Chapitre 4

CONSTRUCTION DES NOMBRES RÉELS

Version du 8 février 2002

4.1 Partitions

DEFINITION Soit X un ensemble. Une famille $(X_j)_{j\in J}$ de parties non-vides de X s'appelle une *partition* de X si

$$X = \bigcup_{j\in J} X_j$$

et si, pour tout $k, l \in J$,

$$k \neq l \quad \Longrightarrow \quad X_k \cap X_l = \emptyset \ .$$

EXEMPLE Soit $f : X \longrightarrow Y$ une application. Alors

$$\left(\overset{-1}{f}(\{y\})\right)_{y\in f(X)}$$

est une partition de X .

Il est clair que $\overset{-1}{f}(\{y\}) \neq \emptyset$ si $y \in f(X)$ et on a

$$\bigcup_{y\in f(X)} \overset{-1}{f}(\{y\}) = X$$

car, pour tout $x \in X$, on a $x \in \overset{-1}{f}(\{f(x)\})$. D'autre part, pour tout $y, z \in f(X)$, si

$$x \in \overset{-1}{f}(\{y\}) \cap \overset{-1}{f}(\{z\}) \ ,$$

on a $y = f(x) = z$, d'où le résultat par contraposition. □

PROPOSITION *Soit $f : X \longrightarrow Y$ une application surjective. Il existe une application injective $g : Y \longrightarrow X$ telle que*

$$f \circ g = \mathrm{id}_Y \ .$$

Puisque f est surjective, pour tout $y \in Y$, on a $\overset{-1}{f}(\{y\}) \neq \emptyset$. D'après l'axiome du choix 2.8 il existe

$$g \in \prod_{y\in Y} \overset{-1}{f}(\{y\}) \subset X^Y \ .$$

Pour tout $y \in Y$, on a alors $f(g(y)) = y$, d'où notre assertion. □

4.2 Relations d'équivalence

DEFINITION 1 Soient X un ensemble et $R \subset X \times X$. On dit que R est une *relation d'équivalence* si, pour tout $x, y, z \in X$, on a

(a) *Transitivité*
$$x \; R \; y \quad \text{et} \quad y \; R \; z \quad \Longrightarrow \quad x \; R \; z$$

(b) *Symétrie*
$$x \; R \; y \Leftrightarrow y \; R \; x$$

(c) *Réflexivité*
$$x \; R \; x \ .$$

On écrit souvent $x \equiv y \mod R$ à la place de $x \; R \; y$, et on pose
$$[x] := \{y \in X \mid x \; R \; y\} \quad , \quad X/R := \{[x] \in \mathfrak{P}(X) \mid x \in X\} \ ,$$
ainsi que
$$p : X \longrightarrow X/R : x \longmapsto [x] \ .$$
On dit que $[x]$ est la *classe d'équivalence* de x et que p est l' *application quotient* de X sur l' *espace quotient* X/R .

PROPOSITION *Pour tout* $x, y \in X$ *, on a*

(i)
$$y \in [x] \quad \Longleftrightarrow \quad x \; R \; y \ .$$

(ii)
$$([x] = [y] \ \text{ et } x \; R \; y) \quad \text{ou} \quad ([x] \cap [y] = \emptyset \ \text{ et } \neg x \; R \; y) \ .$$

(iii)
$$\overset{-1}{p}(\{[x]\}) = [x] \ .$$

Démonstration de (i) C'est évident.

Démonstration de (ii) Il nous suffit de montrer que
$$[x] \cap [y] \neq \emptyset \Longrightarrow [x] = [y] \ .$$
Soit alors $z \in [x] \cap [y]$ et $u \in [x]$, i.e.
$$x \; R \; z \quad , \quad y \; R \; z \quad \text{et} \quad x \; R \; u \ .$$
Par symétrie il vient
$$y \; R \; z \quad , \quad z \; R \; x \quad \text{et} \quad x \; R \; u \ ,$$
donc $y \; R \; u$ par transitivité. Ceci prouve que $u \in [y]$, donc que $[x] \subset [y]$. L'autre inclusion s'obtient en échangeant x et y .

Démonstration de (iii) On a
$$\overset{-1}{p}(\{[x]\}) = \{y \in X \mid \ [y] = [x]\} = \{y \in X \mid x \; R \; y\} = [x] \ .$$
□

DEFINITION 2 On dit que $\left(\overset{-1}{p}(\{c\})\right)_{c \in X/R}$ est la partition de X en classes d'équivalence $\operatorname{mod} R$. Tout $x \in \overset{-1}{p}(c)$ s'appelle un *représentant* de la classe d'équivalence c .

4.3 Groupes

DEFINITION 1 Soit G un ensemble muni d'une opération associative

$$\cdot : G \times G \longrightarrow G : (s,t) \longmapsto s \cdot t \ .$$

On dit que G est un *groupe* si

(g_1) Il existe $e \in G$ tel que, pour tout $s \in G$, on ait

$$e \cdot s = s \cdot e = s \ .$$

(g_2) Pour tout $s \in G$, il existe $t \in G$ tel que

$$s \cdot t = t \cdot s = e \ .$$

Un groupe G est dit *commutatif* ou *abélien* si, pour tout $s, t \in G$, on a

$$s \cdot t = t \cdot s \ .$$

REMARQUE 1 Soit G un groupe.

(a) Un élément e satisfaisant à (g_1) est univoquement déterminé et s'appelle l' *élément neutre* de G .

En effet si $e' \in G$ satisfait aussi à (g_1) , on a

$$e' = e' \cdot e = e \ .$$

$\square$

(b) Soit $s \in G$. Un élément $t \in G$ satisfaisant à (g_2) est univoquement déterminé et s'appelle l' *inverse* de s ; on le note s^{-1} . On a

$$\left(s^{-1}\right)^{-1} = s \ .$$

En effet si $t' \in G$ satisfait aussi à (g_2) , on a

$$t' = t' \cdot e = t' \cdot g \cdot t = e \cdot t = t \ .$$

La seconde partie est immédiate puisqu'on a $s \cdot s^{-1} = s^{-1} \cdot s = e$. $\square$

(c) Soient $s, t \in G$. Les équations

$$s \cdot x = t \quad \text{et} \quad x \cdot s = t$$

possèdent une et une seule solution

$$x = s^{-1} \cdot t \text{ resp. } x = t \cdot s^{-1} \ .$$

En effet

$$x = s^{-1} \cdot s \cdot x = s^{-1} \cdot t \quad \text{et} \quad x = x \cdot s \cdot s^{-1} = t \cdot s^{-1} \ .$$

$\square$

REMARQUE 2 Si l'opération est notée additivement, on note 0 l'élément neutre et on dit que l'inverse de s est son *opposé* et se note $-s$. On écrit

$$s - t := s + (-t) \ .$$

EXEMPLE L'ensemble $\mathbb{N}$ muni de l'addition n'est pas un groupe. En effet l'équation

$$x + 1 = 0$$

n'a pas de solution (dans $\mathbb{N}$), puisque

$$x + 1 > x \geqslant 0 \ .$$

DEFINITION 2 On dit qu'un groupe commutatif G , noté additivement, muni d'un ordre $\leqslant$ est un *groupe ordonné* si l'addition est compatible avec l'ordre, i.e. si pour tout $s, t, u \in G$, on a

compatibilité
$$s \leqslant t \quad \Longrightarrow \quad s + u \leqslant t + u \ .$$

On dit que s est *positif* , resp. *négatif* , si $s \geqslant 0$, resp. $s \leqslant 0$, et *strictement positif* , resp. *strictement négatif* , si $s > 0$, resp. $s < 0$.

4.4 Construction des nombres entiers relatifs

Nous allons construire un groupe additif contenant un image de $\mathbb{N}$ et dont l'addition prolonge celle de $\mathbb{N}$. Notre but est en fait de pouvoir résoudre toute équation de la forme

$$x + b = a \ .$$

Le couple (a, b) peut très bien servir comme objet mathématique représentant dans un nouveau contexte la solution de cette équation. Mais attention, le couple $(a + k, b + k)$ doit aussi représenter cette solution, puisque

$$x + b + k = a + k \quad \Longleftrightarrow \quad x + b = a$$

par la règle de simplification. Il faut en outre définir l'addition dans ce nouveau contexte.

La relation Z définie sur $\mathbb{N} \times \mathbb{N}$ par

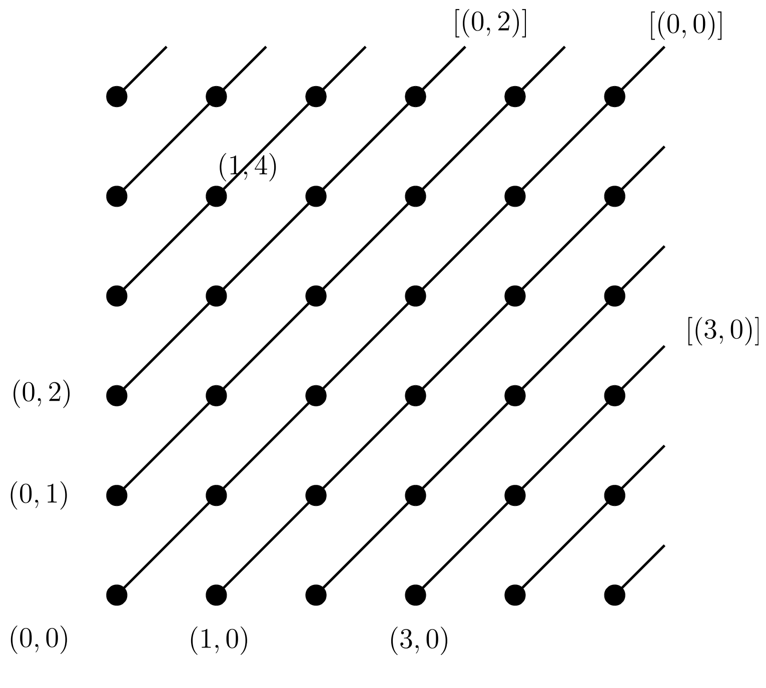
$$(a, b) \ \ Z \ \ (c, d) \quad : \quad a + d = b + c$$

est une relation d'équivalence.

DEFINITION 1 On pose

$$\mathbb{Z} := \mathbb{N} \times \mathbb{N} / \, Z \ ,$$

et on dit que c'est l' *ensemble des nombres entiers relatifs* .



Pour tout $k \in \mathbb{N}$, on a par exemple

$$[(k, 0)] = \{(c, d) \in \mathbb{N} \times \mathbb{N} \mid c = d + k\} = \{(l + k, l) \ \mid l \in \mathbb{N}\} \ \ .$$

et

$$[(0, k)] = \{(c, d) \in \mathbb{N} \times \mathbb{N} \mid d = c + k\} = \{(l, l + k) \ \mid l \in \mathbb{N}\}$$

Le deuxième terme de ces égalités donne une description externe (cf. remarque 2.5.2), le troisième une description interne (cf. remarque 2.6) de ces ensembles.

Comment définir l'addition sur $\mathbb{Z}$? Une classes d'équivalence est déterminée par les représentants qu'elle contient. Ceci nous conduit à poser la définition suivante :

DEFINITION 2 Pour tout $x, y \in \mathbb{Z}$, on définit la somme de x et y par

$$x + y := [(a + c, b + d)] \ ,$$

si $(a, b) \in x$ et $(c, d) \in y$, car cela ne dépend pas du choix des représentants de x et y d'après le

LEMME *Pour tout* $a, b, c, d, r, s, t, u \in \mathbb{N}$ *, on a*

$$(a, b) \ Z \ (r, s) \quad \textit{et} \quad (c, d) \ Z \ (t, u) \quad \Longrightarrow \quad (a + c, b + d) \ Z \ (r + t, s + u) \ .$$

En effet si $(a, b) \ Z \ (r, s)$ et $(c, d) \ Z \ (t, u)$, on a

$$a + s = b + r \quad \text{et} \quad c + u = d + t \ ,$$

donc

$$(a + c) + (s + u) = (a + s) + (c + u) = (b + r) + (d + t) = (b + d) + (r + t) \ ,$$

i.e.

$$(a + c, b + d) \ Z \ (r + t, s + u) \ .$$

□

REMARQUE 1 En d'autres termes, on a

$$[(a, b)] + [(c, d)] = [(a + c, b + d)] \ .$$

THEOREME $\mathbb{Z}$ *est un groupe commutatif, dont l'élément neutre est* $[(0, 0)]$ *. Pour tout* $a, b \in \mathbb{N}$ *, l'opposé de* $[(a, b)]$ *est* $[(b, a)]$ *.*

C'est immédiat. Par exemple, on a

$$[(a, b)] + [(b, a)] = [(a + b, b + a)] = [(0, 0)] \ .$$

□

REMARQUE 2 On identifie $\mathbb{N}$ à une partie de $\mathbb{Z}$ en considérant l'injection

$$\mathbb{N} \hookrightarrow \mathbb{Z} : n \longmapsto [(n, 0)] \ .$$

Ceci est justifié car, pour tout $m, n \in \mathbb{N}$, on a

$$[(m, 0)] + [(n, 0)] = [(m + n, 0)] \ ,$$

ce qui montre que l'addition de $\mathbb{Z}$ induit bien celle de $\mathbb{N}$.

REMARQUE 3 La classe d'équivalence $[(n, 0)]$ est désignée par n afin de simplifier les notations. De même, puisque $[(0, n)] = -[(n, 0)]$ est l'opposé de $[(n, 0)]$, la classe $[(0, n)]$ est notée $-n$.

Remarquons que tout élément de $\mathbb{Z}$ est de la forme $n = [(n,0)]$ pour un $n \in \mathbb{N}$, ou bien de la forme $-n = [(0,n)]$ pour un $n \in \mathbb{N}^*$.

En effet, pour tout $a,b \in \mathbb{N}$, on a

$$[(a,b)] = \left\{ \begin{array}{ll} [(a-b,0)] & \quad a \geqslant b \\ & \text{si} \\ [(0,b-a)] & \quad a < b \end{array} \right.$$

En outre

$$[(a,b)] = [(a,0)] + [(0,b)] = [(a,0)] + (-[(b,0)])$$

est évidemment désigné par $a - b$.

EXERCICE Soit $n \in \mathbb{N}^*$. Pour tout $a,b \in \mathbb{Z}$ on définit

$$a \equiv b \quad \text{s'il existe } s \in \mathbb{Z} \text{ tel que } a = b + s \cdot n \ .$$

(a) Montrer que $\equiv$ est une relation d'équivalence, dite de *congruence modulo* n sur $\mathbb{Z}$. On dit que a est *congru à* b *modulo* n .

(b) Décrire les classes d'équivalence de manière interne.

4.5 Anneaux et corps

DEFINITION 1 Un ensemble A muni de deux opérations $+$ et $\cdot$ s'appelle un *anneau* si l'addition $+$ définit une structure de groupe commutatif sur A , et si la multiplication $\cdot$ est associative et distributive par rapport à l'addition.

On dit que l'anneau A est *commutatif* si la multiplication est commutative, et *unifère* si la multiplication possède un élément neutre. Un anneau unifère A est dit un *corps* si $A^* := A \setminus \{0\}$ est un groupe pour la multiplication.

REMARQUE 1 Soit A un anneau. Pour tout $a, b \in A$, on a

(a)
$$a \cdot 0 = 0 \cdot a = 0 \ .$$

(b)
$$a \cdot (-b) = (-a) \cdot b = -(a \cdot b) \ ,$$

(c) *Règle des signes*
$$(-a) \cdot (-b) = a \cdot b \ .$$

En effet
$$a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 \ ,$$
d'où $a \cdot 0 = 0$ en simplifiant. On prouve de même que $0 \cdot a = 0$. Pour (b) il vient
$$a \cdot b + a \cdot (-b) = a \cdot [b + (-b)] = a \cdot 0 = 0 \ ,$$
ce qui montre que $a \cdot (-b)$ est bien l'opposé de $a \cdot b$. Il en est de même de $(-a) \cdot b$. Quant à la règle des signes, on obtient
$$(-a) \cdot (-b) = [-(-a)] \cdot b = a \cdot b \ .$$

□

DEFINITION 2 On dit qu'un anneau commutatif unifère A muni d'un ordre $\leqslant$ est un *anneau ordonné* si le groupe additif de A est un groupe ordonné et si, la multiplication est compatible avec l'ordre, i.e. si pour tout $a, b, c \in A$, on a

compatibilité
$$a \leqslant b \text{ et } c \geqslant 0 \quad \Longrightarrow \quad a \cdot c \leqslant b \cdot c \ .$$

PROPOSITION *Soient A un anneau ordonné et $a, b, c \in A$. Alors on a*

(i)
$$a \leqslant b \quad \Longleftrightarrow \quad a + c \leqslant b + c \ .$$

(ii)
$$a < b \quad \Longleftrightarrow \quad a + c < b + c \ .$$

(iii)
$$a \leqslant b \quad \Longleftrightarrow \quad -b \leqslant -a \ .$$

(iv)
$$a \leqslant b \text{ et } c \leqslant 0 \quad \Longrightarrow \quad a \cdot c \geqslant b \cdot c \ .$$

(v)
$$a \geqslant 0 \text{ et } b \geqslant 0 \quad \Longrightarrow \quad a + b \geqslant 0 \text{ et } a \cdot b \geqslant 0 \ .$$

Si en plus A est un corps et $c > 0$, alors

(vi)

$$a \leqslant b \iff a \cdot c \leqslant b \cdot c \ .$$

(vii)

$$a < b \iff a \cdot c < b \cdot c \ .$$

Démonstration de (i) L'implication $\Rightarrow$ exprime la compatibilité de l'addition avec l'ordre (cf. définition 4.3.2). Réciproquement $a + c \leqslant b + c$ entraîne

$$a = a + c + (-c) \leqslant b + c + (-c) = b \ .$$

Démonstration de (ii) Cela découle de (i) car $a \neq b$ est équivalent à $a + c \neq b + c$.

Démonstration de (iii) En effet $a \leqslant b$ entraîne

$$-b = a + (-a) + (-b) \leqslant b + (-a) + (-b) = -a \ .$$

L'autre implication découle de celle que nous venons de démontrer et de la règle des signes (remarque 1.b).

Démonstration de (iv) En effet $-c \geqslant 0$ par (iii), donc

$$-a \cdot c = a \cdot (-c) \leqslant b \cdot (-c) = -b \cdot c \ ,$$

et par suite

$$b \cdot c \leqslant a \cdot c \ .$$

Démonstration de (v) En effet

$$a + b \geqslant 0 + b = b \geqslant 0$$

et

$$a \cdot b \geqslant 0 \cdot b = 0 \ .$$

Démonstration de (vi) C'est la même démonstration que celle de (i) en remplaçant l'addition par la multiplication.

Démonstration de (vii) Cela découle de (vi) car $a \neq b$ et $c \neq 0$ est équivalent à $a \cdot c \neq b \cdot c$.

Nous allons maintenant voir que la multiplication et l'ordre de $\mathbb{N}$ peuvent être prolongés à $\mathbb{Z}$.

DEFINITION 3 Pour tout $x, y \in \mathbb{Z}$, on définit le produit de x et y par

$$x \cdot y := [(ac + bd, ad + bc)]$$

si $(a, b) \in x$ et $(c, d) \in y$, car cela ne dépend pas des représentants choisis. La relation sur $\mathbb{Z}$

$$y - x \in \mathbb{N}$$

est désignée par $x \leqslant y$.

REMARQUE 2 Pour tout $m, n \in \mathbb{N}$, on a

$$[(m, 0)] \cdot [(n, 0)] = [(m \cdot n, 0)]$$

et $n - m \in \mathbb{N}$ est équivalent à $m \leqslant n$ par le corollaire 3.7.

On montre facilement le

THEOREME *$\mathbb{Z}$ est un anneau commutatif unifère totalement ordonné. Tout élément de $\mathbb{Z} \setminus \{0\}$ est simplifiable par rapport à la multiplication, et on a la propriété de division avec reste.*

REMARQUE 3 $\mathbb{Z}$ n'est pas un corps, car l'équation $2 \cdot x = 1$ n'a pas de solution.

En effet 0 n'est pas solution, et si $x \geqslant 1$, resp. $x \leqslant -1$, alors

$$2 \cdot x \geqslant 2 > 1 \quad \text{, resp.} \quad 2 \cdot x \leqslant -2 < 1 \ .$$

$\square$

EXERCICE 1 On considère la relation d'équivalence $\equiv$ définie dans l'exercice 4.4. Montrer que pour tout $a, b, c, d \in \mathbb{Z}$, on a

$$a \equiv b \text{ et } c \equiv d \quad \Longrightarrow \quad a \cdot c \equiv b \cdot d \ .$$

EXERCICE 2 Soit K un corps commutatif totalement ordonné. Pour tout $x, y \in K$ et $b \in K^*$ tel que $b > 0$, on a

$$x^2 \geqslant 0 \quad , \quad \frac{1}{b} > 0 \quad \text{et} \quad 2 \cdot x \cdot y \leqslant \frac{1}{b} \cdot x^2 + b \cdot y^2 \ .$$

EXERCICE 3 Soit K un corps commutatif totalement ordonné. Pour tout $x, y \in K$, on a

$$1 < x < y \quad \Longrightarrow \quad x + \frac{1}{x} < y + \frac{1}{y} \ .$$

EXERCICE 4 Soit A un anneau et $P \subset A$ une partie satisfaisant aux trois propriétés suivantes :

P_1
$$A = P \cup (-P) \quad \text{et} \quad P \cap (-P) = \{0\} \ .$$

P_2
$$a, b \in P \quad \Longrightarrow \quad a + b \in P \ .$$

P_3
$$a, b \in P \quad \Longrightarrow \quad ab \in P \ .$$

(a) Montrer que A muni de la relation $\leqslant$ définie par

$$a \leqslant b \quad \text{si} \quad b - a \in P$$

est un anneau totalement ordonné.

(b) Montrer que tout anneau totalement ordonné contient une partie P satisfaisant aux propriétés P_1 à P_3 et définissant l'ordre de A .

4.6 Construction des nombres rationnels

L'équation

$$b \cdot x = a \ ,$$

que nous ne pouvons pas en général résoudre dans $\mathbb{Z}$, n'est intéressante que si $b \neq 0$. En effet si $b = 0$, alors elle n'a jamais de solution si $a \neq 0$, tout $x \in \mathbb{Z}$ est solution si $a = 0$.

Afin de pouvoir résoudre cette équation, nous allons construire un anneau contenant une image de $\mathbb{Z}$ avec compatibilité des structures.

Sur $\mathbb{Z} \times \mathbb{Z}^*$, où $\mathbb{Z}^* := \mathbb{Z} \smallsetminus \{0\}$, on introduit la relation Q définie par

$$(a,b) \ \ Q \ \ (c,d) \quad : \quad a \cdot d = b \cdot c \ .$$

DEFINITION On pose

$$\mathbb{Q} := \mathbb{Z} \times \mathbb{Z}^* / \, Q$$

et on dit que c'est l' *ensemble des nombres rationnels* . Pour tout $(a,b) \in \mathbb{Z} \times \mathbb{Z}^*$, on pose

$$\frac{a}{b} := [(a,b)] \ .$$

Pour tout $x, y \in \mathbb{Q}$, on définit la somme et le produit de x et y par

$$x + y := \frac{a \cdot d + b \cdot c}{b \cdot d}$$

et

$$x \cdot y := \frac{a \cdot c}{b \cdot d} \ ,$$

si $(a,b) \in x$ et $(c,d) \in y$, i.e. $x = \frac{a}{b}$ et $y = \frac{c}{d}$.

On définit une relation sur $\mathbb{Q}$ par

$$x \leqslant y \quad : \quad \text{s'il existe } a,b,c,d \in \mathbb{Z} \text{ tels que } b,d > 0 \ , \ x = \frac{a}{b} \ , \ y = \frac{c}{d} \text{ et } a \cdot d \leqslant b \cdot c \ .$$

On peut montrer que ces définitions sont consistantes, car elles ne dépendent pas des représentants choisis.

REMARQUE 1 On identifie $\mathbb{Z}$ avec une partie de $\mathbb{Q}$ grâce à l'injection

$$\mathbb{Z} \hookrightarrow \mathbb{Q} : n \longmapsto \frac{n}{1} \ .$$

Pour tout $m, n \in \mathbb{Z}$, on a

$$\frac{m}{1} + \frac{n}{1} = \frac{m+n}{1} \quad \text{et} \quad \frac{m}{1} \cdot \frac{n}{1} = \frac{m \cdot n}{1} \ ,$$

ce qui montre que l'addition et la multiplication de $\mathbb{Q}$ induisent bien les opérations correspondantes sur $\mathbb{Z}$. En outre

$$\frac{m}{1} \leqslant \frac{n}{1} \quad \Longleftrightarrow \quad m \leqslant n \ ,$$

ce qui montre que la relation $\leqslant$ sur $\mathbb{Q}$ induit la relation d'ordre sur $\mathbb{Z}$.

On montre alors facilement le

THEOREME $\mathbb{Q}$ *est un corps totalement ordonné.*

La démonstration est laissé au lecteur. □

REMARQUE 2 Si K est un corps, pour tout $x \in K$ et $n \in \mathbb{Z}$ tel que $n < 0$, on pose

$$n \cdot x := -(-n) \cdot x$$

et

$$x^n := \left(x^{-1}\right)^{-n} \text{ si } x \neq 0 \ .$$

Pour tout $x, y \in K$ et $n, m \in \mathbb{Z}$, on a

$$x \cdot (n \cdot y) = n \cdot (x \cdot y) \quad , \quad n \cdot (x + y) = n \cdot x + n \cdot y \quad , \quad (n + m) \cdot x = n \cdot x + m \cdot x \ ,$$

ainsi que

$$x^n \cdot x^m = x^{n+m} \quad , \quad (x^n)^m = x^{n \cdot m} \quad \text{et} \quad x^n \cdot y^n = (x \cdot y)^n \text{ si } x, y \neq 0 \ .$$

EXERCICE Soient K un corps totalement ordonné et $a, b \in K$. Pour que $a \cdot b \geqslant 0$, il faut et il suffit que l'on ait

$$a, b \geqslant 0 \quad \text{ou} \quad a, b \leqslant 0 \ .$$

4.7 Construction des nombres réels

Nous avons déjà vu (exemple 1.4.2) que l'équation $x^2 = 2$ ne possède pas de solution dans $\mathbb{Q}$.

DEFINITION 1 On dit qu'une partie $D \subset \mathbb{Q}$ est une *coupure de Dedekind* si l'on a

D_1
$$\emptyset \neq D \neq \mathbb{Q} \ .$$

D_2
$$\text{Pour tout } x \in D \text{ et } y \in \mathbb{Q} \text{ tels que } y \leqslant x \ , \text{ on a } y \in D \ .$$

D_3
$$\text{Pour tout } x \in D \ , \text{ il existe } y \in D \text{ tel que } y > x \ .$$

On pose alors
$$\mathbb{R} := \{D \in \mathfrak{P}(\mathbb{Q}) \mid D \text{ est une coupure de Dedekind}\}$$
et on dit que c'est l' *ensemble des nombres réels* ou la *droite numérique* .

LEMME *Pour tout $a, b \in \mathbb{Q}$ tels que $a < b$, on a*
$$a < \frac{a+b}{2} < b \ .$$

En effet cela revient à montrer que $2a < a + b < 2b$, ce qui est évident. $\square$

COROLLAIRE *Si $a \in \mathbb{Q}$, alors $a_{\mathbb{R}} := \{x \in \mathbb{Q} \mid x < a\}$ est une coupure de Dedekind et l'application*
$$a \longmapsto a_{\mathbb{R}} : \mathbb{Q} \longrightarrow \mathbb{R}$$
est injective.

En effet, on a $a - 1 \in a_{\mathbb{R}}$, donc $a_{\mathbb{R}} \neq \emptyset$, et $a + 1 \notin a_{\mathbb{R}}$, donc $a_{\mathbb{R}} \neq \mathbb{Q}$. Ceci prouve (D_1) . Si $x \in a_{\mathbb{R}}, y \in \mathbb{Q}$ et $y \leqslant x$, alors $y \leqslant x < a$, donc $y \in a_{\mathbb{R}}$, et par suite (D_2) . Finalement, si $x \in a_{\mathbb{R}}$, alors $x < \frac{x+a}{2} < a$ par le lemme, ce qui prouve (D_3) .

Pour tout $a, b \in \mathbb{Q}$ tels que $a \neq b$, nous devons montrer que $a_{\mathbb{R}} \neq b_{\mathbb{R}}$. Nous pouvons supposer que $a < b$, mais $a \notin a_{\mathbb{R}}$ et $a \in b_{\mathbb{R}}$, d'où le résultat. $\square$

DEFINITION 2 Pour tout $C, D \in \mathbb{R}$, on définit la somme de C et D en posant
$$C + D := \{x + y \mid x \in C, y \in D\}$$
et une relation entre C et D par
$$C \leqslant D \quad : \quad C \subset D \ .$$

REMARQUE 1 Pour tout $C, D \in \mathbb{R}$, $C + D$ est une coupure de Dedekind, i.e. $C + D \in \mathbb{R}$.

Comme $C, D \neq \emptyset$, il est clair que $C + D \neq \emptyset$. Comme $C, D \neq \mathbb{Q}$, il existe $c, d \in \mathbb{Q}$ tels que $c \notin C$ et $d \notin D$, ce qui signifie par (D_2) que $c > x$ pour tout $x \in C$ et $d > y$ pour tout $y \in D$. On a alors

$$c + d > x + d > x + y \ ,$$

donc $c + d \notin C + D$, i.e. $C + D \neq \mathbb{Q}$.

Soient $u \in C + D$ et $v \in \mathbb{Q}$ tel que $v \leqslant u$. Il existe $x \in C$ et $y \in D$ tels que

$$v \leqslant u = x + y \ .$$

Mais alors $v = x + (v - x) \in C + D$, car $v - x \leqslant y$, donc $v - x \in D$.

Finalement, si $x \in C$ et $y \in D$, par (D_3) il existe $u \in C$ et $v \in D$ tels que $u > x$ et $v > y$, donc $u + v \in C + D$ et $u + v > x + y$. □

REMARQUE 2 La relation $\leqslant$ sur $\mathbb{R}$ est par définition induite par l'ordre $\subset$ sur $\mathfrak{P}(\mathbb{Q})$, donc est une relation d'ordre.

PROPOSITION *$\mathbb{R}$ est un groupe commutatif totalement ordonné. L'élément neutre pour l'addition est $0_{\mathbb{R}}$ et, pour tout $D \in \mathbb{R}$, son opposé est*

$$-D := \begin{cases} (-a)_{\mathbb{R}} & \text{si } D = a_{\mathbb{R}} \quad \text{pour un } a \in \mathbb{Q} \\ \{-y \mid y \notin D\} & \text{si } D \neq a_{\mathbb{R}} \quad \text{pour tout } a \in \mathbb{Q} \end{cases} .$$

La démonstration que $\mathbb{R}$ est un groupe commutatif totalement ordonné ne présente pas de difficulté fondamentale. Par exemple on voit immédiatement que $0_{\mathbb{R}}$ est l'élément neutre, car $D + 0_{\mathbb{R}} \subset D$ par (d_2) et $D \subset D + 0_{\mathbb{R}}$ par (D_3) .

Pour démontrer que tout élément de $\mathbb{R}$ est inversible, on a tout d'abord $D + (-D) \subset 0_{\mathbb{R}}$, car si $y \notin D$, on a $y > x$ pour tout $x \in D$, donc $x + (-y) < 0$. D'autre part soient $u \in 0_{\mathbb{R}}$ et $z \notin D$. Nous allons prouver par l'absurde qu'il existe $x \in D$ tel que $x - u \notin D$; on en déduit alors que $u - x \in -D$, donc que $0_{\mathbb{R}} \subset D + (-D)$ puisque $u = x + (u - x)$. Supposons donc que pour tout $x \in D$, on ait $x - u \in D$; par récurrence on obtient

$$x - k \cdot u \in D \text{ pour tout } k \in \mathbb{N} \ .$$

Mais il existe $n \in \mathbb{N}$ tel que $n \geqslant \frac{x-z}{u}$, donc $x - n \cdot u \geqslant z \notin D$, ce qui est absurde.

Le reste est laissé au lecteur. □

DEFINITION 3 Pour tout $C, D \in \mathbb{R}$, on définit le produit de C et D une multiplication en posant

$$C \cdot D := \{x \cdot y \mid x \in C \ , \ y \in D \text{ tel que } y > 0\} \quad \text{si } D > 0 \ ,$$

ainsi que

$$C \cdot D = -C \cdot (-D) \quad \text{si } D < 0 \ ,$$

et

$$C \cdot 0 = 0 \ .$$

On pose

$$\mathbb{R}_+ := \{D \in \mathbb{R} \mid D \geqslant 0_{\mathbb{R}}\} \quad \text{et} \quad \mathbb{R}_- := \{D \in \mathbb{R} \mid D \leqslant 0_{\mathbb{R}}\} \ ,$$

ainsi que

$$\mathbb{R}^* := \mathbb{R} \smallsetminus \{0\} \quad , \quad \mathbb{R}_+^* := \mathbb{R}_+ \smallsetminus \{0\} \quad \text{et} \quad \mathbb{R}_-^* := \mathbb{R}_- \smallsetminus \{0\} \ .$$

REMARQUE 3 Pour tout $C, D \in \mathbb{R}$ tels que $D > 0$, l'ensemble $C \cdot D$ est une coupure de Dedekind, donc $C \cdot D \in \mathbb{R}$.

La démonstration est analogue à celle de la remarque 1. □

THEOREME *$\mathbb{R}$ est un corps totalement ordonné. L'élément neutre pour la multiplication est $1_{\mathbb{R}}$ et, pour tout $D \in \mathbb{R}_+^*$, son inverse est*

$$\frac{1}{D} := \begin{cases} \left(\frac{1}{a}\right)_{\mathbb{R}} & \quad D = a_{\mathbb{R}} \quad \textit{pour un } a \in \mathbb{Q} \\ & \textit{si} \\ \mathbb{R}_- \cup \left\{ \frac{1}{y} \;\middle|\; y \notin D \right\} & \quad D \neq a_{\mathbb{R}} \quad \textit{pour tout } a \in \mathbb{Q} \end{cases} .$$

La démonstration que $\mathbb{R}$ est un corps est malheureusement assez longue, car il faut distinguer les différents cas pour la multiplication. □

REMARQUE 4 Pour tout $a, b \in \mathbb{Q}$, il est clair que

$$a_{\mathbb{R}} + b_{\mathbb{R}} = (a+b)_{\mathbb{R}} \quad \text{et} \quad a_{\mathbb{R}} \cdot b_{\mathbb{R}} = (a \cdot b)_{\mathbb{R}} \ ,$$

et que la relation $a_{\mathbb{R}} \subset b_{\mathbb{R}}$ est équivalente à $a \leqslant b$. Nous identifierons donc $\mathbb{Q}$ à la partie correspondante dans $\mathbb{R}$. La coupure de Dedekind $a_{\mathbb{R}}$, pour $a \in \mathbb{Q}$, sera encore désignée par a .

Grâce à cette identification la première partie de la proposition suivante résume, mais de manière circulaire, la construction de $\mathbb{R}$!

SCOLIE

(i) *Pour tout $c \in \mathbb{R}$ et $x \in \mathbb{Q}$, on a $x < c$ si, et seulement si, $x \in c$. En particulier*

$$c = \{x \in \mathbb{Q} \mid x < c\} \ .$$

(ii) *Pour tout $c, d \in \mathbb{R}$ tels que $c < d$, il existe $q \in \mathbb{Q}$ tel que $c < q < d$.*

C'est immédiat. □

EXERCICE Montrer que, pour tout $k, n \in \mathbb{N}$ tels que $k \leqslant n$, on a

$$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!} = \binom{n}{n-k} .$$

En déduire que

$$\binom{n}{k} = \prod_{l=k+1}^{n} \frac{l}{l-k} = \prod_{l=1}^{n-k} \frac{l+k}{l} = \prod_{l=1}^{k} \frac{n+l-k}{l} ,$$

ainsi que l'inégalité

$$(1+a)^n \geqslant \frac{1}{2} n\,(n-1)\,a^2$$

pour tout $a \in \mathbb{R}_+$.

4.8 Bornes supérieures et théorème de Dedekind

DEFINITION 1 Soient X un ensemble ordonné et $A \subset X$. On dit que $m \in X$ est un *majorant* de A si l'on a $m \geqslant a$ pour tout $a \in A$, et que A est *majorée* si A possède un majorant. On dit que m est le *plus petit élément* de A si $m \in A$ et $m \leqslant a$ pour tout $a \in A$.

On dit que $s \in X$ est la *borne supérieure* de A si s est le plus petit majorant de A , i.e. si

(a) s est un majorant de A.

(b) Pour tout majorant m de A , on a $m \geqslant s$.

On définit les notions de *minorant* , *minorée* , *plus grand élément* et *borne inférieure* en renversant les inégalités.

Le plus grand élément, respectivement le plus petit élément, la borne supérieure et la borne inférieure, de A se note

$$\max A \quad , \quad \min A \quad , \quad \sup A \quad \text{et} \quad \inf A$$

s'ils existent. On dit aussi *maximum* , *minimum* , *supremum* et *infimum* respectivement.

On dit que A est *bornée* si A est majorée et minorée.

Si sup $A \in A$, respectivement inf $A \in A$, alors

$$\sup A = \max A \quad \text{et} \quad \inf A = \min A \ .$$

Si $(a_j)_{j \in J}$ est une famille de X , on pose

$$\sup_{j \in J} a_j := \sup \{a_j \mid j \in J\} \quad , \text{resp.} \quad \inf_{j \in J} a_j := \inf \{a_j \mid j \in J\} \ ,$$

si cette borne supérieure, resp. inférieure, existe.

Lorsque nous écrirons l'un des symboles $\sup A$, $\inf A$, $\max A$ ou $\min A$, cela signifiera, sans que nous le disions explicitement, que cet élément existe.

PROPOSITION *Soient X un ensemble totalement ordonné et $x, y \in X$. Alors* $\max \{x, y\}$ *et* $\min \{x, y\}$ *existent. Plus généralement toute partie finie non-vide de X possède un maximum et un minimum.*

En effet on a $x \leqslant y$ ou $y \leqslant x$. Dans le premier cas il est clair que y est le plus grand élément de $\{x, y\}$, dans le second c'est évidemment x . La seconde partie se démontre par récurrence sur le nombre d'éléments de cette partie. Le cas $n = 1$ est trivial. Pour prouver le pas d'induction il suffit de remarquer que si A a $n+1$ éléments, alors $\max (A \setminus \{0\})$ existe par l'hypothèse de récurrence et

$$\max (\max (A \setminus \{0\}), a)$$

est le maximum de A . □

DEFINITION 2 On écrit $\max (x, y)$ et $\min (x, y)$ à la place de $\max \{x, y\}$ et $\min \{x, y\}$ pour simplifier.

Propriété d'approximation *Soient X un ensemble totalement ordonné, $A \subset X$ et $s \in X$. Pour que s soit la borne supérieure de A , il faut et il suffit que s soit un majorant de A et que, pour tout $x \in X$ tel que $x < s$, il existe $a \in A$ tel que $a > x$.*

Pour tout $m \in X$, la négation de $m \geqslant s$ est $m < s$, puisque X est totalement ordonné. La contraposition de (b) est alors

$$\text{si } m < s \text{ , alors } m \text{ n'est pas un majorant de } A \text{ .}$$

Mais m n'est pas un majorant de A signifie qu'il existe un $a \in A$ tel que $a > m$. Ceci montre que (b) est équivalent à la condition d'approximation. □

THEOREME (de Dedekind) *Soit A une partie non-vide et majorée de $\mathbb{R}$. Alors la borne supérieure* $\sup A$ *existe.*

Rappelons que $\mathbb{R} \subset \mathfrak{P}(\mathbb{Q})$. Si $m \in \mathbb{R}$ est un majorant de A , pour tout $a \in A$, on a $m \geqslant a$, i.e. $m \supset a$. Posons $s := \bigcup_{a \in A} a \subset \mathbb{Q}$. On a évidemment $s \subset m \neq \mathbb{Q}$, donc $s \neq \mathbb{Q}$. On a également $s \neq \emptyset$, puisque $A \neq \emptyset$ et tout $a \in A$ est non-vide.

Montrons que s est une coupure de Dedekind. Remarquons tout d'abord que pour tout $x \in s$, il existe $a \in A$ tel que $x \in a$. Si $y \in \mathbb{Q}$ et $y \leqslant x$, alors $y \in a$, puisque a est une coupure. On en déduit que $y \in s$, d'où (d_2) . D'autre part, il existe $y \in a$ tel que $y > x$. Mais $y \in s$, ce qui prouve (d_3) .

Pour tout $a \in A$, on a évidemment $a \subset s$, i.e. $a \leqslant s$, ce qui montre que s est un majorant de A . Si m est un majorant de A , on a $m \supset a$ quel que soit $a \in A$, donc

$$m \supset \bigcup_{a \in A} a = s \ ,$$

i.e $m \geqslant s$, ce qui finit de prouver que s est le plus petit majorant de A , et par suite la borne supérieure de A . □

EXEMPLE Pour tout $c \in \mathbb{R}$, on a

$$c = \sup \{x \in \mathbb{Q} \mid x < c\} = \sup c \ .$$

Il est clair que c est un majorant de $\{x \in \mathbb{Q} \mid x < c\}$. Mais c satisfait à la propriété d'approximation par la proposition 4.7.ii ou d_3 , d'où le résultat. □

REMARQUE On peut montrer si $c \notin \mathbb{Q}$, que $\{x \in \mathbb{Q} \mid x < c\}$ ne possède pas de borne supérieure dans $\mathbb{Q}$.

4.9 Théorème d'Archimède

LEMME $\mathbb{N}$ *n'est pas majoré dans* $\mathbb{R}$ *.*

En effet si $\mathbb{N}$ est majoré, on a $s := \sup\ \mathbb{N} \in \mathbb{R}$. Mais alors, pour tout $n \in \mathbb{N}$, comme $n + 1 \in \mathbb{N}$, on a $n + 1 \leqslant s$, et par suite $n \leqslant s - 1$. Ceci montre que $s - 1$ est un majorant de $\mathbb{N}$, ce qui est absurde. □

THEOREME (d'Archimède) $\mathbb{R}$ *est archimédien, i.e. pour tout* $x, y \in \mathbb{R}$ *tels que* $x, y > 0$ *, il existe* $n \in \mathbb{N}$ *tel que* $n \cdot x \geqslant y$ *.*

Si tel n'est pas le cas, pour tout $n \in \mathbb{N}$, on a $n \cdot x < y$, donc $n < \frac{y}{x}$. Ceci montre que $\mathbb{N}$ est majoré, ce qui est contradictoire avec le lemme. □

En particulier, pour tout $x \in \mathbb{R}$, il existe $m \in \mathbb{N}$ tel que $-x \leqslant m$, donc $-m \leqslant x$. Ainsi $A := \{n \in \mathbb{Z} \mid n \leqslant x\} \neq \emptyset$ et c'est une partie majorée, donc $\lfloor x \rfloor := \sup A \in \mathbb{R}$ par le théorème de Dedekind. Pour tout $n \in \mathbb{Z}$ tel que $n \leqslant x$, on a $n \leqslant \lfloor x \rfloor \leqslant x$, puisque $\lfloor x \rfloor$ est la plus petite borne supérieure de A .

Par la propriété d'approximation, il existe $N \in A$ tel que

$$\lfloor x \rfloor - 1 < N \leqslant \lfloor x \rfloor \ .$$

Pour tout $m \in \mathbb{N}$ tel que $m \geqslant N + 1$, on a

$$m \geqslant N + 1 > (\lfloor x \rfloor - 1) + 1 = \lfloor x \rfloor \ ,$$

donc $m > x$. Ceci montre que N est le plus grand élément de A et nous permet de définir

DEFINITION 1 Soit $x \in \mathbb{R}$. On pose

$$\lfloor x \rfloor := \max \{n \in \mathbb{Z} \mid n \leqslant x\}$$

et on dit que c'est la *partie entière (par en-dessous)* de x . De même soit

$$\lceil x \rceil := -\lfloor -x \rfloor = \min \{n \in \mathbb{Z} \mid x \leqslant n\} \ .$$

On dit que c'est la *partie entière (par en-dessus)* de x .

On a

$$\lfloor x \rfloor , \lceil x \rceil \in \mathbb{Z} \quad \text{et} \quad \lfloor x \rfloor \leqslant x \leqslant \lceil x \rceil \ .$$

REMARQUE On peut montrer que tout corps totalement ordonné, dans lequel le théorème de Dedekind est vrai, est isomorphe à $\mathbb{R}$. Ceci résoud le problème de la mesure des grandeurs (cf. N. Bourbaki, Topologie générale, chap. V, §2, proposition 2).

DEFINITION 2 L'ensemble

$$\overline{\mathbb{R}} := \mathbb{R} \cup \{\emptyset, \mathbb{Q}\} \subset \mathfrak{P}(\mathbb{Q})$$

est un ensemble totalement ordonné par la relation d'ordre $\subset$ induite par $\mathfrak{P}(\mathbb{Q})$. Les éléments $\emptyset$ et $\mathbb{Q}$ sont désignés respectivement par $-\infty$ et ∞ . On dit que c'est la *droite numérique achevée* .

On a évidemment

$$-\infty < x < \infty \quad \text{pour tout } x \in \mathbb{R} \ ,$$

donc $-\infty$ est le plus petit respectivement ∞ le plus grand élément de $\overline{\mathbb{R}}$.

PROPOSITION *$\overline{\mathbb{R}}$ est un ensemble totalement ordonné et, toute partie $A \subset \overline{\mathbb{R}}$ possède une borne supérieure et une borne inférieure (dans $\overline{\mathbb{R}}$). On a en outre*

$$\sup \emptyset = -\infty \quad \textit{et} \quad \inf \emptyset = \infty \ .$$

Pour qu'une partie $A \subset \mathbb{R}$ ne soit pas majorée ou minorée, dans $\mathbb{R}$, il faut et il suffit que

$$\sup A = \infty \quad , \textit{resp.} \quad \inf A = -\infty \quad \textit{dans } \overline{\mathbb{R}} \ .$$

C'est immédiat. ——— □

DEFINITION 3 Pour tout $a, b \in \overline{\mathbb{R}}$ tels que $a \leqslant b$, on définit les *intervalles* dits *fermés* , *ouverts* , *ouverts à droite* ou respectivement *ouverts à gauche* par

$$[a, b] := \left\{x \in \overline{\mathbb{R}} \mid a \leqslant x \leqslant b\right\} \ ,$$

$$]a, b[:= \left\{x \in \overline{\mathbb{R}} \mid a < x < b\right\} \subset \mathbb{R} \ ,$$

$$[a, b[:= \left\{x \in \overline{\mathbb{R}} \mid a \leqslant x < b\right\}$$

et

$$]a, b] := \left\{x \in \overline{\mathbb{R}} \mid a < x \leqslant b\right\} \ .$$

EXEMPLE FONDAMENTAL $\displaystyle \inf_{n \in \mathbb{N}^*} \frac{1}{n} = 0$.

En particulier, pour tout $x \in \mathbb{R}$, on a

$$x \leqslant \varepsilon \quad \textit{pour tout } \varepsilon > 0 \quad \Longrightarrow \quad x \leqslant 0 \ .$$

Il est clair que 0 est un minorant de l'ensemble des $\frac{1}{n}$ pour $n \geqslant 1$. Si $m \in \mathbb{R}$ est un minorant des $\frac{1}{n}$ tel que $m > 0$, i.e. $0 < m \leqslant \frac{1}{n}$, on a $n \leqslant \frac{1}{m}$ pour tout $n \in \mathbb{N}$, ce qui contredit le lemme. Ceci prouve que tout minorant des $\frac{1}{n}$ est $\leqslant 0$, d'où le résultat. La seconde partie en découle car $x \leqslant \frac{1}{n}$ pour tout $n \in \mathbb{N}^*$, donc $x \leqslant \inf_{n \in \mathbb{N}^*} \frac{1}{n} = 0$.

Cette dernière assertion est en fait immédiate. Si $x > 0$, soit $\varepsilon := \frac{x}{2} > 0$. On a alors

$$x = \frac{x}{2} + \frac{x}{2} > \frac{x}{2} = \varepsilon \ ,$$

ce qui est absurde. ——— □

4.10 Inégalité de Bernouilli

DEFINITION Une suite $(x_k)_{k\in\mathbb{N}}$ dans un ensemble ordonné est dite *croissante* respectivement *décroissante* si, pour tout $k \in \mathbb{N}$, on a

$$x_{k+1} \geqslant x_k \quad \text{resp.} \quad x_{k+1} \leqslant x_k \ .$$

On dit qu'elle est *strictement croissante* , respectivement *strictement décroissante* , si les inégalités sont strictes.

EXEMPLE La suite $\left(\frac{1}{k}\right)_{k\in\mathbb{N}}$ est strictement décroissante dans $\mathbb{R}$.

THEOREME (Inégalité de Bernouilli) *Pour tout $x \in \mathbb{R}$ tel que $x \geqslant -1$ et $n \in \mathbb{N}$, on a*

$$(1+x)^n \geqslant 1 + n \cdot x \ .$$

La démonstration se fait par récurrence. Le cas $n = 0$ est clair. Par l'hypothèse de récurrence, on obtient

$$(1+x)^{n+1} = (1+x) \cdot (1+x)^n \geqslant (1+x) \cdot (1+n \cdot x) =$$

$$= 1 + n \cdot x + x + n \cdot x^2 \geqslant 1 + (n+1) \cdot x \ ,$$

puisque $1 + x$ et $n \cdot x^2$ sont $\geqslant 0$. □

COROLLAIRE *Soit $y \in \mathbb{R}_+^*$.*

(i) Si $y > 1$, alors $\left(y^k\right)_{k\in\mathbb{N}}$ est strictement croissante et, pour tout $M \in \mathbb{R}_+$, il existe $n \in \mathbb{N}$ tel que $y^n \geqslant M$. En d'autres termes on a

$$\sup_{k\in\mathbb{N}} y^k = \infty \ .$$

(ii) Si $0 < y < 1$, alors $\left(y^k\right)_{k\in\mathbb{N}}$ est strictement décroissante et

$$\inf_{n\in\mathbb{N}} y^k = 0 \ .$$

Démonstration de (i) Comme $y > 1$ et $y^k > 0$, on obtient immédiatement

$$y^{k+1} > y^k \ .$$

Par le théorème d'Archimède, il existe $n \in \mathbb{N}$ tel que $n \cdot (y-1) \geqslant M$, puisque $y - 1 > 0$. Utilisant l'inégalité de Bernouilli on obtient alors

$$y^n = [1 + (y-1)]^n \geqslant 1 + n \cdot (y-1) \geqslant M \ .$$

Démonstration de (ii) Il est clair que 0 est un minorant des y^k . Si $m > 0$ est un minorant des y^k , en appliquant (i) à $\frac{1}{y}$ et $M := \frac{2}{m}$, il existe $n \in \mathbb{N}$ tel que $\left(\frac{1}{y}\right)^n \geqslant \frac{2}{m}$, donc

$$y^n \leqslant \frac{m}{2} < m \ ,$$

ce qui est absurde. Ceci prouve que tout minorant des y^k est $\leqslant 0$, donc que

$$\inf_{k\in\mathbb{N}} y^k = 0 \ .$$

$\square$

4.11 Calcul avec les bornes supérieures et inférieures

DEFINITION 1 Si A, B sont des parties de $\mathbb{R}$ et $a \in \mathbb{R}$, on pose

$$-A := \{-x \mid x \in A\} \quad , \quad a + B := \{a + y \mid y \in B\} \ ,$$

$$A + B := \{x + y \mid x \in A, y \in B\} \quad \text{et} \quad A \cdot B := \{x \cdot y \mid x \in A, y \in B\} \ .$$

Si A est une partie de $\mathbb{R}^*$, on pose

$$\frac{1}{A} := \left\{ \frac{1}{x} \,\middle|\, x \in A \right\} \ .$$

PROPOSITION *Soient A, B des parties non-vides de $\mathbb{R}$.*

(i) Si $A \subset B$ et si B est majorée, alors A est majorée et

$$\sup A \leqslant \sup B \ .$$

(ii) Si $(a_{j,k})_{(j,k) \in J \times K}$ est une famille (double) majorée de $\mathbb{R}$, alors les familles $(a_{j,k})_{k \in K}$, $(a_{j,k})_{j \in J}$, $(\sup_{k \in K} a_{j,k})_{j \in J}$ et $\left(\sup_{j \in J} a_{j,k}\right)_{k \in K}$ sont majorées et

$$\sup_{(j,k) \in J \times K} a_{j,k} = \sup_{j \in J} (\sup_{k \in K} a_{j,k}) = \sup_{k \in K} \left(\sup_{j \in J} a_{j,k}\right) \ .$$

(iii) Si A est une partie minorée de $\mathbb{R}$, alors $-A$ est majorée et

$$\inf A = -\sup (-A) \ .$$

(iv) Si $a \in \mathbb{R}$ et B est majorée, alors $a + B$ est majorée et

$$\sup (a + B) = a + \sup B \ .$$

(v) Si A, B sont majorées, alors $A + B$ est majorée et

$$\sup (A + B) = \sup_{a \in A} (a + \sup B) = \sup A + \sup B \ .$$

(vi) Si $a \in \mathbb{R}_+$ et B est majorée, alors $a \cdot B$ est majorée et

$$\sup (a \cdot B) = a \cdot \sup B \ .$$

(vii) Si $A \subset \mathbb{R}_+$ et B sont majorées, alors $A \cdot B$ est majorée et

$$\sup (A \cdot B) = \sup_{a \in A} (a \cdot \sup B) = \sup A \cdot \sup B \ .$$

(viii) Si $A \subset \mathbb{R}_+^*$ est majorée, alors $\frac{1}{A}$ est minorée et

$$\inf \frac{1}{A} = \frac{1}{\sup A} \ .$$

Démonstration de (i) Si m est un majorant de B , alors m est aussi un majorant de A , donc A est majorée. Comme l'ensemble des majorants de A contient l'ensemble des majorants de B , le plus petit majorant de A , i.e. $\sup A$, est plus petit que celui de B , i.e. $\sup B$.

Démonstration de (ii) Soit $m \in \mathbb{R}$ un majorant de $(a_{j,k})_{(j,k)\in J\times K}$. Pour tout $j \in J$, la famille $(a_{j,k})_{k\in K}$ est donc aussi majorée par m , ce qui montre que $\sup_{k\in K} a_{j,k}$ existe et que

$$m \geqslant \sup_{k\in K} a_{j,k} \quad \text{pour tout } j \in J \ .$$

Nous avons ainsi prouvé que la famille $(\sup_{k\in K} a_{j,k})_{j\in J}$ est majorée, donc que son supremum existe et que

$$m \geqslant \sup_{j\in J}\left(\sup_{k\in K} a_{j,k}\right) \ .$$

Puisque $\sup_{j\in J}(\sup_{k\in K} a_{j,k})$ est évidemment un majorant de $(a_{j,k})_{(j,k)\in J\times K}$, ce qui précède montre que c'est le plus petit des majorant. La première formule est ainsi démontrée. La seconde est évidente par symétrie.

Démonstration de (iii) Il est équivalent que m soit un minorant de A , i.e. $m \leqslant a$ pour tout $a \in A$, ou bien que $-m$ soit un majorant de $-A$, i.e $-m \geqslant -a$ pour tout $a \in A$. En particulier $-A$ est majorée et on obtient immédiatement

$$\sup(-A) = -\inf A \ .$$

Démonstration de (iv) L'application $m \longmapsto a + m$ est une bijection de l'ensemble des majorants de B sur l'ensemble des majorants de $a + B$. Comme $\sup(a + B)$ est le plus petit des majorants de $a + B$, on voit immédiatement qu'il est égal à $a + \sup A$.

Démonstration de (v) Utilisant (ii) il vient

$$\sup(A+B) = \sup_{(a,b)\in A\times B} a+b = \sup_{a\in A}[\sup_{b\in B} a+b] = \sup_{a\in A}[\sup(a+B)] =$$

$$= \sup_{a\in A}(a + \sup B) \underset{iv}{=} (\sup_{a\in A} a) + \sup B = \sup A + \sup B \ .$$

Les démonstrations de (vi)-(viii) sont analogues à celles qui précèdent et laissées en exercice au lecteur. □

DEFINITION 2 Pour tout $x \in \mathbb{R}$, on pose

$$|x| := \max(x, -x) = \begin{cases} x & \\ & \text{si} \\ -x & \end{cases} \begin{matrix} x \geqslant 0 \\ \\ x < 0 \end{matrix} \ ,$$

et on dit que c'est la *valeur absolue* de x .

Pour tout $x, y \in \mathbb{R}$ et $r \in \mathbb{R}_+$, on a évidemment

$$|x| \geqslant 0 \quad , \quad \pm x \leqslant |x| \quad , \quad |-x| = |x|$$

et

$$|x - y| \leqslant r \quad \Longleftrightarrow \quad y - r \leqslant x \leqslant y + r \ .$$

LEMME *Pour tout $x, y \in \mathbb{R}$, on a*

$$x^2 \leqslant y^2 \quad \Longleftrightarrow \quad |x| \leqslant |y| \ .$$

Les assertions suivantes sont successivement équivalentes entre elles :

$$x^2 \leqslant y^2$$

$$(y-x)\cdot(y+x) \geqslant 0$$

$$y-x, y+x \geqslant 0 \quad \text{ou} \quad y-x, y+x \leqslant 0$$

$$\pm x \leqslant y \quad \text{ou} \quad \pm x \leqslant -y$$

$$|x| \leqslant y \quad \text{ou} \quad |x| \leqslant -y$$

$$|x| \leqslant |y|$$

Nous avons utilisé l'exercice 4.6.1 pour la deuxième équivalence. $\square$

EXERCICE 1 Déterminer les bornes supérieure et inférieure des ensembles suivants :

(a)

$$\left\{ \left(-\frac{2}{3}\right)^n + \frac{3}{m} \;\middle|\; n, m \in \mathbb{N}^* \right\}$$

(b)

$$\left\{ x \in \mathbb{R}^* \;\middle|\; \frac{1}{x} \leqslant 1 - 2x^2 \right\} .$$

Est-ce que le maximum et le minimum de ces ensembles existent ?

EXERCICE 2 Montrer que, pour tout $x, y \in \mathbb{R}$, on a

$$\min(x,y) + \max(x,y) = x + y \ ,$$

$$\max(x,y) = \frac{1}{2}\cdot(x+y+|x-y|) \quad \text{et} \quad \min(x,y) = \frac{1}{2}\cdot(x+y-|x-y|) \ .$$

EXERCICE 3 Soient X, Y des parties non-vides et bornées de $\mathbb{R}$. Montrer

(a)

$$\sup(X \cup Y) = \max(\sup X, \sup Y)$$

et

$$\inf(X \cup Y) = \min(\inf X, \inf Y) \ .$$

(b) Si $X \cap Y \neq \emptyset$, alors

$$\sup(X \cap Y) \leqslant \min(\sup X, \sup Y)$$

et

$$\max(\inf X, \inf Y) \leqslant \inf(X \cap Y) \ .$$

Peut-on avoit $<$?

4.12 Existence de la racine carrée

THEOREME *Pour tout $a \in \mathbb{R}_+$, il existe une unique solution dans $\mathbb{R}_+$ de l'équation $x^2 = a$, dite la* racine carrée *de a et notée $\sqrt{a}$. On a*

$$\sqrt{a} := \sup \left\{ y \in \mathbb{R}_+ \mid y^2 \leqslant a \right\} \ .$$

Soit $A := \{y \in \mathbb{R}_+ \mid y^2 \leqslant a\}$. On a $0 \in A$ et, pour tout $y \in A$, il vient

$$y^2 \leqslant a \leqslant \max(1, a) \leqslant \max(1, a)^2$$

puisque $1 \leqslant \max(1, a)$. Le lemme 4.11 montre alors que $y \leqslant \max(1, a)$, ce qui finit de prouver que A est une partie non-vide et majorée de $\mathbb{R}$. Posons $r := \sup A$. Nous allons montrer que $r^2 = a$, en prouvant que $r^2 \leqslant a$ et $r^2 < a$ sont impossibles.

Tout d'abord on a

$$r^2 = (\sup A)^2 = \sup (A \cdot A) = \sup \left\{ y \cdot z \mid y, z \in \mathbb{R}_+ \ , \ y^2, z^2 \leqslant a \right\} \leqslant a \ ,$$

car pour tout $y, z \in \mathbb{R}_+$ tels que $y^2, z^2 \leqslant a$, on a

$$(y \cdot z)^2 = y^2 \cdot z^2 \leqslant a^2 \ ,$$

donc $y \cdot z \leqslant a$ par le lemme 4.11.

Si $r^2 < a$, posons $\varepsilon := \min\left(1, \frac{a - r^2}{2r+1}\right) > 0$. On a $\varepsilon^2 \leqslant \varepsilon$, donc

$$(r + \varepsilon)^2 = r^2 + 2r\varepsilon + \varepsilon^2 \leqslant r^2 + 2r\varepsilon + \varepsilon = r^2 + (2r + 1) \cdot \varepsilon \leqslant a \ .$$

Ainsi $r + \varepsilon \in A$ et $r < r + \varepsilon$, ce qui est absurde.

Pour la première partie, nous aurions aussi pu prouver que $r^2 > a$ est absurde. En effet on a $r > 0$ et posons $\varepsilon := \frac{r^2 - a}{2r} > 0$. Il vient

$$(r - \varepsilon)^2 = r^2 - 2r\varepsilon + \varepsilon^2 \geqslant r^2 - 2r\varepsilon = a \geqslant y^2 \quad \text{pour tout } y \in A \ ,$$

et comme

$$r - \varepsilon = r - \frac{r^2 - a}{2r} = \frac{r^2 + a}{2r} > 0 \ ,$$

le lemme 4.11 prouve que $r - \varepsilon \geqslant y$. Ainsi $r - \varepsilon$ est un majorant de A et $r > r - \varepsilon$, ce qui est absurde.

Il nous reste à prouver l'unicité. Si $r, s \in \mathbb{R}_+$ et $r^2 = a = s^2$, on obtient

$$0 = r^2 - s^2 = (r + s) \cdot (r - s) \ ,$$

et par suite $r + s = 0$ ou $r - s = 0$. Dans le premier cas, il vient

$$0 \leqslant r = -s \leqslant 0 \ ,$$

donc $r = 0 = s$. Dans le second on a évidemment $r = s$. □

COROLLAIRE *Pour tout $a, b \in \mathbb{R}_+$, on a $\sqrt{a \cdot b} = \sqrt{a} \cdot \sqrt{b}$.*

En effet

$$\left(\sqrt{a} \cdot \sqrt{b}\right)^2 = \left(\sqrt{a}\right)^2 \cdot \left(\sqrt{b}\right)^2 = a \cdot b \ ,$$

d'où le résultat par l'unicité. $\square$

EXERCICE 1 Soient $a, b, c \in \mathbb{R}$. Déterminer les ensembles

$$\left\{x \in \mathbb{R} \mid a \cdot x^2 + b \cdot x + c \geqslant 0\right\} \quad \text{et} \quad \left\{x \in \mathbb{R} \mid a \cdot x^2 + b \cdot x + c \leqslant 0\right\} \ .$$

EXERCICE 2 Déterminer l'ensemble

$$C := \left\{ (a,b) \in \mathbb{R}^2 \;\middle|\; x^2 + axy + by^2 \geqslant 0 \text{ pour tout } x, y \in \mathbb{R} \right\} \ .$$

EXERCICE 3 Calculer le supremum et l'infimum de l'ensemble

$$\left\{ \sqrt{k+1} - \sqrt{k} \;\middle|\; k \in \mathbb{N} \right\} \ .$$

S'agit-il d'un maximum respectivement d'un minimum ?

Il est utile de modifier $\sqrt{k+1} - \sqrt{k}$ de telle manière que l'on puisse appliquer la formule

$$(a+b)(a-b) = a^2 - b^2 \ .$$

4.13 Construction des nombres complexes

L'équation $x^2 = -1$ n'a pas de solution dans $\mathbb{R}$, puisque $x^2 \geqslant 0$ pour tout $x \in \mathbb{R}$. On est conduit à la définition suivante :

DEFINITION 1 On munit l'ensemble $\mathbb{C} := \mathbb{R}^2$ d'une addition et d'une multiplication définies par

$$(x, y) + (u, v) := (x + u, y + v)$$

et

$$(x, y) \cdot (u, v) := (x \cdot u - y \cdot v, x \cdot v + y \cdot u) \ .$$

On dit que $\mathbb{C}$ est l' *ensemble des nombres complexes* .

On pose

$$i := (0, 1) \ .$$

THEOREME *$\mathbb{C}$ est un corps commutatif. L'élément neutre de l'addition est $(0,0)$, celui de la multiplication $(1,0)$. L'opposé de (x,y) est $(-x,-y)$ et l'inverse de $(x,y) \neq (0,0)$ est*

$$\left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right) \ .$$

Les vérifications pour l'associativité et la commutativité des deux opérations, ainsi que de la distributivité de la multiplication par rapport à l'addition sont immédiates. Pour la dernière assertion on a

$$(x, y) \cdot \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right) = \left(\frac{x^2}{x^2+y^2} - \frac{-y^2}{x^2+y^2}, \frac{-x \cdot y}{x^2+y^2}, \frac{y \cdot x}{x^2+y^2}\right) = (1, 0) \ .$$

□

REMARQUE 1 On a une injection

$$\mathbb{R} \hookrightarrow \mathbb{C} : x \longmapsto (x, 0) \ ,$$

et comme

$$(x, 0) + (u, 0) = (x + u, 0) \quad \text{et} \quad (x, 0) \cdot (u, 0) = (x \cdot u, 0) \ ,$$

la structure de corps de $\mathbb{C}$ induit celle de $\mathbb{R}$. Nous identifierons donc $\mathbb{R}$ à une partie de $\mathbb{C}$ et désignerons $(x,0)$ par x . Pour tout $x, y \in \mathbb{R}$, on a

$$i \cdot y = (0, 1) \cdot (y, 0) = (0 \cdot y - 1 \cdot 0, 0 \cdot 0 + 1 \cdot y) = (0, y) \ ,$$

donc

$$(x, y) = (x, 0) + (0, y) = (x, 0) + (0, 1) \cdot (y, 0) = x + i \cdot y \ .$$

En outre

$$i \cdot (0, y) = (0, 1) \cdot (0, y) = (0 \cdot 0 - y, 0 \cdot y + 1 \cdot 0) = -y \ .$$

En particulier

$$i^2 = -1 \ .$$

Il est clair, par ce qui précède, que tout nombre complexe $z \in \mathbb{C}$ s'écrit de manière unique sous la forme

$$z = x + i \cdot y \quad , \quad x, y \in \mathbb{R} \ .$$

Ceci nous conduit à la

DEFINITION 2 On dit que x est la *partie réelle* de z , notée $\operatorname{Re} z$, et que y est la *partie imaginaire* de z , notée $\operatorname{Im} z$.

On pose

$$\overline{z} := x - i \cdot y$$

et on dit que c'est le *nombre complexe conjugué* de z .

On a

$$\overline{z} \cdot z = (x - i \cdot y) \cdot (x + i \cdot y) = x^2 - i^2 \cdot y^2 = x^2 + y^2 \geqslant 0 \ .$$

REMARQUE 2 Remarquons que l'on a

$$(x + i \cdot y) + (u + i \cdot v) = x + u + i \cdot (y + v)$$

et

$$(x + i \cdot y) \cdot (u + i \cdot v) = x \cdot u + i \cdot x \cdot v + i \cdot y \cdot u + i^2 \cdot y \cdot v = x \cdot u - y \cdot v + i \cdot (x \cdot v + y \cdot u) \ .$$

On retrouve ainsi la définition de la somme et du produit de deux nombres complexes.

REMARQUE 3 Pour tout $z \in \mathbb{C}^*$, on a

$$\frac{1}{z} = \frac{\overline{z}}{\overline{z} \cdot z} = \frac{x - i \cdot y}{x^2 + y^2} \ .$$

On a ainsi une manière simple de calculer l'inverse d'un nombre complexe, sans avoir besoin de se souvenir de la formule. En particulier si $z \cdot \overline{z} = 1$, alors

$$\frac{1}{z} = \frac{\overline{z}}{\overline{z} \cdot z} = \overline{z} \ .$$

Par exemple

$$\overline{i} = -i \quad , \quad i \cdot \overline{i} = 1 \quad \text{et} \quad \frac{1}{i} = \frac{\overline{i}}{\overline{i} \cdot i} = -i \ .$$

PROPOSITION *Soient $z, w \in \mathbb{C}$.*

(i) *On a*

$$z = \operatorname{Re} z + i \cdot \operatorname{Im} z \quad \textit{et} \quad \overline{z} = \operatorname{Re} z - i \cdot \operatorname{Im} z \ ,$$

ainsi que

$$\operatorname{Re} z = \frac{1}{2} \cdot (z + \overline{z}) \quad \text{et} \quad \operatorname{Im} z = \frac{1}{2i} \cdot (z - \overline{z}) \ .$$

(ii) Les propriétés

$$z \in \mathbb{R} \quad , \quad \operatorname{Im} z = 0 \quad \text{et} \quad z = \overline{z}$$

sont équivalentes.

(iii) On a

$$\overline{\overline{z}} = z \quad , \quad \overline{z + w} = \overline{z} + \overline{w} \quad \text{et} \quad \overline{z \cdot w} = \overline{z} \cdot \bar{w} \ .$$

Les démonstrations sont simples et laissées au lecteur. □

EXERCICE Mettre les nombres complexes suivants sous la forme $x + i \cdot y$ pour certains $x, y \in \mathbb{R}$:

$$\frac{2 - 5i}{4 + 3i} \quad \text{et} \quad \left(\frac{4 \cdot i^{11} - i}{1 + 2i} \right)^2 \ .$$

4.14 Valeur absolue dans $\mathbb{C}$

DEFINITION 1 Pour tout $z \in \mathbb{C}$, on pose

$$|z| := \sqrt{\overline{z} \cdot z} \ ,$$

et on dit que c'est la *valeur absolue* de z .

Si $z \in \mathbb{R}$, cette définition coïncide avec la précédente, puisque

$$\sqrt{z \cdot \overline{z}} = \sqrt{z^2} = |z| \ .$$

PROPOSITION *Pour tout* $z, w \in \mathbb{C}$ *, on a*

$$|z| \geqslant 0 \quad , \quad |\overline{z}| = |z| \quad , \quad |z \cdot w| = |z| \cdot |w| \quad , \quad |\mathrm{Re}\, z| , |\mathrm{Im}\, z| \leqslant |z|$$

et

$$|z| = 0 \quad \Longleftrightarrow \quad z = 0 \ .$$

Les deux premières formules sont immédiates. La troisième découle du corollaire 4.12. Pour la quatrième, écrivons $z = x + i \cdot y$ pour certains $x, y \in \mathbb{R}$. On a alors

$$x^2, y^2 \leqslant x^2 + y^2 = |z|^2 \ ,$$

d'où le résultat par le lemme 4.11. Finalement $|z| = 0$ est équivalent à $\overline{z} \cdot z = 0$, donc à $z = 0$ ou $\overline{z} = 0$, et par suite à $z = 0$. □

Inégalité triangulaire *Pour tout* $z, w \in \mathbb{C}$ *, on a*

$$|z + w| \leqslant |z| + |w| \ ,$$

ainsi que

$$|z| - |w| \leqslant |z - w| \quad \textit{et} \quad ||z| - |w|| \leqslant |z - w| \ .$$

Il vient tout d'abord

$$\mathrm{Re}\,(\overline{z} \cdot w) \leqslant |\overline{z} \cdot w| = |z| \cdot |w| \ ,$$

donc

$$|z + w|^2 = \overline{(z + w)} \cdot (z + w) = \overline{z} \cdot z + \overline{z} \cdot w + \overline{w} \cdot z + \overline{w} \cdot w =$$

$$= |z|^2 + 2 \cdot \mathrm{Re}\,(\overline{z} \cdot w) + |w|^2 \leqslant |z|^2 + 2 \cdot |z| \cdot |w| + |w|^2 = (|z| + |w|)^2 \ .$$

On conclut à l'aide du lemme 4.11. Finalement, on a

$$|z| = |z - w + w| \leqslant |z - w| + |w| \ ,$$

d'où la première inégalité. La seconde s'obtient par symétrie, puisque

$$||z| - |w|| = \max\,(|z| - |w| , |w| - |z|) \ .$$

□

EXERCICE On considère les ensembles Z_j , $j = 1, 2$, définis ci-dessous. Déterminer les nombres

$$\sup |Z_j| \quad \text{und} \quad \inf |Z_j|$$

et décider s'il s'agit d'un maximum respectivement d'un minimum. Donner une description géométrique de ces ensembles.

(a)

$$Z_1 := \left\{ \frac{1}{z} \;\middle|\; |z| \geqslant 1 \right\} .$$

(b)

$$Z_2 := \left\{ \frac{z-i}{z+i} \;\middle|\; \operatorname{Im} z > 0 \right\} .$$