^2 \leq b \leq c$. Then (taking $a = c - ks^2$ in (18)), for all b with $c - (k+1)s^2 \leq b \leq c - ks^2$, we have

$$L_b \ \subseteq \ (G_0 y) * L_{c-ks^2} \ \subseteq \ (G_0 y)K * \mathbf{i} \ = \ K * \mathbf{i}.$$

Hence, $L_b \subseteq K * \mathbf{i}$ for $c - (k+1)s^2 \leq b \leq c$. It follows by induction that for all positive integers $n \leq c/s^2$, $L_b \subseteq K * \mathbf{i}$ for all b with $c - (n+1)s^2 \leq b \leq c$.

Because $s \notin M$, s is a unit of the valuation ring V; so $c/s^2 \in V$. Hence, by the definition of V, there is a positive integer m with $c/s^2 < m$. Let $n+1$ be the smallest such m. Then, $n \leq c/s^2 < n+1$, and $n \geq 1$ as $c/s^2 > 1$. For this n, since $c - (n+1)s^2 \leq 0$, we proved in the previous paragraph that for all b with $0 \leq b \leq c$, we have $L_b \subseteq K * \mathbf{i}$. We proved this inclusion earlier for b with $c \leq b \leq 1$. This proves Claim 2, completing the proof of Claim 1 and Th. 15. □

We can now summarize what Th. 8 and Th. 15 combined tell us about a division ring D if D^* has no maximal subgroup:

Theorem 16. *Let D be a division ring finite-dimensional over its center F, and suppose D^* has no maximal subgroup. Then,*

(i) *If $\deg(D)$ is even, then $D \cong (\frac{-1,-1}{F}) \otimes_F E$, where E is a nontrivial division algebra of odd degree, and F is euclidean (so $\mathrm{char}(F) = 0$) with F^{*2} divisible.*
(ii) *If $\deg(D)$ is odd, then $\mathrm{char}(F) > 0$, $\mathrm{char}(F) \nmid \deg(D)$, and F^* is divisible.*
(iii) *In either case, there is an odd prime p dividing $\deg(D)$; for each such p, we have $[F(\mu_p) : F] \geq 4$ (so $p \geq 5$) and ${}_pBr(F)$ is generated by noncyclic algebras of degree p.*

Thus, to produce an example of a D^* with no maximal subgroup, one would have to find a field with a noncyclic division algebra of prime degree. The existence of such noncyclic division algebras is one of the oldest and most challenging questions in the theory of division algebras.

Acknowledgements. The first named author would like to acknowledge the support of Queens University PR grant and EPSRC. Part of the work for the paper was done while he was visiting the second named author at the University of California at San Diego in the Summers 2005 and 2006. He would like to thank him for his care and attention.

References

[1] S. Akbari, R. Ebrahimian, H. Momenaee Kermani, A. Salehi Golsefidy, *Maximal subgroups of* $\mathrm{GL}_n(D)$, J. Algebra, **259** (2003), 201–225
[2] S. Akbari, M. Mahdavi-Hezavehi, M.G. Mahmudi, *Maximal subgroups of* $\mathrm{GL}_1(D)$, J. Algebra, **217** (1999), 422–433.
[3] S. Akbari, M. Mahdavi-Hezavehi, *On the existence of normal maximal subgroups in division rings,* J. Pure Appl. Algebra, **171** (2002), 123–131.
[4] A. Albert, *Structure of Algebras*, American Math. Soc., Colloquium Publ., Providence, 1961.
[5] A. Amitsur, *Finite subgroups of division rings*, Trans. Amer. Math. Soc., **80**, (1955), 361–386.
[6] P. Draxl, *Skew fields*, London Mathematical Society Lecture Note Series **81**, Cambridge University Press, Cambridge, 1983.
[7] R. Ebrahimian, *Nilpotent maximal subgroups of* $\mathrm{GL}_n(D)$, J. Algebra, **280** (2004), 244–248.

[8] R. Hazrat, SK_1*-like functors for division algebras*, J. Algebra, **239** (2001), 573–588.
[9] R. Hazrat, M. Mahdavi-Hezavehi, B. Mirzaii, *Reduced K-theory and the group $G(D) = D^*/F^*D'$*, pp. 403–409 in Algebraic K-theory and its applications, ed. H. Bass, World Sci. Publishing, River Edge, NJ, 1999.
[10] R. Hazrat, U. Vishne, *Triviality of the functor $Coker(K_1(F) \to K_1(D))$ for division algebras*, Comm. Algebra, **33** (2005), 1427–1435.
[11] R. Hazrat, A. Wadsworth, *Nontriviality of certain quotients of K_1 groups of division algebras*, J. Algebra, **312** (2007), 354–361.
[12] B. Jacob, A. Wadsworth, *A new construction of noncrossed product algebras*, Trans. Amer. Math. Soc., **293** (1986), 693–721.
[13] B. Jacob, A. Wadsworth, *Division algebras over Henselian fields*, J. Algebra, **128** (1990), 126–179.
[14] N. Jacobson, *Finite-dimensional division algebras*, Springer-Verlag, Berlin, 1996.
[15] I. Kersten, *Brauergruppen von Körpern*, Vieweg, Braunschweig, Germany, 1990.
[16] T. Keshavarzipour, M. Mahdavi-Hezavehi, *On the non-triviality of $G(D)$ and the existence of maximal subgroups of* $\mathrm{GL}_1(D)$, J. Algebra, **285** (2005), 213–221.
[17] T. Y. Lam, *A first course in noncommutative rings*, Springer-Verlag, New York, 1991.
[18] M. Mahdavi-Hezavehi, *Free subgroups in maximal subgroups of* $\mathrm{GL}_1(D)$, J. Algebra, **241** (2001), 720–730.
[19] W. May, *Multiplicative groups of fields*, Proc. London Math. Soc. (3), **24** (1972), 295–306.
[20] A. S. Merkurjev, *Brauer groups of fields*, Comm. Algebra, **11** (1993), 2611–2624.
[21] A. Rapinchuk, Y. Segev, *Valuation-like maps and the congruence subgroup property*, Invent. Math., **144** (2001), 571–607.
[22] A. Rapinchuk, Y. Segev, G. Seitz, *Finite quotients of the multiplicative group of a finite dimensional division algebra are solvable*, J. Amer. Math. Soc., **15** (2002), 929–978.
[23] C. Riehm, *The norm 1 group of a p-adic division algebra*, Amer. J. Math., **92** (1970), 499–523.
[24] W. Scharlau, *Quadratic and Hermitian forms*, Springer-Verlag, Berlin, 1985.
[25] W. Scott, *On the multiplicative group of a division ring*, Proc. Amer. Math Soc., **8** (1957), 303–305.
[26] V. Srinivas, *Algebraic K-Theory*, 2nd ed., Birkhäuser, Boston, 1996.
[27] A. A. Suslin, *Algebraic K-theory and the norm residue homomorphism*, Itogi Nauki i Tekhniki, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Inform., **25** (1984), 112–207 (Russian); English trans.: J. Soviet Math., **30** (1985), 2556–2611.
[28] C. Stuth, *A generalization of the Cartan-Brauer-Hua theorem*, Proc. Amer. Math Soc., **15** (1964), 211–217.
[29] A. Wadsworth, *Valuation theory on finite dimensional division algebras*, pp. 385–449 in Valuation heory and its applications, Vol. I, eds. F.-V. Kuhlmann et. al., Fields Inst. Commun. **32**, Amer. Math. Soc., Providence, RI, 2002.

Department of Pure Mathematics, Queen's University, Belfast BT7 1NN, United Kingdom

E-mail address: `r.hazrat@qub.ac.uk`

Department of Mathematics, University of California at San Diego, La Jolla, California 92093-0112, U.S.A.

E-mail address: `arwadsworth@ucsd.edu`