

Beyond ideals in the Dickson ring of integral octonions

Françoise Chaitin-Chatelin¹

CERFACS Technical Report TR/PA/04/96

¹Université Toulouse 1 and CERFACS, 42 Ave. G. Coriolis, 31057 Toulouse
Cedex 1, France. E-mail: chatelin@cerfacs.fr

Abstract

This is ongoing work on hypercomputation [4]. We revisit the works of Dickson [5] and Mahler [9] on integral octonions. Nonassociativity (in the form of alternativity) leads to the unexpected consequence that the theorem of (at most) 4 squares (Bachet – Lagrange) becomes a theorem of (exactly) 1, 2 or 4 *identical* squares for a subset of \mathbb{N}^* . These numbers measure the norm of the vectors in the Dickson ring of integral octonions for which the *associator* (with 3 or 7 pairs of distinct imaginary canonical basis vectors in \mathbb{G}) is computable as a product in the Dickson ring.

Key words: theorem of 1, 2, 4, 8 squares, associator, alternativity, integral computability, integral quaternions, integral octonions, field of multiplicative information, ring, ideal, Dickson, Mahler

1. Introduction

1.1. The four hypercomplex division algebras

There are four hypercomplex algebras on the real basis field \mathbb{R} in which multiplication is norm multiplicative, when it is defined by the Dickson inductive process (1914) from the usual multiplication in \mathbb{R} . These algebras A_k have no other zero divisor than zero: they are division algebras. They have dimension 2^k , $0 \leq k \leq 3$ on \mathbb{R} . They define respectively the *real* numbers as $A_0 = \mathbb{R}$, the *complex* numbers as $A_1 = \mathbb{C}$, the *quaternions* as $A_2 = \mathbb{H}$, and the *octonions* as $A_3 = \mathbb{G}$ [2, 4, 5, 6].

For $x \in A_k$, $k \in \mathbb{N}$, the (arithmetic) norm is

$$N(x) = x \bar{x} = \|x\|^2$$

where $\|\cdot\|$ denotes the (geometric) euclidean norm in \mathbb{R}^{2^k} (with $x = \bar{x}$ in A_0).

The norm multiplicativity of hypercomplex multiplication for $0 \leq k \leq 3$ is expressed by:

$$N(x \times y) = N(x) \cdot N(y). \quad (1)$$

When k increases from 0 to 4, multiplication loses a given property at each step, namely reality for $k \geq 1$, commutativity for $k \geq 2$, associativity for $k \geq 3$, and at last norm multiplicativity for $k \geq 4$. However, it retains the weaker property of flexibility for all $k \geq 4$ [4].

1.2. The three theorems of squares

The norm multiplicativity for $k \leq 3$ entails the celebrated theorems of 2, 4 and 8 squares which have a long history ranging from the third century BC to the beginning of the 19th century.

They express in particular that any product of two integers which are sums of 2, 4 or 8 perfect squares is itself a sum of 2, 4 or 8 squares. The possibility of the representation of an integer as a sum of 2, 4 or 8 squares is preserved under multiplication.

1.2.1. The theorem of 2 squares

For $w = u + iv$ and $z = x + iy$ in \mathbb{C} , the identity $|wz| = |w| |z|$ implies

$$(u^2 + v^2)(x^2 + y^2) = (ux - vy)^2 + (uy + vx)^2. \quad (2)$$

This identity was known to Diophantus of Alexandria, and to the Indians. It has an important application in Number Theory.

For example, a positive integer is the sum of 2 squares if each of its prime factors has the same property. Fermat (1640) proved that an odd prime p is the sum of two squares iff $p = 4k + 1$, $k \in \mathbb{N}^*$.

1.2.2. The theorem of 4 squares

It is easy to derive it from the law of (associative) multiplication for quaternions (Hamilton, 1843). However, it was proved directly by Euler in 1748, in a letter to Goldbach. This was a key step in his attempt to prove the assertion of Bachet (1621) and Fermat (1638), apparently known to Diophantus, that any positive integer is the sum of at most 4 squares. This was first established by Lagrange (1770). Since then many other proofs have appeared [7]. We mention, as relevant to our topic, proofs which use the ring $R_2 = H$ of integral quaternions introduced by Hurwitz [8] and the structure of its left or right ideals [7, pp. 303–310; 3, pp. 14–17; 11].

The theorems of Fermat and Lagrange establish that dimensions 2 and 4 are sufficient to factor any rational prime.

1.2.3. The theorem of 8 squares

Again, its discovery by Degen (1818) predated the little-known invention of the octonions by Graves in December 1843, two months after the much-better-known invention of Hamilton's quaternions.

Multiplication for octonions is not associative, but *alternative*. The associator

$$(x, y, z) \longmapsto [x, y, z] = (x \times y) \times z - x \times (y \times z)$$

is a trilinear map which alternates signs with x, y, z :

$$[x, y, z] = [z, x, y] = -[x, z, y] = -[y, x, z].$$

See [4].

Any representation of an integer as a sum of 8 squares is obviously not the shortest possible. Therefore, one is led to wonder about the questions:

- What is the role of norm multiplicativity in a space with 8 dimensions?

- Is there a use for a theorem of 8 squares in Number Theory?

We consider these two questions from the point of view of the rings R_k , $k = 0$ to 3 , of hypercomplex integers of dimension $1, 2, 4, 8$ as they have been defined by Dickson in order to preserve the factorisation into primes [5, pp. 292–293].

We recall the classical (though surprising) result that any ideal in R_3 is principal and 2-sided [1, 11, 12]. Then we revisit the insufficiently appreciated paper of Kurt Mahler [9]. This work amounts to a rational characterisation of a class of vectors in R_3 such that their associator with specific pairs of canonical basis vectors is computable in R_3 . Such vectors are of the form $\gamma = n g_*$, $n \in \mathbb{Z}$ and $N(g_*) = N = 1, 2$ or 4 . Hence follows a theorem of 1, 2 or 4 identical squares for the norm $N(\gamma) = N n^2$ of such vectors.

2. The rings R_k of hypercomplex integers, $k \leq 3$

2.1. The commutative rings R_0 and R_1

In $A_0 = \mathbb{R}$, the ring of rational integers is $R_0 = \mathbb{Z}$ with the 2 units ± 1 of norm 1, $R_0^\times = \{\pm 1\}$. In $A_1 = \mathbb{C}$, the ring of complex integers R_1 consists of the gaussian integers $R_1 = \mathbb{Z}^2$, with the 4 units of norm 1 in $R_1^\times = \{\pm 1, \pm i\}$. Multiplication is commutative in \mathbb{R} and \mathbb{C} , therefore $R_0 = \mathbb{Z}$ and $R_1 = \mathbb{Z}^2$ are commutative.

2.2. The noncommutative ring R_2

In $A_2 = \mathbb{H}$, an integral quaternion defined by Hurwitz (1896) has 4 components on the canonical basis $\{1, i, j, k\}$ which are either (i) all rational integers or (ii) all halves of rational odd integers. Therefore the ring of integral quaternions is

$$R_2 = H = \left\{ \mathbb{Z}^4 \text{ or } \mathbb{Z}^4 + \frac{1}{2}e \right\}$$

with $e = 1 + i + j + k$.

There are 24 units of norm 1 defined by

$$R_2^\times = H^\times = \left\{ \pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k) \right\}.$$

For future reference, we denote

$$B_1 = \{\pm 1, \pm i, \pm j, \pm k\}$$

and

$$B_4 = \left\{ \frac{1}{2}(\pm 1 \pm i \pm j \pm k) \right\},$$

such that $H^\times = B_1 \cup B_4$. We also introduce the linear combinations of *two* basis vectors, with coefficients ± 1 , of norm 2:

$$B_2 = \{\pm 1 \pm i, \pm 1 \pm j, \pm 1 \pm k, \pm i \pm j, \pm i \pm k, \pm j \pm k\},$$

We set

$$K = B_1 \cup B_2 \cup B_4 = H^\times \cup B_2.$$

The results listed below are standard in $R_2 \subset A_2 = \mathbb{H}$ [7]:

- (1) For any $s \in A_2$, there exists t in R_2 such that

$$N(s - t) \leq \alpha < 1.$$

(The best bound is $\alpha = \frac{1}{2}$.)

- (2) The ring R_2 is euclidean: for any $a, b \in R_2$, $b \neq 0$ there are q, r and q', r' in R_2 such that

$$a = q \times b + r, \quad N(r) < N(b)$$

and

$$a = b \times q' + r', \quad N(r') < N(b).$$

- (3) Any left or right ideal $\neq \{0\}$ in R_2 is principal.

We recall that a (left) *ideal* S in a noncommutative ring R is a subgroup (for $+$) which is closed under left multiplication in R , that is

$$R \times S \subseteq S$$

($t \times s \in S$ for any $t \in R$, $s \in S$). A *principal* ideal S in a euclidean ring R is of the form $R \times s$ (left) or $s \times R$ (right), where $s \in S$ has *minimal* norm.

Any left (or right) ideal S in R_2 is generated by one of the minimal norm quaternions q such that $m = N(q) = q\bar{q}$ is minimal. Therefore m is a sum of at most 4 squares, usually different.

2.3. The nonassociative ring R_3

In $A_3 = \mathbb{G}$, the nonassociative ring $R_3 = D$ of integral octonions was introduced by Dickson [5, pp. 319–325]. First, we observe that the multiplication in \mathbb{G} is deduced from that in \mathbb{H} by the inductive Dickson doubling process (1912). The process yields the multiplication table given by Graves (in a letter to Hamilton, January 4, 1844) and Cayley (1845). This table is equivalent, but *not* identical, to the one which is used in [2]. The characterisation of integral octonions in \mathbb{G} goes as follows, [5], p. 322:

g is integral in \mathbb{G} iff

$$g = \sum_{i=1}^8 \alpha_i g_i,$$

where $\alpha_i \in \mathbb{Z}$ in the basis

$$\begin{aligned} g_1 &= (i, 0), \\ g_2 &= (j, 0), \\ g_3 &= (k, 0), \\ g_4 &= \left(\frac{e}{2}, 0\right), \\ g_5 &= (0, 1), \\ g_6 &= \left(\frac{1+i}{2}, \frac{1+j}{2}\right), \\ g_7 &= \left(\frac{1+j}{2}, \frac{1+i}{2}\right), \\ g_8 &= \left(\frac{1+k}{2}, \frac{1+k}{2}\right). \end{aligned}$$

Dickson also gave a characterisation of the set $R_3^\times = D^\times$ of 240 units in R_3 (norm 1). The set D^\times can be divided into $C_1 \cup C_4^*$, with

$$C_1 = (H^\times \times \{0\}) \cup (\{0\} \times H^\times),$$

and C_4^* is the subset in D^\times of

$$\frac{1}{2}C_4 = \frac{1}{2}B_2 \times B_2$$

consisting of those vectors which are divisible by 2. Card $C_1 = 48$ and card $C_4^* = 192$.

However, Dickson missed the euclidean character of R_3 which had to wait 20 years to be proved. Mahler [9] establishes the crucial

Lemma 2.1. *For any s in A_3 , there exists t in R_3 such that*

$$N(s - t) \leq \alpha < 1.$$

In [9], he proves $\alpha = 15/16$. However, he knows that the best bound is again $\alpha = 1/2$.

Lemma 2.1 extends **(1)** to R_3 . This is all that is required to have **(2)** and **(3)** also valid in R_3 . Mahler [9] also establishes the following characterisation of R_3 . Let

$$x = \sum_{i=0}^3 x_i e_i, \quad y = \sum_{i=0}^3 y_i e_i$$

be quaternions where we have set

$$e_0 = 1, \quad e_1 = i, \quad e_2 = j, \quad e_3 = k.$$

Proposition 2.2. *The octonion $g = (x, y)$ belongs to R_3 iff the 8 numbers $2x_i, 2y_i, i = 0$ to 3 , are rational integers in \mathbb{Z} which satisfy the 5 congruence identities mod 2:*

- $2(x_0 + x_1) = 2(y_0 + y_2) \pmod{2},$
- $2(x_0 + x_2) = 2(y_0 + y_1) \pmod{2},$
- $2(x_0 + x_3) = 2(y_0 + y_3) \pmod{2},$
- $\sum_{i=0}^3 2x_i = \sum_{i=0}^3 2y_i = 0 \pmod{2}.$

Therefore the quaternions x and y have to be both either integral or not integral in order for $g = (x, y)$ to be an integral octonion.

3. Ideals in the Dickson ring $D = R_3$

By property **(3)**, the algebraic structures of ideals in R_2 and R_3 are similar: all ideals are principal: they are generated by one of the elements of minimal norm. However the *nonassociativity* (alternativity) of multiplication creates a new situation in A_3 when compared to A_2 . It allows us to derive properties of the generator of any ideal in the ring of integral octonions. A fact which is not possible in integral quaternions because of associativity! Commonly viewed as a *restriction*, the lack of associativity for \times in D does create arithmetic *computational opportunities*, as we shall see later.

3.1. All ideals in R_3 are principal and 2-sided

The following spectacular unification of the structure of ideals in R_3 , when we compare it with the diversity in R_2 , was essentially proved in [12]. In 1963, Lamont extended to an arbitrary ideal the 1942 result by Mahler that the basis of any *odd* ideal is a rational integer [9]. This unification comes from the alternativity and isometry of \times in \mathbb{G} .

Proposition 3.1. *Any ideal S in R_3 is principal and 2-sided. It is generated by $\gamma = nu$, $u \in D^\times$, $n \in \mathbb{Z}$, which has minimal norm n^2 in S .*

Proof [1; 11, pp. 109–110]. S is principal because R_3 is euclidean. A left ideal is closed under unit left multiplication. And any right unit multiplication is the product of seven left ones [11, p. 93]. Therefore S is 2-sided and $S = nD^\times$. More details are found in [1], and [11]. These advanced proofs differ greatly from the explicit elementary computation performed in [9, 12]. Although this is an obvious corollary of his result, Lamont does not explicitly mention the 2-sidedness of ideals in D \square

Any ideal is invariant under the rotation group of R_3 (isomorphic to SO_8 , the special orthogonal group of \mathbb{R}^8 [1, 11]). Such an object is said to be perceived geometrically. In particular, the norm n^2 of an ideal is invariant under any rotation.

Because all ideals S are 2-sided in R_3 , the ring structure $(R_3/S, +, \cdot) = \mathbb{Z}$ which *is* associative is, loosely speaking, “almost homomorphic” to $(R_3, +, \times)$ which *is not* associative. This shows how integers in \mathbb{Z} can emerge by (noncommutative and alternative) multiplication of integral octonions, as

the square root $\pm n$ of the norm n^2 of any ideal.

3.2. Mahler's paper revisited [9]: the field of information

Seeking to study ideals in R_3 , Mahler establishes Theorem 2 [9, p. 133] in which the second statement cannot apply for ideals (when the vectors G_* have norm 2 or 4) as we know from Section 3.1.

Despite its limited success in achieving the characterisation of ideals, Mahler's proof presents an interesting computational approach in D . It constitutes the core of Lamont's paper [12], which shows that indeed vectors of norm 2 or 4 cannot generate ideals. Mahler's approach seeks to measure the nonassociativity of multiplication in D by means of the associator map:

$$[a, b, -] = ((a \times b) \times -) - a \times (b \times -).$$

For this purpose, Mahler introduces the auxiliary map

$$\varphi: (a, b, \gamma) \mapsto c \text{ such that } a \times (b \times \gamma) = c \times \gamma,$$

where the pair (a, b) is restricted to be any of 3 or 7 particular pairs of distinct imaginary canonical basis vectors for \mathbb{G} . For any γ in the domain of definition for φ in D , the associator $[a, b, \gamma]$ is computable as the left multiplication $d \times \gamma$ by $d = a \times b - c$ in D .

The vector $d = [a, b, \gamma] \times \gamma^{-1}$ can be uniquely expressed as

$$d = a \times b - (a \times (b \times \gamma)) \times \gamma^{-1}$$

in the *alternative* algebra $A_3 = \mathbb{G}$, for any $\gamma \neq 0$. d represents the modification of the product $a \times b$ when it is multiplied by an arbitrary third vector $\gamma \neq 0$. Because \times is *not* associative in \mathbb{G} , d need not be 0.

Definition 3.1. For a, b given in \mathbb{G} , the field of multiplicative information associated with (a, b) is the map

$$\gamma \in \mathbb{G} \setminus \{0\} \mapsto [a, b, \gamma] \times \gamma^{-1} \in \mathbb{G}.$$

Set $A = [a, b, \gamma] \in \Im\mathbb{G}$. A does not depend on the real parts of a, b, γ . Moreover $[a, b, \gamma] = -[b, a, \gamma]$ and $[a, a, \gamma] = 0$ by alternativity.

It is clear that for any $\gamma \in \mathfrak{S}\mathbb{G}$:

$$d = A \times \gamma^{-1} = \frac{1}{N(\gamma)} (\langle A, \gamma \rangle - A \wedge \gamma)$$

in \mathbb{G} , where $\langle A, \gamma \rangle \in \mathbb{R}$ and $A \wedge \gamma \in \mathfrak{S}\mathbb{G} \simeq \mathbb{R}^7$ are respectively the scalar and vector products for A, γ in $\mathfrak{S}\mathbb{G}$ (continental notation!).

The field of information depends on the 2 vector parameters (a, b) . Mahler is interested in those $\gamma \neq 0$ in D for which the (multiplicative) information field associated with specific pairs (a, b) belongs to D as well. Let Mahler be our guide on the arithmetical path that he opened in the Dickson ring. This will gradually reveal the landscape, extending *beyond ideals*, that Mahler foresaw in 1942. This greater arithmetical vista has remained completely unexplored since then.

3.3. The root vectors

Let e_l denote an imaginary canonical vector in $\mathfrak{S}\mathbb{H}$, $l = 1, 2, 3$. Then $f_l = (e_l, 0)$ (resp. $f_{l+4} = (0, e_l)$) denote the canonical vectors in $\mathfrak{S}\mathbb{G}$ of ordinal 1, 2, 3 (resp. 5, 6, 7) for $l = 1, 2, 3$. Let (λ, μ, ν) represent a cyclic permutation of (1, 2, 3) or (5, 6, 7).

We define (R) in D to be the set of vectors g of the form $g = (a, 0)$ or $(0, a)$ for a in K , and $g = (a, b)$ for (a, b) in

$$(B_1 \times B_1) \cup (B_2 \times B_2) \cup (B_4 \times B_4) = \Delta,$$

with $N(a) = N(b)$. Hence

$$(R) = (K \times \{0\}) \cup (\{0\} \times K) \cup \Delta = L \cup \Delta.$$

Root vectors in L (for lateral) (resp. Δ (for diagonal)) are said to be external (resp. internal). It will be useful to consider the subsets of D defined as

$$D_b = \{\gamma = (x, y) \text{ in } D \text{ with } N(x) = N(y) > 0\},$$

and

$$D_p = \{\gamma = (x, 0) \text{ or } (0, y) \text{ in } D \text{ with } x \text{ or } y \neq 0\}.$$

Vectors in D_b have their quaternionic parts of equal length (b for balanced). Vectors in D_p have one quaternionic part not reduced to 0 (p for projected).

Lemma 3.2. *The vectors in (R) have norm $N = 1, 2$ or 4 . The vectors of norm 1 describe D^\times .*

Proof. That $(R) \subset D$ is checked by Proposition 2.2. The rest is clear by $N(a) = N(b)$. \square

Definition 3.2. *The set (R) is the set of root vectors in D .*

How many root vectors are there in (R) ? It is known that there are respectively $240 \times 1, 240 \times 9 = 2160$ and $240 \times 73 = 17520$ vectors in D with norm N equal to 1, 2 and 4 ([9], [11, pp. 106 and 135]). However, for $N = 2$ and 4, not all these vectors are in (R) . More precisely,

Proposition 3.3. *There are 992 vectors in (R) with 368 vectors of norm 2 and 384 vectors of norm 4.*

Proof. Let us compute card (R) with $(R) = L \cup \Delta$. One has card $B_1 = 2 \times 4 = 8$, card $B_2 = 4 \times 6 = 24$ and card $B_4 = 16$. Therefore card $K = 2 \times 24 = 48$ and card $L = 2 \times 48 = 96$. Now

$$\Delta = B_1 \times B_1 \cup B_2 \times B_2 \cup B_4 \times B_4$$

and

$$\text{card } \Delta = 8^2 + 24^2 + 16^2 = 896.$$

Hence

$$\text{card } (R) = 896 + 96 = 992 = 31 \times 32.$$

There are *much fewer* root vectors than the totality of vectors of norm 1, 2 and 4 in D , that is $240 \times 83 = 19920$. The percentage is $\frac{992}{19920} \sim 0.05$. We denote by Θ_N , $N = 1, 2, 4$ the sets of root vectors of norm N in (R) . Remarkably, (R) contains *all* unit vectors of D^\times , that is $\Theta_1 = D^\times$. They represent a percentage of

$$\frac{240}{992} = \frac{2^4 \times 15}{2^5 \times 31} = \frac{15}{62} \sim 0.25$$

of the totality of root vectors.

The set Θ_2 of vectors of norm $N = 2$ in (R) corresponds to

$$B_1 \times B_1 \cup B_4 \times B_4 \cup B_2 \times \{0\} \cup \{0\} \times B_2$$

with cardinality equal to

$$64 + 256 + 2 \times 24 = 368 = 2^4 \times 23,$$

yielding the percentage

$$\frac{368}{992} = \frac{23}{62} \sim 0.371.$$

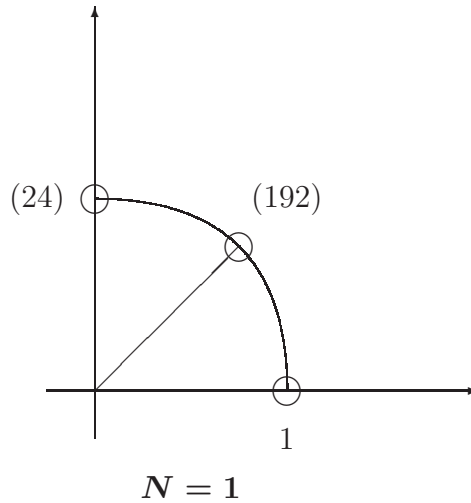
The irreducible vectors of norm $N = 4$ correspond to the set $B_2 \times B_2$, from which one should delete the 192 vectors divisible by 2. This yields $\text{card } \Theta_4 = 576 - 192 = 384$ and

$$\frac{\text{card } \Theta_4}{\text{card } (R)} = \frac{384}{992} = \frac{12}{31} \sim 0.387.$$

Observe that all the vectors in Θ_4 are internal. □

The 3 aspects of the geometric construction of (R) are sketched on Figure 1 below. The 3 sketches in Figure 1 are diagonally symmetric. The numbers in $(.)$ indicate the number of corresponding vectors.

The construction of the *external* vectors is straightforward. The *internal* vectors are constructed by *three* different mechanisms described below.



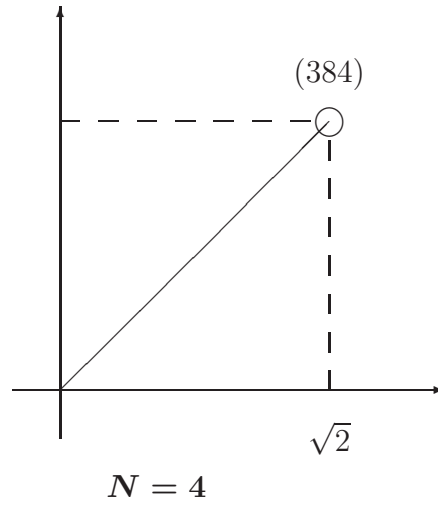
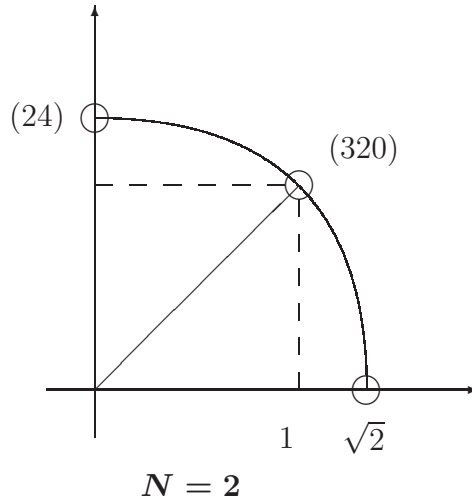


Figure 1. Construction of (R) , $\|\cdot\| = \sqrt{N}$.

1. Case $N = 2$ corresponds to the simplest mechanism: it consists of a complex addition of unit vectors in H^\times .
2. Case $N = 4$ consists of a complex addition of two vectors of norm 2 in H (euclidean norm $\sqrt{2}$), followed by the deletion of the resulting

vectors which are divisible by 2 in D .

3. Case $N = 1$ gathers the reducible vectors previously deleted.

Altogether, the root vectors in $(R) = L \cup \Delta$ can be classified into 7 different classes: 3 classes for each of $N = 1$ and 2, and 1 class for $N = 4$, see Figure 2 in Section 4.3.

Definition 3.3. *The root screen is the set M in D defined as the rational multiples of the root vectors in (R) :*

$$M = \{\gamma = ng_* \text{ for } n \in \mathbb{N}^* \text{ and } g_* \in (R)\}.$$

The set (R) is unevenly divided into 96 vectors in $L \subset D_p$ and 896 vectors in $\Delta \subset D_b$. It is invariant under the symmetry $g \mapsto -g$. The root screen belongs to a pencil of 496 lines passing through 0 and each g_* in (R) . The quantity $\|g_*\| = 1, \sqrt{2}$ or 2 defines the distance between 2 successive points in M on the same line. The complete screen is made of three independent screens, each one corresponding to a different resolution.

The partition $(R) = \Delta \cup L$ induces the partition $M = M_\Delta \cup M_L$ corresponding to 448 (resp. 48) lines defined by g_* in Δ (resp. L) for the root screen.

4. The three canonical fields of information

4.1. Preliminaries on isometries in $\mathbb{H} \sim \mathbb{R}^4$ and $\mathfrak{S}\mathbb{H} \sim \mathbb{R}^3$

Let

$$q = r \left(\cos \frac{\theta}{2} + u \sin \frac{\theta}{2} \right),$$

where u is a unit vector in $\mathfrak{S}\mathbb{H}$. For any $x \in \mathfrak{S}\mathbb{H}$, the map $x \mapsto q^{-1} \times x \times q = y$ defines the 3D-vector y rotated through the angle θ around the axis defined by u (or $\mathfrak{S}q$). Every element in SO_3 , the *special* orthogonal group of \mathbb{R}^3 , has this form and is a simple 3D-rotation [11, pp. 24 and 40]. Every element in GO_4 , the *general* orthogonal group of \mathbb{R}^4 , has the form $x \mapsto l \times x \times r$ where l and r are two unit quaternions [11, p. 41].

The following Lemma establishes an important result on arithmetic versions in H of these maps.

Lemma 4.1. *For (a, b) in Δ ,*

$$\tau = \frac{a \times b}{N(a)} \quad \text{and} \quad u_l = \frac{1}{N(a)} a \times e_l \times b$$

for $l = 1, 2, 3$ belong to H^\times : they are quaternionic units.

Proof.

- 1) When $(a, b) \in H^\times \times H^\times$, the result is clear since H^\times is a multiplicative group.
- 2) When $(a, b) \in B_2 \times B_2$, this can be checked by explicit calculation. For example,

$$\frac{1}{2}(1+i) \times i \times (1+i) = -1$$

and

$$\frac{1}{2}(1+i) \times i \times (1+k) = \frac{1}{2}(-1+i-j-k).$$

The choice $e_l = i$, $a, b \in \{1+i, i+j, j+k\}$ is generic.

By setting $b = \bar{a}$, we deduce that for any $a \in K$, (or b in K),

$$u_l = \frac{1}{N(a)} a \times e_l \times \bar{a} = \frac{1}{N(b)} \bar{b} \times e_l \times b$$

is a unit integer in H^\times , for $l = 1, 2, 3$. □

We consider the rotation ρ_b in $\mathfrak{S}\mathbb{H}$ defined by $b \in K$, that is

$$\rho_b : x \longmapsto b^{-1} \times x \times b = \frac{1}{N(b)} \bar{b} \times x \times b.$$

It is a rotation around $\mathfrak{S}b$ through the angle β , where $\frac{\beta}{2} = \angle(1, b)$ is the angle (mod 2π) formed by the real axis and b .

Proposition 4.2. *For any b in K , the rotation $\rho_b : x \longmapsto b^{-1} \times x \times b$, $x \in \mathfrak{S}\mathbb{H}$, around $\mathfrak{S}b$ is through one of the 6 angles $0, \pm\frac{\pi}{2}, \pm\frac{2\pi}{3}, \pi$.*

Proof. By definition $\cos \frac{\beta}{2} = \langle 1, b \rangle \frac{1}{\|b\|}$. For b in *i*) B_1 , *ii*) B_2 , *iii*) B_4 the corresponding values of $\cos \frac{\beta}{2}$ are *i*) 0 or ± 1 , *ii*) 0 or $\pm \frac{1}{\sqrt{2}}$, *iii*) $\pm \frac{1}{2}$. Therefore $\frac{\beta}{2}$ can take any of the 8 values $0, \pi, \frac{\pi}{4}, \frac{3\pi}{4}, \frac{\pi}{3}, \frac{2\pi}{3}, \pm \frac{\pi}{2}$. This yields the 6 possible values for β listed above, which belong to $[0, 2\pi[$. We mention for future reference that, when $\frac{\beta}{2}$ is defined mod 2π , then β is defined mod 4π . Therefore caution is required when one identifies 0 and 2π , as well as π and $-\pi$. \square

4.2. The three pairs (f_1, f_2) , (f_2, f_3) , and (f_3, f_1)

Let (λ, μ, ν) be a cyclic permutation of $(1, 2, 3)$. The vector

$$\varphi_\lambda(\gamma) = f_\lambda \times (f_\mu \times \gamma)$$

is expressed as $g_\nu \times \gamma$, with $g_\nu = \varphi_\lambda(\gamma) \times \gamma^{-1}$, for any $\gamma \neq 0$. Since $f_\lambda \times f_\mu = f_\nu$, we can write

$$[f_\lambda, f_\mu, \gamma] = (f_\nu - g_\nu) \times \gamma = G_\lambda \times \gamma$$

where the map $\gamma \neq 0 \mapsto G_\lambda = f_\nu - g_\nu$ is the field of information associated with (f_λ, f_μ) .

Definition 4.1. *The map:*

$$\gamma \in \mathbb{G} \setminus \{0\} \mapsto G = (G_\lambda, \lambda = 1, 2, 3) \in \mathbb{G}^3$$

is the field of 3D-canonical information, related to the 3 circular permutations of f_1, f_2, f_3 .

A real vector γ yields $G = 0$. We consider the question (Q):

Characterize the vectors $\gamma = (x, y) \neq 0$ in D such that the field $\gamma \mapsto G \in \mathbb{G}^3$ has only integral values in D^3 ?

Lemma 4.3. *If $g_\nu \in D$ then either γ is arbitrary in D_p or γ belongs to a subset of D_b .*

Proof [9, p. 128]. We use $e_\lambda \times e_\mu = -e_\mu \times e_\lambda = e_\nu$. Let $\gamma = (x, y)$ be given in D .

$$f_\lambda \times (f_\mu \times \gamma) = (e_\nu \times x, -y \times e_\nu) = g_\nu \times \gamma.$$

Therefore

$$g_\nu = \left(\frac{N(x) - N(y)}{N(x) + N(y)} e_\nu, \frac{-2}{N(x) + N(y)} y \times e_\nu \times x \right).$$

If $g_\nu \in D$, then the coefficient

$$\frac{N(x) - N(y)}{N(x) + N(y)}$$

is a rational number $\pm n$, or twice this coefficient is a rational number. The second case is excluded by Proposition 2.2. Hence

$$N(x) - N(y) = n (N(x) + N(y)),$$

$n \in \mathbb{Z}$, that is

$$(n - 1) N(x) + (n + 1) N(y) = 0,$$

or equivalently either $n = 0$ and $N(x) = N(y)$, or $n = \pm 1$ and $N(x)N(y) = 0$. This amounts to $\gamma \neq 0$ in D_p or D_b , with:

- $\gamma \neq 0$ in $D_p \iff g_\nu = (\eta e_\nu, 0)$ with $\eta = 1$ when $\gamma = (x, 0)$ and $\eta = -1$ when $\gamma = (0, y)$,
- $\gamma \neq 0$ in $D_b \implies g_\nu = (0, u_\nu)$ with $u_\nu = -\frac{1}{N(x)} y \times e_\nu \times x$.

We observe that for γ in D_p the vector $g_\nu = \eta f_\nu$ in D does not depend on γ . By comparison, for γ in D_b , g_ν is defined by the isometry

$$e_\nu \longmapsto u_\nu = -\frac{1}{N(x)} y \times e_\nu \times x$$

in \mathbb{R}^4 determined by $\gamma = (x, y)$, $N(x) = N(y) > 0$. Such a g_ν is in D iff u_ν is in H . \square

Theorem 4.4. *Let $\gamma \in D_b$. The following characterisation holds for $\nu = 1, 2, 3$:*

$$g_\nu \in D \text{ iff } \gamma \in M_\Delta \subset D_b.$$

Proof. As we know, $g_\nu = (0, u_\nu) \in D$ iff $u_\nu \in H$, that is, $u_\nu \in H^\times$ since $N(u_\nu) = 1$.

1. We assume that $u_\nu \in H^\times$. We check that the triple product $\tau = -u_\lambda \times \bar{u}_\mu \times u_\nu \in H^\times$ is invariant under an arbitrary cyclic permutation (λ, μ, ν) of $(1, 2, 3)$ with the common value $\tau = \frac{1}{N(x)} y \times x \in H^\times$. Hence $y = \tau \times \bar{x}$. Consider the orthogonal map

$$e_\nu \longmapsto u_\nu = -\tau \times \left(\frac{1}{N(x)} \bar{x} \times e_\nu \times x \right) = -\tau \times \rho_x(e_\nu).$$

It is the product of the rotation around the axis $\Im x$:

$$\rho_x : e_\nu \longmapsto \frac{1}{N(x)} \bar{x} \times e_\nu \times x$$

of e_ν in $\Im\mathbb{H}$, by a left multiplication by $-\tau$. The argument in [9, pp. 129–130] applies to conclude that necessarily $\gamma \in M_\Delta$. It uses a result of Hurwitz ([8], Vorlesung 5). It shows in particular that for $\nu = 1, 2, 3$:

$$\rho_x(e_\nu) = \epsilon_\nu e_{\pi(\nu)},$$

where π is a permutation of $(1, 2, 3)$, and where $\epsilon_\nu = \pm 1$ such that $\epsilon_1 \epsilon_2 \epsilon_3 = 1$.

2. The reciprocal: $\gamma \in M_\Delta \implies u_\nu \in H^\times$ follows from Lemma 4.1. \square

For $\lambda = 1, 2, 3$ we consider $G_\lambda = [f_\lambda, f_\mu, \gamma] \times \gamma^{-1}$ for $\gamma \in M_\Delta \cup D_p$.

For $\gamma \in D_p$, it is useful to distinguish between γ **down** iff $\gamma = (x, 0)$ and γ **up** iff $\gamma = (0, y)$.

Proposition 4.5.

1. For any γ in M_Δ , $G_\lambda = (e_\nu, \tau \times \rho_x(e_\nu)) \in D$ and $N(G_\lambda) = 2$, $N(\gamma) = n^2 N$, $N = 1, 2, 4$.
2. For any γ in D_p , $G_\lambda = (1 - \eta)f_\nu \in D$ and $N(G_\lambda) = 0$ or 4 , $N(\gamma) = M \in \mathbb{N}^*$.

Proof. Clear. $\eta = 1$ (resp. -1) for γ down (resp. up) in D_p . \square

It follows immediately that $N([f_\lambda, f_\nu, \gamma]) = N(G_\lambda)N(\gamma)$ can take the values:

- $2Nn^2$ for $N = 1, 2, 4$ when $\gamma \in M_\Delta$ or
- 0 (resp. $4M$ for $M \in \mathbb{N}^*$) when $\gamma \in D_p$ is down (resp. up).

4.3. The Mahler screen

Definition 4.2. *The Mahler screen \mathcal{M} is the subset of D defined as*

$$\mathcal{M} = M_{\Delta} \cup D_p.$$

It is clear that $G \in D^3$ iff $\gamma \in \mathcal{M}$: the Mahler screen carries the exact answer to (Q): it defines the points in D where G_1, G_2 and G_3 are all integral in D .

The Mahler screen is an *external augmentation* of the root screen M : M_L is augmented into D_p . Therefore \mathcal{M} has a countable basis externally, as well as a finite basis Δ internally.

We saw in Figure 1 that the construction of g_* in $(R) \subset \mathbb{G}$, is related to the direct sum representation of \mathbb{G} as “complex quaternions”

$$A_3 = \mathbb{G} = \mathbb{H}_l \oplus \mathbb{H}_r = \mathbb{H} \oplus \mathbb{H} \times \tilde{\mathbb{I}}$$

which is at work to define multiplication in \mathbb{G} from multiplication in \mathbb{H} , and where octonions are interpreted as “complex” quaternions. The seven possibilities for the structure of g_* are summarized in Figure 2 according to the euclidean norm $\|g_*\| = \sqrt{N}$. The three points on the unit circle correspond to D^\times .

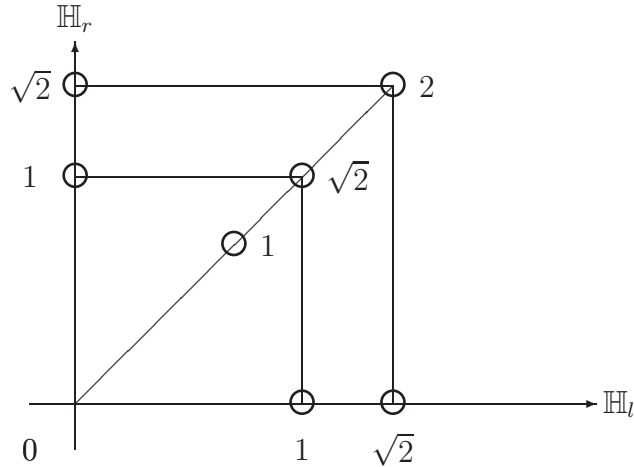


Figure 2. *Seven possibilities for g_* , $\|g_*\| = 1, \sqrt{2}, 2$*

The complex addition which takes place in (R) is materialised on Figure 2 by the horizontal and vertical lines which connect 1 to $\sqrt{2}$ and $\sqrt{2}$ to 2. Such an addition cannot be realised in D^\times . This sheds an additional light on the specificity of D^\times in (R) and D .

4.4. Future directions

In this report we have considered three particular instances of the canonical field of information. In full generality, there is an (antisymmetric) array of $8 \times 8 = 64$ instances to be considered, corresponding to the 64 pairs (f_λ, f_μ) , $\lambda, \mu = 0$ to 7. We leave this question for future work.

The alert reader may have noticed that the sets L and M_L have played no role in this 3D-analysis. Let us say, as a sneak preview, that they play a role when the 3 canonical vectors f_5 to f_7 are considered. This was also discovered by Mahler [9] in 1942.

The present report is meant to call attention on the neglected works of Dickson and Mahler in 8D-arithmetic. It may serve as a modern introduction

to the subject. But it cannot do justice to the wealth of material found in [9].

5. Epistemological remarks

5.1. $N = 1$: unification by arithmetic multiplicative closure

The subset of unit vectors $D^\times \subset (R)$ characterises the generators for all ideals in D as was proved by Lamont [12]. This is a powerful property: an ideal is invariant under any number of successive (left or right) multiplications by arbitrary elements in D . By comparison, when $N = 2$ or 4 , the Mahlerian analysis of the flow of information concerns only *two* successive multiplications by very *particular* pairs of vectors in D .

Comparing the structure of an ideal in R_2 and R_3 shows clearly how the alternativity of \times has drastically reduced the geometric freedom for the generator γ in R_3 . For $S \subset R_2$ the generator can be an arbitrary $q \in R_2$, leading to the integer

$$m = N(q) = q\bar{q}$$

which can be expressed as a sum of at most 4 squares, different from each other in general. For $S \subset R_3$ on the other hand, there is a *finite* number of possibilities for g_* , with $N(g_*) = 1$ and $N(\gamma) = n^2$, a *unique* square. And g_* describes the *finite* set D^\times in D .

To sum up, going from 4 to 8 dimensions for hypercomplex arithmetic has **reduced** — somewhat unexpectedly — the geometric (resp. arithmetic) complexity of ideals from denumerably to finitely generated (resp. from normed by an arbitrary integer equal to the sum of up to 4 squares, to normed by 1 perfect square).

Even though this remarkable unification in 8D appears as the result of a multiplicative closure, one should bear in mind that the internal units of D^\times are the result of a complex addition followed by a selection of the reducible vectors (Section 3.3).

5.2. Norms as 1, 2 or 4 squares

The restriction of the root screen to the densest screen $\{ng_*, g_* \in D^\times, n \in \mathbb{Z}^*\}$ amounts to fixing $N = 1$ instead of letting N belong to the triple $(1, 2, 4)$.

This reduction in choice has the spectacular consequence of opening the possibility of *arbitrary* multiplication in D , while keeping the norm n^2 invariant.

This greater freedom for multiplication is gained at the expense of the information given by the associator at the screen points which are ignored ($N = 2, 4$).

This difference between $N = 1$ and $N \in \{1, 2, 4\}$ should not be underestimated from an epistemological point of view. When Nature does arithmetic in 8D, geometry (group theory) and algebra (closure by \times) tell us that it delivers only *one* kind of classical 1D-numbers: the natural integers \mathbb{N}^* . Whereas, as we are told by Mahler, the information from D can be delivered in \mathbb{R} as *three* kinds of real numbers: all integers \mathbb{N}^* , the even integers $2\mathbb{N}^*$, or all integers times $\sqrt{2}$, that is $\sqrt{2}\mathbb{N}^*$.

Remark 5.1. The notion of geometry referred to above is the modern notion of *algebraic geometry*, where the concept of group is central.

It is clear that classical geometry uses irrational numbers such as π , or $\sqrt{2}$. Plato's celebrated dialogue between Socrates and Meno's slave testifies to this. Socrates asks the young man to construct a square of area 2 from a unit square of area 1. He says: "If you cannot compute it, show it to me!" In this case, computation is restricted to integers, and plane geometry serves to establish the existence of $\sqrt{2}$.

In the 8D-ring of integral octonions, the fact that \times is *not* associative creates *new* computational opportunities, which may lead to a partial unification/discrimination.

It is natural to look at the associator which is not trivial anymore in \mathbb{G} . With Mahler as our guide, we have explored the opportunity opened by the conditional computability in D of specific associators, leading to 3 canonical fields of information.

The set of units g_* in D^\times can be extended to the finite set of root vectors of norm $N = 1, 2$ or 4 , from which are defined the root and Mahler screens. The *internal* vectors $\gamma \in M_\Delta$ for M and \mathcal{M} have a norm

$$m = N(\gamma) = Nn^2, \quad N = 1, 2, 4, \quad n \in \mathbb{Z}.$$

m is the sum of 1, 2 or 4 **identical** squares. The 3 possibilities for m are sketched in Figure 3.

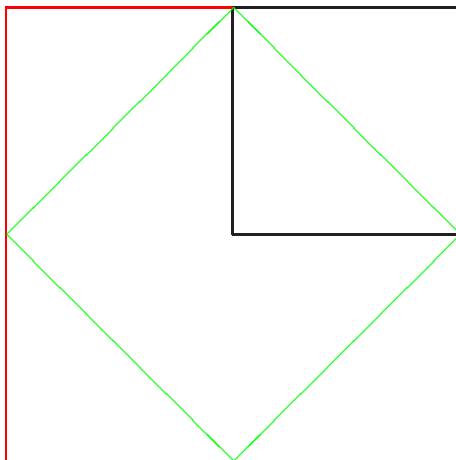


Figure 3. $m = N n^2$, $N = 1, 2, 4$

The black line corresponds to $N = 1$, green to $N = 2$, and red to $N = 4$.

We remark that, whereas Lagrange's theorem allows for 3 squares, in 8D-arithmetic no *three* identical squares are possible to represent $m = N(\gamma)$. By comparison, the external vectors $\gamma \in D_p \subset \mathcal{M}$ have a norm which is an arbitrary integer m in \mathbb{N}^* .

6. Conclusion

We have introduced this report by asking two questions which can be answered now as follows. The possibility of a nonassociative multiplication with a multiplicative norm in 8 dimensions induces a great reduction in the variety of possible ideals which are all principal and two-sided, that are finitely generated with a norm which is a perfect square. By considering the integral computability of information, one can create a companion reduction for the theorem of at most 4 squares: it becomes a theorem of 1, 2 or 4 identical squares for a subset of \mathbb{N}^* .

In an algebra A_k of dimension 2^k , $k \geq 4$, it is still possible to define a ring R_k of hypercomplex integers. However multiplication is not norm multiplicative anymore. This ruins the hope of using a euclidean division algorithm for $k \geq 4$. We leave for a future report the investigation of the role of zerodivisors in the definition of information.

Let us ponder now on the still elusive role of the octonions A_3 for our

understanding of the flow of information in the world. It has been shown by physicists [2] that the remarkable periodicity 8 found by Cartan (1908) for Clifford (associative) algebras, and by Bott (1957) for homotopy groups can be, in some sense, “explained” by octonions. Moreover, the normalized zerodivisors in A_4 form a real algebraic variety in a 14-dimensional subspace, that is homeomorphic to the group of automorphisms in A_3 (F. R. Cohen, 1992; Khalil and Yiu, 1997; Moreno, 1998). This group is itself isomorphic to the G_2 Lie group (Cartan, 1914). Even though physicists have not yet found a convincing proof that the octonions are useful to describe physical reality [2], they offer many hints pointing in this direction [10].

These hints become more compelling when we follow Mahler’s steps beyond ideals in the ring of integral octonions. The notion of ideal is replaced by the concept of three screens based on root vectors in D , each with a different resolution, namely 1, $\sqrt{2}$, and 2. Closure by multiplication imposes the resolution 1. But computing information in D requires all three resolutions. Even more convincing is the fact that the field of information is non trivial only in algebras of dimension ≥ 8 .

Should our attitude to physical reality be modified in view of these ideas? The answer could be yes, if we believe that the image of the physical reality that each of us perceives differently is produced in our minds by computation in Dickson algebras.

References

- [1] D. Allcock (1999), *Ideals in the integral octaves*. J. Alg. **220**, 396–400.
- [2] J. Baez (2001), *The octonions*. Bull. AMS **39**, 145-205.
- [3] A. Blanchard (1972), **Les corps non commutatifs**. PUF, Paris.
- [4] F. Chaitin-Chatelin (2003), *Elements of hypercomputation on \mathbb{R} and \mathbb{Z}_2 with the Dickson – Albert inductive process*. Cerfacs Technical Report TR/PA/03/34.
- [5] L. E. Dickson (1923), *A new simple theory of hypercomplex integers*. J. de Math. Pures et Appl. **2**, 281-326.
- [6] H. D. Ebbinghaus et al. (1998), **Les Nombres**. Vuibert, Paris.

- [7] G. H. Hardy and E. M. Wright (1979), **An Introduction to the Theory of Numbers, fifth edition.** Oxford Science Publ., Clarendon Press, Oxford.
- [8] A. Hurwitz (1919), **Vorlesungen über die Zahlentheorie der Quaternionen.** Julius Springer, Berlin.
- [9] K. Mahler (1942), *On ideals in the Cayley – Dickson algebra.* Proc. Royal Irish Acad. **48**, 123-133.
- [10] I. Stewart (2002), *The missing link.* New Scientist **2368**, 9 November 2002, pp. 30-33.
- [11] J. H. Conway and D. A. Smith (2003), **On Quaternions and Octonions.** A. K. Peters, Natick.
- [12] P. J. C. Lamont (1963), *Ideals in Cayley’s algebra.* Indag. Math. **25**, pp. 394–400.

The Cerfacs reports are available from <http://aton.cerfacs.fr/algor/reports/>