Beyond octonions: Hic sunt leones (?)

Pepa Dvořák & Hanka Štěpánková

Basic definitions

- A ring $\mathcal{R}$ (not necessarily commutative or associative) is an **algebra over T** (T a commutative field), if

Basic definitions

- A ring $\mathcal{R}$ (not necessarily commutative or associative) is an **algebra over T** (T a commutative field), if
  1. $\mathcal{R}$ is a vector space over T

Basic definitions

- A ring $\mathcal{R}$ (not necessarily commutative or associative) is an **algebra over T** (T a commutative field), if
  1. $\mathcal{R}$ is a vector space over T
  2. $\forall t \in T; \forall r,\ s \in \mathcal{R}$: $t \cdot (r \cdot_R) = r \cdot_R (t \cdot s) = (t \cdot r) \cdot_R$

Basic definitions

- A ring $\mathcal{R}$ (not necessarily commutative or associative) is an **algebra over T** (T a commutative field), if
  1. $\mathcal{R}$ is a vector space over T
  2. $\forall t \in T; \forall r,\ s \in \mathcal{R}$: $t \cdot (r \cdot_R) = r \cdot_R (t \cdot s) = (t \cdot r) \cdot_R$
- An algebra $\mathcal{C}$ is a **composition algebra**, if

Basic definitions

- A ring $\mathcal{R}$ (not necessarily commutative or associative) is an **algebra over T** (T a commutative field), if
  1. $\mathcal{R}$ is a vector space over T
  2. $\forall t \in T; \forall r,\ s \in \mathcal{R}$: $t \cdot (r \cdot_R) = r \cdot_R (t \cdot s) = (t \cdot r) \cdot_R$
- An algebra $\mathcal{C}$ is a **composition algebra**, if
  1. $\mathcal{C}$ is a unitary $\mathbb{R}$-algebra

Basic definitions

- A ring $\mathcal{R}$ (not necessarily commutative or associative) is an **algebra over T** (T a commutative field), if
  1. $\mathcal{R}$ is a vector space over T
  2. $\forall t \in T; \forall r,\ s \in \mathcal{R}$: $t \cdot (r \cdot_R) = r \cdot_R (t \cdot s) = (t \cdot r) \cdot_R$
- An algebra $\mathcal{C}$ is a **composition algebra**, if
  1. $\mathcal{C}$ is a unitary $\mathbb{R}$-algebra
  2. there exists a non-degenerate quadratic form $|\cdot|$, which satisfies: $\forall c, d \in \mathcal{C}\ |cd| = |c|\,|d|$

The scalar product

- For a composition algebra $\mathcal{C}$ we define a **scalar product** $|\cdot,\cdot|$ as the polar bilinear form of $|\cdot|$.

The scalar product

- For a composition algebra $\mathcal{C}$ we define a **scalar product** $|\cdot,\cdot|$ as the polar bilinear form of $|\cdot|$, i.e.

$$|c,d| := \frac{|c+d| - |c| - |d|}{2}.$$

The scalar product

- For a composition algebra $\mathcal{C}$ we define a **scalar product** $|\cdot,\cdot|$ as the polar bilinear form of $|\cdot|$, i.e.

$$|c,d| := \frac{|c+d| - |c| - |d|}{2}.$$

Note: $|c,c| = 0 \Leftrightarrow c = 0$

The scalar product

- For a composition algebra $\mathcal{C}$ we define a **scalar product** $|\cdot,\cdot|$ as the polar bilinear form of $|\cdot|$, i.e.

$$|c,d| := \frac{|c+d| - |c| - |d|}{2}.$$

  Note: $|c,c| = 0 \Leftrightarrow c = 0$
- Corollary: We know now what "**orthogonality**" means.

Properties of $|\cdot, \cdot|$

- If for all $t \in \mathcal{C}$ $|c, t| = |d, t|$, then $c = d$.

Properties of $|\cdot,\cdot|$

- If for all $t \in \mathcal{C}$ $|c,t| = |d,t|$, then $c = d$.
- $|cd, ce| = |c|\,|d,e|$ and $|dc, ec| = |d,e|\,|c|$

Properties of $|\cdot,\cdot|$

- If for all $t \in \mathcal{C}$ $|c,t| = |d,t|$, then $c = d$.
- $|cd, ce| = |c|\,|d,e|$ and $|dc, ec| = |d,e|\,|c|$
- $|cd, ef| = 2\,|c,e|\,|d,f| - |cf, ed|$

Properties of $|\cdot,\cdot|$

- If for all $t \in \mathcal{C}$ $|c,t| = |d,t|$, then $c = d$.
- $|cd, ce| = |c|\,|d,e|$ and $|dc, ec| = |d,e|\,|c|$
- $|cd, ef| = 2\,|c,e|\,|d,f| - |cf, ed|$
  Proof: $|cd + ed, ef + cf|$

Properties of $|\cdot,\cdot|$

- If for all $t \in \mathcal{C}$ $|c,t| = |d,t|$, then $c = d$.
- $|cd, ce| = |c|\,|d,e|$ and $|dc, ec| = |d,e|\,|c|$
- $|cd, ef| = 2\,|c,e|\,|d,f| - |cf, ed|$
  Proof: $|cd + ed, ef + cf| =$
  $= |cd, ef| + |c|\,|d,f| + |e|\,|d,f| + |ed, cf|$

Properties of $|\cdot,\cdot|$

- If for all $t \in \mathcal{C}$ $|c,t| = |d,t|$, then $c = d$.
- $|cd, ce| = |c|\,|d,e|$ and $|dc, ec| = |d,e|\,|c|$
- $|cd, ef| = 2\,|c,e|\,|d,f| - |cf, ed|$
  Proof: $|cd + ed, ef + cf| =$
  $= |cd, ef| + |c|\,|d,f| + |e|\,|d,f| + |ed, cf|$, therefore
  $|cd, ef| = |c+e|\,|d,f| - |c|\,|d,f| - |e|\,|d,f| - |ed, cf|$

Properties of $|\cdot,\cdot|$

- If for all $t \in \mathcal{C}$ $|c,t| = |d,t|$, then $c = d$.
- $|cd, ce| = |c|\,|d,e|$ and $|dc, ec| = |d,e|\,|c|$
- $|cd, ef| = 2\,|c,e|\,|d,f| - |cf, ed|$
  Proof: $|cd + ed, ef + cf| =$
  $= |cd, ef| + |c|\,|d,f| + |e|\,|d,f| + |ed, cf|$, therefore
  $|cd, ef| = |c+e|\,|d,f| - |c|\,|d,f| - |e|\,|d,f| - |ed, cf| \;=$
  $= (|c+e| - |c| - |e|)\,|d,f| - |ed, cf|$

Conjugation

- For $c \in \mathcal{C}$ we define $\bar{c} := 2\,|c, 1| - c$ (a **conjugate of** c).

Conjugation

- For $c \in \mathcal{C}$ we define $\bar{c} := 2\,|c, 1| - c$ (a **conjugate of** c). Note: the usual conjugation in $\mathbb{C}$ is coherent with this definition.

Properties of conjugation

- $|cd, e| = |d, \bar{c}e|$ and $|cd, e| = |c, e\bar{d}|$

Properties of conjugation

- $|cd, e| = |d, \bar{c}e|$ and $|cd, e| = \left|c, e\bar{d}\right|$
  Proof: $|cd, e| =$

Properties of conjugation

- $|cd, e| = |d, \bar{c}e|$ and $|cd, e| = \left|c, e\bar{d}\right|$
  Proof: $|cd, e| = 2\,|c, 1|\,|d, e| - |ce, d|$

Properties of conjugation

- $|cd, e| = |d, \bar{c}e|$ and $|cd, e| = \left|c, e\bar{d}\right|$
  Proof: $|cd, e| = 2\,|c, 1|\,|d, e| - |ce, d|$
  $= |d, (2\,|c, 1|)\, e| - |d, ce|$

Properties of conjugation

- $|cd, e| = |d, \bar{c}e|$ and $|cd, e| = \left|c, e\bar{d}\right|$
  Proof: $|cd, e| = 2\,|c, 1|\,|d, e| - |ce, d|$
  $= |d, (2\,|c, 1|)\,e| - |d, ce| = |d, (2\,|c, 1| - c)\,e|$

Properties of conjugation

- $|cd, e| = |d, \bar{c}e|$ and $|cd, e| = |c, e\bar{d}|$
  Proof: $|cd, e| = 2\,|c, 1|\,|d, e| - |ce, d|$
  $= |d, (2\,|c, 1|)\,e| - |d, ce| = |d, (2\,|c, 1| - c)\,e| = |d, \bar{c}e|$

Properties of conjugation

- $|cd, e| = |d, \bar{c}e|$ and $|cd, e| = \left|c, e\bar{d}\right|$

Properties of conjugation

- $|cd, e| = |d, \bar{c}e|$ and $|cd, e| = \left|c, e\bar{d}\right|$
- $\bar{\bar{c}} = c$

Properties of conjugation

- $|cd, e| = |d, \bar{c}e|$ and $|cd, e| = |c, e\bar{d}|$
- $\bar{\bar{c}} = c$
  Proof: take arbitrary $t \in \mathcal{C}$;
  $|x, t| = |1, \bar{x}t| = |\bar{x}t, 1| = |t, \bar{\bar{x}}| = |\bar{\bar{x}}, t|$

Properties of conjugation

- $|cd, e| = |d, \bar{c}e|$ and $|cd, e| = \left|c, e\bar{d}\right|$
- $\bar{\bar{c}} = c$
- $\overline{(ce)} = \bar{e}\,\bar{c}$

Definition

- Let $\mathcal{C}$ be a composition algebra and $\mathcal{D}$ its n-dimensional proper subalgebra containing 1. Let $i \in \mathcal{C}$ be a unit element orthogonal to $\mathcal{D}$. The **Dickson double algebra** of $\mathcal{D}$ is $\mathcal{D} + i\mathcal{D} = \{a + ib \mid a, b \in \mathcal{D}\}$.

Definition

- Let $\mathcal{C}$ be a composition algebra and $\mathcal{D}$ its n-dimensional proper subalgebra containing 1. Let $i \in \mathcal{C}$ be a unit element orthogonal to $\mathcal{D}$. The **Dickson double algebra** of $\mathcal{D}$ is $\mathcal{D} + i\mathcal{D} = \{a + ib \mid a, b \in \mathcal{D}\}$.
- it is always possible to find such an i

Definition

- Let $\mathcal{C}$ be a composition algebra and $\mathcal{D}$ its n-dimensional proper subalgebra containing 1. Let $i \in \mathcal{C}$ be a unit element orthogonal to $\mathcal{D}$. The **Dickson double algebra** of $\mathcal{D}$ is $\mathcal{D} + i\mathcal{D} = \{a + ib \mid a, b \in \mathcal{D}\}$.
- it is always possible to find such an i
- $|a, i| = 0$ for every $a \in \mathcal{D}$

Definition

- Let $\mathcal{C}$ be a composition algebra and $\mathcal{D}$ its n-dimensional proper subalgebra containing 1. Let $i \in \mathcal{C}$ be a unit element orthogonal to $\mathcal{D}$. The **Dickson double algebra** of $\mathcal{D}$ is $\mathcal{D} + i\mathcal{D} = \{a + ib \mid a, b \in \mathcal{D}\}$.
- it is always possible to find such an i
- $|a, i| = 0$ for every $a \in \mathcal{D}$
- $\bar{i} = -i$

Properties of the Dickson double algebra I.

- $|a + ib, c + id| = |a, c| + |b, d|$

Properties of the Dickson double algebra I.

- $|a + ib, c + id| = |a, c| + |b, d|$
  Proof: $|a + ib, c + id|$

Properties of the Dickson double algebra I.

- $|a + ib, c + id| = |a, c| + |b, d|$
  Proof: $|a + ib, c + id| = |a, c| + |a, id| + |ib, c| + |ib, id|$

Properties of the Dickson double algebra I.

- $|a+ib, c+id| = |a,c| + |b,d|$
  Proof: $|a+ib, c+id| = |a,c| + |a,id| + |ib,c| + |ib,id| =$
  $\overset{M2,C1}{=} |a,c| + 0 + 0 + |i|\,|b,d|$

Properties of the Dickson double algebra I.

- $|a+ib, c+id| = |a,c| + |b,d|$
  Proof: $|a+ib, c+id| = |a,c| + |a,id| + |ib,c| + |ib,id| \overset{M2,C1}{=} |a,c| + 0 + 0 + |i|\,|b,d| = |a,c| + |b,d|$

Properties of the Dickson double algebra I.

- $|a + ib, c + id| = |a, c| + |b, d|$
- $\overline{a + ib} = \overline{a} - ib$

Properties of the Dickson double algebra I.

- $|a + ib, c + id| = |a, c| + |b, d|$
- $\overline{a + ib} = \overline{a} - ib$
  Proof: $2\,|a + ib, 1| - a - ib$

Properties of the Dickson double algebra I.

- $|a + ib, c + id| = |a, c| + |b, d|$

- $\overline{a + ib} = \overline{a} - ib$
  Proof: $2\,|a + ib, 1| - a - ib = 2\,|a, 1| + 2\,|ib, 1| - a - ib =$

Properties of the Dickson double algebra I.

- $|a + ib, c + id| = |a, c| + |b, d|$
- $\overline{a + ib} = \overline{a} - ib$
  Proof: $2\,|a + ib, 1| - a - ib = 2\,|a, 1| + 2\,|ib, 1| - a - ib =$
  $= \overline{a} - ib$

Properties of the Dickson double algebra I.

- $|a + ib, c + id| = |a, c| + |b, d|$
- $\overline{a + ib} = \overline{a} - ib$

Properties of the Dickson double algebra I.

- $|a + ib, c + id| = |a, c| + |b, d|$
- $\overline{a + ib} = \overline{a} - ib$
- Corollary: we have $ib = -\overline{ib} = -\overline{b}\overline{i} = \overline{b}i$.

Properties of the Dickson double algebra II.

- $\mathcal{D} + i\mathcal{D}$ is closed under multiplication:
$$(a + ib)(c + id) = \left(ac - d\overline{b}\right) + i\,(cb + \overline{a}d)$$

Properties of the Dickson double algebra II.

- $\mathcal{D} + i\mathcal{D}$ is closed under multiplication:
  $$(a + ib)(c + id) = \left(ac - d\overline{b}\right) + i\,(cb + \overline{a}d)$$
  Proof: $(a + ib)(c + id)$

Properties of the Dickson double algebra II.

- $\mathcal{D} + i\mathcal{D}$ is closed under multiplication:
$$(a+ib)(c+id) = \left(ac - d\overline{b}\right) + i\,(cb + \overline{a}d)$$
Proof: $(a+ib)(c+id) = ac + (ib)\,c + a\,(id) + (ib)\,(id)$

Properties of the Dickson double algebra II.

- $\mathcal{D} + i\mathcal{D}$ is closed under multiplication:
$$(a+ib)(c+id) = \left(ac - d\overline{b}\right) + i\left(cb + \overline{a}d\right)$$
Proof: $(a+ib)(c+id) = ac + (ib)c + a(id) + (ib)(id)$
We need to show that these equalities stand for every $t \in \mathcal{D}$:
    1. $|(ib)c, t| = |i(cb), t|$
    2. $|a(id), t| = |i(\overline{a}d), t|$
    3. $|(ib)(id), t| = \left|-d\overline{b}, t\right|$

Properties of the Dickson double algebra II.

- $\mathcal{D} + i\mathcal{D}$ is closed under multiplication:
$$(a + ib)(c + id) = \left(ac - d\overline{b}\right) + i\left(cb + \overline{a}d\right)$$
Proof: $(a + ib)(c + id) = ac + (ib)c + a(id) + (ib)(id)$
We need to show that these equalities stand for every $t \in \mathcal{D}$:
  1. $|(ib)c, t| = |i(cb), t|$
  2. $|a(id), t| = |i(\overline{a}d), t|$
  3. $|(ib)(id), t| = \left|-d\overline{b}, t\right|$

$|(ib)(id), t|$

Properties of the Dickson double algebra II.

- $\mathcal{D} + i\mathcal{D}$ is closed under multiplication:

$$(a+ib)(c+id) = \left(ac - d\overline{b}\right) + i\left(cb + \overline{a}d\right)$$

Proof: $(a+ib)(c+id) = ac + (ib)c + a(id) + (ib)(id)$
We need to show that these equalities stand for every $t \in \mathcal{D}$:

1. $|(ib)c, t| = |i(cb), t|$
2. $|a(id), t| = |i(\overline{a}d), t|$
3. $|(ib)(id), t| = \left|-d\overline{b}, t\right|$

$$|(ib)(id), t| \overset{C1}{=} \left|ib, t\left(\overline{id}\right)\right|$$

Properties of the Dickson double algebra II.

- $\mathcal{D} + i\mathcal{D}$ is closed under multiplication:

$$(a + ib)(c + id) = \left(ac - d\overline{b}\right) + i\left(cb + \overline{a}d\right)$$

Proof: $(a + ib)(c + id) = ac + (ib)c + a(id) + (ib)(id)$

We need to show that these equalities stand for every $t \in \mathcal{D}$:

1. $|(ib)c, t| = |i(cb), t|$
2. $|a(id), t| = |i(\overline{a}d), t|$
3. $|(ib)(id), t| = \left|-d\overline{b}, t\right|$

$$|(ib)(id), t| \overset{C1}{=} \left|ib, t\left(\overline{id}\right)\right| \overset{D2}{=} -|ib, t(id)|$$

Properties of the Dickson double algebra II.

- $\mathcal{D} + i\mathcal{D}$ is closed under multiplication:
$$(a+ib)(c+id) = \left(ac - d\overline{b}\right) + i\left(cb + \overline{a}d\right)$$
Proof: $(a+ib)(c+id) = ac + (ib)\,c + a\,(id) + (ib)\,(id)$
We need to show that these equalities stand for every $t \in \mathcal{D}$:
    1. $|(ib)\,c, t| = |i\,(cb), t|$
    2. $|a\,(id), t| = |i\,(\overline{a}d), t|$
    3. $|(ib)\,(id), t| = \left|-d\overline{b}, t\right|$

$|(ib)\,(id), t| \stackrel{C1}{=} \left|ib, t\left(\overline{id}\right)\right| \stackrel{D2}{=} -|ib, t\,(id)|$
$\stackrel{M3}{=} -2\,|i, t|\,|id, b| + |i\,(id), tb|$

Properties of the Dickson double algebra II.

- $\mathcal{D} + i\mathcal{D}$ is closed under multiplication:
$$(a+ib)(c+id) = \left(ac - d\overline{b}\right) + i\left(cb + \overline{a}d\right)$$
Proof: $(a+ib)(c+id) = ac + (ib)c + a(id) + (ib)(id)$
We need to show that these equalities stand for every $t \in \mathcal{D}$:
  1. $|(ib)c, t| = |i(cb), t|$
  2. $|a(id), t| = |i(\overline{a}d), t|$
  3. $|(ib)(id), t| = \left|-d\overline{b}, t\right|$

$|(ib)(id), t| \overset{C1}{=} \left|ib, t\left(\overline{id}\right)\right| \overset{D2}{=} -|ib, t(id)|$
$\overset{M3}{=} -2|i,t||id,b| + |i(id), tb| \overset{C1}{=} 0 - |id, i(tb)|$

Properties of the Dickson double algebra II.

- $\mathcal{D} + i\mathcal{D}$ is closed under multiplication:

$$(a + ib)(c + id) = \left(ac - d\overline{b}\right) + i\left(cb + \overline{a}d\right)$$

Proof: $(a + ib)(c + id) = ac + (ib)c + a(id) + (ib)(id)$

We need to show that these equalities stand for every $t \in \mathcal{D}$:

1. $|(ib)c, t| = |i(cb), t|$
2. $|a(id), t| = |i(\overline{a}d), t|$
3. $|(ib)(id), t| = \left|-d\overline{b}, t\right|$

$$|(ib)(id), t| \overset{C1}{=} \left|ib, t\left(\overline{id}\right)\right| \overset{D2}{=} -|ib, t(id)|$$

$$\overset{M3}{=} -2|i, t||id, b| + |i(id), tb| \overset{C1}{=} 0 - |id, i(tb)| \overset{M2}{=} -|i||d, tb|$$

Properties of the Dickson double algebra II.

- $\mathcal{D} + i\mathcal{D}$ is closed under multiplication:

$$(a+ib)(c+id) = \left(ac - d\overline{b}\right) + i\left(cb + \overline{a}d\right)$$

Proof: $(a+ib)(c+id) = ac + (ib)c + a(id) + (ib)(id)$

We need to show that these equalities stand for every $t \in \mathcal{D}$:

1. $|(ib)c, t| = |i(cb), t|$
2. $|a(id), t| = |i(\overline{a}d), t|$
3. $|(ib)(id), t| = \left|-d\overline{b}, t\right|$

$$\left|(ib)(id), t\right| \overset{C1}{=} \left|ib, t\left(\overline{id}\right)\right| \overset{D2}{=} -\left|ib, t(id)\right|$$

$$\overset{M3}{=} -2|i,t||id,b| + |i(id), tb| \overset{C1}{=} 0 - |id, i(tb)| \overset{M2}{=} -|i||d, tb|$$

$$\overset{C1}{=} \left|-d\overline{b}, t\right|$$

Properties of the Dickson double algebra II.

- $\mathcal{D} + i\mathcal{D}$ is closed under multiplication:

$$(a+ib)(c+id) = \left(ac - d\overline{b}\right) + i\left(cb + \overline{a}d\right)$$

Proof: $(a+ib)(c+id) = ac + (ib)c + a(id) + (ib)(id)$

We need to show that these equalities stand for every $t \in \mathcal{D}$:

1. $|(ib)c, t| = |i(cb), t|$
2. $|a(id), t| = |i(\overline{a}d), t|$
3. $|(ib)(id), t| = \left|-d\overline{b}, t\right|$

$$|(ib)(id), t| \overset{C1}{=} \left|ib, t\left(\overline{id}\right)\right| \overset{D2}{=} -|ib, t(id)|$$

$$\overset{M3}{=} -2|i,t|\,|id,b| + |i(id), tb| \overset{C1}{=} 0 - |id, i(tb)| \overset{M2}{=} -|i|\,|d, tb|$$

$$\overset{C1}{=} \left|-d\overline{b}, t\right|$$

1. and 2. are proved similarly

Properties of the Dickson double algebra II.

- $\mathcal{D} + i\mathcal{D}$ is closed under multiplication:
$$(a + ib)(c + id) = \left(ac - d\overline{b}\right) + i\,(cb + \overline{a}d)$$

- Corollary: Let $\mathcal{D}$ be a proper subalgebra of a composition algebra $\mathcal{C}$ and let $\mathcal{D} + i\mathcal{D}$ be its Dickinson double algebra. Then $\mathcal{D} + i\mathcal{D}$ is also a subalgebra of $\mathcal{D}$.

The Hurwitz's theorem (1898)

The Hurwitz's theorem (1898)

- The only finitely-dimensional composition algebras are (up to isomorphisms): $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$.

Lemma 1

- Let $\mathcal{D}$ be a proper n-dimensional ($n \in \mathbb{N}$) subalgebra of a composition algebra $\mathcal{C}$ and let $i \in \mathcal{D}^{\perp}$. Then
$$dim\,(\mathcal{D} + i\mathcal{D}) = 2n.$$

Lemma 1

- Let $\mathcal{D}$ be a proper n-dimensional ($n \in \mathbb{N}$) subalgebra of a composition algebra $\mathcal{C}$ and let $i \in \mathcal{D}^{\perp}$. Then
$$dim\,(\mathcal{D} + i\mathcal{D}) = 2n.$$
Proof:Let $a, b \in \mathcal{D}$. Is $a \perp ib$?

Lemma 1

- Let $\mathcal{D}$ be a proper n-dimensional ($n \in \mathbb{N}$) subalgebra of a composition algebra $\mathcal{C}$ and let $i \in \mathcal{D}^{\perp}$. Then
$$dim\left(\mathcal{D} + i\mathcal{D}\right) = 2n.$$
Proof:Let $a, b \in \mathcal{D}$. Is $a \perp ib$?
We have $|a, ib| = \left|a\overline{b}, i\right| = 0$.

Lemma 1

- Let $\mathcal{D}$ be a proper n-dimensional ($n \in \mathbb{N}$) subalgebra of a composition algebra $\mathcal{C}$ and let $i \in \mathcal{D}^{\perp}$. Then
$$dim\,(\mathcal{D} + i\mathcal{D}) = 2n.$$

Lemma 1

- Let $\mathcal{D}$ be a proper n-dimensional ($n \in \mathbb{N}$) subalgebra of a composition algebra $\mathcal{C}$ and let $i \in \mathcal{D}^{\perp}$. Then
$$dim\,(\mathcal{D} + i\mathcal{D}) = 2n.$$
- Corollary: Let $\mathcal{C}$ be a composition algebra of a finite dimension. Then $dim\,(\mathcal{C}) = 2^k$ for some $k \in \mathbb{N}$.

Lemma 1

- Let $\mathcal{D}$ be a proper n-dimensional ($n \in \mathbb{N}$) subalgebra of a composition algebra $\mathcal{C}$ and let $i \in \mathcal{D}^{\perp}$. Then
$$dim\,(\mathcal{D} + i\mathcal{D}) = 2n.$$

- Corollary: Let $\mathcal{C}$ be a composition algebra of a finite dimension. Then $dim\,(\mathcal{C}) = 2^k$ for some $k \in \mathbb{N}$.
Proof: Recall that $\mathcal{C}$ is an algebra over $\mathbb{R}$.

Lemma 1

- Let $\mathcal{D}$ be a proper n-dimensional ($n \in \mathbb{N}$) subalgebra of a composition algebra $\mathcal{C}$ and let $i \in \mathcal{D}^{\perp}$. Then
$$dim\,(\mathcal{D} + i\mathcal{D}) = 2n.$$

- Corollary: Let $\mathcal{C}$ be a composition algebra of a finite dimension. Then $dim\,(\mathcal{C}) = 2^k$ for some $k \in \mathbb{N}$.
Proof: Recall that $\mathcal{C}$ is an algebra over $\mathbb{R}$. $\mathbb{R}$ is therefore a proper subalgebra of $\mathcal{C}$.

Lemma 2

- Let $\mathcal{D} = \mathcal{F} + i\mathcal{F}$ ($i \in \mathcal{F}^{\perp}$ is a unitary vector) be a Dickson algebra. Then $\mathcal{D}$ is a composition algebra iff $\mathcal{F}$ is an associative composition algebra.

Lemma 2, The proof

Proof: $\mathcal{D} = \mathcal{F} + i\mathcal{F}$ is a composition algebra iff it satisfies:

$$|xy| = |x|\,|y| \;\; \forall x, y \in \mathcal{D}.$$

Lemma 2, The proof

Proof: $\mathcal{D} = \mathcal{F} + i\mathcal{F}$ is a composition algebra iff it satisfies:

$$|xy| = |x|\,|y| \ \forall x, y \in \mathcal{D}.$$

It means, written in terms of $\mathcal{F}$:

$$|(a+ib)(c+id)| = |a+ib|\,|c+id| \ \forall a, b, c, d \in \mathcal{F}$$

Lemma 2, The proof

Proof: $\mathcal{D} = \mathcal{F} + i\mathcal{F}$ is a composition algebra iff it satisfies:

$$|xy| = |x|\,|y| \;\; \forall x, y \in \mathcal{D}.$$

It means, written in terms of $\mathcal{F}$:
$|(a + ib)(c + id)| = |a + ib|\,|c + id| \;\; \forall a, b, c, d \in \mathcal{F}$
We have $\left|(ac - d\overline{b}) + i(cb + \overline{a}d)\right| = |a + ib|\,|c + id|$

Lemma 2, The proof

Proof: $\mathcal{D} = \mathcal{F} + i\mathcal{F}$ is a composition algebra iff it satisfies:

$$|xy| = |x|\,|y| \ \ \forall x, y \in \mathcal{D}.$$

It means, written in terms of $\mathcal{F}$:

$|(a+ib)(c+id)| = |a+ib|\,|c+id| \ \ \forall a, b, c, d \in \mathcal{F}$

We have $\left|(ac - d\bar{b}) + i(cb + \bar{a}d)\right| = |a+ib|\,|c+id|$

We have also: $|x+y| = |x| + |y| + 2\,|x, y|$.

Lemma 2, The proof

Proof: $\mathcal{D} = \mathcal{F} + i\mathcal{F}$ is a composition algebra iff it satisfies:

$$|xy| = |x|\,|y| \;\; \forall x, y \in \mathcal{D}.$$

It means, written in terms of $\mathcal{F}$:
$|(a + ib)(c + id)| = |a + ib|\,|c + id| \;\; \forall a, b, c, d \in \mathcal{F}$
We have $\left|(ac - d\bar{b}) + i(cb + \bar{a}d)\right| = |a + ib|\,|c + id|$
We have also: $|x + y| = |x| + |y| + 2\,|x, y|$.
We get $|ac| + \left|d\bar{b}\right| - 2\left|ac, d\bar{b}\right| + |cb| + |\bar{a}d| + 2\,|cb, \bar{a}d|$

Lemma 2, The proof

Proof: $\mathcal{D} = \mathcal{F} + i\mathcal{F}$ is a composition algebra iff it satisfies:

$$|xy| = |x|\,|y| \ \ \forall x, y \in \mathcal{D}.$$

It means, written in terms of $\mathcal{F}$:
$|(a+ib)(c+id)| = |a+ib|\,|c+id| \ \ \forall a,b,c,d \in \mathcal{F}$
We have $\left|(ac - d\bar{b}) + i(cb + \bar{a}d)\right| = |a+ib|\,|c+id|$
We have also: $|x+y| = |x| + |y| + 2\,|x,y|$.
We get $|ac| + \left|d\bar{b}\right| - 2\left|ac, d\bar{b}\right| + |cb| + |\bar{a}d| + 2\,|cb, \bar{a}d| =$
$= |a|\,|c| + |a|\,|d| + |b|\,|c| + |b|\,|d|$

Lemma 2, The proof

Proof: $\mathcal{D} = \mathcal{F} + i\mathcal{F}$ is a composition algebra iff it satisfies:

$$|xy| = |x|\,|y| \;\; \forall x, y \in \mathcal{D}.$$

It means, written in terms of $\mathcal{F}$:

$|(a + ib)(c + id)| = |a + ib|\,|c + id| \;\; \forall a, b, c, d \in \mathcal{F}$

We have $\left|(ac - d\overline{b}) + i(cb + \overline{a}d)\right| = |a + ib|\,|c + id|$

We have also: $|x + y| = |x| + |y| + 2\,|x, y|$.

We get $|ac| + \left|d\overline{b}\right| - 2\left|ac, d\overline{b}\right| + |cb| + |\overline{a}d| + 2\,|cb, \overline{a}d| =$

$= |a|\,|c| + |a|\,|d| + |b|\,|c| + |b|\,|d|$

$$\left|ac, d\overline{b}\right| = |cb, \overline{a}d|$$

Lemma 2, The proof

Proof: $\mathcal{D} = \mathcal{F} + i\mathcal{F}$ is a composition algebra iff it satisfies:

$$|xy| = |x|\,|y| \;\; \forall x, y \in \mathcal{D}.$$

It means, written in terms of $\mathcal{F}$:
$|(a+ib)(c+id)| = |a+ib|\,|c+id| \;\; \forall a, b, c, d \in \mathcal{F}$
We have $\left|(ac - d\bar{b}) + i(cb + \bar{a}d)\right| = |a+ib|\,|c+id|$
We have also: $|x+y| = |x| + |y| + 2\,|x, y|$.
We get $|ac| + \left|d\bar{b}\right| - 2\left|ac, d\bar{b}\right| + |cb| + |\bar{a}d| + 2\,|cb, \bar{a}d| =$
$= |a|\,|c| + |a|\,|d| + |b|\,|c| + |b|\,|d|$

$$\left|ac, d\bar{b}\right| = |cb, \bar{a}d|$$

And finally: $(ac)b = a(cb)$, which is true iff $\mathcal{F}$ is an associative composition algebra.

Lemma 3

- Let $\mathcal{D} := \mathcal{F} + i\mathcal{F}$ ($i \in \mathcal{F}^{\perp}$ is a unitary vector) be a Dickson algebra. Then $\mathcal{D}$ is an associative composition algebra iff $\mathcal{F}$ is a commutative and associative composition algebra.

Lemma 3

- Let $\mathcal{D} := \mathcal{F} + i\mathcal{F}$ ($i \in \mathcal{F}^{\perp}$ is a unitary vector) be a Dickson algebra. Then $\mathcal{D}$ is an associative composition algebra iff $\mathcal{F}$ is a commutative and associative composition algebra.
  Proof: "$\Rightarrow$":

Lemma 3

- Let $\mathcal{D} := \mathcal{F} + i\mathcal{F}$ ($i \in \mathcal{F}^{\perp}$ is a unitary vector) be a Dickson algebra. Then $\mathcal{D}$ is an associative composition algebra iff $\mathcal{F}$ is a commutative and associative composition algebra.
  Proof: "$\Rightarrow$": We have: $(ib)\,c = i\,(cb)$ (for $b, c \in \mathcal{F}$);

Lemma 3

- Let $\mathcal{D} := \mathcal{F} + i\mathcal{F}$ ($i \in \mathcal{F}^{\perp}$ is a unitary vector) be a Dickson algebra. Then $\mathcal{D}$ is an associative composition algebra iff $\mathcal{F}$ is a commutative and associative composition algebra.
  Proof: "$\Rightarrow$": We have: $(ib)\,c = i\,(cb)$ (for $b, c \in \mathcal{F}$); by associativity of $\mathcal{D}$ we get $i\,(bc) = i\,(cb)$.

Lemma 3, The proof

- "$\Leftarrow$":

Lemma 3, The proof

- "$\Leftarrow$": We want:

$$[(a+ib)(c+id)](e+if) = (a+ib)[(c+id)(e+if)].$$

Lemma 3, The proof

- "$\Leftarrow$": We want:

$$[(a+ib)(c+id)](e+if) = (a+ib)[(c+id)(e+if)].$$

We get:

  - LHS: $(ac)e - \left(d\overline{b}\right)e - f\left(\overline{b}\overline{c}\right) - f\left(\overline{d}a\right)$
$$+i\left[e(cb) + e(\overline{a}d) + (\overline{c}\overline{a})f - \left(b\overline{d}\right)f\right]$$

Lemma 3, The proof

- "$\Leftarrow$": We want:

$$[(a+ib)(c+id)](e+if) = (a+ib)[(c+id)(e+if)].$$

We get:

- LHS: $(ac)e - (d\overline{b})e - f(\overline{b}\overline{c}) - f(\overline{d}a) + i\left[e(cb) + e(\overline{a}d) + (\overline{c}\overline{a})f - (b\overline{d})f\right]$
- RHS: $a(ce) - a(f\overline{d}) - (ed)\overline{b} - (\overline{c}f)\overline{b} + i\left[(ce)b - (f\overline{d})b + \overline{a}(ed) + \overline{a}(\overline{c}f)\right]$

Lemma 4

- Let $\mathcal{D} := \mathcal{F} + i\mathcal{F}$ ($i \in \mathcal{F}^{\perp}$ is a unitary vector) be a Dickson algebra. Then $\mathcal{D}$ is an associative and commutative composition algebra iff $\mathcal{F}$ is a commutative and associative composition algebra with a trivial conjugation.

Lemma 4

- Let $\mathcal{D} := \mathcal{F} + i\mathcal{F}$ ($i \in \mathcal{F}^{\perp}$ is a unitary vector) be a Dickson algebra. Then $\mathcal{D}$ is an associative and commutative composition algebra iff $\mathcal{F}$ is a commutative and associative composition algebra with a trivial conjugation.
Proof: "$\Rightarrow$"

Lemma 4

- Let $\mathcal{D} := \mathcal{F} + i\mathcal{F}$ ($i \in \mathcal{F}^{\perp}$ is a unitary vector) be a Dickson algebra. Then $\mathcal{D}$ is an associative and commutative composition algebra iff $\mathcal{F}$ is a commutative and associative composition algebra with a trivial conjugation.
  Proof: "$\Rightarrow$"
  We get
  - $ie = \bar{e}i$ for all $e \in \mathcal{F}$ from

Lemma 4

- Let $\mathcal{D} := \mathcal{F} + i\mathcal{F}$ ($i \in \mathcal{F}^\perp$ is a unitary vector) be a Dickson algebra. Then $\mathcal{D}$ is an associative and commutative composition algebra iff $\mathcal{F}$ is a commutative and associative composition algebra with a trivial conjugation.
  Proof: "$\Rightarrow$"
  We get
  - $ie = \bar{e}i$ for all $e \in \mathcal{F}$ from

  and
  - $\mathcal{D}$ is commutative $\Rightarrow ie = i\bar{e} \Rightarrow e = \bar{e}$ for all $e \in \mathcal{F}$.

Lemma 4

- Let $\mathcal{D} := \mathcal{F} + i\mathcal{F}$ ($i \in \mathcal{F}^{\perp}$ is a unitary vector) be a Dickson algebra. Then $\mathcal{D}$ is an associative and commutative composition algebra iff $\mathcal{F}$ is a commutative and associative composition algebra with a trivial conjugation.
  Proof: "$\Rightarrow$"
  We get
  - $ie = \bar{e}i$ for all $e \in \mathcal{F}$ from

  and
  - $\mathcal{D}$ is commutative $\Rightarrow ie = i\bar{e} \Rightarrow e = \bar{e}$ for all $e \in \mathcal{F}$.

  It means that $\mathcal{F}$ is a commutative associative algebra with a trivial conjugation.

Lemma 4, The proof

- "$\Leftarrow$":

Lemma 4, The proof

- "$\Leftarrow$":
  If $\mathcal{F}$ is commutative with trivial conjugation, we have:

Lemma 4, The proof

- "$\Leftarrow$":
  If $\mathcal{F}$ is commutative with trivial conjugation, we have:
  $$(a+ib)(c+id) = (ac - d\bar{b}) + i(cb + \bar{a}d) =$$

Lemma 4, The proof

- "$\Leftarrow$":
  If $\mathcal{F}$ is commutative with trivial conjugation, we have:
  $$(a+ib)(c+id) = (ac - d\bar{b}) + i(cb + \bar{a}d) =$$
  $$= (ca - b\bar{d}) + i(ad + \bar{c}b) = (c+id)(a+ib)$$

Lemma 4, The proof

- "$\Leftarrow$":
  If $\mathcal{F}$ is commutative with trivial conjugation, we have:
  $$(a+ib)(c+id) = (ac - d\bar{b}) + i(cb + \bar{a}d) =$$
  $$= (ca - b\bar{d}) + i(ad + \bar{c}b) = (c+id)(a+ib)$$
  and therefore $\mathcal{D} := \mathcal{F} + i\mathcal{F}$ is commutative.

Lemma 5

- Let $\mathcal{C}$ be a composition algebra. If the conjugation in $\mathcal{C}$ is trivial, then $dim(\mathcal{C}) = 1$.

Lemma 5

- Let $\mathcal{C}$ be a composition algebra. If the conjugation in $\mathcal{C}$ is trivial, then $dim(\mathcal{C}) = 1$.
  Proof: Suppose $dim(\mathcal{C}) > 1$ and take a nonzero $c \in \mathcal{C}$ such that $|c, 1| = 0$.

Lemma 5

- Let $\mathcal{C}$ be a composition algebra. If the conjugation in $\mathcal{C}$ is trivial, then $dim(\mathcal{C}) = 1$.
  Proof: Suppose $dim(\mathcal{C}) > 1$ and take a nonzero $c \in \mathcal{C}$ such that $|c, 1| = 0$.
  On the other hand, $c = \overline{c} = 2|c, 1| - c$ and $c = 0$, a contradiction.

Proof of The Hurwitz's theorem

Proof of The Hurwitz's theorem

$\boxed{Z = Y + iY}$

$\downarrow$

$\boxed{Y = X + jX}$

$\downarrow$

$\boxed{X = W + kW}$

$\downarrow$

$\boxed{W}$

if Z is a composition algebra, it must satisfy |xy| = |x||y| for all x, y in Z

x = a + ib
y = c + id
|(a + ib)(c + id)| = |a + ib||c + id|
a(cb) = (ac)b

Z = Y + iY is a composition algebra iff Y is an associative composition algebra

Y = X + jX is an associative composition algebra
iff X is an associative commutative compositon algebra

X = W + kW is an associative commutative algebra
iff W is an associative commutative algebra with trivial conjugation

dim W = 1 and the process ends...

The Hurwitz's theorem

Blah blah blah..

Blah blah blah..

- *"The real numbers are the dependable breadwinner of the family, the complete ordered field we all rely on. The complex numbers are a slightly flashier but still respectable younger brother: not ordered, but algebraically complete. The quaternions, being noncommutative, are the eccentric cousin who is shunned at important family gatherings. But the octonions are the crazy old uncle nobody lets out of the attic: they are nonassociative."*

—John Baez

The Hurwitz's theorem

The end