Axiomatique des nombres

Christine Laurent-Thiébaut

Enfin, vous allez apprendre comment définir les ensembles de nombres que vous manipulez depuis si longtemps. Ce chapitre n'est pas indispensable au reste du cours, mais fait néanmoins partie de la culture générale de tout mathématicien. Pour le comprendre, vous n'aurez besoin que d'une bonne maîtrise de la notion d'ensemble quotient, ainsi que des notions de base sur les structures algébriques : groupes, anneaux, corps et espaces vectoriels.

Table des matières

1 Cours

1.1 Contruction des entiers naturels

Nous allons proposer une définition axiomatique de l'ensemble $\mathbb{N}$ des entiers naturels. Nous déduirons ensuite de cette définition axiomatique les principales propriétés de $\mathbb{N}$. En particulier nous définirons l'addition de deux entiers naturels, la relation d'ordre sur $\mathbb{N}$ et la multiplication de deux entiers naturels.

Nous avons choisi d'exposer ici l'axiomatique dite de Peano. D'autres choix sont possibles comme par exemple l'axiomatique de l'ordre, comme nous le verrons plus loin.

Définition 1. *On appelle* triplet naturel *un triplet* $(O, \mathcal{N}, s)$*, où* $\mathcal{N}$ *est un ensemble,* O *un élément de* $\mathcal{N}$ *et* s *une application de* $\mathcal{N}$ *dans* $\mathcal{N}$ *qui vérifie les propriétés suivantes :*
(P_1) *s est injective,*
(P_2) $s(\mathcal{N}) = \mathcal{N} \setminus \{O\}$*,*
(P_3) *Si A est une partie de $\mathcal{N}$ telle que si $O \in A$ et $s(A) \subset A$ alors $A = \mathcal{N}$.*

Les 3 propriétés (P_1), (P_2), (P_3) sont les *axiomes de Peano* (bien qu'ils soient dus à Dedekind). L'application s est l'application « *successeur* » : comprenez $O =$« origine » ou « zéro », et $s(n) = n + 1$; mais ne le dites pas tout haut tant que nous n'avons pas défini l'addition.

Il convient de s'assurer qu'il existe effectivement de tels triplets $(O, \mathcal{N}, s)\ldots$ sans bien sûr invoquer l'ensemble des entiers que nous sommes en train de construire. On peut en exhiber dans différents contextes, selon le langage logique que l'on suppose connu. Puisque la notion de triplet naturel suppose la notion d'ensemble, nous pouvons supposer au minimum que les notions d'ensemble vide et de réunion sont connues. Dans notre premier exemple $\mathcal{N}$ sera un ensemble d'ensembles dont le zéro est l'ensemble vide. Définissons l'application successeur s par $s(A) = A \cup \{A\}$. Les premiers éléments de $\mathcal{N}$ sont :

$$\emptyset\,,\ \{\emptyset\}\,,\ \{\emptyset, \{\emptyset\}\}\,,\ \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\,,\ \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}\} \ldots$$

Ce n'est pas le plus commode pour compter, d'accord. Disons que vous soyez doté de la notion de chaîne de caractères, et de la concaténation. Commencez par la chaîne vide, puis définissez le successeur d'une chaîne comme la concaténation de cette chaîne avec la chaîne composée d'un seul caractère, mettons a. Voici les premiers éléments.

$$[]\,,\ [a]\,,\ [a, a]\,,\ [a, a, a]\,,\ [a, a, a, a]\,,\ [a, a, a, a, a]\ \ldots$$

Disons maintenant que vous soyez à la préhistoire, et que vos « naturels » sont des paquets de barres, tracées sur la paroi de la caverne. L'application successeur consiste à tracer une nouvelle barre à la suite des barres déjà écrites.

$$|\,,\ ||\ |||\,,\ ||||\,,\ |||||\,,\ ||||||\ \ldots$$

L'axiome (P_3) s'appelle l'axiome de *récurrence*. On en déduit la formulation classique du raisonnement par récurrence.

Proposition 1 (raisonnement par récurrence)**.** *Soit $(O, \mathcal{N}, s)$ un triplet naturel et $\mathcal{P}$ une propriété définie sur $\mathcal{N}$, qui vérifie :*

- *$\mathcal{P}(O)$ est vraie*
- *Pour tout $a \in \mathcal{N}$, ($\mathcal{P}(a)$ vraie) implique ($\mathcal{P}(s(a))$ vraie).*

Alors $\mathcal{P}(a)$ est vraie pour tout $a \in \mathcal{N}$.

Démonstration : Il suffit d'appliquer l'axiome (P_3) au sous-ensemble

$$A = \{a \in \mathcal{N} \mid \mathcal{P}(a) \text{ est vraie}\}$$

de $\mathcal{N}$. □

Théorème 1. *Soient $(O_1, \mathcal{N}_1, s_1)$ et $(O_2, \mathcal{N}_2, s_2)$ deux triplets qui vérifient les axiomes $(P_1), (P_2), (P_3)$, il existe une unique application bijective $f_{12} : \mathcal{N}_1 \to \mathcal{N}_2$ telle que*

$$f_{12}(O_1) = O_2, \tag{1}$$

et

$$f_{12} \circ s_1 = s_2 \circ f_{12}. \tag{2}$$

Démonstration : Vérifions que les deux conditions (1) et (2) définissent une unique application f_{12} de $\mathcal{N}_1$ dans $\mathcal{N}_2$. Soit A l'ensemble des éléments a de $\mathcal{N}_1$ pour lesquels $f_{12}(a)$ est défini de manière unique. La partie A satisfait les hypothèses de l'axiome (P_3) et par conséquent $A = \mathcal{N}_1$.

De manière analogue on définit f_{21} en échangeant les rôles de $\mathcal{N}_1$ et $\mathcal{N}_2$. Montrons que $f_{21} \circ f_{12} = Id_{\mathcal{N}_1}$ par récurrence. Pour $a \in \mathcal{N}_1$ considérons la propriété :

$$\mathcal{P}(a) \ : \ f_{21} \circ f_{12}(a) = a.$$

Par définition de f_{12} et f_{21}, $\mathcal{P}(O_1)$ est vraie. Soit $a \in \mathcal{N}_1$, supposons que $\mathcal{P}(a)$ est vraie, c'est-à-dire $f_{21} \circ f_{12}(a) = a$. Alors

$$f_{21} \circ f_{12}(s_1(a)) = f_{21}(s_2(f_{12}(a)) = s_1(f_{21} \circ f_{12}(a)) = s_1(a)$$

et $\mathcal{P}(s(a))$ est donc vraie. De la même manière on montrerait que $f_{12} \circ f_{21} = Id_{\mathcal{N}_2}$, ce qui prouve que f_{12} est bijective. □

Le Théorème 1 montre que les axiomes $(P_1), (P_2), (P_3)$ caractérisent le triplet $(O, \mathcal{N}, s)$ à isomorphisme près.

On peut donc identifier tous les triplets $(O, \mathcal{N}, s)$ qui vérifient les axiomes (P_1), (P_2), (P_3) à un triplet modèle que l'on notera $(0, \mathbb{N}, s)$ et que l'on appelle *ensemble des entiers naturels*.

Opérations sur les entiers

Sur l'ensemble des entiers naturels, nous allons maintenant définir l'addition, la multiplication et la relation d'ordre. Commençons par l'addition.

Définition 2. *On définit par récurrence sur l'ensemble* $\mathbb{N}$ *des entiers naturels, une loi de composition interne appelée* addition *et notée* $+$*, en posant :*

(i) $\forall a \in \mathbb{N}, \quad a + 0 = a$

(ii) $\forall (a, b) \in \mathbb{N}^2, \quad a + s(b) = s(a + b)$

Ces propriétés définissent complètement la loi $+$. En effet considérons la partie A de $\mathbb{N}$ définie par

$$A = \{b \in \mathbb{N} \mid \forall a \in \mathbb{N} \quad a + b \text{ est bien défini}\}.$$

On vérifie facilement que $0 \in A$ et $s(A) \subset A$ d'où $A = \mathbb{N}$ par (P_3).

Traditionnellement on note $1 = s(0)$ et, par définition de la loi $+$, on a $s(a) = s(a + 0) = a + s(0) = a + 1$ pour tout $a \in \mathbb{N}$.

Proposition 2. *La loi* $+$ *définie ci-dessus est associative, commutative, admet* 0 *comme élément neutre et tout entier naturel est régulier par rapport à cette opération.*

Démonstration :

- *Associativité* : Soient $a, b, c \in \mathbb{N}$, on montre que $(a + b) + c = a + (b + c)$ par récurrence sur c, a et b étant fixés. Le cas $c = 0$ est une conséquence immédiate de (i). Supposons que $(a + b) + c = a + (b + c)$ alors

$$\begin{aligned} (a + b) + s(c) &= s((a + b) + c) && \text{d'après (ii)} \\ &= s(a + (b + c)) && \text{par hypothèse de récurrence} \\ &= a + s(b + c) && \text{d'après (ii)} \\ &= a + (b + s(c)) && \text{d'après (ii),} \end{aligned}$$

  d'où le résultat.
- *Élément neutre* : Montrons par récurrence que pour tout $a \in \mathbb{N}$ on a $0 + a = a$, d'après (i) on aura $a + 0 = 0 + a = a$ et 0 sera donc l'élément neutre de la loi $+$. Par définition de $+$, $0 + 0 = 0$ et pour $a \in \mathbb{N}$ tel que $0 + a = a$, on a $0 + s(a) = s(0 + a) = s(a)$. Par conséquent si $A = \{a \in \mathbb{N} \mid 0 + a = a\}$, $0 \in A$ et $s(A) \subset A$ et par (P_3) $A = \mathbb{N}$.
- *Commutativité* : Si $a \in \mathbb{N}$ est fixé, montrons par récurrence sur b que $a + b = b + a$. On sait déjà que $a + 0 = 0 + a$, car 0 est l'élément neutre de $+$.
  Montrons que $a + 1 = 1 + a$ pour tout $a \in \mathbb{N}$. C'est vrai pour $a = 0$ et si c'est vrai pour un a donné, l'associativité permet d'écrire

$$s(a) + 1 = (a + 1) + 1 = (1 + a) + 1 = 1 + (a + 1) = 1 + s(a)$$

  ce qui achève le raisonnement.
  Supposons que $a + b = b + a$, alors grâce à l'associativité,

$$\begin{aligned} a + s(b) = a + (b + 1) &= (a + b) + 1 = (b + a) + 1 \\ &= b + (a + 1) = b + (1 + a) = (b + 1) + a = s(b) + a \end{aligned}$$

  ce qui termine la récurrence.

– *Régularité* : Montrons que pour tous a, x et y de $\mathbb{N}$ on a

$$a + x = a + y \Longrightarrow x = y. \tag{3}$$

Soient $x, y \in \mathbb{N}$, on pose $A = \{a \in \mathbb{N} \mid a + x = a + y \Rightarrow x = y\}$. La partie A contient 0, par définition de l'élément neutre. Soit $a \in A$, supposons que $s(a) + x = s(a) + y$. Par la propriété (ii) de $+$, on obtient $s(a + x) = s(a + y)$ et grâce à l'injectivité de s (axiome (P_2)) $a + x = a + y$. Mais puisque $a \in A$, cela implique $x = y$ et donc $s(A) \subset A$ d'où $A = \mathbb{N}$ par P_3.

□

Proposition 3. *Soient $a, b \in \mathbb{N}$ tels que $a + b = 0$ alors $a = b = 0$.*

Démonstration : Soit $b \in \mathbb{N}^*$, il existe alors $c \in \mathbb{N}$ tel que $b = s(c)$ et si $a \in \mathbb{N}$ on a $a+b = a+s(c) = s(a+c)$ par définition de l'addition. Mais l'application s est à valeurs dans $\mathbb{N}^*$ et par conséquent $a + b \neq 0$. On a donc prouvé que si $a, b \in \mathbb{N}$ sont tels que $a + b = 0$ alors $b = 0$ et de plus $a = a + 0 = 0$. □

Passons maintenant à la relation d'ordre.

Définition 3. *Soient $(a, b) \in \mathbb{N}^2$, on dira que $a \leqslant b$, s'il existe $c \in \mathbb{N}$ tel que $b = a + c$.*

Proposition 4. *La relation $\leqslant$ est une relation d'ordre sur $\mathbb{N}$ compatible avec l'addition.*

Démonstration : Nous devons prouver que $\leqslant$ est réflexive, antisymétrique, transitive et que si $a, b \in \mathbb{N}$ vérifient $a \leqslant b$, alors $a + n \leqslant b + n$ pour tout $n \in \mathbb{N}$.

– *Réflexivité* : Pour tout $a \in \mathbb{N}$, on a $a = a + 0$ par définition de l'addition, soit $a \leqslant a$.
– *Antisymétrie* : Soient $a, b \in \mathbb{N}$ tels que $a \leqslant b$ et $b \leqslant a$, c'est-à-dire il existe $c, d \in \mathbb{N}$ tels que $b = a + c$ et $a = b + d$. Par conséquent $b = (b + d) + c$ et puisque $+$ est associative et que tout élément est régulier pour $+$, on a $d+c = 0$, d'où $c = d = 0$ par la Proposition 3, soit $a = b$.
– *Transitivité* : Soient $a, b, c \in \mathbb{N}$ tels que $a \leqslant b$ et $b \leqslant c$, c'est-à-dire il existe $n, p \in \mathbb{N}$ tel que $b = a + n$ et $c = b + p$. Alors $c = (a + n) + p = a + (n + p)$ car $+$ est associative, d'où $a \leqslant c$.
– *Compatibilité avec l'addition* : Soient $a, b \in \mathbb{N}$ tels que $a \leqslant b$, c'est-à-dire il existe $c \in \mathbb{N}$ tel que $b = a + c$, et $n \in \mathbb{N}$. Alors

$$b + n = (a + c) + n = a + (c + n) = a + (n + c) = (a + n) + c$$

grâce à l'associativité et à la commutativité de l'addition, soit $a + n \leqslant b + n$.

□

Proposition 5. *L'ensemble ordonné $(\mathbb{N}, \leqslant)$ vérifie les propriétés suivantes :*
– *0 est le plus petit élément de $\mathbb{N}$;*

- (O_1) *toute partie non vide de* $\mathbb{N}$ *possède un plus petit élément ;*
- (O_2) *toute partie non vide et majorée de* $\mathbb{N}$ *possède un plus grand élément ;*
- (O_3) *l'ensemble* $\mathbb{N}$ *n'admet pas de plus grand élément.*

Les propriétés (O_1), (O_2) et (O_3) constituent les *axiomes de l'ordre* : le terme *axiome* peut vous sembler inappropri'e, car ce sont autant de *propositions* que nous allons démontrer. Il se trouve que (O_1), (O_2) et (O_3), si on les prend comme axiomes, constituent une définition alternative de $\mathbb{N}$, à partir de laquelle on peut démontrer ce qui précède.

Démonstration : Puisque 0 est élément neutre de l'addition, pour tout $a \in \mathbb{N}$ on a $a = 0 + a$, soit $0 \leqslant a$ par définition de la relation d'ordre. L'élément 0 de $\mathbb{N}$ est donc son plus petit élément.

- *Axiome* (O_1) : Soit A une partie non vide de $\mathbb{N}$. Si $0 \in \mathbb{N}$, c'est terminé, 0 est le plus petit élément de A. Si $0 \notin A$, l'ensemble $B = \{n \in \mathbb{N} \backslash A \mid \forall a \in A,\ n \leqslant a\}$ des minorants stricts de A est non vide puisqu'il contient 0, de plus $B \neq \mathbb{N}$ puisque $A \neq \emptyset$. Il résulte alors de l'axiome (P_3) qu'il existe $b \in B$ tel que $s(b) = b+1 \notin B$. Vérifions que $b + 1$ est un minorant de A. Puisque $b \in B$, on a $b \leqslant a$ pour tout $a \in A$. Si $a \in A$, il existe donc $c \in \mathbb{N}$ tel que $a = b+c$ avec $c \neq 0$ car $b \neq a$ et donc $c = s(d) = d + 1$. Par conséquent, grâce à l'associativité et à la commutativité de l'addition, $a = b + (d + 1) = (b + 1) + d$, soit $s(b) = b + 1 \leqslant a$. Mais $s(b) \in A$ car sinon il serait dans B ce qui contredirait la définition de b, c'est donc le plus petit élément de a.
- *Axiome* (O_3) : Supposons que $\mathbb{N}$ possède un plus grand élément N. Alors $s(N) = N + 1$ vérifie $N \leqslant s(N)$, par définition de la relation d'ordre, et comme N est le plus grand élément de $\mathbb{N}$, $s(N) \leqslant N$ et donc $N = s(N)$, c'est-à-dire $N = N + 1$ et par régularité de N pour l'addition $0 = 1 = s(0)$, ce qui contredit (P_2).
- *Axiome* (O_2) : Soit A une partie non vide, majorée de $\mathbb{N}$ et $B = \{n \in \mathbb{N} \setminus A \mid \forall a \in A,\ a \leqslant n\}$ l'ensemble des majorants stricts de A. L'ensemble B n'est pas vide car nous avons prouvé que $\mathbb{N}$ satisfait (O_3), il possède donc, comme nous venons de le montrer, un plus petit élément $b \neq 0$ puisque A est non vide. Grâce à (P_2), il existe alors $c \in \mathbb{N}$ tel que $b = s(c)$. Vérifions que c est un majorant de A. Puisque $s(c) \in B$, on a $a \leqslant s(c)$ et $a \neq s(c)$ pour tout $a \in A$. Si $a \in A$, il existe donc $d \in \mathbb{N}^*$ tel que $s(c) = a + d$, avec $d = s(e) = e + 1$ et par conséquent, grâce à l'associativité de l'addition, $c + 1 = a + (e + 1) = (a + e) + 1$ et, par régularité de 1 pour $+$, $c = a + e$, soit $a \leqslant c$. Mais alors $c \in A$ car sinon il serait dans B ce qui contredirait la définition de b comme plus petit élément de B, puisque $b = s(c)$.

□

Sur le même modèle que l'addition, nous allons construire une nouvelle loi de composition interne dans $\mathbb{N}$, la multiplication.

Définition 4. *On définit par récurrence sur l'ensemble* $\mathbb{N}$ *des entiers naturels, une loi de composition interne appelée* multiplication *et notée* $\times$*, en posant :*

(i) $\forall a \in \mathbb{N}, \quad a \times 0 = 0$

(ii) $\forall (a,b) \in \mathbb{N}^2, \quad a \times s(b) = (a \times b) + a$

Comme dans le cas de l'addition, ces propriétés définissent complètement la loi $\times$, en vertu de (P_3).

Proposition 6. *La loi $\times$ définie ci-dessus est associative, commutative, distributive par rapport à l'addition, admet 1 comme élément neutre et tout entier naturel non nul est régulier par rapport à cette opération.*

Démonstration : Remarquons tout d'abord que par définition de la multiplication on a pour tout $n \in \mathbb{N}$

$$n \times 1 = n \times s(0) = (n \times 0) + n = 0 + n = n.$$

Montrons par récurrence que pour tout $n \in \mathbb{N}$ on a

$$0 \times n = 0 \quad \text{et} \quad 1 \times n = n.$$

Ces propriétés sont vraies pour $n = 0$ et si elles sont vraies au rang n, on a

$$0 \times s(n) = (0 \times n) + 0 = 0 + 0 = 0 \quad \text{et} \quad 1 \times s(n) = (1 \times n) + 1 = n + 1 = s(n),$$

ce qui termine la récurrence.

Nous venons en particulier de prouver que 1 est l'élément neutre de la multiplication.

- *Distributivité* : Montrons par récurrence sur c que pour tout $a, b, c \in \mathbb{N}$ on a $(a+b) \times c = a \times c + b \times c$. Fixons $a, b \in \mathbb{N}$, pour $c = 0$ nous obtenons $(a+b) \times 0 = 0$ et $a \times 0 + b \times 0 = 0$, d'où $(a+b) \times 0 = a \times 0 + b \times 0 = 0$. Supposons que l'égalité est satisfaite pour c et calculons $(a+b) \times s(c)$ et $a \times s(c) + b \times s(c)$. En appliquant l'hypothèse de récurrence, on obtient

  $$(a+b) \times s(c) = (a+b) \times c + a + b = a \times c + b \times c + a + b$$

  et

  $$a \times s(c) + b \times s(c) = a \times c + a + b \times c + b = a \times c + b \times c + a + b$$

  par définition de la multiplication et grâce à la commutativité de l'addition, d'où le résultat.
- *Commutativité* : Montrons par récurrence sur b que pour tout $a, b \in \mathbb{N}$ on a $a \times b = b \times a$. Fixons a quelconque dans $\mathbb{N}$, si $b = 0$, nous avons déjà prouvé que $a \times 0 = 0 = 0 \times a$. Supposons que $a \times b = b \times a$, alors $a \times s(b) = a \times b + a$ et $s(b) \times a = (b+1) \times a = (b \times a) + (1 \times a) = (b \times a) + a$ grâce à la distributivité de $\times$ par rapport à $+$, soit $a \times s(b) = s(b) \times a$ en utilisant l'hypothèse de récurrence.
- *Associativité* : Montrons par récurrence sur c que pour tout $a, b, c \in \mathbb{N}$ on a $(a \times b) \times c = a \times (b \times c)$. Fixons $a, b \in \mathbb{N}$, pour $c = 0$ nous obtenons $(a \times b) \times 0 = 0$ et $a \times (b \times 0) = a \times 0 = 0$. Supposons que l'égalité est satisfaite pour c et calculons

$(a \times b) \times s(c)$ et $a \times (b \times s(c))$. Par définition de la multiplication, on obtient en utilisant l'hypothèse de récurrence

$$(a \times b) \times s(c) = ((a \times b) \times c) + a \times b = (a \times (b \times c)) + a \times b$$

et

$$\begin{aligned} a \times (b \times s(c)) &= a \times ((b \times c) + b) = ((b \times c) + b) \times a \\ &= (b \times c) \times a + b \times a \\ &= = (a \times (b \times c)) + a \times b \,, \end{aligned}$$

grâce à la commutativité de $\times$ et à la distributivité de $\times$ par rapport à $+$. D'où le résultat.

– *Régularité* : Montrons que pour tous $a \neq 0$, x et y de $\mathbb{N}$ on a :

$$x \times a = y \times a \Longrightarrow x = y. \tag{4}$$

Soient $x, y \in \mathbb{N}$, on pose $A = \{a \in \mathbb{N}^* \mid x \times a = y \times a \Rightarrow x = y\}$. La partie A contient 1, par définition de l'élément neutre. Soit $a \in A$, supposons que $x \times s(a) = y \times s(a)$. Par définition de la multiplication, on obtient $(x \times a) + x = (y \times a) + y$ puis $(y \times a) + x = (y \times a) + y$, puisque $a \in A$. La régularité de l'addition implique alors $x = y$, donc $s(a) \in A$ et par conséquent $A = \mathbb{N}^*$.
Notons que la régularité des éléments non nuls de $\mathbb{N}$ par rapport à la multiplication implique en particulier que si $a, b \in \mathbb{N}$ vérifient $a \times b = 0$ alors $a = 0$ ou $b = 0$.

□

Montrons maintenant le lien entre la multiplication et l'addition dans $\mathbb{N}$.

Proposition 7. *Soient $a \in \mathbb{N}$ et $n \in \mathbb{N}^*$, alors :*

$$a \times n = \underbrace{a + \cdots + a}_{\text{n fois}} \,.$$

Démonstration : Soit $a \in \mathbb{N}$, prouvons le résultat par récurrence sur n. Si $n = 1$, c'est évident puisque $a \times 1 = a$. Supposons le résultat vrai pour $n \leqslant 1$ alors par définition de la multiplication

$$a \times s(n) = (a \times n) + a = (\underbrace{a + \cdots + a}_{\text{n fois}}) + a = \underbrace{a + \cdots + a}_{\text{(n+1) fois}} \,,$$

d'où le résultat puisque $s(n) = n + 1$. □

Voici maintenant la compatibilité entre la relation d'ordre et la multiplication.

Proposition 8. *La relation d'ordre $\leqslant$ sur $\mathbb{N}$ est compatible avec la multiplication :*

$$a \leqslant b \implies \Big(\forall n \in \mathbb{N},\ an \leqslant bn\Big).$$

Démonstration : Soient $a, b \in \mathbb{N}$ tels que $a \leqslant b$, prouvons que, pour tout $n \in \mathbb{N}$, on a $a \times n \leqslant b \times n$. Puisque $a \leqslant b$, il existe $c \in \mathbb{N}$ tel que $b = a + c$, alors $b \times n = (a + c) \times n = a \times n + c \times n$ grâce à la distributivité de $\times$ par rapport à $+$, d'où $a \times n \leqslant b \times n$.

Notons que si de plus $a \neq b$ et $n \neq 0$ alors $a \times n \neq b \times n$. En effet si $a \neq b$ alors $c \neq 0$ et $c \times n \neq 0$ puisque $n \neq 0$. □

Proposition 9. *L'ensemble ordonné $(\mathbb{N}, \leqslant)$ est archimédien, c'est-à-dire pour tout $a \in \mathbb{N}^*$ et tout $b \in \mathbb{N}$, il existe $n \in \mathbb{N}$ tel que $b \leqslant n \times a$ et $n \times a \neq b$.*

Démonstration : Soient $a, b \in \mathbb{N}$. Si $b \leqslant a$ et $a \neq b$, $n = 1$ convient. Si $a \leqslant b$, on considère l'ensemble

$$B = \{x \times a, x \in \mathbb{N} \mid 1 \leqslant x \times a \leqslant b\}.$$

L'ensemble B est non vide, puisque $a \in B$, et il est majoré par b. Il possède donc un plus grand élément $x_0 \times a$. Posons $n = s(x_0) = x_0 + 1$, alors $x_0 \times a \leqslant n \times a$ et $n \times a \neq x_0 \times a$ donc $n \times a \notin B$ soit $b \leqslant n \times a$ et $n \times a \neq b$. □

1.2 Bases de numération

Le but de cette section est de définir un système d'écriture qui permette de manipuler aisément les nombres entiers, en particulier d'expliciter facilement les opérations addition et multiplication.

Pour simplifier les notations, la multiplication sur $\mathbb{N}$ sera notée ab pour $a \times b$, le résultat de la multiplication de a par a itérée n fois sera noté a^n et l'inégalité stricte $a < b$ pour $a \leqslant b$ et $a \neq b$.

On décide de représenter les premiers entiers par un symbole unique appelé *chiffre* et on cherche un moyen d'utiliser ces symboles pour écrire tous les nombres entiers. Deux symboles ont déjà été définis : 0 pour le plus petit élément de $\mathbb{N}$ et 1 pour $s(0)$. Traditionnellement on note 2 pour $s(1)$, 3 pour $s(2)$, 4 pour $s(3)$, 5 pour $s(4)$, 6 pour $s(5)$, 7 pour $s(6)$, 8 pour $s(7)$, 9 pour $s(8)$, A pour $s(9)$, B pour $s(A)$, C pour $s(B)$, D pour $s(C)$, E pour $s(D)$, F pour $s(E)\ldots$

Etant donné un nombre entier $a > 1$ appelé *base*, par exemple 2, 8, A, C ou G, on peut proposer l'algorithme suivant pour dénombrer un ensemble :

on fait autant de paquets de a éléments qu'il est possible, puis autant de paquets de a paquets et ainsi de suite...

Remarquons qu'à la n-ième étape, on obtient des regroupements de a^n éléments.

Par exemple pour $a = 2$, considérons l'ensemble $E = \{\clubsuit\clubsuit\clubsuit\clubsuit\clubsuit\clubsuit\clubsuit\}$ et appliquons l'algorithme

nous obtenons un paquet de 2 paquets, qui regroupe donc 2^2 éléments, plus un paquet de 2 éléments, plus 1 élément. Le nombre d'éléments de E pourrait alors être représenté par le triple symbole $\overline{111}$, le premier 1 à gauche correspondant au nombre de paquets de paquets, le second 1 au nombre de paquets restant et le dernier 1 au nombre d'éléments distincts.

L'algorithme se formalise de la manière suivante : écrire un nombre entier x sous la forme

$$x = x_n a^n + \cdots + x_1 a + x_0,\ 0 \leqslant x_i < a,$$

appelé *développement de x dans la base a*. Si cette écriture est unique le nombre x pourrait alors être représenté par le multi-symbole $\overline{x_n \dots x_1 x_0}$.

Proposition 10. *Si $a \in \mathbb{N}$ vérifie $1 < a$, la suite de terme général $u_n = a^n$ est strictement croissante et non majorée.*

Démonstration : Puisque $1 < a$, la compatibilité de la relation d'ordre avec la multiplication implique $a^n < a^{n+1}$ car a^n est non nul. La suite $(u_n)_{n\in\mathbb{N}}$ est donc croissante.

Nous devons prouver que pour tout $b \in \mathbb{N}$, il existe $n \in \mathbb{N}$ tel que $b < u_n$. Puisque $\mathbb{N}$ est archimédien (cf. Proposition 9), il suffit de montrer que $na \leqslant a^n$ pour tout n tel que $1 \leqslant n$.

Pour $n = 1$ on a bien $a^1 = a$. Supposons que $na \leqslant a^n$. Puisque $1 \leqslant n$ et $1 < a$, soit $2 \leqslant a$, on a

$$(n+1)a \leqslant 2(na) \leqslant 2a^n \leqslant aa^n \leqslant a^{n+1}.$$

On a donc montré par récurrence que $na \leqslant a^n$ pour tout n tel que $1 \leqslant n$. □

Théorème 2. *Pour tout $a \in \mathbb{N}$ et tout $b \in \mathbb{N}^*$, il existe des entiers q et r uniques tels que*

$$a = bq + r \quad \textit{et} \quad 0 \leqslant r < b.$$

Démonstration : On considère l'ensemble $A = b\mathbb{N} \cap \{x \in \mathbb{N} \mid x \leqslant a\}$, où $b\mathbb{N} = \{x \in \mathbb{N} \mid \exists n \in \mathbb{N}, x = bn\}$. L'ensemble A contient 0 et est majoré par a, il possède donc un plus grand élément bq. L'élément bq ainsi défini est unique et vérifie $bq \leqslant a < b(q+1)$. On note r la solution de l'équation $bq + x = a$, qui existe puisque $bq \leqslant a$, elle vérifie $0 \leqslant r < b$ puisque $a < b(q+1)$. □

L'opération définie dans le théorème s'appelle la *division euclidienne de a par b*, q est le *quotient* de la division et r le *reste*. Si $r = 0$, on dit que a est *divisible* par b.

Théorème 3. *Si $a \in \mathbb{N}$ vérifie $1 < a$, tout nombre entier x s'écrit de manière unique*

$$x = x_n a^n + \cdots + x_1 a + x_0,\ 0 \leqslant x_i < a,\ 1 \leqslant i \leqslant n,\ \textit{et}\ x_n \neq 0\ .$$

Démonstration :

– *Unicité* : Supposons qu'un tel développement existe alors

$$x = \underbrace{(x_n a^{n-1} + \cdots + x_1)}_{X_1} a + x_0 \quad \text{et} \quad x_0 < a.$$

Les nombres x_0 et X_1 sont respectivement le reste et le quotient de la division euclidienne de x par a, ils sont donc déterminés de manière unique. Si on pose

$$X_k = x_n a^{n-k} + \cdots + x_{k+1} a + x_k$$

on remarque que x_k est le reste de la division euclidienne de X_k par a et X_{k+1} son quotient. En posant $X_0 = x$ une récurrence immédiate prouve que les x_k sont déterminés de manière unique.

– *Existence* : Pour x fixé dans $\mathbb{N}$, les conditions

$$y_0 = x, \quad y_k = a y_{k+1} + x_k \quad \text{avec} \quad x_k < a$$

déterminent par récurrence deux suites $(x_k)_{k\in\mathbb{N}}$ et $(y_k)_{k\in\mathbb{N}}$. Nous allons prouver que la suite $(y_k)_{k\in\mathbb{N}}$ est stationnaire identiquement égale à 0 à partir d'un certain rang. Remarquons que, puisque $1 < a$, la suite $(y_k)_{k\in\mathbb{N}}$ vérifie

$$2y_{k+1} \leqslant a y_{k+1} \leqslant y_k,$$

ce qui implique que $2^k y_k \leqslant x$. Nous avons vu dans la preuve de la Proposition 9 que $2k \leqslant 2^k$, on en déduit donc que $2k y_k \leqslant x$ et par conséquent $y_k = 0$ dès que $x < 2k$ en raison de la compatibilité de la relation d'ordre avec la multiplication. On désigne par n le plus grand entier k tel que $y_k \neq 0$. Par définition de n et de la suite $(y_k)_{k\in\mathbb{N}}$, on a

$$y_n = x_n \quad \text{et} \quad y_{n-k} = x_n a^k + \cdots + x_{n-k},\ k = 1, \ldots, n,$$

en particulier pour $k = n$, on obtient

$$x = y_0 = x_n a^n + \cdots + x_1 a + x_0.$$

□

Notons que dans la base a, le nombre entier a s'écrit toujours $\overline{10}$ puisque $a = (1 \times a) + 0$.

La base communément utilisée est $a = s(9)$, que l'on appelle la *base dix*, et tout nombre entier s'écrit alors en utilisant les chiffres $0, 1, 2, 3, 4, 5, 6, 7, 8$ et 9. L'usage courant veut que l'on écrive simplement 545 pour $\overline{545}$ lorsqu'il n'y a pas d'ambiguïté sur la base choisie.

En informatique les bases $a = 2$ et $a = s(F)$ sont souvent utilisées, c'est ce qui est appelé *système de numération binaire* et *système de numération hexadécimale*.

Exemple : Si x s'écrit $\overline{125}$ en base dix, il s'écrit $\overline{1111101}$ en binaire et $\overline{7D}$ en hexadécimal.

La démonstration de l'existence du développement dans une base a fixée donne un algorithme pour calculer les chiffres qui apparaissent dans l'écriture d'un nombre entier x dans cette base. Le premier chiffre de droite est donné par le reste de la division euclidienne de x par a, le second chiffre par le reste de la division euclidienne du quotient de la division précédente par a et ainsi de suite jusqu'à l'obtention d'un quotient nul.

Relation d'ordre et numération

On considère le problème suivant : étant donnés deux entiers x et y, peut-on déterminer facilement si $x \leqslant y$ à partir de leur écriture dans une base donnée.

Fixons une base a arbitraire. L'unicité du développement d'un entier relativement à la base a implique que $x = y$ si et seulement si ils ont même écriture dans la base a.

Lemme 1. *Si $x \in \mathbb{N}$ s'écrit $\overline{x_n \dots x_0}$ dans la base a, alors $a^n \leqslant x < a^{n+1}$.*

Démonstration : L'hypothèse du lemme se traduit par

$$x = x_n a^n + \cdots + x_1 a + x_0.$$

Par conséquent $a^n \leqslant x_n a^n \leqslant x$ puisque $1 \leqslant x_n$. Montrons par récurrence sur n que $x < a^{n+1}$. Si $n = 0$, $x = x_0 < a$. Supposons l'inégalité vraie pour les nombres dont l'écriture dans la base a contient $n + 1$ chiffres. Soit x qui s'écrit $\overline{x_{n+1} x_n \dots x_0}$, alors

$$x = x_{n+1} a^{n+1} + y,$$

avec y qui s'écrit $\overline{x_n \dots x_0}$ dans la base a et par conséquent on obtient

$$x < x_{n+1} a^{n+1} + a^{n+1} \leqslant a^{n+1}(x_{n+1} + 1) \leqslant a^{n+2}$$

en utilisant l'hypothèse de récurrence et le fait que $x_{n+1} < a$. □

Supposons que x et y s'écrivent respectivement $\overline{x_n \dots x_0}$ et $\overline{y_m \dots y_0}$ dans la base a et que $x \neq y$.

Supposons que $n < m$ alors $n + 1 \leqslant m$ et puisque $1 < a$, le Lemme 1 implique

$$x < a^{n+1} \leqslant a^m \leqslant y,$$

d'où $x < y$.

Nous avons donc prouvé que :

Si deux entiers s'écrivent dans une même base avec un nombre de chiffres différent, le plus petit est celui dont l'écriture possède le moins de chiffres.

Supposons que $m = n$. Puisque $x \neq y$, il existe $1 \leqslant r \leqslant n+1$ tel que $x_i = y_i$ pour tout $r \leqslant i$ et $x_{r-1} < y_{r-1}$. On déduit alors du Lemme 1 que

$$\begin{aligned} x &= x_n a^n + \cdots + x_{r-1}a^{r-1} + x_{r-2}a^{r-2} + \cdots + x_1 a + x_0 \\ &< x_n a^n + \cdots + x_{r-1}a^{r-1} + a^{r-1} \\ &< x_n a^n + \cdots + (x_{r-1}+1)a^{r-1} \\ &< x_n a^n + \cdots + y_{r-1}a^{r-1} \\ &< y \end{aligned}$$

Nous avons donc prouvé que :

Si deux entiers s'écrivent dans une même base avec un même nombre de chiffres et si en partant de la gauche les chiffres sont tous égaux jusqu'au rang r, alors le plus petit des deux est celui qui a le plus petit chiffre de rang $r-1$.

Lois de composition internes et numération

Soient x et y deux nombres entiers qui s'écrivent respectivement $\overline{x_n \dots x_0}$ et $\overline{y_m \dots y_0}$ dans la base a, on cherche un mécanisme pour déterminer l'écriture dans la base a des nombres $x+y$ et $x \times y$.

Comme $+$ et $\times$ sont toutes deux commutatives, on peut supposer sans perte de généralité que $m \leqslant n$.

• *Cas de l'addition*

Si $m \neq n$ on pose $y_n = \cdots = y_{m+1} = 0$. Les propriétés de commutativité et d'associativité de $+$ et de distributivité de $\times$ par rapport à $+$ donnent

$$x + y = (x_n + y_n)a^n + \cdots + (x_1 + y_1)a + (x_0 + y_0).$$

Si pour tout $i = 0, \dots, n$, $x_i + y_i < a$, le développement ci-dessus correspond au développement de $x+y$ dans la base a.

Sinon supposons que l'un des entiers $x_i + y_i$ est supérieur ou égal à a, alors

$$x_i + y_i = a + z_i \quad \text{avec} \quad z_i < a$$

et le nombre $x_i + y_i$ s'écrit alors $\overline{1z_i}$ dans la base a. Par suite $(x_i + y_i)a^i = a^{i+1} + z_i a^i$ et $x_{i+1} + y_{i+1}$ doit être remplacé par $x_{i+1} + y_{i+1} + 1$, c'est le mécanisme de la retenue.

En conclusion, l'écriture dans la base a du résultat de l'addition de deux entiers nécessite seulement la connaissance de la table d'addition en base a des nombres dont l'écriture en base a ne possède qu'un seul chiffre.

• *Cas de la multiplication*

Grâce à la distributivité de $\times$ par rapport à $+$ et à l'associativité de $\times$, on a

$$xy = x_n(a^n y) + \cdots + x_1(ay) + x_0 y.$$

On est donc ramené

1) à multiplier un entier par une puissance de la base,

2) à multiplier un entier par un nombre strictement inférieur à la base et qui s'écrit donc avec un seul chiffre,

3) à faire des additions.

- *Multiplication par a^k*

Cherchons l'écriture en base a de $a^k y$. On a

$$a^k y = y a^k = y_m a^{m+k} + \cdots + y_0 a^k$$

et $a^k y$ s'écrit donc

$$\overline{y_m \dots y_0 \underbrace{0 \dots 0}_{k}}.$$

L'existence des k chiffres 0 dans la partie droite de l'écriture de $a^k y$ en base a, explique le décalage dans la disposition pratique de la multiplication.

Exemple : En base a avec $5 < a$, effectuons la multiplication de $\overline{45}$ par $\overline{101}$, on aura

$$\overline{45} \times \overline{101} = (4a + 5)(a^2 + 1) = (4a^3 + 5a^2) + (4a + 5) = \overline{4500} + \overline{45}$$

qui en pratique s'écrit

$$\begin{array}{r} 45 \\ \times 101 \\ \hline 45 \\ 45 \\ \hline 4545 \end{array}$$

- *Multiplication par un entier strictement inférieur à a*

Soit $b < a$, alors $by = by_m a^m + \cdots + by_0$. Si $by_i < a$ pour tout $i = 0, \dots, m$, c'est fini sous réserve de connaître la table de multiplication en base a des nombres dont l'écriture en base a ne possède qu'un seul chiffre.

Si l'un des by_i est supérieur ou égal à a, alors

$$by_i = c_i a + z_i \quad \text{avec} \quad c_i < a \quad et \quad z_i < a$$

car $by_i < a^2$ et le nombre by_i s'écrit alors $\overline{c_i z_i}$ dans la base a. Par suite $(by_i)a^i = c_i a^{i+1} + z_i a^i$ et by_{i+1} doit être remplacé par $by_{i+1} + c_i$, c'est le mécanisme de la retenue.

1.3 Construction des entiers relatifs

L'ensemble $\mathbb{N}$ des entiers naturels a été défini de manière axiomatique et deux lois de composition interne ont été définies sur cet ensemble : l'addition et la multiplication. Certaines équations liées à ces deux lois comme

$$a = b + x \quad \text{ou} \quad a = b \times x, b \neq 0 \ ,$$

n'admettent pas toujours une solution. Il serait intéressant de construire un ensemble de nombres contenant $\mathbb{N}$ dans lequel ces équations simples auraient toujours une solution.

Étant donné un couple $(a, b) \in \mathbb{N} \times \mathbb{N}$, on s'intéresse d'abord à l'équation

$$a = b + x. \tag{5}$$

Par définition de la relation d'ordre sur $\mathbb{N}$, cette équation possède une solution dans $\mathbb{N}$ si et seulement si $b \leqslant a$. On cherche à construire un nouvel ensemble de nombres $\mathbb{Z}$ contenant $\mathbb{N}$, muni d'une loi de composition interne associative et commutative, notée $+$, dont la restriction à $\mathbb{N}$ coïncide avec l'addition de $\mathbb{N}$ et dans lequel l'équation (5) possède toujours une unique solution. Dans le cas particulier où $a = 0$, x sera un inverse de b pour $+$ et $(\mathbb{Z}, +)$ sera un groupe abélien.

L'idée est d'identifier la solution x de (5) au couple (a, b), mais malheureusement deux couples (a, b) et (a', b'), vérifiant $a \leqslant b$ et $a' \leqslant b'$, peuvent définir le même entier x. Cherchons à quelle condition les deux couples (a, b) et (a', b') définissent le même entier x. Si $x \in \mathbb{N}$ satisfait à la fois

$$a = b + x \quad \text{et} \quad a' = b' + x,$$

alors $a + b' + x = a' + b + x$ et par régularité de l'addition, on doit avoir $a + b' = a' + b$.

Proposition 11. *La relation $\mathcal{R}$ définie sur $\mathbb{N} \times \mathbb{N}$ par*

$$(a, b)\mathcal{R}(a', b') \Leftrightarrow a + b' = a' + b \tag{6}$$

est une relation d'équivalence compatible avec l'addition sur $\mathbb{N} \times \mathbb{N}$.

Démonstration : La relation $\mathcal{R}$ est clairement réflexive et symétrique. Montrons qu'elle est transitive. Soient (a, b), (a', b') et (a'', b'') trois couples d'entiers tels que $(a, b)\mathcal{R}(a', b')$ et $(a', b')\mathcal{R}(a'', b'')$, ils vérifient donc

$$a + b' = a' + b \quad \text{et} \quad a' + b'' = a'' + b'.$$

En ajoutant membre à membre ces deux égalités on obtient

$$a + b'' + a' + b' = a'' + b + a' + b'$$

grâce à l'associativité et à la commutativité de l'addition dans $\mathbb{N}$, soit $a + b'' = a'' + b$ par régularité de l'addition. La relation $\mathcal{R}$ est donc une relation d'équivalence sur $\mathbb{N} \times \mathbb{N}$.

Montrons qu'elle est compatible avec l'addition. Soient (a, b), (a', b') deux couples d'entiers tels que $(a, b)\mathcal{R}(a', b')$ et (c, d), (c', d') deux autres couples d'entiers tels que $(c, d)\mathcal{R}(c', d')$, alors $a + b' = a' + b$ et $c + d' = c' + d$ et en ajoutant membre à membre

$$(a + c) + (b' + d') = (a' + c') + (b + d),$$

ce qui signifie que $(a + c, b + d)\mathcal{R}(a' + c', b' + d')$. □

On notera $\overline{(a, b)}$ la classe du couple (a, b) pour la relation $\mathcal{R}$.

Définition 5. *On appelle ensemble des entiers relatifs l'ensemble quotient* $\mathbb{N} \times \mathbb{N}/\mathcal{R}$ *et on le note* $\mathbb{Z}$.

Proposition 12. *L'ensemble* $\mathbb{Z}$ *muni de la loi quotient déduite de l'addition sur* $\mathbb{N}\times\mathbb{N}$*, notée encore* $+$*, est un groupe abélien.*

Démonstration : La relation $\mathcal{R}$ étant compatible avec l'addition sur $\mathbb{N} \times \mathbb{N}$, on définit une loi de composition interne sur $\mathbb{Z}$ en posant

$$\overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}.$$

Cette loi conserve les propriétés d'associativité et de commutativité de l'addition sur $\mathbb{N} \times \mathbb{N}$. Vérifions que $e = \overline{(0,0)}$ est un élément neutre pour cette loi. En effet si $x = \overline{(a,b)} \in \mathbb{Z}$, $x + e = e + x$ par commutativité et

$$x + e = \overline{(a,b)} + \overline{(0,0)} = \overline{(a+0, b+0)} = \overline{(a,b)} = x.$$

On peut remarquer que $(a,b) \in \overline{(0,0)}$ si et seulement si $a = b$. En effet $(a,b)\mathcal{R}(0,0)$ si et seulement si $a + 0 = 0 + b$, i.e. $a = b$.

Pour obtenir une structure de groupe abélien, il reste à prouver que tout élément x de $\mathbb{Z}$ possède un inverse pour cette loi. Si $x = \overline{(a,b)}$, posons $\widetilde{x} = \overline{(b,a)}$, alors $x+\widetilde{x} = \widetilde{x}+x$ par commutativité et

$$x + \widetilde{x} = \overline{(a,b)} + \overline{(b,a)} = \overline{(a+b, b+a)} = \overline{(a+b, a+b)} = \overline{(0,0)} = e.$$

□

Proposition 13. *On définit un morphisme injectif* $f : \mathbb{N} \to \mathbb{Z}$ *en posant* $f(a) = \overline{(a,0)}$

Démonstration : Vérifions que l'application $f : \mathbb{N} \to \mathbb{Z}$ définie par $f(a) = \overline{(a,0)}$ est additive. Soient a et b dans $\mathbb{N}$, alors

$$f(a+b) = \overline{(a+b, 0)} = \overline{(a,0)} + \overline{(b,0)} = f(a) + f(b)$$

par définition de l'addition dans $\mathbb{Z}$. Montrons maintenant que f est injective. Soient a et b dans $\mathbb{N}$ tels que $f(a) = f(b)$, c'est-à-dire $\overline{(a,0)} = \overline{(b,0)}$. Par définition de la relation $\mathcal{R}$ cela signifie que $a + 0 = b + 0$, soit $a = b$, d'où l'injectivité de l'application f. □

Pour simplifier les écritures on utilise les conventions de notations suivantes :

(i) Si $a \in \mathbb{N}$, on note encore a l'élément $\overline{(a,0)}$ de $\mathbb{Z}$, identifiant ainsi $\mathbb{N}$ et son image par f dans $\mathbb{Z}$.

(ii) Si $a \in \mathbb{N}$, on note $-a$ l'élément $\overline{(0,a)}$ de $\mathbb{Z}$, c'est-à-dire l'inverse de a pour l'addition dans $\mathbb{Z}$.

(iii) Si $a \in \mathbb{N}$ et $b \in \mathbb{N}$, on écrira $a - b$ pour $a + (-b)$.

Remarquons également que tout élément $\overline{(a,b)}$ possède un représentant de la forme $(x,0)$ ou $(0,x)$. En effet $(x,0) \in \overline{(a,b)}$ si et seulement si $a = b + x$ dans $\mathbb{N}$, ce qui

équivaut à $b \leqslant a$ par définition de la relation d'ordre sur $\mathbb{N}$, de même $(0,x) \in \overline{(a,b)}$ si et seulement si $a+x=b$ ce qui équivaut à $a \leqslant b$. La relation d'ordre sur $\mathbb{N}$ étant une relation d'ordre total, si $a \in \mathbb{N}$ et $b \in \mathbb{N}$ alors soit $a \leqslant b$, soit $b \leqslant a$ et d'après ce qui précède dans le premier cas il existe $x \in \mathbb{N}$ tel que $a+x=b$ et alors $\overline{(x,0)} \in \overline{(a,b)}$ et dans le deuxième cas il existe $x \in \mathbb{N}$ tel que $b+x=a$ et alors $(0,x) \in \overline{(a,b)}$.

On en déduit que $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$, où $-\mathbb{N} = \{y \in \mathbb{Z} \mid y = -x,\ x \in \mathbb{N}\}$. De plus $\mathbb{N} \cap (-\mathbb{N}) = \{0\}$ car si $u = \overline{(a,b)} \in \mathbb{Z}$ vérifie $u \in \mathbb{N}$ et $-u \in \mathbb{N}$, alors $\overline{(a,b)} = \overline{(b,a)}$ soit $a+a=b+b$ et donc $a=b$ et $u=0$.

On dit que deux éléments x et y de $\mathbb{Z}$ sont de *même signe* si x et y sont tous deux dans $\mathbb{N}$ ou dans $-\mathbb{N}$ et de *signes contraires* si parmi x et y l'un est dans $\mathbb{N}$ et l'autre dans $-\mathbb{N}$.

Nous venons de voir que $\mathbb{Z}$ contient strictement $\mathbb{N}$ et même que l'ensemble $\mathbb{Z} \setminus \mathbb{N}$ est infini, mais néanmoins il existe une bijection de $\mathbb{N}$ sur $\mathbb{Z}$: $\mathbb{Z}$ est dénombrable.

Proposition 14. *L'ensemble $\mathbb{Z}$ est dénombrable.*

Démonstration : L'application $f : \mathbb{N} \to \mathbb{Z}$ de $\mathbb{N}$ dans $\mathbb{Z}$ définie par $f(2n) = n$ et $f(2n+1) = -(n+1)$ est clairement bijective. □

Revenons à l'équation (5) *du début de ce paragraphe.* Soient a et b dans $\mathbb{N}$, alors avec les notations ci-dessus si x satisfait $a = b+x$ dans $\mathbb{Z}$, cela signifie $\overline{(a,0)} = \overline{(b,0)} + x$, soit $x = \overline{(0,b)} + \overline{(a,0)} = \overline{(a,b)}$. L'équation (5) possède donc toujours une solution dans $\mathbb{Z}$ et $x \in \mathbb{N}$ si et seulement si $b \leqslant a$. Plus généralement si a et b sont dans $\mathbb{Z}$, $a = b+x$ équivaut à $x = b-a$ puisque $(\mathbb{Z},+)$ est un groupe et l'équation $a = b+x$ possède toujours une unique solution.

Relation d'ordre dans $\mathbb{Z}$

Rappelons que si $(a,b) \in \mathbb{N} \times \mathbb{N}$, on a $a \leqslant b$, s'il existe $c \in \mathbb{N}$ tel que $b = a+c$, c'est-à-dire $b-a \in \mathbb{N}$. Nous pouvons alors prolonger de manière naturelle à $\mathbb{Z}$ la relation d'ordre sur $\mathbb{N}$ en posant $x \leqslant y$ si et seulement si $y - x \in \mathbb{N}$. Vérifions qu'il s'agit bien d'une relation d'ordre. Elle est réflexive car $x \leqslant x$ puisque $x - x = 0 \in \mathbb{N}$. Elle est antisymétrique, puisque $x - y = -(y-x)$ et $\mathbb{N} \cap (-\mathbb{N}) = \{0\}$ impliquent $x = y$ si $x-y$ et $y-x$ sont tous deux dans $\mathbb{N}$. Soient $x, y, z \in \mathbb{Z}$ tels que $x \leqslant y$ et $y \leqslant z$, c'est-à-dire $y - x \in \mathbb{N}$ et $z - y \in \mathbb{N}$, alors $(y-x) + (z-y) = z - x \in \mathbb{N}$ et donc $x \leqslant z$, ce qui prouve la transitivité de $\leqslant$.

Remarquons que les éléments de $\mathbb{N}$ sont exactement les $x \in \mathbb{Z}$ tels que $0 \leqslant x$, on les appelle les *entiers positifs* et que les éléments de $-\mathbb{N}$ sont exactement les $x \in \mathbb{Z}$ tels que $x \leqslant 0$, ils sont dits *négatifs*.

Multiplication dans $\mathbb{Z}$

Pour terminer nous allons définir dans $\mathbb{Z}$ une deuxième loi de composition interne qui prolongera la multiplication sur $\mathbb{N}$ et telle que $(\mathbb{Z},+,\times)$ possède une structure d'anneau intègre.

Soient $x = \overline{(a,b)}$ et $y = \overline{(c,d)}$ deux éléments de $\mathbb{Z}$, on pose

$$x \times y = \overline{(a,b)} \times \overline{(c,d)} = \overline{(ac+bd, bc+ad)}.$$

Vérifions que cette définition a bien un sens en remarquant qu'elle est indépendante des représentants choisis. Nous devons prouver que si $(a,b)\mathcal{R}(a',b')$ et $(c,d)\mathcal{R}(c',d')$ alors $(ac+bd, bc+ad)\mathcal{R}(a'c'+b'd', b'c'+a'd')$. Supposons que $a+b' = a'+b$ et $c+d' = c'+d$, alors

$$\begin{aligned}
(ac+bd)+(b'c'+a'd')+bc' &= ac+b(d+c')+(b'c'+a'd') \\
&= ac+b(c+d')+(b'c'+a'd') \\
&= ac+bc+(b+a')d'+b'c' \\
&= ac+bc+(a+b')d'+b'c' \\
&= a(c+d')+bc+b'd'+b'c' \\
&= a(c'+d)+bc+b'd'+b'c' \\
&= ad+bc+(a+b')c'+b'd' \\
&= ad+bc+(a'+b)c'+b'd' \\
&= (ad+bc)+(a'c'+b'd')+bc'
\end{aligned}$$

d'où $(ac+bd)+(b'c'+a'd') = (a'c'+b'd')+(ad+bc)$ et donc $(ac+bd, bc+ad)\mathcal{R}(a'c'+b'd', b'c'+a'd')$.

Par un calcul direct, il résulte immédiatement des propriétés de l'addition et de la multiplication dans $\mathbb{N}$ que la loi $\times$ est associative, commutative et distributive par rapport à l'addition. L'élément $1 = \overline{(1,0)}$ est un élément neutre pour $\times$ puisque $1 \times \overline{(a,b)} = \overline{(1a+0b, 0a+1b)} = \overline{(a,b)}$. $(\mathbb{Z},+,\times)$ *est donc un anneau*. Vérifions qu'il est *intègre*. Soient x et y deux éléments de $\mathbb{Z}$ tels que $xy = 0$. Pour simplifier les calculs choisissons pour x un représentant de la forme $(u,0)$ ou $(0,u)$ et pour y un représentant de la forme $(v,0)$ ou $(0,v)$, alors suivant les cas $xy = 0$ implique

$$(uv,0)\mathcal{R}(0,0) \quad \text{ou} \quad (0,uv)\mathcal{R}(0,0),$$

d'où $uv = 0$ et donc $u = 0$ ou $v = 0$ par les propriétés de la multiplication dans $\mathbb{N}$.

Notons également que tout élément de $\mathbb{Z}$ distinct de 0 est régulier pour $\times$. Soient x, y et $z \neq 0$ dans $\mathbb{Z}$ tels que $xz = yz$. Comme précédemment choisissons pour x un représentant de la forme $(u,0)$ ou $(0,u)$, pour y un représentant de la forme $(v,0)$ ou $(0,v)$ et pour z un représentant de la forme $(w,0)$ ou $(0,w)$ avec $w \neq 0$, alors $xz = \overline{(uw,0)}$ ou $\overline{(0,uw)}$ et $yz = \overline{(vw,0)}$ ou $\overline{(0,vw)}$. L'égalité $xz = yz$ implique donc soit $uw = vw$ si x et y sont de même signe, soit $uw + vw = 0$ si x et y sont de signes contraires et puisque $w \neq 0$, on obtient $u = v$ dans le premier cas et $u = v = 0$ dans le second cas, et donc $x = y$.

Si x et y sont dans $\mathbb{N}$, on identifie x avec $\overline{(x,0)}$ et y avec $\overline{(y,0)}$, alors

$$x \times y = \overline{(xy,0)} = xy\ ,$$

après identification. La loi $\times$ prolonge donc la multiplication sur $\mathbb{N}$. Par ailleurs, notons que

$$x \times (-y) = \overline{(x,0)} \times \overline{(0,y)} = \overline{(0,xy)} = -(xy),$$

de même $(-x) \times y = -(xy)$ et

$$(-x) \times (-y) = \overline{(0,x)} \times \overline{(0,y)} = \overline{(xy,0)} = xy.$$

Nous retrouvons ainsi la règle usuelle des signes : le produit de deux entiers positifs ou de deux entiers négatifs est toujours un entier positif et le produit d'un entier positif et d'un entier négatif est toujours un entier négatif. Cette règle s'exprime également de la manière suivante : le produit de deux entiers de même signe est toujours un entier positif et le produit de deux entiers de signes contraires est toujours un entier négatif.

Remarquons également que $-x = (-1) \times x = x \times (-1)$.

1.4 Construction des rationnels

Il reste dans $\mathbb{Z}$ des équations sans solution, comme $a = b \times x$ pour $b \neq 0$, dont la solution en x devrait être le produit de a par un inverse de b pour la multiplication. Or dans $\mathbb{Z} \setminus \{0\}$ seuls $+1$ et -1 ont un inverse. L'idée est alors de reproduire pour la multiplication dans $\mathbb{Z} \setminus \{0\}$ la procédure utilisée pour l'addition dans $\mathbb{N}$ afin de construire un groupe multiplicatif $\mathbb{Q}^*$ contenant $\mathbb{Z} \setminus \{0\}$. La structure d'anneau de $\mathbb{Z}$ sera alors prolongée à ce nouvel ensemble, faisant de $(\mathbb{Q}, +, \times)$ un corps.

Dans l'ensemble $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ la loi de composition interne $\times$ possède les mêmes propriétés que l'addition dans $\mathbb{N}$, on peut donc appliquer la même procédure que dans la section 1.3 pour construire un nouvel ensemble de nombres noté $\mathbb{Q}$ contenant $\mathbb{Z}$ et tel que $\mathbb{Q} \setminus \{0\}$ possède une structure de groupe multiplicatif.

Considérons sur $\mathbb{Z}^* \times \mathbb{Z}^*$, la relation $\mathcal{R}$ définie par

$$(a,b)\mathcal{R}(a',b') \iff a \times b' = a' \times b. \tag{7}$$

C'est une relation d'équivalence compatible avec la multiplication sur $\mathbb{Z}^* \times \mathbb{Z}^*$. La démonstration de cette assertion est analogue à celle de la Proposition 11 .

On notera $\frac{a}{b}$ la classe du couple (a,b) pour la relation $\mathcal{R}$. On remarquera que pour tout $c \in \mathbb{Z}^*$, on a $\frac{a}{b} = \frac{a \times c}{b \times c}$.

Proposition 15. *L'ensemble quotient $\mathbb{Z}^* \times \mathbb{Z}^*/\mathcal{R}$ munit de la loi quotient déduite de la multiplication sur $\mathbb{Z}^* \times \mathbb{Z}^*$, notée encore $\times$, est un groupe abélien, on le note $\mathbb{Q}^*$.*

L'élément neutre ce groupe est la classe du couple $(1,1)$. Un élément (a,b) de $\mathbb{Z}^* \times \mathbb{Z}^*/\mathcal{R}$ appartient à $\frac{1}{1}$ si et seulement si $a \times 1 = 1 \times b$, c'est-à-dire $a = b$. L'inverse de $\frac{a}{b}$ est $\frac{b}{a}$.

La démonstration de la proposition est analogue à celle de la Proposition 12.

Proposition 16. *On définit un morphisme injectif $f : \mathbb{Z}^* \to \mathbb{Q}^*$ en posant $f(a) = \frac{a}{1}$*

Démonstration : Vérifions que l'application $f : \mathbb{Z}^* \to \mathbb{Q}^*$ définie par $f(a) = \frac{a}{1}$ est multiplicative. Soient a et b dans $\mathbb{Z}^*$, alors

$$f(a \times b) = \frac{a \times b}{1} = \frac{a}{1} \times \frac{b}{1} = f(a) \times f(b)$$

par définition de la multiplication dans $\mathbb{Q}^*$. Montrons maintenant que f est injective. Soient a et b dans $\mathbb{Z}^*$ tels que $f(a) = f(b)$, c'est-à-dire $\frac{a}{1} = \frac{b}{1}$. Par définition de la relation $\mathcal{R}$ cela signifie que $a \times 1 = b \times 1$, soit $a = b$, d'où l'injectivité de l'application f. □

Pour simplifier les écritures, on notera a à la place de $\frac{a}{1}$ l'élément $f(a)$ si $a \in \mathbb{Z}^*$. On écrira souvent ab à la place de $a \times b$ pour le produit de deux éléments de $\mathbb{Z}^*$.

En raison de la structure de groupe multiplicatif de $\mathbb{Q}^*$, si $a \in \mathbb{Z}^*$ et $b \in \mathbb{Z}^*$, l'équation $a = b \times x$ possède toujours une unique solution : l'élément $\frac{a}{b}$ de $\mathbb{Q}^*$. De plus si $a = 0$ et $b \in \mathbb{Z}^*$, l'élément 0 de $\mathbb{Z}$ est l'unique solution de $a = b \times x$, car $\mathbb{Z}$ est un anneau intègre.

Définition 6. *On appelle* ensemble des nombres rationnels *l'ensemble* $\mathbb{Q}^*$ *auquel on a ajouté l'élément* 0 *de* $\mathbb{Z}$*. On le note* $\mathbb{Q}$*.*

Pour compléter la structure algébrique de $\mathbb{Q}$ nous allons prolonger à $\mathbb{Q}$ la structure de groupe additif de $\mathbb{Z}$. Soient $x = \frac{a}{b}$ et $y = \frac{c}{d}$ deux éléments de $\mathbb{Q}$, on pose

$$x + y = \frac{ad + bc}{bd}.$$

Vérifions que cette définition a bien un sens en remarquant qu'elle est indépendante des représentants choisis. Nous devons prouver que si $(a, b)\mathcal{R}(a', b')$ et $(c, d)\mathcal{R}(c', d')$ alors $(ad + bc, bd)\mathcal{R}(a'd' + b'c', b'd')$. Supposons que $ab' = a'b$ et $cd' = c'd$, alors

$$\begin{aligned}(ad + bc)b'd' &= (ab')dd' + (cd')bb' \\ &= (a'b)dd' + (c'd)bb' \\ &= (a'd' + c'd')bd,\end{aligned}$$

c'est-à-dire $(ad + bc, bd)\mathcal{R}(a'd' + b'c', b'd')$.

Par un calcul direct, il résulte immédiatement des propriétés de l'addition et de la multiplication dans $\mathbb{Z}$ que l'addition est associative, commutative et que la multiplication est distributive par rapport à l'addition. Notons que $0 = \frac{0}{1}$ vérifie :

$$\frac{a}{b} + 0 = 0 + \frac{a}{b} = \frac{a \times 1 + 0 \times b}{b \times 1} = \frac{a}{b}\ ,$$

c'est donc un élément neutre pour l'addition. De plus si $x = \frac{a}{b}$, posons $-x = \frac{-a}{b} = (-1) \times x$, alors

$$x + (-x) = \frac{ab + (-a)b}{bb} = \frac{ab - ab}{bb} = \frac{0}{bb} = 0\ .$$

Tout élément x de $\mathbb{Q}$ possède un inverse pour l'addition et $(\mathbb{Q}, +)$ est donc un groupe abélien.

L'ensemble $\mathbb{Q}$ ainsi construit muni des lois $+$ et $\times$ possède une structure de corps.

Si x et y sont dans $\mathbb{Z}$, on identifie x avec $\frac{x}{1}$ et y avec $\frac{y}{1}$, alors

$$x + y = \frac{x \times 1 + 1 \times y}{1 \times 1} = \frac{x + y}{1} ,$$

après identification. La loi $+$ prolonge donc l'addition sur $\mathbb{Z}$ et $(\mathbb{Z}, +, \times)$ est un sous anneau de $\mathbb{Q}$.

Proposition 17. *L'ensemble $\mathbb{Q}$ est dénombrable.*

Démonstration : L'ensemble $\mathbb{Q}$ s'injecte dans le produit cartésien $\mathbb{Z} \times \mathbb{N}$ et contient $\mathbb{N}$. Il suffit donc de prouver que $\mathbb{Z} \times \mathbb{N}$ est dénombrable, mais comme $\mathbb{Z}$ est dénombrable on est ramené à prouver que $\mathbb{N} \times \mathbb{N}$ est dénombrable. L'application $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ définie par

$$f(p, q) = q + \sum_{i=0}^{p+q} i = \frac{(p + q)(p + q + 1)}{2} + q ,$$

qui consiste à compter diagonalement les couples (p, q) donne la bijection cherchée. □

Relation d'ordre dans $\mathbb{Q}$

Pour terminer nous allons étendre à $\mathbb{Q}$ la relation d'ordre de $\mathbb{Z}$. Rappelons que si x et y sont deux éléments de $\mathbb{Z}$ alors $x \leqslant y$ si et seulement si $y - x \in \mathbb{N}$ soit $0 \leqslant y - x$. Pour commencer nous allons définir la notion de *nombre rationnel positif*. Si $\frac{a}{b} \in \mathbb{Q}$, nous dirons que $0 \leqslant \frac{a}{b}$ si et seulement si $0 \leqslant a \times b$. Cette définition ne dépend pas du représentant choisi. En effet si $\frac{a}{b} = \frac{a'}{b'}$, c'est-à-dire si $a \times b' = a' \times b$, alors $(a \times b) \times (b' \times b') = (a' \times b') \times (b \times b)$ et puisque $b \times b$ et $b' \times b'$ sont tous deux positifs et non nuls comme produits de nombres entiers de même signe, $a \times b$ et $a' \times b'$ ont le même signe.

Avec cette définition, les éléments de $\mathbb{Z}$ positifs au sens de $\mathbb{Q}$ sont exactement les éléments positifs de $\mathbb{Z}$, c'est-à-dire les éléments de $\mathbb{N}$. Par analogie avec la relation d'ordre dans $\mathbb{Z}$, si x et y sont deux éléments de $\mathbb{Q}$, nous posons $x \leqslant y$ si et seulement si $0 \leqslant y - x$. Cette relation est une relation d'ordre qui prolonge la relation d'ordre de $\mathbb{Z}$.

La relation d'ordre $\leqslant$ est compatible avec l'addition et la multiplication sur $\mathbb{Q}$ au sens suivant : soient x, y et z trois éléments de $\mathbb{Q}$

• si $x \leqslant y$, alors $x + z \leqslant y + z$ puisque $y - x = (y + z) - (x + z)$,

• si $x \leqslant y$ et $0 \leqslant z$, alors $x \times z \leqslant y \times z$ puisque $(y \times z) - (x \times z) = (y - x) \times z$ et en particulier si $x = 0$ on obtient que, si $0 \leqslant y$ et $0 \leqslant z$, alors $0 \leqslant y \times z$.

On écrira de manière équivalente :

$x \leqslant y$ ou $y \geqslant x$,

$x \leqslant y,\ x \neq y$ ou $x < y$ ou $y > x$.

Dans la suite nous utiliserons la notation suivante : si $x \in \mathbb{Q}$, on pose $|x| = \max(x, -x)$. On a bien sûr $|x| = x$, si $x \geqslant 0$, et $|x| = -x$, si $x \leqslant 0$.

1.5 Construction des réels

Par des arguments d'arithmétique élémentaire, il est facile de prouver qu'il n'existe pas de carré de côté de longueur rationnelle dont l'aire est égale à 2 : l'équation $x^2 = 2$ n'a pas de solution dans $\mathbb{Q}$. Néanmoins, il existe une infinité de *suites de rationnels* $(x_n)_{n\in\mathbb{Q}}$, telles que x_n^2 converge vers 2. C'est le cas par exemple, pour toute suite définie par $x_0 \in \mathbb{Q}^{+*}$ et :

$$\forall n \in \mathbb{N}\,, \quad x_{n+1} = x_n - \frac{x_{n+1}^2 - 2}{2x}\,.$$

(Démontrez-le !) Une conséquence est que la suite $(x_n)_{n\in\mathbb{N}}$ ne converge pas dans $\mathbb{Q}$.

Sans perdre de propriétés algébriques, nous allons construire un nouveau corps $\mathbb{R}$ totalement ordonné contenant $\mathbb{Q}$ et dans lequel toutes les suites qui devraient naturellement converger (ce seront les suites de Cauchy) seront effectivement convergentes.

Définition 7. *Soit $(x_n)_{n\in\mathbb{N}}$ une suite d'éléments de $\mathbb{Q}$, c'est-à-dire une application de $\mathbb{N}$ dans $\mathbb{Q}$.*

(i) La suite $(x_n)_{n\in\mathbb{N}}$ est bornée *s'il existe $M \in \mathbb{Q}$ tel que*

$$(\forall n \in \mathbb{N}) \quad (|x_n| \leqslant M).$$

(ii) La suite $(x_n)_{n\in\mathbb{N}}$ converge dans $\mathbb{Q}$ vers $x \in \mathbb{Q}$ si

$$(\forall \varepsilon > 0, \varepsilon \in \mathbb{Q}) \quad (\exists N_\varepsilon \in \mathbb{N}) \quad (\forall n \in \mathbb{N}) \quad (n > N_\varepsilon \implies |x_n - x| < \varepsilon).$$

(iii) La suite $(x_n)_{n\in\mathbb{N}}$ est de Cauchy dans $\mathbb{Q}$ si

$$(\forall \varepsilon > 0, \varepsilon \in \mathbb{Q}) \quad (\exists N_\varepsilon \in \mathbb{N}) \quad (\forall p, q \in \mathbb{N}) \quad (p > N_\varepsilon,\ q > N_\varepsilon \implies |x_p - x_q| < \varepsilon).$$

Proposition 18.

1. *Toute suite convergente est de Cauchy.*
2. *Toute suite de Cauchy est bornée.*
3. *Si la suite $(x_n)_{n\in\mathbb{N}}$ converge vers 0 et si la suite $(y_n)_{n\in\mathbb{N}}$ est bornée, la suite $(x_n \times y_n)_{n\in\mathbb{N}}$ converge vers 0.*
4. *Si les suites $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ sont de Cauchy, les suites $(x_n + y_n)_{n\in\mathbb{N}}$, $(x_n - y_n)_{n\in\mathbb{N}}$ et $(x_n \times y_n)_{n\in\mathbb{N}}$ sont de Cauchy.*
5. *Si la suite $(x_n)_{n\in\mathbb{N}}$ converge vers a et si la suite $(y_n)_{n\in\mathbb{N}}$ converge vers b, la suite $(x_n + y_n)_{n\in\mathbb{N}}$ converge vers $a + b$, la suite $(x_n - y_n)_{n\in\mathbb{N}}$ converge vers $a - b$ et la suite $(x_n \times y_n)_{n\in\mathbb{N}}$ converge vers $a \times b$.*
6. *Soit $(x_n)_{n\in\mathbb{N}}$ une suite de Cauchy ne convergeant pas vers 0, alors il existe un entier n_0 tel que si $n > n_0$ on a $x_n \neq 0$ et la suite $(\frac{1}{x_n})_{n>n_0}$ est de Cauchy.*

Démonstration :

1. Soit $(x_n)_{n\in\mathbb{N}}$ une suite qui converge dans $\mathbb{Q}$ vers $x \in \mathbb{Q}$, alors pour $\varepsilon > 0$, $\varepsilon \in \mathbb{Q}$, il existe $N_\varepsilon \in \mathbb{N}$ tel que pour tout $n \in \mathbb{N}$

$$n > N_\varepsilon \implies |x_n - x| < \varepsilon.$$

Par conséquent pour $n > N_{\varepsilon/2}$ et $p > N_{\varepsilon/2}$ on a $|x_p - x_n| \leqslant |x_p - x| + |x_n - x| < \varepsilon$ et la suite $(x_n)_{n\in\mathbb{N}}$ est donc de Cauchy dans $\mathbb{Q}$.

2. Soit $(x_n)_{n\in\mathbb{N}}$ une suite de Cauchy dans $\mathbb{Q}$, alors

$$(\forall \varepsilon > 0, \varepsilon \in \mathbb{Q}) \quad (\exists N_\varepsilon \in \mathbb{N}) \quad (\forall p, q \in \mathbb{N}) \quad (p > N_\varepsilon,\ q > N_\varepsilon \implies |x_p - x_q| < \varepsilon).$$

En prenant $\varepsilon = 1$ on obtient que si $n > N_1$ on a $x_{N_1+1} - 1 < x_n < x_{N_1+1} + 1$. Par conséquent si on pose $M = \max(|x_0|, \ldots, |x_{N_1}|, |x_{N_1+1}| + 1)$, pour tout $n \in \mathbb{N}$, $|x_n| \leqslant M$ et la suite $(x_n)_{n\in\mathbb{N}}$ est bornée.

3. Soit $(x_n)_{n\in\mathbb{N}}$ une suite qui converge dans $\mathbb{Q}$ vers 0 et $(y_n)_{n\in\mathbb{N}}$ une suite bornée, alors pour $\varepsilon > 0$, $\varepsilon \in \mathbb{Q}$, il existe $N_\varepsilon \in \mathbb{N}$ tel que pour tout $n \in \mathbb{N}$

$$n > N_\varepsilon \implies |x_n| < \varepsilon,$$

et il existe $M > 0$, $M \in \mathbb{Q}$, tel que pour tout $n \in \mathbb{N}$

$$|y_n| \leqslant M.$$

On en déduit que si $n > N_{\varepsilon/M}$ alors

$$|x_n \times y_n| \leqslant M \times |x_n| < M \times \frac{\varepsilon}{M} = \varepsilon.$$

Les assertions 4) et 5) pour les sommes et les différences de suites sont des conséquences immédiates de l'inégalité triangulaire et des définitions et leur démonstration est laissée au lecteur. Prouvons 4) pour le produit, la démonstration de 5) pour le produit est analogue. Soient $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ deux suites de Cauchy, alors pour $\varepsilon > 0$, $\varepsilon \in \mathbb{Q}$, il existe $N_\varepsilon \in \mathbb{N}$ et $N'_\varepsilon \in \mathbb{N}$ tels que pour tout $p, q \in \mathbb{N}$

$$p > N_\varepsilon,\ q > N_\varepsilon \implies |x_p - x_q| < \varepsilon \quad \text{et} \quad p > N'_\varepsilon,\ q > N'_\varepsilon \implies |y_p - y_q| < \varepsilon.$$

De plus, d'après 2), il existe $M, M' > 0$, $M, M' \in \mathbb{Q}$, tels que pour tout $n \in \mathbb{N}$

$$|y_n| \leqslant M \quad \text{et} \quad |y_n| \leqslant M.$$

On en déduit que, pour tout $p, q \in \mathbb{N}$,

$$|x_p \times y_p - x_q \times y_q| = |(x_p - x_q) \times y_p + x_q \times (y_p - y_q)| \leqslant M'|x_p - x_q| + M|y_p - y_q|.$$

Posons $N = \max(N_{\varepsilon/2M'}, N'_{\varepsilon/2M})$, alors si $p > N$ et $q > N$ on a

$$|x_p \times y_p - x_q \times y_q| < M' \times \frac{\varepsilon}{2M'} + M \times \frac{\varepsilon}{2M} = \varepsilon.$$

6. Soit $(x_n)_{n\in\mathbb{N}}$ une suite de Cauchy ne convergeant pas vers 0, alors

$$(\exists\alpha>0,\alpha\in\mathbb{Q})\quad(\forall N\in\mathbb{N})\quad(\exists n\in\mathbb{N})\quad(n>N \text{ et } |x_n|\geqslant\alpha).$$

La suite $(x_n)_{n\in\mathbb{N}}$ étant de Cauchy, il existe $n_0\in\mathbb{N}$ tel que

$$p>n_0,\ q>n_0 \implies |x_p-x_q|<\frac{\alpha}{2}.$$

En prenant $N=n_0$, $n=p$ alors pour tout $q>n_0$ on a

$$|x_n-x_q|<\frac{\alpha}{2}\quad\text{et}\quad|x_n|\geqslant\alpha,$$

soit $|x_q|>\frac{\alpha}{2}$ grâce à l'inégalité triangulaire, d'où $x_q\neq 0$ si $q>n_0$. Soient $p,q>n_0$, alors $|x_p|>\frac{\alpha}{2}$ et $|x_q|>\frac{\alpha}{2}$, d'où

$$\left|\frac{1}{x_p}-\frac{1}{x_q}\right|<\frac{4}{\alpha^2}|x_p-x_q|.$$

Donc puisque $(x_n)_{n\in\mathbb{N}}$ est une suite de Cauchy, la suite $(\frac{1}{x_n})_{n>n_0}$ est de Cauchy.

□

Dans $\mathbb{Q}$, il existe des suites de Cauchy non convergentes. Nous en avons vu des exemples plus haut. En voici un autre. Considérons la suite $(x_n)_{n\in\mathbb{N}^*}$ définie par

$$x_n=1+\frac{1}{1!}+\cdots+\frac{1}{n!}.$$

Si $p>q$, on a

$$\begin{aligned}x_p-x_q&=\frac{1}{(q+1)!}+\cdots+\frac{1}{p!}\\&\leqslant\frac{1}{(q+1)!}(1+\frac{1}{q+1}+\cdots+\frac{1}{(q+1)^{p-q-1}})\\&\leqslant\frac{1}{(q+1)!}\frac{1}{1-\frac{1}{q+1}}=\frac{1}{q\ q!}.\end{aligned}$$

Pour $\varepsilon=\frac{a}{b}$, $a,b\in\mathbb{N}^*$, $p>b$ et $q>b$ implique

$$|x_p-x_q|<\frac{1}{b\ b!}\leqslant\varepsilon.$$

Cette suite est donc de Cauchy, mais ne converge pas vers un nombre rationnel $\frac{a}{b}$. Supposons qu'elle converge vers $\frac{a}{b}$. Puisque l'inégalité

$$0<x_p-x_q<\frac{1}{q\ q!}$$

est valable pour tout $p > q$, en faisant tendre p vers l'infini on aurait

$$0 < \frac{a}{b} - x_q < \frac{1}{q\ q!},$$

la première inégalité restant stricte puisque la suite $(x_n)_{n\in\mathbb{N}^*}$ est croissante. Par définition de x_q, si $q \leqslant b$, le nombre rationnel $\frac{a}{b} - x_q$ peut être représenté par une fraction de la forme $\frac{\alpha}{q!}$, $\alpha \in \mathbb{Z}$, et donc $0 < \alpha \leqslant \frac{1}{q}$, ce qui est impossible si $q > 1$.

On peut également considérer la suite $(y_n)_{n\in\mathbb{N}^*}$ définie par

$$y_n = 1 + \frac{1}{1!} + \cdots + \frac{1}{n!} + \frac{1}{n!}.$$

La suite $(x_n)_{n\in\mathbb{N}^*}$ est clairement croissante et la suite $(y_n)_{n\in\mathbb{N}^*}$ est décroissante puisque

$$y_{n+1} - y_n = \frac{1}{(n+1)!} + \frac{1}{(n+1)!} - \frac{1}{n!} = \frac{1-n}{(n+1)!} \leqslant 0.$$

De plus la suite $(y_n - x_n = \frac{1}{n!})_{n\in\mathbb{N}^*}$ est une suite de rationnels positifs qui converge vers 0 et pour tous $p, q \in \mathbb{N}^*$ on a $x_p \leqslant y_q$. Par conséquent si ces suites convergeaient leurs limites seraient égales et cette limite l vérifierait $x_p \leqslant l \leqslant y_q$ pour tous $p, q \in \mathbb{N}^*$.

On aimerait alors compléter $\mathbb{Q}$ en un nouvel ensemble ordonné de nombres dans lequel toute suite de Cauchy serait convergente. Les deux suites $(x_n)_{n\in\mathbb{N}^*}$ et $(y_n)_{n\in\mathbb{N}^*}$ précédentes auraient alors une limite commune dans cet ensemble qui serait située entre chacun des nombres rationnels x_n et y_n. Nous allons construire un tel ensemble.

Précisons tout d'abord les propriétés souhaitées pour le nouvel ensemble de nombres que nous souhaitons construire.

Définition 8.

1. *Un corps K est dit* totalement ordonné *s'il est muni d'une relation d'ordre totale notée $\leqslant$ telle que*

$$(\forall x, y, z \in K) \quad (x \leqslant y \implies x + z \leqslant y + z), \tag{8}$$

$$(\forall x, y \in K) \quad (x \geqslant 0 \text{ et } y \geqslant 0 \implies xy \geqslant 0). \tag{9}$$

2. *Un corps K est dit* archimédien *s'il est totalement ordonné et si pour tous $x, y \in K$ tel que $x > 0$, il existe $n \in \mathbb{N}$ tel que $nx > y$.*
3. *Un corps K totalement ordonné est dit* complet *si toute suite de Cauchy dans K est convergente.*

Nous allons construire un corps commutatif noté $\mathbb{R}$ contenant $\mathbb{Q}$ et qui sera archimédien et complet comme quotient de l'ensemble des suites de Cauchy de $\mathbb{Q}$.

Notons $\mathbb{Q}^{\mathbb{N}}$ l'ensemble des suites de rationnels, c'est-à-dire l'ensemble des applications de $\mathbb{N}$ dans $\mathbb{Q}$, et $\mathcal{C}$ le sous-ensemble de $\mathbb{Q}^{\mathbb{N}}$ constitué des suites de Cauchy.

Grâce à la propriété 4) des suites de rationnels l'ensemble $\mathcal{C}$ des suites de Cauchy dans $\mathbb{Q}$ est muni d'une structure d'anneau commutatif si on pose pour $x = (x_n)_{n\in\mathbb{N}}$ et $y = (y_n)_{n\in\mathbb{N}}$

$$x + y = (x_n + y_n)_{n\in\mathbb{N}}$$
$$x \times y = xy = (x_n y_n)_{n\in\mathbb{N}}.$$

l'élément neutre de + est (0), la suite stationnaire nulle et l'élément neutre de $\times$ est (1) la suite stationnaire d'éléments égaux à 1.

Proposition 19. *L'ensemble $\mathcal{C}_0$ des suites de rationnels qui convergent vers* 0 *est un idéal de $\mathcal{C}$.*

Démonstration : Le fait que $\mathcal{C}_0$ soit un sous-groupe additif de $\mathcal{C}$ est une conséquence directe des propriétés 1) et 5) des suites de rationnels. Pour prouver que $\mathcal{C}_0$ est un idéal de $\mathcal{C}$, il reste à montrer que si $x = (x_n)_{n\in\mathbb{N}}$ est un élément de $\mathcal{C}_0$ et si $y = (y_n)_{n\in\mathbb{N}}$ est une suite Cauchy de rationnels alors $xy \in \mathcal{C}_0$. Cela résulte immédiatement des propriétés 2) et 3) des suites de rationnels. □

Définition 9. *L'anneau quotient $\mathcal{C}/\mathcal{C}_0$ est appelé* droite numérique *et noté $\mathbb{R}$. Ses éléments sont appelés* nombres réels.

Proposition 20. *$\mathbb{R}$ est un corps commutatif.*

Démonstration : $\mathbb{R}$ est un anneau commutatif qui admet pour unité la classe $\overline{u}$ des suites qui convergent vers 1. Il reste à prouver que si une suite de Cauchy $x = (x_n)_{n\in\mathbb{N}}$ ne converge pas vers 0, il existe une suite de Cauchy $y = (y_n)_{n\in\mathbb{N}}$ telle que xy converge vers 1. Par la propriété 6) des suites de rationnels, si x ne converge pas vers 0 il existe un entier n_0 tel que la suite $(\frac{1}{x_n})_{n>n_0}$ est de Cauchy. Posons $y_n = 0$ si $n \leqslant n_0$ et $y_n = \frac{1}{x_n}$ si $n > n_0$, la suite $y = (y_n)_{n\in\mathbb{N}}$ ainsi construite est telle que la suite xy converge vers 1. Ainsi on a

$$\overline{x}\ \overline{y} = \overline{xy} = \overline{u},$$

ce qui prouve, puisque $\overline{x} \neq 0$ si et seulement si $x \notin \mathcal{C}_0$, que tout élément non nul de $\mathbb{R}$ possède un inverse dans $\mathbb{R}$. □

Proposition 21. *On définit un isomorphisme φ de $\mathbb{Q}$ sur un sous-corps de $\mathbb{R}$ en associant à chaque rationnel q la classe $\overline{q}$ constituée des suites de rationnels qui convergent vers q.*

Démonstration : Il résulte immédiatement de la propriété 4) des suites de rationnels que φ est un homomorphisme d'anneau. De plus puisque $\overline{0} = \mathcal{C}_0$, $\ker\varphi = \{0\}$ et φ est donc injectif. Il définit donc un isomorphisme de $\mathbb{Q}$ sur un sous-corps de $\mathbb{R}$. □

Relation d'ordre dans $\mathbb{R}$

Soit $x \in \mathcal{C}$ une suite de Cauchy de rationnels, on dira que $x \in \mathcal{C}^+$ si et seulement si

$$(\forall \varepsilon > 0,\ \varepsilon \in \mathbb{Q}) \quad (\exists N_\varepsilon) \quad (n > N_\varepsilon \implies x_n > -\varepsilon)$$

et que $x \in \mathcal{C}^-$ si et seulement si

$$(\forall \varepsilon > 0,\ \varepsilon \in \mathbb{Q}) \quad (\exists N_\varepsilon) \quad (n > N_\varepsilon \implies x_n < \varepsilon).$$

Lemme 2. *On a*

$$\mathcal{C}^+ \cap \mathcal{C}^- = \mathcal{C}_0 \quad \text{et} \quad \mathcal{C}^+ \cup \mathcal{C}^- = \mathcal{C}.$$

Démonstration : Soient $x \in \mathcal{C}^+ \cap \mathcal{C}^-$, pour ε donné il existe N_ε et N'_ε tels que si $n > N_\varepsilon$ et $n > N'_\varepsilon$ on ait respectivement $x_n > -\varepsilon$ et $x_n < \varepsilon$, d'où si $n > \max(N_\varepsilon, N'_\varepsilon)$ on aura $|x_n| < \varepsilon$, c'est-à-dire $x \in \mathcal{C}_0$.

Soit $x \in \mathcal{C}$, alors $x \notin \mathcal{C}^-$ équivaut à

$$(\exists \alpha > 0,\ \alpha \in \mathbb{Q}) \quad (\forall n \in \mathbb{N}) \quad (\exists p \in \mathbb{N}) \quad (p > n \text{ et } x_p \geqslant \alpha).$$

Puisque x est une suite de Cauchy, il existe n_0 tel que si $n > n_0$ et $p > n_0$ on a $|x_n - x_p| < \frac{\alpha}{2}$. Choisissons $p > n_0$ tel que $x_p \geqslant \alpha$, alors pour tout $n > n_0$ on a $x_n > \frac{\alpha}{2} > 0$ et donc $x \in \mathcal{C}^+$. □

Lemme 3. *Les assertions suivantes sont satisfaites :*

(i) $x \in \mathcal{C}^- \ \Leftrightarrow\ (-x) \in \mathcal{C}^+$ *;*

(ii) $x \in \mathcal{C}^+$ et $y \in \mathcal{C}^+ \implies x + y \in \mathcal{C}^+$ *;*

(iii) $x \in \mathcal{C}^+$ et $y \in \mathcal{C}^+ \implies xy \in \mathcal{C}^+$ *;*

(iv) Si $x, x' \in \mathcal{C}$ *vérifient* $x - x' \in \mathcal{C}_0$*, alors* x *et* x' *appartiennent toutes deux à* $\mathcal{C}^+$ *ou à* $\mathcal{C}^-$*.*

Démonstration : Les assertions (i) et (ii) sont des conséquences directes de la définition de $\mathcal{C}^+$. Considérons l'assertion (iii) : si parmi x et y l'un est dans $\mathcal{C}_0$, alors $xy \in \mathcal{C}_0$ par les propriétés 2) et 3) des suites de rationnels et si x et y ne sont pas dans $\mathcal{C}^-$, pour n assez grand on a $x_n > 0$ et $y_n > 0$ et donc $x_n y_n > 0$, soit $xy \in \mathcal{C}^+$, ce qui prouve (iii).

Pour l'assertion (iv) considérons le cas où $x \in \mathcal{C}^+$, le cas où $x \in \mathcal{C}^-$ se traite de manière analogue. Si $x \in \mathcal{C}^+$ et si $\varepsilon > 0$, $\varepsilon \in \mathbb{Q}$ est donné, il existe n_1 tel que $x_n > -\frac{\varepsilon}{2}$ si $n > n_1$. Comme $x - x' \in \mathcal{C}_0$, il existe n_2 tel que si $n > n_2$ alors $|x_n - x'_n| < \frac{\varepsilon}{2}$. Ainsi pour $n > \max(n_1, n_2)$ on a $x'_n > x_n - \frac{\varepsilon}{2} > -\varepsilon$, c'est-à-dire $x' \in \mathcal{C}^+$. □

L'assertion (iv) du Lemme 3 permet de donner la définition suivante :

Définition 10. *Un nombre réel est dit* positif *(resp.* négatif*) s'il est représenté par une suite de Cauchy appartenant à* $\mathcal{C}^+$ *(resp.* $\mathcal{C}^-$*).*

On note $\mathbb{R}^+ = \mathcal{C}^+/\mathcal{C}_0$ *et* $\mathbb{R}^- = \mathcal{C}^-/\mathcal{C}_0$*.*

Les Lemmes 2 et 3 permettent de définir une relation d'ordre sur $\mathbb{R}$ en posant $a \leqslant b$ si et seulement si $b-a \in \mathbb{R}^+$. Grâce aux propriétés (i), (ii) et (iii) du Lemme 3, $(\mathbb{R}, \leqslant)$ *est un corps totalement ordonné.* Notons que l'injection φ de $\mathbb{Q}$ dans $\mathbb{R}$ est croissante, puisque $q \geqslant 0$ dans $\mathbb{Q}$ équivaut à $\varphi(q) \in \mathbb{R}^+$.

Théorème 4. $\mathbb{R}$ *est un corps archimédien.*

Démonstration : Il suffit de prouver que pour tout $a \in \mathbb{R}$, il existe $p \in \mathbb{N}$ tel que $p > a$ (si $x, y \in \mathbb{R}$ avec $x > 0$, en posant $a = \frac{y}{x}$ on aura $px > y$). Soit $a = \overline{(a_n)_{n\in\mathbb{N}}}$. La suite $(a_n)_{n\in\mathbb{N}}$ étant de Cauchy, elle est bornée et par conséquent il existe $M = \frac{m}{q} \in \mathbb{Q}$ tel que $|a_n| \leqslant M$ pour tout $n \in \mathbb{N}$. La suite $(M - a_n)_{n\in\mathbb{N}}$ est constituée de rationnels positifs, elle est donc dans $\mathcal{C}^+$, ce qui signifie que le nombre réel M-a est positif. On a donc $\frac{m}{q} \geqslant a$, d'où $m \geqslant a$ et $p = m + 1$ convient. □

Notion de suite de Cauchy et de suite convergente dans $\mathbb{R}$

Les définitions sont analogues à celles des suites de Cauchy et des suites convergentes dans $\mathbb{Q}$, mais cette fois on autorise ε à appartenir à $\mathbb{R}$. Comme $\mathbb{R}$ est archimédien cela n'apporte rien car si $\varepsilon > 0$ est un nombre réel, il existe $\varepsilon_1 \in \mathbb{Q}$ tel que $0 < \varepsilon_1 < \varepsilon$ (il suffit de poser $\varepsilon_1 = \frac{1}{p}$, avec $p\ \varepsilon > 1$).

Pour prouver que $\mathbb{R}$ est complet nous avons besoin de quelques lemmes qui ont un intérêt intrinsèque.

Lemme 4. *Si x et y sont deux éléments de $\mathbb{R}$ tels que $x < y$, il existe $r \in \mathbb{Q}$ tel que $x < r < y$.*

Démonstration : Puisque $\mathbb{R}$ est archimédien, il existe $q \in \mathbb{N}$ tel que $q(y - x) > 1$. Soit $E = \{n \in \mathbb{Z} \mid \frac{n}{q} \leqslant x\}$. Comme $\mathbb{R}$ est archimédien et $\frac{1}{q} > 0$, il existe $n_0 \in \mathbb{N}$ tel que $\frac{n_0}{q} \geqslant |x|$, par conséquent l'ensemble E n'est pas vide car il contient $-n_0$ et il est majoré par n_0 ; il possède donc un plus grand élément p qui vérifie

$$\frac{p}{q} \leqslant x < \frac{p+1}{q}.$$

Posons $r = \frac{p+1}{q}$, alors $x < r < x + \frac{1}{q} < y$ par définition de q. □

Lemme 5. *Toute suite de Cauchy de rationnels converge dans $\mathbb{R}$ vers le nombre réel qu'elle représente.*

Démonstration : Soit $x = (x_n)_{n\in\mathbb{N}}$ une suite de Cauchy dans $\mathbb{Q}$. Choisissons $\varepsilon > 0$, $\varepsilon \in \mathbb{Q}$, il existe alors N_ε tel que si $p > N_\varepsilon$ et $q > N_\varepsilon$ on a $|x_p - x_q| < \varepsilon$, c'est-à-dire

$$x_p - \varepsilon < x_q < x_p + \varepsilon.$$

Fixons $p > N_\varepsilon$, par définition de la relation d'ordre sur $\mathbb{R}$ on obtient

$$x_p - \varepsilon \leqslant \overline{x} \leqslant x_p + \varepsilon,$$

ce qui implique que la suite $(x_n)_{n\in\mathbb{N}}$ converge vers $\overline{x}$ dans $\mathbb{R}$. □

Théorème 5. $\mathbb{R}$ *est complet.*

Démonstration : Soit $(x_n)_{n\in\mathbb{N}}$ une suite de Cauchy dans $\mathbb{R}$. Nous allons construire une suite $y = (y_n)_{n\in\mathbb{N}}$ de rationnels assez « proche » de la suite $(x_n)_{n\in\mathbb{N}}$ pour qu'elle soit encore de Cauchy et nous montrerons que la suite $(x_n)_{n\in\mathbb{N}}$ converge vers $\overline{y}$ dans $\mathbb{R}$.

Construction de la suite $(y_n)_{n\in\mathbb{N}}$

Pour tout $n \in \mathbb{N}^*$, il résulte du Lemme 4 qu'il existe $y_n \in \mathbb{Q}$ tel que

$$x_n - \frac{1}{n} < y_n < x_n + \frac{1}{n}.$$

Pour $\varepsilon > 0$, $\varepsilon \in \mathbb{Q}$ donné, il existe n_ε tel que si $p > n_\varepsilon$ et $q > n_\varepsilon$ on a $|x_p - x_q| < \frac{\varepsilon}{3}$ et donc

$$\begin{aligned} |y_p - y_q| &< |y_p - x_p| + |x_p - x_q| + |x_q - y_q| \\ &< \frac{1}{p} + \frac{1}{q} + |x_p - x_q| \\ &< \frac{1}{p} + \frac{1}{q} + \frac{3}{\varepsilon}. \end{aligned}$$

Posons $m_\varepsilon = \max(n_\varepsilon, \frac{3}{\varepsilon})$, alors si $p > m_\varepsilon$ et $q > m_\varepsilon$ on a $|y_p - y_q| < \varepsilon$. La suite $(y_n)_{n\in\mathbb{N}}$ est donc de Cauchy dans $\mathbb{Q}$.

Convergence de la suite $(x_n)_{n\in\mathbb{N}}$

Il résulte de la démonstration du Lemme 5 que $|\overline{y} - y_p| < \varepsilon$ si $p > m_\varepsilon$, d'où

$$|\overline{y} - x_p| < \varepsilon + \frac{1}{p} < \frac{4\varepsilon}{3}$$

et la suite $(x_n)_{n\in\mathbb{N}}$ converge donc vers $\overline{y}$. □

Représentation décimale d'un nombre réel

L'objet de ce paragraphe est de prouver que, pour tout $x \in \mathbb{R}$, il existe une unique suite $(x_n)_{n\in\mathbb{N}}$ d'éléments de $\mathbb{Z}$ tels que, pour tout $n \in \mathbb{N}^*$, $0 \leqslant x_n \leqslant 9$ et pour tout $N \in \mathbb{N}$ il existe $n \geqslant N$ tel que $x_n \neq 9$ et $x = \lim_{n\to\infty} \sum_{k=0}^{n} x_k \; 10^{-k}$. La suite $(x_n)_{n\in\mathbb{N}}$ est unique. La suite $(x_n)_{n\in\mathbb{N}}$ s'appelle un *développement décimal propre* de x et il est d'usage de le noter

$$x_0, x_1 x_2 \dots x_n \dots$$

Lemme 6. *Pour tout $\varepsilon > 0$ et tout $x \in \mathbb{R}$, il existe un unique entier $p \in \mathbb{Z}$ tel que*

$$p\varepsilon \leqslant x < (p+1)\varepsilon.$$

Démonstration : Comme $\mathbb{R}$ est archimédien, il existe $n \in \mathbb{N}$ tel que $n\varepsilon \geqslant |x|$, i.e. $-n\varepsilon \leqslant x \leqslant n\varepsilon$, donc l'ensemble P des entiers relatifs tels que $p\varepsilon \leqslant x$ est non vide ($-n \in P$) et majoré par n, il admet donc un plus grand élément p qui vérifie bien sûr

$$p\varepsilon \leqslant x < (p+1)\varepsilon.$$

Si p' vérifiait également $p'\varepsilon \leqslant x < (p'+1)\varepsilon$, on aurait $p'\varepsilon < (p+1)\varepsilon$ et $p\varepsilon < (p'+1)\varepsilon$, d'où $p' < p+1$ et $p < p'+1$ puisque $\varepsilon \neq 0$, soit $p = p'$. □

Lorsque $\varepsilon = 1$, l'entier p du Lemme 6 s'appelle la *partie entière* de x et est habituellement noté $\lfloor x \rfloor$. On appelle *partie décimale* de x la différence $x - \lfloor x \rfloor$. On la note $D(x)$, elle appartient à l'intervalle $[0, 1[$.

Soit $d \in \mathbb{N}$, $d \geqslant 2$, prenons $\varepsilon = d^{-n}$. Si $x \in \mathbb{R}$, d'après le Lemme 6, il existe un unique $p_n \in \mathbb{Z}$ tel que

$$p_n d^{-n} \leqslant x < (p_n + 1)d^{-n}.$$

Le nombre rationnel $\zeta_n = p_n d^{-n}$ s'appelle la *valeur approchée par défaut de x à d^{-n} près*.

En remplaçant n par $n+1$, on obtient p_{n+1} qui vérifie

$$p_n d^{-n} < (p_{n+1} + 1)d^{-n-1} \quad \text{et} \quad p_{n+1} d^{-n-1} < (p_n + 1)d^{-n},$$

d'où $dp_n \leqslant p_{n+1} < d(p_n + 1)$. On peut alors définir par récurrence une unique suite $(x_n)_{n\in\mathbb{N}}$ telle que $x_0 = p_0 \in \mathbb{Z}$ et $p_n = \sum_{k=0}^{n} x_k d^{n-k}$ avec $0 \leqslant x_k \leqslant d-1$ si $k \geqslant 1$. La valeur approchée par défaut de x à d^{-n} près est alors donnée par

$$\zeta_n = \sum_{k=0}^{n} x_k d^{-k}.$$

Remarquons que, puisque $d \geqslant 2$, $d^n \geqslant 1 + n(d-1) \geqslant 1 + n$ par la formule du binôme de Newton donc $\lim_{n\to\infty} d^{-n} = 0$. La suite $(\zeta_n)_{n\in\mathbb{N}}$ des valeurs approchées vérifie $|x - \zeta_n| < d^{-n}$ et converge donc vers x quand n tend vers l'infini.

Lorsque $d = 10$ la suite $(x_n)_{n\in\mathbb{N}}$ s'appelle un *développement décimal illimité* de x et on écrit

$$\zeta_n = x_0, x_1 \dots x_n.$$

On dira que le développement décimal est *propre* si, pour tout $N \in \mathbb{N}$, il existe $n \geqslant N$ tel que $x_n \neq 9$. Les développements obtenus par la méthode développée ici sont toujours propres. En effet si $x_n = 9$ pour tout $n > p$, on aurait

$$\zeta_n - \zeta_p = 9 \sum_{k=p+1}^{n} 10^{-k} = 10^{-p} - 10^{-n}$$

et $\zeta = \zeta_n + 10^{-n} = \zeta_p + 10^{-p}$ pour tout $n > p$, mais

$$\zeta - 10^{-n} = \zeta_n \leqslant x < \zeta_n + 10^{-n} = \zeta$$

par définition de ζ_n, soit $0 < 10^n(\zeta - x) \leqslant 1$ pour tout $n > p$ ce qui est impossible puisque $\mathbb{R}$ est archimédien.

Nous venons donc de prouver que tout nombre réel x possède un unique développement décimal illimité propre. Si on note $\mathcal{D}$ l'ensemble des suites $(x_n)_{n\in\mathbb{N}}$ d'entiers relatifs telles que pour tout $n \in \mathbb{N}$, $0 \leqslant x_n \leqslant 9$ et pour tout $N \in \mathbb{N}$ il existe $n \geqslant N$ tel que $x_n \neq 9$, nous avons donc défini une application $\delta : \mathbb{R} \to \mathcal{D}$ qui a chaque nombre réel x associe son développement décimal illimité propre.

Proposition 22. *L'application δ de $\mathbb{R}$ dans $\mathcal{D}$ qui a chaque nombre réel x associe son développement décimal illimité propre $(x_n)_{n\in\mathbb{N}}$ est une bijection et pour tout $x \in \mathbb{R}$ on a*

$$x = \lim_{n\to\infty} \sum_{k=0}^{n} x_k \ 10^{-k}. \tag{10}$$

Démonstration : L'existence de l'application δ et la formule (10) résultent de ce qui précède. Il reste à prouver que δ est une bijection. Soit $(x_n)_{n\in\mathbb{N}}$ un élément de $\mathcal{D}$, cherchons $x \in \mathbb{R}$ tel que $\delta(x) = (x_n)_{n\in\mathbb{N}}$. Remarquons que la suite de rationnels $(\zeta_n)_{n\in\mathbb{N}}$ définie par $\zeta_n = \sum_{k=0}^{n} x_k \ 10^{-k}$ est croissante et de Cauchy. En effet $\zeta_{n+1} - \zeta_n = x_{n+1}10^{-n-1} \geqslant 0$ et si $n < m$

$$0 \leqslant \zeta_m - \zeta_n = \sum_{k=n+1}^{m} x_k \ 10^{-k} \leqslant 9 \sum_{k=n+1}^{m} 10^{-k} = 10^{-n} - 10^{-m} < 10^{-n}.$$

La suite de rationnels $(\zeta_n)_{n\in\mathbb{N}}$ définit donc un nombre réel x. De plus si on pose $p_n = 10^n\zeta_n$, $p_n \in \mathbb{Z}$ et $p_n 10^{-n} \leqslant x < (p_n + 1)10^{-n}$, et par conséquent $\delta(x) = (x_n)_{n\in\mathbb{N}}$ par construction de δ.

Notons φ l'application de $\mathcal{D}$ dans $\mathbb{R}$ qui à la suite $(x_n)_{n\in\mathbb{N}}$ associe le nombre réel x défini par la suite $(\zeta_n)_{n\in\mathbb{N}}$, il est clair que $\delta \circ \varphi$ et $\varphi \circ \delta$ sont respectivement l'application identique de $\mathcal{D}$ et celle de $\mathbb{R}$, ce qui prouve que δ est bijective et que $\delta^{-1} = \varphi$. □

La proposition suivante permet de caractériser nombres rationnels par leurs développements décimaux.

Proposition 23. *L'ensemble $\mathbb{Q}$ des nombres rationnels correspond au sous-ensemble des nombres réels dont le développement décimal est périodique.*

Démonstration : Soit $x \in \mathbb{R}$ un nombre réel dont le développement décimal est périodique,i.e.

$$x = x_0, x_1 \dots x_p y_1 \dots y_q y_1 \dots y_q \dots$$

Alors

$$\begin{aligned} x &= \sum_{k=0}^{p} x_k \ 10^{-k} + \frac{\sum_{k=1}^{q} y_k \ 10^{-k}}{10^{p+q}} (\sum_{k=0}^{\infty} 10^{-kq}) \\ &= \sum_{k=0}^{p} x_k \ 10^{-k} + \frac{\sum_{k=1}^{q} y_k \ 10^{-k}}{10^{p+q}} \frac{1}{10^{-q} - 1} \end{aligned}$$

et par conséquent $x \in \mathbb{Q}$.

Réciproquement soit $x = \frac{p}{q} \in \mathbb{Q}$ avec p et q des entiers premiers entre eux. On définit par récurrence une suite d'entiers r_n, $n \geqslant 1$, tels que $0 \leqslant r_n < q$ en considérant les restes des divisions euclidiennes successives de p par q, puis de 10 r_1 par q et ainsi de suite. En notant x_{n-1} les différents quotients on aura

$$x = \frac{p}{q} = x_0 + 10^{-1}x_1 + 10^{-2}x_2 + \cdots + 10^{-n}x_n + r_{n+1}\frac{10^{-n}}{q}.$$

La suite $(r_n)_{n\in\mathbb{N}}$ prenant ses valeurs dans un ensemble fini à q éléments, les nombres $r_1, \ldots, r_{n+1}$ ne peuvent pas être deux à deux distincts. Si $r_i = r_j$ pour $1 \leqslant i < j \leqslant q+1$, la suite $(x_n)_{n\in\mathbb{N}}$ vérifie $x_p = x_{p+k(j-i+1)}$ pour $p \geqslant i$ et $k \in \mathbb{N}$, elle est donc périodique.

De plus $x_0, x_1 \ldots x_n \ldots$ est le développement décimal de x car

$$\zeta_n = \sum_{k=0}^{n} x_k \ 10^{-k} \leqslant x \leqslant \zeta_n + \frac{r_{n+1}}{q} 10^{-n} < \zeta_n + 10^{-n}$$

puisque $r_{n+1} < q$. □

Grâce aux développement décimaux on peut montrer que $\mathbb{R}$, qui contient $\mathbb{Q}$, est en fait beaucoup plus gros que $\mathbb{Q}$.

Proposition 24. *L'ensemble $\mathbb{R}$ n'est pas dénombrable.*

Démonstration : Nous allons démontrer que l'intervalle $[0, 1] \subset \mathbb{R}$ n'est pas dénombrable. Il suffit de prouver que pour tout sous-ensemble dénombrable D de $[0, 1]$ on peut construire un élément de $[0, 1]$ qui n'est pas dans D.

Soit $(x_n)_{n\in\mathbb{N}}$ une suite de nombres réels contenus dans l'intervalle $[0, 1]$. Chaque terme de cette suite possède un développement décimal illimité propre

$$x_n = 0, x_{n_1} x_{n_2} \ldots x_{n_p} \ldots$$

On construit maintenant un nombre réel y dans [0,1] en considérant le n-ième chiffre après la virgule de x_n. On définit le nombre réel y par son développement décimal propre : $y = 0, y_1 y_2 \ldots y_p \ldots$ où si la n-ième décimale de x_n est différente de 1, alors $y_n = 1$, sinon $y_n = 2$. Le nombre y est clairement dans l'intervalle [0, 1] mais ne peut pas apparaître dans la suite $(x_n)_{n\in\mathbb{N}}$, car il ne peut être égal à aucun des x_n puisque pour tout n sa n-ième décimale est différente de la n-ième décimale de x_n. □

Définitions axiomatiques de $\mathbb{R}$

Le corps $\mathbb{R}$ contenant $\mathbb{Q}$ que nous avons construit est un corps commutatif archimédien et complet. Nous allons montrer qu'un tel corps est unique à isomorphisme près.

Notons que si K est un corps commutatif totalement ordonné on peut définir, comme nous l'avons fait pour le corps $\mathbb{Q}$, les notions de suites convergentes et de suites de Cauchy et que les propriétés 1) à 6) restent encore valables.

Théorème 6. *Si K est un corps commutatif archimédien et complet, alors il existe un isomorphisme de $\mathbb{R}$ sur K prolongeant l'identité de $\mathbb{Q}$ (quand on identifie $\mathbb{Q}$ au sous-corps de K formé des éléments $\frac{p}{q}e = (pe)(qe)^{-1}$, où e est l'élément unité de K).*

Démonstration : Définissons une application $f : \mathbb{R} \to K$ par : si $a \in \mathbb{R}$ est la classe d'une suite de Cauchy de rationnels $(a_n)_{n\in\mathbb{N}}$ alors, on pose, $f(a) = \lim_{n\to\infty} a_n e$ (cette limite existe puisque K est complet et ne dépend pas du choix du représentant $(a_n)_{n\in\mathbb{N}}$).

Par construction, f est un morphisme d'anneau strictement croissant. Enfin, f est surjective, grâce au fait que K est archimédien : pour tout $b \in K$, $b \geqslant 0$ et tout entier $n > 0$, il existe un rationnel $a_n e$ compris entre b et $b + 1/n$ et $a_n = \frac{p}{n}$, où p est le plus petit entier majorant nb. Une telle suite $(a_n)_{n\in\mathbb{N}}$ est de Cauchy, et sa classe $a \in \mathbb{R}$ est un antécédent de b par f. □

L'unicité à isomorphisme près de $\mathbb{R}$ a plusieurs conséquences. D'une part $\mathbb{R}$ est indépendant du choix de son mode de construction, nous avons privilégié ici une construction à partir des suites de Cauchy (c'est une méthode classique que l'on retrouve en topologie pour construire le complété d'un espace vectoriel topologique), d'autres constructions sont possibles à l'aide des coupures de Dedekind ou à l'aide des développements décimaux. D'autre part cela permet de donner une définition axiomatique de $\mathbb{R}$ comme étant *le seul corps commutatif archimédien et complet.*

Prouvons pour terminer que $\mathbb{R}$ est *le seul corps commutatif totalement ordonné tel que toute partie non vide majorée admet une borne supérieure*, ce qui donne une autre définition axiomatique de $\mathbb{R}$.

Proposition 25. *Soit K un corps commutatif totalement ordonné tel que toute partie non vide majorée admet une borne supérieure, alors K est archimédien et complet.*

Démonstration : Prouvons que K est archimédien. Soient a, b deux éléments de K, on suppose $a > 0$. On cherche un entier n tel que $na > b$. Si $b \leqslant 0$, $n = 1$ convient. Si $b > 0$, on considère l'ensemble $A = \{ka \mid k \in \mathbb{N}, ka \leqslant b\}$. Cet ensemble est non vide (il contient 0) et majoré par b, donc il possède une borne supérieure c. L'élément $c - a$ est strictement inférieur à c, par conséquent ce n'est pas un majorant de A. Il existe donc un élément ka de A tel que $c - a < ka$. Mais $c < (k + 1)a$ donc $(k + 1)a$ n'appartient pas à A, si bien que $(k + 1)a > b$.

Montrons maintenant que K est complet. Soit $(a_n)_{n\in\mathbb{N}}$, une suite de Cauchy dans K, nous devons prouver que $(a_n)_{n\in\mathbb{N}}$ converge. La suite $(a_n)_{n\in\mathbb{N}}$ est bornée, il existe donc un élément M de K tel que pour tout entier n, $|a_n| \leqslant M$.

Pour tout n, l'ensemble $A_n = \{a_m \mid m \geqslant n\}$ est majoré par M et non vide, il possède donc une borne supérieure b_n. La suite $(-b_n)_{n\in\mathbb{N}}$ est alors croissante et majorée par M. Soit $b = \sup\{-b_n \mid n \in \mathbb{N}\}$. Par définition de la borne supérieure, pour tout $\varepsilon > 0$, $\varepsilon \in K$, il existe N tel que $b - \varepsilon < -b_N \leqslant b$ et, puisque la suite $(-b_n)_{n\in\mathbb{N}}$ est croissante, pour tout $n > N$ on a $b - \varepsilon < -b_n \leqslant b$, soit $-b \leqslant b_n < -b + \varepsilon$ et la suite $(b_n)_{n\in\mathbb{N}}$ converge donc vers $a = -b$.

La suite $(a_n)_{n\in\mathbb{N}}$ étant de Cauchy pour tout $\varepsilon > 0$ dans K, il existe $\widetilde{N}$ tel que pour tous $p, q \in \mathbb{N}$

$$p, q \geqslant \widetilde{N} \implies a_p < a_q + \frac{\varepsilon}{2}.$$

Posons $N' = \max(N, \widetilde{N})$. Pour tout $n \geqslant N'$, $a_n + \frac{\varepsilon}{2}$ est alors un majorant de $A_{N'}$, donc un majorant de $b_{N'}$, si bien que

$$a - \varepsilon < b_N - \varepsilon/2 \leq a_n \leqslant b_N < a + \varepsilon.$$

Ce qui montre que la suite $(a_n)_{n\in\mathbb{N}}$ converge vers a. □

Pour prouver la réciproque de la Proposition 25, nous allons introduire la notion d'ensembles adjacents dans un corps commutatif K totalement ordonné.

Définition 11. *Soient A et B deux parties non vides de K, on dit que (A, B) est un* couple d'ensembles adjacents *si et seulement si*
(i) Pour tout $(a, b) \in A \times B$, $a \leqslant b$;
(ii) Pour tout $\varepsilon > 0$, $\varepsilon \in K$, il existe $(a, b) \in A \times B$ tel que $b - a \leqslant \varepsilon$.

Lemme 7. *Si le corps K est archimédien et complet et si (A, B) est un couple d'ensembles adjacents de K, il existe un unique élément $c \in K$ tel que pour tout $(a, b) \in A \times B$, $a \leqslant c \leqslant b$.*

Démonstration : Par définition des ensembles adjacents, pour tout $n \in \mathbb{N}$, il existe $(a_n, b_n) \in A \times B$ tel que $b_n - a_n \leqslant \frac{1}{n+1}$ Nous allons prouver que la suite $(a_n)_{n\in\mathbb{N}}$ est une suite de Cauchy dans K.

Grâce au (i) de la définition des ensembles adjacents on a $a_n \leqslant b_p$ pour tous $n, p \in \mathbb{N}$, par conséquent

$$a_n - a_p \leqslant b_p - a_p \leqslant \frac{1}{p+1}$$
$$a_p - a_n \leqslant b_n - a_n \leqslant \frac{1}{n+1}$$

et donc

$$|a_n - a_p| \leqslant \max(\frac{1}{n+1}, \frac{1}{p+1}).$$

Soit $\varepsilon > 0$, $\varepsilon \in K$, le corps K étant archimédien, il existe $N \in \mathbb{N}$ tel que $\frac{1}{N+1} < \varepsilon$. Alors pour $n, p > N$ on a $|a_n - a_p| \leqslant \varepsilon$ et la suite $(a_n)_{n\in\mathbb{N}}$ est de Cauchy dans K. Puisque K est complet, elle converge vers une limite c.

De plus par définition de a_n et b_n, la suite $(b_n - a_n)_{n\in\mathbb{N}}$ converge vers 0. On en déduit que la suite $(b_n)_{n\in\mathbb{N}}$ converge également vers c. Par ailleurs, si $b \in B$, on a, pour tout $n \in \mathbb{N}$, $a_n \leqslant b$ et par passage à la limite $c \leqslant b$. De manière analogue on a $a \leqslant c$ pour tout $a \in A$.

Vérifions maintenant que c est unique. Supposons qu'il existe c et c' tels que pour tout $(a, b) \in A \times B$

$$a \leqslant c < c' \leqslant b.$$

Alors pour tout $(a, b) \in A \times B$, on a $b - a \geqslant c' - c$, ce qui contredit la propriété (ii) de la définition des ensembles adjacents. □

Proposition 26. *Soit K un corps commutatif archimédien et complet contenant $\mathbb{Q}$, alors K est totalement ordonné et toute partie non vide majorée de K admet une borne supérieure.*

Démonstration : Soit A une partie non vide majorée de K, notons B l'ensemble des majorants de A. Nous allons prouver que (A, B) est un couple d'ensembles adjacents de K. Remarquons tout d'abord que B est non vide (puisque A est majorée) et pour tout $(a, b) \in A \times B$, $a \leqslant b$. Soit $\varepsilon > 0$, $\varepsilon \in K$. Fixons $b_0 \in B$ et posons

$$I = \{n \in \mathbb{N} \mid b_0 - n\varepsilon \in B\}.$$

L'ensemble I n'est pas vide car $0 \in I$ et il est majoré. En effet soit $a_0 \in A$ (A est non vide), pour tout $n \in I$ on a $a_0 \leqslant b_0 - n\varepsilon$ et donc $n \leqslant \frac{b_0 - a_0}{\varepsilon}$. L'ensemble I possède donc un plus grand élément n_0. Posons $b = b_0 - n\varepsilon$, alors $b \in B$ et $b - \varepsilon \notin B$, il existe donc $a \in A$ tel que $b - \varepsilon < a$, soit $b - a < \varepsilon$. Le couple (A, B) est donc adjacent.

D'après le lemme 7, il existe $M \in K$ tel que pour tout $(a, b) \in A \times B$, $a \leqslant M \leqslant b$. M est alors le plus petit majorant de A donc sa borne supérieure. □

1.6 Construction des complexes

Soit d un élément de $\mathbb{R}$, considérons l'équation $x^2 = x \times x = d$. Cette équation ne peut avoir de solution dans $\mathbb{R}$ que si $d \geqslant 0$, puisque dans un corps totalement ordonné le produit de deux éléments de même signe, en particulier d'un élément par lui-même, est nécessairement positif. En particulier l'équation $x^2 = -1$ n'a pas de solution dans $\mathbb{R}$.

Nous voulons construire un sur-corps de $\mathbb{R}$ dans lequel l'équation $x^2 = -1$ possède au moins une solution. La construction proposée s'appuie sur les propriétés algébriques classiques du quotient d'un anneau par un idéal. Des constructions plus élémentaires vous seront proposées en exercices.

Considérons $\mathbb{R}[X]$, l'anneau des polynômes à coefficients dans $\mathbb{R}$. C'est un anneau intègre qui contient $\mathbb{R}$ si on identifie $\mathbb{R}$ à l'ensemble des polynômes de degré nul auquel on adjoint le polynôme nul. Le corps $\mathbb{R}$ peut également être identifié au quotient de $\mathbb{R}[X]$ par l'idéal engendré par le polynôme irréductible X. Cherchons $\mathbb{C}$ sous la forme du quotient de $\mathbb{R}[X]$ par un idéal engendré par un polynôme P irréductible (il aura alors naturellement une structure de corps). Rappelons que deux éléments Q et R de $\mathbb{R}[X]$ sont dans la même classe d'équivalence modulo P si et seulement si ils ont même reste dans la division euclidienne par P. Considérons le cas où $P(X) = X^2 + 1$. Alors la classe $\overline{Q}$ de tout polynôme Q contient un unique polynôme de degré inférieur ou égal à 1, le reste $r_P(Q)$ de la division euclidienne du polynôme Q par le polynôme P. On obtient donc par définition de la division euclidienne et du quotient par un idéal

Proposition 27. *L'application $\widetilde{r_P} : \mathbb{R}[X]/(X^2+1) \to \mathbb{R}^1[X]$, qui à la classe $\overline{Q}$ d'un polynôme Q associe $r_P(Q)$, définit une bijection de $\mathbb{R}[X]/(X^2+1)$ sur $\mathbb{R}^1[X]$ telle que :*

(i) $\widetilde{r_P}(\overline{Q} + \overline{R}) = \widetilde{r_P}(\overline{Q}) + \widetilde{r_P}(\overline{R})$

(ii) $\widetilde{r_P}(\overline{QR}) = \widetilde{r_P}(\overline{\widetilde{r_P}(\overline{Q})\widetilde{r_P}(\overline{R})})$

Remarquons que la classe $\overline{X}$ du polynôme X vérifie $(\overline{X})^2 = \overline{X^2} = \overline{-1}$. Par conséquent si $\widetilde{r_P}(\overline{Q}) = aX + b$ et $\widetilde{r_P}(\overline{R}) = cX + d$, on a :

$$\widetilde{r_P}(\overline{QR}) = \overline{r_P}((aX+b)(cX+d)) = \widetilde{r_P}(\overline{acX^2 + (ad+bc)X + bd}) = (ad+bc)X + bd - ac.$$

On définit le corps $\mathbb{C}$ des *nombres complexes* par $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$. Grâce à la Proposition 27 et à la remarque qui suit, on peut identifier $\mathbb{C}$ à $\mathbb{R}[\mathrm{i}]$, où désigne l'ensemble des polynômes dans $\mathbb{R}$ à une indéterminée i qui vérifie $\mathrm{i}^2 = -1$. Un élément $z \in \mathbb{C}$ s'écrit donc $z = x + \mathrm{i}y$, où x et y sont des nombres réels, et si $z = x + \mathrm{i}y$ et $w = u + \mathrm{i}v$ sont deux nombres complexes, on a

$$\begin{aligned} z + w &= (x+u) + \mathrm{i}(y+v) \\ zw &= (xu - yv) + \mathrm{i}(xv + yu). \end{aligned}$$

Soit $z \in \mathbb{C}$ tel que $z = x + \mathrm{i}y$. Alors x s'appelle la *partie réelle* de z et y la *partie imaginaire* de z. On pose $\overline{z} = x - \mathrm{i}y$, $\overline{z} \in \mathbb{C}$, c'est le *conjugué* de z. L'application $c : z \mapsto \overline{z}$ définit un endomorphisme d'anneau qui vérifie $c \circ c = \mathrm{Id}$ et dont l'ensemble des points fixes est $\mathbb{R}$. Le *module* de z est le nombre réel positif $|z|$ tel que $|z|^2 = z\overline{z} = x^2 + y^2$. Comme nous l'avons déjà remarqué $z = 0$ si et seulement si $|z| = 0$. De plus on vérifie aisément que si $z, z' \in \mathbb{C}$ alors $|zz'| = |z||z'|$ et l'ensemble $\mathbb{T} = \{z \in \mathbb{C} \mid |z| = 1\}$ définit un sous-groupe multiplicatif de $\mathbb{C}^*$.

2 Entraînement

2.1 Vrai ou faux

Vrai-Faux 1. Pour chacune des définitions de $O, \mathcal{N}$ et s qui suivent, $(O, \mathcal{N}, s)$ est-il un triplet naturel (oui ou non et pourquoi) ?

1. ☒ $O = 1$, $\mathcal{N} = \{2^n\,,\ n \in \mathbb{N}\}$, $s(n) = 2n$.
2. ☐ $O = 1$, $\mathcal{N} = \{2^n\,,\ n \in \mathbb{Z}\}$, $s(n) = 2n$.
3. ☒ $O = 1$, $\mathcal{N} = \{2^{-n}\,,\ n \in \mathbb{N}\}$, $s(n) = n/2$.
4. ☐ $O = \{1\}$, $\mathcal{N} = \{\{n\}\,,\ n \in \mathbb{N}\}$, $s(n) = \{n\} \cup \{1\}$.
5. ☐ $O = \emptyset$, $\mathcal{N} = \{\{1, \ldots, n\}\,,\ n \in \mathbb{N}\}$, $s(\{1, \ldots, n\}) = \{1, \ldots, n+1\}$.
6. ☒ $O = \{0\}$, $\mathcal{N} = \{n\}$, $s(\{n\}) = \{n+1\}$).

Vrai-Faux 2. Soit $H(n)$ un énoncé dépendant de l'entier n. Les assertions suivantes entraînent-elles que $H(n)$ est vraie pour tout $n \in \mathbb{N}$ (oui ou non et pourquoi) ?

1. ☒ $H(0) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n) \Longrightarrow H(n+1)\Big)$.
2. ☐ $H(1) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n) \Longrightarrow H(n+1)\Big)$.
3. ☐ $H(0) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n+1) \Longrightarrow H(n)\Big)$.
4. ☐ $H(0) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n) \Longrightarrow H(n+2)\Big)$.
5. ☒ $H(0) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n) \Longrightarrow H(n+2)\Big) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n+1) \Longrightarrow H(n)\Big)$.
6. ☐ $H(0) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n) \Longrightarrow H(2n)\Big) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n+1) \Longrightarrow H(n)\Big)$.
7. ☒ $(H(0) \wedge H(1)) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n) \Longrightarrow H(2n)\Big) \wedge \Big(\forall n \in \mathbb{N}\,,\ H(n+1) \Longrightarrow H(n)\Big)$.

Vrai-Faux 3. Les affirmations suivantes sont-elles vraies ou fausses et pourquoi ?

1. ☐ Toute partie de $\mathbb{N}$ admet un plus petit élément.
2. ☐ Toute partie non vide de N admet un plus grand élément.
3. ☒ Toute partie non vide et majorée de $\mathbb{Z}$ admet un plus grand élément.
4. ☐ Toute partie de $\mathbb{N}$ différente de $\mathbb{N}$ admet un plus grand élément.
5. ☒ Toute partie finie de $\mathbb{Q}$ admet un plus grand élément.
6. ☐ L'ensemble des majorants d'un sous-ensemble non vide de $\mathbb{Q}$ admet un plus petit élément dans $\mathbb{Q}$.
7. ☒ L'ensemble des minorants d'un sous-ensemble non vide de $\mathbb{Q}^+$ admet un plus grand élément dans $\mathbb{R}$.

Vrai-Faux 4. Les affirmations suivantes sont-elles vraies ou fausses et pourquoi ?

1. ☐ Si un nombre entier est une puissance de 2 alors son écriture dans une base b impaire ne contient aucun 0.
2. ☒ Si un nombre entier est une puissance de 2 alors son écriture dans une base $b \neq 2$ ne se termine pas par 0.
3. ☐ Si l'écriture d'un nombre entier dans une base impaire se termine par 0, alors ce nombre est impair.
4. ☒ Si l'écriture d'un nombre entier dans un base paire se termine par 0, alors ce nombre est pair.
5. ☒ Si l'écriture hexadécimale d'un nombre commence par 8, suivi seulement de zéros, alors ce nombre est une puissance de 2.
6. ☐ Si l'écriture hexadécimale d'un nombre ne contient que des 2, alors ce nombre est divisible par 32.

Vrai-Faux 5. Soient a et b deux réels quelconques. Parmi les affirmations suivantes lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☐ Si $a + b$ est rationnel, alors soit a est rationnel soit b est rationnel.
2. ☒ Si $a + b$ est irrationnel, alors soit a est irrationnel soit b est irrationnel.
3. ☒ Si a est rationnel, alors sa partie décimale est rationnelle.
4. ☐ Si a est irrationnel, alors la partie décimale de $a + b$ est irrationnelle.
5. ☒ Si la partie décimale de a est rationnelle, alors a est rationnel.

Vrai-Faux 6. Soit (x_n) une suite de rationnels. Parmi les affirmations suivantes lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☐ Si (x_n) est une suite de Cauchy, alors elle converge dans $\mathbb{Q}$.
2. ☒ Si (x_n) converge dans $\mathbb{Q}$ alors c'est une suite de Cauchy.
3. ☐ Si la suite (x_n) est majorée, alors c'est une suite de Cauchy.
4. ☒ Si la suite (x_n) tend vers 0, alors elle est bornée.
5. ☒ Si (x_n) est une suite de Cauchy, alors elle converge dans $\mathbb{R}$.

Vrai-Faux 7. Soit A une partie non vide de $\mathbb{R}$. Parmi les affirmations suivantes lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☒ Si A est minorée, alors A possède une borne inférieure.
2. ☐ Si $x \leqslant \sup(A)$ alors $x \in A$.
3. ☐ Si A contient au moins 2 réels distincts, alors A contient un rationnel.
4. ☐ Si A est infinie, alors A contient une infinité d'irrationnels.
5. ☒ Si A contient un intervalle de $\mathbb{R}$, contenant lui-même deux points distincts, alors A contient une infinité d'irrationnels.

6. ☐ Si A contient un intervalle de $\mathbb{R}$, alors A contient une infinité de rationnels.

Vrai-Faux 8. Soit A une partie non vide de $\mathbb{R}$. On note $|A| = \{|x|\,,\ x \in A\}$. Parmi les affirmations suivantes lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☐ Si A est majorée, alors $|A|$ possède une borne supérieure.
2. ☒ 0 est un minorant de $|A|$.
3. ☒ $|A|$ possède toujours une borne inférieure.
4. ☐ $|A|$ possède toujours une borne supérieure.
5. ☒ A est bornée si et seulement si $|A|$ est majorée.
6. ☒ Si A est un intervalle, alors $|A|$ est un intervalle.
7. ☐ Si $|A|$ est un intervalle, alors A est un intervalle.
8. ☐ Si A est un intervalle ouvert, alors $|A|$ est un intervalle ouvert.
9. ☒ Si A est un intervalle fermé, alors $|A|$ est un intervalle fermé.

Vrai-Faux 9. Soient a et b deux réels quelconques. Parmi les affirmations suivantes lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☒ $|ab| = |a|\,|b|$.
2. ☒ $|a| - |b| \leqslant |a - b|$.
3. ☐ $|a - b| \leqslant \max\{|a|, |b|\}$.
4. ☒ $|a - b| = |a - (a + b)/2| + |(a + b)/2 - b|$.
5. ☐ $|a - b| = |a - (a + b)| + |(a + b) - b|$.
6. ☐ Si $|a - b| < |a|$, alors $|ab| = ab$.
7. ☐ $\lfloor a + b \rfloor = \lfloor a \rfloor + \lfloor b \rfloor$.
8. ☒ $\lfloor a + b \rfloor \geqslant \lfloor a \rfloor + \lfloor b \rfloor$.
9. ☒ $\lfloor a + b \rfloor \leqslant \lfloor a \rfloor + \lfloor b \rfloor + 1$.
10. ☐ $D(a + b) = D(a) + D(b)$.

Vrai-Faux 10. Parmi les affirmations suivantes lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☒ Le corps des rationnels est archimédien.
2. ☐ Tout corps archimédien contenant $\mathbb{Q}$ est isomorphe à $\mathbb{R}$.
3. ☐ Le corps des rationnels est archimédien et complet.
4. ☐ Dans un corps archimédien, toute partie non vide et majorée possède une borne supérieure.
5. ☒ Tout corps archimédien et complet est isomorphe à $\mathbb{R}$.

Vrai-Faux 11. On considère le quotient $\mathbb{Q}[X]/(X^2-2)$. Parmi les affirmations suivantes lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. ☒ Il est isomorphe à $\mathbb{Q} + \sqrt{2}\mathbb{Q}$.
2. ☒ C'est un corps archimédien.
3. ☐ C'est un corps complet.
4. ☐ C'est un corps isomorphe à $\mathbb{C}$.
5. ☒ C'est un corps isomorphe à $\mathbb{Q} + \mathrm{i}\mathbb{Q}$.

2.2 Exercices

Exercice 1. On considère un triplet naturel $(O, \mathcal{N}, s)$.

1. Montrer que $(s(O), \mathcal{N} \setminus \{O\}, s)$ est un triplet naturel.
2. On note s^2 l'application composée $s \circ s$. Soit $\mathcal{P}$ une propriété définie sur $\mathcal{N}$ telle que $\mathcal{P}(O)$ est vraie, $\mathcal{P}(s(O))$ fausse et :

$$\forall a \in \mathbb{N}\ , \quad P(a) \implies P(s^2(a))\ .$$

   On note $\mathcal{N}_2$ l'ensemble des éléments de $\mathcal{N}$ tels que $\mathcal{P}(a)$ est vraie. Montrer que $\mathcal{N}_2$ est un ensemble non majoré.
3. Montrer que $(O, \mathcal{N}_2, s^2)$ est un triplet naturel.
4. On note s^0 l'application identique, et on définit par récurrence s^n comme l'application composée $s \circ s^{n-1}$, pour $n \geqslant 1$. Définir l'application successeur σ telle que $(s^0, \{s^n\ ,\ n \in \mathbb{N}\}, \sigma)$ soit un triplet naturel.

Exercice 2. On dit qu'un ensemble A est infini s'il existe une application injective de A vers un sous-ensemble de A différent de A.

1. Montrer que $\mathbb{N}$ est infini.
2. Montrer que tout sous-ensemble de $\mathbb{N}$ non majoré est infini.
3. Soit A un ensemble tel qu'un de ses sous-ensembles soit infini. Montrer que A est infini.
4. Soit A un ensemble infini. Montrer que le complémentaire de tout sous-ensemble fini de A est infini.
5. Soit A un ensemble infini, et O un élément de A. Construire un sous-ensemble $\mathcal{N}$ et une application s tels que $(O, \mathcal{N}, s)$ soit un triplet naturel.
6. Montrer qu'un ensemble A est infini si et seulement si il existe une application injective de $\mathbb{N}$ dans A.

Exercice 3.

1. Écrire dans les bases 2, 3, 4, 5, 8, 16 le nombre qui s'écrit 2345816 en base 10.
2. Écrire en base 10 le nombre qui s'écrit $\overline{12345}$ en base 8.
3. Écrire en base 10 le nombre qui s'écrit $\overline{ABCDEF}$ en base 16.

4. Écrire en base 4, puis 8, puis 16 le nombre qui s'écrit $\overline{1001101011101}$ en base 2 (sans passer par la base 10).
5. Écrire en base 2 le nombre qui s'écrit $\overline{ABCDEF}$ en base 16 (sans passer par la base 10).
6. En base 16, quel est le successeur du nombre $\overline{EFFEF}$?
7. En base 16, quel est le prédécesseur du nombre $\overline{A0000}$?

Exercice 4. Soit $E = \mathbb{R}^2 \setminus \{(0,0)\}$. Soit $\mathcal{R}$ la relation sur E définie par :

$$(x,y)\mathcal{R}(x',y') \iff \Big(\exists \lambda \in \mathbb{R}\,,\ (x,y) = \lambda(x',y') \Big)\,.$$

1. Montrer que $\mathcal{R}$ est une relation d'équivalence.
2. Montrer que l'ensemble quotient $E/\mathcal{R}$ est en bijection avec les droites vectorielles du plan.
3. Pour tout $(x,y) \in E$, on note $\overline{(x,y)}$ sa classe d'équivalence pour $\mathcal{R}$. On considère l'application f, de $\mathbb{R}$ dans $E/\mathcal{R}$, qui à x associe $\overline{(x,1)}$. Montrer que f est injective et déterminer $\mathrm{Im}(f)$.
4. L'addition vectorielle sur E induit-elle une loi de composition interne sur $E/\mathcal{R}$?
5. Soient (a,b,c,d) quatre réels tels que $ad - bc \neq 0$. On considère l'application g de $\mathbb{R}^2$ dans $\mathbb{R}^2$ qui à (x,y) associe $(ax+by, cx+dy)$.
   (a) Montrer que g est une bijection de $\mathbb{R}^2$ dans $\mathbb{R}^2$, et qu'elle induit une bijection de E dans E.
   (b) Montrer que
   $$\forall (x,y),(x',y') \in E\,, \quad (x,y)\mathcal{R}(x',y') \implies g(x,y)\mathcal{R}g(x',y')\,.$$
   (c) En déduire que g induit une bijection de $E/\mathcal{R}$ dans lui-même.

Exercice 5. Soit $d \in \mathbb{N}^*$ un nombre fixé. On note $\mathbb{D}$ l'ensemble des « d-cimaux », à savoir l'ensemble des éléments de $\mathbb{Q}$ multiples entiers d'une puissance de d.

$$\mathbb{D} = \{\, nd^m\,,\ (n,m) \in \mathbb{Z}^2 \,\}\,.$$

1. Montrer que $(\mathbb{D}, +, \times)$ est un sous-anneau de $(\mathbb{Q}, +, \times)$. Est-ce un sous-corps ?
2. On considère le sous-ensemble de $\mathbb{D}^{\mathbb{N}}$, formé des suites de Cauchy à valeurs dans $\mathbb{D}$. On le note $\mathcal{D}$. On le munit de la multiplication et de l'addition terme à terme. Montrer que $(\mathcal{D}, +, \times)$ est un sous-anneau de $(\mathcal{C}, +, \times)$ (suites de Cauchy à valeurs dans $\mathbb{Q}$).
3. Soit $\mathcal{D}_0$ l'ensemble des suites de Cauchy à valeurs dans $\mathbb{D}$, dont la limite est 0. Montrer que $\mathcal{D}_0$ est un idéal de $\mathcal{D}$.
4. Montrer que l'anneau quotient $\mathcal{D}/\mathcal{D}_0$ est un corps commutatif, noté $\mathbb{K}$.

5. On note $\mathcal{D}^+$ et $\mathcal{D}^-$ les intersections de $\mathcal{D}$ avec $\mathcal{C}^+$ et $\mathcal{C}^-$. Montrer que $\mathcal{D}^+ \cap \mathcal{D}^- = \mathcal{D}_0$, et que $\mathcal{D}^+ \cup \mathcal{D}^- = \mathcal{D}$.
6. On considère la relation $\preceq$ sur $\mathcal{D}$ définie par $((u_n) \preceq (v_n)) \iff (v_n - u_n) \in \mathcal{D}^+$. Montrer que cette relation est compatible avec le quotient par $\mathcal{D}_0$, et qu'elle définit donc une relation d'ordre sur $\mathbb{K}$ encore notée $\preceq$.
7. Montrer que $\mathbb{K}$ muni de la relation $\preceq$ est un corps totalement ordonné et archimédien.
8. On note I l'injection canonique de $\mathcal{D}$ dans $\mathcal{C}$. Montrer que I passe au quotient en une injection canonique de $\mathbb{K}$ dans $\mathbb{R}$.
9. On appelle *suite d'approximation d-cimale*, toute suite (u_n) d'éléments de $\mathbb{D}$ telle que :
$$\forall n \in \mathbb{N}\,,\ u_n \leqslant u_{n+1} < u_n + d^{-n}\ .$$
Montrer que toute suite d'approximation d-cimale appartient à $\mathcal{D}$.
10. Soit x un réel. Pour tout $n \in \mathbb{N}$, on pose $u_n = d^{-n}\lfloor x\, d^n \rfloor$. Montrer que la suite $(u_n)_{n\in\mathbb{N}}$ est une suite d'approximation d-cimale, et qu'elle converge vers x dans $\mathbb{R}$. En déduire que $\mathbb{K} = \mathbb{R}$.
11. Soit x un réel compris entre 0 et 1. Pour tout $m \geqslant 1$, on définit $c_m = \lfloor d^m x \rfloor - d\lfloor d^{m-1} x \rfloor$. Montrer que $c_m \in \{0, \ldots, d-1\}$. La suite (c_m) est le *développement d-cimal* de x. Montrer que la suite de terme général $c_1\, d^{-1} + \ldots + c_m\, d^{-m}$ est une suite d'approximation d-cimale et qu'elle converge vers x.
12. Montrer qu'un réel x est un rationnel si et seulement si son développement d-cimal est périodique.
13. Soit x un réel compris entre 0 et 1 et (c_n) son développement d-cimal. Soient $p(x)$ et $i(x)$ les deux réels donc les développements d-cimaux sont les suites $(c_{2n})_{n\in\mathbb{N}}$ et $(c_{2n+1})_{n\in\mathbb{N}}$. Montrer que l'application $x \longmapsto (p(x), i(x))$ est une bijection de $[0,1]$ dans $[0,1]^2$.
14. On se place désormais dans le cas $d = 3$. On appelle *ensemble de Cantor* et on note $\mathbb{T}$, l'ensemble des réels x compris entre 0 et 1, tels que pour tout n, l'entier $\lfloor x\, 3^n \rfloor$ vaut 0 ou 2. Construire une bijection entre $\mathbb{T}$ et l'intervalle $[0,1]$. (Indication : transformer un développement 3-cimal en un développement 2-cimal).
15. Soit $m \in \mathbb{N}^*$ un entier. Soit $\mathbb{T}_m$ l'ensemble des éléments de $\mathbb{D}$:
$$\mathbb{T}_m = \{\, c_1 3^{-1} + \cdots c_m 3^{-m}\,,\ c_1, \ldots c_m \in \{0,2\}\,\}\ .$$
Montrer que $\mathbb{T}_m$ est une réunion finie d'intervalles de longueur $1/3^m$. En déduire la mesure de Lebesgue de $\mathbb{T}_m$.
16. Montrer que pour tout $m \in \mathbb{N}^*$, $\mathbb{T} \subset \mathbb{T}_n$. En déduire que la mesure de Lebesgue de $\mathbb{T}$ est nulle.

Exercice 6. Soit $\mathbb{K}$ un corps totalement ordonné. On appelle *coupure de Dedekind* un couple (A, B) de sous-ensembles de $\mathbb{K}$ vérifiant :

(i) $A \neq \emptyset$, $B \neq \emptyset$,
(ii) $A \cap B = \emptyset$
(iii) $A \cup B = \mathbb{K}$
(iv) $\forall x \in A\,,\ \forall y \in \mathbb{B}\,,\ x < y$
(v) A ne possède pas de plus grand élément.

1. Soit $r \in \mathbb{K}$. On note $A_r = \{x \in \mathbb{K}\,,\ x < r\}$, et $\overline{A_r}$ son complémentaire. Montrer que le couple $(A_r, \overline{A_r})$ est une coupure de Dedekind.
2. Soit (A, B) une coupure de Dedekind. Montrer qu'il existe au plus un $r \in \mathbb{K}$ tel que $A = A_r$.
3. Pour $\mathbb{K} = \mathbb{R}$: montrer que si (A, B) est une coupure de Dedekind, alors il existe $r \in \mathbb{R}$ tel que $A = A_r$.
4. Pour $\mathbb{K} = \mathbb{Q}$: montrer que le couple (A, B) défini comme suit est une coupure de Dedekind.
$$A = \{x \in \mathbb{Q}\,,\ x \leqslant 0 \text{ ou } x^2 < 2\} \quad \text{et} \quad B = \{y \in \mathbb{Q}\,,\ y > 0 \text{ et } y^2 \geqslant 2\}\,.$$
5. Retour au cas général : montrer que si (A, B) est une coupure de Dedekind alors
$$\forall x \in \mathbb{K}\,,\ \Big((a \in A) \wedge (x \leqslant a)\Big) \implies x \in A\,,$$
et
$$\forall y \in \mathbb{K}\,,\ \Big((b \in B) \wedge (y \geqslant b)\Big) \implies y \in B\,.$$
6. Soient (A, B) et (C, D) deux coupures de Dedekind. On définit la relation $\preceq$ en posant :
$$(A, B) \preceq (C, D) \iff A \subset C\,.$$
Montrer que $\preceq$ est une relation d'ordre total sur l'ensemble des coupures de Dedekind.
7. Soient r et s deux éléments de $\mathbb{K}$. Montrer que
$$(A_r, \overline{A_r}) \preceq (A_s, \overline{A_s}) \iff r \leqslant s\,.$$
8. Montrer que l'ensemble des coupures de Dedekind, muni de l'ordre $\preceq$, possède la propriété de la borne supérieure.
9. Désormais, $\mathbb{K} = \mathbb{Q}$. On définit l'addition de deux sous-ensembles A et C de $\mathbb{Q}$ par :
$$A \oplus C = \{\, a + c\,,\ a \in A\,,\ c \in C\,\}\,,$$
et l'addition des coupures de Dedekind par :
$$(A, \overline{A}) \oplus (C, \overline{C}) = (A \oplus C, \overline{A + C})\,.$$
Montrer que si r et s sont deux rationnels, alors $(A_r, \overline{A_r}) \oplus (A_s, \overline{A_s}) = (A_{r+s}, \overline{A_{r+s}})$. Montrer que l'ensemble de coupures de Dedekind, muni de cette addition est un groupe commutatif.

10. Procéder comme dans la question précédente pour définir la multiplication $\otimes$ des coupures de Dedekind (attention aux nombres négatifs). Montrer que si r et s sont deux rationnels, alors $(A_r, \overline{A_r}) \otimes (A_s, \overline{A_s}) = (A_{rs}, \overline{A_{rs}})$. Montrer que l'ensemble de coupures de Dedekind, muni de $\oplus$ et $\otimes$ est un corps commutatif.
11. Montrer que ce corps est archimédien et complet.
12. En déduire qu'il est isomorphe à $\mathbb{R}$.

Exercice 7.

1. On munit $\mathbb{R}^2$ des deux lois de composition interne définies par :

$$(x, y) \oplus (x', y') = (x + x', y + y') \quad \text{et} \quad (x, y) \otimes (x', y') = (xx' - yy', xy' + yx') \ .$$

   Montrer que $(\mathbb{R}^2, \oplus, \otimes)$ est un corps, isomorphe à $\mathbb{C}$.
2. On considère le sous-ensemble E suivant de $\mathcal{M}_{2,2}(\mathbb{R})$:

$$E = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ , \ (a, b) \in \mathbb{R}^2 \right\} \ .$$

   Montrer que E, muni de l'addition et de la multiplication matricielles est un corps, isomorphe à $\mathbb{C}$.

Exercice 8. Montrer qu'il n'existe pas de relation d'ordre total sur $\mathbb{C}$ qui prolonge la relation d'ordre sur $\mathbb{R}$ et qui soit compatible avec la somme et le produit c'est-à-dire telle que :

- $a \leq b$ et $c \leq d$ entraîne $a + c \leq c + d$, et
- $a \leq b$ et $0 \leq c$ entraîne $ac \leq bc$.

Exercice 9.

1. On considère le sous-ensemble $\mathbb{H}$ suivant de $\mathcal{M}_{2,2}(\mathbb{C})$:

$$E = \left\{ \begin{pmatrix} a + b\mathrm{i} & -c + d\mathrm{i} \\ c + d\mathrm{i} & a - b\mathrm{i} \end{pmatrix} \ , \ (a, b, c, d) \in \mathbb{R}^4 \right\} \ .$$

   Montrer que $\mathbb{H}$, muni de l'addition et de la multiplication matricielles est un corps non commutatif (c'est le *corps des quaternions*).
2. On pose :

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ , \ I = \begin{pmatrix} \mathrm{i} & 0 \\ 0 & -\mathrm{i} \end{pmatrix} \ , \ J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \ , \ K = \begin{pmatrix} 0 & \mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \ .$$

   Vérifier que $\mathbb{H}$ est un $\mathbb{R}$-espace vectoriel de dimension 4, dont $(1, I, J, K)$ est une base.
3. Calculer I^2, J^2, K^2, IJ, IK, KJ, IJK.

4. On munit $\mathbb{R}^4$ de sa base canonique, que l'on note (e_1, e_i, e_j, e_k). On munit $\mathbb{R}^4$ de l'addition vectorielle $+$. Montrer que les trois propriétés suivantes définissent une loi de composition interne $\times$ sur $\mathbb{R}^4$.
   i) $\times$ est distributive par rapport à $+$;
   ii) e_1 est élément neutre pour $\times$;
   iii) $e_i \times e_i = e_j \times e_j = e_k \times e_k = e_i \times e_j \times e_k = -e_1$.
5. Montrer que $(\mathbb{R}^4, +, \times)$ est un corps non commutatif, isomorphe à $\mathbb{H}$.
6. On considère le sous-ensemble $\mathbf{H}$ de $\mathcal{M}_{4,4}(\mathbb{R})$, formé des matrices de la forme

$$M(a,b,c,d) = \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix},$$

   pour tout $(a,b,c,d) \in \mathbb{R}^4$. Montrer que $\mathbf{H}$, muni de l'addition et de la multiplication matricielles est un corps non commutatif, isomorphe à $\mathbb{H}$.

Exercice 10. Soit K un anneau commutatif. On dit qu'un élément d de K est un *carré* dans K s'il existe un élément $x \in K$ tel que $x^2 = x \times x = d$. Soit K un anneau commutatif et d un élément de K qui n'est pas un carré dans K. On note L le produit cartésien $K \times K$.

1. Supposons qu'il existe un anneau A contenant K dans lequel l'équation $x^2 = d$ possède au moins une solution. Notons ω une des solutions de cette équation. Soit f l'application de L dans A qui à (x,y) associe $x + \omega y$. Notons $A' = \mathrm{Im}(f)$. Montrer que A' est un sous-anneau de A contenant K, dans lequel l'équation $x^2 = d$ possède au moins une solution.
2. Montrer que si K est un corps, alors f est injective.
3. On définit sur L deux lois de composition interne par :

$$(x,y) \oplus (x',y') = (x + x', y + y'), \tag{11}$$

$$(x,y) \otimes (x',y') = (xx' + dyy', xy' + x'y). \tag{12}$$

   Montrer que $(L, \oplus, \otimes)$ est un anneau commutatif. On le note $K[d]$, et on l'appelle *extension quadratique* de K.
4. Soit j l'application de K dans L qui à x associe $(x,0)$. Montrer que $j(K)$ est un sous-anneau de L, et que j est un isomorphisme d'anneaux de K sur $j(K)$.
5. Notons ω l'élément $(0,1)$ de L. Vérifier que $\omega^2 = (0,1) \otimes (0,1) = d$.
6. Vérifier que pour tout $(x,y) \in L$, $(x,y) = j(x) + \omega j(y)$.
7. Montrer que si K est un corps, alors $K[d]$ est un corps.
8. Vérifier que $\mathbb{R}$[i] est isomorphe à $\mathbb{C}$.

Exercice 11. Soit $\mathbb{Z}[\mathrm{i}]$ l'ensemble des nombres complexes de la forme $a + \mathrm{i}b$ avec a et b éléments de $\mathbb{Z}$.

1. Montrer que $\mathbb{Z}[\mathrm{i}]$ est un sous-anneau de $\mathbb{C}$.
2. Soit z un élément de $\mathbb{Z}[\mathrm{i}]$. Montrer que le conjugué $\overline{z}$ de z appartient à $\mathbb{Z}[i]$ et que $|z|^2$ appartient à $\mathbb{N}$.
3. Soit z un élément de $\mathbb{Z}[\mathrm{i}]$. Montrer que z appartient au groupe $\mathbb{Z}[\mathrm{i}]^*$ des unités de $\mathbb{Z}[\mathrm{i}]$ si et seulement si $|z| = 1$.
4. Déterminer le groupe $\mathbb{Z}[\mathrm{i}]^*$.
5. Montrer que pour tout z élément de $\mathbb{C}$, il existe un élément z_0 de $\mathbb{Z}[\mathrm{i}]$ tel que $|z - z_0|^2 \leq \frac{1}{2}$.
6. Prouver que pour tous z_0 et z_1 éléments de $\mathbb{Z}[\mathrm{i}]$ avec $z_1 \neq 0$, il existe des éléments a_0 et a_1 de $\mathbb{Z}[\mathrm{i}]$ tels que $z_0 = a_0 z_1 + a_1$ avec $|a_1| < |z_1|$.
7. Montrer que $\mathbb{Z}[\mathrm{i}]$ est un anneau principal.

Exercice 12. L'objet de cet exercice est de prouver que $\mathbb{Z}[\sqrt{10}]$ n'est pas un anneau principal.

1. Prouver que l'équation $10\,y^2 = x^2$ n'a pas de solution (x, y) dans $\mathbb{Z}^2$ à part $x = y = 0$.
2. Déterminer l'ensemble des carrés modulo 10 : un élément y de $\mathbb{Z}/10\mathbb{Z}$ est un carré modulo 10 s'il existe un élément x de $\mathbb{Z}/10\mathbb{Z}$ tel que $y = x^2$.
3. Prouver qu'il n'existe pas de couple (x, y) dans $\mathbb{Z}^2$ tel que $10y^2 = x^2 + 3$ ou $10y^2 = x^2 - 3$.
4. Soit $v = \sqrt{10}$ tel que $v^2 = 10$ et A l'ensemble des $x + yv$ pour x et y éléments de $\mathbb{Z}$. Prouver que A est un sous-anneau de K et que pour tout élément a de A, les entiers x et y tels que $a = x + yv$ sont uniques. On note souvent $A = \mathbb{Z}[\sqrt{10}]$.
5. Soit $c : A \to A$ définie par $c(x + yv) = x - yv$, pour tous x et y entiers. Montrer que c est un endomorphisme d'anneau et que les seuls points fixes de c sont les éléments de $\mathbb{Z}$.
6. Expliciter $ac(a)$ en fonction des coordonnées (x, y) de $a = x + yv$. En déduire qu'il n'existe pas d'élément a de A tel que $|ac(a)| = 3$.
7. Soit $n : A \to A$ définie par $n(a) = ac(a)$. Montrer que n est à valeurs dans $\mathbb{Z}$ et vérifie les propriétés suivantes : pour tous a et b éléments de A, $n(ab) = n(a)n(b)$; pour tout a élément de A, $n(a) = 0$ si et seulement si $a = 0$.
8. Soit I l'ensemble des $3a + (2 + v)b$ pour a et b éléments de A. Montrer que I est un idéal de A contenant 3 et $2 + v$ et déduire de ce qui précède que cet idéal n'est pas principal.

Exercice 13. On considère l'anneau $\mathbb{Z}[\sqrt{-5}]$. Vérifier que

$$(2 + \mathrm{i}\sqrt{-5})(2 - \mathrm{i}\sqrt{-5}) = 3.3 = 9.$$

En déduire que $\mathbb{Z}[\sqrt{-5}]$ n'est pas principal.

2.3 QCM

Donnez-vous une heure pour répondre à ce questionnaire. Les 10 questions sont indépendantes. Pour chaque question 5 affirmations sont proposées, parmi lesquelles 2 sont vraies et 3 sont fausses. Pour chaque question, cochez les 2 affirmations que vous pensez vraies. Chaque question pour laquelle les 2 affirmations vraies sont cochées rapporte 2 points.

Question 1. Soit $(O, \mathcal{N}, s)$ un triplet naturel.

A $(s(O), \mathcal{N}, s)$ est un triplet naturel.

B $(O, \mathcal{N} \setminus \{O\}, s)$ est un triplet naturel.

C $(s(O), s(\mathcal{N}), s \circ s)$ est un triplet naturel.

D $(s(O), \mathcal{N} \setminus \{O\}, s)$ est un triplet naturel.

E $(s(O), s(\mathcal{N}), s)$ est un triplet naturel.

Question 2. Soit $H(n)$ un énoncé dépendant de l'entier n. L'assertion entraîne que $H(n)$ est vraie pour tout $n \geqslant 1$.

A $H(1) \wedge \Big(\forall n \geqslant 1\,,\ H(n) \Longrightarrow H(n+1)\Big)$.

B $H(1) \wedge \Big(\forall n \geqslant 1\,,\ H(n) \Longrightarrow H(n+2)\Big)$.

C $H(1) \wedge \Big(\forall n \geqslant 2\,,\ H(n) \Longrightarrow H(n+1)\Big)$.

D $H(1) \wedge \Big(\forall n \geqslant 1\,,\ H(n+1) \Longrightarrow H(n)\Big)$.

E $H(1) \wedge \Big(\forall n \geqslant 1\,,\ H(n) \Longrightarrow H(2n)\Big) \wedge \Big(\forall n \geqslant 4\,,\ H(n) \Longrightarrow H(n-1)\Big)$.

Question 3.

A Toute partie non vide de $\mathbb{Z}$ admet un plus petit élément.

B Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.

C Toute partie non vide et majorée de $\mathbb{Q}$ admet un plus grand élément.

D L'ensemble des minorants d'une partie non vide de $\mathbb{R}^+$ admet un plus grand élément.

E Toute partie non vide et minorée de $\mathbb{R}$ admet un plus petit élément.

Question 4.

A Si un nombre entier est multiple de 16, alors son écriture en base 8 se termine par deux zéros.

B Si l'écriture d'un nombre en base hexadécimale se termine par deux zéros, ce nombre est une puissance de deux.

C Si un nombre s'écrit avec deux lettres en base hexadécimale, il est au moins égal à 170.

D Si l'écriture d'un nombre en base hexadécimale ne comporte que des 8 et des zéros, alors ce nombre est mutiple de 16.

E Si l'écriture d'un nombre en base hexadécimale se comporte que des A, et des zéros, alors ce nombre est multiple de 10.

Question 5. Soit x un réel.

A Si $\sqrt{x}$ est irrationnel, alors $\sqrt[4]{x}$ est irrationnel.

B Si $\sqrt{x}$ est rationnel, alors $\sqrt[3]{x}$ est irrationnel.

C Si $\sqrt{x}$ est irrationnel, alors $\sqrt{3x}$ est irrationnel.

D Si $\sqrt{x}$ est rationnel, alors x^3 est rationnel.

E Si $\sqrt[4]{x}$ est irrationnel, alors $\sqrt[3]{x}$ est irrationnel.

Question 6. Soit I un intervalle de $\mathbb{R}$.

A Si I est non vide, alors il contient au moins un rationnel.

B Si I contient au moins deux réels distincts, alors il contient au moins deux irrationnels.

C Si I contient un rationnel et un irrationnel, alors il contient un nombre décimal.

D Si I contient un nombre rationnel, alors il contient un nombre décimal.

E Si I contient un multiple entier d'une puissance négative de 2, alors il contient un irrationnel.

Question 7. Soit $(x_n)_{n\in\mathbb{N}}$ une suite de rationnels.

A Si (x_n) est une suite de Cauchy, alors (x_n) converge dans $\mathbb{Q}$.

B Si (x_n) est bornée, alors (x_n) est une suite de Cauchy.

C Si (x_n) est une suite de Cauchy, alors (x_n) converge dans $\mathbb{R}$.

D Si (x_n) converge dans $\mathbb{Q}$, alors (x_n) est bornée.

E Si (x_n) converge dans $\mathbb{R}$, alors (x_n) converge dans $\mathbb{Q}$.

Question 8. Soient x et y deux réels quelconques.

A $|x-y| \leqslant |x| + |y|$.

B $|x| - |y| \leqslant |x-y|$.

C $|x-y| \leqslant \big|\, |x| - |y| \,\big|$.

D $|x+y| < |x| + |y|$.

E $|x+y| < |x-y| + 2|y|$.

Question 9. Soit $x \in \mathbb{R}^+ \setminus \mathbb{N}$ un réel positif non entier.

A $\lfloor -x \rfloor = -\lfloor x \rfloor$.

B $\lfloor 1-x \rfloor = -\lfloor x \rfloor$.

C $x + D(x) = \lfloor x \rfloor$.

D $D(2-x) = 2 - D(x)$.

E $D(-x) = 1 - D(x)$.

Question 10.

A $\mathbb{Q}$ est un corps archimédien.

B Tout corps archimédien contient $\mathbb{Q}[\sqrt{2}]$.
C Tout corps archimédien complet est isomorphe à $\mathbb{R}$.
D Dans un corps archimédien, toute partie non vide et majorée possède une borne supérieure.
E Tout corps totalement ordonné est archimédien.

Réponses : 1–DE 2–AE 3–BD 4–CE 5–AD 6–BC 7–CD 8–AB 9–BE 10–AC

2.4 Devoir

Essayez de bien rédiger vos réponses, sans vous reporter ni au cours, ni au corrigé. Si vous souhaitez vous évaluer, donnez-vous deux heures ; puis comparez vos réponses avec le corrigé et comptez un point pour chaque question à laquelle vous aurez correctement répondu.

Questions de cours :

1. Énoncer la définition d'un triplet naturel.
2. Démontrer que si $(O_1, \mathcal{N}_1, s_1)$ et $(O_2, \mathcal{N}_2, s_2)$ sont deux triplets naturels, il existe une unique application bijective $f_{12} : \mathcal{N}_1 \to \mathcal{N}_2$ telle que :
$$f_{12}(O_1) = O_2 \quad \text{et} \quad f_{12} \circ s_1 = s_2 \circ f_{12} \, .$$
3. Énoncer la définition de la relation $\leqslant$ sur $\mathbb{N}$.
4. Démontrer que $\leqslant$ est une relation d'ordre sur $\mathbb{N}$.
5. Démontrer que toute partie non vide de $\mathbb{N}$ possède un plus petit élément.
6. Démontrer que $\mathbb{N}$ n'admet pas de plus grand élément.
7. Démontrer que toute partie non vide et majorée de $\mathbb{N}$ possède un plus grand élément.

Exercice 1 : On appelle *ensemble naturel* le couple formé d'un ensemble non vide $\mathcal{N}$ et d'une relation d'ordre $\prec$ sur $\mathcal{N}$, qui vérifie les trois propriétés suivantes.

- (O_1) toute partie non vide de $\mathcal{N}$ possède un plus petit élément ;
- (O_2) toute partie non vide et majorée de $\mathcal{N}$ possède un plus grand élément ;
- (O_3) l'ensemble $\mathcal{N}$ n'admet pas de plus grand élément.

Nous avons montré que $(\mathbb{N}, \leqslant)$ est un ensemble naturel : la définition n'est donc pas vide. Dans ce qui suit, $(\mathcal{N}, \prec)$ désigne un ensemble naturel quelconque.

1. Montrer que $(\mathcal{N}, \prec)$ possède un plus petit élément. On le notera O.
2. Montrer que $(\mathcal{N}, \prec)$ est totalement ordonné.
3. Soit $a \in \mathcal{N}$, on appelle *successeur* de a un élément $b \in \mathcal{N}$ qui vérifie $a \prec b$, $a \neq b$ et tel qu'il n'existe aucun élément $n \in \mathcal{N}$ distinct de a et de b qui vérifie $a \prec n \prec b$. Montrer que tout élément a de $\mathcal{N}$ possède un unique successeur. On le note $s(a)$.

4. On considère l'application s qui à a associe $s(a)$. Montrer que s est une application strictement croissante
5. Montrer que s est une bijection de $\mathcal{N}$ sur $\mathcal{N} \setminus \{O\}$.
6. Soit A une partie de $\mathcal{N}$ telle que :
   i) $O \in A$
   ii) $s(A) \subset A$.
   Montrer que $A = \mathcal{N}$.
7. En déduire que $(O, \mathcal{N}, s)$ est un triplet naturel.

Exercice 2 : On suppose connue une définition de l'ensemble $\mathbb{R}$ des nombres réels, indépendante des autres ensembles de nombres. Le but de l'exercice est d'en déduire une définition de l'ensemble des entiers. On appelle *partie inductive* de $\mathbb{R}$ tout sous-ensemble U de $\mathbb{R}$ contenant 0 et tel que :

$$\forall u \in \mathbb{R}\,, \quad (u \in U) \implies ((u+1) \in U)\,.$$

1. Montrer que $\mathbb{R}^+$ est une partie inductive de $\mathbb{R}$.
2. Soit K un sous-anneau de $\mathbb{R}$. Montrer que K est une partie inductive de $\mathbb{R}$.
3. Soit $\{U_i\,,\ i \in I\}$ une famille de parties inductives de $\mathbb{R}$. Montrer que $\bigcap_{i \in I} U_i$ est une partie inductive de $\mathbb{R}$.
4. On note $\mathcal{N}$ l'intersection de toutes les parties inductives de $\mathbb{R}$, et s l'application de $\mathbb{R}$ dans $\mathbb{R}$ qui à x associe $x+1$. Montrer que $s(\mathcal{N}) = \mathcal{N} \setminus \{0\}$.
5. Soit A une partie de $\mathcal{N}$ telle que $0 \in A$ et $s(A) \subset A$. Montrer que $A = \mathcal{N}$.
6. En déduire que $(0, \mathcal{N}, s)$ est un triplet naturel.

2.5 Corrigé du devoir

Questions de cours :

1. On appelle *triplet naturel* un triplet $(O, \mathcal{N}, s)$, où $\mathcal{N}$ est un ensemble, O un élément de $\mathcal{N}$ et s une application de $\mathcal{N}$ dans $\mathcal{N}$ qui vérifie les trois axiomes de Peano :
   (P_1) s est injective,
   (P_2) $s(\mathcal{N}) = \mathcal{N} \setminus \{O\}$,
   (P_3) Si A est une partie de $\mathcal{N}$ telle que si $O \in A$ et $s(A) \subset A$ alors $A = \mathcal{N}$.
2. L'application f_{12} est définie pour O_1, puisque $f_{12}(O_1) = O_2$. Si elle est définie pour $x \in \mathcal{N}_1$, alors elle est définie pour $s_1(x)$ par $f_{12}(s_1(x)) = s_2(f_{12}(x))$. D'après l'axiome de récurrence, f_{12} est donc définie pour tout $x \in \mathcal{N}_1$. De même, en permutant les indices 1 et 2, on définit f_{21} sur $\mathcal{N}_2$ par $f_{21}(O_2) = O_1$ et $f_{21}(s_2(y)) =$

$s_1(f_{21}(y))$. Considérons sur $\mathcal{N}_1$ la propriété $f_{21}(f_{12}(x)) = x$. Elle est vraie pour $x = O_1$. Supposons qu'elle soit vraie pour x, alors :

$$f_{21}(f_{12}(s_1(x))) = f_{21}(s_2(f_{12}(x))) = s_1(f_{21}(f_{12}(x))) = s_1(x) \ .$$

Par l'axiome de récurrence, la propriété est vraie pour tout x : les applications f_{12} et f_{21} sont réciproques l'une de l'autre et elles sont donc bijectives.

3. La relation $\leqslant$ est définie à partir de l'addition par :

$$\forall (a,b) \in \mathbb{N}^2 \ , \quad (a \leqslant b) \iff \Big(\exists c \in \mathbb{N} \, , \ b = a + c \Big) \ .$$

4. La relation $\leqslant$ est :
   - *réflexive* car pour tout $a \in \mathbb{N}$, $a + 0 = a$, donc $a \leqslant a$.
   - *antisymétrique* car si $a \leqslant b$ et $b \leqslant a$, alors il existe $c, d \in \mathbb{N}$ tels que $b = a + c$ et $a = b + d$. Par conséquent $b = (b + d) + c$ et puisque $+$ est associative et que tout élément est régulier pour $+$, on en déduit $d + c = 0$, ce qui entraîne $c = d = 0$ (propriété de l'addition), soit $a = b$.
   - *transitive* car si $a \leqslant b$ et $b \leqslant c$, alors il existe $d, e \in \mathbb{N}$ tels que $b = a + d$ et $c = b + e$. Par conséquent $c = (a + d) + e = a + (d + e)$ car $+$ est associative, donc $a \leqslant c$.

5. Pour tout $a \in \mathbb{N}$, $0 + a = a$: il s'ensuit que $0 \leqslant a$, donc 0 est le plus petit élément de $\mathbb{N}$. Soit A une partie non vide de $\mathbb{N}$. Si A contient 0, alors 0 est le plus petit élément de A. Sinon, notons B l'ensemble des minorants de A n'appartenant pas à A :

$$B = \{ \, b \in \mathbb{N} \setminus A \, , \ b \leqslant a \, , \ \forall a \in A \, \} \ .$$

L'ensemble B contient 0. D'après l'axiome de récurrence, si pour tout $b \in B$, $s(b)$ appartenait à B, alors B serait égal à $\mathbb{N}$ et A serait vide, ce qui est exclu. Donc il existe $b \in \mathbb{B}$ tel que $s(b) \in A$. Nous allons vérifier que $\forall a \in A$, $s(b) \leqslant a$, ce qui entraîne que $s(b)$ est le plus petit élément de A. Soit a un élément quelconque de A. Par définition de B, $b \leqslant a$, donc il existe $c \in \mathbb{N}$ tel que $a = b + c$. Or $c \neq 0$ car $b \notin A$, donc $b \neq a$. Donc il existe d tel que $c = s(d) = d + 1$. Donc $a = b + (d + 1) = (b + 1) + d = s(b) + d$, soit $s(b) \leqslant a$.

6. Supposons que $\mathbb{N}$ possède un plus grand élément N. Alors $s(N) = N + 1$ vérifie $N \leqslant s(N)$, par définition de la relation d'ordre, et comme N est le plus grand élément de $\mathbb{N}$, $s(N) \leqslant N$ et donc $N = s(N)$, c'est-à-dire $N = N + 1$ et par régularité de N pour l'addition $0 = 1 = s(0)$, ce qui est faux car s est injective.

7. Soit A une partie non vide, majorée de $\mathbb{N}$. Si b est un majorant de A, alors pour tout $a \in A$, il existe $c \in \mathbb{N}$ tel que $b = a + c$, donc $s(b) = a + (c + 1)$: $s(b)$ est aussi un majorant de A. Par l'axiome de récurrence, l'ensemble des majorants de A, contient $\{b + c \, , \ c \in \mathbb{N}\}$. Or cet ensemble n'est pas majoré, car $\mathbb{N}$ ne l'est pas, donc

il ne peut pas être inclus dans A : il existe un majorant de A qui n'appartient pas à A. Notons B l'ensemble des majorants de A n'appartenant pas à A :

$$B = \{\, b \in \mathbb{N} \setminus A\,,\ a \leqslant b\,,\ \forall a \in A \,\}\,.$$

Puisque cet ensemble est non vide, il possède un plus petit élément : notons-le b. Le plus petit élément de B est non nul, car A est non vide. Il existe donc c tel que $b = s(c)$. Nous devons montrer que c est le plus grand élément de A, c'est-à-dire que c'est un majorant, et qu'il appartient à A. Puisque $s(c) \in B$, $a \leqslant s(c)$ et $a \neq s(c)$ pour tout $a \in A$. Si $a \in A$, il existe donc $d \in \mathbb{N}^*$ tel que $s(c) = a + d$, avec $d = s(e) = e + 1$ et par conséquent, grâce à l'associativité de l'addition, $c + 1 = a + (e + 1) = (a + e) + 1$ et, par régularité de 1 pour $+$, $c = a + e$, soit $a \leqslant c$. Mais alors $c \in A$ car sinon il serait dans B ce qui contredirait la définition de b comme plus petit élément de B, puisque $b = s(c)$.

Exercice 1 :

1. $\mathcal{N}$ est non vide, donc il possède un plus petit élément d'après (O_1).
2. Pour tout $(a, b) \in \mathcal{N}$, l'ensemble $\{a, b\}$ possède un plus petit élément, d'après (O_1). Donc $a \prec b$ ou $b \prec a$: l'ordre $\prec$ est total.
3. Considérons l'ensemble A des majorants stricts de a :

   $$A = \{\, b \in \mathcal{N} \setminus \{a\}\,,\ a \prec b\,\}\,.$$

   Si A était vide, puisque l'ordre $\prec$ est total, a serait un majorant de $\mathcal{N}$, ce qui est impossible d'après (O_3). Donc A est non vide, et admet un plus petit élément d'après (O_1). Notons-le b. Par construction, $a \prec b$ et $a \neq b$. Soit $n \in \mathcal{N}$ tel que $a \prec n \prec b$ et $n \neq a$. Alors $n \in A$ et donc $b \prec n$ puisque b est le plus petit élément de A. Donc $n = b$. Reste à montrer l'unicité. Soient b_1 et b_2 deux éléments de $\mathcal{N}$ qui répondent à la définition : il n'existe aucun $n \in \mathcal{N}$ tel que $a \prec n \prec b_1$ avec $n \neq a$ et $n \neq b_1$. Puisque $a \prec b_2$ et $a \neq b_2$, cela entraîne que $b_1 \prec b_2$ (car l'ordre est total). Par symétrie, $b_2 \prec b_1$, donc $b_1 = b_2$.
4. Supposons $a \prec b$ et $a \neq b$. Alors $s(a) \prec b$ car $s(a)$ est le plus petit des majorants stricts de a. Or $b \leqslant s(b)$ par définition de s, donc $s(a) \prec s(b)$ car $\prec$ est transitive. Si $s(b)$ était égal à $s(a)$, alors on aurait $a \prec b \prec s(a)$ avec $a \neq b$ et $b \neq s(a)$, ce qui est exclu. Donc $s(b) \neq s(a)$: s est strictement croissante.
5. Comme s est strictement croissante, elle est injective, et il suffit de montrer que $s(\mathcal{N}) = \mathcal{N} \setminus \{O\}$. Commençons par vérifier que O n'est le successeur d'aucun élément de $\mathcal{N}$. Soit a tel que $s(a) = O$. Alors $a \prec O$ par définition de s, donc $a = O$ car O est le plus petit élément de $\mathcal{N}$. Ceci contredit la définition de s. Nous devons maintenant montrer que pour tout élément a de $\mathcal{N}$ différent de O, il existe $b \in \mathcal{N}$, tel que $a = s(b)$. Considérons pour cela l'ensemble des minorants stricts de a :

   $$B = \{\, b \in \mathbb{N} \setminus \{a\}\,,\ b \prec a\,\}\,.$$

Puisque $a \neq O$, B contient O. C'est donc un sous-ensemble non vide de $\mathcal{N}$, majoré par a. Par (O_2), il possède un plus grand élément. Notons-le b. Nous devons prouver que $s(b) = a$. Par construction, $b \prec a$ et $b \neq a$. Soit n tel que $b \prec n \prec a$ avec $n \neq a$. Par définition $n \in B$, donc $n \prec b$ car b est le plus grand élément de B. Donc $n = b$. Par définition de s, $s(b) = a$.

6. Notons B le complémentaire de A, et supposons B non vide. D'après (O_1), B possède un plus petit élément. Notons-le b. Nécessairement $b \neq O$ car $O \in A$. Donc il existe $a \in \mathcal{N}$ tel que $b = s(a)$. Par définition de s, $a \neq b$ et $a \prec b$. Puisque b est le plus petit élément de B, $a \notin B$, donc $a \in A$. Mais l'hypothèse entraîne que $s(a) \in A$, ce qui contredit la définition de b. Donc B est vide et $A = \mathcal{N}$.
7. Nous avons montré que s est injective à la question 4, que $s(\mathcal{N}) = \mathcal{N} \setminus \{0\}$ à la question 5, et que l'axiome de récurrence est vérifié à la question 6. Le triplet $(O, \mathcal{N}, s)$ vérifie les 3 axiomes de Peano, c'est donc un triplet naturel.

Exercice 2 :

1. En supposant que $\mathbb{R}$ a été défini, et muni de sa relation d'ordre total $\leqslant$ compatible avec l'addition, alors 0 (élément neutre pour l'addition) est inférieur ou égal à 1 (élément neutre pour la multiplication). Donc pour tout $x \in \mathbb{R}^+$,

$$0 \leqslant x = x + 0 \leqslant x + 1 \ ,$$

donc $\mathbb{R}^+$ est une partie inductive.

2. Si K est un sous-anneau de $\mathbb{R}$, il contient les éléments neutres pour l'addition et la multiplication, 0 et 1. Pour tout $x \in K$, $x + 1 \in K$, car K est stable pour l'addition : K est une partie inductive.
3. Si x appartient à chacun des U_i, alors $x + 1$ appartient à chacun des U_i, donc à leur intersection.
4. Par définition, si U est une partie inductive de $\mathbb{R}$, alors $s(U) \subset U$. En particulier, $s(\mathcal{N}) \subset \mathcal{N}$ puisque l'intersection de toutes les parties inductives est une partie inductive d'après la question précédente. Si $s(\mathcal{N})$ contenait 0, ce serait une partie inductive, donc $s(\mathcal{N})$ serait égal à $\mathcal{N}$ d'après la définition de $\mathcal{N}$. Dans ce cas, $\mathcal{N}$ contiendrait le sous-anneau de $\mathbb{R}$ engendré par 0 et 1. Mais d'après les questions 1, 2 et 3, l'intersection de ce sous-anneau avec $\mathbb{R}^+$ est encore une partie inductive, qui contient donc $\mathcal{N}$: c'est une contradiction. Donc $s(\mathcal{N}) \subset \mathcal{N} \setminus \{0\}$. Réciproquement, soit $x \in \mathcal{N} \setminus \{0\}$ tel que $x \notin s(\mathcal{N})$. Alors $\mathcal{N} \setminus \{x\}$ contient 0 et $s(\mathcal{N} \setminus \{x\}) \subset \mathcal{N} \setminus \{x\}$: c'est une partie inductive strictement incluse dans $\mathcal{N}$, ce qui contredit la définition de $\mathcal{N}$. Donc $s(\mathcal{N}) = \mathcal{N} \setminus \{0\}$.
5. Si $0 \in A$ et $s(A) \subset A$, alors A est une partie inductive, donc $\mathcal{N} \subset A$, par définition de $\mathcal{N}$. Si de plus $A \subset \mathcal{N}$, alors $A = \mathcal{N}$.
6. L'application s est injective (régularité de l'addition dans $\mathbb{R}$), $s(\mathcal{N}) = \mathcal{N} \setminus \{0\}$ (question 4) et l'axiome de récurrence est vérifié (question 5). Le triplet $(0, \mathcal{N}, s)$ vérifie les 3 axiomes de Peano, c'est donc un triplet naturel.

---

3 Compléments

3.1 Every Texan kills a Texan

« Aucune découverte scientifique ne porte le nom de son inventeur ». Tel est l'énoncé de la « Loi de Stigler »... qui n'a pas été découverte par Stigler ! Les axiomes de Peano ne font pas exception à la règle. Peano n'a d'ailleurs jamais prétendu être le premier : voici ce qu'on lit dans la préface de « Arithmetices Principia nova methodo exposita », daté de 1889.

> In arithmeticae demonstrationibus usus sum libro : H. Grassmann, Lehrbuch der Arithmetik, Berlin 1861.
>
> Utilius quoque niibi fuit recens scriptum : R. Dedekind, Was sind und was sollen die Zahlen ; Braunschweig, 1888, in quo quaestiones, quae ad numerorum fundamenta pertinent, acute examinantur.

Effectivement Grassmann, près de trente ans auparavant, donnait déjà essentiellement la caractérisation moderne de l'ensemble des entiers, ainsi qu'une définition inductive de l'addition de de la multiplication. Mais il ne posait pas en axiome le fait que le premier entier ne soit le successeur d'aucun autre, ni le fait que deux nombres ne puissent avoir le même successeur, ce qui était considéré comme allant de soi [1]. La définition de $\mathbb{N}$ que nous vous avons donnée est bien, à quelques détails près, celle de Dedekind, dans « Que sont les nombres et que signifient-ils ». Voici comment il en décrivait l'idée, quelques années auparavant.

> Je vois l'ensemble de l'arithmétique comme une conséquence nécessaire, ou au moins naturelle du plus simple des actes arithmétiques, celui de compter, et compter n'est rien d'autre que la création successive de la suite infinie des nombres entiers positifs dans laquelle chaque individu est défini en termes de celui qui le précède.

Dans une lettre de février 1890, il va plus loin.

> Parlant de l'arithmétique (algèbre, analyse) comme d'une partie de la logique, je veux dire que je considère le concept de nombre comme entièrement indépendant de notions ou d'intuitions d'espace et de temps, et que je le considère comme un résultat immédiat des lois de la pensée.

Quelque temps avant Dedekind, de l'autre côté de l'Atlantique, un philosophe avait lui aussi réflechi aux fondements de la notion de nombre : Charles Sanders Peirce (1839–1914) [2]. Son article se termine par l'énoncé selon lequel une application injective d'un ensemble sur lui-même est bijective. Son illustration est plutôt vigoureuse.

> From this we deduce the validity of the following mode of inference :

1. Hao Wang : The axiomatization of arithmetics, *The Journal of Symbolic Logic, (22)2, p. 145–158 (1957)*
2. C.S. Peirce : On the Logic of Number, *American Journal of Mathematics, 4(1), pp. 85–95, 1881*

> Every Texan kills a Texan,
> Nobody is killed by but one person,
> Hence, every Texan is killed by a Texan,
>
> supposing Texans to be a finite lot. For, by the first premise, every Texan killed by a Texan is a Texan killer of a Texan. By the second premise, the Texans killed by Texans are as many as the Texans killers of Texans. Whence we conclude that every Texan killer of a Texan is a Texan killed by a Texan, or, by the first premise, every Texan is killed by a Texan. This mode of reasoning is frequent in the theory of numbers.

Peirce n'était pas texan, et n'est pas mort assassiné, même si son caractère difficile et ses opinions peu orthodoxes ne lui valaient pas que des amis. Notez qu'il ne se prononce pas sur la valeur de vérité de ses propositions.

3.2 Les démons de Cantor

Nous sommes en 1871, la grande vague de rigueur mathématique, initialisée par Cauchy, et puissamment portée par l'École de Berlin, Weierstrass en tête, trouve en Georg Cantor (1845–1918) un zélateur scrupuleux. Pour Cantor, il n'est pas question de démontrer l'unicité du développement en série trigonométrique sans avoir défini auparavant ce qu'est une « grandeur numérique ». Voici comment il commence son article[3].

> Les nombres rationnels servent de fondement pour arriver à la notion plus étendue d'une grandeur numérique ; je les désignerai sous le nom de système A, en y comprenant zéro.
>
> On rencontre une première généralisation de la notion de grandeur numérique dans le cas où on a, obtenue par une loi, une série infinie de nombres rationnels :
>
> $$a_1\,,\ a_2\,,\ \ldots\,,\ a_n\,,\ \ldots\,, \tag{1}$$
>
> constituée de telle sorte que la différence $a_{n+m}-a_n$ devient infiniment petite à mesure que n croît, quel que soit le nombre positif m, ou, en d'autres termes, qu'avec ε (positif rationnel) pris arbitrairement on a un nombre entier n, tel que $(a_{n+m}-a_n)<\varepsilon$, si $n \geqslant n_1$, et si m est un nombre entier positif pris à volonté.
>
> J'exprime ainsi cette propriété de la série (1) : « La série (1) a une limite déterminée b ».
>
> Ces mots ne servent donc qu'à énoncer cette propriété de la série, sans exprimer d'abord autre chose, et de même que nous lions la série (1) avec un signe particulier b, de même on doit aussi attacher différents signes b, b', b'' à diverses séries de même espèce.

3. G. Cantor, Extension d'un théoréme de la théorie des séries trigonométriques, traduction d'un article paru aux Annales Mathématiques de Leipzich, *Acta Mathematica 2(1), pp. 336–348 (1883)*

Eh bien oui, Cantor construit les réels par les classes d'équivalence des suites de Cauchy de rationnels, comme vous l'avez vu dans ce chapitre. Mais il ne s'arrête pas en si bon chemin. Il définit par récurrence des systèmes de nombres d'ordre k en itérant le procédé, pour plus tard les identifier par un axiome aux points de la droite géométrique. Il exprime tout de même quelques scrupules par rapport au sujet de son article.

> Dans une autre circonstance je reviendrai avec plus de détail sur tous ces rapports. Ce n'est pas non plus ici le lieu d'expliquer comment les conventions et les opérations dont j'ai parlé dans ce paragraphe peuvent servir à l'analyse infinitésimale. Dans ce qui suit, en exposant le rapport des grandeurs numériques avec la géométrie de la ligne droite, je me bornerai presque exclusivement aux théorèmes nécessaires, d'où l'on peut, si je ne me trompe, déduire le reste au moyen d'une démonstration purement logique.

Ce seront encore les séries trigonométriques, et plus précisément leurs discontinuités, qui l'amèneront à travailler sur les ensembles infinis, en commençant par donner un fondement rigoureux à la notion d'ensemble. Sa réflexion sur les cardinaux infinis l'amène à se demander s'il est si évident que cela qu'il y a plus de points dans un carré que dans un segment. Voici ce qu'il écrit à son ami Dedekind, le 5 janvier 1874.

> Est-ce qu'une surface (disons un carré incluant sa frontière) peut être ramenée de façon unique à une ligne (disons un segment de droite incluant les extrémités) de sorte que pour chaque point sur la surface il y ait un point correspondant sur la ligne et, réciproquement, pour chaque point sur la ligne il y ait un point correspondant sur la surface ? Je crois qu'il ne sera pas facile de répondre à cette question, malgré le fait que la réponse semble si clairement être « non » qu'une démonstration apparaisse presque superflue.

Quand il finit par répondre « oui » en 1877, il dit « Je le vois, mais je ne le crois pas ». Ce résultat étonnant suscita le scepticisme de beaucoup de ses collègues, en particulier Kronecker. Cantor était douloureusement conscient de l'opposition que ses travaux, en particulier sur la théorie des ensembles et les cardinaux transfinis, suscitaient.

> Je réalise qu'en entreprenant cela, je me place dans une certaine opposition par rapport aux vues largement répandues sur l'infini mathématique, et aux opinions fréquemment défendues sur la nature des nombres.

Querelles avec Kronecker, Mittag-Leffler et les autres ? Problèmes psychologiques liés à son enfance ? À partir de 1884, Cantor connaît le premier d'une série d'épisodes de dépression qui ne lui laissèrent que peu de répit jusqu'à son décès. Ses efforts pour démontrer que Francis Bacon est le véritable auteur des pièces de Shakespeare ont été moins reconnus par la postérité que sa théorie des ensembles que Hilbert considérait comme « le plus beau produit du génie mathématique, et une des réalisations suprêmes de l'activité humaine purement intellectuelle ».

3.3 Pourquoi pas douze ?

L'Encyclopedia Londinensis, publiée à Londres dans les premières décennies du XIX^e^ siècle, vaut souvent son pesant de prégugés racistes, comme la plupart des écrits européens de son temps. Voici ce qu'on y lit, à l'article « Numbers » [4].

> We are told that the Guaranis and the Lulos, two of the very lowest races of savages which inhabit the boundless forests of South America, count only by fours ; at least, they express five by four-and-one, six by four-and-two, and so forth. We may gather from Aristotle, that a certain tribe of Thracians were accustomed to use the quaternary scale of numeration ; for he says that they proceeded no farther than four, which they would doubtless continue to repeat. If such was the historical fact, those simple people must have never advanced beyond the early practice of reckoning successively by *casts* or *warps*. It seems probable that Pythagoras was acquainted with the quaternary system, which he brought from Egypt and India. Hence perhaps the mystical veneration which the followers of that philosopher professed to entertain for the *tetractys*, or quaternion, the root of the scale, which contains besides, within itself, the number denoting the elementary musical proportions. Near the end of the seventeenth century, Weigelius seriously proposed, in Germany, the adoption of the *tetraetic* or *quaternary* numeration, which he explained, with copious detail, in a learned work, entitled *Aretologistica*, printed at Nuremberg in 1687. This writer even goes so far as to invent names for the several orders of his *Tetractic system*. They will appear to have a sufficiently German air, though not harsher than the terms we now use.
>
> [. . .]
>
> Mr. Barlow and Mr. Lessie have scarcely noticed the octary scale of numbers ; but this system has been revived or rather newly-modelled, by a Mr Richardson, of Churchill in Somersetshire ; an ingenious gentleman who, we are sorry to say, has been for many years totally blind. The title of his pamphlet, which lies before us, is "Octary Arithmetic, or the Art of Doubling and Halving by the Cypher ; containing a perfect system of measure and weight, with specimens of the new logarithms" (Lond. 1817).
>
> [. . .]
>
> Mr. Richardson's idea is original and bold ; but his style is obscure, and the new names and phrases that he introduces are not very harmonious. Moreover, the complete revolution which the introduction (or indeed of any other) would make in all books, rules, weights, measures, and systems of education, makes us less sanguine than the author as to its ultimate success.

Des "ingenious gentlemen", peu avares de propositions originales et hardies, il n'en a jamais manqué pour prôner l'adoption généralisée d'autres bases que la base 10 à la fois

4. J. Wilkes : Encyclopedia Londinensis, Vol. XVII, *London, 1820*

pour l'arithmétique, pour les mesures et pour les monnaies. Il faut dire que selon les domaines, certains comptes se sont toujours faits tantôt en base 60 (heures, minutes et secondes ou bien mesures angulaires), tantôt en base 12 (œufs, huîtres, ...). Jusqu'au "Decimal Day" (15 février 1971), une livre britannique se composait de 20 shillings, eux-mêmes divisés en 12 pence. Il y a toujours 12 inches dans un foot et 3 feet dans un yard. Pour nous qui sommes habitués à la simplicité du système métrique, il est difficile d'imaginer le casse-tête pour convertir des inches cubiques en yards cubiques. Pour autant, des tentatives pour imposer le système métrique en Grande-Bretagne ou aux États-Unis échouent régulièrement.

Ce système, basé sur une division en puissances de dix de toutes les unités de mesure, a été créé sous la Révolution. Son acte fondateur est un « Rapport fait à l'Académie des Sciences le 27 octobre 1790 sur le titre des métaux monnayés & sur l'échelle de division des poids, des mesures et des monnaies, par MM. Borda, Lagrange, Lavoisier, Tillet & Condorcet ». Voici ce qu'on y lit.

> L'adoption de l'échelle arithmétique pour toutes les divisions, diminuera beaucoup les embarras qui doivent naître de l'établissement des nouvelles mesures, & tous ceux qui sauront l'arithmétique simple, pourront en calculer toutes les divisions, tandis que ceux qui savent calculer les anciennes n'éprouveront aucun embarras, puisqu'ils pourront calculer les nouvelles avec encore plus de facilité.
>
> On aurait pu proposer de changer aussi l'échelle arithmétique, & de prendre l'échelle duocécimale, c'est-à -dire, celle qui emploie onze chiffres, & qui suit la progression des puissances de douze ; mais ce changement ajouté à tous les autres, en ôtant à ceux qui ne sont pas accoutumés au calcul, une base à laquelle ils puissent entendre les changements & s'y conformer, en rendroit le succès presqu'impossible. Ajoutons que non-seulement il faudroit deux chiffres nouveaux, mais que l'arithmétique parlée a pour base l'arithmétique décimale, ce qui obligeroit à la changer encore, de manière que les effets de tous ces changements réunis, incommodes aux personnes les plus habituées à réfléchir, seroient insupportables à toutes les autres.
>
> Nous conclurons donc que l'échelle décimale doit servir de base à toutes les divisions, & que même le succès de l'opération générale sur les poids & mesures tient en grande partie à l'adoption de cette échelle.

Cette décision de bon sens n'alla pas semble-t-il sans quelques débats houleux, les partisants de la base 12 et du changement radical étant nombreux et passionnés. Quatre ans plus tard, quand Pierre-Simon de Laplace (1749–1827) inaugure ses leçons de Mathématiques à l'École Normale par un cours d'arithmétique, on y sent pointer quelques regrets.

> Vous concevez, par les principes métaphysiques sur lesquels est fondé notre système de numération, que rien n'obligeait de s'en tenir à dix caractères ; on pouvait en employer plus ou moins.

> Il paraît très probable que le nombre des doigts est ce qui a déterminé l'arithmétique décimale. Les hommes primitivement ont compté par leurs doigts jusqu'à dix ; mais de ce que cette arithmétique était bonne dans l'enfance des sociétés, est-elle maintenant la meilleure ? C'est ce que nous allons examiner. [...] De tous les systèmes de numération, le meilleur est celui qui, n'employant pas un trop grand nombre de caractères, renferme dans son échelle, le plus grand nombre de diviseurs ; et, à cet égard, le système *duodécimal* me paraît mériter la préférence. Il eût suffi d'ajouter deux caractères aux nôtres ; on aurait eu l'avantage d'exprimer le tiers et le quart de l'unité principale, au moyen des divisions de ce système, ce qui eût été très-commode. C'est pour cela que les divisions de presque toutes nos mesures sont duodécimales ; ainsi le pied se divise en douze pouces, le pouce en douze lignes, etc.
>
> La commission des poids et mesures a balancé les avantages qu'offre le système duodécimal, avec l'inconvénient de changer totalement, et l'arithmétique écrite, et l'arithmétique parlée, et nos livres et nos tables formées sur le système décimal. Elle a craint qu'en proposant le système duodécimal, les obstacles qu'éprouverait l'introduction de ce système, ne se joignissent à ceux que présenterait déjà l'institution du nouveau système de poids et mesures. Elle a donc jugé à propos de conserver l'arithmétique décimale.

Il avait apparemment fallu toute l'autorité du « plus illustre géomètre du temps », Joseph-Louis Lagrange (1746–1813) pour emporter la décision. Jean-Baptiste Delambre (1749–1822), qui avait durement payé de sa personne en triangulant un arc de méridien depuis Barcelone pour établir la valeur du mètre, se souvient bien des années plus tard de ces débats passionnés [5].

> La Révolution offrit aux savants l'occasion d'une grande et difficile innovation : l'établissement d'un système métrique, fondé sur la nature, et parfaitement analogue à notre échelle de numération. Lagrange fut un des Commissaires que l'Académie chargea de ce travail ; il en fut un des ardents promoteurs ; il voulait le système décimal dans toute sa pureté ; il ne pardonnait pas à Borda l'idée qu'il avait eue de faire exécuter des quarts de mètre. Il était peu frappé de l'objection que l'on tirait contre ce système du petit nombre des diviseurs de sa base. Il regrettait presque qu'elle ne fût pas un nombre premier, tel que 11, qui nécessairement eût donné un même dénominateur à toutes les fractions. On regardera, si l'on veut, cette idée comme une de ces exagérations qui échappent aux meilleurs esprits dans le feu de la dispute ; mais il n'employait ce nombre 11 que pour écarter le nombre 12, que des novateurs plus intrépides auraient voulu substituer à celui de 10, qui fait partout la base de la numération.

5. J.B.J. Delambre : Mémoire sur la vie et les ouvrages de M. Le Comte J.-L. Lagrange *in Oeuvres de Lagrange, J.-A. Serret ed., Tome 1, Paris 1867*

Si le cœur vous en dit, n'hésitez pas à reprendre le flambeau, vous ne serez pas seuls : www.dozenal.org

3.4 Et après ?

À partir des entiers naturels, nous avons construit les entiers relatifs, puis les rationnels, les réels, les complexes, chaque nouvel ensemble ainsi construit incluant les précédents. L'histoire ne s'arrête pas là. Le corps des complexes est en même temps un espace vectoriel de dimension 2 sur $\mathbb{R}$: on appelle cela une *algèbre*. Existe-t-il d'autres algèbres commutatives sur $\mathbb{R}$? Non ! La réponse a été donnée par Weierstrass en 1863 : toute algèbre commutative de dimension finie sur $\mathbb{R}$ est isomorphe à $\mathbb{C}$. Nous vous avons proposé en exercice plusieurs constructions du corps des *quaternions*, qui est à la fois une algèbre de dimension 4 sur $\mathbb{R}$, et de dimension 2 sur $\mathbb{C}$. La multiplication des quaternions a beau n'être pas commutative, $\mathbb{H}$ n'en est pas moins un corps. En existe-t-il d'autres ? Non ! La réponse a été donnée par Frobenius en 1877 : toute algèbre de dimension finie sur $\mathbb{R}$ est isomorphe à $\mathbb{R}$, $\mathbb{C}$ ou $\mathbb{H}$. Cela n'empêche toujours pas de continuer : les *octonions* sont un espace vectoriel de dimension 8 sur $\mathbb{R}$, 4 sur $\mathbb{C}$ et 2 sur $\mathbb{H}$. On y définit une « multiplication », qui n'est pas commutative, ni même associative. Cette multiplication permet les calculs d'inverses, donc la division. On y étend aussi la notion de module : le produit d'un octonion par son conjugué est un réel positif, et la racine carrée de ce réel est une norme sur l'espace vectoriel des octonions $\mathbb{O}$. On appelle cela une « algèbre de division normée ». En existe-t-il d'autres ? Non ! La réponse a été donnée par Hurwitz en 1898 : toute algèbre de division normée sur $\mathbb{R}$ est isomorphe à $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ ou $\mathbb{O}$. Alors on arrête là ? Non, toujours pas : les *sedenions* sont un espace vectoriel de dimension 16 sur $\mathbb{R}$, 8 sur $\mathbb{C}$, etc. etc.

Ces ensembles de nombres dits hypercomplexes, datent de la première moitié du XIX^e^ siècle. Les quaternions ont une date de naissance précise, le 16 octobre 1843. Sir William Rowan Hamilton (1805–1865) a donné plusieurs récits de son « étincelle ». Celui qui figure dans la lettre qu'il écrit à un de ses fils le 15 octobre 1858 est particulièrement émouvant.

> If I may be allowed to speak of myself in connexion with the subject, I might do so in a way which would bring you in, by referring to an ante-quaternionic time, when you were a mere child, but had caught from me the conception of a Vector, as represented by a Triplet : and indeed I happen to be able to put the finger of memory upon the year and month – October, 1843 – when having recently returned from visits to Cork and Parsonstown, connected with a meeting of the British Association, the desire to discover the laws of the multiplication referred to regained with me a certain strength and earnestness, which had for years been dormant, but was then on the point of being gratified, and was occasionally talked of with you. Every morning in the early part of the above-cited month, on my coming down to breakfast, your (then) little brother William Edwin, and yourself, used

> to ask me, "Well, Papa, can you multiply triplets" ? Whereto I was always obliged to reply, with a sad shake of the head : "No, I can only add and subtract them."
>
> But on the 16th day of the same month – which happened to be a Monday, and a Council day of the Royal Irish Academy – I was walking in to attend and preside, and your mother was walking with me, along the Royal Canal, to which she had perhaps driven ; and although she talked with me now and then, yet an under-current of thought was going on in my mind, which gave at last a result, whereof it is not too much to say that I felt at once the importance. An electric circuit seemed to close ; and a spark flashed forth, the herald (as I foresaw, immediately) of many long years to come of definitely directed thought and work, by myself if spared, and at all events on the part of others, if I should even be allowed to live long enough distinctly to communicate the discovery. Nor could I resist the impulse – unphilosophical as it may have been – to cut with a knife on a stone of Brougham Bridge, as we passed it, the fundamental formula with the symbols, i, j, k ; namely,
>
> $$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{ijk} = -1 \ .$$
>
> which contains the Solution of the Problem, but of course, as an inscription, has long since mouldered away. A more durable notice remains, however, on the Council Books of the Academy for that day (October 16th, 1843), which records the fact, that I then asked for and obtained leave to read a Paper on Quaternions, at the First General Meeting of the session : which reading took place accordingly, on Monday the 13th of the November following.

Les travaux de Hamilton sur la multiplication des vecteurs avaient été inspirés par ses discussions avec son ami John Thomas Graves (1806–1870), à qui il s'empressa de faire part de sa découverte. Le 26 décembre 1843, la réponse de Graves contenait une construction à base de couples de quaternions : les octonions. Deux ans plus tard, Cayley publiait essentiellement la même contruction, et donnait le moyen de l'étendre aux dimensions supérieures. Oui, vous avez bien suivi ces compléments, et il n'y a pas d'erreur de date. Les octonions ont été définis avant les réels, et les réels avant les entiers. Ainsi vont l'histoire et la pédagogie des mathématiques : il est rare que les notions aient été découvertes dans l'ordre où elles vous sont présentées.