Ensembles de nombres

lundi 11 février

Table des matières

1 L'ensemble Z des entiers relatifs

L'ensemble $\mathbf{N}$ n'est pas un groupe pour l'addition (seul 0 est opposable) : quand on rajoute[1] à $\mathbf{N}$ les opposés de ses éléments, on obtient l'ensemble[2] $\mathbf{Z}$ dont les éléments sont appelés ***entiers relatifs***. Ainsi, on a "par construction"

$$\mathbf{Z} = \mathbf{N} \cup (-\mathbf{N}) \qquad \text{(admis)},$$

ce qui s'écrit aussi

$$\begin{aligned} \forall n &\in \mathbf{N},\ (n \in \mathbf{Z} \text{ et } -n \in \mathbf{Z}) && \text{(traduit l'inclusion } \mathbf{N} \cup -\mathbf{N} \subset \mathbf{Z}) \\ \forall z &\in \mathbf{Z},\ \exists n \in \mathbf{N},\ (z = n \text{ ou } z = -n) && \text{(traduit l'inclusion } \mathbf{Z} \subset \mathbf{N} \cup -\mathbf{N}). \end{aligned}$$

On prolonge à $\mathbf{Z}$ les addition, multiplication et ordre de $\mathbf{N}$. La plupart des propriétés sont conservées. CEPENDANT :

★ pour a et b dans $\mathbf{Z}$, l'entier relatif a^b n'a pas toujours de sens si $b < 0$ (par exemple, $2^{-1} \notin \mathbf{Z}$) ;

★ faire attention aux *signes* quand on multiplie des comparaisons (par exemple, on a $-1 \leq 0$ mais $(-1)^2 \not\leq 0^2$) ;

★ on *n*'a *pas* l'équivalence $\forall (a, b) \in \mathbf{Z}^2,\ a \leq b \not\Leftrightarrow \exists z \in \mathbf{Z},\ b = a + z$; en revanche on a toujours l'équivalence

$$\forall (a, b) \in \mathbf{Z}^2,\ a \leq b \Longleftrightarrow \exists n \in \mathbf{N},\ b = a + n\,;$$

★★ $\mathbf{Z}$ est un groupe additif ;

★★★ toute partie de $\mathbf{Z}$ non vide *minorée* admet un plus petit élément (sans l'hypothèse de minoration, $-\mathbf{N}$ est une partie non vide de $\mathbf{Z}$ sans plus petit élément) ;

de même, toute partie non vide *majorée* admet un plus grand élément (sans l'hypothèse de majoration, $\mathbf{N}$ est une partie non vide de $\mathbf{Z}$ sans plus grand élément).

Corollaire / définition (partie entière). *Soit a un réel. Il existe un unique entier relatif, noté $\lfloor a \rfloor$ ou $E(a)$ et appelé* ***partie entière***[3] *de a, tel que $\lfloor a \rfloor \leq a < \lfloor a \rfloor + 1$.*

Démonstration. Les comparaisons souhaitées $\lfloor a \rfloor \leq a < \lfloor a \rfloor + 1$ disent que $\lfloor a \rfloor$ est le plus grand entier relatif inférieur ou égal à a. Il est donc naturel d'introduire l'ensemble $E := \{z \in \mathbf{Z}\ ;\ z \leq a\}$. C'est une partie

[1] la description et la légitimation de ce rajout sont hors programme
[2] de l'allemand "Zahl" signifiant "nombre"
[3] On pourrait définir une autre partie entière de a comme étant le plus petit entier $\lceil a \rceil$ supérieur ou égal à a. Elle serait caractérisée par les comparaisons $\lceil a \rceil - 1 < a \leq \lceil a \rceil$.

de $\mathbf{Z}$, non vide (admis), majorée (par a), donc admet un plus grand élément $M := \max E$. Puisque $M \in E$, on a $M \leq a$; si l'on n'avait pas $a < M+1$, on aurait $M+1 \leq a$, d'où $M+1 \in E$, ce qui imposerait $M+1 \leq \max E = M$, d'où une contradiction. (On admet l'unicité –> exercice !)

On retiendra les équivalences (pour tout réel a et pour tout entier relatif k)

$$k = \lfloor a \rfloor \iff k \leq a < k+1$$
$$a \in \mathbf{Z} \iff a = \lfloor a \rfloor .$$

Arithmétique.

Définition (divisibilité). *Soient $(d,m) \in \mathbf{Z}^2$. On dit que d **divise** m ou que d est un **diviseur** de m ou que m est divisible par d ou que m est un **multiple** de d si m est le produit de d par un entier relatif : on note alors*

$$d \mid m \overset{\text{déf.}}{\iff} \exists k \in \mathbf{Z},\ m = kd.$$

Remarque. L'entier 0 est divisible par tous les entiers puisque $\forall a \in \mathbf{Z},\ 0 = 0a$.

Remarque. Soit $a \in \mathbf{Z}$. Alors 1 et a sont toujours des diviseurs de a. Le cas où il n'y a qu'eux deux motive la définition suivante.

Définition (nombre premier). *Soit $p \in \mathbf{N}$. On dit que p est **premier** s'il possède exactement deux diviseurs positifs (qui sont alors nécessairement 1 et p).*

Exemples. Les premiers nombres premiers sont

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37...$$

★ les entiers 0 et 1 ne sont pas premiers car 0 admet une infinité de diviseurs et 1 n'en admet qu'un seul positif.

Théorème (décomposition en facteur premier) (admis) *Tout entier naturel non nul est un produit de nombres premiers, avec unicité des facteurs à l'ordre près.*

Exemples. Un algorithme a été vu en T. G. : $18 = 2 \cdot 3^2$, $42 = 2 \cdot 3 \cdot 7$.

Remarque. L'entier 1 est produit de zéro nombres premiers.

2 L'ensemble Q des nombres rationnels

L'ensemble $\mathbf{Z}^*$ n'est pas un groupe pour $\times$ (seul ± 1 sont inversibles) : quand on rajoute[4] à $\mathbf{Z}$ les inverses de ses éléments non nuls puis les produits d'entiers avec des inverses d'entiers, on obtient l'ensemble[5] $\mathbf{Q}$ dont les éléments sont appelés ***nombres rationnels***[6]. Ainsi, on a "par construction"

$$\mathbf{Q} = \left\{ \frac{n}{d} \ ;\ n \in \mathbf{Z},\ d \in \mathbf{N}^* \right\} \qquad \text{(admis)}$$

(on peut prendre le dénominateur[7] dans $\mathbf{N}$ au lieu de $\mathbf{Z}$ en envoyant l'éventuel signe dans le numérateur[8]).

On prolonge à $\mathbf{Q}$ les addition, multiplication et ordre de $\mathbf{Z}$. On rappelle au besoin les égalités

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad \text{et} \qquad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd} \qquad \begin{array}{c}\text{(où } a,b,c,d \text{ sont des entiers} \\ \text{avec } b \text{ et } d \text{ non nuls)}\end{array} .$$

La plupart des propriétés sont conservées. CEPENDANT :

[4] la description et la légitimation de ce rajout sont hors programme

[5] "Q" comme "quotient", au sens de "fraction"

[6] La mot "rationnel" vient du latin "*ratio*" qui signifie "mesure" ou "comparaison" et qui a donné "raison", "rapport" et "quotient".

[7] ce qui *dénomme* : regardons-nous des tiers ? des quarts ? des dix-huitièmes ?

[8] le *nombre* de choses (cinquièmes, quarante-deuxièmes...) dénommées par le dénominateur

★ étant données deux fractions f et g dans $\mathbf{Q}$, le rationnel f^g n'a pas toujours de sens si $g \notin \mathbf{Z}$ (par exemple, $2^{\frac{1}{2}}$ dénote l'irrationnel[9] $\sqrt{2}$) ;

★ toute partie majorée *n'*admet *pas toujours* un plus grand élément (par exemple, l'intervalle $[0,1[$ ou la partie $\{r \in \mathbf{Q} \; ; \; r^2 < 2\}$) ;

★ toute partie minorée *n'*admet *pas toujours* un plus petit élément (par exemple, si la partie $\mathbf{Q}_+^*$ admettait un plus petit élément m, alors on aurait d'une part $\frac{m}{2} \in \mathbf{Q}_+^*$, d'autre part $\frac{m}{2} < m = \min \mathbf{Q}_+^*$, d'où une contradiction) ;

★ on *n'*a *plus* l'équivalence $\forall (a,b) \in \mathbf{Q}^2, \; a < b \not\Leftrightarrow a \leq b - 1$ (par exemple, remplacer a par 0 et b par $\frac{1}{2}$) :

deux rationnels peuvent être arbitrairement proches

(dans la même veine, on *n'*a *plus* l'équivalence $\forall (a,b) \in \mathbf{Q}^2, \; a \leq b \not\Leftrightarrow \exists n \in \mathbf{N}, \; b = a + z$).

Proposition. *Tout intervalle de longueur*[10] *strictement plus grande que* 1 *contient un entier.*

Démonstration. Soient $a < b$ deux rationnels tels que $b - a > 1$.

[dessin] Si $b \notin \mathbf{Z}$, alors on a $\lfloor b \rfloor < b$; ayant par ailleurs $\lfloor b \rfloor > b - 1 > a$, on a trouvé un entier $\lfloor b \rfloor$ dans l'intervalle $]a,b[$ (donc dans les trois autres intervalles de mêmes "bornes").

[dessin] Sinon, on a $a < b - 1 = \lfloor b \rfloor - 1 < b$ et l'entier $\lfloor b \rfloor - 1$ convient.

3 L'ensemble R des nombres réels

L'ensemble $\mathbf{Q}$ n'est pas "complet", certaine parties n'ont pas de plus petit ou plus grand élément. Quand on rajoute[11] ces *extrema*, on obtient l'ensemble $\mathbf{R}$ dont les éléments sont appelés ***nombres réels***[12]. On pourra ainsi visualiser l'ensemble des réels comme la droite des rationnels dans laquelle on a bouché tous les "trous". [dessin]

Précisons cette notion de complétude.

3.1 Bornes supérieures & inférieures

Définitions (majoration, minoration). Soit A une partie de $\mathbf{R}$.

*Un **majorant** de A est un réel M tel que $\forall a \in A, \; a \leq M$. On dit que A est **majorée** s'il existe un majorant de A.*

*Un **maximum** de A est un majorant de A qui appartient à A, un **plus grand élément** de A est un élément de A qui majore A (c'est la même chose).*

*Un **minorant** de A est un réel m tel que $\forall a \in A, \; m \leq a$. On dit que A est **minorée** s'il existe un minorant de A.*

*Un **minimum** de A est un minorant de A qui appartient à A, un **plus petit élément** de A est un élément de A qui minore A (c'est la même chose).*

*Un **extremum**[13] (de A) est un maximum (de A) ou un minimum (de A).*

Exemples.

42 majore $\left[0, \sqrt{2}\right]$;

-18 minore $\mathbf{N}$;

$\{42^n \; ; \; n \in \mathbf{Z}\}$ n'est pas majorée ;

---

[9] Selon l'école pythagoricienne, les seuls nombres que notre *raison* peut comprendre s'obtiennent à partir des entiers naturels (à l'aide des opérations usuelles) ; le fait que $\sqrt{2}$ déroge à cette règle montre en quoi il défie notre raison, en quel sens il est "irrationnel".

[10] *cf.* section *Intervalles* pour une définition de longueur et d'intervalle

[11] la description et la légitimation de ce rajout sont hors programme

[12] Le terme "réel" apparaît sous la plume de Descartes dans *La Géométrie* (1637) par opposition à "imaginaire" (Descartes parlait de racines de polynômes). Un nombre réel est donc à l'origine un nombre qui n'est pas "impossible" : le champ de possibles reste large !

[13] Rappelons que le pluriel d'"extremum" est "*extrema*" (certains dictionnaires tolèrent cependant le pluriel avec un "s"). Il en va de même pour "maximum" et "minimum".

la partie vide $\emptyset$ est majorée et minorée par n'importe quoi (puiqu'un énoncé de la forme $\forall a \in \emptyset,\ P(a)$ est toujours vrai).

Proposition (unicité des *extrema*). *Une partie de* $\mathbf{R}$ *ne peut admettre qu'un plus un maximum (resp. minimum).*

Démonstration. Soit $A \subset \mathbf{R}$, soient M et M' deux maxima de A. Puisque M' majore A, il majore tous les éléments de A, en particulier M, d'où $M \leq M'$; par symétrie, on a la comparaison dans l'autre sens, d'où l'égalité $M = M'$.

Notation. Soit $A \subset \mathbf{R}$. Si A possède un minimum (resp. maximum), ce dernier sera noté $\min A$ (resp. $\max A$).

Exemples.
$[0,1]$ possède un minimum (0) et un maximum (1) ;
$]0,1]$ possède un maximum mais pas de minimum ;
$]0,1[$ ne possède ni minimum ni maximum
Ces exemples montrent que les notions de minimum et maximum ne captent pas ce que l'on aimerait (il est frustant que 0 ne soit pas le "plus petit élément" de $]0,1[$), ce qui motive la définition suivante.

Définition (bornes supérieure & inférieure). Soit A une partie de $\mathbf{R}$.
On appelle ***borne supérieure*** *(ou* ***supremum****) de* A *le plus petit majorant de* A *(s'il existe ; on le note alors* $\sup A$*).*
On appelle ***borne inférieure*** *(ou* ***infimum****) de* A *le plus grand minorant de* A *(s'il existe ; on le note alors* $\inf A$*).*

MNÉNO : le supremum de A ressemble à un "maximum" qui n'appartient pas forcément à A.

Remarque. Il faut bien comprendre ce changement de point vue du maximum au supremum : au lieu de chercher à atteindre le maximum depuis l'*intérieur* (comme plus grand élément), on atteint le supremum depuis l'*extérieur* (comme plus petit majorant). Le supremum ressemble ainsi à un "maximum" qui n'appartient pas forcément à la partie considérée.

Exemples.
$\sup [0,1[= 1$;
$\sup [0,1] = \max [0,1] = 1$;
si $A \subset \mathbf{R}$ admet un maximum, alors $\sup A$ fait sens et vaut $\max A$;
Si $A \subset \mathbf{R}$ admet un minimum, alors $\inf A$ fait sens et vaut $\min A$.

On peut à présent traduire une conséquence de la "complétion" des rationnels : la "*complétude*" des réels.

Axiome (complétude de R). *Toute partie non vide majorée (resp. minorée) de* $\mathbf{R}$ *admet un supremum (resp. infimum).*

MNÉMO (ordre sur Z). *Toute partie non vide majorée (resp. minorée) de* $\mathbf{Z}$ *admet un maximum (resp. minimum).*

Ce mnémo (qui concerne le monde du *discret*) est là pour penser l'axiome de complétude (qui concerne le monde du *continu*) dans les mêmes termes.

Exemples.
$\sup \left\{ \lambda \in \mathbf{R} \ ; \ \lambda^2 < 2 \right\} = \sqrt{2}$;
$\inf \left\{ \frac{1}{n} \ ; \ n \in \mathbf{N}^* \right\} = 0$.

Proposition (critère pour déterminer un supremum) (admise). *Soient* A *une partie de* $\mathbf{R}$ *et* s *un réel. On a alors l'équivalence*

$$s = \sup A \iff \forall \varepsilon > 0,\ \exists a \in A,\ s - \varepsilon < a \leq s.$$

Mnémo. Pour ne pas mélanger $<$ et $\leq$, prendre $A := \{0,1\}$ et $\varepsilon = \frac{1}{2}$: [dessin] l'égalité est imposible à gauche et la seule possibilité à droite est l'égalité.

Application. *Soient A et B deux parties majorées de* $\mathbf{R}$*. Montrer que* $\sup(A+B) = \sup A + \sup B$.

Démonstration. Notons $\alpha := \sup A$ et $\beta := \sup B$. Soit $E > 0$. Par définition de α et β, il y a un $a \in A$ tel que $\alpha - \frac{E}{2} < a \leq \alpha$ et il y a un $b \in B$ tel que $\beta - \frac{E}{2} < b \leq \beta$ (remplacer ε dans la proposition ci-dessus par $\frac{E}{2}$), d'où (en ajoutant) $(\alpha+\beta) - E < \underbrace{a+b}_{\in A+B} \leq (\alpha+\beta)$, ce qui conclut $\alpha + \beta = \sup(A+B)$ d'après la proposition ci-dessus.

3.2 Droite réelle achevée

L'axiome de complétude garantite que toute partie de $\mathbf{R}$ non vide *majorée* admet un supremum. Afin de lever cette hypothèse, il est agréable d'"achever" l'ordre des réels en rajoutant un maximum ∞ et un minimum $-\infty$.

Définition / notation (achèvement de l'ordre réel). *Soit ∞ un symbole ne dénotant aucun réel. On appelle **droite réelle achevée** l'ensemble*

$$\overline{\mathbf{R}} := \{-\infty\} \cup \mathbf{R} \cup \{\infty\} \qquad \textit{(lire "}\mathbf{R}\textit{ achevé").}$$

On note de même

$$\begin{aligned} \overline{\mathbf{R}}_+ = \overline{\mathbf{R}_+} \quad &: \quad = \mathbf{R}_+ \cup \{\infty\} = \overline{\mathbf{R}} \cap \mathbf{R}_+ \textit{ et} \\ \overline{\mathbf{R}}_- = \overline{\mathbf{R}_-} \quad &: \quad = \{-\infty\} \cup \mathbf{R}_- = \overline{\mathbf{R}} \cap \mathbf{R}_-. \end{aligned}$$

On admet les prolongements à $\mathbf{R}$ des addition, multiplication et ordre de $\mathbf{Q}$.

Défintion (ordre et lois sur $\overline{\mathbf{R}}$).
On prolonge l'ordre réel sur tout $\overline{\mathbf{R}}$ en imposant

$$\forall a \in \mathbf{R}, \ -\infty < a < \infty.$$

On prolonge partiellement l'addition et la multiplication réelles via les tables

$+ \Rsh$	$-\infty$	réel	∞
$-\infty$	$-\infty$	$-\infty$	♠
réel	$-\infty$		∞
∞	♠	∞	∞

et

$\times \Rsh$	$-\infty$	réel < 0	0	réel > 0	∞
$-\infty$	∞	∞	♠	$-\infty$	$-\infty$
réel < 0	∞				$-\infty$
0	♠				♠
réel > 0	$-\infty$				∞
∞	$-\infty$	$-\infty$	♠	∞	∞

(la présence d'un ♠ dans une case signifie que la somme (resp. le produit) ne fait pas sens).

Proposition (admis, *cf* T. G.). *Toute partie de $\overline{\mathbf{R}}$ admet un supremum et un infimum.*

Exemples.
$\inf \emptyset = \infty = \max \overline{\mathbf{R}}$;
$\sup \emptyset = -\infty = \min \overline{\mathbf{R}}$;
si $A \subset \mathbf{R}$ n'est pas majorée, alors $\sup A = \infty$;
si $A \subset \mathbf{R}$ n'est pas minorée, alors $\inf A = -\infty$.

3.3 Intervalles

Définition (intervalles). *Soient a et b dans $\overline{\mathbf{R}}$. On note*

$$\begin{aligned}
[a,b] &: = \left\{x \in \overline{\mathbf{R}}\ ;\ a \leq x \leq b\right\} && \textit{(appelé un \textbf{segment} ou \textbf{intervalle fermé})\,;}\\
[a,b[&: = \left\{x \in \overline{\mathbf{R}}\ ;\ a \leq x < b\right\} && \textit{(appelé un \textbf{intervalle semi-ouvert})\,;}\\
]a,b] &: = \left\{x \in \overline{\mathbf{R}}\ ;\ a < x \leq b\right\} && \textit{(appelé un \textbf{intervalle semi-ouvert})\,;}\\
]a,b[&: = \left\{x \in \overline{\mathbf{R}}\ ;\ a < x < b\right\} && \textit{(appelé un \textbf{intervalle ouvert}).}
\end{aligned}$$

La ***longueur*** *de n'importe lequel de ces quatre intervalles est définie par $b - a$.*

Remarque. Les quatre intervalles exemples ci-dessus ont pour infimum a et pour supremum b.
Remarque. Soit I un intervalle de $\overline{\mathbf{R}}$. Notons $i := \inf I$ et $s := \sup I$. Alors

1. ou bien I est vide (par exemple si $i > s$) ;
2. ou bien I ne contient qu'un seul élément $s = i$;
3. ou bien I contient une infinité d'éléments (ce qui correspond à $i < s$)

★ Le segment $[1,0]$ est vide. Cependant, dans d'autres contextes[14], on pourrait définir

$$[a,b] \stackrel{?}{:=} [\min\{a,b\}, \max\{a,b\}] .$$

Un peu de souplesse est donc conseillée pour éviter les déconvenues.

Proposition (densité de $\mathbf{Q}$ et $\mathbf{R}\backslash\mathbf{Q}$). *Tout intervalle infini contient un rationnel et un irrationnel. (On dit que $\mathbf{Q}$ et $\mathbf{R}\backslash\mathbf{Q}$ sont* ***denses*** *dans $\mathbf{R}$).*

Démonstration. Soient $a < b$ deux réels.
Soit $n \in \mathbf{N}$ tel que $n(b-a) > 1$ (par exemple $n := \left\lfloor \frac{1}{b-a} \right\rfloor + 1 > \frac{1}{b-a}$). [dessin] Alors l'intervalle $]na, nb[$ est de longueur strictement plus grande que 1, donc contient un entier m, donc l'intervalle $]a,b[$ contient le rationnel $\frac{m}{n}$.

En corollaire, l'intervalle $\left]\frac{a}{\sqrt{2}}, \frac{b}{\sqrt{2}}\right[$ contient un rationnel r, donc l'intervalle $]a,b[$ contient $r\sqrt{2}$ qui est irrationnel quand $r \neq 0$ (sinon $\sqrt{2} = \frac{r\sqrt{2}}{r}$ serait rationnel) Si $r = 0$, on applique le même raisonnement à l'intervalle $\left]\frac{a}{\sqrt{2}}, 0\right[\subset \left]\frac{a}{\sqrt{2}}, \frac{b}{\sqrt{2}}\right[$.

[14] comme celui des barycentres