# Octonions

Alberto Elduque

Universidad de Zaragoza









4 Some surprises in low characteristics



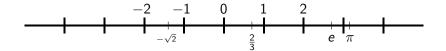






 $\mathbb{R} = \{\text{real numbers}\}$ 

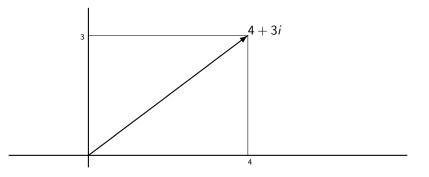
#### Real numbers are used in measurements.



But we cannot solve equations as simple as  $X^2 + 1 = 0!$ 

Complex numbers

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\} (\simeq \mathbb{R}^2)$$



$$(a+bi)(c+di) = (ac-bd) + (ad+bc)i$$

#### Exercise

$$|z_1 z_2| = |z_1| |z_2|$$

(|.| denotes the usual length.)

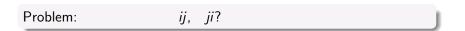
#### Exercise

Rotation of angle  $\alpha$  in  $\mathbb{R}^2 \leftrightarrow$  multiplication by  $e^{i\alpha} = \cos \alpha + i \sin \alpha$ .

$$SO(2)\simeq \{z\in \mathbb{C}: |z|=1\}\simeq S^1$$

Hamilton tried to find a multiplication, analogous to the multiplication of complex numbers, but in dimension 3, that should respect the "law of moduli":  $|z_1z_2| = |z_1||z_2|$ :

$$(a + bi + cj)(a' + b'i + c'j) =???$$
  
(assuming  $i^2 = -1 = j^2$ )



After years of struggle, he found the solution on October 16, 1843.

Letter from Sir W. R. Hamilton to his son Rev. Archibald H. Hamilton, dated August 5 1865:

MY DEAR ARCHIBALD -

(1) I had been wishing for an occasion of corresponding a little with you on QUATERNIONS: and such now presents itself, by your mentioning in your note of yesterday, received this morning, that you "have been reflecting on several points connected with them" (the quaternions), "particularly on the Multiplication of Vectors."

(2) No more important, or indeed fundamental question, in the whole Theory of Quaternions, can be proposed than that which thus inquires What is such MULTIPLICATION? What are its Rules, its Objects, its Results? What Analogies exist between it and other Operations, which have received the same general Name? And finally, what is (if any) its Utility?

### A spark flashed forth

(3) If I may be allowed to speak of myself in connexion with the subject, I might do so in a way which would bring you in, by referring to an ante-quaternionic time, when you were a mere child, but had caught from me the conception of a Vector, as represented by a Triplet: and indeed I happen to be able to put the finger of memory upon the year and month - October, 1843 - when having recently returned from visits to Cork and Parsonstown, connected with a meeting of the British Association, the desire to discover the laws of the multiplication referred to regained with me a certain strength and earnestness, which had for years been dormant, but was then on the point of being gratified, and was occasionally talked of with you. Every morning in the early part of the above-cited month, on my coming down to breakfast, your (then) little brother William Edwin, and yourself, used to ask me, "Well, Papa, can you multiply triplets"? Whereto I was always obliged to reply, with a sad shake of the head: "No, I can only add and subtract them."

(4) But on the 16th day of the same month - which happened to be a Monday, and a Council day of the Royal Irish Academy - I was walking in to attend and preside, and your mother was walking with me, along the Royal Canal, to which she had perhaps driven; and although she talked with me now and then, yet an under-current of thought was going on in my mind, which gave at last a result, whereof it is not too much to say that I felt at once the importance. An electric circuit seemed to close; and a spark flashed forth, the herald (as I foresaw, immediately) of many long years to come of definitely directed thought and work, by myself if spared, and at all events on the part of others, if I should even be allowed to live long enough distinctly to communicate the discovery.

Nor could I resist the impulse -unphilosophical as it may have beento cut with a knife on a stone of Brougham Bridge as we passed it, the fundamental formula with the symbols, *i*, *j*, *k*; namely,

$$i^2 = j^2 = k^2 = ijk = -1$$

which contains the Solution of the Problem, but of course, as an inscription, has long since mouldered away. A more durable notice remains, however, on the Council Books of the Academy for that day (October 16th, 1843), which records the fact, that I then asked for and obtained leave to read a Paper on Quaternions, at the First General Meeting of the session: which reading took place accordingly, on Monday the 13th of the November following. With this quaternion of paragraphs I close this letter I.; but I hope to follow it up very shortly with another. Your affectionate father. WILLIAM ROWAN HAMILTON.



$$\begin{split} \mathbb{H} &= \mathbb{R} \mathbf{1} \oplus \mathbb{R} i \oplus \mathbb{R} j \oplus \mathbb{R} k, \\ i^2 &= j^2 = k^2 = -1, \\ ij &= -ji = k, \quad jk = -kj = i, \quad ki = -ik = j. \end{split}$$



Hamilton and his quaternions

### Some properties of $\mathbb H$

- $|q_1q_2| = |q_1||q_2| \ \forall q_1, q_2 \in \mathbb{H}$  $(|a+bi+cj+dk|^2 = a^2 + b^2 + c^2 + d^2)$
- $\mathbb{H}_0 = \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k \simeq \mathbb{R}^3$ ,  $\mathbb{H} = \mathbb{R} \oplus \mathbb{H}_0$ , and  $\forall u, v \in \mathbb{H}_0$ :

 $uv = -u \cdot v + u \times v$ 

(where  $u \cdot v$  and  $u \times v$  denote the usual scalar and cross products).

• 
$$orall q=a1+u\in\mathbb{H},\ q^2=(a^2-u\cdot u)+2au,$$
 so  $q^2-(2a)q+|q|^2=0$  ( $\mathbb{H}$  is quadratic.)

- The map  $q = a + u \mapsto \overline{q} = a u$  is an involution, with  $q + \overline{q} = 2a$  and  $q\overline{q} = \overline{q}q = |q|^2$ .

$$(p_1+p_2j)(q_1+q_2j)=(p_1q_1-ar q_2p_2)+(q_2p_1+p_2ar q_1)j$$

- ∀p ∈ ℍ with |p| = 1, the left (resp. right) multiplication L<sub>p</sub> (resp. R<sub>p</sub>) by p is an isometry, due to the multiplicativity of the norm.
- For p ∈ ℍ \ ℝ1, the minimal polynomial of L<sub>p</sub> (or R<sub>p</sub>) is the irreducible polynomial X<sup>2</sup> 2aX + |p|<sup>2</sup>. It follows that for |p| = 1, the determinant of the multiplication by p is 1.

Multiplication by norm 1 quaternions are rotations in  $\mathbb{H} \simeq \mathbb{R}^4$ .

Conjugation by q preserves 1 and  $\mathbb{H}_0$ , so the linear map :

$$arphi_q : \mathbb{H}_0 \longrightarrow \mathbb{H}_0,$$
  
 $x \mapsto q x q^{-1} = q x ar{q}.$ 

is a rotation in  $\mathbb{H}_0 \simeq \mathbb{R}^3$ .

### Rotations in three-dimensional space

#### Exercise

$$arphi_{m{q}}$$
 is the rotation around the axis  $\mathbb{R}^+ u$  of angle  $2lpha.$ 

(Hint: If  $v \in \mathbb{H}_0$  is orthogonal to u, the  $qvq^{-1} = qv\bar{q} = q^2v$ , and  $q^2 = \cos(2\alpha) + \sin(2\alpha)u$ .)

Therefore the map

$$arphi: S^3 \simeq \{q \in \mathbb{H}: |q| = 1\} \longrightarrow SO(3),$$
  
 $q \mapsto \varphi_q$ 

is a surjective (Lie) group homomorphism with  $\ker \varphi = \{\pm 1\}$ :

$$S^3/_{\{\pm 1\}}\simeq SO(3)$$

 $(S^3$  is the universal cover of SO(3))

 $\begin{array}{rcl} \mbox{Rotations in $\mathbb{R}^3$} &\longleftrightarrow & \mbox{Conjugation in $\mathbb{H}_0$ by norm $1$} \\ & \mbox{quaternions "modulo $\pm1"$} \end{array}$ 

It is quite easy now to compose rotations in three-dimensional space!

It is enough to multiply norm 1 quaternions!  $(\varphi_p \circ \varphi_q = \varphi_{pq})$ 

Now one can deduce easily the formulas by Olinde Rodrigues (1840) for the composition of rotations.

### Rotations in $\mathbb{R}^4$

• If  $\psi$  is a rotation in  $\mathbb{R}^4\simeq\mathbb{H}$ ,  $a=\psi(1)$  is a norm 1 quaternion, and

$$L_{\bar{a}}\circ\psi(1)=\bar{a}a=|a|^2=1,$$

so  $L_{\bar{a}} \circ \psi$  is actually a rotation in  $\mathbb{R}^3 \simeq \mathbb{H}_0$ .

• Therefore, there is a norm 1 quaternion  $q \in \mathbb{H}$  such that

$$\bar{a}\psi(x) = qxq^{-1}$$

for any  $x \in \mathbb{H}$ . That is:

$$\psi(x) = (aq)xq^{-1} \quad \forall x \in \mathbb{H}.$$

# *SO*(4)

The map

$$egin{aligned} \Psi:S^3 imes SO(4),\ (p,q)\mapsto\psi_{p,q}\;(x\mapsto pxq^{-1}) \end{aligned}$$

is a surjective (Lie) group homomorphism with ker  $\Psi=\{\pm(1,1)\}.$ 

$$S^3 \times S^3/_{\{\pm(1,1)\}} \simeq SO(4)$$

It is quite easy to compose rotations in four-dimensional space! It is enough to multiply pairs of norm 1 quaternions!  $(\psi_{p_1,q_1} \circ \psi_{p_2,q_2} = \psi_{p_1p_2,q_1q_2})$ 









There is still something in the system which gravels me. I have not yet any clear views as to the extent to which we are at liberty arbitrarily to create imaginaries, and to endow them with supernatural properties. If with your alchemy you can make three pounds of gold, why should you stop there?

(Letter from John T. Graves to Hamilton, dated October 26, 1843!)

The algebra of quaternions is obtained by doubling suitably the field of complex numbers:

 $\mathbb{H}=\mathbb{C}\oplus\mathbb{C}j.$ 

Doubling again we get the octonions (Graves – Cayley):

 $\mathbb{O}=\mathbb{H}\oplus\mathbb{H}\textit{I}.$ 



Arthur Cayley

$$\mathbb{O} = \mathbb{H} \oplus \mathbb{H} I = \mathbb{R} \langle 1, i, j, k, l, il, jl, kl \rangle$$

with multiplication

$$(p_1 + p_2 l)(q_1 + q_2 l) = (p_1 q_1 - \bar{q}_2 p_2) + (q_2 p_1 + p_2 \bar{q}_1) l$$

and norm:

$$|p_1 + p_2 I|^2 = |p_1|^2 + |p_2|^2$$

These are the same formulas that allow us to pass from  $\mathbb C$  to  $\mathbb H!$ 

# Some algebraic properties

- $|xy| = |x||y|, \forall x, y \in \mathbb{O}.$
- $\mathbb{O}$  is a division algebra, it is neither commutative nor associative!

But it is *alternative*: any two elements generate an associative subalgebra.

**Theorem (Zorn 1933):** The only finite-dimensional real alternative division algebras are  $\mathbb{R}$ ,  $\mathbb{C}$ ,  $\mathbb{H}$  and  $\mathbb{O}$ .

The only such associative algebras are  $\mathbb{R}$ ,  $\mathbb{C}$  and  $\mathbb{H}$  (Frobenius 1877).

- $\mathbb{O}$  is quadratic:  $\forall x = a1 + u \in \mathbb{O}$ ,  $x^2 2ax + |x|^2 = 0$ .
- S<sup>7</sup> ≃ {x ∈ 𝔅 : |x| = 1} is not a group (associativity fails), but it constitutes the most important example of a *Moufang loop*.

### Some algebraic properties

• 
$$\mathbb{O}_0 = \mathbb{R}\langle i, j, k, l, il, jl, kl \rangle$$
.  $\forall u, v \in \mathbb{O}_0$ :

$$uv = -u \cdot v + u \times v.$$

Cross product in  $\mathbb{R}^{7}$ !:  $(u \times v) \times v = (u \cdot v)v - (v \cdot v)u$ .  $(\mathbb{O}_{0}, \times)$  is an example of a *Malcev algebra*.

• The group of automorphisms (i.e., the group of symmetries) Aut( $\mathbb{O}$ )  $\simeq$  Aut( $\mathbb{O}_0, \times$ ) is the exceptional compact Lie group  $G_2$ .

 $\mathbb{O}_{0}$  is the smallest nontrivial irreducible module of the group of automorphisms.

Its Lie algebra  $\mathfrak{Der}(\mathbb{O}) \simeq \mathfrak{Der}(\mathbb{O}_0, \times)$  is the compact simple real Lie algebra of type  $G_2$ .

### Some geometric properties

- The groups *Spin*<sub>7</sub> and *Spin*<sub>8</sub> (universal covers of *SO*(7) and *SO*(8)) can be described easily in terms of octonions.
- $\mathbb{O}$  division algebra  $\Rightarrow S^7$  parallelizable.  $S^1$ ,  $S^3$  and  $S^7$  are the only parallelizable spheres (Bott–Milnor and Kervaire).
- S<sup>6</sup> ≃ {x ∈ O<sub>0</sub> : |x| = 1} is endowed with an *almost complex structure*, inherited from the multiplication of octonions.
   S<sup>2</sup> and S<sup>6</sup> are the only spheres with such structures (Adams).
- Non-desarguesian projective plane  $\mathbb{OP}^2$ .
- The only spheres that can be described as homogeneous spaces of nonclassical groups are S<sup>6</sup> = Aut 𝔅/SU(3), S<sup>7</sup> = Spin<sub>7</sub> / Aut 𝔅 and S<sup>15</sup> = Spin<sub>9</sub>/Spin<sub>7</sub>.









### Definition

A composition algebra over a field  $\mathbb{F}$  is a triple  $(C, \cdot, n)$  where

- C is a vector space over  $\mathbb{F}$ ,
- $x \cdot y$  is a bilinear multiplication  $C \times C \rightarrow C$ ,
- $n: C \to \mathbb{F}$  is a multiplicative  $(n(x \cdot y) = n(x)n(y) \ \forall x, y \in C)$ nonsingular quadratic form.

The unital composition algebras are called Hurwitz algebras.

Hurwitz algebras form a class of degree two algebras:

$$x^{2} - n(x, 1)x + n(x)1 = 0$$

for any x. (n(x, y) := n(x + y) - n(x) - n(y).)

They are endowed with an involution, the standard conjugation:

$$\bar{x}=n(x,1)1-x,$$

satisfying

$$\overline{\overline{x}} = x$$
,  $x + \overline{x} = n(x, 1)1$ ,  $x \cdot \overline{x} = \overline{x} \cdot x = n(x)1$ .

# Cayley-Dickson doubling process

Let  $(B, \cdot, n)$  be an associative Hurwitz algebra, and let  $\lambda$  be a nonzero scalar in the ground field  $\mathbb{F}$ . Consider the direct sum of two copies of B:

$$C = B \oplus Bu$$
,

with the following multiplication and nondegenerate quadratic form that extend those on B:

$$(a + bu) \cdot (c + du) = (a \cdot c + \lambda \overline{d} \cdot b) + (d \cdot a + b \cdot \overline{c})u,$$
  
$$n(a + bu) = n(a) - \lambda n(b).$$

Then  $(C, \cdot, n)$  is again a Hurwitz algebra, which is denoted by  $CD(B, \lambda)$ 

Notation:  $CD(A, \mu, \lambda) := CD(CD(A, \mu), \lambda).$ 

#### Theorem

Every Hurwitz algebra over a field  $\mathbb F$  is isomorphic to one of the following:

- (i) The ground field  $\mathbb{F}$ .
- (ii) A quadratic commutative and associative separable algebra K(μ) = F1 + Fv, with v<sup>2</sup> = v + μ and 4μ + 1 ≠ 0. The norm is given by its generic norm.
  If the characteristic of F is ≠ 2, these are the algebras CD(F, α).
- (iii) A quaternion algebra  $Q(\mu, \beta) = CD(K(\mu), \beta)$ . (These four dimensional algebras are associative but not commutative.)
- (iv) A Cayley algebra  $C(\mu, \beta, \gamma) = CD(K(\mu), \beta, \gamma)$ . (These eight dimensional algebras are alternative, but not associative.)

#### Proposition

Two Hurwitz algebras are isomorphic if and only if their norms are isometric.

### Proposition

For each dimension 2, 4 or 8, there is a unique, up to isomorphism, Hurwitz algebra with isotropic norm.

- $\mathbb{F} \times \mathbb{F}$  with  $n((\alpha, \beta)) = \alpha \beta$ ,
- $Mat_2(\mathbb{F})$  with n = det,
- $\mathcal{C}_s := CD(Mat_2(\mathbb{F}), 1)$  (the split Cayley algebra).

Given a finite-dimensional simple Lie algebra  $\mathfrak{g}$  of type  $X_r$  over the complex numbers, and a Chevalley basis  $\mathcal{B}$ , let  $\mathfrak{g}_{\mathbb{Z}}$  be the  $\mathbb{Z}$ -span of  $\mathcal{B}$  (a Lie algebra over  $\mathbb{Z}$ ). The Lie algebra  $\mathfrak{g}_{\mathbb{F}} := \mathfrak{g}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{F}$  is the Chevalley algebra of type  $X_r$ .

#### Theorem

- The Chevalley algebra of type  $G_2$  is isomorphic to  $\mathfrak{Der}(\mathcal{C}_s)$ .
- For any Cayley algebra C, the Lie algebra Der(C) is a twisted form of the Chevalley algebra Der(C<sub>s</sub>).
- If char  $\mathbb{F} \neq 2,3$ , then  $\mathfrak{Der}(\mathbb{C})$  is simple.

# Cayley algebras and simple Lie algebras of type $G_2$

#### Theorem (Jacobson 1931, Barnes 1961)

If char  $\mathbb{F} \neq 2, 3$ ,

- Any twisted form of the Chevalley algebra of type G<sub>2</sub> is isomorphic to  $\mathfrak{Der}(\mathbb{C})$  for a Cayley algebra  $\mathbb{C}$ .
- Two Cayley algebras  $C_1$  and  $C_2$  are isomorphic if and only if their Lie algebras of derivations are isomorphic.

# Sketch of a 'modern' proof For any Cayley algebra $\mathcal{C}$ , the adjoint map Ad : Aut( $\mathcal{O}$ ) $\longrightarrow$ Aut( $\mathcal{O}$ er( $\mathcal{C}$ ))

,

is an isomorphism of affine group schemes.









4 Some surprises in low characteristics

#### Theorem

Let  $\mathbb{C}$  be a Cayley algebra over a field  $\mathbb{F}$  of characteristic 3.

- The simple Malcev algebra  $\mathcal{C}_0$  is a Lie algebra!!
- $\mathcal{C}_0$  is a twisted form of the projective special linear algebra  $\mathfrak{psl}_3(\mathbb{F})$ .
- Der(C) is a semisimple Lie algebra, but not a direct sum of simple ideals.
- $\mathfrak{Der}(\mathbb{C})$  contains a unique proper ideal:  $\operatorname{ad}(\mathbb{C}_0)$ , isomorphic to  $\mathbb{C}_0$ , and the quotient  $\mathfrak{Der}(\mathbb{C})/\operatorname{ad}(\mathbb{C}_0)$  is isomorphic again to  $\mathbb{C}_0$ .

In spite of this strange behavior, still we get:

#### Theorem

Let  ${\mathbb C}$  be a Cayley algebra over a field  ${\mathbb F}$  of characteristic 3, the adjoint map

is an isomorphism of affine group schemes.

The proof uses the fact that, even in characteristic 3, any derivation of  $\mathfrak{Der}(\mathbb{C})$  is inner.

#### Corollary

Denote by Isom(Cayley), Isom( $G_2$ ), and Isom( $\overline{A}_2$ ), the sets of isomorphism classes of Cayley algebras, twisted forms of the Chevalley algebra of type  $G_2$ , and twisted forms of  $\mathfrak{psl}_3(\mathbb{F})$ , respectively.

Then we have bijections:

 $\begin{array}{rcl} \mathsf{Isom}(\bar{A}_2) & \longleftrightarrow & \mathsf{Isom}(\mathsf{Cayley}) & \longleftrightarrow & \mathsf{Isom}(G_2) \\ [\mathfrak{C}_0] & \leftarrow & [\mathfrak{C}] & \to & [\mathfrak{Der}(\mathfrak{C})] \end{array}$ 

#### Theorem

Let  $\mathbb{C}$  be a Cayley algebra over a field  $\mathbb{F}$  of characteristic 2, then the Lie algebra  $\mathfrak{Dec}(\mathbb{C})$  is isomorphic to the projective special linear Lie algebra  $\mathfrak{psl}_4(\mathbb{F})$ .

The isomorphism class of  $\mathfrak{Der}(\mathcal{C})$  does not depend on  $\mathcal{C}!!$ 

### Sketch of proof

- Any  $d \in \mathfrak{Der}(\mathbb{C})$  preserves  $\mathbb{C}_0$  and  $\mathbb{F}_1$ , and  $1 \in \mathbb{C}_0!!!$
- Hence d induces a linear map on the six-dimensional quotient C<sub>0</sub>/F1, which is endowed with a nondegenerate alternating bilinear form induced by the norm n. (n(x, x) = 2n(x) = 0!!)
- This embeds  $\mathfrak{Der}(\mathbb{C})$  into the symplectic Lie algebra  $\mathfrak{sp}_6(\mathbb{F})$ , and hence into  $\mathfrak{sp}_6(\mathbb{F})^{(2)}$ , which is isomorphic to  $\mathfrak{psl}_4(\mathbb{F})$ . But  $\dim \mathfrak{psl}_4(\mathbb{F}) = 14 = \dim \mathfrak{Der}(\mathbb{C})$ .

#### Corollary

In characteristic 2, the Chevalley algebra of type  $G_2$  is isomorphic to  $\mathfrak{psl}_4(\mathbb{F})$  (the classical simple Lie algebra of type  $A_3$ ).

#### Theorem

Let  $\mathbb{F}$  be a field of characteristic 2. Then the affine group scheme of automorphisms of  $\mathfrak{psl}_4(\mathbb{F})$  is isomorphic to the affine group scheme of automorphisms of the algebra with involution (Mat<sub>6</sub>( $\mathbb{F}$ ),  $t_s$ ), where  $t_s$  is the canonical symplectic involution.

### Sketch of proof

Any automorphism of  $Mat_6(\mathbb{F})$  commuting with the involution  $t_s$  restricts to an automorphism of the Lie algebra  $\mathfrak{sp}_6(\mathbb{F})^{(2)}$ . This induces a closed embedding of group schemes. But the two group schemes involved are connected, smooth and of the same dimension.

### Corollary

Let  $\mathbb{F}$  be a field of characteristic 2. The map:

Isomorphism classes of degree 6 central simple associative algebras with a symplectic involution

### $[(\mathcal{B}, \tau)]$

Isomorphism classes
 of twisted forms of
 the Lie algebra psl<sub>4</sub>(F)

$$[\text{Skew}(\mathcal{B}, \tau)^{(2)}]$$

is a bijection.

#### Thank you!