

About real and binary algebras: the interplay between Geometry and Algebra

F. Chaitin–Chatelin¹, T. Meškauskas² and A. N. Zaoui³
CERFACS, 42 Av. G. Coriolis, F-31057 Toulouse cedex 1, France

CERFACS Technical Report No. TR/PA/00/74

Abstract

We provide the reader with a systematic introduction to hypercomplex algebras also giving the proofs of the main results in full details. In particular, we show that it is Geometry which plays a very important role in the construction of hypercomplex algebras. Both real and binary algebras are studied from the point of view of their suitability for computations.

Keywords: hypercomplex numbers, hypercomplex algebras, quaternions, octonions, division algebra, composition algebra, geometry, four-color theorem.

1 Introduction

This work is a follow-up from [1, 2, 3] where we started to look at algebraic computation with a geometric point of view. In particular we wish to give in full details some proofs which were omitted in [2, 3].

2 Basic concepts in the theory of algebras ([4, p. 189-193])

In the paragraph to follow, the basis field will be the field \mathbb{R} of real numbers. But any commutative field \mathbb{K} could be chosen. We recall that any vector space V on \mathbb{R} with dimension n is isomorphic to \mathbb{R}^n .

Definition 2.1 *A vector space V on \mathbb{R} is an **algebra** on \mathbb{R} , or equivalently, a **real algebra**, if, in addition to the addition $+$, it is equipped with a **multiplication** \times which is*

i) internal: $(x, y) \in V \times V \mapsto x \times y \in V$.

ii) bilinear: $\forall(\alpha, \beta) \in \mathbb{R}^2, \quad \forall(x, y, z) \in V^3 \Rightarrow$

$$\begin{cases} (\alpha x + \beta y) \times z = \alpha(x \times z) + \beta(y \times z), \\ x \times (\alpha y + \beta z) = \alpha(x \times y) + \beta(x \times z). \end{cases}$$

¹Université Toulouse I and CERFACS. E-mail: chatelin@cerfacs.fr

²CERFACS. E-mail: meska@cerfacs.fr

³CERFACS. E-mail: zaoui@cerfacs.fr

Note that property ii) expresses the left and right distributivity of \times with respect to $+$. Note also that the relations $\alpha(x \times y) = (\alpha x) \times y = x \times (\alpha y)$ are always valid.

Definition 2.2 \times is *associative* iff

$$\forall x, y, z \in V, \quad x \times (y \times z) = (x \times y) \times z.$$

Definition 2.3 \times is *commutative* iff

$$\forall x, y \in V, \quad x \times y = y \times x.$$

An algebra is in general not associative nor commutative.

Definition 2.4 The algebra is *with unity* e if there exists $e \in V$ such that $x = e \times x = x \times e, \forall x \in V$.

Any algebra has at most one unity element e (often denoted 1).

Definition 2.5 If the algebra has a unit element e , then any nonzero element x may have a *right* (resp. *left*) inverse such that $x \times x_r^{-1} = e$ (resp. $x_l^{-1} \times x = e$). If $x_l^{-1} = x_r^{-1}$, then x is said to have an *inverse* x^{-1} which satisfies $x \times x^{-1} = x^{-1} \times x = e$.

Definition 2.6 The dimension of the vector space V on \mathbb{R} is the dimension of the algebra.

Definition 2.7 $0 \neq x \in V$ is a *divisor of 0* iff there exists $y \neq 0, y \in V$ such that $x \times y = 0$ or $y \times x = 0$. If this is impossible, V is an *algebra without zero divisor*. This is equivalent to

$$x \times y = 0 \quad \Leftrightarrow \quad x = 0 \quad \text{or} \quad y = 0.$$

Definition 2.8 An algebra is said to be *with division* if for any $a, b \in V, a \neq 0$ the two equations $a \times x = b$ and $y \times a = b$ have unique solutions x and y . One says equivalently that V is a *division algebra*.

Lemma 2.1 If V is an associative division algebra, then $V - \{0\}$ is a group with respect to \times : the algebra is a field.

Proof: Let $a \neq 0$. From Definition 2.8, there exists $e \neq 0$ such that $a \times e = a$. Using the decomposition $b = y \times a$ and the associativity, we then obtain $b \times e = b$ for any b in V . Since $e \neq 0$, any b can also be written $b = e \times x$. With $e \times e = e$ and the previous arguments, we then obtain $e \times b = b$ for any b in V . Therefore, e is a unity.

Next, it is immediate from Definition 2.8 that any nonzero vector a in V has a left and right inverse (by letting $b = e$). △

Lemma 2.2 If V is a division algebra any nonzero element has unique left and right inverses.

Proof: In the Definition 2.8, let $b = e$. Therefore $a \times a_r^{-1} = e$ and $a_l^{-1} \times a = e$ have unique solutions a_r^{-1} and a_l^{-1} . △

Examples:

1. \mathbb{R} and \mathbb{C} are real associative commutative algebras with a unit element, without zero divisor, and with respective dimension 1 and 2.
2. The space of square matrices $\mathbb{R}^{n \times n}$ of order n on \mathbb{R} (with the usual matrix product) is a real associative algebra with the identity matrix as unit element, with dimension n^2 . For $n > 1$, such algebras are not commutative. They admit zero divisors.
3. On \mathbb{R}^3 , we define the product $x \times y$ to be the vector product

$$x \wedge y = (x_2y_3 - x_3y_2, x_3y_1 - x_1y_3, x_1y_2 - x_2y_1).$$

Therefore \mathbb{R}^3 is a non associative algebra of dimension 3, which is anti-commutative:

$$x \wedge y = -y \wedge x.$$

Lemma 2.3 *For algebras of finite dimension, one has the equivalence:*

$$i) V \text{ is with division} \quad \Leftrightarrow \quad ii) V \text{ is without zero divisor.}$$

Proof: Clearly i) \Rightarrow ii) in general. If, for $a \neq 0$, there exists $c \neq 0$ such that $a \times c = 0$ then the equation $a \times x = b$ would have for solution $x + c \neq x$ as well as x , since $a \times (x + c) = b$. This is impossible by i).

Conversely we suppose that ii) holds: $x \mapsto a \times x$ is a linear injective map. Because the algebra has a finite dimension, the map is also onto: it is a bijection. Any equation $a \times x = b$ has a unique solution. One conclude similarly by considering the map $y \mapsto y \times a$. \triangle

In conclusion of this paragraph we can say that the multiplication operator \times which defines an algebra (of finite dimension) by Definition 2.1, may or may not be such that:

- a) there exists a unit element (Definition 2.4),
- b) any nonzero vector has an inverse (Def. 2.5),
- c) it is associative (Def. 2.2),
- d) it is commutative (Def. 2.3),
- e) there exist no zero divisor (Def. 2.7).

3 Characterization of real division algebras of finite dimension

In this paragraph the basis field is specified to be \mathbb{R} . After the spectacular discovery of the quaternions by Hamilton in 1843, it seemed for a while that a zoo of real algebras could be created. However, it was proved – between 1877 and 1960 – that, despite the appearances, there is only a limited number of “interesting” real algebras up to an isomorphism. The “interesting” algebras which have been characterized are the real division algebras.

3.1 The three real fields (Frobenius (1877) [4, p. 239])

Theorem 3.1 *Let $V \neq 0$ be an algebra on \mathbb{R} with finite dimension, which is associative and without zero divisor. Then only three possibilities exist:*

- 1) V is isomorphic to the field \mathbb{R} of real numbers,
- 2) V is isomorphic to the field \mathbb{C} of complex numbers,
- 3) V is isomorphic to the field \mathbb{H} of quaternions.

There are essentially **two** commutative fields (over \mathbb{R}): \mathbb{R} and \mathbb{C} , of respective dimension 1 and 2. There is essentially **one** noncommutative field (over \mathbb{R}) \mathbb{H} , of dimension 4.

3.2 The four real division algebras

Once the quaternions were discovered, it was easy to show that \mathbb{R} , \mathbb{C} , \mathbb{H} and the octonions \mathbb{G} are division algebras (over \mathbb{R}) of respective dimension 1, 2, 4 and 8. Surprisingly, it has been extremely difficult to prove that these four algebras are essentially the **only** real division algebras. The proof was completed at the end of the 1950s: it uses sophisticated topological methods [4, p. 295].

In other words, relaxing associativity in the definition of \mathbb{H} does not yield more than essentially one new division algebra, that is the octonions \mathbb{G} [10].

3.3 The three vector product algebras

Let V be a vector space on \mathbb{R} , with the scalar product: $(x, y) \rightarrow \langle x, y \rangle$.

Definition 3.1 *The **vector product** on V is an internal operation $(x, y) \rightarrow x \wedge y \in V$ such that*

- i) $\forall x, y \in V, \quad x \wedge y = -y \wedge x,$
- ii) $\forall x, y, z \in V, \quad \langle x \wedge y, z \rangle = \langle x, y \wedge z \rangle.$

The scalar product defines the norm $\|x\| = \sqrt{\langle x, x \rangle}$ on V .

Definition 3.2 *A **vector product algebra** is an algebra V where the multiplication is taken to be the vector product, which satisfies:*

$$\forall x, y \in V, \quad \|x\| = \|y\| = 1 \quad \text{and} \quad \langle x, y \rangle = 0 \quad \text{imply} \quad \|x \wedge y\| = 1. \quad (1)$$

It can be shown [4, p. 289] that the property (1) is equivalent to any of the following 2 properties:

$$\forall x, y \in V, \quad x \wedge (x \wedge y) = \langle x, y \rangle x - \|x\|^2 y, \quad (2)$$

$$\forall x, y \in V, \quad \|x \wedge y\|^2 = \|x\|^2 \|y\|^2 - \langle x, y \rangle^2. \quad (3)$$

We remark that the Gram determinant

$$\det \begin{pmatrix} \langle x, x \rangle & \langle x, y \rangle \\ \langle y, x \rangle & \langle y, y \rangle \end{pmatrix} = \|x\|^2 \|y\|^2 - \langle x, y \rangle^2$$

is the right hand side of (3).

Examples:

1. With the scalar product $(x, y) \mapsto xy$, \mathbb{R} is a vector product algebra with the trivial vector product $(x, y) \mapsto 0$. The reader can check that this vector product satisfies (3).
2. With the canonical scalar product, \mathbb{R}^3 is a vector product algebra with the classical vector product. One remarks that $x \wedge y = \frac{1}{2}(x \times y - y \times x)$, where x and y are pure quaternions (3 dimensional vectors with zero real part in \mathbb{H}) and \times is the multiplication in \mathbb{H} .

One can prove rather easily that up to an isometric isomorphism, there are only three vector product algebras of respective dimension 1, 3 and 7. They correspond to vectors which are pure imaginary (dimension 1), pure quaternions (dimension 3) and pure octonions (dimension 7) respectively [4, p. 292].

3.4 The four real composition algebras

The four division algebras \mathbb{R} , \mathbb{C} , \mathbb{H} and \mathbb{G} can also be characterized, up to an isomorphism, as the only composition algebras with unit element and finite dimension [4, p. 279].

What is a **composition algebra**? It is a real algebra with a scalar product $\langle x, y \rangle$ and associated norm $\|x\| = \sqrt{\langle x, x \rangle}$ such that:

$$\|x \times y\| = \|x\| \|y\|. \quad (4)$$

The property (4) means that the multiplication is **isometric**. It can hold only for a division algebra. This property is closely connected with the theorem of squares (Gauss, Euler, Degen, Hurwitz) [4, 5].

4 An epistemological interlude

The results presented in the previous paragraph are quite remarkable. They prove that only the first four hypercomplex algebras \mathbb{R} , \mathbb{C} , \mathbb{H} and \mathbb{G} are “interesting” from the point of view of no zero divisor, or from the point of view of the isometry of \times . No other type of multiplication \times yields the same properties.

What is so special about the multiplication operation which creates the hypercomplex numbers? We shall investigate this little studied question in the next paragraph from a computational/geometrical point of view.

But before, let us pause to meditate upon the geometric significance of the four types of characterizations of real division algebras that were reviewed in paragraph 3.

Even though the properties are expressed algebraically, the flavour is strongly geometrical, and even topological. The geometrical flavour is only reinforced if one thinks of the unexpected connection made a decade ago between the **4-color theorem** in \mathbb{R}^2 and the possibility of **associativity for the vector product** in \mathbb{R}^3 by Kauffman [7, 8, 9]. Essentially, he has proved that the celebrated 4-color theorem is equivalent to the following theorem:

Theorem 4.1 *Consider any two bracketings for a vector product of any finite number of vectors in \mathbb{R}^3 , such as*

$$L = a \wedge (b \wedge ((c \wedge d) \wedge e)) \quad \text{and} \quad R = ((a \wedge b) \wedge c) \wedge (d \wedge e).$$

There always exists a choice of vectors a, b, c, d, e (for example) amongst the 3 vectors e_1, e_2, e_3 of the canonical basis of \mathbb{R}^3 such that $L = R \neq 0$.

In the paragraph to follow, the reason why Geometry is so intimately connected with hypercomplex Algebra will be put in a fuller light by means of recursivity.

5 The recursive construction of hypercomplex algebras of finite dimension

In order to define hypercomplex algebras, one has to consider not only two **algebraic** operations $+$ and \times , but also one **geometric** map: $x \in V \mapsto \bar{x} \in V$, where \bar{x} denotes the conjugate vector of x in V .

The three operations are defined recursively as we define the algebras, in the following manner. Let A_k be the real hypercomplex algebra of dimension 2^k , $k \geq 1$. It is constructed recursively as $A_k = A_{k-1} \times A_{k-1}$ by means of the **three** following operations:

$$\text{addition:} \quad (a, b) + (c, d) = (a + c, b + d), \quad (5)$$

$$\text{conjugacy:} \quad \overline{(a, b)} = (\bar{a}, -b), \quad (6)$$

$$\text{multiplication:} \quad (a, b) \times (c, d) = (ac - \bar{d}b, da + b\bar{c}), \quad (7)$$

where ac denotes $a \times c$ in A_{k-1} . For $k = 0$, A_0 is taken to be the field \mathbb{R} with the arithmetic operations $+$ and \times , the conjugacy map being the identity on \mathbb{R} : $a \mapsto \bar{a} = a \in \mathbb{R}$. This construction is known to algebraists as the Albert-Dickson doubling process [11].

In the above definitions (5), (6) and (7), the multiplication \times depends on the conjugacy and on the addition, the conjugacy depends on the addition. This expresses a **tight connection between Geometry and Algebra**.

Because of the existence of the geometric conjugacy – a third operation which is never explicated in standard presentations – we are led to introduce the following new definition:

Definition 5.1 *A real algebra is **selfconjugate** when the conjugacy map $x \in V \mapsto \bar{x} \in V$ is the identity: $x = \bar{x}$.*

Example: The field \mathbb{R} is selfconjugate but the field \mathbb{C} is not: $x = \bar{x} \Leftrightarrow x \in \mathbb{R}$.

The existence of a nontrivial conjugacy operation in A_k , $k > 0$, allows to partition each A_k into its

- **real** part $\mathcal{R}e A_k = \{x \in A_k; x = \bar{x}\} \sim \mathbb{R}$
- **imaginary** part $\mathcal{I}m A_k = \{x \in A_k; x = -\bar{x}\} \sim \mathbb{R}^{2^k - 1}$

such that $A_k = \mathcal{R}e A_k \oplus \mathcal{I}m A_k$. The vectors in the imaginary part are called “pure” or “imaginary” vectors.

5.1 Properties of the multiplication in A_k

Lemma 5.1 *The unit (resp. zero) element of A_k is $1 = (1, 0)$ (resp. $0 = (0, 0)$), $k > 0$.*

Proof: By induction on k . It is true for $k = 0$ and $k = 1$:

$$(a, b) \times (1, 0) = (1, 0) \times (a, b) = (a, b),$$

$$(a, b) + (0, 0) = (a, b).$$

△

Lemma 5.2 *i) $\overline{(\bar{x})} = x$, ii) $\overline{(x + y)} = (\bar{x} + \bar{y})$, iii) $\overline{(x \times y)} = \bar{y} \times \bar{x}$.*

Proof: i) $\bar{x} = (\bar{a}, -b)$ and $\overline{(\bar{x})} = ((\bar{a}), b)$. The conjugacy is an idempotent operator (its square is the identity operator).

ii) Clear.

$$\text{iii) } \overline{(x \times y)} = \overline{((ac - \bar{d}b), -da - b\bar{c})} = ((\overline{ac}) - \overline{(\bar{d}b)}, -da - b\bar{c}),$$

$$\bar{y} \times \bar{x} = (\bar{c}, -d) \times (\bar{a}, -b) = (\bar{c}\bar{a} - \bar{d}d, -b\bar{c} - da).$$

△

Lemma 5.3 *$x \times \bar{x} = \bar{x} \times x$ is a real positive number iff $x \neq 0$ in A_k , $k \geq 0$.*

Proof: $(a, b) \times (\bar{a}, -b) = (a\bar{a} + b\bar{b}, 0)$ and $(\bar{a}, -b) \times (a, b) = (\bar{a}a + \bar{b}b, 0)$. $x \neq 0$ implies $a \neq 0$ or $b \neq 0$ by induction. Therefore the real numbers $a\bar{a}$ and $b\bar{b}$ which are nonnegative cannot be simultaneously zero: $a\bar{a} + b\bar{b} = x \times \bar{x} > 0$. △

Lemma 5.4 *The map $x \mapsto |x| = \sqrt{x \times \bar{x}}$ defines the euclidean norm on any algebra A_k , $k \geq 0$.*

Proof: Let $x = (x_i)_{i=1}^{2^k}$ be a vector of the vector space A_k of dimension 2^k , $k \geq 0$. By induction on k , it is clear that $|x|^2 = x \times \bar{x} = \sum_{i=1}^{2^k} x_i^2$. △

Corollary 5.5 *Any nonzero vector x in A_k has a unique inverse*

$$x^{-1} = \frac{1}{x \times \bar{x}} \bar{x} = \frac{1}{|x|^2} \bar{x}.$$

Proof: It follows from $x \times \bar{x} = \bar{x} \times x = |x|^2$ that $x \times \frac{\bar{x}}{|x|^2} = \frac{\bar{x}}{|x|^2} \times x = 1$. △

To lighten the presentation to follow, we shall refer to the possible properties of a real algebra A by the following notation:

- (i) A is with division: Definition 2.8,
- (ii) A is associative: Definition 2.2,
- (iii) A is commutative: Definition 2.3,
- (iv) A is selfconjugate: Definition 5.1.

Lemma 5.6 *The following properties hold for any algebra A_k , $k > 0$:*

- a) A_{k-1} satisfies (i) and (ii) $\Rightarrow A_k$ satisfies (i),
- b) A_{k-1} satisfies (i), (ii) and (iii) $\Rightarrow A_k$ satisfies (i) and (ii),
- c) A_{k-1} satisfies (i) to (iv) $\Rightarrow A_k$ satisfies (i), (ii) and (iii).

Proof: a) We have to show $x \times y = 0 \Leftrightarrow x = 0$ or $y = 0$. We assume that $0 = (0, 0) = x \times y = (a, b) \times (c, d) = (ac - \bar{d}b, da + b\bar{c})$. This yields

$$\begin{cases} ac - \bar{d}b = 0 \\ da + b\bar{c} = 0 \end{cases} \Rightarrow \begin{cases} (ac)\bar{c} - (\bar{d}b)\bar{c} = 0\bar{c} = 0 \\ \bar{d}(da) + \bar{d}(b\bar{c}) = \bar{d}0 = 0. \end{cases}$$

Because of the associativity of \times for a, b, c, d : $(ac)\bar{c} = a(c\bar{c})$, $(\bar{d}b)\bar{c} = \bar{d}(b\bar{c})$ and $\bar{d}(da) = (\bar{d}d)a$. Therefore $a(c\bar{c}) + (\bar{d}d)a = a(c\bar{c} + \bar{d}d) = 0$ yields either i) $a = 0$, hence $\bar{d}b = 0 = b\bar{c}$, that is $(b = 0)$ or $(c = 0$ and $d = 0)$, ii) $c\bar{c} + \bar{d}d = 0$, hence $c = d = 0$.

b) For the associativity of \times , we consider first

$$\begin{aligned} ((a, b) \times (c, d)) \times (e, f) &= (ac - \bar{d}b, da + b\bar{c}) \times (e, f) = \\ &((ac - \bar{d}b)e - \bar{f}(da + b\bar{c}), f(ac - \bar{d}b) + (da + b\bar{c})\bar{e}) = \\ &((ac)e - (\bar{d}b)e - \bar{f}(da) - \bar{f}(b\bar{c}), f(ac) - f(\bar{d}b) + (da)\bar{e} + (b\bar{c})\bar{e}). \end{aligned}$$

Then

$$\begin{aligned} (a, b) \times ((c, d) \times (e, f)) &= \\ &(a(ce) - a(\bar{f}d) - (\bar{c}f)b - (e\bar{d})b, (fc)a + (d\bar{e})a + b(\bar{e}\bar{c}) - b(\bar{d}f)). \end{aligned}$$

Associativity at the $(k-1)^{\text{st}}$ level yields $(ac)e = a(ce)$ for example, and commutativity yields $(\bar{d}b)e = e(\bar{d}b) = (e\bar{d})b$.

c) To prove commutativity, we consider

$$\begin{aligned} (a, b) \times (c, d) &= (ac - \bar{d}b, da + b\bar{c}), \\ (c, d) \times (a, b) &= (ca - \bar{b}d, bc + d\bar{a}). \end{aligned}$$

By commutativity at the $(k-1)^{\text{st}}$ level $ac = ca$, and by selfconjugacy $\bar{\bar{d}} = d$, $\bar{\bar{b}} = b$, $a = \bar{\bar{a}}$, $c = \bar{\bar{c}}$. Δ

Corollary 5.7 $A_0 = \mathbb{R}$ satisfies (i) to (iv), $A_1 = \mathbb{C}$ satisfies (i) to (iii), $A_2 = \mathbb{H}$ satisfies (i) and (ii), $A_3 = \mathbb{G}$ satisfies (i). For the algebras A_k , $k > 3$ none of these properties is satisfied.

Proof: Immediate consequence of Lemma 5.6 for A_1, A_2, A_3 . That $A_4 = \mathbb{G} \times \mathbb{G}$, the algebra of hexadecanions is not a division algebra can be seen from the following example: let $x = (e_7, e_8)$ and $y = (e_5, e_6)$, where e_1, e_2, \dots, e_8 denote the 8 vectors of the canonical basis of \mathbb{G} . x and y are nonzero vectors of A_4 and to prove $x \times y = 0$ we write

$$x \times y = (e_7e_5 - \bar{e}_6e_8, e_6e_7 + e_8\bar{e}_5).$$

Let us denote e'_1, e'_2, e'_3, e'_4 and e''_1, e''_2 the canonical basis vectors in \mathbb{H} and \mathbb{C} , respectively. We have

$$\begin{aligned} e_7e_5 &= (0, e'_3) \times (0, e'_1) = (0 \cdot 0 - e'_1 \cdot e'_3, e'_1 \cdot 0 + e'_3 \cdot 0) = (-e'_3, 0), \\ \bar{e}_6e_8 &= (0, -e'_2) \times (0, e'_4) = (\bar{e}'_4e'_2, 0), \\ e'_3 + \bar{e}'_4e'_2 &= (0, e''_1) + (0, -e''_2) \times (e''_2, 0) = (0, e''_1) + (0, -e''_2\bar{e}''_2) = \\ &(0, e''_1) + (0, -e''_1) = 0. \end{aligned}$$

Analogously

$$e_6 e_7 = (0, e'_2) \times (0, e'_3) = (-\bar{e}'_3 e'_2, 0), \quad e_8 \bar{e}_5 = (0, e'_4) \times (0, -e'_1) = (e'_4, 0),$$

$$-\bar{e}'_3 e'_2 + e'_4 = (0, e''_1) \times (e''_2, 0) + (0, e''_2) = (0, \bar{e}''_2) + (0, e''_2) = 0.$$

Therefore $x \times y = (0, 0) = 0$. \triangle

Proposition 5.8 *The multiplication is isometric in A_0, A_1, A_2 and A_3 .*

Proof: The isometry $|xy| = |x||y|$ is evident in $A_0 = \mathbb{R}$. In $A_1 = \mathbb{C}$, we check from $(a + ib) \times (c + id) = ac - bd + i(bc + ad)$ that $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (bc + ad)^2$. Similarly in $A_2 = \mathbb{H}$ and $A_3 = \mathbb{G}$, one can establish the four squares theorem (Euler, 1748) and the eight squares theorem (Degen, 1818) by direct computation. \triangle

For the other algebras $A_k, k \geq 4$, one has only the metric property: there exists $\sigma > 0$ such that $|x \times y| \leq \sigma|x||y|$ for $x, y \in V$ [4, p.241]. In A_4 , a preliminary numerical study shows that $\sigma > 1$ as could be expected. But the average value for $\frac{|x \times y|}{|x||y|}$ seems surprisingly close to 1. Similarly, the $A_k, k \geq 3$, are not associative, but retain the weaker form of associativity called **power-associativity** which concerns exponentiation: $x^m \times x^n = x^{m+n}$, for all $m \geq 1, n \geq 1$, and all $x \in A_k$ [4, p.190].

Proposition 5.9 *The multiplication is power associative in $A_k, k \geq 0$.*

Proof: We prove by recurrence that $x \times x^2 = x^2 \times x$ for x in $A_k, k > 0$. In $A_0 = \mathbb{R}$, the recurrence assumption is true.

Let $x = (a, b)$, then $x^2 = (-|b|^2 + a^2, 2(\mathcal{R}e a)b)$ and $\overline{x^2} = (\bar{x})^2$, with $\bar{x} = (\bar{a}, -b)$. We assume that $a \cdot a^2 = a^2 \cdot a$. Therefore

$$x \times x^2 - x^2 \times x = (a \cdot a^2 - a^2 \cdot a, 2 \mathcal{R}e a (b \cdot (a - \bar{a}) + b(\bar{a} - a))) = (0, 0).$$

\triangle

As we saw, for $k = 0$ to 3, the multiplication has stronger properties (respectively selfconjugate, commutative, associative and alternative [4]). The power associativity, which is valid for any k , makes it possible to define exponentiation $n \rightarrow x^n$, for any integer value $n \in \mathbb{N}^* = \mathbb{N} \setminus \{0\}$ of the exponent, and for any x in A_k .

It can be shown that an algebra is associative (respectively alternative, or power associative) iff the subalgebra generated by any 3 (respectively 2, or 1) different elements is itself associative.

5.2 The recursive structure of the multiplication in A_k

In order to make the recursive structure of the multiplication on A_k more apparent, we explicit below the multiplication $x'' = x \times x'$ for x and x' in $\mathbb{R}, \mathbb{C}, \mathbb{H}$ and \mathbb{G} respectively, the components of x and x' being a, b, c, \dots, h and a', b', c', \dots, h' respectively.

i) multiplication in \mathbb{R}

$$\mathbf{a} \times \mathbf{a}' = \mathbf{a}'' = \mathbf{a}\mathbf{a}',$$

ii) multiplication in \mathbb{C}

$$(\mathbf{a}, \mathbf{b}) \times (\mathbf{a}', \mathbf{b}') = (\mathbf{a}'', \mathbf{b}'')$$

$$\mathbf{a}'' = \mathbf{a}\mathbf{a}' - \mathbf{b}\mathbf{b}'$$

$$\mathbf{b}'' = \mathbf{a}\mathbf{b}' + \mathbf{b}\mathbf{a}',$$

iii) multiplication in \mathbb{H}

$$(\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}) \times (\mathbf{a}', \mathbf{b}', \mathbf{c}', \mathbf{d}') = (\mathbf{a}'', \mathbf{b}'', \mathbf{c}'', \mathbf{d}'')$$

$$\mathbf{a}'' = \mathbf{a}\mathbf{a}' - \mathbf{b}\mathbf{b}' - \mathbf{c}\mathbf{c}' - \mathbf{d}\mathbf{d}'$$

$$\mathbf{b}'' = \mathbf{a}\mathbf{b}' + \mathbf{b}\mathbf{a}' + \mathbf{c}\mathbf{d}' - \mathbf{d}\mathbf{c}'$$

$$\mathbf{c}'' = \mathbf{a}\mathbf{c}' + \mathbf{c}\mathbf{a}' + \mathbf{d}\mathbf{b}' - \mathbf{b}\mathbf{d}'$$

$$\mathbf{d}'' = \mathbf{a}\mathbf{d}' + \mathbf{d}\mathbf{a}' + \mathbf{b}\mathbf{c}' - \mathbf{c}\mathbf{b}',$$

iv) multiplication in \mathbb{G}

$$(\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{e}, \mathbf{f}, \mathbf{g}, \mathbf{h}) \times (\mathbf{a}', \mathbf{b}', \mathbf{c}', \mathbf{d}', \mathbf{e}', \mathbf{f}', \mathbf{g}', \mathbf{h}') = (\mathbf{a}'', \mathbf{b}'', \mathbf{c}'', \mathbf{d}'', \mathbf{e}'', \mathbf{f}'', \mathbf{g}'', \mathbf{h}'')$$

$$\mathbf{a}'' = \mathbf{a}\mathbf{a}' - \mathbf{b}\mathbf{b}' - \mathbf{c}\mathbf{c}' - \mathbf{d}\mathbf{d}' - \mathbf{e}\mathbf{e}' - \mathbf{f}\mathbf{f}' - \mathbf{g}\mathbf{g}' - \mathbf{h}\mathbf{h}'$$

$$\mathbf{b}'' = \mathbf{a}\mathbf{b}' + \mathbf{b}\mathbf{a}' + \mathbf{c}\mathbf{d}' - \mathbf{d}\mathbf{c}' + \mathbf{h}\mathbf{g}' - \mathbf{g}\mathbf{h}' + \mathbf{e}\mathbf{f}' - \mathbf{f}\mathbf{e}'$$

$$\mathbf{c}'' = \mathbf{a}\mathbf{c}' + \mathbf{c}\mathbf{a}' + \mathbf{d}\mathbf{b}' - \mathbf{b}\mathbf{d}' + \mathbf{f}\mathbf{h}' - \mathbf{h}\mathbf{f}' + \mathbf{e}\mathbf{g}' - \mathbf{g}\mathbf{e}'$$

$$\mathbf{d}'' = \mathbf{a}\mathbf{d}' + \mathbf{d}\mathbf{a}' + \mathbf{b}\mathbf{c}' - \mathbf{c}\mathbf{b}' + \mathbf{g}\mathbf{f}' - \mathbf{f}\mathbf{g}' + \mathbf{e}\mathbf{h}' - \mathbf{h}\mathbf{e}'$$

$$\mathbf{e}'' = \mathbf{a}\mathbf{e}' + \mathbf{e}\mathbf{a}' - \mathbf{b}\mathbf{f}' + \mathbf{f}\mathbf{b}' - \mathbf{c}\mathbf{g}' + \mathbf{g}\mathbf{c}' - \mathbf{d}\mathbf{h}' + \mathbf{h}\mathbf{d}'$$

$$\mathbf{f}'' = \mathbf{a}\mathbf{f}' + \mathbf{f}\mathbf{a}' + \mathbf{b}\mathbf{e}' - \mathbf{e}\mathbf{b}' - \mathbf{c}\mathbf{h}' + \mathbf{h}\mathbf{c}' + \mathbf{d}\mathbf{g}' - \mathbf{g}\mathbf{d}'$$

$$\mathbf{g}'' = \mathbf{a}\mathbf{g}' + \mathbf{g}\mathbf{a}' + \mathbf{b}\mathbf{h}' - \mathbf{h}\mathbf{b}' + \mathbf{c}\mathbf{e}' - \mathbf{e}\mathbf{c}' - \mathbf{d}\mathbf{f}' + \mathbf{f}\mathbf{d}'$$

$$\mathbf{h}'' = \mathbf{a}\mathbf{h}' + \mathbf{h}\mathbf{a}' - \mathbf{b}\mathbf{g}' + \mathbf{g}\mathbf{b}' + \mathbf{c}\mathbf{f}' - \mathbf{f}\mathbf{c}' + \mathbf{d}\mathbf{e}' - \mathbf{e}\mathbf{d}'$$

6 The recursive construction of binary algebras

In the mathematical literature, hypercomplex numbers have **real** components. And real algebras are based on the field of real numbers. However, since Computer Science (and logic) make such a heavy use of the finite field $\mathbb{Z}/2\mathbb{Z}$ consisting of the two numbers $\{0, 1\}$, it is tempting to see how the construction of the preceding paragraph is modified if one starts the recursion from $B_0 = \mathbb{Z}/2\mathbb{Z} = \mathbb{Z}_2$.

The successive algebras B_k , $k \geq 0$, are obviously finite. And the theorem of Wedderburn (1905) applies: every finite division algebra is actually a field [6]. Such algebras are considered in [11].

Lemma 6.1 *In the algebras B_k , $k \geq 0$, the conjugacy map is the identity and the multiplication is associative and commutative.*

Proof: Clear by induction on k . The identity (6) becomes $\overline{(a, b)} = (a, b)$. The expression (7) yields

$$(a, b) \times (c, d) = (ac + db, da + bc) = (c, d) \times (a, b) = (ca + bd, bc + da).$$

△

It is easy to conclude that B_0 is the only binary division algebra. For the other algebras B_k , $k > 0$, the multiplication is associative and commutative. The inverse x^{-1} of $x \neq 0$ does not always exist: this is a consequence of $x = \bar{x}$, therefore $x \times \bar{x} = x^2$ cannot play the role of a norm: it can be zero for $x \neq 0$. However, because the computation in \mathbb{Z}_2 is mod 2, the square $x^2 = (a, b) \times (a, b) = (a^2 + b^2, 2ab)$ is such that $2ab = 0$ and $a^2 + b^2 \in \mathbb{Z}_2$. Therefore $x^2 = 0$ or $x^2 = 1$, depending on the number of nonzero components in x . Because of addition mod 2, $x^2 = 1$ iff x has an odd number of nonzero components, then $x^{-1} = x$.

Lemma 6.2 *In B_k , $k \geq 0$, $x^2 = 1$, or equivalently, x^{-1} exists and $x^{-1} = x$ iff x has an odd number of nonzero components.*

We remark that with the change of notation $00 \rightarrow 0$, $10 \rightarrow 1$, $11 \rightarrow 2$, $01 \rightarrow 3$, the multiplication of $B_1 = B_0 \times B_0$ becomes that of $\mathbb{Z}/4\mathbb{Z} = \mathbb{Z}_4$, the ring of integers modulo 4 (where $2 \times 2 = 0 \pmod{4}$).

The reader should notice that the above notation **differs** from the usual binary notation: $00 \rightarrow 0$, $01 \rightarrow 1$, $10 \rightarrow 2$, $11 \rightarrow 3$ by a cyclic permutation of the 3 numbers different from 0.

7 Conclusion

We have studied the recursive construction of algebras of dimension 2^k , $k \geq 0$ from $A_0 = \mathbb{R}$ and from $B_0 = \mathbb{Z}_2$. In the case of real algebras of hypercomplex numbers, we showed that there is really 3 operations to consider: the classical arithmetic operations $+$ and \times , and the geometric conjugacy operation. Only the four first algebras are with division. They correspond to the well-known systems of hypercomplex numbers \mathbb{R} , \mathbb{C} , \mathbb{H} and \mathbb{G} of dimension 1, 2, 4 and 8. The inverse of any nonzero vector always exists in A_k , $k \geq 0$.

In the case of binary algebras, only the first $B_0 = \mathbb{Z}_2$ is with division (it is a field). The multiplication in B_k , $k > 0$ satisfies the two properties (ii) and (iii), but the inverse $x^{-1} = x$ does not always exist for $x \neq 0$. All B_k , $k \geq 0$ are selfconjugate.

The interplay between Algebra and Geometry is effectively at work only for real hypercomplex computation when the conjugacy map is not trivially reduced to the identity. The intimate connection between Algebra and Geometry expressed by (6) and (7) may be the reason why it has been so difficult to prove that there are essentially only four real division algebras, hence justifying the use of **sophisticated topological** methods.

References

- [1] Chaitin–Chatelin F., Le Sens de la Vie, *CERFACS Technical Report* TR/PA/99/20.
- [2] Chaitin–Chatelin F., The computing power of Geometry, In D.F. Griffiths and G.A. Watson, editors, *Numerical Analysis 1999*, CRC Press LLC, pp.83–92 (1999). (Also available as CERFACS Technical Report TR/PA/99/24).

- [3] Chaitin–Chatelin F., Meškauskas T., Computation With Hypercomplex Numbers, *Nonlinear Analysis*, **47**, pp.3391–3400 (2001). (Also available as *CERFACS Technical Report TR/PA/00/69*).
- [4] Ebbinghaus H-D et al., *Les nombres*, Vuibert, Paris (1998).
- [5] Dickson L.E, On quaternions and their generalization and the history of the 8 square theorem, *Annals of Math*, **20**, pp.155–171 (1919).
- [6] Parshall K.H, In pursuit of the finite division algebra theorem and beyond, *Arch. Int. Hist. Sciences*, **33**, N° 111, pp.274–299 (1983).
- [7] Kauffman L., Map coloring and the vector cross product, *J. Comb. Theory B*, **48**, 45 (1990).
- [8] Kauffman L., Saleur H., An algebraic approach to the planar colouring problem, *Comm. Math. Phys.*, **152**, pp.565–590 (1993).
- [9] Baez J., This week’s finds in mathematical physics (week 8), Available at <http://www.math.ucr.edu/home/baez/week8.html>
- [10] Rusin D., Product structures and division rings over the real numbers, Available at <http://www.math.niu.edu/~rusin/papers/known-math/index/products.html>
- [11] Albert A.A., Quadratic forms permitting composition, *Annals of Math*, **43**, pp.161–177 (1942).