A CHARACTERIZATION OF THE QUATERNIONS USING COMMUTATORS

Yoav Segev, Ben-Gurion university
joint work with Erwin Kleinfeld

Ischia group theory 2022
June 24, 2022

OUTLINE

Introduction

Let D be a quaternion division algebra over a field $\mathbb{F}$. Thus $D = \mathbb{F} + \mathbb{F}i + \mathbb{F}j + \mathbb{F}k$, with $i^2, j^2 \in \mathbb{F}$, and $k = ij = -ji$.

A pure quaternion is an element $p \in D$ such that $p \in \mathbb{F}i + \mathbb{F}j + \mathbb{F}k$.

It is easy to check that $p^2 \in \mathbb{F}$, for a pure quaternion p, and that given $x, y \in D$, the commutator $(x, y) = xy - yx$ is a pure quaternion.

In this talk we show that this characterizes the quaternion division algebras. (Note, we do not assume finite dimensionality.)

Introduction

Let D be a quaternion division algebra over a field $\mathbb{F}$. Thus $D = \mathbb{F} + \mathbb{F}i + \mathbb{F}j + \mathbb{F}k$, with $i^2, j^2 \in \mathbb{F}$, and $k = ij = -ji$.

A pure quaternion is an element $p \in D$ such that $p \in \mathbb{F}i + \mathbb{F}j + \mathbb{F}k$.

It is easy to check that $p^2 \in \mathbb{F}$, for a pure quaternion p, and that given $x, y \in D$, the commutator $(x, y) = xy - yx$ is a pure quaternion.

In this talk we show that this characterizes the quaternion division algebras. (Note, we do not assume finite dimensionality.)

Introduction

Let D be a quaternion division algebra over a field $\mathbb{F}$. Thus $D = \mathbb{F} + \mathbb{F}i + \mathbb{F}j + \mathbb{F}k$, with $i^2, j^2 \in \mathbb{F}$, and $k = ij = -ji$.

A pure quaternion is an element $p \in D$ such that $p \in \mathbb{F}i + \mathbb{F}j + \mathbb{F}k$.

It is easy to check that $p^2 \in \mathbb{F}$, for a pure quaternion p, and that given $x, y \in D$, the commutator $(x, y) = xy - yx$ is a pure quaternion.

In this talk we show that this characterizes the quaternion division algebras. (Note, we do not assume finite dimensionality.)

Introduction

Let D be a quaternion division algebra over a field $\mathbb{F}$. Thus $D = \mathbb{F} + \mathbb{F}i + \mathbb{F}j + \mathbb{F}k$, with $i^2, j^2 \in \mathbb{F}$, and $k = ij = -ji$.

A pure quaternion is an element $p \in D$ such that $p \in \mathbb{F}i + \mathbb{F}j + \mathbb{F}k$.

It is easy to check that $p^2 \in \mathbb{F}$, for a pure quaternion p, and that given $x, y \in D$, the commutator $(x, y) = xy - yx$ is a pure quaternion.

In this talk we show that this characterizes the quaternion division algebras. (Note, we do not assume finite dimensionality.)

MAIN THEOREM.

Let R be an associative ring with **1** *which is not commutative such that*

(I) *A non-zero commutator in R is not a divisor of zero in R;*

(II) $(x, y)^2 \in C$, *for all $x, y \in R$, where C is the center of R.*

Then

1. *R contains no divisors of zero.*
2. *If, in addition, the characteristic of R is not 2, then the localization of R at C is a quaternion division algebra, whose center is the fraction field of C.*

We note that if $x, y \in R$ are non-zero elements such that $xy = 0$, then we say that both x and y are zero divisors in R.

Proof of the main theorem

In this section R is an associative ring with **1** which is not commutative. We denote by C the center of R. We assume that:

(1) Non-zero commutators are not divisors of zero in R.

(2) Squares of commutators in R are in C.

LEMMA 1.

If $0 \neq c \in C$, then c is not a zero divisor in R.

PROOF.

Suppose $cr = 0$, and let $v := (x, y)$ be a non-zero commutator. Then $(vc)r = 0$, but $vc = (x, yc) \neq 0$, hence $r = 0$.. □

PROPOSITION 2.

Let $x \in R \setminus C$, and let $v = (x, y)$ be a non-zero commutator. Then

1. *$v + vx$ and vx are commutators.*
2. *$ax^2 + bx + c = 0$, for some $a, b, c \in C$, with a, c non-zero.*
3. *x is not a divisor of zero in R.*
4. *R contains no zero divisors.*

PROOF.

(1) We have $v + vx = v(\mathbf{1} + x) = (x, y(\mathbf{1} + x))$, and $vx = (x, yx)$.

(2) Let $\alpha := (v + vx)^2 = v^2 + v^2x + vxv + (vx)^2$. Then $\alpha \in C$. We have $\alpha x = (v^2 + (vx)^2)x + v^2x^2 + (vx)^2$. Letting $a := v^2$, $b := v^2 + (vx)^2 - \alpha$ and $c := (vx)^2$, we see that $a, b, c \in C$, and $ax^2 + bx + c = 0$, with $a \neq 0 \neq c$.

(3) Suppose that $xy = 0$, for some non-zero $y \in R$, then we immediately get that $cy = 0$, contradicting Lemma 1.

(4) This follows from (3) and Lemma 1.

Proposition 2.

Let $x \in R \setminus C$, and let $v = (x, y)$ be a non-zero commutator. Then

1. *$v + vx$ and vx are commutators.*
2. *$ax^2 + bx + c = 0$, for some $a, b, c \in C$, with a, c non-zero.*
3. *x is not a divisor of zero in R.*
4. *R contains no zero divisors.*

Proof.

(1) We have $v + vx = v(\mathbf{1} + x) = (x, y(\mathbf{1} + x))$, and $vx = (x, yx)$.

(2) Let $\alpha := (v + vx)^2 = v^2 + v^2x + vxv + (vx)^2$. Then $\alpha \in C$. We have $\alpha x = (v^2 + (vx)^2)x + v^2x^2 + (vx)^2$. Letting $a := v^2$, $b := v^2 + (vx)^2 - \alpha$ and $c := (vx)^2$, we see that $a, b, c \in C$, and $ax^2 + bx + c = 0$, with $a \neq 0 \neq c$.

(3) Suppose that $xy = 0$, for some non-zero $y \in R$, then we immediately get that $cy = 0$, contradicting Lemma 1.

(4) This follows from (3) and Lemma 1. $\square$

PROPOSITION 2.

Let $x \in R \setminus C$, and let $v = (x, y)$ be a non-zero commutator. Then

1. *$v + vx$ and vx are commutators.*
2. *$ax^2 + bx + c = 0$, for some $a, b, c \in C$, with a, c non-zero.*
3. *x is not a divisor of zero in R.*
4. *R contains no zero divisors.*

PROOF.

(1) We have $v + vx = v(\mathbf{1} + x) = (x, y(\mathbf{1} + x))$, and $vx = (x, yx)$.

(2) Let $\alpha := (v + vx)^2 = v^2 + v^2x + vxv + (vx)^2$. Then $\alpha \in C$. We have $\alpha x = (v^2 + (vx)^2)x + v^2x^2 + (vx)^2$. Letting $a := v^2$, $b := v^2 + (vx)^2 - \alpha$ and $c := (vx)^2$, we see that $a, b, c \in C$, and $ax^2 + bx + c = 0$, with $a \neq 0 \neq c$.

(3) Suppose that $xy = 0$, for some non-zero $y \in R$, then we immediately get that $cy = 0$, contradicting Lemma 1.

(4) This follows from (3) and Lemma 1.

PROPOSITION 2.

Let $x \in R \setminus C$, and let $v = (x, y)$ be a non-zero commutator. Then

1. *$v + vx$ and vx are commutators.*
2. *$ax^2 + bx + c = 0$, for some $a, b, c \in C$, with a, c non-zero.*
3. *x is not a divisor of zero in R.*
4. *R contains no zero divisors.*

PROOF.

(1) We have $v + vx = v(\mathbf{1} + x) = (x, y(\mathbf{1} + x))$, and $vx = (x, yx)$.

(2) Let $\alpha := (v + vx)^2 = v^2 + v^2x + vxv + (vx)^2$. Then $\alpha \in C$. We have $\alpha x = (v^2 + (vx)^2)x + v^2x^2 + (vx)^2$. Letting $a := v^2$, $b := v^2 + (vx)^2 - \alpha$ and $c := (vx)^2$, we see that $a, b, c \in C$, and $ax^2 + bx + c = 0$, with $a \neq 0 \neq c$.

(3) Suppose that $xy = 0$, for some non-zero $y \in R$, then we immediately get that $cy = 0$, contradicting Lemma 1.
(4) This follows from (3) and Lemma 1. □

Remark 3.

In view of Proposition 2(4), we can form the localization of R at C, $R//C$. This is the set of all formal fractions $x/c,\ x \in R,\ c \in C,\ c \neq 0$, with the obvious definitions: (i) $x/c = y/d$ if and only if $dx = cy$; (ii) $(x/c) + (y/d) = (dx + cy)/(cd)$; (iii) $(x/c)(y/d) = (xy)/(cd)$. It is easy to check that $r \mapsto r/\mathbf{1}$ is an embedding of R into $R//C$ and that the center of $R//C$ is the fraction field of C. Thus **from now on we replace R with $R//C$ and assume that C is a field.**

Next we construct a quaternion division algebra within R.

Lemma 4.

1. *There exists a comutator $i := (x, y)$ which is not in C.*
2. *For i as in (1), let $j := (i, s)$ be nonzero. Then $ij = -ji$.*
3. *Let $k := ij$. Then $\mathbf{Q} := C + Ci + Cj + Ck$ is a quaternion division algebra.*

Proof.

(1) Let $x \in R \setminus C$, and let $v := (x, y) \neq 0$. Suppose that $v \in C$, then $vx \notin C$, and $vx = (x, yx)$.

(2) Since $i \notin C$, there is $s \in R$, with $j := (i, s) \neq 0$. But then

$$ij = i(is - si) = i^2 s - isi = -(isi - si^2) = -ji.$$

(3) Since $i^2, j^2 \in C$, and $ij = -ji$, and since R has no zero divisors, part (3) holds. □

Lemma 4.

1. *There exists a comutator $i := (x, y)$ which is not in C.*
2. *For i as in (1), let $j := (i, s)$ be nonzero. Then $ij = -ji$.*
3. *Let $k := ij$. Then $\mathbf{Q} := C + Ci + Cj + Ck$ is a quaternion division algebra.*

Proof.

(1) Let $x \in R \setminus C$, and let $v := (x, y) \neq 0$. Suppose that $v \in C$, then $vx \notin C$, and $vx = (x, yx)$.

(2) Since $i \notin C$, there is $s \in R$, with $j := (i, s) \neq 0$. But then

$$ij = i(is - si) = i^2 s - isi = -(isi - si^2) = -ji.$$

(3) Since $i^2, j^2 \in C$, and $ij = -ji$, and since R has no zero divisors, part (3) holds. □

Lemma 4.

1. *There exists a comutator $i := (x, y)$ which is not in C.*
2. *For i as in (1), let $j := (i, s)$ be nonzero. Then $ij = -ji$.*
3. *Let $k := ij$. Then $\mathbf{Q} := C + Ci + Cj + Ck$ is a quaternion division algebra.*

Proof.

(1) Let $x \in R \setminus C$, and let $v := (x, y) \neq 0$. Suppose that $v \in C$, then $vx \notin C$, and $vx = (x, yx)$.

(2) Since $i \notin C$, there is $s \in R$, with $j := (i, s) \neq 0$. But then

$$ij = i(is - si) = i^2 s - isi = -(isi - si^2) = -ji.$$

(3) Since $i^2, j^2 \in C$, and $ij = -ji$, and since R has no zero divisors, part (3) holds. $\square$

From now on we let

$$\mathbf{Q} = C + Ci + Cj + Ck, \quad \text{as in Lemma 4.}$$

Proposition 5.

Assume that $\operatorname{char}(C) \neq 2$. *Then*

1. *If* $p \in R$ *satisfies*
$$(*) \quad pu + up = d_u \in C, \quad \text{for all } u \in \{i, j, k\},$$
then $p \in \mathbf{Q}$.
2. *If* $R \neq \mathbf{Q}$, *then there exists* $p \in R \setminus \mathbf{Q}$ *satisfying* $(*)$ *above.*
3. $R = \mathbf{Q}$.

Notice that (3) is immediate from (1) and (2).

1. If $p \in R$ satisfies
$$(*) \quad pu + up = d_u \in C, \quad \text{for all } u \in \{i, j, k\},$$
then $p \in \mathbf{Q}$.

PROOF.

(1) Set
$$m = p - (d_i/2i^2)i - (d_j/2j^2)j - (d_k/2k^2)k.$$
Then
$$mi+im = pi+ip-d_i-(d_j/2j^2)ji-(d_j/2j^2)ij-(d_k/2k^2)ki-(d_k/2k^2)ik = 0.$$
Similarly $mj + jm = 0 = mk + km$.
But then
$$0 = mk + km = mij + ijm = 2ijm = 2km.$$
Since $(C) \neq 2$, and R has no zero divisors we must have $m = 0$, so $p \in \mathbf{Q}$. □

1. If $p \in R$ satisfies
$$(*) \quad pu + up = d_u \in C, \quad \text{for all } u \in \{i, j, k\},$$
then $p \in \mathbf{Q}$.

PROOF.

(1) Set
$$m = p - (d_i/2i^2)i - (d_j/2j^2)j - (d_k/2k^2)k.$$
Then
$$mi + im = pi + ip - d_i - (d_j/2j^2)ji - (d_j/2j^2)ij - (d_k/2k^2)ki - (d_k/2k^2)ik = 0.$$
Similarly $mj + jm = 0 = mk + km$.
But then
$$0 = mk + km = mij + ijm = 2ijm = 2km.$$
Since $(C) \neq 2$, and R has no zero divisors we must have $m = 0$, so $p \in \mathbf{Q}$. □

2. If $R \neq \mathbf{Q}$, then there exists $p \in R \setminus \mathbf{Q}$ satisfying $(*)$ above.

PROOF.

(2) Let $x \in R \setminus \mathbf{Q}$. By Proposition 2(2), x satisfies a quadratic, and hence a monic quadratic equation $x^2 - bx + c = 0$. Let $p := x - b/2$. Then $p \notin \mathbf{Q}$, and $p^2 \in C$. Let $u \in \{i, j, k\}$. Then both $p + u$ and $p - u$ satisfy a quadratic equation over C. That is

$$(p+u)^2 = c_1(p+u) + c_2$$
$$(p-u)^2 = c_3(p-u) + c_4.$$

Adding we get

$$(c_1 + c_3)p + (c_1 - c_3)u + c_5 = 0, \quad \text{where } c_5 = c_2 + c_4 - 2p^2 - 2u^2 \in C.$$

Now $c_1 + c_3 = 0$, since $p \notin \mathbf{Q}$, and then $c_1 - c_3 = 0$, since $u \notin C$. We thus get that

$$pu + up = c_2 - p^2 - u^2 \in C.$$

2 If $R \neq \mathbf{Q}$, then there exists $p \in R \setminus \mathbf{Q}$ satisfying $(*)$ above.

PROOF.

(2) Let $x \in R \setminus \mathbf{Q}$. By Proposition 2(2), x satisfies a quadratic, and hence a monic quadratic equation $x^2 - bx + c = 0$. Let $p := x - b/2$. Then $p \notin \mathbf{Q}$, and $p^2 \in C$. Let $u \in \{i, j, k\}$. Then both $p + u$ and $p - u$ satisfy a quadratic equation over C. That is

$$(p+u)^2 = c_1(p+u) + c_2$$
$$(p-u)^2 = c_3(p-u) + c_4.$$

Adding we get

$$(c_1 + c_3)p + (c_1 - c_3)u + c_5 = 0, \quad \text{where } c_5 = c_2 + c_4 - 2p^2 - 2u^2 \in C.$$

Now $c_1 + c_3 = 0$, since $p \notin \mathbf{Q}$, and then $c_1 - c_3 = 0$, since $u \notin C$. We thus get that

$$pu + up = c_2 - p^2 - u^2 \in C.$$

2 If $R \neq \mathbf{Q}$, then there exists $p \in R \setminus \mathbf{Q}$ satisfying $(*)$ above.

Proof.

(2) Let $x \in R \setminus \mathbf{Q}$. By Proposition 2(2), x satisfies a quadratic, and hence a monic quadratic equation $x^2 - bx + c = 0$. Let $p := x - b/2$. Then $p \notin \mathbf{Q}$, and $p^2 \in C$. Let $u \in \{i, j, k\}$. Then both $p + u$ and $p - u$ satisfy a quadratic equation over C. That is

$$(p+u)^2 = c_1(p+u) + c_2$$
$$(p-u)^2 = c_3(p-u) + c_4.$$

Adding we get

$$(c_1 + c_3)p + (c_1 - c_3)u + c_5 = 0, \quad \text{where } c_5 = c_2 + c_4 - 2p^2 - 2u^2 \in C.$$

Now $c_1 + c_3 = 0$, since $p \notin \mathbf{Q}$, and then $c_1 - c_3 = 0$, since $u \notin C$. We thus get that

$$pu + up = c_2 - p^2 - u^2 \in C.$$

2. If $R \neq \mathbf{Q}$, then there exists $p \in R \setminus \mathbf{Q}$ satisfying $(*)$ above.

PROOF.

(2) Let $x \in R \setminus \mathbf{Q}$. By Proposition 2(2), x satisfies a quadratic, and hence a monic quadratic equation $x^2 - bx + c = 0$. Let $p := x - b/2$. Then $p \notin \mathbf{Q}$, and $p^2 \in C$. Let $u \in \{i, j, k\}$. Then both $p + u$ and $p - u$ satisfy a quadratic equation over C. That is

$$(p+u)^2 = c_1(p+u) + c_2$$
$$(p-u)^2 = c_3(p-u) + c_4.$$

Adding we get

$$(c_1 + c_3)p + (c_1 - c_3)u + c_5 = 0, \quad \text{where } c_5 = c_2 + c_4 - 2p^2 - 2u^2 \in C.$$

Now $c_1 + c_3 = 0$, since $p \notin \mathbf{Q}$, and then $c_1 - c_3 = 0$, since $u \notin C$. We thus get that

$$pu + up = c_2 - p^2 - u^2 \in C.$$

Proof of the Main Theorem.

Part (1) follows from and Proposition 2(4), and part (2) follows from Proposition 5(3). ∎

Thank you!

Proof of the Main Theorem.

Part (1) follows from and Proposition 2(4), and part (2) follows from Proposition 5(3). $\square$

Thank you!