



Ensembles de nombres

Taladris, Silk78, Seirios,
Telchar, Tigerfou, Médiat

Forum Futura-Science
6 septembre 2011

Réalisé en L^AT_EX

Table des matières

I	Introduction	3
I.1	Définitions algébriques générales	4
II	Hiérarchie algébrique	10
II.1	Proto-nombres	11
II.2	Entiers naturels \mathbb{N}^* et \mathbb{N}	13
II.3	Entiers relatifs \mathbb{Z}	16
II.4	Rationnels \mathbb{Q}	18
II.5	Nombres réels \mathbb{R}	20
II.6	Complexes \mathbb{C}	62
III	Variations sur la hiérarchie algébrique	66
III.1	Décimaux \mathbb{D}	66
III.2	Entiers de Gauss $\mathbb{Z}[i]$	68
III.3	Nombres entiers d'Eisenstein $\mathbb{Z}[j]$	72
III.4	Dyadiques \mathfrak{D}	74
III.5	Nombres constructibles \mathcal{C}	76
III.6	Entiers modulo p $\mathbb{Z}/p\mathbb{Z}$	78
III.7	Nombres p -adiques \mathbb{Z}_p , \mathbb{Q}_p et \mathbb{C}_p	82
III.8	Compactification des Entiers Naturels $\omega + 1, \overline{\mathbb{N}}, \mathbb{N}^*, \beta\mathbb{N}$	87
III.9	Droite réelle achevée $\overline{\mathbb{R}}$	92
III.10	Supernaturels \mathbb{SN}	94
IV	Méthodes de construction	96
IV.1	Multicomplexes \mathbb{MC}_n	96
IV.2	Multicomplexes \mathbb{C}_n	98
IV.3	Hypercomplexes	100
IV.4	Cayley-Dickson $\mathcal{CD}(\mathbb{A}, \lambda)$	102
IV.5	Algèbres de Clifford $\mathcal{Cl}_{p,q}(\mathbb{R})$ et $\mathcal{Cl}_n(\mathbb{C})$	106
IV.6	Tessarines \mathcal{T}	111
V	Infinitésimaux	115
V.1	Hyperréels ${}^*\mathbb{R}$	115
V.2	Surréels \mathbf{No}	120
V.3	Superréels \mathfrak{R} (David Tall)	125
V.4	Corps de Levi-Civita \mathcal{R}	128
VI	Théorie des ensembles ZF(C)	130
VI.1	Ordinaux Ord	130
VI.2	Cardinaux Card	135
VI.3	Ordinaux de Hessenberg \mathcal{H}	139
VI.4	Réels définissables, calculables	141
VII	Algèbres de dimension 2 sur \mathbb{R}	144
VII.1	Nombres Duaux \mathbb{D}_1	146
VII.2	Complexes fendus \mathbb{C}	148
VIII	Algèbres de dimension 4 sur \mathbb{R}	151
VIII.1	Quaternions \mathbb{H}	154
VIII.2	Quaternions de Hurwitz $\mathbb{H}(\mathbb{Z})$	158
VIII.3	Quaternions hyperboliques (Macfarlane) \mathbb{M}	162
VIII.4	Coquaternion \mathbb{H}	164
VIII.5	Bicomplexes \mathbb{C}_2	166

IX	Algèbres de dimension 8 sur \mathbb{R}	169
IX.1	Octonions \mathbb{O}	169
IX.2	Octonions Fendus \mathbb{O}	173
IX.3	BiQuaternions \mathbb{B}	176
IX.4	BiQuaternions de Clifford \mathbb{B}	179
IX.5	Quaternions duaux \mathbb{D}_4	182
X	Algèbres de dimension 32 sur \mathbb{R}	186
X.1	Trigintaduonions \mathbb{T}	186
XI	Algèbres de dimension 64 sur \mathbb{R} et au-delà	190
XI.1	Sexagintaquatronions \mathbb{X}	190

(Certains chapitres prévus ne sont pas encore disponibles)

I Introduction

« Dieu fit le nombre entier, le reste est l'oeuvre de l'Homme »
Léopold Kronecker (1823-1891)¹

Si l'origine empirique des nombres entiers naturels est incontestable, la volonté de perfectionner le raisonnement nécessite la formalisation du langage, et la clarification de ses fondements. C'est dans cette optique que les nombres entiers furent construits sur une axiomatique moderne².

Méthode axiomatique qui permet de nombreuses constructions abstraites de nombres très divers : nombres relatifs, décimaux, rationnels, réels, irrationnels, algébriques, transcendants, complexes, multicomplexes, hypercomplexes, quaternions, octonions, supernaturels, superréels, surréels... cette liste est elle-même surréelle, et n'est pourtant pas exhaustive!

Ce document est une tentative d'introduction aux ensembles de nombres dont cette liste encyclopédique n'est qu'une faible partie...

1. Cité dans Eric Temple Bell, *Men of Mathematics*, Simon and Schuster, New York, 1986, p. 527.

2. [The Axiomatic Method](#).

I.1 Définitions algébriques générales

Le but de ce chapitre est de fixer certaines définitions utilisées dans les chapitres ultérieurs. Le choix de la terminologie est arbitraire et varie d'un ouvrage à un autre.

I.1.1 Lois de composition internes et externes

Définition : Soit E un ensemble non vide. Une loi de composition interne (ou opération) sur E est une application $*$: $E \times E \rightarrow E$. En général, on note $x * y$ au lieu de $*(x, y)$. Un ensemble muni d'une opération est appelé magma (on trouve aussi les noms de monade et de groupoïde).

Propriétés usuelles des lois de composition internes :

Commutativité	$\forall (x, y) \in E^2 (x * y = y * x)$
Associativité	$\forall (x, y, z) \in E^3 (x * y) * z = x * (y * z)$
Régularité	$\forall (x, y, z) \in E^3 ((x * y = x * z) \wedge (y * x = z * x)) \Rightarrow y = z$
e est un élément neutre	$\forall x \in E (x * e = e * x = x)$
x' est le symétrique de x	e est l'élément neutre et $x' * x = x * x' = e$
a est un élément absorbant	$\forall x \in E (x * a = a * x = a)$
i est un élément idempotent	$i * i = i$

Remarques :

- Les notions de régularité, d'éléments neutre, d'élément symétrique et d'élément absorbant peuvent être précisées « à gauche » ou « à droite », mais ces distinctions ne sont pas pertinentes ici.
- Si x' est le symétrique de x pour la loi $*$, alors x est le symétrique de x' pour cette même loi $*$.
- Le symétrique pour une opération notée additivement est généralement appelé *opposé*.
- Le symétrique pour une opération notée multiplicativement est généralement appelé *inverse*.
- Dans le cas général le symétrique de x est noté x^{-1} .

Certaines propriétés sont moins connues, mais seront utiles par la suite.

Alternativité	$\forall (x, y) \in E^2 ((x * (x * y) = (x * x) * y) \wedge ((x * y) * y = x * (y * y)))$
Associativité des puissances	$\forall x \in E (x * (x * x) = (x * x) * x)$
Flexibilité	$\forall (x, y) \in E^2 (x * (y * x) = (x * y) * x)$
Permutativité	$\forall (x, y, z, t) \in E^4 (x * y) * (z * t) = (x * z) * (y * t)$
Neutroactivité	$\forall (x, y, z) \in E^3 ((x * (y * z)) * x = (x * y) * (z * x))$
Identité de Moufang	$\forall (x, y, z) \in E^3 (x * y) * (z * x) = x * (y * z) * x$

Remarques :

- Associativité \Rightarrow Alternativité \Rightarrow Flexibilité \Rightarrow Associativité des puissances.
- L'associativité des puissances permet de définir la notation x^n , et au delà la notion de polynôme.
- Associativité + Commutativité \Rightarrow Permutativité.
- Associativité \Rightarrow Neutroactivité.

Définition : Soit E et K deux ensembles non vides. Un loi de composition externe est une application \cdot : $K \times E \rightarrow E$. Là encore, on note usuellement $\lambda \cdot x$, voire λx au lieu de $\cdot(\lambda, x)$.

I.1.2 Structures algébriques avec une loi de composition interne

Soit $(E, *)$ un magma.

Définition : On dit que $(E, *)$ est un demi-groupe si $*$ est associative.

Définition : On dit que $(E, *)$ est un monoïde si $*$ est associative et possède un élément neutre.

Définition : On dit que $(E, *)$ est un semi-groupe si $*$ est associative, possède un élément neutre et est régulière.

Définition : On dit que $(E, *)$ est un groupe si $*$ est associative, possède un élément neutre et si tout élément admet un symétrique pour la loi $*$.

Si, de plus, $*$ est commutative, on parle de demi-groupe, de monoïde, de semi-groupe ou de groupe commutatif. Un groupe commutatif est aussi appelé groupe abélien.

Remarque : Soit $(E, *)$ un magma. Alors
 $(E, *)$ groupe $\Rightarrow (E, *)$ semi-groupe $\Rightarrow (E, *)$ monoïde $\Rightarrow (E, *)$ demi-groupe.

Définition : Soit $(E, *)$ et (F, \star) deux magmas. Un morphisme de magmas est une application $\phi : E \rightarrow F$ vérifiant

$$\forall (x, y) \in E^2, \phi(x * y) = \phi(x) \star \phi(y)$$

Si $(E, *)$ et (F, \star) sont deux groupes (resp. deux demi-groupes, deux monoïdes, deux semi-groupes), on parle plutôt de morphisme de groupes (resp. de morphisme de demi-groupes, de morphisme de monoïdes, de morphisme de semi-groupes) ce qui représente un abus de langage (très répandu) dans la mesure où les propriétés de la loi de composition interne n'interviennent pas dans la définition d'un morphisme.

Il existe de nombreuses autres structures, mais qui ne seront pas utiles ici (paragroupe, antigroupe, etc.)

Citons néanmoins :

Définition : On dit que $(E, *)$ est un quasigroupe si $(E, *)$ est un magma non vide vérifiant :

1. $\forall x \forall y \exists ! z (x * z = y)$
2. $\forall x \forall y \exists ! z (z * x = y)$

Un quasigroupe est régulier, mais l'inverse n'est pas certain.

Définition : On dit que $(E, *)$ est un quasigroupe unitaire (loop en anglais) si $(E, *)$ est un quasigroupe et $*$ possède un élément neutre.

Définition : On dit que $(E, *)$ est un quasigroupe de Moufang si $(E, *)$ est un quasigroupe unitaire et que $*$ vérifie en plus l'identité de Moufang.

I.1.3 Structures algébriques avec deux lois de composition interne

Un ensemble A muni de deux lois de composition interne est un anneau. Il est d'usage de noter les lois d'un anneau $+$ et \cdot ; de plus, s'ils existent, les éléments neutres de $+$ et de \cdot sont notés respectivement 0 et 1 (éventuellement 0_A et 1_A si on veut préciser l'anneau).

Propriétés usuelles avec deux lois de composition interne ($+$ et \cdot).

\cdot distributive sur $+$	$\forall (x, y, z) \in A^3 ((x + y) \cdot z = (x \cdot z) + (y \cdot z)) \wedge (z \cdot (x + y) = (z \cdot x) + (z \cdot y))$
x est un diviseur de 0	$\exists y \in E ((x \neq 0) \wedge (y \neq 0) \wedge (x \cdot y = 0))$
x est nilpotent	Pour un certain $n \ x^n = 0$

Dans la suite, $(A, +, \cdot)$ désigne un anneau.

Définition : On dit que $(A, +, \cdot)$ est un semi-anneau si :

- $(A, +)$ est un monoïde commutatif.
- \cdot est associative.
- \cdot est distributive par rapport à $+$.

Définition : On dit que $(A, +, \cdot)$ est un anneau si :

- $(A, +)$ est un groupe commutatif
- \cdot est associative
- \cdot est distributive par rapport à $+$.

Un anneau (ou un semi-anneau) dont la multiplication possède un élément neutre est appelé anneau (ou semi-anneau) unitaire. Si la multiplication est commutative, on parle d'anneau (ou de semi-anneau) commutatif.

Définition : On dit qu'un anneau sans diviseur de 0 est un anneau intègre.

Définition : On dit que $(A, +, \cdot)$ est un corps si $(A, +, \cdot)$ est un anneau unitaire tel que les éléments neutres 0 et 1 sont distincts, et tel que tout élément non nul (i.e tout élément différent de l'élément neutre 0) admet un symétrique. De manière équivalente, $(A, +, \cdot)$ est un corps si $(A, +)$ est un groupe abélien et si $(A \setminus \{0\}, \cdot)$ est un groupe.

Un corps dont la multiplication est commutative est appelé corps commutatif.

Définition : Soit $(A, +, \cdot)$ et $(B, +, \cdot)$ deux anneaux. Un morphisme d'anneaux (c'est à nouveau un abus de langage, morphisme d'annélides serait plus approprié) est une application $\phi : A \rightarrow B$ vérifiant

- $\forall (x, y) \in A^2 (\phi(x + y) = \phi(x) + \phi(y))$
- $\forall (x, y) \in A^2 (\phi(x \cdot y) = \phi(x) \cdot \phi(y))$

De plus, si A et B sont unitaires, on impose souvent la condition supplémentaire $\phi(1_A) = 1_B$.

Si $(A, +, \cdot)$ et $(B, +, \cdot)$ sont deux semi-anneaux (resp. deux corps), on parle plutôt (toujours pas abus de langage) de morphisme de semi-anneaux (resp. de morphisme de corps).

I.1.4 Modules et espaces vectoriels

Un ensemble E muni d'une loi interne et d'une loi externe est appelé moduloïde. On note usuellement $+$ la loi interne et \cdot la loi externe. L'élément neutre de $+$, s'il existe, se note généralement 0 (éventuellement, 0_E).

Dans la suite $(A, +, \cdot)$ est un anneau commutatif unitaire et $(E, +, \cdot)$ un moduloïde.

Définition : On dit que $(E, +, \cdot)$ est un A -module si $(E, +)$ est un groupe commutatif et si les conditions suivantes sont vérifiées :

- $\forall \lambda \in A \forall (x, y) \in E^2 ((\lambda \cdot (x + y)) = (\lambda \cdot x) + (\lambda \cdot y))$
- $\forall (\lambda, \mu) \in A^2 \forall x \in E ((\lambda + \mu) \cdot x = (\lambda \cdot x) + (\mu \cdot x))$
- $\forall (\lambda, \mu) \in A^2 \forall x \in E ((\lambda \cdot \mu) \cdot x = \lambda \cdot (\mu \cdot x))$
- $\forall x \in E (1_A \cdot x = x)$

Définition : On dit que $(E, +, \cdot)$ est un A -espace vectoriel si $(E, +, \cdot)$ est un A -module et $(A, +, \cdot)$ est un corps.

I.1.5 Treillis et algèbres de Boole

Soit (A, \wedge, \vee) un annélide.

Définition : On dit (A, \wedge, \vee) est un treillis si les lois \vee et \wedge sont commutatives et associatives et vérifient aussi les lois d'absorption :

$$\forall (a, b) \in A^2 (a \vee (a \wedge b) = a \wedge (a \vee b) = a)$$

De plus, le treillis est distributif si \vee est distributif par rapport à \wedge ³. Il est borné s'il existe un élément absorbant, 0, pour la loi \wedge et un élément absorbant, 1, pour la loi \vee . Enfin, un treillis borné est complété si pour tout élément x , il existe y tel que $x \vee y = 1$ et $x \wedge y = 0$.

3. Ou si \wedge est distributif par rapport à \vee , ces deux propriétés étant équivalentes dans un treillis

Définition : Un treillis distributif, borné et complémenté est appelé algèbre de Boole.

Définition : Un treillis est dit complet si $\forall X \subset A$ ($\bigwedge X$ existe), ou, de façon équivalente, si $\forall X \subset A$ ($\bigvee X$ existe).

Définition : Soit (A, \wedge, \vee) un treillis, et $I \subset A$, I est un idéal de A si et seulement si :

$$\forall x \forall y ((x \in I) \wedge (y \in I)) \Rightarrow ((x \vee y) \in I).$$

$$\forall x \forall y ((x \in A) \wedge (y \in I)) \Rightarrow ((x \wedge y) \in I).$$

A noter que la définition de treillis peut être donné avec le langage des relations d'ordre (cf. infra), aussi il est courant de trouver le vocabulaire inf et sup en place de \wedge et \vee (respectivement).

Définition : On peut aussi définir la notion de demi-treillis, qui, comme son nom l'indique n'est muni que d'une seule des deux lois de composition qui composent un treillis, cette loi étant associative, commutative et idempotente, on notera \wedge -treillis et \vee -treillis selon que le demi-treillis est muni de l'opération inf ou sup.

Dans les demi-treillis, on peut définir une relation d'ordre : $(x \leq y) \Leftrightarrow (x \wedge y = x)$ ou $(x \leq y) \Leftrightarrow (x \vee y = y)$.

Bien que la définition habituelle de la distributivité nécessite deux lois de composition interne, on peut donner la définition de la distributivité dans un demi-treillis :

$$\forall x \forall y \forall z ((x \wedge y \leq z) \Rightarrow \exists x' \exists y' ((x \leq x') \wedge (y \leq y') \wedge (x' \wedge y' = z)))$$

ou

$$\forall x \forall y \forall z ((x \vee y \geq z) \Rightarrow \exists x' \exists y' ((x \geq x') \wedge (y \geq y') \wedge (x' \vee y' = z)))$$

I.1.6 Relations binaire sur un ensemble

Définition : Soit E un ensemble non vide. Une relation (binaire) R sur E est une partie de $E \times E$. On note xRy si $(x, y) \in R$.

Propriétés usuelles des relations binaires :

Réflexivité	$\forall x \in E, xRx$
Irréflexivité	$\forall x \in E, \neg(xRx)$
Transitivité	$\forall (x, y, z) \in E^3, ((xRy) \wedge (yRz)) \Rightarrow (xRz)$
Symétrie	$\forall (x, y) \in E^2, (xRy) \Rightarrow (yRx)$
Antisymétrie	$\forall (x, y) \in E^2, ((xRy) \wedge (yRx)) \Rightarrow (x = y)$
Totalité	$\forall (x, y) \in E^2, (xRy) \vee (yRx)$

Définition : On dit que (E, R) est une relation d'équivalence (ou que R est une relation d'équivalence sur E) si R est réflexive, transitive et symétrique.

Définition : On dit que (E, R) est une relation de pré-ordre si R est réflexive et transitive (donc un pré-ordre symétrique est une relation d'équivalence, et un pré-ordre antisymétrique est un ordre).

Soit E, \preceq un pré-ordre, alors la relation définie par $x \simeq y \Leftrightarrow ((x \preceq y) \wedge (y \preceq x))$ est une relation d'équivalence telle que l'ensemble quotient E / \simeq peut être naturellement muni d'une relation d'ordre \leq définie par $(\bar{x} \leq \bar{y}) \Leftrightarrow (x \preceq y)$ (il est aisé de vérifier que cette définition est cohérente, c'est à dire ne dépend des représentants de chaque classe).

Définition : On dit que (E, R) est une relation d'ordre strict si R est irréflexive et transitive (ce qui entraîne l'antisymétrie).

Définition : On dit que (E, R) est une relation d'ordre si R est réflexive, transitive et antisymétrique.

Définition : On dit que (E, R) est une relation d'ordre (resp. strict) total si R est une relation d'ordre (resp. strict) vérifiant l'axiome de totalité (resp. $\forall (x, y) \in E^2, (xRy) \vee (x = y) \vee (yRx)$).

Définition : On dit que (E, R) est une relation de bon ordre si R est une relation d'ordre telle que toute partie non vide de E admet un minimum.

Définition : Soit E un ensemble muni d'une relation d'équivalence \sim . Soit x un élément de E . L'ensemble $\bar{x} = \{y \in E \mid x \sim y\}$ est la classe d'équivalence de x dans E , on dit aussi que x est un représentant de \bar{x} . L'ensemble des classes d'équivalence est appelé ensemble quotient de E pour la relation \sim et se note E/\sim .

Soit (E, \preceq) un ensemble ordonné, c'est-à-dire que \preceq est une relation d'ordre sur E ; on définit une relation d'ordre strict \prec sur E par $x \prec y \Leftrightarrow (x \neq y) \wedge (x \preceq y)$.

De même, soit (E, \prec) un ensemble strictement ordonné, c'est-à-dire que \prec est une relation d'ordre strict sur E ; on définit une relation d'ordre \preceq sur E par $x \preceq y \Leftrightarrow (x = y) \vee (x \prec y)$.

Définition : Si A est une partie non vide de E , on dit que $M \in E$ majore A (resp. $m \in E$ minore A) si $\forall a \in A, a \preceq M$ (resp. $\forall a \in A, m \preceq a$), on dit aussi que M est un majorant (resp. m est un minorant) de A .

Définition : Si $a \in A$ on dit que a est un élément minimal, ou un minimum (resp. un élément maximal, ou maximum) de A s'il n'existe pas d'élément b de A tel que $b \prec a$ (tel que $a \prec b$).

Définition : S'il existe, un majorant (resp. minorant) qui est élément minimal (resp. élément maximal) de l'ensemble des majorants (resp. de l'ensemble des minorants) de A est appelé borne supérieure (resp. borne inférieure) de A .

Remarquons que si l'ordre \preceq est total, alors une partie A a au plus un minimum, un maximum, une borne inférieure et une borne supérieure; s'ils existent, on note respectivement $\min(A)$, $\max(A)$, $\inf(A)$ et $\sup(A)$ ces éléments.

Définition : Soit (E, \preceq) un ensemble ordonné, pour x et y dans E , et $A \subset E$, on note :

- $\uparrow x = \{y \mid x \preceq y\}$, l'ensemble des majorants de x , appelé section finissante.
- $\downarrow x = \{y \mid y \preceq x\}$, l'ensemble des minorants de x , appelé section commençante.
- A est appelé partie finissante si $\forall x \in E \forall y \in A ((y \preceq x) \Rightarrow (x \in A))$
- A est appelé partie commençante si $\forall x \in E \forall y \in A ((x \preceq y) \Rightarrow (x \in A))$

Soit (E, \preceq) est un ensemble ordonné tel que $\min(\{x, y\})$ et $\max(\{x, y\})$ soient définis pour tous x et y , en posant $x \wedge y = \min(\{x, y\})$ et $x \vee y = \max(\{x, y\})$, alors (E, \wedge, \vee) est un treillis.

Inversement, si (E, \wedge, \vee) est un treillis, on peut définir une relation d'ordre \preceq sur E par $x \preceq y \Leftrightarrow x \vee y = y$. Cette relation d'ordre est telle que $\min(\{x, y\})$ et $\max(\{x, y\})$ sont définis pour tous x et y dans E .

Le treillis (E, \preceq) est borné si et seulement si E admet un minimum et un maximum.

I.1.7 Idéal et Anneau quotient

Définitions : Idéaux

Soit $(A, +, \times)$ un anneau. On dit qu'une partie I de A est un idéal à gauche (resp. à droite) de A si :

- $(I, +)$ est un sous-groupe de $(A, +)$
- $\forall (x, a) \in I \times A (ax \in I)$ (resp. $xa \in I$)

On dit que I est un idéal bilatère de A si il est un idéal à gauche et à droite de A .

Théorème :

Soient $(A, +, \times)$ un anneau et I un idéal bilatère de A . La relation R définie par $\forall (x, y) \in A^2, xRy \Leftrightarrow (x-y) \in I$ est une relation d'équivalence sur A compatible avec les lois $+$ et \times .

Définition : Anneau quotient

Soient $(A, +, \times)$ un anneau, I un idéal bilatère de A et R la relation d'équivalence définie par $\forall (x, y) \in A^2, xRy \Leftrightarrow (x-y) \in I$. On appelle anneau quotient de A par I , et on note A/I , l'ensemble quotient de A par la relation d'équivalence R .

Définition : Lois de composition interne dans un anneau quotient

Soient $(A, +, \times)$ un anneau, I un idéal bilatère de A et R la relation d'équivalence définie par : $\forall (x, y) \in A^2, xRy \Leftrightarrow (x-y) \in I$.

Soient $(a, b) \in (A/I)^2$ et α et β des représentants de a et b , on définit les lois d'addition interne $\overline{+}$ et de multiplication interne $\overline{\times}$ sur A/I par : $a \overline{+} b = \overline{(\alpha + \beta)}$ et $a \overline{\times} b = \overline{(\alpha \times \beta)}$

Remarque : l'unicité d'une telle définition provient de la compatibilité de R avec les lois $+$ et \times et du fait que $y \in \overline{x} \Leftrightarrow \overline{x} = \overline{y}$.

Théorème :

Avec les notations de la définition précédente : $(A/I, \overline{+}, \overline{\times})$ est un anneau.

Remarque importante :

Les propriétés citées précédemment, à l'exception de celles concernant la loi \times , restent vrai pour un sous-groupe (noté additivement) G de A au lieu d'un idéal.

La relation R définie par $\forall(x, y) \in A^2(xRy \Leftrightarrow (x - y) \in G)$ est une relation d'équivalence sur A , compatible avec la loi $+$.

On définit alors l'ensemble quotient A/G , que l'on peut munir de la loi d'addition interne $\overline{+}$. $(G, \overline{+})$ a alors une structure de groupe.

Un exemple de groupe quotient est l'ensemble $\mathbb{R}/a\mathbb{Z}$ avec a un réel et $a\mathbb{Z}$ le sous-groupe additif de \mathbb{R} défini par $a\mathbb{Z} = \{ak \mid k \in \mathbb{Z}\}$. $\mathbb{R}/a\mathbb{Z}$ est isomorphe à tout segment de \mathbb{R} de la forme $[x, x + a[$ et donc notamment à $[0, a[$.

Les sous-ensembles $\mathbb{R}/2\pi\mathbb{Z}$ et $\mathbb{R}/\pi\mathbb{Z}$, confondus avec les segments $[0, 2\pi[$ et $[0, \pi[$, sont souvent utiles pour la résolution d'équations trigonométriques et la définition des fonctions trigonométriques inverses. Ainsi, l'équation $\cos(x) = y$ avec $y \in [-1, 1[$, admet une unique solution dans $\mathbb{R}/\pi\mathbb{Z}$.

I.1.8 Références

1. [Structure algébrique sur wikipedia](#)
2. J. Lafontaine, [Quelques informations sur l'origine de la terminologie](#), CNRS, 2011
3. P. Tauvel, *Algèbre Pour L'agrégation Interne*, Masson, 1996

II.1 Proto-nombres

II.1.1 Définition

On appelle proto-nombres les ensembles de la forme $1, 2, 3, \dots, n$, Beaucoup, c'est-à-dire un ensemble fini, ordonné, sur lequel deux opérations peuvent être définies, la table des opérations pour $n = 5$ est donnée ci-dessous, pour l'exemple.

Un ensemble de proto-nombres étant fini, l'application qui à n fait correspondre $n + 1$, finit toujours par tomber sur « Beaucoup », puis est stationnaire.

II.1.2 Table de multiplication

+	1	2	3	4	5	Beaucoup
1	2	3	4	5	Beaucoup	Beaucoup
2	3	4	5	Beaucoup	Beaucoup	Beaucoup
3	4	5	Beaucoup	Beaucoup	Beaucoup	Beaucoup
4	5	Beaucoup	Beaucoup	Beaucoup	Beaucoup	Beaucoup
5	Beaucoup	Beaucoup	Beaucoup	Beaucoup	Beaucoup	Beaucoup
Beaucoup	Beaucoup	Beaucoup	Beaucoup	Beaucoup	Beaucoup	Beaucoup

×	1	2	3	4	5	Beaucoup
1	1	2	3	4	5	Beaucoup
2	2	4	Beaucoup	Beaucoup	Beaucoup	Beaucoup
3	3	Beaucoup	Beaucoup	Beaucoup	Beaucoup	Beaucoup
4	4	Beaucoup	Beaucoup	Beaucoup	Beaucoup	Beaucoup
5	5	Beaucoup	Beaucoup	Beaucoup	Beaucoup	Beaucoup
Beaucoup	Beaucoup	Beaucoup	Beaucoup	Beaucoup	Beaucoup	Beaucoup

II.1.3 Propriétés algébriques

L'addition et la multiplication sont commutatives et associatives, mais non régulières, la multiplication possède un élément neutre (1); du point de vue algébrique $(P, +)$ est un demi-groupe commutatif, et (P, \times) est un monoïde commutatif.

La relation d'ordre naturelle est compatible avec les opérations.

II.1.4 Synonymes, Isomorphismes, Exemples

On peut ajouter 0 à un ensemble de proto-nombres, afin d'avoir un élément neutre pour l'addition.

II.1.5 Utilisation en physique

D'une certaine façon tout le monde utilise des proto-nombres (généralement avec 0). Ils s'en distinguent toutefois car le proto-nombre qui précède « Beaucoup » est rarement identifié, et c'est lui qui caractérise l'ensemble des proto-nombres. De plus, son choix dépend des circonstances et peut fortement varier.

Mais même quand nous utilisons des proto-nombres, cela n'efface pas notre connaissance des nombres entiers naturels, qui reste présente, ce qui fait que nous avons deux intuitions différentes et concomitantes dans notre appréhension des grands nombres.

Pour prendre un exemple simple, mais forcément personnel : pour mesurer les fortunes, même données sous formes de nombres par les journeaux, si je veux avoir une perception de ces montants, au-delà de 100 000 000 d'euros, je ne fais pas la différence tous ces nombres sont Beaucoup.

Je fais bien la différence entre 100 000 euros (qui me permettrait de faire quelques achats, de faire un beau voyage ...) et 1 000 000 (je peux arrêter de travailler et continuer à vivre comme aujourd'hui (et même mieux) avec les intérêts) et 10 000 000 (non seulement j'arrête de travailler mais ma vie va radicalement changer) mais au-delà je suis incapable de faire la différence (du point de vue de ce que cela changerait à ma vie), par exemple entre 100 000 000 et 17 000 000 000 (même si la différence comptable ne m'échappe pas).

Les enfants commencent la maîtrise de la notion de « nombre d'éléments » d'une collection sous la forme de proto-nombres (sans les opérations) :

Extrait du livre *Le comptage : vers la construction du nombre* Par Catherine Van Nieuwenhoven :

« Au départ les enfants peuvent compter des collections de deux ou trois objets correctement, mais pas des collections plus importantes.

Ce type de comptage a d'ailleurs été caractérisé par certains auteurs (Sophian, 1995) comme étant "1, 2, 3, beaucoup" suggérant que les grandes collections sont de manière indifférenciée considérées comme étant des "beaucoup". »

On retrouve aussi les proto-nombres dans certains langages : [Heiltsuk](#), [Guana](#) etc.

II.1.6 Références

1. INRP, 1, 2, beaucoup... passionnément!, Rencontres pédagogiques, cahier N° 21.
2. Children's numbers, Catherine Sophian, Brown & Benchmark Publishers (ISBN 0697131351)
3. [Le comptage : vers la construction du nombre](#)

II.2 Entiers naturels \mathbb{N}^* et \mathbb{N}

II.2.1 Introduction

Les nombres naturels ont une histoire vieille de près de douze mille ans. De la numération sumérienne à la numération indo-arabe que nous utilisons de nos jours, en passant par la numération mésopotamienne, maya, romaine, hébraïque, chinoise, etc., les nombres "naturels", indépendamment de la base de numération ou des symboles utilisés, sont profondément liés au besoin d'ordre, et de comptage, et sont des piliers de la connaissance mathématique.

Leur construction rigoureuse, grâce aux travaux de Grassman, de Dedekind et de Peano, fut une des premières étapes historiques de l'établissement des fondements - au sens moderne - des mathématiques.

II.2.2 Définition

L'ensemble des entiers naturels \mathbb{N} peut être défini comme un ensemble vérifiant les axiomes de Peano (formalisés ici, dans la logique du 2nd ordre, donc non soumis au théorème d'incomplétude de Gödel) :

- Il existe un entier naturel 0.
- Tout entier naturel n a un unique successeur, noté $s(n)$.
- Aucun entier naturel n'a 0 pour successeur.
- Deux entiers naturels ayant même successeur sont égaux.
- Si un ensemble d'entiers naturels contient 0 et contient le successeur de chacun de ses éléments, alors cet ensemble est égal à \mathbb{N} .

L'ensemble \mathbb{N}^* est l'ensemble des entiers naturels non nuls, i.e. $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$.

II.2.3 Mode de construction

Basiquement, les axiomes de Peano expriment le fait qu'intuitivement, \mathbb{N} est construit en commençant par 0 et les entiers successifs sont obtenus en "ajoutant 1" successivement. Les entiers naturels sont ainsi construits "par récurrence".

II.2.4 Table de multiplication

Le principe de récurrence usuel, découle directement de la construction précédente. On peut l'utiliser pour définir l'addition $+$ sur \mathbb{N} : soit n et p deux entiers naturels, alors on pose :

- $n + 0 = n$.
- $n + s(p) = s(n + p)$.

Par exemple, $n + 2$ désigne le successeur du successeur de n . On a donc

$$n + 2 = n + s(1) = s(n + 1) = s(n + s(0)) = s(s(n + 0)) = s(s(n)) = s^2(n)$$

On peut définir de manière analogue la multiplication \times : si n et p sont deux entiers naturels, alors on pose :

- $0 \times n = 0$.
- $s(p) \times n = (p \times n) + n$.

Enfin, on peut définir une relation d'ordre $<$ sur \mathbb{N} appelé "ordre usuel" en décrétant que $n \leq m$ si et seulement s'il existe $p \in \mathbb{N}$ tel que $m = n + p$.

L'ordre usuel est compatible avec l'addition et la multiplication. C'est un bon ordre.

II.2.5 Propriétés algébriques

Addition et multiplication sont définies, commutatives, associatives, la multiplication possède un élément neutre dans \mathbb{N}^* et l'addition en possède un dans \mathbb{N} (mais pas dans \mathbb{N}^*), la multiplication possède un élément absorbant sur \mathbb{N} (pas dans \mathbb{N}^*), l'addition est régulière sur \mathbb{N} et la multiplication est régulière sur \mathbb{N}^* . De plus la multiplication est distributive sur l'addition.

La soustraction et la division ne sont pas définies partout.

- $(\mathbb{N}^*, +)$ est un magma associatif, commutatif et régulier donc un demi-groupe régulier et commutatif.
- $(\mathbb{N}, +)$ est un magma associatif, unitaire, commutatif, régulier donc un semi-groupe commutatif.
- (\mathbb{N}^*, \cdot) est un magma associatif, unitaire, commutatif, régulier donc un semi-groupe commutatif.
- (\mathbb{N}, \cdot) est un magma associatif, unitaire, commutatif, non régulier donc un monoïde commutatif.
- $(\mathbb{N}, +, \cdot)$ est un demi-anneau commutatif.

Dans \mathbb{N} , certaines équations de la forme $x + a = b$, n'ont pas de solution ne serait-ce que $x + 1 = 0$ (sinon 0 serait successeur de x, ce qui est interdit par l'axiomatisation).

II.2.6 Synonymes, Isomorphismes, Exemples

Dans ZF, les seuls objets considérés sont les ensembles. L'idée de Von Neumann est de représenter chaque entier n par un ensemble ayant n éléments⁴. Ainsi, l'entier 0 est défini comme étant \emptyset et 1 doit être défini par un singleton. Le plus simple est de choisir $1 = \{\emptyset\} = \{0\}$. Ensuite, 2 doit être défini comme un ensemble à deux éléments, par exemple $2 = \{0, 1\}$. Et ainsi de suite... si n est défini, on définit⁵ $n + 1$ comme étant le successeur de n , c'est-à-dire l'ensemble $s(n) = n \cup \{n\}$. On peut ainsi définir tous les entiers que l'on souhaite, quitte à devoir y consacrer beaucoup de temps; cependant, en procédant de cette manière, on n'a pas défini l'ensemble de tous les entiers naturels, qui nécessite l'axiome de l'infini.

Pour cela, on définit un ensemble transitif comme étant un ensemble X tel que que si x est élément de X , alors son successeur $s(x) = x \cup \{x\}$ est aussi élément de X . A noter que l'axiome de l'infini est nécessaire pour affirmer l'existence d'un tel ensemble. D'après ce qui précède, un ensemble transitif contenant $0 = \emptyset$ contiendra en particulier tous les entiers de Von Neumann imaginables. Comme l'ensemble \mathbb{N} devrait être "l'ensemble de tous les entiers de Von Neumann imaginables", on le définit comme l'intersection de tous les ensembles transitifs contenant 0.

L'addition et la multiplication définies sur les entiers de Von Neumann sont l'addition et la multiplication usuelle des ordinaux.

Si les entiers naturels sont construits en utilisant les ensembles transitifs, on a $n \leq m$ si et seulement si $n = m$ ou $n \in m$.

On peut aussi définir l'ensemble des entiers naturels en passant par la théorie des catégories : \mathbb{N} est l'objet initial (unique à isomorphisme près) de la catégorie des diagrammes de Lawvere dont les objets sont les diagrammes de la forme $(1 \xrightarrow{0} N \xrightarrow{s} N)$, et les flèches φ entre $(1 \xrightarrow{0} X \xrightarrow{h} X)$ et $(1 \xrightarrow{0} Y \xrightarrow{k} Y)$ vérifient $\varphi \circ 0 = 0$ et $\varphi \circ h = k \circ \varphi$.

Autrement dit le diagramme suivant est commutatif :

$$\begin{array}{ccc} 1 & \xrightarrow{0} & X & \xrightarrow{h} & X \\ & & \downarrow \varphi & & \downarrow \varphi \\ 1 & \xrightarrow{0} & Y & \xrightarrow{k} & Y \end{array}$$

Une façon équivalente mais moins "catégorique" de dire les choses : On appelle entiers naturels, un triplet $(\mathbb{N}, 0, s)$ tel que :

- \mathbb{N} est un ensemble,
- 0 est un élément de \mathbb{N} (appelé zéro),

4. Ici, n désigne un entier naturel "intuitif"

5. La notation est abusive puisque l'addition n'a pas encore été définie.

- s est une application de \mathbb{N} vers \mathbb{N} (appelée successeur),
- Pour tout ensemble X , tout élément a de X , et toute application $h : X \mapsto X$, il existe une unique application $\varphi : \mathbb{N} \mapsto X$, telle que (pour tout $n \in \mathbb{N}$) : $\varphi(0) = a$; et $\varphi(s(n)) = h(\varphi(n))$.

II.2.7 Utilisation en physique

Il n'est pas nécessaire d'être physicien pour utiliser les entiers naturels, qui sont utilisés dans la plupart des activités intellectuelles.

II.2.8 Références

1. [Daniel PERRIN](#)
2. [Site expert des Ecoles Normales Supérieures](#)
3. [Alain Prouté](#)
4. [Stéphane Gonnord](#)
5. [Martial Leroy](#)

II.3 Entiers relatifs \mathbb{Z}

II.3.1 Introduction

Les nombres négatifs sont apparus avec le besoin de dénombrer non pas des quantités, mais des *différences de quantités*, avec les premiers banquiers et les calculs financiers. On dénombre dans ces situations la *différence* entre le débit et le crédit d'argent.

La soustraction était déjà connue des Egyptiens, et les nombres négatifs utilisés en Inde au VII^{ème} siècle, symbolisés par un point au dessus du nombre (le symbole moins actuel "−" est apparu beaucoup plus tard - au XVI^{ème} siècle - en Allemagne)⁶. Toujours est-il que de Diophante (III^{ème} siècle) à Nicolas Chuquet (XV^{ème} siècle), les solutions négatives d'une équation de type $x + b = a$ (avec b non nul) étaient considérées comme absurdes. Ce n'est qu'avec les travaux du XX^{ème} siècle sur les structures algébriques abstraites que leur rôle d'extension algébrique des nombres naturels fut établi.

II.3.2 Définition

Dans \mathbb{N} , certaines équations du type $x + b = a$ (avec b non nul) n'ont pas de solution. On construit l'ensemble \mathbb{Z} des entiers relatifs dans le but de pouvoir résoudre ce type d'équation. La lettre \mathbb{Z} provient du mot allemand Zahlen, qui signifie nombre.

L'addition $+$ et la multiplication \cdot définie sur \mathbb{N} font de cet ensemble un semi-anneau. L'ensemble \mathbb{Z} est défini comme le symétrisé de \mathbb{N} . La construction de $(\mathbb{Z}, +, \cdot)$ à partir de $(\mathbb{N}, +, \cdot)$ se généralise à tout semi-anneau $(A, +, \cdot)$.

II.3.3 Mode de construction

Les entiers relatifs peuvent se construire à partir des entiers naturels en munissant $\mathbb{N} \times \mathbb{N}$ d'une relation d'équivalence définie par $(a, b) \simeq (a', b') \Leftrightarrow a + b' = a' + b$. On notera $\overline{(a, b)}$ la classe d'équivalence de $(a, b) \in \mathbb{N} \times \mathbb{N}$ pour la relation \simeq . L'ensemble \mathbb{Z} est l'ensemble quotient $(\mathbb{N} \times \mathbb{N}) / \simeq$.

L'injection canonique $\pi : \mathbb{N} \rightarrow \mathbb{Z}$ définie par $\pi(n) = \overline{(n, 0)}$ permet d'identifier \mathbb{N} avec une partie de \mathbb{Z} .

On peut noter que $|\mathbb{N}| = |\mathbb{Z}| = \aleph_0$.

II.3.4 Table de multiplication

On peut définir une addition sur \mathbb{Z} de la manière suivante :

L'addition sur $(\mathbb{N} \times \mathbb{N})$ est définie par $(a, b) + (a', b') = (a + a', b + b')$. Cette addition est compatible avec la relation \simeq , c'est-à-dire que la propriété suivante est vérifiée :

$$\forall (a, b, a', b', c, d, c', d') \in \mathbb{N}^8, ((a, b) \simeq (a', b') \wedge (c, d) \simeq (c', d')) \Rightarrow ((a, b) + (c, d) \simeq (a', b') + (c', d'))$$

Par conséquent, on peut définir une addition $+$ sur \mathbb{Z} par $\overline{(a, b)} + \overline{(c, d)} = \overline{(a + b, c + d)}$. La compatibilité de l'addition sur $\mathbb{N} \times \mathbb{N}$ avec la relation \simeq implique que $+$ est bien définie, i.e ne dépend pas des choix des représentants de $\overline{(a, b)}$ et de $\overline{(c, d)}$.

La multiplication de \mathbb{Z} peut être définie de manière analogue. On définit une multiplication sur $(\mathbb{N} \times \mathbb{N})$ par $(a, b) \cdot (a', b') = (aa' + bb', a'b + ab')$.

Là encore, la multiplication est compatible avec la relation d'équivalence \simeq . Par conséquent, elle "passe au quotient" et permet de définir la multiplication sur \mathbb{Z} par

$$\overline{(a, b)} \cdot \overline{(a', b')} = \overline{(a, b) \cdot (a', b')}$$

L'injection canonique $\pi : \mathbb{N} \mapsto \mathbb{Z}$ définie par $\pi(n) = \overline{(n, 0)}$, qui permet d'identifier \mathbb{N} à son image par π est un morphisme de semi-anneaux.

6. F.Cajori, *A history of mathematical notations*, Vol I, 1929, §106-109 et §200-201.

II.3.5 Conjugué, module, norme, forme polaire et inverse

Pour tout élément k de \mathbb{Z} , il existe un unique entier naturel n tel que $k = \overline{(n, 0)}$ ou $k = \overline{(0, n)}$. L'entier n est la valeur absolue de k et se note $|k|$. De plus, l'opposé de $\overline{(n, 0)}$ (i.e son symétrique pour la loi $+$) est $\overline{(0, n)}$. Ainsi, on a construit \mathbb{Z} à partir de \mathbb{N} en rajoutant tous les symétriques des éléments de \mathbb{N} pour la loi $+$, et seulement ces symétriques. Cela justifie le terme de "symétrisé de \mathbb{N} " pour désigner \mathbb{Z} .

II.3.6 Propriétés algébriques

La relation d'ordre \leq sur \mathbb{Z} est définie par $\overline{(a, b)} \leq \overline{(a', b')}$ si et seulement si $a + b' \leq_{\mathbb{N}} a' + b$. (où $\leq_{\mathbb{N}}$ est la relation d'ordre sur \mathbb{N}). La relation est bien définie (i.e. ne dépend pas du choix des représentants de $\overline{(a, b)}$ et de $\overline{(a', b')}$). De plus, cet ordre est total et prolonge l'ordre usuel de \mathbb{N} (c'est-à-dire que si m et n sont deux entiers naturels tels que $n \leq m$, alors $\pi(n) \leq \pi(m)$).

$(\mathbb{Z}, +, \cdot)$ est un anneau commutatif ordonné (l'ordre est compatible avec l'addition et avec la multiplication par un entier strictement positif). C'est un anneau euclidien relativement à la valeur absolue. Par conséquent, c'est un anneau intègre, principal et factoriel.

Dans $(\mathbb{Z}, +)$, toutes les équations de la forme $x + a = b$ ont une unique solution, mais les équations de la forme $a \cdot x = b$ n'ont pas toujours de solution, même si on impose a différent de 0. Par exemple, $2 \cdot x = 1$ n'a pas de solution dans \mathbb{Z} . Néanmoins, la multiplication est régulière sur \mathbb{Z}^* .

II.3.7 Synonymes, Isomorphismes, Exemples

En anglais, le mot *integer* désigne un entier relatif alors que sa traduction en français, *entiers*, désigne plutôt un entier naturel.

II.3.8 Utilisation en physique

Comme pour les entiers naturels, il n'est pas nécessaire d'être physicien pour utiliser les entiers relatifs, même si, conceptuellement, les nombres négatifs sont moins "naturels" que les "entiers naturels".

II.3.9 Références

1. Patrice Tauvel, *Algèbre Pour L'agrégation Interne*, Masson, 1996.

II.4 Rationnels \mathbb{Q}

II.4.1 Introduction

La construction de \mathbb{Q} ressemble à celle de \mathbb{Z} par beaucoup d'aspects. Dans \mathbb{Z} , certaines équations du type $a \cdot x = b$ n'ont pas de solution. On construit \mathbb{Q} pour que de telles équations aient toujours une solution (unique), si a est non nul.

II.4.2 Définition

L'ensemble des nombres rationnels \mathbb{Q} est le corps des fractions de l'anneau des entiers naturels \mathbb{Z} , c'est-à-dire le plus petit corps contenant \mathbb{Z} . La construction de \mathbb{Q} à partir de \mathbb{Z} se généralise à tout anneau commutatif unitaire intègre.

II.4.3 Mode de construction

Les nombres rationnels peuvent se construire à partir des entiers relatifs naturels en munissant $\mathbb{Z} \times \mathbb{Z}^*$ d'une relation d'équivalence \simeq puis en construisant une addition et une multiplication compatible avec cette relation.

Sur $\mathbb{Z} \times \mathbb{Z}^*$, on définit une relation d'équivalence \simeq par $(a, b) \simeq (a', b') \Leftrightarrow a \cdot b' = a' \cdot b$. La classe d'équivalence d'un élément (a, b) de $\mathbb{Z} \times \mathbb{Z}^*$ se note usuellement $\overline{(a, b)} = \frac{a}{b}$.

II.4.4 Table de multiplication

On peut définir une addition sur \mathbb{Q} de la manière suivante :

L'addition sur $\mathbb{Z} \times \mathbb{Z}^*$ est définie par $(a, b) + (a', b') = (a \cdot b' + a' \cdot b, b \cdot b')$. Cette addition est compatible avec la relation \simeq , c'est-à-dire que la propriété suivante est vérifiée :

$$\forall a, b, a', b', c, d, c', d' \in \mathbb{N}^{\neq 0}, (a, b) \simeq (a', b') \text{ et } (c, d) \simeq (c', d') \Rightarrow (a, b) + (c, d) \simeq (a', b') + (c', d')$$

Par conséquent, on peut définir une addition $+$ sur \mathbb{Q} par

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

. La compatibilité de l'addition sur $\mathbb{Z} \times \mathbb{Z}^*$ avec la relation \simeq implique que $+$ est bien définie, i.e ne dépend pas des choix des représentants de $\frac{a}{b}$ et de $\frac{c}{d}$.

La multiplication de \mathbb{Q} peut être définie de manière analogue. On définit une multiplication sur $\mathbb{Z} \times \mathbb{Z}^*$ par $(a, b) \cdot (a', b') = (aa', bb')$.

Là encore, la multiplication est compatible avec la relation d'équivalence \simeq . Par conséquent, elle « passe au quotient » et permet de définir la multiplication sur \mathbb{Q} par

$$\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$$

L'application $\pi : \mathbb{Z} \times \mathbb{Z}^* \rightarrow \mathbb{Q}$ définie par $\pi(k) = \frac{k}{1}$ est un morphisme d'anneaux injectif. On identifie usuellement \mathbb{Z} à son image par π .

On peut remarquer que $(\frac{a}{b} = \frac{0}{1}) \Leftrightarrow (a = 0)$, ce qui avec l'identification $\pi(0)$ avec 0 peut aussi s'écrire $(\frac{a}{b} = 0) \Leftrightarrow (a = 0)$.

Il est alors immédiat que $(\frac{a}{b} \neq 0) \Rightarrow (\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1} = \pi(1) = 1)$.

Autrement dit, tout élément non nul de \mathbb{Q} possèdent un symétrique.

La relation d'ordre usuel sur \mathbb{Z} peut être prolongée sur \mathbb{Q} . Pour cela, il suffit de remarquer que toute fraction (c'est-à-dire tout élément de \mathbb{Q}) peut être représentée sous la forme $\frac{p}{q}$, où q est un entier naturel non nul. Si $\frac{a}{b}$ et $\frac{a'}{b'}$ sont deux fractions représentées sous cette forme, on définit $\frac{a}{b} \leq \frac{a'}{b'}$ si et seulement si $ab' \leq_{\mathbb{Z}} a'b$ (ici, $\leq_{\mathbb{Z}}$ désigne l'ordre usuel sur \mathbb{Z}). Là encore, cette définition ne dépend pas du choix des représentants. La relation \leq est totale et prolonge la relation d'ordre sur \mathbb{Z} .

Muni de cette ordre, \mathbb{Q} est un corps totalement ordonné. Il est de plus archimédien mais ne vérifie pas la propriété de la borne supérieure. Par exemple, l'ensemble $\{x \in \mathbb{Q} / x^2 < 2\}$, bien que non vide et majoré, n'admet pas de borne supérieure.

II.4.5 Conjugué, Module, Norme, Forme Polaire et Inverse

II.4.6 Propriétés algébriques

$(\mathbb{Q}, +, \cdot)$ est le plus petit corps commutatif de caractéristique 0. C'est-à-dire que tout corps commutatif de caractéristique 0 contient un sous-corps isomorphe à \mathbb{Q} .

$(\mathbb{Q}, +, \cdot, <)$ est un corps ordonné archimédien.

Dans $(\mathbb{Q}, +, \cdot)$, toutes les équations de la forme $x + a = b$ et toutes les équations de la forme $a \cdot x = b$, avec a différent de 0, ont une unique solution mais les équations de la forme $P(x) = 0$, où P est un polynôme en x n'ont pas toujours des solutions (ne serait-ce que $x^2 = 2$). Cela signifie que \mathbb{Q} n'est pas algébriquement clos.

L'ordre sur \mathbb{Q} , permet de munir \mathbb{Q} d'une topologie métrique en définissant la distance \lceil par $\lceil(x, y) = |x - y|$ pour laquelle l'addition et la multiplication sont continues, c'est à dire que $(\mathbb{Q}, +, \cdot, \lceil)$ est un corps topologique.

A noter que \mathbb{Q} peut aussi être munie d'une distance **p-adique**.

\mathbb{Q} est un ensemble dénombrable, comme le montre la bijection suivante :

$$\varphi : \mathbb{N} \mapsto \mathbb{Q} \begin{cases} \varphi(0) & = & 0 \\ \varphi(4n) & = & \frac{1}{\varphi(2n) + 1} \\ \varphi(4n + 1) & = & -(\varphi(2n) + 1) \\ \varphi(4n + 2) & = & \varphi(2n) + 1 \\ \varphi(4n + 3) & = & \frac{-1}{\varphi(2n + 2) + 1} \end{cases}$$

II.4.7 Utilisation en physique

Non seulement les physiciens, mais tout le monde utilise les nombres rationnels, que ce soit pour compter des pommes, des crédits, des débits, ou des parts de pizza.

II.4.8 Références

1. Patrice Tauvel, *Algèbre Pour L'agrégation Interne*, Masson, 1996.
2. [Lecture notes, California State University San Marcos](#)

II.5 Nombres réels \mathbb{R}

*L'ensemble des nombres réels est le pilier fiable de la famille,
le corps ordonné complet sur lequel nous comptons tous.*
John Baez⁷

II.5.1 Introduction

L'ensemble des nombres réels, noté \mathbb{R} , est un ensemble de nombres dont la perception est généralisée, en effet une définition informelle peut être utilisée très tôt auprès des collégiens, et aujourd'hui, tous les scientifiques, et pas seulement eux, utilisent les nombres réels, ou plus exactement **croient** utiliser les réels, en effet aucun instrument de mesure ne délivre un nombre réel.

La nécessité d'une définition claire des nombres réels s'est vraiment fait jour au XIX^{ème} siècle, quelques noms apparaissent sur ce sujet en une poignée d'années :

- Karl Theodor Wilhelm Weierstrass, un mathématicien allemand (1815 - 1897) enseigne, dès les années 1850, une construction des nombres réels dont Heine et Cantor s'inspireront.
- Julius Wilhelm Richard Dedekind, un mathématicien allemand (1831 - 1916) publie en 1872 « Continuité et nombres irrationnels », un ouvrage qui reprend ses travaux et conférences initiés en 1858 sur les coupures qui portent son nom aujourd'hui.
- Hugues Charles Robert Méray, un mathématicien français (1835 - 1911), propose la construction à partir des suites de Cauchy en 1869 dans un article baptisé : « Remarques sur la nature des quantités définies par la condition de servir de limites à des variables données. ».
- Eduard Heine, un mathématicien allemand (1821 - 1881) publie en 1872 un article « Les éléments de la théorie des fonctions » dans lequel il expose de façon très didactique la méthode des suites de Cauchy.
- Georg Ferdinand Ludwig Philip Cantor, un mathématicien allemand (1831 - 1916), publie en 1872 un article dans lequel il reprend les travaux de Heine de façon plus synthétique, la méthode par les suites de Cauchy est parfois appelé, *Méthode de Cantor*.

Un peu plus tard en 1899, David Hilbert, un mathématicien allemand (1862 - 1943) donna la première définition axiomatique des réels.

On peut aussi noter que l'accueil des nombres réels, même parmi les mathématiciens du XVIII^{ème} siècle n'a pas été immédiat :

$\sqrt{2}$ n'est point un nombre proprement dit, c'est une quantité qui n'existe point, qu'il est impossible de trouver⁸.

II.5.2 Définition

Il a déjà été noté que l'on sait additionner, multiplier et ordonner les nombres rationnels, on peut faire la même chose avec les longueurs mesurées sur une droite, et, grâce à un repère (le choix de 0 et de 1), on peut reporter tous les nombres rationnels (voir **les nombres Constructibles**), par contre on sait (depuis les mathématiciens grecs du V^{ème}, voire du VI^{ème} siècle AV J.C.) que certaines longueurs sont incommensurables (la diagonale d'un carré de longueur 1, par exemple), il y a donc « plus » de points sur une droite que de nombres dans \mathbb{Q} , d'où l'idée de boucher les trous⁹, de compléter \mathbb{Q} .

Les Nombres Réels comprennent donc les Nombres Rationnels et les Nombres Constructibles, mais on peut noter tout de suite que, parmi les Irrationnels, certains sont solutions d'une équation polynomiale à coefficients entiers (c'est le cas de $\sqrt{2}$, par exemple), ces nombres sont dits Algébriques ; attention néanmoins, l'ensemble des Nombres Algébriques n'est pas inclus dans \mathbb{R} , par exemple les solutions de l'équation $x^2 + 1 = 0$ ne sont pas réelles ; mais il existe aussi dans \mathbb{R} des nombres qui ne sont pas solutions d'équations polynomiales à coefficients entiers (c'est le cas de e ou de π , par exemple), ces nombres sont dits transcendants.

7. Cité par Valentin Ovsienko (Lyon 1) comme résumé d'une conférence sur les algèbres au Laboratoire Paul Painlevé. Voir aussi : les **Complexes**, les **Quaternions**, les **Octonions**.

8. d'Alembert, 1751.

9. Ce qui a donné naissance au problème de la puissance du continu.

II.5.3 Méthodes de construction

Il existe plusieurs méthodes pour construire les nombres réels à partir de l'ensemble des rationnels, des entiers ou par des méthodes purement axiomatiques.

Nous donnons ci-dessous un certain nombre de ces méthodes que nous avons regroupées selon des critères parfaitement arbitraires, il aurait, sans aucun doute, été plus objectif de regrouper ensemble toutes les méthodes utilisant, de façon plus ou moins explicite, les suites de Cauchy, mais cela aurait pu occulter les différences fondamentales qui existent néanmoins entre ces diverses méthodes (différences mathématiques et/ou différences pédagogiques).

- 1) **Constructions Usuelles.**
 - i) **Construction de Simon Stevin.**
 - ii) **Coupures de Dedekind.**
 - iii) **Suites de Cauchy.**
- 2) **Méthodes Axiomatiques.**
 - i) **Axiomatique Usuelle.**
 - ii) **Axiomatique de Tarski.**
- 3) **Suites Particulières.**
 - i) **Fractions Continues.**
 - ii) **Méthode Générale.**
 - iii) **Série de Engel.**
 - iv) **Séries de Pierce.**
 - v) **Série de Sylvester.**
 - vi) **Séries Alternées de Sylvester.**
 - vii) **Série de Lüroth.**
 - viii) **Séries Alternées de Lüroth.**
 - ix) **Série de Knopfmacher.**
 - x) **Produit de Cantor.**
 - xi) **Produit Alterné de Cantor.**
 - xii) **Produit Négatif de Cantor.**
 - xiii) **Série Binaire.**
- 4) **Développement Décimal.**
 - i) **Construction de Rota.**
 - ii) **Autres Méthodes Décimales.**
- 5) **A partir de la soustraction.**
 - i) **Construction de de Bruijn à partir de la soustraction.**
 - ii) **Construction de Udding à partir de la soustraction.**
- 6) **Autres Constructions.**
 - i) **Suites non décroissantes de rationnels positifs.**
 - ii) **Quasi-endomorphismes.**
 - iii) **Complétion de MacNeille.**
 - iv) **Construction à base de Recouvrements.**
 - v) **Construction à partir des Nombres Hyperrationnels.**
 - vi) **Construction à partir des Nombres Surréels.**

II.5.4 Constructions Usuelles.

Nous avons regroupé sous ce nom les trois méthodes de construction des réels que l'on voit au lycée.

Construction de Simon Stevin

La construction de Simon Stevin, un mathématicien belge (1548 - 1620) ou construction informelle consiste à considérer les nombres comme une suite finie de chiffres à gauche de la virgule et une suite éventuellement infinie de « décimales » ; on sait que les rationnels sont les nombres dont la suite des décimales est soit finie soit périodique, les réels sont obtenus lorsque l'on ne pose aucune condition sur les décimales sauf que cette suite ne doit pas être stationnaire égal à 9 à partir d'un certain rang (afin d'éviter les développements impropres).

Cette construction peut être formalisée (et étendue a toutes les bases de numération) :

Soit $p \in \mathbb{N}$ nous noterons \mathbf{U}^p l'ensemble des suites $(\mathbf{u}_n^p)_{n \in \mathbb{N}}$ d'éléments de $\mathbb{Z}/p\mathbb{Z}$ (autrement dit de nombres entiers entre 0 et $p - 1$ compris), qui ne soit pas stationnaire égale à $(p - 1)$ à partir d'un certain rang).

On définit $\mathbb{R} = \{(m, (\mathbf{u}_n^p)_{n \in \mathbb{N}}) \mid m \in \mathbb{Z} \wedge (\mathbf{u}_n^p)_{n \in \mathbb{N}} \in \mathbf{U}^p\}$

La définition informelle a l'avantage d'être intuitive, et sa version formalisée semble combler le manque de rigueur, malheureusement, avec cette définition, il n'est pas facile de donner des définition de l'addition et de la multiplication (à cause de la gestion de la retenue), aussi cette définition n'est-elle jamais réellement utilisée (sauf a des fins pédagogiques au collège et sans approfondissement), voir néanmoins [les développements décimaux](#).

Pour se convaincre de la difficulté de la définition des opérations à partir du développement décimal, il n'est que de calculer $1.\underline{2} \times 0.\underline{81}$ ¹⁰ en n'utilisant que le développement décimal.

Coupsures de Dedekind

On appelle Coupure de Dedekind, toute partition de \mathbb{Q} en deux ensembles A^- et A^+ vérifiant :

1. $A^- \cup A^+ = \mathbb{Q}$ (puisque'il s'agit d'une partition)
2. $A^- \cap A^+ = \emptyset$ (puisque'il s'agit d'une partition)
3. $A^- \neq \emptyset$
4. $A^+ \neq \emptyset$
5. $\forall x \forall y ((x \in A^- \wedge y \in A^+) \Rightarrow (x < y))$

Il va de soi qu'une coupure est entièrement définie par l'un de ces deux ensembles.

Il est immédiat de constater que tout nombre rationnel q définit deux coupures :

$A^- = \{x \mid x \in \mathbb{Q} \wedge x < q\}$ ou $A^- = \{x \mid x \in \mathbb{Q} \wedge x \leq q\}$ pour éviter ce petit souci, certains auteurs ajoute une condition à la définition d'une coupure : A^- ne possède pas de plus grand élément, ce qui permet de n'avoir qu'une seule coupure par nombre rationnel.

On peut constater que certaines coupures ne sont pas définies par un nombre rationnel, par exemple : $A^- = \{x \mid (x \leq 0) \vee (x^2 < 2)\}$

D'où la définition : \mathbb{R} est l'ensemble des coupures de \mathbb{Q} ; bien sur, il faut définir un ordre, une addition et une multiplication sur cet ensemble.

Si X^-, Y^- et Z^- sont des coupures définissant les nombres réels x, y et z , alors, par définition :

$$x < y \Leftrightarrow X^- \subsetneq Y^-$$

$$x + y = z \Leftrightarrow Z^- = \{\alpha + \beta \mid \alpha \in X^- \wedge \beta \in Y^-\}$$

Si x et y sont positifs, on peut définir leur produit (les autres cas sont définis par application de la règle des signes) :

$$x \times y = z \Leftrightarrow Z^+ = \{\alpha \times \beta \mid \alpha \in X^+ \wedge \beta \in Y^+\}$$

10. Exemple dû à D. Fowler dans l'article « Dedekind's theorem : $\sqrt{2} \times \sqrt{3} = \sqrt{6}$ », American Mathematical Monthly, Volume 99 No 8, p. 725-733, 1992

Avec ces définitions, $(\mathbb{R}, +, \times, <)$ est un corps ordonné, complet dans le sens où, si on calcule des coupures à partir de ce nouvel ensemble, on ne fabrique aucun nouvel élément.

Suites de Cauchy

Une suite de rationnels est une application : $u : \mathbb{N} \mapsto \mathbb{Q}$, il est d'usage de noter u_n plutôt que $u(n)$ l'image de n par u .

Une suite de terme général u_n est dite convergente de limite ℓ et on note $\lim_{n \rightarrow \infty} u_n = \ell$ si et seulement si :

$$\forall \varepsilon \in \mathbb{Q}^{+*} \exists \eta \in \mathbb{N} \forall n \in \mathbb{N} (n > \eta \Rightarrow |u_n - \ell| < \varepsilon)$$

Cette définition présente un gros inconvénient : pour appliquer la définition, il faut connaître la limite.

Une première idée, pour trouver un critère de convergence, est de vérifier que la différence entre deux images successives devient infiniment petite, malheureusement ce n'est pas suffisant, par exemple la suite ci-dessous devient infiniment grande ¹¹ :

$$u_n = \sum_{i=0}^n \frac{1}{i+1}$$

Cauchy imagina de « compléter » cette première idée en étudiant non la différence entre deux termes consécutifs, mais entre deux termes quelconques au-delà d'une certaine valeur de la variable : une suite est dite « de Cauchy » si elle vérifie :

$$\forall \varepsilon \in \mathbb{Q}^{+*} \exists \eta \in \mathbb{N} \forall n \in \mathbb{N} \forall m \in \mathbb{N} ((n > \eta) \wedge (m > \eta)) \Rightarrow |u_n - u_m| < \varepsilon$$

Dans cette nouvelle définition, la limite ℓ n'intervient plus, malheureusement ce n'est toujours pas suffisant : une suite de Cauchy n'est pas forcément convergente (dans \mathbb{Q}), par exemple :

$$u_n = \sum_{i=0}^n \frac{1}{i!}$$

Ne converge pas dans \mathbb{Q} ¹², par contre elle est bornée, comme toutes les suites de Cauchy.

Il est immédiat de montrer que l'ensemble des suites de rationnels, noté $\mathbb{Q}^{\mathbb{N}}$, peut être très naturellement muni de relations :

$$\begin{aligned} \text{Une addition} & \quad \forall u \in \mathbb{Q}^{\mathbb{N}} \forall v \in \mathbb{Q}^{\mathbb{N}} \forall w \in \mathbb{Q}^{\mathbb{N}} ((w = u + v) \Leftrightarrow \forall n \in \mathbb{N} (w_n = u_n + v_n)) \\ \text{Une multiplication} & \quad \forall u \in \mathbb{Q}^{\mathbb{N}} \forall v \in \mathbb{Q}^{\mathbb{N}} \forall w \in \mathbb{Q}^{\mathbb{N}} ((w = u \cdot v) \Leftrightarrow \forall n \in \mathbb{N} (w_n = u_n \cdot v_n)) \\ \text{Une relation d'ordre} & \quad \forall u \in \mathbb{Q}^{\mathbb{N}} \forall v \in \mathbb{Q}^{\mathbb{N}} (u < v) \Leftrightarrow \exists \eta \forall n \in \mathbb{N} (n > \eta \Rightarrow u_n < v_n) \end{aligned}$$

On peut vérifier simplement que $(\mathbb{Q}^{\mathbb{N}}, +, \times)$ est un anneau commutatif, par contre $<$ n'est pas une relation d'ordre, mais \leq est une relation de pré-ordre.

Soit \mathcal{C} l'ensemble des suites Cauchy, comme $\mathcal{C} \subset \mathbb{Q}^{\mathbb{N}}$, \mathcal{C} hérite des relations ci-dessus, et même $(\mathcal{C}, +, \times)$ est un sous-anneau (la démonstration est aisée en utilisant le fait que les suites de Cauchy sont bornées).

Soit \mathcal{Z} le sous-ensemble de \mathcal{C} constitué des suites convergeant vers 0. \mathcal{Z} est un idéal de $(\mathcal{C}, +, \times)$ (là encore la démonstration assez simple utilise le fait que les suites de Cauchy sont bornées).

\mathcal{Z} est même un idéal maximal ¹³ (de \mathcal{C}) d'où on déduit que $(\mathcal{C}/\mathcal{Z}, +, \times)$ est un corps qui sera noté $(\mathbb{R}, +, \times)$.

Il va de soi que les suites constantes égales à un rationnel sont de Cauchy, et que l'application de \mathbb{Q} dans \mathcal{C}/\mathcal{Z} qui a un nombre rationnel fait correspondre la suite constante égale à ce rationnel, est injective (trivial) ce qui permet de plonger naturellement \mathbb{Q} dans \mathbb{R} .

11. C'est la suite des sommes partielles de la série harmonique.

12. Sa limite dans \mathbb{R} est e .

13. Si \mathcal{Z} contenait une suite ne convergeant pas vers 0, \mathcal{Z} contiendrait une suite jamais nulle et donc toutes les suites de Cauchy.

II.5.5 Méthodes Axiomatiques.

Les méthodes axiomatiques ne sont pas, au sens strict des méthodes de constructions, mais elles restent néanmoins très intéressantes, car dans le cas des réels, les axiomatiques sont catégoriques, c'est à dire ne possèdent qu'un seul modèle, à isomorphisme près.

Il est important de noter que ces axiomatiques sont du second ordre, on peut légitimement se demander si une axiomatique du premier ordre est possible : la réponse est non !

On peut même montrer qu'il existe un modèle élémentairement équivalent à $(\mathbb{R}, +, \times, <)$ (donc dans ce langage) mais qui n'est pas archimédien¹⁴ alors que \mathbb{R} l'est.

Axiomatique Usuelle

Dans les propositions ci-dessous, les lettres minuscules x, y, z, t représentent des éléments de \mathbb{R} et les majuscules X, Y représentent des sous-ensembles de \mathbb{R} .

- 1) $(\mathbb{R}, +, \times, \leq)$ est un corps commutatif, totalement ordonné (c'est donc un corps réel, cf. infra).
 - a) $(\mathbb{R}, +)$ est un groupe abélien.
 - b) (\mathbb{R}^*, \times) est un groupe abélien.
 - c) (\mathbb{R}, \leq) est un ordre total
 - d) \leq est compatible avec les opérations $+$ et \times .
 - i) $\forall x \forall y \forall z (((x \leq y) \Rightarrow (((x + z) \leq (y + z)) \wedge ((z + x) \leq (z + y))))$
 - ii) $\forall x \forall y \forall z (((x \leq y) \wedge (0 \leq z)) \Rightarrow (((x \times z) \leq (y \times z)) \wedge ((z \times x) \leq (z \times y))))$
- 2) Tout sous-ensemble X majoré de \mathbb{R} admet une borne supérieure (pas forcément dans X).
 $\forall X \exists y \forall x \forall z \exists t (((X \neq \emptyset) \wedge (x \in X)) \Rightarrow (x \leq y)) \wedge ((z < y) \Rightarrow ((t \in X) \wedge (z < t)))$
- 3) \mathbb{R} est archimédien¹⁵.
 $\forall x \in \mathbb{R}^{+*} \forall y \in \mathbb{R} \exists n \in \mathbb{N} (nx > y)$

Tous les modèles de cette axiomatique sont isomorphes, c'est d'ailleurs cette propriété qui sert, généralement, pour montrer qu'une construction particulière donne bien $(\mathbb{R}, +, \times, \leq)$.

Axiomatique de Tarski

Alfred Tarski a mis au point (dans *Introduction to Logic and to the Methodology of Deductive Sciences*) deux systèmes d'axiomes Dans les propositions ci-dessous, les lettres minuscules v, w, x, y, z représentent des éléments de \mathbb{R} et les majuscules X, Y représentent des sous-ensembles de \mathbb{R} .

Système 1

- Axiome 1 : $\forall x \forall y ((x \neq y) \Rightarrow ((x < y) \vee (y < x)))$
 Axiome 2 : $\forall x \forall y (x < y \Rightarrow \neg(y < x))$
 Axiome 3 : $\forall x \forall y \exists z (x < y \Rightarrow ((x < z) \wedge (z < y)))$
 Axiome 4 : $\forall X \forall Y \forall x \forall y (((x \in X) \wedge (y \in Y)) \Rightarrow (x < y)) \Rightarrow \exists z \forall v \forall w (((v \in X) \wedge (w \in Y)) \Rightarrow ((v \leq z) \wedge (z \leq w)))$
 Axiome 5 : $\forall x \forall y \forall z (x + (y + z) = (x + z) + y)$
 Axiome 6 : $\forall x \forall y \exists z (x + z = y)$
 Axiome 7 : $\forall w \forall x \forall y \forall z ((x + y) < (z + w)) \Rightarrow ((x < z) \vee (y < w))$
 Axiome 8 : $1 \in \mathbb{R}$
 Axiome 9 : $1 < 1 + 1$

Tarski a démontré que cette axiomatique permettait de définir une multiplication, compatible avec la relation d'ordre.

Tout modèle de cette axiomatique est isomorphe à $(\mathbb{R}, +, \times, <)$.

14. Cette propriété n'est donc pas du premier ordre.

15. Cette propriété est souvent citée, mais n'est pas nécessaire comme axiome puisque démontrable à partir des autres.

Système 2

- Axiome 1 : $\forall x \forall y ((x \neq y) \Rightarrow ((x < y) \vee (y < x)))$
 Axiome 2 : $\forall x \forall y (x < y \Rightarrow \neg(y < x))$
 Axiome 3 : $\forall x \forall y \exists z (((x < y) \wedge (y < z)) \Rightarrow (x < z))$
 Axiome 4 : $\forall X \forall Y \forall x \forall y (((x \in X) \wedge (y \in Y)) \Rightarrow (x < y)) \Rightarrow$
 $\exists z \forall v \forall w (((v \in X) \wedge (w \in Y)) \Rightarrow ((v \leq z) \wedge (z \leq w)))$
 Axiome 5 : $\forall x \forall y \exists z (x + y = z)$
 Axiome 6 : $\forall x \forall y (x + y = y + x)$
 Axiome 7 : $\forall x \forall y \forall z (x + (y + z) = (x + y) + z)$
 Axiome 8 : $\forall x \forall y \exists z (x = y + z)$
 Axiome 9 : $\forall x \forall y \forall z ((y < z) \Rightarrow (x + y < x + z))$
 Axiome 10 : $0 \in \mathbb{R}$
 Axiome 11 : $\forall x (x + 0 = x)$
 Axiome 12 : $\forall x \forall y \exists z (x \cdot y = z)$
 Axiome 13 : $\forall x \forall y (x \cdot y = y \cdot x)$
 Axiome 14 : $\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$
 Axiome 15 : $\forall x \forall y \exists z ((y \neq 0) \Rightarrow x = y \cdot z)$
 Axiome 16 : $\forall x \forall y \forall z (((0 < x) \wedge (y < z)) \Rightarrow (x \cdot y < x \cdot z))$
 Axiome 17 : $\forall x \forall y \forall z (x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
 Axiome 18 : $1 \in \mathbb{R}$
 Axiome 19 : $\forall x (x \cdot 1 = x)$
 Axiome 20 : $0 \neq 1$

Tarski a montré que les systèmes 1 et 2 sont équivalents ; le sens $2 \Rightarrow 1$ est facile, mais le sens $1 \Rightarrow 2$ est très difficile.

II.5.6 Suites Particulières.

Les méthodes suivantes sont toutes basées sur la même idée qui consiste à définir des suites (qui de facto sont de Cauchy) particulières de telle sorte que l'on puisse définir les réels non comme des classes d'équivalence de suites de Cauchy, mais directement comme une suite d'entiers possédant quelques propriétés spécifiques et qui peut donc être vue comme une suite formelle.

Nous commencerons par donner un exemple particulièrement intéressant, celui des fractions continues, puis une méthode générale, enfin plusieurs exemples d'application de cette méthode avec des suites plus ou moins connues.

Fractions Continues.

L'idée des fractions continues prend sa source dans l'algorithme de calcul du plus grand diviseur commun d'Euclide, un mathématicien grec (environ -325 à -265), mais l'histoire commence réellement avec Rafael Bombelli (1526 - 1572) et Pietro Antonio Cataldi (1548 - 1626), deux mathématiciens italiens ; par la suite elles furent très étudiées par Leonhard Paul Euler (1707 - 1783), un mathématicien suisse, Jean Henri Lambert (1728 - 1777), un mathématicien français (de Mulhouse, ce qui fait qu'on le trouve parfois sous le nom Johann Heinrich Lambert) et Joseph Louis Lagrange (1736 - 1813), un mathématicien italo-français.

Une fraction continue simple¹⁶ finie est une fraction de la forme :

$$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_n}}}}$$

16. Comme nous ne considérerons que des fractions continues simples, nous omettrons systématiquement cette précision.

où $a_0 \in \mathbb{Z}$ et $\bigwedge_{i=1}^n a_i \in \mathbb{N}$.

Il est évident qu'une fraction continue finie est un nombre rationnel, mais on peut aussi montrer assez facilement qu'un nombre rationnel peut se mettre sous la forme d'une fraction continue, pour un nombre relatif, c'est évident ($n = a_0$) :

Soit $\frac{p}{q} \in \mathbb{Q} \setminus \mathbb{Z}$ un nombre rationnel, comme \mathbb{Z} est un anneau euclidien, on peut trouver $a_0 \in \mathbb{Z}$ et $r_0 \in]0; q[$ tels que $p = a_0q + r_0$, ce qui peut s'écrire $\frac{p}{q} = a_0 + \frac{r_0}{q}$, ou encore $\frac{p}{q} = a_0 + \frac{1}{\left(\frac{q}{r_0}\right)}$. Si $r_0|q$ ¹⁷, alors $a_1 = \frac{q}{r_0}$

et $\frac{p}{q} = a_0 + \frac{1}{a_1}$, et la démonstration est terminée, sinon, il existe $a_1 \in \mathbb{N}$ et $r_1 \in]0; r_0[$ tels que $q = a_1r_0 + r_1$, et on recommence. La suite (r_i) étant décroissante dans \mathbb{N} , elle se termine forcément en 0, ce qui achève la démonstration.

Il peut apparaître de peu d'utilité de transformer une fraction simple en une fraction continue, mais heureusement on peut aller plus loin, et on peut montrer que tous les nombres réels peuvent s'écrire sous forme de fractions continues (possiblement infinies), prenons d'abord un exemple :

$$\pi = 3.14159265358979\dots$$

$$\pi = 3 + 0.14159265358979\dots$$

ce qui donne une approximation bien connue : $\pi \approx 3$

$$\pi = 3 + \frac{1}{\frac{1}{0.14159265358979\dots}}$$

$$\pi = 3 + \frac{1}{7,06251330593105\dots}$$

$$\pi = 3 + \frac{1}{7 + 0.06251330593105\dots}$$

ce qui donne une approximation bien connue : $\pi \approx \frac{22}{7}$

$$\pi = 3 + \frac{1}{7 + \frac{1}{\frac{1}{0.06251330593105\dots}}}$$

$$\pi = 3 + \frac{1}{7 + \frac{1}{15.9965944066841\dots}}$$

$$\pi = 3 + \frac{1}{7 + \frac{1}{15 + 0.9965944066841\dots}}$$

ce qui donne une approximation bien connue : $\pi \approx \frac{333}{106}$

$$\pi = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{\frac{1}{0.9965944066841\dots}}}}$$

$$\pi = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1,003417231015\dots}}}$$

$$\pi = 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \dots}}}$$

ce qui donne une approximation bien connue : $\pi \approx \frac{355}{113}$.

Montrons que tout réel peut s'écrire comme une fraction continue :

Soit $x \in \mathbb{R}$, posons $a_0 = [x]$ et $x_1 = x - a_0$, on peut écrire $x = a_0 + x_1$, où $0 \leq x_1 < 1$ si $x_1 = 0$, la démonstration est terminée, sinon $\frac{1}{x_1} > 1$.

^{17.} $r_0|q$ se lit : r_0 divise q

En posant $a_1 = \left\lfloor \frac{1}{x_1} \right\rfloor$ et $x_2 = \frac{1}{x_1} - a_1$ nous pouvons écrire : $\frac{1}{x_1} = a_1 + x_2$ ou encore $x = a_0 + \frac{1}{a_1 + x_2}$, où $0 \leq x_2 < 1$, si $x_2 = 0$, la démonstration est terminée, sinon $\frac{1}{x_2} > 1$.

En posant $a_2 = \left\lfloor \frac{1}{x_2} \right\rfloor$ et $x_3 = \frac{1}{x_2} - a_2$ nous pouvons écrire : $\frac{1}{x_2} = a_2 + x_3$ ou encore $x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + x_3}}$,

où $0 \leq x_3 < 1$, si $x_3 = 0$, la démonstration est terminée, sinon $\frac{1}{x_3} > 1$.

etc.

Pour résumer l'algorithme (à chaque étape si $x_i = 0$, l'algorithme est terminé) :

$a_0 = \lfloor x \rfloor$	$x_1 = x - a_0$	$x = a_0 + x_1$	$0 \leq x_1 < 1$	$x = a_0 + x_1$
$a_1 = \left\lfloor \frac{1}{x_1} \right\rfloor$	$x_2 = \frac{1}{x_1} - a_1$	$\frac{1}{x_1} = a_1 + x_2$	$0 \leq x_2 < 1$	$x = a_0 + \frac{1}{a_1 + x_2}$
$a_2 = \left\lfloor \frac{1}{x_2} \right\rfloor$	$x_3 = \frac{1}{x_2} - a_2$	$\frac{1}{x_2} = a_2 + x_3$	$0 \leq x_3 < 1$	$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + x_3}}$
\vdots	\vdots	\vdots	\vdots	\vdots
$a_n = \left\lfloor \frac{1}{x_n} \right\rfloor$	$x_{n+1} = \frac{1}{x_n} - a_n$	$\frac{1}{x_n} = a_n + x_{n+1}$	$0 \leq x_{n+1} < 1$	$x = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\ddots + \frac{1}{a_n + x_{n+1}}}}}$
\vdots	\vdots	\vdots	\vdots	\vdots

On pose $u_n = a_0 + \frac{1}{\ddots + \frac{1}{a_n}}$

Il ne reste plus qu'à montrer que cette suite est convergente :

On peut facilement montrer que la sous suite u_{2n} est croissante et la sous-suite u_{2n+1} est décroissante, on peut aussi montrer (c'est un peu moins simple) que $\lim_{m \rightarrow \infty} (u_{n+1} - u_n) = 0$ ce qui établit la convergence de la suite $(u_n)_{n \in \mathbb{N}}$.

Il existe quelques cas particuliers intéressants :

$$\phi = \frac{1 + \sqrt{5}}{2} = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\ddots}}} \quad \text{Ce qui peut s'écrire } \phi = 1 + \frac{1}{\phi} \left(\phi \text{ est solution de } x = 1 + \frac{1}{x} \right).$$

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{\ddots}}} \quad \text{Ce qui peut s'écrire } \sqrt{2} = 1 + \frac{1}{1 + \sqrt{2}} \left(\sqrt{2} \text{ est solution de } x = 1 + \frac{1}{1 + x} \right).$$

On peut d'ailleurs montrer (sans grande difficulté) que les fractions continues périodiques à partir d'un certain rang correspondent exactement aux nombres quadratiques¹⁸ non rationnels.

Il est d'usage de noter les fractions continues finies sous la forme $\langle a_0, a_1, \dots, a_n \rangle$, les fractions continues infinies sous la forme $\langle a_0, a_1, \dots \rangle$, et dans le cas particulier des fractions continues infinies périodiques à partir d'un certain rang, on utilise la même convention que dans les développements décimaux :

18. C'est à dire les solutions d'équations entières du second degré.

$$\frac{7}{4} = 1 + \frac{1}{1 + \frac{1}{3}} = \langle 1, 1, 3 \rangle$$

$$\pi = \langle 3, 7, 15, 1, \dots \rangle$$

$$\phi = \langle \bar{1} \rangle$$

$$\sqrt{2} = \langle 1, \bar{2} \rangle$$

$$x = \langle a_0, a_1, a_2, \dots, a_n, \overline{a_{n+1}, a_{n+2}, \dots, a_{n+m}} \rangle \quad \text{Pour } x \text{ quadratique.}$$

On peut donc construire les réels comme l'ensemble des suites finies ou non de la forme $\langle a_0, a_1, \dots \rangle$ où $a_0 \in \mathbb{Z}$ et $\bigwedge_{i=1}^n a_i \in \mathbb{N}$ et $\langle a_0, a_1, \dots, a_n, 1 \rangle$ est remplacé par $\langle a_0, a_1, \dots, a_n + 1 \rangle$.

On vérifie aisément que si $a = \langle a_0, a_1, a_2, \dots \rangle$, on peut calculer facilement $-a$ et a^{-1} (si $a \neq 0$)

$$\text{Pour le calcul de l'opposé : } \begin{cases} a_1 = 1 \Rightarrow -a = \langle -a_0 - 1, 1 + a_2, a_3, \dots \rangle \\ a_1 > 1 \Rightarrow -a = \langle -a_0 - 1, 1, a_1 - 1, a_2, a_3, \dots \rangle \end{cases}$$

La démonstration des deux cas, qui sont symétriques, se fait en une seule étape : on doit montrer que

$$a_0 + \frac{1}{1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \dots}}}} + (-a_0 - 1) + \frac{1}{1 + a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \dots}}} = 0$$

Ce qui peut s'écrire : $-1 + \frac{1}{1 + \frac{1}{X}} + \frac{1}{1 + X}$ dont on vérifie facilement que c'est égal à 0.

$$\text{Pour le calcul de l'inverse}(a \neq 0) : \begin{cases} a_0 = 0 \Rightarrow a^{-1} = \langle a_1, a_2, a_3, \dots \rangle \\ a_0 > 0 \Rightarrow a^{-1} = \langle 0, a_0, a_1, a_2, a_3, \dots \rangle \\ a_0 < 0 \Rightarrow a^{-1} = -(-a)^{-1} \end{cases}$$

La démonstration des deux premier cas, qui sont symétriques, se fait en une seule étape : on doit montrer que

$$\frac{1}{a_1 + \frac{1}{a_2 + \dots}} \times \left(a_1 + \frac{1}{a_2 + \dots} \right) = 1$$

Ce qui peut s'écrire $\frac{1}{X} \times X$, qui est trivialement égal à 1.

On peut représenter les fractions rationnelles sous la forme d'une suite d'entiers, finie ou infinie, que nous écrirons : $a = \langle a_0, a_1, \dots, a_n, \dots \rangle$, mais sous cette forme nous sommes obligés de traiter différemment les fractions rationnelles finies (correspondant à des suites finies et donc à des rationnels), et les fractions rationnelles infinies (correspondant à des suites infinies et donc des irrationnels).

Georg Johann Rieger, un mathématicien allemand (1931 -) dans un article de 1982 eut l'idée très fructueuse de considérer ces suites sous la forme suivante :

Soit ω un élément plus grand que tout entier ($\forall n \in \mathbb{N} (\omega > n)$), on écrit une fraction rationnelle sous la forme d'une suite **toujours** infinie $a = \langle a_0, a_1, \dots, a_n, \dots \rangle$ vérifiant les conditions suivantes :

- $a_0 \in \mathbb{Z} \wedge \forall n \in \mathbb{N}^* (a_n \in \mathbb{N}^* \cup \{\omega\})$
- $\forall \eta \in \mathbb{N} \forall n \in \mathbb{N} ((a_n = \omega) \wedge (n > \eta)) \Rightarrow (a_n = \omega)$
- $\forall n \in \mathbb{N}^* ((a_n = 1) \Rightarrow (a_{n+1} \neq \omega))$

Nous noterons \mathfrak{S} l'ensemble de ces suites.

\mathfrak{S} peut être muni d'une relation d'ordre totale compatible avec l'ordre sur \mathbb{Q} :

Soit $a \in \mathfrak{S}$ et $b \in \mathfrak{S}$, nous noterons η_a^b , le plus petit indice pour lequel les termes des suites a et b sont différents (c'est à dire que $\forall n((n < \eta_a^b) \Rightarrow (a_n = b_n)) \wedge (a_{\eta_a^b} \neq b_{\eta_a^b})$).

$$a < b \Leftrightarrow \begin{cases} (\eta_a^b \in 2\mathbb{N}) & \wedge (a_{\eta_a^b} < b_{\eta_a^b}) \\ \vee \\ (\eta_a^b \in 2\mathbb{N} + 1) & \wedge (a_{\eta_a^b} > b_{\eta_a^b}) \end{cases}$$

Muni de cette relation d'ordre nous pouvons montrer que pour toute partie majorée $\mathfrak{M} \subset \mathfrak{S}$, il existe une borne supérieure dans \mathfrak{S} :

Soit $\sigma_0 = \sup_{\alpha \in \mathfrak{M}} (\alpha_0)$, cette borne supérieure existe et est atteinte puisque \mathfrak{M} est bornée.

On pose $\mathfrak{M}_0 = \{\alpha \in \mathfrak{M} \mid \alpha_0 = \sigma_0\}$ qui n'est donc pas vide.

Soit $\sigma_1 = \inf_{\alpha \in \mathfrak{M}_0} (\alpha_1)$, cette borne inférieure existe et est atteinte puisque, par construction, l'ensemble des α_1 est minoré par 1.

On pose $\mathfrak{M}_1 = \{\alpha \in \mathfrak{M}_0 \mid \alpha_1 = \sigma_1\}$ qui n'est donc pas vide.

Pour $n > 0$, soit :

$$\sigma_{2n} = \sup_{\alpha \in \mathfrak{M}_{2n-1}} (\alpha_{2n}) \begin{cases} \sigma_{2n} \in \mathbb{N}^* & \text{cette borne supérieure est atteinte, on pose } \mathfrak{M}_{2n} = \{\alpha \in \mathfrak{M}_0 \mid \alpha_{2n} = \sigma_{2n}\} \\ \vee \\ \sigma_{2n} = \omega & \text{atteint ou non, on pose : } \sigma = \langle s_0, s_1, \dots, \sigma_{2n-1}, \bar{\omega} \rangle, \text{ et on arrête le calcul.} \end{cases}$$

Pour $n > 0$, soit $\sigma_{2n+1} = \inf_{\alpha \in \mathfrak{M}_{2n+1}} (\alpha_{2n+1})$, cette borne inférieure existe et est atteinte puisque l'ensemble des α_{2n+1} est minoré par 1.

On pose $\mathfrak{M}_{2n+1} = \{\alpha \in \mathfrak{M}_{2n} \mid \alpha_{2n+1} = \sigma_{2n+1}\}$ et on continue les calculs.

Alors $\sigma = \langle \sigma_0, \sigma_1, \dots \rangle$ est la borne supérieure de \mathfrak{M} . Le seul problème qui peut éventuellement se poser c'est que la suite obtenue ne vérifie pas les conditions pour appartenir à \mathfrak{S} , et plus précisément, il est possible que $\sigma = \langle \sigma_0, \sigma_1, \dots, \sigma_n, 1, \bar{\omega} \rangle$ mais dans ce cas, il suffit de remplacer cette suite par $\sigma = \langle \sigma_0, \sigma_1, \dots, \sigma_n + 1, \bar{\omega} \rangle$.

$(\mathfrak{M}, <)$ est donc un ensemble totalement ordonné possédant la propriété de la borne supérieure, il ne reste plus qu'à le munir d'une addition et d'une multiplication adéquates pour obtenir \mathbb{R} .

Soit $\alpha \in \mathfrak{S}$, on note $\alpha^{(n)} = \langle \alpha_0, \alpha_1, \dots, \alpha_n, \bar{\omega} \rangle$, $\widehat{\alpha^{(n)}}$ le nombre rationnel auquel correspond $\alpha^{(n)}$, et $\langle [q] \rangle$ la suite (finie) correspondant au nombre rationnel q .

Néanmoins, au lieu d'écrire, par exemple, $\langle [\widehat{\alpha^{(2n)}} + \widehat{\beta^{(2n)}}] \rangle$, nous écrirons plus simplement $\alpha^{(2n)} + \beta^{(2n)}$, dans la mesure où il n'y a pas d'ambiguïté.

Ceci permet de définir l'addition et la multiplication sur \mathfrak{S} ¹⁹ :

$$\alpha + \beta = \sup_{n \in \mathbb{N}} (\alpha^{(2n)} + \beta^{(2n)})$$

$$\begin{cases} (\alpha \geq 0) \wedge (\beta \geq 0) & \Rightarrow \alpha \cdot \beta = \sup_{n \in \mathbb{N}} (\alpha^{(2n)} \cdot \beta^{(2n)}) \\ (\alpha \geq 0) \wedge (\beta \leq 0) & \Rightarrow \alpha \cdot \beta = -\sup_{n \in \mathbb{N}} (\alpha^{(2n)} \cdot (-\beta)^{(2n)}) \\ (\alpha \leq 0) \wedge (\beta \geq 0) & \Rightarrow \alpha \cdot \beta = -\sup_{n \in \mathbb{N}} ((-\alpha)^{(2n)} \cdot \beta^{(2n)}) \\ (\alpha \leq 0) \wedge (\beta \leq 0) & \Rightarrow \alpha \cdot \beta = \sup_{n \in \mathbb{N}} ((-\alpha)^{(2n)} \cdot (-\beta)^{(2n)}) \end{cases}$$

On ne prend en compte que les suites de la forme $\alpha^{(2n)}$, car l'application $n \mapsto \alpha^{(2n)}$ est croissante (et tend donc vers sa limite par valeur inférieure).

19. Ne pas oublier que $\alpha^{(2n)}$ et $\beta^{(2n)}$ sont des rationnels dont on sait calculer la somme.

Ensembles de Nombres

Avec ces définitions, on peut montrer que $(\mathbf{S}, +, \times, <)$ est isomorphe à $(\mathbb{R}, +, \times, <)$ (on a déjà montré la propriété de la borne supérieure).

La commutativité et l'associativité des deux opérations, ainsi que la distributivité de la multiplication sur l'addition se démontrent facilement à l'aide de ces mêmes propriétés dans \mathbb{Q} , il est très simple de montrer que $\langle 0, \bar{\omega} \rangle$, et $\langle 1, \bar{\omega} \rangle$ sont les éléments neutres, quant aux inverses ils ont été calculés précédemment.

Méthode Générale

Soit $\mathfrak{S} = \{a = \langle a_0, a_1, \dots, a_n, \dots \rangle\}$ un ensemble de suites infinies possédant les propriétés suivantes :

1. $a_0 \in \mathbb{Z} \wedge \left(\bigwedge_{i \in \mathbb{N}^*} a_i \in \mathbb{N} \cup \{\omega\} \right)$, où ω est plus grand que tous les entiers.
2. $\forall i \in \mathbb{N} \forall j \in \mathbb{N} ((a_i = \omega) \wedge (j > i)) \Rightarrow (a_j = \omega)$
3. Soit $a \in \mathfrak{S}$, nous noterons $a^{(n)} = \langle a_0, a_1, \dots, a_n, \omega, \dots, \omega, \dots \rangle$.
4. $\forall a \in \mathfrak{S} \forall n \in \mathbb{N} (a^{(n)} \in \mathfrak{S})$. Autrement dit, tous les segments initiaux de suites de \mathfrak{S} sont dans \mathfrak{S} .
5. Il existe une suite que nous noterons $\widehat{a} = (\widehat{a}_n)_{n \in \mathbb{N}}$, telle que :
 - i) $\widehat{a}_0 = a_0$
 - ii) $\widehat{a}_n = \varphi(a_0, a_1, a_2, \dots, a_n)$. Autrement dit, \widehat{a}_n ne dépend que des a_i précédents
 - iii) $a_n = \omega \Rightarrow \widehat{a}_n = \widehat{a}_{n-1}$
 - iv) $\widehat{a}_n \in \mathbb{Q}$.
 - v) On pose $\widehat{a} = \lim_{n \rightarrow \infty} \widehat{a}_n$, quand celle-ci existe dans \mathbb{Q} ²⁰ (donc en particulier pour les suites finies). On peut remarquer que $\widehat{a}_n = \widehat{a^{(n)}}$
 - vi) Pour tout $x \in \mathbb{Q}$ il existe une suite $a \in \mathfrak{S}$ telle que $x = \widehat{a}$.
6. Il existe une famille de relations $(\mathcal{R}_i)_{i \in \mathbb{N}}$ telle que $\mathcal{R}_i \in \{<, >\}$ et telle que l'on peut définir une relation d'ordre sur \mathfrak{S} , notée $<$ et vérifiant :

$$a < b \Leftrightarrow \exists \eta \in \mathbb{N} \forall i \in \mathbb{N} ((i < \eta) \Rightarrow (((a_i = b_i) \wedge (a_\eta \neq b_\eta) \wedge (\mathcal{R}_\eta(a_\eta, b_\eta)))).$$

Par la suite nous noterons η_a^b , le plus petit indice pour lequel les termes des suites a et b sont différents.

7. Pour la relation d'ordre précédente, toute partie bornée $\mathfrak{M} \subset \mathfrak{S}$ possède une borne supérieure.
8. Il existe une fonction croissante $f : \mathbb{N} \mapsto \mathbb{N}$ telle que l'application $\mathbb{N} \mapsto \mathbb{Q}$ définie par $n \mapsto a^{(f(n))}$ soit monotone.

Dans la suite de ce document nous utiliserons les notations suivantes :

- $\mathfrak{S}^{<\omega}$ le sous-ensemble de \mathfrak{S} tel qu'il existe $k \in \mathbb{N}^*$ tel que $a_k = \omega$, on l'appelle ensemble des suites finies.
- \mathfrak{S}^\sim le sous-ensemble de \mathfrak{S} des suites périodiques à partir d'un certain rang (on a donc le sous-ensemble de $\mathfrak{S}^\sim \subset \mathfrak{S}^{<\omega}$).
- \mathfrak{S}^δ le sous-ensemble de \mathfrak{S} des suites dont les différences entre deux termes consécutifs sont périodiques.

A partir de cette ensemble de suite, on peut définir des opérations, comme pour les fractions continues :

Ceci permet de définir l'addition et la multiplication sur \mathfrak{S}^{21} (dans le cas où la fonction f définie ci-dessus est décroissante, il faut prendre le inf à la place du sup) :

$$\alpha + \beta = \sup_{n \in \mathbb{N}} \left(\alpha^{(f(n))} + \beta^{(f(n))} \right).$$

$$\left\{ \begin{array}{l} (\alpha \geq 0) \wedge (\beta \geq 0) \Rightarrow \alpha \cdot \beta = \sup_{n \in \mathbb{N}} \left(\alpha^{(f(n))} \cdot \beta^{(f(n))} \right) \\ (\alpha \geq 0) \wedge (\beta \leq 0) \Rightarrow \alpha \cdot \beta = - \sup_{n \in \mathbb{N}} \left(\alpha^{(f(n))} \cdot (-\beta)^{(f(n))} \right) \\ (\alpha \leq 0) \wedge (\beta \geq 0) \Rightarrow \alpha \cdot \beta = - \sup_{n \in \mathbb{N}} \left((-\alpha)^{(f(n))} \cdot \beta^{(f(n))} \right) \\ (\alpha \leq 0) \wedge (\beta \leq 0) \Rightarrow \alpha \cdot \beta = \sup_{n \in \mathbb{N}} \left((-\alpha)^{(f(n))} \cdot (-\beta)^{(f(n))} \right) \end{array} \right.$$

Comme pour les fractions continues, les propriétés de commutativité, d'associativité, et la distributivité sont évidentes, les éléments neutres sont $(0, \bar{\omega})$ et $(1, \bar{\omega})$.

20. La notion de limite se définit très bien dans \mathbb{Q} .

21. Ne pas oublier que $\widehat{\alpha^{(f(n))}}$ et $\widehat{\beta^{(f(n))}}$ sont des rationnels dont on sait calculer la somme et le produit.

Par contre, les inverses, contrairement aux fractions continues ne sont pas toujours faciles à exprimer, nous allons donc donner une formule générale :

$$-\alpha = \inf_{n \in \mathbb{N}} \left((-\alpha)^{f(n)} \right).$$

$$\begin{cases} (\alpha > 0) & \Rightarrow \alpha^{-1} = \inf_{n \in \mathbb{N}} \left(\left(\frac{1}{\alpha} \right)^{f(n)} \right) \\ (\alpha < 0) & \Rightarrow \alpha^{-1} = \sup_{n \in \mathbb{N}} \left(\left(\frac{1}{\alpha} \right)^{f(n)} \right) \end{cases}$$

Remarque : avec les notations vues dans la partie sur les fractions rationnelles, il faut comprendre que $(-\alpha)^{f(n)} = [-\widehat{(\alpha^{f(n)})}]$ c'est à dire qu'à partir de la suite α , on calcule le rationnel qui correspond à la sous-suite qui s'arrête en $f(n)$, on prend l'opposé de ce rationnel, qui est bien évidemment un rationnel, et on construit la suite (finie ou non) qui correspond à ce rationnel, (et similairement pour $\left(\frac{1}{\alpha}\right)^{f(n)}$).

Une remarque importante : la démonstration de la propriété de la borne supérieure se fait comme pour les fractions continues, à l'aide de la fonction f et des relations (\mathcal{R}_i) .

Les pages qui suivent donnent des exemples pour lesquels on peut appliquer cette méthode générale, ce sont donc autant de méthodes pour construire l'ensemble des nombres Réels.

Certains des exemples ci-dessous ne permettent de générer que \mathbb{R}^+ (resp. \mathbb{R}^{*+}), mais ce n'est en rien un problème dans la mesure où fabriquer \mathbb{R} à partir de \mathbb{R}^+ (resp. \mathbb{R}^{*+}) est aussi facile que de passer de \mathbb{N} (resp. \mathbb{N}^*) à \mathbb{Z} .

Le calcul des termes successifs des expansions usuelles des nombres réelles nécessite d'effectuer les opérations avec beaucoup de décimales, par exemples l'utilisation d'un tableur d'une marque bien connue (bien pratique pourtant pour ce genre de calculs), ne donne que 15 décimales, un développement en langage C standard n'en fourni que 17 ce qui est très, très insuffisant, l'utilisation d'une base de données (avec récursion) permet d'obtenir 38 décimales ce qui est déjà beaucoup mieux, une solution qui semble prometteuse est le développement en langage C avec une librairie spécialisée du genre GMP, mais même dans ce cas, il existe toujours un risque lors des calculs de $\lceil x \rceil$ ou de $\lfloor x \rfloor$; idéalement, il ne faudrait faire les calculs qu'avec des entiers.

A titre l'exemple, page 31 du document [Normal Numbers With Respect to the Cantor Series Expansion](#)²² il est indiqué que l'expansion en série de Sylvester de π , commence par :

$$\pi = 3 + \frac{1}{8} + \frac{1}{61} + \frac{1}{5020} + \frac{1}{128541347} + \dots$$

ce qui est faux²³ (un calcul manuel montre que la somme de ces 5 termes est supérieure à π), les calculs fait avec ORACLE donne

$$\pi = 3 + \frac{1}{8} + \frac{1}{61} + \frac{1}{5020} + \frac{1}{128541455} + \dots$$

Dans la partie *Exemples* des Suites ci-dessous, la première colonne est la valeur exacte, littérale, d'une constante, la deuxième est le début du développement de cette constante, et, dans le cas des séries infinies, ou finies mais trop longues, la troisième colonne est le début du développement décimal donné par l'expansion de la suite, les décimales restituées sont les décimales correctes de la constante, ce qui donne une idée de la vitesse de convergence de la Série (ou Produit).

Dans les Séries ci-dessous, nous appelons « Constante Primaire », ou plus simplement « Primaire », la constante obtenu en affectant la plus petite valeur possible à chacun des éléments a_i des différentes suites, en respectant les conditions, et en ajoutant 1 si l'application systématique du minimum conduit à une forme simplifiable.

22. Partie d'une thèse pour un Ph. D. à « The Ohio State University ».

23. Il manque aussi le $\frac{1}{61}$, mais je mets cet oubli sur le compte d'une erreur de copie, dans la mesure où ce terme est nécessaire pour le calcul du terme suivant.

Par exemple pour la série de Engel, l'application des conditions donnerait $\langle 0, 2, 2, 2, 2, \bar{2} \rangle$, mais cette forme se simplifie, le Primaire est donc, dans ce cas $\langle 0, 2, 3, 4, 5, 6, \dots \rangle$.

Lorsque la constante Primaire est donnée uniquement sous forme d'un développement décimale, c'est que l'inverseur de Plouffe²⁴ n'a pas permis d'en déterminer une valeur littérale.

Le formalisme utilisé ici n'est pas universel, par exemple pour le développement en série de Engel de π , on trouve, dans la littérature $\pi = \langle 1, 1, 1, 8, 8, 17, 19, 300, 1991 \dots \rangle$, alors qu'ici nous noterons : $\pi = \langle 3, 8, 8, 17, 19, 300, 1991 \dots \rangle$, ce qui rend les comparaisons beaucoup plus simple.

24. [L'inverseur de Plouffe.](#)

Série de Engel.

Historique : Le développement des réels en Série de Engel a été étudié en 1913 par Friedrich Engel, un mathématicien allemand (1861 - 1941), mais le premier à avoir envisagé cette série est Jean-Henri Lambert un mathématicien français (1728 - 1777).

Définition : $a_0 + \frac{1}{a_1} + \frac{1}{a_1 a_2} + \frac{1}{a_1 a_2 a_3} + \dots + \left(\prod_{i=1}^n \frac{1}{a_i} \right) + \dots$

Conditions : $a_0 \in \mathbb{Z} \wedge \left(\bigwedge_{i \in \mathbb{N}^*} a_i \in \mathbb{N}^* \cup \{\omega\} \right)$
 : $\forall n \in \mathbb{N}^* (a_{n+1} \geq a_n > 1)$
 : $\exists \eta > 1 (a_{\eta-1} < a_\eta) \Rightarrow \langle a_0, a_1, a_2, \dots, a_{\eta-1}, \overline{a_\eta} \rangle = \langle a_0, a_1, a_2, \dots, a_{\eta-1}, a_\eta - 1, \overline{\omega} \rangle$
 : $\langle a_0, \overline{2} \rangle = \langle a_0 + 1, \overline{\omega} \rangle$
 : $a_1 > 2 \Rightarrow \langle a_0, \overline{a_1} \rangle = \langle a_0, a_1 - 1, \overline{\omega} \rangle$

	$a_0 = \lfloor x \rfloor$	$x_1 = x - a_0$
<i>Algorithme</i> :	$x_i = 0 \Rightarrow a_i = \omega$	$x_{i+1} = 0$
	$x_i \neq 0 \Rightarrow a_i = \left\lceil \frac{1}{x_i} \right\rceil$	$x_{i+1} = a_i \cdot x_i - 1$

Ordre : $a < b \Leftrightarrow \begin{cases} \eta_a^b = 0 \wedge a_0 < b_0 \\ \eta_a^b \neq 0 \wedge a_{\eta_a^b} > b_{\eta_a^b} \end{cases}$

Fonction \uparrow : $f(n) = n$

Unicité : La décomposition d'un réel en Série de Engel est unique.

Rationnels : $\widehat{\mathfrak{S}}^{<\omega} = \mathbb{Q}$

Exemples : $\frac{25}{29} = \langle 0, 2, 2, 3, 3, \overline{30} \rangle = \langle 0, 2, 2, 3, 3, 29, \overline{\omega} \rangle$

: $\pi = \langle 3, 8, 8, 17, 19, 300, 1991, 2492 \dots \rangle = 3,141592\dots$

: $e = \langle 2, 2, 3, 4, 5, 6, 7, 8, 9, 10, \dots \rangle = 2,7182818\dots$

: $\sqrt{2} = \langle 1, 3, 5, 5, 16, 18, 78, \dots \rangle = 1,4142135\dots$

: $\varphi = \langle 1, 2, 5, 6, 13, 16, 16, \dots \rangle = 1,618033\dots$

Primaire : $e - 2 = \langle 0, 2, 3, 4, 5, 6, 7, 8, 9, 10, \dots \rangle = 0,7182818\dots$

Série de Pierce.

Historique : Le développement des réels en Série de Pierce a été étudié en 1929 par T. A. Pierce, mais le premier à avoir envisagé cette série (en 1911) est Waclaw Franciszek Sierpiński un mathématicien polonais (1882 - 1969).
Ces séries ont été étudiées par **John et Arnold Knopfmacher** à partir de 1988.
On trouve parfois le nom de *Série Alternée de Engel*.

Définition : $a_0 + \frac{1}{a_1} - \frac{1}{a_1 a_2} + \frac{1}{a_1 a_2 a_3}, \dots + (-1)^{n+1} \cdot \left(\prod_{i=1}^n \frac{1}{a_i} \right) \dots$

Conditions : $a_0 \in \mathbb{Z} \wedge \left(\bigwedge_{i \in \mathbb{N}^*} a_i \in \mathbb{N}^* \cup \{\omega\} \right)$
 : $\forall n \in \mathbb{N}^* (a_{n+1} > a_n \geq 1)$
 : Pour $\eta > 0$: $\langle a_0, a_1, a_2, \dots, a_{\eta-1}, a_\eta, a_\eta + 1, \bar{\omega} \rangle = \langle a_0, a_1, a_2, \dots, a_{\eta-1}, a_\eta + 1, \bar{\omega} \rangle$

Algorithme :

	$a_0 = \lfloor x \rfloor$	$x_1 = x - a_0$
$x_i = 0 \Rightarrow$	$a_i = \omega$	$x_{i+1} = 0$
$x_i \neq 0 \Rightarrow$	$a_i = \left\lfloor \frac{1}{x_i} \right\rfloor$	$x_{i+1} = \left(\frac{1}{a_i} - x_i \right) \cdot a_i$

Ordre : $a < b \Leftrightarrow \begin{cases} \eta_a^b \in 2\mathbb{N} \wedge a_{\eta_a^b} < b_{\eta_a^b} \\ \eta_a^b \notin 2\mathbb{N} \wedge a_{\eta_a^b} > b_{\eta_a^b} \end{cases}$

Fonction \hat{f} : $f(n) = 2n$

Unicité : La décomposition d'un réel en Série de Pierce est unique.

Opposé : $a = \langle a_0, 1, a_2, \dots, a_n, \dots \rangle \Leftrightarrow -a = \langle -a_0 - 1, a_2, \dots, a_{n-1}, \dots \rangle$

Rationnels : $\widehat{\mathfrak{S}^{<\omega}} = \mathbb{Q}$

Exemples :

$\frac{25}{29}$	$= \langle 0, 1, 7, 28, 29, \bar{\omega} \rangle = \langle 0, 1, 7, 29, \bar{\omega} \rangle$	
π	$= \langle 3, 7, 112, 115, 157, 372, 432 \dots \rangle$	$= 3,14159265358979\dots$
e	$= \langle 2, 1, 3, 6, 14, 142, 327, 398, \dots \rangle$	$= 2,7182818284590\dots$
$\sqrt{2}$	$= \langle 1, 2, 5, 7, 197, 199 \dots \rangle$	$= 1,414213562373\dots$
φ	$= \langle 1, 1, 2, 4, 17, 19, 5777, 5779, \dots \rangle$	$= 1,61803398874989\dots$
<i>Primaire</i> : e^{-1}	$= \langle 0, 2, 3, 4, 5, 6, 7, 8, 9, 10, \dots \rangle$	$= 0,3678794 \dots$

Série de Sylvester.

Historique : Le développement des réels en Série de Sylvester a été étudié en 1880 par James Joseph Sylvester, un mathématicien anglais (1814 - 1897).
Ces séries ont été étudiées par **John et Arnold Knopfmacher** à partir de 1988.

Définition : $a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} + \dots + \frac{1}{a_n} + \dots$

Conditions :

- $a_0 \in \mathbb{Z} \wedge \left(\bigwedge_{i \in \mathbb{N}^*} a_i \in \mathbb{N}^* \cup \{\omega\} \right)$
- $\forall n \in \mathbb{N}^* ((a_{n+1} \geq a_n^2 - a_n + 1) \wedge (a_n > 1))$
- $\langle a_0, a_1, \dots, a_{n-1}, a_{n-1}, \bar{a}_n \rangle = \langle a_0, a_1, \dots, a_{n-1} - 1, \bar{\omega} \rangle$
- $\exists \eta \in \mathbb{N}^* \forall n \in \mathbb{N} ((n \geq \eta > 1) \Rightarrow (a_{n+1} = a_n^2 - a_n + 1) \Rightarrow$
 $(\langle a_0, a_1, a_2, \dots, a_{\eta-1}, a_\eta, a_{\eta+1}, \dots \rangle = \langle a_0, a_1, a_2, \dots, a_{\eta-1}, a_\eta - 1, \bar{\omega} \rangle)$
 $\langle a_0, 2, 3, 7, 43, \dots, (a_n^2 - a_n + 1), \dots \rangle = \langle a_0 + 1, \bar{\omega} \rangle$
 Pour $a_1 > 2$: $\langle a_0, a_1, (a_1^2 - a_1 + 1), \dots, (a_n^2 - a_n + 1), \dots \rangle = \langle a_0, a_1 - 1, \bar{\omega} \rangle$

Commentaire : C'est une forme particulière de fraction égyptienne.

	$a_0 = [x]$	$x_1 = x - a_0$
<i>Algorithme</i> :	$x_i = 0 \Rightarrow a_i = \omega$	$x_{i+1} = 0$
	$x_i \neq 0 \Rightarrow a_i = \left\lceil \frac{1}{x_i} \right\rceil$	$x_{i+1} = x_i - \frac{1}{a_i}$

Ordre : $a < b \Leftrightarrow \begin{cases} \eta_a^b = 0 \wedge a_0 < b_0 \\ \eta_a^b \neq 0 \wedge a_{\eta_a^b} > b_{\eta_a^b} \end{cases}$

Fonction ↗ : $f(n) = n$

Unicité : La décomposition d'un réel en Série de Sylvester est unique.

Rationnels : $\widehat{\mathfrak{S}^{<\omega}} = \mathbb{Q}$

Exemples :

- $\frac{25}{29} = \langle 0, 2, 3, 35, 6090, \bar{\omega} \rangle$
- $\pi = \langle 3, 8, 61, 5020, 128541455, \dots \rangle = 3,14159265358979 \dots$
- $e = \langle 2, 2, 5, 55, 9999, 3620211523, \dots \rangle = 2,7182818284590 \dots$
- $\sqrt{2} = \langle 1, 3, 13, 253, 218201, 61323543802, \dots \rangle = 1,41421356237309 \dots$
- $\varphi = \langle 1, 2, 9, 145, 37986, 2345721887, \dots \rangle = 1,618033988749 \dots$
- Primaires* : ? = $\langle 2, 4, 14, 184, 33674, 1133904604, \dots \rangle = 0,8268930514209280 \dots$

Série Alternée de Sylvester.

Historique : Le développement des réels en Série Alternée de Sylvester ont été étudiées par **John et Arnold Knopfmacher** à partir de 1988.

Définition : $a_0 + \frac{1}{a_1} - \frac{1}{a_2} + \frac{1}{a_3}, \dots + \frac{(-1)^{n+1}}{a_n} \dots$

Conditions : $a_0 \in \mathbb{Z} \wedge \left(\bigwedge_{i \in \mathbb{N}^*} a_i \in \mathbb{N}^* \cup \{\omega\} \right)$
 : $\forall n \in \mathbb{N}^* ((a_{n+1} \geq a_n(a_n + 1)) \wedge (a_n \geq 1))$
 : $\langle a_0, a_1, a_2, \dots, a_{n-1}, a_n, a_n(a_n + 1), \bar{\omega} \rangle = \langle a_0, a_1, a_2, \dots, a_{n-1}, a_n + 1, \bar{\omega} \rangle$

Algorithme :

	$a_0 = \lfloor x \rfloor$	$x_1 = x - a_0$
$x_i = 0 \Rightarrow$	$a_i = \omega$	$x_{i+1} = 0$
$x_i \neq 0 \Rightarrow$	$a_i = \left\lfloor \frac{1}{x_i} \right\rfloor$	$x_{i+1} = \left(\frac{1}{a_i} - x_i \right)$

Ordre : $a < b \Leftrightarrow \begin{cases} \eta_a^b \in 2\mathbb{N} \wedge a_{\eta_a^b} < b_{\eta_a^b} \\ \eta_a^b \notin 2\mathbb{N} \wedge a_{\eta_a^b} > b_{\eta_a^b} \end{cases}$

Fonction ↗ : $f(n) = 2n$

Unicité : La décomposition d'un réel en Série de Sylvester Alternée est unique.

Opposé : $a = \langle a_0, 1, a_2, \dots, a_n, \dots \rangle \Leftrightarrow -a = \langle -a_0 - 1, a_2, \dots, a_{n-1}, \dots \rangle$

Rationnels : $\widehat{\mathfrak{S}^{<\omega}} = \mathbb{Q}$

Exemples :

$\frac{25}{29}$	$= \langle 0, 1, 7, 202, 41006, \bar{\omega} \rangle = \langle 0, 1, 7, 203, \bar{\omega} \rangle$: $(41006 = 202 \times 203)$
π	$= \langle 3, 7, 790, 749896, \dots \rangle$	$= 3,1415926535\dots$
e	$= \langle 2, 1, 3, 19, 983, 1140455, \dots \rangle$	$= 2,718281828459\dots$
$\sqrt{2}$	$= \langle 1, 2, 11, 195, 180120, \dots \rangle$	$= 1,4142135623\dots$
φ	$= \langle 1, 1, 2, 8, 143, 37042, 1563518960, \dots \rangle$	$= 1,61803398874989\dots$
<i>Primaire</i>	$? = \langle 1, 1, 2, 6, 42, 1806, 3263442, \dots \rangle$	$= 1,64285714285714\dots$

Série de Lüroth.

Historique : Le développement des réels en Série de Lüroth ont été introduites en 1883 par Jacob Lüroth, un mathématicien allemand (1844 - 1910).

Définition : $a_0 + \frac{1}{a_1} + \frac{1}{a_1(a_1-1)a_2} + \dots + \left(\prod_{i=1}^{n-1} \frac{1}{a_i(a_i-1)} \right) \frac{1}{a_n} + \dots$

Conditions : $a_0 \in \mathbb{Z} \wedge \left(\bigwedge_{i \in \mathbb{N}^*} a_i \in \mathbb{N}^* \cup \{\omega\} \right)$
 : $\forall n \in \mathbb{N}^* (a_n > 1)$

	$a_0 = \lfloor x \rfloor$	$x_1 = x - a_0$
<i>Algorithme</i> :	$x_i = 0 \Rightarrow a_i = \omega$	$x_{i+1} = 0$
	$x_i \neq 0 \Rightarrow a_i = \left\lfloor \frac{1}{x_i} \right\rfloor$	$x_{i+1} = (a_i - 1) \cdot (a_i x_i - 1)$

Ordre : $a < b \Leftrightarrow \begin{cases} \eta_a^b = 0 \wedge a_0 < b_0 \\ \eta_a^b \neq 0 \wedge a_{\eta_a^b} > b_{\eta_a^b} \end{cases}$

Fonction ↗ : $f(n) = n$

Unicité : La décomposition d'un réel en Série de Lüroth est unique.

Rationnels : $\widehat{\mathfrak{S}} = \mathbb{Q}$

Exemples :

$\frac{25}{29}$	$= \langle 0, 2, \overline{2, 3, 2, 3, 4, 4} \rangle$	
π	$= \langle 3, 8, 2, 2, 2, 3, 2, 5, 24, \dots \rangle$	$= 3,1415926 \dots$
e	$= \langle 2, 2, 3, 2, 5, 2, 2, 10, \dots \rangle$	$= 2,718281 \dots$
$\sqrt{2}$	$= \langle 1, 3, 3, 2, 2, 2, 4, 2, \dots \rangle$	$= 1,4142 \dots$
φ	$= \langle 1, 2, 5, 2, 3, 2, 4, 2, \dots \rangle$	$= 1,6180 \dots$
$n > 1 \Rightarrow$	$\langle 0, \bar{n} \rangle$	$= \frac{n-1}{n^2-n-1}$

Primaire : $1 = \langle 0, 2, 2, 2, 2, 2, \dots \rangle = 0,99999 \dots$

Série Alternée de Lüroth.

Historique : Le développement des réels en Série Alternée de Lüroth ont été étudiées par **John et Arnold Knopfmacher** à partir de 1988. Ces séries ont aussi été étudiées par Chryssoula Ganatsiou, une mathématicienne grecque à partir de 2000.

Définition :
$$a_0 + \frac{1}{a_1} - \frac{1}{(a_1+1)a_1a_2} + \dots + (-1)^{n+1} \cdot \left(\prod_{i=1}^{n-1} \frac{1}{a_i(a_i+1)} \right) \frac{1}{a_n} + \dots$$

Conditions :
$$a_0 \in \mathbb{Z} \wedge \left(\bigwedge_{i \in \mathbb{N}^*} a_i \in \mathbb{N}^* \cup \{\omega\} \right)$$

 : $\forall n \in \mathbb{N}^* (a_n \geq 1)$
 Pour $\eta > 0$: $\langle a_0, a_1, a_{\eta-1}, a_\eta, 1, \bar{\omega} \rangle = \langle a_0, a_1, a_{\eta-1}, a_\eta + 1, \bar{\omega} \rangle$

Algorithme :

	$a_0 = \lfloor x \rfloor$	$x_1 = x - a_0$
$x_i = 0 \Rightarrow$	$a_i = \omega$	$x_{i+1} = 0$
$x_i \neq 0 \Rightarrow$	$a_i = \left\lfloor \frac{1}{x_i} \right\rfloor$	$x_{i+1} = (a_i + 1)(1 - x_i a_i)$

Ordre :
$$a < b \Leftrightarrow \begin{cases} \eta_a^b \in 2\mathbb{N} \wedge a_{\eta_a^b} < b_{\eta_a^b} \\ \eta_a^b \notin 2\mathbb{N} \wedge a_{\eta_a^b} > b_{\eta_a^b} \end{cases}$$

Fonction \uparrow : $f(n) = 2n$

Unicité : La décomposition d'un réel en Série Alternée de Lüroth est unique.

Rationnels : $\widehat{\mathfrak{S}} = \mathbb{Q}$

Exemples :

$\frac{25}{29}$	$= \langle 0, 1, 3, \overline{1, 1, 1, 2, 9} \rangle$	
	$\pi = \langle 3, 7, 14, 7, 1, 1, 1, 15, \dots \rangle$	$= 3,14159265\dots$
	$e = \langle 2, 1, 1, 1, 3, 1, 11, 7, 2, 4, 12, 3, \dots \rangle$	$= 2,7182818284\dots$
	$\sqrt{2} = \langle 1, 2, 1, 1, 16, 1, 36, 15, \dots \rangle$	$= 1,414213562\dots$
	$\varphi = \langle 1, 1, 1, 2, 5, 1, 32, 4, 1, \dots \rangle$	$= 1,61803398\dots$
	$n \geq 1 \Rightarrow \langle 0, \bar{n} \rangle$	$= \frac{n+1}{n^2+n+1}$
<i>Primaire</i>	$\frac{2}{3} = \langle 0, 1, 1, 1, 1, 1, 1, 1, 1, \dots \rangle$	$= 0,66\dots$

Série de Knopfmacher.

Historique : Le développement des réels en série de Knopfmacher a été étudié à partir de 1989 par John Peter Louis Knopfmacher, un mathématicien sud-africain (1937 - 1999), et son fils Arnold Knopfmacher (1961 -), qui lui avaient donné le nom de « Série Alternée de Engel Modifiée ». Ils ont travaillé aussi sur ce sujet avec une mathématicienne grecque, Sofia Kalpazidou.

Définition : $a_0 + \frac{1}{a_1} - \frac{1}{(a_1+1)a_2} + \dots + (-1)^{n+1} \cdot \left(\prod_{i=1}^{n-1} \frac{1}{(a_i+1)} \right) \frac{1}{a_n} + \dots$

Conditions : $a_0 \in \mathbb{Z} \wedge \left(\bigwedge_{i \in \mathbb{N}^*} a_i \in \mathbb{N}^* \cup \{\omega\} \right)$
 $\forall n \in \mathbb{N}^* (a_{n+1} \geq a_n \geq 1)$
 Pour $\eta > 0$: $\langle a_0, a_1, a_{\eta-1}, a_\eta, a_\eta, \bar{\omega} \rangle = \langle a_0, a_1, a_{\eta-1}, a_\eta + 1, \bar{\omega} \rangle$

Algorithme :

	$a_0 = \lfloor x \rfloor$	$x_1 = x - a_0$
$x_i = 0 \Rightarrow$	$a_i = \omega$	$x_{i+1} = 0$
$x_i \neq 0 \Rightarrow$	$a_i = \left\lfloor \frac{1}{x_i} \right\rfloor$	$x_{i+1} = \left(\frac{1}{a_i} - x_i \right) (a_i + 1)$

Ordre : $a < b \Leftrightarrow \begin{cases} \eta_a^b \in 2\mathbb{N} \wedge a_{\eta_a^b} < b_{\eta_a^b} \\ \eta_a^b \notin 2\mathbb{N} \wedge a_{\eta_a^b} > b_{\eta_a^b} \end{cases}$

Fonction \hat{f} : $f(n) = 2n$

Unicité : La décomposition d'un réel en Série de Knopfmacher est unique.

Rationnels : $\mathfrak{S} \not\subseteq \mathbb{Q}$

Exemples :

$\frac{25}{29}$	$=$	$\langle 0, 1, 3, 4, 9, 9, 17, 41, \bar{\omega} \rangle$	
π	$=$	$\langle 3, 7, 98, 114, 200, 331, 349, 549, \dots \rangle$	$= 3,14159265358979\dots$
e	$=$	$\langle 2, 1, 1, 1, 3, 3, 16, 22, 25, 38, \dots \rangle$	$= 2,718281828\dots$
$\sqrt{2}$	$=$	$\langle 1, 2, 3, 3, 8, 15, 44, 109, 1396, \dots \rangle$	$= 1,41421356237309\dots$
φ	$=$	$\langle 1, 1, 1, 2, 11, 11, 26, 31, 1794, \dots \rangle$	$= 1,618033988749\dots$
$n \geq 1 \Rightarrow$	$\langle 0, \bar{n} \rangle$		$= \frac{n+1}{n^2+2n}$
$n \geq 2 \Rightarrow$	$\langle 0, n, 2n-1, 2n^2-1, 2(2n^2-1)-1, \dots \rangle$		$= \frac{2}{2n+1}$

Primaire : ? $= \langle 0, 1, 2, 3, 4, 5, 6, 7, 8, \dots \rangle = 0,796599599297053\dots$

Le dernier exemple montre qu'il existe des nombres rationnels dont le développement en série de Knopfmacher n'est pas périodique.

La définition complète de cet exemple est :

$$\begin{cases} a_0 & = 0 \\ a_1 & = n \geq 2 \\ a_{2n} & = 2a_{2n-1} - 1 \\ a_{2n+1} & = 2a_{2n-1}^2 - 1 \end{cases}$$

Produit de Cantor.

Historique : Le développement des réels en produit de Cantor a été étudié à partir de 1869 par Georg Ferdinand Ludwig Philip Cantor, un mathématicien allemand (1845 - 1918).

Définition : $\frac{1}{a_0} \cdot \left(1 + \frac{1}{a_1}\right) \cdot \left(1 + \frac{1}{a_2}\right) \cdot \left(1 + \frac{1}{a_3}\right) \cdot \dots \cdot \left(1 + \frac{1}{a_n}\right) \cdot \dots$

Conditions :

- $a_0 \in \mathbb{N}^* \wedge \left(\bigwedge_{i \in \mathbb{N}^*} a_i \in \mathbb{N}^* \cup \{\omega\}\right)$
- $\forall n \in \mathbb{N}^* (a_{n+1} \geq a_n^2 \geq 1)$
- $\exists \eta \forall n ((n \geq \eta) \Rightarrow (a_n > 1))$
- $(a_1 = 1) \Rightarrow (a_0 \notin 2\mathbb{N})$
- $\exists \eta \in \mathbb{N}^* \forall n \in \mathbb{N} ((n \geq \eta > 1) \Rightarrow (a_{n+1} = a_n^2) \Rightarrow$
 $(\langle a_0, a_1, a_2, \dots, a_{\eta-1}, a_\eta, a_{\eta+1}, \dots \rangle = \langle a_0, a_1, a_2, \dots, a_{\eta-1}, a_\eta - 1, \bar{\omega} \rangle))$

	$a_0 = \left\lfloor \frac{1}{x} \right\rfloor$	$x_1 = a_0 \cdot x$
<i>Algorithme</i> :	$x_i = 1 \Rightarrow a_i = \omega$	$x_{i+1} = 0$
	$x_i \neq 1 \Rightarrow a_i = \left\lfloor \frac{x_i}{x_i - 1} \right\rfloor$	$x_{i+1} = \frac{x_i}{1 + \frac{1}{a_i}}$

Ordre : $a < b \Leftrightarrow \begin{cases} \eta_a^b = 0 \wedge a_{\eta_a^b} > b_{\eta_a^b} \\ \eta_a^b \neq 0 \wedge a_{\eta_a^b} > b_{\eta_a^b} \end{cases}$

Fonction ↗ : $f(n) = n$

Unicité : La décomposition d'un réel strictement positif en Produit de Cantor est unique.

Rationnels : $\widehat{\mathfrak{S}}^{<\omega} = \mathbb{Q}$

Exemples :

- $\frac{25}{29} = \langle 2, 2, 7, 175, 30625, \dots \rangle = \langle 2, 2, 7, 174, \bar{\omega} \rangle$
- $\pi = \langle 1, 1, 2, 22, 600, 1800856, \dots \rangle = 3,141592653589\dots$
- $e = \langle 1, 1, 3, 52, 8160, 95179273, \dots \rangle = 2,7182818284590\dots$
- $\sqrt{2} = \langle 1, 3, 17, 577, 665857, 886731088897, \dots \rangle = 1,41421356237309\dots$
- $\varphi = \langle 1, 2, 13, 610, 1346269, 6557470319842, \dots \rangle = 1,618033988749\dots$
- $n > 1 \Rightarrow \langle 1, n, 2n^2 - 1, 2(2n^2 - 1)^2 - 1, \dots \rangle = \sqrt{\frac{n+1}{n-1}}$

Primaires : ? = $\langle 1, 2, 5, 26, 677, 458330, \dots \rangle = 1,8719959034\dots$

Produit Alterné de Cantor

Historique : Le développement des réels en Produit Alterné de Cantor a été étudié à partir de 1989 par John Peter Louis Knopfmacher, un mathématicien sud-africain (1937 - 1999), et son fils Arnold Knopfmacher (1961 -).

Définition : $2^{a_0} \left(1 + \frac{1}{a_1}\right) \cdot \left(1 - \frac{1}{a_2}\right) \cdot \left(1 + \frac{1}{a_3}\right) \cdot \dots \cdot \left(1 + \frac{(-1)^{n-1}}{a_n}\right) \dots$

Conditions : $a_0 \in \mathbb{Z} \wedge \left(\bigwedge_{i \in \mathbb{N}^*} a_i \in \mathbb{N}^* \cup \{\omega\}\right)$
 : $\forall n \in \mathbb{N}^* (a_{n+1} \geq (a_n + 1) \cdot (a_n + (-1)^{n-1}))$
 $\langle a_0, a_1, \dots, a_{2\eta-1}, a_{2\eta}, a_{2\eta}^2 - 1, \bar{\omega} \rangle = \langle a_0, a_1, \dots, a_{2\eta-1}, a_{2\eta} + 1, \bar{\omega} \rangle$
 $\langle a_0, a_1, \dots, a_{2\eta}, a_{2\eta+1}, (a_{2\eta+1} + 1)^2, \bar{\omega} \rangle = \langle a_0, a_1, \dots, a_{2\eta}, a_{2\eta+1} + 1, \bar{\omega} \rangle$
 : $x \in \mathbb{R}^{+\star}$

Algorithme :

	$a_0 = \lfloor \log_2(x) \rfloor$	$x_1 = \frac{x}{2^{a_0}}$
$x_i = 1 \Rightarrow$	$a_i = \omega$	$x_{i+1} = 1$
$x_i \neq 1 \Rightarrow$	$a_i = \left\lfloor \frac{(-1)^{i-1}}{x_i - 1} \right\rfloor$	$x_{i+1} = \frac{x_i}{1 + \frac{(-1)^{i-1}}{a_i}}$

Ordre : $a < b \Leftrightarrow \begin{cases} \eta_a^b \in 2\mathbb{N} \wedge a_{\eta_a^b} < b_{\eta_a^b} \\ \eta_a^b \notin 2\mathbb{N} \wedge a_{\eta_a^b} > b_{\eta_a^b} \end{cases}$

Fonction ↗ : $f(n) = 2n$

Unicité : La décomposition d'un réel strictement positif en Produit Alterné de Cantor existe et est unique.

Inverse : $a = \langle a_0, 1, a_2, \dots, a_{2n-1}, a_{2n}, a_{2n+1}, \dots \rangle \Leftrightarrow$
 $a^{-1} = \langle -a_0 - 1, a_2 - 1, a_3 + 1, \dots, a_{2n} - 1, a_{2n+1} + 1, a_{2n+2} - 1, \dots \rangle$

Rationnels : $\widehat{\mathfrak{S}}^{<\omega} = \mathbb{Q}$

Exemples :

$\frac{25}{29}$	$= \langle -1, 1, 7, 174, \bar{\omega} \rangle$	
π	$= \langle 1, 1, 4, 21, 2485, 12983006, \dots \rangle$	$= 3,141592653589\dots$
e	$= \langle 1, 2, 10, 147, 31786, 1122846592, \dots \rangle$	$= 2,7182818284590\dots$
$\sqrt{2}$	$= \langle 0, 2, 17, 576, 665857, 886731088896, \dots \rangle$	$= 1,41421356237309\dots$
φ	$= \langle 0, 1, 5, 88, 10946, 433494436, \dots \rangle$	$= 1,618033988749\dots$
<i>Primaire</i>	$? = \langle 0, 1, 5, 25, 677, 458329, \dots \rangle$	$= 1,661545722\dots$

Produit Négatif de Cantor.

Historique : Une définition de ce produit infini fut donnée par Vincent Granville en 2010, mais avec une définition très insuffisante; la définition utilisée ci-dessous, ainsi que les démonstrations sont de l'auteur de ce document.

Définition : $2^{a_0} \cdot \left(1 - \frac{1}{a_1}\right) \left(1 - \frac{1}{a_2}\right) \left(1 - \frac{1}{a_3}\right) \dots \left(1 - \frac{1}{a_n}\right) \dots$

Conditions : $a_0 \in \mathbb{Z} \wedge \left(\bigwedge_{i \in \mathbb{N}^*} a_i \in \mathbb{N}^* \cup \{\omega\}\right)$
 : $\forall n \in \mathbb{N}^* ((a_n > 2) \wedge (a_{n+1} > (a_n - 1)^2))$
 : $\exists \eta \in \mathbb{N}^* \forall n \in \mathbb{N} ((n > \eta > 1) \Rightarrow (a_{n+1} = (a_n - 1)^2 + 1)) \Rightarrow$
 $\langle a_0, a_1, a_2, \dots, a_{\eta-1}, a_\eta, a_{\eta+1}, \dots \rangle = \langle a_0, a_1, a_2, \dots, a_{\eta-1}, a_\eta - 1, \bar{\omega} \rangle$
 $\langle a_0, 3, 5, 17, \dots, (a_n - 1)^2 + 1, \dots \rangle = \langle a_0 - 1, \bar{\omega} \rangle$
 Pour $a_1 > 3$: $\langle a_0, a_1, (a_1 - 1)^2 + 1, \dots, (a_n - 1)^2 + 1, \dots \rangle = \langle a_0, a_1 - 1, \bar{\omega} \rangle$

	$a_0 = \lceil \log_2(x) \rceil$	$x_1 = \frac{x}{2^{a_0}}$
<i>Algorithme</i> :	$x_i = 1 \Rightarrow a_i = \omega$	$x_{i+1} = 0$
	$x_i \neq 1 \Rightarrow a_i = \left\lceil \frac{1}{1 - x_i} \right\rceil$	$x_{i+1} = \frac{x_i}{\left(1 - \frac{1}{a_i}\right)}$

Ordre : $a < b \Leftrightarrow \begin{cases} \eta_a^b = 0 \wedge a_{\eta_a^b} < b_{\eta_a^b} \\ \eta_a^b \neq 0 \wedge a_{\eta_a^b} < b_{\eta_a^b} \end{cases}$

Fonction \setminus : $f(n) = n$

Unicité : La décomposition d'un réel strictement positif en Produit Négatif de Cantor existe et est unique.

Rationnels : $\widehat{\mathfrak{S}}^{<\omega} = \mathbb{Q}$

Exemples : $\frac{25}{29} = \langle 0, 8, 68, 13601, \bar{\omega} \rangle$
 : $\pi = \langle 2, 5, 55, 13931, 2811273900 \dots \rangle = 3, 14159265358979 \dots$
 : $e = \langle 2, 4, 11, 304, 138640 \dots \rangle = 2, 718281828 \dots$
 : $\sqrt{2} = \langle 1, 4, 18, 578, 665858 \dots \rangle = 1, 41421356237 \dots$
 : $\varphi = \langle 1, 6, 35, 1598, 3524579, \dots \rangle = 1, 618033988749 \dots$
Primaire : ? = $\langle 0, 3, 6, 27, 678, 458331, \dots \rangle = 0, 534189203156132 \dots$

Série Binaire Spéciale.

Définition : $a_0 + \frac{1}{2^{a_1}} + \frac{1}{2^{a_2}} + \frac{1}{2^{a_3}}$

Conditions : $a_0 \in \mathbb{Z} \wedge \left(\bigwedge_{i \in \mathbb{N}^*} a_i \in \mathbb{N}^* \cup \{\omega\} \right)$

: $\forall n \in \mathbb{N}^* (a_{n+1} > a_n)$

: $\exists \eta \forall n ((\eta > 1) \wedge (a_{\eta-1} + 1 < a_\eta) \wedge ((n \geq \eta) \Rightarrow (a_{n+1} = a_n + 1)) \Rightarrow$
 $(\langle a_0, a_1, a_2, \dots, a_{\eta-1}, a_\eta, a_{\eta+1}, \dots \rangle = \langle a_0, a_1, a_2, \dots, a_{\eta-1}, a_\eta - 1, \bar{\omega} \rangle)$
 $\langle a_0, 1, 2, 3, 4, \dots, (a_n + 1), \dots \rangle = \langle a_0 + 1, \bar{\omega} \rangle$
 Pour $a_1 > 1$: $\langle a_0, a_1, (a_1 + 1), \dots, (a_n + 1), \dots \rangle = \langle a_0, a_1 - 1, \bar{\omega} \rangle$

	$a_0 = \lfloor x \rfloor$	$x_1 = x - a_0$
<i>Algorithme</i> :	$x_i = 0 \Rightarrow a_i = \omega$	$x_{i+1} = 0$
	$x_i \neq 0 \Rightarrow a_i = \left\lceil \log_2 \left(\frac{1}{x_i} \right) \right\rceil$	$x_{i+1} = x_i - \frac{1}{2^{a_i}}$

Ordre : $a < b \Leftrightarrow \begin{cases} \eta_a^b = 0 \wedge a_{\eta_a^b} < b_{\eta_a^b} \\ \eta_a^b \neq 0 \wedge a_{\eta_a^b} > b_{\eta_a^b} \end{cases}$

Fonction \uparrow : $f(n) = n$

Unicité : Le développement en Série Binaire Spéciale d'un nombre réel (qui n'est pas exactement le développement en base 2) est unique.

Rationnels : $\widehat{\mathfrak{S}}^\delta = \mathbb{Q}$

Exemples : $\frac{25}{29} = \langle 0, 1, 2, 4, 5, 6, 9, 11, 12, 17, \dots \rangle = 0,862068\dots$

: $\pi = \langle 3, 3, 6, 11, 12, 13, 14, 15, 16, 18, \dots \rangle = 3,1415\dots$

: $e = \langle 2, 1, 3, 4, 6, 7, 8, 9, \dots \rangle = 2,71\dots$

: $\sqrt{2} = \langle 1, 2, 3, 5, 7, 13, 16, \dots \rangle = 1,414\dots$

: $\varphi = \langle 1, 1, 4, 5, 6, 7, 11, 12, \dots \rangle = 1,61\dots$

Primaire : $\frac{2}{3} = \langle 0, 1, 3, 5, 7, 9, 11, 13 \dots \rangle = 0,6666\dots$

On peut prolonger cette idée en étudiant d'autres suites, par exemple, Chrysoula Ganatsiou et Perakis Konstantinos ont proposé en 2010 la série

$$x = a_0 + \frac{1}{a_1} - \left(1 + \frac{1}{a_1}\right) \cdot \frac{1}{a_2} + \left(1 + \frac{1}{a_1}\right) \cdot \left(1 - \frac{1}{a_2}\right) \cdot \frac{1}{a_3} + \dots + (-1)^{n+1} \cdot \left(\prod_{i=1}^{n-1} \left(1 + \frac{(-1)^i}{a_{i-1}}\right)\right) \cdot \frac{1}{a_n} + \dots$$

On peut aussi envisager l'expansion factorielle :

$$x = \frac{a_0}{0!} + \frac{a_1}{1!} + \frac{a_2}{2!} + \dots + \frac{a_n}{n!} + \dots$$

Par exemple $\pi = \langle 3, 0, 0, 0, 3, 1, 5, 6, 5, 0, 1, 4, 7, 8, 0, 6, 7, 10, \dots \rangle$

Ou encore la β -expansion :

Soit $\beta > 1$ un réel, $a_0 \in \mathbb{Z}$ et pour a_i des entiers naturels tels que $\forall i((i > 0) \Rightarrow (a_i \in \{0, 1, \dots, \lfloor \beta \rfloor\}))$:

$$x = a_0 + \frac{a_1}{\beta} + \frac{a_1}{\beta^2} + \dots$$

Un cas particulier a été particulièrement étudié : $\beta = \varphi = \frac{1 + \sqrt{5}}{2}$.

Une variation sur le nombre d'or, et qui n'a pas été étudié à ma connaissance :

On note F_n le $n^{\text{ième}}$ nombre de la suite de Fibonacci :

$$x = a_0 + F_0/F_{n_1} + F_{n_1}/F_{n_2} + F_{n_2}/F_{n_3} + \dots$$

Qui peut se représenter par la suite (a_0, n_1, n_2, \dots) où $a_0 \in \mathbb{Z}$ et les $a_i \in \mathbb{N}^*$.

f-Expansion.

L'idée des f -Expansion fut proposée par Barnard H. Bissinger (un mathématicien américain (1918 - 2011)) en 1944, pas spécifiquement pour mettre au point des méthodes de construction des réels, mais, l'idée peut être exploitée dans ce sens.

Bissinger a remarqué que le développement d'un réel en fractions continues était de la forme :

$$x = a_0 + f(a_1 + f(a_2 + f(a_3 + \dots)))$$

Avec, dans le cas des fractions continues $f(x) = \frac{1}{x}$.

Le travail de Bissinger a été de trouver des conditions sur f pour qu'un développement de la forme ci-dessus existe pour tout $x \in \mathbb{R}$ et soit unique.

1. $f : [1, \infty[\mapsto \mathbb{R}$
2. $f(1) = 1$
3. $\forall x \forall y ((1 \leq x < y) \Rightarrow (f(x) > f(y) > 0))$
4. $\lim_{x \rightarrow \infty} f(x) = 0$
5. $\forall x \forall y ((1 \leq x < y) \Rightarrow (|f(y) - f(x)| < |y - x|))$
6. $\exists \lambda \forall x \forall y ((0 < \lambda < 1) \wedge ((1 + f(2) < x < y) \Rightarrow (|f(y) - f(x)| < \lambda^2 |y - x|)))$

Un tel développement vérifiant en plus que l'image d'un rationnel soit un rationnel, permet, a priori de construire $(\mathbb{R}, +, \times, <)$.

On peut aussi envisager une méthode plus « géométrique » en utilisant l'expansion de János Bolyai (un mathématicien hongrois 1802 - 1860) à l'aide de radicaux imbriqués :

$$\forall x \in \mathbb{R} \exists a \in \{0, 1, 2\}^{\mathbb{N}} \left(x = a_0 + \sqrt{a_1 + \sqrt{a_2 + \dots \sqrt{a_n + \dots}}} \right)$$

Cette méthode est assez différente des précédentes dans la mesure où les suites finies ne correspondent pas à des nombres rationnels, ce qui empêche de faire les calculs simplement, néanmoins les suites finies

correspondent à des **nombres constructibles**, on peut donc faire le même genre de construction, mais de façon géométrique, c'est à dire que cette méthode permet de construire les réels avec une règle et un compas (avec une infinité de mouvements, et pour être honnête, toutes les méthodes à base de suites de rationnels (qui sont constructibles) permettent aussi une construction géométrique).

Par exemple, on obtient $\pi = \langle 2, 3, 1, 1, 0, 1, 2, 1, 0, 0, 1, 1, 2, 1, 0, \dots \rangle$, ce qui explicite un moyen de résoudre la quadrature du cercle (avec une infinité de tracés, et en commençant par le dernier).

II.5.7 Développement Décimal.

Construction de Rota.

La construction de Rota est due à Gian-Carlo Rota en 1974, un mathématicien américain (1932 - 1999), elle permet de passer de \mathbb{Z} à \mathbb{R} sans passer par \mathbb{Q} . Il s'agit essentiellement d'une méthode basée sur un pseudo-développement binaire²⁵ d'un nombre, manipulé comme une suite de nombres entiers relatifs.

Soit $\mathfrak{C} = \{\langle \dots, a_{-n}, \dots (a_{-2})(a_{-1})(a_0) \cdot (a_1)(a_2) \dots \rangle\}$ ²⁶ tel qu'en dessous d'un certain rang, tous les a_i sont nuls (autrement dit il n'y a qu'un nombre fini de « chiffres » à gauche de la virgule) :

$$\exists \eta \forall i ((i < \eta) \Rightarrow (a_i = 0))$$

On peut définir très facilement une addition et une multiplication sur \mathfrak{C} (c'est un sous-ensemble de $\mathbb{Z}^{\mathbb{Z}}$) :

On pose $a = \langle a_i \rangle_{i \in \mathbb{Z}}$ et $b = \langle b_i \rangle_{i \in \mathbb{Z}}$.

$$a + b = \langle a_i + b_i \rangle_{i \in \mathbb{Z}}$$

$$a \times b = \left\langle \sum_{j=0}^i a_j \cdot b_{i-j} \right\rangle_{i \in \mathbb{Z}}$$

Il est immédiat que $(\mathfrak{C}, +, \times)$ est un anneau commutatif.

Il s'agit d'un pseudo développement binaire dans la mesure où l'idée est que $\langle a_i \rangle_{i \in \mathbb{Z}}$ doit représenter le réel $x = \sum_{i \in \mathbb{Z}} a_i 2^{-i}$, sauf que les a_i peuvent être n'importe quel entier relatif.

On pose $\mathbb{K} = \langle \dots (0)(1) \cdot (-2)(0) \dots \rangle$.

On peut constater immédiatement qu'avec l'interprétation précédente, \mathbb{K} représente $1 + \frac{-2}{2}$, c'est à dire 0 (on sent venir un idéal et le quotient qui va avec).

Un élément $a = \langle a_i \rangle_{i \in \mathbb{Z}}$ de \mathfrak{C} est dit borné si :

$$\exists N \in \mathbb{Z} \forall n \in \mathbb{Z} \left(\sum_{i \leq n} |a_i| 2^{n-i} \leq N 2^n \right)$$

On remarquera que cette définition ne fait intervenir aucun nombre rationnel qui ne soit un entier relatif.

Nous noterons $\widehat{\mathfrak{C}}$ le sous ensemble de \mathfrak{C} constitué des chaînes bornées $((\widehat{\mathfrak{C}}, +, \times)$ est un sous-anneau de $(\mathfrak{C}, +, \times)$.

On définit une relation d'équivalence sur $\widehat{\mathfrak{C}}$:

$$\forall a \forall b ((a \sim b) \Leftrightarrow \exists c (a = b + \mathbb{K}c))$$

Où $\mathbb{K}c$ est bornée et $\forall N \in \mathbb{N} \exists \eta \forall i ((i > \eta) \Rightarrow (N|c_i| \leq 2^i))$

Voici le quotient (et l'idéal principal) dont il était question plus haut ; $\mathbb{K}c$ est appelé « Chaîne de retenues » (Carry-string en anglais).

Une première remarque²⁷ :

- $\langle (0) \cdot \overline{(1)} \rangle$ est bornée.
- $\langle (1) \cdot \overline{(1)} \rangle$ est bornée.
- $\mathbb{K} \times \langle (1) \cdot \overline{(1)} \rangle = \langle (1) \cdot \overline{(-1)} \rangle$
- $\langle (1) \cdot \overline{(0)} \rangle = \langle (0) \cdot \overline{(1)} \rangle + \mathbb{K} \times \langle (1) \cdot \overline{(1)} \rangle$

Certains auront sans doute reconnu que ceci démontre de façon très simple que $0, \overline{9} = 1$, ou plutôt son équivalent en base 2, dans le quotient $\widehat{\mathfrak{C}} / \sim$.

La notion de chaîne bornée est nécessaire pour ne pas avoir à gérer « trop » de retenues, par exemple, on peut vérifier très simplement que $\langle (1) \cdot \overline{} \rangle = \langle (0) \cdot \overline{} \rangle + \mathbb{K} \langle (1) \cdot \overline{(2)(4)(8) \dots (2^n)} \rangle$ (autrement dit $0 = 1$, semble-t-il),

25. Cela marcherait avec n'importe quelle base.

26. Le point \cdot ne sera utilisé que pour enlever toute ambiguïté lorsque nécessaire.

27. Les (0) initiaux ne seront pas notés s'il n'y a pas d'ambiguïté, et nous utiliserons les conventions habituelles pour les suites périodiques

mais on peut tout aussi facilement montrer que la chaîne $c = \langle (1) \cdot (2)(4)(8) \cdots (2^n) \rangle$ ne vérifie pas les conditions de la relation d'équivalence puisque $N|c_i| \leq 2^i \Leftrightarrow N \leq 1$ qui n'est pas vérifié pour tous les entiers N .

Cela semble nous amener une fois de plus à la définition des réels comme des classes d'équivalence, à un détail près néanmoins, c'est que dans chaque classe il y a un élément privilégié. L'addition et la multiplication passe au quotient sans problème, de plus la relation d'ordre est facile à définir sur les chaînes propres (néanmoins les opérations ne fonctionnent bien que sur les classes).

Soit $\mathfrak{R} = \{ \langle \cdots, a_{-n}, \cdots, a_2, a_1, a_0, a_1, a_2, \cdots \rangle \}$ avec les propriétés suivantes :

$$\begin{aligned} \exists \eta \forall i ((a_\eta \in \{-1, 1\}) \wedge ((a_\eta = -1) \Rightarrow (a_{\eta+1} = 0)) \wedge ((i < \eta) \Rightarrow (a_i = 0)) \wedge ((i > \eta) \Rightarrow (a_i \in \{0, 1\}))) \\ \forall i \exists j ((j > i) \wedge (a_j = 0)) \end{aligned}$$

Les éléments de \mathfrak{R} sont appelés des Chaînes Propres.

Attention, cette façon d'écrire les nombres n'est pas exactement la façon habituelle, pour les négatifs :

$$\begin{aligned} \text{Dans l'écriture binaire usuelle, on a : } (-101)_2 &= (-5)_{10} \\ \text{Dans } \mathfrak{R}, \text{ on a } &: \langle (-1)(0)(1) \rangle = (-3)_{10} \end{aligned}$$

Pour bien comprendre la méthode de Rota, il suffit de faire un exemple « à la main », avec la somme de deux chaînes quelconques :

$$\begin{array}{cccccccc} (-3) & (5) & \cdot & (0) & (-2) & (5) & & \\ (1) & (-1) & \cdot & (2) & (3) & (1) & (2) & \\ \hline (-2) & (4) & \cdot & (2) & (1) & (6) & (2) & \end{array}$$

Cette somme n'est clairement pas une chaîne propre, il suffit de lui ajouter 0, c'est à dire $\mathbb{K} = \langle (1) \cdot (-2) \rangle$, judicieusement multiplié par différents coefficients, un certain nombre de fois pour y arriver :

$$\begin{array}{cccccccc} (-2) & (4) & \cdot & (2) & (1) & (6) & (2) & \\ \hline & & & & & (1) & (-2) & \\ & & & & & (3) & (-6) & \\ & & & & & (2) & (-4) & \\ & & & & & (2) & \cdot & (-4) & \\ (3) & (-6) & \cdot & & & & & \\ \hline (1) & (0) & \cdot & (0) & (0) & (1) & & \end{array} \quad \text{Qui est bien une chaîne propre}$$

On peut démontrer que toute chaîne bornée est équivalente à une chaîne propre, et que deux chaînes propres sont équivalentes si et seulement si elles sont égales, et in fine que $(\mathfrak{R}, +, \times, <)$ est isomorphe à $(\mathbb{R}, +, \times, <)$.

Chaque réel correspond à une et une seule chaîne propre, malheureusement dès que l'on fait des calculs, le résultat n'a aucune raison d'être une chaîne propre, d'où la nécessité de passer par la relation d'équivalence.

Autres Méthodes Décimales.

Les trois méthodes présentées ci-dessous sont des variations sur la méthode de Simon Stevin.

Liangpan Li.

Un première façon de construire les réels à partir de leur développement décimal, est de considérer les suites $\langle a_0, a_1, a_2 \cdots \rangle$ où $a_0 \in \mathbb{Z} \wedge \forall n \in \mathbb{N}^* (a_n \in \mathbb{Z}_{10})$, et on peut facilement vérifier que l'on peut se ramener au cas des **Suites Particulières**, avec néanmoins quelques petites différences (la gestion de l'équivalent de ω par exemple). Cette méthode a été étudiée en détail par Liangpan Li, un mathématicien chinois dans l'article : [A New Approach to the Real Numbers](#) .

Jim Propp.

Une autre façon de construire les réels à partir de leur développement décimal a été présenté par Jim Propp de l'Université Lowell du Massachussetts et quelques membres du MIT dans le document *Carrying On with Infinite Decimals* consiste à faire les opérations position par position, donc avec un résultat potentiellement strictement supérieur à 9, puis à effectuer les calculs de retenues. Une des façon de calculer ces retenues consiste à effectuer ces retenues en commençant par la retenue la plus à gauche à **chaque étape**, la démonstration essentielle dans cet article consiste à montrer que la stratégie de résolution des retenues aboutit toujours à un

réel quelque soit cette stratégie (donc pas forcément celle décrite ci-dessus), ou n'aboutit jamais quelque soit cette stratégie.

Martin Klazar.

La méthode présentée ci-dessous a été développée par Martin Klazar dans l'article : [Real Numbers as Infinite Decimals and Irrationality of \$\sqrt{2}\$](#) .

On appelle Chaîne Décimale Signée, et nous noterons \mathfrak{D} , l'ensemble des couples $x = (s, a)$ où $s \in \{+, -\}$ est le signe de x , et $a \in (\mathbb{Z}_{10})^{\mathbb{Z}^+}$ est une chaîne infinie d'éléments de \mathbb{Z}_{10} indexée par une partie finie à droite de \mathbb{Z} (attention, une partie finie à droite de \mathbb{Z} correspond à un nombre fini de décimales à gauche de la virgule) telle que le premier élément n'est pas nul, sauf pour la chaîne correspondant à 0, pour laquelle le signe n'existe pas, $k = 0$, et $\forall k((k < 0) \Rightarrow (a_k = 0))$. Les conventions habituelles seront utilisées pour écrire les éléments de \mathfrak{D} , par exemple $(+1_1, 2_0, 3_{-1}, 4_{-2})$ sera plutôt écrit $+12.34$ voire 12.34 .

Un éléments x s'écrit donc $x = (\pm, (a_k, a_{k-1}, \dots))$ où $a_k \neq 0$.

Attention : cette définition n'exclut pas les développements impropres.

On peut munir \mathfrak{D} d'une relation d'ordre, les éléments dont le signe est $-$ sont dit négatifs, ceux dont le signe est $+$ sont dits positifs :

$$x < y \Leftrightarrow \begin{cases} (x \text{ est négatif}) \wedge ((y = 0) \vee (y \text{ est positif})) \\ (x = 0) \wedge (y \text{ est positif}) \\ (x \text{ est négatif} \wedge y \text{ est négatif}) \wedge \exists m \in \mathbb{Z} \forall i \in \mathbb{Z}((i > m) \Rightarrow (x_i = y_i)) \wedge (y_i < x_i) \\ (x \text{ est positif} \wedge y \text{ est positif}) \wedge \exists m \in \mathbb{Z} \forall i \in \mathbb{Z}((i > m) \Rightarrow (x_i = y_i)) \wedge (x_i < y_i) \end{cases}$$

Cette relation est bien une relation d'ordre linéaire totale, mais elle n'est pas dense, par exemple $0.\bar{9} < 1.\bar{0}$, alors qu'il existe aucun élément x vérifiant $0.\bar{9} < x < 1.\bar{0}$. Les couples (x, y) tels qu'il n'existe pas de z vérifiant $x < z < y$ sont appelés des Sauts.

Soit \sim la relation sur \mathfrak{D} définie par : $x \sim y \Leftrightarrow ((x = y) \vee ((x, y) \text{ est un saut}) \vee ((y, x) \text{ est un saut}))$.

Par définition, on pose $\mathbb{R} = \mathfrak{D} / \sim$.

Il est facile de montrer que $(\mathbb{R}, <)$ possède la propriété de la borne supérieure, et que le sous ensemble des éléments de \mathfrak{D} se terminant par une infinité de 0 est dense dans \mathbb{R} . Comme l'addition et la multiplication sur cet ensemble sont faciles à définir (on peut se ramener à des opérations sur les entiers), il reste à prolonger ces opérations à \mathbb{R} par continuité (en estimant ces opérations sur l'ensemble des troncatures de chacun des opérands).

II.5.8 A partir de la Soustraction.

Cette méthode de construction des nombres réels a été introduite en 1976 par Nicolaas Govert de Bruijn, un mathématicien hollandais (1918 -).

Quelques mois auparavant le même Nicolaas Govert de Bruijn avait publié un article utilisant l'addition plutôt que la soustraction, nous en donnerons un très bref aperçu avant d'aborder la méthode basée sur la soustraction, car les idées développées pour l'addition sont plus intuitives que leurs homologues pour la soustraction, par contre la définition de la multiplication pose plus de problème (cette partie n'a d'ailleurs pas été publiée dans l'article de 1975).

Soit b un entier strictement plus grand que 1 (c'est donc une base possible pour la numération de position). On note $\Sigma = \{f \mid f \in \{0, 1, \dots, b-1\}^{\mathbb{Z}} \wedge (\forall x \exists y ((y > x) \wedge (f(y) < b-1)))\}$ autrement dit on ne prend pas en compte les développements impropres²⁸.

Dans un premier temps, on définit une addition, notée \oplus sur $\mathbb{Z}^{\mathbb{Z}}$:

$$\forall x \in \mathbb{Z} ((f \oplus g)(x) = f(x) + g(x))$$

Cette addition n'est pas interne sur Σ , en effet : $f \in \Sigma \wedge g \in \Sigma (f \oplus g \in \{0, 1, \dots, 2b-2\}^{\mathbb{Z}})$.

A toute application $f \in \mathbb{Z}^{\mathbb{Z}}$, on peut associer une application notée f_{\equiv_b} et définie par :

$$f_{\equiv_b}(x) = \begin{cases} \forall x (f_{\equiv_b}(x) \equiv f(x) [b]) \\ \forall x (0 \leq f_{\equiv_b}(x) < b) \end{cases}$$

Pour définir la fonction qui va permettre de calculer les retenues, on pourrait, intuitivement, dire que pour avoir une retenue à la position x , il faut et il suffit que pour une position $y > x$, une retenue soit générée, c'est à dire que $f(y) > b-1$, et que toutes les positions intermédiaires, transmettent cette retenue, c'est à dire $(x < z < y) \Rightarrow f(z) = b-1$.

Cette définition a un tout petit défaut : la fonction f définie par :

$$f(x) = \begin{cases} x \leq 0 & \Leftrightarrow f(x) = 0 \\ x > 0 & \Leftrightarrow f(x) = b-1 \end{cases}$$

Autrement dit, dans le cas où $b = 10$, f représente $0,999\bar{9}$, mais ne génère aucune retenue, aussi une définition un petit peu différente sera utilisée (et telle que la fonction précédente génère une retenue ce qui permet de démontrer que $0,999\bar{9} = 1$).

A toute application $f \in \{0, 1, \dots, 2b-2\}^{\mathbb{Z}}$, on associe $f_{\Delta} \in \{0, 1\}^{\mathbb{Z}}$, définie par

$$f_{\Delta}(x) = \begin{cases} f_{\Delta}(x) = 0 & \Leftrightarrow \exists y ((y > x) \wedge (f(y) < b-1) \wedge (\forall z ((x < z < y) \Rightarrow (f(z) \leq b-1))) \\ f_{\Delta}(x) = 1 & \text{dans tous les autres cas} \end{cases}$$

Finalement, on peut définir une addition interne sur Σ :

$$f + g = ((f \oplus g) \oplus (f \oplus g)_{\Delta})_{\equiv_b}$$

La fonction f_{Δ} permet bien de gérer les retenues, et surtout de les propager autant que nécessaire. La définition devient intuitivement très naturelle après l'avoir manipulée un peu, par exemple dans le cas habituel où $b = 10$:

\mathbb{Z}	-4	-3	-2	-1	0	1	2	3	
f	0	0	7	8	4	7	5	0	
g	0	0	5	1	3	2	7	0	
$f \oplus g$	0	0	12	9	7	9	12	0	
$(f \oplus g)_{\Delta}$	0	1	0	0	1	1	0	0	Cette ligne nécessite un peu de calcul.
$(f \oplus g) \oplus (f \oplus g)_{\Delta}$	0	1	12	9	8	10	12	0	
$f + g$	0	1	2	9	8	0	2	0	Qui est bien la somme attendue.

²⁸. Par contre on autorise un nombre infini de positions à gauche de la virgule, en fait les chaînes où il existe un N tel que $f(n) = b-1$ pour tout $n < N$ représente un négatif

Construction de de Bruijn à partir de la soustraction.

Cette méthode de construction des nombres réels a été introduite en 1976 par Nicolaas Govert de Bruijn, un mathématicien hollandais (1918 -).

Similairement à la construction précédente, on pose :

$$\Sigma = \{f \mid f \in \{0, 1, \dots, b-1\}^{\mathbb{Z}} \wedge (\forall x \exists y ((y > x) \wedge (f(y) < b-1)))\}.$$

Autrement dit Σ ne contient pas de développement impropre, mais contient des développements infinis à gauche de la virgule, y compris ceux dont la valeur à partir d'un certain rang (à gauche) est égal à $b-1$, qui représentent les négatifs.

Pour $(f, g) \in \Sigma^2$ on définit la fonction $f \ominus g$ par : $(f \ominus g)(x) = f(x) - g(x)$, évidemment cette opération n'est pas interne sur Σ .

Pour $(f, g) \in \Sigma^2$, on note $(f \ominus g)_{\Delta}$ la fonction suivante

$$(f \ominus g)_{\Delta}(x) = \begin{cases} (f \ominus g)_{\Delta}(x) = 1 & \Leftrightarrow \exists y ((y > x) \wedge (f(y) < g(y)) \wedge (\forall z ((x < z < y) \Rightarrow (f(z) \leq g(z)))) \\ (f \ominus g)_{\Delta}(x) = 0 & \text{dans tous les autres cas} \end{cases}$$

Et finalement on définit la soustraction sur Σ par :

$$f - g = ((f \ominus g) \ominus (f \ominus g)_{\Delta})_{\equiv_b}$$

Il est immédiat que $(f - g) \in \Sigma$.

Comme pour le cas précédent, le plus simple est de faire effectivement les calculs sur quelques exemples

\mathbb{Z}	-4	-3	-2	-1	0	1	2	3	
f	0	0	7	1	4	7	5	0	
g	0	0	5	2	3	7	7	0	
$f \ominus g$	0	0	2	-1	1	0	-2	0	
$(f \ominus g)_{\Delta}$	0	0	1	0	1	1	0	0	Cette ligne nécessite un peu de calcul.
$(f \ominus g) \ominus (f \ominus g)_{\Delta}$	0	0	1	-1	0	-1	-2	0	
$f - g$	0	0	1	9	0	9	8	0	Qui est bien le résultat attendu.

Parfois le résultat est négatif :

\mathbb{Z}	-4	-3	-2	-1	0	1	2	3	
f	$\bar{0}$	0	5	2	3	7	7	0	
g	$\bar{0}$	0	7	1	4	7	5	0	
$f \ominus g$	$\bar{0}$	0	-2	1	-1	0	2	0	
$(f \ominus g)_{\Delta}$	$\bar{1}$	1	0	1	0	0	0	0	Cette ligne nécessite un peu de calcul.
$(f \ominus g) \ominus (f \ominus g)_{\Delta}$	$\bar{-1}$	-1	-2	0	-1	0	2	0	
$f - g$	$\bar{9}$	9	8	0	9	0	2	0	Qui est bien le résultat attendu.

On peut démontrer assez facilement que $(f - g)(x) = f(x) - g(x) - (f \ominus g)_{\Delta}(x) + b \cdot (f \ominus g)_{\Delta}(x - 1)$, ce qui permet de démontrer que $(f - g) \in \Sigma$.

On peut, bien sur, définir la fonction $\mathbf{0}$ par $\forall x \in \mathbb{Z} (\mathbf{0}(x) = 0)$, par la suite cette fonction sera simplement notée 0 , on peut montrer sans difficulté que $(f - 0) = f$ et que $(f - f) = 0$. De la même façon, nous pouvons définir $\mathbf{1}$ par $\forall x \in \mathbb{Z} ((x \neq 0) \Rightarrow (\mathbf{1}(x) = 0)) \wedge (\mathbf{1}(0) = 1)$, par la suite cette fonction sera simplement notée 1 .

En définissant l'addition sur Σ par $(f + g) = f - (0 - g)$, on peut démontrer que $(\Sigma, +)$ est un groupe abélien.

Comme vu précédemment Σ contient des éléments qui, intuitivement, ne sont pas des réels, aussi quelques définitions supplémentaires sont nécessaires :

1. Soit $f \in \Sigma$, f est dit strictement positive, ce qui sera noté $f > 0$ si et seulement si :

$$(f \neq 0) \wedge (\exists x \forall y((y < x) \Rightarrow (f(y) = 0)))$$

Autrement dit f est strictement positive si f n'est pas nulle est si f n'a qu'un nombre fini de décimales non nulles à gauche de la virgule.

2. Soit $f \in \Sigma$, f est dit strictement négative, ce qui sera noté $f < 0$ si et seulement si :

$$\exists x \forall y((y < x) \Rightarrow (f(y) = b - 1))$$

Autrement dit f est strictement négative si f n'a qu'un nombre fini de décimales différentes de $b - 1$ à gauche de la virgule.

3. Il est facile de voir que « strictement positive », « nulle » et « strictement négative » sont des cas exclusifs les uns des autres, mais ne couvrent pas Σ en entier.
4. Nous noterons $\mathbb{Q}_b = \{f \in \Sigma \mid \exists x \forall y((y > x) \Rightarrow (f(y) = 0))\}$. Autrement dit f n'a qu'un nombre fini de décimales non nulles à droite de la virgule (ce sont donc bien les nombres b-adiques).
5. Nous noterons $\mathbb{Z}_b = \{f \in \Sigma \mid \forall x((x > 0) \Rightarrow (f(x) = 0))\}$. Autrement dit f n'a aucune décimale non nulle à droite de la virgule (ce sont donc bien les entiers b-adiques).
6. Nous noterons $\mathbb{R} = \{f \in \Sigma \mid (f \text{ est strictement négative}) \vee (f = 0) \vee (f \text{ est strictement positive})\}$.
($\mathbb{R}, +$) est un sous-groupe de $(\Sigma, +)$
7. $f < g \Leftrightarrow f - g < 0$.
8. $\mathbb{Q}_b \cap \mathbb{R}$ est l'ensemble des réels n'ayant qu'un nombre fini de décimales à droite de la virgule (l'équivalent des décimaux en base b). ($\mathbb{Q}_b \cap \mathbb{R}, +$) est un sous-groupe de $(\mathbb{R}, +)$.
9. Nous noterons $\mathbb{Z}_\Sigma = \mathbb{Z}_p \cap \mathbb{R}$ (il s'agit bien de \mathbb{Z} dans Σ , mais nous le distinguons du \mathbb{Z} utilisé pour définir Σ).

On peut montrer que : $\forall f \in \mathbb{R} \forall g \in \mathbb{R} ((f < g) \Rightarrow (\exists h \in \mathbb{Q}_b \cap \mathbb{R} (f < h < g)))$ autrement dit $\mathbb{Q}_b \cap \mathbb{R}$ est dense dans \mathbb{R} , cette propriété très importante sera utilisée pour la définition de la multiplication.

La propriété d'Archimède peut aussi être assez facilement démontrée : $\forall f \in \mathbb{R} \exists g \in \mathbb{Z}_\Sigma (g > f)$.

Il ne reste plus qu'à définir la multiplication :

On peut montrer (par une récurrence²⁹ sur $\mathbb{Q}_b \cap \mathbb{R}$) que pour tout $f \in \mathbb{Q}_b \cap \mathbb{R}$, il existe un et un seul homomorphisme $\mathfrak{h}_f : (\mathbb{Q}_b \cap \mathbb{R}) \mapsto (\mathbb{Q}_b \cap \mathbb{R})$ vérifiant (ci-dessous, 1 est la fonction 1 et non le relatif 1) :

$$\forall g \in (\mathbb{Q}_b \cap \mathbb{R}) \forall h \in (\mathbb{Q}_b \cap \mathbb{R}) \left((\mathfrak{h}_f(g + h) = \mathfrak{h}_f(g) + \mathfrak{h}_f(h)) \wedge (\mathfrak{h}_f(1) = f) \right)$$

La composée d'homomorphismes étant un homomorphisme, il est clair que :

$$\forall f \in (\mathbb{Q}_b \cap \mathbb{R}) \forall g \in (\mathbb{Q}_b \cap \mathbb{R}) \exists \mathfrak{h} \in \mathcal{H}om(\mathbb{Q}_b \cap \mathbb{R}) \left(\mathfrak{h}_f \circ \mathfrak{h}_g = \mathfrak{h} \right)$$

En posant $h = \mathfrak{h}(1)$, nous pouvons écrire $\mathfrak{h}_f \circ \mathfrak{h}_g = \mathfrak{h}_h$, il devient alors naturel de poser $h = f \cdot g$, ce qui permet de définir la multiplication sur $\mathbb{Q}_b \cap \mathbb{R}$ (et donc, pas encore sur \mathbb{R}).

Pour étendre la définition de la multiplication de $\mathbb{Q}_b \cap \mathbb{R}$ à \mathbb{R} , c'est la densité de $\mathbb{Q}_b \cap \mathbb{R}$ dans \mathbb{R} qui sera utilisée.

Pour $f \in \mathbb{R}$, on pose f_x , la fonction définie par

$$\forall y \in \mathbb{Z} (((y \leq x) \Rightarrow (f_x(y) = f(y))) \wedge ((y > x) \Rightarrow (f_x(y) = 0)))$$

C'est à dire que f_x est l'arrondi de f à x décimales.

Soit $S \subset \mathbb{R}$, une partie minorée de \mathbb{R} , on pose $S_x = \{f_x \mid f \in S\}$ et $f_x^{\downarrow S} = \min_{f \in S_x} (f)$ (ce minimum est bien atteint puisqu'il s'agit de trouver le minimum parmi b éléments, un nombre fini de fois).

29. La récurrence sur $\mathbb{Q}_b \cap \mathbb{R}$ est un peu différente de la récurrence habituelle sur \mathbb{N} .

Enfin on pose $f^{\downarrow S} = \inf(S) \Leftrightarrow f^{\downarrow S}(x) = f_x^{\downarrow S}(x)$ (on ne peut plus parler de minimum, puisque cette fois-ci il s'agit d'un nombre infini de décimales).

A partir de cette définition on peut facilement définir, pour $S \subset \mathbb{R}$, une partie majorée de \mathbb{R} :
 $\sup(S) = -\inf(-S)$.

A partir des définitions précédentes, on peut utiliser des méthodes comme celle de Cantor (utilisant des suites de Cauchy) (comme dans l'article de de Bruijn), ou les coupures de Dedekind, pour obtenir la multiplication sur les réels (les objets existent contrairement aux constructions à partir de \mathbb{Q}) comme une fonction continue sur chacun des ses opérands.

Construction de Udding à partir de la soustraction.

Cette méthode de construction des nombres réels a été introduite en 1980 par Jan Tijmen Udding, un mathématicien hollandais élève de Nicolaas de Bruijn (et de Dijkstra).

La méthode de Udding est un cas particulier de celle de de Bruijn, avec $b = 2$, ce qui permet de ré-écrire plus simplement certaines démonstrations et de donner la définition de la soustraction, sans passer par les calculs modulaires mais directement sous la forme :

$$(f - g)(x) = f(x) - g(x) - (f \ominus g)_\Delta(x) + (f \ominus g)_\Delta(x - 1) + (f \ominus g)_\Delta(x - 1)$$

Bien sur l'addition se définit comme dans la méthode précédente : $f + g = f - (0 - g)$, et comme dans la méthode de de Bruijn, la multiplication passe par sa définition (là encore un peu plus simple que le cas général) sur un ensemble dénombrable et dense dans \mathbb{R} .

II.5.9 Autres Constructions

Suites non décroissantes de rationnels positifs.

Cette méthode, qui semble être due à Richard Kaye, un mathématicien anglais, dont le site personnel propose un fichier datant de 2007 sur ce sujet, repose sur le même fond que la méthode par les suites de Cauchy, mais d'une façon qui simplifie certaines définitions.

Une suite bornée, non décroissante de rationnels positifs est une suite $u = (u_n)_{n \in \mathbb{N}}$ vérifiant :

1. $\forall n \in \mathbb{N} (u_n \in \mathbb{Q}^+)$
2. $\forall n \in \mathbb{N} (u_{n+1} \geq u_n)$
3. $\exists M_u \in \mathbb{Q} \forall n \in \mathbb{N} (u_n \leq M_u)$

Nous noterons \mathcal{R}^+ , l'ensemble des suites bornées, non décroissantes de rationnels positifs, ce n'est clairement pas encore un ensemble que l'on peut considérer comme isomorphe à \mathbb{R}^+ , dans la mesure où plusieurs éléments de \mathcal{R}^+ peuvent être identifiés à un même élément de \mathbb{R}^+ , nous allons donc passer par une relation d'équivalence, mais qui dans le cas présent est particulièrement facile à définir :

$$\forall u \in \mathcal{R}^+ \forall v \in \mathcal{R}^+ ((u \sim v) \Leftrightarrow ((\forall n \in \mathbb{N} \exists m \in \mathbb{N} (u_n \leq v_m)) \wedge (\forall n \in \mathbb{N} \exists m \in \mathbb{N} (v_n \leq u_m))))$$

Il est clair que \sim est une relation d'équivalence, et nous noterons $\mathbb{R}^+ = \mathcal{R}^+ / \sim$.

Trivialement \mathbb{Q}^+ peut être identifié avec le sous-ensemble de \mathbb{R}^+ des classes des suites constantes de rationnels positifs.

On peut définir sur \mathbb{R}^+ (nous noterons $[u]$ la classe de u) :

$$\begin{aligned} \text{Une relation d'ordre} & : ([u] \leq [v]) \Leftrightarrow \forall n \in \mathbb{N} \exists m \in \mathbb{N} (u_n \leq v_m) \\ \text{Une addition} & : [u] + [v] = [(u_n + v_n)_{n \in \mathbb{N}}] \\ \text{Une multiplication} & : [u] \cdot [v] = [(u_n \cdot v_n)_{n \in \mathbb{N}}] \end{aligned}$$

On peut vérifier que ces définitions sont valides (ne dépendent pas du représentant de la classe), qu'elles prolongent les définitions correspondantes sur \mathbb{Q} , et vérifient bien les propriétés attendues, y compris la propriété de la borne supérieure.

Cette méthode a permis de fabriquer $(\mathbb{R}^+, +, \cdot, \leq)$, mais la fabrication de $(\mathbb{R}, +, \cdot, \leq)$ s'en déduit facilement, de la même façon que l'on peut construire \mathbb{Z} à partir de \mathbb{N} .

Quasi-endomorphismes

L'idée de base de cette construction remonte à la théorie des proportions due à Eudoxe de Cnide, médecin, mathématicien, philosophe et astronome grec (-400 à -350 environ).

Cette méthode permet de passer de \mathbb{Z} à \mathbb{R} sans passer par \mathbb{Q} .

L'ensemble $\mathbb{Z}^{\mathbb{Z}}$ des applications de \mathbb{Z} dans \mathbb{Z} , peut être muni, naturellement de deux opérations :

$$\begin{aligned} \text{Addition} & : (f + g)(n) = f(n) + g(n) \\ \text{Composition} & : (f \circ g)(n) = f(g(n)) \end{aligned}$$

Il est immédiat de vérifier que $(\mathbb{Z}^{\mathbb{Z}}, +)$ est un groupe abélien, et que $(\mathbb{Z}^{\mathbb{Z}}, \circ)$ est associatif et unitaire, mais ni commutatif, ni distributif sur l'addition et seuls les bijections ont un inverse pour \circ .

Définition : un quasi-endomorphisme³⁰ est une fonction $\varphi \in \mathbb{Z}^{\mathbb{Z}}$ vérifiant :

$$\exists K_{\varphi} \in \mathbb{N} \forall m \in \mathbb{Z} \forall n \in \mathbb{Z} (|\varphi(n + m) - \varphi(n) - \varphi(m)| \leq K_{\varphi})$$

La notation K_{φ} permet d'identifier la constante d'une fonction φ particulière.

Définition : deux quasi-endomorphismes sont dits équivalents, et on note $\varphi \sim \psi$:

$$\varphi \sim \psi \Leftrightarrow \exists K_{\psi}^{\varphi} \in \mathbb{N} \forall n \in \mathbb{Z} (|\varphi(n) - \psi(n)| \leq K_{\psi}^{\varphi})$$

(Une autre façon de le dire, c'est que la fonction différence $(\varphi - \psi)$ est bornée).

La motivation de ces définitions est que pour tout réel α la fonction définie par $\varphi_{\alpha}(n) = \lfloor \alpha n \rfloor$ ³¹ est un quasi-endomorphisme et si α et β sont des réels différents, les fonctions φ_{α} et φ_{β} ne sont pas équivalentes (\mathbb{R} est archimédien).

L'ensemble des quasi-endomorphismes sera noté \mathfrak{O} .

On peut facilement vérifier que $(\mathfrak{O}, +)$ est un sous-groupe abélien de $(\mathbb{Z}^{\mathbb{Z}}, +)$.

On peut tout aussi facilement vérifier que le sous-ensemble de $\mathbb{Z}^{\mathbb{Z}}$ des fonctions bornées est en fait un sous-ensemble de \mathfrak{O} .

La démonstration que l'opération \circ est interne dans \mathfrak{O} est un petit peu plus compliquée.

$$\left\{ \begin{aligned} & |f \circ g(n + m) - f \circ g(n) - f \circ g(m)| \\ = & |f(g(n + m)) - f(g(n)) - f(g(m))| \\ = & |f(g(n + m)) - f(g(n) + g(m)) + f(g(n) + g(m)) - f(g(n)) - f(g(m))| \\ \leq & |f(g(n + m)) - f(g(n) + g(m))| + |f(g(n) + g(m)) - f(g(n)) - f(g(m))| \\ \leq & |f(g(n + m)) - f(g(n) + g(m))| + K_f \\ = & |f(g(n + m) - g(n) - g(m)) - f(g(n + m) - g(n) - g(m)) + f(g(n + m)) - f(g(n) + g(m))| + K_f \\ = & |f(g(n + m) - g(n) - g(m)) + f((g(n) + g(m)) + (g(n + m) - g(n) - g(m))) \\ & - f(g(n + m) - g(n) - g(m)) - f(g(n) + g(m))| + K_f \\ \leq & |f(g(n + m) - g(n) - g(m))| \\ + & |f((g(n) + g(m)) + (g(n + m) - g(n) - g(m))) - f(g(n + m) - g(n) - g(m)) - f(g(n) + g(m))| + K_f \\ \leq & |f(g(n + m) - g(n) - g(m))| + 2K_f \\ \leq & M + 2K_f \end{aligned} \right.$$

Les deux seuls points nécessitant une petite explication sont les passages concernant :

1. $|f((g(n) + g(m)) + (g(n + m) - g(n) - g(m))) - f(g(n + m) - g(n) - g(m)) - f(g(n) + g(m))|$ qui est de la forme $|f(X + Y) - f(X) - f(Y)|$.
2. $|f(g(n + m) - g(n) - g(m))| \leq M$, il s'agit de l'image par f , d'un ensemble borné (par définition d'un quasi-endomorphisme), c'est donc bien un ensemble borné, par un nombre M , par exemple.

30. On trouve parfois quasi-homomorphisme, pseudo-homomorphisme, ou encore almost-homomorphism ou slope (qui peut se traduire par pente) en anglais.

31. $\lfloor x \rfloor$ représente la partie entière de x .

Les démonstrations qui permettent de montrer que $(\mathfrak{O}/\sim, +, \circ, <)$ est un corps commutatif totalement ordonné, vérifiant la propriété de la borne supérieure sont simples (aucune connaissance qui ne soit élémentaire n'est nécessaire), mais très calculatoires, et certaines un peu longues ; ces démonstrations se trouvent dans le document *Analysis of an Efficient Construction of the reals* (voir les références ci-dessous).

Ces démonstrations permettent de montrer que $(\mathfrak{O}/\sim, +, \circ, <)$ est isomorphe à $(\mathbb{R}, +, \times, <)$.

On peut identifier \mathbb{Z} avec l'ensemble des classes des fonctions de la forme $\varphi_n(i) = ni$ et \mathbb{Q} avec l'ensemble des classes de fonctions de la forme :

$$\begin{cases} i \geq 0 \Rightarrow \varphi_q^p(i) = \min_{n \in \mathbb{N}} \{n \mid qn \geq pi\} \\ i < 0 \Rightarrow \varphi_q^p(i) = -\varphi_q^p(-i) \end{cases}$$

On peut vérifier facilement que $\varphi_q^p \circ \varphi_q \sim \varphi_p$.

Complétion de MacNeille.

Cette méthode, qui s'inspire des coupures de Dedekind, est due à Holbrook Mann MacNeille (en 1937), un mathématicien américain (1907 - 1973).

La complétion de MacNeille (ou de Dedekind-MacNeille) est une méthode, très générale, qui permet de compléter une relation d'ordre quelconque (même, et surtout, les ordres partiels) pour en faire un **treillis complet**, et, bien sur, le résultat est « le plus petit » treillis complet contenant (via un isomorphisme) la relation d'ordre de départ.

Soit $(X, <)$ une relation d'ordre, pour tout sous-ensemble $A \subseteq X$, on note :

1. $\mathfrak{u}(A)$, l'ensemble des bornes supérieures de A (c'est à dire l'ensemble des éléments de X plus grands (ou égaux) que tous les éléments de A).
2. $\mathfrak{L}(A)$, l'ensemble des bornes inférieures de A (c'est à dire l'ensemble des éléments de X plus petits (ou égaux) que tous les éléments de A).
3. $A^\sharp = \mathfrak{u}(\mathfrak{L}(A))$.
4. $X^\sharp = \{A \mid (A \subseteq X) \wedge (A = A^\sharp)\}$,

(X^\sharp, \subset) ³² est un treillis complet dans lequel on peut plonger (canoniquement) $(X, <)$, c'est le complété de MacNeille de X .

On peut montrer que $\mathbb{Q}^\sharp = \overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, \infty\}$ ou, de la même façon que, par exemple, $(\mathbb{Z} + \sqrt{2}\mathbb{Z})^\sharp = \overline{\mathbb{R}}$.

La définition des opérations se fait comme dans la méthode des coupures de Dedekind, et en éliminant les deux infinis, on retrouve bien $(\mathbb{R}, +, \times, <)$.

³². Le complété de MacNeille est usuellement noté X^* , mais ici nous ne voulons pas prendre le risque de confondre le complété de MacNeille de \mathbb{Q} et $\mathbb{Q} \setminus \{0\}$.

Construction à base de Recouvrements.

Cette méthode de construction des réels semble tirer son origine d'un article de Michael Paul Fourman, un mathématicien anglais (1950 -) et John Martin Elliott Hyland un autre mathématicien anglais : Sheaf models for analysis (1979).

Il est nécessaire de commencer par quelques définitions.

Dans la partie Généralités algébriques on trouvera les définitions de **Treillis**, **\wedge -treillis**, et dans la partie **Relation d'Ordre** section et partie commençante, section et partie finissante.

Définition : Soit (E, \leq) un \wedge -treillis, on appelle *Relation de Recouvrement* une relation notée \triangleright entre éléments de $\mathfrak{P}(E)$ et de E (c'est à dire dont le graphe $\mathcal{G}_{\triangleright} \subset \mathfrak{P}(E) \times E$) vérifiant :

- $\forall X \in \mathfrak{P}(E) \forall x \in E ((X \triangleright x) \Rightarrow X \subseteq \downarrow x)$
- $\forall X \in \mathfrak{P}(E) \forall x \in E \forall y \in E (((X \triangleright x) \wedge (y \leq x)) \Rightarrow (\{y \wedge z \mid z \in X\} \triangleright y))$

Définition : Soit (E, \leq) un \wedge -treillis, et \triangleright , une relation de Recouvrement de E , I est appelé un \triangleright -Idéal si et seulement si :

- $I \subseteq E$
- $\forall x \in E \forall y \in E (((x \in I) \wedge (y \leq x)) \Rightarrow (y \in I))$ une autre façon de le dire : $(I = \downarrow I)$.
- $\forall X \in \mathfrak{P}(E) \forall x \in E ((X \triangleright x) \wedge ((X \subseteq I)) \Rightarrow (x \in I))$

Un exemple simple et naturel³³ pour illustrer la notion de Recouvrement :

Soit \mathcal{O} les ouverts d'une topologie, il est clair que (\mathcal{O}, \subseteq) est un \wedge -treillis, on définit une relation de Recouvrement \triangleright par :

$$\forall X \in \mathfrak{P}(\mathcal{O}) \forall x \in E ((X \triangleright x) \Leftrightarrow (X \text{ est un recouvrement ouvert de } x))$$

Nous noterons $\overset{-\infty}{\mathbb{Q}} = \mathbb{Q} \cup \{-\infty\}$ et $\overset{+\infty}{\mathbb{Q}} = \mathbb{Q} \cup \{+\infty\}$, et nous appellerons intervalle uniquement les éléments $(p, q) \in \overset{-\infty}{\mathbb{Q}} \times \overset{+\infty}{\mathbb{Q}}$ vérifiant $p \leq q$, et plus spécifiquement singleton quand $p = q$.

Soit la relation \preceq définie par :

$$((p, q) \preceq (p', q')) \Leftrightarrow ((p \geq p') \wedge (q \leq q'))$$

Il est facile de vérifier que $(\overset{-\infty}{\mathbb{Q}} \times \overset{+\infty}{\mathbb{Q}}, \preceq)$ est un \wedge -treillis dont le sup est $\{-\infty, +\infty\}$ et un calcul immédiat donne : $(p, q) \wedge (p', q') = (\max(p, p'), \min(q, q'))$.

Autrement dit :

$$(p, q) \preceq (p', q') \begin{cases} p < q \Rightarrow (p, q) \text{ est un intervalle et } (p', q') \text{ est un intervalle qui le contient.} \\ p = q \Rightarrow (p, q) \text{ est un singleton et } (p', q') \text{ est un intervalle qui le contient.} \\ p > q \Rightarrow \begin{cases} (q, p) \text{ est un intervalle et } (p', q') \text{ est un intervalle qui contient } p \text{ ou } q. \\ (q, p) \text{ est un intervalle qui contient l'intervalle } (p', q'). \\ (q, p) \text{ est un intervalle qui contient l'intervalle } (q', p'). \end{cases} \end{cases}$$

Nous définissons le recouvrement \triangleright par :

$$\begin{cases} p \geq q \Rightarrow \emptyset \triangleright (p, q) \\ p < q \Rightarrow \begin{cases} \forall p' \forall q' ((p \leq q' < p' \leq q) \Rightarrow (\{(p, p'), (q, q')\} \triangleright (p, q))) \\ \{(p', q') \mid p < p' < q' < q\} \triangleright (p, q) \end{cases} \end{cases}$$

On peut identifier \mathbb{Q} et l'ensemble des \triangleright -Idéaux engendrés par les singletons, et finalement on peut montrer que l'ensemble des \triangleright -Idéaux est isomorphes à \mathbb{R} .

Les démonstrations sont très techniques, elles se trouvent détaillées dans le livre *Stone Spaces* par Peter T. Johnstone (voir dans les références).

33. Cette notion est très liée à la « Topologie sans Point ».

Construction à partir des Nombres Surréels.

On peut aussi construire les réels à partir des **Nombres Surréels** :

On peut construire \mathbb{Z} très facilement
$$\begin{cases} 0 &= \{|\} \\ n &= \{(n-1)|\} \quad \text{si } n > 0 \\ n &= \{|(n+1)\} \quad \text{si } n < 0 \end{cases}$$

On peut aussi, facilement construire \mathfrak{D} **l'ensemble des Nombres Dyadiques** : $\frac{j}{2^k} = \left\{ \frac{j-1}{2^k} \mid \frac{j+1}{2^k} \right\}$

Dans les deux cas précédents, les nombres sont définis uniquement à partir de nombres précédemment définis.

Les nombres réels sont alors définis comme les nombres surréels de la forme $(D_g|D_d)^{34}$, où :

$$\begin{cases} D_g \cup D_d = \mathfrak{D} \\ D_g \cap D_d = \emptyset \\ \forall x \forall y ((x \in X_g) \wedge (y \in X_d) \Rightarrow (x < y)) \end{cases}$$

Les opérations sont les opérations standard sur les Surréels, et la relation d'ordre est celle des Surréels.

³⁴. C'est donc une méthode très semblable aux coupures de Dedekind, sauf que l'on se plonge d'entrée dans un sur-ensemble de \mathbb{R} .

Construction à partir des Nombres Hyperrationnels.

Cette méthode passe par l'analyse non standard : à partir de \mathbb{Q} , on considère l'ensemble des suites de rationnels, c'est à dire l'ensemble $\mathbb{Q}^{\mathbb{N}}$ et on note \mathcal{U} un ultrafiltre sur \mathbb{N} .

L'ultraproduit $\mathbb{Q}^{\mathbb{N}}/\mathcal{U}$, appelé ensemble des Hyperrationnels, hérite des relations et opérations définies sur \mathbb{Q} , et \mathbb{Q} se plonge naturellement dans cette ultraproduit (donc nous ne ferons pas la différence entre \mathbb{Q} et son image dans $\mathbb{Q}^{\mathbb{N}}/\mathcal{U}$), ce qui permet de donner quelques définitions de base :

- α est un infinitesimal si $\forall q \in \mathbb{Q}^{\mathbb{N}}/\mathcal{U} (|\alpha| < q)$
- α est fini si $\exists q \in \mathbb{Q}^{\mathbb{N}}/\mathcal{U} (|\alpha| < q)$
- α est un infini si $\forall q \in \mathbb{Q}^{\mathbb{N}}/\mathcal{U} (|\alpha| > q)$
- α et β sont dit ultra-proches (ou infiniment-proches), et on note $(\alpha \doteq \beta) \Leftrightarrow (\alpha - \beta)$ est in infinitésimal.
- On appelle monade de α , et on note $\text{Mon}(\alpha) = \{\beta \mid \alpha \doteq \beta\}$.

On note \mathbb{Q}_f le sous-ensemble de $\mathbb{Q}^{\mathbb{N}}/\mathcal{U}$ des hyperrationnels finis.

On peut alors montrer que $(\mathbb{Q}_f/\doteq, +, \times, <)$ est isomorphe à $(\mathbb{R}, +, \times, <)$.

Cette construction passe par les Hyperrationnels et suit le schéma :

$$\mathbb{Q} \longrightarrow \mathbb{Q}^{\mathbb{N}} \longrightarrow \mathbb{Q}^{\mathbb{N}}/\mathcal{U} \supset \mathbb{Q}_f \longrightarrow (\mathbb{Q}_f/\doteq) \cong \mathbb{R}$$

Ou

$$\mathbb{Q} \longrightarrow \mathbb{Q}^{\mathbb{N}} \longrightarrow \mathbb{Q}^{\mathbb{N}}/\mathcal{U} \supset \mathbb{Q}_f \supset \text{Mon}(0) \longrightarrow (\mathbb{Q}_f/\text{Mon}(0)) \cong \mathbb{R}$$

A comparer avec le schéma de la méthode de Cantor à l'aide des suites de Cauchy ; en notant \mathfrak{C} l'ensemble des suites de Cauchy et \mathfrak{Z} l'ensemble des suites de Cauchy qui convergent vers 0 (et qui est trivialement un idéal maximal de \mathfrak{C}) :

$$\mathbb{Q} \longrightarrow \mathbb{Q}^{\mathbb{N}} \supset \mathfrak{C} \supset \mathfrak{Z} \longrightarrow (\mathfrak{C}/\mathfrak{Z}) \cong \mathbb{R}$$

II.5.10 Propriétés algébriques et Topologiques

$(\mathbb{R}, +, \times, <)$ est un corps totalement ordonné (donc de caractéristique 0), complet (au sens de la propriété de la borne supérieure), mais ce n'est pas un corps algébriquement clos ($x^2 + 1 = 0$ n'a pas de racine dans \mathbb{R}). Etant de caractéristique 0, son corps premier est $(\mathbb{Q}, +, \times)$.

On peut citer quelques théorèmes :

- Soit une suite d'intervalles fermés $([a_n, b_n])_{n \in \mathbb{N}}$ tels que

$$\forall n \in \mathbb{N} \left(((a_n \leq b_n) \wedge (a_n \leq a_{n+1}) \wedge (b_{n+1} \leq b_n)) \Rightarrow \left(\bigcap_{n \in \mathbb{N}} [a_n, b_n] \neq \emptyset \right) \right)$$

- Dans \mathbb{R} , toute suite croissante majorée est convergente.
- $\forall x \in \mathbb{R} \exists ! n \in \mathbb{N} (n \leq x < n + 1)$, ce nombre entier n est appelé partie entière de x et on le note $[x] = n$.
- \mathbb{Q} est dense dans \mathbb{R} .
- Dans \mathbb{R} toute suite de Cauchy est convergente.
- Les parties compactes de \mathbb{R} sont exactement les fermés bornés.
- \mathbb{R} possède la propriété de Baire : toute intersection dénombrable d'ouverts denses de \mathbb{R} est dense dans \mathbb{R} .
- Théorème de Bolzano-Weierstrass : Toute suite bornée de nombres réels admet une sous-suite convergente.
- Les sous-groupes de $(\mathbb{R}, +)$ sont soit de la forme $\alpha\mathbb{Z}$ (sous-groupes discrets), soit denses dans \mathbb{R} (sous-groupes continus).
- \mathbb{R} n'est pas dénombrable : $|\mathbb{R}| = 2^{\aleph_0}$.

$(\mathbb{R}, +, \times)$ est aussi un corps réel clos, c'est à dire vérifie :

Axiome 1 : $(\mathbb{R}, +, \times)$ est un corps commutatif.

Axiome 2 : $\forall x \exists y ((x = y^2) \vee (x + y^2 = 0))$

Schéma 1 : Pour tout nombre entier n : $\forall x_1 \forall x_2 \cdots \forall x_n (x_1^2 + x_2^2 + \cdots + x_n^2 + 1 \neq 0)$.

Schéma 2 : Pour tout nombre entier n : $\forall a_0 \forall a_1 \cdots \forall a_{2n} \exists x \left(x^{2n+1} + \sum_{i=0}^{2n} a_i x^i \right) = 0$

Un théorème intéressant concernant les corps réels clos (RCF³⁵ en général dans la littérature anglaise) : La clôture algébrique d'un corps réel clos est de degré fini.

La théorie des corps réels clos s'écrit donc dans le langage des anneaux $\mathcal{L}(0, 1, +, \times)$, néanmoins, on peut définir une relation d'ordre dans ce langage : $x < y \Leftrightarrow \exists z ((z \neq 0) \wedge (x + z^2 = y))$.

La théorie des corps réels clos est exactement la même dans le langage des anneaux, ou dans le langage des anneaux ordonnés (puisque l'ordre est définissable dans le langage des anneaux), à un « détail » près : La théorie des corps réels clos admet l'élimination des quantificateurs dans le langage $\mathcal{L}(0, 1, +, \times, <)$ des anneaux ordonnés.

La théorie des corps réels clos est donc complète et décidable, ce qui a pour conséquence que tous les corps réels clos sont élémentairement équivalents à $(\mathbb{R}, +, \times, <)$.

II.5.11 Utilisation en physique

Les Réels sont omniprésent dans les modèles physiques, mais totalement absent des mesures, ce qui fait que, dans la pratique, les physiciens utilisent essentiellement les nombres **Rationnels**.

II.5.12 Références

1. Modes de Construction

- i) R. Dedekind, *Les nombres : que sont-ils et à quoi servent-ils ?*, Vieweg. Braunschweig, 1888, ré-édité Paris, 1979.
- ii) Gary Sng Chee Hien, *Construction of the Real Number System*, Department of Mathematics National University of Singapore, 2000 - 2001.
- iii) Huan Long, *Construction of the Real Numbers*, Shanghai Jiao Tong University.
- iv) E.A. Maier & D. Maier, *A Construction of the Real Numbers*, The Two-Year College Mathematics Journal, Mathematical Association of America, 1973.
- v) E. D. Bloch, *Construction of the Real Numbers*, The Real Numbers and Real Analysis, Springer, 2011.
- vi) F. Faltin, N. Metropolis, B. Ross & G. C. Rota, *The real numbers as a wreath product*, Advances in Mathematics, Volume 16 No 3, p. 278 - 304, 1975.
- vii) B. Odgers & Nguyen Hanh Vo, *Analysis of an Efficient Construction of the reals*, 2002.
- viii) R.D. Arthan, *The Eudoxus Real Numbers*, 2004
- ix) N. G. de Bruijn, *Defining Reals Without the Use of Rationals*, Indagationes mathematicae Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen. Series A, Volume 38, No. 2 2, p. 100 - 108, 1976.
- x) A. Knopfmacher & J. Knopfmacher, *Two Constructions of the Real Numbers via Alternating Series*, The International Journal of Mathematics and Mathematical Sciences, Volume 12, No 3, p. 603 - 613, 1989.
- xi) P.T. Johnstone, *Stone Spaces*, Cambridge University Press, 1982.

2. Propriétés Algébriques

- i) J. R. Buchanan, *Algebraic and Order Properties of \mathbb{R}* , Millersville University, Pennsylvanie, 2007.
- ii) R. G. Bartle & D. R. Sherbert, *Basic Concepts of Analysis*, New Mexico Institute of Mining and Technology, 2004.
- iii) B. E. Blank, *Introduction to Real Analysis*, Washington University, St. Louis, 2008
- iv) J. Hutchinson, *Calculus Notes*, Department of Mathematics, School of Mathematical Sciences, Australian National University, 1998

35. Real Closed Field.

- v) R. Pruim, *Axioms for the Real Number System*, Department of Mathematics and Statistics, Calvin College, Grand Rapids, Michigan, 2003.
- vi) B. Kahng, *The Properties Of Real Numbers I*, Division of Science and Mathematics University of Minnesota, Morris, 2008.
- vii) B. Kahng, *The Properties Of Real Numbers II*, Division of Science and Mathematics University of Minnesota, Morris, 2008.
- viii) J. K. Mattila, *Predicate Logic*, Lappeenranta University of Technology, Finlande, 2009

3. Corps Réels Clos

- i) V. L. Noquez, *Model Theory of Real Closed Fields*, Carnegie Mellon University, Logic and Computation Senior Thesis, 2008.
- ii) E. Artin & O. Schreier, *Construction algébrique d'un corps réel*, séminaire de mathématiques, Hambourg, Volume 5, p. 85- 99, 1926.
- iii) M. Deronne, P. Hauweele & N. Meunier, *Algorithme d'Élimination des Quantificateurs pour les Corps Algébriquement/Réels Clos selon A.Muchnik*, 2009.
- iv) R. van der Meyden & M. K. Patra, *The Theory of a Real Closed Field and its Algebraic Closure*, School of Computer Science and Engineering, University of New South Wales, Sydney 2052, Australia, 2008.

4. Propriétés Topologiques

- i) C. Blanchet, *Propriétés topologiques des nombres réels*, Université Paris 7 (Denis Diderot), 2007.
- ii) N. Lanchier, *Propriétés topologiques de \mathbb{R}* , Arizona State University, School of Mathematical and Statistical Sciences, 2007.
- iii) E. Le Yaouanc, *Nombres Réels*, Université de Caen, Basse Normandie, 2006.
- iv) A. Decomps, *Nombres Réels, Droite Réelle*, Université de Lille 1.
- v) J. M. Erdman, *A ProblemText in Advanced Calculus*, Portland State University, Oregon, 2009.

II.6 Complexes \mathbb{C}

*L'ensemble des nombres complexes est un jeune frère
légèrement plus voyant mais encore respectable :
non ordonné, mais néanmoins algébriquement clos.*
John Baez³⁶

II.6.1 Introduction

La notion de racine d'un nombre négatif date de très, très longtemps : les premières références datent de Héron d'Alexandrie (~ 60), puis avec Diophante (275) qui posa la question de trouver un triangle rectangle dont le périmètre est 12 pieds et l'aire 7 pieds², 1275 ans plus tard Jérôme Cardan se posa une question similaire (et toujours sans solution réelle).

Le développement de la notion de racine d'un nombre négatif prit vraiment son essor au 16^{ième} siècle avec Niccolo Tartaglia, Scipion del Ferro, Rafael Bombelli et Jérôme Cardan dans la résolution d'équation du troisième degré. Cette utilisation des racines de nombres négatifs est effectivement plus convaincante que les tentatives de chercher des solutions réelles à des problèmes qui n'en ont pas ; en effet, les *nombres imaginaires* sont utilisés dans les calculs afin de trouver les racines **réelles** d'une équation du troisième degré (cf. infra pour un exemple de la méthode de Cardan).

II.6.2 Définition

Il existe plusieurs façon de définir les nombres complexes (voir par exemple [les nombres complexes comme \$\mathbb{R}\$ -algèbre de dimension 2](#)), Nous garderons, dans ce chapitre, une définition issue de considérations algébriques déjà vues.

Définition : $(\mathbb{C}, +, \cdot)$ est la clôture algébrique de $(\mathbb{R}, +, \cdot)$.

La clôture algébrique d'un corps est le plus petit corps le contenant et algébriquement clos (cf. [Clôture Algébrique des rationnels](#)).

II.6.3 Mode de construction

En tant qu'extension algébrique de $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ est de dimension finie (puisque \mathbb{R} est un **corps réel clos**), plus précisément, $[\mathbb{C} : \mathbb{R}] = 2$.

On peut construire les complexes, comme l'extension algébrique $\mathbb{R}[i]$, où $i^2 = -1$, c'est à dire que

$$\mathbb{C} = \{x_0 + ix_1 \mid (x_0, x_1) \in \mathbb{R}^2\}$$

x_0 est appelé la partie réelle de z et est notée $\Re(z)$,

x_1 est appelé la partie imaginaire de z et est notée $\Im(z)$.

L'addition est définie simplement : $(x_0 + ix_1) + (y_0 + iy_1) = (x_0 + y_0) + i(x_1 + y_1)$, il est immédiat de vérifier que cette addition confère à $(\mathbb{C}, +)$ une structure de groupe abélien.

La multiplication par un scalaire est aussi définie de façon très naturelle : $\lambda \times (x_0 + ix_1) = \lambda x_0 + i\lambda x_1$. Cette définition confère à $(\mathbb{C}, +, \times)$ une structure de \mathbb{R} -espace vectoriel de dimension 2.

La multiplication est définie par $(x_0 + ix_1) \cdot (y_0 + iy_1) = (x_0y_0 - x_1y_1) + i(x_0y_1 + x_1y_0)$ (en appliquant la distributivité de la multiplication sur l'addition).

Ces deux opérations font de $(\mathbb{C}, +, \cdot)$ un corps commutatif, qui vérifie le **théorème fondamental de l'algèbre** :

Tout polynôme de $\mathbb{C}[X]$ de degré n admet n racines (comptées avec leur multiplicité) dans \mathbb{C} .

36. Cité par Valentin Ovsienko (Lyon 1) comme résumé d'une conférence sur les algèbres au Laboratoire Paul Painlevé. Voir aussi : les [Réels](#), les [Quaternions](#), les [Octonions](#).

II.6.4 Table de multiplication

Pour définir complètement la multiplication des Complexes, il suffit de connaître la table de multiplication des éléments d'une base de \mathbb{C} (en tant que \mathbb{R} -Espace vectoriel), une base contenant seulement deux éléments, cette table de multiplication est particulièrement simple.

\cdot	1	i
1	1	i
i	i	-1

II.6.5 Conjugué, Module, Norme, Forme Polaire et Inverse

Soit $z = x_0 + ix_1 \in \mathbb{C}$, alors \bar{z} , le conjugué de z est défini par $\bar{z} = x_0 - ix_1$.
La conjugaison possède quelques propriétés intéressantes :

1. Involutive : $\overline{\bar{z}} = z$.
2. Additive : $\overline{(z + z')} = \bar{z} + \bar{z}'$.
3. Multiplicative : $\overline{(z \cdot z')} = \bar{z} \cdot \bar{z}'$.
4. $z + \bar{z} = 2\Re(z)$.
5. $z - \bar{z} = 2i\Im(z)$.
6. $z \cdot \bar{z} = x^2 + y^2 = (\Re(z))^2 + (\Im(z))^2 \in \mathbb{R}^+$.
7. On définit le module de z par : $|z| = \sqrt{z \cdot \bar{z}}$, et donc $|z \cdot z'| = |z| \cdot |z'|$. Nous noterons $\rho = |z|$.
8. $|z| = 0 \Leftrightarrow z = 0$.
9. $z \neq 0 \Rightarrow z^{-1} = \frac{\bar{z}}{|z|^2}$.

II.6.6 Interprétation géométrique

Comme $(\mathbb{C}, +, \times) \cong (\mathbb{R}^2, +, \times)$ en tant qu'espaces vectoriels, il est naturel d'identifier le complexe $z = x_0 + ix_1$, avec le point de \mathbb{R}^2 de coordonnées (x_0, x_1) (on dit que le point (x_0, x_1) est d'*affixe* z).

En remarquant que si z est différent de 0, on peut écrire $z = \rho \left(\frac{x_0}{\rho} + \frac{ix_1}{\rho} \right)$, alors le système d'équations :

$$\begin{cases} \cos(\theta) &= \frac{x_0}{\rho} \\ \sin(\theta) &= \frac{x_1}{\rho} \end{cases}$$

possède une et une seule solution (modulo 2π), qui est appelé l'*Argument de z* que nous noterons θ ou $\text{Arg}(z)$.

Attention : L'argument de 0 n'est pas défini.

Par conséquent, nous obtenons la relation suivante : $z = \rho(\cos(\theta) + i \sin(\theta))$, cette écriture est appelé la *forme trigonométrique de z* .

Rappelons que (\mathbb{K} est un corps de nombres de caractéristique 0 quelconque) $\forall z \in \mathbb{K}, e^z = \sum_{n=0}^{+\infty} \frac{z^n}{n!}$

On peut écrire la relation précédente de façon un peu différente :

$$\forall z \in \mathbb{K}, e^z = \sum_{n=0}^{+\infty} \frac{z^{4n}}{(4n)!} + \sum_{n=0}^{+\infty} \frac{z^{4n+1}}{(4n+1)!} + \sum_{n=0}^{+\infty} \frac{z^{4n+2}}{(4n+2)!} + \sum_{n=0}^{+\infty} \frac{z^{4n+3}}{(4n+3)!}$$

Dans le cas particulier où $z = ix$, nous pouvons ré-écrire cette relation ($i^2 = -1, i^3 = -i, i^4 = 1$) :

$$\forall x \in \mathbb{R}, e^{ix} = \sum_{n=0}^{+\infty} \frac{x^{4n}}{(4n)!} + \sum_{n=0}^{+\infty} \frac{ix^{4n+1}}{(4n+1)!} + \sum_{n=0}^{+\infty} \frac{-x^{4n+2}}{(4n+2)!} + \sum_{n=0}^{+\infty} \frac{-ix^{4n+3}}{(4n+3)!}$$

ou encore

$$\forall x \in \mathbb{R}, e^{ix} = \sum_{n=0}^{+\infty} \frac{x^{4n}}{(4n)!} + \sum_{n=0}^{+\infty} \frac{-x^{4n+2}}{(4n+2)!} + i \left(\sum_{n=0}^{+\infty} \frac{x^{4n+1}}{(4n+1)!} + \sum_{n=0}^{+\infty} \frac{-x^{4n+3}}{(4n+3)!} \right)$$

On reconnaît ci-dessus les séries entières définissant le $\cos(x)$ et le $\sin(x)$, d'où la formule d'Euler ³⁷ :
 $e^{ix} = \cos(x) + i \sin(x)$

Finalement nous pouvons écrire $z = \rho e^{i\theta}$, qui est appelé la *forme polaire* de z .

Sous cette dernière forme, la multiplication prend une forme particulièrement simple :
 $(\rho e^{i\theta}) \cdot (\rho' e^{i\theta'}) = \rho\rho' e^{i(\theta+\theta')}$.

Ce qui permet d'écrire (pour z et z' non nuls) :

1. $\text{Arg}(z \cdot z') = \text{Arg}(z) + \text{Arg}(z')$
2. $\text{Arg}\left(\frac{z}{z'}\right) = \text{Arg}(z) - \text{Arg}(z')$
3. $\text{Arg}(\bar{z}) = -\text{Arg}(z)$
4. $\text{Arg}(z^{-1}) = -\text{Arg}(z)$

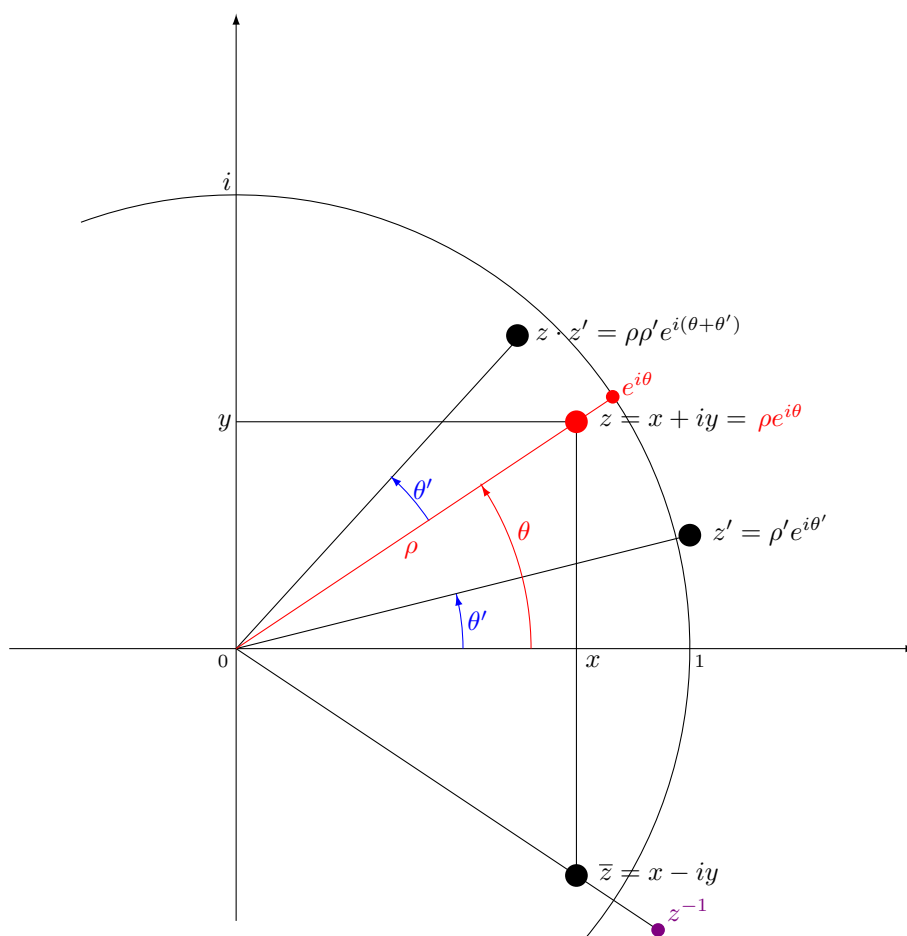


FIGURE 1 – Plan d'Argand-Cauchy

II.6.7 Propriétés algébriques

$(\mathbb{C}, +, \times)$ est un \mathbb{R} -espace vectoriel de dimension 2.

$(\mathbb{C}, +, \cdot)$ est un corps algébriquement clos (qui est une théorie complète) \aleph_1 -catégorique, c'est à dire qu'il n'existe pas de corps algébriquement clos de même cardinal que \mathbb{C} qui ne soit pas isomorphe à \mathbb{C} .

$(\mathbb{C}, +, \cdot, \times)$ est une \mathbb{R} -algèbre de dimension 2, voir [Les Complexes comme \$\mathbb{R}\$ -algèbre](#).

On peut noter que \mathbb{C} est complet au sens algébrique et au sens topologique, ce qui suggère de se poser la question : est-il utile d'aller plus loin ?

Ce document donne une réponse à cette question.

³⁷. Et la célèbre identité d'Euler : $e^{i\pi} = -1$.

II.6.8 Synonymes, Isomorphismes, Exemples

Une autre construction utilise le quotient d'un anneau par un de ses idéaux : $\mathbb{C} = \mathbb{R}[X]/(X^2 + 1)$.

II.6.9 Exemple d'utilisation des complexes dans la méthode de Cardan

Soit l'équation $x^3 - 3x + \sqrt{2} = 0$, en utilisant la méthode de Cardan :

On pose $x = u + v$, l'équation devient $u^3 + v^3 + (u + v)(3uv - 3) + \sqrt{2} = 0$.

En imposant la condition $uv = 1$, on obtient $u^3 + v^3 + \sqrt{2} = 0$.

L'équation du troisième degré du départ devient le système :

$$\begin{cases} u^3 v^3 & = & 1 \\ u^3 + v^3 & = & -\sqrt{2} \end{cases}$$

Les valeurs de u^3 et v^3 sont données par la résolution de l'équation : $X^2 + \sqrt{2}X + 1 = 0$.

$$\text{On trouve } \begin{cases} u^3 & = & \frac{-\sqrt{2} + i\sqrt{2}}{2} & = & e^{3i\frac{\pi}{4}} \\ v^3 & = & \frac{-\sqrt{2} - i\sqrt{2}}{2} & = & e^{-3i\frac{\pi}{4}} \end{cases} \text{ d'où } \begin{cases} u_0 & = & \sqrt[3]{\frac{-\sqrt{2} + i\sqrt{2}}{2}} & = & (e^{3i\frac{\pi}{4}})^{\frac{1}{3}} & = & e^{i\frac{\pi}{4}} \\ v_0 & = & \sqrt[3]{\frac{-\sqrt{2} - i\sqrt{2}}{2}} & = & (e^{-3i\frac{\pi}{4}})^{\frac{1}{3}} & = & e^{-i\frac{\pi}{4}} \end{cases}$$

Où u_0 et v_0 sont des racines cubiques particulières, et en posant $j = e^{2i\frac{\pi}{3}}$ (une racine cubique de l'unité), les solutions sont

$$\begin{aligned} x_1 &= u_0 + v_0 = e^{i\frac{\pi}{4}} + e^{-i\frac{\pi}{4}} = 2 \cos\left(\frac{\pi}{4}\right) = \sqrt{2}. \\ x_2 &= ju_0 + j^2v_0 = e^{2i\frac{\pi}{3}} \cdot e^{i\frac{\pi}{4}} + e^{4i\frac{\pi}{3}} \cdot e^{-i\frac{\pi}{4}} = e^{11i\frac{\pi}{12}} + e^{-11i\frac{\pi}{12}} = 2 \cos\left(\frac{11\pi}{12}\right). \\ x_3 &= j^2u_0 + jv_0 = e^{4i\frac{\pi}{3}} \cdot e^{i\frac{\pi}{4}} + e^{2i\frac{\pi}{3}} \cdot e^{-i\frac{\pi}{4}} = e^{19i\frac{\pi}{12}} + e^{-19i\frac{\pi}{12}} = 2 \cos\left(\frac{19\pi}{12}\right). \end{aligned}$$

On constate que l'on a utilisé les nombres complexes explicitement (pour les valeurs de u^3 et v^3 et aussi pour calculer les racines cubiques sous forme trigonométrique), pour calculer ... des nombres réels.

II.6.10 Utilisation en physique

La liste des usages des nombres complexes en physiques est pléthoriques, voici quelques exemples :

- Tout phénomène qui se mesure par une grandeur qui est une fonction sinusoïdale du temps, d'équation $f(t) = K \cos(\omega t + \varphi)$, on peut faire correspondre le nombre complexe $z(t) = K e^{i(\omega t + \varphi)}$ ³⁸, alors $f(t) = \Re(z(t))$.

- En courant alternatif en régime sinusoïdal, on utilise l'impédance complexe Z d'un circuit (RLC), ce qui

$$\text{simplifie les calculs } \begin{cases} \text{Résistance} & : & Z & = & R \\ \text{Inductance} & : & Z & = & iL\omega \\ \text{Capacité} & : & Z & = & \frac{-i}{C\omega} \end{cases}$$

- Description des oscillateurs électriques.
- Electromagnétisme.
- Traitement du signal au travers de l'analyse de Fourier : Soit f une fonction intégrable sur \mathbb{R} sa transformée de Fourier est la fonction $\mathcal{F}(f) = \hat{f}$ définie par $\hat{f}(t) = \int_{-\infty}^{+\infty} f(x) e^{-i2\pi tx} dx$
- Mécanique des fluides.
- Relativité générale.
- Mécanique quantique.

II.6.11 Références

1. *Nombres complexes*, ENS.
2. F. Sturm, *Les nombres complexes*, INSA-Lyon, 2010-2011.
3. J.-B. Hiriart-Urruty, *Les nombres complexes de A à ... Z*, Université de Toulouse, 2009.
4. L. Leroux, *Nombres complexes*, Université de Caen, 2007-2008.

³⁸. Les physiciens utilisent généralement j en place de i .

III Variations sur la hiérarchie algébrique

III.1 Décimaux \mathbb{D}

III.1.1 Introduction

L'ensemble des nombres décimaux, noté traditionnellement \mathbb{D} , est un sous ensemble des **nombres rationnels**, mais nous allons plutôt le construire comme un sur-ensemble de l'ensemble des **entiers relatifs**.

III.1.2 Définition

\mathbb{D} est constitué des fractions dont le dénominateur est une puissance de 10, et pour être parfaitement intuitif, on peut ajouter que c'est l'ensemble des nombres réels dont le développement décimal *propre* est à support fini (ne contient que des 0 à partir d'un certain rang), mais cette définition fait appel aux réels contrairement à la première.

L'ensemble des décimaux est aussi exactement l'ensemble des **nombres réels** ayant deux développements décimaux l'un, dit propre, avec un nombre fini de décimales, l'autre, dit impropre, avec un développement décimal périodique (de période 1) à partir d'un certain rang et constitué uniquement de 9 à partir de ce rang, par exemple $3, 25 = 3.24\underline{9}$ (pour rappel, les chiffres soulignés identifient la partie périodique du développement).

L'ensemble \mathbb{D} présente un avantage sur \mathbb{N} , c'est que l'on peut y effectuer certaines divisions (pas toutes), et un avantage sur \mathbb{Q} , c'est que le développement décimal y est fini.

III.1.3 Mode de construction

Les nombres décimaux peuvent se construire à partir des entiers relatifs en munissant $(\mathbb{Z} \times \mathbb{N})$ d'une addition, d'une multiplication, et en faisant le quotient de $(\mathbb{Z} \times \mathbb{N})$ par une relation d'équivalence compatible avec les opérations.

L'addition sur $(\mathbb{Z} \times \mathbb{N})$ est définie par $(a, b) + (a', b') = (a \cdot 10^{b'} + a' \cdot 10^b, b + b')$

La multiplication sur $(\mathbb{Z} \times \mathbb{N})$ est définie par $(a, b) \cdot (a', b') = (aa', b + b')$.

On peut aussi définir une relation d'ordre qui prolonge celle sur \mathbb{Z} : $(a, b) < (a', b') \Leftrightarrow a \cdot 10^{b'} < a' \cdot 10^b$.

La relation d'équivalence est définie par $(a, b) \simeq (a', b') \Leftrightarrow a \cdot 10^{b'} = a' \cdot 10^b$

L'application $\pi : \mathbb{Z} \mapsto (\mathbb{Z} \times \mathbb{N}) / \simeq$ définie par $\pi(a) = \overline{(a, 0)}$, permet de plonger canoniquement $(\mathbb{Z}, +, \cdot)$ dans $((\mathbb{Z} \times \mathbb{N}) / \simeq, +, \cdot)$.

Usuellement un élément de \mathbb{D} , c'est à dire la classe d'un élément de $(\mathbb{Z} \times \mathbb{N})$ pour la relation \simeq est représenté sous forme de fraction : $\overline{(a, b)} = \frac{a}{10^b}$, ou sous la forme de son développement décimal (qui est fini).

III.1.4 Conjugué, Module, Norme, Forme Polaire et Inverse

La valeur absolue de \mathbb{Z} peut se prolonger à \mathbb{D} (et c'est bien une norme sur \mathbb{D}) : $|\overline{(a, b)}| = \overline{(|a|, b)}$.

L'inverse, quand il existe, d'un décimal, non nul, sous la forme d'une classe d'équivalence n'est pas très utile (utilise le logarithme en base 10), alors que sous sa forme fractionnaire, le résultat est évident : $\left(\frac{a}{10^b}\right)^{-1} = \frac{10^b}{a}$, mais ceci n'est valide que si cette fraction est bien un nombre décimal, c'est à dire si et seulement si $a = 2^n \cdot 5^m$ où n et m sont des entiers naturels.

III.1.5 Propriétés algébriques

$(\mathbb{D}, +, \times, <)$ est un anneau unitaire, commutatif, intègre et ordonné, mais ce n'est pas un corps, puisque certains éléments, 3 par exemple, n'ont pas d'inverse.

L'ensemble des décimaux est dénombrable : $|\mathbb{D}| = \aleph_0$ (cf. [les cardinaux](#)).

$(\mathbb{D}, <)$ est un ordre total, dense sans extremums donc isomorphe à $(\mathbb{Q}, <)$.

Le corps des fractions de $(\mathbb{D}, +, \times, <)$ est, bien évidemment $(\mathbb{Q}, +, \times, <)$.

Pour la topologie usuelle, celle induite par la valeur absolue, \mathbb{D} est dense dans \mathbb{R} (attention la densité pour la relation d'ordre et la densité pour la topologie ne sont pas synonymes).

III.1.6 Synonymes, Isomorphismes, Exemples

Voir le chapitre sur les [nombres dyadiques](#) (à ne pas confondre avec les [nombres diadiques](#)).

III.1.7 Utilisation en physique

Les décimaux ne sont pas, à ma connaissance, utilisés en physique pour des besoins théoriques (ce qui n'interdit pas de théoriser leur utilité), comme peuvent l'être les [réels](#), les [complexes](#) ou les [quaternions](#), par contre seuls les décimaux sont utilisés par les instruments de mesure (c'est criant pour ceux à affichage digital) et dans les calculs pratiques ; la densité de \mathbb{D} dans \mathbb{R} et la facilité d'utilisation des décimaux en sont les principales causes (avec l'incertitude des mesures).

Finalement, devant la paillasse, le physicien n'utilise que des décimaux.

III.1.8 Références

1. [Nicolas Bourgeois](#)
2. [Raphaël Galante](#)

III.2 Entiers de Gauss $\mathbb{Z}[i]$

III.2.1 Introduction

L'ensemble des entiers de Gauss, qui sera noté $\mathbb{Z}[i]$, est nommé ainsi d'après le nom de Johann Carl Friedrich Gauss, un mathématicien allemand (1777 – 1855) qui a été surnommé le Prince des Mathématiciens.

III.2.2 Définition

Les entiers de Gauss sont les nombres complexes de la forme $n_0 + in_1$, où n_0 et n_1 sont des nombres entiers relatifs, c'est-à-dire forment un ensemble isomorphe à $\mathbb{Z} + i\mathbb{Z}$, ce qui justifie la notation $\mathbb{Z}[i]$.

III.2.3 Table de multiplication

Comme i est bien le nombre complexe i vérifiant $i^2 = -1$, on peut mettre en place la table de multiplication (celle de (\mathbb{C}, \times) en fait) :

\times	1	i
1	1	i
i	i	-1

Entiers de Gauss : $\mathbb{Z}[i]$.

III.2.4 Conjugué, Module, Norme, Forme Polaire et Inverse

Du fait de l'inclusion $\mathbb{Z}[i] \subset \mathbb{C}$, le conjugué naturel d'un entier de Gauss est son conjugué au sens complexe : $\overline{n_0 + in_1} = n_0 - in_1$.

Et la norme est aussi la norme au sens complexe (elle est donc multiplicative et vérifie $N(g) = N(\bar{g})$), ce qui donne

$$|g|^2 = N(g) = g\bar{g} = |n_0 + in_1|^2 = N(n_0 + in_1) = n_0^2 + n_1^2.$$

Le groupe des unités de $\mathbb{Z}[i]$, qui correspond aussi au groupe des inversibles de $\mathbb{Z}[i]$ est l'ensemble des entiers de Gauss de norme 1, donc $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$ ³⁹.

Et bien sur, l'inverse est l'inverse au sens de \mathbb{C} , mais le résultat ($z^{-1} = \frac{\bar{z}}{|z|^2}$) n'est pas forcément un entier de Gauss, seuls les éléments du groupe des unités ont un inverse dans $\mathbb{Z}[i]$.

III.2.5 Propriétés algébriques

$(\mathbb{Z}[i], +, \times)$ est un anneau unitaire, commutatif et intègre (c'est un sous-anneau de $(\mathbb{C}, +, \times)$), dont tous les éléments sont des entiers algébriques⁴⁰ du corps $\mathbb{Q}(i)$, c'est aussi un anneau principal.

$(\mathbb{Z}[i], +, \times, \cdot)$ est une \mathbb{Z} -algèbre (c'est à dire un \mathbb{Z} -module muni d'une multiplication) de dimension 2.

La norme, N , d'un entier de Gauss est donc toujours un entier naturel⁴¹ (strictement positif, sauf pour 0) qui est un stathme qui permet de munir $\mathbb{Z}[i]$ d'une division euclidienne :

$$\forall \alpha \in \mathbb{Z}[i] \forall \beta \in \mathbb{Z}[i]^* \exists q \in \mathbb{Z}[i] \exists r \in \mathbb{Z}[i] ((\alpha = q\beta + r) \wedge (N(r) < N(\beta)))$$

L'algorithme de calcul du quotient (q) et du reste (r) est assez simple :

On commence par calculer : $\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{N(\beta)}$, la division restante est une division par un nombre entier, elle est donc facile à effectuer ; avec des nombres entiers naturels, il suffirait de prendre la partie entière du résultat pour avoir le quotient, puis le reste est facile à calculer, cette méthode permet d'avoir un reste positif, en prenant l'arrondi on pourrait avoir un reste négatif, mais de norme minimale, c'est cette dernière méthode que nous allons mettre en oeuvre, sur un exemple :

$$\text{Calculons le quotient et le reste de } (-15 + 17i) = (3 + 4i)q + r : \frac{\alpha\bar{\beta}}{N(\beta)} = \frac{23 + 111i}{25}.$$

^{39.} A^\times représente l'ensemble des inversibles de A , à ne pas confondre avec A^* qui représente l'ensemble des éléments non nuls de A .

^{40.} $(n_0 + in_1)$ est solution du polynôme $x^2 - (2n_0)x + (n_0^2 + n_1^2)$.

^{41.} On peut noter que certains nombres entiers ne sont pas la norme d'un entier de Gauss, par exemple 3, qui n'est pas la somme de deux carrés

En prenant les parties entières, on peut d'écrire :

$(-15+17i) = (3+4i)(4i)+r$ on trouve immédiatement que $r = 1+5i$, mais $N(1+5i) = 26 > N(3+4i) = 25$, ce qui n'est donc pas acceptable.

En prenant le plus proche entier, on peut d'écrire : $(-15+17i) = (3+4i)(1+4i)+r$ on trouve immédiatement que $r = -2+i$, et cette fois $N(-2+i) = 5 < N(3+4i) = 25$, solution acceptable.

Finalement, nous pouvons donc écrire $(-15+17i) = (3+4i)(1+4i) + (-2+i)$

Un entier de Gauss g est premier si et seulement si

$$\forall u \in \mathbb{Z}[i] \forall v \in \mathbb{Z}[i] (g = uv \Leftrightarrow ((u \in \mathbb{Z}[i]^\times) \vee (v \in \mathbb{Z}[i]^\times)))$$

Tous les entiers de Gauss admettent une factorisation unique en produit de facteurs qui sont des entiers de Gauss premiers. Mais attention, unique, ici, veut dire « unique à l'ordre et à un produit d'unités près ».

Les entiers de Gauss premiers sont parfaitement définis (à un produit par une unité près) :

- $\forall \alpha \in \mathbb{Z}[i] (N(\alpha) \in \mathbb{P} \Rightarrow \alpha \text{ est premier dans } \mathbb{Z}[i]).$
- $\forall p \in \mathbb{P} (p \equiv 3[4] \Rightarrow p \text{ est premier dans } \mathbb{Z}[i]).$

Remarque : 2, 5, 13 etc. sont premiers dans \mathbb{Z} mais pas dans $\mathbb{Z}[i]$:

$$\begin{aligned} 2 &= (1-i) \times (1+i) \\ 5 &= (1-2i) \times (1+2i) = (2+i) \times (2-i) \\ 13 &= (3-2i) \times (3+2i) = (2-3i) \times (2+3i) \end{aligned}$$

Les nombres premiers (dans \mathbb{Z}) p impairs qui peuvent s'écrire comme la somme de deux carrés sont exactement les nombre premiers de la forme $p \equiv 1[3]$ (et alors $p = a^2 + b^2 \Rightarrow p = (a-ib)(a+ib)$).

D'une façon plus générale, on peut citer le théorème :

Théorème : Un entier n peut s'écrire comme la somme de deux carrés si et seulement si :

$$\left(\prod_{\substack{j=0 \\ p_j \in \mathbb{P} \\ p_j \not\equiv 3[4]}}^{j=n} p_j^{\alpha_j} \right) \times \left(\prod_{\substack{j=0 \\ p_j \in \mathbb{P} \\ p_j \equiv 3[4]}}^{j=m} p_j^{2\beta_j} \right)$$

III.2.6 Synonymes, Isomorphismes, Exemples

On aurait aussi pu construire $\mathbb{Z}[i]$ à l'aide de polynômes⁴² (technique usuelle) : $\mathbb{Z}[i] \sim \mathbb{Z}[X]/(X^2 + 1)$:

Soit $P \in \mathbb{Z}[X]$, nous noterons \hat{P} la classe de P dans le quotient $\mathbb{Z}[X]/(X^2 + 1)$

L'application $\varphi : \mathbb{Z}[X]/(X^2 + 1) \mapsto \mathbb{Z}[i]$ définie par : $\varphi(\hat{P}) = P(i)$ ⁴³ est un isomorphisme dans le langage des anneaux.

On peut utiliser l'arithmétique dans $\mathbb{Z}[i]$ pour démontrer des résultats dans l'arithmétique de \mathbb{Z} , par exemple :

- Démontrer qu'un nombre premier qui est somme de deux entiers l'est de façon unique (à l'ordre et au signe près).
- Etablir une classification des triplets Pythagoriciens.
- La seule solution de $x^3 = y^2 + 1$ est $(1, 0)$.
- Recherche des entiers qui sont sommes de deux carrés de plusieurs façons différentes (sans tenir compte de l'ordre ou du signe).

De la même façon que l'on peut étudier l'arithmétique modulaire dans \mathbb{Z} , on peut étudier l'arithmétique modulaire dans $\mathbb{Z}[i]$:

$$\begin{aligned} \forall n \in \mathbb{N}^* (\mathbb{Z}[i]/(n) \sim \mathbb{Z}_n[i]) \\ \forall n \in (\mathbb{N}^* \setminus \{1\}) (\mathbb{Z}_n[X]/(X^2 + 1) \sim \mathbb{Z}_n[i]) \end{aligned}$$

42. En notant (z) l'idéal engendré par l'élément z dans un anneau quelconque.

43. Il est immédiat de vérifier que cette définition ne dépend pas du polynôme choisi dans sa classe d'équivalence.

III.2.7 Ecriture des entiers de Gauss dans un système de numération positionnelle

Ecrire un nombre entier n en base b (b est un nombre entier) revient à écrire :

$$n = \sum_{j=0}^k a_j b^j \text{ où } a_j \in [0, b-1].$$

Nous écrirons $(\alpha\beta\gamma\cdots)_{(b)}$ pour indiquer que l'écriture $\alpha\beta\gamma\cdots$ est en base b , b lui-même étant écrit en base 10.

Katái & Szabó ont démontré que tous les entiers de Gauss⁴⁴ peuvent s'écrire de manière unique en base $(-n+i)$ ⁴⁵, quelque soit n entier naturel : $g = \sum_{j=0}^k a_j (-n+i)^j$ où $a_j \in [0, n^2]$

Tous les entiers de Gauss peuvent donc s'écrire comme une chaîne de « chiffres » et on peut redéfinir addition et multiplication sous cette forme, la seule *difficulté* dans les calculs vient des retenues qui sont un peu plus compliquée que dans le cas habituel.

Deux remarques qui permettent d'effectuer facilement les opérations :

$$\begin{aligned} (-n+i)^3 + (2n-1)(-n+i)^2 + (n-1)^2(-n+i) &= n^2 + 1 \\ (-n+i)^2 + 2n(-n+i) + n^2 + 1 &= 0 \end{aligned}$$

Cette égalité permet de savoir ce qu'il faut ajouter lorsqu'il y a une retenue.

Dans le cas particulier où $n=3$ (les chiffres autorisés sont donc $[0, 9]$) on obtient que $(10)_{(10)} = (1540)_{(-3+i)}$ et $(16(10))_{(-3+i)} = 0$ (attention cette écriture n'est pas propre puisque $10 > 9$).

Notons tout de suite que $(-3+i)^2 = 8 - 6i$ et $(-3+i)^3 = -18 + 26i$.

La traduction de la base $-3+i$ vers base 10 est très simple, il suffit d'appliquer la définition :

$$(4521)_{(-3+i)} = 4(-3+i)^3 + 5(-3+i)^2 + 2(-3+i) + 1 = 4(-18 + 26i) + 5(8 - 6i) + 2(-3+i) + 1 = -37 + 76i$$

La traduction de la base 10 vers base $-3+i$ est un peu plus compliquée, mais en utilisant une des remarques précédentes, on peut mettre en place un algorithme très simple :

Exemple : $7 - 5i = -5(3+i) - 8$, ce premier calcul est très simple, mais -5 et -8 ne sont pas des chiffres acceptables, il suffit d'ajouter 0 pour obtenir :

$$7 - 5i = -5(-3+i) - 8 + (-3+i)^2 + 6(-3+i) + 10 = (-3+i)^2 + (-3+i) + 2 = (112)_{(-3+i)}$$

On peut présenter cette opération de façon plus simple, même dans un cas un peu plus compliqué : comment écrire $(-19)_{(10)}$ en base $(-3+i)$?

					-19	Départ en base 10. Une décimale doit être comprise entre 0 et 9
2	12	20				Ajout de 2 fois (1 - 6 - 10) à cause du -19
2	12	1				Somme des deux lignes précédentes
-1	-6	-10	0			Soustraction de (1 - 6 - 10) × 10 à cause du 12
-1	-4	2	1			Somme des deux lignes précédentes
1	6	10	0	0		Ajout de (1 - 6 - 10) × 100 à cause du -4
1	5	6	2	1		Somme des deux lignes précédentes

La dernière ligne nous donne $(-19)_{(10)} = (15621)_{(-3+i)}$.

Dans le cas général, la première étape consiste à écrire le nombre à convertir sous la forme $a(-3+i) + b$, alors la première ligne du tableau commence par a dans l'avant dernière colonne et b dans la dernière.

44. Cette écriture des entiers de Gauss se généralisent à \mathbb{C} .
 45. Cela marche aussi avec $(-n-i)$, et ce sont les seuls cas.

Calculons par exemple $(905)_{(-3+i)} + (655)_{(-3+i)}$:

9 0 5	C'est à dire $(77 - 54i)$
6 5 5	C'est à dire $(38 - 31i)$
5 5 0	Somme sans tenir compte des retenues cf. ci-dessous
1 5 4 0	Retenue due à $5 + 5$ de la dernière colonne
1 5 4 0	Retenue due à $9 + 6$ de la colonne 6
1 5 5 0 9 0	Somme des trois lignes précédentes sans tenir compte des retenues
1 5 4 0	Retenue due à $5 + 5$ de la colonne 6
2 0 9 0 9 0	Somme des deux lignes précédentes sans tenir compte des retenues
1 5 4 0	Retenue due à $5 + 5$ de la colonne 4
1 5 6 0 9 0 9 0	Somme des deux lignes précédentes = $(115 - 85i)$

Nous avons donc trouvé que $(905)_{(-3+i)} + (655)_{(-3+i)} = (15609090)_{(-3+i)}$, ou avec les notations habituelles : $(77 - 54i) + (38 - 31i) = (115 - 85i)$.

Calculons par exemple $(37)_{(-3+i)} \times (148)_{(-3+i)}$

3 7	C'est à dire $(-2 + 3i)$
1 4 8	C'est à dire $(4 - 2i)$
24 56	Multiplication usuelle sans propager de retenue
12 28	Multiplication usuelle sans propager de retenue
3 7	Multiplication usuelle sans propager de retenue
3 19 52 56	Somme des trois lignes précédentes sans propager la retenue
-5 -30 -50	Soustraction de $(1 - 6 - 10) \times 5$ à cause du 56
3 14 22 6	Somme des deux lignes précédentes sans propager la retenue
-2 -12 -20 0	Soustraction de $(1 - 6 - 10) \times 20$ à cause du 22
1 2 2 6	Somme des deux lignes précédentes = $(-2 + 16i)$

Nous avons donc trouvé que $(37)_{(-3+i)} \times (148)_{(-3+i)} = (1226)_{(-3+i)}$, ou avec les notations habituelles : $(-2 + 3i) \times (4 - 2i) = (-2 + 16i)$

III.2.8 Utilisation en physique

L'ensemble des Entiers de Gauss ne semble pas beaucoup utilisé en physique, néanmoins, on trouve :

- Les Entiers de Gauss dans l'étude des variétés de Calabi-Yau.
- Le groupe modulaire de Picard $(SU(2, 1; \mathbb{Z}[i]))$ est utilisé en physique quantique.

III.2.9 Références

1. P. Caldero, *L'Arithmétique de $\mathbb{Z}[I]$* , Université de Lyon 1, Agrégation interne.
2. A. Míngues, *Les Entiers de Gauss*, Université de Paris-Jussieu, 2010.
3. B. Edixhoven, L. Moret-Bailly, *Cours de Maîtrise de Mathématiques : Théorie Algébrique des Nombres*, Université de Rennes 1, 2004.
4. P. L. Clark, *The Gaussian Integers I : The Fundamental Theorem*, University of Georgia.
5. G. E. Collins, *A Fast Euclidean Algorithm for Gaussian Integers*, Journal of Symbolic Computation, Volume 33, p. 385–392, 2002.

III.3 Nombres entiers d'Eisenstein $\mathbb{Z}[j]$

III.3.1 Introduction

L'ensemble des entiers d'Eisenstein, qui sera noté $\mathbb{Z}[j]$, est nommé ainsi d'après le nom de Ferdinand Gotthold Max Eisenstein, un mathématicien allemand (1823 - 1852) qui faisait l'admiration de Gauss lui-même.

III.3.2 Définition

Les entiers d'Eisenstein sont les nombres complexes de la forme $n_0 + jn_1$, où n_0 et n_1 sont des nombres entiers relatifs, c'est-à-dire forment un ensemble isomorphe à $\mathbb{Z} + j\mathbb{Z}$, ce qui justifie la notation $\mathbb{Z}[j]$.

III.3.3 Table de multiplication

Comme $j = \frac{-1 + i\sqrt{3}}{2}$, une racine cubique de l'unité, il est immédiat de vérifier que $1 + j + j^2 = 0$, on peut donc dresser la table de multiplication :

·	1	j
1	1	j
j	j	-1 - j

Entiers d'Eisenstein : $\mathbb{Z}[j]$.

III.3.4 Conjugué, Module, Norme, Forme Polaire et Inverse

Du fait de l'inclusion $\mathbb{Z}[j] \subset \mathbb{C}$, le conjugué naturel d'un entier d'Eisenstein est son conjugué au sens complexe : $\overline{n_0 + jn_1} = n_0 + \overline{j}n_1$ (on peut vérifier facilement que $\overline{j} = j^2 = -1 - j$).

Et la norme est aussi la norme au sens complexe (elle est donc multiplicative), ce qui donne $|n_0 + jn_1|^2 = N(n_0 + jn_1) = (n_0 - \frac{n_1}{2})^2 + \frac{3n_1^2}{4} = n_0^2 - n_0n_1 + n_1^2$, le groupe des unités de $\mathbb{Z}[j]$ est donc $\{\pm 1, \pm j, \pm j^2\}$.

N , tel que défini ci-dessus, est un stathme qui permet de munir $\mathbb{Z}[j]$ d'une division euclidienne.

La norme d'un entier d'Eisenstein est donc toujours un entier naturel (strictement positif, sauf pour 0).

Et bien sur, l'inverse est l'inverse au sens de \mathbb{C} , mais le résultat $\left(z^{-1} = \frac{\overline{z}}{|z|^2}\right)$ n'est pas forcément un entier d'Eisenstein.

III.3.5 Propriétés algébriques

$(\mathbb{Z}[j], +, \times)$ est un anneau euclidien, unitaire, commutatif et intègre (c'est un sous-anneau de $(\mathbb{C}, +, \times)$), dont tous les éléments sont des entiers algébriques⁴⁶ du corps $\mathbb{Q}(j)$.

$(\mathbb{Z}[j], +, \times, \cdot)$ est une \mathbb{Z} -algèbre (c'est à dire un \mathbb{Z} -module muni d'une multiplication) de dimension 2.

On peut définir la notion de nombre premier dans $\mathbb{Z}[j]$, de façon assez proche de son équivalent dans \mathbb{Z} :

$$z \in \mathbb{Z}[j] \text{ est premier} \Leftrightarrow (\forall u \in \mathbb{Z}[j] \forall v \in \mathbb{Z}[j] (z = uv \Rightarrow (N(u) = 1 \vee N(v) = 1))).$$

Un nombre premier dans \mathbb{Z} n'est pas forcément premier dans $\mathbb{Z}[j]$, par exemple 7 n'est pas premier dans $\mathbb{Z}[j]$ ($7 = (3 + j)(2 - j)$).

En remarquant : $N(n_0 + jn_1) = n_0^2 - n_0n_1 + n_1^2 = (n_0 + n_1)^2 - 3n_0n_1$, on peut noter $N(z) \not\equiv 2 \pmod{3}$.

Tout entier d'Eisenstein se décompose de façon unique en facteurs premiers d'Eisenstein, mais, attention, unique, ici, veut dire à l'ordre et à un produit par une unité près. Par exemple $7 = (3 + j)(2 - j) = (3 + 2j)(1 - 2j)$, mais on peut vérifier facilement que $(3 + j)(-j) = 1 - 2j$ et $(2 - j)(-j^2) = 3 + 2j$.

46. $(n_0 + jn_1)$ est solution du polynôme $x^2 - (2n_0 - n_1)x + (n_0^2 - n_0n_1 + n_1^2)$.

On appelle élément premier de $\mathbb{Z}[j]$, tout élément irréductible de $\mathbb{Z}[j]$.

x est premier dans $\mathbb{Z}[j]$ si et seulement si :

1. $x = 1 - i$.
2. $(x \in \mathbb{P}) \wedge (x \equiv 2 [3])$, c'est à dire un nombre premier de \mathbb{Z} congru à 2 modulo 3.
3. $(|x|^2 \in \mathbb{P}) \wedge (|x| \equiv 1 [3])$

Une conséquence immédiate du point 3 ci-dessus est que si p est un nombre premier dans \mathbb{Z} , il peut s'écrire sous la forme $p = x^2 - xy + y^2$ si et seulement si $p \not\equiv 2 [3]$.

Définition : Un réseau de \mathbb{R}^n est un sous-groupe discret de $(\mathbb{R}^n, +)$, tel que le sous-espace vectoriel qu'il engendre soit \mathbb{R}^n , tout entier.

$\mathbb{Z}[j]$ est un réseau triangulaire, c'est d'ailleurs le réseau le plus dense de \mathbb{R}^2 .

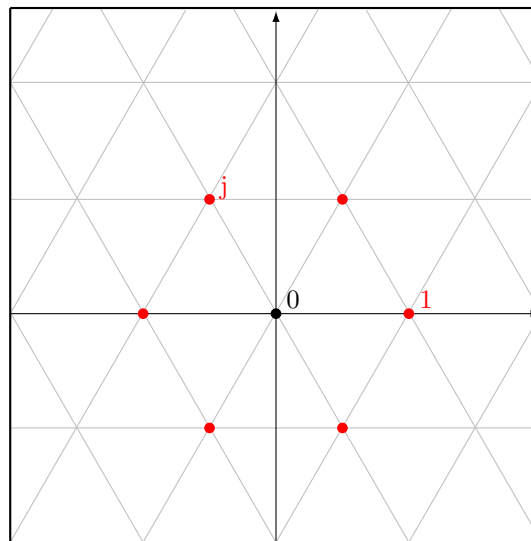


FIGURE 2 – Réseau triangulaire des entiers d'Eisenstein $\mathbb{Z}[j]$

Dans la figure ci-dessus, les points rouges correspondent aux six unités de $\mathbb{Z}[j]$.

III.3.6 Synonymes, Isomorphismes, Exemples

On aurait aussi pu construire $\mathbb{Z}[j]$ à l'aide de polynômes (technique usuelle pour étendre un anneau) : $\mathbb{Z}[j] \sim \mathbb{Z}[X]/(X^2 + X + 1)$

Il est aussi possible d'étudier les entiers d'Eisenstein modulo n , c'est à dire $\mathbb{Z}[j]/n\mathbb{Z}[j]$; on peut démontrer que $\mathbb{Z}[j]/n\mathbb{Z}[j] \sim \mathbb{Z}_n[j]$.

III.3.7 Utilisation en physique

Les entiers de Eisenstein sont utilisés pour des méthodes d'encryption à clé publique (ETRU, par exemple).

III.3.8 Références

1. O. Alkam & E. Abu Osba, *On Eisenstein Integers Modulo n* , International Mathematical Forum, Volume 5, No. 22, p. 1075 - 1082, 2010.
2. K. Jarvis, *NTRU over the Eisenstein Integers*, Thèse soumise à la Faculté des Sciences, University d'Ottawa, Canada, 2011.
3. A. Kumar, *Lattices, Sphere Packings and Voronoi's Theorem*, Conférence au MIT.

III.4 Dyadiques \mathfrak{D}

III.4.1 Introduction

Ceux qui ont lu le chapitre sur les **nombre**s **décimaux**, ne trouveront rien de nouveau dans ce chapitre, sauf la généralisation que l'on trouve dans la sous-section **Synonymes, Isomorphismes, Exemples**, et surtout la sous-section **Utilisation en informatique**.

L'ensemble des nombres dyadiques⁴⁷, que nous noterons \mathfrak{D} , est un sous ensemble des **nombre**s **rationnels**, mais nous allons plutôt le construire comme un sur-ensemble de l'ensemble des **entiers relatifs**, sur le même modèle que la construction des **nombre**s **décimaux**.

III.4.2 Définition

\mathfrak{D} est constitué des fractions dont le dénominateur est une puissance de 2, et pour être parfaitement intuitif, on peut ajouter que c'est l'ensemble des nombres réels dont le développement binaire *propre* est à support fini (ne contient que des 0 à partir d'un certain rang), mais cette définition fait appel aux réels contrairement à la première.

L'ensemble des dyadiques est aussi exactement l'ensemble des **nombre**s **réels** ayant deux développements binaires l'un, dit propre, avec un nombre fini de décimales, l'autre, dit impropre, avec un développement binaire périodique (de période 1) à partir d'un certain rang et constitué uniquement de 1 à partir de ce rang.

III.4.3 Mode de construction

Les nombres dyadiques peuvent se construire à partir des entiers relatifs naturels en munissant $(\mathbb{Z} \times \mathbb{N})$ d'une addition, d'une multiplication, et en faisant le quotient de $(\mathbb{Z} \times \mathbb{N})$ par une relation d'équivalence compatible avec les opérations.

L'addition sur $(\mathbb{Z} \times \mathbb{N})$ est définie par $(a, b) + (a', b') = (a \cdot 2^{b'} + a' \cdot 2^b, b + b')$.

La multiplication sur $(\mathbb{Z} \times \mathbb{N})$ est définie par $(a, b) \cdot (a', b') = (aa', b + b')$.

La relation d'équivalence est définie par $(a, b) \simeq (a', b') \Leftrightarrow a \cdot 2^{b'} = a' \cdot 2^b$.

L'application $\pi : \mathbb{Z} \mapsto (\mathbb{Z} \times \mathbb{N}) / \simeq$ définie par $\pi(a) = \overline{(a, 0)}$, permet de plonger canoniquement $(\mathbb{Z}, +, \cdot)$ dans $(\mathbb{Z} \times \mathbb{N} / \simeq, +, \cdot)$.

III.4.4 Conjugué, Module, Norme, Forme Polaire et Inverse

Comme pour les décimaux, on peut définir une norme sur \mathfrak{D} qui est tout simplement la restriction à \mathfrak{D} de la norme usuelle sur \mathbb{Q} .

III.4.5 Propriétés algébriques

$(\mathfrak{D}, +, \cdot, <)$ est un anneau unitaire, commutatif, intègre et ordonné, mais ce n'est pas un corps, puisque certains éléments, 3 par exemple, n'ont pas d'inverse.

L'ensemble des dyadiques est dénombrable : $|\mathfrak{D}| = \aleph_0$ (cf. **les cardinaux**).

$(\mathfrak{D}, <)$ est un ordre total, dense sans extremums donc isomorphe à $(\mathbb{Q}, <)$.

Le corps des fractions de $(\mathfrak{D}, +, \times, <)$ est, bien évidemment $(\mathbb{Q}, +, \times, <)$.

Pour la topologie usuelle, celle induite par la valeur absolue, \mathfrak{D} est dense dans \mathbb{R} (attention la densité pour la relation d'ordre et la densité pour la topologie ne sont pas synonymes).

47. A ne pas confondre avec les nombres diadiques qui sont les nombres 2-adiques, cas particulier des **nombre**s **p-adiques**.

III.4.6 Synonymes, Isomorphismes, Exemples

On peut généraliser la notion de nombre décimal et de nombre dyadique très facilement : L'ensemble de nombres \mathfrak{D}_n , pour $n > 1$ peuvent se construire à partir des entiers relatifs naturels en munissant $(\mathbb{Z} \times \mathbb{N})$ d'une addition, d'une multiplication, et en faisant le quotient de $(\mathbb{Z} \times \mathbb{N})$ par une relation d'équivalence compatible avec les opérations.

L'addition sur $(\mathbb{Z} \times \mathbb{N})$ est définie par $(a, b) + (a', b') = (a \cdot n^{b'} + a' \cdot n^b, b + b')$.

La multiplication sur $(\mathbb{Z} \times \mathbb{N})$ est définie par $(a, b) \cdot (a', b') = (aa', b + b')$.

La relation d'équivalence est définie par $(a, b) \simeq (a', b') \Leftrightarrow a \cdot n^{b'} = a' \cdot n^b$.

L'application $\pi : \mathbb{Z} \mapsto (\mathbb{Z} \times \mathbb{N}) / \simeq$ définie par $\pi(a) = \overline{(a, 0)}$, permet de plonger canoniquement $(\mathbb{Z}, +, \cdot)$ dans $(\mathbb{Z} \times \mathbb{N} / \simeq, +, \cdot)$.

Une façon plus simple de dire les choses est que \mathfrak{D}_n est constitué des fractions dont le dénominateur est une puissance de n .

III.4.7 Utilisation en informatique

Les nombres dyadiques sont très utilisés en informatique, pour les fonctions d'approximation, qui sont particulièrement efficace sur \mathfrak{D} , et la densité de \mathfrak{D} permet d'approcher n'importe quel réel, avec la précision que l'on veut (en particulier à l'aide d'intervalles centrés sur des nombres dyadiques, et de rayon dyadique).

Les nombres dyadiques sont aussi utilisés aussi dans de nombreux algorithmes, comme :

- La recherche des racines complexes de polynômes.
- L'implémentation efficace de la DCT (Discrete Cosine Transform).
- L'algorithme d'interpolation de Deslauriers et Dubuc.
- Simulation de mouvements browniens.
- Implémentation de calculs rapides et efficaces (en Coq, par exemple)

III.4.8 Utilisation en physique

Une partie des unités impériales se découpe à l'aide de nombres dyadiques, le pouce par exemple, mais aussi une unité bien plus agréable : Une pinte = $\frac{1}{64}$ de pied³.

III.4.9 Références

1. J. van der Hoeven, *Computations with effective real numbers*, Université Paris-Sud, 2004
2. Trong Wu, *Foundations of Interval Computation*, Proceedings of the International MultiConference of Engineers and Computer Scientists, Volume I, 2008
3. R. Joshi, Y. A. Reznik, & M. Karczewicz, *Efficient Large Size Transforms for High-Performance Video Coding*, Proceedings of the Conference on Applications of Digital Image Processing XXXIII 2010
4. M. Braverman, *Computational Complexity of Euclidean Sets*, University of Toronto, 2004
5. Chee Yap, *Theory of Real Computation according to EGC*, New York University, 2007
6. Y. Demichel, *Analyse Fractale d'une Famille de Fonctions Aléatoires : Les Fonctions De Bosses*, Thèse Université Blaise Pascal, 2006

III.5 Nombres constructibles \mathcal{C}

III.5.1 Introduction

Un des héritages que nous ont laissé les mathématiques grecques sont les constructions à la règle et au compas, pour lesquelles ils avaient beaucoup d'estime. Certains de leurs problèmes ont d'ailleurs traversé les siècles comme la quadrature du cercle, la trisection de l'angle ou la duplication du cube.

Une question qu'il est naturel de se poser, est de savoir à quelle condition une figure (un cas particulier a été particulièrement étudié : les polygones réguliers), voire simplement un point est-il constructible. De manière plus algébrique, cela revient à caractériser l'ensemble des nombres constructibles, qui correspondent aux abscisses ou aux ordonnées des points constructibles.

III.5.2 Définition

Soit \mathcal{B} un ensemble de points du plan. On dit qu'une droite est construite à partir de \mathcal{B} à la règle et au compas si elle passe par deux points distincts de \mathcal{B} ; on dit qu'un cercle est construit à partir de \mathcal{B} à la règle et au compas s'il a pour centre un point de \mathcal{B} et pour rayon la distance entre deux points de \mathcal{B} .

On dit qu'un point M du plan est constructible à partir de \mathcal{B} à la règle et au compas s'il existe une suite finie de points $M_1, M_2, \dots, M_n = M$ telle que pour tout $1 \leq i \leq n$, M_i soit un point d'intersection de deux cercles, de deux droites ou d'une droite et d'un cercle, ces cercles et droites étant construits à la règle et au compas à partir de $\mathcal{B} \cup \{M_1, \dots, M_{i-1}\}$.

On dit qu'un réel est constructible à la règle et au compas, ou simplement constructible, s'il est l'abscisse d'un point constructible à la règle et au compas à partir de $\mathcal{B} = \{(0, 0), (1, 0)\}$ (c'est-à-dire de deux points qui permettent de définir une origine et une échelle). On note \mathcal{C} l'ensemble des nombres constructibles. Il est immédiat que \mathbb{Z} (trivial), et \mathbb{Q} sont constructibles (cf. la Figure 1, ci-dessous).

A noter que l'on peut définir de manière équivalente un nombre constructible comme l'ordonnée d'un point constructible : en effet, si $r \in \mathbb{R}$ est un nombre constructible, le point $(0, r)$ est constructible, étant l'intersection de la perpendiculaire à l'axe des abscisses passant par l'origine et du cercle de rayon r ayant pour centre l'origine; la réciproque se fait de la même manière.

III.5.3 Constructions élémentaires

On peut facilement montrer, grâce aux propriétés élémentaires de la géométrie, que \mathcal{C} est stable par addition, par produit, par la racine carrée et que chaque élément admet un symétrique pour la multiplication (sauf pour l'élément nul) et pour l'addition (cf. ci-dessous les schémas pour les cas non triviaux⁴⁸).

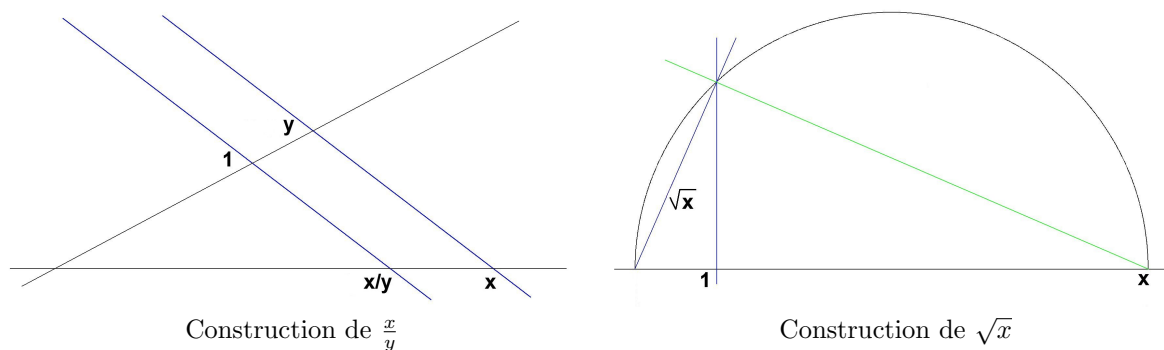


FIGURE 3 – Construction à la règle et au compas.

Ainsi, \mathcal{C} est un sous-corps de \mathbb{R} stable par racine carrée.

On montre de surcroît que \mathcal{C} est le plus petit sous-corps de \mathbb{R} stable par racine carrée.

48. le tracé d'un cercle de diamètre donné, d'une parallèle à une droite passant par un point extérieur à cette droite et d'une droite orthogonale à une droite passant par un point donné, sont des cas très simples.

III.5.4 Propriétés algébriques

Il est possible de montrer que : $t \in \mathbb{R}$ est constructible si, et seulement si, il existe une suite finie croissante (pour l'inclusion) de sous-corps de \mathbb{R} , $(L_i)_{i \in \llbracket 1, p \rrbracket}$, tel que $L_1 = \mathbb{Q}$, $t \in L_p$ et pour tout $i \in \llbracket 1, p \rrbracket$, $[L_{i+1} : L_i] = 2$ (cf. [Extension algébrique](#)).

Le résultat précédent se comprend facilement :

- Le point intersection de deux droites passant pas des points de L_i a des coordonnées dans L_i (équation du premier degré dans un corps).
- Les points d'intersection d'une droite et d'un cercle, ou de deux cercles définis par des points de L_i a des coordonnées dans une extension quadratique de L_i , voire dans L_i (équation du second degré).

On déduit de ce théorème une condition suffisante d'appartenance très utile en pratique : Tout élément de \mathcal{C} est algébrique sur \mathbb{Q} de degré une puissance de 2. Ce résultat est par exemple utilisé pour montrer que les problèmes de la quadrature du cercle, de la duplication du cube et de la trisection de l'angle, cités en introduction, sont insolubles, du fait que π , $\sqrt[3]{2}$ et $\cos(\frac{\pi}{9})$ ne répondent pas à ce critère.

Remarquons que cela implique : $\mathbb{Q} \subsetneq \mathcal{C} \subsetneq \mathcal{A}$, en notant \mathcal{A} l'ensemble des nombres algébriques sur \mathbb{Q} . On en déduit notamment que \mathcal{C} est dénombrable.

Le problème de la construction des polygones réguliers à l'aide de la règle et du compas, est entièrement résolu par le :

Théorème de Gauss : Les polygones réguliers constructibles sont ceux dont le nombre de côtés est de la forme $2^n \prod_{i \in I} F_i$ où $n \in \mathbb{N}$ et les F_i sont des nombres de Fermat *premiers distincts*⁴⁹. L'ensemble I peut être vide.

III.5.5 Synonymes, Isomorphismes, Exemples

Il existe de nombreuses variantes de l'ensemble des nombres constructibles. On peut par exemple rajouter des points initiaux à \mathcal{B} ou modifier les outils à notre disposition.

Ainsi, on peut montrer que \mathcal{C} peut être défini comme l'ensemble des points constructibles au compas seul (théorème de Mohr-Mascheroni) ou bien comme l'ensemble des points constructibles à la règle seule pourvu que \mathcal{B} contienne le cercle unité. On peut alors étendre les problèmes de construction à ces différentes définitions, comme le [problème de Napoléon](#)⁵⁰, dont la construction est plus complexe à partir du compas seul qu'à partir de la règle et du compas.

Il est alors naturel de se demander s'il est possible de résoudre la quadrature du cercle, la duplication du cube et la trisection de l'angle en étendant les nombres constructibles. Des solutions ont en effet été apportées, avec l'ajout d'une courbe à \mathcal{B} , comme les coniques de Menechme, la conchoïde de Nicomède ou la cissoïde de Dioclès.

On peut également étudier les constructions à la règle et à l'équerre ou à la règle et au bissecteur. On montre par exemple que l'ensemble des points constructibles à la règle et au bissecteur est le plus petit sous-corps pythagoricien de \mathbb{R} (un corps étant pythagoricien lorsque toute somme de deux carrés est un carré).

III.5.6 Utilisation en physique

L'étude des nombres constructibles peut être utile dans toute construction géométrique, et donc dans toute résolution ou étude graphique d'un problème physique. Cet intérêt tend cependant à disparaître au profit des logiciels informatiques.

III.5.7 Références

1. Jean-Claude Carrega, *Théorie des corps : la règle et le compas*, Hermann, Paris, 1981, réédité 1989.
2. Antoine Chambert-Loir, *Sur les nombres algébriques constructibles à la règle et au compas.*, Gazette des mathématiciens 118, p. 10-13, octobre 2008.
3. Bernard Le Stum, *Construction de polygones réguliers, Leçon d'agrégation*, Université de Rennes 1, 2001.

49. Un nombre de Fermat est un nombre entier qui peut s'écrire $F_i = 2^{2^i} + 1$ pour un $i \in \mathbb{N}$.

50. Trouver le centre d'un cercle donné.

III.6 Entiers modulo p $\mathbb{Z}/p\mathbb{Z}$

III.6.1 Introduction

L'ensemble des entiers modulus p , souvent noté $\mathbb{Z}/p\mathbb{Z}$ est un sous-ensemble fini des entiers naturels, servant de base à l'arithmétique modulaire. Il peut être construit grâce à la division euclidienne et plus précisément à partir de la congruence sur les entiers.

III.6.2 Définition

Pour $p \in \mathbb{N}^*$, l'ensemble des « entiers modulo p » $\mathbb{Z}/p\mathbb{Z}$ désigne l'ensemble des restes possibles d'une division euclidienne d'un entier par p .

$\mathbb{Z}/p\mathbb{Z}$ est donc l'ensemble des entiers naturels strictement inférieurs à p soit $\mathbb{Z}/p\mathbb{Z} = \{0, 1, \dots, p-1\}$. $\mathbb{Z}/p\mathbb{Z}$ est donc de cardinal p .

III.6.3 Mode de construction

Il est possible de construire $\mathbb{Z}/p\mathbb{Z}$ à partir de la congruence modulo p sur les entiers. On rappelle que deux entiers a et b sont dits congruents modulo p si le reste de la division euclidienne de a par p est égal au reste de la division euclidienne de b par p ; on note alors $a \equiv b [p]$.

On a l'équivalence suivante : $a \equiv b [p] \Leftrightarrow p \mid (a - b) \Leftrightarrow \exists k \in \mathbb{Z} (a - b = kp)$ ($p \mid q$ se lit « p divise q »)

La relation $\equiv [p]$ est donc la relation d'équivalence définie par l'idéal $p\mathbb{Z}$ de \mathbb{Z} . On peut alors définir l'anneau quotient $\mathbb{Z}/p\mathbb{Z}$, ensemble des classes d'équivalence de \mathbb{Z} par la relation de congruence.

Bien que la notation $\mathbb{Z}/p\mathbb{Z}$ désigne un ensemble de classes d'équivalence (et donc de sous-ensembles de \mathbb{Z}), il est courant de confondre un élément de $\mathbb{Z}/p\mathbb{Z}$ avec son unique représentant inférieur à p . La méthode décrite plus haut permet bien alors de construire l'ensemble $\{0, 1, \dots, p-1\}$.

Exemple de la construction de $\mathbb{Z}/2\mathbb{Z}$: Les deux seules classes d'équivalence de la congruence modulo 2 sont les ensembles des nombres pairs P et des nombres impairs I , on a donc $\mathbb{Z}/2\mathbb{Z} = \{P, I\}$. L'unique entier pair strictement inférieur à 2 étant 0 et l'unique entier impair inférieur à 2 étant 1, la construction présentée ci-dessus conduit bien à l'ensemble $\{0, 1\}$.

III.6.4 Tables d'addition et de multiplication

Pour tout $a \in \mathbb{Z}$, notons $a[p]$ le reste de la division euclidienne de a par p .

On peut définir une loi d'addition $\bar{+}$ et une loi de multiplication $\bar{\times}$ sur l'ensemble $\mathbb{Z}/p\mathbb{Z}$ à partir de celles sur l'anneau $(\mathbb{Z}, +, \times)$, en considérant les éléments de $\mathbb{Z}/p\mathbb{Z}$ comme des éléments de \mathbb{Z} :

$$\forall (a, b) \in (\mathbb{Z}/p\mathbb{Z})^2, a \bar{+} b = (a + b)[p] \text{ et } a \bar{\times} b = (a \times b)[p]$$

Par la suite, pour alléger les notations, on notera les lois d'addition et de multiplication de $\mathbb{Z}/p\mathbb{Z}$, $+$ et \times , bien que celles-ci soit différentes de celles définies sur \mathbb{Z} .

On peut remarquer que $\mathbb{Z}/p\mathbb{Z}$ est stable par les lois $+$ et \times et que les éléments neutres 0 et 1 de ces lois appartiennent à $\mathbb{Z}/p\mathbb{Z}$. De plus, les propriétés de l'addition et de la multiplication dans \mathbb{Z} assurent celles dans $\mathbb{Z}/p\mathbb{Z}$. Notamment :

- La loi $+$ est commutative et associative
- La loi \times est commutative, associative et distributive par rapport à la loi $+$

Nous reviendrons sur ces propriétés dans les paragraphes suivants.

Un premier exemple avec p un nombre premier :

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Tables de $\mathbb{Z}/5\mathbb{Z}$

Un deuxième exemple avec p un nombre non premier :

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

×	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Tables de $\mathbb{Z}/6\mathbb{Z}$

On observe que chaque élément non nul de $\mathbb{Z}/5\mathbb{Z}$ possède un élément inverse pour la multiplication, alors que ce n'est pas le cas pour $\mathbb{Z}/6\mathbb{Z}$. Nous reviendrons sur cette propriété dans les paragraphes suivants.

III.6.5 Conjugué, Module, Norme, Forme Polaire et Inverse

En tant que sous-ensemble de \mathbb{Z} , $\mathbb{Z}/p\mathbb{Z}$ peut-être muni de la valeur absolue dans \mathbb{Z} comme norme et de la relation d'infériorité définie sur \mathbb{Z} comme relation d'ordre.

Tout élément a de $\mathbb{Z}/p\mathbb{Z}$ possède un inverse pour la loi d'addition, qui est 0 si $a = 0$ et $p - a$ sinon (en effet $1 \leq a \leq p - 1$ d'où $p - 1 \geq p - a \geq 1$ donc $p - a \in \mathbb{Z}/p\mathbb{Z}$ et $a + (p - a) \equiv p [p] \equiv 0 [p]$).

Comme vu dans le paragraphe précédent, certains éléments de $\mathbb{Z}/p\mathbb{Z}$ ne possèdent pas d'inverse pour la multiplication.

On montre en fait que l'ensemble des inversibles de $\mathbb{Z}/p\mathbb{Z}$ est l'ensemble des éléments a de $\mathbb{Z}/p\mathbb{Z}$ premiers avec p , l'existence de l'inverse étant alors fourni par la relation de Bezout ($\exists(u, v) \in \mathbb{Z}^2 (au + pv = 1)$ (dans \mathbb{Z}) d'où (dans $\mathbb{Z}/p\mathbb{Z}$) $au \equiv (1 - pv) [p] \equiv 1 [p]$).

L'ensemble des inversibles de $\mathbb{Z}/p\mathbb{Z}$ muni de la loi \times est donc un groupe commutatif de cardinal $\varphi(p)$ où φ est la fonction indicatrice d'Euler (cf. [la définition de \$\varphi\$](#)).

L'algorithme d'Euclide étendu permet de trouver v et donc de déterminer l'inverse de a .

Un cas particulier très important du dernier résultat est celui où p est premier. Tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ possède alors un élément inverse pour la multiplication. Nous reviendrons sur cette propriété dans le paragraphe suivant.

III.6.6 Propriétés algébriques

$(\mathbb{Z}/p\mathbb{Z}, +, \times)$ est un anneau commutatif (les conditions nécessaires étant établies dans les paragraphes précédents) de caractéristique non nulle p (en effet $p \times 1 \equiv p [p] \equiv 0 [p]$).

Si p est premier, l'existence pour chaque élément de $\mathbb{Z}/p\mathbb{Z}$ d'un inverse pour la loi \times fait de $(\mathbb{Z}/p\mathbb{Z}, +, \times)$ un corps commutatif fini. On l'appelle alors corps premier et on le note \mathbb{F}_p (le sous-corps premier d'un corps est son plus petit sous-corps pour l'inclusion, il est inclus dans tous ses sous-corps, le sous-corps premier est \mathbb{Q} pour un corps de caractéristique 0 et \mathbb{F}_p pour un corps de caractéristique p).

III.6.7 Résultats d'arithmétique modulaire

L'arithmétique modulaire est une branche des mathématiques appartenant à la théorie algébrique des nombres, traitant des nombres entiers et des congruences modulo p . Plusieurs théorèmes d'arithmétique modulaire peuvent se démontrer grâce aux structures algébriques de l'ensemble $\mathbb{Z}/p\mathbb{Z}$ ou de son sous-groupe des inversibles.

Théorème de Wilson

Un entier naturel p est premier si et seulement si $(p-1)! + 1 \equiv 0 [p]$, où $(p-1)!$ est la factorielle de $p-1$.

Petit théorème de Fermat

Si p est premier et a est un entier non divisible par p , alors $a^{p-1} \equiv 1 [p]$.

Définition : fonction indicatrice d'Euler

On appelle fonction indicatrice d'Euler et on note φ la fonction de \mathbb{N}^* dans \mathbb{N}^* qui à tout entier strictement positif n associe le nombre, noté $\varphi(n)$, d'entiers naturels inférieurs à n et premier avec n .

Le petit théorème de Fermat peut être généralisé à l'aide de la fonction φ par le théorème d'Euler.

Théorème d'Euler

Soit n un entier strictement positif. Si a est un entier naturel premier avec n alors $a^{\varphi(n)} \equiv 1 [n]$

Théorème des restes chinois

Soient k un entier naturel non nul, n_1, \dots, n_k des entiers deux à deux premiers entre eux et a_1, \dots, a_k des entiers. Posons $n = \prod_{i=1}^k n_i$.

Le système de congruence $\forall i \in \{1, \dots, k\}, x \equiv a_i [n_i]$ admet une unique solution modulo n .

On remarque que n_i et $\frac{n}{n_i}$ sont premiers entre eux, donc, d'après le théorème de Bezout, il existe α_i et β_i tels

que $\alpha_i \frac{n}{n_i} + \beta_i n_i = 1$, alors une solution de ce système est donnée par $x = \sum_{i=1}^k a_i \alpha_i \frac{n}{n_i}$.

En effet on peut vérifier facilement que $\alpha_i \frac{n}{n_i} \equiv 1 [n_i]$ et $\bigwedge_{i \neq j} (\alpha_i \frac{n}{n_i} \equiv 0 [n_j])$

La raison purement algébrique qui permet d'expliquer le théorème des restes chinois est que l'application $\varphi : \mathbb{Z}/n\mathbb{Z} \mapsto \prod_{i=1}^k \mathbb{Z}/n_i\mathbb{Z}$ défini par :

$$\varphi(\alpha[n]) = (\alpha[n_1], \alpha[n_2], \dots, \alpha[n_k])$$

est un isomorphisme d'anneaux.

III.6.8 Synonymes, Isomorphismes, Exemples

L'ensemble $\mathbb{Z}/p\mathbb{Z}$ est parfois appelé anneau résiduel ou anneau quotient modulo p .

Un exemple d'anneau résiduel tiré de la vie quotidienne est celui du décompte du temps à travers le système heures/secondes/minutes.

L'heure par exemple est un nombre qui décrit l'ensemble $\mathbb{Z}/12\mathbb{Z}$ (ou $\mathbb{Z}/24\mathbb{Z}$), variant de 0 à 11. On retrouve de plus la loi d'addition sur $\mathbb{Z}/12\mathbb{Z}$ définie plus haut : s'il est 7h et que l'on attend 2 heures, il sera 9h, mais s'il est 7h et que l'on attend 6 heures il sera 1h (ce qui correspond à $7 + 6 [12]$).

L'exemple de l'heure ne possède cependant pas de loi de multiplication interne.

III.6.9 Utilisation dans les sciences

L'ensemble $\mathbb{Z}/p\mathbb{Z}$ est utilisé en cryptographie : on peut définir des algorithmes de chiffage dont le décodage nécessite une clé secrète, basée sur deux éléments de $\mathbb{Z}/p\mathbb{Z}$.

Bien que l'on utilise assez couramment l'arithmétique modulaire sans parfois s'en rendre compte (voire exemple de l'heure), il n'y a pas à ma connaissance de travaux de physique qui utilise explicitement l'ensemble $\mathbb{Z}/p\mathbb{Z}$ et qui nécessite le formalisme mathématique décrit plus haut.

Il y a cependant une science qui utilise énormément le corps $\mathbb{Z}/2\mathbb{Z}$, sans pour autant le nommer ainsi : l'informatique.

En effet, la base de l'algorithme, la logique binaire (aussi appelée logique de Boole) repose sur les concepts de FAUX et de VRAI, que l'on modélise usuellement par 0 et 1. On peut alors définir entre deux propriétés plusieurs lois internes, dont certaines correspondent aux loi + et \times .

La loi ET renvoie VRAI si et seulement si les deux propriétés sont toutes les deux vraies (et donc FAUX si au moins une des deux est fausse). Elle correspond à loi \times .

La loi XOU (OU exclusif) renvoie VRAI si et seulement si une et une seule des deux propriétés est vraie. Elle correspond à la loi +.

On a alors les tables de vérités suivantes, correspondant à celles de \times et + sur $\mathbb{Z}/2\mathbb{Z}$:

ET	FAUX	VRAI
FAUX	FAUX	FAUX
VRAI	FAUX	VRAI

XOU	FAUX	VRAI
FAUX	FAUX	VRAI
VRAI	VRAI	FAUX

Ou, d'une façon plus symbolique ($\wedge = \text{ET}$, $\wp = \text{XOU}$ ⁵¹, $\top = \text{VRAI}$ et $\perp = \text{FAUX}$) :

\wedge	\perp	\top
\perp	\perp	\perp
\top	\perp	\top

\wp	\perp	\top
\perp	\perp	\top
\top	\top	\perp

Ou encore d'une façon plus arithmétique :

\otimes	0	1
0	0	0
1	0	1

\oplus	0	1
0	0	1
1	1	0

III.6.10 Références

1. Thomas Plantard, *Arithmétique modulaire pour la cryptographie*, Université Montpellier II, 2005.
2. Robert Rolland, *Introduction à l'étude des Corps Finis*.
3. Miguel A. Lerma, *Modular Arithmetic*, Northwestern University (Illinois), 2005.
4. E. Bresson, *Cryptographie, Rappels mathématiques*, ENS.
5. Bas Edixhoven, *Cours de maîtrise de mathématiques : Théorie algébrique des nombres*, Université de Rennes 1, 2002.

51. Pour le XOU on trouve aussi les symboles : $\underline{\vee}$ et $\dot{\vee}$

III.7 Nombres p -adiques \mathbb{Z}_p , \mathbb{Q}_p et \mathbb{C}_p

III.7.1 Introduction

On passe de l'ensemble des entiers \mathbb{Z} (ou des **décimaux** \mathbb{D}) à l'ensemble des réels \mathbb{R} en autorisant les nombres à avoir une infinité de chiffres (nuls ou non nuls) à droite de la virgule. Par exemple $\pi = 3,14159265358979\dots$

Il existe une autre façon de compléter \mathbb{D} en un ensemble intéressant. Il s'agit d'autoriser les nombres à avoir une infinité de chiffres (nuls ou non nuls) à gauche de la virgule. Par exemple, $a = \dots 11266421216213$ ou $b = \dots 455323152,156$. Nous verrons plusieurs aspects (informels et formels) de ces nouveaux nombres

Le développement de cette idée de départ vient de Kurt Hensel⁵², un mathématicien allemand (1861-1941) dans un article publié en 1897 (voir les références).

III.7.2 Définition informelle

Les nombres avec une infinité de chiffres à gauche et un nombre fini de chiffres à droite de la virgule en base p sont appelés nombres p -adiques, et leur ensemble est noté \mathbb{Q}_p .

Les nombres p -adiques qui n'ont aucun chiffre non nul à droite de la virgule sont appelés entiers p -adiques. Leur ensemble est noté \mathbb{Z}_p et il est inclus dans \mathbb{Q}_p . On peut aussi noter que $\mathbb{Z} \subset \mathbb{Z}_p$ et, si p est premier, $\mathbb{Q} \subset \mathbb{Q}_p$.

Par exemple le nombre a de l'introduction est un entier p -adique alors que b est un nombre p -adique qui n'est pas entier.

Il s'avère qu'il y a une différence fondamentale entre ces nombres p -adiques et les nombres réels : Les nombres p -adiques dépendent de la base de numération choisie.

Par exemple, en base 10 il existe des diviseurs de 0 ; pour éviter ce problème, dans la suite de ce document p sera un nombre premier (à une exception qui sera signalée.)

Il existe donc autant d'ensembles \mathbb{Q}_p et \mathbb{Z}_p qu'il existe de nombres premiers p , et ces \mathbb{Q}_p et \mathbb{Z}_p sont tous différents les uns des autres.

Par exemple, dans \mathbb{Z}_7 , il existe une racine carrée de 2 qui est $\dots 11266421216213$. En revanche, 2 n'a pas de racine carrée dans \mathbb{Z}_2 .

III.7.3 Addition et multiplication

On calcule avec les nombres p -adiques comme avec les nombres décimaux, la présence d'une infinité de chiffres vers la gauche ne pose pas de problème particulier.

Exemple d'addition dans \mathbb{Q}_7 :

$$\begin{array}{r}
 \dots 4 2 1 2 1 6 2 1 3 \\
 + \dots 4 5 5 3 2 3 1 5 2 \quad , \quad 1 5 6 \\
 \hline
 \dots 2 0 6 5 4 2 3 6 5 \quad , \quad 1 5 6
 \end{array}$$

(Attention à la retenue en base 7!)

Un autre exemple intéressant, toujours en base 7 :

$$\begin{array}{r}
 \dots 6 6 6 6 6 6 6 6 6 \\
 + \dots 1 \\
 \hline
 \dots 0 0 0 0 0 0 0 0 0
 \end{array}$$

Autrement dit $\dots 66666666 = -1$ (comme nombres 7-adiques).

Ceci se généralise et permet d'exprimer les nombres négatifs.

52. Elle trouve son origine chez E. Kummer, un autre mathématicien allemand

Exemple de multiplication dans \mathbb{Z}_7 :

$$\begin{array}{r}
 \dots 4 \ 2 \ 1 \ 2 \ 1 \ 6 \ 2 \ 1 \ 3 \\
 \times \dots 4 \ 2 \ 1 \ 2 \ 1 \ 6 \ 2 \ 1 \ 3 \\
 \hline
 \dots 5 \ 6 \ 3 \ 6 \ 5 \ 4 \ 6 \ 4 \ 2 \\
 \dots 2 \ 1 \ 2 \ 1 \ 6 \ 2 \ 1 \ 3 \\
 \dots 2 \ 4 \ 3 \ 5 \ 4 \ 2 \ 6 \\
 \dots 6 \ 4 \ 2 \ 6 \ 1 \ 4 \\
 \dots 1 \ 6 \ 2 \ 1 \ 3 \\
 \dots 5 \ 4 \ 2 \ 6 \\
 \dots 2 \ 1 \ 3 \\
 \dots 2 \ 6 \\
 \dots 5 \\
 \hline
 \dots 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 0 \ 2
 \end{array}$$

Exemple de multiplication dans \mathbb{Z}_{10} (10 qui n'est pas premier) :

$$\begin{array}{r}
 \dots 0 \ 1 \ 0 \ 1 \ 1 \ 2 \\
 \times \dots 1 \ 4 \ 0 \ 6 \ 2 \ 5 \\
 \hline
 \dots 0 \ 5 \ 0 \ 5 \ 6 \ 0 \\
 \dots 2 \ 0 \ 2 \ 2 \ 4 \\
 \dots 0 \ 6 \ 7 \ 2 \\
 \dots 0 \ 0 \ 0 \\
 \dots 4 \ 8 \\
 \dots 2 \\
 \hline
 \dots 0 \ 0 \ 0 \ 0 \ 0 \ 0
 \end{array}$$

III.7.4 Valuation et valeur absolue

La valuation $v_p(x)$ d'un nombre p -adique x non nul est le rang de son chiffre non nul le plus à droite. Exemples :

$$\begin{array}{rcl}
 v_7(\dots 456321000) & = & 3 \\
 v_7(\dots 1564231,0123) & = & -4 \\
 v_7(\dots 13262123) & = & 0 \\
 \text{On convient que : } v_p(0) & = & +\infty
 \end{array}$$

La valeur absolue $|x|_p$ d'un nombre p -adique x non nul est égale à $p^{-v_p(x)}$. Exemples :

$$\begin{array}{rcl}
 |\dots 456321000|_7 & = & 7^{-3} = \frac{1}{343} \\
 |\dots 1564231,0123|_7 & = & 7^4 = 2401 \\
 |\dots 13262123|_7 & = & 7^0 = 1 \\
 \text{On convient que : } |0|_p & = & p^{-\infty} = 0
 \end{array}$$

Cette valeur absolue vérifie toutes les propriétés attendues :

$$\begin{array}{l}
 |x|_p \geq 0 \\
 |x|_p = 0 \Leftrightarrow x = 0 \\
 |xy|_p = |x|_p |y|_p \\
 |x + y|_p \leq |x|_p + |y|_p
 \end{array}$$

Elle a en outre la propriété d'être *ultramétrique*, c'est à dire :

$$|x + y|_p \leq \max(|x|_p, |y|_p)$$

III.7.5 Définition formelle

Soit p un nombre premier. L'ensemble \mathbb{Q}_p des nombres p -adiques est l'ensemble des nombres de la forme

$$x = \sum_{n \geq k} a_n p^n,$$

où $k \in \mathbb{Z}$ et les a_n sont des nombres entre 0 et $p - 1$, en particulier $a_k \neq 0$.

L'ensemble \mathbb{Z}_p des entiers ⁵³ p -adiques est l'ensemble des nombres de la forme

$$x = \sum_{n \geq k} a_n p^n.$$

où $k \in \mathbb{N}$ et les a_n sont des nombres entre 0 et $p - 1$, en particulier $a_k \neq 0$.

On peut retrouver facilement les inclusions : $\mathbb{Z} \subset \mathbb{Z}_p \subset \mathbb{Q}_p$ et (p est premier) $\mathbb{Q} \subset \mathbb{Q}_p$.

Les définitions précédentes permettent de définir une fonction appelée valuation p -adique : $v_p(x) = k$, et d'une valeur absolue p -adique $|x|_p = p^{-v_p(x)}$, et donc d'une distance p -adique : $d_p(x, y) = |x - y|_p$. Il va de soi que cette définition correspond exactement à la définition donnée dans la partie informelle, la distance définie ici est donc une distance ultramétrique (tous les points d'une boule en sont un centre, tous les triangles sont isocèles).

Pour cette distance, deux nombres sont d'autant plus proches que leur différence est divisible pas une puissance plus grande de p . Par exemple $d_3(1, 2) = |1|_3 = 1$, alors que $d_3(1, 244) = |243|_3 = |3^5|_3 = 3^{-5}$.

Cette valeur absolue munit l'ensemble des nombres p -adiques d'une topologie. Il faut prendre garde qu'elle est différente de celle de \mathbb{R} . Le sens du « grand » et du « petit » peut être inversé :

Dans \mathbb{R} , la suite $u_n = p^{-n}$, c'est à dire des nombres qui s'écrivent 0, 1 ; 0, 01 ; 0, 001 ; 0, 0001 ; ... en base p tend vers 0 (u_n devient de plus en plus petit).

Dans \mathbb{Q}_p , la suite $u_n = p^{-n}$ n'est pas convergente (u_n devient de plus en plus grand).

Dans \mathbb{R} , la suite $u_n = p^n$, c'est à dire des nombres qui s'écrivent 1 ; 10 ; 100 ; 1000 ; ... en base p n'est pas convergente (u_n devient de plus en plus grand).

Dans \mathbb{Q}_p , la suite $u_n = p^n$, tend vers 0 (u_n devient de plus en plus petit).

III.7.6 Propriétés algébriques et analytiques

L'ensemble \mathbb{Z}_p est un anneau intègre. Les entiers p -adiques qui n'ont pas d'inverse dans \mathbb{Z}_p sont les éléments de l'idéal $p\mathbb{Z}_p$ (du point de vue informel, c'est exactement ceux dont le premier chiffre à gauche de la virgule est 0). Cet ensemble des non inversibles est un idéal de \mathbb{Z}_p et c'est même son seul idéal maximal : on dit que \mathbb{Z}_p est un anneau local.

L'ensemble \mathbb{Q}_p est un corps. Muni de sa topologie, il est complet. Il a donc beaucoup de points communs avec \mathbb{R} (en fait, en un certain sens que l'on ne détaillera pas, on peut considérer \mathbb{R} comme l'ensemble des nombres ∞ -adiques).

On peut définir sur \mathbb{Q}_p une fonction exponentielle, à l'aide d'une série entière :

$$\exp_p(x) = \sum \frac{x^n}{n!}.$$

On peut définir de même les fonctions transcendantes usuelles : logarithme p -adique, fonctions trigonométriques p -adiques...

On dispose sur \mathbb{Q}_p des notions de limite, de dérivée, de primitive, d'équations différentielles... Bref c'est un corps où on peut faire de l'analyse.

Le corps \mathbb{Q}_p n'est pas algébriquement clos : les exemples ci-dessous utilisent un petit résultat sur les polynômes ⁵⁴ et le Lemme de Hensel (cf. infra),

Dans \mathbb{Q}_2 , le polynôme $X^2 + X + 1 = 0$ n'a pas de racine.

Dans \mathbb{Q}_p , il existe $k \in [1, p[$ tel que le polynôme $X^2 - k = 0$ ⁵⁵ n'ait pas de racine.

53. Un simple argument diagonal permet de montrer que \mathbb{Z}_p n'est pas dénombrable

54. On peut vérifier facilement que les polynômes utilisés ont une racine dans \mathbb{Q}_p si et seulement si ses solutions sont dans \mathbb{Z}_p

55. Si $n > 2$ et $0 < i < p$, alors $i^2 \equiv (p - i)^2 [p]$, il est donc possible de trouver un k qui ne soit pas carré modulo p

III.7.7 Quelques théorèmes intéressants

Lemme de Hensel : soit $\varphi \in \mathbb{Z}_p[X]$ et soit $a \in \mathbb{Z}_p$ tel que $\varphi(a) \equiv 0 \pmod{p}$ et $\varphi'(a) \not\equiv 0 \pmod{p}$, alors il existe un unique entier p -adique α tel que $(\varphi(\alpha) = 0) \wedge (a \equiv \alpha \pmod{p})$.

Remarque : la démonstration du lemme de Hensel (pas très compliquée) est constructive, elle repose sur la construction d'une suite de Cauchy donc convergente dans \mathbb{Z}_p , dont la limite est la valeur cherchée.

Théorème d'Ostrowski : Toute valeur absolue $|\cdot|$ sur \mathbb{Q} est équivalente à l'un des cas suivants :

- La valeur absolue triviale $|\cdot|_0$ définie par $|0|_0 = 0 \wedge \forall x(x \neq 0 \Rightarrow |x|_0 = 1)$.
- La valeur absolue euclidienne $|\cdot|_\infty$ (c'est à dire la valeur absolue usuelle sur \mathbb{Q}).
- La valeur absolue p -adique $|\cdot|_p$ pour un certain p premier.

Théorème de Hasse-Minkowski : Une forme quadratique possède une racine non nulle dans \mathbb{Q} si et seulement si elle admet une racine non nulle dans \mathbb{R} et dans chacun des \mathbb{Q}_p pour tous p nombres premiers (Principe Local-Global).

A noter qu'il existe des contre-exemples pour les degrés supérieurs, en particulier, le contre-exemple de Selmer $3x^3 + 4y^3 + 5z^3 = 0$ qui possède des racines dans \mathbb{R} (trivial) et dans chacun des \mathbb{Q}_p , mais pas dans \mathbb{Q} .

Formule du produit En notant \mathbb{P} l'ensemble des nombres premiers : $\forall n \in \mathbb{N} \left(\prod_{p \in \mathbb{P}} |n|_p \right) \cdot |n|_\infty = 1$.

III.7.8 Les nombres complexes p -adiques

Comme \mathbb{Q}_p n'est pas algébriquement clos, on peut s'intéresser à sa clôture algébrique $\overline{\mathbb{Q}_p}$. Malheureusement ce corps n'est plus complet.

En revanche, le complété de la clôture algébrique de \mathbb{Q}_p est à la fois complet et algébriquement clos. C'est le corps des nombres complexes p -adiques, noté \mathbb{C}_p du fait de sa ressemblance avec \mathbb{C} .

Quelques propriétés :

- \mathbb{C} et \mathbb{C}_p sont isomorphes en tant que corps (la théorie des corps algébriquement clos est \aleph_1 -catégorique).
- Par contre, il n'y a pas d'isomorphisme unique entre les deux, ni même d'isomorphisme canonique, et encore moins d'isomorphisme explicite.
- \mathbb{C} et \mathbb{C}_p ont des topologies complètement différentes.

III.7.9 Synonymes, Isomorphismes, Exemples

Les nombres p -adiques ont été introduits dans certains collèges français par l'association MATH en JEANS, sous le terme de *bretnoms*. Une illustration du fait qu'on peut faire d'excellentes mathématiques dès le collège...

On peut donner deux constructions alternatives à la définition formelle, ci-dessus :

L'ensemble des entiers p -adiques \mathbb{Z}_p est la limite projective des $\mathbb{Z}/p^n\mathbb{Z}$:

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

Le lecteur qui n'est pas familier avec cette notion peut la comprendre de la façon suivante : pour tout n , la troncation aux n chiffres les plus à droite est un morphisme de \mathbb{Z}_p dans $\mathbb{Z}/p^n\mathbb{Z}$. L'ensemble \mathbb{Z}_p est donc en quelque sorte l'ensemble $\mathbb{Z}/p^n\mathbb{Z}$ où « on a fait tendre n vers l'infini ».

Une fois \mathbb{Z}_p construit, \mathbb{Q}_p s'obtient de la même façon qu'on obtient \mathbb{Q} à partir de \mathbb{Z} (son corps des fractions).

Seconde construction :

Tout nombre entier relatif α , peut s'écrire comme un produit de nombres premiers : $\alpha = \pm \prod_{k=1}^n p_k^{\alpha_k}$ où p_k est le $k^{\text{ième}}$ nombre premier ; pour tout nombre premier p , on peut donc écrire $\alpha = p^n \cdot q$ où q est un entier relatif premier avec p .

La valuation p -adique est alors définie par $v_p(\alpha) = n$ et la valeur absolue p -adique par $|\alpha|_p = p^{-v_p(\alpha)} = p^{-n}$ (ce qui permet de construire une distance p -adique, c'est à dire une (nouvelle) topologie, sur \mathbb{Z}).

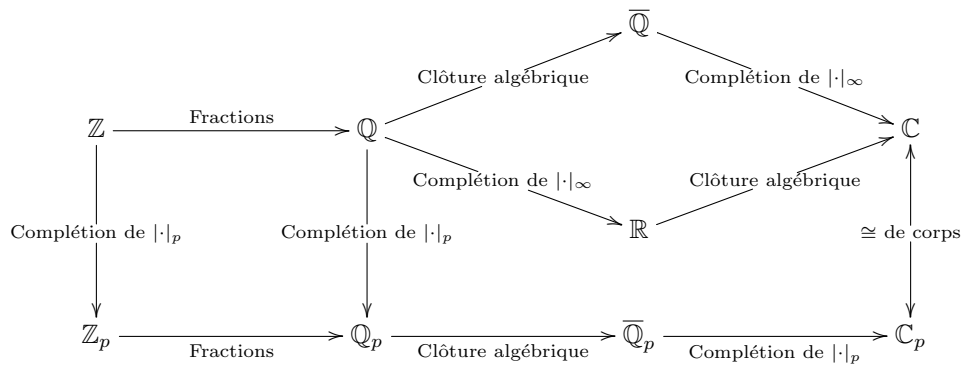
Avec cette valeur absolue, \mathbb{Z} n'est pas complet, par exemple la suite $u_n = 1 + p^2 + \dots + p^{2n}$ est bien de Cauchy, mais elle n'est pas convergente (elle converge vers $\frac{1}{1-p^2} \notin \mathbb{Z}$). On pose $\mathbb{Z}_p =$ le complété de \mathbb{Z} pour la distance p -adique. On peut alors envisager le corps des fractions de \mathbb{Z}_p , noté \mathbb{Q}_p . La valuation p -adique se prolonge naturellement à ce corps de fractions :

Soit $\alpha \in \mathbb{Z}_p, \beta \in \mathbb{Z}_p$ alors on pose $v_p\left(\frac{\alpha}{\beta}\right) = v_p(\alpha) - v_p(\beta)$ ce qui permet de définir la valeur absolue et la distance p -adique sur \mathbb{Q}_p qui est complet pour la topologie associée.

Remarque : on aurait pu partir de \mathbb{Q} en munissant cet ensemble d'une distance p -adique (définie comme ci-dessus, mais avec α et β dans \mathbb{Z}), puis en complétant cet ensemble pour cette distance, le résultat eut été le même : \mathbb{Q}_p , qui est donc au choix :

1. Le complété de \mathbb{Q} pour la valeur absolue p -adique (de même que \mathbb{R} est le complété de \mathbb{Q} pour la valeur absolue usuelle).
2. Le corps des fractions du complété de \mathbb{Z} pour la valeur absolue p -adique (de même que \mathbb{Q} est le corps des fractions de \mathbb{Z}).

Pour résumer :



III.7.10 Utilisation en physique

Si les nombres p -adiques semblent aussi naturels que les nombres réels dans le paysage mathématique, il n'en est pas de même en physique, où ils sont pratiquement absents. Quelques tentatives ont été faites pour construire une physique p -adique, mais relèvent pour l'instant, au moins en partie, d'un jeu de l'esprit.

Les nombres p -adiques sont utilisés en cryptographie, et pour la mise au point de « Code Correcteurs d'Erreurs ».

Topological Geometroynamics (TGD) : une théorie physique en essor depuis les années 80.

On pourra aussi consulter *p-Adic Mathematical Physics*, ci-dessous.

III.7.11 Références

1. K. Hensel, *Über eine neue Begründung der Theorie der algebraischen Zahlen*, Jahresbericht der Deutschen Mathematiker, Volume 6, p. 83-88, 1897.
2. Irem de Limoges, *Nombres p-adiques*, Stage « Arithmétique », Limoges, 2009.
3. V. Lefèvre, *Thème de recherche N° 2 : les BRENOMS*, 1994.
4. Site : [Maths en jeans](#), il y a plusieurs sujets sur les brenoms (niveau 6^{ième} à 2^{nde}).
5. L. Merel, *Nombres algébriques et nombres p-adiques*, Université Pierre et Marie Curie, Université Denis Diderot, cours préparatoire aux études doctorales, 2003-2004.
6. B. Dragovich, A. Yu. Khrennikov, S. V. Kozyrev, I. V. Volovich, *p-Adic Mathematical Physics*, Institute of Physics Belgrade Serbie, Växjö University Suède, Steklov Mathematical Institute Moscou Russie, 2009.
7. M. Pitkanen, *Topological Geometroynamics (TGD) : an Overall View*, Finland, 2009.

III.8 Compactification des Entiers Naturels $\omega + 1, \overline{\mathbb{N}}, \mathbb{N}^*, \beta\mathbb{N}$

III.8.1 Introduction

De la même façon que dans les **Proto-nombres** on prend en compte la notion de « Beaucoup », on peut se demander s'il est possible d'ajouter cette notion dans l'ensemble des **Entiers Naturels**, voire lui ajouter d'autres types d'éléments (principalement pour des raisons topologiques).

Nous allons passer en revue plusieurs façons d'ajouter des éléments à \mathbb{N} , différentes des raisons algébriques déjà vues, et qui ont donné naissance à $\mathbb{Z}, \mathbb{Q}, \mathbb{Q}$ (etc.). En particulier nous verrons plusieurs méthodes topologiques, mais pas toutes, car il en existe de nombreuses, mais nous pouvons donner une courte liste de méthodes de compactification assez courantes.

Définition⁵⁶ : soit \mathcal{X} , un ensemble muni d'une topologie \mathcal{T} , une compactification de $(\mathcal{X}, \mathcal{T})$ est un triplet $(\widehat{\mathcal{X}}, \widehat{\mathcal{T}}, \varphi)$, où :

- $(\widehat{\mathcal{X}}, \widehat{\mathcal{T}})$ est un espace topologique compact.
- $\varphi : \mathcal{X} \mapsto \widehat{\mathcal{X}}$.
- $(\mathcal{X}, \mathcal{T})$ et $(\varphi(\mathcal{X}), \widehat{\mathcal{T}})$ sont homéomorphes.
- $\varphi(\mathcal{X})$ est dense dans $\widehat{\mathcal{X}}$ (pour la topologie $\widehat{\mathcal{T}}$).

Quelques exemples de compactifications que nous ne détaillerons pas (cf. les références).

1. La **Compactification de Wallman** doit son nom à Henry Wallman (1915 - 1992), un mathématicien Américain. Soit \mathcal{X} un espace topologique dont tous les singletons sont des fermés, le compactifié de Wallman de \mathcal{X} , qui est noté $\omega\mathcal{X}$, est l'ensemble des ultrafiltres fermés sur \mathcal{X} muni de la topologie engendrée par la base de fermés constitués des ensembles de la forme : pour chaque \mathcal{A} fermé de $\mathcal{X} : \mathcal{A}^* = \{\mathcal{U} \mid \mathcal{U} \in \omega\mathcal{X} \wedge \mathcal{A} \in \mathcal{U}\}$
2. La **Compactification de Bohr** doit son nom à Harald Bohr (1887 - 1951), un mathématicien danois, frère de Niels. Cette méthode, initialement développée pour des groupes topologiques a été généralisée depuis à tous types de structure munie d'une topologie (y compris la topologie discrète) : La compactification de Bohr de la structure \mathfrak{A} , munie de la topologie \mathcal{T} , est maximale dans la famille des compactifications compatibles avec la structure \mathfrak{A} .
3. La **Compactification de Royden** doit son nom à Halsey Lawrence Royden (1928 - 1993), un mathématicien américain. Cette méthode a été initialement développée pour l'étude des frontières des espaces de Riemann, elle a été étendue par la suite à différents graphes. Dans le cas de \mathbb{N} , son compactifié de Royden, noté $\mathfrak{R}\mathbb{N}$, est le quotient du compactifié de Stone-Ćech $\beta\mathbb{N}$, par une relation d'équivalence entre ultrafiltres définissant la même limite généralisée pour les suites réelles bornées.
4. La **\mathcal{G} -Compactification**. Soit \mathcal{G} un groupe topologique localement compact agissant continuellement sur un espace topologique $(\mathcal{X}, \mathcal{T})$, une compactification $\gamma\mathcal{X}$ ⁵⁷ de $(\mathcal{X}, \mathcal{T})$ est une \mathcal{G} -Compactification, si l'action de \mathcal{G} sur \mathcal{X} se prolonge continuellement à $\gamma\mathcal{X}$.

III.8.2 Ordinaux

La première idée qui peut venir c'est de regarder un ensemble qui existe déjà, par exemple l'**ordinal** $\omega + 1$, qui contient un élément de plus que ω , strictement plus grand que tous les éléments de ω .

Rappelons que $\omega + 1 = \omega \cup \{\omega\}$, du point de vue de l'ordre, cet ensemble correspond bien à l'idée de « Beaucoup », ou de « Infini », puisque le nouvel élément est strictement plus grand que tous les entiers.

Malheureusement, s'il existe des opérations naturelles sur ω , qui correspondent parfaitement aux opérations sur \mathbb{N} , les opérations naturelles sur $\omega + 1$ ne correspondent pas (toutes) à ce que nous voulions modéliser :

Dans $\omega + 1$, l'opération $1 + \omega$ donne le résultat ω , ce qui correspond bien à l'idée intuitive de « Beaucoup », mais l'opération $\omega + 1$ n'est même pas définie, contrairement à ce que nous souhaitions.

⁵⁶. Certains auteurs donnent des définitions légèrement différentes.

⁵⁷. Avec quelques abus d'écriture faciles à déchiffrer.

III.8.3 Solution arithmétique

Posons $\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$, plus généralement noté $\overline{\mathbb{N}} = \mathbb{N} \cup \{\infty\}$, ce nouvel élément vérifie quelques formules :

- $\forall n \in \mathbb{N} (n < \infty)$
- $\forall n \in \mathbb{N} (n + \infty = \infty)$
- $\forall n \in \mathbb{N}^* (n \times \infty = \infty)$
- $0 \times \infty = 0$

Ces règles (et la commutativité) permettent de créer les tables d'addition et de multiplication dans $\overline{\mathbb{N}}$:

+	0	1	...	n	...	∞
0	0	1	...	n	...	∞
1	1	2	...	n+1	...	∞
...
n	n	n+1	...	2n	...	∞
...
∞	∞	∞	...	∞	...	∞

×	0	1	...	n	...	∞
0	0	0	...	0	...	0
1	0	1	...	n	...	∞
...
n	0	n	...	n ²	...	∞
...
∞	0	∞	...	∞	...	∞

III.8.4 Compactifié d'Alexandrov

Car Dieu est le compactifié d'Alexandrov de l'univers.

A. Grothendieck ⁵⁸

Cette méthode, très générale (elle s'applique à la classe des espaces localement compacts, mais non compacts), est due à Pavel Sergejevich Alexandrov (1896 – 1982), un mathématicien russe.

La compactification d'Alexandrov d'un espace topologique \mathcal{X} , consiste en un espace compact noté \mathcal{X}^* (ou $\overline{\mathcal{X}}$) et un plongement continu $\varphi : \mathcal{X} \rightarrow \mathcal{X}^*$, tels que $\varphi(\mathcal{X})$ est dense dans \mathcal{X}^* , et $\mathcal{X}^* \setminus \varphi(\mathcal{X})$ est de cardinal 1, cet élément est appelé « Point à l'infini » et est souvent noté ∞ , de ce fait, par un léger abus de langage on peut écrire : $\mathcal{X}^* = \mathcal{X} \cup \{\infty\}$.

Les ouverts de \mathcal{X}^* sont les ouverts de \mathcal{X} et les ensembles de la forme $\mathcal{X}^* \setminus \mathcal{K}$ où \mathcal{K} est un compact de \mathcal{X} ; cette définition assure que \mathcal{X}^* est compact, mais en plus que \mathcal{X} est dense dans \mathcal{X}^* .

Nous n'allons nous intéresser qu'au cas où $\mathcal{X} = \mathbb{N}$, son compactifié d'Alexandrov sera noté $\overline{\mathbb{N}}$.

La topologie de \mathbb{N} , étant discrète, et comme $|\mathbb{N}| = \aleph_0$, pour que $\overline{\mathbb{N}}$ soit compact, il faut et il suffit qu'un ouvert de $\overline{\mathbb{N}}$ contenant ∞ soit un ensemble cofini ⁵⁹ contenant ∞ .

Il est immédiat de démontrer que $\psi : \overline{\mathbb{N}} \rightarrow \{0\} \cup \{\frac{1}{n} \mid n \in \mathbb{N}\}$ définie par : $\begin{cases} \psi(\infty) &= 0 \\ \psi(n) &= \frac{1}{n} \end{cases}$ est un homéomorphisme.

Les trois méthodes précédentes semblent donner le même résultat, c'est exact dans le sens où dans les trois cas, le résultat consiste à adjoindre à \mathbb{N} un élément supplémentaire (le point à l'infini), mais :

1. La première ne tient compte que de l'ordre et les opérations ne sont pas totalement définies.
2. La deuxième ne tient compte que de l'arithmétique.
3. La troisième ne tient compte que de la topologie. Comme le compactifié d'Alexandrov ne contient qu'un point qui ne soit pas déjà dans \mathbb{N} , il est facile de prolonger l'addition et la multiplication de \mathbb{N} à $\overline{\mathbb{N}}$, d'autant plus que les opérations définies dans le cas 2 correspondent à un prolongement par continuité de ces opérations dans le cas 3.

⁵⁸. Cité dans M. Chouhan *Nicolas Bourbaki, Faits et légendes*, Éditions du Choix, 1995

⁵⁹. C'est à dire un sous-ensemble de $\overline{\mathbb{N}}$ de complémentaire fini.

III.8.5 Compactifié de Stone-Čech

Actuellement, le compactifié de the Stone-Čech des entiers naturels, $\beta\mathbb{N}$, est un sujet d'étude majeure en topologie ensembliste, car il existe de nombreuses pathologies cachées dans la structure de $\beta\mathbb{N}$.

Tarun Chitra⁶⁰

Cette méthode, encore plus générale (qui peut s'appliquer à tous les espaces topologiques complètement régulier⁶¹), doit son nom à Marshall Harvey Stone, un mathématicien américain (1903 – 1989) et Eduard Čech, un mathématicien tchèque, tchécoslovaque à l'époque (1893 - 1960).

Le besoin d'une autre compactification que celle d'Alexandroff est parfaitement illustré par le cas de \mathbb{N} muni de sa topologie habituelle (la topologie discrète) : soit $f : \mathbb{N} \mapsto \mathbb{R}$ définie par $\begin{cases} f(2n) &= 0 \\ f(2n+1) &= 1 \end{cases}$.

Cette fonction est bien évidemment continue et bornée sur \mathbb{N} , mais elle n'est pas prolongeable par continuité au compactifié d'Alexandroff $\bar{\mathbb{N}}$.

Le compactifié de Stone-Čech de \mathcal{X} est le plus gros compact engendré par \mathcal{X} (alors que le compactifié d'Alexandroff est le plus petit : on ajoute un seul point), dans le sens précis où :

Pour tout compact \mathcal{K} et toute application continue $f : \mathcal{X} \mapsto \mathcal{K}$, il existe une application unique $\beta f : \beta\mathcal{X} \mapsto \mathcal{K}$, tel que $f = \beta f \circ i$, ce qui peut se traduire sous la forme d'une propriété universelle (et d'objet initial) dans le langage des catégories :

D'où le Diagramme commutatif :

$$\begin{array}{ccc} \mathcal{X} & \xrightarrow{i} & \beta\mathcal{X} \\ & \searrow f & \downarrow \beta f \\ & & \mathcal{K} \end{array}$$

Nous n'allons nous intéresser essentiellement au cas où $\mathcal{X} = \mathbb{N}$

Il existe plusieurs façon de construire le compactifié de Stone-Čech d'un espace \mathcal{X} :

1. Méthode topologique (plongement de \mathcal{X} dans un produit infini de l'intervalle $[0; 1]$).
2. Méthode algébrique/topologique (à partir de l'anneau des fonctions à valeurs réelles, continues et bornées sur \mathcal{X}).
3. Méthode ensembliste (à l'aide d'ultrafiltres).

Pour étudier le cas de \mathbb{N} , nous allons développer la méthode des ultrafiltres (nous travaillerons dans ZFC, c'est à dire avec axiome du choix).

Définition : Soit \mathcal{X} un ensemble (nous ne considérerons que des ensembles de cardinal infini), une famille de sous-ensembles de \mathcal{X} , notée \mathcal{U} , c'est à dire que $\mathcal{U} \in \mathfrak{P}(\mathfrak{P}(\mathcal{X}))$, est un ultrafiltre si et seulement si :

- $\forall \mathcal{A} \forall \mathcal{B} ((\mathcal{A} \in \mathcal{U}) \wedge (\mathcal{B} \in \mathcal{U}) \Rightarrow (\mathcal{A} \cap \mathcal{B} \in \mathcal{U}))$
- $\forall \mathcal{A} \forall \mathcal{B} (((\mathcal{A} \in \mathcal{U}) \wedge (\mathcal{A} \subset \mathcal{B} \subset \mathcal{X})) \Rightarrow (\mathcal{B} \in \mathcal{U}))$
- $\emptyset \notin \mathcal{U}$
- $\forall \mathcal{A} ((\mathcal{A} \in \mathcal{U}) \vee ((\mathcal{X} \setminus \mathcal{A}) \in \mathcal{U}))$

Les trois premières conditions correspondent à la définition d'un filtre sur \mathcal{X} .

Des exemples de filtres sont très faciles à donner :

Soit $\mathcal{A} \subset \mathcal{X}$, $\mathcal{A} \neq \emptyset$, alors l'ensemble des sur-ensembles de \mathcal{A} est un filtre sur \mathcal{X} , mais n'est un ultrafiltre que si \mathcal{A} est un singleton, dans ce cas l'ultrafiltre est dit *ultrafiltre principal*.

Un exemple plus intéressant est le filtre de Fréchet (ensemble des sous-ensembles cofinis) :

$$\forall \mathcal{A} \subset \mathcal{X} ((\mathcal{A} \in \mathcal{F}) \Leftrightarrow |\mathcal{X} \setminus \mathcal{A}| < \aleph_0)$$

Le filtre de Fréchet n'est pas un ultrafiltre, il suffit de considérer l'ensemble $2\mathbb{N}$ des entiers pairs qui n'est pas cofini et dont le complémentaire n'est pas cofini non plus.

60. Dans *The Stone-Čech Compactification*, Cornell University, Cours de Topologie, 2009.

61. Un espace topologique \mathcal{X} est complètement séparé si tout singleton est un fermé et si pour tout fermé $\mathcal{F} \subset \mathcal{X}$ et tout $x \notin \mathcal{F}$ il existe une fonction continue $f : \mathcal{X} \mapsto [0; 1]$ telle que $f(x) = 0$ et $f(\mathcal{F}) = 1$.

On peut montrer très facilement qu'un ultrafiltre est principal ou contient le filtre de Fréchet, ce qui est une façon de dire que les ultrafiltres « intéressants » contiennent le filtre de Fréchet.

Le lemme de Zorn (équivalent à l'axiome du choix) permet de démontrer que pour tout filtre \mathcal{F} , il existe un ultrafiltre \mathcal{U} qui contient \mathcal{F} (cette propriété est appelé *Axiome de l'ultrafiltre*, il est plus faible que l'axiome du choix ($AC \Rightarrow AU$, mais le contraire n'est pas vrai)).

Soit $\beta\mathcal{X}$ l'ensemble des ultrafiltres sur \mathcal{X} , on peut déjà remarquer que \mathcal{X} s'injecte naturellement dans $\beta\mathcal{X}$ en identifiant chaque élément x de \mathcal{X} avec \mathcal{F}_x , l'ultrafiltre principal engendré par $\{x\}$.

On peut munir $\beta\mathcal{X}$ d'une topologie, appelée topologie de Stone, que nous noterons \mathcal{T}_S :

A tout $\mathcal{A} \subset \mathcal{X}$ on associe $\widehat{\mathcal{A}} = \{\mathcal{U} \mid (\mathcal{U} \in \beta\mathcal{X}) \wedge (\mathcal{A} \in \mathcal{U})\}$. L'ensemble $\mathcal{V} = \{\widehat{\mathcal{A}} \mid \mathcal{A} \subset \mathcal{X}\}$ est une base d'ouverts pour la topologie de Stone.

Avec cette topologie on peut vérifier facilement que \mathcal{X} est dense dans $\beta\mathcal{X}$.

Il est tout aussi immédiat que $\beta\mathcal{X}$, muni de la topologie Stone est compact (tout ouvert contenant un élément de $\beta\mathcal{X} \setminus \mathcal{X}$ contient au moins un ultrafiltre contenant le filtre de Fréchet, comme tous les éléments de $\beta\mathcal{X}$ qui sont donc tous dans le même ouvert, et comme il contient au moins un cofini de \mathcal{X} et qu'il inclut les filtres principaux de chacun de ses éléments, au pire il reste un ensemble fini qui peut être recouvert par un nombre fini d'ouverts).

Nous avons donc que $(\beta\mathcal{X}, \mathcal{T}_S)$, est bien une compactification de \mathcal{X} .

Dans le cas particulier de \mathbb{N} , $\beta\mathbb{N}$ peut être muni d'une addition qui prolonge (continuellement) l'addition sur \mathbb{N} :

Soit $\mathcal{A} \subset \mathbb{N}$ et $n \in \mathbb{N}$, on note $\mathcal{A} - n = \{m \mid (m \in \mathbb{N}) \wedge (k + n \in \mathcal{A})\}$

Soit \mathcal{U} et \mathcal{V} , deux ultrafiltres sur \mathbb{N} , on définit leur somme par :

$$\mathcal{U} + \mathcal{V} = \{\mathcal{A} \mid (\mathcal{A} \subset \mathbb{N}) \wedge (\{n \mid (n \in \mathbb{N}) \wedge (A - n \in \mathcal{U})\} \in \mathcal{V})\}$$

Avec cette définition, on peut vérifier :

- $\mathcal{U} + \mathcal{V}$ est un ultrafiltre.
- $(\mathcal{U} + \mathcal{V}) + \mathcal{W} = \mathcal{U} + (\mathcal{V} + \mathcal{W})$.
- $\mathcal{F}_n + \mathcal{F}_m = \mathcal{F}_{n+m}$

Par contre cette addition des ultrafiltres n'est pas commutatives.

III.8.6 Utilisation en physique

Le compactifié de Stone-Čech est utilisé en mécanique quantique et en théorie des cordes, ainsi qu'en théorie des probabilités.

III.8.7 Références

1. Compactifié d'Alexandroff

- i) C. Byliński, *Alexandroff One Point Compactification*, Formalized Mathematics, Volume 15, No. 4, p. 167 - 170, Université de Białystok, Pologne, 2007.
- ii) S. Jabuka, *The One Point Compactification*, University of Nevada, Reno, 2006.
- iii) P. Larson & F. D. Tall, *Locally Compact Perfectly Normal Spaces May All Be Paracompact*, Department of Mathematics, University of Toronto, Canada, 2010.

2. Compactifié de Stone-Čech

- i) M. Rubin & D. Leung, *The Stone-Čech Compactification*, Department of Mathematics, National University of Singapore, Singapore, 14th NUROP Congress, 2009.
- ii) D. Bar-Natan, *Ultrafilters, Compactness, and the Stone-Čech Compactification*, Department of Mathematics, University of Toronto, Canada, 1993.
- iii) T. Chitra, *The Stone-Čech Compactification*, Cornell University, Cours de Topologie, 2009.

3. Compactifié de Wallman

- i) F. G. Arenas & M. A. Sánchez-Granero, *Wallman Compactification and Zero-Dimensionality*, Divulgaciones Matemáticas, Volume 7, No. 2, p. 151 - 155, 1999.

- ii) F. G. Arenas & M. A. Sánchez-Granero, *Compactifications of Fractal Structures*, Acta Mathematica Universitatis Comenianae, Bratislava, Slovaquie, Volume LXXIII, No 1, p. 1 – 20, 2004.

4. Compactifié de Bohr

- i) J. E. Hart & K. Kunen, *Bohr Compactifications of Discrete Structures*, Fundamenta Mathematicae, Volume 160, p. 101 - 151, 1999.
- ii) Y. Katznelson, *Suites Aléatoires d'Entiers*, Springer Lecture Notes in Math, Volume 336, p. 148 - 152, 1972.

5. Compactifié de Royden

- i) J. Wysoczański, *Royden Compactification of Integers*, Hiroshima Mathematical Journal, Volume 26, No 3, p. 515 - 529, 1996.
- ii) I. Okajima, *Study of the Topological Structure of the Royden Compactification of the Unit Disk*, Thèse de l'Université de l'Etat de l'Orégon, 1971.

6. \mathcal{G} -Compactifié

- i) J. van Mill, *On the G -Compactifications of the Rational Numbers*, Monatshefte für Mathematik, Volume 157, p. 257 - 266, 2009.
- ii) G. Barat, T. Downarowicz, A. Iwanik & P. Liardet, *Propriétés Topologiques et Combinatoires des Echelles de Numération*, Université de Provence, Centre de Mathématiques et Informatique, 1991.
- iii) J. de Vries, *On The G -Compactification of Products*, Pacific Journal Of Mathematics, Volume 110, No 2, p. 447 - 470, 1984

III.9 Droite réelle achevée $\overline{\mathbb{R}}$

III.9.1 Introduction

Il est facile de montrer que \mathbb{R} , muni de sa topologie usuelle, n'est pas compact ; on peut donc s'intéresser aux différentes compactifications possibles de cet espace topologique (l'espace topologique séparé Y est un compactifié de l'espace topologique séparé X si X est homéomorphe à un sous-espace dense de Y). Il existe plusieurs compactifications de \mathbb{R} : de la plus petite, le compactifié d'Alexandroff (homéomorphe au cercle unité du plan S^2) à la plus grande, le compactifié de Stone-Čech (dont le cardinal est le même que celui de l'ensemble des parties de \mathbb{R} , c'est à dire $2^{2^{\aleph_0}}$). Entre ces deux extrêmes il y a la Droite Réelle Achevée (homéomorphe à $[0, 1]$) usuellement notée $\overline{\mathbb{R}}$ ⁶².

III.9.2 Définition

On définit l'ensemble $\overline{\mathbb{R}}$ par adjonction de deux nouveaux éléments $-\infty$ et $+\infty$ à \mathbb{R} : $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$.

La droite réelle achevée est l'ensemble $\overline{\mathbb{R}}$ muni de la topologie rendant l'espace topologique ainsi obtenu homéomorphe au sous-espace $[0, 1]$ (muni de la topologie usuelle).

III.9.3 Mode de construction

Il est possible d'étendre la relation d'ordre sur \mathbb{R} en une relation d'ordre total sur $\overline{\mathbb{R}}$ en imposant : $\forall x \in \overline{\mathbb{R}}, -\infty \leq x \leq +\infty$.

Notons pour tout $x \in \mathbb{R}$, $]x, \rightarrow[= \{y \in \overline{\mathbb{R}}, y > x\}$ et de même $[\leftarrow, x[= \{y \in \overline{\mathbb{R}}, y < x\}$. Alors, $\{]x, \rightarrow[, [\leftarrow, x[, x \in \mathbb{R}\}$ définit une base topologique sur $\overline{\mathbb{R}}$ telle que l'espace topologique ainsi obtenu soit bien un compactifié de \mathbb{R} homéomorphe à $[0, 1]$.

III.9.4 Tables d'addition et de multiplication

On étend l'addition et la multiplication entre réels sur $\overline{\mathbb{R}}$ par :

+	$-\infty$	$y \in \mathbb{R}$	$+\infty$
$-\infty$	$-\infty$	$-\infty$	
$x \in \mathbb{R}$	$-\infty$	$x + y$	$+\infty$
$+\infty$		$+\infty$	$+\infty$

\times	$-\infty$	$y \in \mathbb{R}_-^*$	0	$y \in \mathbb{R}_+^*$	$+\infty$
$-\infty$	$+\infty$	$+\infty$		$-\infty$	$-\infty$
$x \in \mathbb{R}_-^*$	$+\infty$	$x \cdot y$	0	$x \cdot y$	$-\infty$
0		0	0	0	
$x \in \mathbb{R}_+^*$	$-\infty$	$x \cdot y$	0	$x \cdot y$	$+\infty$
$+\infty$	$-\infty$	$-\infty$		$+\infty$	$+\infty$

En réalité, il s'agit des prolongements par continuité des applications :

$$\begin{cases} \mathbb{R} \times \mathbb{R} & \rightarrow & \mathbb{R} \\ (x, y) & \mapsto & x + y \end{cases} \text{ sur } \mathbb{R} \times \overline{\mathbb{R}} \text{ (et sur } \overline{\mathbb{R}} \times \mathbb{R})$$

et

$$\begin{cases} \mathbb{R}^* \times \mathbb{R}^* & \rightarrow & \mathbb{R} \\ (x, y) & \mapsto & x \cdot y \end{cases} \text{ sur } \overline{\mathbb{R}}^* \times \overline{\mathbb{R}}^*.$$

De même, on peut prolonger sur $\overline{\mathbb{R}}$ d'autres fonctions, ce qui permet notamment d'écrire $e^{-\infty} = 0$, $\frac{1}{\pm\infty} = 0$, $\ln(+\infty) = +\infty$.

On remarquera que $+\infty$ et $-\infty$ ne sont pas réguliers ni pour l'addition ni pour le produit.

62. Le compactifié d'Alexandroff est malheureusement souvent noté de la même façon.

III.9.5 Conjugué, Module, Norme, Forme Polaire et Inverse

Après avoir ordonné $\overline{\mathbb{R}}$, on peut définir pour tout $x \in \overline{\mathbb{R}}$, $x^+ = \max(x, 0)$ et $x^- = \min(x, 0)$. Une manière naturelle d'étendre la valeur absolue réelle est alors de poser pour tout $x \in \overline{\mathbb{R}}$, $|x| = x^+ + x^-$; à noter cependant que $|\cdot|$ ne définit ni une valeur absolue, ni une norme sur $\overline{\mathbb{R}}$, n'étant pas à valeur dans \mathbb{R} ; néanmoins $|\cdot|$ vérifie bien $|x \cdot y| = |x| \cdot |y|$ et $|x + y| \leq |x| + |y|$ **lorsque ces opérations sont définies**.

III.9.6 Propriétés algébriques

La construction de $\overline{\mathbb{R}}$ est avant tout topologique, et ses propriétés algébriques sont très pauvres pour la simple raison que ni l'addition ni la multiplication ne constitue une loi de composition interne : les opérations $(+\infty) + (-\infty)$ et $0 \times (\pm\infty)$ ne sont en effet pas définies.

La droite réelle achevée possède cependant une propriété importante : toute partie de $\overline{\mathbb{R}}$ admet une borne supérieure et une borne inférieure.

III.9.7 Synonymes, Isomorphismes, Exemples

Le sous-espace $\overline{\mathbb{N}} = \mathbb{N} \cup \{+\infty\} \subset \overline{\mathbb{R}}$, qui n'est autre que le compactifié d'Alexandroff de \mathbb{N} muni de sa topologie usuelle, est aussi parfois utilisé, notamment dans l'étude des suites. (On pourra également rapprocher d'une certaine manière $\overline{\mathbb{N}}$ et l'ensemble des proto-nombres.)

III.9.8 Utilisation en physique

L'infini, en tant que valeur, n'est pas vraiment utilisé en physique, car souvent synonyme de limite d'un modèle. C'est pourquoi $\overline{\mathbb{R}}$ n'est, à ma connaissance, pas utilisé en physique.

III.9.9 Références

1. Topologie générale. Chapitres 1 à 4, N. Bourbaki.

III.10 Supernaturels \mathbb{SN}

III.10.1 Introduction

L'ensemble des nombres Supernaturels que nous noterons \mathbb{SN} par la suite, est une extension naturelle de \mathbb{N}^* , en tant que treillis (pour la relation de divisibilité).

\mathbb{SN} permet de prolonger à certains [groupes profinis](#) des théorèmes valides pour les groupes finis.

Un Supernaturel peut aussi caractériser le degré d'une extension algébrique de corps quelconque (et pas seulement les extensions finies).

III.10.2 Définition

Un nombre Supernaturel est défini comme un produit formel indexé par \mathbb{P} l'ensemble des nombres entiers naturels premiers :

$$x = \prod_{p \in \mathbb{P}} p^{n_p}. \text{ Où } n_p \in \mathbb{N} \cup \{\infty\} = \overline{\mathbb{N}}, \text{ ensemble dans lequel l'addition est prolongée par } n + \infty = \infty.$$

L'exposant n_p est parfois noté $v_p(x)$ par prolongation de la valuation p-adique à $\overline{\mathbb{N}}$.

On peut remarquer que si l'ensemble des p tels que $v_p(x) \neq 0$ est fini, et si aucun $v_p(x) = \infty$, alors x est simplement un nombre entier naturel, (c'est à dire $\mathbb{N}^* \subset \mathbb{SN}$). A noter que 0 n'est pas considéré comme un Supernaturel.

III.10.3 Table de multiplication

Il n'existe pas de définition naturelle d'une addition sur l'ensemble des Supernaturels (il est difficile de se faire une idée de la signification de $2^\infty + 3$)

La multiplication sur \mathbb{SN} au contraire se définit de façon très naturelle (elle prolonge naturellement la multiplication sur \mathbb{N}) :

$$\prod_{p \in \mathbb{P}} p^{v_p(x)} \times \prod_{p \in \mathbb{P}} p^{v_p(y)} = \prod_{p \in \mathbb{P}} p^{v_p(x) + v_p(y)}$$

On peut aussi définir la relation de divisibilité en prolongeant la divisibilité sur \mathbb{N}) :

$$(x \mid y) \Leftrightarrow (\forall p \in \mathbb{P} (v_p(x) \leq v_p(y)))$$

(\mathbb{SN}, \mid) est un ensemble partiellement ordonné, avec un minimum et un maximum.

Et, bien sur, on peut prolonger les notions de PPCM et de PGCD :

Pour une famille $(x_i)_{i \in I}$ de nombres Supernaturels :

- $\text{PPCM}((x_i)_{i \in I}) = \prod_{p \in \mathbb{P}} p^{\sup_{i \in I} (v_p(x_i))}$
- $\text{PGCD}((x_i)_{i \in I}) = \prod_{p \in \mathbb{P}} p^{\inf_{i \in I} (v_p(x_i))}$

Ces définitions permettent de calculer le PPCM et le PGCD de toutes familles de nombres Supernaturels, donc en particulier d'une famille infinie de nombres entiers naturels (même si le PGCD peut être un nombre Supernaturel qui n'est pas un entier naturel).

Lorsque la famille est réduite à deux éléments, on note plutôt :

- $x \vee y = \text{PPCM}(x, y)$
- $x \wedge y = \text{PGCD}(x, y)$

III.10.4 Propriétés algébriques

$(\mathbb{SN}, \vee, \wedge)$ est un treillis distributif complet (donc borné), pseudo-complémenté mais non complémenté, donc ce n'est pas une algèbre de Boole.

Le minimum de ce treillis est 1 et le maximum est $\omega = \prod_{p \in \mathbb{P}} p^\infty$

Les atomes de ce treillis sont les nombres premiers.

C'est une algèbre de Heyting complète, c'est à dire un treillis borné, complet qui possède la propriété supplémentaire :

Pour tout a et tout b il existe un x maximum tel que $a \wedge x \leq b$; cet élément est le pseudo complément de a par rapport à b , et il est généralement noté $a \rightarrow b$

Le pseudo complément d'un élément est le pseudo complément de cet élément par rapport au minimum du treillis, généralement noté $\neg x$.

Soit a et b deux supernaturels, alors le pseudo complément de a par rapport à b , x est défini par (la vérification est triviale) :

$$v_p(x) = \begin{cases} v_p(a) \neq 0 & \Rightarrow v_p(b) \\ v_p(a) = 0 & \Rightarrow \infty \end{cases}$$

Dans le cas où $b = 0$, on trouve $\neg a$ le pseudo complément de a , dont on peut vérifier que $\neg a \vee a$, n'est généralement pas égal à ω (le maximum de \mathbb{SN}), et n'est donc pas un complément de a .

On peut munir \mathbb{SN} de la topologie de Scott, c'est à dire une topologie dont une base d'ouverts est donnée par :

$$U_n = \{x \in \mathbb{SN} \mid x \geq n\} \text{ (la relation d'ordre étant la divisibilité).}$$

Cette topologie permet de définir la catégorie des multiset (une extension de la notion de multiset fini).

III.10.5 Synonymes, Isomorphismes, Exemples

Les nombres Supernaturels sont parfois appelés « Entiers naturels généralisés » ou « Nombres de Steinitz ».

Attention l'expression "nombres supernaturels" désigne parfois les éléments non-standard de certains modèles de l'arithmétique de Peano.

On peut aussi, de façon très naturelle, définir $\mathbb{SN} = \overline{\mathbb{N}}^{\mathbb{P}}$, ou encore, de façon un peu moins naturelle (il suffit de changer l'interprétation) $\mathbb{SN} = \overline{\mathbb{N}}^{\mathbb{N}}$

Une extension possible de \mathbb{SN} , est d'autoriser les $v_p(x)$ à prendre leur valeur dans $\overline{\mathbb{Z}} = \mathbb{Z} \cup \{-\infty, \infty\}$, avec les trois règles d'addition supplémentaires :

$$\begin{aligned} \infty + n &= \infty \\ -\infty + n &= -\infty \\ \infty - \infty &= 0 \end{aligned}$$

Néanmoins ce nouvel ensemble n'est pas un groupe pour la multiplication, cette opération n'étant pas régulière (elle n'est plus associative).

III.10.6 Utilisation en physique

Aucune référence attestant de l'utilisation des Supernaturels en physique n'a pu être trouvée.

III.10.7 Références

1. [Détails sur les extensions algébriques et les groupes profinis](#)
2. [Diagonal direct limits of monomial groups](#)
3. [Weakly locally finite MV-algebras and real-valued multisets](#)
4. [The Modular Representation Theory of Profinite Groups](#)

IV Méthodes de construction

IV.1 Multicomplexes \mathbb{MC}_n

IV.1.1 Introduction

La dénomination Multicomplexe peut faire référence à deux types d'ensembles assez différents, ceux qui sont présentés ici et qui sont notés \mathbb{MC}_n et les **multicomplexes** \mathbb{C}_n .

IV.1.2 Définition

Soit e un élément tel que $e^n = -1$ (ce n'est donc pas la constante de Neper).

L'ensemble \mathbb{MC}_n est l'ensemble des nombres de la forme $x = \sum_{i=0}^{n-1} a_i \cdot e^i$, où les a_i sont des réels.

Attention : pour $n > 2$, e n'est pas une racine n -ième complexe de -1 .

IV.1.3 Mode de construction

\mathbb{MC}_n est un cas particulier **d'algèbre de Clifford généralisée**.

IV.1.4 Table de multiplication

La table de multiplication des nombres multicomplexes est très simple et surtout elle est unique pour un n donné.

Exemple
n = 5

×	1	e	e ²	e ³	e ⁴
1	1	e	e ²	e ³	e ⁴
e	e	e ²	e ³	e ⁴	-1
e ²	e ²	e ³	e ⁴	-1	e
e ³	e ³	e ⁴	-1	e	e ²
e ⁴	e ⁴	-1	e	e ²	e ³

Exemple
n = 4

×	1	e	e ²	e ³
1	1	e	e ²	e ³
e	e	e ²	e ³	-1
e ²	e ²	e ³	-1	e
e ³	e ³	-1	e	e ²

IV.1.5 Conjugué, Module, Norme, Forme Polaire et Inverse

On peut aussi représenter les éléments de \mathbb{MC}_n par un élément de $M_n(\mathbb{R})$. Soit $x = \sum_{i=0}^{n-1} a_i \cdot e^i$, on peut lui associer la matrice $n \times n$:

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots & a_{n-1} \\ -a_{n-1} & a_0 & a_1 & \cdots & a_{n-2} \\ -a_{n-2} & -a_{n-1} & a_0 & \cdots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_1 & -a_2 & -a_3 & \cdots & a_0 \end{pmatrix}$$

Cette écriture sous forme d'une matrice permet de définir une pseudo-norme ($|x| = 0$ n'entraîne pas $x = 0$) sur \mathbb{MC}_n :

$|x|^n = \det(A)$, c'est à dire que dans le cas $n = 2$ on retrouve bien le module des nombres complexes, mais pour $n = 3$ on trouve $|x|^3 = a_0^3 - a_1^3 + a_2^3 + 3a_0a_1a_2$ qui est nul, par exemple, pour $a_0 = a_1$ et $a_2 = 0$.

Les éléments de pseudo-norme nulle sont des diviseurs de 0, par exemple, pour $n = 3$: $(1+e)(1-e+e^2) = 0$

Si $|x| \neq 0$, il est possible d'écrire x sous forme polaire : $x = |x| \exp\left(\sum_{i=0}^{n-1} \Phi_i \cdot e^i\right)$

IV.1.6 Propriétés algébriques

\mathbb{MC}_n est une algèbre commutative et associative de dimension n sur \mathbb{R} , générée par un seul élément : e ($\oplus^n \mathbb{R}$).

Mais on peut aussi décomposer \mathbb{MC}_n sur \mathbb{C} , Plus précisément :

Si n est pair $\mathbb{MC}_n = \oplus^{\frac{n}{2}} \mathbb{C}$

Si n est impair $\mathbb{MC}_n = \mathbb{R} \oplus^{\frac{n-1}{2}} \mathbb{C}$

IV.1.7 Synonymes, Isomorphismes, Exemples

Les multicomplexes sont des cas particuliers des **algèbres hypercomplexes**.

Pour $n = 2$ on retrouve les **nombres complexes**,

Pour $n = 4$ on retrouve les **bicomplexes**.

Rappel de la table de multiplication des bicomplexes (en utilisant les notations habituelles i, j, ij à la place des e_i :

\times	1	i	j	ij
1	1	i	j	ij
i	i	-1	ij	-j
j	j	ij	-1	-i
ij	ij	-j	-i	1

Pour définir un isomorphisme $\varphi : \mathbb{C}_2 \mapsto \mathbb{M}\mathbb{C}_4$ ($\mathbb{C}_2 =$ les **bicomplexes**), il suffit de définir les images d'une base.

Par exemple :

$$\varphi(1) = 1 \text{ (pas le choix pour une } \mathbb{R}\text{-algèbre)}$$

$$\varphi(i) = e^2$$

$$\varphi(j) = \frac{\sqrt{2}}{2}(e^3 + e)$$

$$\varphi(ij) = \varphi(i) \cdot \varphi(j) = e^2 \cdot \frac{\sqrt{2}}{2}(e^3 + e) = \frac{\sqrt{2}}{2}(e^3 - e)$$

Avec ces données il est facile de construire la table de multiplication des images et de vérifier que c'est la même que celle de \mathbb{C}_2 .

Variations : on peut aussi définir des ensembles de nombres en posant $e^n = 1$ (en place de $e^n = -1$)

IV.1.8 Utilisation en physique

Théorie des Champs, cf. ci-dessous.

IV.1.9 Références

1. [Algèbres de Clifford - Supersymétrie et Symétries \$\mathbb{Z}_n\$ - Applications en Théorie des Champs](#)
2. Commutative Extended Complex Numbers and Connected Trigonometry N. Fleury, M. Rausch De Trautenberg, R. M. Yamaleev Journal of mathematical analysis and applications ISSN 0022-247X 1993, vol. 180, No2, pp. 431-457
3. Extended Complex Number Analysis and Conformal-like Transformations N. Fleury, M. Rausch de Trautenberg, R.M. Yamaleev Journal of mathematical analysis and applications ISSN 0022-247X 1995, vol. 191, N° 1, pp. 118-136

IV.2 Multicomplexes \mathbb{C}_n

IV.2.1 Introduction

Les nombres multicomplexes \mathbb{C}_n ⁶³ ont été introduit au 19^{ème} siècle par Corrado Segre (mathématicien italien, 1863 - 1924), dans le but de généraliser les nombres complexes, (idée qui amena W. R. Hamilton à définir les **quaternions**), il les nomma *Nombres n-complexes*.

Ils ont été particulièrement étudiés par G. B. Price et N. Fleury. ⁶⁴

IV.2.2 Définition

L'ensemble \mathbb{C} des **nombres complexes** peut être vu comme une \mathbb{R} -algèbre engendrée par un nouvel élément $i \notin \mathbb{R}$ vérifiant $i^2 = -1$.

L'idée fondatrice des nombres multicomplexes est d'appliquer la même idée à \mathbb{C} , puis au résultat ainsi obtenu, puis au résultat ainsi obtenu, etc.

IV.2.3 Mode de construction

La définition des nombres multicomplexes \mathbb{C}_n est donnée par récurrence :

1. $\mathbb{C}_0 = \mathbb{R}$
2. $\mathbb{C}_{n+1} = \{x_0 + x_1 \cdot i_{n+1} \mid ((x_0, x_1) \in \mathbb{C}_n^2) \wedge (i_{n+1} \notin \mathbb{C}_n) \wedge (i_{n+1}^2 = -1)\}$

Les premiers ensembles de multicomplexes ont reçus des noms :

- $\mathbb{C}_1 = \mathbb{C}$
- $\mathbb{C}_2 =$ **nombres bicomplexes**.
- $\mathbb{C}_3 =$ nombres tricomplexes.

IV.2.4 Table de multiplication

En prenant l'exemple des tricomplexes, on obtient la table de multiplication suivante (où i_1 est en fait le i de \mathbb{C} , et, pour simplifier les écritures, nous noterons $i_{nm} = i_n \cdot i_m = i_m \cdot i_n$) :

\cdot	1	i_1	i_2	i_3	i_{12}	i_{13}	i_{23}	i_{123}
1	1	i_1	i_2	i_3	i_{12}	i_{13}	i_{23}	i_{123}
i_1	i_1	-1	i_{12}	i_{13}	$-i_2$	$-i_3$	i_{123}	$-i_{23}$
i_2	i_2	i_{12}	-1	i_{23}	$-i_1$	i_{123}	$-i_3$	$-i_{13}$
i_3	i_3	i_{13}	i_{23}	-1	i_{123}	$-i_1$	$-i_2$	$-i_{12}$
i_{12}	i_{12}	$-i_2$	$-i_1$	i_{123}	1	$-i_{23}$	$-i_{13}$	i_3
i_{13}	i_{13}	$-i_3$	i_{123}	$-i_1$	$-i_{23}$	1	$-i_{12}$	i_2
i_{23}	i_{23}	i_{123}	$-i_3$	$-i_2$	$-i_{13}$	$-i_{12}$	1	i_1
i_{123}	i_{123}	$-i_{23}$	$-i_{13}$	$-i_{12}$	i_3	i_2	i_1	-1

IV.2.5 Propriétés algébriques

Addition et multiplication sont associatives et commutatives, la multiplication est distributive sur l'addition, c'est à dire que, $(\mathbb{C}_n, +, \cdot)$ est un anneau unitaire.

En appliquant deux fois la définition, on obtient, pour $n \geq 2$:

$$\mathbb{C}_n = \{x_{00} + x_{01} \cdot i_{n-1} + x_{10} \cdot i_n + x_{11} \cdot i_{n-1} \cdot i_n \mid ((x_{00}, x_{01}, x_{10}, x_{11}) \in \mathbb{C}_{n-2}^4)\}$$

Et en itérant ces calculs, on peut finalement exprimer un élément de \mathbb{C}_n à l'aide de 2^k éléments de \mathbb{C}_{n-k} , ou 2^{n-1} éléments de \mathbb{C} ou 2^n éléments de \mathbb{R} . Autrement dit \mathbb{C}_n est une \mathbb{C}_{n-k} -algèbre de dimension 2^k (pour $n \geq k$), une \mathbb{C} -algèbre de dimension 2^{n-1} (pour $n \geq 1$), et une \mathbb{R} -algèbre de dimension 2^n .

Pour $n > 1$, \mathbb{C}_n contient des éléments non réels de carré 1 (par exemple e_{12} élément des bicomplexes) donc des diviseurs de 0.

⁶³. A ne pas confondre avec les **Nombres Multicomplexes**

⁶⁴. cf. les références.

IV.2.6 Synonymes, Isomorphismes, Exemples

Pour $n \geq 2$, posons $j_n = \frac{1 + i_{n-1} \cdot i_n}{2}$ et $\bar{j}_n = \frac{1 - i_{n-1} \cdot i_n}{2}$, un élément de \mathbb{C}_n qui s'écrit $x = x_0 + x_1 \cdot i_n$ peut alors aussi s'écrire $x = (x_0 - x_1 \cdot i_{n-1}) \cdot j_n + (x_0 + x_1 \cdot i_{n-1}) \cdot \bar{j}_n$.

Autrement dit (j_n, \bar{j}_n) est une base de \mathbb{C}_n en tant que \mathbb{C}_{n-1} -algèbre. Dans cette nouvelle base, la table de multiplication devient :

\cdot	j_n	\bar{j}_n
j_n	j_n	0
\bar{j}_n	0	\bar{j}_n

Cette base est appelée *base idempotente* de \mathbb{C}_n sur \mathbb{C}_{n-1} ; comme dans cette base, le produit de deux nombres multicomplexes se fait terme à terme, cela montre que $\mathbb{C}_n \cong \mathbb{C}_{n-1} \oplus \mathbb{C}_{n-1}$.

En itérant le résultat précédent et en posant $\overset{n}{\oplus} \mathcal{K}$ la somme directe de n copies de \mathcal{K} , on obtient le résultat : $\mathbb{C}_{n+1} \cong \overset{2^n}{\oplus} \mathbb{C}$

On peut aussi trouver une base idempotente de \mathbb{C}_n en tant que \mathbb{C} -algèbre (donc de taille 2^{n-1}). En remarquant que le produit de deux idempotents est idempotent, et qu'avec les notations précédentes $j_k \cdot \bar{j}_k = 0$, la famille suivante :

$$\left(\mathcal{J}_E = \prod_{2 \leq k \leq n}^{k \in E} j_k \cdot \prod_{2 \leq k \leq n}^{k \notin E} \bar{j}_k \right)_{E \subset [2, n]}$$

contient 2^{n-1} éléments idempotents (un élément de cette famille correspond à un sous ensemble de $[2, n]$) dont on peut montrer par récurrence qu'ils permettent d'écrire (sous forme de combinaisons linéaires) tous les éléments de \mathbb{C}_n , de plus si $E \neq F$ alors il existe un élément k dans E et pas dans F (ou le contraire), c'est à dire que j_k est un facteur de \mathcal{J}_E et \bar{j}_k est un facteur de \mathcal{J}_F (ou le contraire), et donc $\mathcal{J}_E \cdot \mathcal{J}_F = 0$.

La famille précédente est donc une base qui permet de mettre en évidence l'écriture de \mathbb{C}_n sous forme de somme directe d'algèbres de 2^{n-1} copies de \mathbb{C} . Cette base permet aussi de démontrer rapidement que \mathbb{C}_n ne contient pas d'élément nilpotent, et d'identifier rapidement les éléments inversibles : ceux dont toutes les coordonnées dans cette base sont des complexes inversibles, autrement dit, différents de 0.

On peut remarquer que \mathbb{C}_n est une sous-algèbre de l'algèbre de Clifford $\mathcal{Cl}_{0,2n}(\mathbb{R})$.

IV.2.7 Utilisation en physique

Les nombres multicomplexes \mathbb{C}_n permettent d'implémenter des algorithmes très performants de calcul de dérivée de tous ordres, ce qui peut intéresser beaucoup de branches de la physique, en particulier l'aéronautique.

IV.2.8 Références

1. C. Segre, *Le rappresentazioni reali delle forme complesse e gli enti iperalgebrici*, Mathematische Annalen, Vol. 40, No. 3, p. 413–467, 1892.
2. G. B. Price, *An Introduction to Multicomplex Spaces and Functions*, New York, Marcel Dekker Inc., 1991.
3. N. Fleury, M. R. Detraubenberg, et R. M. Yamaleev, *Commutative Extended Complex Numbers and Connected Trigonometry* Journal of Mathematical Analysis and Applications, Vol. 180, p. 431–457, 1993.
4. S. Olariu, *Complex Numbers in n Dimensions*, Institute of Physics and Nuclear Engineering, Bucarest, Roumanie, 2000.
5. G. Lantoine, R. P. Russelly et T. Dargent, *Using Multicomplex Variables for Automatic Computation of High-Order Derivatives*, Paper AAS 10-218, AAS/AIAA Space Flight Mechanics Meeting, San Diego, Californie, 2010.

IV.3 Hypercomplexes

IV.3.1 Introduction

La définition des nombres hypercomplexes n'est pas stable, pour certains, cette appellation ne désigne que les quaternions, pour d'autres elle désigne tous les ensembles construits par la méthode de **Cayley-Dickson** à partir de \mathbb{C} , ou seulement \mathbb{C} , \mathbb{H} et \mathbb{O} (voire d'autres combinaisons), pour d'autres la définition est très générale : un espace vectoriel de dimension finie sur \mathbb{R} sur lequel une multiplication distributive sur l'addition est définie (donc une \mathbb{R} -algèbre de dimension finie) ; on pourrait d'ailleurs généraliser encore : module sur n'importe quel anneau de dimension finie ou non, sur lequel une multiplication est définie.

IV.3.2 Définition

Dans ce document nous prendrons comme définition celle de I.L. Kantor (à ne pas confondre avec G. Cantor) et A.S. Solodovnikov : Un ensemble de nombres hypercomplexes est un espace vectoriel de dimension finie sur \mathbb{R} , muni d'une opération supplémentaire, la multiplication, qui soit unitaire et distributive (c'est à dire une \mathbb{R} -algèbre unitaire de dimension finie) avec la propriété suivante :

soit $(1, e_1, e_2, \dots, e_n)$ une base (c'est à dire que les nombres hypercomplexes peuvent s'écrire : $z = a_0 + a_1 \cdot e_1 + \dots + a_n \cdot e_n$, où les a_i sont des nombres réels) alors pour tout i , $e_i^2 \in \{-1, 0, 1\}$.

On peut catégoriser les algèbres hypercomplexes en fonctions des carrés de la base :

- Elliptique : pour tout i $e_i^2 = -1$
- Parabolique : pour tout i $e_i^2 = 0$
- Hyperbolique : pour tout i $e_i^2 = 1$
- Mixte : les autres cas.

Mais cette nomenclature n'est pas stable, pour certains auteurs une algèbre hypercomplexe est Elliptique si elle possède au moins un élément de base de carré égale à -1, et parabolique si elle possède au moins un élément de base de carré égale à 0 (mixte si elle possède au moins un de ces deux derniers cas).

IV.3.3 Mode de construction

Il est immédiat qu'une \mathbb{R} -algèbre avec un axe réel et un seul axe non-réel est complètement déterminé par la valeur de $e_1^2 = a + b \cdot e_1$, or il est aisé de démontrer qu'en fonction du signe de $b^2 + 4a$ une telle algèbre est isomorphe à un ensemble hypercomplexe avec un seul axe non réel où soit $e_1^2 = -1$ soit $e_1^2 = 0$ soit $e_1^2 = 1$.

Il y a donc 3 exemples pour les hypercomplexes avec un seul axe non réel ($n = 1$) : Les **complexes** ($e_1^2 = -1$, généralement noté i), les **nombres duaux** ($e_1^2 = 0$, généralement noté ε), les **complexes fendus** ($e_1^2 = 1$ généralement noté j) (cf. **Introduction sur les algèbres de dimension 2 sur \mathbb{R}**).

IV.3.4 Table de multiplication

Les contraintes dans la définition des hypercomplexes étant assez faibles au delà de $n = 1$, il n'est pas raisonnable de donner une liste des cas possibles, certains exemples de tables de multiplications sont disponibles dans les chapitres concernant les cas particuliers d'algèbre hypercomplexe.

A titre d'exemple "peu intéressant", dans le cas $n = 2$:

\times	1	e_1	e_2
1	1	e_1	e_2
e_1	e_1	1	0
e_2	e_2	0	1

On peut vérifier facilement que cette algèbre est commutative, mais non associative, qu'elle possède des diviseurs de 0, des éléments idempotents non triviaux (par exemple $(\frac{1+e_1}{2})$), et des éléments nilpotents.

Deux algèbres hypercomplexes sont isomorphes si elles sont de même dimension, et si leur table de multiplication sont identiques en interchangeant les bases ou par combinaisons linéaires de leur base.

IV.3.5 Conjugué, Module, Norme, Forme Polaire et Inverse

On peut définir un conjugué hypercomplexe, si $z = a_0 + a_1 \cdot e_1 + \dots + a_n \cdot e_n$, alors le conjugué de z est $\bar{z} = a_0 - a_1 \cdot e_1 + \dots - a_n \cdot e_n$, mais dans le cas général, cette notion n'est pas très intéressante et ne donne pas systématiquement naissance à une notion de norme.

IV.3.6 Propriétés algébriques

Les ensembles hypercomplexes sont des algèbres unitaires de dimension finie sur \mathbb{R} , certaines de ces structures sont commutatives et/ou associatives, d'autres non.

La définition des hypercomplexes étant très générale, ils ne possèdent pas de propriétés communes à part celles contenues dans la définition, pour plus de détails, cf. les différents exemples d'hypercomplexes de ce document.

Le théorème de Hurwitz précise : toute \mathbb{R} -algèbre normée, unitaire à division est soit \mathbb{R} , soit \mathbb{C} , soit \mathbb{H} , soit \mathbb{O} , donc de dimension 1, 2, 4 ou 8.

On peut noter néanmoins que seuls \mathbb{C} et \mathbb{H} sont des corps (et seul \mathbb{C} est un corps commutatif).

Une conséquence triviale, mais pas forcément intuitive du théorème de Hurwitz est qu'un espace Euclidien ne peut être muni d'un produit vectoriel que s'il est de dimension 0, 1, 3 ou 7 (Les cas 0 et 1 ne sont guère intéressants).

Démonstration : Soit V un espace euclidien muni d'un produit vectoriel (noté \wedge), alors $(\mathbb{R} \oplus V)$ peut être muni d'une multiplication définie par :

$$(a, \vec{u}) \cdot (b, \vec{v}) = (ab - \vec{u}\vec{v}, a\vec{v} + b\vec{u} + \vec{u} \wedge \vec{v})$$

Il est immédiat de vérifier que cela munit $(\mathbb{R} \oplus V)$ d'une structure de \mathbb{R} -algèbre unitaire.

En posant $|(a, \vec{u})| = \sqrt{a^2 + \vec{u}^2}$, on peut vérifier que $|(a, \vec{u})|$ est bien une norme d'algèbre (vérifiant en plus des axiomes d'une norme que $|x \cdot y| = |x| \cdot |y|$).

Et comme $(a, \vec{u}) \cdot \left(\frac{a}{|(a, \vec{u})|^2}, \frac{-\vec{u}}{|(a, \vec{u})|^2} \right) = (1, 0)$, on en déduit que $(\mathbb{R} \oplus V)$ est une \mathbb{R} -algèbre normée, unitaire à division, donc de dimension 1, 2, 4 ou 8 (CQFD).

IV.3.7 Synonymes, Isomorphismes, Exemples

De nombreux ensembles sont en fait des hypercomplexes (à commencer par les complexes et ses variations) :

- Les **algèbres de Clifford** sont des cas particuliers d'hypercomplexes.
- La construction de **Cayley-Dickson** donne des hypercomplexes.

Le produit tensoriel d'algèbres hypercomplexes donne une algèbre hypercomplexe, par exemple :

- $\mathbb{C} \otimes \mathbb{C}$ donne les **nombres BiComplexes** de dimension 4.
- $\mathbb{C} \otimes \mathbb{H}$ donne les **BiQuaternions** de dimension 8.
- $\mathbb{C} \otimes \mathbb{O}$ donne les **Octonions Complexes** de dimension 16.

Synonyme = Hyper-nombres (à ne pas confondre avec les hypernombres de Musès).

IV.3.8 Utilisation en physique

Voir chacun des ensembles hypercomplexes particuliers.

Il existe de très nombreux sites sur le sujet accessible sur le net.

Par exemple : [Hyper-Complex Numbers in Geometry and-Physics](#)

IV.3.9 Références

1. [Site russe dédié aux hypercomplexes \(en anglais\)](#)
2. [Un historique remontant à 665 \(en anglais\)](#)
3. Hypercomplex Numbers : An Elementary Introduction to Algebras par I.L. Kantor, A.S. Solodovnikov Springer-Verlag ISBN : 0387969802 1989

IV.4 Cayley-Dickson $\mathcal{CD}(\mathbb{A}, \lambda)$

IV.4.1 Introduction

La méthode de Cayley-Dickson a été mise au point par Arthur Cayley (1821 - 1895) et Leonard Eugene Dickson (1874 - 1954) afin de généraliser les travaux de Hamilton, Cockle etc. sur les quaternions et autres extensions des nombre complexes.

IV.4.2 Définition

La méthode de Cayley-Dickson permet de fabriquer une **algèbre** de dimension $2n$ sur son anneau (ou corps) de base, à partir d'une algèbre de dimension n sur cet anneau (ou corps).

IV.4.3 Mode de construction

Nous allons décrire ici la méthode de Cayley-Dickson *Généralisée*.

Soit A une algèbre de dimension n sur K , un anneau ou un corps ; rappelons qu'un anneau (ou un corps) est une algèbre de dimension 1 sur lui-même.

Pour des raisons de lisibilité, la multiplication (interne) entre couples sera toujours notée \times , la multiplication interne entre éléments sera notée \cdot , ou sera omise suivant le contexte, et la multiplication externe sera notée \cdot ou sera omise suivant le contexte.

Une algèbre A peut être munie d'une involution, appelé conjugaison, compatible avec les opérations interne (lorsque $A = K$, cette involution est tout simplement l'identité).

Cette involution sera noté avec une barre au-dessus de l'élément à conjuguer, comme il est d'usage dans \mathbb{C} , (par exemple si $x \in A$, le conjugué de x est noté \bar{x} ; dans certains textes il est noté x^* , d'ailleurs, en anglais, une algèbre munie d'une involution est appelé une **-Algebra*).

La conjugaison est une involution, c'est à dire que $\overline{\bar{x}} = x$

La conjugaison est compatible avec les opérations, c'est à dire que $\overline{x + y} = \bar{x} + \bar{y}$ et $\overline{xy} = \bar{y}\bar{x}$.

Soit $B = A \oplus A$, B est donc un espace vectoriel de dimension $2n$ sur K , l'addition et la multiplication par un scalaire sont parfaitement définies par cette somme directe, mais nous devons préciser la multiplication et l'involution.

La multiplication sur B est définie par : $(x, x') \times (y, y') = (xy - \lambda \bar{y}'x', y'x + x'\bar{y})$, où $\lambda \in K^*$.

L'involution sur B est définie par : $\overline{(x, x')} = (\bar{x}, -x')$

L'application $\pi : \mathbb{A} \mapsto (\mathbb{A} \times \mathbb{A})$ définie par $\pi(x) = (x, 0)$, permet de plonger canoniquement $(\mathbb{A}, +, \times, \cdot, \bar{\cdot})$ dans $(\mathbb{A} \times \mathbb{A}, +, \times, \cdot, \bar{\cdot})$ (ou $(\mathbb{A} \oplus \mathbb{A}, +, \times, \bar{\cdot})$). Par la suite nous identifierons $(x, 0)$, élément de B avec x (considéré comme élément de B , ou de A suivant le contexte), en particulier pour l'unité.

D'une façon générale, l'algèbre construite par la méthode Cayley-Dickson à partir de l'algèbre \mathbb{A} et de paramètre λ sera notée $\mathcal{CD}(\mathbb{A}, \lambda)$.

La version standard de la méthode de Cayley-Dickson est obtenu en posant $\lambda = 1$, c'est à dire que le produit est défini par $(x, x') \times (y, y') = (xy - \bar{y}'x', y'x + x'\bar{y})$.

Les algèbres construites en itérant la méthode de Cayley-Dickson à partir de \mathbb{R} sont des **hypercomplexes**.

IV.4.4 Conjugué, Module, Norme et Inverse

Une \mathbb{R} -algèbre munie d'une involution est dite « régulièrement normée »⁶⁵ si les conditions suivantes sont vérifiées :

- $x + \bar{x} \in \mathbb{R}$
- $x\bar{x} = \bar{x}x \in \mathbb{R}^+$
- $x\bar{x} = 0 \Leftrightarrow x = 0$

65. Traduction non officielle de "nicely normed"

Dans la suite de ce sous-chapitre nous ne considérerons que des \mathbb{R} -algèbres régulièrement normées munies d'une involution.

Sur ces algèbres, on définit la norme par $|x| = \sqrt{x\bar{x}}$ (ce qui est valide puisque $|x| \in \mathbb{R}^+$) et la trace par $\text{tr}(x) = x + \bar{x}$.

Il est immédiat que $|x| \neq 0 \Rightarrow x^{-1} = \frac{\bar{x}}{|x|^2}$.

Les résultats précédents permettent de donner les définitions suivantes :

1. Partie réelle de x , notée $\Re(x) = \frac{x + \bar{x}}{2}$
2. Partie imaginaire de x , notée $\Im(x) = \frac{x - \bar{x}}{2}$

Ce qui donne une nouvelle façon d'écrire un élément de ce type d'algèbre : $x = \Re(x) + \Im(x)$ (attention la définition de la partie imaginaire est légèrement différente de la définition habituelle sur \mathbb{C}).

On peut aussi remarquer que $\forall x (x^2 - \text{tr}(x)x + |x|^2 = 0)$, c'est à dire que ces algèbres sont quadratiques (une algèbre est quadratique si elle est unitaire et si, pour tout x les éléments $1, x, x^2$ sont linéairement dépendants).

IV.4.5 Propriétés algébriques

Dans la suite de ce chapitre nous ne considérerons que des \mathbb{R} -algèbres munies d'une involution.

On peut vérifier que l'involution sur $A \oplus A$ possède bien les trois propriétés définissant une involution compatible avec les opérations, nous vérifierons aussi que quelques propriétés qui se transmettent de A à $A \oplus A$:

1. Définition d'une involution :

$$\overline{(x, x')} = (\bar{x}, -x') = (\bar{x}, -(-x')) = (x, x')$$

2. Propriété de l'addition :

$$\overline{(x, x') + (y, y')} = \overline{(x + y, x' + y')} = (\overline{x + y}, -(x' + y')) = (\bar{x} + \bar{y}, -x' - y')$$

$$\overline{(x, x')} + \overline{(y, y')} = (\bar{x}, -x') + (\bar{y}, -y') = (\bar{x} + \bar{y}, -x' + (-y'))$$

$$\text{Et donc, finalement, } \overline{(x, x') + (y, y')} = \overline{(x, x')} + \overline{(y, y')}$$

3. Propriété de la multiplication

$$\overline{(x, x') \times (y, y')} = \overline{(xy - \lambda y'x', y'x + x'y')} = \overline{(xy - \lambda y'x', -(y'x + x'y))} = (\bar{y}\bar{x} - \lambda \overline{y'x'}, -y'x - x'y)$$

$$\overline{(y, y')} \times \overline{(x, x')} = (\bar{y}, -y') \times (\bar{x}, -x') = (\bar{y}\bar{x} - \lambda(-y')(-x'), (-x')\bar{y} + (-y')\bar{x}) = (\bar{y}\bar{x} - \lambda \overline{y'x'}, -x'\bar{y} - y'x)$$

$$\text{Et donc, finalement, } \overline{(x, x') \times (y, y')} = \overline{(y, y')} \times \overline{(x, x')}$$

4. $A \oplus A$ est unitaire

Soit 0_A l'élément neutre de l'addition dans A et 1_A l'élément neutre de la multiplication dans A .

$$(1_A, 0_A) \times (x, x') = (1_A \times x - \lambda \cdot \bar{x}' \times 0_A, x' \times 1_A + 0_A \times \bar{x}) = (x, x')$$

$$(x, x') \times (1_A, 0_A) = (x \times 1_A - \lambda \cdot \overline{0_A} \times x', 0_A \times x + x' \times \overline{1_A}) = (x, x')$$

Et donc, $1_{A \oplus A} = (1_A, 0)$ et, finalement, on obtient $1_{A \oplus A} = 1_K$ (avec les légers abus de notation habituels).

5. Si $\lambda > 0$, $A \oplus A$ est régulièrement normée.

$$\text{tr}((x, x')) = (x, x') + \overline{(x, x')} = (x, x') + (\bar{x}, -x') = (x + \bar{x}, 0) = (\text{tr}(x), 0) = \text{tr}(x)$$

En itérant le calcul précédent, on arrive à : $\text{tr}((x, x')) \in \mathbb{R}$.

$$(x, x') \cdot \overline{(x, x')} = (x, x') \cdot (\bar{x}, -x') = (x\bar{x} + \lambda \overline{x'x'}, -x'x + x'\bar{x}) = (x\bar{x} + \lambda \overline{x'x'}, 0)$$

En itérant le calcul précédent, on arrive à : $(x, x') \cdot \overline{(x, x')} \in \mathbb{R}^+$. Une démonstration similaire permet de démontrer $\overline{(x, x')} \cdot (x, x') \in \mathbb{R}^+$

$$(x, x') \cdot \overline{(x, x')} = 0 \Leftrightarrow x\bar{x} + \lambda \overline{x'x'} = 0$$

En itérant le calcul précédent, on arrive à : $(x, x') \cdot \overline{(x, x')} = 0 \Leftrightarrow x = x' = 0$.

6. $A \oplus A$ est flexible (donc est puissance-associative)

La démonstration nécessite plusieurs lemmes dont les démonstrations sont un peu fastidieuses.

Dans le cas particulier où on part du corps $(\mathbb{R}, +, \times)$, et où $\lambda = 1$, on obtient successivement les **complexes**, les **quaternions**, les **octonions**, les **sédénions**, les **trigintaduonions**, les **sexagintaquatrons**, etc. jusqu'à \mathbb{A} qui est l'algèbre union de la suite des algèbres de Cayley construites à partir de \mathbb{R} :

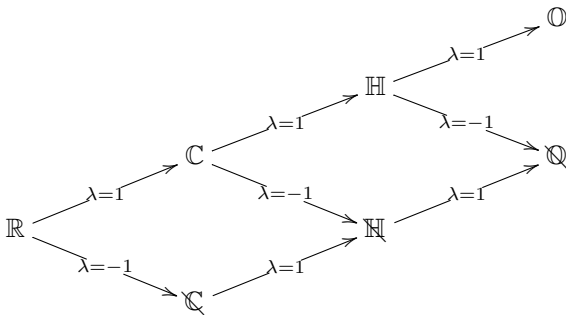
$$\mathbb{R} \xrightarrow{\lambda=1} \mathbb{C} \xrightarrow{\lambda=1} \mathbb{H} \xrightarrow{\lambda=1} \mathbb{O} \xrightarrow{\lambda=1} \mathbb{S} \xrightarrow{\lambda=1} \mathbb{T} \xrightarrow{\lambda=1} \mathbb{X} \xrightarrow{\lambda=1} \dots \mathbb{A}$$

On remarquera que les quatre premières algèbres de cette suite sont les quatre seules \mathbb{R} -algèbres normées sans diviseurs de 0, dont les trois premières sont les seuls corps (théorème de Hurwitz).

Propriété	\mathbb{R}	\mathbb{C}	\mathbb{H}	\mathbb{O}
Flexibilité	Oui	Oui	Oui	Oui
Régulièrement Normée	Oui	Oui	Oui	Oui
Associativité	Oui	Oui	Oui	Non
Commutativité	Oui	Oui	Non	Non
$\bar{x} = x$	Oui	Non	Non	Non

IV.4.6 Synonymes, Isomorphismes, Exemples

Quelques exemples obtenus par l'application de la méthode avec $\lambda = 1$ ou $\lambda = -1$ (les symboles barrés correspondent aux versions fendues de ces algèbres) :



Il existe plusieurs variantes dans la définition même de la méthode, par exemple en définissant le produit par :

$$(x, y) \times (x', y') = (xx' - \lambda \bar{y}'y, y'x + y\bar{x}'), \text{ où } \lambda \text{ peut être :}$$

- Un élément de K (à la place de K^*).
- Un élément inversible de A .
- Un élément quelconque de A .

Mais on peut fabriquer d'autres variantes, comme :

$$(x, y) \times (x', y') = (xx' - y'\lambda\bar{y}, y'x + y\bar{x}')$$

$$(x, y) \times (x', y') = (xx' - y'\bar{y}\lambda, y'x + y\bar{x}')$$

IV.4.7 Utilisation en physique

La méthode de Cayley-Dickson n'est pas utilisée per se en physique, mais de nombreuses algèbres, parmi celles construites à partir de cette méthode, sont utilisées dans diverses branches de la physique.

En particulier les M-théoristes :

1. [Superalgebras of \(split-\)division algebras and the split octonionic M-theory in \(6, 5\)-signature](#) par Zhanna Kuznetsova et Francesco Toppan.
2. [Usage des sédénions](#)

IV.4.8 Références

1. [On Quaternions and Their Generalization and the History of the Eight Square Theorem](#) par Dickson, L. E. , Annals of Mathematics 1919.
2. [The zero divisors of the Cayley-Dickson algebras over the real numbers](#) par Guillermo Moreno.
3. [Division algebras over the real numbers](#) par Matthew Badger.
4. [Some equations in algebras obtained by the Cayley-Dickson process](#) par Cristina Flaut.
5. L.E. Dickson (1914) : Linear Algebras, Cambridge Univ. Tracts no 16.

IV.5 Algèbres de Clifford $\mathcal{C}\ell_{p,q}(\mathbb{R})$ et $\mathcal{C}\ell_n(\mathbb{C})$

IV.5.1 Introduction

William Kingdon Clifford (1845 - 1879), était un mathématicien britannique qui a introduit une famille d'algèbres contenant à la fois les **nombres complexes** et les **quaternions**, tout en les généralisant.

Il avait baptisé cette famille *Algèbres Géométriques* (à cause de leur lien avec la géométrie), mais elles sont connues aujourd'hui sous le nom d'*Algèbres de Clifford*, en son honneur.

IV.5.2 Définition

Définition : Soit \mathbb{K} un corps, \mathcal{V} un \mathbb{K} -Espace vectoriel de dimension finie, et \mathcal{Q} une forme quadratique non dégénérée sur \mathcal{V} .

Alors l'algèbre de Clifford $\mathcal{C}\ell(\mathcal{V}, \mathcal{Q})$ est l'algèbre unitaire et associative vérifiant :

1. $\mathcal{C}\ell(\mathcal{V}, \mathcal{Q})$ contient \mathbb{K} et \mathcal{V} comme sous-espaces distincts.
2. $\forall x \in \mathcal{V} (x^2 = \mathcal{Q}(x))$.
3. \mathcal{V} engendre $\mathcal{C}\ell(\mathcal{V}, \mathcal{Q})$ comme \mathbb{K} -algèbre.
4. Un sous-espace propre de \mathcal{V} ne peut pas engendrer $\mathcal{C}\ell(\mathcal{V}, \mathcal{Q})$.

Il existe d'autres formulations de cette définition, en utilisant une propriété universelle par exemple, mais elles sont, bien sur, équivalentes.

Définition : Soit \mathbb{K} un corps, \mathcal{V} un \mathbb{K} -Espace vectoriel de dimension finie, et \mathcal{Q} une forme quadratique non dégénérée sur \mathcal{V} .

Alors l'algèbre de Clifford $\mathcal{C}\ell(\mathcal{V}, \mathcal{Q})$ est la \mathbb{K} -algèbre unitaire et associative vérifiant :

1. Il existe une application linéaire $i_{\mathcal{Q}} : \mathcal{V} \mapsto \mathcal{C}\ell(\mathcal{V}, \mathcal{Q})$, vérifiant $\forall v \in \mathcal{V} ((i_{\mathcal{Q}}(v))^2 = \mathcal{Q}(v))$
2. Pour toute \mathbb{K} -algèbre \mathcal{A} , et pour toute application linéaire $f : \mathcal{V} \mapsto \mathcal{A}$, il existe un unique homomorphisme d'algèbre $\hat{f} : \mathcal{C}\ell(\mathcal{V}, \mathcal{Q}) \mapsto \mathcal{A}$, tel que le diagramme suivant commute :

$$\begin{array}{ccc}
 \mathcal{V} & \xrightarrow{i_{\mathcal{Q}}} & \mathcal{C}\ell(\mathcal{V}, \mathcal{Q}) \\
 & \searrow f & \downarrow \hat{f} \\
 & & \mathcal{A}
 \end{array}$$

IV.5.3 Mode de construction de $\mathcal{C}\ell_{p,q}(\mathbb{R})$

Dans le cas particulier des algèbres de Clifford sur \mathbb{R} , il faut avant tout noter qu'une forme quadratique non dégénérée sur un \mathbb{R} -Espace vectoriel de dimension n est toujours équivalente à une forme quadratique \mathcal{Q} de la forme⁶⁶ : $\mathcal{Q}(X) = \sum_{i=1}^p X_i^2 - \sum_{i=1}^q X_{p+i}^2$. Le couple (p, q) est appelé la signature de \mathcal{Q} .

Une Algèbre de Clifford sur \mathbb{R} peut donc se noter $\mathcal{C}\ell(\mathbb{R}^n, \mathcal{Q}) = \mathcal{C}\ell_{p,q}(\mathbb{R})$ (avec $n = p + q$).

Les Algèbres de Clifford sur \mathbb{R} sont donc des cas particuliers des **nombres hypercomplexes** définies de la façon suivante à partir d'une base de $\mathcal{V}(e_1, e_2, \dots, e_p, e_{p+1}, e_{p+2}, \dots, e_{p+q})$:

$$\bullet \bigwedge_{i=1}^p e_i^2 = 1 \quad \bullet \bigwedge_{i=1}^q e_{p+i}^2 = -1 \quad \bullet \bigwedge_{\substack{i \neq j \\ 0 < i \leq n \\ 0 < j \leq n}} e_i \cdot e_j = -e_j \cdot e_i$$

(toujours avec $n = p + q$)

La base de l'algèbre $\mathcal{C}\ell_{p,q}(\mathbb{R})$, est donc : $(1, e_1, \dots, e_n, e_1 \cdot e_2, e_1 \cdot e_3, \dots, e_{n-1} \cdot e_n, \dots, e_1 \cdot e_2 \cdots e_n)$

C'est à dire (en posant $e_0 = 1$), tous les éléments de la forme $\prod_{i \in I} e_i$, pour tous les $I \subset [1, n]$ (avec la convention que $\prod_{i \in \emptyset} e_i = e_0$), soit 2^{p+q} éléments.

66. Voir la [Méthode de Gauss](#) en page 7

Ensembles de Nombres

On peut remarquer qu'en notant $\mathbb{R}_{p,q}$ l'espace sous-jacent à l'algèbre $\mathcal{C}\ell_{p,q}(\mathbb{R})$ et $\mathbb{R}_{p,q}^k$, l'espace vectoriel engendré par les produits (dans $\mathcal{C}\ell_{p,q}(\mathbb{R})$) de k éléments différents de la base de \mathbb{R}^{p+q} , on obtient une décomposition naturelle en somme directe (d'espaces vectoriels) :

$$\mathbb{R}_{p,q} = \mathbb{R}_{p,q}^0 \oplus \mathbb{R}_{p,q}^1 \oplus \mathbb{R}_{p,q}^2 \oplus \dots \oplus \mathbb{R}_{p,q}^n$$

Les éléments de $\mathbb{R}_{p,q}^0 = \mathbb{R}$ sont appelés des scalaires, les éléments de $\mathbb{R}_{p,q}^1 = \mathbb{R}^n$ sont appelés des vecteurs, les éléments de $\mathbb{R}_{p,q}^2$ sont appelés des bivecteurs, les éléments de $\mathbb{R}_{p,q}^3$ sont appelés des trivecteurs, les éléments de $\mathbb{R}_{p,q}^k$ sont appelés des k -vecteurs, les éléments de $\mathbb{R}_{p,q}^n$ sont parfois appelés des pseudos-scalaires (c'est aussi un espace de dimension 1).

IV.5.4 Table de multiplication de $\mathcal{C}\ell_{p,q}(\mathbb{R})$

En dimension 1 sur \mathbb{R} (c'est à dire $p + q = 0$), il n'y a qu'un seul cas possible : $\mathcal{C}\ell_{0,0}(\mathbb{R}) = \mathbb{R}$.

En dimension 2 sur \mathbb{R} (c'est à dire $p + q = 1$), il n'y a que deux cas possibles, Comme $p + q = 1$, une base de \mathbb{R} contient un vecteur (e_1), et une base de $\mathcal{C}\ell_{p,q}(\mathbb{R})$ en contient 2 : $(1, e_1)$.

·	1	e_1
1	1	e_1
e_1	e_1	-1

$$\mathcal{C}\ell_{0,1}(\mathbb{R}) \cong \mathbb{C}$$

·	1	e_1
1	1	e_1
e_1	e_1	1

$$\mathcal{C}\ell_{1,0}(\mathbb{R}) \cong \mathbb{C} \cong \mathbb{R} \oplus \mathbb{R}$$

En dimension 4 sur \mathbb{R} (c'est à dire $p + q = 2$), il n'y a que trois cas possibles (dont deux sont isomorphes), Comme $p + q = 2$, une base de \mathbb{R}^2 contient deux vecteurs (e_1 et e_2), et une base de $\mathcal{C}\ell_{p,q}(\mathbb{R})$ en contient quatre : $(1, e_1, e_2, e_1 \cdot e_2)$, pour simplifier la lecture, nous noterons $e_{12} = e_1 \cdot e_2$, donc nous avons la relation $e_{12} = -e_{21}$.

·	1	e_1	e_2	e_{12}
1	1	e_1	e_2	e_{12}
e_1	e_1	-1	e_{12}	$-e_2$
e_2	e_2	e_{21}	-1	e_1
e_{12}	e_{12}	e_2	$-e_1$	-1

$$\mathcal{C}\ell_{0,2}(\mathbb{R}) \cong \mathbb{H}$$

·	1	e_1	e_2	e_{12}
1	1	e_1	e_2	e_{12}
e_1	e_1	-1	e_{12}	$-e_2$
e_2	e_2	e_{21}	1	$-e_1$
e_{12}	e_{12}	e_2	e_1	1

$$\mathcal{C}\ell_{1,1}(\mathbb{R}) \cong \mathbb{H} \cong M_2(\mathbb{R})$$

·	1	e_1	e_2	e_{12}
1	1	e_1	e_2	e_{12}
e_1	e_1	1	e_{12}	e_2
e_2	e_2	e_{21}	1	$-e_1$
e_{12}	e_{12}	$-e_2$	e_1	-1

$$\mathcal{C}\ell_{2,0}(\mathbb{R}) \cong \mathbb{H} \cong M_2(\mathbb{R})$$

L'isomorphisme entre $\mathcal{C}\ell_{1,1}(\mathbb{R})$ et $\mathcal{C}\ell_{2,0}(\mathbb{R})$ est défini par :

$$\varphi : \mathcal{C}\ell_{1,1}(\mathbb{R}) \mapsto \mathcal{C}\ell_{2,0}(\mathbb{R}) \begin{cases} \varphi(1) = 1 \\ \varphi(e_1) = e_{12} \\ \varphi(e_2) = e_2 \end{cases}$$

Trois théorèmes d'isomorphismes vont permettre de classifier complètement les Algèbres de Clifford réelles :

1. $\mathcal{Cl}_{0,n+2}(\mathbb{R}) \cong \mathcal{Cl}_{n,0}(\mathbb{R}) \otimes \mathcal{Cl}_{0,2}(\mathbb{R}) \cong \mathcal{Cl}_{n,0}(\mathbb{R}) \otimes M_2(\mathbb{R})$
2. $\mathcal{Cl}_{n+2,0}(\mathbb{R}) \cong \mathcal{Cl}_{0,n}(\mathbb{R}) \otimes \mathcal{Cl}_{2,0}(\mathbb{R}) \cong \mathcal{Cl}_{0,n}(\mathbb{R}) \otimes \mathbb{H}$
3. $\mathcal{Cl}_{p+1,q+1}(\mathbb{R}) \cong \mathcal{Cl}_{p,q}(\mathbb{R}) \otimes \mathcal{Cl}_{1,1}(\mathbb{R}) \cong \mathcal{Cl}_{p,q}(\mathbb{R}) \otimes M_2(\mathbb{R})$

En itérant la règle 3 on obtient : $\begin{cases} p \leq q \Rightarrow \mathcal{Cl}_{p,q}(\mathbb{R}) \cong \mathcal{Cl}_{p-q,0}(\mathbb{R}) \otimes M_{2^q}(\mathbb{R}) \\ q \leq p \Rightarrow \mathcal{Cl}_{p,q}(\mathbb{R}) \cong \mathcal{Cl}_{0,q-p}(\mathbb{R}) \otimes M_{2^p}(\mathbb{R}) \end{cases}$.

En itérant les règles 1 et 2 on obtient :

$$\begin{aligned} \mathcal{Cl}_{0,n+8}(\mathbb{R}) &\cong \mathcal{Cl}_{n+6,0}(\mathbb{R}) \otimes M_2(\mathbb{R}) \\ \mathcal{Cl}_{n+6,0}(\mathbb{R}) \otimes M_2(\mathbb{R}) &\cong \mathcal{Cl}_{0,n+4}(\mathbb{R}) \otimes \mathbb{H} \otimes M_2(\mathbb{R}) \\ \mathcal{Cl}_{0,n+4}(\mathbb{R}) \otimes \mathbb{H} \otimes M_2(\mathbb{R}) &\cong \mathcal{Cl}_{n+2,0}(\mathbb{R}) \otimes \mathbb{H} \otimes M_4(\mathbb{R}) \\ \mathcal{Cl}_{n+2,0}(\mathbb{R}) \otimes \mathbb{H} \otimes M_4(\mathbb{R}) &\cong \mathcal{Cl}_{0,n}(\mathbb{R}) \otimes \mathbb{H} \otimes \mathbb{H} \otimes M_4(\mathbb{R}) \end{aligned}$$

Sachant que $\mathbb{H} \otimes \mathbb{H} \cong M_4(\mathbb{R})$, on obtient finalement

$$\mathcal{Cl}_{0,n+8}(\mathbb{R}) \cong \mathcal{Cl}_{0,n}(\mathbb{R}) \otimes M_{16}(\mathbb{R})$$

De la même façon on démontrerait que

$$\mathcal{Cl}_{n+8,0}(\mathbb{R}) \cong \mathcal{Cl}_{n,0}(\mathbb{R}) \otimes M_{16}(\mathbb{R})$$

Il suffit donc de connaître les Algèbres de Clifford $\mathcal{Cl}_{0,n}(\mathbb{R})$ ⁶⁷ et $\mathcal{Cl}_{n,0}(\mathbb{R})$ ⁶⁸ pour $n < 8$, pour avoir une décomposition de toutes les Algèbres de Clifford, or ces dernières s'obtiennent facilement à l'aides des règles 1 et 2 ci-dessus, et des cas déjà cités.

A titre d'exemple voici une courte liste des premières algèbres de Clifford réelles établies en utilisant les résultats précédents ainsi que quelques isomorphismes « bien connus » :

$$\begin{aligned} M_n(\mathbb{R}) \otimes M_m(\mathbb{R}) &\cong M_{nm}(\mathbb{R}) \\ M_n(\mathbb{R}) \otimes \mathbb{C} &\cong M_n(\mathbb{C}) \\ M_n(\mathbb{R}) \otimes \mathbb{H} &\cong M_n(\mathbb{H}) \\ \mathbb{C} \otimes \mathbb{C} &\cong \mathbb{C} \oplus \mathbb{C} \\ \mathbb{C} \otimes \mathbb{H} &\cong M_2(\mathbb{C}) \\ \mathbb{H} \otimes \mathbb{H} &\cong M_4(\mathbb{R}) \end{aligned}$$

Nous utiliserons la notations suivante (pour gagner de la place) : $\mathcal{K} \oplus \mathcal{K} = \overset{2}{\oplus} \mathcal{K}$

p \ q	0	1	2	3	4	5
0	\mathbb{R}	$\overset{2}{\oplus} \mathbb{R}$	$M_2(\mathbb{R})$	$M_2(\mathbb{C})$	$M_2(\mathbb{H})$	$\overset{2}{\oplus} M_2(\mathbb{H})$
1	\mathbb{C}	$M_2(\mathbb{R})$	$\overset{2}{\oplus} M_2(\mathbb{R})$	$M_4(\mathbb{R})$	$M_4(\mathbb{C})$	$M_4(\mathbb{H})$
2	\mathbb{H}	$M_2(\mathbb{C})$	$M_4(\mathbb{R})$	$\overset{2}{\oplus} M_2(\mathbb{H})$	$M_8(\mathbb{R})$	$M_8(\mathbb{C})$
3	$\overset{2}{\oplus} \mathbb{H}$	$M_2(\mathbb{H})$	$M_4(\mathbb{C})$	$M_8(\mathbb{R})$	$\overset{2}{\oplus} M_8(\mathbb{R})$	$M_{16}(\mathbb{R})$
4	$M_2(\mathbb{H})$	$\overset{2}{\oplus} M_2(\mathbb{H})$	$M_4(\mathbb{H})$	$M_8(\mathbb{C})$	$M_{16}(\mathbb{R})$	$\overset{2}{\oplus} M_{16}(\mathbb{R})$
5	$M_4(\mathbb{C})$	$M_4(\mathbb{H})$	$\overset{2}{\oplus} M_4(\mathbb{H})$	$M_8(\mathbb{H})$	$M_{16}(\mathbb{C})$	$M_{32}(\mathbb{R})$

$\mathcal{Cl}_{p,q}(\mathbb{R})$ où $0 \leq p \leq 4$ et $0 \leq q \leq 4$

67. Ces algèbres sont dites *Anti-Euclidiennes*.

68. Ces algèbres sont dites *Euclidiennes*.

IV.5.5 Mode de construction de $\mathcal{Cl}_n(\mathbb{C})$

Le cas complexe est plus simple (j'ai toujours rêvé d'écrire cette phrase) pour plusieurs raisons :

1. Une forme quadratique non dégénérée sur un \mathbb{C} -Espace vectoriel de dimension n est toujours équivalente à une forme quadratique \mathcal{Q} de la forme : $\mathcal{Q}(X) = \sum_{i=1}^n X_i^2$. Ce qui explique la notation, pour les algèbres de Clifford sur \mathbb{C} : $\mathcal{Cl}_n(\mathbb{C}) = \mathcal{Cl}(\mathbb{C}^n, \mathcal{Q})$
2. Il existe un isomorphisme permettant de montrer que $\mathbb{C} \otimes \mathcal{Cl}_{p,q}(\mathbb{R}) \cong \mathcal{Cl}_{p+q}(\mathbb{C})$, les algèbres de Clifford complexes s'obtiennent donc par la complexification d'algèbres réelles.

$$3. \text{ En particulier : } \begin{cases} \mathcal{Cl}_{n+2}(\mathbb{C}) & \cong & \mathbb{C} \otimes \mathcal{Cl}_{n+2,0}(\mathbb{R}) \\ & \cong & \mathbb{C} \otimes (\mathcal{Cl}_{2,0}(\mathbb{R}) \otimes \mathcal{Cl}_{0,n}(\mathbb{R})) \\ & \cong & (\mathbb{C} \otimes \mathcal{Cl}_{2,0}(\mathbb{R})) \otimes (\mathbb{C} \otimes \mathcal{Cl}_{0,n}(\mathbb{R})) \\ & \cong & \mathcal{Cl}_n(\mathbb{C}) \otimes (\mathbb{C} \otimes \mathbb{H}) \\ \mathcal{Cl}_{n+2}(\mathbb{C}) & \cong & \mathcal{Cl}_n(\mathbb{C}) \otimes M_2(\mathbb{C}) \end{cases}$$

4. En itérant le résultat précédent (et en remarquant que $\mathbb{C} \otimes (\mathbb{R} \oplus \mathbb{R}) \cong \mathbb{C} \oplus \mathbb{C}$), on obtient

$$\mathcal{Cl}_n(\mathbb{C}) \cong \begin{cases} n = 2k & M_{2^k}(\mathbb{C}) \\ n = 2k + 1 & M_{2^k}(\mathbb{C}) \oplus M_{2^k}(\mathbb{C}) \end{cases}$$

IV.5.6 Involutions, Norme, et Inverse

Dans toutes les algèbres de Clifford, $\mathcal{Cl}(\mathcal{V}, \mathcal{Q})$, on peut définir trois involutions linéaires assez naturelles :

1. La **graduation** (ou involution principale) qui est un automorphisme.
2. La **réversion** (ou transposition) qui est un anti-automorphisme.
3. La **conjugaison** qui est un anti-automorphisme.

Ces involutions sont définies sur les vecteurs de base de \mathcal{V} (en fait du plongement de \mathcal{V} dans $\mathcal{Cl}(\mathcal{V}, \mathcal{Q})$), avec des règles qui permettent d'étendre cette définition à $\mathcal{Cl}(\mathcal{V}, \mathcal{Q})$.

Dans le cas particulier des algèbres $\mathcal{Cl}_{p,q}(\mathbb{R})$ on peut facilement étendre la définition

Involution	$e_i \in \mathcal{V}$	$(x, y) \in \mathcal{Cl}_{p,q}(\mathbb{R})^2$	$x \in \mathbb{R}_{p,q}^k$	Relations
Graduation	$\widehat{e}_i = -e_i$	$\widehat{(x, y)} = \widehat{x} \widehat{y}$	$\widehat{x} = (-1)^k x$	$\widehat{\widehat{x}} = \widetilde{\widetilde{x}} = \widetilde{\widehat{x}}$
Réversion	$\widetilde{e}_i = e_i$	$\widetilde{(x, y)} = \widetilde{y} \widetilde{x}$	$\widetilde{x} = (-1)^{\frac{k(k-1)}{2}} x$	$\widetilde{\widetilde{x}} = \widehat{\widehat{x}} = \widehat{\widetilde{x}}$
Conjugaison	$\overline{e}_i = -e_i$	$\overline{(x, y)} = \overline{y} \overline{x}$	$\overline{x} = (-1)^{\frac{k(k+1)}{2}} x$	$\overline{\overline{x}} = \widehat{\widehat{x}} = \widehat{\overline{x}}$

IV.5.7 Propriétés algébriques

Les algèbres de Clifford sont des algèbres unitaires, associatives (donc les parenthèses ne sont pas nécessaires dans les calculs), mais non commutatives.

Toutes les algèbres de Clifford, hormis les complexes et les quaternions contiennent des éléments non réels de carré égal à 1, et donc contiennent des diviseurs de 0 ; si $p \neq 0$, c'est évident, et si $q > 2$, alors :

$$(e_1 \cdot e_2 \cdot e_3)^2 = e_1 \cdot e_2 \cdot e_3 \cdot e_1 \cdot e_2 \cdot e_3, \text{ avec 3 permutations, on génère un changement de signe :}$$

$$e_1 \cdot e_2 \cdot e_3 \cdot e_1 \cdot e_2 \cdot e_3 = -e_2 \cdot e_1 \cdot e_1 \cdot e_3 \cdot e_3 \cdot e_2, \text{ et comme } e_1^2 = -1 \text{ et } e_3^2 = -1 \text{ on obtient finalement :}$$

$$(e_1 \cdot e_2 \cdot e_3)^2 = -e_2^2 = 1.$$

IV.5.8 Synonymes, Isomorphismes, Exemples

Parmi les algèbres de Clifford, on trouve :

- $\mathcal{Cl}_{0,1}(\mathbb{R})$: les nombres Complexes
- $\mathcal{Cl}_{1,0}(\mathbb{R})$: les Complexes Fendus
- $\mathcal{Cl}_{0,2}(\mathbb{R})$: les Quaternions
- $\mathcal{Cl}_{0,3}(\mathbb{R})$: les BiQuaternions Fendus (ou BiQuaternions de Clifford)
- $\mathcal{Cl}_{1,1}(\mathbb{R})$: les CoQuaternions
- $\mathcal{Cl}_{2,0}(\mathbb{R})$: L'algèbre naturel sur un espace 2D ($\mathcal{Cl}_{1,1}(\mathbb{R}) \cong \mathcal{Cl}_{2,0}(\mathbb{R})$)
- $\mathcal{Cl}_{3,0}(\mathbb{R})$: L'algèbre naturel sur un espace 3D

- $\mathcal{Cl}_{1,3}(\mathbb{R})$: L'algèbre de l'espace-temps (espace de Minkowski).

A noter que ni les **octonions**, ni les **sédénions** (ni les autres algèbres de dimension supérieure construites par la **méthode de Cayley-Dickson**) ne sont des algèbres de Clifford, car elles sont non associatives.

L'algèbre des matrices de Pauli est isomorphe à $\mathcal{Cl}_{3,0}(\mathbb{R})$.

IV.5.9 Utilisation en physique

1. D. Hestenes, *Clifford Algebra And The Interpretation Of Quantum Mechanics*, Clifford Algebras and their Applications in Mathematical Physics, Reidel, Dordrecht/Bostonp. 321–346, 1986.
2. D. Hestenes, *New Foundations for Classical Mechanics*, Springer ; 2nde édition, 1999.
3. J. Ryan and W. Sprössig, *Clifford Algebras and Their Applications in Mathematical Physics, Vol. 2*, Birkhäuser Boston, 2000.
4. A. Micali, R. Boudet et J. Helmstetter, *Clifford Algebras and Their Applications in Mathematical Physics*, Springer, 2010.
5. P. R. Girard, *Einstein'S Equations And Clifford Algebra*, INSA de Lyon, 1999.
6. B. J. Hiley et R. E. Callaghan, *The Clifford Algebra approach to Quantum Mechanics A : The Schrödinger and Pauli Particles.*, University of London, 2010.
7. V. Labunets, *Clifford Algebras As Unified Language For Image Processing And Pattern Recognition*, Urals State Technical University, Ekaterinburg, Russia, 2006

IV.5.10 Références

La littérature sur les algèbres de Clifford est pléthorique, en voici un tout petit exemple :

1. R. Delanghe, *Clifford Analysis : History and Perspective*, Computational Methods and Function Theory Volume 1, No. 1, p. 107-153.
2. G. Franssens, *Introduction To Clifford Analysis*, 18th International Conference on the Application of Computer Science and Mathematics in Architecture and Civil Engineering, Weimar, Germany, 2009.
3. S. Franchini, G. Vassallo et F. Sorbello , *A brief introduction to Clifford algebra*, Université de Palerme, 2010.
4. J. Gallier, *Clifford Algebras, Clifford Groups, and a Generalization of the Quaternions : The Pin and Spin Groups*, University of Pennsylvania Philadelphia, 2010.
5. P. Leopardi, *A quick introduction to Clifford algebras*, Presented at School of Mathematics, University of New South Wales, 2003.
6. G. Laville, *Clifford algebra, Geometric algebra*, Université de Caen, 2009.
7. D. Lee et Y. Song, *The Matrix Representation Of Clifford Algebra*, Journal Of The Chungcheong Mathematical Society Volume 23, No. 2, 2010.

IV.6 Tessarines \mathcal{T}

IV.6.1 Introduction

Idée introduite par James Cockle⁶⁹, un mathématicien anglais (1819 - 1895) en 1848 dans plusieurs articles portant sur $\mathcal{T}_{\mathbb{C}}$ (cf. infra pour la notation) ayant pour but l'étude des sinus et cosinus hyperboliques.

En 1892 Corrado Segre, un mathématicien italien (1863 - 1924), a introduit les **Bicomplexes** qui sont très exactement la tessarine : $\mathcal{T}_{\mathbb{C}}$.

IV.6.2 Définition

Un ensemble de Tessarines est construit à partir d'une \mathbb{K} -algèbre, le résultat étant une \mathbb{K} -algèbre hyperbolique de dimension double de la \mathbb{K} -algèbre de départ.

IV.6.3 Mode de construction

Soit A une \mathbb{K} -algèbre. L'ensemble des tessarines \mathcal{T}_A sur A est constitué des matrices 2×2 de la forme : $\begin{pmatrix} u & v \\ v & u \end{pmatrix}$ avec $(u, v) \in A^2$. En munissant \mathcal{T}_A de l'addition et de la multiplication des matrices, les tessarines constitue une sous-algèbre de $(M_2(A), +, \times, \cdot)$ de dimension double de la dimension de A sur \mathbb{K} .

IV.6.4 Table de multiplication

Si l'algèbre A est unitaire, toute tessarine s'écrit de manière unique sous la forme $u \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + v \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, il est donc naturel de poser $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ et $j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ de telle sorte que les tessarines s'écrivent $u + j \cdot v$.

En utilisant le produit matriciel, on obtient la table de multiplication suivante (qui est celle des **complexes fendus**) :

·	1	j
1	1	j
j	j	1

A titre d'exemple, on peut développer la table de multiplication de $\mathcal{T}_{\mathbb{H}}$, dans laquelle on reconnaît les **BiQuaternions de Clifford** :

·	1	i	j	k	l	li	lj	lk
1	1	i	j	k	l	li	lj	lk
i	i	-1	k	-j	li	-l	lk	-lj
j	j	-k	-1	i	lj	-lk	-l	li
k	k	j	-i	-1	lk	lj	-li	-l
l	l	li	lj	lk	1	i	j	k
li	li	-l	lk	-lj	i	-1	k	-j
lj	lj	-lk	-l	li	j	-k	-1	i
lk	lk	lj	-li	-l	k	j	-i	-1

Dans les quatre premières colonnes et quatre premières lignes on reconnaît les Quaternions.

La partie du tableau en teinte plus ou moins rose/rouge correspond presque⁷⁰ aux bicomplexes.

69. Voir aussi : **les coquaternions**

70. c'est plus net en posant $k = -l$ et $j = li$

IV.6.5 Conjugué, Module, Norme, Forme Polaire et Inverse

Les possibilité de définition de conjugués et de normes sont directement liées aux propriétés de la \mathbb{K} -algèbre, A sur laquelle on construit la Tessarine \mathcal{T}_A .

En tout état de cause, si A est unitaire, on peut toujours définir le conjugué suivant : $\overline{u + j \cdot v} = u - j \cdot v$, et le module associé $|u + j \cdot v| = (u + j \cdot v) \cdot \overline{(u + j \cdot v)}$, qui dans le cas où A est une algèbre commutative $|u + j \cdot v| = u^2 + v^2$ (donc $|u + j \cdot v| \in A$).

Si en plus $u^2 + v^2$ est inversible dans A , alors $u + j \cdot v$ est inversible dans \mathcal{T}_A et :

$$(u + j \cdot v)^{-1} = \frac{u - j \cdot v}{u^2 + v^2}$$

IV.6.6 Propriétés algébriques

$(\mathcal{T}_A, +, \times, \cdot)$ est une \mathbb{K} -algèbre de dimension double de la dimension de A (en tant que \mathbb{K} -algèbre).

\mathcal{T}_A est commutative (resp. unitaire) si, et seulement si, A est commutative (resp. unitaire).

L'application $\begin{pmatrix} p & q \\ q & p \end{pmatrix} \mapsto (p + q, p - q)$, qui est un isomorphisme, montre que : $\mathcal{T}_A \cong A \oplus A$.

Cet isomorphisme permet notamment de montrer qu'un polynôme unitaire $P \in \mathcal{T}_{\mathbb{C}}[X]$ de degré $n \in \mathbb{N}$ admet n^2 racines (comptées avec multiplicité) : en effet les projections sur chacune des composantes donnent un polynôme de $\mathbb{C}[X]$ de degré n , donc ayant n racines ; si on note x_i les n racines du polynôme sur la première composante et y_i les n racines du polynôme sur la deuxième composante, alors les n^2 couples $(x_i, y_j)_{(i,j) \in [1,n]^2}$ sont les racines du polynôme P .

\mathcal{T}_A admet toujours des diviseurs de zéro, puisque $j^2 = 1$ implique $(j + 1)(j - 1) = 0$.

\mathcal{T}_A admet toujours des éléments idempotents, puisque $j^2 = 1$ implique $\left(\frac{j + 1}{2}\right)^2 = \frac{j + 1}{2}$.

\mathcal{T}_A admet des éléments nilpotents si et seulement si A en contient.

IV.6.7 Synonymes, Isomorphismes, Exemples

On peut noter quelques isomorphismes :

- $\mathcal{T}_{\mathbb{R}}$ est isomorphe aux **Complexes Fendus** : \mathfrak{C} .
- $\mathcal{T}_{\mathbb{C}}$ est isomorphe aux **BiComplexes** : \mathbb{C}_2 .
- $\mathcal{T}_{\mathbb{H}}$ est isomorphe aux **BiQuaternions de Clifford** : \mathbb{R} .
- $\mathcal{T}_{\mathbb{O}}$ est isomorphe aux Sédénions Coniques.

On peut aussi remarquer que l'on pourrâit définir les Multicomplexes Fendus sur le modèle des **Multicomplexes \mathfrak{C}_n** :

1. $\mathfrak{C}_0 = \mathbb{R}$
2. $\mathfrak{C}_{n+1} = \{x_0 + x_1 \cdot i_{n+1} \mid ((x_0, x_1) \in \mathfrak{C}_n^2) \wedge (i_{n+1} \notin \mathfrak{C}_n) \wedge (i_{n+1}^2 = -1)\}$

Avec cette définition, on a la relation $\mathfrak{C}_{n+1} = \mathcal{T}_{\mathfrak{C}_n}$.

\mathfrak{C}_1 est noté plus simplement \mathfrak{C} .

Notons également que $\mathcal{T}_{\mathbb{H}}$ contient certaines sous-algèbres remarquables :

- Les réels, si $v = 0$ et $u \in \mathbb{R}$.
- Les complexes, si $v = 0$ et $u \in \mathbb{C}$.
- Les quaternions, si $v = 0$ et $u \in \mathbb{H}$.

Une construction alternative dans le cas de $\mathcal{T}_{\mathbb{C}} (= \mathbb{C}_2)$ est de considérer l'idéal \mathcal{I} de $\mathbb{C}[X, Y]$ généré par les polynômes $X^2 + 1$, $Y^2 - 1$ et $XY - YX$ puis de définir les tessarines sur \mathbb{C} comme l'algèbre quotient $\mathbb{C}[X, Y]/\mathcal{I}$.

Soit l'application définie par $\varphi : \mathcal{T}_{\mathbb{C}} \mapsto \mathbb{C}[X, Y]/\mathcal{I}$ $\left\{ \begin{array}{l} \varphi(1) = 1 \\ \varphi(i) = X \\ \varphi(j) = Y \\ \varphi(k) = XY \end{array} \right.$

Alors φ se prolonge naturellement en un isomorphisme de \mathbb{K} -algèbre.

IV.6.8 Utilisation en physique

Les tessarines sont utilisées dans le traitement des signaux digitaux (cf. Soo-Chang Pei (2004) et Alfsmann (2006, 2007) ci-dessous).

Les Tessarines apparaissent aussi dans l'étude de certains système markovien :

Soit $X = ((x_i)_{i \in [1,n]}, (a_{i,j})_{(i,j) \in [1,n]^2})$ un système où, pour \mathcal{K} une \mathbb{K} -algèbre :
 $x_i : \mathbb{N} \mapsto \mathcal{K}$, et $a_{i,j} \in \mathcal{K}$, vérifiant les relations :

$$x_i(n+1) = \sum_{j=1}^n a_{i,j} \cdot x_j(n)$$

Autrement dit la valeur de chacun des $x_i(n+1)$ ne dépend que de la valeur des $x_i(n)$, et de la « structure » du système ⁷¹.

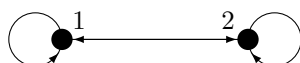


FIGURE 4 – Système 2×2 symétriques

Dans le cas particulier d'un système symétrique à deux éléments, les relations s'écrivent :

$$\begin{cases} x_1(n+1) = a \cdot x_1(n) + b \cdot x_2(n) \\ x_2(n+1) = b \cdot x_1(n) + a \cdot x_2(n) \end{cases}$$

En posant $x(n) = x_1(n) + j \cdot x_2(n)$ et $\alpha = a + j \cdot b$ où $j^2 = 1$, on obtient le système suivant, où $x(n) \in \mathcal{T}_{\mathcal{K}}$, et $\alpha \in \mathcal{T}_{\mathcal{K}}$:

$$x(n+1) = \alpha \cdot x(n)$$

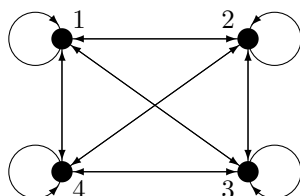


FIGURE 5 – Système 4×4 symétriques

Dans le cas particulier d'un système symétrique à quatre éléments, les relations s'écrivent :

$$\begin{cases} x_1(n+1) = a \cdot x_1(n) + b \cdot x_2(n) + c \cdot x_3(n) + d \cdot x_4(n) \\ x_2(n+1) = b \cdot x_1(n) + a \cdot x_2(n) + d \cdot x_3(n) + c \cdot x_4(n) \\ x_3(n+1) = c \cdot x_1(n) + d \cdot x_2(n) + a \cdot x_3(n) + b \cdot x_4(n) \\ x_4(n+1) = d \cdot x_1(n) + c \cdot x_2(n) + b \cdot x_3(n) + a \cdot x_4(n) \end{cases}$$

En posant : $A = \begin{pmatrix} a & b \\ b & a \end{pmatrix}$, $B = \begin{pmatrix} c & d \\ d & c \end{pmatrix}$, $X_1(n) = \begin{pmatrix} x_1(n) & x_2(n) \\ x_2(n) & x_1(n) \end{pmatrix}$ et $X_2(n) = \begin{pmatrix} x_3(n) & x_4(n) \\ x_4(n) & x_3(n) \end{pmatrix}$

Par définition $A, B, X_1(n)$ et $X_2(n)$ sont des éléments de la Tessarine $\mathcal{T}_{\mathcal{K}}$.

Le système précédent peut être remplacé par (où $j^2 = 1$) :

$$X_1(n+1) + j \cdot X_2(n+1) = (A + j \cdot B) \cdot (X_1(n) + j \cdot X_2(n))$$

⁷¹. On peut trouver un exemple d'un tel système en considérant un ensemble de points dans un champ Electrique et/ou Magnétique et/ou Gravitationnel, chacun des points participant à la valeur des champs.

Autrement dit, en posant $X(n) = X_1(n) + j \cdot X_2(n)$ et $\alpha = A + j \cdot B$, $X(n)$ et α appartiennent à la Tessarine de $\mathcal{T}_{\mathcal{K}}$ (autrement dit à $\mathcal{T}_{\mathcal{K}}$), on peut ré-écrire le système précédent sous la forme d'une équation dans cette Tessarine :

$$X(n+1) = \alpha \cdot X(n)$$

Dans le tableau ci-dessous, les systèmes directionnels sont les mêmes que les systèmes symétriques sauf que dans ce cas $a_{i,j} = -a_{j,i}$ (dans ce cas les ensembles dans lesquels le système peut s'écrire simplement ne sont plus ds Tessarines). Les paramètres de ce tableau sont le type de système et l'ensemble dans lequel les valeurs sont prises.

Système	\mathbb{R}	\mathbb{C}	\mathbb{H}	...
2×2 symétrique	$\mathcal{T}_{\mathbb{R}} = \mathbb{C}$	$\mathcal{T}_{\mathbb{C}} = \mathbb{C}_2$	$\mathcal{T}_{\mathbb{H}} = \mathbb{B}$	
2×2 directionnel	\mathbb{C}	\mathbb{C}_2	\mathbb{B}	
4×4 symétrique	$\mathcal{T}_{\mathbb{C}} = \mathbb{C}_2$	$\mathcal{T}_{\mathbb{C}_2}$	$\mathcal{T}_{\mathbb{B}}$	
4×4 directionnel	\mathbb{H}	\mathbb{B}	$\mathbb{H} \otimes \mathbb{H}$	
⋮				

IV.6.9 Références

1. J. Cockle, *On Certain Functions Resembling Quaternions and on a New Imaginary in Algebra*, London-Dublin-Edinburgh Philosophical Magazine, Volume 33, p.435-439, 1848
2. J. Cockle, *On a New Imaginary in Algebra*, London-Dublin-Edinburgh Philosophical Magazine, Volume 34, p. 37-47, 1849
3. J. Cockle, *On the Symbols of Algebra and on the Theory of Tessarines*, London-Dublin-Edinburgh Philosophical Magazine, Volume 34, p. 406-410, 1849
4. J. Cockle, *On Impossible Equations, on Impossible Quantities and on Tessarines*, London - Dublin - Edinburgh Philosophical Magazine, Volume 37, p. 281-283, 1850
5. J. Cockle, *On the true amplitude of a tessarine ; on the derivation of the word theodolite ; and on light under the action of magnetism*, Philosophical Magazine Series 3, Volume 36, Issue 243, P. 290-295, 1850
6. D. Alfsmann, *On families of 2^N dimensional hypercomplex algebras suitable for digital signal processing*, 14th European Signal Processing Conference, Florence, Italy, 2006.
7. D. Alfsmann & H. G. Göckler, *On Hyperbolic Complex LTI Digital Systems*, Digital Signal Processing Group, Université de la Ruhr, 2007.
8. F. Catoni, R. Cannata, E. Nichelatti & P. Zampetti, *Commutative Hypercomplex Numbers and Functions of Hypercomplex Variable : A Matrix Study*, Advances in Applied Clifford Algebras, Volume 15 No. 2, p. 183-212, 2005.
9. Soo-Chang Pei, Ja-Han Chang & Jian-Jiun Ding, *Commutative Reduced Biquaternions and their Fourier Transform for Signal and Image Processing*, IEEE Transactions on Signal Processing, volume 52 N° 7, p. 2012-31, 2004.

V Infinitésimaux

V.1 Hyperréels ${}^*\mathbb{R}$

V.1.1 Introduction

L'ensemble des nombres hyperréels, noté ${}^*\mathbb{R}$, dans leur version moderne, trouve sa source dans l'analyse non standard et les travaux de A. Robinson.

V.1.2 Définition

L'ensemble des nombres hyperréels est un modèle non standard de la théorie $(\mathbb{R}, 0, 1, +, \times, <)$, c'est à dire un modèle de l'ensemble des propositions *du premier ordre*, dans le langage des corps ordonnés, vraies dans \mathbb{R} (c'est à dire que $(\mathbb{R}, 0, 1, +, \times, <)$ et $({}^*\mathbb{R}, 0, 1, +, \times, <)$ sont élémentairement équivalents), mais ${}^*\mathbb{R}$ contient des éléments non réels, on verra, que (avec un léger abus de langage) $\mathbb{R} \subsetneq {}^*\mathbb{R}$.

V.1.3 Mode de construction

La méthode de construction habituelle utilise une méthode de théorie des modèles, les ultrapuissances (une puissance infinie d'un modèle, quotientée par un ultrafiltre), la méthode présentée ici est légèrement différente, tout à fait équivalente, mais un peu plus intuitive, en utilisant la notion de mesure.

La première étape consiste à considérer l'ensemble noté \mathbb{R}^ω , des suites de réels.

Il est facile de munir \mathbb{R}^ω d'opérations et de relations héritées de \mathbb{R} :

$$a = (a_0, a_1, \dots)$$

$$b = (b_0, b_1, \dots)$$

$$a + b = (a_0 + b_0, a_1 + b_1, \dots)$$

$$a \times b = (a_0 \times b_0, a_1 \times b_1, \dots)$$

$$a < b \Leftrightarrow (a_0 < b_0) \wedge (a_1 < b_1) \wedge \dots$$

Tout aussi facilement, on peut identifier \mathbb{R} et un sous-ensemble de \mathbb{R}^ω , en identifiant un réel x avec la suite constante égale à x :

$$\pi : \mathbb{R} \mapsto \mathbb{R}^\omega \text{ défini par } \pi(x) = (x, x, \dots)$$

Ci dessous nous écrivons x pour désigner en fait $\pi(x)$

Il est facile de vérifier que l'addition est bien définie et possède les propriétés attendues (0 ($\pi(0)$ en fait) est bien l'élément neutre, par exemple), mais il n'en va pas de même pour la multiplication (beaucoup d'éléments n'ont pas de symétrique), ni pour la relation d'ordre qui n'est pas totale.

En prenant l'exemple de la relation d'ordre, une première idée consiste à considérer deux ensembles :

$$E_{a < b} = \{i \mid i \in \mathbb{N} \wedge a_i < b_i\} \text{ et } E_{b < a} = \{i \mid i \in \mathbb{N} \wedge b_i < a_i\}$$

Puis à déclarer que $a < b$ si et seulement si $E_{a < b}$ est plus grand que $E_{b < a}$; malheureusement, s'il est facile de dire lequel de deux ensembles finis est le plus grand, ou lequel entre un ensemble fini et un ensemble infini est le plus grand, il n'y a plus de *bonne* réponse entre deux ensembles infinis.

Nous allons formaliser l'idée, pour les sous-ensembles de \mathbb{N} , qu'un sous-ensemble puisse être *Grand* ou *Petit* :

1. \mathbb{N} est *Grand*.
2. Tout sous-ensemble de \mathbb{N} est soit *Grand*, soit *Petit*, mais pas les deux.
3. Tout sous-ensemble fini est *Petit* (et tout ensemble cofini est *Grand*).
4. Si A est *Grand* et si $A \subset B$, alors B est *Grand*.
5. Si A et B sont *Grands*, alors $A \cap B$ est *Grand* (peut-être plus intuitivement : Si A et B sont *Petits*, alors $A \cup B$ est *Petit*)
6. Pour tout sous-ensemble A de \mathbb{N} , soit A est *Grand* soit $\mathbb{N} \setminus A$ est *Grand*

Les spécialistes auront reconnu la définition d'un ultrafiltre non principal sur \mathbb{N} .

Nous allons voir qu'avec une notion de Mesure sur \mathbb{N} (ce n'est pas tout à fait la définition habituelle) on répond aux besoins ci-dessus.

Définition : Une Mesure (finiment additive et non σ -additive) μ sur \mathbb{N} est une fonction définie sur $\mathfrak{P}(\mathbb{N})$ ne prenant que les valeurs 0 et 1 et vérifiant :

1. $\mu(\mathbb{N}) = 1$.
2. Si A est un sous-ensemble fini de \mathbb{N} , alors $\mu(A) = 0$.
3. Si A et B sont deux sous-ensembles de \mathbb{N} , tels que $A \cap B = \emptyset$, alors $\mu(A \cup B) = \mu(A) + \mu(B)$.

Il est immédiat de vérifier que, si l'on définit un sous-ensemble A de \mathbb{N} comme *Grand* si et seulement si $\mu(A) = 1$, alors les « axiomes » de *Grand* sont bien vérifiés.

Il nous reste à définir une relation d'équivalence (notée \simeq) sur \mathbb{R}^ω qui nous permettra de bien définir la relation d'ordre.

Soit $a \in \mathbb{R}^\omega$ et $b \in \mathbb{R}^\omega$: $a \simeq b \Leftrightarrow \mu(\{i \mid a_i = b_i\}) = 1$
 Autrement dit, plus intuitivement, $a \simeq b$ si et seulement si $a_i = b_i$ « presque partout ».

Finalement on pose ${}^*\mathbb{R} = \mathbb{R}^\omega / \simeq$.

Il est facile de vérifier que la notion de nombre réel (comme sous-ensemble de \mathbb{R}^ω), l'addition, la multiplication et la relation d'ordre « passent » au quotient (c'est un exercice très simple).

Mais nous devons vérifier aussi que l'on récupère bien les propriétés perdues. Par exemple, nous avons signalé que beaucoup d'éléments n'avaient pas de symétrie pour la multiplication dans \mathbb{R}^ω , ne serait-ce que $(0, 1, 1, 1, \dots)$.

Soit $a \in {}^*\mathbb{R} \setminus \{0\}$ et $\mathbf{a} = (a_i)_{i \in \mathbb{N}}$ un de ses représentants dans \mathbb{R}^ω .

L'hypothèse $a \neq 0$ se traduit par $\mu(\{i \mid a_i \neq 0\}) = 1$.

On pose $\mathbf{a}^{-1} = \begin{pmatrix} a_i^{-1} & \Leftrightarrow & a_i \neq 0 \\ 0 & \Leftrightarrow & a_i = 0 \end{pmatrix}_{i \in \mathbb{N}}$. On a donc $\mathbf{a} \times \mathbf{a}^{-1} = \begin{pmatrix} 1 & \Leftrightarrow & a_i \neq 0 \\ 0 & \Leftrightarrow & a_i = 0 \end{pmatrix}_{i \in \mathbb{N}}$

Par conséquent $\{i \mid (\mathbf{a} \times \mathbf{a}^{-1})_i = 1\} = \{i \mid a_i \neq 0\}$, c'est dire que $\mu(\{i \mid (\mathbf{a} \times \mathbf{a}^{-1})_i = 1\}) = 1$, donc que $\mathbf{a} \times \mathbf{a}^{-1} \simeq 1$, et finalement que $a \times a^{-1} = 1$ (avec $a^{-1} = \overline{\mathbf{a}^{-1}}$ (C'est à dire la classe de \mathbf{a}^{-1} modulo \simeq)).

Un inconvénient majeur à ce qui vient d'être écrit : l'existence d'une telle mesure n'est pas garantie ! En fait on peut démontrer qu'une telle mesure (et donc qu'un tel ultrafiltre) existe, en utilisant **l'axiome du choix**.

Il reste un inconvénient mineur : on ne sait pas exhiber une telle mesure (ou un tel ultrafiltre).

Note importante : la construction par ultrafiltre est strictement équivalente à celle présentée ici (mais la notion de « presque partout » me paraît plus intuitive), et elle présente le gros avantage de permettre d'utiliser le théorème de Loś :

Toute formule du premier ordre est vraie dans un ultraproduit (et donc dans une ultrapuissance) si l'ensemble des indices pour lesquels la formule est vraie, appartient à l'ultrafiltre.

V.1.4 Infinitésimaux et infinis

On définit un *infinitésimal* positif comme un nombre ε vérifiant $(\varepsilon > 0) \wedge (\forall n (n \in \mathbb{N} \Rightarrow \varepsilon < \frac{1}{n}))$ (il y a beaucoup d'autres définitions équivalentes, et certaines qui incluent 0 parmi les infinitésimaux).

On définit un *infini* positif comme un nombre ω vérifiant $(\omega > 0) \wedge (\forall n (n \in \mathbb{N} \Rightarrow \omega > n))$

Les définitions pour *infinitésimal* négatif, *infini* négatif, *infinitésimal* et *infini* sont celles que l'on peut attendre. Les nombres *non infinis* sont dits *finis*.

Soit $\mathbf{a} = \left(1, \frac{1}{2}, \dots, \frac{1}{n}, \dots\right) \in \mathbb{R}^\omega$

Soit $\frac{1}{\mathbf{n}} = \left(\frac{1}{n}, \frac{1}{n}, \dots, \frac{1}{n}, \dots\right) \in \mathbb{R}^\omega$

Autrement dit $\frac{1}{\mathbf{n}} = \pi\left(\frac{1}{n}\right)$

Pour tout n donné, l'ensemble des indices pour lesquels $\mathbf{a}_i < \left(\frac{1}{n}\right)_i$ est cofini, donc $\mathbf{a} < \frac{1}{\mathbf{n}}$, et il en va de même pour les classes (modulo \simeq), et donc $\bar{\mathbf{a}} = \varepsilon$ est bien un infinitésimal.

De la même façon on peut démontrer que $\mathbf{b} = (1, 2, \dots, n, \dots) \in \mathbb{R}^\omega$ est plus grand que tous les entiers (que tous les $\pi(n)$ pour $n \in \mathbb{N}$, pour être rigoureux), et donc $\bar{\mathbf{b}} = \omega$ est bien un infini.

Il est immédiat que $\mathbf{a} \times \mathbf{b} = (1, 1, \dots)$ autrement dit que $\mathbf{a} \times \mathbf{b} = \pi(1)$, ou encore $\varepsilon \times \omega = 1$

Quelques définitions supplémentaires :

Soit $(x, y) \in {}^*\mathbb{R}$, x et y sont dit **infinitement proches** (noté $x \approx y$) si leur différence est infinitésimale : $x \approx y \Leftrightarrow (x - y)$ est infinitésimal).

Monade : soit $x \in {}^*\mathbb{R}$, alors la Monade de x est $M_x = \{y \mid y \in {}^*\mathbb{R} \wedge x \approx y\}$, en particulier M_0 est l'ensemble des infinitésimaux (incluant 0) (positifs et négatifs). A noter qu'une monade contient un et un seul nombre réel. M_x peut aussi être appelé **halo** de x .

Partie standard : soit $x \in {}^*\mathbb{R}$, fini, alors il existe un nombre réel r unique tel que $r \approx x$, r est appelé la partie standard de x et notée $st(x) = r$. $st(x)$ est parfois appelé **shadow** ou **ombre** de x .

Galaxie : soit $x \in {}^*\mathbb{R}$, alors la Galaxie de x est $Galaxie(x) = \{y \mid x - y \text{ est fini}\}$, en particulier $Galaxie(0)$ est l'ensemble des nombres hyperréels finis.

V.1.5 Limite, Continuité et Dérivée

L'analyse non standard permet de reformuler des définitions usuelles de l'analyse avec une grande économie de moyens :

Dans ce qui suit nous considérerons une fonction $f : \mathbb{R} \mapsto \mathbb{R}$, et son extension à ${}^*\mathbb{R}$, notée aussi f .

Définition standard de la limite.

$$\lim_{x \rightarrow x_0} f(x) = \ell \Leftrightarrow \forall \varepsilon \exists \eta \forall x ((\varepsilon > 0) \wedge (\eta > 0) \wedge (|x - x_0| < \eta) \Rightarrow (|f(x) - \ell| < \varepsilon))$$

Définition non standard de la limite.

$$\lim_{x \rightarrow x_0} f(x) = \ell \Leftrightarrow \forall x ((x \approx x_0) \Rightarrow (f(x) \approx \ell))$$

Définition standard de la continuité.

f est dite continue en x_0 si

$$\forall \varepsilon \forall \eta \forall x ((\varepsilon > 0) \wedge (\eta > 0) \wedge (|x - x_0| < \eta) \Rightarrow (|f(x) - f(x_0)| < \varepsilon)).$$

Définition non standard de la continuité.

f est dite continue en x_0 si

$$\forall x ((x \approx x_0) \Rightarrow (f(x) \approx f(x_0)))$$

Sur le même modèle on peut redéfinir la dérivée, et sans rentrer dans tous les détails, on notera que la définition de la dérivée devient (sous réserve d'existence) :

$$f'(x) = st \left(\frac{f(x + dx) - f(x)}{dx} \right)$$

Autrement dit on remplace $f'(x) = \frac{dy}{dx}$ par $f'(x) = st(\frac{dy}{dx})$, où dx est un infinitésimal. La différence peut paraître infime, mais dans la conduite des démonstrations, elle permet d'éliminer la notion de « on néglige ».

Calcul standard de la dérivée de la fonction définie par $f(x) = x^2$

$$f'(x) = \frac{(x + dx)^2 - x^2}{dx} = \frac{2x dx + dx^2}{dx} = 2x + dx$$

Et arrivé là, on se contente de dire que l'on « néglige » dx devant $2x$ pour obtenir le résultat $f'(x) = 2x$.

Calcul non standard de la dérivée de la fonction définie par $f(x) = x^2$

$$f'(x) = st \left(\frac{(x + dx)^2 - x^2}{dx} \right) = st \left(\frac{2x dx + dx^2}{dx} \right) = st(2x + dx) = 2x$$

L'utilisation d'un infinitésimal et de la notion de partie standard a permis de formaliser la notion de « négligeable ».

Dans l'article de H. J. Keisler, *Foundations of Infinitesimal Calculus*, on trouvera les notions d'intégrale, de fonctions trigonométriques, exponentielle, etc.

V.1.6 Propriétés algébriques

$(^*\mathbb{R}, 0, 1, +, \times, <)$ est un corps réel clos, vérifiant toutes les formules du premier ordre vérifiées par $(\mathbb{R}, +, \times, 0, 1, <)$.

$(^*\mathbb{R}, 0, 1, +, \times, <)$ n'est pas archimédien (qui n'est pas une propriété du premier ordre).

On sait que \mathbb{R} n'a pas de trous, c'est-à-dire est Dedekind-complet, bizarrement, en ajoutant un halo autour de chaque réel, on recrée des trous, autrement dit $^*\mathbb{R}$ n'est plus Dedekind-complet.

Par exemple la monade M_0 est bornée supérieurement, mais ne possède pas de borne supérieure.

V.1.7 Synonymes, Isomorphismes, Exemples

Il existe d'autres modes de construction des hyperréels :

Vieri Benci et Mauro Di Nasso ont présenté une construction de $^*\mathbb{R}$ à partir d'anneaux de fonctions *composables*.

Vladimir Kanovei et Saharon Shelah ont montré qu'il existe une extension élémentaire de \mathbb{R} qui est définissable et ω -saturé (et c'est bien un modèle non standard).

V.1.8 Utilisation en physique

Comme pour tous les infinitésimaux, ce qui s'exprime en analyse classique par des notions de limites peut s'exprimer en analyse non standard à l'aide d'infinitésimaux.

[Nonstandard analysis in classical physics and quantum formal scattering](#). Les auteurs (F. Bagarello et S. Valenti) présentent, en termes d'analyse non standard, une formulation lagrangienne de la physique classique et une formulation de la diffusion quantique formelle.

V.1.9 Références

1. Robinson, A., Non-Standard Analysis (Rev. Ed.). Princeton University Press, Princeton, NJ, 1996.
2. Goldblatt, Lecture on the Hyperreals Springer-Verlag, New York, NY, 1998.
3. [Balade en Analyse non standard sur les traces de A. Robinson.](#)
4. [The Hyperreals par Larry Susanka.](#)
5. [Foundations of Infinitesimal Calculus par H. J. Keisler.](#)
6. [The Hyperreal Numbers and Applications to Elementary Calculus par Doug Babcock.](#)
7. [Un article de Vieri Benci et Mauro Di Nasso : A Purely Algebraic Characterization of the Hyperreal Numbers.](#)
8. [Un article de Vladimir Kanovei et Saharon Shelah : A definable nonstandard model of the reals.](#)

V.2 Surréels No

V.2.1 Introduction

Les nombres surréels ont été introduits par J.H. Conway dans le cadre de sa théorie des jeux (publication en 1976, longtemps après ses premiers travaux). Ils furent popularisés par D.E. Knuth dans un article (1974, donc avant la publication de Conway, mais inspiré par Conway néanmoins) sous-titré : "comment deux anciens étudiants découvrirent les mathématiques pures et vécurent heureux".

Les nombres surréels sont généralement notés : **No**.

V.2.2 Définition

Il existe trois façons très différentes de construire les nombres surréels :

1. Une définition à base de coupures (celle de Conway)
2. Une définition à base de fonctions (présentée par Gonshor)
3. Une définition purement axiomatique (présentée par Alling)

V.2.3 Mode de construction

La définition à base de coupures due à Conway est la suivante :

Règle 1) un nombre surréel est défini par la donnée de deux ensembles (pas quelconques, cf. infra) de nombres surréels, le premier est appelé ensemble Gauche, le deuxième ensemble Droit.

Une telle définition peu paraître peu utile puisqu'il semble qu'il soit nécessaire de connaître des nombres surréels pour fabriquer des nombres surréels.

En fait, sans connaître le moindre nombre surréel, on peut en construire un facilement : (\emptyset, \emptyset) (noté aussi $\{\emptyset \mid \emptyset\}$, ou encore $\{\mid\}$, et finalement : 0).

A l'aide de ce nouveau nombre surréel on peut tenter d'en fabriquer d'autres :

$\{0 \mid \}$, $\{\mid 0\}$ et $\{0 \mid 0\}$, ce dernier n'est pas un nombre surréel à cause de la règle 2 ci-dessous (à noter que dans la notation des nombres surréels, il est d'usage de ne pas écrire \emptyset , mais de laisser la zone vide, et ne de pas mettre les accolades pour les singletons (ni même parfois pour des ensembles plus grand, les parenthèse et le \mid servant de séparateur)).

Nous noterons les nombres surréels par des lettres minuscules et les ensembles de nombres surréels par des lettres majuscules, par exemple $x = \{X_g \mid Y_d\}$.

Règle 2) aucun élément de l'ensemble Droit ne peut être plus petit ou égal à un élément de l'ensemble Gauche ($\forall x \forall y ((x \in X_g) \wedge (y \in X_d)) \Rightarrow (y \not\leq x)$). Parmi les exemples donnés ci-dessus, ceux ou intervient \emptyset , vérifient effectivement cette règle, pour le dernier, il faudrait savoir ce que veut dire "plus petit ou égal" pour des nombres surréels.

Règle 3) un nombre surréel x est plus petit ou égal à un surréel y si et seulement si aucun élément de l'ensemble Gauche de x n'est plus grand ou égal à y , et aucun élément de l'ensemble Droit de y n'est plus petit ou égal à x . c'est à dire :

$$\forall x \forall y ((x \leq y) \Leftrightarrow (\forall x_g (x_g \in X_g \Rightarrow (y \not\leq x_g)) \wedge \forall y_d (y_d \in Y_d \Rightarrow (y_d \not\leq x))))$$

Vérifions que les nombres déjà cités sont bien (ou non) des nombres surréels valides.

$\{\mid\}$: il est clair qu'aucun élément de l'ensemble vide ne vérifie une propriété donnée, ce nombre est donc bien un surréel valide.

Pour la même raison (l'ensemble vide vérifie les propositions universelles, mais pas les existentielles), les nombres notés $\{X_g \mid \}$ et $\{\mid X_d\}$ sont des surréels valides.

En particulier $\{0 \mid \}$ et $\{\mid 0\}$, c'est à dire 1 et -1, sont des nombres surréels valides.

On peut vérifier facilement que $\{\mid\} \leq \{\mid\}$, c'est à dire que $0 \leq 0$, et donc que $\{0 \mid 0\}$ est invalide (il faut se souvenir que $\{0 \mid 0\}$ est une abréviation de $\{\{0\} \mid \{0\}\}$).

On peut aussi vérifier que $0 \leq 1$, et $-1 \leq 0$

Ensembles de Nombres

On peut aussi démontrer que $\{-1 \mid 1\} \leq 0$, et que $0 \leq \{-1 \mid 1\}$, c'est à dire, par définition que $\{-1 \mid 1\} = 0$, d'une façon plus générale, par définition :

$$\forall x \forall y ((x = y) \Leftrightarrow ((x \leq y) \wedge (y \leq x)))$$

Ayant démontré que $0 \leq 0$, nous avons donc démontré que $0 = 0$.

Les plus mathématiciens parmi les lecteurs pourront vérifier que la relation $=$ est bien une relation d'équivalence, et retrouver la définition habituelle de l'égalité en passant au quotient.

On peut remarquer qu'ajouter ou retirer un élément à X_g (resp. X_d) qui n'est pas le plus grand (resp. petit) de X_g (resp. X_d) ne modifie pas le nombre surréel $\{X_g \mid X_d\}$.

Par exemple $\{-5, -2, 0 \mid \{2, 5, 9\}\} = \{\{0\} \mid \{2\}\}$

Quelques exemples de nombres réels identifiés à des nombres surréels (pour n un entier positif) :

$0 = \{\mid\}$		$\frac{1}{2} = \{0 \mid 1\}$
$1 = \{0 \mid\}$	$-1 = \{\mid 0\}$	$\frac{3}{2} = \{1 \mid 2\}$
$2 = \{1 \mid\}$	$-2 = \{\mid -1\}$	$\frac{1}{4} = \{0 \mid \frac{1}{2}\}$
$\dots = \dots$	$\dots = \dots$	$\frac{1}{3} = \{\{\frac{0}{2}, \frac{1}{4}, \frac{2}{8} \dots \frac{a_n}{2^n} \dots\} \mid \{\{\frac{1}{2}, \frac{2}{4}, \frac{3}{8} \dots \frac{a_n+1}{2^n} \dots\}\}\}$
$n + 1 = \{n \mid\}$	$-(n + 1) = \{\mid -n\}$	$\pi = \{\{u_n\} \mid \{v_n\}\}$

Dans la définition de $\frac{1}{3}$, il y a des répétitions dans les ensembles gauche et droit, mais c'est sans importance, et $a_n = e(\frac{2^n}{3})$, où $e(x)$ est la partie entière de x .

Dans la définition de π , u_n peut être n'importe quelle suite tendant vers π , et ne prenant que des valeurs **dyadiques** inférieures à π , et v_n peut être n'importe quelle suite tendant vers π , et ne prenant que des valeurs **dyadiques** supérieures à π .

Les **nombres dyadiques** étant denses dans \mathbb{R} , on voit bien que tous les réels sont des surréels que l'on peut construire avec les **dyadiques**, qui eux mêmes sont construits à partir des entiers (qui eux-mêmes sont construits à partir de 0, et in fine, à partir de \emptyset).

Une fois tous les réels définis, on peut définir π comme ci-dessus en supprimant la condition que les éléments des ensembles Gauche et Droit sont **dyadiques**.

Quelques exemple de surréels infiniment grands ou infiniment petits.

$\omega = \{\{0, 1, 2, \dots\} \mid\}$
$\omega + 1 = \{\omega \mid\}$
$\omega - 1 = \{\{0, 1, 2, \dots\} \mid \omega\}$
$\sqrt{\omega} = \{\{1, 2, 3, \dots\} \mid \{\omega, \frac{\omega}{2}, \frac{\omega}{3}, \dots\}\}$
$\omega^2 = \{\{\omega, 2\omega, 3\omega, \dots\} \mid\}$
$\varepsilon = \{0 \mid \{1, \frac{1}{2}, \frac{1}{3}, \dots\}\}$

On peut vérifier facilement que ω est plus grand que tous les entiers (un infiniment grand), et que ε est plus petit que tous les $\frac{1}{n}$ (un infiniment petit).

V.2.4 Table de multiplication

Quelques définitions dont nous allons avoir besoin, soit x et y des nombres ainsi que X et Y des ensembles de nombres :

$x + Y = \{x + y \mid y \in Y\}$
$x \times Y = \{x \times y \mid y \in Y\}$
$X \times Y = \{x \times y \mid (x \in X) \wedge (y \in Y)\}$
En particulier
$\emptyset + X = \emptyset$
$\emptyset \times X = \emptyset$

$x + y = \{(X_g + y) \cup (x + Y_g) \mid (X_d + y) \cup (x + Y_d)\}$
$x \times y = \{(X_g \times y + x \times Y_g - X_g \times Y_g) \cup (X_d \times y + x \times Y_d - X_d \times Y_d) \mid (X_g \times y + x \times Y_d - X_g \times Y_d) \cup (X_d \times y + x \times Y_g - X_d \times Y_g)\}$
$-x = \{-X_d \mid -X_g\}$

Quelques démonstrations détaillées (en faisant apparaître les ensembles pour améliorer la compréhension de la démarche) afin de se familiariser avec les surréels et surtout pour vérifier le bien-fondé des notations adoptées.

$$0 + 2 = 2$$

1	$0 + 2 = \{\emptyset \mid \emptyset\} + \{\{1\} \mid \emptyset\}$
2	$0 + 2 = \{(\emptyset + 2) \cup (0 + \{1\}) \mid (\emptyset + 2) \cup (0 + \emptyset)\}$
3	$0 + 2 = \{0 + \{1\} \mid \emptyset\} = \{0 + 1 \mid \emptyset\}$
4	$0 + 2 = \{1 \mid \} = 2$

1. Par définition de 0 et de 2
2. En appliquant la définition de la somme
3. En appliquant les règles de calculs déjà vues
4. Il reste à démontrer $0 + 1 = 1$, cette partie est laissée au lecteur qui prendra soin de ne pas tomber dans un petit (très petit) piège.

$$0 \times x = 0$$

$0 \times x = \{\emptyset \mid \emptyset\} \times \{X_g \mid X_d\}$
$0 \times x = \{(\emptyset \times x + 0 \times X_g - \emptyset \times X_g) \cup (\emptyset \times x + 0 \times X_d - \emptyset \times X_d) \mid (\emptyset \times x + 0 \times X_d - \emptyset \times X_d) \cup (\emptyset \times x + 0 \times X_g - \emptyset \times X_g)\}$
$0 \times x = \{\emptyset \mid \emptyset\}$
$0 \times x = 0$

$$1 \times 2 = 2$$

$1 \times 2 = \{\{0\} \mid \emptyset\} \times \{\{1\} \mid \emptyset\}$
$1 \times 2 = \{(\{0\} \times 2 + 1 \times \{1\} - \{0\} \times \{1\}) \cup (\emptyset \times 2 + 1 \times \emptyset - \emptyset \times \emptyset) \mid (\{0\} \times 2 + 1 \times \emptyset - \{0\} \times \emptyset) \cup (\emptyset \times 2 + 1 \times \{1\} - \emptyset \times \{1\})\}$
$1 \times 2 = \{\{1 \times 1\} \mid \emptyset\}$ (et en admettant que $1 \times 1 = 1$ soit déjà démontré)
$1 \times 2 = 2$

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

$$\begin{aligned}
 2 \times \frac{1}{2} &= \{\{1\} \mid \emptyset\} \times \{\{0\} \mid \{1\}\} \\
 2 \times \frac{1}{2} &= \{(\{1\} \times \frac{1}{2} + 2 \times \{0\} - \{1\} \times \{0\}) \cup (\emptyset \times \frac{1}{2} + 2 \times \{1\} - \emptyset \times \{1\}) \\
 &\quad \mid (\{1\} \times \frac{1}{2} + 2 \times \{1\} - \{1\} \times \{1\}) \cup (\emptyset \times \frac{1}{2} + 2 \times \{0\} - \emptyset \times \{0\})\} \\
 2 \times \frac{1}{2} &= \{\{\frac{1}{2}\} + \{0\} - \{0\}\} \mid \{\{\frac{1}{2}\} + \{2\} - \{1\}\} \\
 2 \times \frac{1}{2} &= \{\{\frac{1}{2}\} \mid \{\frac{3}{2}\}\} = \{\{0\} \mid \emptyset\} \text{ dernière égalité à démontrer} \\
 2 \times \frac{1}{2} &= 1
 \end{aligned}$$

On pourrait aussi démontrer (mais c'est un peu plus long) que $\omega \times \varepsilon = 1$.

V.2.5 Propriétés algébriques

$(\mathbf{No}, +, \times)$ est un corps totalement ordonné non archimédien (\mathbf{No} contient (par isomorphisme) tous les corps totalement ordonnés).

$(\mathbf{No}, +, \times)$ est un corps réel clos (\mathbf{No} contient une copie (par isomorphisme) de tout corps réel clos).

Un corps réel clos est un corps totalement ordonné tel que, tout élément positif est un carré, et tout polynôme de degré impair admet au moins une racine (il y a beaucoup de définitions équivalentes).

Une chose importante à propos des corps réels clos : ils admettent l'élimination des quantificateurs.

Du point de vue de la théorie des ensembles NBG, \mathbf{No} est une classe propre et non un ensemble.

Si c'était le cas (\mathbf{No} |) serait un nombre surréels valide dont on peut démontrer qu'il ne serait pas égal à lui-même. ...

V.2.6 Synonymes, Isomorphismes, Exemples

Gonsior définit un nombre surréel comme une application d'un ordinal dans un ensemble de cardinal 2 (y compris l'application vide), donc des suites (généralisées) d'éléments choisis parmi deux.

L'ensemble de cardinal 2 usuellement utilisé est $\{-, +\}$, mais on trouve parfois $\{1, \downarrow\}$

De la même façon que pour la définition par des coupures, on peut identifier les entiers assez facilement :

$$\begin{aligned}
 0 &= \emptyset \\
 1 &= \{+\} \\
 2 &= \{++\} \\
 -1 &= \{-\} \\
 -2 &= \{--\} \\
 &\text{etc.}
 \end{aligned}$$

Les réels **dyadiques** sont représentés par des suites finies. Par exemple :

$$\{++++-+-\} = 3 - \frac{1}{2} + \frac{1}{4} + \frac{1}{8} - \frac{1}{16} = \frac{45}{16}$$

Les autres réels sont obtenus pas des suites de domaine ω

Avec cette nouvelle définition, on peut démontrer un théorème qui permet d'associer à chaque nombre surréel, deux ensembles de nombres surréels, correspondant aux ensemble Gauche et Droit de la définition par des coupures.

Alling ne définit pas l'ensemble des nombres surréels mais une axiomatique : $(\mathbf{No}, <, b)$ est un système de nombres surréels si :

1. $(\mathbf{No}, <)$ est un ordre total.
2. $b : \mathbf{No} \mapsto \mathbf{On}^{72}$ est surjective (b est appelé fonction Anniversaire, Birthday en anglais)
3. Pour tous sous-ensembles A et B de \mathbf{No} tels que $\forall x \forall y ((x \in A) \wedge (y \in B)) \Rightarrow (x < y)$, il existe un unique $z \in \mathbf{No}$, tel que $b(z)$ soit minimal et $\forall x \forall y ((x \in A) \wedge (y \in B)) \Rightarrow (x < z < y)$
4. De plus si α est un ordinal tel que $b(x) \leq \alpha$ pour tous les éléments de A et de B, alors $b(z) \leq \alpha$

L'axiome 3 permet d'associer à chaque nombre surréel, deux ensembles de nombres surréels, correspondant aux ensemble Gauche et Droit de la définition par des coupures.

72. \mathbf{On} désigne la classe des ordinaux

V.2.7 Utilisation en physique

Théorie des jeux.

Surreal numbers can be a basis for the Feynman checkerboard representation of the many-worlds of sum-over-histories quantum field theory.

V.2.8 Références

1. J. H. Horton, *On Numbers and Games*, A.K. Peters, Massachusetts, 2nde édition 2001.
2. D. E. Knuth, *Comment deux anciens étudiants découvrirent les mathématiques pures et vécutent heureux.*, Addison Wesley Publishing Company, 1974. (Un document indispensable, qui est un magnifique morceau de mathématiques).
3. H. Gonshor, *An Introduction to the Theory of Surreal Numbers*, London Mathematical Society Lecture Note Series, 1986.
4. H. Gonshor, [Les 10 premières pages gratuites du texte de Gonshor.](#)
5. N. L. Alling, *Foundations of Analysis over Surreal Number Fields*, North-Holland, Mathematics studies, Amsterdam, 1987.
6. P. Ehrlich, *An alternative construction of Conway's surreal numbers*, Algebra Universalis, Volume 25, Number 1, p. 7-16, 1988.
7. C. Tøndering, *Surreal Numbers – An Introduction*, 2005 (Un document clair et assez complet).
8. M. Hollingworth, *Surreal Numbers*, University of Liverpool, 2001 (Une présentation à partir d'un jeu).

V.3 Superréels \mathfrak{R} (David Tall)

V.3.1 Introduction

L'ensemble des Superréels dont il est question ici, et qui sera noté \mathfrak{R} dans la suite de ce document, est dû à [David Tall](#) et ne doit pas être confondu avec l'ensemble des [Super-réels dus à H. Garth Dales et W. Hugh Woodin](#).

V.3.2 Définition

L'idée fondatrice de \mathfrak{R} est de prolonger l'ensemble des [réels](#) avec des [infinitésimaux](#), afin de construire un cadre pour le calcul différentiel qui soit simple, efficace et intuitif.

Pour rappel : ε est un infinitésimal positif si $\varepsilon > 0$ et $\forall x \in \mathbb{R}^+$ ($\varepsilon < x$) (sous réserve de donner une définition de la relation d'ordre), il va de soi que pour donner un cadre utilisable pour le calcul différentiel, il est nécessaire de pouvoir effectuer les calculs algébriques, et donc être capable de donner un sens à des expressions du genre : $\frac{\varepsilon^3 + 4\varepsilon - 5\varepsilon^{-12}}{\varepsilon^{-5} - 2}$.

On peut tout de suite remarquer que ceci serait très insuffisant, et qu'il faudrait être capable de donner un sens à $\sin(\varepsilon)$, $\ln(\varepsilon)$, e^ε etc.

V.3.3 Mode de construction

Un nombre Superréel est une série formelle prolongée par un nombre fini de puissance négatives :

$\alpha = \sum_{i \in Z} a_i \varepsilon^i$ où Z est un sous-ensemble de \mathbb{Z} fini à gauche, c'est à dire ne contenant qu'un nombre fini d'entiers négatifs et où les $a_i \in \mathbb{R}$.

On peut réécrire la définition de la façon suivante (avec les $a_i \in \mathbb{R}$) : $\alpha = \sum_{i=n}^{\infty} a_i \varepsilon^i$ où $n \in \mathbb{Z}$.

Ou encore (toujours avec les $a_i \in \mathbb{R}$) : $\alpha = a_{-n}\varepsilon^{-n} + \dots + a_{-2}\varepsilon^{-2} + a_{-1}\varepsilon^{-1} + a_0 + a_1\varepsilon + a_2\varepsilon^2 + \dots + a_m\varepsilon^m + \dots$

On remarque que si tous les a_i sont nuls, sauf éventuellement a_0 , alors α est un nombre réel, et donc que $\mathbb{R} \subset \mathfrak{R}$.

A noter que les termes ε^n , où n est strictement positif sont des infinitésimaux, c'est à dire des nombres infiniment petits, alors que si n est strictement négatif il s'agit d'un infiniment grand.

On peut remarquer que $|\mathfrak{R}| = |\mathbb{R}|$, en effet il est facile d'associer à chaque élément de \mathfrak{R} , une application de \mathbb{N} dans \mathbb{R} , on a donc :

$$2^{\aleph_0} \leq |\mathfrak{R}| \leq |\mathbb{R}^{\mathbb{N}}| = |\mathbb{R}|^{|\mathbb{N}|} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \times \aleph_0} = 2^{\aleph_0} \quad (\text{cqfd}).$$

V.3.4 Table de multiplication

L'addition et la multiplication sur \mathfrak{R} sont celles des séries formelles, $(\mathfrak{R}, +, \times)$ est donc un anneau (commutatif), mais contrairement aux séries formelles, tout élément de \mathfrak{R}^* possède un inverse, et donc, en fait $(\mathfrak{R}, +, \times)$ est un corps commutatif.

Pour le calcul de l'inverse de $\alpha = \sum_{i=n}^{\infty} a_i \varepsilon^i$ où $a_n \neq 0$, il "suffit" de remarquer que $\varepsilon^{-n} \cdot \alpha$ est une vraie série formelle ($\varepsilon^{-n} \cdot \alpha \in \mathbb{R}[[\varepsilon]]$) dont le terme de degré 0 est inversible donc admet un inverse qu'il suffit de multiplier par ε^n pour trouver l'inverse de α .

On peut aussi munir \mathfrak{R} d'une relation d'ordre de la façon suivante :

Soit $\alpha = \sum_{i=n}^{\infty} a_i \varepsilon^i$ et $\beta = \sum_{i=m}^{\infty} b_i \varepsilon^i$, si $\alpha \neq \beta$, alors il existe un ou des i tels que $a_i \neq b_i$, et comme l'ensemble des indices est fini à gauche il en existe un (j) qui est le plus petit, alors :

$$\alpha < \beta \Leftrightarrow a_j < b_j$$

On peut vérifier que cette relation d'ordre est compatible avec l'addition et la multiplication par un nombre positif.

Cette définition de la relation d'ordre permet de démontrer que ε est bien un infinitésimal :

$$\forall x((\varepsilon > 0) \wedge ((x \in \mathbb{R}^+) \Rightarrow (\varepsilon < x)))$$

V.3.5 Propriétés algébriques

$(\mathfrak{R}, +, \times, <)$ est un corps commutatif ordonné, non-archimédien (pour tout entier $n(n \times \varepsilon < 1)$)

α est dit infini positif si $\forall x(x \in \mathbb{R} \Rightarrow x < \alpha)$

α est dit infini négatif si $\forall x(x \in \mathbb{R} \Rightarrow x > \alpha)$

α est dit fini dans les autres cas, c'est à dire quand α peut s'écrire $\alpha = \sum_{i=0}^{\infty} a_i \varepsilon^i$, et dans ce cas on peut définir la partie standard de α par $st(\alpha) = a_0$.

Le prédicat st vérifie $st(\alpha + \beta) = st(\alpha) + st(\beta)$ et $st(\alpha \times \beta) = st(\alpha) \times st(\beta)$

Un grand intérêt de \mathfrak{R} est de pouvoir étendre de façon très naturelle une certaine classe de fonctions réelles, plus précisément les fonctions analytiques :

Par exemple pour le sinus, et pour $\alpha \in \mathfrak{R}$:

$$\sin(\alpha) = \alpha - \frac{\alpha^3}{3!} + \frac{\alpha^5}{5!} - \dots + (-1)^n \frac{\alpha^{2n+1}}{(2n+1)!} \dots$$

qui est bien un élément de \mathfrak{R} .

V.3.6 Application

A la question "Quel angle fait un cercle avec sa tangente?", la réponse la plus naturelle est sans doute 0. Or si on trace deux cercles tangents intérieurement et la tangente commune, on peut zoomer autant que l'on veut, les deux portions de cercles sont toujours distinctes.

Plus précisément, si l'un des cercles est de diamètre D_1 et l'autre de diamètre D_2 , en prenant comme origine le point de tangence et comme axe, la tangente, en coordonnées polaires on a les relations :

$$\sin(\theta) = \frac{\rho}{D} \text{ (le raisonnement usuel consiste à dire que } \lim_{\rho \rightarrow 0} \theta = 0).$$

En utilisant le développement en série entière de la fonction arcsin :

$$\arcsin(x) = x + \frac{x^3}{2 \cdot 3} + \frac{1 \cdot 3 \cdot x^5}{2 \cdot 4 \cdot 5} + \dots + \frac{1 \cdot 3 \cdot 5 \dots (2n-1)x^{2n+1}}{2 \cdot 4 \cdot 6 \dots (2n) \cdot (2n+1)} \dots$$

On obtient, pour une valeur de ρ fixée et pour chacun des deux cercles :

$$\begin{aligned} \theta_1 &= \frac{\rho}{D_1} + \frac{(\frac{\rho}{D_1})^3}{2 \cdot 3} + \frac{1 \cdot 3 \cdot (\frac{\rho}{D_1})^5}{2 \cdot 4 \cdot 5} + \dots + \frac{1 \cdot 3 \cdot 5 \dots (2n-1)(\frac{\rho}{D_1})^{2n+1}}{2 \cdot 4 \cdot 6 \dots (2n) \cdot (2n+1)} \dots \\ \theta_2 &= \frac{\rho}{D_2} + \frac{(\frac{\rho}{D_2})^3}{2 \cdot 3} + \frac{1 \cdot 3 \cdot (\frac{\rho}{D_2})^5}{2 \cdot 4 \cdot 5} + \dots + \frac{1 \cdot 3 \cdot 5 \dots (2n-1)(\frac{\rho}{D_2})^{2n+1}}{2 \cdot 4 \cdot 6 \dots (2n) \cdot (2n+1)} \dots \end{aligned}$$

Et comme la valeur qui nous intéresse correspond à ρ très petit, disons même infinitésimal, on obtient finalement :

$$\theta_1 = \frac{\varepsilon}{D_1} + \frac{\left(\frac{\varepsilon}{D_1}\right)^3}{2 \cdot 3} + \frac{1 \cdot 3 \cdot \left(\frac{\varepsilon}{D_1}\right)^5}{2 \cdot 4 \cdot 5} + \dots + \frac{1 \cdot 3 \cdot 5 \dots (2n-1) \left(\frac{\varepsilon}{D_1}\right)^{2n+1}}{2 \cdot 4 \cdot 6 \dots (2n) \cdot (2n+1)} \dots$$
$$\theta_2 = \frac{\varepsilon}{D_2} + \frac{\left(\frac{\varepsilon}{D_2}\right)^3}{2 \cdot 3} + \frac{1 \cdot 3 \cdot \left(\frac{\varepsilon}{D_2}\right)^5}{2 \cdot 4 \cdot 5} + \dots + \frac{1 \cdot 3 \cdot 5 \dots (2n-1) \left(\frac{\varepsilon}{D_2}\right)^{2n+1}}{2 \cdot 4 \cdot 6 \dots (2n) \cdot (2n+1)} \dots$$

C'est à dire que l'on obtient une mesure pour chacun de ces angles, mesure qui n'est pas un nombre réel, mais un Superréel, on peut d'ailleurs vérifier que le rapport de ces mesures est "à peu près" $\frac{D_2}{D_1}$, ce qui est conforme à l'intuition.

A titre personnel je trouve cette explication pas totalement convainquante pour deux raisons :

- On aurait pu choisir une autre façon de calculer la limite de l'angle (en fonction de ρ , comme ici, mais on aurait pu choisir l'abscisse, la longueur de l'arc ...).
- On attribue à ρ une valeur infinitésimale, ici ε , mais pourquoi pas ε^2 , ou n'importe quel autre infinitésimal?

V.3.7 Utilisation en physique

Le calcul infinitésimal est lourdement utilisé en physique, par conséquent toutes les théories mathématiques permettant de travailler simplement avec des infinitésimaux peuvent intéresser les physiciens.

V.3.8 Références

1. [Site de David Tall à Warwick University](#)
2. [Looking at graphs through infinitesimal microscopes, windows and telescope](#)
3. David Tall, Standard infinitesimal calculus using the superreal numbers. Warwick University (1979).
4. David Tall, Infinitesimals constructed algebraically and interpreted geometrically. Mathematical Education for Teaching 4, 1 34-53 (1981).

V.4 Corps de Levi-Civita \mathcal{R}

V.4.1 Introduction

Le corps de Levi-Civita doit son nom à un mathématicien Italien, Tullio Levi-Civita (1873-1941), c'est un corps qui étend \mathbb{R} avec des quantités infinitésimales.

V.4.2 Définition

Le corps de Levi-Civita, est traditionnellement noté \mathcal{R} , il est défini comme un ensemble de séries formelles où ε représente une quantité infinitésimale positive (c'est à dire un élément strictement plus grand que 0, mais plus petit que tous les réels positifs) :

$$\mathcal{R} = \left\{ \sum_{q \in \mathbb{Q}} a_q \varepsilon^q \mid a_q \in \mathbb{R} \wedge \mathbb{Q} \subset \mathbb{Q} \wedge \mathbb{Q} \text{ est fini à gauche} \right\}$$

Un ensemble X ordonné est dit « fini à gauche » si pour tout élément $x \in X$, l'ensemble des éléments de X plus petits que x est fini.

Une autre façon de définir les ensembles finis à gauche est de les définir comme les images de suites strictement croissantes, finies ou divergentes.

V.4.3 Table de multiplication

Avant de donner les définitions des opérations sur \mathcal{R} , il est nécessaire de faire quelques remarques.

Si X et Y sont deux ensembles finis à gauche tels que $X \subset Y$, si $x = \sum_{q \in X} a_q \varepsilon^q$, alors en posant :

$$\forall q \in Y ((b_q = a_q \Leftrightarrow q \in X) \wedge (b_q = 0 \Leftrightarrow q \notin X)), \text{ on a le résultat trivial } \sum_{q \in X} a_q \varepsilon^q = \sum_{q \in Y} b_q \varepsilon^q.$$

Dans la suite de ce document et pour simplifier la lecture, si X et Y sont deux ensembles finis à gauche tels que $X \subset Y$, nous écrirons que $\sum_{q \in X} a_q \varepsilon^q = \sum_{q \in Y} a_q \varepsilon^q$, en sous-entendant que les coefficients correspondant à des éléments de $Y - X$ sont égaux à 0.

Lemme 1 : Si X et Y sont des ensembles finis à gauche, alors $X \cup Y$ est fini à gauche.

Lemme 2 : Si X et Y sont des ensembles finis à gauche, alors $X + Y = \{x + y \mid (x \in X) \wedge (y \in Y)\}$ est fini à gauche, et chacun de ses éléments ne peut être issu que d'un nombre fini de couples $(x, y) \in X \times Y$.

On définit l'addition de la façon suivante :

$$\text{Soit } x = \sum_{q \in X} a_q \varepsilon^q \text{ et } y = \sum_{q \in Y} b_q \varepsilon^q, \text{ alors : } x + y = \sum_{q \in X \cup Y} (a_q + b_q) \varepsilon^q.$$

On définit la multiplication de la façon suivante :

$$\text{Soit } x = \sum_{q \in X} a_q \varepsilon^q \text{ et } y = \sum_{q \in Y} b_q \varepsilon^q, \text{ alors : } x \times y = \sum_{p \in X, q \in Y} (a_p \cdot b_q) \varepsilon^{p+q}.$$

A noter que la définition précédente ne donne pas une écriture canonique de $x \times y$, dans la mesure où une même valeur de l'exposant peut être atteinte par plusieurs valeurs de p et de q .

V.4.4 Support, λ, \sim, \approx , et Inverse

Le support d'un élément x est le sous-ensemble de \mathbb{Q} , tel que $a_q \neq 0$, il est noté $\text{supp}(x)$.

$\lambda(x)$ est le plus petit élément de $\text{supp}(x)$ si $x \neq 0$, qui existe, puisque $\text{supp}(x)$ est fini à gauche, et $\lambda(0) = \infty$. $\lambda(x)$ représente l'ordre de magnitude de x .

La relation \sim est définie par : $x \sim y \Leftrightarrow \lambda(x) = \lambda(y)$

C'est à dire que deux éléments de \mathcal{R} ont le même ordre de magnitude, c'est une relation d'équivalence.

La relation \approx est définie par : $x \approx y \Leftrightarrow (\lambda(x) = \lambda(y)) \wedge (a_{\lambda(x)} = b_{\lambda(y)})$

C'est à dire que deux éléments de \mathcal{R} ont le même ordre de magnitude, et son identique à cet ordre là, c'est une relation d'équivalence.

On définit la relation d'ordre de la façon suivante : Soit $x = \sum_{q \in X} a_q \varepsilon^q$ et $y = \sum_{q \in Y} b_q \varepsilon^q$, $x \neq y$, alors :

$$x < y \Leftrightarrow (a_{\lambda(x-y)} < b_{\lambda(x-y)}).$$

Cette relation est compatible avec l'addition et la multiplication par un élément plus grand que 0.

On peut aussi remarquer qu'avec cette définition, et pour tout $n : n \times \varepsilon < 1$, c'est à dire que \mathcal{R} n'est pas archimédien.

La démonstration et le calcul de l'inverse dépasse le cadre de ce document, mais on peut la trouver dans le document disponibles sur le net [New Elements of Analysis on the Levi-Civita Field](#).

V.4.5 Propriétés algébriques

Le corps de Levi-Civita, comme son nom l'indique est un corps, de plus il est ordonné non archimédien.

L'injection $\pi : \mathbb{R} \mapsto \mathcal{R}$ définie par $\pi(x) = x\varepsilon^0$, permet de plonger canoniquement $(\mathbb{R}, +, \times)$ dans $(\mathcal{R}, +, \times)$. C'est le plus petit corps contenant \mathbb{R} , non archimédien et complet (au sens de Cauchy).

V.4.6 Synonymes, Isomorphismes, Exemples

Il aurait aussi été possible de définir \mathcal{R} sans introduire une quantité infinitésimale, mais à l'aide de fonctions :

$$\mathcal{R} = \{f : \mathbb{Q} \mapsto \mathbb{R} \mid \{x \mid f(x) \neq 0\} \text{ est fini à gauche} \}.$$

A partir de cette définition on peut introduire la notion de support, de $\lambda(x)$, les relations d'équivalence \sim et \approx , puis de définir l'addition la multiplication et la relation d'ordre de façon naturelle, afin de retrouver les définitions précédentes.

Il est possible d'étendre le corps de Levi-Civita en un corps algébriquement clos en prenant les coefficients dans \mathbb{C} à la place de \mathbb{R} .

V.4.7 Utilisation en physique

Le calcul infinitésimal est lourdement utilisé en physique, par conséquent toutes les théories mathématiques permettant de travailler simplement avec des infinitésimaux peuvent intéresser les physiciens.

V.4.8 Références

1. [Levi-Civita theory for irrotational water waves in a one-dimensional channel and the complex Korteweg-de Vries equation](#).
2. M. Berz. Analysis on a Nonarchimedean Extension of the Real Numbers. Lecture Notes, 1992 and 1995 Mathematics Summer Graduate Schools of the German National Merit Foundation. MSUCL-933, Department of Physics, Michigan State University, 1994
3. Tullio Levi-Civita. Sugli infiniti ed infinitesimi attuali quali elementi analitici. Atti Ist. Veneto di Sc., Lett. ed Art., 7a, 4 :1765, 1892.
4. Tullio Levi-Civita. Sui numeri transfiniti. Rend. Acc. Lincei, 5a, 7 :91,113, 1898.
5. Khodr Shamseddine, [Analysis on the Levi-Civita Field : A Brief Overview](#).
6. Khodr Shamseddine, [New Elements of Analysis on the Levi-Civita Field](#)
7. D'une façon générale on peut consulter le site de [Khodr Shamseddine](#).

VI Théorie des ensembles ZF(C)

Introduction

Les deux sous-sections suivantes, traitant des **ordinaux** et des **cardinaux**, se placent dans le cadre de la théorie des ensembles ZF. L'axiome du choix n'est pas nécessaire pour la définition des **ordinaux**, par contre il est essentiel pour les **cardinaux**.

VI.1 Ordinaux *Ord*

VI.1.1 Introduction

Les nombres ordinaux constituent une généralisation, due originellement à G. Cantor, de la suite des entiers naturels au-delà du fini et jouent un rôle important dans la théorie des ensembles. Notamment, la récurrence transfinie permet de construire de nouveaux objets mathématiques. La construction suivante est due à Von Neumann.

VI.1.2 Définitions

Définition : Un ensemble bien ordonné A est transitif si tout élément d'un élément de A est lui-même un élément de A . Autrement dit, A est transitif si $a \in A$ entraîne $a \subset A$.

Par exemple, l'ensemble vide est transitif. De plus, si A est transitif, alors $s(A) = A \cup \{A\}$ est aussi transitif. Par conséquent, tous les entiers naturels, construits comme dans la **section synonymes des entiers naturels**, sont transitifs. L'ensemble des entiers naturels \mathbb{N} est lui aussi transitif.

Définition : Un ordinal est un ensemble transitif α tel que la relation \in soit un bon ordre strict sur α .

VI.1.3 Mode de construction

Les exemples précédents (l'ensemble vide, les entiers naturels (\mathbb{N})) sont des ordinaux. De plus, le successeur $s(\alpha) = \alpha \cup \{\alpha\}$ d'un ordinal α est aussi un ordinal. La classe des ordinaux est notée *Ord* (ou aussi *On*). D'après le théorème de Burali-Forti, ce n'est pas un ensemble (au sens de ZF).

Une propriété fondamentale des ordinaux affirme que si α, β sont des ordinaux, on a $\alpha \subsetneq \beta$ ou $\alpha = \beta$ ou $\beta \subsetneq \alpha$. On définit une relation d'ordre $<$ sur *Ord* par $\alpha < \beta \Leftrightarrow \alpha \subsetneq \beta$. C'est un bon ordre sur *Ord* qui généralise l'ordre usuel sur \mathbb{N} .

Les ordinaux permettent aussi de définir un principe d'induction (ou récurrence transfinie) généralisant la récurrence des entiers naturels : si \mathcal{P} est une propriété portant sur les ordinaux et telle que si $\mathcal{P}(\beta)$ est vraie pour tout $\beta < \alpha$ implique que $\mathcal{P}(\alpha)$ est aussi vraie, alors la propriété \mathcal{P} est vraie pour tout ordinal.

VI.1.4 Table de multiplication

Le successeur d'un ordinal, $s(\alpha) = \alpha \cup \{\alpha\}$, sera noté α^+ .

Un ordinal α tel qu'il existe un ordinal β tel que $\alpha = \beta^+$ est appelé *ordinal successeur* ; si $\alpha \neq 0$ n'est pas un ordinal successeur il est dit *ordinal limite*.

Par exemple $\omega = \bigcup_{n \in \mathbb{N}} n$ est un ordinal limite, c'est d'ailleurs le plus petit.

Définition de l'addition :

- $\alpha + 0 = \alpha$
- $\alpha + \beta^+ = (\alpha + \beta)^+$
- $\alpha + \lambda = \lim_{\beta < \lambda} (\alpha + \beta)$ Si λ est un ordinal limite

On a donc que le successeur d'un ordinal, $s(\alpha) = \alpha \cup \{\alpha\} = \alpha + 1$.

Définition de la multiplication :

- $\alpha \cdot 0 = 0$
- $\alpha \cdot \beta^+ = \alpha \cdot \beta + \alpha$
- $\alpha \cdot \lambda = \lim_{\beta < \lambda} (\alpha \cdot \beta)$ Si λ est un ordinal limite

Ces définition permettent de définir une division euclidienne sur les nombres ordinaux :

$$\forall \alpha \in \text{Ord} \forall \beta \in \text{Ord} \setminus \{0\} \exists ! (\sigma, \rho) \in \text{Ord} ((\alpha = \beta \cdot \sigma + \rho) \wedge (\rho < \beta)).$$

Définition de l'exponentiation :

- $\alpha^0 = 1$
- $\alpha^{\beta^+} = \alpha^\beta \cdot \alpha$
- $\alpha^\lambda = \lim_{\beta < \lambda} (\alpha^\beta)$ Si λ est un ordinal limite

† Attention, l'exponentiation ordinaire n'est pas compatible avec l'exponentiation **cardinale**.

† Par exemple $2^\omega = \lim_{n < \omega} (2^n) = \omega$, dont le cardinal est \aleph_0 qui est strictement plus petit que 2^{\aleph_0} .

VI.1.5 Propriétés algébriques

Ainsi définie, l'addition est associative et admet 0 pour élément neutre. $(\text{Ord}, +)$ est donc un monoïde. De plus l'addition est régulière à gauche $((\alpha + \beta = \alpha + \gamma) \Rightarrow (\beta = \gamma))$.

Par contre, l'addition n'est pas commutative : si ω désigne l'ordinal (\mathbb{N}, \in) , alors on a $1 + \omega = \omega \neq \omega + 1$.

On peut noter que l'ordinal $\alpha + 1 = \alpha^+$ est le successeur de α .

En appliquant la définition, on obtient :

$$\begin{array}{rclcl} \omega + 1 & = & (\omega + 0)^+ & = & \omega^+ \\ 1 + \omega & = & \lim_{n < \omega} (1 + n) & = & \omega \quad \text{Or } \omega \neq \omega^+ \end{array}$$

La multiplication admet 1 pour élément neutre et 0 pour élément absorbant. Elle est associative. Elle est distributive à gauche par rapport à l'addition (on a $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$ pour tout ordinaux α, β et γ) mais n'est pas distributive à droite par rapport à l'addition : par exemple, on a $(1 + 1) \cdot \omega = \omega \neq \omega + \omega$. Le même exemple montre que la multiplication \cdot n'est pas régulière à droite, mais elle est régulière à gauche $((\alpha \neq 0) \wedge (\alpha \cdot \beta = \alpha \cdot \gamma)) \Rightarrow (\beta = \gamma)$.

Cependant, elle n'est pas commutative : par exemple, $2 \cdot \omega = \omega \neq \omega \cdot 2$.

En appliquant la définition, on obtient :

$$\begin{array}{rclcl} \omega \cdot 2 & = & (\omega \cdot 1) + \omega & = & \omega + \omega \\ 2 \cdot \omega & = & \lim_{n < \omega} (2 \cdot n) & = & \omega \quad \text{Or } \omega \neq \omega + \omega \end{array}$$

L'exponentiation possède les propriétés suivantes :

$$\begin{array}{rcl} \alpha^1 & = & \alpha \\ 1^\alpha & = & 1 \\ \alpha^\mu \cdot \alpha^\nu & = & \alpha^{\mu+\nu} \\ (\alpha^\mu)^\nu & = & \alpha^{\mu \cdot \nu} \end{array}$$

VI.1.6 Exemple d'utilisation : les suites de Goodstein

L'écriture d'un entier naturel n non nul en base p itérée, où p est un entier naturel supérieur ou égal à 2, est l'écriture de n obtenue en écrivant n dans la base p puis en remplaçant les entiers apparaissant dans cette décomposition par leur propre décomposition dans la base p , et en itérant le procédé jusqu'à obtenir une écriture n'utilisant que les entiers compris entre 1 et $p - 1$. Par exemple, $26 = 2^4 + 2^3 + 2 = 2^{2^2} + 2^{2^1+1} + 2^1$ est la décomposition de 26 en base 2 itérée.

On définit les suites de Goodstein de la manière suivante : si p et q sont deux entiers naturels vérifiant $p \geq q \geq 2$, l'application $f_{p,q} : \mathbb{N} \rightarrow \mathbb{N}$ définie par $f_{p,q}(0) = 0$ et si n est non nul $f_{p,q}(n)$ est le nombre obtenu en écrivant n en base p itérée et en remplaçant toutes les occurrences de p par q .

La suite de Goodstein $(g_n(a))_{n \geq 2}$ de premier terme $a \in \mathbb{N}$ est la suite définie par

$$g_p : \mathbb{N} \mapsto \mathbb{N} \begin{cases} g_2(a) & = & a \\ g_{p+1}(a) & = & f_{p,p+1}(g_p(a)) - 1 \\ g_{p+1}(a) & = & 0 \end{cases} \quad \begin{matrix} \Leftrightarrow & g_p(a) \neq 0 \\ \Leftrightarrow & g_p(a) = 0 \end{matrix}$$

Par exemple la suite de Goodstein commençant par 3 donne :

$$\begin{aligned} g_2(3) &= 3 & &= 2^1 + 2^0 \\ g_3(3) &= (3^1 + 3^0) - 1 & &= 3^1 \\ g_4(3) &= (4^1) - 1 & &= 3 \cdot 4^0 \\ g_5(3) &= (3 \cdot 5^0) - 1 & &= 2 \cdot 5^0 \\ g_6(3) &= (2 \cdot 6^0) - 1 & &= 1 \cdot 6^0 \\ g_7(3) &= (1 \cdot 7^0) - 1 & &= 0 \end{aligned}$$

Le calcul des premiers termes de la suite donne l'impression que la suite est croissante et tend très rapidement vers l'infini.

Pour information, la suite de Goodstein commençant par 4 nécessite environ $6.895 \times 10^{121210694}$ étapes pour arriver à 0.

Cependant, le théorème de Goodstein affirme que, pour tout entier a , la suite de Goodstein associée converge vers 0. L'intérêt de ce théorème est avant tout logique : on peut définir les suites de Goodstein à partir de l'axiomatique de Peano, mais dans une telle axiomatique, le théorème de Goodstein est en fait une proposition indécidable. Il existe donc des modèles de l'axiomatique de Peano où le théorème est vrai (par exemple dans tous les modèles de ZF, puisque ZF permet de démontrer le théorème de Goodstein) et d'autres où il est faux.

VI.1.7 Un exemple d'utilisation en topologie

Si (X, \mathcal{O}) est un espace topologique, A une partie de X , on appelle fermeture de A le plus petit fermé contenant A et on le note \bar{A} . L'ensemble des limites des suites d'éléments de A est appelée fermeture séquentielle de A et se note $cl(A)$. On a $A \subset cl(A) \subset \bar{A}$ et les inclusions sont strictes en général. On a toujours $\overline{\bar{A}} = \bar{A}$ mais pas nécessairement $cl(cl(A)) = cl(A)$. Si β est un ordinal, on définit $cl^\beta(A) = cl(\bigcup_{\alpha < \beta} cl^\alpha(A))$. L'ordre séquentiel de (X, \mathcal{O}) est le plus petit ordinal vérifiant $cl^\beta(A) = cl^{\beta+1}(A)$ pour toute partie A de X . On le note $\sigma(X)$

Par exemple, si X est muni de la topologie discrète, alors $\sigma(X) = 0$ et si (X, d) est un espace métrique (induisant une topologie qui n'est pas la topologie discrète), alors $\sigma(X) = 1$. On a toujours $\sigma(X) < \omega_1$ (où ω_1 désigne le plus petit ordinal non dénombrable).

On peut construire un espace topologique pour lequel l'ordre séquentiel est un ordinal non fini. Par exemple, la topologie radiale est la topologie de \mathbb{R}^2 dont les fermés sont exactement les parties de \mathbb{R}^2 dont l'intersection avec toute droite D est un fermé de D . Son ordre séquentiel est $\omega = (\mathbb{N}, \in)$.

VI.1.8 Forme Normale de Cantor

Cantor a démontré que pour tout ordinal α , il existe une suite finie unique strictement décroissante d'ordinaux $\alpha_0 > \alpha_1 > \dots > \alpha_k$ et une suite finie unique d'entiers non nuls (n_0, n_1, \dots, n_k) tels que

$$\alpha = \omega^{\alpha_0} \cdot n_0 + \omega^{\alpha_1} \cdot n_1 + \dots + \omega^{\alpha_k} \cdot n_k$$

Cette écriture de α est appelé la Forme Normale de Cantor.

On peut noter que la Forme Normale de Cantor est assez triviale pour certains ordinaux qui vérifient $\varepsilon = \omega^\varepsilon$ (par exemple la limite de $\omega^{\omega^{\omega^{\dots}}}$), le plus petit de ces ordinaux est noté ε_0 qui a une certaine importance en logique, par exemple Gentzen a montré que la récurrence jusqu'à ε_0 permet de démontrer la consistance de l'arithmétique de Peano.

On peut utiliser la Forme Normale de Cantor pour simplifier les additions et multiplications d'ordinaux, pour cela nous avons besoin de quelques résultats préliminaires :

Soit α et β deux ordinaux et m et n deux entiers, alors :

$$\omega^\alpha \cdot n + \omega^\beta \cdot m = \begin{cases} 1. & \omega^\beta \cdot m & \Leftrightarrow & \alpha < \beta \\ 2. & \omega^\alpha (n + m) & \Leftrightarrow & \alpha = \beta \\ 3. & \omega^\alpha \cdot n + \omega^\beta \cdot m & \Leftrightarrow & \alpha > \beta \end{cases}$$

Dans le cas 3, l'ordinal somme est déjà en Forme Normale de Cantor.

Soit α un ordinal en Forme Normale de Cantor $\alpha = \omega^{\alpha_0} \cdot n_0 + \omega^{\alpha_1} \cdot n_1 + \dots + \omega^{\alpha_k} \cdot n_k$, β un ordinal et n et m des entiers.

1. $\alpha \cdot n = \omega^{\alpha_0} \cdot n_0 \cdot n + \omega^{\alpha_1} \cdot n_1 + \dots + \omega^{\alpha_k} \cdot n_k$
2. $\alpha \cdot (\omega^\beta \cdot m) = \omega^{\alpha_1 + \beta} \cdot m$

Dans le cas 1, notez que seul le premier coefficient de α est multiplié par l'entier n .

Ces résultats, plus l'associativité de l'addition et de la multiplication et plus la distributivité à gauche de la multiplication sur l'addition permettent de calculer la somme et le produit d'ordinaux en Forme Normale de Cantor.

Prenons quelques exemples :

$$(\omega^\omega + \omega^5 + \omega^3 \cdot 5 + \omega^2 \cdot 456 + 12) + (\omega^3 \cdot 2 + \omega + 3) = \omega^\omega + \omega^5 + \omega^3 \cdot 7 + \omega + 3$$

On remarquera que tous les termes du premier opérande dont l'exposant est strictement plus petit que le plus grand exposant du second opérande ont disparu.

Soit à calculer $(\omega^{\omega+2} + \omega^\omega + \omega) \cdot (\omega^{\omega+1} + \omega^\omega + 3)$, en appliquant la distributivité à gauche de la multiplication sur l'addition, on obtient :

$$(\omega^{\omega+2} + \omega^\omega + \omega) \cdot (\omega^{\omega+1} + \omega^\omega + 3) = (\omega^{\omega+2} + \omega^\omega + \omega) \cdot \omega^{\omega+1} + (\omega^{\omega+2} + \omega^\omega + \omega) \cdot \omega^\omega + (\omega^{\omega+2} + \omega^\omega + \omega) \cdot 3$$

En appliquant les règles ci-dessus :

$$\begin{aligned} (\omega^{\omega+2} + \omega^\omega + \omega) \cdot \omega^{\omega+1} &= \omega^{(\omega+2)+(\omega+1)} \\ (\omega^{\omega+2} + \omega^\omega + \omega) \cdot \omega^\omega &= \omega^{(\omega+2)+\omega} \\ (\omega^{\omega+2} + \omega^\omega + \omega) \cdot 3 &= \omega^{\omega+2} \cdot 3 + \omega^\omega + \omega \end{aligned}$$

et finalement

$$\omega^{(\omega+2)+(\omega+1)} + \omega^{(\omega+2)+\omega} + (\omega^{\omega+2} \cdot 3 + \omega^\omega + \omega) = \omega^{\omega \cdot 2 + 1} + \omega^{\omega \cdot 2} + \omega^{\omega+2} \cdot 3 + \omega^\omega + \omega$$

Remarque : le théorème Cantor, ci-dessus, reste vrai dans une version plus générale :

Pour tout ordinal α , et pour tout ordinal $\beta \leq 2$ il existe une suite finie strictement décroissante unique d'ordinaux $\alpha_0 > \alpha_1 > \dots > \alpha_k$ et une suite finie unique d'ordinaux non nuls et strictement plus petit que β ($\eta_0, \eta_1, \dots, \eta_k$) tels que

$$\alpha = \beta^{\alpha_0} \cdot \eta_0 + \beta^{\alpha_1} \cdot \eta_1 + \dots + \beta^{\alpha_k} \cdot \eta_k$$

VI.1.9 Synonymes, Isomorphismes, Exemples

On définit un isomorphisme d'ensembles bien ordonnés comme étant une application bijective préservant l'ordre entre deux ensembles bien ordonnés. Le théorème de représentation (ou de comparaison) affirme que tout ensemble bien ordonné est isomorphe à un unique ordinal. On peut ainsi définir un ordinal comme une classe d'isomorphie d'ensembles bien ordonnés. C'est la définition originelle des ordinaux due à Cantor.

On verra dans le chapitre sur les **cardinaux** que le théorème de Zermelo (équivalent à l'axiome du choix) permet de bien ordonner tous les ensembles.

Avec cette définition, on peut redéfinir une addition, une multiplication et une exponentiation, identique aux définitions précédentes sur *Ord* prolongeant l'addition et la multiplication des entiers naturels.

Si $(A, <)$ et $(B, <)$ sont des représentants des ordinaux α et β respectivement, l'ordinal $\alpha + \beta$ est la classe d'isomorphie de l'ensemble $A \times \{1\} \cup B \times \{2\}$ muni du bon ordre \leq définie par $(a, i) \leq (b, j)$ si et seulement si $(a \leq b$ et $i = j)$ ou $(i = 1$ et $j = 2)$.

Cette addition revient à placer α « après » β .

Avec cette définition alternative, on peut aussi démontrer que $1 + \omega \neq \omega + 1$:

En notant $<$ le bon ordre sur les ordinaux, et en ajoutant des indices sur les éléments pour expliciter leur appartenance :

$$1 + \omega \equiv \{0_1 < 0_\omega < 1_\omega < \dots\}$$

Une bijection croissante de ω dans $1 + \omega$ est facile à trouver.

$$\omega + 1 \equiv \{0_\omega < 1_\omega < \dots < 0_1\}$$

Au contraire il est impossible de trouver une bijection croissante ω dans $\omega + 1$ (ω n'a pas de plus grand élément, contrairement à $\omega + 1$).

Si $(A, <)$ et (B, \prec) sont des représentants des ordinaux α et β respectivement, l'ordinal $\alpha \cdot \beta$ est la classe d'isomorphie de l'ensemble $A \times B$ muni de l'ordre lexicographique inversé (i.e. $(a, b) \prec (a', b')$ si et seulement si $b \prec b'$ ou $(b = b'$ et $a < a')$).

Cette multiplication revient à copier « β » copies de α les unes « derrière » les autres.

Avec les mêmes notation que pour l'addition et des indices significatifs :

$$2 \cdot \omega \equiv \{0_{2_0} < 1_{2_0} < 0_{2_1} < 1_{2_1} < \dots\}$$

Une bijection croissante de ω dans $2 \cdot \omega$ est facile à trouver.

$$\omega \cdot 2 \equiv \{0_{\omega_0} < 1_{\omega_0} < 2_{\omega_0} < \dots < 0_{\omega_1} < 1_{\omega_1} < 2_{\omega_1} < \dots\}$$

Au contraire il est impossible de trouver une bijection croissante ω dans $\omega \cdot 2$ (ω ne contient qu'un seul élément qui n'est pas successeur, alors que $\omega \cdot 2$ en contient 2).

On peut aussi définir une exponentiation sur les bons ordres :

Si $(A, <)$ et (B, \prec) sont des représentants des ordinaux α et β respectivement, l'ordinal α^β est la classe d'isomorphie de l'ensemble $A^{(B)}$ (le sous-ensemble de A^B constitué des suites à support fini) muni du bon ordre \prec définie par $\Phi \prec \Psi$ si et seulement si $(\exists i \in B((\Phi(i) < \Psi(i)) \wedge \forall j \in B((i \prec j) \Rightarrow (\Phi(j) = \Psi(j))))))$.

VI.1.10 Utilisation en physique

Il est peu probable que les ordinaux soient utilisés en physique, sauf, peut-être, en informatique théorique.

VI.1.11 Références

1. Jech T, *Set Theory*, 2nd edition, Springer-Verlag, Heidelberg, 1997.
2. J.L. Krivine, *Théorie des ensembles*, Cassini, 1998.
3. [Théorie des ensembles par P.Dehornoy.](#)
4. [Les ordinaux par P.Dehornoy.](#)
5. [On the Independence of Goodstein's Theorem par Justin T. Miller.](#)

VI.2 Cardinaux *Card*

VI.2.1 Introduction

La notion de Cardinal est due à Georg Cantor, un mathématicien allemand (1845 - 1918), qui est à l'origine de la théorie moderne des ensembles, et surtout de l'étude des infinis ⁷³.

Le « bon » cadre pour définir les cardinaux est ZFC (c'est à dire ZF + Axiome du choix) essentiellement à cause du théorème de Zermelo (cf. infra).

Notons tout de suite qu'une mauvaise façon de se représenter la notion de cardinal est :

« Le cardinal d'un ensemble est son nombre d'éléments ».

La bonne façon de comprendre cette notion est au contraire :

« Le nombre d'éléments d'un ensemble est son cardinal ».

C'est à dire que l'on ne peut pas définir une notion formelle comme le cardinal à partir d'une notion intuitive mais informelle, surtout quand cette intuition n'a de sens que dans le cas fini ; par contre on peut très bien donner un nom qui rappelle l'intuition à une notion définie formellement, même si le cadre formel dépasse le cadre intuitif.

VI.2.2 Définition

1. Pour tout ensemble x on appelle *le cardinal* de x et on note $|x|$, le plus petit ordinal en bijection avec x .
2. Deux ensembles x et y sont dits *équipotents* s'il existe une bijection entre les deux, cette relation sera notée \sim par la suite.
3. Un ordinal est *un cardinal* s'il est son propre cardinal (autrement dit, si $\alpha = |\alpha|$), c'est à dire qu'un cardinal est un ordinal qui ne s'injecte pas dans une de ses parties strictes).

On aurait pu aussi définir un cardinal comme une classe d'équipotence (classe d'équivalence pour la relation d'équipotence), donc sans faire le moins du monde appel à la notion d'ordinal, mais cette définition est bien moins pratique que la précédente, sauf à décider de choisir un représentant particulier dans chaque classe : le plus petit ordinal lui appartenant et on revient à la définition première.

La classe des Cardinaux sera notée *Card*, c'est une classe propre (cf. infra).

$Card(x)$ ⁷⁴, dont la sémantique est « x est un cardinal », est définissable :

$$Card(x) \Leftrightarrow (Ord(x) \wedge \forall y (Ord(y) \wedge x \sim y) \Rightarrow x \leq y)$$

Il est immédiat de vérifier que tous les ordinaux finis sont des cardinaux, et que ω (qui le plus petit ordinal infini) est le plus petit cardinal infini, par contre l'ordinal $\omega + 1$, qui est strictement plus grand que l'ordinal ω , n'est pas un Cardinal.

Nous noterons $Card_\infty$ la classe des cardinaux infinis (qui sont tous des Ordinaux limites).

VI.2.3 Mode de construction

Les Cardinaux sont des **Ordinaux**, on peut donc les construire de la même façon que les Ordinaux, mais à condition de rejeter les Ordinaux qui s'injectent dans un ordinal strictement plus petit.

Notons d'abord que le successeur d'un cardinal κ est le plus petit cardinal strictement plus grand que κ , il est noté κ^+ . Un Cardinal qui n'est successeur d'aucun Cardinal est appelé *Cardinal limite* (selon les auteurs 0 est considéré comme Cardinal limite ou non (ce qui revient à réserver cette qualification aux Cardinaux infinis)) ; on peut noter que tous les Cardinaux infinis sont des Ordinaux limites, mais qu'il existe des Ordinaux limites qui ne sont pas des Cardinaux ($\omega + \omega$, par exemple).

On peut aussi construire un isomorphisme, généralement noté \aleph entre *Ord* et $Card_\infty$:

$$\begin{aligned} \aleph_0 &= \omega \\ \aleph_{\alpha+1} &= (\aleph_\alpha)^+ \\ \aleph_\beta &= \sup_{\alpha < \beta} \aleph_\alpha \text{ (Si } \beta \text{ est un ordinal limite)} \end{aligned}$$

Le cardinal \aleph_α est appelé α -ème *aleph*. Un résultat important affirme que tout cardinal infini est un aleph.

⁷³. Hilbert : « Personne ne pourra nous chasser du paradis que Cantor a créé. »

⁷⁴. On ne peut pas écrire $x \in Card$

VI.2.4 Arithmétique cardinale

On peut définir, sur la classe des Cardinaux, un successeur, une addition, une multiplication et une exponentiation, mais attention, ces opérations ne coïncident que rarement avec les opérations homologues sur la classe des Ordinaux⁷⁵, et *malheureusement* ces opérations sont notées de la même façon, c'est à dire que, a priori, la notation $\omega + 1$, n'a pas vraiment de sens puisque le résultat n'est pas le même selon que l'on considère qu'il s'agit d'une opération sur les Ordinaux ω et 1 ou sur les Cardinaux ω et 1. Aussi, sauf si le contexte est clair, il est d'usage d'utiliser la notation ω pour les Ordinaux et \aleph pour les Cardinaux, et donc $\omega + 1$ représente la somme des Ordinaux ω et 1, alors que $\aleph_0 + 1$ représente la somme des Cardinaux \aleph_0 et 1, par exemple :

$$1 + \omega = \omega < \omega + 1 \text{ alors que } 1 + \aleph_0 = \aleph_0 + 1 = \aleph_0.$$

Le **successeur** d'un cardinal (déjà défini) κ est le plus petit cardinal plus grand que κ , il est noté κ^+ .

L'**addition** des Cardinaux est définie de la façon suivante (x et y sont des ensembles quelconques) :

$$|x| + |y| = |(x \times \{0\}) \cup (y \times \{1\})|$$

(Ce qui revient à l'union disjointe de x et y).

La **multiplication** des Cardinaux est définie de la façon suivante :

$$|x| \times |y| = |x \times y|$$

L'**exponentiation** des Cardinaux est définie de la façon suivante :

$$|x|^{|y|} = |x^y|$$

(Où x^y désigne l'ensemble des fonctions de y dans x).

Pour les Cardinaux finis, ces opérations coïncident avec les opérations sur les Ordinaux.

Pour κ et λ des Cardinaux dont l'un au moins est infini, les opérations sont triviales :

$$\kappa + \lambda = \kappa \cdot \lambda = \text{Max}(\kappa, \lambda)$$

L'addition des cardinaux est commutative, associative, et admet 0 comme élément neutre. Hormis 0, aucun élément n'admet de symétrique pour l'addition.

La multiplication est commutative, associative, admet 0 comme élément absorbant et 1 comme élément neutre. Elle est distributive par rapport à l'addition.

Les propriétés usuelles des puissances de nombres finis, telles $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$, $(\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}$ et $(\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu$ sont aussi vérifiées par les cardinaux quelconques.

Le cardinal de $\mathfrak{P}(\mathbb{N})$ est 2^{\aleph_0} . Par le théorème de Cantor, ce cardinal est strictement plus grand que \aleph_0 (et donc supérieur ou égal à \aleph_1). Cependant, rien ne permet d'affirmer que $2^{\aleph_0} = \aleph_1$. Plus précisément, cette égalité est appelée *hypothèse du continu*. Kurt Gödel a démontré en 1938 que l'hypothèse du continu est consistante avec la théorie des ensembles ZF et Paul Cohen a montré en 1963 que sa négation était aussi consistante avec la théorie ZF.

L'hypothèse $2^{\aleph_\alpha} = \aleph_{\alpha+1}$, est appelée *hypothèse du continu généralisée*. Les travaux de Gödel et Cohen montrent qu'elle est aussi indécidable dans ZF.

Enfin, l'hypothèse du continu généralisé implique, dans ZF, l'axiome du choix (Waclaw Sierpinski en 1947).

VI.2.5 Propriétés algébriques

La classe des Cardinaux n'est pas un ensemble (comme les ordinaux), ce qui s'illustre bien par le paradoxe de Cantor (cf. infra, avec le théorème de Cantor).

Par définition, deux ensembles x et y sont en bijection si et seulement si $|x| = |y|$. Plus précisément, les trois propositions suivantes sont équivalentes (l'implication 2) \Rightarrow 1) nécessitant l'axiome du choix) :

1. Il existe une injection de x dans y .
2. Il existe une surjection de y sur x .
3. $|x| \leq |y|$.

75. D'une façon générale $\omega_\alpha = \aleph_\alpha$ en tant qu'ensemble, mais les opérations ordinales et cardinales ne coïncident pas.

VI.2.6 Théorèmes et résultats

Avec l'axiome du choix, on peut utiliser le théorème de Zermelo ⁷⁶ : tout ensemble peut être muni d'un bon ordre ; c'est à dire que tout ensemble peut être mis en bijection avec un ordinal, et il suffit de prendre le plus petit (toujours possible avec une famille d'ordinaux) pour obtenir son cardinal ; autrement dit, tout ensemble possède un cardinal, c'est ce résultat qui justifie en tout premier lieu, que le bon cadre pour la définition des Cardinaux est ZFC plutôt que ZF.

Un résultat important est la trichotomie des Cardinaux (avec axiome du choix) :

Soit x et y deux ensembles quelconques, alors une et une seule des propositions suivantes est vérifiée :

1. $|x| < |y|$
2. $|x| = |y|$
3. $|x| > |y|$

Un ensemble de même cardinal que \mathbb{N} (c'est à dire de cardinal \aleph_0) est dit *dénombrable* et un ensemble s'injectant dans \mathbb{N} est dit *au plus dénombrable* ⁷⁷. Quelques résultats sur la comparaison des cardinaux d'ensembles usuels :

1. Un ensemble au plus dénombrable est soit dénombrable soit fini.
2. Une union au plus dénombrable d'ensembles dénombrables est dénombrable. (Ce théorème nécessite l'axiome du choix dénombrable ⁷⁸)
3. \mathbb{N} , toute partie infinie de \mathbb{N} , \mathbb{Z} , \mathbb{N}^n , \mathbb{Q} , l'ensemble des nombres algébriques dans \mathbb{R} , ainsi que l'ensemble des points de discontinuité d'une fonction croissante de \mathbb{R} dans \mathbb{R} sont dénombrables.
4. L'ensemble des polynômes à coefficients dans un anneau dénombrable est dénombrable.
5. Tout ensemble infini contient une partie dénombrable.
6. \mathbb{R} n'est pas dénombrable. Son cardinal est appelé *cardinal ou puissance du continu* et est noté \mathfrak{c} .
7. $\mathfrak{P}(\mathbb{N})$, tout intervalle de \mathbb{R} , $\mathbb{R} \setminus \mathbb{Q}$, \mathbb{C} , \mathbb{R}^n , l'ensemble des fonctions de \mathbb{N} dans $\{0, 1\}$ ont le même cardinal que \mathbb{R} .

Les points 3) et 6) implique en particulier l'existence de nombres transcendants dans \mathbb{R} . En utilisant le point 2), on en déduit même que l'ensemble des nombres transcendants de \mathbb{R} n'est pas dénombrable.

Théorème de Cantor : Ce théorème affirme que l'ensemble des parties d'un ensemble x a un cardinal strictement plus grand que le cardinal de x : $|\mathfrak{P}(x)| = 2^{|x|} > |x|$

Ce théorème permet une autre démonstration du paradoxe de Bertrand : si la classe \mathcal{E} de tous les ensembles était un ensemble, alors les ensembles qui sont des parties de \mathcal{E} seraient des éléments de \mathcal{E} . En particulier, $\mathfrak{P}(\mathcal{E})$ serait inclus dans \mathcal{E} , ce qui contredirait le théorème de Cantor.

Le théorème de Cantor permet d'envisager une suite strictement croissante de Cardinaux, la suite des *beth* (deuxième lettre de l'alphabet hébreu : \beth) :

$$\begin{aligned} \beth_0 &= \omega \\ \beth_{\alpha+1} &= 2^{\beth_\alpha} \\ \beth_\beta &= \sup_{\alpha < \beta} \beth_\alpha \text{ (Si } \beta \text{ est un ordinal limite)} \end{aligned}$$

On peut donc ré-écrire l'hypothèse du continu : $\beth_1 = \aleph_1$ ou encore $\aleph_0^+ = 2^{\aleph_0}$, et l'hypothèse généralisée du continu : $\beth_\alpha = \aleph_\alpha$ ou encore $\aleph_\alpha^+ = 2^{\aleph_\alpha}$.

Le théorème de Cantor permet aussi de résoudre le paradoxe de Cantor : si la classe des cardinaux est un ensemble, alors cet ensemble a un cardinal qui est le plus grand cardinal (puisqu'il contient tous les cardinaux), alors qu'il est strictement plus petit que le cardinal de l'ensemble de ses parties.

Théorème de Cantor-Bernstein-Schröder : Soit deux ensembles x et y non vides, s'il existe une injection de x dans y et une injection de y dans x , alors il existe une bijection de x dans y (autrement dit : $|x| = |y|$).

Le théorème de Cantor-Bernstein-Schröder (qui n'utilise pas l'axiome du choix) est utilisé dans de nombreuses démonstrations sur les Cardinaux.

⁷⁶. D'ailleurs équivalent à l'axiome du choix.

⁷⁷. Chez un certain nombre d'auteurs, un ensemble dénombrable est un ensemble de cardinal inférieur ou égal à celui de \mathbb{N} .

⁷⁸. Une version plus faible de l'axiome du choix.

VI.2.7 Synonymes, Isomorphismes, Exemples

On peut définir les cardinaux sans axiome du choix, mais beaucoup de théorèmes ne sont plus démontrables, par exemple, tous les ensembles n'ont pas de cardinal et la trichotomie n'est plus vérifiée.

VI.2.8 Utilisation des cardinaux en mathématiques

Les cardinaux apparaissent naturellement dans de nombreux domaines des mathématiques. Par exemple, en théorie de la mesure, on peut montrer que tout ensemble dénombrable est de mesure nulle pour toute mesure absolument continue.

En topologie, une conséquence du théorème de Baire est le fait qu'il n'existe pas d'espace de Banach à base dénombrable. Les propriétés des cardinaux, et en particulier certaines hypothèses les concernant, jouent un rôle important dans la métrisabilité des espaces topologiques.

En logique on trouve le très important *théorème de Löwenheim-Skolem* qui utilise directement les cardinaux :

Soit \mathcal{T} une théorie dans le langage \mathcal{L} , si \mathcal{T} admet des modèles infinis, alors \mathcal{T} admet des modèles dans toutes les cardinalités supérieures ou égales à $\text{Max}(\omega, |\mathcal{L}|)$.

VI.2.9 Utilisation en physique

A part les Cardinaux finis (qui ne sont rien d'autres que des entiers), je n'ai trouvé aucune référence à l'utilisation des Cardinaux en physique.

VI.2.10 Références

Il est extrêmement facile de trouver des documents gratuits sur le net concernant les cardinaux, ou plus généralement sur la théorie des ensembles.

1. Jech T, *Set Theory*, 2nd edition, Springer-Verlag, Heidelberg, 1997.
2. Dehornoy, *Les Cardinaux*, Université de Caen, 2007.
3. L. A. Steen & J. A. Seebach Jr, *Counterexamples in Topology*, Dover Publications, 1970, 1978, 1995

VI.3 Ordinaux de Hessenberg \mathcal{H}

VI.3.1 Introduction

Les ordinaux de Hessenberg, notés ci dessous \mathcal{H} , doivent leur nom à Gerhard Hessenberg (1874 – 1925) un mathématicien allemand, en fait les ordinaux de Hessenberg sont les **ordinaux ordinaires**, mais munis d'une addition et d'une multiplication (cette dernière est parfois attribuée à Felix Hausdorff (1868 - 1942) un autre mathématicien allemand, néanmoins, nous parlerons des opérations de Hessenberg) très différentes des opérations usuelles.

Comme il est d'usage de donner des noms différents à des structures différentes, par exemple aux **quaternions** et aux **quaternions fendus**, alors que dans les deux cas, l'ensemble sous-jacent est \mathbb{R}^4 , et que seule la multiplication est différente dans ces deux algèbres, il m'a semblé normal d'utiliser un autre nom pour les ordinaux munis de nouvelles opérations.

VI.3.2 Définition

Les opérations usuelles sur les ordinaux posent quelques problèmes : elles ne sont pas commutatives, ni associatives, les opérations de Hessenberg, appelés aussi opérations naturelles sont commutatives, distributives, régulières et la multiplication (notée \ast dans ce document) est distributive sur l'addition (notée $\#$).

VI.3.3 Mode de construction

Les opérations définies par Hessenberg sont appelées somme naturelle et produit naturel, elles sont définies à l'aide de la **forme normale de Cantor** :

Soit α et β deux ordinaux dont l'écriture en forme normale de Cantor est :

$$\alpha = \sum_{i=0}^{k_\alpha} \omega^{\alpha_i} n_i \text{ et } \beta = \sum_{i=0}^{k_\beta} \omega^{\beta_i} m_i$$

Rappelons que (α_i) et (β_i) sont des suites finies strictement décroissantes d'ordinaux, et les n_i ainsi que les m_i sont des entiers non nuls, en réorganisant les deux suites (α_i) et (β_i) et en autorisant les entiers nuls on peut écrire α et β sous la forme suivante :

$$\alpha = \sum_{i=0}^k \omega^{\mu_i} n_i \text{ et } \beta = \sum_{i=0}^k \omega^{\mu_i} m_i$$

Où la suite (μ_i) est une suite finie strictement décroissantes d'ordinaux, et les n_i ainsi que les m_i sont des entiers éventuellement nuls.

On définit alors la somme naturelle (ou somme de Hessenberg) de α et β par :

$$\alpha \# \beta = \sum_{i=0}^k \omega^{\mu_i} (n_i + m_i)$$

Le produit naturel se définit très simplement dans un cas particulier :

$\omega^\alpha \ast \omega^\beta = \omega^{\alpha \# \beta}$ et s'étend facilement à tous les ordinaux sous forme normale de Cantor en imposant que la multiplication soit distributive sur l'addition, à savoir :

$$\left(\sum_{i=0}^{k_\alpha} \omega^{\alpha_i} n_i \right) \ast \left(\sum_{i=0}^{k_\beta} \omega^{\beta_i} m_i \right) = \sum_{\mu \in \{ \alpha_i \# \beta_j \}_{\substack{0 \leq j \leq k_\beta \\ 0 \leq i \leq k_\alpha}}} \omega^\mu \left(\sum_{\alpha_i \# \beta_j = \mu} n_i \cdot m_j \right)$$

Autrement dit l'addition et la multiplication naturelle des ordinaux sous forme normale de Cantor, revient à considérer cette dernière comme un polynôme de variable ω et à leur appliquer les opérations usuelles sur les polynômes.

On peut vérifier facilement que $\alpha + \beta \leq \alpha \# \beta$, et que $\alpha \times \beta \leq \alpha \ast \beta$

VI.3.4 Autres définitions

Les définitions précédentes de la somme et du produit de Hessenberg peuvent paraître « de circonstances » et être trop éloignées de la notion d'ordinal (c'est à dire de la notion de bon ordre) contrairement aux définitions cantorienne, ce n'est qu'une impression :

Soit α et β deux ordinaux, et $\alpha \uplus \beta$ l'union disjointe de α et β , il existe des bons ordres sur $\alpha \uplus \beta$ qui prolonge l'ordre partiel obtenu en ordonnant naturellement les éléments de α et de β , le plus petit de ces bons ordres est la somme de Hessenberg.

De la même façon, on peut définir le produit de Hessenberg comme le plus petit des bons ordres sur le produit cartésien $\alpha \times \beta$, qui prolonge l'ordre partiel obtenu en ordonnant les éléments de $\alpha \times \beta$ si et seulement si les deux coordonnées sont comparables.

On peut aussi définir la somme de Hessenberg par récurrence :

- $\alpha \# 0 = \alpha$
- $0 \# \alpha = \alpha$
- $\alpha \# \beta$ est le plus petit ordinal strictement plus grand que $\alpha \# \gamma$ et strictement plus grand que $\delta \# \beta$, pour $\gamma < \beta$ et $\delta < \alpha$.

VI.3.5 Propriétés algébriques

- $(\mathcal{H}, \#)$ est un **semi-groupe** commutatif.
- (\mathcal{H}, \times) est un semi-groupe commutatif.
- $(\mathcal{H}, \#, \times)$ est un **semi-anneau** unitaire, intègre et commutatif.

VI.3.6 Synonymes, Isomorphismes, Exemples

Les opérations de Hessenberg sont identiques aux opérations sur les surréels restreintes aux ordinaux (qui sont bien des surréels).

On peut généraliser la notion de somme naturelle et de produit naturel sur la classe des ordinaux :

On dit que \oplus est **une** somme naturelle sur les ordinaux si :

- $\alpha \oplus \beta = \beta \oplus \alpha$ (*commutativité*).
- $\alpha \oplus 0 = \alpha$ (*0 est l'élément neutre*).
- $(\alpha \oplus \beta) \oplus \gamma = \alpha \oplus (\beta \oplus \gamma)$ (*associativité*).
- $\gamma \oplus \alpha < \gamma \oplus \beta \Leftrightarrow \alpha < \beta$ (*croissance de la somme naturelle*).

Il est évident avec cette définition que la somme de Hessenberg est bien une somme naturelle, et plus précisément c'est la plus petite. En notant $+$ la somme cantorienne des ordinaux, on a le résultat suivant :

$$\alpha + \beta \leq \alpha \# \beta \leq \alpha \oplus \beta$$

On dit que \otimes est **un** produit naturel sur les ordinaux si :

- $\alpha \otimes \beta = \beta \otimes \alpha$ (*commutativité*).
- $\alpha \otimes 1 = \alpha$ (*1 est l'élément neutre*).
- $(\alpha \otimes \beta) \otimes \gamma = \alpha \otimes (\beta \otimes \gamma)$ (*associativité*).
- $\gamma \otimes \alpha < \gamma \otimes \beta \Leftrightarrow \alpha < \beta$ (*croissance du produit naturel*).
- $\alpha \otimes (\beta \# \gamma) = (\alpha \otimes \beta) \# (\alpha \otimes \gamma)$ (*distributivité sur la somme de Hessenberg*).
- $\omega^\alpha \otimes \omega^\beta = \omega^{\alpha \oplus \beta}$ pour une somme naturelle.

Il est clair qu'avec cette définition, le produit de Hessenberg est un produit naturel (le plus petit), et plus particulièrement, si dans le dernier axiome ci-dessus, la somme naturelle est en fait la somme de Hessenberg, alors le produit naturel est bien le produit de Hessenberg. En notant \cdot le produit cantorien des ordinaux, on a le résultat suivant :

$$\alpha \cdot \beta \leq \alpha \times \beta \leq \alpha \otimes \beta$$

VI.3.7 Références

1. P. Ehrlich, *The Absolute Arithmetic Continuum*, Ohio University, 2011
2. M. Mia Minnes, *Computability And Complexity Properties Of Automatic Structures And Their Applications*, Cornell University, 2008.
3. P. W. Carruth, *Arithmetic Of Ordinals With Applications To The Theory Of Ordered Abelian Groups*, Bulletin of the American Mathematical Society, Volume 48, N° 4, p. 262-271, 1942.
4. G. Hessenberg, *Grundbegriffe der Mengenlehre*, Abhandlungen der Friesschen Schule, Göttingen, Vandenhoeck & Ruprecht, 1906

VI.4 Réels définissables, calculables

VI.4.1 Introduction

La notion de nombre entier *définissable* devient nécessaire face à quelques paradoxes (bien connus) :

- Soit « n est le plus petit nombre entier qui ne soit pas définissable en moins de vingt mots ». La définition précédente de n tient en moins de vingt mots, ce qui est une contradiction.
- Soit I l'ensemble des nombres entiers n'ayant rien de remarquable. Comme tout sous-ensemble de \mathbb{N} , I possède un plus petit élément, qui est donc le plus petit entier n'ayant rien de remarquable, ce qui le rend ... remarquable.

Ces deux paradoxes montrent que la notion de définissabilité est trop floue pour être vraiment utile et qu'elle nécessite une définition formelle.

La notion de nombre *calculable* est moins intuitive, en effet, selon que l'on pense que pour qu'un nombre réel soit calculable on doit pouvoir écrire effectivement toutes ses décimales, et un nombre aussi banal que $\frac{1}{3}$ ne serait pas calculable ; ou au contraire que l'on pense que pour qu'un nombre réel soit calculable on doit pouvoir écrire toutes ses décimales, éventuellement en un temps infini et alors tous les réels sont calculables (si x est un réel tel que $x \in [0, 1[$, alors il suffit d'écrire la première décimale de x , puis la deuxième, puis ...).

Ces deux pseudo-définitions (très naïves) sont trop floues pour être vraiment utiles, et montrent que la notion de calculabilité nécessite une définition formelle.

VI.4.2 Définition

Un nombre réel α est *définissable* au premier ordre dans le langage de la théorie des ensembles⁷⁹ ($\mathcal{L}(\in, =)$) s'il existe une formule $\varphi(x)$ du premier ordre dans le langage $\mathcal{L}(\in, =)$, telle que α soit le seul nombre réel vérifiant $\varphi(\alpha)$.

Un nombre réel α est *calculable* s'il existe une machine de Turing⁸⁰ qui, lorsqu'on lui donne un entier n en entrée, se termine en un temps fini et donne la $n^{\text{ième}}$ décimale de α .

VI.4.3 Exemples de nombres définissables et calculables

Les entiers naturels, donc les relatifs, donc les rationnels sont définissables, et, bien sûr, les constantes mathématiques utilisées par les mathématiciens sont définissables.

Les entiers naturels, donc les relatifs, donc les rationnels sont calculables, et la très grosse majorité des constantes utilisées par les mathématiciens est calculable : $\sqrt{2}, e, \pi$ en sont des exemples.

VI.4.4 Opérations

On peut remarquer immédiatement que les nombres réels définissables possèdent quelques propriétés simples :

1. On peut associer un nombre de Gödel à chaque formule du premier ordre dans le langage des corps ordonnés, celles qui permettent effectivement de calculer un réel sont donc en nombre au plus dénombrable, et comme tous les entiers sont définissables, l'ensemble des réels définissables est bien de cardinal \aleph_0 .
2. α et β définissables $\Rightarrow \alpha + \beta$ définissable.
3. α et β définissables $\Rightarrow \alpha \times \beta$ définissable.
4. α définissable $\Rightarrow -\alpha$ définissable.
5. α définissable et non nul $\Rightarrow \frac{1}{\alpha}$ définissable.

On peut remarquer immédiatement que les nombres réels calculables possèdent quelques propriétés simples (dont certaines sont triviales avec la définition donnée là) :

1. On peut associer un nombre de Gödel à chaque machine de Turing, celles qui permettent effectivement de calculer un réel sont donc en nombre au plus dénombrable, et comme tous les entiers sont calculables, l'ensemble des réels calculables est bien de cardinal \aleph_0 .
2. α et β calculables $\Rightarrow \alpha + \beta$ calculable.

79. On peut donner d'autres définitions, simplement en changeant le langage (et choisir celui de l'arithmétique par exemple) ou la logique (et choisir le 2nd ordre), ou en autorisant des paramètres dans la formule.

80. Il existe de nombreuses autres définitions équivalentes, certaines sont citées dans la section « Synonymes, Isomorphismes, Exemples ».

3. α et β calculables $\Rightarrow \alpha \times \beta$ calculable.
4. α calculable $\Rightarrow -\alpha$ calculable.
5. α calculable et non nul $\Rightarrow \frac{1}{\alpha}$ calculable.

Par contre l'ensemble des nombres calculables ne possède pas la propriété de la borne supérieure.

Un résultat plus inattendu : la relation d'ordre entre nombres réels calculables n'est pas calculable (il n'est pas possible de savoir, par avance, combien de décimales de α et de β il faut calculer pour savoir lequel est le plus grand), pour la même raison, l'égalité entre nombres calculables n'est pas calculable.

Les nombres réels calculables sont a fortiori définissables, mais le contraire n'est pas toujours vrai :

La constante Ω de Chaitin est l'exemple le plus connu.

VI.4.5 Propriétés algébriques

Munis des opérations usuelles héritées de \mathbb{R} , l'ensemble des réels calculables, ainsi que l'ensemble des réels définissables sont des corps commutatifs dénombrables (c'est à dire de cardinal \aleph_0).

VI.4.6 Synonymes, Isomorphismes, Exemples

Au lieu de donner une définition utilisant les machines de Turing, on aurait pu donner d'autres définitions équivalentes utilisant la notion de fonctions récursives (ce qui nécessite une **définition formelle**) :

1. Un nombre réel α est *calculable* s'il existe une fonction récursive telle que pour tout $n \in \mathbb{N}^*$ elle produise un entier k tel que :

$$\frac{k-1}{n} \leq \alpha \leq \frac{k+1}{n}$$

2. Un nombre réel α est *calculable* s'il existe une fonction récursive telle que pour tout $\varepsilon \in \mathbb{Q}^*$ elle produise un rationnel a tel que :

$$|\alpha - a| \leq \varepsilon$$

3. Un nombre réel α est *calculable* s'il existe une suite récursive de rationnels $(r_i)_{i \in \mathbb{Q}}$ convergeant vers α telle que pour tout i

$$|r_{i+1} - r_i| < 2^{-i}$$

Autrement dit il existe une fonction récursive qui permet d'approcher α avec la précision que l'on veut.

On aurait pu aussi donner des définitions pour les nombres complexes : un nombre complexe est définissable ou calculable, si et seulement si sa partie réelle et sa partie imaginaire le sont.

VI.4.7 Fonctions récursives

On appelle fonctions de base, les fonctions (qui peuvent être partielles) suivantes⁸¹ :

- Les fonctions nulles $o : \mathbb{N}^k \mapsto \mathbb{N}$ définies par $o(\bar{\alpha}) = 0$.
- La fonction successeur $s : \mathbb{N} \mapsto \mathbb{N}$ définie par $s(n) = n + 1$.
- Les fonctions $i^{\text{ième}}$ projection $\pi_i : \mathbb{N}^k \mapsto \mathbb{N}$ définies par $\pi_i(\bar{\alpha}) = \alpha_i$.

On appelle fonctions récursives primitives la plus petite classe contenant les fonctions de base et close pour l'application un nombre fini de fois des opérateurs suivants :

- La composition d'application : si $(f_i : \mathbb{N}^k \mapsto \mathbb{N})_{0 < i \leq l}$ et $g : \mathbb{N}^l \mapsto \mathbb{N}$, alors la composée des f_i et de g est l'application : $c : \mathbb{N}^k \mapsto \mathbb{N}$ définie par $c(\bar{\alpha}) = g(f_1(\bar{\alpha}), f_2(\bar{\alpha}), \dots, f_l(\bar{\alpha}))$.
- La récursion primitive : soit $f : \mathbb{N}^k \mapsto \mathbb{N}$ et $g : \mathbb{N}^{k+2} \mapsto \mathbb{N}$, alors la *récursée* de f et g est la fonction

$$h : \mathbb{N}^{k+1} \mapsto \mathbb{N} \text{ définie par } \begin{cases} h(\bar{\alpha}, 0) = f(\bar{\alpha}) \\ h(\bar{\alpha}, p+1) = g(\bar{\alpha}, p, h(\bar{\alpha}, p)) \end{cases}$$

La classe des fonctions primitives récursives contient des fonctions qui sont calculables, mais il existe des fonctions calculables qui ne sont pas primitives récursives : par exemple la fonction d'Ackermann (cf. [Fonctions récursives et machine de Turing](#)).

On appelle classe des fonctions récursives la plus petite classe contenant les fonctions primitives récursives et close par minimisation non bornée :

⁸¹. les éléments de \mathbb{N}^k sont notés $\bar{\alpha}$

- Soit la fonction $f : \mathbb{N}^{k+1} \mapsto \mathbb{N}$, alors la minimisation (non bornée) de f est la fonction $m : \mathbb{N}^k \mapsto \mathbb{N}$ définie par $m(\bar{\alpha}) =$ le plus petit i tel que $f(\bar{\alpha}, i) = 0$, et pour tous $j < i$, $f(\bar{\alpha}, j)$ est défini si ce i existe, et n'est pas définie sinon.

La fonction d'Ackermann citée ci-dessus est bien récursive.

Nous en profitons pour rappeler la *thèse de Church-Turing* (qui n'est donc pas un théorème) : La classe des fonctions récursives est exactement la classe des fonctions calculables par un algorithme quelconque.

VI.4.8 Utilisation en physique

L'ensemble de cette problématique ne concerne que les mathématiciens et même de façon plus précise les logiciens.

VI.4.9 Références

1. B. Mariou, *Fonctions Récursives*, Université Paris 8, (1 page), 2005
2. N. Le Thanh, *Fonctions récursives et machine de Turing*, Université de Nice Sophia Antipolis, (17 pages), 2008
3. A. Turing, *On Computable Numbers, With An Application To The Entscheidungsproblem*, Proceedings London Mathematical Society, Volume 2-42, p. 230-265, 1936-1937
4. J. Ferreirós, *The Crisis in the Foundations of Mathematics*, The Princeton Companion to Mathematics, Timothy Gowers Editeur, Princeton University Press, p 142-156, 2008
5. C. H. Bennett, *On Random and Hard-to-Describe Numbers*, IBM Watson Research Center Yorktown Heights, 1979
6. É. Janvresse, T. de la Rue, *La face cachée des nombres*, Université de Rouen (CNRS), 2007

VII Algèbres de dimension 2 sur \mathbb{R}

Introduction

Les algèbres de dimension 2 sur \mathbb{R} sont des cas particuliers d'**hypercomplexes** de la forme $\mathbb{R} \oplus \mathbb{R}$ en tant qu'espace vectoriel, et sur lesquels on définit une multiplication distributive sur l'addition, vérifiant la relation $(\alpha_0 z_0) \cdot (\alpha_1 z_1) = (\alpha_0 \alpha_1)(z_0 \cdot z_1)$ (pour $\alpha_i \in \mathbb{R}$) et unitaire.

Il y a deux façons naturelles de représenter un élément de $\mathbb{R} \oplus \mathbb{R}$:

- Un couple : $z = (x_0, x_1)$, où $(x_0, x_1) \in \mathbb{R}^2$
- Une combinaison linéaire d'éléments d'une base de l'espace vectoriel $\mathbb{R} \oplus \mathbb{R}$: $z = x_0 \cdot e_0 + x_1 \cdot e_1$

Les deux représentations sont parfaitement interchangeables grâce à l'identification :

$$(1, 0) = e_0 \text{ et } (0, 1) = e_1.$$

Il est d'usage d'identifier \mathbb{R} avec la première composante de $\mathbb{R} \oplus \mathbb{R}$, c'est à dire que si $x \in \mathbb{R}$, on identifie x et $(x, 0)$, et comme $(x, 0) = x \cdot (1, 0)$, on identifie aussi x et $x \cdot e_0$, et en particulier 1 et e_0 (ou encore, on identifie $1_{\mathbb{R}}$ et $1_{\mathbb{R} \oplus \mathbb{R}}$), de ce fait, la méthode la plus courante pour représenter un élément de $\mathbb{R} \oplus \mathbb{R}$ est $z = x_0 + x_1 \cdot e_1$. C'est cette représentation que nous utiliserons par la suite.

Pour définir complètement la structure d'algèbre sur $\mathbb{R} \oplus \mathbb{R}$, il reste à définir la multiplication de deux éléments, et grace aux propriétés de la multiplication, il suffit de définir la multiplication sur les éléments d'une base, comme, de plus, 1 est l'élément neutre de cette multiplication, nous avons forcément $1 \cdot e_1 = e_1 \cdot 1 = e_1$, il ne reste plus qu'à définir $e_1 \cdot e_1$ ce que nous pouvons résumer par la table de multiplication :

·	1	e_1
1	1	e_1
e_1	e_1	$a + b \cdot e_1$

Nous noterons $(\mathbb{R} \oplus \mathbb{R})_{a,b}$ pour l'algèbre $\mathbb{R} \oplus \mathbb{R}$ munie de la multiplication précédente.

Trois cas particuliers sont particulièrement intéressants \mathbb{C} , \mathbb{D}_1 ⁸² et \mathbb{C} :

·	1	e_1
1	1	e_1
e_1	e_1	-1

Complexe : \mathbb{C}

·	1	e_1
1	1	e_1
e_1	e_1	0

Dual complexe : \mathbb{D}_1

·	1	e_1
1	1	e_1
e_1	e_1	1

Complexe fendu : \mathbb{C}

Ces trois structures ne sont pas isomorphes 2 à 2 :

- ▷ $(\mathbb{C}, +, \cdot)$ est un corps
- ▷ $(\mathbb{D}_1, +, \cdot)$ contient des éléments non nuls vérifiant $x^2 = 0$ (par exemple e_1)
- ▷ $(\mathbb{C}, +, \cdot)$ contient des diviseurs de zéro (par exemple $(1 - e_1) \cdot (1 + e_1) = 0$), mais pas d'éléments non nuls vérifiant $x^2 = 0$

Il est d'usage de noter $e_1 = i$ dans le cas \mathbb{C} , $e_1 = \varepsilon$ dans le cas \mathbb{D}_1 et $e_1 = j$ dans le cas \mathbb{C} .

La question naturelle suivante consiste à se demander s'il y a d'autres cas, pour cela cherchons à quelle(s) condition(s) sur a et b il existe un isomorphisme φ entre $(\mathbb{R} \oplus \mathbb{R})_{a,b}$ et $(\mathbb{R} \oplus \mathbb{R})_{\delta,0}$ où $\delta \in \{-1, 0, 1\}$.

^{82.} A ne pas confondre avec l'ensemble des décimaux

Par définition d'un isomorphisme d'algèbre, φ vérifie les propriétés suivantes (nous noterons f_1 le deuxième élément de la base de $(\mathbb{R} \oplus \mathbb{R})_{\delta,0}$, et donc $f_1^2 = \delta$) :

1. $\varphi(1) = 1$
2. $\varphi(a + b \cdot e_1) = a + b \cdot \varphi(e_1)$
3. $\varphi(e_1^2) = (\varphi(e_1))^2$
4. $\exists \alpha \in \mathbb{R} \exists \beta \in \mathbb{R}^* (\varphi(e_1) = \alpha + \beta \cdot f_1)$

β doit être différent de 0 sinon φ ne serait pas une bijection.

On a donc :

$$\begin{aligned} \varphi(e_1^2) &= \varphi(a + b \cdot e_1) = a + b \cdot \varphi(e_1) = a + b \cdot (\alpha + \beta \cdot f_1) = a + b\alpha + b\beta \cdot f_1 \\ (\varphi(e_1))^2 &= (\alpha + \beta \cdot f_1)^2 = \alpha^2 + \delta\beta^2 + 2\alpha\beta \cdot f_1 \end{aligned}$$

Nous devons donc résoudre $a + b\alpha + b\beta \cdot f_1 = \alpha^2 + \delta\beta^2 + 2\alpha\beta \cdot f_1$, ce qui est équivalent au système (a et b sont des paramètres réels et α et β les inconnues réelles) :

$$\begin{cases} a + b\alpha &= \alpha^2 + \delta\beta^2 \\ b\beta &= 2\alpha\beta \end{cases}$$

Or $\beta \neq 0$, nous obtenons donc le système $\begin{cases} a + b\alpha &= \alpha^2 + \delta\beta^2 \\ b &= 2\alpha \end{cases}$

Après quelques calculs élémentaires le système devient $\begin{cases} 4a + b^2 &= 4\delta\beta^2 \\ \frac{b}{2} &= \alpha \end{cases}$

Système qui a des solutions sous certaines conditions :

\mathbb{C}	$\delta = -1$	Ce système a une solution si et seulement si $4a + b^2 < 0$
\mathbb{D}_1	$\delta = 0$	Ce système a une solution si et seulement si $4a + b^2 = 0$
\mathbb{C}	$\delta = 1$	Ce système a une solution si et seulement si $4a + b^2 > 0$

Ce résultat permet, non seulement de savoir à quelle condition sur a et b $(\mathbb{R} \oplus \mathbb{R})_{a,b}$ est isomorphe à \mathbb{C} , \mathbb{D}_1 ou \mathbb{C} , mais en plus ce résultat montre que ce sont les trois seuls cas possibles de \mathbb{R} -algèbre de dimension 2.

VII.1 Nombres Duaux \mathbb{D}_1

VII.1.1 Introduction

Les nombres duaux sont une des trois algèbres hypercomplexes de dimension 2 (cf nombres complexes et nombres complexes fendus).

L'ensemble des nombres duaux est parfois noté \mathbb{C}_0 (avec les mêmes notations, l'ensemble des nombres complexes peut être noté \mathbb{C}_{-1} , et l'ensemble des nombres complexes fendus, \mathbb{C}_1), il est aussi appelé ensemble des nombres complexes paraboliques. Nous noterons l'ensemble des nombres duaux \mathbb{D}_1 (dualisation de \mathbb{R}) pour être cohérent avec la notation des complexes duaux (\mathbb{D}_2), quaternions duaux (\mathbb{D}_4) etc.

\mathbb{D}_1 correspond à la géométrie Galiléenne.

VII.1.2 Définition

Les nombres duaux sont des nombres hypercomplexes de la forme $z = a_0 + a_1 \cdot e_1$, où $a_i \in \mathbb{R}$ et $e_1^2 = 0$. a_0 est appelée la partie réelle et a_1 la partie duale de z .

Usuellement e_1 est noté ε , c'est un élément nilpotent.

VII.1.3 Mode de construction

L'ensemble des nombres duaux peut donc être construit comme un ensemble hypercomplexe

L'ensemble des nombres duaux peut aussi être construit comme $\mathbb{R}[X]/X^2$, c'est-à-dire le quotient de l'anneau des polynômes réels par l'idéal principal engendré par le polynôme X^2 ; cette construction est généralisable à partir de n'importe quel anneau en place de \mathbb{R} .

Les nombres duaux ne sont pas une algèbre de Clifford.

VII.1.4 Table de multiplication

+	1	ε
1	1	ε
ε	ε	0

L'exponentielle est définie comme la série entière (pour une variable appartenant à un ensemble de "nombres" E :

$$\forall x \in E, e^x = \sum_{n=0}^{+\infty} \frac{x^n}{n!}$$

Dans le cas des nombres duaux on obtient :

$$\forall x \in \mathbb{R} (e^{x\varepsilon} = 1 + x\varepsilon)$$

Par analogie avec le résultat usuel pour les nombres complexes, on peut définir le cosinus parabolique (cosp) et le sinus parabolique (sinp) :

$$\begin{aligned} - \text{cosp}(x) &= 1 \\ - \text{sinp}(x) &= x \end{aligned}$$

Il est facile de vérifier que la formule de De Moivre reste vraie (mais pas vraiment passionnante), pour x un réel :

$$(\text{cosp}(x) + \varepsilon \text{sinp}(x))^n = \text{cosp}(nx) + \varepsilon \text{sinp}(nx)$$

VII.1.5 Conjugué, Module, Norme, Forme Polaire et Inverse

Pour $z = a_0 + a_1 \cdot \varepsilon$ alors $\bar{z} = a_0 - a_1 \cdot \varepsilon$. La conjugaison est un automorphisme d'ordre 2.

Le module de z , $|z|^2 = z \cdot \bar{z} = a_0^2$ est multiplicatif $|z \cdot z'| = |z| |z'|$, mais ce n'est pas une norme.

Tous les nombres duaux n'ont pas d'inverse, un nombre dual est inversible si et seulement si son module est différent de 0, c'est-à-dire si sa partie réelle est différente de 0 et dans ce cas :

$$z^{-1} = \frac{\bar{z}}{|z|^2}, \text{ c'est à dire : } z^{-1} = \frac{1}{a_0} - \frac{a_1}{a_0^2} \varepsilon.$$

On peut noter que la multiplication de z par un nombre dual de module 1, conserve le module de z : $|z \cdot e^{x\varepsilon}| = |z|$, autrement dit cette multiplication conserve $z \cdot \bar{z} = a_0^2$, autrement dit, toute parabole d'équation

$a_0^2 = k$ est globalement invariante par une multiplication par un nombre dual de module 1, d'où le nom de nombres paraboliques que l'on utilise parfois à la place de nombres duaux.

Représentation polaire (pour $a_0 \neq 0$) : $a_0 + a_1\varepsilon = a_0(1 + \frac{a_1}{a_0}\varepsilon)$.

Représentation exponentielle (pour $a_0 \neq 0$) : $a_0 + a_1\varepsilon = a_0e^{\frac{a_1}{a_0}\varepsilon}$

La géométrie associée à \mathbb{D}_1 est appelée « parabolique », et pour cette géométrie, le "cercle unité", c'est à dire l'ensemble des points tels que $|z| = 1$, est constituée de deux droites parallèles à l'axe des ordonnées.

VII.1.6 Propriétés algébriques

Les nombres duaux sont une algèbre associative, unitaire, commutative de dimension deux sur \mathbb{R} . \mathbb{D}_1 , le plan complexe parabolique correspond au plan de Laguerre.

VII.1.7 Synonymes, Isomorphismes, Exemples

Les nombres duaux peuvent être représentés par des matrices de $M_2(\mathbb{R})$: $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$

VII.1.8 Utilisation en physique

Les nombres duaux sont utilisés pour représenter un hyperespace, la direction le long de l'axe ε est dit "fermionique", l'axe réel définissant la direction "bosonique".

Liste de domaines où les nombres duaux sont utilisés :

- Rigid body motion.
- Displacement analysis of spatial mechanisms.
- Robotics.
- Surface shape analysis and computer graphics.
- Human body motion analysis.
- Kinematic synthesis.
- Dynamic analysis.

VII.1.9 Références

1. Yaglom I. M., *A Simple Non-Euclidean geometry and its Physical Basis*, Springer-Verlag, New York, (1979).
2. [Linear Algebra and Numerical Algorithms Using Dual Numbers](#) E. Pennestri, R. Stefanelli

VII.2 Complexes fendus \mathbb{C}

VII.2.1 Introduction

Les complexes fendus, notés \mathbb{C} , sont construits, comme les nombres complexes *standard*, en ajoutant à \mathbb{R} un nouvel élément, mais dans ce cas, le carré de ce nouvel élément est 1 (et non -1).

L'aspect le plus utile des complexes fendus est leur usage en relativité général (ce qui explique qu'ils soient parfois appelés *nombres Espaces-Temps*).

VII.2.2 Définition

Les complexes fendus sont des hypercomplexes de dimension 2, c'est à dire qu'ils sont isomorphes à $\mathbb{R} \oplus \mathbb{R}$, en tant qu'espace vectoriel, de plus une multiplication distributive sur l'addition est définie entre complexes fendus.

VII.2.3 Mode de construction

Les nombres complexes fendus sont des nombres de la forme $z = a_0 + a_1 \cdot e_1$, où $a_i \in \mathbb{R}$ et $e_1^2 = 1$.

Dans le cas des nombres complexes fendus, l'élément de base e_1 est généralement noté j ⁸³.

VII.2.4 Table de multiplication

Dans une telle algèbre, la multiplication est entièrement définie par la table de multiplication des éléments d'une base, ici, la base naturelle est $(1, j)$, et comme 1 est l'élément neutre de la multiplication ($1 \cdot j = j \cdot 1 = j$), et comme j^2 est déterminé par la définition, la table de multiplication est facile à écrire :

·	1	j
1	1	j
j	j	1

Cette multiplication est associative, elle permet donc de définir la notion de série entière, en particulier la fonction exponentielle.

L'exponentielle est définie comme la série entière (pour une variable appartenant à un ensembles de « nombres » $E : \forall x \in E, e^x = \sum_{n=0}^{+\infty} \frac{x^n}{n!}$

Dans le cas des complexes fendus on obtient : $\forall x \in \mathbb{R} e^{x \cdot j} = 1 + \frac{x \cdot j}{1!} + \frac{x^2}{2!} + \frac{x^3 \cdot j}{3!} + \dots$

En regroupant les termes, on obtient : $e^{x \cdot j} = (1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \dots) + (\frac{x}{1!} + \frac{x^3}{3!} + \frac{x^5}{5!} + \dots) \cdot j$

Relation que nous pouvons écrire sous la forme d'une relation d'Euler : $e^{x \cdot j} = ch(x) + j \cdot sh(x)$.

VII.2.5 Conjugué, Module, Norme, Forme Polaire et Inverse

Pour $z = a_0 + a_1 \cdot j$ alors $\bar{z} = a_0 - a_1 \cdot j$. La conjugaison est un automorphisme d'ordre 2 ($\bar{\bar{z}} = z$).

Le module de z , $|z|^2 = z \cdot \bar{z} = a_0^2 - a_1^2$ est multiplicatif, mais ce n'est pas une norme.

On peut noter que la multiplication de z par un complexe fendu de module 1, conserve le module de z : $|z \cdot e^{x \cdot j}| = |z|$, autrement dit cette multiplication conserve $z \cdot \bar{z} = a_0^2 - a_1^2$, autrement dit, tout hyperbole d'équation $a_0^2 - a_1^2 = k$ est globalement invariante par une multiplication par un complexe fendu de module 1, d'où le nom de complexes hyperboliques que l'on utilise parfois à la place de complexes fendus.

Tous les nombres complexes fendus n'ont pas d'inverse, un nombre complexe fendu est inversible si et seulement si son module est différent de 0, et dans ce cas :

$$z^{-1} = \frac{\bar{z}}{|z|^2}$$

On peut donner une forme polaire aux complexes fendus :

⁸³. A ne pas confondre avec une racine troisième de l'unité dans \mathbb{C} .

$$\text{Soit } z = a_0 + a_1 \cdot j \begin{cases} a_0^2 < a_1^2 & a_0 + a_1 \cdot j = j \cdot \rho e^{x \cdot j} \\ a_0^2 = a_1^2 & \text{Pas de forme polaire} \\ a_0^2 > a_1^2 & a_0 + a_1 \cdot j = \rho e^{x \cdot j} \end{cases}$$

VII.2.6 Propriétés algébriques

L'ensemble des complexes fendus est une algèbre unitaire, associative et commutative de dimension 2 sur \mathbb{R} .

\mathbb{C} contient des éléments idempotent (autre que 0 et 1), des diviseurs de 0 (ce n'est donc pas un corps) mais pas d'élément nilpotent.

$$\text{Par exemple : } \begin{cases} (\frac{1}{2} + \frac{1}{2} \cdot j)^2 & = (\frac{1}{2} + \frac{1}{2} \cdot j) \\ (\frac{1}{2} - \frac{1}{2} \cdot j)^2 & = (\frac{1}{2} - \frac{1}{2} \cdot j) \\ (1 - j)(1 + j) & = 0 \end{cases}$$

Les résultats précédents permettent de définir une autre base pour \mathbb{C} :
$$\begin{cases} e_0 & = \frac{1 + j}{2} \\ e_1 & = \frac{1 - j}{2} \end{cases}$$

Or pour cette nouvelle base, la table de multiplication devient :

\cdot	e_0	e_1
e_0	e_0	0
e_1	0	e_1

Dans cette base, la multiplication de deux éléments se fait coordonnée par coordonnée, c'est à dire que \mathbb{C} est en fait isomorphe à $\mathbb{R} \oplus \mathbb{R}$ **en tant qu'algèbre** et non seulement en tant qu'espace vectoriel.

La résolution des équations du 2nd degré est un peu différente dans \mathbb{C} et dans \mathbb{C} :

Nombre de solutions		
\mathbb{R}	\mathbb{C}	\mathbb{C}
0	2	0
1	1	1
2	2	4

Si on représente dans le plan le deux racines réelles d'une équation (a et b ci-dessous) ainsi que les deux nouvelles racines appartenant à \mathbb{C} , on obtient ... un carré.

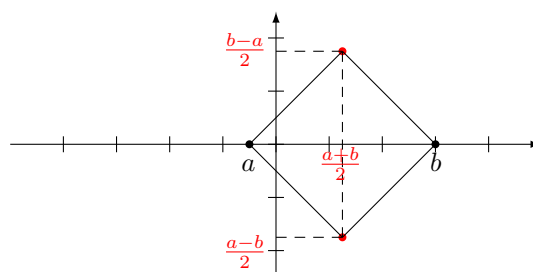


FIGURE 6 – Racines d'une équation du 2nd degré.

VII.2.7 Synonymes, Isomorphismes, Exemples

Les complexes fendus sont une algèbre de Clifford, plus précisément : $\mathcal{C}\ell_{1,0}(\mathbb{R})$.

Ce sont aussi des **Tessarines** :

Les Tessarines forment un sous-ensemble des matrices de $M_2(\mathbb{H})$, plus précisément c'est l'ensemble des matrices de la forme $\begin{pmatrix} q & q' \\ q' & q \end{pmatrix}$ où q et q' sont des quaternions, pour obtenir les complexes fendus, il suffit d'imposer que q et q' soient en fait des réels (ce qui rend \mathbb{C} isomorphe à un sous-ensemble de $M_2(\mathbb{R})$, celui des matrices réelles $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$).

L'ensemble des nombres complexes fendus peut aussi être construit comme $\mathbb{R}[X]/(X^2 - 1)$, c'est-à-dire le quotient de l'anneau des polynômes réels par l'idéal principal engendré par le polynôme $(X^2 - 1)$.

Dans la littérature on trouve de nombreux synonymes pour \mathbb{C} :

- Nombres complexes hyperboliques.
- Moteurs algébrique (Clifford).
- Nombres bi-réels.
- Contre-complexe.
- Nombres doubles.
- Nombres complexes anormaux.
- Nombres perplexes.
- Nombres de Lorentz.
- Nombres espace-temps.

Lorsque les nombres complexes fendus sont utilisés dans le cadre « Espace-Temps », le vocabulaire suivant est utilisé :

$$\text{Soit } z = a_0 + a_1 \cdot j \begin{cases} a_0^2 < a_1^2 & \text{Nombre de type Temps} \\ a_0^2 = a_1^2 & \text{Nombre de type Lumière} \\ a_0^2 > a_1^2 & \text{Nombre de type Espace} \end{cases}$$

VII.2.8 Utilisation en physique

Les complexes fendus sont utilisés pour représenter les sommes de spins en 1882.

Ils sont devenus un moyen usuel pour décrire les transformations de Lorentz de la relativité.

L'espace de Minkowski de la relativité restreinte possède une géométrie hyperbolique.

VII.2.9 Références

1. N. Borota, E. Flores et T. Osler, *Spacetime Numbers The Easy Way*, Mathematics and Computer Education, Vol. 34, No. 2, p. 159-168, 2000.
2. P. Fjelstad, *Extending relativity via the perplex numbers*, American Journal of Physics, Volume 54, N° 5, p. 416-422, 1986.
3. D. Hestenes, *Space Time Algebra*, Gordon and Breach, 1966.
4. D. Lambert, *Les nombres complexes hyperboliques : des complexes qui nous laissent perplexes*, Revue des Questions Scientifiques 166, no. 4, p. 383-400, 1996.
5. A. Ronveaux, *About perplex numbers*, Am. J. Phys., 55, p. 392, 1987.
6. G. Sobczyk, *The hyperbolic number plane*, The College Mathematics Journal, 26, p. 268-280, 1995.
7. S. Olariu, *Complex Numbers in n Dimensions*, Bentham, 2004

VIII Algèbres de dimension 4 sur \mathbb{R}

Introduction

En dimension 2 il est aisé de déterminer toutes les \mathbb{R} -algèbres (cf. le chapitre sur les **hypercomplexes**), par contre en dimension 4, le nombre de possibilités est trop important pour en faire une liste exhaustive.

Par contre en imposant quelques contraintes, il est possible d'établir une liste intéressante ⁸⁴.

Les éléments d'une algèbre de dimension 4 sur \mathbb{R} peuvent s'écrire, en adaptant le cas général au cas de la dimension 4 : $z = a_0 + a_1 \cdot e_1 + a_2 \cdot e_2 + a_3 \cdot e_3$, mais pour ce cas particulier nous adopterons plutôt la notation $z = a_0 + a_1 \cdot i + a_2 \cdot j + a_3 \cdot k$.

Rappelons qu'une telle algèbre est parfaitement définie par la table de multiplication des éléments d'une base (sachant que 1 est l'élément neutre de l'algèbre, seule la partie purement imaginaire de la base nécessite des calculs).

Les conditions que nous imposons sont les suivantes :

- $i^2 \in \{-1, 0, 1\}$
- $j^2 \in \{-1, 0, 1\}$
- Par définition, nous choisirons $k = i \cdot j$ comme troisième élément de base.
- Soit i, j et k commutent tous entre eux, soit ils anti-commutent tous (par exemple $i \cdot j = -i \cdot j$)
- Soit i, j et k alternent ⁸⁵ tous entre eux, soit ils anti-alternent tous (par exemple $i^2 \cdot j = -i \cdot (i \cdot j)$)

Ces conditions permettent de construire la table de multiplication partielle suivante :

·	1	i	j	k
1	1	i	j	k
i	i	i^2	k	
j	j		j^2	
k	k			

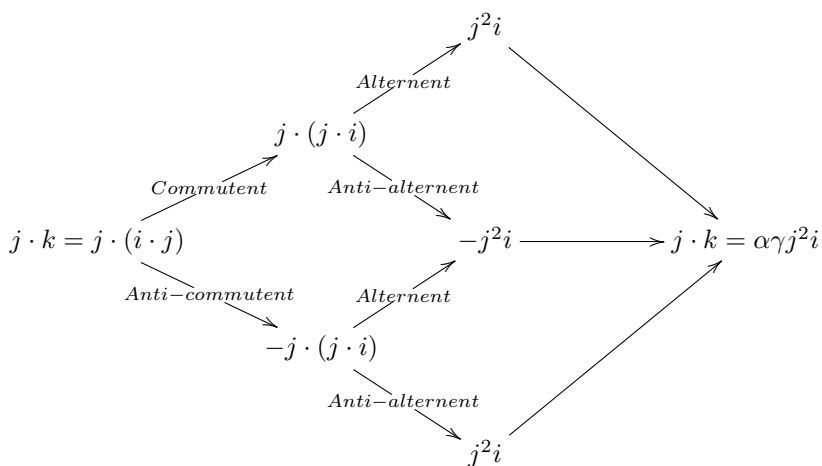
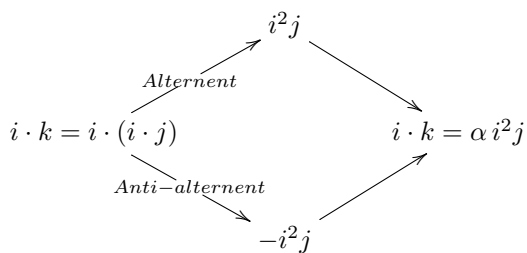
Les cellules sur fond bleu doivent être calculées en fonction des choix faits pour les quatre conditions ci-dessus, les cellules sur fond pourpre se déduisent immédiatement des cellules bleues ou blanches en fonction uniquement de la condition 3.

Pour les calculs ci-dessous, nous poseront :

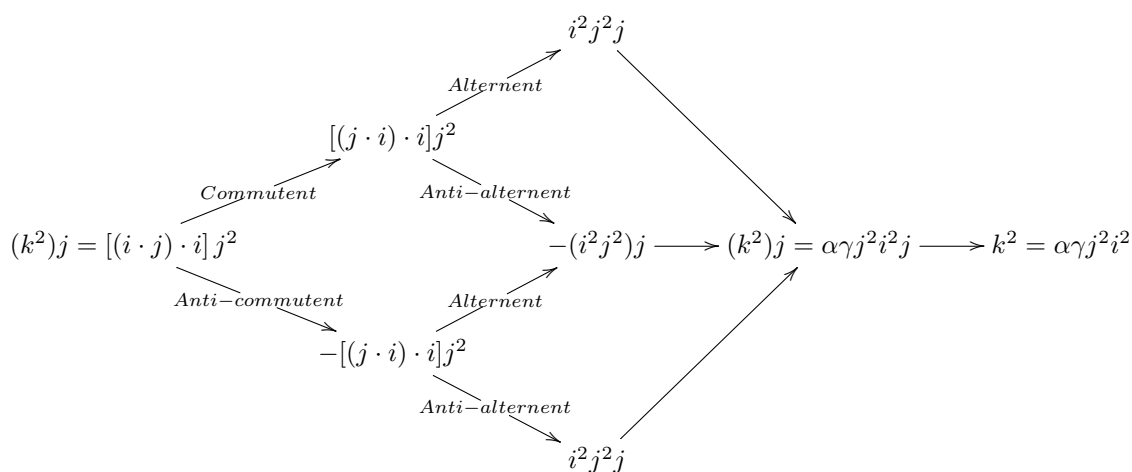
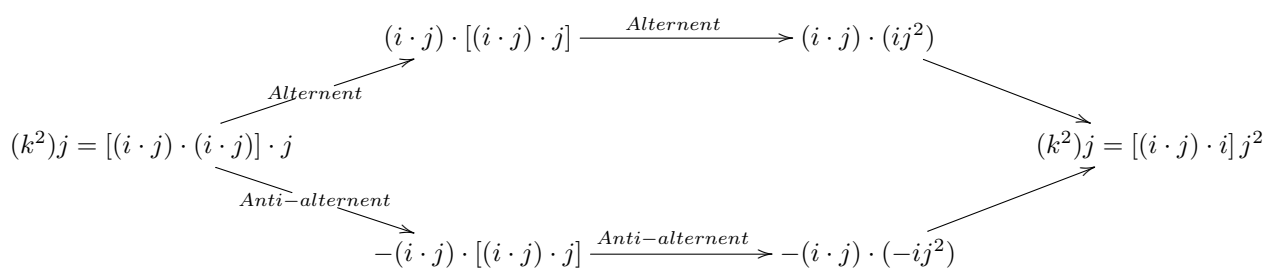
- $\alpha = 1$ si i, j et k alternent.
- $\alpha = -1$ si i, j et k anti-alternent.
- $\gamma = 1$ si i, j et k commutent.
- $\gamma = -1$ si i, j et k anti-commutent.

⁸⁴. J'ai trouvé dans un forum une proposition à peu près similaire, mais fautive, ce qui m'a amené à creuser la question et à cette proposition.

⁸⁵. cf. la définition de **l'alternativité**



Le calcul de k^2 est un peu plus compliqué, et en fait nous devons passer par le calcul de $(k^2)j$



Finalement nous pouvons compléter la table de multiplication :

\cdot	1	i	j	k
1	1	i	j	k
i	i	i^2	k	$\alpha i^2 j$
j	j	γk	j^2	$\alpha \gamma j^2 i$
k	k	$\alpha \gamma i^2 j$	$\alpha j^2 i$	$\alpha \gamma j^2 i^2$

Il est très facile de programmer cette table de multiplication dans un tableur afin de générer toutes les tables possibles :

Soit (3 choix pour i^2) \times (3 choix pour j^2) \times (2 choix pour α) \times (2 choix pour γ) = 36 tables.

On peut réduire un peu ce nombre en remarquant que i et j joue le même rôle et en imposant $i^2 \leq j^2$, ce qui laisse encore 24 possibilités, parmi lesquelles certaines sont isomorphes entre elles (cf. le tableau ci-dessous pour des exemples).

Quelques exemples :

i^2	j^2	α	γ	Nom
-1	1	1	-1	Coquaternion
1	1	1	-1	Coquaternion
-1	1	-1	-1	Quaternion hyperbolique fendus
-1	-1	-1	-1	Quaternion hyperbolique fendus
-1	0	1	-1	Dual complexe
-1	-1	1	1	Bicomplexe
-1	-1	1	-1	Quaternion
1	1	-1	-1	Quaternion hyperbolique
1	1	1	1	4-Complexe hyperbolique
-1	-1	1	1	4-Complexe circulaire

Les contraintes choisies dans ce chapitre ne permettent pas de mettre en évidence toutes les possibilités de \mathbb{R} -algèbres de dimension 4.

Par exemple :

\cdot	1	i	j	k
1	1	i	j	k
i	i	j	k	1
j	j	k	1	i
k	k	1	i	j

4-Complexe polaire

VIII.1 Quaternions \mathbb{H}

*L'ensemble des quaternions, étant non commutatif,
est le cousin excentrique qui est soigneusement évité
par tout le monde lors des réunions de famille.*

John Baez⁸⁶

VIII.1.1 Introduction

Les quaternions ont été introduits en 1843⁸⁷ par le mathématicien irlandais W. R. Hamilton (1805-1865), ce qui explique la notation \mathbb{H} , alors qu'il cherchait un moyen de représenter les points de l'espace (de dimension 3) de la même façon que les complexes permettent de représenter le plan (de dimension 2) mais il ne réussit pas à définir une multiplication avec les « bonnes » propriétés sur \mathbb{R}^3 , par contre il réussit sur \mathbb{R}^4 .

L'histoire veut que Sir Hamilton eut un flash en traversant le pont de Brougham à Cabra (faubourg de Dublin) et qu'il grava la formule principale dans une pierre du pont, comme le rappelle une plaque que l'on peut lire aujourd'hui :

*Here, as he walked by
on the 16th of October 1843
Sir William Rowan Hamilton
in a flash of genius discovered
the fundamental formula for
quaternion multiplication
 $i^2 = j^2 = k^2 = ijk = -1$
& cut it on a stone of this bridge*

VIII.1.2 Définition

L'ensemble des quaternions est une \mathbb{R} -algèbre de dimension 4, c'est à dire isomorphe à \mathbb{R}^4 en tant qu'espace vectoriel, avec les opérations naturelles d'addition et de multiplication par un réel, mais muni en plus d'une multiplication interne.

Les quaternions sont donc des nombres qui peuvent s'écrire $q = a_0 + a_1 \cdot e_1 + a_2 \cdot e_2 + a_3 \cdot e_3$, où les a_i sont des nombres réels, et les e_i une base dont la table de multiplication est donnée ci-dessous.

Pour un quaternion $q = a + a_1 \cdot e_1 + a_2 \cdot e_2 + a_3 \cdot e_3$, en posant $\vec{u} = (a_1, a_2, a_3)$ (un vecteur de \mathbb{R}^3), on peut noter un quaternion sous la forme $q = (a, \vec{u})$, l'addition et la multiplication par un réel sont les opérations naturelles, et la multiplication est définie par : $(a, \vec{u}) \times (b, \vec{v}) = (a \cdot b - \vec{u} \cdot \vec{v}, a \cdot \vec{v} + b \cdot \vec{u} + \vec{v} \wedge \vec{u})$

VIII.1.3 Mode de construction

Les quaternions sont des nombres **hypercomplexes**, une **algèbre de Clifford** ($\mathcal{C}\ell_{0,2}(\mathbb{R})$), et le résultat de la construction de **Cayley-Dickson** à partir des complexes : $\mathbb{H} = \mathcal{CD}(\mathbb{C}, 1)$.

VIII.1.4 Table de multiplication

A partir des définitions, il est immédiat que la table de multiplication des quaternions est :

·	1	e_1	e_2	e_3
1	1	e_1	e_2	e_3
e_1	e_1	-1	e_3	$-e_2$
e_2	e_2	$-e_3$	-1	e_1
e_3	e_3	e_2	$-e_1$	-1

Dans le cas des quaternions, les éléments de la base sont plus traditionnellement notés i, j et k (où le i est exactement celui de \mathbb{C}) :

86. Cité par Valentin Ovsienko (Lyon 1) comme résumé d'une conférence sur les algèbres au Laboratoire Paul Painlevé. Voir aussi : les **Réels**, les **Complexes**, les **Octonions**.

87. Gauss aurait travaillé sur les quaternions dès 1819, mais dans un travail publié seulement en 1900

·	1	<i>i</i>	<i>j</i>	<i>k</i>
1	1	<i>i</i>	<i>j</i>	<i>k</i>
<i>i</i>	<i>i</i>	-1	<i>k</i>	- <i>j</i>
<i>j</i>	<i>j</i>	- <i>k</i>	-1	<i>i</i>
<i>k</i>	<i>k</i>	<i>j</i>	- <i>i</i>	-1

VIII.1.5 Conjugué, Module, Norme, Forme Polaire et Inverse

Si $q = a_0 + a_1 \cdot i + a_2 \cdot j + a_3 \cdot k$, alors le conjugué de q est : $\bar{q} = a_0 - a_1 \cdot i - a_2 \cdot j - a_3 \cdot k$.

Le conjugué possède bien les propriétés attendues :

- $\overline{\bar{p}} = p$
- $\overline{p + q} = \bar{p} + \bar{q}$
- $\overline{p \cdot q} = \bar{q} \cdot \bar{p}$

Comme pour les nombres complexes, on peut définir une partie réelle et une partie imaginaire :

$$\Re(q) = \frac{p + \bar{p}}{2} \text{ et } \Im(q) = \frac{p - \bar{p}}{2}$$

Les quaternions dont la partie réelle est nulle sont appelés des quaternions purs.

La norme est $|q|^2 = q \cdot \bar{q} = a_0^2 + a_1^2 + a_2^2 + a_3^2$. C'est une norme multiplicative : $|p \times q| = |p| \cdot |q|$.

De plus comme $|q|^2 = 0 \Leftrightarrow q = 0$, donc l'inverse est défini par $q \neq 0 \Rightarrow q^{-1} = \frac{\bar{q}}{|q|^2}$

Tout quaternion non nul peut s'écrire de façon unique $q = |q| \cdot u$, où u est un quaternion unitaire, cette écriture est la forme polaire de q .

VIII.1.6 Propriétés algébriques

$(\mathbb{H}, +, \times)$ est un corps normé, non commutatif (par exemple $i \times j = -j \times i$).

$(\mathbb{H}, +, \times, \cdot)$ est aussi une algèbre de dimension 4 sur \mathbb{R} .

Frobenius a démontré (1877) que les seuls corps de dimension finie (en tant qu'algèbre) sur \mathbb{R} , sont \mathbb{R} , \mathbb{C} et \mathbb{H} .

Les quaternions unitaires (de norme 1) permettent de représenter simplement les rotations en 3 dimensions :

Mais d'abord quelques notations, nous omettrons ou non le symbole de la multiplication (\cdot) dans \mathbb{H} selon que celui-ci facilite ou non la lecture.

- \mathbb{R}^3 = L'espace vectoriel de dimension 3 sur \mathbb{R} ($\vec{v} = (x, y, z)$).
- \mathbb{E}^3 = L'espace Euclidien affine de dimension 3 ($X = (x, y, z)$).
- \mathbb{H} = L'ensemble des quaternions ($q = a + bi + cj + dk$).
- $\mathbb{H}_{\mathbb{R}}$ = L'ensemble des quaternions purs (dont la partie réelle est nulle)
- $1 + \mathbb{H}_{\mathbb{R}}$ = L'ensemble des quaternions de la forme $1 + ai + bj + ck$ (avec $(a, b, c) \in \mathbb{R}$).
- \mathbb{H}_1 = L'ensemble des quaternions unitaires (de norme 1).

L'application $\nu : \mathbb{R}^3 \mapsto \mathbb{H}$, définie par $\nu(\vec{v}) = xi + yj + zk$ permet d'identifier \mathbb{R}^3 et $\mathbb{H}_{\mathbb{R}}$.

L'application $\pi : \mathbb{E}^3 \mapsto \mathbb{H}$, définie par $\pi(X) = 1 + xi + yj + zk$ permet d'identifier \mathbb{E}^3 et $1 + \mathbb{H}_{\mathbb{R}}$.

Soit $X \in \mathbb{E}^3$ ($X = (x, y, z)$), $\vec{u} \in \mathbb{R}^3$, un vecteur unitaire ($\vec{u} = (\alpha, \beta, \gamma)$), $\theta \in \mathbb{R}$, les termes précédents permettent de définir un quaternion unitaire : $q_{\vec{u}, \theta} = \cos(\theta) + \alpha \sin(\theta)i + \beta \sin(\theta)j + \gamma \sin(\theta)k$ (Nous noterons $\bar{q}_{\vec{u}, \theta}$ son conjugué), alors l'application $r_{\vec{u}, \theta}$ définie par :

$r_{\vec{u}, \theta}(X) = \pi^{-1}(q_{\vec{u}, \theta} \cdot \pi(X) \cdot \bar{q}_{\vec{u}, \theta})$ est bien définie (c'est à dire que $q_{\vec{u}, \theta} \cdot \pi(X) \cdot \bar{q}_{\vec{u}, \theta} \in 1 + \mathbb{H}_{\mathbb{R}}$) et correspond à une rotation d'axe orienté \vec{u} et d'angle 2θ dans \mathbb{E}^3 .

VIII.1.7 Synonymes, Isomorphismes, Exemples

Synonyme : Quaternions circulaires.

Les quaternions aussi peuvent être vus comme une sous-algèbre de $M_2(\mathbb{C})$:

Un quaternion $q = a_0 + a_1 \cdot i + a_2 \cdot j + a_3 \cdot k$, pouvant s'écrire $q = (a_0 + a_1 \cdot i) + (a_2 + a_3 \cdot i) \cdot j$ en posant $u = a_0 + a_1 \cdot i$ et $v = a_2 + a_3 \cdot i$ (et en identifiant le i de \mathbb{H} avec le i de \mathbb{C}), alors l'application qui à q associe la matrice : $\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}$ est un isomorphisme d'algèbre.

Les quaternions peuvent aussi être vus comme une sous-algèbre de $M_4(\mathbb{R})$:

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ -a_1 & a_0 & -a_3 & a_2 \\ -a_2 & a_3 & a_0 & -a_1 \\ -a_3 & -a_2 & a_1 & a_0 \end{pmatrix}$$

Il est possible de définir la notion d'**Algèbre Quaternionique** ou algèbre de quaternions, en généralisant la définition à d'autres corps :

Soit \mathbb{K} un corps de caractéristique différente de 2, soit $(a, b) \in (\mathbb{K}^*)^2$, on note : $A = \left(\frac{a, b}{\mathbb{K}}\right)$, l'algèbre associative de dimension 4 sur \mathbb{K} engendrée par (i, j) et vérifiant les relations suivantes :

- $i^2 = a$
- $j^2 = b$
- $i \cdot j = -j \cdot i$

Il est d'usage de noter $k = ij$, ce qui donne la table de multiplication :

·	1	i	j	k
1	1	i	j	k
i	i	a	k	aj
j	j	$-k$	b	$-bi$
k	k	$-aj$	bi	$-ab$

Bien sur on retrouve aisément les Quaternions : $\mathbb{H} = \left(\frac{-1, -1}{\mathbb{R}}\right)$.

D'une façon plus générale on peut obtenir les résultats suivants :

- $a < 0 \wedge b < 0 \Rightarrow \left(\frac{a, b}{\mathbb{R}}\right) = \mathbb{H}$
- $a > 0 \vee b > 0 \Rightarrow \left(\frac{a, b}{\mathbb{R}}\right) = \mathbb{C}$
- $(a, b) \in (\mathbb{C}^*)^2 \Rightarrow \left(\frac{a, b}{\mathbb{C}}\right) = M_2(\mathbb{C})$
- $(a, b) \in (\mathbb{Q}^*)^2 \Rightarrow$ il existe une infinité de $\left(\frac{a, b}{\mathbb{C}}\right)$ non isomorphes

VIII.1.8 Utilisation en physique

On trouve les quaternions dans de nombreuses branches de la physique y compris la relativité ou la mécanique quantique.

Les quaternions peuvent être utilisés pour la représentation des couleurs et la mise au point de filtres (cf. ci-dessous *Exploration in Quaternion Colour*).

Ludwik Silberstein utilise une fonction de potentiel à un quaternion comme variable pour exprimer les équations de Maxwell sous la forme d'une seule équation différentielle.

Voir ci-dessous : *Utility of Quaternions in Physics*.

1. Solides élastiques
2. Electricité et magnétisme

3. Hydrodynamique
4. Théorie Vortex-Atome

Pour l'usage en Physique, voir, par exemple : [The quaternion group and modern physics](#).

VIII.1.9 Références

1. W. R. Hamilton, *On Quaternions; or on a new System of Imaginaries in Algebra*, Philosophical Magazine, (1844-1850), Edité par David R. Wilkins, 2000.
2. A. Macfarlane, *Principles of the Algebra of Physics*, Salem Press Publishing and Printing Co, 1891.
3. A. Macfarlane, *Vector Analysis and Quaternions*, Mathematical Monographs, John Wiley & Sons, New York, 1906.
4. A. Macfarlane, *Hyperbolic Quaternions*, Proceedings of the Royal Society at Edinburgh, 1899-1900 session, p. 169-181, 1900.
5. L. Shi, *Exploration in quaternion colour*, Thèse obtenue à : School of Computing Science - Simon Fraser University, 2005
6. K. Shoemaker, *Animating Rotation with Quaternion Curves*, SIGGRAPH '85, Volume 19, Number 3, 1985
7. S. Särkkä, *Notes on Quaternions*, 2007
8. A. Gsponer et J. P. Hurni, *Quaternions in mathematical physics (1) : Alphabetical bibliography*, Independent Scientific Research Institute, Oxford, 2008
9. A. McAulay, *Utility of Quaternions in Physics*, Macmillan And Co. London, 1893

VIII.2 Quaternions de Hurwitz $\tilde{\mathbb{H}}(\mathbb{Z})$

VIII.2.1 Introduction

Les quaternions de Hurwitz, qui seront notés $\tilde{\mathbb{H}}(\mathbb{Z})$ dans ce document, doivent leur nom à Adolf Hurwitz (1859 – 1919) un mathématicien allemand ; ils sont liés aux quaternions de Lipschitz, qui, eux, doivent leur nom à Rudolph Otto Sigismund Lipschitz un autre mathématicien allemand (1832 - 1903).

VIII.2.2 Définition

Soit \mathbb{A} un anneau, on définit $\mathbb{H}(\mathbb{A})$, comme l'algèbre construite sur le \mathbb{A} -module libre engendré par les éléments $(1_{\mathbb{A}}, i, j, k)$ en lui ajoutant une multiplication (notée \cdot) vérifiant les relations suivantes sur les éléments de la base :

- L'élément neutre de \mathbb{A} est l'élément neutre de $\mathbb{H}(\mathbb{A})$ (nous le noterons 1 et non plus $1_{\mathbb{A}}$)
- $i^2 = j^2 = k^2 = -1$
- $i \cdot j = k = -j \cdot i$
- $j \cdot k = i = -k \cdot j$
- $k \cdot i = j = -i \cdot k$

Cette algèbre est appelée algèbre des quaternions sur \mathbb{A} (les relations vérifiées par les éléments de la base étant celles qui définissent les **quaternions**).

$\mathbb{H}(\mathbb{Z})$ est donc l'algèbre des quaternions sur \mathbb{Z} , elle est appelée « Ensemble des Quaternions de Lipschitz ».

On appelle quaternions de Hurwitz, l'algèbre $\tilde{\mathbb{H}}(\mathbb{Z}) = \mathbb{H}(\mathbb{Z}) \cup \left\{ \left(\frac{1+i+j+k}{2} \right) + \mathbb{H}(\mathbb{Z}) \right\}$.

VIII.2.3 Mode de construction

Par sa définition même, les quaternions de Hurwitz sont des quaternions dont les coefficients sont, soit tous des entiers relatifs, soit tous des entiers relatifs + $\frac{1}{2}$, on peut donc aussi écrire :

$$\tilde{\mathbb{H}}(\mathbb{Z}) = \left\{ a_0 + a_1 \cdot i + a_2 \cdot j + a_3 \cdot k \mid (a_0, a_1, a_2, a_3) \in \mathbb{Z}^4 \cup \left(\frac{1}{2} + \mathbb{Z} \right)^4 \right\}$$

VIII.2.4 Table de multiplication

Nous noterons $\bar{\mathbb{H}}(\mathbb{Z}) = \tilde{\mathbb{H}}(\mathbb{Z}) \setminus \mathbb{H}(\mathbb{Z}) = \left(\frac{1+i+j+k}{2} \right) + \mathbb{H}(\mathbb{Z})$.

+	$\mathbb{H}(\mathbb{Z})$	$\bar{\mathbb{H}}(\mathbb{Z})$	×	$\mathbb{H}(\mathbb{Z})$	$\bar{\mathbb{H}}(\mathbb{Z})$
$\mathbb{H}(\mathbb{Z})$	$\mathbb{H}(\mathbb{Z})$	$\bar{\mathbb{H}}(\mathbb{Z})$	$\mathbb{H}(\mathbb{Z})$	$\mathbb{H}(\mathbb{Z})$	$\tilde{\mathbb{H}}(\mathbb{Z})$
$\bar{\mathbb{H}}(\mathbb{Z})$	$\bar{\mathbb{H}}(\mathbb{Z})$	$\mathbb{H}(\mathbb{Z})$	$\bar{\mathbb{H}}(\mathbb{Z})$	$\tilde{\mathbb{H}}(\mathbb{Z})$	$\tilde{\mathbb{H}}(\mathbb{Z})$

VIII.2.5 Conjugué, Module, Norme, Forme Polaire et Inverse

Le conjugué et la norme ont la même définition que dans les quaternions, puisque les quaternions de Hurwitz forment un sous-anneau des quaternions :

En posant $z = a_0 + a_1 \cdot i + a_2 \cdot j + a_3 \cdot k$, on obtient

$$\bar{z} = a_0 - a_1 \cdot i - a_2 \cdot j - a_3 \cdot k$$

$$N(z) = z \cdot \bar{z} = a_0^2 + a_1^2 + a_2^2 + a_3^2, \text{ dont on peut remarquer que c'est toujours un entier.}$$

Comme pour les quaternions, le conjugué vérifie $\overline{z \cdot z'} = \bar{z'} \cdot \bar{z}$ et donc la norme est multiplicative ($N(z \cdot z') = N(z)N(z')$).

On sait que $z \in \mathbb{H}^* \Rightarrow z^{-1} = \frac{\bar{z}}{N(z)}$, mais dans si $z \in \tilde{\mathbb{H}}(\mathbb{Z})^*$, alors $z^{-1} \in \tilde{\mathbb{H}}(\mathbb{Z})$ si et seulement si $N(z) = 1$, il y a donc seulement 24 éléments inversibles dans $\tilde{\mathbb{H}}(\mathbb{Z})$, dont 8 sont dans $\mathbb{H}(\mathbb{Z})$ (en rouge ci-dessous). Ces 24 éléments forment un groupe appelé *Groupe Tétrahédral Binaire* :

$$\left\{ \pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2} \right\}$$

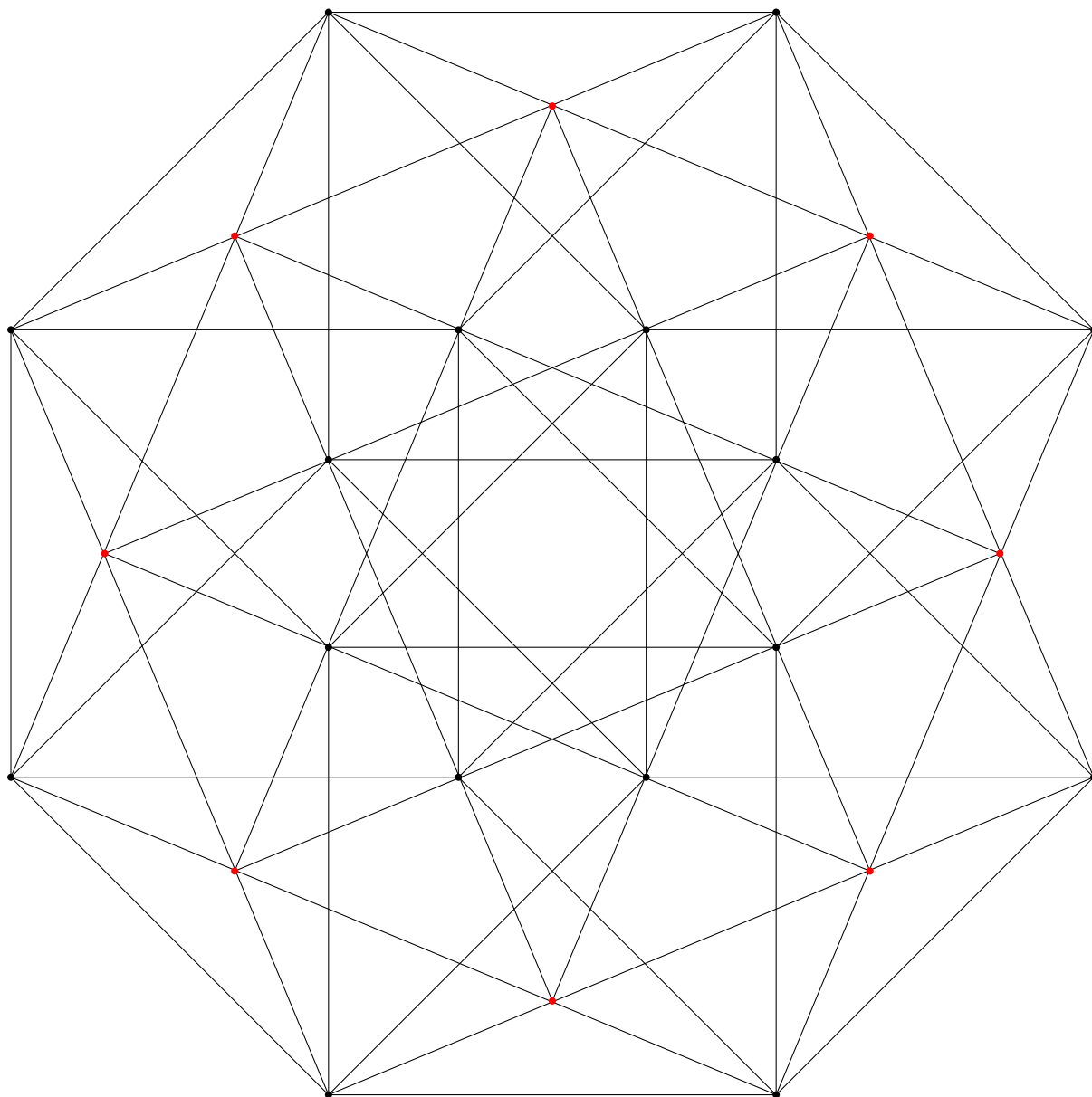


FIGURE 7 – *Projection sur \mathbb{R}^2 du groupe des unités.*

VIII.2.6 Propriétés algébriques

$(\tilde{\mathbb{H}}(\mathbb{Z}), +, \times, \cdot)$ est une algèbre associative et unitaire, mais non commutative.

$(\tilde{\mathbb{H}}(\mathbb{Z}), +, \cdot)$ est un anneau euclidien à gauche et à droite (c'est à dire que l'on peut y définir une division euclidienne à gauche et à droite).

La factorisation dans $\tilde{\mathbb{H}}(\mathbb{Z})$ est unique (ce qui veut toujours dire « à un facteur inversible près »).

VIII.2.7 Synonymes, Isomorphismes, Exemples

Les Quaternions de Lipschitz, peuvent à première vue passer pour un excellent choix pour définir la notion de « quaternions entiers »⁸⁸, mais $\mathbb{H}(\mathbb{Z})$ possède quelques défauts qui l'empêche de prétendre à ce titre :

1. Il n'est pas possible de couvrir \mathbb{R}^4 par de boules ouvertes centrées sur des points de $\mathbb{H}(\mathbb{Z})$ et de rayon 1.
2. $\mathbb{H}(\mathbb{Z})$ n'est pas euclidien (on ne peut pas diviser $(1 + i + j + k)$ par 2 avec un reste de norme < 4).
3. La factorisation dans $\mathbb{H}(\mathbb{Z})$ n'est pas unique, à un élément inversible près (par exemple $(1 + i) \cdot (1 - i) = (1 + j) \cdot (1 - j) = (1 + k) \cdot (1 - k) = 2$).

VIII.2.8 Théorème de Lagrange

Théorème de Lagrange : Tout nombre entier peut s'écrire comme la somme de quatre carrés de nombres entiers (éventuellement nuls) :

$$\forall n \in \mathbb{N} \exists (a_0, a_1, a_2, a_3) \in \mathbb{N}^4 (n = a_0^2 + a_1^2 + a_2^2 + a_3^2)$$

Il existe plusieurs démonstrations du théorème de Lagrange, mais il en existe une assez simple à l'aide des quaternions de Hurwitz.

La démonstration repose sur quelques résultats préalables :

1. 0, 1, et 2 peuvent s'écrire comme la somme de 4 carrés (trivial).
2. Si n et m peuvent s'écrire sous la forme de 4 carrés, alors nm peut s'écrire comme la somme de 4 carrés (caractère multiplicatif de la norme sur $\widetilde{\mathbb{H}}(\mathbb{Z})$).
3. Tout nombre entier premier impair peut s'écrire comme le produit de deux quaternions de Hurwitz non inversibles (cette partie repose sur un petit résultat d'arithmétique).

Le résultat 3) permet de démontrer que tout nombre premier impair est somme de 4 carrés :

Soit n un nombre premier impair et z et z' deux quaternions de Hurwitz non inversibles tels que $n = z \cdot z'$.

Donc $N(n) = N(z)N(z') = n^2$, comme ni $N(z)$ ni $N(z')$ ne peuvent être égaux à 1, on a forcément $N(z) = n$ (et $N(z') = n$).

En posant $z = a_0 + a_1 \cdot i + a_2 \cdot j + a_3 \cdot k$, on a donc $N(z) = a_0^2 + a_1^2 + a_2^2 + a_3^2 = n$.

Si $z \in \mathbb{H}(\mathbb{Z})$, le résultat voulu est atteint, mais si $z \in \left\{ \left(\frac{1 + i + j + k}{2} \right) + \mathbb{H}(\mathbb{Z}) \right\}$, le résultat nécessite encore quelques remarques.

Les a_i étant alors tous des nombre impairs divisés par 2, on peut poser :

$$a_0 = \frac{4k_0 + \alpha_0}{2} \quad ; \quad a_1 = \frac{4k_1 + \alpha_1}{2} \quad ; \quad a_2 = \frac{4k_2 + \alpha_2}{2} \quad ; \quad a_3 = \frac{4k_3 + \alpha_3}{2}$$

Où $k_i \in \mathbb{N}$ et $\alpha_i = \pm 1$.

En posant $\omega = \frac{\alpha_0 + \alpha_1 \cdot i + \alpha_2 \cdot j + \alpha_3 \cdot k}{2}$, on peut noter que $N(\omega) = 1$.

$$\text{Or } z = \omega + 2k_0 + 2k_1 \cdot i + 2k_2 \cdot j + 2k_3 \cdot k$$

$$N(z \cdot \bar{\omega}) = N(z)N(\bar{\omega}) = N(z) = n$$

$$z \cdot \bar{\omega} = \omega \cdot \bar{\omega} + (k_0 + k_1 \cdot i + k_2 \cdot j + k_3 \cdot k) \cdot (2\bar{\omega})$$

$$\text{Or } \omega \cdot \bar{\omega} = 1, 2\bar{\omega} \in \mathbb{H}(\mathbb{Z}) \text{ et } (k_0 + k_1 \cdot i + k_2 \cdot j + k_3 \cdot k) \in \mathbb{H}(\mathbb{Z})$$

Finalement $z \cdot \bar{\omega} = A_0 + A_1 \cdot i + A_2 \cdot j + A_3 \cdot k$, où $(A_0, A_1, A_2, A_3) \in \mathbb{N}^4$, et donc $n = A_0^2 + A_1^2 + A_2^2 + A_3^2$, ce qui termine la démonstration que tout nombre premier impair est somme de 4 carrés.

Ce résultat, associé aux deux premiers, ci-dessus termine la démonstration du théorème de Lagrange.

⁸⁸. Voir aussi [les entiers de Gauss](#) et [les entiers d'Eisenstein](#).

VIII.2.9 Utilisation en physique

Le groupe des unités de $\widetilde{\mathbb{H}}(\mathbb{Z})$, c'est à dire le groupe tétraédral binaire a été utilisé dans le cadre de la théorie de Yang-Mills, et aussi dans la construction de modèles par Paul Frampton et Thomas Kephart (voir ci-dessous dans les références).

VIII.2.10 Références

1. P. H. Frampton & T. W. Kephart, *Simple Non-Abelian Finite Flavor Groups and Fermion Masses*, International Journal of Modern Physics , A10 volume 32, p. 4689-4704, 1995.
2. E. Hallouin & C. Maire, *Cancellation in totally definite quaternion algebras*, Université de Toulouse Le Mirail, 2004.
3. J. C. Baez, *On Quaternions and Octonions : Their Geometry, Arithmetic, and Symmetry by John H. Conway and Derek A. Smith*, Université de Californie, 2004.
4. G. Laville & M. Paugam, *Arithmétique dans les algèbres de Clifford $\mathbb{R}_{0,q}$* , Université de Caen, Séminaire d'analyse, 2007 - 2008.
5. B. Meyer, *Représentation comme somme de carrés*, Université Bordeaux 1, Séminaire λ , 2008.
6. J. Martinet, *L'Arithmétique des algèbres de quaternions*, Université Bordeaux 1 & Ecole Polytechnique Federale de Lausanne, 2002.
7. M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics, Volume 800, Springer-Verlag, 1980.

VIII.3 Quaternions hyperboliques (Macfarlane) \mathbb{M}

VIII.3.1 Introduction

Les quaternions hyperboliques de ce chapitre ont été introduits par Alexander Macfarlane (ce qui explique la notation \mathbb{M}), mathématicien et physicien écossais (1851 - 1913) en 1890 dans son article *Principles of the Algebra of Physics* ; ils ne doivent pas être confondus avec les quaternions hyperboliques de Musès.

VIII.3.2 Définition

Les quaternions hyperboliques de Macfarlane sont une \mathbb{R} -algèbre de dimension 4 vérifiant certaines relations vérifiées par les quaternions, mais dont tous les éléments de base ont un carré égal à 1, même si cette condition entraîne la perte de l'associativité (ce qui fut reproché à Macfarlane).

VIII.3.3 Mode de construction

\mathbb{M} est un cas particulier d'**hypercomplexes**, mais n'étant pas associative, ce n'est pas une **algèbre de Clifford**.

\mathbb{M} est une \mathbb{R} -algèbre de dimension 4, dont les éléments de base seront notés $(1, i, j, k)$ et vérifient une partie des relations vérifiées par les **quaternions** :

- $i \cdot j = k = -j \cdot i$
- $j \cdot k = i = -k \cdot j$
- $k \cdot i = j = -i \cdot k$

Mais, au contraire des quaternions, ils vérifient : $i^2 = j^2 = k^2 = 1$

Les quaternions hyperboliques seront donc représentés dans cette base par :
 $z = x_0 + x_1 \cdot i + x_2 \cdot j + x_3 \cdot k$ où $(x_0, x_1, x_2, x_3) \in \mathbb{R}^4$.

VIII.3.4 Table de multiplication

La table de multiplication de \mathbb{M} est entièrement définie par les relations ci-dessus.

\cdot	1	i	j	k
1	1	i	j	k
i	i	1	k	$-j$
j	j	$-k$	1	i
k	k	j	$-i$	1

VIII.3.5 Conjugué, Module, Norme, Forme Polaire et Inverse

Si $z \in \mathbb{M}$, z s'écrit $z = x_0 + x_1 \cdot i + x_2 \cdot j + x_3 \cdot k$, et son conjugué, $\bar{z} = x_0 - x_1 \cdot i - x_2 \cdot j - x_3 \cdot k$, et la pseudo-norme $|z|^2 = x_0^2 - x_1^2 - x_2^2 - x_3^2$, ce qui correspond à la norme dans l'espace de Minkowski.

Comme $|z|^2 \in \mathbb{R}$, on peut définir un inverse (dans certains cas) : $|z| \neq 0 \Rightarrow z^{-1} = \frac{\bar{z}}{|z|^2}$.

VIII.3.6 Propriétés algébriques

$(\mathbb{M}, +, \times, \cdot)$ est une \mathbb{R} -algèbre unitaire de dimension 4 qui n'est ni associative ($((i \cdot j) \cdot j = k \cdot j = -i$, alors que $i \cdot (j \cdot j = i \cdot 1 = i)$ ni commutative ($i \cdot j = k = -(j \cdot i)$), qui ne possède ni éléments idempotents ni éléments nilpotents (non triviaux), mais qui possèdent des diviseurs de 0, par exemple $(1 - i) \cdot (1 + i) = 0$.

VIII.3.7 Utilisation en physique

- **En relativité :**

L'algèbre des quaternions hyperboliques est considéré comme la généralisation naturelle à quatre dimensions des **complexes fendus** qui permettent de formaliser les transformations de Lorentz en deux dimensions ; le groupe des transformations de Lorentz en dimension 4 sont expressibles avec \mathbb{M} .

- **En électromagnétisme :**

Les quaternions hyperboliques de Macfarlane permettent d'exprimer les équations de Maxwell de façon économique et élégante, voir *Hyperbolic Quaternion Formulation of Electromagnetism* dans les références.

- **En Mécanique quantique :**

Généralisation du concept d'interférence de probabilité (A. Khrennikov).

La description des états d'une mémoire quantique utilise \mathbb{M}

D'une façon plus générale, il est possible d'utiliser \mathbb{M} pour représenter les **algèbres de Clifford**.

VIII.3.8 Références

1. Alexander Macfarlane, *Principles of the algebra of physics*, Salem press publishing and printing co, 1894
2. S. Demir, M. Tanişli et N. Candemir, *Hyperbolic Quaternion Formulation of Electromagnetism*, Advances in Applied Clifford Algebras, Volume 20, N° 3-4, p. 547-563, Springer Bâle, 2010
3. S. Ulrych, *Spinors in the hyperbolic algebra*, Wehrenbachhalde, Zürich, Suisse, 2005
4. A. Macfarlane, *Hyperbolic Quaternions*, Proceedings of the Royal Society at Edinburgh, session 1899-1900, p. 169–181, 1900.

VIII.4 Coquaternion \mathbb{H}

VIII.4.1 Introduction

Les Coquaternions furent introduits par Sir James Cockle (1819 - 1895) en 1849 (6 ans après que Hamilton ait publié son article sur les **Quaternions**), peu après les **Tessarines**.

Les Coquaternions sont souvent appelés Quaternions fendus, ce qui explique qu'on les note \mathbb{H} , mais on trouve aussi, $\widehat{\mathbb{H}}$ et $\widetilde{\mathbb{H}}$

VIII.4.2 Définition

Comme les **Quaternions**, les Coquaternions sont des hypercomplexes de dimension 4, mais avec les relations $e_1^2 = -1$ et $e_2^2 = e_3^2 = 1$, et comme les Quaternions : $\bigwedge_{i \neq j} (e_i \cdot e_j = -e_j \cdot e_i)$.

VIII.4.3 Mode de construction

La façon la plus naturelle de construire les quaternions fendus est de les construire avec la méthode de **Cayley-Dickson**, soit en partant des **complexes** \mathbb{C} , soit en partant des **complexes fendus** \mathbb{C} , c'est à dire que les quaternions fendus sont construits comme $\mathcal{CD}(\mathbb{C}, -1)$ ou comme $\mathcal{CD}(\mathbb{C}, 1)$

VIII.4.4 Table de multiplication

·	1	e_1	e_2	e_3
1	1	e_1	e_2	e_3
e_1	e_1	-1	e_3	$-e_2$
e_2	e_2	$-e_3$	1	$-e_1$
e_3	e_3	e_2	e_1	1

plus
généralement
notée

·	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	1	$-i$
k	k	j	i	1

Les éléments de base de \mathbb{H} , sont souvent notés (1, i, j, k), plus ou moins décorés de signes diacritiques.

On peut remarquer que cette table de multiplication est entièrement définie par les relations suivantes

1. \cdot est associative
2. 1 est élément neutre
3. $i^2 = -1$
4. $j^2 = 1$
5. $ij = k = -ji$

La propriété précédente permet de montrer que l'application $\varphi : \mathbb{H} \mapsto M_2(\mathbb{R})$ définie ci-dessous s'étend naturellement en un isomorphisme de \mathbb{R} -Algèbre :

$$\varphi(i) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ et } \varphi(j) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

VIII.4.5 Conjugué, Module, Norme, Forme Polaire et Inverse

$z = a_0 + a_1 \cdot i + a_2 \cdot j + a_3 \cdot k$, alors le conjugué est $\bar{z} = a_0 - a_1 \cdot i - a_2 \cdot j - a_3 \cdot k$.

Le conjugué possède bien les propriétés attendues :

- $\overline{\bar{z}} = z$
- $\overline{z + z'} = \bar{z} + \bar{z}'$
- $\overline{z \cdot z'} = \bar{z}' \cdot \bar{z}$
- $(z \cdot z') \cdot \overline{(z \cdot z')} = (z \cdot z') \cdot (\bar{z}' \cdot \bar{z}) = z \cdot (z' \cdot \bar{z}') \cdot \bar{z} = (z' \cdot \bar{z}') \cdot (z \cdot \bar{z})$

Le module (multiplicatif) est $|z|^2 = z \cdot \bar{z} = a_0^2 + a_1^2 - a_2^2 - a_3^2$.

On peut remarquer que $|z|^2$ peut être négatif, dans ce cas, si $|z|^2 = -k$, où k est un réel positif, on pose $|z| = i\sqrt{k}$

D'après la propriété de la conjugaison vue ci-dessus, on peut déduire : $|z \cdot z'|^2 = |z|^2 \cdot |z'|^2$.

Si le module de z est différent de 0, alors z possède un inverse : $z^{-1} = \frac{\bar{z}}{z \cdot \bar{z}}$.

VIII.4.6 Propriétés algébriques

$(\mathbb{H}, +, \times, \cdot)$ est une algèbre associative, non commutative de dimension 4 sur \mathbb{R} , qui contient des idempotents non triviaux, par exemple $\left(\frac{1}{2} + \frac{1}{2}i + \frac{\sqrt{2}}{2}j\right)^2 = \left(\frac{1}{2} + \frac{1}{2}i + \frac{\sqrt{2}}{2}j\right)$, des diviseurs de 0, par exemple : $(1 - j) \times (1 + j) = 0$ et des nilpotents non triviaux, par exemple $(i + j)^2 = 0$.

On peut montrer facilement que z est un diviseur de 0 si et seulement si $|z| = 0$.

VIII.4.7 Synonymes, Isomorphismes, Exemples

Synonymes :

- Quaternions fendus.
- Para-quaternions.
- Quaternions hyperbolique de Musès.
- Antiquaternions.
- Pseudoquaternions.
- Système ex-sphérique.
- Quaternions de Gödel.

L'ensemble des coquaternions muni de l'addition, de la multiplication interne, et de la multiplication scalaire est isomorphe à $M_2(\mathbb{R})$, comme vu dans le sous chapitre [Table de multiplication](#).

$(\mathbb{H}, +, \times, \cdot)$ est aussi isomorphe à la sous-algèbre de $M_2(\mathbb{C})$, de la forme : $\begin{pmatrix} a & b \\ \bar{b} & \bar{a} \end{pmatrix}$, comme le montre l'application φ définie par :

$$\varphi(i) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \text{ et } \varphi(j) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

On peut remarquer que $z = a_0 + a_1 \cdot i + a_2 \cdot j + a_3 \cdot k = (a_0 + a_1 \cdot i) + (a_2 + a_3 \cdot i) \cdot j$, ce qui rend \mathbb{H} isomorphe à $\mathbb{C} \oplus \mathbb{C}$ (munies des opérations évidentes).

L'algèbre des quaternions fendus est aussi isomorphe à des algèbres de Clifford :

$$(\mathbb{H}, +, \times, \cdot) \approx (\mathcal{C}\ell_{1,1}(\mathbb{R}), +, \times, \cdot) \approx (\mathcal{C}\ell_{2,0}(\mathbb{R}), +, \times, \cdot)$$

VIII.4.8 Utilisation en physique

Les Coquaternions sont utilisés en traitement du signal (filtre adaptatif non linéaire).

Les points d'un espace de Minkowski, sont décrit par des Coquaternions.

Dorje C Brody et Eva-Maria Graefe, [On complexified mechanics and coquaternions](#), arXiv, 2011.

VIII.4.9 Références

1. Matvei Libine, [An Invitation to Split Quaternionic Analysis](#), Hypercomplex Analysis and Applications, Birkhäuser, Bâle, p. 161-180, 2011.
2. Anatoliy A. Pogoruy et Ramón M. Rodríguez-Dagnino, [Some Algebraic and Analytical Properties of Coquaternion Algebra](#), Advances in Applied Clifford Algebras, Volume 20 N° 1, Birkhäuser, Bâle, p. 79-84, 2008.
3. Stancho Dimiev, Mihail Konstantinov et Vladimir Todorov, [The coquaternion algebra and complex partial differential equations](#), 35th International Conference "Applications of Mathematics in Engineering and Economics" : AMEE-2009. AIP Conference Proceedings, Volume 1184, p. 177-186, 2009.

VIII.5 Bicomplexes \mathbb{C}_2

VIII.5.1 Introduction

L'ensemble des nombres bicomplexes est un cas particulier de **multicomplexes** \mathbb{C}_n (donc d'hypercomplexes).

VIII.5.2 Définition

Les nombres bicomplexes forment l'ensemble multicomplexe \mathbb{C}_2 , c'est-à-dire qu'un nombre bicomplexe peut s'écrire $z_0 + z_1 \cdot e_2$ où e_2 est un élément n'appartenant pas à \mathbb{C} tel que $e_2^2 = -1$, et où z_0 et z_1 sont des nombres complexes, ce qui explique le nom de cet ensemble.

En tant qu'espaces vectoriels, on a donc $\mathbb{C}_2 = \mathbb{C} \oplus \mathbb{C}$.

VIII.5.3 Mode de construction

Comme les **Quaternions**, les Bicomplexes sont des **hypercomplexes** de dimension 4, c'est à dire qu'ils s'écrivent $a_0 + a_1 \cdot e_1 + a_2 \cdot e_2 + a_3 \cdot e_3$ où les a_i sont des nombres réels, et les e_i des éléments de la base, mais avec les relations $e_1^2 = e_2^2 = -1$ et $e_3^2 = 1$, et contrairement aux Quaternions : $\bigwedge_{i \neq j} (e_i \cdot e_j = e_j \cdot e_i)$, c'est à dire que les bicomplexes sont commutatifs.

VIII.5.4 Table de multiplication

La table de multiplication de \mathbb{C}_2 , construite à partir de \mathbb{C} , ressemble à celle de \mathbb{C} :

·	1	e_2
1	1	e_2
e_2	e_2	-1

La même table remplie du point de vue hypercomplexe devient :

·	1	e_1	e_2	e_3
1	1	e_1	e_2	e_3
e_1	e_1	-1	e_3	- e_2
e_2	e_2	e_3	-1	- e_1
e_3	e_3	- e_2	- e_1	1

plus
généralement
notée

·	1	i	j	k
1	1	i	j	k
i	i	-1	k	- j
j	j	k	-1	- i
k	k	- j	- i	1

Les éléments de base de \mathbb{C}_2 , sont souvent notés (1, i, j, k), plus ou moins décorés de signes diacritiques (c'est le cas pour l'ensemble des \mathbb{R} -algèbres de dimension 4).

On peut remarquer que cette table de multiplication est entièrement définie par les relations suivantes

1. \cdot est associative
2. 1 est élément neutre
3. $i^2 = -1$
4. $j^2 = -1$
5. $ij = k = ji$

VIII.5.5 Conjugué, Module, Norme, Forme Polaire et Inverse

Si l'on écrit les nombres bicomplexes sous la forme $z = z_0 + z_1 \cdot e_2$, trois définitions de conjugaisons paraissent naturelles, nous les noterons \dagger_1 , \dagger_2 , et \dagger_3 :

$$\begin{aligned} z^{\dagger_1} &= \overline{z_0} + \overline{z_1} \cdot e_2 \\ z^{\dagger_2} &= z_0 - z_1 \cdot e_2 \\ z^{\dagger_3} &= \overline{z_0} - \overline{z_1} \cdot e_2 \end{aligned}$$

Où \bar{z}_i désigne la conjugaison standard sur \mathbb{C} .

On peut noter que ces trois conjugaisons ont des liens entre elles, par exemple en notant Id , l'identité de \mathbb{C}_2 , et \circ la composition habituelle des applications, on peut montrer rapidement que :

\circ	Id	\dagger_1	\dagger_2	\dagger_3
Id	Id	\dagger_1	\dagger_2	\dagger_3
\dagger_1	\dagger_1	Id	\dagger_3	\dagger_2
\dagger_2	\dagger_2	\dagger_3	Id	\dagger_1
\dagger_3	\dagger_3	\dagger_2	\dagger_1	Id

Ces trois conjugaisons possèdent les propriétés attendues :

1. $(z + z')^{\dagger_i} = z^{\dagger_i} + z'^{\dagger_i}$
2. $(z \cdot z')^{\dagger_i} = z^{\dagger_i} \cdot z'^{\dagger_i}$
3. $(z^{\dagger_i})^{\dagger_i} = z$

A chacune de ces conjugaisons, on peut associer un module bicomplexe défini par $|z|_{\dagger_i}^2 = z \cdot z^{\dagger_i}$.

Mais le plus intéressant de ces modules est $|z|_{\dagger_2}^2 = z \cdot z^{\dagger_2} = z_0^2 + z_1^2$.

Comme $|z|_{\dagger_2}^2 \in \mathbb{C}$, ce module est appelé le *module complexe*, et il est particulièrement intéressant, car z est inversible si et seulement si $|z|_{\dagger_2}^2 \neq 0$, et alors $z^{-1} = \frac{z^{\dagger_2}}{|z|_{\dagger_2}^2}$.

On peut ajouter un quatrième module, en posant $|z| = \sqrt[4]{zz^{\dagger_1}z^{\dagger_2}z^{\dagger_3}} = \sqrt{|z_0^2 + z_1^2|}$, module qui possède les propriétés suivantes :

- $|z| \in \mathbb{R}^+$, ce qui explique que ce module est appelé le *module réel* de z .
- $|z| = 0 \Leftrightarrow z$ est un diviseur de 0.
- $|z \cdot z'| = |z| \cdot |z'|$

VIII.5.6 Propriétés algébriques

La multiplication est commutative (contrairement aux quaternions), associative, distributive sur l'addition, mais elle possède des diviseurs de 0, par exemple $(1-k)(1+k) = 0$, des idempotents non triviaux, par exemple $\left(\frac{1}{2} + \frac{1}{2} \cdot k\right)^2 = \left(\frac{1}{2} + \frac{1}{2} \cdot k\right)$, mais pas d'éléments nilpotents non triviaux.

C'est donc une \mathbb{R} -algèbre commutative avec diviseurs de zéro, c'est l'unique algèbre de Clifford commutative avec diviseurs de zéro.

VIII.5.7 Synonymes, Isomorphismes, Exemples

Il est possible d'opérer un changement de base (comme dans toute algèbre) particulièrement intéressant :

Soit $z = z_0 + z_1 \cdot j$, en posant $i_0 = \frac{1+k}{2}$ et $i_1 = \frac{1-k}{2}$, on peut vérifier aisément que $i_0^2 = i_0$ et $i_1^2 = i_1$ (i_0 et i_1 sont des idempotents) et que l'on peut écrire $z = (z_0 - z_1 \cdot i) \cdot i_0 + (z_0 + z_1 \cdot i) \cdot i_1$ (les coefficients de i_0 et i_1 sont bien des nombres complexes).

La table de multiplication de cette base est :

\cdot	i_0	i_1
i_0	i_0	0
i_1	0	i_1

L'intérêt de cette base, c'est que la multiplication de deux nombres bicomplexes peut se faire coordonnée par coordonnée :

$$(\alpha \cdot i_0 + \alpha' \cdot i_1) \cdot (\beta \cdot i_0 + \beta' \cdot i_1) = (\alpha\beta) \cdot i_0 + (\alpha'\beta') \cdot i_1.$$

Ce résultat montre que l'égalité $\mathbb{C}_2 = \mathbb{C} \oplus \mathbb{C}$, est en fait valide pour la somme directe des algèbres (et pas seulement pour la somme directe des espaces vectoriels).

L'algèbre des bicomplexes est isomorphe à l'algèbre de Clifford complexe $\mathcal{C}\ell_1(\mathbb{C})$.

Les nombres bicomplexes sont isomorphes à des tessarines : $\mathcal{T}_{\mathbb{C}} = \left\{ \begin{pmatrix} u & v \\ v & u \end{pmatrix} \mid (u, v) \in \mathbb{C} \right\}$

Les propriétés qui permettent d'engendrer la table de multiplication de \mathbb{C}_2 , permet de montrer que l'application $\varphi : \mathbb{C}_2 \mapsto M_2(\mathbb{C})$ définie ci-dessous s'étend naturellement en un isomorphisme de \mathbb{C} -Algèbre :

$$\varphi(i) = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix} \text{ et } \varphi(j) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Les Bicomplexes sont parfois appelés *Quaternions coniques* ou *Système Unipodal*.

VIII.5.8 Utilisation en physique

Les bicomplexes sont utilisés en électromagnétique, en particulier pour la résolution des équations de Maxwell.

Les bicomplexes permettent de simplifier le découplage des équations de Helmholtz, dans le cadre de l'analyse des guides d'ondes courbes.

Les bicomplexes fournissent aussi un cadre pour l'étude des oscillateurs harmoniques quantiques.

VIII.5.9 Références

1. K.S. Charak, D. Rochon et N. Sharma, *Normal Families of Bicomplex Holomorphic Functions*, arXiv, 2008.
2. Stefan Rönn, *Bicomplex algebra and function theory*, arXiv, 2008.
3. Faik Babadağ, Yusuf Yayli et Nejat Ekmekci, *Homothetic Motions and Bicomplex Numbers*, Commun. Fac. Sci. Univ. Ank., Series A1, Volume 58, Number 1, p. 23-28, 2009.
4. D. Rochon et M. Shapiro, *On algebraic properties of bicomplex and hyperbolic numbers*, Anal. Univ. Oradea, fasc. math., vol. 11, p. 71-110, 2004.
5. Ahmad Zireh, *A Generalized Mandelbrot Set of Polynomials of Type E_d for Bicomplex Numbers*, Georgian Mathematical Journal, Volume 15, Number 1, p 189–194, 2008.
6. Masahiro Hashimoto, *Bicomplex electromagnetic waves in scattering and diffraction problems*, Proceedings Third International Workshop on Electromagnetic Wave Scattering, Gebze Institute of Technology Press, Turquie, 2000.

IX Algèbres de dimension 8 sur \mathbb{R}

IX.1 Octonions \mathbb{O}

*L'ensemble des Octonions est le vieil oncle fou
que personne ne laisse sortir du grenier :
il n'est pas associatif.*
John Baez ⁸⁹

IX.1.1 Introduction

L'ensemble des Octonions, qui est noté \mathbb{O} , est appelé ainsi car huit en latin se dit *octo*.

\mathbb{O} a été introduit en 1843 par John Thomas Graves, un mathématicien irlandais (1806 - 1870) ami de William Rowan Hamilton (Voir les [Quaternions](#)) et, de façon indépendante, en 1845 par Arthur Cayley, un mathématicien anglais (1821 - 1895).

IX.1.2 Définition

Les octonions sont obtenus par [la construction de Cayley-Dickson](#) à partir des quaternions $\mathbb{O} = \mathcal{CD}(\mathbb{H}, 1)$.

\mathbb{S} est donc la 4^{ième} algèbre obtenue par application successive de la [méthode de Cayley-Dickson standard](#) à partir de \mathbb{R} .

$$\mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O}$$

C'est la première algèbre de cette suite à ne pas être associative (et donc les suivantes ne le sont pas non plus).

IX.1.3 Mode de construction

Par définition de $\mathcal{CD}(\mathbb{O}, 1)$, $(\mathbb{O}, +, \times) \cong (\mathbb{H} \oplus \mathbb{H}, +, \times)$ en tant que \mathbb{R} -espaces vectoriels.

En appliquant la définition de la méthode de Cayley-Dickson on obtient la définition du produit dans $\mathbb{H} \oplus \mathbb{H} : \forall q_0 \in \mathbb{H} \forall q_1 \in \mathbb{H} \forall q'_0 \in \mathbb{H} \forall q'_1 \in \mathbb{H} (q_0, q_1) \cdot (q'_0, q'_1) = (q_0 q'_0 - \overline{q'_1} q_1, q'_1 q_0 + q_1 \overline{q'_0})$.

IX.1.4 Table de multiplication

Les définitions ci-dessus permettent de créer la table de multiplication, qui elle-même permet de définir complètement la multiplication dans \mathbb{O} .

\cdot	1	i	j	k	e_4	e_5	e_6	e_7
1	1	i	j	k	e_4	e_5	e_6	e_7
i	i	-1	k	$-j$	e_5	$-e_4$	$-e_7$	e_6
j	j	$-k$	-1	i	e_6	e_7	$-e_4$	$-e_5$
k	k	j	$-i$	-1	e_7	$-e_6$	e_5	$-e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	-1	i	j	k
e_5	e_5	e_4	$-e_7$	e_6	$-i$	-1	$-k$	j
e_6	e_6	e_7	e_4	$-e_5$	$-j$	k	-1	$-i$
e_7	e_7	$-e_6$	e_5	e_4	$-k$	$-j$	i	-1

⁸⁹. Cité par Valentin Ovsienko (Lyon 1) comme résumé d'une conférence sur les algèbres au Laboratoire Paul Painlevé. Voir aussi : les [Réels](#), les [Complexes](#), les [Quaternions](#).

IX.1.5 Le plan de Fano

Le plan de Fano (baptisé ainsi d'après le nom de Gino Fano, un mathématicien italien (1871 - 1852) qui a donné son nom au plus petit plan projectif) est un moyen considéré comme mnémotechnique de décrire la multiplication des 7 éléments purs (un octonion pur est un octonion dont la partie réelle est nulle) de la base des octonions :

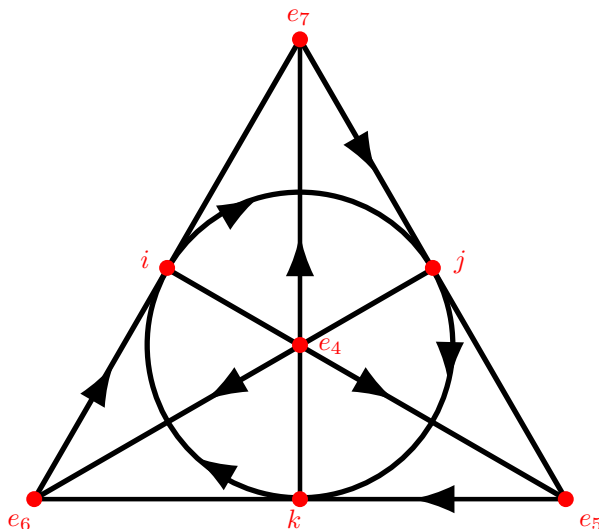


FIGURE 8 – Plan de Fano

Cette figure est constitué de 7 points (les 7 octonions pur de la base), et de 7 segments ordonnés (6 segments de droites et un cercle). Soit (a, b, c) un triplet ordonné de points situés sur un segment selon l'ordre donné par la direction de la flèche du schéma ci-dessus. La multiplication est donnée par : $a \cdot b = c$ et $b \cdot a = -c$, plus les permutations circulaires.

IX.1.6 Conjugué, Module, Norme, Forme Polaire et Inverse

Un Octonion peut s'écrire

$$o = (q_0, q_1), \text{ ou encore } o = a_0 + a_1 \cdot i + a_2 \cdot j + a_3 \cdot k + a_4 \cdot e_4 + a_5 \cdot e_5 + a_6 \cdot e_6 + a_7 \cdot e_7.$$

Et comme l'impose la méthode de Cayley-Dickson, son conjugué est défini par : $\bar{o} = (\bar{q}_0, -q_1)$. En développant, on obtient :

$$o = a_0 - a_1 \cdot i - a_2 \cdot j - a_3 \cdot k - a_4 \cdot e_4 - a_5 \cdot e_5 - a_6 \cdot e_6 - a_7 \cdot e_7.$$

Comme d'habitude dans les algèbres de Cayley-Dickson, la norme d'un Octonion est définie par : $N(o) = o \cdot \bar{o}$.

On peut vérifier rapidement que cette norme est multiplicative ($N(o \cdot o') = N(o)N(o')$) et on peut la calculer :

$$|o|^2 = N(o) = a_0^2 + a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_6^2 + a_7^2.$$

Les a_i étant des nombres réels, on voit que cette norme n'est nulle que pour $o = 0$. Ce qui permet de calculer l'inverse d'un octonion non nul : $o^{-1} = \frac{\bar{o}}{|o|^2}$.

Comme pour les complexes, on note

$\Re(o) = a_0$ la partie réelle de o et

$\Im(o) = a_1 \cdot i + a_2 \cdot j + a_3 \cdot k + a_4 \cdot e_4 + a_5 \cdot e_5 + a_6 \cdot e_6 + a_7 \cdot e_7$ la partie imaginaire de o ;

avec cette notation, un octonion est pur si et seulement si $\Re(o) = 0$.

Nous noterons aussi $\mathbb{O}^* = \mathbb{O} \setminus \{0\}$

Soit u un octonion pur de norme 1, on a donc $u \cdot \bar{u} = 1$, mais comme u est pur, on a $\bar{u} = -u$ et donc $u \cdot (-u) = 1$ ou encore $u^2 = -1$; réciproquement, si $u^2 = -1$, on peut vérifier facilement que u est un octonion pur de norme 1. L'ensemble des Octonions vérifiant $u^2 = -1$ est donc la sphère S^6 plongée dans \mathbb{R}^7 .

Soit o tel que $\Im(o) \neq 0$, on peut écrire $o = \Re(o) + \Im(o)$, ou encore $o = |o| \left(\frac{\Re(o)}{|o|} + \frac{\Im(o)}{|o|} \right)$ et finalement :

$$o = |o| \left(\frac{\Re(o)}{|o|} + \frac{|\Im(o)|}{|o|} \cdot \frac{\Im(o)}{|\Im(o)|} \right)$$

On peut vérifier facilement que $\frac{\Im(o)}{|\Im(o)|}$ est un octonion pur de norme 1, et que

$$\left(\frac{\Re(o)}{|o|} \right)^2 + \left(\frac{|\Im(o)|}{|o|} \right)^2 = 1.$$

Dans le cas $o \neq 0$, mais $\Im(o) = 0$, on peut écrire $o = |o| \left(\frac{o}{|o|} + 0 \right)$

Autrement dit, $\forall o \in \mathbb{O}^* \exists u \in \mathbb{O} \exists \alpha \in \mathbb{R} \exists \beta \in \mathbb{R} ((\alpha^2 + \beta^2 = 1) \wedge (u^2 = -1) \wedge (o = |o|(\alpha + \beta u)))$.

Comme α et β sont des réels tels que $\alpha^2 + \beta^2 = 1$, on sait qu'il existe un et un seul $\theta \in [0; 2\pi]$ ⁹⁰, tel que $\alpha = \cos(\theta)$ et $\beta = \sin(\theta)$; ce qui permet de donner la forme polaire d'un Octonion : $o = |o|(\cos(\theta) + u \sin(\theta))$.

La démonstration de la formule d'Euler dans le chapitre consacré aux **Complexes** fonctionne très bien ici, nous avons donc $\forall u \in \mathbb{O} \forall \theta \in \mathbb{R} (u^2 = -1) \Rightarrow (e^{u\theta} = \cos(\theta) + u \sin(\theta))$; ce qui permet de donner la forme exponentielle des Octonions : $o = |o|e^{u\theta}$.

On peut remarquer que la démonstration ci-dessus permet de montrer que l'algèbre engendrée par un Octonion pur non nul est isomorphe à \mathbb{C} .

IX.1.7 Propriétés algébriques

$(\mathbb{O}, +, \times, \cdot)$ est une \mathbb{R} -algèbre de dimension 8, ni commutative, ni associative, par contre elle est alternative donc flexible et associative en puissance. Elle ne contient ni élément idempotent, ni élément nilpotent, ni diviseur de 0.

Exemple de non associativité :

$$\begin{aligned} i \cdot (e_4 \cdot e_7) &= i \cdot k &= -j \\ (i \cdot e_4) \cdot e_7 &= e_5 \cdot e_7 &= j \end{aligned}$$

Rappelons le théorème de Hurwitz : Les seules algèbres normées à division (c'est à dire sans diviseur de 0) sur le corps des réels sont \mathbb{R} (**les Réels**), \mathbb{C} (**les Complexes**), \mathbb{H} (**les Quaternions**) et \mathbb{O} (**les Octonions**).

Une conséquence immédiate de ce théorème : un espace Euclidien ne peut être muni d'un produit vectoriel que s'il est de dimension 0, 1, 3 ou 7 (Les cas 0 et 1 ne n'étant guère intéressants)

Rappelons que l'on peut écrire un Quaternion $q = (a, \vec{u})$, avec la multiplication définie par :

$$(a, \vec{u}) \times (b, \vec{v}) = (a \cdot b - \vec{u} \cdot \vec{v}, a \cdot \vec{v} + b \cdot \vec{u} + \vec{v} \wedge \vec{u}).$$

Ceci permet de définir le produit vectoriel de \mathbb{R}^3 , grâce à l'homomorphisme :

$\varphi : \mathbb{R}^3 \mapsto \mathbb{H}$ défini par $\varphi(\vec{x}) = (0, \vec{x})$, en effet, il suffit de poser :

$$\forall \vec{x} \in \mathbb{R}^3 \forall \vec{y} \in \mathbb{R}^3 (\vec{x} \wedge \vec{y} = \Im(\varphi(\vec{x}) \cdot \varphi(\vec{y}))).$$

De la même façon, l'homomorphisme : $\varphi : \mathbb{R}^7 \mapsto \mathbb{O}$ défini par $\varphi(\vec{x}) = (0, \vec{x})$, permet de définir le produit vectoriel dans \mathbb{R}^7 , on pose :

$$\forall \vec{x} \in \mathbb{R}^7 \forall \vec{y} \in \mathbb{R}^7 (\vec{x} \wedge \vec{y} = \Im(\varphi(\vec{x}) \cdot \varphi(\vec{y}))).$$

L'ensemble $\{\pm 1, \pm i, \pm j, \pm k, \pm e_4, \pm e_5, \pm e_6, \pm e_7\}$ à 16 éléments n'est pas un groupe (puisque non associatif), néanmoins, c'est un quasigroupe unitaire (cf. **Structures algébriques avec une loi de composition interne**), qui vérifie en plus l'identité de Moufang (C'est donc un « Moufang loop » en anglais).

90. En fait, comme β est positif, $\theta \in [0; \pi]$, pour avoir un angle dans $[0; 2\pi]$, il faudrait privilégier certaines directions parmi les octonions purs unitaires, c'est à dire choisir une moitié de la sphère S^6 .

IX.1.8 Synonymes, Isomorphismes, Exemples

Les Octonions sont parfois appelés d'un autre nom :

- Octonions Circulaires.
- Octaves (même en anglais).
- Nombres de Cayley.
- Nombres de Cayley-Graves.
- Algèbre de Cayley.

On aurait pu contruire les Octonions à l'aide d'une multiplication particulière définie sur des « Tableaux⁹¹ » : Cette multiplication ressemble beaucoup à la multiplication des matrices, mais, dans certains cas l'ordre naturel des opérandes est changé.

$$\begin{bmatrix} \alpha_0 & \alpha_1 \\ \alpha_2 & \alpha_3 \end{bmatrix} \circ \begin{bmatrix} \beta_0 & \beta_1 \\ \beta_2 & \beta_3 \end{bmatrix} = \begin{bmatrix} \alpha_0 \cdot \beta_0 + \beta_2 \cdot \alpha_1 & \beta_1 \cdot \alpha_0 + \alpha_1 \cdot \beta_3 \\ \beta_0 \cdot \alpha_2 + \alpha_3 \cdot \beta_2 & \alpha_2 \cdot \beta_1 + \beta_3 \cdot \alpha_3 \end{bmatrix}$$

Cette multiplication permet d'écrire la définition des Octonions sous une autre forme :

$$(\mathbb{O}, +, \times, \cdot) \cong \left(\left\{ \begin{bmatrix} q_0 & q_1 \\ -q_1 & q_0 \end{bmatrix} \mid (q_0, q_1) \in \mathbb{H}^2 \right\}, +, \times, \circ \right)$$

(En remplaçant \mathbb{H} par \mathbb{A} , on obtient une redéfinition générale de la méthode de Cayley-Dickson Standard).

IX.1.9 Utilisation en physique

Susumu Okubo, *Introduction to Octonion and other Non-Associative Algebras in Physics*, Cambridge University Press, 1995.

Les Octonions trouvent des applications en théorie des cordes, relativité restreinte, logique quantique, en électrodynamique.

IX.1.10 Références

1. T. Šukilović, *Octonions and Octonionic Projective Geometry*, Faculty of Mathematics, University of Belgrade, 2010.
2. R. A. Wilson, *WWW-O : The Weird and Wonderful World of Octonions*, Queen Mary, University of London, 2004.
3. J. Löhmus, E. Paal & L. Sorgsepp, *About Nonassociativity in Physics and Cayley-Graves' Octonions*, Acta Applicandae Mathematicae, Volume 50, No 1-2, p. 3 - 31, 1998.
4. J. C. Baez, *The Octonions*, Bulletin of the American Mathematical Society, Volume 39, No 2, p. 145 - 205, 2001.
5. B. C. Chanyal, P. S. Bisht & O. P. S. Negi, *Generalized Octonion Electrodynamics*, International Journal Of Theoretical Physics, Volume 49, No 6, p. 1333-1343, 2010.

91. Voir une idée similaire : [les matrices-vecteurs de Zorn](#)

IX.2 Octonions Fendus \mathbb{O}

IX.2.1 Introduction

Les Octonions Fendus forment une extension non associative des quaternions, au même titre que les **Octonions**.

IX.2.2 Définition

Les octonions fendus sont le résultat de l'application de la **méthode de Cayley-Dickson** au corps des **Quaternions**, mais avec $\lambda = -1$ (avec la valeur $\lambda = 1$, on obtient les **Octonions standard**).

IX.2.3 Mode de construction

Les octonions fendus sont des paires de quaternions munis de deux opérations internes, d'une multiplication externe par un réel et d'une involution :

- $\mathbb{O} = \{(x_0, x_1) \mid (x_0, x_1) \in \mathbb{H}^2\}$
- $(x_0, x_1) + (y_0, y_1) = (x_0 + y_0, x_1 + y_1)$
- $(x_0, x_1) \cdot (y_0, y_1) = (x_0 \cdot y_0 + \bar{y}_1 \cdot x_1, y_1 \cdot x_0 + x_1 \cdot \bar{y}_0)$
- $a \times (x_0, x_1) = (ax_0, ax_1)$ (où a est un réel).
- $\overline{(x_0, x_1)} = (\bar{x}_0, -x_1)$, où \bar{x}_0 est le conjugué de x_0 dans \mathbb{H}

L'application $\pi : \mathbb{H} \mapsto \mathbb{O}$ définie par $\pi(x) = (x, 0)$ permet d'identifier \mathbb{H} avec un sous-ensemble de \mathbb{O} , de plus en posant $\ell = (0, 1)$, on peut écrire les éléments $x \in \mathbb{O}$ sous la forme $x = x_0 + \ell \cdot x_1$ où $(x_0, x_1) \in \mathbb{H}^2$. La famille $(1, i, j, k, \ell, \ell i, \ell j, \ell k)$ est une base naturelle de \mathbb{O} en tant que \mathbb{R} -algèbre de dimension 8, .

En appliquant la définition on obtient rapidement :

$$\begin{aligned} \ell \cdot i &= (0, 1) \cdot (i, 0) = (0 \cdot i + \bar{0} \cdot 1, 0 \cdot 0 + 1 \cdot \bar{i}) = (0, -i) \\ \ell \cdot j &= (0, 1) \cdot (j, 0) = (0 \cdot j + \bar{0} \cdot 1, 0 \cdot 0 + 1 \cdot \bar{j}) = (0, -j) \\ \ell \cdot k &= (0, 1) \cdot (k, 0) = (0 \cdot k + \bar{0} \cdot 1, 0 \cdot 0 + 1 \cdot \bar{k}) = (0, -k) \end{aligned}$$

Ces résultats vont permettre de mettre en place la table de multiplication ci-dessous (attention, la multiplication des octonions fendus n'est pas associative).

IX.2.4 Table de multiplication

En utilisant la base définie dans le paragraphe précédent, on obtient rapidement la table de multiplication suivante :

·	1	i	j	k	ℓ	ℓi	ℓj	ℓk
1	1	i	j	k	ℓ	ℓi	ℓj	ℓk
i	i	-1	k	-j	-ℓi	ℓ	-ℓk	ℓj
j	j	-k	-1	i	-ℓj	ℓk	ℓ	-ℓi
k	k	j	-i	-1	-ℓk	-ℓj	ℓi	ℓ
ℓ	ℓ	ℓi	ℓj	ℓk	1	i	j	k
ℓi	ℓi	-ℓ	-ℓk	ℓj	-i	1	k	-j
ℓj	ℓj	ℓk	-ℓ	-ℓi	-j	-k	1	i
ℓk	ℓk	-ℓj	ℓi	-ℓ	-k	j	-i	1

La partie du tableau en teinte plus ou moins rose/rouge correspond aux quaternions.

IX.2.5 Conjugué, Module, Norme, Forme Polaire et Inverse

Soit $x \in \mathbb{O}$, dans la base précédente on peut écrire :

$$x = x_0 + x_1 \cdot i + x_2 \cdot j + x_3 \cdot k + x_4 \cdot \ell + x_5 \cdot \ell i + x_6 \cdot \ell j + x_7 \cdot \ell k$$

alors son conjugué peut s'écrire :

$$\bar{x} = x_0 - x_1 \cdot i - x_2 \cdot j - x_3 \cdot k - x_4 \cdot \ell - x_5 \cdot \ell i - x_6 \cdot \ell j - x_7 \cdot \ell k$$

Un calcul un peu pénible, mais sans réelle difficulté, permet de montrer que $\overline{x \cdot y} = \bar{y} \cdot \bar{x}$.

On peut alors définir une pseudo-norme : $|x|^2 = x \cdot \bar{x}$.

Il est trivial d'établir que $|x|^2 = x_0^2 + x_1^2 + x_2^2 + x_3^2 - x_4^2 - x_5^2 - x_6^2 - x_7^2$, il est donc clair qu'il existe des éléments de \mathbb{O} non nuls dont la pseudo-norme est nulle (ce qui fait que ce n'est pas une norme).

Malgré tout cette pseudo-norme est multiplicative : $|x \cdot y| = |x||y|$.

Comme $|x|^2 \in \mathbb{R}$, l'inverse d'un élément $x \in \mathbb{O}$ peut se calculer facilement :

$$|x| \neq 0 \Rightarrow x^{-1} = \frac{\bar{x}}{|x|^2}$$

IX.2.6 Propriétés algébriques

$(\mathbb{O}, +, \cdot, \times)$ est une \mathbb{R} -algèbre unitaire de dimension 8 qui n'est ni associative ni commutative. Par contre elle est bien **alternative**.

\mathbb{O} contient des éléments :

Idempotents : $\frac{1 \pm \ell}{2}; \frac{1 \pm \ell i}{2}$; etc.

Nilpotent : $(i + \ell j)^2 = i^2 + i \cdot \ell j + \ell j \cdot i + (\ell j)^2 = -1 - \ell k + \ell k + 1 = 0$ (par exemple).

Diviseurs de 0 : $(1 - \ell) \cdot (1 + \ell)$, il n'y a donc pas que les nilpotents qui soient diviseurs de 0.

IX.2.7 Synonymes, Isomorphismes, Exemples

Les Octonions Fendus sont parfois appelés Octonions hyperboliques, on peut aussi noter que, par définition, $\mathbb{O} \cong \mathcal{CD}(\mathbb{H}, -1) \cong \mathcal{CD}(\mathbb{H}, \pm 1)$

Matrices de Zorn

$(\mathbb{O}, +, \cdot, \times)$ ne peut être représenté par des matrices, puisque le produit des matrices est associatif, néanmoins M. Zorn a proposé une forme particulière de *matrices-vecteurs*.

Une matrice-vecteur de Zorn à la forme suivante : $\begin{pmatrix} a & \vec{u} \\ \vec{v} & b \end{pmatrix}$, où $(a, b) \in \mathbb{R}^2$ et $(\vec{u}, \vec{v}) \in (\mathbb{R}^3)^2$.

L'addition de deux matrices-vecteurs se fait terme à terme, la multiplication par un scalaire se fait en multipliant tous les termes de la matrice-vecteur par ce scalaire, et la multiplication est définie par :

$$\begin{pmatrix} a & \vec{u} \\ \vec{v} & b \end{pmatrix} \cdot \begin{pmatrix} \alpha & \vec{\lambda} \\ \vec{\mu} & \beta \end{pmatrix} = \begin{pmatrix} a\alpha + \vec{u} \cdot \vec{\mu} & a\vec{\lambda} + \beta\vec{u} - \vec{v} \wedge \vec{\mu} \\ \alpha\vec{v} + b\vec{\mu} + \vec{u} \wedge \vec{\lambda} & b\beta + \vec{v} \cdot \vec{\lambda} \end{pmatrix}$$

$\vec{u} \cdot \vec{v}$ représente le produit scalaire de \vec{u} et \vec{v} , et $\vec{u} \wedge \vec{v}$ représente le produit vectoriel de \vec{u} et \vec{v} .

On peut ajouter la définition de la conjugaison, en posant :

$$z = \begin{pmatrix} a & \vec{u} \\ \vec{v} & b \end{pmatrix}, \text{ on définit son conjugué, } \bar{z} = \begin{pmatrix} b & -\vec{u} \\ -\vec{v} & a \end{pmatrix}.$$

L'algèbre des matrices de Zorn sera noté \mathcal{Z} .

Il est courant de représenter un **quaternion** $z = x_0 + x_1 \cdot i + x_2 \cdot j + x_3 \cdot k$ sous la forme (x, \vec{u}) , où $x = x_0 \in \mathbb{R}$, et $\vec{u} = (x_1, x_2, x_3) \in \mathbb{R}^3$.

En appliquant cette idée à $z \in \mathbb{O}$, en écrivant $z = z_0 + l \cdot z_1$, à partir de deux quaternions, et en utilisant deux fois la transformation ci-dessus, il est possible d'associer 2 réels et 2 vecteurs à chaque octonions fendus : $z_0 = (x_0, \vec{u}_0)$ et $z_1 = (x_1, \vec{u}_1)$.

L'application $\varphi : \mathbb{O} \mapsto \mathcal{Z}$, définie (avec les notations précédentes) par :

$$\varphi(z) = \begin{pmatrix} x_0 + x_1 & \vec{u}_0 + \vec{u}_1 \\ -\vec{u}_0 + \vec{u}_1 & x_0 - x_1 \end{pmatrix} \text{ établit un isomorphisme entre } (\mathcal{Z}, +, \cdot, \times, \bar{\cdot}) \text{ et } (\mathbb{O}, +, \cdot, \times, \bar{\cdot}).$$

IX.2.8 Utilisation en physique

Electrodynamique : les équations de Maxwell peuvent être ré-écrite dans l'algèbre des Octonions fendus. Les Octonions fendus sont aussi utilisés en théorie des cordes.

IX.2.9 Références

1. D. E. Taylor, *Constructing the split octonions*, Algorithms and Computation in Mathematics, Volume 19, p. 161-185, Springer, 2006
2. P. L. Nash, *On the structure of the split octonion algebra*, Il Nuovo Cimento, Volume 105, Number 1, p. 31-41, Springer, 1990
3. P. S. Bisht, S. Dangwal et O. P. S. Negi, *Unified Split Octonion Formulation of Dyons*, International Journal of Theoretical Physics, Volume 47, Number 9, p. 2297-2313, Springer, 2008
4. P. S. Bisht et O. P. S. Negi, *Octonion wave equation and tachyon electrodynamics*, Pramana - Journal of physics, Vol. 73, No. 3, p. 605-613, 2009
5. M. Gogberashvili, *Rotations in the Space of Split Octonions*, Hindawi Publishing Corporation, Advances in Mathematical Physics, 2009
6. P. Nurowski, *Split Octonions and Maxwell Equations*, Acta Physica Polonica, Volume 116, N° 6, p. 992-993, 2009
7. M. Gogberashvili, *Octonionic electrodynamics*, Journal of Physics, Mathematical and General, Volume 39 Number 22, 2006

IX.3 BiQuaternions \mathbb{B}

IX.3.1 Introduction

C'est Sir Hamilton qui a proposé les BiQuaternions⁹² dans un article, *On the geometrical interpretation of some results obtained by calculation with biquaternions*. publiés dans les Proceedings of the Royal Irish Academy en 1853.

IX.3.2 Définition

L'algèbre des BiQuaternions (notée \mathbb{B}) est constitués des éléments de la forme $q = z_0 + z_1 \cdot i + z_2 \cdot j + z_3 \cdot k$, où i, j et k sont les éléments de la base naturelle des quaternions, et $(z_0, z_1, z_2, z_3) \in \mathbb{C}^4$, comme l'élément de base de \mathbb{C} est traditionnellement noté i , il y a donc un conflit de notation avec le i de \mathbb{H} , aussi Hamilton pris l'habitude de noter h le i de \mathbb{C} (on trouve aussi I ou différente police de caractères dans la littérature). Dans la suite de ce chapitre, le i de \mathbb{C} sera noté \mathbf{i} , celui de \mathbb{B} et de \mathbb{H} sera noté i .

Comme \mathbb{C} est considéré comme l'ensemble des scalaires de \mathbb{B} , \mathbf{i} commute avec les éléments de base de \mathbb{H} .

On peut donc aussi représenter les éléments de \mathbb{B} sous la forme $q = q_0 + q_1 \cdot \mathbf{i}$

IX.3.3 Mode de construction

En tant que \mathbb{R} -algèbre, \mathbb{B} est de dimension 8, dont une base est : $(1, i, j, k, \mathbf{i}, \mathbf{ij}, \mathbf{ik})$.

Dans cette base un BiQuaternion s'écrit $q = x_0 + x_1 \cdot i + x_2 \cdot j + x_3 \cdot k + x_4 \cdot \mathbf{i} + x_5 \cdot \mathbf{ij} + x_6 \cdot \mathbf{ik} + x_7 \cdot \mathbf{ijk}$.

En tant que \mathbb{C} -algèbre, \mathbb{B} est de dimension 4, dont une base est : $(1, i, j, k)$

Dans cette base un BiQuaternion s'écrit $q = z_0 + z_1 \cdot i + z_2 \cdot j + z_3 \cdot k$

En tant que \mathbb{H} -algèbre, \mathbb{B} est de dimension 2, dont une base est : $(1, \mathbf{i})$

Dans cette base un BiQuaternion s'écrit $q = q_0 + q_1 \cdot \mathbf{i}$

Dans la suite de ce chapitre nous noterons x_n les éléments de \mathbb{R} , z_n ceux de \mathbb{C} et q_n ceux de \mathbb{H} .

IX.3.4 Table de multiplication

\cdot	1	i	j	k	\mathbf{i}	\mathbf{ij}	\mathbf{ik}	
1	1	i	j	k	\mathbf{i}	\mathbf{ij}	\mathbf{ik}	
i	i	-1	k	$-j$	\mathbf{ij}	\mathbf{ik}	\mathbf{ijk}	
j	j	$-k$	-1	i	\mathbf{ij}	\mathbf{ik}	\mathbf{ijk}	
k	k	j	$-i$	-1	\mathbf{ij}	\mathbf{ik}	\mathbf{ijk}	
\mathbf{i}	\mathbf{i}	\mathbf{ij}	\mathbf{ik}	\mathbf{ijk}	-1	$-i$	$-j$	$-k$
\mathbf{ij}	\mathbf{ij}	\mathbf{ijk}	\mathbf{ijk}	\mathbf{ijk}	$-i$	1	$-k$	j
\mathbf{ik}	\mathbf{ik}	\mathbf{ijk}	\mathbf{ijk}	\mathbf{ijk}	$-j$	k	1	$-i$
\mathbf{ijk}	\mathbf{ijk}	\mathbf{ijk}	\mathbf{ijk}	\mathbf{ijk}	$-k$	$-j$	i	1

Le quadrant supérieur gauche, correspond, bien évidemment aux **quaternions**.

La partie du tableau en teinte plus ou moins rose/rouge correspond aux **coquaternions**.

On peut aussi vérifier que l'algèbre engendré sur \mathbb{R} par \mathbf{ij} est isomorphe aux **complexes fendus** : $\langle \mathbf{ij} \rangle = \mathbb{C}$.

On a aussi l'isomorphisme suivant : $\langle \mathbf{i}, \mathbf{i} \rangle = \mathbb{C}_2$

IX.3.5 Conjugué, Module, Norme, Forme Polaire et Inverse

Que l'on écrive les BiQuaternions sous la forme $q = q_0 + q_1 \cdot \mathbf{i}$, ou sous la forme $q = u_0 + u_1 \cdot i + u_2 \cdot j + u_3 \cdot k$ trois définitions de conjugaisons paraissent naturelles, nous les noterons \dagger_1, \dagger_2 , et \dagger_3 :

$$\begin{array}{lcl}
 \text{Conjugaison complexe} & : & q^{\dagger_1} = q_0 - q_1 \cdot \mathbf{i} = \bar{z}_0 + \bar{z}_1 \cdot i + \bar{z}_2 \cdot j + \bar{z}_3 \cdot k \\
 \text{Conjugaison quaternionique} & : & q^{\dagger_2} = \bar{q}_0 + \bar{q}_1 \cdot \mathbf{i} = z_0 - z_1 \cdot i - z_2 \cdot j - z_3 \cdot k \\
 \text{Conjugaison hermitienne} & : & q^{\dagger_3} = \bar{q}_0 - \bar{q}_1 \cdot \mathbf{i} = \bar{z}_0 - \bar{z}_1 \cdot i - \bar{z}_2 \cdot j - \bar{z}_3 \cdot k
 \end{array}$$

92. A ne pas confondre avec les **BiQuaternions de Clifford**

Où \bar{z} et \bar{q} désigne la conjugaison standard sur \mathbb{C} et sur \mathbb{H} .

Ces trois conjugaisons possèdent les propriétés attendues (plus une autre) :

1. $(q + q')^\dagger = q^\dagger + q'^\dagger$.
2. $(q \cdot q')^\dagger = q'^\dagger \cdot q^\dagger$ si $n \in \{1, 3\}$ et $(q \cdot q')^{\dagger 2} = q^{\dagger 2} \cdot q'^{\dagger 2}$.
3. $(q^{\dagger n})^\dagger = z$.
4. $(q^{\dagger n})^{\dagger m} = q^{\dagger p}$ ou m, n et p sont tous différents.

A chacune de ces conjugaisons, on peut associer une pseudo-norme défini par $|z|_{\dagger n}^2 = z \cdot z^{\dagger n}$.

Mais le plus intéressant de ces modules est $|q|_{\dagger 1}^2 = q \cdot q^{\dagger 1} = z_0^2 + z_1^2 + z_2^2 + z_3^2$.

Par la suite $q^{\dagger 1}$ sera noté \bar{q} , et $|q|_{\dagger 1}$ sera noté $|q|$. Comme $|q|^2 \in \mathbb{C}$, ce module est appelé le *module complexe*, et il est particulièrement intéressant, car on peut démontrer facilement que q est inversible si et seulement si $|q|^2 \neq 0$, et alors $q^{-1} = \frac{\bar{q}}{|z|^2}$.

IX.3.6 Propriétés algébriques

$(\mathbb{B}, +, \times, \cdot)$ est une algèbre unitaire, associative, mais non commutative.

$$\mathbb{B} \text{ possède des éléments : } \begin{cases} \text{Diviseurs de 0, exemple} & : (1 - hi) \cdot (1 + hi) = 1 - (hi)^2 = 1 - 1 = 0 \\ \text{Idempotents, exemple} & : \left(\frac{1 \pm hi}{2}\right)^2 = \frac{1 + 1 \pm 2hi}{4} = \frac{1 \pm hi}{2} \\ \text{Nilpotents, exemple} & : (i + hj)^2 = -1 + 1 + hk - hk = 0 \end{cases}$$

IX.3.7 Synonymes, Isomorphismes, Exemples

Les BiQuaternions sont parfois appelés Octonions Coniques, en particulier dans la nomenclature de Musès.

$\mathbb{B} \cong \mathbb{C} \otimes \mathbb{H}$ ce qui explique qu'ils sont parfois appelés *quaternions complexifiés*.

\mathbb{B} est aussi une **algèbre de Clifford** : $\mathcal{Cl}_2(\mathbb{C})$ et donc $\mathbb{B} \cong M_2(\mathbb{C})$.

L'application $\varphi : \mathbb{B} \mapsto M_2(\mathbb{C})$ définie par

$$\varphi(z_0 + z_1 \cdot i + z_2 \cdot j + z_3 \cdot k) = \begin{pmatrix} z_0 + iz_1 & z_2 + iz_3 \\ -z_2 + iz_3 & z_0 - iz_1 \end{pmatrix}$$

est bien un isomorphisme établissant que $\mathbb{B} \cong M_2(\mathbb{C})$. on peut d'ailleurs remarquer que $Det(\varphi(q)) = |q|$.

En remplaçant \mathbb{C} par une autre algèbre de dimension 2, on obtient :

- Les **Quaternions Daux** : $\mathbb{D}_4 \cong \mathbb{D}_1 \otimes \mathbb{H}$
- Les **BiQuaternions Fendus** : $\mathbb{B} \cong \mathbb{C} \otimes \mathbb{H}$

IX.3.8 Utilisation en physique

Equation de Dirac (pour le changement de spin de l'électron).

Electromagnétisme et équations de Maxwell.

Mécanique Quantique (cf. le document d'E. Conte dans les références).

Représentation du groupe de Lorentz (fondamental pour la relativité), en effet les matrices de Pauli correspondent à :

- $\sigma_1 = ik$
- $\sigma_2 = ij$
- $\sigma_3 = -ii$

IX.3.9 Références

1. W. R. Hamilton, *On the geometrical interpretation of some results obtained by calculation with biquaternions.*, Proceedings of the Royal Irish Academy, p. 388–390, 1853.
2. S. J. Sangwine et D. Alfsmann, *Determination of the biquaternion divisors of zero, including the idempotents and nilpotents* , Advances in Applied Clifford Algebra volume 20, Springer Bâle, p.401-410, 2010
3. S. J. Sangwine, T. A. Ell et N. Le Bihan, *Fundamental representations and algebraic properties of biquaternions or complexified quaternions* , Advances in Applied Clifford Algebra, Springer Bâle, p.401-410, 2010
4. E. Conte, *Biquaternion Quantum Mechanics* , Advances in Applied Clifford Algebras, Volume 10, Number 2, p. 298-299, 2000

IX.4 BiQuaternions de Clifford \mathbb{R}

IX.4.1 Introduction

L'ensemble des BiQuaternions de Clifford, noté \mathbb{R} dans ce chapitre, ont été introduits en 1873 par William Kingdon Clifford, mathématicien anglais (1845-1879), dans l'article *Preliminary Sketch of Biquaternions* (cf. les références).

IX.4.2 Définition

Les **BiQuaternions de Hamilton** sont construits à partir des **quaternions** et des **complexes**, en remplaçant les réels de la définition des quaternions par des nombres complexes ($\mathbb{B} = \mathbb{H} \otimes \mathbb{C}$), pour les BiQuaternions de Clifford, on remplace les réels par des **complexes fendus**, ce sont donc aussi des hypercomplexes et des **tessarines**⁹³.

Dans la suite de ce chapitre nous noterons x_n les éléments de \mathbb{R} , z_n ceux de \mathbb{C} et q_n ceux de \mathbb{H} .

Les BiQuaternions de Clifford sont donc de la forme $q = z_0 + z_1 \cdot i + z_2 \cdot j + z_3 \cdot k$ où $(z_0, z_1, z_2, z_3) \in \mathbb{C}$, et (i, j, k) sont les éléments de la base naturelle des Quaternions.

En notant j l'élément de \mathbb{C} vérifiant $j^2 = 1$, on peut écrire

$$q = (x_{00} + j \cdot x_{01}) + (x_{10} + j \cdot x_{11}) \cdot i + (x_{20} + j \cdot x_{21}) \cdot j + (x_{30} + j \cdot x_{31}) \cdot k$$

En regroupant autrement les termes précédents, un tel nombre peut aussi être écrit sous la forme : $q = q_0 + j \cdot q_1$, avec q_0 et q_1 dans le corps non commutatif des quaternions d'Hamilton.

ou encore : $q = x_0 + x_1 \cdot e_1 + x_2 \cdot e_2 + x_3 \cdot e_3 + x_4 \cdot e_4 + x_5 \cdot e_5 + x_6 \cdot e_6 + x_7 \cdot e_7$

L'ensemble des BiQuaternions de Clifford forme une algèbre de Clifford de dimension 8 sur \mathbb{R} .

IX.4.3 Mode de construction

On peut construire \mathbb{R} de trois façons différentes assez naturelles :

- Une algèbre de Clifford : $\mathcal{Cl}_{0,3}$
- La complexification de \mathbb{H} : $\mathbb{H} \otimes \mathbb{C}$
- La somme directe de \mathbb{H} avec elle-même : $\mathbb{H} \oplus \mathbb{H}$

IX.4.4 Table de multiplication

En prenant le point de vue de l'**algèbre de Clifford** $\mathbb{R} = \mathcal{Cl}_{0,3}$, nous noterons (e_1, e_2, e_3) , la base de \mathbb{R}^3 ; les vecteurs, bivecteurs et pseudo-scalaires seront écrit en prenant comme convention $e_{ij} = e_i e_j$.

\cdot	1	e_1	e_2	e_3	e_{12}	e_{23}	e_{31}	e_{123}
1	1	e_1	e_2	e_3	e_{12}	e_{23}	e_{31}	e_{123}
e_1	e_1	-1	e_{12}	$-e_{31}$	$-e_2$	e_{123}	e_3	$-e_{23}$
e_2	e_2	$-e_{12}$	-1	e_{23}	e_1	$-e_3$	e_{123}	$-e_{31}$
e_3	e_3	e_{31}	$-e_{23}$	-1	e_{123}	e_2	$-e_1$	$-e_{12}$
e_{12}	e_{12}	e_2	$-e_1$	e_{123}	-1	e_{31}	$-e_{23}$	$-e_3$
e_{23}	e_{23}	e_{123}	e_3	$-e_2$	$-e_{31}$	-1	e_{12}	$-e_1$
e_{31}	e_{31}	$-e_3$	e_{123}	e_1	e_{23}	$-e_{12}$	-1	$-e_2$
e_{123}	e_{123}	$-e_{23}$	$-e_{31}$	$-e_{12}$	$-e_3$	$-e_1$	$-e_2$	1

Table de multiplication de $\mathcal{Cl}_{0,3}$.

La partie du tableau en teinte plus ou moins rose/rouge correspond aux quaternions.

93. Plus précisément : $\mathcal{T}_{\mathbb{H}}$

En prenant le point de vue $\mathbb{R} = \mathbb{H} \otimes \mathbb{C}$

·	1	<i>i</i>	<i>j</i>	<i>k</i>	<i>j</i>	<i>j · i</i>	<i>j · j</i>	<i>j · k</i>
1	1	<i>i</i>	<i>j</i>	<i>k</i>	<i>j</i>	<i>j · i</i>	<i>j · j</i>	<i>j · k</i>
<i>i</i>	<i>i</i>	-1	<i>k</i>	<i>-j</i>	<i>j · i</i>	<i>-j</i>	<i>j · k</i>	<i>-j · j</i>
<i>j</i>	<i>j</i>	<i>-k</i>	-1	<i>i</i>	<i>j · j</i>	<i>-j · k</i>	<i>-j</i>	<i>j · i</i>
<i>k</i>	<i>k</i>	<i>j</i>	<i>-i</i>	-1	<i>j · k</i>	<i>j · j</i>	<i>-j · i</i>	<i>-j</i>
<i>j</i>	<i>j</i>	<i>j · i</i>	<i>j · j</i>	<i>j · k</i>	1	<i>i</i>	<i>j</i>	<i>k</i>
<i>j · i</i>	<i>j · i</i>	<i>-j</i>	<i>j · k</i>	<i>-j · j</i>	<i>i</i>	-1	<i>k</i>	<i>-j</i>
<i>j · j</i>	<i>j · j</i>	<i>-j · k</i>	<i>-j</i>	<i>j · i</i>	<i>j</i>	<i>-k</i>	-1	<i>i</i>
<i>j · k</i>	<i>j · k</i>	<i>j · j</i>	<i>-j · i</i>	<i>-j</i>	<i>k</i>	<i>j</i>	<i>-i</i>	-1

Table de multiplication de $\mathcal{Cl}_{0,3}$.

La partie du tableau en teinte plus ou moins rose/rouge correspond aux quaternions.

En prenant le point de vue $\mathbb{R} = \mathbb{H} \oplus \mathbb{H}$

·	(1, 0)	(<i>i</i> , 0)	(<i>j</i> , 0)	(<i>k</i> , 0)	(0, 1)	(0, <i>i</i>)	(0, <i>j</i>)	(0, <i>k</i>)
(1, 0)	(1, 0)	(<i>i</i> , 0)	(<i>j</i> , 0)	(<i>k</i> , 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)
(<i>i</i> , 0)	(<i>i</i> , 0)	(-1, 0)	(<i>k</i> , 0)	(<i>-j</i> , 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)
(<i>j</i> , 0)	(<i>j</i> , 0)	(<i>-k</i> , 0)	(-1, 0)	(<i>i</i> , 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)
(<i>k</i> , 0)	(<i>k</i> , 0)	(<i>j</i> , 0)	(<i>-i</i> , 0)	(-1, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)
(0, 1)	(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 1)	(0, <i>i</i>)	(0, <i>j</i>)	(0, <i>k</i>)
(0, <i>i</i>)	(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, <i>i</i>)	(-0, 1)	(0, <i>k</i>)	(-0, <i>j</i>)
(0, <i>j</i>)	(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, <i>j</i>)	(-0, <i>k</i>)	(-0, 1)	(0, <i>i</i>)
(0, <i>k</i>)	(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, <i>k</i>)	(0, <i>j</i>)	(-0, <i>i</i>)	(-0, 1)

Table de multiplication de $\mathbb{H} \oplus \mathbb{H}$.

La partie du tableau en teinte plus ou moins rose/rouge correspond aux quaternions, et la partie en bleu/cyan aussi, on retrouve bien les deux copies de \mathbb{H} .

Attention, dans cette façon de présenter les choses, (1, 0) n'est pas l'élément neutre (c'est (1, 1)).

IX.4.5 Conjugué, Module, Norme, Forme Polaire et Inverse

En prenant le point de vue $\mathbb{R} = \mathbb{H} \oplus \mathbb{H}$, il apparaît immédiatement que $q = (q_0, q_1)$ admet un inverse si et seulement si $q_0 q_1 \neq 0$, et dans ce cas : $(q_0, q_1)^{-1} = \left(\frac{\overline{q_0}}{|q_0|^2}, \frac{\overline{q_1}}{|q_1|^2} \right)$ ⁹⁴.

IX.4.6 Propriétés algébriques

$(\mathbb{R}, +, \times, \cdot)$ est une \mathbb{R} -algèbre de dimension 8, associative, unitaire, non commutative, possédant des diviseurs de 0, des éléments idempotents et des éléments nilpotents (ces trois types d'éléments sont immédiatement visibles dans la table de multiplication de $\mathbb{H} \oplus \mathbb{H}$).

IX.4.7 Synonymes, Isomorphismes, Exemples

- Elliptic BiQuaternions.
- Octonions (dénomination à éviter).
- DyQuaternions.

⁹⁴. Dans cette équation la conjugaison et la norme sont celles de l'ensemble des quaternions.

L'application $\varphi : \mathcal{Cl}_{0,3} \mapsto \mathbb{H} \otimes \mathbb{C}$ définie par :

$$\begin{array}{llll} \varphi(1) = 1 & \varphi(e_1) = i & \varphi(e_2) = j & \varphi(e_3) = -j \cdot k \\ \varphi(e_{12}) = k & \varphi(e_{23}) = -j \cdot i & \varphi(e_{31}) = -j \cdot j & \varphi(e_{123}) = j \end{array}$$

se prolonge naturellement en un isomorphisme de \mathbb{R} -algèbre.

Soit $q = (q_0 + j \cdot q_1) \in \mathbb{H} \otimes \mathbb{C}$.

L'application $\psi : \mathbb{H} \otimes \mathbb{C} \mapsto \mathbb{H} \oplus \mathbb{H}$ définie par :

$\psi(q_0 + j \cdot q_1) = (q_0 + q_1, q_0 - q_1)$ est un isomorphisme de \mathbb{R} -algèbre.

On peut vérifier, pour la multiplication :

$$\begin{aligned} & \psi((q_0 + j \cdot q_1) \cdot (q'_0 + j \cdot q'_1)) = \\ & \psi((q_0 q'_0 + q_1 q'_1) + j \cdot (q_0 q'_1 + q_1 q'_0)) = \\ & ((q_0 q'_0 + q_1 q'_1) + (q_0 q'_1 + q_1 q'_0), (q_0 q'_0 + q_1 q'_1) - (q_0 q'_1 + q_1 q'_0)). \end{aligned}$$

$$\begin{aligned} & \psi(q_0 + j \cdot q_1) \cdot \psi(q'_0 + j \cdot q'_1) = \\ & (q_0 + q_1, q_0 - q_1) \cdot (q'_0 + q'_1, q'_0 - q'_1) = \\ & ((q_0 + q_1)(q'_0 + q'_1), (q_0 - q_1)(q'_0 - q'_1) = \\ & (q_0 q'_0 + q_0 q'_1 + q_1 q'_0 + q_1 q'_1, q_0 q'_0 - q_0 q'_1 - q_1 q'_0 + q_1 q'_1). \end{aligned}$$

Et donc finalement : $\psi((q_0 + j \cdot q_1) \cdot (q'_0 + j \cdot q'_1)) = \psi(q_0 + j \cdot q_1) \cdot \psi(q'_0 + j \cdot q'_1)$.

IX.4.8 Utilisation en physique

Les BiQuaternions de Clifford sont utilisés pour la description de certains mouvements en robotique.

IX.4.9 Références

1. W. K. Clifford, *Preliminary Sketch of Biquaternions*, Paper XX, Proceedings of the London Mathematical Society, p. 381-395, 1873.
2. M. Shoham, *A note on Clifford's Derivation of Bi-Quaternions*, 10th World Congress on the Theory of Machines and Mechanisms, Oulu, Finlande, 1999

IX.5 Quaternions duaux \mathbb{D}_4

IX.5.1 Introduction

L'ensemble des nombres quaternions duaux sera noté \mathbb{D}_4 ici (la notation n'est pas stable, on trouve \mathbf{H} , \mathcal{H} , \mathbb{H}_ε , $\mathbb{H}_{\mathbb{D}_1}$, $\mathbb{D}_{1\mathbb{H}}$, \dots , ces trois dernières notations s'expliquent par les modes de constructions de \mathbb{D}_4).

La notation \mathbb{D}_4 indique que cet ensemble est la « dualisation » d'une \mathbb{R} -algèbre de dimension 4.

La notion de « nombres duaux » remonte à W. K. Clifford (1873), et E. Study (1903).

IX.5.2 Définition

L'ensemble \mathbb{D}_4 est une algèbre de dimension 8 sur \mathbb{R} , mais aussi une algèbre de dimension 4 sur \mathbb{D}_1 (**les nombres duaux**), ou encore une algèbre de dimension 2 sur \mathbb{H} (**les quaternions**), dans les deux derniers cas les éléments de base sont $(1, i, j, k, \varepsilon, i\varepsilon, j\varepsilon, k\varepsilon)$. A noter que dans les deux cas, ε , élément de base de \mathbb{D}_1 , commute avec les éléments (i, j, k) de la base des quaternions.

IX.5.3 Mode de construction

Les deux modes habituelles de constructions reposent sur la définition de \mathbb{D}_4 en tant qu'algèbre de dimension 2 ou 4 :

$z \in \mathbb{D}_4 \Leftrightarrow \exists (q_0, q_1) \in \mathbb{H}^2 (z = q_0 + q_1 \cdot \varepsilon)$. Dans ce cas la notation $\mathbb{D}_{1\mathbb{H}}$ est pleinement justifiée.

$z \in \mathbb{D}_4 \Leftrightarrow \exists (d_0, d_1, d_2, d_3) \in \mathbb{D}_1^4 (z = d_0 + d_1 \cdot i + d_2 \cdot j + d_3 \cdot k)$. Dans ce cas la notation $\mathbb{H}_{\mathbb{D}_1}$ est pleinement justifiée.

IX.5.4 Table de multiplication

On pourrait donner les deux tables de multiplications qui correspondent à $\mathbb{D}_{1\mathbb{H}}$ et $\mathbb{H}_{\mathbb{D}_1}$, mais ce sont tout simplement les tables de multiplication des **nombres duaux** et des **quaternions** respectivement.

La table de multiplication la plus intéressante est celle d'une base de \mathbb{D}_4 en tant que \mathbb{R} -algèbre de dimension 8 :

·	1	<i>i</i>	<i>j</i>	<i>k</i>	ε	εi	εj	εk
1	1	<i>i</i>	<i>j</i>	<i>k</i>	ε	εi	εj	εk
<i>i</i>	<i>i</i>	-1	<i>k</i>	- <i>j</i>	εi	$-\varepsilon$	εk	$-\varepsilon j$
<i>j</i>	<i>j</i>	- <i>k</i>	-1	<i>i</i>	εj	$-\varepsilon k$	$-\varepsilon$	εi
<i>k</i>	<i>k</i>	<i>j</i>	- <i>i</i>	-1	εk	εj	$-\varepsilon i$	$-\varepsilon$
ε	ε	εi	εj	εk	0	0	0	0
εi	εi	$-\varepsilon$	εk	$-\varepsilon j$	0	0	0	0
εj	εj	$-\varepsilon k$	$-\varepsilon$	εi	0	0	0	0
εk	εk	εj	$-\varepsilon i$	$-\varepsilon$	0	0	0	0

IX.5.5 Conjugué, Module, Norme, Forme Polaire et Inverse

Si l'on écrit les éléments de \mathbb{D}_4 sous la forme $q = q_0 + q_1 \cdot \varepsilon$, trois définitions de conjugaison paraissent naturelles, nous les noterons \dagger_1 , \dagger_2 , et \dagger_3 :

$$\begin{aligned} q^{\dagger_1} &= \overline{q_0} + \overline{q_1} \cdot \varepsilon \\ q^{\dagger_2} &= q_0 - q_1 \cdot \varepsilon \\ q^{\dagger_3} &= \overline{q_0} - \overline{q_1} \cdot \varepsilon \end{aligned}$$

Où $\overline{q_i}$ désigne la conjugaison standard sur \mathbb{H} .

On peut noter que ces trois conjugaisons ont des liens entre elles, par exemple en notant Id , l'identité de \mathbb{D}_4 , et \circ la composition habituelle des applications, on peut montrer rapidement que :

\circ	Id	\dagger_1	\dagger_2	\dagger_3
Id	Id	\dagger_1	\dagger_2	\dagger_3
\dagger_1	\dagger_1	Id	\dagger_3	\dagger_2
\dagger_2	\dagger_2	\dagger_3	Id	\dagger_1
\dagger_3	\dagger_3	\dagger_2	\dagger_1	Id

Ces trois conjugaisons possèdent (presque) les propriétés attendues :

1. $(q + q')^{\dagger i} = q^{\dagger i} + q'^{\dagger i}$
2. $(q \cdot q')^{\dagger 1} = q^{\dagger 1} \cdot q'^{\dagger 1}$; $(q \cdot q')^{\dagger 2} = q^{\dagger 2} \cdot q'^{\dagger 2}$; $(q \cdot q')^{\dagger 3} = q^{\dagger 3} \cdot q'^{\dagger 3}$
3. $(q^{\dagger i})^{\dagger i} = q$

La conjugaison \dagger_1 est intéressante car le module associé $|q|_{\dagger_1}^2 = q \cdot q^{\dagger 1}$ permet de donner une condition nécessaire et suffisante pour que q ait un inverse, et permet aussi de le calculer :

Si $q = q_0 + q_1 \cdot \varepsilon$, alors $|q|_{\dagger_1}^2 = q \cdot q^{\dagger 1} = (q_0 + q_1 \cdot \varepsilon) \cdot (\overline{q_0} + \overline{q_1} \cdot \varepsilon)$.

En développant on obtient $|q|_{\dagger_1}^2 = q_0 \overline{q_0} + (q_0 \overline{q_1} + q_1 \overline{q_0}) \cdot \varepsilon + q_1 \overline{q_1}$, ce qui peut s'écrire $|q|_{\dagger_1}^2 = q_0 \overline{q_0} + ((q_0 \overline{q_1} + \overline{q_0 q_1})) \cdot \varepsilon$.

On peut remarquer que $|q|_{\dagger_1}^2 \in \mathbb{D}_1$ et est inversible si et seulement si $q_0 \overline{q_0} \neq 0 \Leftrightarrow q_0 \neq 0 \Leftrightarrow |q|_{\dagger_1}^2 \neq 0$

Et finalement q est inversible si et seulement si $|q|_{\dagger_2}^2 \neq 0$, et alors $q^{-1} = \frac{q^{\dagger 2}}{|q|_{\dagger_2}^2}$.

Par la suite, seule \dagger_3 sera utilisée, et sera notée comme d'habitude : $q^{\dagger 3} = \overline{q}$.

IX.5.6 Propriétés algébriques

Nous allons montrer l'intérêt de \mathbb{D}_4 pour exprimer des rotations et des translations dans un espace affine euclidien de dimension 3, ce qui explique son utilisation en robotique.

Mais d'abord quelques rappels concernant les **quaternions**.

Nous omettrons ou non le symbole de la multiplication (\cdot) dans \mathbb{H} selon que celui-ci facilite ou non la lecture. Nous noterons :

- \mathbb{R}^3 = L'espace vectoriel de dimension 3 sur \mathbb{R} ($\vec{v} = (x, y, z)$).
- \mathbb{E}^3 = L'espace Euclidien affine de dimension 3 ($X = (x, y, z)$).
- \mathbb{H} = L'ensemble des quaternions ($q = a + bi + cj + dk$).
- $\mathbb{H}_{\mathfrak{S}}$ = L'ensemble des quaternions purs (dont la partie réelle est nulle)
- $1 + \mathbb{H}_{\mathfrak{S}}$ = L'ensemble des quaternions de la forme $1 + ai + bj + ck$ (avec $(a, b, c) \in \mathbb{R}$).
- \mathbb{H}_1 = L'ensemble des quaternions unitaires (de norme 1).

L'application $\nu : \mathbb{R}^3 \mapsto \mathbb{H}$, définie par $\nu(\vec{v}) = xi + yj + zk$ permet d'identifier \mathbb{R}^3 et $\mathbb{H}_{\mathfrak{S}}$.

L'application $\pi : \mathbb{E}^3 \mapsto \mathbb{H}$, définie par $\pi(X) = 1 + xi + yj + zk$ permet d'identifier \mathbb{E}^3 et $1 + \mathbb{H}_{\mathfrak{S}}$.

Soit $X \in \mathbb{E}^3$ et $\vec{v} \in \mathbb{R}^3$, alors l'application $t_{\vec{v}} : \mathbb{E}^3 \mapsto \mathbb{E}^3$ définie par :

$t_{\vec{v}}(X) = \pi^{-1}(\pi(X) + \nu(\vec{v}))$ est bien définie (c'est à dire que $\pi(X) + \nu(\vec{v}) \in 1 + \mathbb{H}_{\mathfrak{S}}$) et correspond à une translation dans \mathbb{E}^3 .

Soit $X \in \mathbb{E}^3$ ($X = (x, y, z)$), $\vec{u} \in \mathbb{R}^3$, un vecteur unitaire ($\vec{u} = (\alpha, \beta, \gamma)$), $\theta \in \mathbb{R}$, les termes précédents permettent de définir un quaternion unitaire : $q_{\vec{u}, \theta} = \cos(\theta) + \alpha \sin(\theta)i + \beta \sin(\theta)j + \gamma \sin(\theta)k$ (Nous noterons $\overline{q_{\vec{u}, \theta}}$ son conjugué), alors l'application $r_{\vec{u}, \theta}$ définie par :

$r_{\vec{u}, \theta}(X) = \pi^{-1}(q_{\vec{u}, \theta} \cdot \pi(X) \cdot \overline{q_{\vec{u}, \theta}})$ est bien définie (c'est à dire que $q_{\vec{u}, \theta} \cdot \pi(X) \cdot \overline{q_{\vec{u}, \theta}} \in 1 + \mathbb{H}_{\mathfrak{S}}$) et correspond à une rotation d'axe orienté \vec{u} et d'angle 2θ dans \mathbb{E}^3 .

Il est, bien évidemment, impossible de « coder » une translation suivie d'une rotation (ou le contraire) avec un seul quaternion, nous allons voir que c'est possible avec les quaternions duaux.

Comme il est possible, de façon très naturelle d'identifier \mathbb{H} et un sous-ensemble de \mathbb{D}_4 ($\varphi : \mathbb{H} \mapsto \mathbb{D}_4$ définie par $\varphi(q) = q + 0 \cdot \varepsilon$), nous pouvons étendre un peu les définitions précédentes :

L'application $\nu : \mathbb{R}^3 \mapsto \mathbb{D}_4$, définie par $\nu(\vec{v}) = \varepsilon(xi + yj + zk)$ permet d'identifier \mathbb{R}^3 et $\varepsilon\varphi(\mathbb{H}_{\mathfrak{S}})$.

L'application $\pi : \mathbb{E}^3 \mapsto \mathbb{D}_4$, définie par $\pi(X) = 1 + \varepsilon(xi + yj + zk)$ permet d'identifier \mathbb{E}^3 et $1 + \varepsilon\varphi(\mathbb{H}_{\mathfrak{S}})$.

Soit $X \in \mathbb{E}^3$ ($X = (x, y, z)$), $\vec{u} \in \mathbb{R}^3$, un vecteur unitaire ($\vec{u} = (\alpha, \beta, \gamma)$), $\vec{v} \in \mathbb{R}^3$ un vecteur quelconque ($\vec{v} = (a, b, c)$), $\theta \in \mathbb{R}$.

Posons $q_{\vec{u},\theta} = \cos(\theta) + \alpha \sin(\theta)i + \beta \sin(\theta)j + \gamma \sin(\theta)k$ (donc $q_{\vec{u},\theta} \in \varphi(\mathbb{H}_1)$), nous noterons $\bar{q}_{\vec{u},\theta}$ son conjugué), alors l'application $s_{\vec{u},\theta,\vec{v}}$ définie par :

$$s_{\vec{u},\theta,\vec{v}}(X) = \pi^{-1}\left(\left(q_{\vec{u},\theta} + \frac{1}{2}\nu(\vec{v})q_{\vec{u},\theta}\right) \cdot \pi(X) \cdot \overline{\left(q_{\vec{u},\theta} + \frac{1}{2}\nu(\vec{v})q_{\vec{u},\theta}\right)}\right)$$

est bien définie (c'est à dire, en posant $q' = \left(q_{\vec{u},\theta} + \frac{1}{2}\nu(\vec{v})q_{\vec{u},\theta}\right) \cdot \pi(X) \cdot \overline{\left(q_{\vec{u},\theta} + \frac{1}{2}\nu(\vec{v})q_{\vec{u},\theta}\right)}$) que $q' \in 1 + \varepsilon\varphi(\mathbb{H}_3)$, de plus la transformation qui fait passer de X à $s_{\vec{u},\theta,\vec{v}}(X)$ correspond à une rotation d'axe orienté \vec{u} et d'angle 2θ suivi d'une translation de vecteur \vec{v} dans \mathbb{E}^3 .

Pour les calculs, nous allons alléger un peu les notations en posant :

1. $q = q_{\vec{u},\theta}$ (q est un quaternion unitaire, $q\bar{q}$).
2. $\varepsilon v = \nu(\vec{v})$ (v est un quaternion pur, par conséquent $\bar{v} = -v$).
3. $1 + \varepsilon X = \pi(X)$.

$$q' = \left(q + \frac{1}{2}\varepsilon v q\right)(1 + \varepsilon X)\overline{\left(q + \frac{1}{2}\varepsilon v q\right)}$$

$$q' = \left(q + \frac{1}{2}\varepsilon v q\right)(1 + \varepsilon X)(\bar{q} - \frac{1}{2}\varepsilon \bar{q} \bar{v})$$

$$q' = \left(q + \frac{1}{2}\varepsilon v q + \varepsilon q X\right)(\bar{q} + \frac{1}{2}\varepsilon \bar{q} \bar{v})$$

$$q' = q\bar{q} + \frac{1}{2}\varepsilon v q\bar{q} + \varepsilon q X\bar{q} + \frac{1}{2}\varepsilon q\bar{q} \bar{v}$$

Or q est unitaire, donc $q' = 1 + \frac{1}{2}\varepsilon v + \varepsilon q X\bar{q} + \frac{1}{2}\varepsilon v$

$$q' = 1 + \varepsilon(qX\bar{q} + v)$$

Ce qui correspond bien, dans \mathbb{E}^3 , à une rotation (celle définie par q) suivie d'une translation (celle définie par v).

Dans l'autre sens, on pose :

$$s_{\vec{v},\vec{u},\theta}(X) = \pi^{-1}\left(\left(q_{\vec{u},\theta} + \frac{1}{2}q_{\vec{u},\theta}\nu(\vec{v})\right) \cdot \pi(X) \cdot \overline{\left(q_{\vec{u},\theta} + \frac{1}{2}q_{\vec{u},\theta}\nu(\vec{v})\right)}\right)$$

$$q' = \left(q + \frac{1}{2}\varepsilon q v\right)(1 + \varepsilon X)\overline{\left(q + \frac{1}{2}\varepsilon q v\right)}$$

$$q' = \left(q + \frac{1}{2}\varepsilon q v\right)(1 + \varepsilon X)(\bar{q} - \frac{1}{2}\varepsilon \bar{v} \bar{q})$$

$$q' = \left(q + \frac{1}{2}\varepsilon q v + \varepsilon q X\right)(\bar{q} + \frac{1}{2}\varepsilon \bar{v} \bar{q})$$

$$q' = q\bar{q} + \frac{1}{2}\varepsilon q v \bar{q} + \varepsilon q X\bar{q} + \frac{1}{2}\varepsilon q v \bar{q}$$

$$q' = 1 + \varepsilon(qX\bar{q} + qv\bar{q})$$

$$q' = 1 + \varepsilon(q(X + v)\bar{q})$$

Ce qui correspond bien à une translation (celle définie par v) suivie d'une rotation (celle définie par q).

IX.5.7 Synonymes, Isomorphismes, Exemples

On trouve parfois les noms suivants à la place de quaternions duaux :

- Dual Bi-Quaternions.
- Study Bi-Quaternions.
- Clifford Bi-Quaternions (appellation trompeuse, puisque parfois elle désigne les Split-Quaternions).

\mathbb{D}_4 est aussi isomorphe à un sous-ensemble de $M_2(\mathbb{H})$: $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ (donc où a et b sont des quaternions).

IX.5.8 Utilisation en physique

L'ensemble des quaternions duaux a été utilisé dans plusieurs domaines dont le *traitement d'image*, la *Navigation inertielle* ou la *robotique*.

IX.5.9 Références

1. Traitement d'image

L. Kavan, S. Collins, C. O'Sullivan, J. Zara, *Dual Quaternions for Rigid Transformation Blending*.

2. Robotique

A. Perez et J. M. McCarthy, *Dual Quaternion Synthesis of Constrained Robotic Systems.*, University of California (Irvine), 2003

3. Navigation inertielle

Y. Wu, X. Hu, M. Wu and D. Hu, *Strapdown Inertial Navigation using Dual Quaternion.*, IEEE Transactions On Aerospace And Electronic Systems Vol. 42, No. 1, Janvier 2006

4. Mathématiques

M. Shoham, *A note on Clifford's Derivation of Bi-Quaternions*, Tenth World Congress on the Theory of Machine ans Mechanisms, Juin 1999

X Algèbres de dimension 32 sur \mathbb{R}

X.1 Trigintaduonions \mathbb{T}

X.1.1 Introduction

L'ensemble des trigintaduonions, noté \mathbb{T} fait partie de la chaîne des algèbres réelles construites par l'application successive de la **méthode de Cayley-Dickson** à partir de \mathbb{R} :

$$\mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O} \subset \mathbb{S} \subset \mathbb{T} \subset \mathbb{X} \subset \dots$$

X.1.2 Définition

\mathbb{T} est le résultat de l'application de la méthode de Cayley-Dickson standard à **l'ensemble des sédénions**.

$$\mathbb{T} = \mathcal{CD}(\mathbb{S}, 1)$$

X.1.3 Mode de construction

Les trigintaduonions peuvent être construits de plusieurs façons :

Une algèbre de dimension 2 sur \mathbb{S} , donc comme des couples de sédénions : (s_0, s_1) , ou $s_0 + e \cdot s_1$.

En appliquant la définition de la méthode de Cayley-Dickson, on obtient :

- $(s_0, s_1) + (s'_0, s'_1) = (s_0 + s'_0, s_1 + s'_1)$
- $(s_0, s_1) \cdot (s'_0, s'_1) = (s_0 \cdot s'_0 - \overline{s'_1} \cdot s_1, s'_1 \cdot s_0 + s_1 \cdot \overline{s'_0})$
- $\overline{(s_0, s_1)} = (\overline{s_0}, -s_1)$

Mais aussi comme (attention, dans les lignes qui suivent, les a_i et les e_i ne représentent pas la même chose, sauf e_0 toujours égal à 1) :

1. Une algèbre de dimension 4 sur \mathbb{O} : $\sum_{i=0}^3 a_i \cdot e_i$ où $a_i \in \mathbb{O}$ et $e_i \notin \mathbb{O}$.
2. Une algèbre de dimension 8 sur \mathbb{H} : $\sum_{i=0}^7 a_i \cdot e_i$ où $a_i \in \mathbb{H}$ et $e_i \notin \mathbb{H}$.
3. Une algèbre de dimension 16 sur \mathbb{C} : $\sum_{i=0}^{15} a_i \cdot e_i$ où $a_i \in \mathbb{C}$ et $e_i \notin \mathbb{C}$.
4. Une algèbre de dimension 32 sur \mathbb{R} : $\sum_{i=0}^{31} a_i \cdot e_i$ où $a_i \in \mathbb{R}$ et $e_i \notin \mathbb{R}$.

Il est de tradition de noter e_i les éléments d'une base des algèbres de dimensions 8 et au-delà, mais on pourrait utiliser une autre notation, plus significative de la construction de Cayley-Dickson :

Ensemble	Eléments d'une base
\mathbb{R}	(1).
\mathbb{C}	(1, i).
\mathbb{H}	(1, i, j, ij).
\mathbb{O}	(1, $i, j, ij, k, ik, jk, (ij)k$).
\mathbb{S}	(1, $i, j, ij, k, ik, jk, (ij)k, l, il, jl, (ij)l, kl, (ik)l, (jk)l, ((ij)k)l$).
\mathbb{T}	(1, $i, j, ij, k, ik, jk, (ij)k, l, il, jl, (ij)l, kl, (ik)l, (jk)l, ((ij)k)l, m, im, jm, (ij)m, km, (ik)m, (jk)m, ((ij)k)m, lm, (il)m, (jl)m, ((ij)l)m, (kl)m, ((ik)l)m, ((jk)l)m, (((ij)k)l)m$).

Dans la suite de ce document, la notation e_i sera adoptée, sauf pour les quatre premiers éléments qui seront notés $(1, i, j, k)$, afin de bien reconnaître les réels, les complexes et les quaternions.

X.1.4 Table de multiplication

Il n'est pas possible de présenter un tableau 33×33 , nous allons le découper en quatre quadrants (dans l'ordre NW - NE - SW - SE).

·	1	<i>i</i>	<i>j</i>	<i>k</i>	<i>e</i> ₄	<i>e</i> ₅	<i>e</i> ₆	<i>e</i> ₇	<i>e</i> ₈	<i>e</i> ₉	<i>e</i> ₁₀	<i>e</i> ₁₁	<i>e</i> ₁₂	<i>e</i> ₁₃	<i>e</i> ₁₄	<i>e</i> ₁₅
1	1	<i>i</i>	<i>j</i>	<i>k</i>	<i>e</i> ₄	<i>e</i> ₅	<i>e</i> ₆	<i>e</i> ₇	<i>e</i> ₈	<i>e</i> ₉	<i>e</i> ₁₀	<i>e</i> ₁₁	<i>e</i> ₁₂	<i>e</i> ₁₃	<i>e</i> ₁₄	<i>e</i> ₁₅
<i>i</i>	<i>i</i>	-1	<i>k</i>	- <i>j</i>	<i>e</i> ₅	- <i>e</i> ₄	- <i>e</i> ₇	<i>e</i> ₆	<i>e</i> ₉	- <i>e</i> ₈	- <i>e</i> ₁₁	<i>e</i> ₁₀	- <i>e</i> ₁₃	<i>e</i> ₁₂	<i>e</i> ₁₅	- <i>e</i> ₁₄
<i>j</i>	<i>j</i>	- <i>k</i>	-1	<i>i</i>	<i>e</i> ₆	<i>e</i> ₇	- <i>e</i> ₄	- <i>e</i> ₅	<i>e</i> ₁₀	<i>e</i> ₁₁	- <i>e</i> ₈	- <i>e</i> ₉	- <i>e</i> ₁₄	- <i>e</i> ₁₅	<i>e</i> ₁₂	<i>e</i> ₁₃
<i>k</i>	<i>k</i>	<i>j</i>	- <i>i</i>	-1	<i>e</i> ₇	- <i>e</i> ₆	<i>e</i> ₅	- <i>e</i> ₄	<i>e</i> ₁₁	- <i>e</i> ₁₀	<i>e</i> ₉	- <i>e</i> ₈	- <i>e</i> ₁₅	<i>e</i> ₁₄	- <i>e</i> ₁₃	<i>e</i> ₁₂
<i>e</i> ₄	<i>e</i> ₄	- <i>e</i> ₅	- <i>e</i> ₆	- <i>e</i> ₇	-1	<i>i</i>	<i>j</i>	<i>k</i>	<i>e</i> ₁₂	<i>e</i> ₁₃	<i>e</i> ₁₄	<i>e</i> ₁₅	- <i>e</i> ₈	- <i>e</i> ₉	- <i>e</i> ₁₀	- <i>e</i> ₁₁
<i>e</i> ₅	<i>e</i> ₅	<i>e</i> ₄	- <i>e</i> ₇	<i>e</i> ₆	- <i>i</i>	-1	- <i>k</i>	<i>j</i>	<i>e</i> ₁₃	- <i>e</i> ₁₂	<i>e</i> ₁₅	- <i>e</i> ₁₄	<i>e</i> ₉	- <i>e</i> ₈	<i>e</i> ₁₁	- <i>e</i> ₁₀
<i>e</i> ₆	<i>e</i> ₆	<i>e</i> ₇	<i>e</i> ₄	- <i>e</i> ₅	- <i>j</i>	<i>k</i>	-1	- <i>i</i>	<i>e</i> ₁₄	- <i>e</i> ₁₅	- <i>e</i> ₁₂	<i>e</i> ₁₃	<i>e</i> ₁₀	- <i>e</i> ₁₁	- <i>e</i> ₈	<i>e</i> ₉
<i>e</i> ₇	<i>e</i> ₇	- <i>e</i> ₆	<i>e</i> ₅	<i>e</i> ₄	- <i>k</i>	- <i>j</i>	<i>i</i>	-1	<i>e</i> ₁₅	<i>e</i> ₁₄	- <i>e</i> ₁₃	- <i>e</i> ₁₂	<i>e</i> ₁₁	<i>e</i> ₁₀	- <i>e</i> ₉	- <i>e</i> ₈
<i>e</i> ₈	<i>e</i> ₈	- <i>e</i> ₉	- <i>e</i> ₁₀	- <i>e</i> ₁₁	- <i>e</i> ₁₂	- <i>e</i> ₁₃	- <i>e</i> ₁₄	- <i>e</i> ₁₅	-1	<i>i</i>	<i>j</i>	<i>k</i>	<i>e</i> ₄	<i>e</i> ₅	<i>e</i> ₆	<i>e</i> ₇
<i>e</i> ₉	<i>e</i> ₉	<i>e</i> ₈	- <i>e</i> ₁₁	<i>e</i> ₁₀	- <i>e</i> ₁₃	<i>e</i> ₁₂	<i>e</i> ₁₅	- <i>e</i> ₁₄	- <i>i</i>	-1	- <i>k</i>	<i>j</i>	- <i>e</i> ₅	<i>e</i> ₄	<i>e</i> ₇	- <i>e</i> ₆
<i>e</i> ₁₀	<i>e</i> ₁₀	<i>e</i> ₁₁	<i>e</i> ₈	- <i>e</i> ₉	- <i>e</i> ₁₄	- <i>e</i> ₁₅	<i>e</i> ₁₂	<i>e</i> ₁₃	- <i>j</i>	<i>k</i>	-1	- <i>i</i>	- <i>e</i> ₆	- <i>e</i> ₇	<i>e</i> ₄	<i>e</i> ₅
<i>e</i> ₁₁	<i>e</i> ₁₁	- <i>e</i> ₁₀	<i>e</i> ₉	<i>e</i> ₈	- <i>e</i> ₁₅	<i>e</i> ₁₄	- <i>e</i> ₁₃	<i>e</i> ₁₂	- <i>k</i>	- <i>j</i>	<i>i</i>	-1	- <i>e</i> ₇	<i>e</i> ₆	- <i>e</i> ₅	<i>e</i> ₄
<i>e</i> ₁₂	<i>e</i> ₁₂	<i>e</i> ₁₃	<i>e</i> ₁₄	<i>e</i> ₁₅	<i>e</i> ₈	- <i>e</i> ₉	- <i>e</i> ₁₀	- <i>e</i> ₁₁	- <i>e</i> ₄	<i>e</i> ₅	<i>e</i> ₆	<i>e</i> ₇	-1	- <i>i</i>	- <i>j</i>	- <i>k</i>
<i>e</i> ₁₃	<i>e</i> ₁₃	- <i>e</i> ₁₂	<i>e</i> ₁₅	- <i>e</i> ₁₄	<i>e</i> ₉	<i>e</i> ₈	<i>e</i> ₁₁	- <i>e</i> ₁₀	- <i>e</i> ₅	- <i>e</i> ₄	<i>e</i> ₇	- <i>e</i> ₆	<i>i</i>	-1	<i>k</i>	- <i>j</i>
<i>e</i> ₁₄	<i>e</i> ₁₄	- <i>e</i> ₁₅	- <i>e</i> ₁₂	<i>e</i> ₁₃	<i>e</i> ₁₀	- <i>e</i> ₁₁	<i>e</i> ₈	<i>e</i> ₉	- <i>e</i> ₆	- <i>e</i> ₇	- <i>e</i> ₄	<i>e</i> ₅	<i>j</i>	- <i>k</i>	-1	<i>i</i>
<i>e</i> ₁₅	<i>e</i> ₁₅	<i>e</i> ₁₄	- <i>e</i> ₁₃	- <i>e</i> ₁₂	<i>e</i> ₁₁	<i>e</i> ₁₀	- <i>e</i> ₉	<i>e</i> ₈	- <i>e</i> ₇	<i>e</i> ₆	- <i>e</i> ₅	- <i>e</i> ₄	<i>k</i>	<i>j</i>	- <i>i</i>	-1

Premier quadrant (Nord-Ouest) qui correspond très exactement aux **sédénions**.

Dans ce tableau, on reconnaît facilement la table de multiplication de :

- \mathbb{R} (première colonne et première ligne).
- \mathbb{C} (deux premières colonnes et deux premières lignes).
- \mathbb{H} (quatre premières colonnes et quatre premières lignes).
- \mathbb{O} (huit premières colonnes et huit premières lignes).
- \mathbb{S} (seize premières colonnes et seize premières lignes).

·	<i>e</i> ₁₆	<i>e</i> ₁₇	<i>e</i> ₁₈	<i>e</i> ₁₉	<i>e</i> ₂₀	<i>e</i> ₂₁	<i>e</i> ₂₂	<i>e</i> ₂₃	<i>e</i> ₂₄	<i>e</i> ₂₅	<i>e</i> ₂₆	<i>e</i> ₂₇	<i>e</i> ₂₈	<i>e</i> ₂₉	<i>e</i> ₃₀	<i>e</i> ₃₁
1	<i>e</i> ₁₆	<i>e</i> ₁₇	<i>e</i> ₁₈	<i>e</i> ₁₉	<i>e</i> ₂₀	<i>e</i> ₂₁	<i>e</i> ₂₂	<i>e</i> ₂₃	<i>e</i> ₂₄	<i>e</i> ₂₅	<i>e</i> ₂₆	<i>e</i> ₂₇	<i>e</i> ₂₈	<i>e</i> ₂₉	<i>e</i> ₃₀	<i>e</i> ₃₁
<i>i</i>	<i>e</i> ₁₇	- <i>e</i> ₁₆	- <i>e</i> ₁₉	<i>e</i> ₁₈	- <i>e</i> ₂₁	<i>e</i> ₂₀	<i>e</i> ₂₃	- <i>e</i> ₂₂	- <i>e</i> ₂₅	<i>e</i> ₂₄	<i>e</i> ₂₇	- <i>e</i> ₂₆	<i>e</i> ₂₉	- <i>e</i> ₂₈	- <i>e</i> ₃₁	<i>e</i> ₃₀
<i>j</i>	<i>e</i> ₁₈	<i>e</i> ₁₉	- <i>e</i> ₁₆	- <i>e</i> ₁₇	- <i>e</i> ₂₂	- <i>e</i> ₂₃	<i>e</i> ₂₀	<i>e</i> ₂₁	- <i>e</i> ₂₆	- <i>e</i> ₂₇	<i>e</i> ₂₄	<i>e</i> ₂₅	<i>e</i> ₃₀	<i>e</i> ₃₁	- <i>e</i> ₂₈	- <i>e</i> ₂₉
<i>k</i>	<i>e</i> ₁₉	- <i>e</i> ₁₈	<i>e</i> ₁₇	- <i>e</i> ₁₆	- <i>e</i> ₂₃	<i>e</i> ₂₂	- <i>e</i> ₂₁	<i>e</i> ₂₀	- <i>e</i> ₂₇	<i>e</i> ₂₆	- <i>e</i> ₂₅	<i>e</i> ₂₄	<i>e</i> ₃₁	- <i>e</i> ₃₀	<i>e</i> ₂₉	- <i>e</i> ₂₈
<i>e</i> ₄	<i>e</i> ₂₀	<i>e</i> ₂₁	<i>e</i> ₂₂	<i>e</i> ₂₃	- <i>e</i> ₁₆	- <i>e</i> ₁₇	- <i>e</i> ₁₈	- <i>e</i> ₁₉	- <i>e</i> ₂₈	- <i>e</i> ₂₉	- <i>e</i> ₃₀	- <i>e</i> ₃₁	<i>e</i> ₂₄	<i>e</i> ₂₅	<i>e</i> ₂₆	<i>e</i> ₂₇
<i>e</i> ₅	<i>e</i> ₂₁	- <i>e</i> ₂₀	<i>e</i> ₂₃	- <i>e</i> ₂₂	<i>e</i> ₁₇	- <i>e</i> ₁₆	<i>e</i> ₁₉	- <i>e</i> ₁₈	- <i>e</i> ₂₉	<i>e</i> ₂₈	- <i>e</i> ₃₁	<i>e</i> ₃₀	- <i>e</i> ₂₅	<i>e</i> ₂₄	- <i>e</i> ₂₇	<i>e</i> ₂₆
<i>e</i> ₆	<i>e</i> ₂₂	- <i>e</i> ₂₃	- <i>e</i> ₂₀	<i>e</i> ₂₁	<i>e</i> ₁₈	- <i>e</i> ₁₉	- <i>e</i> ₁₆	<i>e</i> ₁₇	- <i>e</i> ₃₀	<i>e</i> ₃₁	<i>e</i> ₂₈	- <i>e</i> ₂₉	- <i>e</i> ₂₆	<i>e</i> ₂₇	<i>e</i> ₂₄	- <i>e</i> ₂₅
<i>e</i> ₇	<i>e</i> ₂₃	<i>e</i> ₂₂	- <i>e</i> ₂₁	- <i>e</i> ₂₀	<i>e</i> ₁₉	<i>e</i> ₁₈	- <i>e</i> ₁₇	- <i>e</i> ₁₆	- <i>e</i> ₃₁	- <i>e</i> ₃₀	<i>e</i> ₂₉	<i>e</i> ₂₈	- <i>e</i> ₂₇	- <i>e</i> ₂₆	<i>e</i> ₂₅	<i>e</i> ₂₄
<i>e</i> ₈	<i>e</i> ₂₄	<i>e</i> ₂₅	<i>e</i> ₂₆	<i>e</i> ₂₇	<i>e</i> ₂₈	<i>e</i> ₂₉	<i>e</i> ₃₀	<i>e</i> ₃₁	- <i>e</i> ₁₆	- <i>e</i> ₁₇	- <i>e</i> ₁₈	- <i>e</i> ₁₉	- <i>e</i> ₂₀	- <i>e</i> ₂₁	- <i>e</i> ₂₂	- <i>e</i> ₂₃
<i>e</i> ₉	<i>e</i> ₂₅	- <i>e</i> ₂₄	<i>e</i> ₂₇	- <i>e</i> ₂₆	<i>e</i> ₂₉	- <i>e</i> ₂₈	- <i>e</i> ₃₁	<i>e</i> ₃₀	<i>e</i> ₁₇	- <i>e</i> ₁₆	<i>e</i> ₁₉	- <i>e</i> ₁₈	<i>e</i> ₂₁	- <i>e</i> ₂₀	- <i>e</i> ₂₃	<i>e</i> ₂₂
<i>e</i> ₁₀	<i>e</i> ₂₆	- <i>e</i> ₂₇	- <i>e</i> ₂₄	<i>e</i> ₂₅	<i>e</i> ₃₀	<i>e</i> ₃₁	- <i>e</i> ₂₈	- <i>e</i> ₂₉	<i>e</i> ₁₈	- <i>e</i> ₁₉	- <i>e</i> ₁₆	<i>e</i> ₁₇	<i>e</i> ₂₂	<i>e</i> ₂₃	- <i>e</i> ₂₀	- <i>e</i> ₂₁
<i>e</i> ₁₁	<i>e</i> ₂₇	<i>e</i> ₂₆	- <i>e</i> ₂₅	- <i>e</i> ₂₄	<i>e</i> ₃₁	- <i>e</i> ₃₀	<i>e</i> ₂₉	- <i>e</i> ₂₈	<i>e</i> ₁₉	<i>e</i> ₁₈	- <i>e</i> ₁₇	- <i>e</i> ₁₆	<i>e</i> ₂₃	- <i>e</i> ₂₂	<i>e</i> ₂₁	- <i>e</i> ₂₀
<i>e</i> ₁₂	<i>e</i> ₂₈	- <i>e</i> ₂₉	- <i>e</i> ₃₀	- <i>e</i> ₃₁	- <i>e</i> ₂₄	<i>e</i> ₂₅	<i>e</i> ₂₆	<i>e</i> ₂₇	<i>e</i> ₂₀	- <i>e</i> ₂₁	- <i>e</i> ₂₂	- <i>e</i> ₂₃	- <i>e</i> ₁₆	<i>e</i> ₁₇	<i>e</i> ₁₈	<i>e</i> ₁₉
<i>e</i> ₁₃	<i>e</i> ₂₉	<i>e</i> ₂₈	- <i>e</i> ₃₁	<i>e</i> ₃₀	- <i>e</i> ₂₅	- <i>e</i> ₂₄	- <i>e</i> ₂₇	<i>e</i> ₂₆	<i>e</i> ₂₁	<i>e</i> ₂₀	- <i>e</i> ₂₃	<i>e</i> ₂₂	- <i>e</i> ₁₇	- <i>e</i> ₁₆	- <i>e</i> ₁₉	<i>e</i> ₁₈
<i>e</i> ₁₄	<i>e</i> ₃₀	<i>e</i> ₃₁	<i>e</i> ₂₈	- <i>e</i> ₂₉	- <i>e</i> ₂₆	<i>e</i> ₂₇	- <i>e</i> ₂₄	- <i>e</i> ₂₅	<i>e</i> ₂₂	<i>e</i> ₂₃	<i>e</i> ₂₀	- <i>e</i> ₂₁	- <i>e</i> ₁₈	<i>e</i> ₁₉	- <i>e</i> ₁₆	- <i>e</i> ₁₇
<i>e</i> ₁₅	<i>e</i> ₃₁	- <i>e</i> ₃₀	<i>e</i> ₂₉	<i>e</i> ₂₈	- <i>e</i> ₂₇	- <i>e</i> ₂₆	<i>e</i> ₂₅	- <i>e</i> ₂₄	<i>e</i> ₂₃	- <i>e</i> ₂₂	<i>e</i> ₂₁	<i>e</i> ₂₀	- <i>e</i> ₁₉	- <i>e</i> ₁₈	<i>e</i> ₁₇	- <i>e</i> ₁₆

Deuxième quadrant (Nord-Est).

·	1	<i>i</i>	<i>j</i>	<i>k</i>	<i>e</i> ₄	<i>e</i> ₅	<i>e</i> ₆	<i>e</i> ₇	<i>e</i> ₈	<i>e</i> ₉	<i>e</i> ₁₀	<i>e</i> ₁₁	<i>e</i> ₁₂	<i>e</i> ₁₃	<i>e</i> ₁₄	<i>e</i> ₁₅
<i>e</i> ₁₆	<i>e</i> ₁₆	- <i>e</i> ₁₇	- <i>e</i> ₁₈	- <i>e</i> ₁₉	- <i>e</i> ₂₀	- <i>e</i> ₂₁	- <i>e</i> ₂₂	- <i>e</i> ₂₃	- <i>e</i> ₂₄	- <i>e</i> ₂₅	- <i>e</i> ₂₆	- <i>e</i> ₂₇	- <i>e</i> ₂₈	- <i>e</i> ₂₉	- <i>e</i> ₃₀	- <i>e</i> ₃₁
<i>e</i> ₁₇	<i>e</i> ₁₇	<i>e</i> ₁₆	- <i>e</i> ₁₉	<i>e</i> ₁₈	- <i>e</i> ₂₁	<i>e</i> ₂₀	<i>e</i> ₂₃	- <i>e</i> ₂₂	- <i>e</i> ₂₅	<i>e</i> ₂₄	<i>e</i> ₂₇	- <i>e</i> ₂₆	<i>e</i> ₂₉	- <i>e</i> ₂₈	- <i>e</i> ₃₁	<i>e</i> ₃₀
<i>e</i> ₁₈	<i>e</i> ₁₈	<i>e</i> ₁₉	<i>e</i> ₁₆	- <i>e</i> ₁₇	- <i>e</i> ₂₂	- <i>e</i> ₂₃	<i>e</i> ₂₀	<i>e</i> ₂₁	- <i>e</i> ₂₆	- <i>e</i> ₂₇	<i>e</i> ₂₄	<i>e</i> ₂₅	<i>e</i> ₃₀	<i>e</i> ₃₁	- <i>e</i> ₂₈	- <i>e</i> ₂₉
<i>e</i> ₁₉	<i>e</i> ₁₉	- <i>e</i> ₁₈	<i>e</i> ₁₇	<i>e</i> ₁₆	- <i>e</i> ₂₃	<i>e</i> ₂₂	- <i>e</i> ₂₁	<i>e</i> ₂₀	- <i>e</i> ₂₇	<i>e</i> ₂₆	- <i>e</i> ₂₅	<i>e</i> ₂₄	<i>e</i> ₃₁	- <i>e</i> ₃₀	<i>e</i> ₂₉	- <i>e</i> ₂₈
<i>e</i> ₂₀	<i>e</i> ₂₀	<i>e</i> ₂₁	<i>e</i> ₂₂	<i>e</i> ₂₃	<i>e</i> ₁₆	- <i>e</i> ₁₇	- <i>e</i> ₁₈	- <i>e</i> ₁₉	- <i>e</i> ₂₈	- <i>e</i> ₂₉	- <i>e</i> ₃₀	- <i>e</i> ₃₁	<i>e</i> ₂₄	<i>e</i> ₂₅	<i>e</i> ₂₆	<i>e</i> ₂₇
<i>e</i> ₂₁	<i>e</i> ₂₁	- <i>e</i> ₂₀	<i>e</i> ₂₃	- <i>e</i> ₂₂	<i>e</i> ₁₇	<i>e</i> ₁₆	<i>e</i> ₁₉	- <i>e</i> ₁₈	- <i>e</i> ₂₉	<i>e</i> ₂₈	- <i>e</i> ₃₁	<i>e</i> ₃₀	- <i>e</i> ₂₅	<i>e</i> ₂₄	- <i>e</i> ₂₇	<i>e</i> ₂₆
<i>e</i> ₂₂	<i>e</i> ₂₂	- <i>e</i> ₂₃	- <i>e</i> ₂₀	<i>e</i> ₂₁	<i>e</i> ₁₈	- <i>e</i> ₁₉	<i>e</i> ₁₆	<i>e</i> ₁₇	- <i>e</i> ₃₀	<i>e</i> ₃₁	<i>e</i> ₂₈	- <i>e</i> ₂₉	- <i>e</i> ₂₆	<i>e</i> ₂₇	<i>e</i> ₂₄	- <i>e</i> ₂₅
<i>e</i> ₂₃	<i>e</i> ₂₃	<i>e</i> ₂₂	- <i>e</i> ₂₁	- <i>e</i> ₂₀	<i>e</i> ₁₉	<i>e</i> ₁₈	- <i>e</i> ₁₇	<i>e</i> ₁₆	- <i>e</i> ₃₁	- <i>e</i> ₃₀	<i>e</i> ₂₉	<i>e</i> ₂₈	- <i>e</i> ₂₇	- <i>e</i> ₂₆	<i>e</i> ₂₅	<i>e</i> ₂₄
<i>e</i> ₂₄	<i>e</i> ₂₄	<i>e</i> ₂₅	<i>e</i> ₂₆	<i>e</i> ₂₇	<i>e</i> ₂₈	<i>e</i> ₂₉	<i>e</i> ₃₀	<i>e</i> ₃₁	<i>e</i> ₁₆	- <i>e</i> ₁₇	- <i>e</i> ₁₈	- <i>e</i> ₁₉	- <i>e</i> ₂₀	- <i>e</i> ₂₁	- <i>e</i> ₂₂	- <i>e</i> ₂₃
<i>e</i> ₂₅	<i>e</i> ₂₅	- <i>e</i> ₂₄	<i>e</i> ₂₇	- <i>e</i> ₂₆	<i>e</i> ₂₉	- <i>e</i> ₂₈	- <i>e</i> ₃₁	<i>e</i> ₃₀	<i>e</i> ₁₇	<i>e</i> ₁₆	<i>e</i> ₁₉	- <i>e</i> ₁₈	<i>e</i> ₂₁	- <i>e</i> ₂₀	- <i>e</i> ₂₃	<i>e</i> ₂₂
<i>e</i> ₂₆	<i>e</i> ₂₆	- <i>e</i> ₂₇	- <i>e</i> ₂₄	<i>e</i> ₂₅	<i>e</i> ₃₀	<i>e</i> ₃₁	- <i>e</i> ₂₈	- <i>e</i> ₂₉	<i>e</i> ₁₈	- <i>e</i> ₁₉	<i>e</i> ₁₆	<i>e</i> ₁₇	<i>e</i> ₂₂	<i>e</i> ₂₃	- <i>e</i> ₂₀	- <i>e</i> ₂₁
<i>e</i> ₂₇	<i>e</i> ₂₇	<i>e</i> ₂₆	- <i>e</i> ₂₅	- <i>e</i> ₂₄	<i>e</i> ₃₁	- <i>e</i> ₃₀	<i>e</i> ₂₉	- <i>e</i> ₂₈	<i>e</i> ₁₉	<i>e</i> ₁₈	- <i>e</i> ₁₇	<i>e</i> ₁₆	<i>e</i> ₂₃	- <i>e</i> ₂₂	<i>e</i> ₂₁	- <i>e</i> ₂₀
<i>e</i> ₂₈	<i>e</i> ₂₈	- <i>e</i> ₂₉	- <i>e</i> ₃₀	- <i>e</i> ₃₁	- <i>e</i> ₂₄	<i>e</i> ₂₅	<i>e</i> ₂₆	<i>e</i> ₂₇	<i>e</i> ₂₀	- <i>e</i> ₂₁	- <i>e</i> ₂₂	- <i>e</i> ₂₃	<i>e</i> ₁₆	<i>e</i> ₁₇	<i>e</i> ₁₈	<i>e</i> ₁₉
<i>e</i> ₂₉	<i>e</i> ₂₉	<i>e</i> ₂₈	- <i>e</i> ₃₁	<i>e</i> ₃₀	- <i>e</i> ₂₅	- <i>e</i> ₂₄	- <i>e</i> ₂₇	<i>e</i> ₂₆	<i>e</i> ₂₁	<i>e</i> ₂₀	- <i>e</i> ₂₃	<i>e</i> ₂₂	- <i>e</i> ₁₇	<i>e</i> ₁₆	- <i>e</i> ₁₉	<i>e</i> ₁₈
<i>e</i> ₃₀	<i>e</i> ₃₀	<i>e</i> ₃₁	<i>e</i> ₂₈	- <i>e</i> ₂₉	- <i>e</i> ₂₆	<i>e</i> ₂₇	- <i>e</i> ₂₄	- <i>e</i> ₂₅	<i>e</i> ₂₂	<i>e</i> ₂₃	<i>e</i> ₂₀	- <i>e</i> ₂₁	- <i>e</i> ₁₈	<i>e</i> ₁₉	<i>e</i> ₁₆	- <i>e</i> ₁₇
<i>e</i> ₃₁	<i>e</i> ₃₁	- <i>e</i> ₃₀	<i>e</i> ₂₉	<i>e</i> ₂₈	- <i>e</i> ₂₇	- <i>e</i> ₂₆	<i>e</i> ₂₅	- <i>e</i> ₂₄	<i>e</i> ₂₃	- <i>e</i> ₂₂	<i>e</i> ₂₁	<i>e</i> ₂₀	- <i>e</i> ₁₉	- <i>e</i> ₁₈	<i>e</i> ₁₇	<i>e</i> ₁₆

Troisième quadrant (Sud-Ouest).

·	<i>e</i> ₁₆	<i>e</i> ₁₇	<i>e</i> ₁₈	<i>e</i> ₁₉	<i>e</i> ₂₀	<i>e</i> ₂₁	<i>e</i> ₂₂	<i>e</i> ₂₃	<i>e</i> ₂₄	<i>e</i> ₂₅	<i>e</i> ₂₆	<i>e</i> ₂₇	<i>e</i> ₂₈	<i>e</i> ₂₉	<i>e</i> ₃₀	<i>e</i> ₃₁
<i>e</i> ₁₆	-1	<i>i</i>	<i>j</i>	<i>k</i>	<i>e</i> ₄	<i>e</i> ₅	<i>e</i> ₆	<i>e</i> ₇	<i>e</i> ₈	<i>e</i> ₉	<i>e</i> ₁₀	<i>e</i> ₁₁	<i>e</i> ₁₂	<i>e</i> ₁₃	<i>e</i> ₁₄	<i>e</i> ₁₅
<i>e</i> ₁₇	- <i>i</i>	-1	- <i>k</i>	<i>j</i>	- <i>e</i> ₅	<i>e</i> ₄	<i>e</i> ₇	- <i>e</i> ₆	- <i>e</i> ₉	<i>e</i> ₈	<i>e</i> ₁₁	- <i>e</i> ₁₀	<i>e</i> ₁₃	- <i>e</i> ₁₂	- <i>e</i> ₁₅	<i>e</i> ₁₄
<i>e</i> ₁₈	- <i>j</i>	<i>k</i>	-1	- <i>i</i>	- <i>e</i> ₆	- <i>e</i> ₇	<i>e</i> ₄	<i>e</i> ₅	- <i>e</i> ₁₀	- <i>e</i> ₁₁	<i>e</i> ₈	<i>e</i> ₉	<i>e</i> ₁₄	<i>e</i> ₁₅	- <i>e</i> ₁₂	- <i>e</i> ₁₃
<i>e</i> ₁₉	- <i>k</i>	- <i>j</i>	<i>i</i>	-1	- <i>e</i> ₇	<i>e</i> ₆	- <i>e</i> ₅	<i>e</i> ₄	- <i>e</i> ₁₁	<i>e</i> ₁₀	- <i>e</i> ₉	<i>e</i> ₈	<i>e</i> ₁₅	- <i>e</i> ₁₄	<i>e</i> ₁₃	- <i>e</i> ₁₂
<i>e</i> ₂₀	- <i>e</i> ₄	<i>e</i> ₅	<i>e</i> ₆	<i>e</i> ₇	-1	- <i>i</i>	- <i>j</i>	- <i>k</i>	- <i>e</i> ₁₂	- <i>e</i> ₁₃	- <i>e</i> ₁₄	- <i>e</i> ₁₅	<i>e</i> ₈	<i>e</i> ₉	<i>e</i> ₁₀	<i>e</i> ₁₁
<i>e</i> ₂₁	- <i>e</i> ₅	- <i>e</i> ₄	<i>e</i> ₇	- <i>e</i> ₆	<i>i</i>	-1	<i>k</i>	- <i>j</i>	- <i>e</i> ₁₃	<i>e</i> ₁₂	- <i>e</i> ₁₅	<i>e</i> ₁₄	- <i>e</i> ₉	<i>e</i> ₈	- <i>e</i> ₁₁	<i>e</i> ₁₀
<i>e</i> ₂₂	- <i>e</i> ₆	- <i>e</i> ₇	- <i>e</i> ₄	<i>e</i> ₅	<i>j</i>	- <i>k</i>	-1	<i>i</i>	- <i>e</i> ₁₄	<i>e</i> ₁₅	<i>e</i> ₁₂	- <i>e</i> ₁₃	- <i>e</i> ₁₀	<i>e</i> ₁₁	<i>e</i> ₈	- <i>e</i> ₉
<i>e</i> ₂₃	- <i>e</i> ₇	<i>e</i> ₆	- <i>e</i> ₅	- <i>e</i> ₄	<i>k</i>	<i>j</i>	- <i>i</i>	-1	- <i>e</i> ₁₅	- <i>e</i> ₁₄	<i>e</i> ₁₃	<i>e</i> ₁₂	- <i>e</i> ₁₁	- <i>e</i> ₁₀	<i>e</i> ₉	<i>e</i> ₈
<i>e</i> ₂₄	- <i>e</i> ₈	<i>e</i> ₉	<i>e</i> ₁₀	<i>e</i> ₁₁	<i>e</i> ₁₂	<i>e</i> ₁₃	<i>e</i> ₁₄	<i>e</i> ₁₅	-1	- <i>i</i>	- <i>j</i>	- <i>k</i>	- <i>e</i> ₄	- <i>e</i> ₅	- <i>e</i> ₆	- <i>e</i> ₇
<i>e</i> ₂₅	- <i>e</i> ₉	- <i>e</i> ₈	<i>e</i> ₁₁	- <i>e</i> ₁₀	<i>e</i> ₁₃	- <i>e</i> ₁₂	- <i>e</i> ₁₅	<i>e</i> ₁₄	<i>i</i>	-1	<i>k</i>	- <i>j</i>	<i>e</i> ₅	- <i>e</i> ₄	- <i>e</i> ₇	<i>e</i> ₆
<i>e</i> ₂₆	- <i>e</i> ₁₀	- <i>e</i> ₁₁	- <i>e</i> ₈	<i>e</i> ₉	<i>e</i> ₁₄	<i>e</i> ₁₅	- <i>e</i> ₁₂	- <i>e</i> ₁₃	<i>j</i>	- <i>k</i>	-1	<i>i</i>	<i>e</i> ₆	<i>e</i> ₇	- <i>e</i> ₄	- <i>e</i> ₅
<i>e</i> ₂₇	- <i>e</i> ₁₁	<i>e</i> ₁₀	- <i>e</i> ₉	- <i>e</i> ₈	<i>e</i> ₁₅	- <i>e</i> ₁₄	<i>e</i> ₁₃	- <i>e</i> ₁₂	<i>k</i>	<i>j</i>	- <i>i</i>	-1	<i>e</i> ₇	- <i>e</i> ₆	<i>e</i> ₅	- <i>e</i> ₄
<i>e</i> ₂₈	- <i>e</i> ₁₂	- <i>e</i> ₁₃	- <i>e</i> ₁₄	- <i>e</i> ₁₅	- <i>e</i> ₈	<i>e</i> ₉	<i>e</i> ₁₀	<i>e</i> ₁₁	<i>e</i> ₄	- <i>e</i> ₅	- <i>e</i> ₆	- <i>e</i> ₇	-1	<i>i</i>	<i>j</i>	<i>k</i>
<i>e</i> ₂₉	- <i>e</i> ₁₃	<i>e</i> ₁₂	- <i>e</i> ₁₅	<i>e</i> ₁₄	- <i>e</i> ₉	- <i>e</i> ₈	- <i>e</i> ₁₁	<i>e</i> ₁₀	<i>e</i> ₅	<i>e</i> ₄	- <i>e</i> ₇	<i>e</i> ₆	- <i>i</i>	-1	- <i>k</i>	<i>j</i>
<i>e</i> ₃₀	- <i>e</i> ₁₄	<i>e</i> ₁₅	<i>e</i> ₁₂	- <i>e</i> ₁₃	- <i>e</i> ₁₀	<i>e</i> ₁₁	- <i>e</i> ₈	- <i>e</i> ₉	<i>e</i> ₆	<i>e</i> ₇	<i>e</i> ₄	- <i>e</i> ₅	- <i>j</i>	<i>k</i>	-1	- <i>i</i>
<i>e</i> ₃₁	- <i>e</i> ₁₅	- <i>e</i> ₁₄	<i>e</i> ₁₃	<i>e</i> ₁₂	- <i>e</i> ₁₁	- <i>e</i> ₁₀	<i>e</i> ₉	- <i>e</i> ₈	<i>e</i> ₇	- <i>e</i> ₆	<i>e</i> ₅	<i>e</i> ₄	- <i>k</i>	- <i>j</i>	<i>i</i>	-1

Quatrième quadrant (Sud-Est).

X.1.5 Conjugué, Module, Norme, Forme Polaire et Inverse

Comme toutes les algèbres construites à l'aide de la méthode de Cayley-Dickson, le conjugué d'un trigintaduonions se calcule à partir du conjugué de l'algèbre sur laquelle cet ensemble est construit, à savoir les sédénions : $\overline{s_0 + e \cdot s_1} = \overline{s_0} - e \cdot s_1$.

Ce qui permet de définir une norme (non multiplicative cf. infra) : $|s_0 + e \cdot s_1|^2 = |s_0|^2 + |s_1|^2$.

On peut calculer ce conjugué et cette norme en remontant des sédénions aux octonions, etc. jusqu'aux réels :

$$\text{Définition du conjugué : } \overline{\left(1 + \sum_{i=1}^{31} a_i \cdot e_i\right)} = 1 - \sum_{i=1}^{31} a_i \cdot e_i$$

$$\text{Définition de la norme : } \left| \sum_{i=0}^{31} a_i \cdot e_i \right|^2 = \sum_{i=0}^{31} a_i^2$$

$$\text{d'où l'inverse, pour } z \neq 0 : z^{-1} = \frac{\overline{z}}{|z|^2}$$

On peut vérifier facilement que la norme n'est pas multiplicative : $|k + e_{10}|^2 = 2$, $|e_6 - e_{15}|^2 = 2$, mais comme $(k + e_{10}) \cdot (e_6 - e_{15}) = 0$, la norme du produit est nulle.

X.1.6 Propriétés algébriques

$(\mathbb{T}, +, \times, \cdot)$ est une \mathbb{R} -algèbre de dimension 32, ni commutative, ni associative, ni même alternative, par contre elle est flexible et associative en puissance.

Exemple de non alternativité : $(e_4 + e_{15})^2 \cdot i = -2i$ alors que $(e_4 + e_{15}) \cdot ((e_4 + e_{15}) \cdot i) = -2i - 2e_{10}$

\mathbb{T} contient des diviseurs de 0 : l'exemple déjà donné, ou encore $(i + e_{10}) \cdot (e_{15} - e_4) = 0$.

X.1.7 Synonymes, Isomorphismes, Exemples

On trouve parfois le nom Pathions (pour pathologique), proposé par R.P.C. de Marrais & T. Smith. John Wayland Bales utilise le terme quinipotentials (puisque $32 = 2^5$).

X.1.8 Utilisation en physique

Les trigintaduonions sont utilisés comme cadre pour l'étude des interactions électromagnétique, gravitationnelle, fortes et faibles.

Zihua Weng, dans ce cadre, prédit la possibilité de nouvelles particules.

X.1.9 Références

1. Zihua Weng, *Some helicities in electromagnetic and gravitational fields*, School of Physics and Mechanical & Electrical Engineering, Xiamen University, China, 2011
2. Zihua Weng, *Compounding Fields and Their Quantum Equations in the Trigintaduonion Space*, School of Physics and Mechanical & Electrical Engineering, Xiamen University, China, 2007
3. R. E. Cawagas & al., *The Basic Subalgebra Structure of the Cayley-Dickson Algebra of Dimension 32 (Trigintaduonions)*, Polytechnic University of the Philippines, 2009

XI Algèbres de dimension 64 sur \mathbb{R} et au-delà

XI.1 Sexagintaquatrons \mathbb{X}

XI.1.1 Introduction

L'ensemble des Sexagintaquatrons, noté \mathbb{X} est nommé ainsi car c'est une \mathbb{R} -de dimension 64 (qui se dit sexaginta quattuor en latin).

XI.1.2 Définition

Par définition $\mathbb{X} = \mathcal{CD}(\mathbb{T}, 1)$, c'est à dire le résultat de l'application de la méthode de Cayley Dickson standard (avec $\lambda = 1$) aux Tringtaduonions.

XI.1.3 Mode de construction

Les sexagintaquatrons peuvent être construits de plusieurs façons, comme la plupart des \mathbb{R} -algèbres, la principale méthode de construction est issue directement de la définition. :

Une algèbre de dimension 2 sur \mathbb{T} , donc comme des couples de tringtaduonions : (t_0, t_1) , ou $t_0 + e \cdot t_1$.

En appliquant la définition de la méthode de Cayley-Dickson, on obtient :

- $(t_0, t_1) + (t'_0, t'_1) = (t_0 + t'_0, t_1 + t'_1)$
- $(t_0, t_1) \cdot (t'_0, t'_1) = (t_0 \cdot t'_0 - \overline{t'_1} \cdot t_1, t'_1 \cdot t_0 + t_1 \cdot \overline{t'_0})$
- $\overline{(t_0, t_1)} = (\overline{t_0}, -t_1)$

XI.1.4 Table de multiplication

Il n'est pas raisonnable, ni très utile de donner la table de multiplication dans \mathbb{X} , par contre nous pouvons donner un algorithme qui permet de construire cette table très facilement (dans un tableur par exemple) :

En notant $\mathbb{A}_0 = \mathbb{R}$ et $\mathbb{A}_{n+1} = \mathcal{CD}(\mathbb{A}_n, 1)$, on peut noter que \mathbb{A}_n est une \mathbb{R} -algèbre de dimension 2^n , et dans le reste de ce document, nous noterons $(e_0, e_1, \dots, e_{2^n-1})$ les éléments de sa base naturelle.

Nous noterons aussi $\mathbb{A} = \bigcup_{n \in \mathbb{N}} \mathbb{A}_n$. Donc tout élément de \mathbb{A} est une \mathbb{R} -combinaison linéaire finie d'éléments de (e_0, e_1, \dots) , rappelons que :

1. $e_0 = 1$
2. $p \neq 0 \Rightarrow \overline{e_p} = -e_p$
3. $((p \neq 0) \wedge (q \neq 0)) \Rightarrow e_p \cdot e_q = -e_q \cdot e_p$
4. $(x, x') \times (y, y') = (xy - \overline{y'}x', y'x + x'\overline{y})$

Remarque : $\forall p' \in \mathbb{N}^* \exists!(n, p) \in \mathbb{N}^2 ((p' = 2^n + p) \wedge (p < 2^n))$ et donc pour tous couples d'entiers non nuls (p', q') , ils se trouvent dans un et un seul des trois cas suivants :

1. $(p' = 2^n + p) \wedge (q' = q) \wedge (p < 2^n) \wedge (q < 2^n)$
2. $(p' = p) \wedge (q' = 2^n + q) \wedge (p < 2^n) \wedge (q < 2^n)$
3. $(p' = 2^n + p) \wedge (q' = 2^n + q) \wedge (p < 2^n) \wedge (q < 2^n)$

Donc, pour tous les couples d'entiers non nuls (p', q') , il est possible de plonger $e_{p'}$ et $e_{q'}$ dans le même \mathbb{A}_{n+1} , et on peut, en fonction des trois cas précédents, les écrire comme des éléments de $\mathbb{A}_n \times \mathbb{A}_n$:

1. $(p' = 2^n + p) \wedge (q' = q) \wedge (p < 2^n) \wedge (q < 2^n) \Rightarrow (e_{p'} = (0, e_p)) \wedge (e_{q'} = (e_q, 0))$
2. $(p' = p) \wedge (q' = 2^n + q) \wedge (p < 2^n) \wedge (q < 2^n) \Rightarrow (e_{p'} = (e_p, 0)) \wedge (e_{q'} = (0, e_q))$
3. $(p' = 2^n + p) \wedge (q' = 2^n + q) \wedge (p < 2^n) \wedge (q < 2^n) \Rightarrow (e_{p'} = (0, e_p)) \wedge (e_{q'} = (0, e_q))$

En appliquant la définition de la méthode de Cayley-Dickson, et en posant $e_r = e_p \cdot e_q$ on obtient, pour $p > 0$ et $q > 0$:

1. $e_{p'} \cdot e_{q'} = (0, e_p) \cdot (e_q, 0) = (0, e_p \cdot \overline{e_q} = (0, e_q \cdot e_p) = (0, -e_r) = -e_{2^n+r}$
2. $e_{p'} \cdot e_{q'} = (e_p, 0) \cdot (0, e_q) = (0, e_q \cdot e_p) = (0, -e_r) = -e_{2^n+r}$
3. $e_{p'} \cdot e_{q'} = (0, e_p) \cdot (0, e_q) = (-\overline{e_q} \cdot e_p = (e_q \cdot e_p, 0) = (-e_r, 0) = -e_r$

Ces relations permettent de démontrer par une récurrence très facile que $e_p \cdot e_q = s(p, q)e_{p \wedge q}$ où $p \wedge q$ est la fonction qui effectue un ou exclusif bit à bit⁹⁵ entre p et q et $s(p, q)$ est une fonction qui vaut 1 ou -1 et qui calcule le signe de $e_p \cdot e_q$ (cf. l'algorithme ci-dessous).

```

input  :  $(p, q) \in \mathbb{N}^2$ 
output :  $\pm 1$ , signe du produit de  $e_p \cdot e_q$ 

1 if  $p = 0$  Or  $q = 0$  then
2 |   return 1
3 end
4 if  $p = q$  then
5 |   return -1
6 end

7  $pi \leftarrow p$  ;
8  $qi \leftarrow q$  ;

9  $n \leftarrow \left\lfloor \frac{\ln(\max(p, q))}{\ln(2)} \right\rfloor$  // ( $n = 6$  suffit pour tous les SexagintaQuatrons) ;
10  $j \leftarrow 2^n$ ;
11 while  $j \geq 1$  do
12 |   if  $pi \geq j$  And  $qi \geq j$  then
13 | |    $Temp \leftarrow pi$ ;
14 | |    $pi \leftarrow qi - j$ ;
15 | |    $qi \leftarrow Temp - j$ ;
16 |   else if  $pi \geq j$  then
17 | |    $Temp \leftarrow pi$ ;
18 | |    $pi \leftarrow qi$ ;
19 | |    $qi \leftarrow Temp - j$ ;
20 | |   if  $pi = qi$  then
21 | | |   return 1
22 | |   end
23 |   else if  $qi \geq j$  then
24 | |    $Temp \leftarrow pi$ ;
25 | |    $pi \leftarrow qi - j$ ;
26 | |    $qi \leftarrow Temp$  ;
27 | |   if  $pi = qi$  then
28 | | |   return -1
29 | |   end
30 |   end
31 |    $j \leftarrow j/2$ ;
32 |   if  $pi = j$  Or  $qi = j$  then
33 | |   if  $pi < qi$  then
34 | | |   return 1
35 | |   else
36 | | |   return -1
37 | |   end
38 |   end
39 end

```

Algorithme 1: Calcul du Signe de $e_p \cdot e_q$

Cet algorithme permet de construire la table de multiplication de n'importe quel élément de \mathbb{A} , en particulier les centumduodetringintanions ou Routons(128 D, appelés ainsi à cause de la route 128, parallèle à la Silicon Valley), et les ducentinquingintasexions ou Voudons(256 D, appelés ainsi à cause des 256 Dieux du panthéon Vaudou).

XI.1.5 Conjugué, Module, Norme, Forme Polaire et Inverse

Comme toutes les algèbres construites à l'aide de la méthode de Cayley-Dickson, le conjugué d'un sexagintaquatration se calcule à partir du conjugué de l'algèbre sur laquelle cet ensemble est construit, à savoir les

⁹⁵. Bit-wise xor en anglais.

trigintaduonions : $\overline{t_0 + e \cdot t_1} = \overline{t_0} - e \cdot t_1$.

Ce qui permet de définir une norme (non multiplicative cf. infra) : $|t_0 + e \cdot t_1|^2 = |t_0|^2 + |t_1|^2$.

On peut calculer ce conjugué et cette norme en remontant des trigintaduonions aux sédénions puis aux octonions, etc. jusqu'aux réels :

Définition du conjugué : $\overline{\left(1 + \sum_{i=1}^{63} a_i \cdot e_i\right)} = 1 - \sum_{i=1}^{63} a_i \cdot e_i$

Définition de la norme : $\left|\sum_{i=0}^{63} a_i \cdot e_i\right|^2 = \sum_{i=0}^{63} a_i^2$

d'où l'inverse, pour $z \neq 0$: $z^{-1} = \frac{\overline{z}}{|z|^2}$

On peut vérifier facilement que la norme n'est pas multiplicative (cf. les trigintaduonions) $|e_3 + e_{10}|^2 = 2$, $|e_6 - e_{15}|^2 = 2$, mais comme $(e_3 + e_{10}) \cdot (e_6 - e_{15}) = 0$, la norme du produit est nulle.

XI.1.6 Propriétés algébriques

$(\mathbb{X}, +, \times, \cdot)$ est une \mathbb{R} -algèbre de dimension 64, ni commutative, ni associative, ni même alternative, par contre elle est flexible et associative en puissance.

XI.1.7 Synonymes, Isomorphismes, Exemples

Les Sexagintaquatronions sont parfois appelés Chingons⁹⁶ à cause des 64 hexagrammes du livre de divination chinois « I Ching ».

XI.1.8 Utilisation en physique

Aucune utilisation des sexagintaquatronions n'a pu être référencée.

XI.1.9 Références

1. R. P. C. de Marrais, *Kite-Chain Middens, Sand Mandalas, and Zero-Divisor Patterns in the 2ⁿ-ions Beyond the Sedenions*, 2002

96. Les noms alternatifs non issus du latin sont dus à R.P.C. de Marrais et T. Smith.