PCSI - mathématiques

Ensembles de nombres usuels

1 Entiers relatifs

Chez les entiers naturels, seul 0 est symétrisable pour l'addition. On construit $\mathbb{Z}$ pour disposer d'une structure où tout élément aurait un opposé.

On admet l'existence d'un ensemble, noté $\mathbb{Z}$, dont les éléments sont appelés *entiers relatifs*, contenant $\mathbb{N}$, vérifiant les propriétés suivantes :

[$\mathbb{Z}$1] $(\mathbb{Z},+,\times)$ est un *anneau commutatif* : $\mathbb{Z}$ est muni

- d'une loi d'addition commutative, associative, admettant un élément neutre 0, et telle que tout élément x admet un symétrique $-x$ pour $+$;
- d'une loi multiplicative associative, commutative, admettant un élément neutre 1 et distributive par rapport à $+$.

[$\mathbb{Z}$2] $\mathbb{Z}$ est un *anneau ordonné* : il est muni d'une relation d'ordre *totale* $\leq$, *compatible* avec l'addition et la multiplication *par un entier* ≥ 0.

[$\mathbb{Z}$3] $\mathbb{Z}$ est le plus petit (modulo $\subset$) ensemble vérifiant ces propriétés.

La dernière condition permet de distinguer $\mathbb{Z}$ de $\mathbb{Q}$ et $\mathbb{R}$ qui possèdent aussi ces propriétés. De plus, elle assure l'unicité de l'ensemble $\mathbb{Z}$.

En outre, les opérations et la relation d'ordre de $\mathbb{Z}$ *prolongent* celles de $\mathbb{N}$: sur $\mathbb{N}$, elles coïncident avec les opérations et la relation d'ordre de $\mathbb{N}$.

1.1 Valeur absolue

Si $x \in \mathbb{Z}$, comme l'ordre est total, $-x$ et x sont comparables. La *valeur absolue* de x est

$$|x| = \max(-x, x).$$

Si $x \geq 0$, $x+(-x) \geq 0+(-x)$ donc $0 \geq -x$ d'où $-x \leq x$ et $|x| = x$. Si au contraire $x \leq 0$, $x+(-x) \leq 0+(-x)$ soit $0 \leq -x$ et $x \leq -x$, donc : $|x| = -x$ dans ce cas. On a ainsi une autre définition de la valeur absolue :

$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x \leq 0 \end{cases}.$$

Propriétés de $|\cdot|$

- $|x| \geq 0$ pour tout entier x.
- $-|x| \leq x \leq |x|$.
- $|x| \leq a \Leftrightarrow -a \leq x \leq a$.
- $|xy| = |x|\,|y|$ pour tous x, $y \in \mathbb{Z}$.

Le résultat le plus important pour $|\cdot|$ est le

Théorème 1 (inégalité triangulaire) *Si x, $y \in \mathbb{Z}$,*

$$||x| - |y|| \leq |x+y| \leq |x| + |y|.$$

1.2 Division euclidienne

Théorème 2 *$\mathbb{Z}$ est* archimédien*, càd que pour tout $x \in \mathbb{Z}_+$ et $a > 0$, il existe $n \in \mathbb{N}$ tel que $n.a > x$.*

Ce résultat, qui signifie qu'en considérant des multiples successifs d'un entier > 0, on atteint des valeurs arbitrairement grandes, est une conséquence directe de la compatibilité de la relation d'ordre de $\mathbb{Z}$ avec la multiplication des entiers > 0.

On peut en donner une formulation plus précise :

Corollaire 1 *Si $x \in \mathbb{Z}$ et $a \in \mathbb{Z}$, $a > 0$, il existe un unique $p \in \mathbb{Z}$ tel que*

$$p\,a \leq x < (p+1)\,a.$$

Dans cet énoncé, il est crucial de bien respecter les inégalités. Avec deux inégalités larges, l'unicité ne serait plus assurée, tandis qu'avec deux inégalités strictes on perdrait l'existence.

On en déduit une propriété fondamentale de $\mathbb{Z}$:

Théorème 3 (division euclidienne) *Soient a, $b \in \mathbb{Z}$, $b > 0$. Il existe un unique couple (q, r) d'entiers tels que*

$$a = b\,q + r \qquad (1)$$
$$0 \leq r < b \qquad (2)$$

q est le *quotient*, r est le *reste* dans la *division euclidienne* de a par b, qui est la relation (1) assortie de la condition (2). Sans celle-ci le couple (q, r) ne serait pas unique.

Grâce à la division euclidienne, à défaut de toujours pouvoir diviser un entier a par un entier $b > 0$, on peut comparer a aux multiples successifs de b.

1.3 Nombres premiers

Définition 1 *Un entier naturel non nul est dit* premier *s'il est différent de 1 et s'il n'est divisible que par 1 et par lui-même.*

Exemple 1 2, 3, 5, 7, 11, 13, ..., $2^{32\,582\,657} - 1$ ([1]), ...

Notation 1 *L'ensemble des nombres premiers est noté $\mathbb{P}$.*

On voit facilement que si $n \in \mathbb{N}$, $n > 1$ alors n admet un diviseur premier. On en déduit le résultat suivant, connu depuis l'antiquité :

[1] Le plus grand nombre premier connu, découvert le 4/11/2006. Son écriture décimale comporte 9 808 358 chiffres.

Proposition 1 (Euclide) *L'ensemble $\mathbb{P}$ des nombres premiers est* infini.

Les nombres premiers sont fondamentaux dans le sens où ils permettent, par multiplications et exponentiations, d'engendrer tous les nombres entiers :

Théorème 4 (décomposition en facteurs premiers) *Soit $n \in \mathbb{Z}$, $n \neq 0$. n se décompose de manière unique sous la forme*

$$n = \varepsilon \prod_{k=1}^{r} p_k^{\alpha_k} = \varepsilon p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$$

avec

- $\varepsilon = \pm 1$;
- $r \in \mathbb{N}$;
- $p_1, ..., p_r \in \mathbb{P}$ *deux à deux distincts ;*
- $\alpha_1, ..., \alpha_r \in \mathbb{N}^*$.

L'unicité dans ce théorème doit être comprise *à l'ordre près*. Elle signifie que si $n = \varepsilon \prod_{k=1}^{r} p_k^{\alpha_k} = \varepsilon' \prod_{l=1}^{s} q_l^{\beta_l}$ sont deux telles décompositions, alors $\varepsilon = \varepsilon'$, $r = s$, $\{p_1, ..., p_r\} = \{q_1, ..., q_r\}$ et pour k, $l \in [\![1, r]\!]$, $p_k = q_l \Rightarrow \alpha_k = \beta_l$.

La décomposition d'un entier en produit de facteurs premiers permet de traiter toutes les questions de divisibilité le concernant.

2 Rationnels

On a besoin de l'ensemble des rationnels pour disposer d'une structure où les éléments non nuls[2] seraient inversibles (symétrisables pour $\times$). Dans $\mathbb{Z}$, ce n'est le cas que pour -1 et 1.

On admet l'existence d'un ensemble, noté $\mathbb{Q}$, contenant $\mathbb{Z}$, dont les éléments sont les *rationnels*, vérifiant les conditions

[$\mathbb{Q}$1] $(\mathbb{Q}, +, \times)$ est un *corps commutatif*, càd un anneau commutatif (comme $\mathbb{Z}$) où en outre tout élément *non nul* est *inversible*, autrement dit symétrisable pour $\times$.

[$\mathbb{Q}$2] $\mathbb{Q}$ est un *corps ordonné* : il est muni d'une relation d'ordre *totale* $\leq$, compatible avec $+$ et $\times$ *sur* $\mathbb{Q}_+$.

[$\mathbb{Q}$3] $\mathbb{Q}$ est le plus petit (modulo $\subset$) ensemble vérifiant ces propriétés.

Cette dernière condition distingue $\mathbb{Q}$ de $\mathbb{R}$, et garantit également son unicité. Elle permet de plus de décrire les éléments de $\mathbb{Q}$: il doit contenir tous les entiers p, tous les entiers non nuls q ainsi que leurs inverses, ainsi que tous les produits du type pq^{-1}. Ainsi l'ensemble

$$\mathbb{Q} = \left\{ p\, q^{-1} \,|\, p \in \mathbb{Z},\, q \in \mathbb{Z} - \{0\} \right\}$$

est le plus petit ensemble vérifiant [$\mathbb{Q}$1] et [$\mathbb{Q}$2].

De plus, les opérations et la relations d'ordre de $\mathbb{Q}$ sont des prolongements de celles de $\mathbb{Z}$.

[2] pour 0, c'est évidemment impossible.

2.1 Quotients dans $\mathbb{Q}$

Si x, $y \in \mathbb{Q}$, $y \neq 0$ on pose $\frac{x}{y} = x.y^{-1}$ $(= y^{-1}.x)$: *quotient* du rationnel x par le rationnel non nul y. Cette notation sera aussi utilisée dans $\mathbb{R}$ et $\mathbb{C}$, mais attention : elle repose sur la commutativité de la multiplication. (Si ce n'était pas le cas, $x.y^{-1}$ et $y^{-1}.x$ auraient des significations différentes.)

On vérifie très facilement les propriétés suivantes des quotients :

- $x^{-1} = \frac{1}{x}$ si $x \neq 0$;
- $\frac{x}{y} \times \frac{x'}{y'} = \frac{xx'}{yy'}$ si y, $y' \neq 0$;
- $\frac{x}{y} + \frac{x'}{y'} = \frac{xy' + x'y}{yy'}$ si y, $y' \neq 0$;
- $\left(\frac{x}{y}\right)^{-1} = \frac{y}{x}$ si x, $y \neq 0$;
- $\frac{x}{y} + \frac{x'}{y} = \frac{x + x'}{y}$ si $y \neq 0$.

On définit la valeur absolue comme dans $\mathbb{Z}$, et elle conserve ses propriétés avec en plus :

Proposition 2

1. *Si $x \in \mathbb{Q}^*$, $\left|\frac{1}{x}\right| = \frac{1}{|x|}$;*
2. *Si $x \in \mathbb{Q}$ et $y \in \mathbb{Q}^*$, $\left|\frac{x}{y}\right| = \frac{|x|}{|y|}$.*

$\mathbb{Q}$ possède également le caractère archimédien :

Théorème 5 *Pour tous $x \in \mathbb{Q}_+$, $a \in \mathbb{Q}_+^*$, il existe $n \in \mathbb{N}$ tel que $n.a > x$.*

Corollaire 2 *Si $x \in \mathbb{Q}$ et $a \in \mathbb{Q}_+^*$, il existe un unique entier p tel que $p\,a \leq x < (p+1)\,a$.*

2.2 Partie entière

Le cas particulier $a = 1$ dans le corollaire précédent conduit à la définition suivante :

Définition 2 *Si $x \in \mathbb{Q}$, la* partie entière *de x est l'unique entier $p \in \mathbb{Z}$ tel que :*

$$p \leq x < p + 1.$$

En d'autres termes, p est le plus grand entier inférieur ou égal à x. Il revient au même de dire que x s'écrit de manière unique sous la forme $p + r$ avec $p \in \mathbb{Z}$ et $r \in [0, 1[$.

Notation 2 *La partie entière de x est notée $E(x)$.*

Elle est donc *caractérisée* par

$$E(x) \leq x < E(x) + 1.$$

Autrement dit, $E(x)$ est le plus grand entier $\leq x$.

Définition 3 *Le rationnel $r = x - E(x)$ (qui appartient à $[0, 1[$) est la* partie décimale *de x, notée $D(x)$.*

Contrairement aux entiers, il est toujours possible de trouver un rationnel strictement compris entre deux rationnels distincts :

Théorème 6 (caractère "sans trou") *Si a, $b \in \mathbb{Q}$, $a < b$, il existe $c \in \mathbb{Q}$ tel que $a < c < b$.*

Il n'y a donc pas de "rationnels consécutifs", de "premier rationnel > 0" etc.

2.3 Une lacune de $\mathbb{Q}$

Considérons l'ensemble $A = \{r \in \mathbb{Q} \,|\, r^2 < 2\}$ ([3]). A est assurément non vide ($0, 1 \in A$) ; A est majoré (par 10, par 2...). Cependant on peut montrer que si M est un majorant de A dans $\mathbb{Q}$, il existe toujours $M' < M$ tel que M' majore A : A n'admet pas de *plus petit majorant.*

Exercice 1 *Montrer que l'on peut poser $M' = M - \frac{1}{n}$ pour un entier n bien choisi. Montrer par le même principe que A n'admet pas de plus grand élément dans $\mathbb{Q}$.*

L'ensemble des réels vient pallier, entre autres, ce défaut des rationnels.

3 Réels

On admet l'existence d'un ensemble noté $\mathbb{R}$ (contenant $\mathbb{Q}$), dont les éléments sont les *réels*, vérifiant les conditions

[$\mathbb{R}$1] $(\mathbb{R}, +, \times)$ est un *corps commutatif* comme $\mathbb{Q}$.

[$\mathbb{R}$2] $\mathbb{R}$ est un *corps ordonné* : il possède d'une relation d'ordre *totale* $\leq$, compatible avec $+$ et $\times$ *sur* $\mathbb{R}_+$.

[$\mathbb{R}$3] **(propriété de la borne supérieure)** Toute partie non vide majorée de $\mathbb{R}$ admet une *borne supérieure* dans $\mathbb{R}$. (voir définition 4).

Aucune clause de minimalité n'est nécessaire dans cette caractérisation de $\mathbb{R}$. Une seule structure peut réunir l'ensemble des propriétés demandées.

Les opérations et la relation d'ordre de $\mathbb{R}$ sont des extensions de celles de $\mathbb{Q}$.

Définition 4 *Si $A \subset \mathbb{R}$, $A \neq \varnothing$, majorée, la* borne supérieure *de A est le plus petit élément de l'ensemble des majorants de A.*

Elle est donc unique (en tant que plus petit élément d'un ensemble). On la note $\sup(A)$.

Exemple 2 $\sup(\mathbb{R}_-) = 0$ *;* $\sup(\mathbb{R}_-^*) = 0$.

La borne supérieure de A n'a donc aucune raison d'appartenir à A, par conséquent elle peut exister même dans le cas d'une partie qui n'admet pas de plus grand élément. Cependant, lorsque ce dernier existe, c'est aussi la borne supérieure de A :

Proposition 3 *Si $A \subset \mathbb{R}$, $A \neq \varnothing$ et si A est majorée dans $\mathbb{R}$, alors A admet un plus grand élément* ssi $\sup(A) \in A$, *auquel cas* $\max(A) = \sup(A)$.

On peut caractériser ainsi la borne supérieure d'une partie non vide A de $\mathbb{R}$:

Proposition 4 *M est la borne supérieure de A* ssi

1. *M est un majorant de A et*
2. *$\forall \varepsilon > 0$, $\exists x \in A$, $M - \varepsilon < x$.*

[3] Dans $\mathbb{R}$, A serait simplement l'intervalle ouvert $]-\sqrt{2}, \sqrt{2}[$. Mais il ne faut pas perdre de vue que 2 n'est le carré d'aucun *rationnel.*

De la propriété de la borne supérieure, on *déduit* (sans hypothèse supplémentaire) une version pour les minorants :

Proposition 5 *Toute partie non vide minorée de $\mathbb{R}$ admet une borne inférieure dans $\mathbb{R}$, càd un plus grand minorant.*

La borne inférieure d'une partie A se note $\inf(A)$.

Des résultats analogues aux propositions 3. et 4. existent pour les bornes inférieures :

Proposition 6 *Si $A \subset \mathbb{R}$, $A \neq \varnothing$ et si A est minorée dans $\mathbb{R}$, alors A admet un plus petit élément* ssi $\inf(A) \in A$, *auquel cas* $\min(A) = \inf(A)$.

On peut caractériser de même la borne inférieure d'une partie non vide A de $\mathbb{R}$:

Proposition 7 *m est la borne inférieure de A* ssi

1. *m est un minorant de A et*
2. *$\forall \varepsilon > 0$, $\exists x \in A$, $x < m + \varepsilon$.*

$\mathbb{R}$ conserve le caractère archimédien de $\mathbb{Q}$:

Théorème 7 $\mathbb{R}$ *est archimédien.*

Ceci permet de reconduire sur $\mathbb{R}$ les définitions de la partie entière et de partie décimale données pour $\mathbb{Q}$.

3.1 Intervalles de $\mathbb{R}$

Définition 5 *Un* intervalle *de $\mathbb{R}$ est une partie de $\mathbb{R}$ de l'une des formes suivantes :*

- $[a, b] = \{x \in \mathbb{R} \,|\, a \leq x \leq b\}$ *;*
- $[a, b[= \{x \in \mathbb{R} \,|\, a \leq x < b\}$ *;*
- $]a, b] = \{x \in \mathbb{R} \,|\, a < x \leq b\}$ *;*
- $]a, b[= \{x \in \mathbb{R} \,|\, a < x < b\}$ *;*
- $[a, +\infty[= \{x \in \mathbb{R} \,|\, a \leq x\}$ *;*
- $]a, +\infty[= \{x \in \mathbb{R} \,|\, a < x\}$ *;*
- $]-\infty, b] = \{x \in \mathbb{R} \,|\, x \leq b\}$ *;*
- $]-\infty, b[= \{x \in \mathbb{R} \,|\, x < b\}$ *;*
- $]-\infty, +\infty[= \mathbb{R}$.

On remarque que $\mathbb{R}$ est un intervalle, de même que $\varnothing$ ($= [a, a[$ pour tout a) et les singletons ($\{a\} = [a, a]$).

Pour manipuler commodément les intervalles sans avoir à distinguer de multiples cas, il serait pratique de disposer d'une caractérisation unique. La solution est fournie par la notion de partie convexe.

3.2 Convexes de $\mathbb{R}$

Définition 6 *Une partie $\mathcal{C}$ de $\mathbb{R}$ est* convexe *si :*

$$\text{pour tous } a,\ b \in \mathcal{C},\ [a,b] \subset \mathcal{C}.$$

Exemple 3

- *$\varnothing$; les singletons ;*
- *$\mathbb{R}$;*
- *plus généralement, tous les intervalles de $\mathbb{R}$.*

Ce dernier exemple ne peut pas être étendu, puisque la convexité est en fait une propriété caractéristique des intervalles de $\mathbb{R}$:

Théorème 8 *Les convexes de $\mathbb{R}$ sont les intervalles de $\mathbb{R}$.*

3.3 Densité de $\mathbb{Q}$ et $\mathbb{R} - \mathbb{Q}$

On montre facilement que $\mathbb{R}$ est sans trou, au même titre que $\mathbb{Q}$, en tant que corps ordonné archimédien. Mais on peut être plus précis :

Proposition 8 *Pour tous $a,\ b \in \mathbb{R}$, $a < b$, il existe $r \in \mathbb{Q}$ tel que $a < r < b$.*

On dit que $\mathbb{Q}$ est *dense* dans $\mathbb{R}$. Il en est de même de l'ensemble $\mathbb{R} - \mathbb{Q}$ des nombres irrationnels.

Proposition 9 *Pour tous $a,\ b \in \mathbb{R}$, $a < b$, il existe $\omega \in \mathbb{R} - \mathbb{Q}$ tel que $a < \omega < b$.*

Les ensembles (infinis) $\mathbb{Q}$ et $\mathbb{R} - \mathbb{Q}$ sont ainsi imbriqués l'un dans l'autre. Il ne faudrait pas tenter d'en déduire qu'ils ont le même cardinal. $\mathbb{Q}$ est dénombrable, ce qui signifie qu'il a le même cardinal que $\mathbb{N}$, noté $\aleph_0$ ([4]). Si $\mathbb{R} - \mathbb{Q}$ l'était également, $\mathbb{R}$ le serait aussi. Or le cardinal de $\mathbb{R}$, noté $\aleph_1$, est strictement plus grand que $\aleph_0$.

Du point de vue de la structure, $\mathbb{R} - \mathbb{Q}$ ne possède aucune propriété particulière. Tout au plus peut on remarquer que

- si $r \in \mathbb{Q}$ et $\omega \in \mathbb{R} - \mathbb{Q}$, $r + \omega \in \mathbb{R} - \mathbb{Q}$;
- si $r \in \mathbb{Q}^*$ et $\omega \in \mathbb{R} - \mathbb{Q}$, $r\,\omega \in \mathbb{R} - \mathbb{Q}$.

3.4 Valeurs décimales approchées d'un réel

Les *nombres décimaux* sont les rationnels qui *peuvent s'écrire* sous la forme $\frac{a}{10^n}$ où $a \in \mathbb{Z}$, $n \in \mathbb{N}$.

Exemple 4 1, $\frac{3}{100}$, $\frac{1}{5}$ *mais pas* $\frac{1}{6}$, $\frac{2}{3}$...

Notation 3 *On note $\mathbb{D}$ l'ensemble des décimaux.*

Remarque 1 *On observe facilement (cf. "propriétés des quotients") que la somme, le produit de nombres décimaux sont des décimaux. Par contre, l'inverse d'un décimal non nul n'appartient pas forcément à $\mathbb{D}$.*

[4] Lire *aleph-zéro*. $\aleph$ est la première lettre de l'alphabet hébraïque, et celle qu'a choisie CANTOR pour désigner le cardinal de $\mathbb{N}$, le plus petit cardinal infini.

Soit x un nombre réel. Soit $n \in \mathbb{N}$.

Lemme 1 *Il existe un unique $p \in \mathbb{Z}$ tel que*

$$\frac{p}{10^n} \leq x < \frac{p+1}{10^n}.$$

Preuve. $p = E\left(10^n x\right)$. ■

Définition 7 *On pose alors $p = a_n\left(x\right)$ et*

$$u_n(x) = \frac{a_n(x)}{10^n} \text{ et } v_n(x) = \frac{1 + a_n(x)}{10^n}$$

*$u_n\left(x\right)$ (*resp. *$v_n\left(x\right)$) est la* valeur décimale approchée par défaut *(*resp. par excès*)* à 10^{-n} près de *x.*

$u_n\left(x\right)$ et $v_n\left(x\right)$ sont caractérisés par les conditions suivantes :

- $u_n\left(x\right)$, $v_n\left(x\right)$ sont des décimaux de la forme $\frac{a}{10^n}$;
- $u_n\left(x\right) \leq x < v_n\left(x\right)$;
- $v_n\left(x\right) - u_n\left(x\right) = \frac{1}{10^n}$.

Il résulte de cette construction que tout nombre réel peut être approché arbitrairement près par des *décimaux*, autrement dit, au même titre que $\mathbb{Q}$ et $\mathbb{R} - \mathbb{Q}$:

Proposition 10 *$\mathbb{D}$ est* dense *dans $\mathbb{R}$.*

Ainsi, non seulement entre deux réels quelconques on peut toujours trouver un rationnel, mais on peut même supposer si nécessaire que celui-ci est un décimal.

3.5 Droite numérique achevée $\overline{\mathbb{R}}$

On choisit deux objets n'appartenant pas à $\mathbb{R}$ (il en existe) qu'on note $-\infty$ et $+\infty$. On pose

$$\overline{\mathbb{R}} = \mathbb{R}\ \cup\ \{-\infty, +\infty\}.$$

On étend à $\overline{\mathbb{R}}$ la relation d'ordre de $\mathbb{R}$ en convenant que $-\infty < x < +\infty$ pour tout réel x.

Ainsi, $-\infty$ (*resp.* $+\infty$) est le plus petit (*resp.* plus grand) élément de $\overline{\mathbb{R}}$, et minore (*resp.* majore) toute partie de $\mathbb{R}$. Ceci permet de donner une formulation "universelle" à la propriété de la borne supérieure :

Théorème 9 *Soit A une partie non vide de $\mathbb{R}$. Alors A admet une borne supérieure* dans *$\overline{\mathbb{R}}$:*

- $\sup\left(A\right) \in \mathbb{R}$ ssi *A est majorée dans $\mathbb{R}$;*
- $\sup\left(A\right) = +\infty$ ssi *A n'est pas majorée dans $\mathbb{R}$.*

On a bien sûr un énoncé analogue pour les bornes inférieures :

Théorème 10 *Soit A une partie non vide de $\mathbb{R}$. Alors A admet une borne inférieure* dans *$\overline{\mathbb{R}}$:*

- $\inf\left(A\right) \in \mathbb{R}$ ssi *A est minorée dans $\mathbb{R}$;*
- $\inf\left(A\right) = -\infty$ ssi *A n'est pas minorée dans $\mathbb{R}$.*